Optimized infrastructure for Unified Communications

Jerome Paquay

Systems Engineer

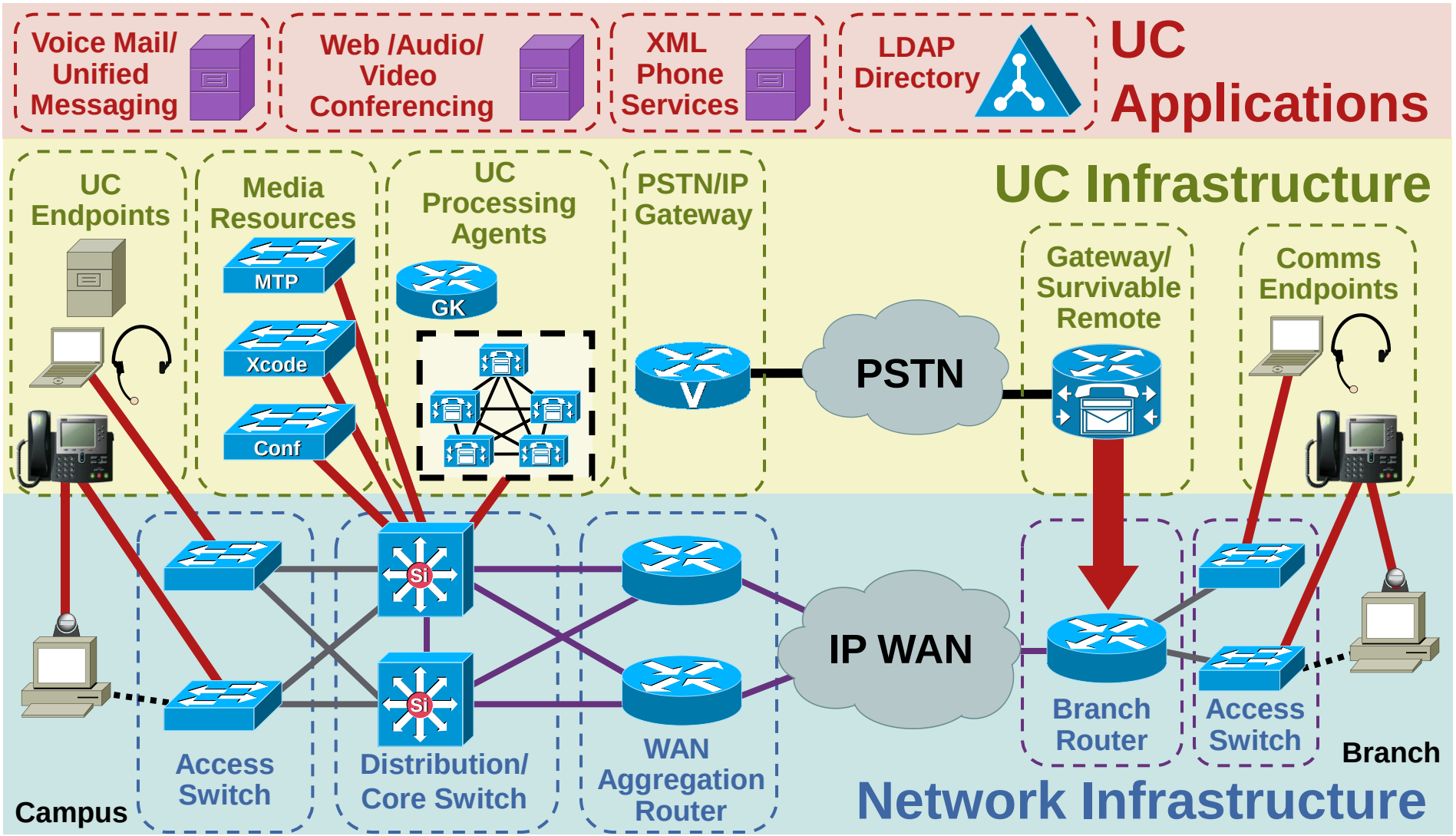
jpa@cisco.com

Agenda

- **Introduction**
- The Campus Network
- QoS considerations
- Trusted Relay Point

= Reference slide

Unified Communications
A layered approach



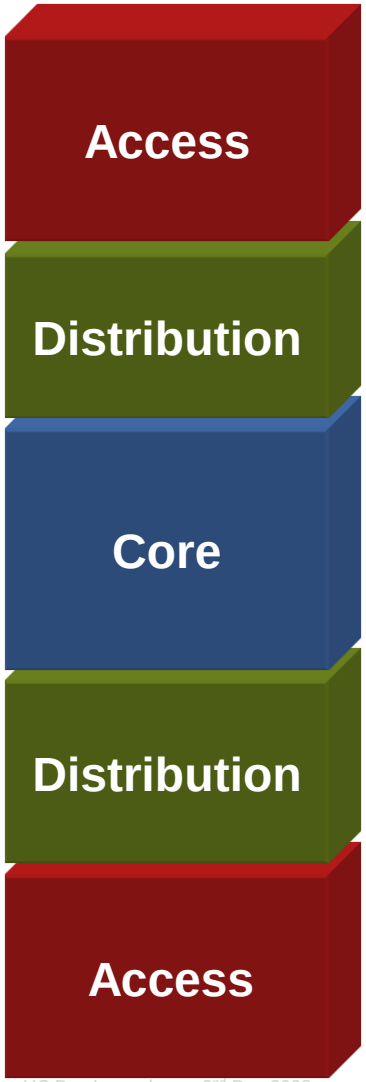
Agenda

- Introduction
- The Campus Network
- QoS considerations
- Trusted Relay Point

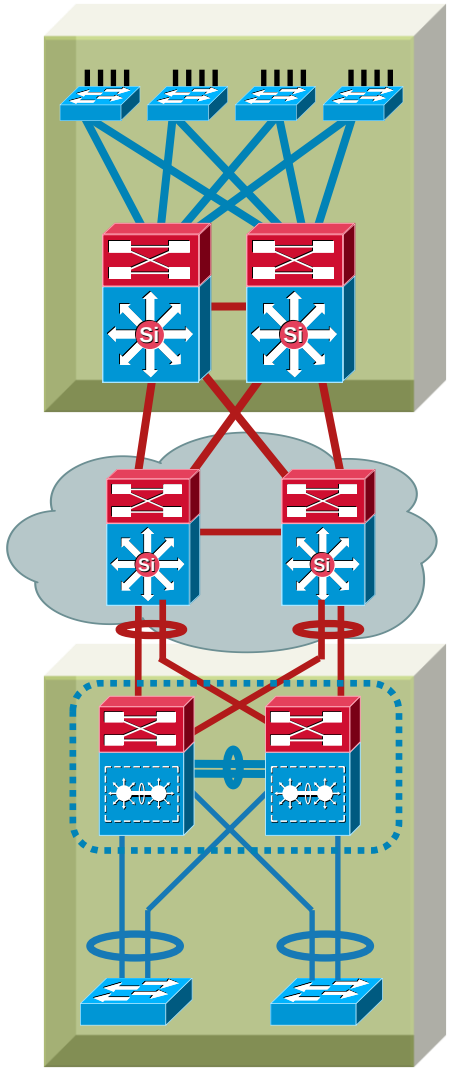
= Reference slide

Campus UC Networks: The Basics Still Apply… Hierarchical Network Design

Without a Rock Solid Foundation the Rest Doesn't Matter



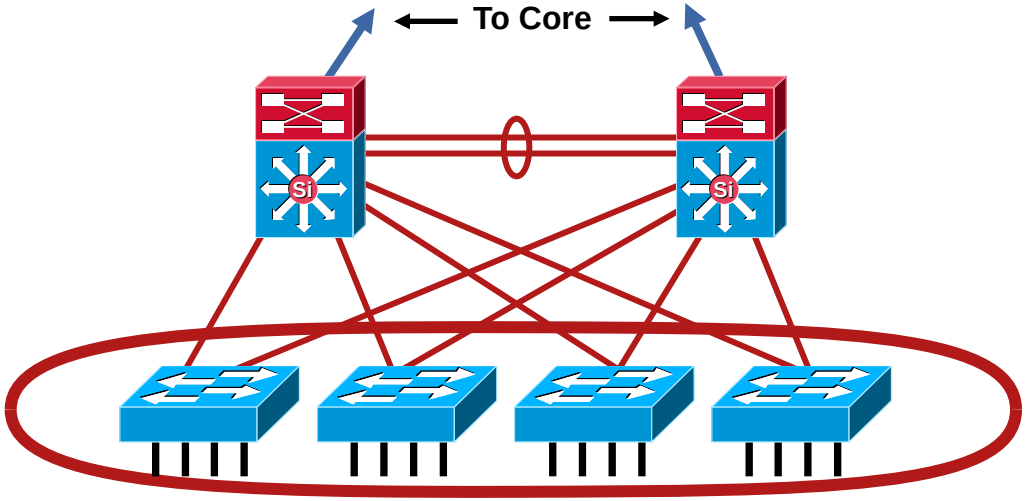
- Access/Distribution/Core hierarchy—each layer has specific role
- Modular scalable topology—building blocks
- Easy to grow, understand, and troubleshoot
- Creates small fault domains—clear demarcations and isolation
- Promotes load balancing and redundancy
- Promotes deterministic traffic patterns
- Incorporates balance of both Layer 2 and Layer 3 technology, leveraging the strength of both
- Utilizes Layer 3 Routing for load balancing, fast convergence, scalability, and control
- Sub-second convergence possible



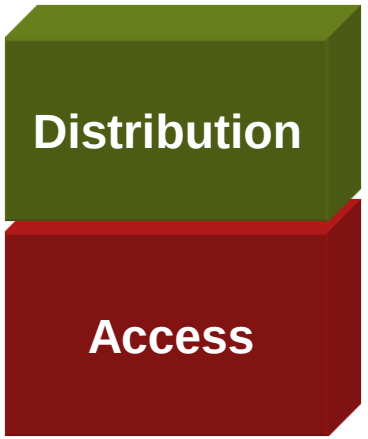
Building Block

Campus UC Networks: The Access Layer

UC Feature Rich Environment—Not Just About Connectivity



VLANS Do Not Span Access Switches



- The Access Layer provides aggregation for Voice, Video and Data endpoints
- Can provide switched or routed access—is typically feature rich…

