Cisco live!

What You Make Possible

TOMORROW
starts here.

CISCO

Unified Communications Security: Design and Best Practices

BRKUCC-2041

TOMORROW starts here.

Agenda

- Security Requirements for Unified Communications
- Unified Communications System Environment
- Defining Attacks on UC Systems
- Access Layer Security
- Endpoint Security
- Encryption
- Firewalls
- Secure Remote Access
- Security for IP PSTN
- Security for Video

Security Requirements for Unified Communications

What Security Do You Have Now?

You Are Running Your Business Critical Applications on Your Network Today

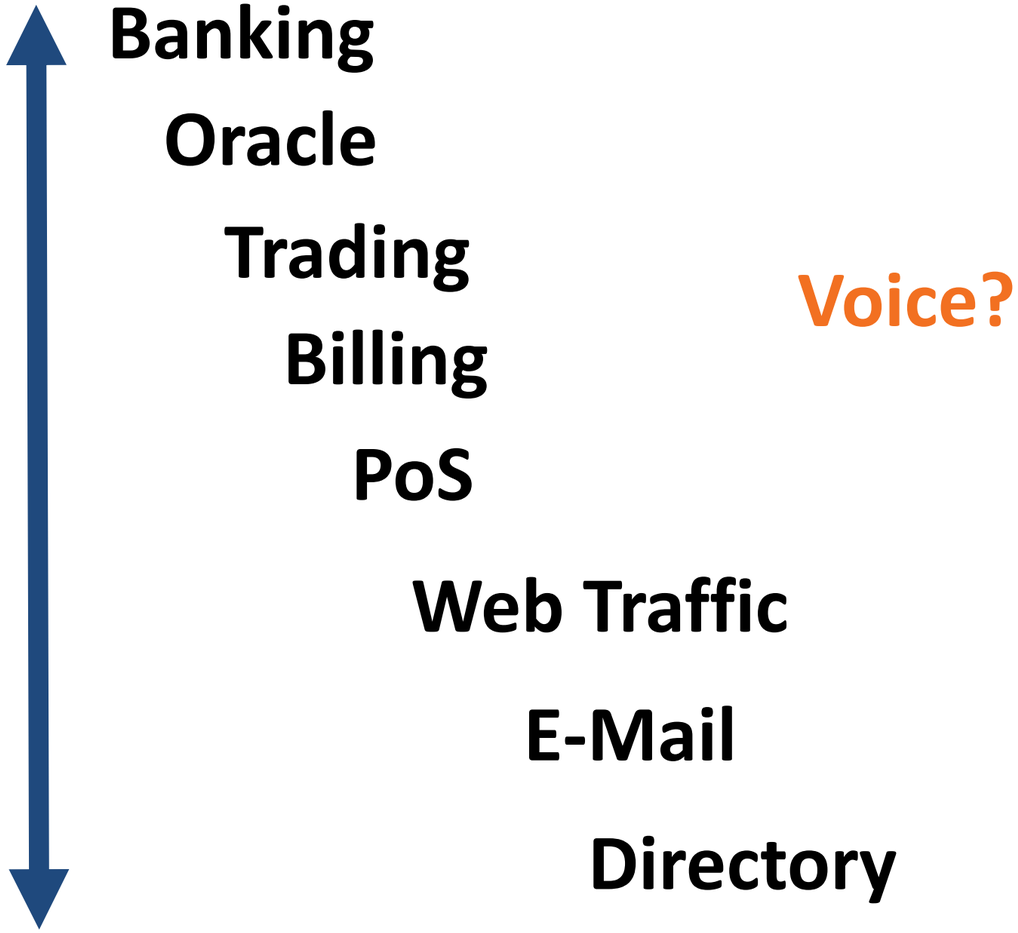
- Is your current network security enough?
  - If not, how much is enough?
- Will VoIP make your network less secure?
- What are the risks of putting UC on your current network?
- Will everything you do for security now work with VoIP?

VoIP Security Assessment

- What is important to you?
  - What attacks worry you or your management?
- How much security do you need?
- Where are you going to run your Unified Communications (UC) system?
  - Call Centre, emergency services, etc.
- How do we manage all this security?
- How much will this security cost?

Voice Is Data

- Don’t make security an end to itself
- Rank voice by your business requirements
- Evaluate whether your existing security policy for data is sufficient for voice
- I can not tell you how much security you need
- I can help you determine what is acceptable to you and your management



Unified Communications Policy

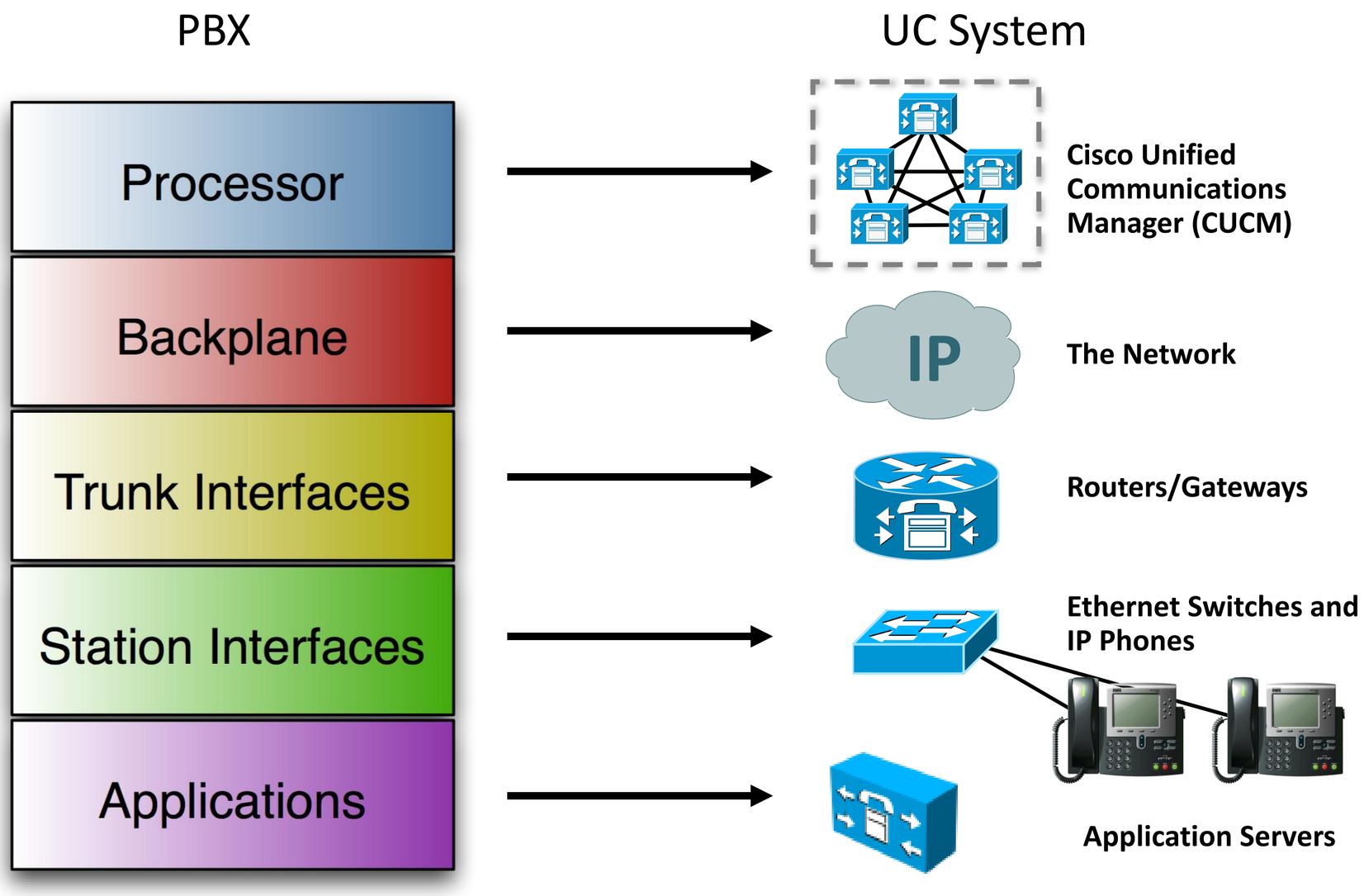
- You need a security policy for voice/video/IM style of data
- Look at the overall system
  - What does it look like compared to what applications are already on your network
- Have a way to respond if something does happen
  - How will the issue be addressed?
  - What are the repercussions to the attacker?
- Make sure that management knows the defined risks
  - If they know the risks going in, better decisions can be made
  - If security does need to increase—this will help define expenditures

Agenda

- Security Requirements for Unified Communications
- Unified Communications System Environment
- Defining Attacks on UC Systems
- Access Layer Security
- Endpoint Security
- Encryption
- Firewalls
- Secure Remote Access
- Security for IP PSTN
- Security for Video

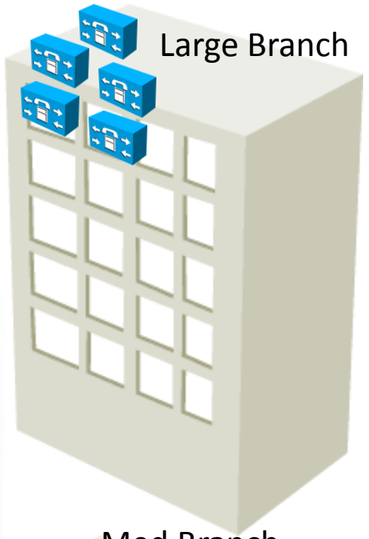
Unified Communications System Environment