Key Features for Unified Communications

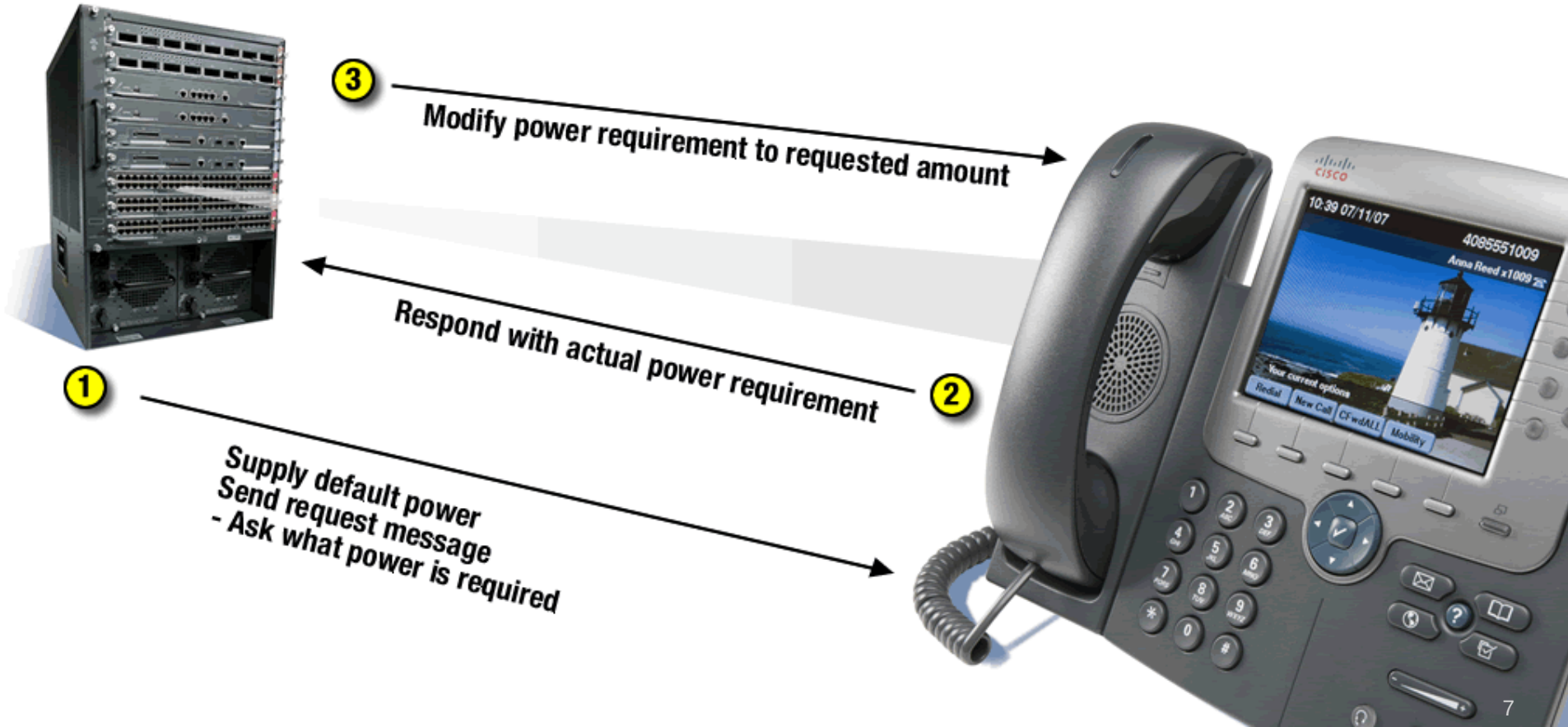
Automatic Phone Discovery
Power over Ethernet
Voice VLAN Allocation
Multiple Security Features
QoS Trust Boundaries
AutoQoS
Queuing
Network Access Control

Campus UC Networks

CDP and Inline Power Discovery

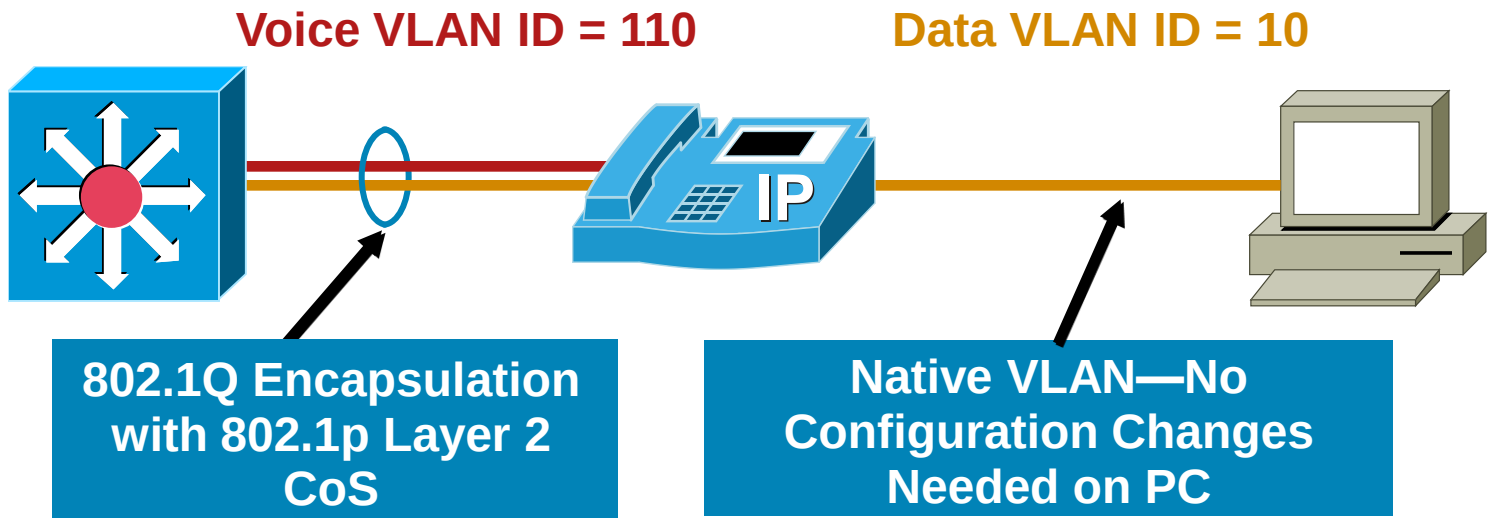
Automated power adjustement
CDP & LLDP

- Cisco Discovery Protocol—allows the switch to discover the attached inline powered device and negotiate the power requirements to optimize power consumption in the switch…



Campus UC Networks:
Voice and Data VLANs

Automated configuration for Voice

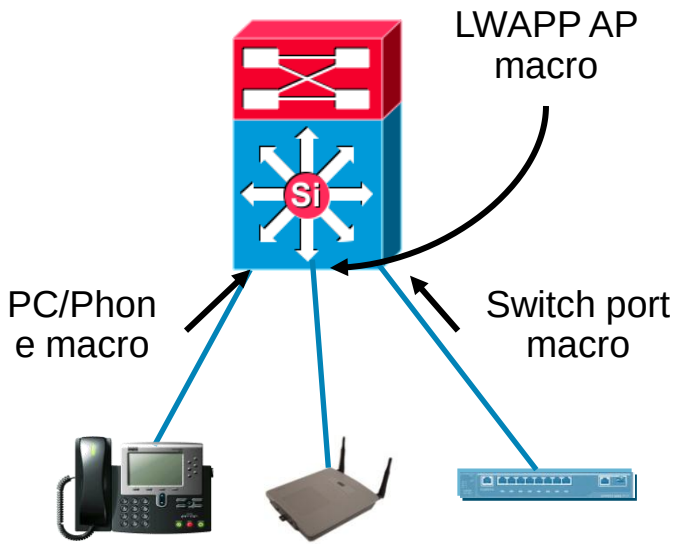


- Separate Voice and Data VLANs create partitioned broadcast domains in separate IP subnets
- Cisco Discovery Protocol (CDP) used during Phone boot up to configure Voice VLAN ID
- Phone also supplied with QoS configuration information
- For Security—different network policies can be applied for different subnets; e.g. WORM attacks can be contained to the Data VLANs

Auto Smartports

Automatic application of smartport macros

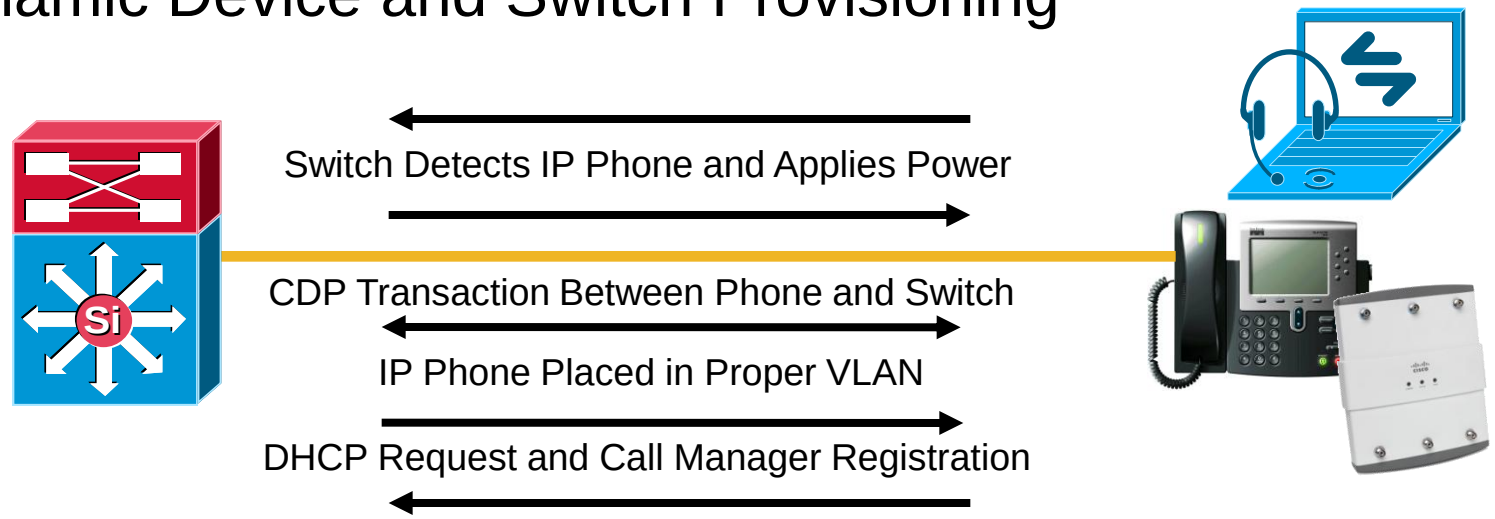
- Smartports first developed to ease the configuration for a variety of switch port types based on Cisco recommended best practices
- Challenges
  - Existing macros tended towards lowest common denominator behaviour in order to minimize the number of potential corner cases
  - Initial implementation utilized the IOS parser to implement a macro capability which meant no “undo” capability
- Updating the implementation to address these issues plus add the ability to dynamically apply a macro based on detection of the device type



Automatic configuration of the access port as devices connect

Summary of UC Network Services

Dynamic Device and Switch Provisioning



- Plug and play provisioning of edge devices (phones and APs) necessary to manage operational overhead

  Power negotiation

  VLAN configuration

  802.1x interoperation

  QoS configuration

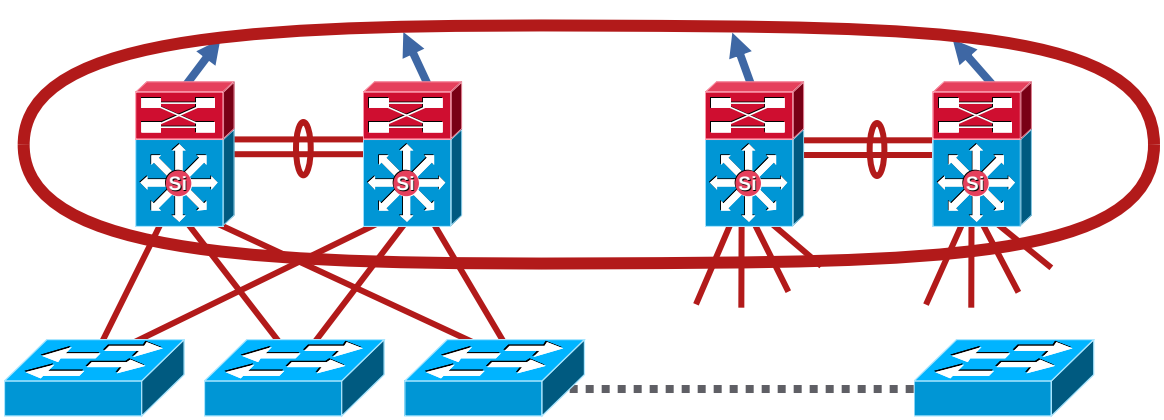
  DHCP

  Call Agent (CCM) or LWAPP registration

The end devices relationship to the network is changing and we need an Intelligence at the edge of the network to be able to support the evolving requirements

Campus UC Networks: The Distribution Layer

Fast Convergence, QoS, and High Availability



- Important considerations for Unified Communications in the Distribution Layer: Sub-Second Convergence, High Availability, Load Balancing, and QoS
- The Distribution Layer uses Layer 3 switching and aggregates wiring closet links (access layer) and uplinks to the core with route summarization
- Protects the core from high density peering and problems in the access layer
- EIGRP/OSPF—sub-second convergence possible with timer adjustment, redundant path load sharing, route summarization,
- HSRP or GLBP to provide first hop redundancy, sub-second convergence possible with timer adjustment

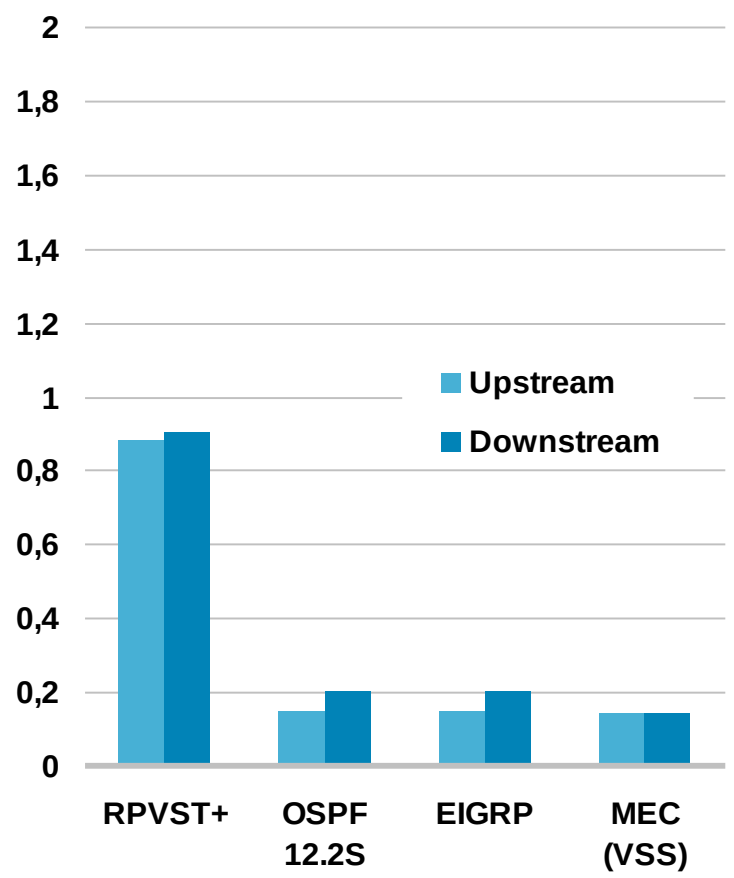
UC Campus Network Design: Routing to the Edge?

Provides Real Advantages for UC Traffic

Both L2 and L3 Can Provide Sub-Second Convergence

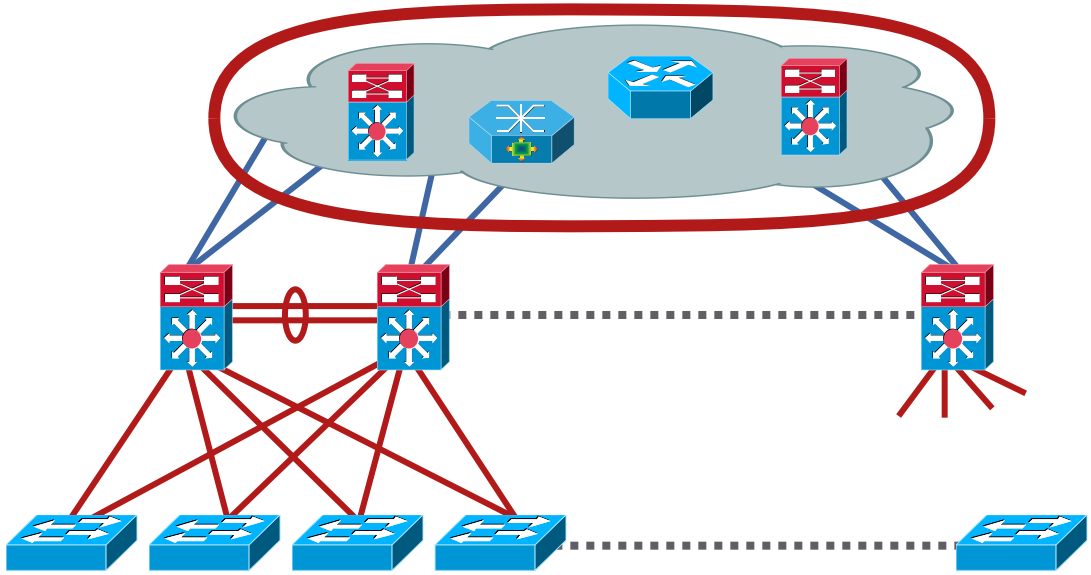
L3 Provides Sub-200 msec Convergence—Highly Desirable for UC

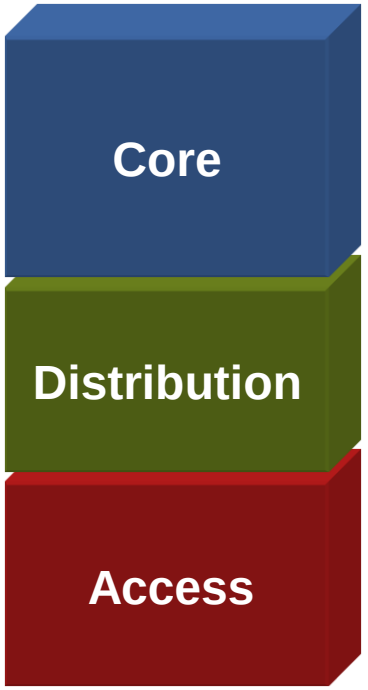
- Easier implement, less to get right
  - No matching of STP/HSRP/GLBP priority
  - No L2/L3 Multicast topology inconsistencies
- Well known tool set
  - traceroute, show ip route, show ip eigrp neighbor, etc.
- Most Cisco Catalyst® switches support L3 Switching
- EIGRP converges in <200 msec
- OSPF with sub-second tuning converges in <200 msec
- RPVST+ convergence times dependent on HSRP tuning
- New features such as VSS also offer great improvements in redundancy and convergence (for both L2 and L3)



Campus UC Networks: The Core Layer

Scalability, High Availability, and Fast Convergence





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

Agenda

- Introduction
- The Campus Network
- **QoS considerations**
- Trusted Relay Point

= Reference slide

QoS in the Campus

Traffic Profiles and Requirements

Voice

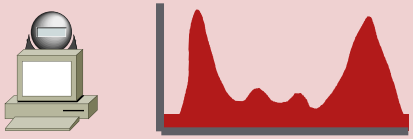
- Smooth
- Benign
- Drop sensitive
- Delay sensitive
- UDP priority