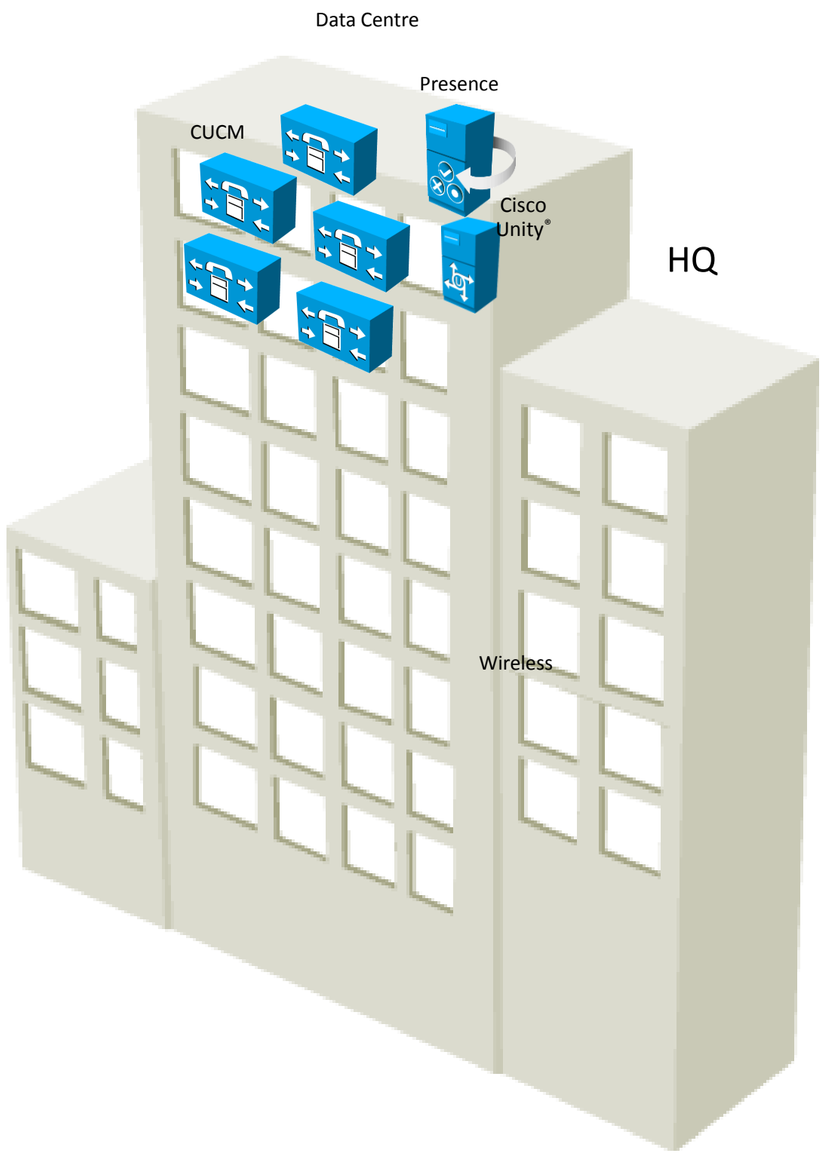
What a UC System Looks Like



General Deployment

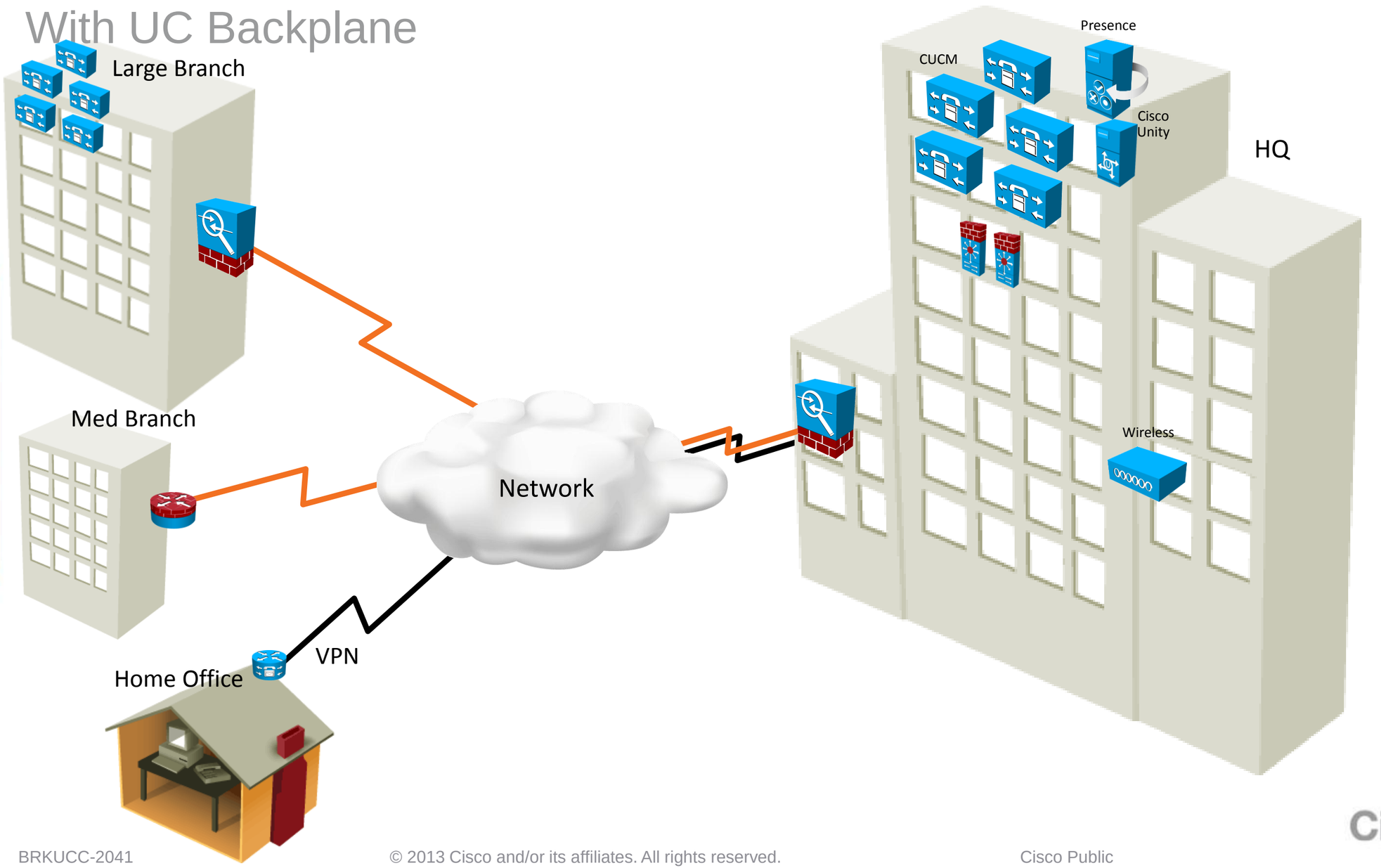
UC Processors





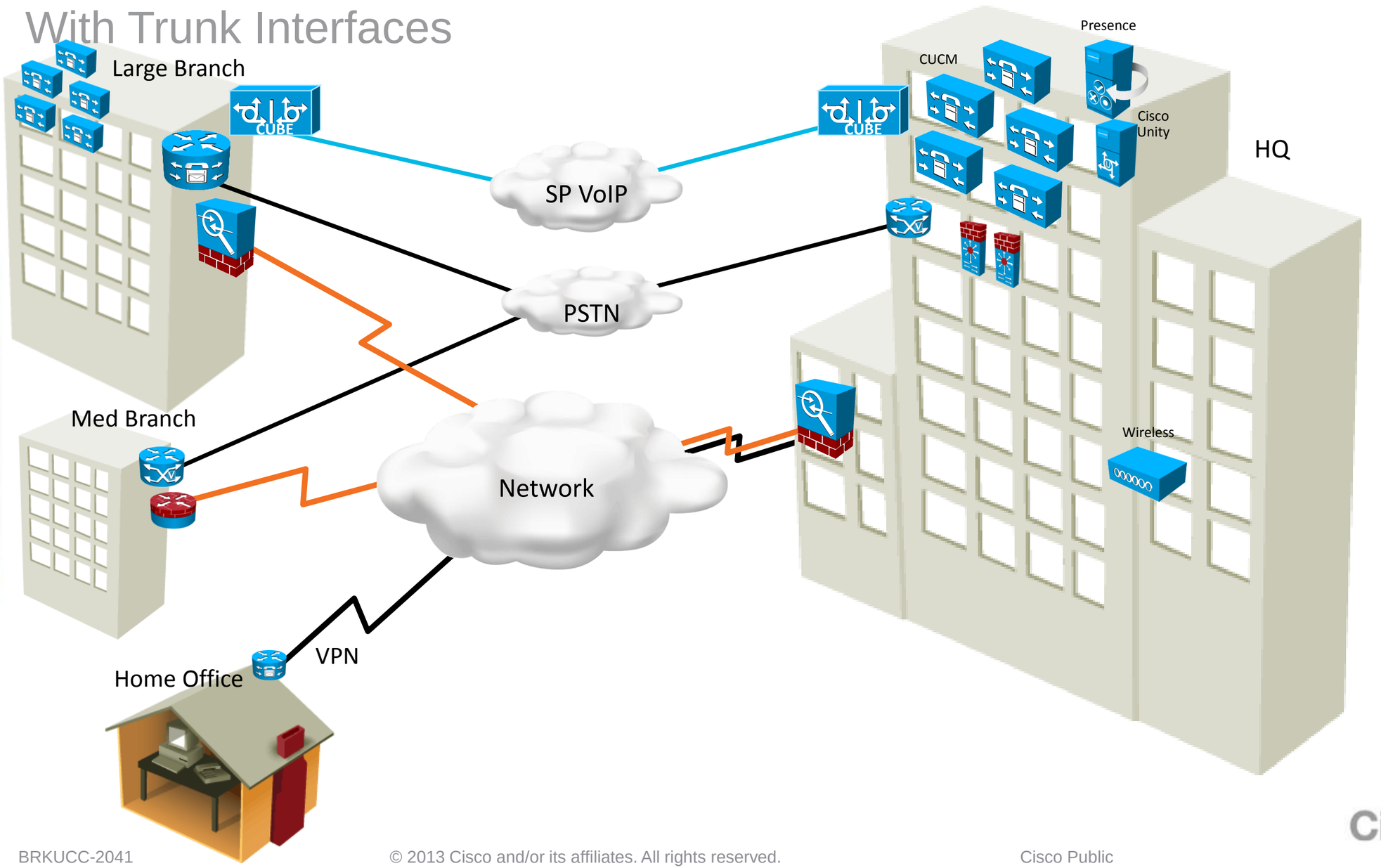
General Deployment

With UC Backplane



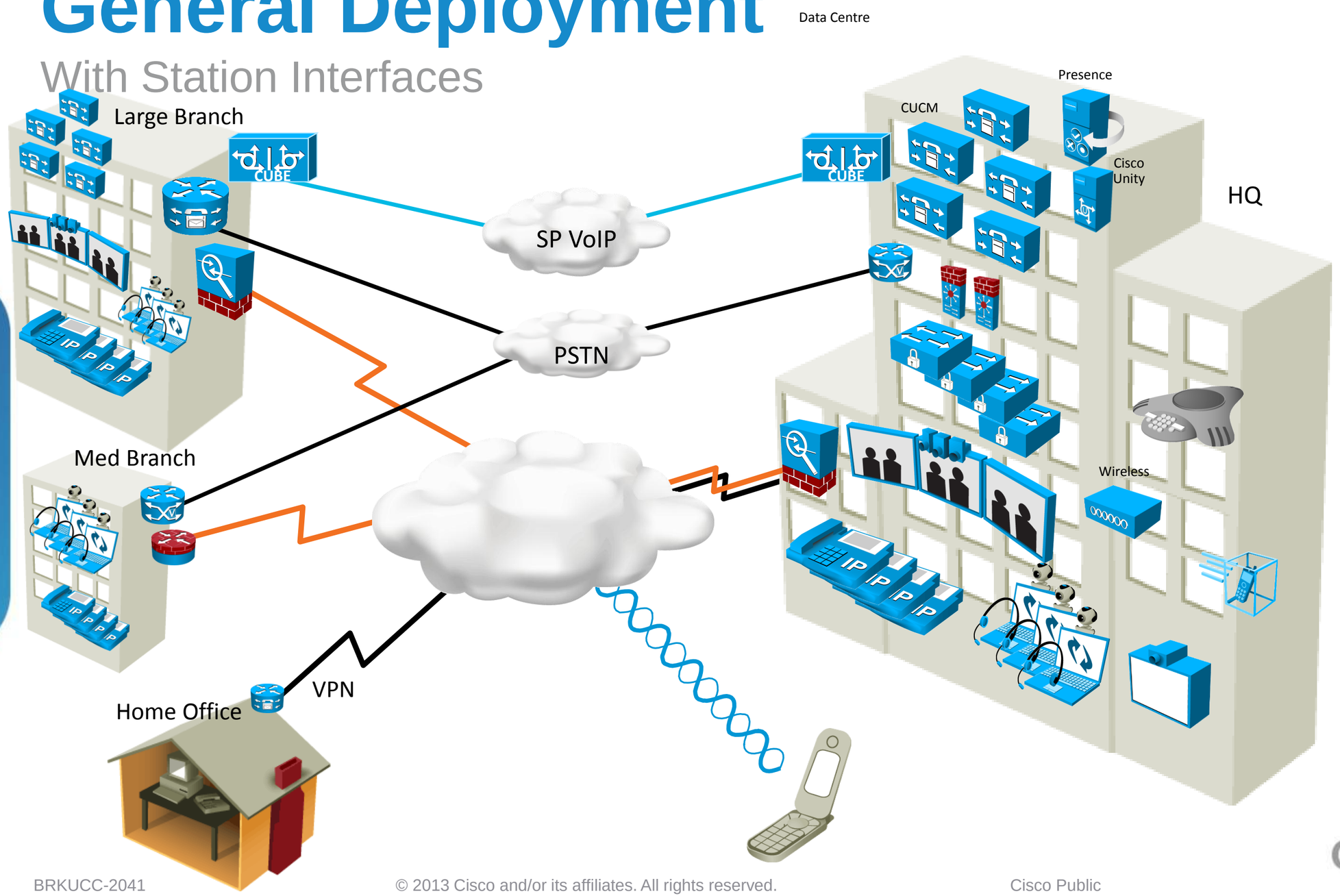
General Deployment

With Trunk Interfaces



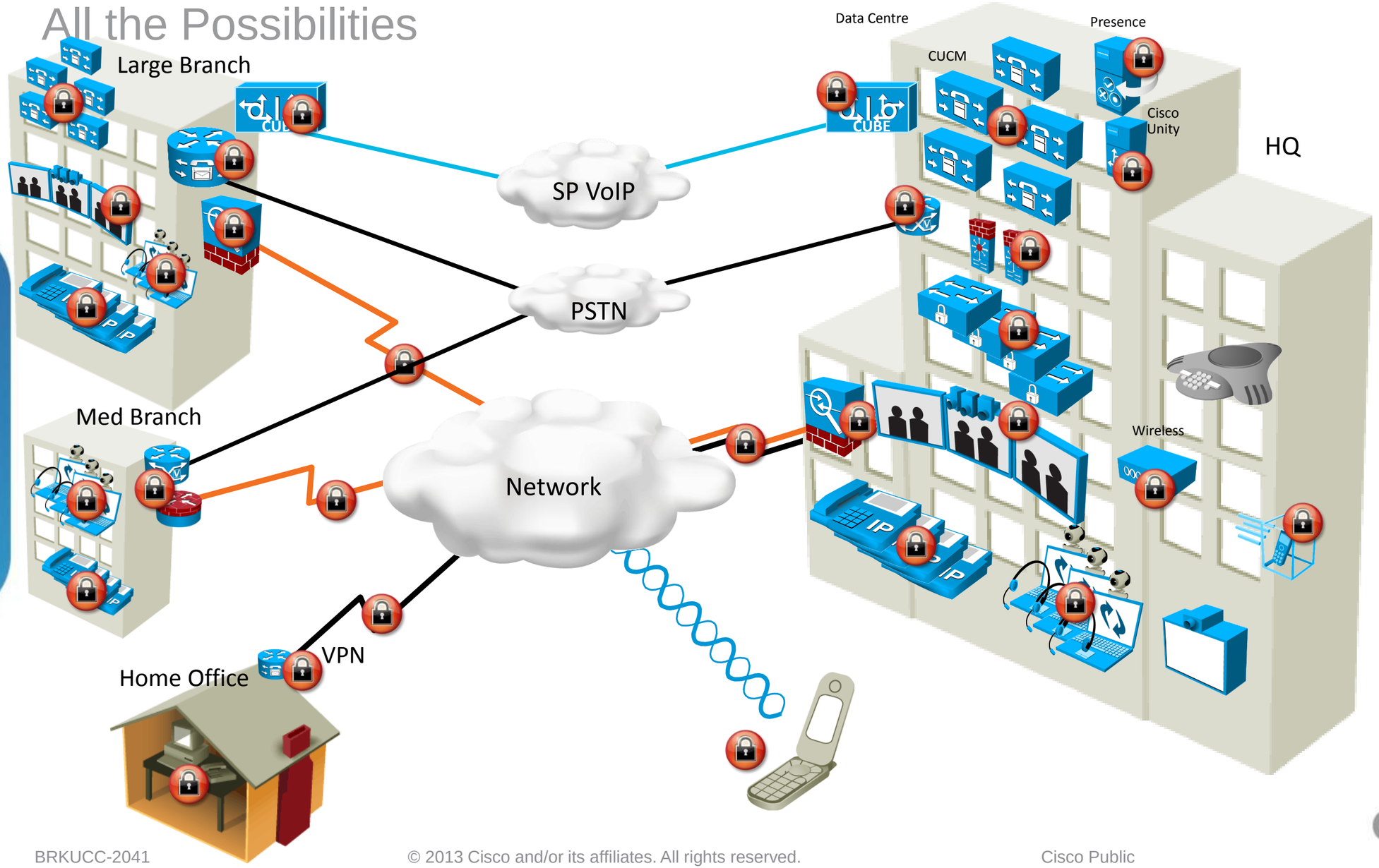
General Deployment

With Station Interfaces



Security Deployments

All the Possibilities



Agenda

- Security Requirements for Unified Communications
- Unified Communications System Environment
- Defining Attacks on UC Systems
- Access Layer Security
- Endpoint Security
- Encryption
- Firewalls
- Secure Remote Access
- Security for IP PSTN
- Security for Video

Defining Attacks

Types of Attacks

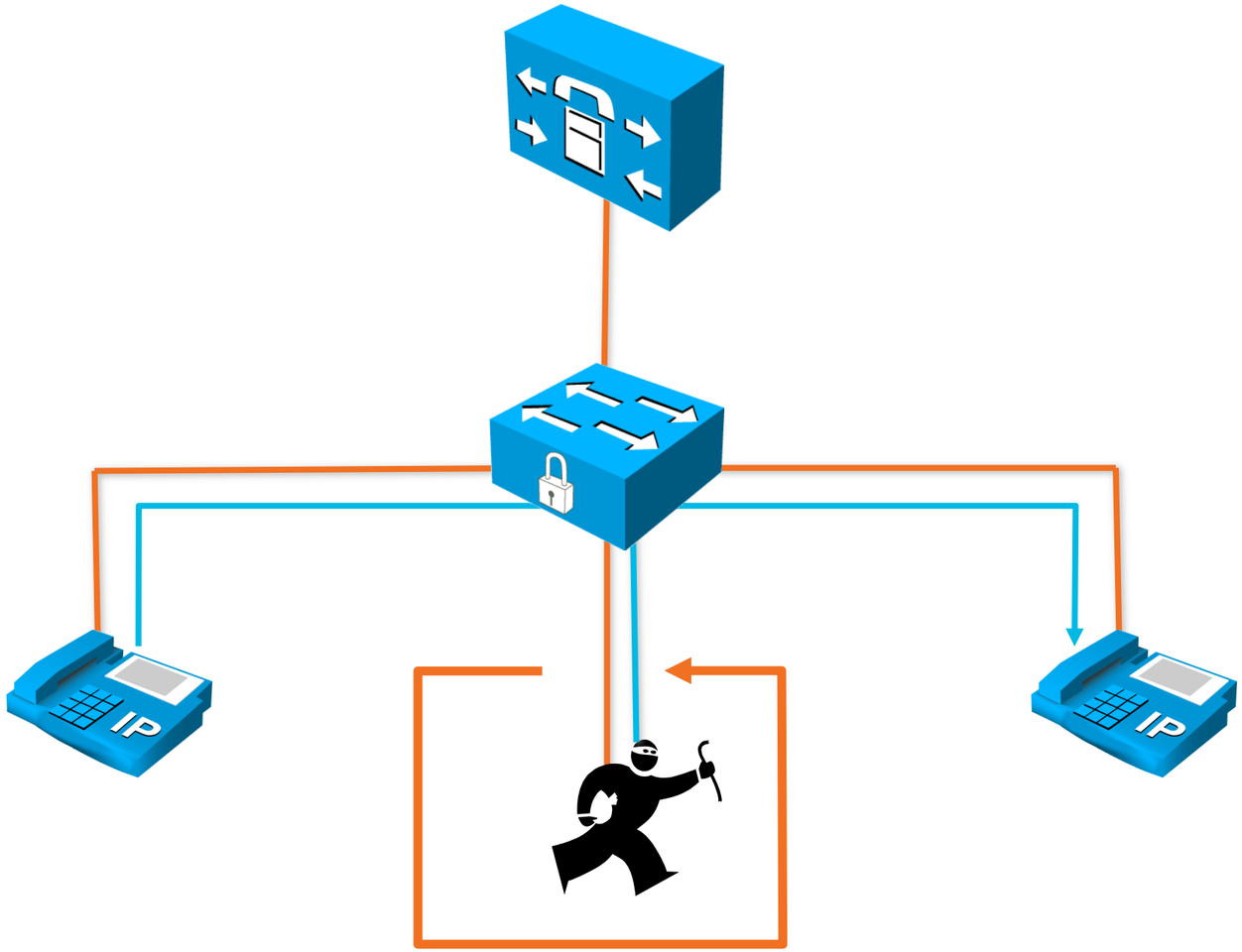
- Break stuff or create havoc
  - In it just for the joy of damaging things (script kiddies)
  - Create problems to cover an actual intelligent attack
- Recon/intelligent/profit
- Wants information
- Looking for something (passwords, confidential)
- Willing to sell this information
- Redirect or misuse network resources
- Steal services (toll fraud)

Type of Attacks on UC Systems

- Eavesdropping
  - Listening or recording data without approval
- Denial of Service (DoS) or Distributed Denial of Service (DDoS)
  - Flood bandwidth or resources of a targeted system
- Impersonation
  - Attempt to be something or someone that you are not
- Modification
  - RTP stream mixing/insertion
- Toll fraud
  - Making calls that the users are not approved to do, usually long distance calls
- SPIT
  - Calls generate annoyance for users, lower productivity

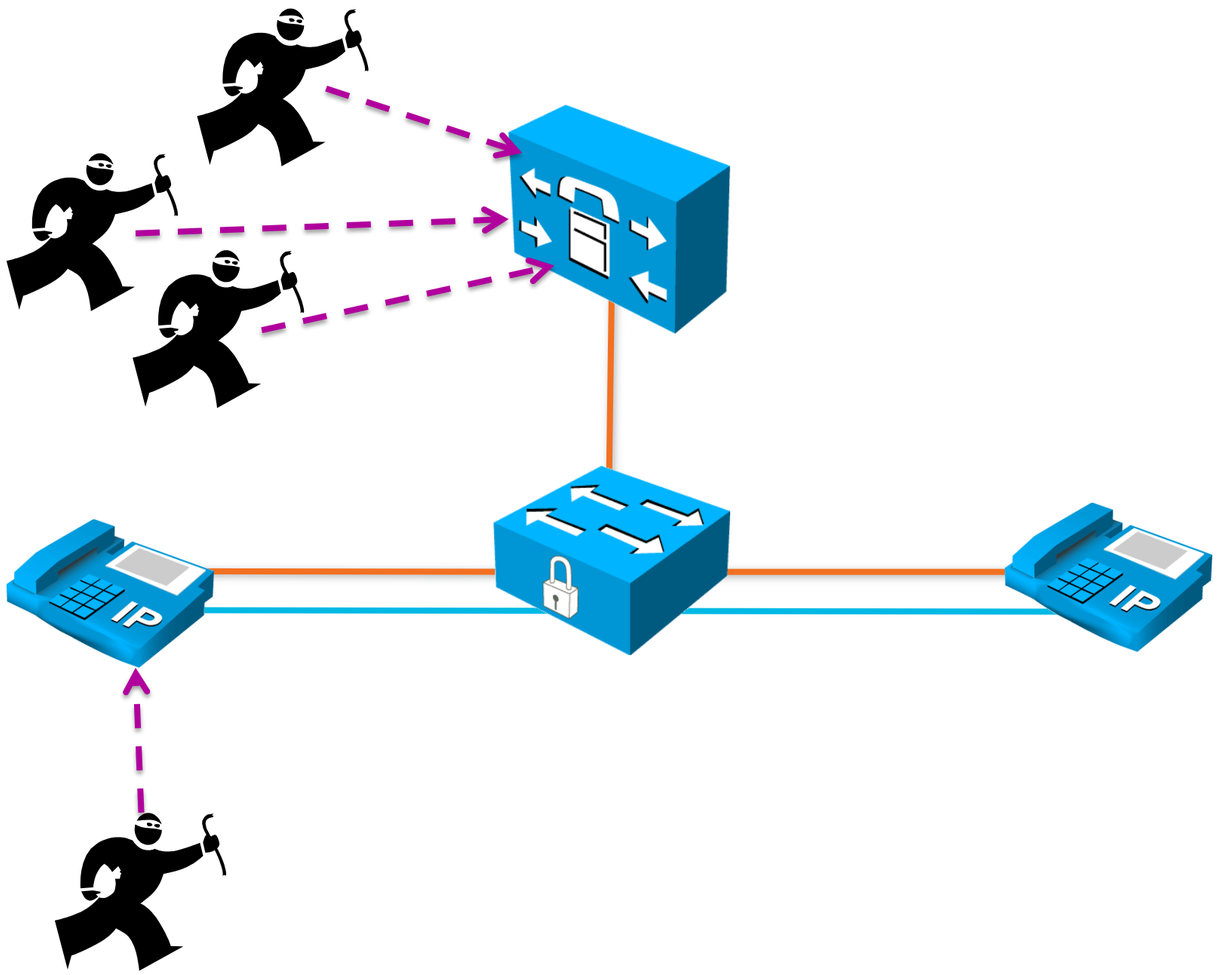
Eavesdropping Attacks

- Eavesdropping is the act of surreptitiously listening to a private conversation
- Eavesdropping can be done over telephone conversations, email, IM, and other methods of communication considered private
- Man in the Middle Attack
  - Attacker gets between the two endpoints in a conversation and captures relevant traffic



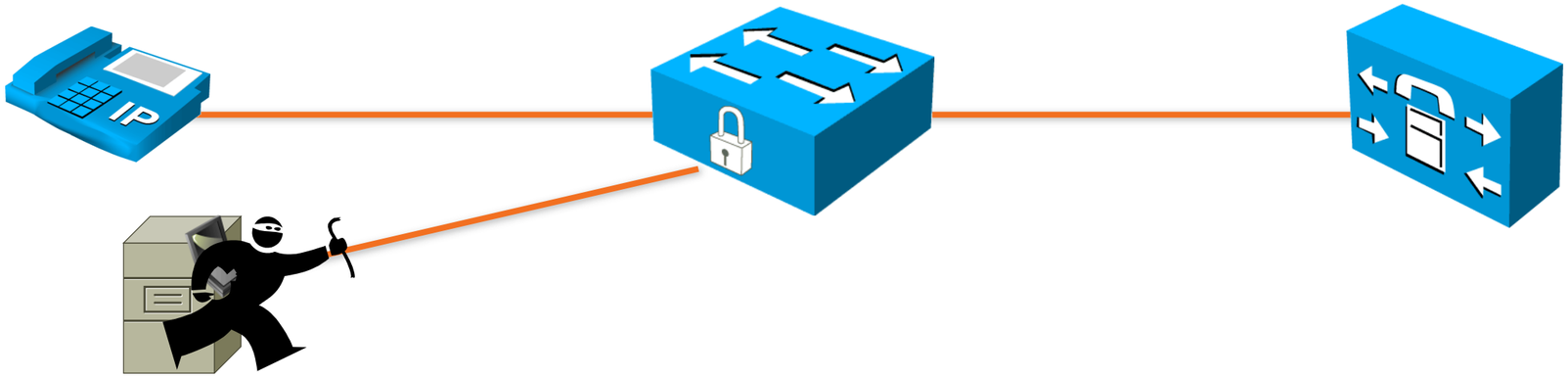
DoS and DDoS

- Risks to availability of UC systems is one of the biggest threats
- Denial of Service can be carried out by saturating the network with too much traffic
- DoS attacks can also be endpoint targeted, changing the state or presence of endpoints



Impersonation Attacks

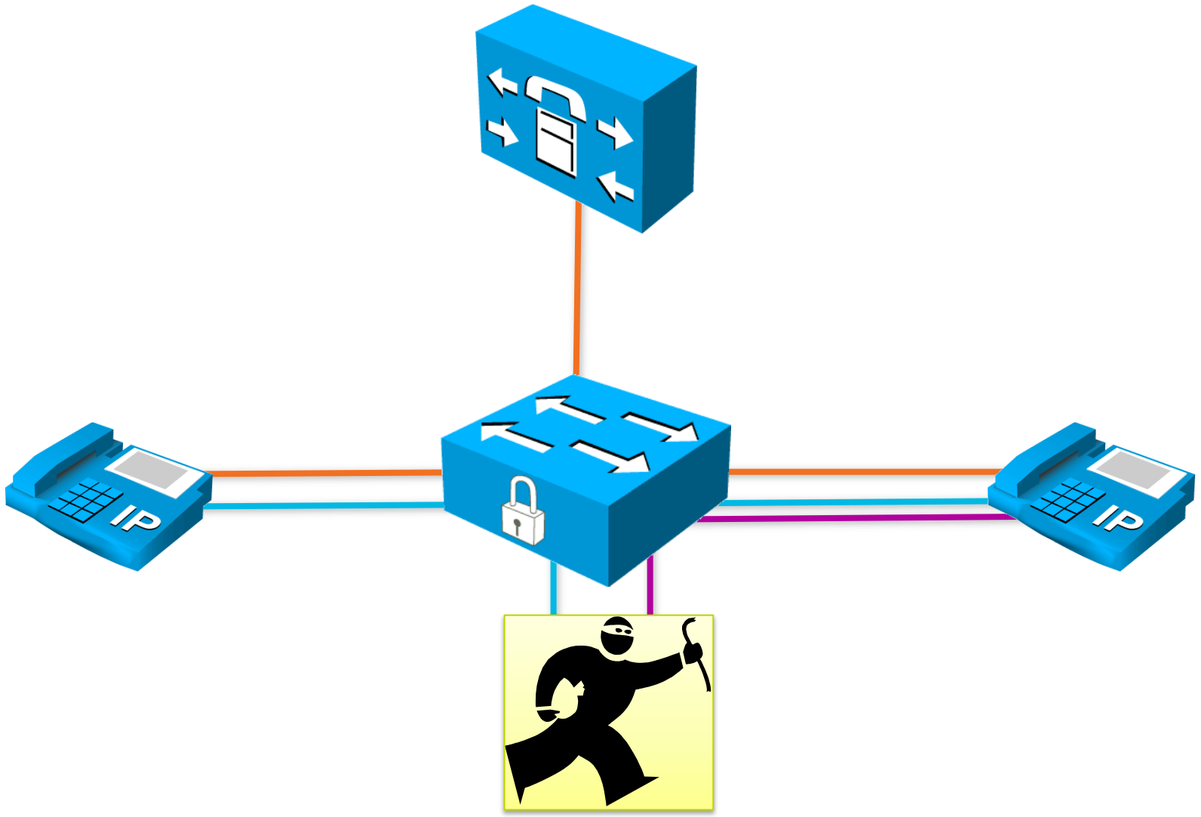
- Impersonation attacks use captured account information to impersonate a user
- Prelude to modification attacks and toll fraud
- Attack prevention focuses on establishing authentication



Spoofed Identity

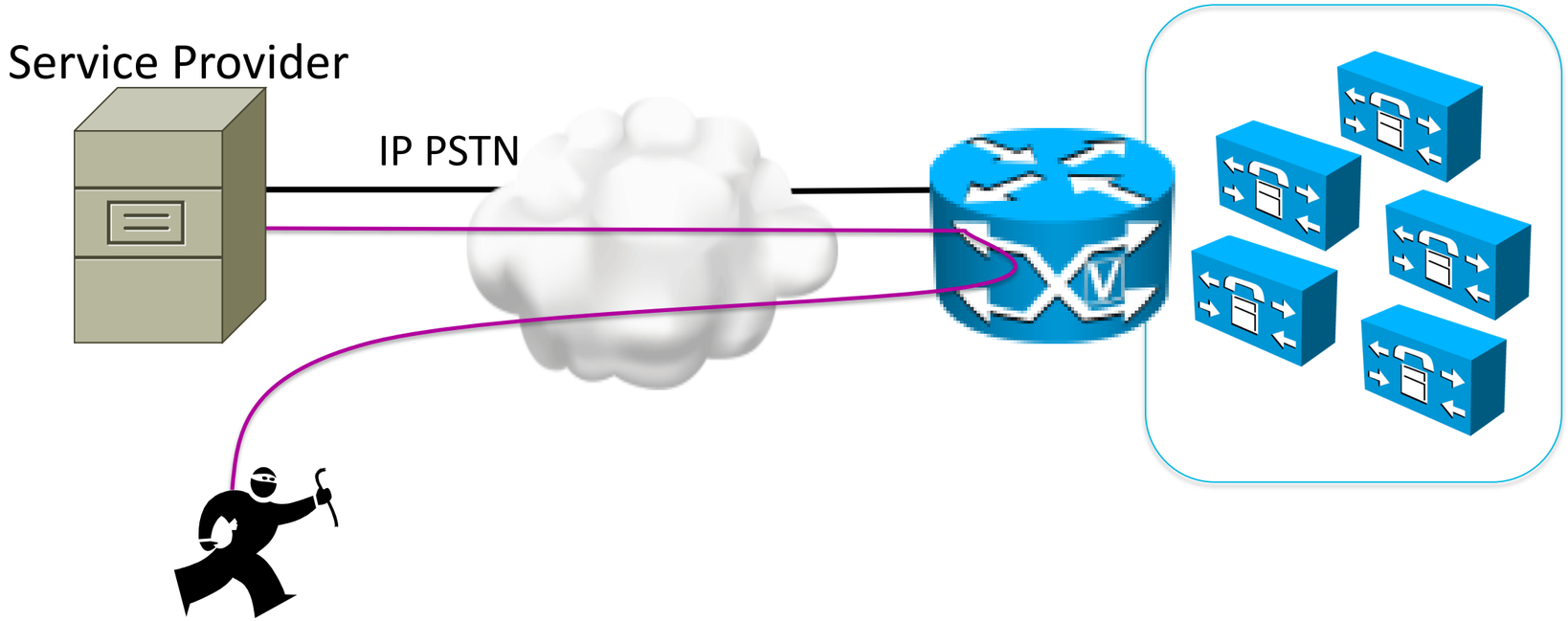
Modification Attacks

- Malicious insertion of RTP packets in a media stream
  - rtpinsertsound and rtpmixsound tools
- Can cause confusion among users or misinformation