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:

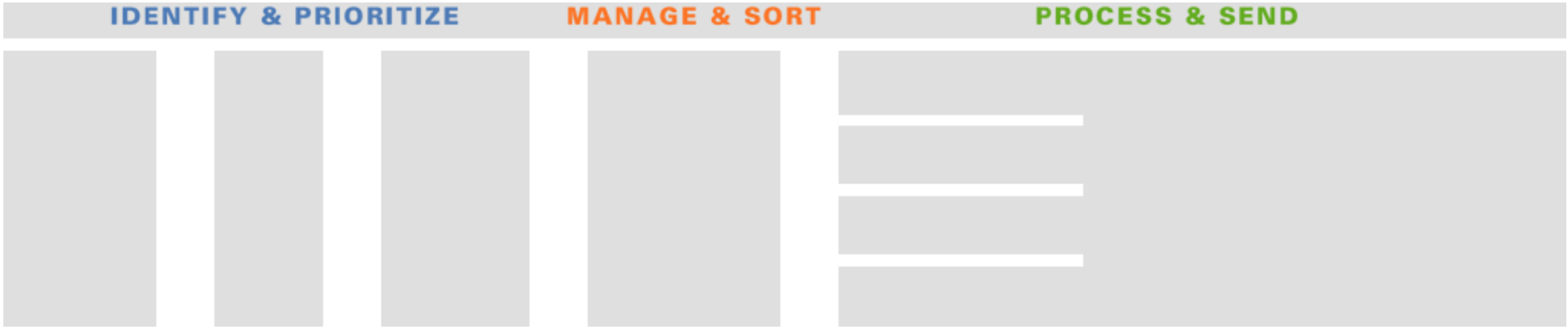
Mission-Critical Apps

Transactional/Interactive Apps

Bulk Data Apps

Best Effort Apps (Default)

The QoS Building Blocks
IETF DiffServ Architecture (RFC2475)

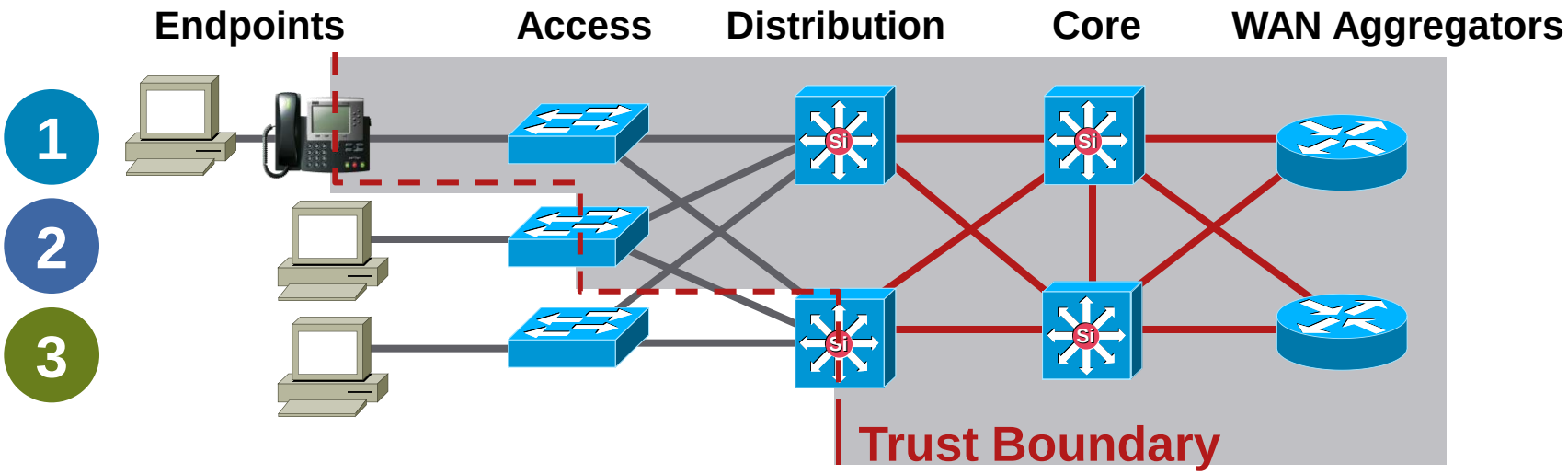


- Defines the mechanisms that control traffic management
- User defines parameters that control the behavior of those mechanisms

Mark or Trust Classify (Scheduling) Queue

Campus QoS Considerations

Establishing Trust Boundaries



For scalability, classification should be done as close to the edge as possible

The outermost trusted devices represent the trust boundary

1. **Optimal Trust Boundary: Trusted Endpoint**
   A device is trusted if it correctly classifies packets
2. **Optimal Trust Boundary: Untrusted Endpoint**
3. **Suboptimal Trust Boundary**
   Only use if access switch cannot perform classification

QoS in the Campus: Switch Port AutoQoS

- AutoQoS allows the application of a pre-defined set of QoS statements to an interface with one CLI command…

AutoQoS in the Campus

AutoQoS Macro Example

For campus Cisco Catalyst switches, AutoQoS command macro enables the following QoS features automatically:

- Enforces a trust boundary at Cisco IP Phones
- Enforces a trust boundary on Cisco Catalyst switch access ports and uplinks/downlinks
- Enables Cisco Catalyst strict priority queuing for voice and weighted round robin queuing for data traffic
- Modifies queue admission criteria (i.e. CoS-to-queue mapping)
- Modifies queue sizes, as well as queue weights where required
- Modifies CoS-to-DSCP and IP precedence to-DSCP mappings

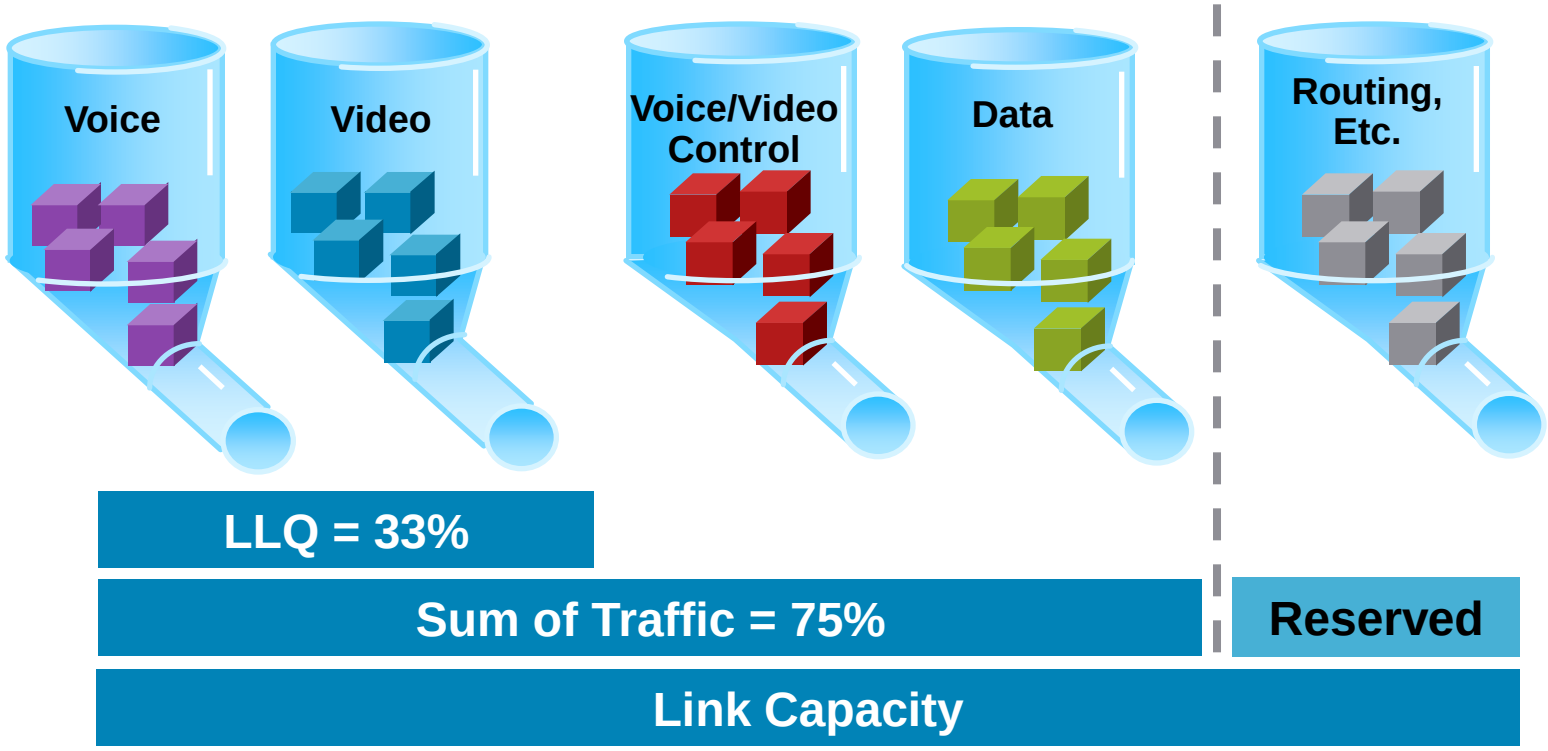
Catalyst (config-if) # auto qos voip cisco-phone

```
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos srr-queue output cos-map queue 1 threshold 3  5
mls qos srr-queue output cos-map queue 2 threshold 3  3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3  2 4
mls qos srr-queue output cos-map queue 4 threshold 2  1
mls qos srr-queue output cos-map queue 4 threshold 3  0
mls qos srr-queue output dscp-map queue 1 threshold 3  40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3  24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3  48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3  56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3  16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3  32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1  8
mls qos srr-queue output dscp-map queue 4 threshold 2  9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3  0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 138 138 92 138
mls qos queue-set output 1 threshold 2 138 138 92 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
mls qos queue-set output 2 threshold 4 42 72 100 242
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
mls qos
!
interface GigabitEthernet0/1
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 queue-set 2
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
```

QoS in the WAN

Bandwidth Provisioning

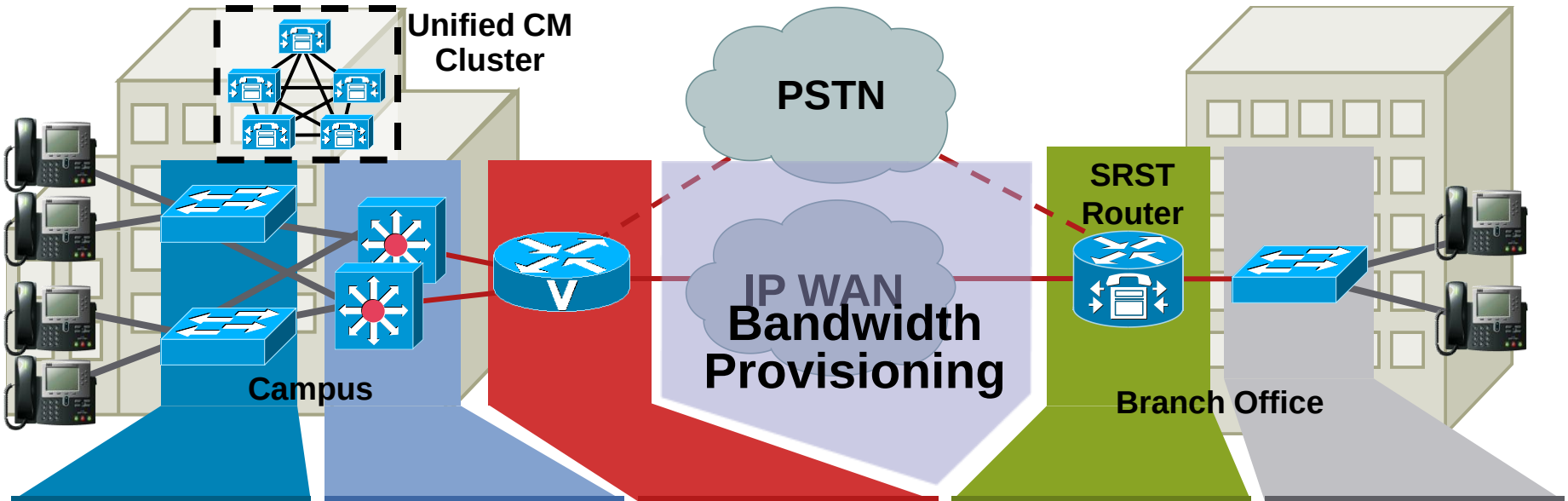
Voice Is Not Free—Especially on Low-Speed Links—Engineer the Network for Data, Voice, and Video



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

Enabling QoS

Overall QoS Design Summary



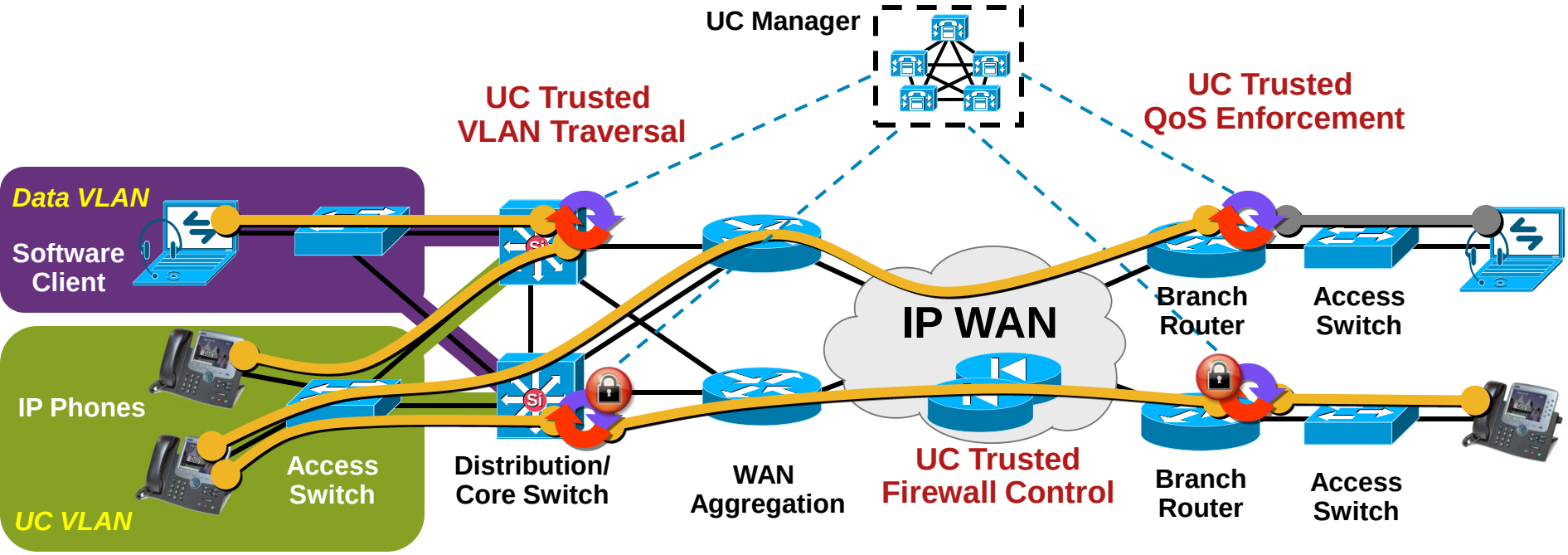
Campus Access	Campus Distribution	WAN Aggregation	Branch Router	Branch Switch
Inline power Multiple Qs 802.1p/Q Fast link Convergence	Multiple Qs 802.1p/Q Classification Reclassification	Multiple Qs 802.1p/Q Traffic Shaping Link Efficiency (LFI, cRTP) Classification Reclassification	Multiple Qs 802.1p/Q Link Efficiency (LFI, cRTP) Classification Reclassification	Inline Power Multiple Qs 802.1p/Q

Agenda

- Introduction
- The Campus Network
- QoS considerations
- **Trusted Relay Point**

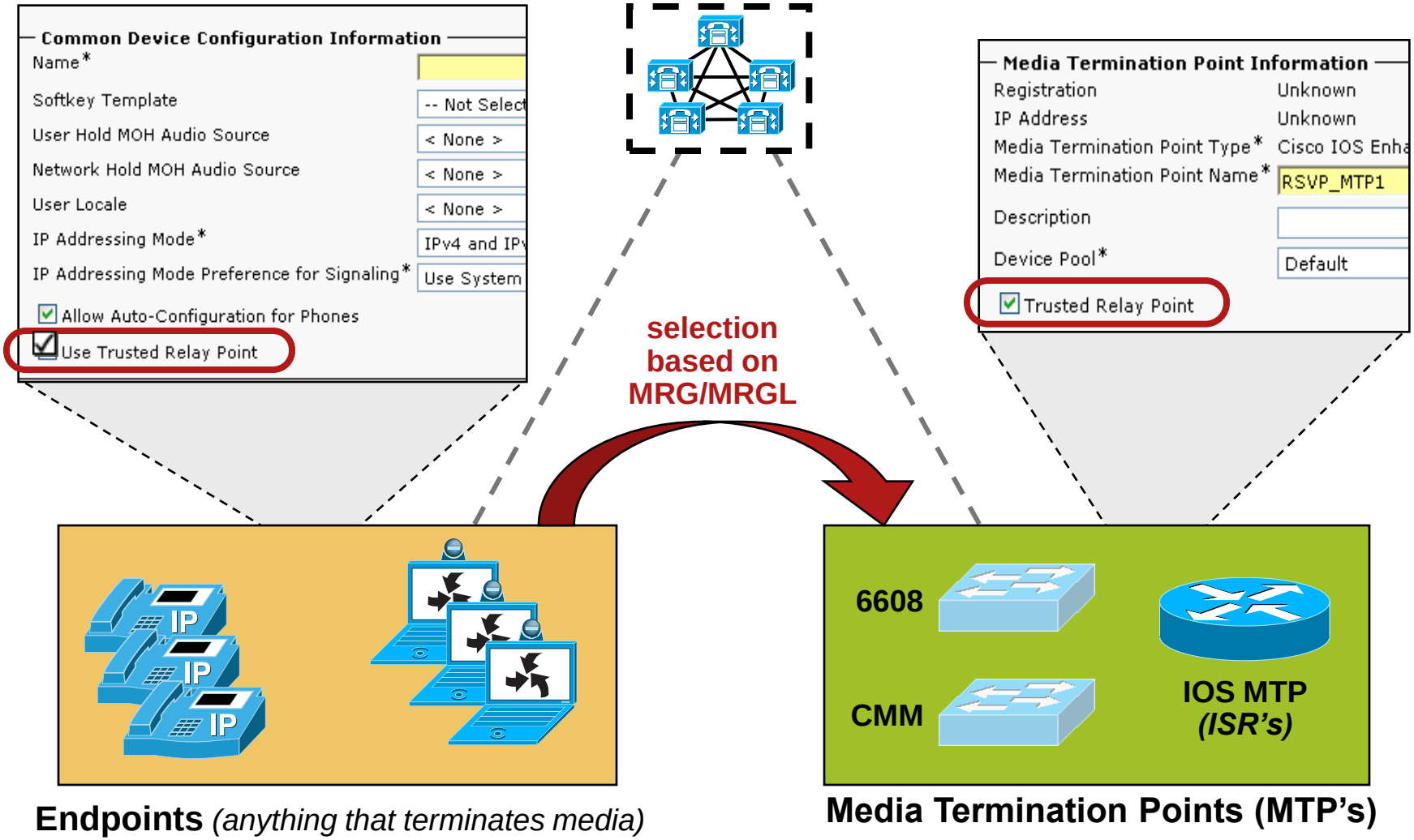
= Reference slide

Trusted Relay Point (TRP)
Overview



- Software function that runs on Cisco network devices such as campus switches and routers *(similar to an MTP)*
- Inserted in the call flow by CUCM 7.0 (or CUCME 4.0) based on config
- Provides **trusted** anchoring point for media to enable several functionalities (QoS enforcement, Trusted VLAN traversal, ...)