Toll Fraud

- Toll fraud refers to internal or external users using the corporate phone system to place unauthorised toll calls
- Can incur very large costs to the organisation, financial risk is greatest
- Carried out by gaining access to endpoints or trunks



Toll Fraud

- Traditional dial plan configs as on all call processing devices
- Call forwarding, remote call forwarding, and trunk-to-trunk transfers
- Partitions and calling search spaces limit what parts of the dial plan certain phones have access to
- Dial plan filters control access to exploitive phone numbers
- Ad hoc conference calls can optionally be dropped when the originator hangs up
- Forced authentication codes or client matter codes prevent unauthorised calls and provide a mechanism for billing and tracking

SPIT Attacks

- Spam over IP Telephony calls are unsolicited telemarketing calls made over VoIP
- Theoretical problem, as yet insignificant
- Main problem with SPIT is the level of annoyance it presents to users
- Can be resource sapping
- Attack prevention
  - Enable SIP Trunk Registration and Authentication
  - Manual Blacklisting of identified problem numbers on CUCM and CUBE
  - Dynamic Blacklisting on CUBE (SP Edition)

Agenda

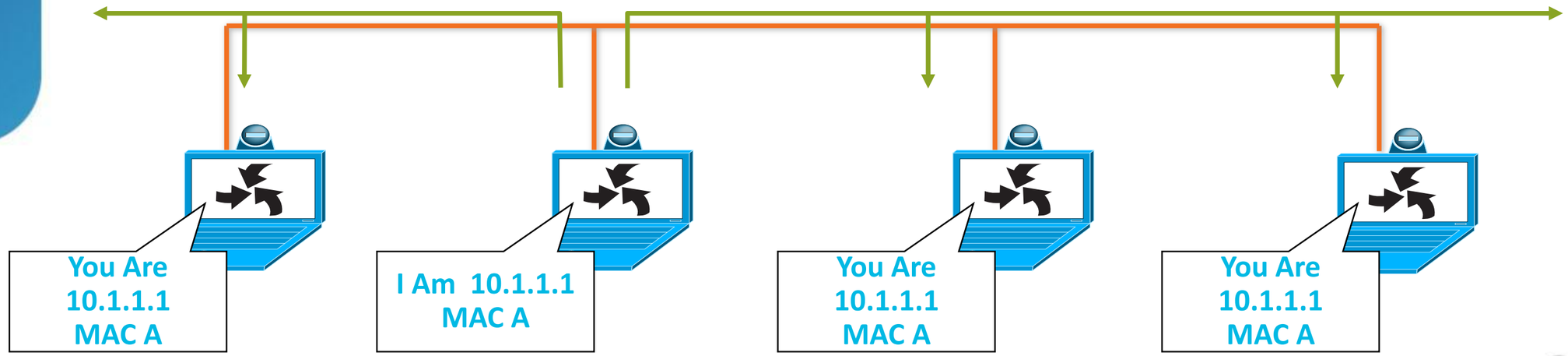
- Security Requirements for Unified Communications
- Unified Communications System Environment
- Defining Attacks on UC Systems
- Access Layer Security
- Endpoint Security
- Encryption
- Firewalls
- Secure Remote Access
- Security for IP PSTN
- Security for Video

Access Layer Security

Eavesdropping Protection

ARP Explained

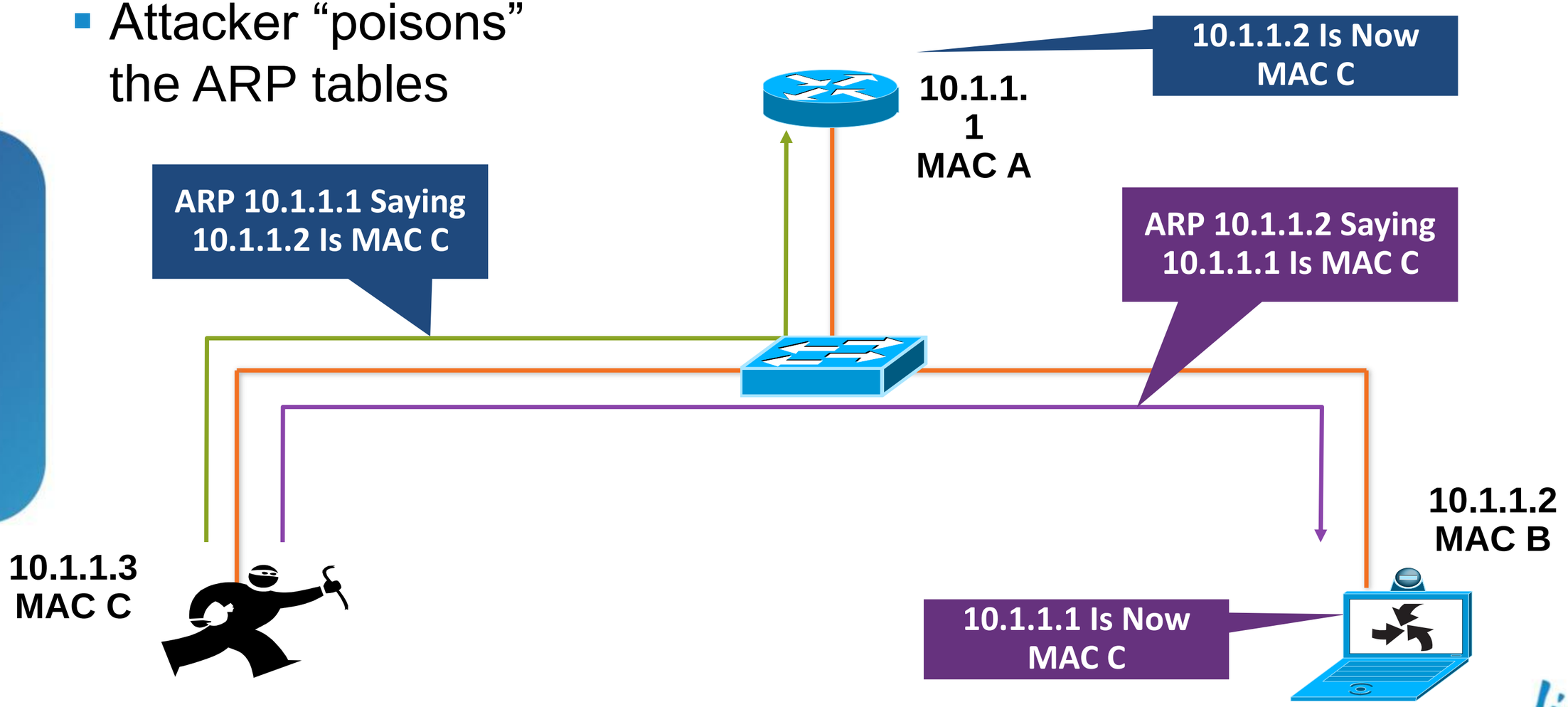
- According to the ARP RFC, a client is allowed to send an unsolicited ARP reply; this is called a gratuitous ARP; other hosts on the same subnet can store this information in their ARP tables
- Anyone can claim to be the owner of any IP/MAC address they like
- ARP attacks use this to redirect traffic



Eavesdropping Protection

Switches: ARP Attacks

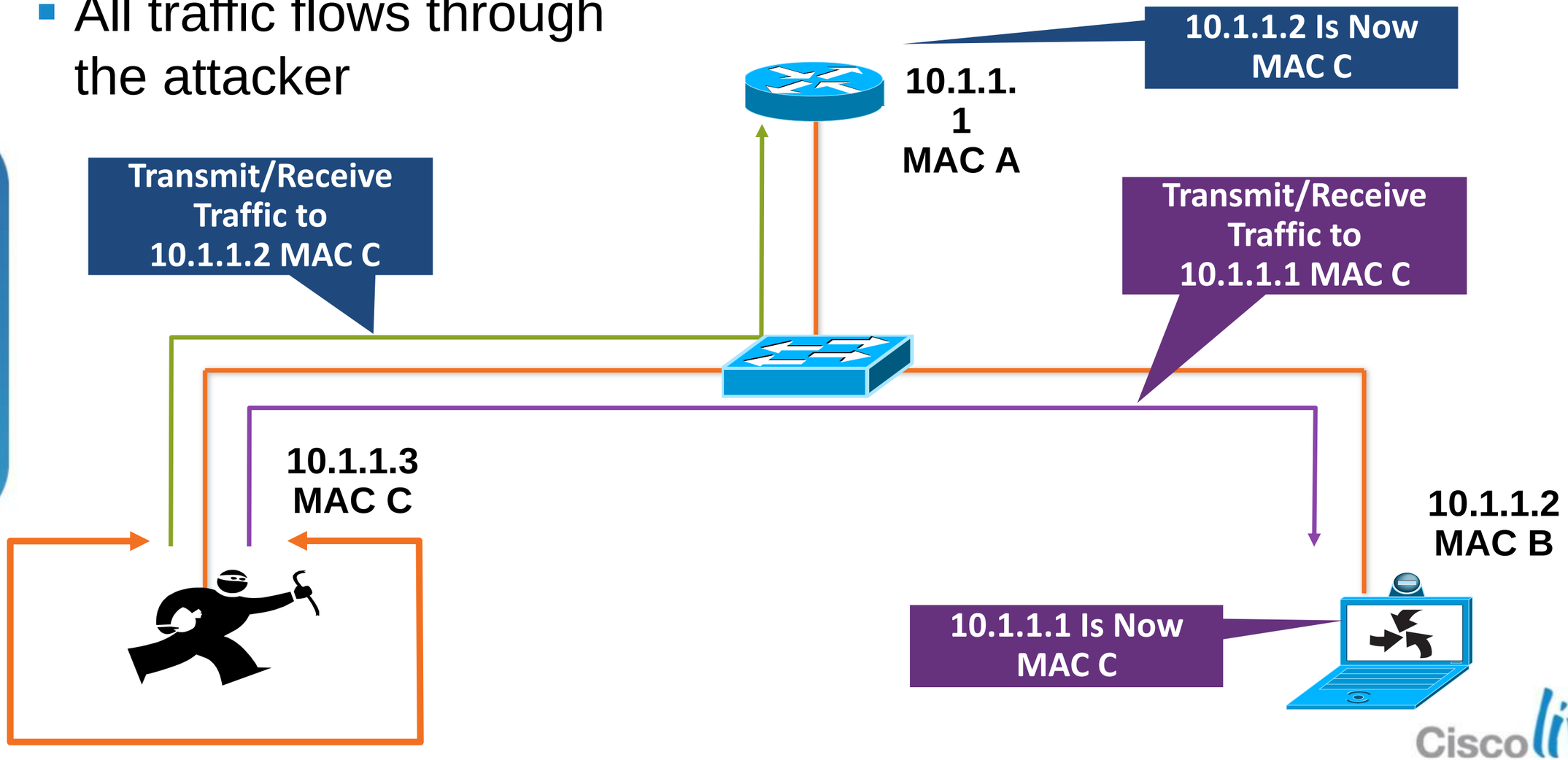
- Attacker “poisons” the ARP tables



Eavesdropping Protection

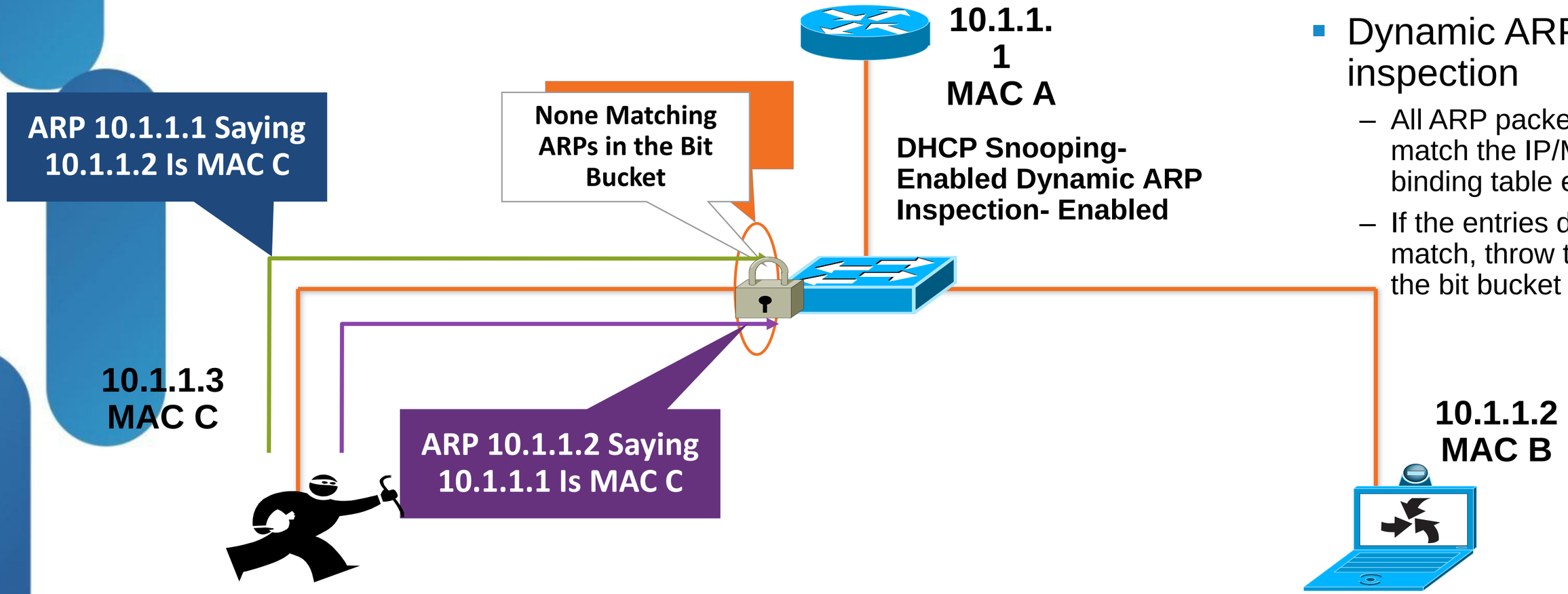
Switches: ARP Attacks

- All traffic flows through the attacker



Eavesdropping Protection

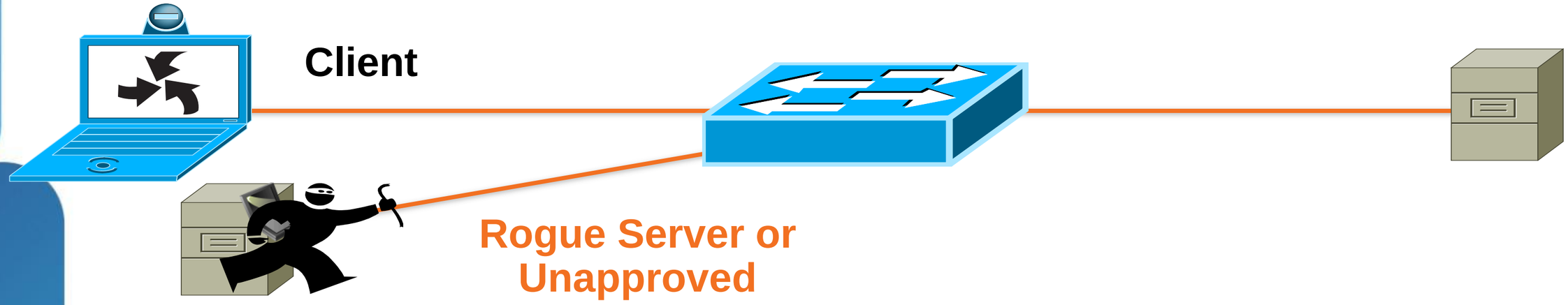
Switches: Dynamic ARP Inspection



- Uses the DHCP snooping binding table information
- Dynamic ARP inspection
  - All ARP packets must match the IP/MAC binding table entries
  - If the entries do not match, throw them in the bit bucket

Eavesdropping Protection

Switches: Rouge DHCP Server



DHCP Discovery (Broadcast) →

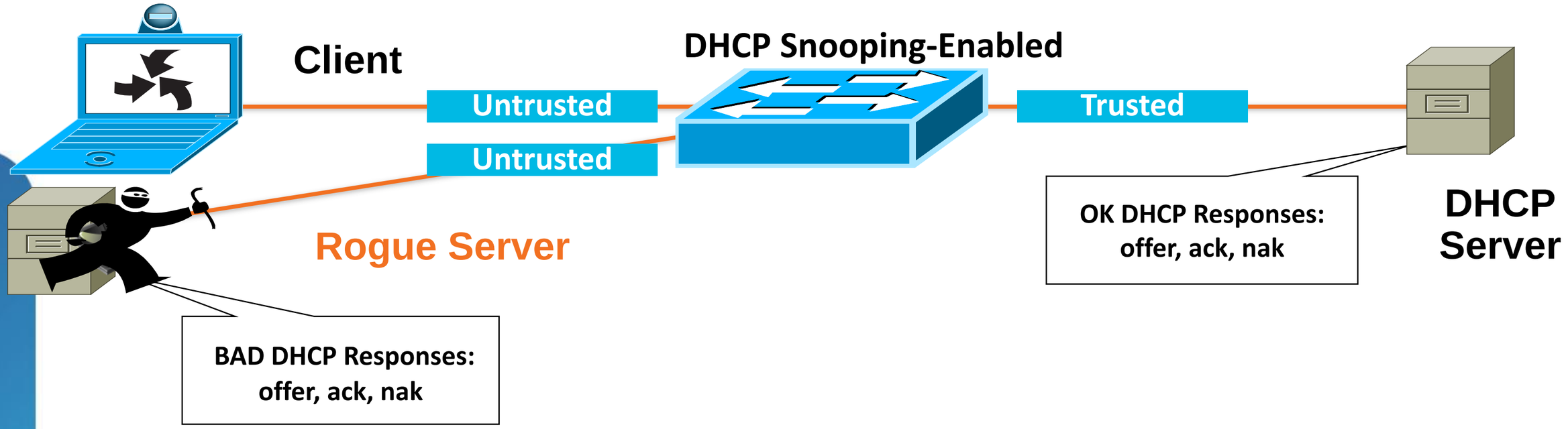
← **DHCP Offer (Unicast) from Rogue Server**

DHCP Request (Broadcast) →

← **DHCP Ack (Unicast) from Rogue Server**

Eavesdropping Protection

Switches: DHCP Snooping



- DHCP snooping prevents someone from becoming a DHCP server
  - They can not reroute traffic to themselves as the router
  - They cannot blackhole data by giving out the wrong default gateway

DoS Attack Prevention

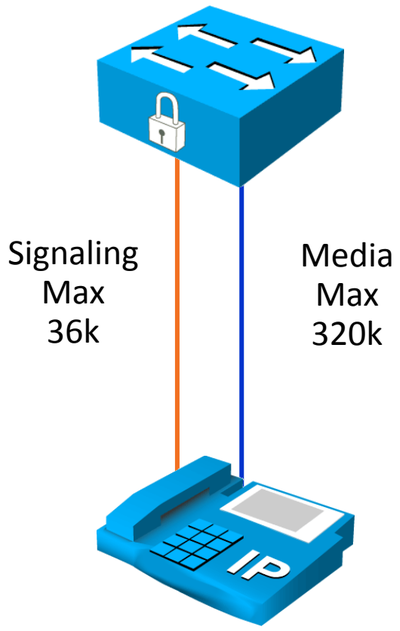
Switches

- Many ways to prevent DoS on a switch
  - Port Security
  - Voice VLAN
  - STP features
- Single biggest tool to use for VoIP is something you already should have turned on
  - QoS

DoS Attack Prevention

Switches

- Most basic QoS limits (Auto QoS)
  - Signaling 36k
  - Media 320k
- Protects both your applications servers and gateways from being overrun
- With more advance QoS you can run “scavenger class” QoS
  - This limits the entire amount the user can send before the traffic is remarked to less then best effort



DoS Attack Prevention

Switches—Port Security (Dynamic)

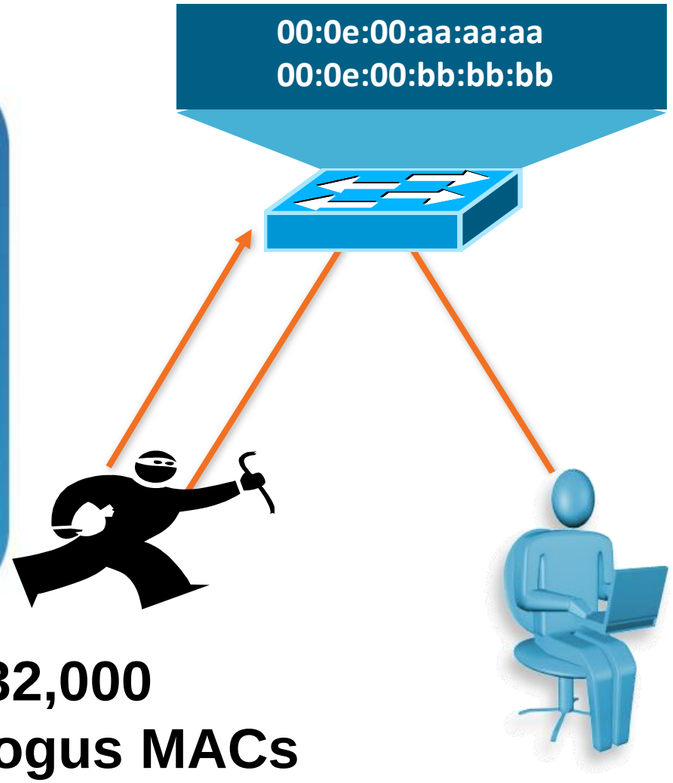
- Port security (dynamic) learns the amount of MAC addresses that are allowed either on the port or the VLAN
- Will protect the switch from a “MAC CAM Flooding Attack”

```
macof –i eth1
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512
```

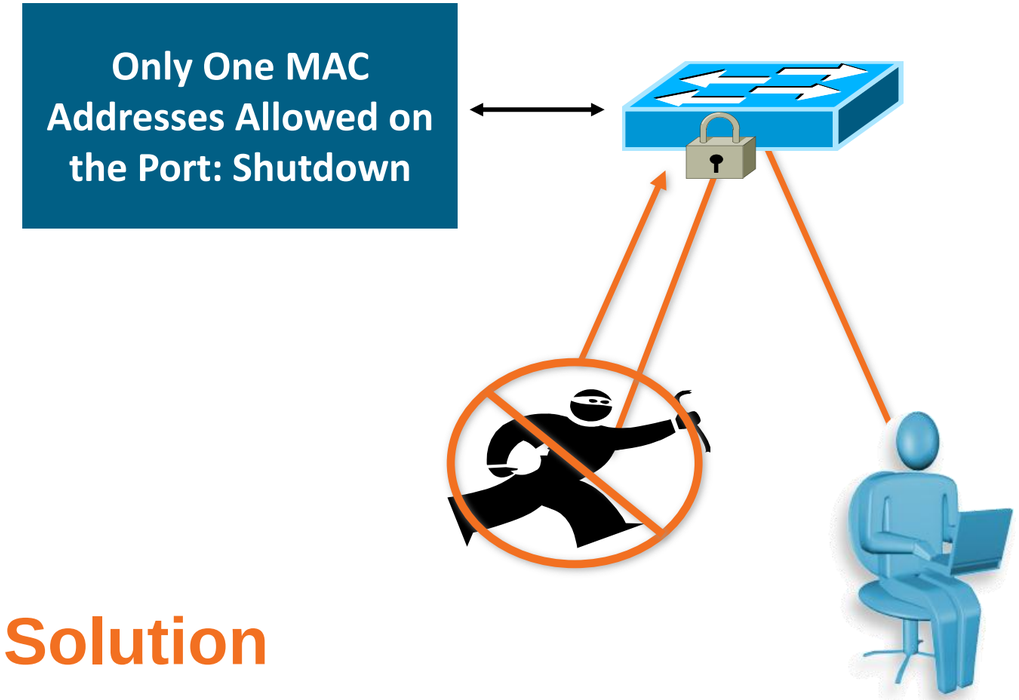
- Macof sends random source MAC and IP addresses
- Can send up to 8000 MACs a second
- Turns your VLAN on a switch into a hub

DoS Attack Prevention

Switches—Port Security (Dynamic)



132,000 Bogus MACs



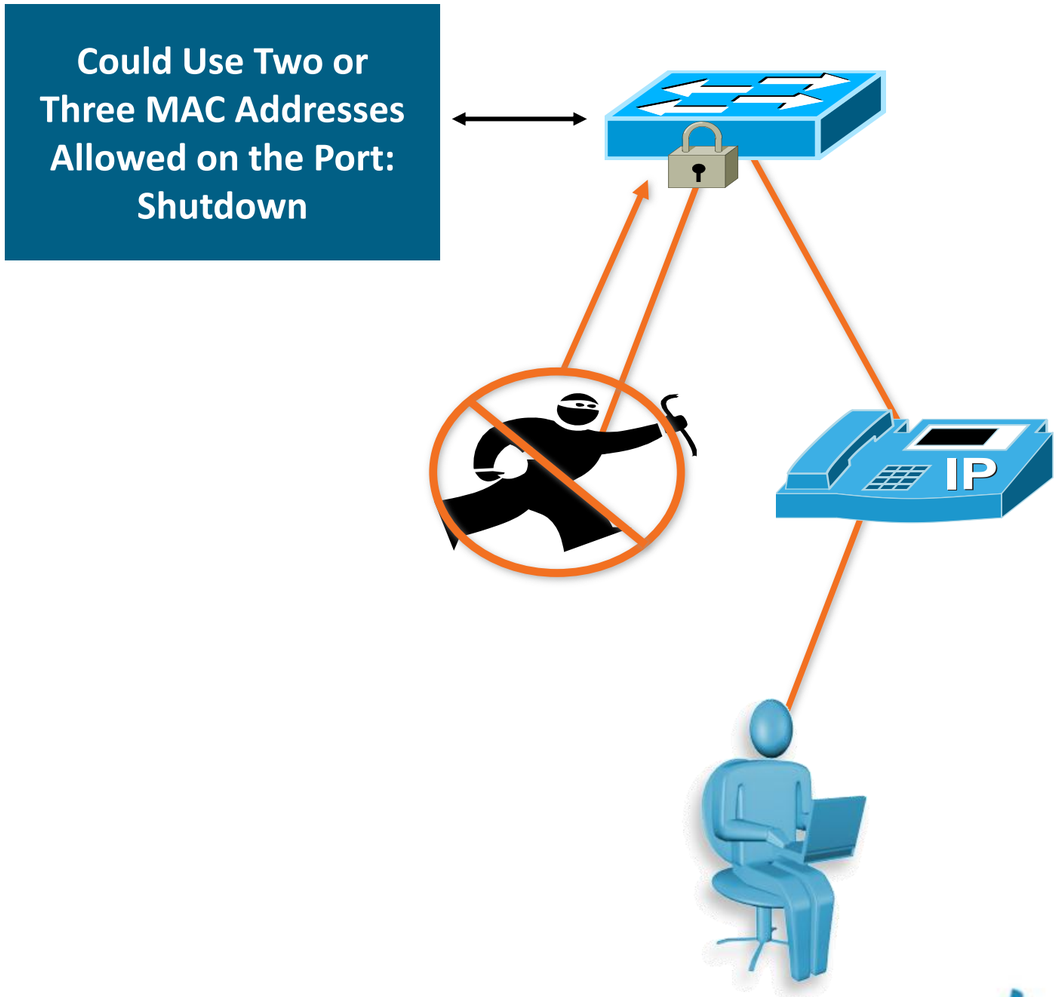
Solution

- Port security limits MAC flooding attack and locks down port and sends an SNMP trap

DoS Attack Prevention

Switches—Port Security (Dynamic)

- Phones can use two or three depending on the switch hardware and software
- Default config is disable port, might want to restrict for VoIP
- This feature is to protect that switch, you can make the number anything you like as long as you don't overrun the CAM table



Port Security and LLDP-MED

- Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP)
  - A standard that works like CDP for media endpoints
  - Could affect port security deployments
- If the switch does not understand LLDP-MED
  - You will need to set the port to three; the device (phone) can be in both VLAN—voice and data—and the PC will be in the data VLAN
  - Or the setting can be two for the data VLAN (one phone and one PC) and one in the voice VLAN for the phone
- If the switch supports LLDP-MED
  - The LLDP-MED should be treated as CDP and will not be counted on the port so the setting could be two or higher
  - Early versions of switch Cisco IOS did count the LLDP-MED, so please be careful with the settings

Switch Configuration

Voice VLAN

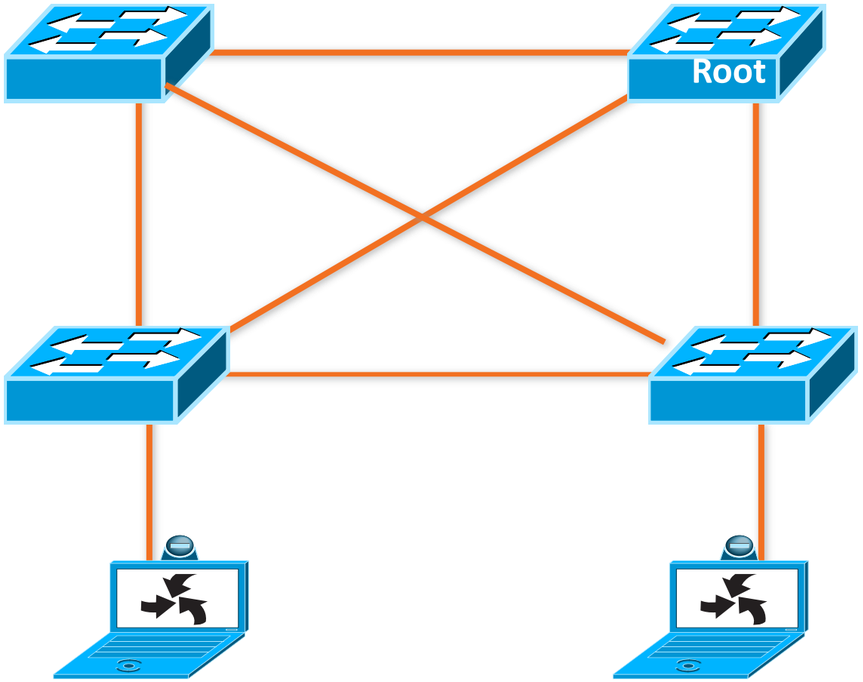
- Does give you logical separation from the rest of your data
- Allows for easier ACLs if all VoIP devices are in their own IP scope
- Control point for allowing communications in and out of the voice segment of the network
  - Example: Phones only use UDP to talk to each other, an ACL can be written to prevent all TCP traffic between a softphone and a hard phone
  - Best attacks are usually TCP-based