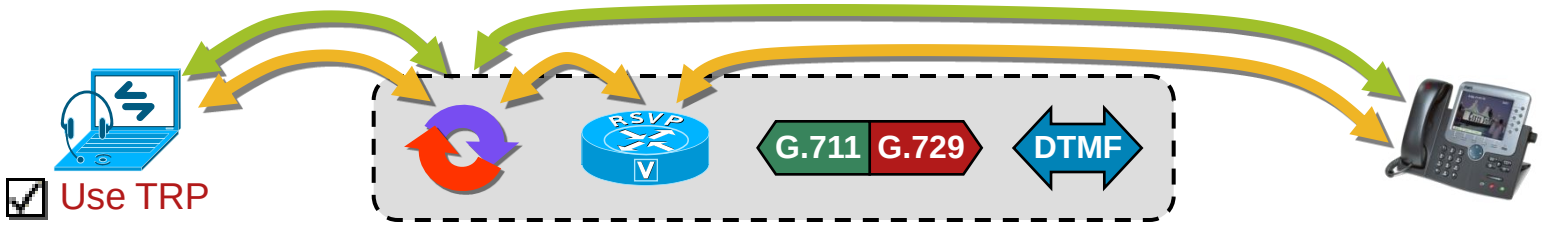
Trusted Relay Point (TRP)
Enabling TRP-based features in CUCM 7.0



Endpoints *(anything that terminates media)*

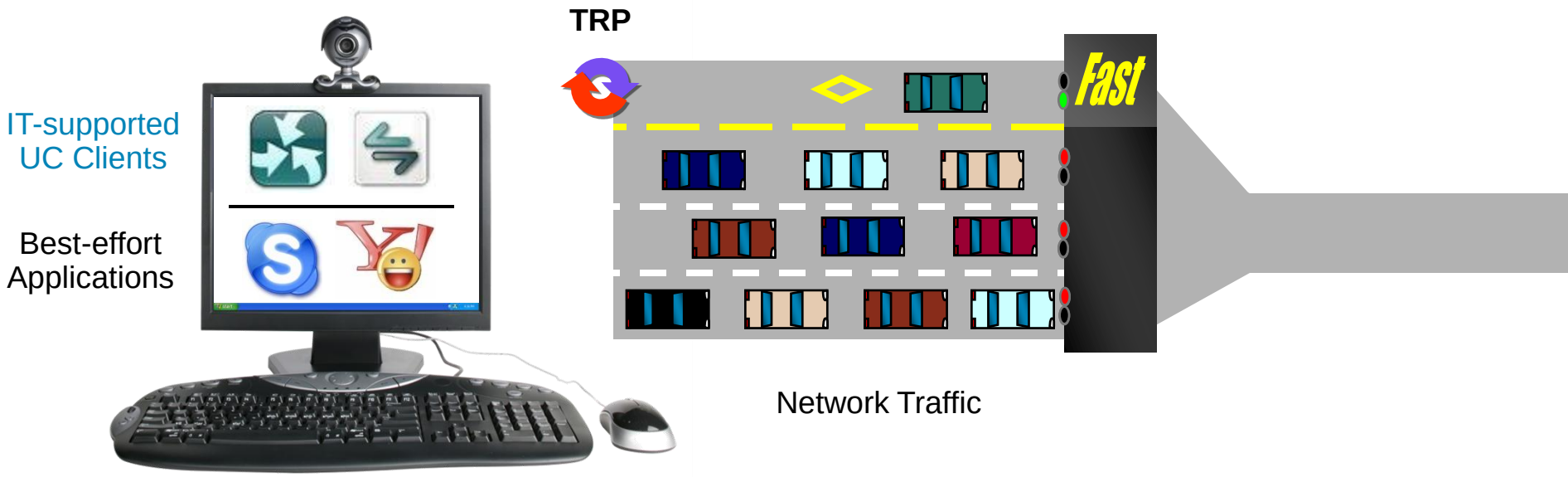
Media Termination Points (MTP's)

Trusted Relay Point (TRP)
Unified CM Insertion "Rules"



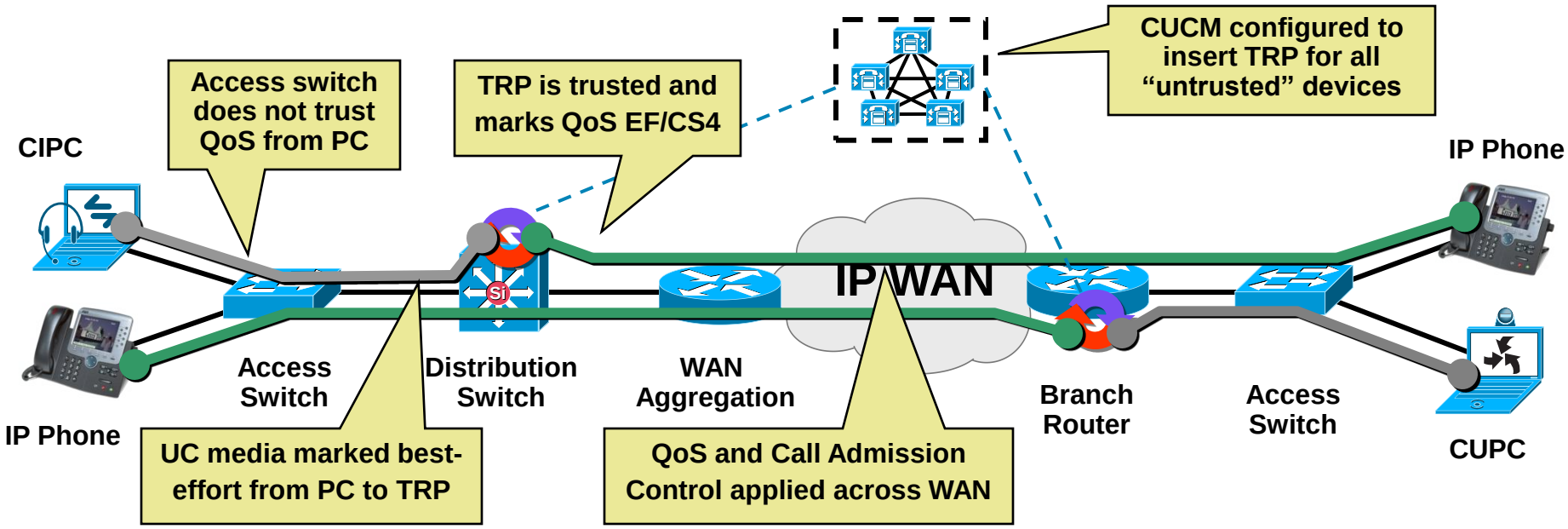
- If multiple functions are required for a given call (Xcoder, TRP, RSVP Agent, DTMF relay...), CUCM will first attempt to select an MTP that can fulfill them all
- If that is not possible, the TRP will be placed 'closest' to the endpoint
- TRP supports sRTP and video ("pass-through" codec)
- If a call is placed on hold, TRP stops streaming media, but resource is kept
- If CUCM is unable to allocate a TRP for a call, the call will fail or not depending on the service parameter "Fail Call if Trusted Relay Point allocation fails" (default is true)

UC Trusted QoS Enforcement
Network-based QoS for Software UC Clients



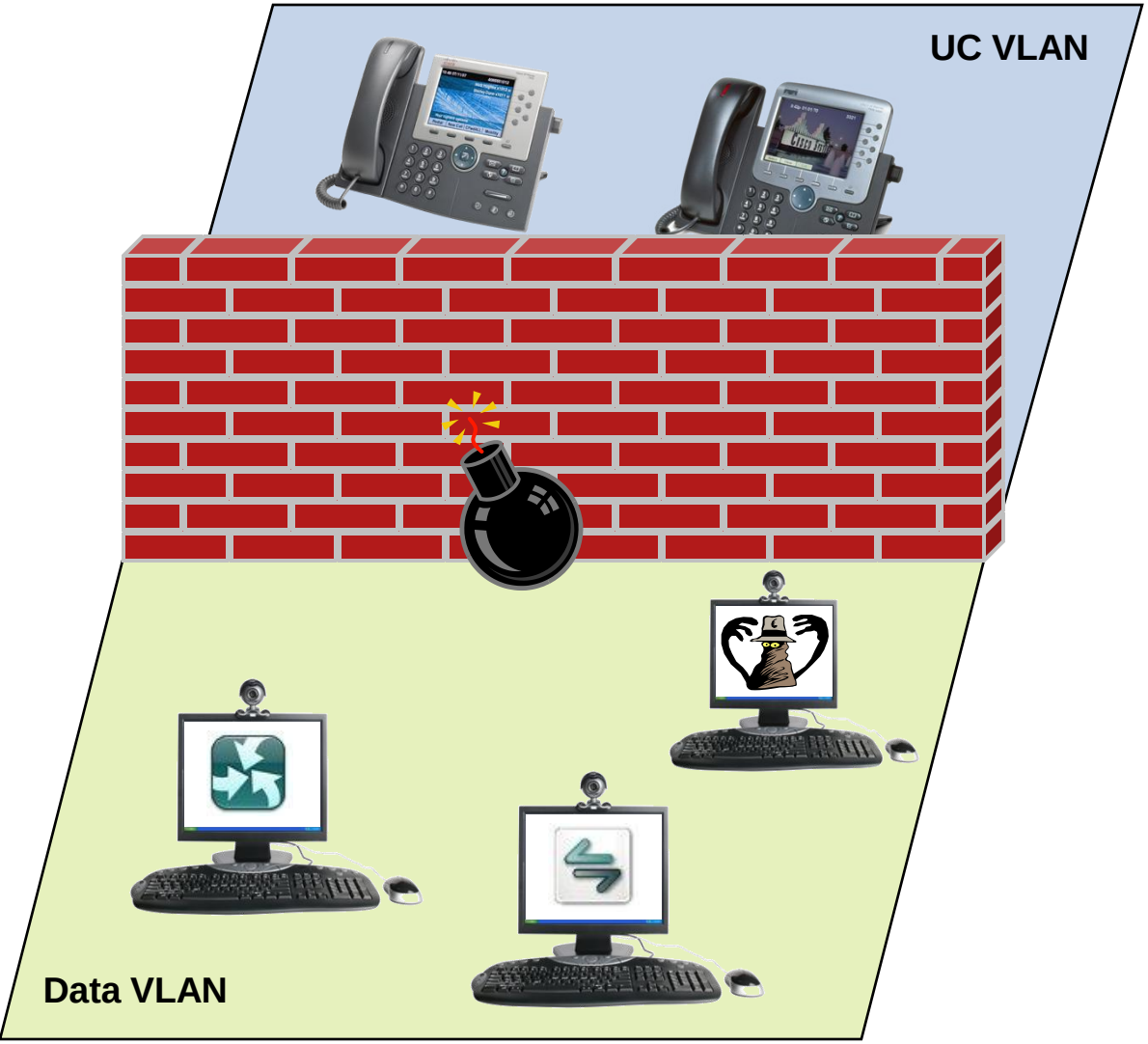
- User-controlled PC's are typically **untrusted** devices
- Cisco UC collaborates with Cisco network devices to enable QoS and call admission control for IT-supported UC clients
- Simple solution that provides software clients the same real-time network treatment available to hardware endpoints