Switch Configuration

STP Enhancements

- STP purpose: to maintain loop-free topologies in a redundant Layer 2 infrastructure
- A switch is selected as root
- A ‘tree’ like loop free topology is established from the perspective of the root bridge

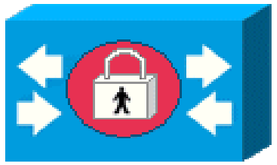
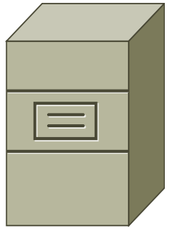
- Avoiding loops ensures broadcast traffic does not become storms
  - BPDU Guard
  - Root Guard



IEEE 802.1X

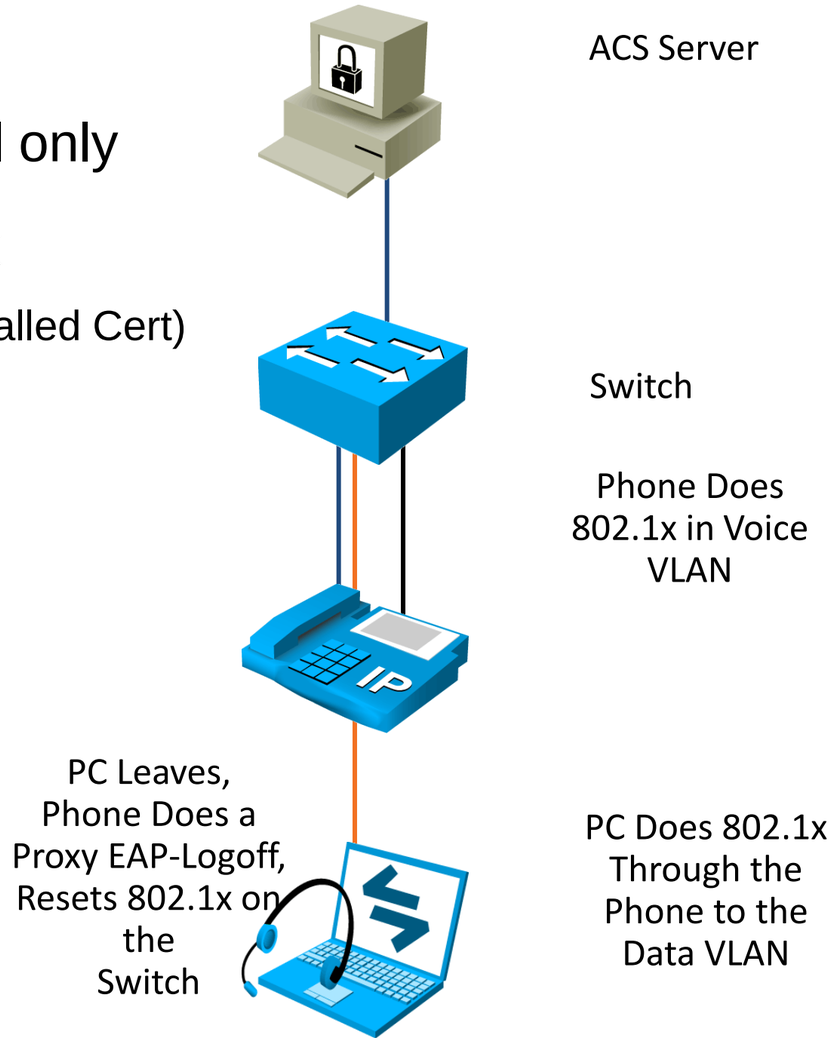
- 802.1x on IP phones
  - Network based rather than applications-based identity
  - Can be used in conjunction with extension mobility
  - Once the authentication is completed, the phone will operate normally
- 802.1x on host OSs of Soft Clients
  - Can be used to identify the end user or device
  - Will dynamically assign the VLAN they are allowed to use
  - VLAN-based authentication will determine if they have access to the UC system

802.1X Components

Supplicant	Authenticator	Authentication Server	Backend Database
802.1X Client	Switch	RADIUS Server	AD, LDAP etc
			
Submits credentials for authentication	Forwards credentials to the authentication server	Validates supplicant credentials	Supports authentication server functions

802.1x Port Based Authentication

- 802.1x is an admittance protocol only
- Cisco supports EAP-TLS 802.1x
  - Based on the MIC (Manufactured Installed Cert)
  - Or LSC (Locally Significant Cert)
- Multi-Domain Auth (MDA) with MAC-Auth-Bypass (MAB)
  - MDA authenticates two devices bound to an assigned VLAN
  - MAB authenticates MAC address only for devices without supplicants



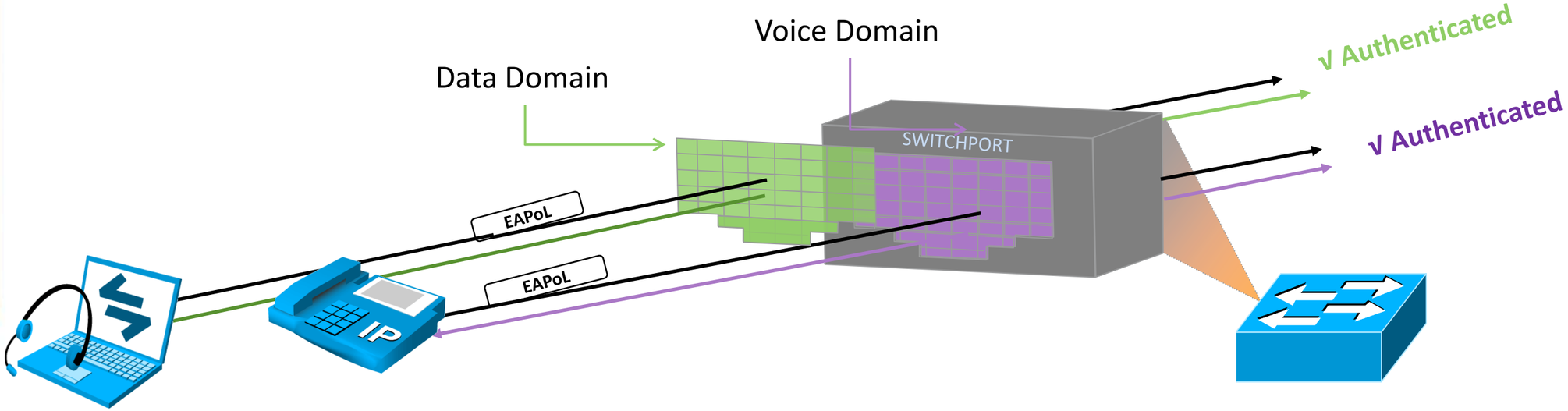
Multi Domain Authentication (MDA)

IEEE 802.1X

Single device per port

MDA

Single device *per domain* per port

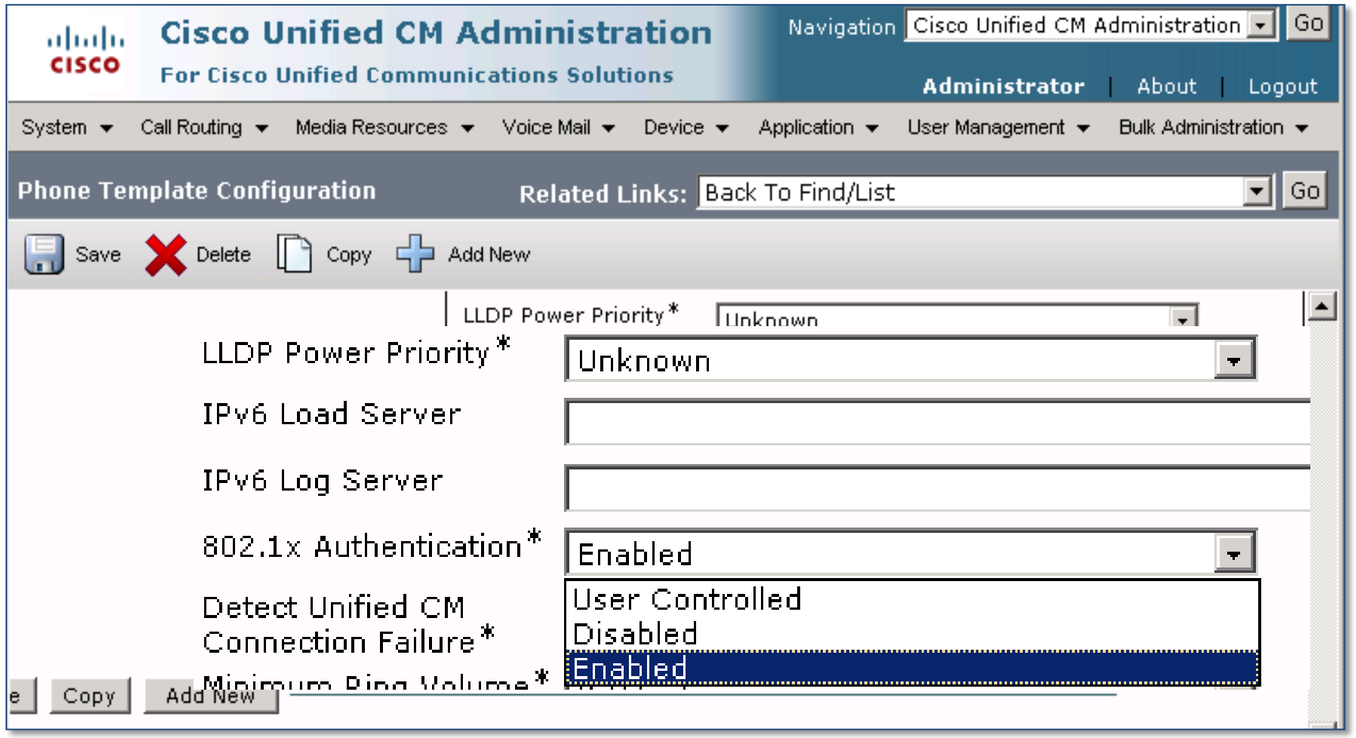


802.1X EAP Methods on Cisco IP Phones

Method	Phone Credential	Deployment Considerations
EAP-MD5	Username/Password	Password manually configured on phone Phone name/password must be in AAA Difficult to deploy
EAP-FAST with TLS	MIC or LSC	Supported on ACS 4.2
EAP-TLS	MIC or LSC	Phone certificate configuration done on CUCM Deployable with ACS 5.x TLS certificate validation does not require entering phone username in any database

802.1X on Cisco IP Phones

- 802.1X is enabled in IP Phone Device configuration page in CUCM Administration
- Can be edited in BAT template
- Requires phone to be registered to CUCM



802.1X Deployment for IP Phones

- Non 802.1X staging area
  - Initial phone boot up in network without 802.1X
- Manually configure phone for 802.1X
- Use MAB to get the device on the network
  - Limited access for configuration
- Use MIC to get the device on the network
  - Limited access for configuration
- After initial configuration using MAB or MIC certificate, install LSC on phones for full access
  - CUCM 8.x and later: LSC installs don't require etokens

Agenda

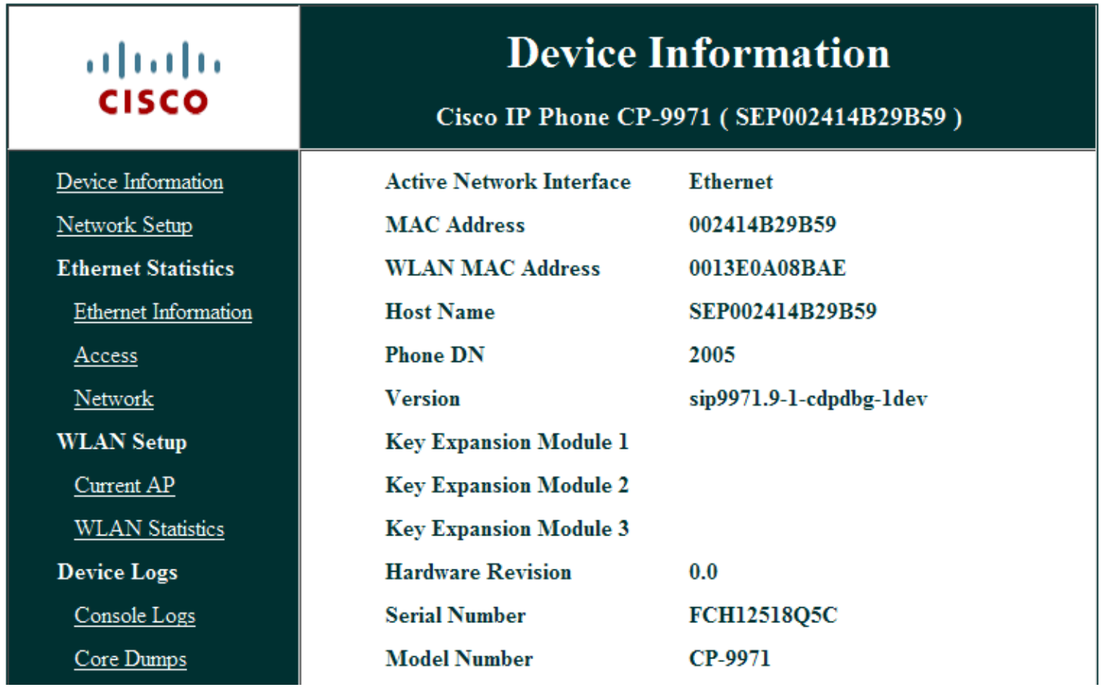
- Security Requirements for Unified Communications
- Unified Communications System Environment
- Defining Attacks on UC Systems
- Access Layer Security
- Endpoint Security
- Encryption
- Firewalls
- Secure Remote Access
- Security for IP PSTN
- Security for Video

Endpoint Security

IP Phone Hardening

Web Access

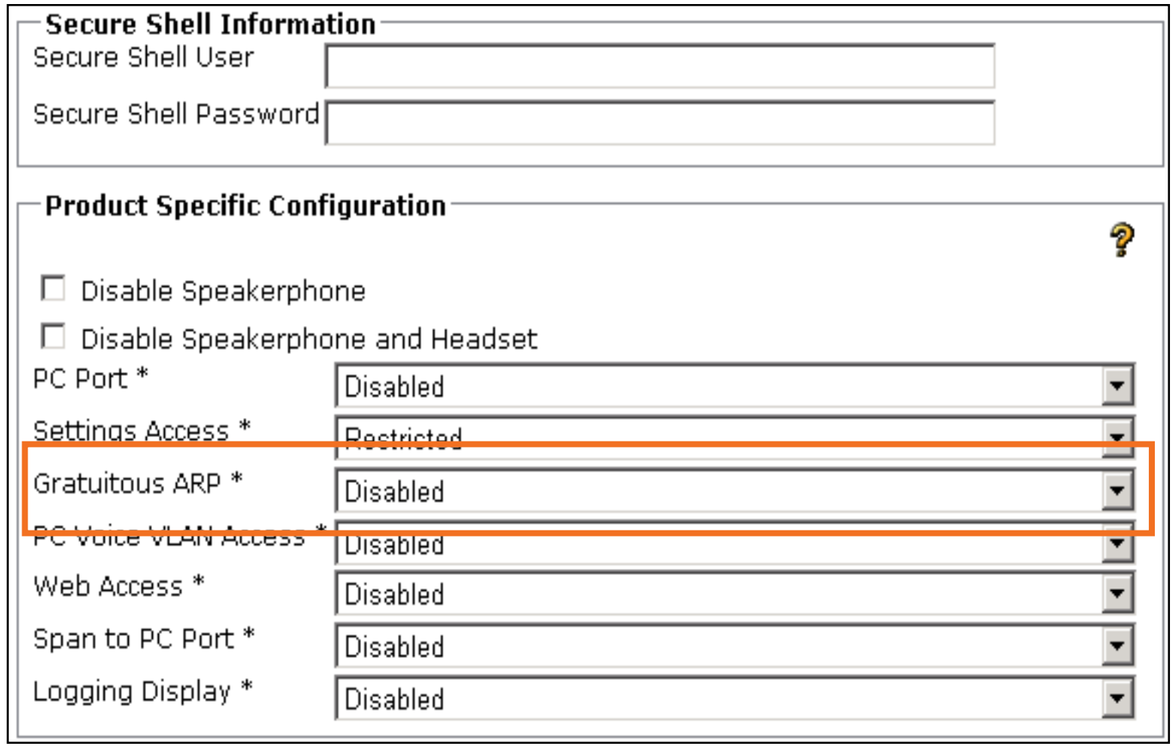
- Control web access to phones with ACLs
  - Default gateway
  - DHCP server
  - DNS server
  - TFTP server
  - CUCM(s)
  - Directory server
  - etc.
- Disable the phone's web server
  - Disabling web access also breaks XML pushing apps



IP Phone Hardening

MITM Prevention

- Phones have the capability to protect their data streams from Man in the Middle Attacks
- Only protects data from the phone
- If devices are not Layer 2 adjacent it is much harder to run a MITM attack



IP Phone Hardening

Settings

- Restricting the Settings Access to the phone
- Keeps a phone from displaying network information
  - Call Managers IP, VLAN ID, etc.
- Usually enabled by default

Secure Shell Information

Secure Shell User

Secure Shell Password

Product Specific Configuration

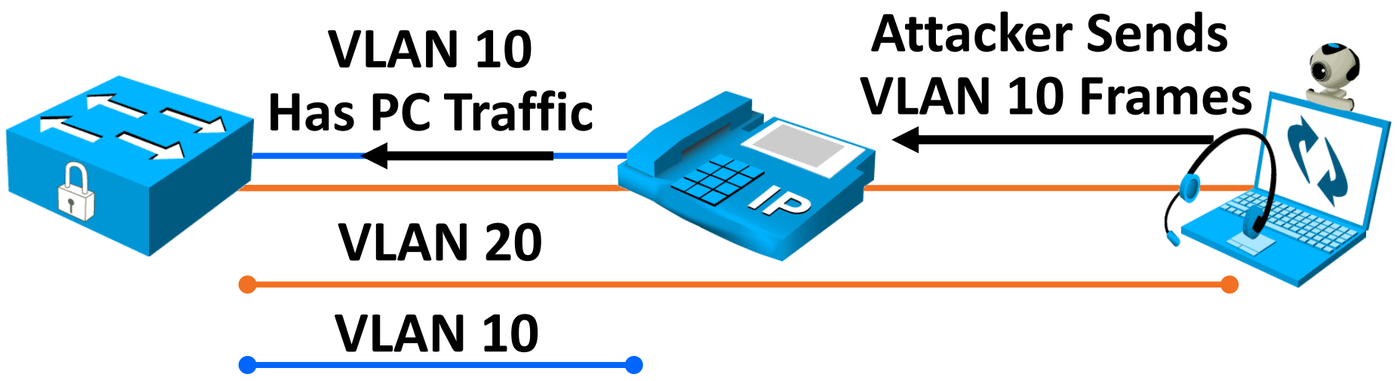
☐ Disable Speakerphone

☐ Disable Speakerphone and Headset

PC Port *	Disabled
Settings Access *	Restricted
Gratuitous ARP *	Disabled
PC Voice VLAN Access *	Disabled
Web Access *	Disabled
Span to PC Port *	Disabled
Logging Display *	Disabled

IP Phone Hardening

Voice VLAN Access



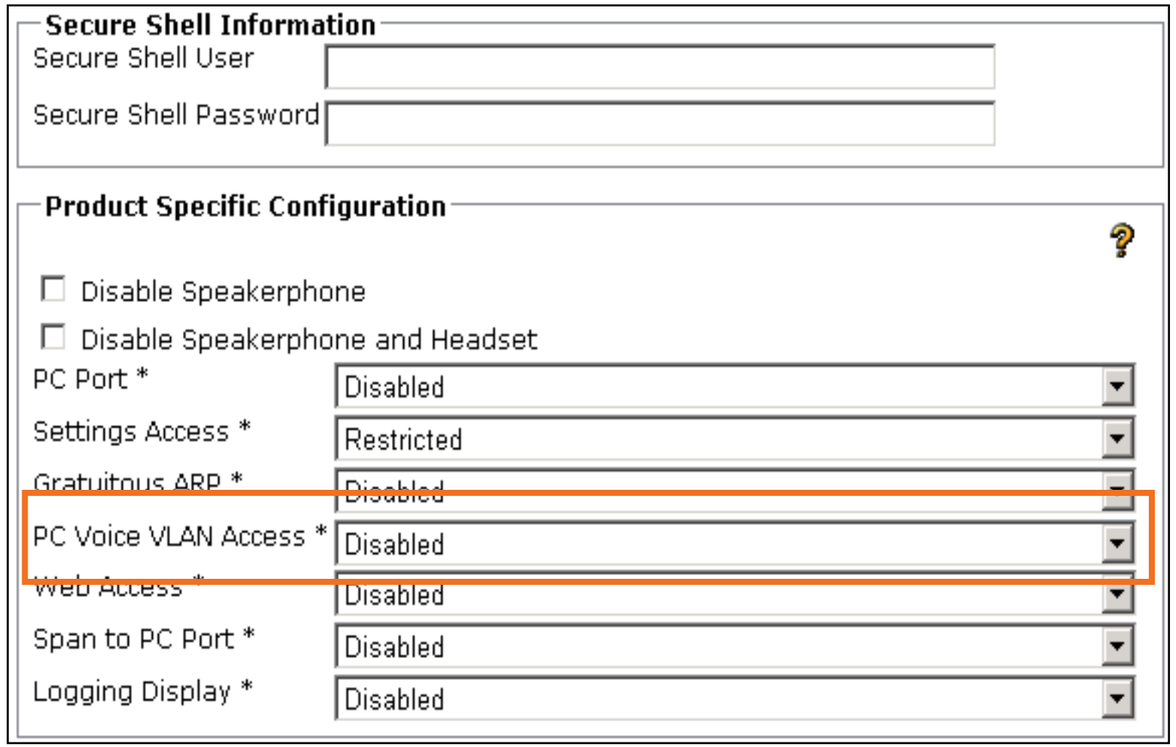
Getting Into the Voice VLAN

- Attacker sends 802.1q tagged frames from the PC to the phone
- Traffic from the PC is now in the voice VLAN

IP Phone Hardening

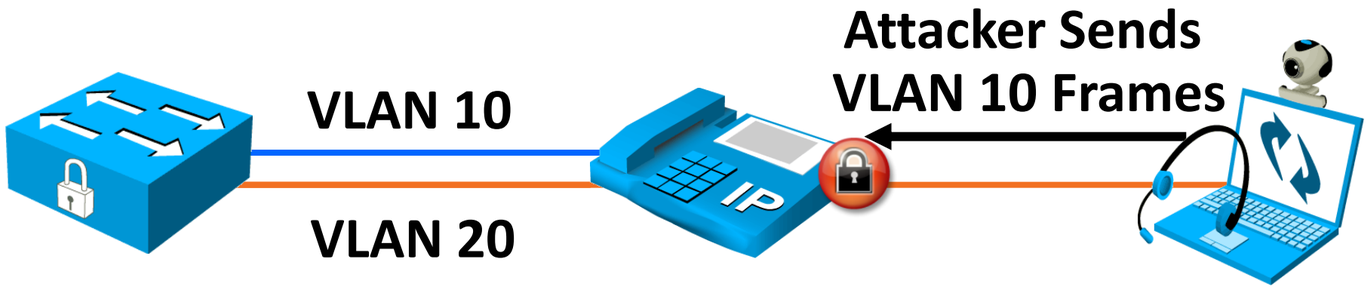
Voice VLAN Access

- Phones have the ability to prevent Voice VLAN access
- Will prevent someone plugged into the phone getting access
- Usually enabled by default



IP Phone Hardening

Voice VLAN Access



- Preventing voice VLAN attacks
  - Enable settings for PC voice VLAN access
  - Tagged traffic will be stopped at the PC port on the phone
- Differences between phone model implementations
  - 7940, 7960, 7941G, 7961G, and 7971G only block voice VLAN, allowing PC to run 802.1Q on any other VLAN
  - 7970, 7961, and 7941 block all packets containing an 802.1Q header
  - 7912 doesn't block anything

IP Phones DoS Protection

- Phones have been tested for network-based attacks
- Runts, shorts, giants, malformed packets, etc.
- Will not accept invites from other non CUCM devices
  - Cannot send any SIP invite to a SIP phone registered to a CUCM

Agenda

- Security Requirements for Unified Communications
- Unified Communications System Environment
- Defining Attacks on UC Systems
- Access Layer Security
- Endpoint Security
- Encryption
- Firewalls
- Secure Remote Access
- Security for IP PSTN
- Security for Video

Encryption

Attack Prevention

IP Phone Integrity

- Signed firmware images
- Signed configuration files
- TLS/SRTP

Encryption

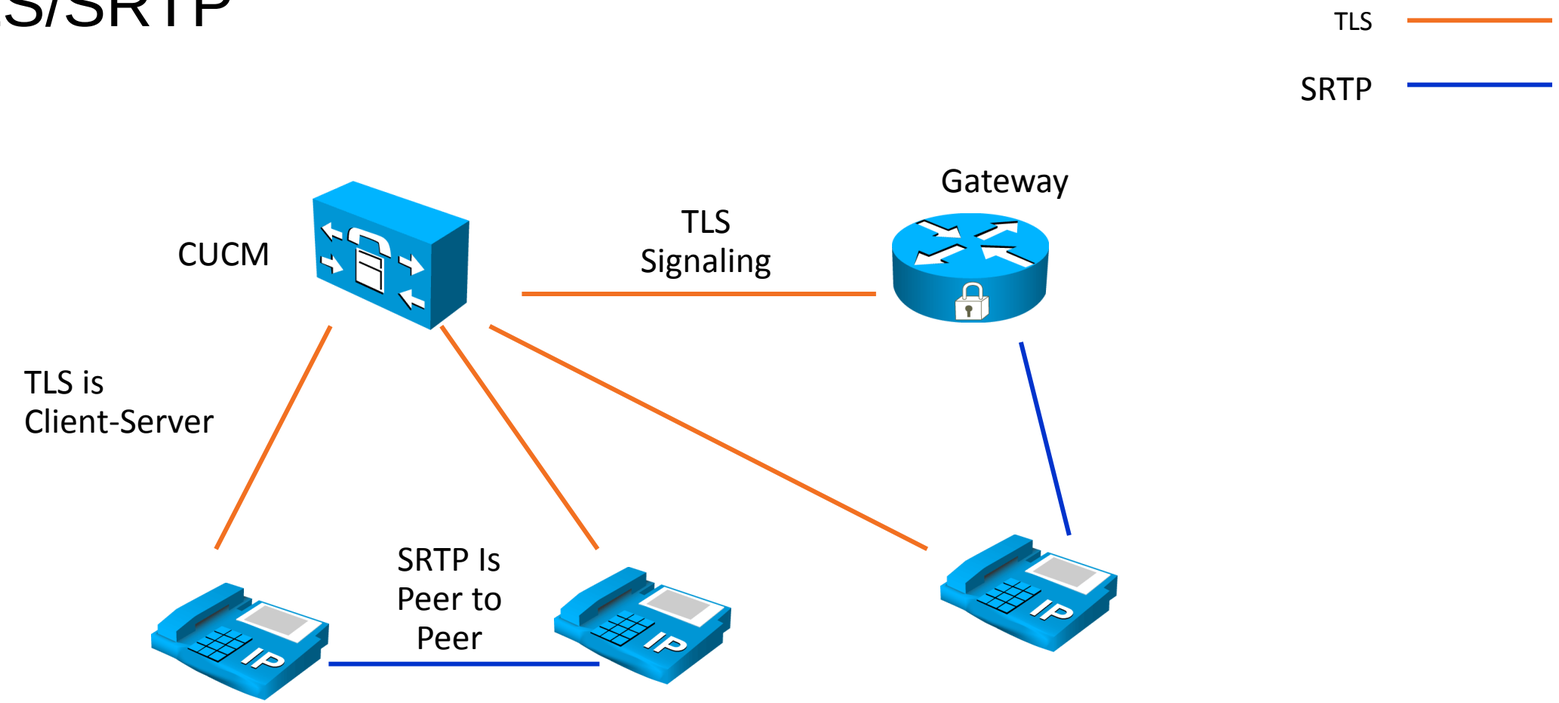
Signaling and Media

- Prevents attackers from playing back the conversation
  - The system uses new keys for every conversation
  - X.509v3 digital certificates
  - Transport Layer Security (TLS)
  - Secure Real Time Protocol (SRTP)

- Does not prevent someone from being able to capture the streams
  - MITM attacks still work, unable to replay the voice because of the encryption

Encryption

TLS/SRTP



- Will affect the number of phones that can be attached to a cluster
  - Use the Unified Communications sizing tool to make sure everything will fit on the systems you have
  - http://tools.cisco.com/cucst/faces/login.jsp