UC Trusted QoS Enforcement Details



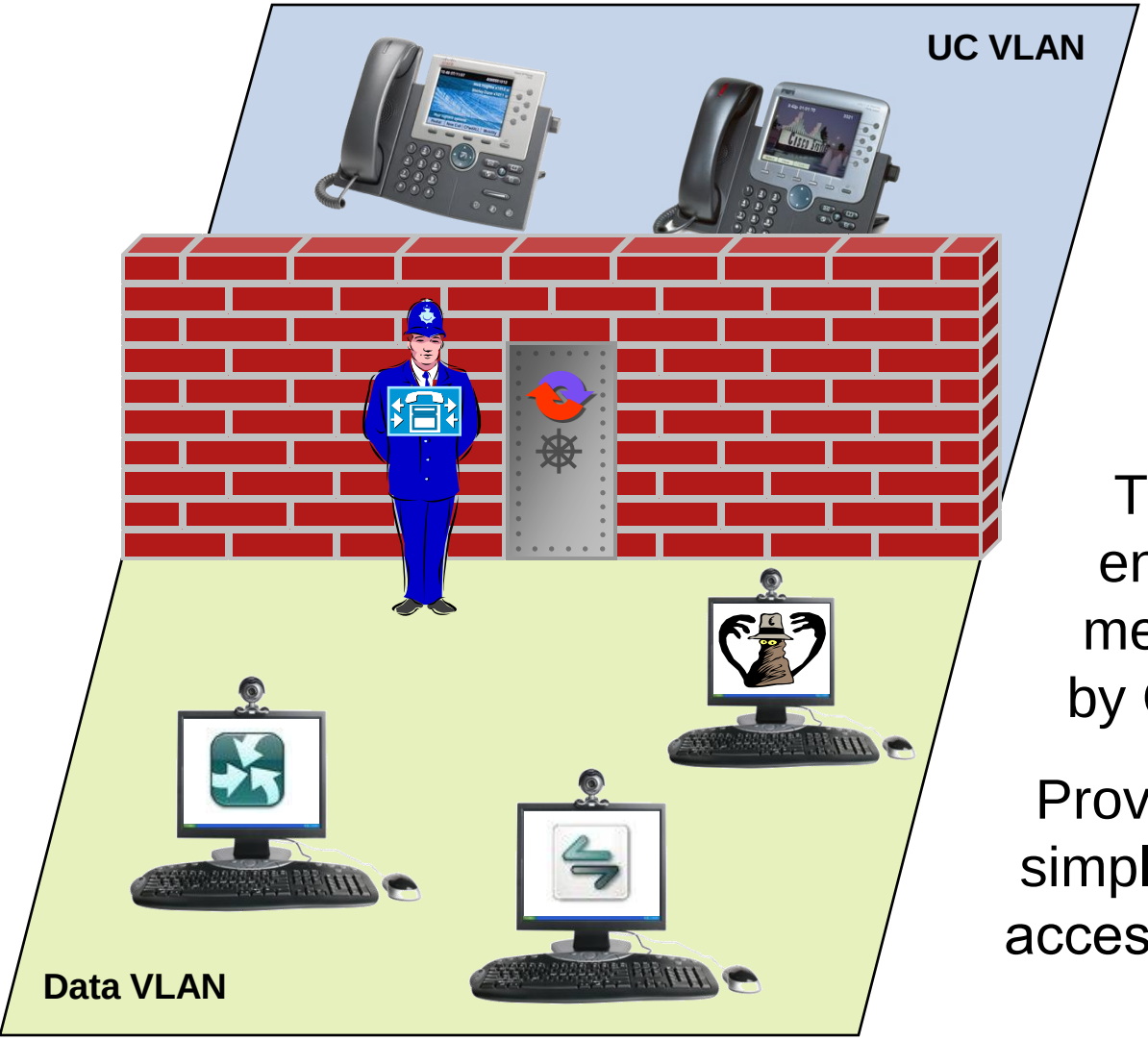
- Feature may be enabled for all "untrusted" endpoints that register to CUCM/CME (software-based, video, 3rd party, ...)
- To minimize number of MTP's involved in a call, ensure the same network device can perform all needed functions (TRP, RSVP Agent, Xcoder, ...)

UC Trusted VLAN Traversal
Controlling Access to UC VLAN's (1)



Mechanisms based on ACL's rely on port numbers—no way to ensure only 'trusted' media enters UC VLAN

UC Trusted VLAN Traversal
Controlling Access to UC VLAN's (2)

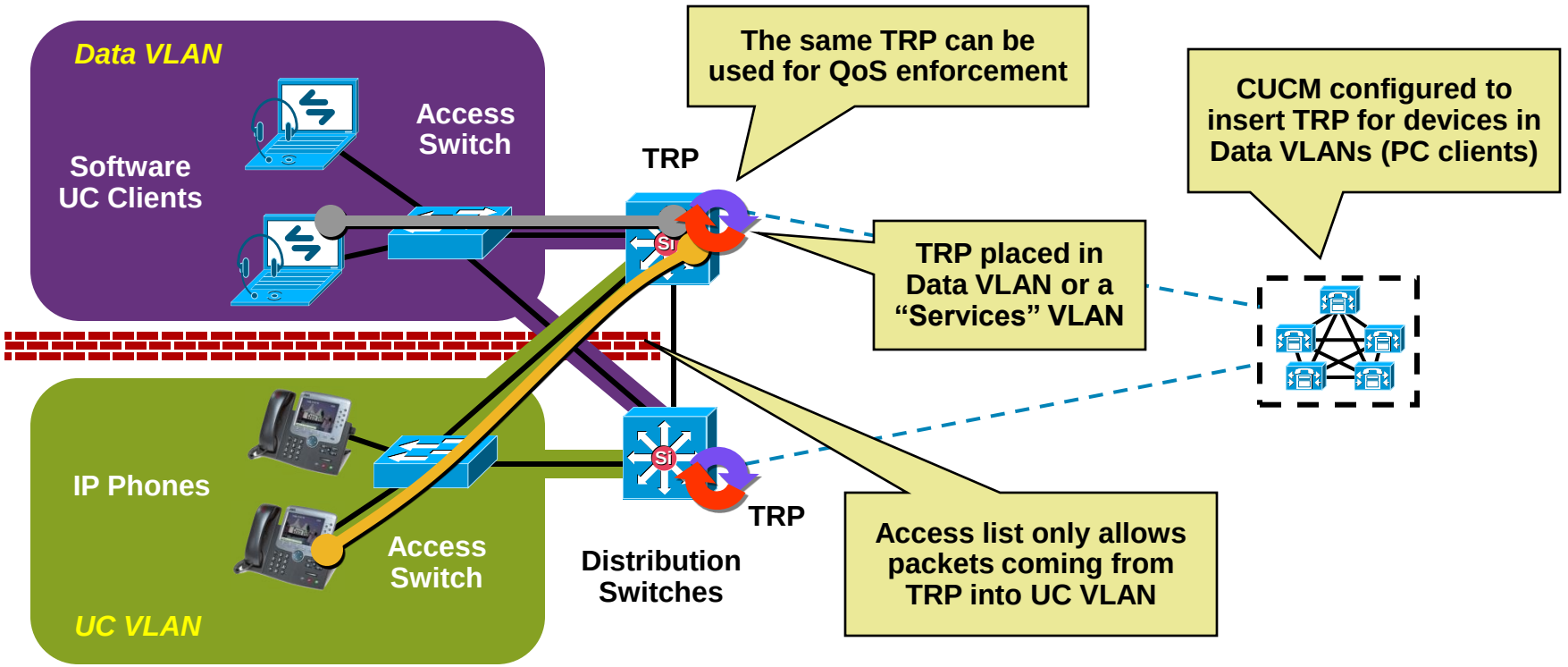


Mechanisms based on ACL's rely on port numbers—no way to ensure only 'trusted' media enters UC VLAN

TRP enables you to limit entry into UC VLAN only to media streams controlled by CUCM (or CUCME)

Provides an effective and simple mechanism to control access to UC VLAN's

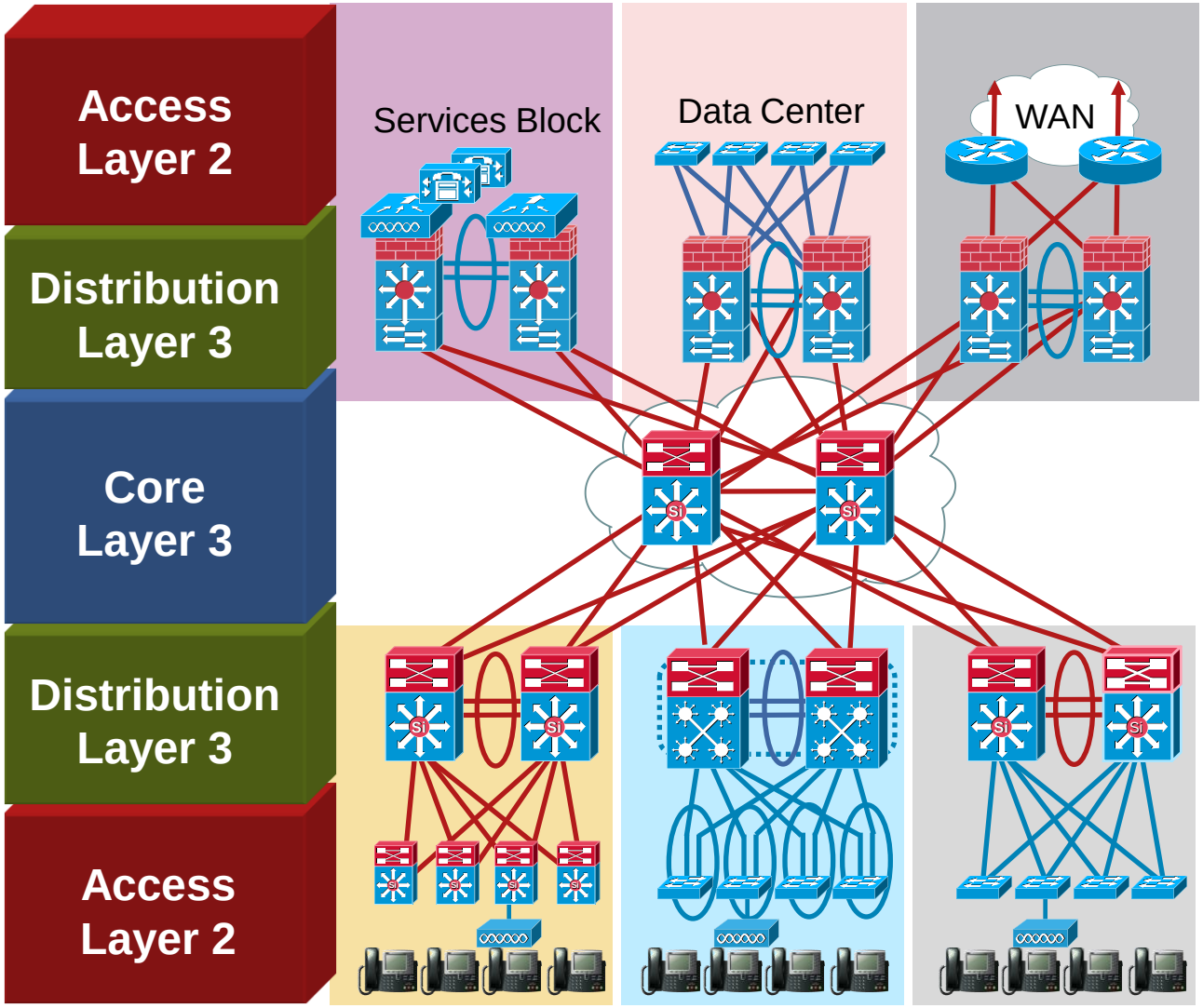
UC Trusted VLAN Traversal Details



- Examples of ACL policies to control access to UC VLAN from Data VLAN:
  1. Only packets with source IP address of the TRP
  2. Only packets with DSCP marked EF or CS4

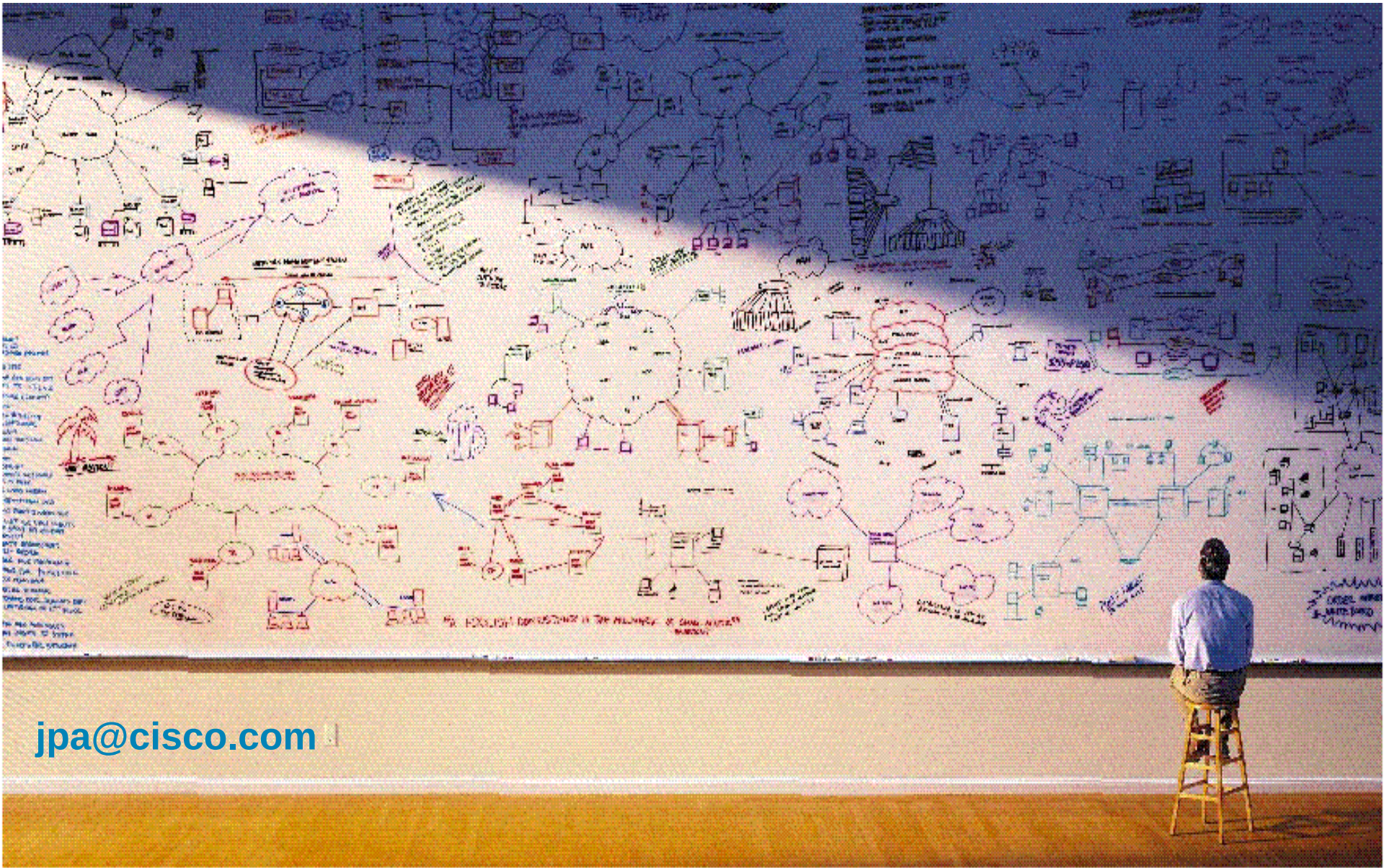
Building a Campus UC Network
Summary

- Access layer
  - Automatic Phone Discovery
  - Power over Ethernet
  - Voice VLAN allocation
  - Multiple Security features
  - QoS Trust Boundaries
  - AutoQoS
  - Trusted Relay Point
- Distribution Layer
  - Fast Convergence
  - QoS
  - High Availability
- Core Layer
  - Fast Convergence
  - Scalability
  - High Availability



Q & A

Thanks for your attention

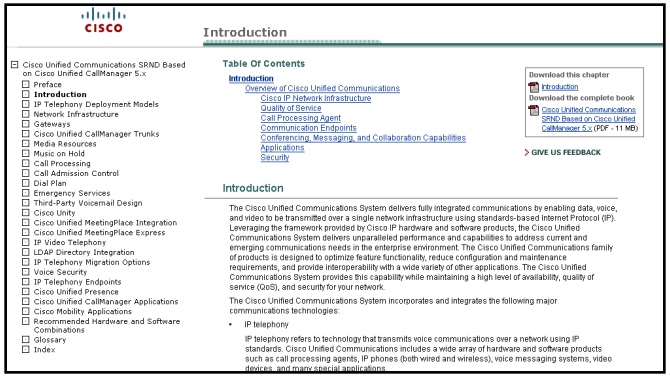


jpa@cisco.com

Need more info ?

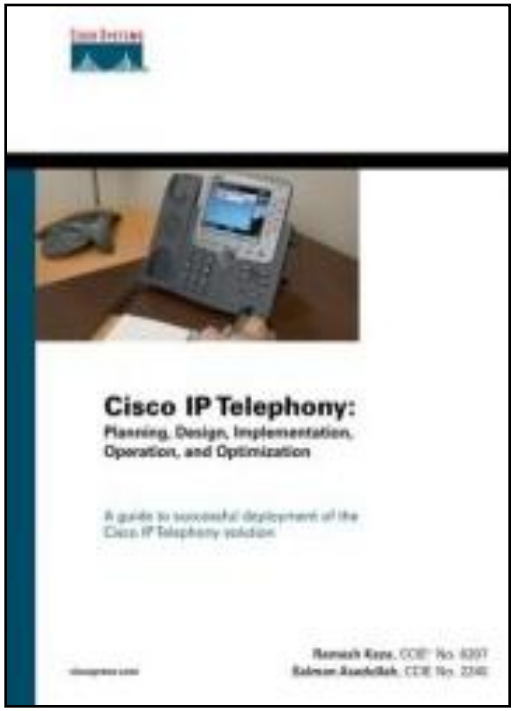
- Unified Communications SRND

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



- Cisco Press Book

  Cisco IP Telephony: Planning, Design, Implementation, Operation, and Optimization



- Networkers 2009

  BRKCAM-3014 Impact of Emerging Technologies on Campus Design - Intelligent Access

Cisco Networkers 2009
January 26-29 Barcelona, Spain