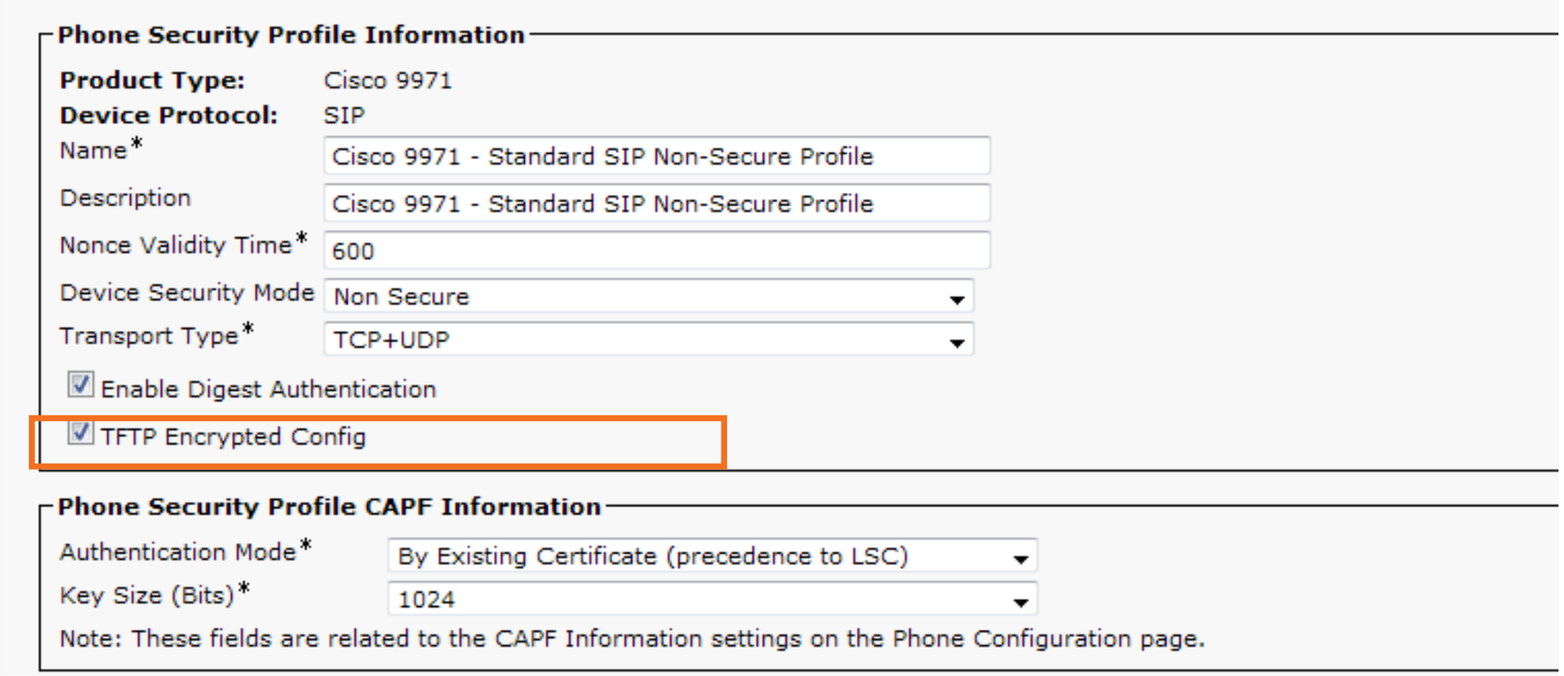
Encryption

Configuration File Encryption

- Protect privileged information
  - SIP Digest Authentication Credentials
  - SSH Passwords used for CLI debugging
  - Server addresses such as CUCM, TFTP & CAPF
- Integrity provided by config file signing in both SCCP and SIP loads
- Encrypted configuration file keys
  - Can use public key if phone has a certificate
  - Must manually enter into phone otherwise

Encryption

Configuration File Encryption



- TFTP Encrypted Config option in Phone Security Profile
- CUCM 7.x - Cluster in Mixed Mode
- CUCM 8.x and later – Security By Default

Agenda

- Security Requirements for Unified Communications
- Unified Communications System Environment
- Defining Attacks on UC Systems
- Access Layer Security
- Endpoint Security
- Encryption
- Firewalls
- Secure Remote Access
- Security for IP PSTN
- Security for Video

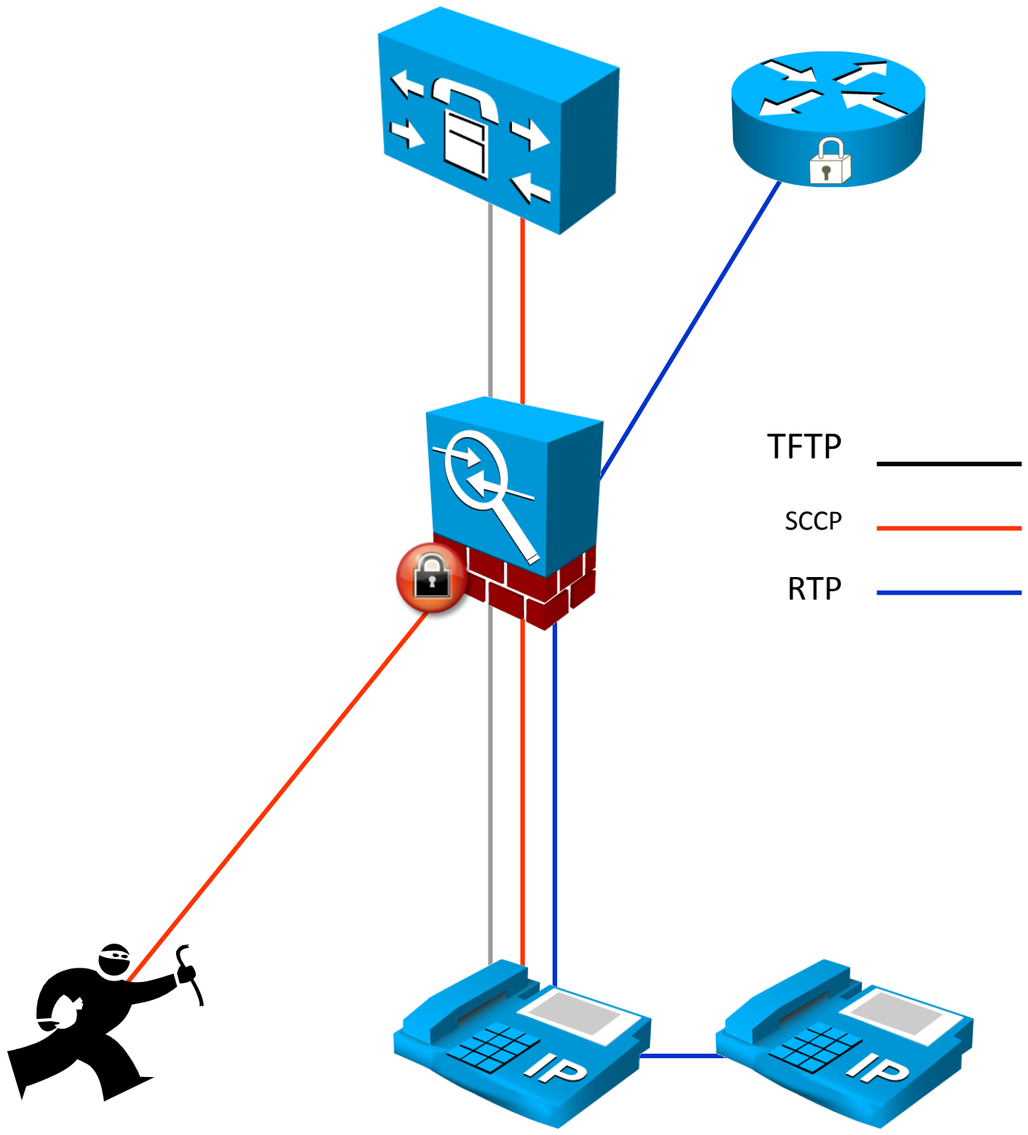
Firewalls

DoS Prevention using ASA and IOS Firewalls

- Application Layer Protocol Inspection Engine for
  - H.323, SIP, SCCP, MGCP, RTSP, RTP, RTCP
- These packets are checked as they flow through the firewall to ensure they meet the RFCs or Cisco specs
- If messages and packets do not meet the requirements through the firewall they are blocked
- Rate limit on most of the protocols that flow through the firewall

DoS Prevention using ASA and IOS Firewalls

- Phone registers, gets its image, config and then operates normally
- All the protocols that are used are inspected
- If anything out of the ordinary happens, those packets are thrown away
- Dynamically opens ports for the RTP through the firewall based on signaling
- Protects data going through the firewall, RTP is peer to peer



Firewalls and UC Systems

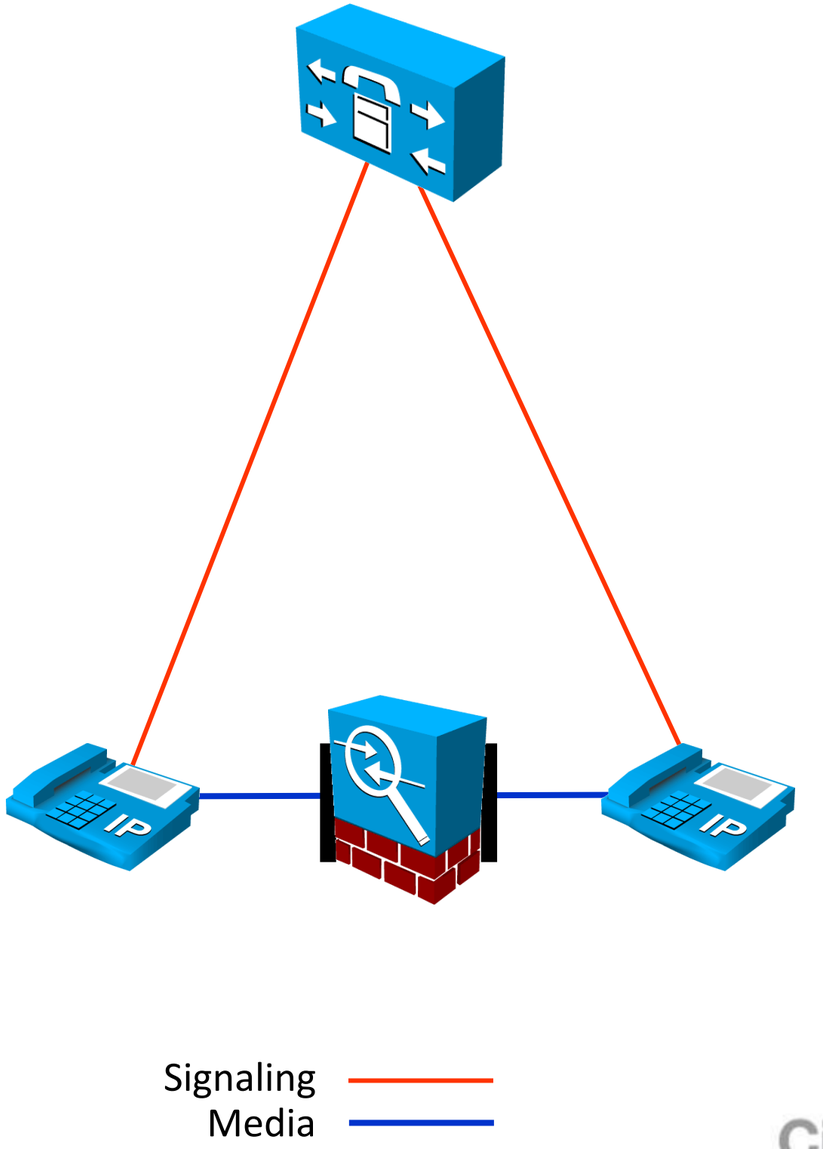
General Firewall Rules

- Signaling makes a firewall work
  - As long as the firewall understands the signaling, RTP will function correctly
- If you upgrade a voice application server the firewall might be affected
- As we add new media to the solution it might not work through the firewall day one
- A constant battle to keep up with the changes
- Check the software compatibility list from system test on
  - http://www.cisco.com/go/firewalls/

Firewalls and UC Systems

General Firewall Rules

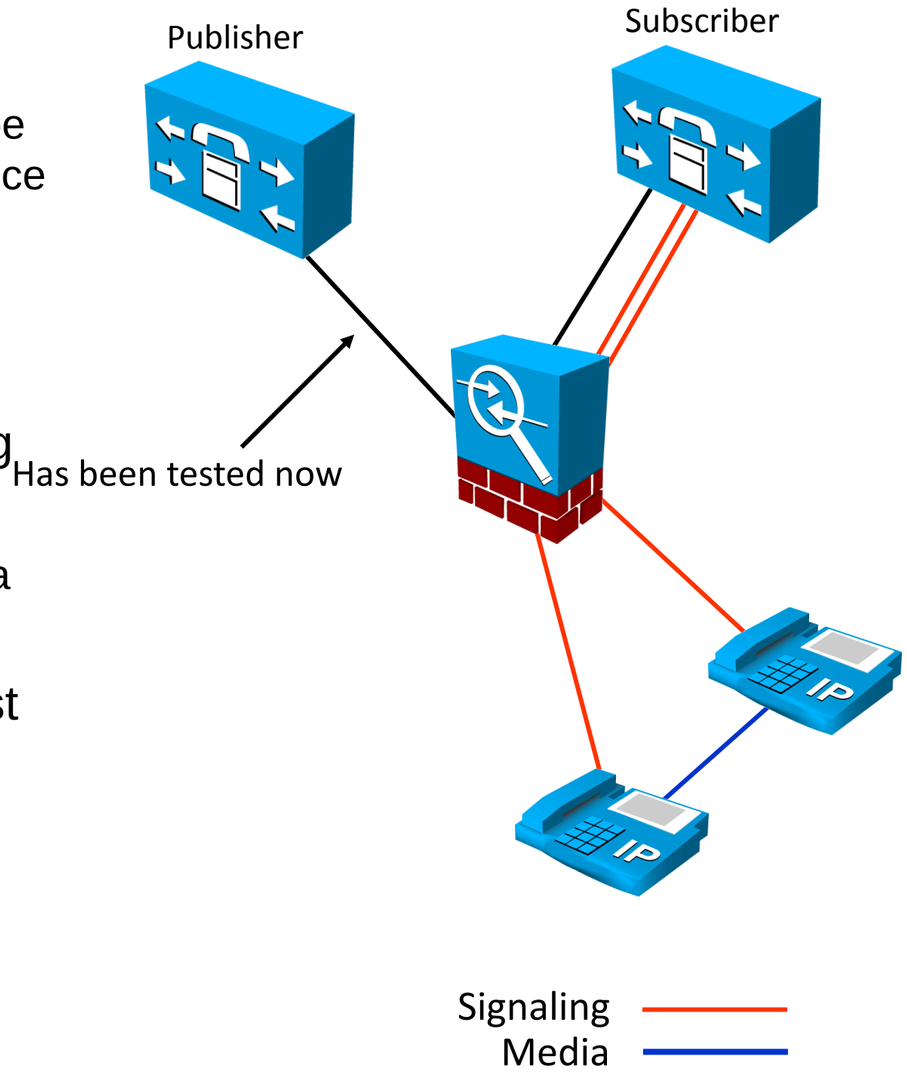
- If the signaling is not through the firewall
  - Dynamic RTP ports cannot be opened
  - Media will not flow through the firewall
  - Calls will not complete
- Have to open up the UDP port range for RTP to make this work (ACL)
- Most firewall deployments are centralised to make sure that the signaling runs through the firewall
- Can make VoIP designs hard with firewalls



Firewalls and UC Systems

General Firewall Rules

- Operationally hard
  - Firewall will almost always need to be upgraded when you install a new voice application with inspections
- Run IPSec/MPLS or some other method to protect the cluster data
- The published ports list is a running system—not an upgrade
  - Upgrade ports will be different then a running system
- Check the software compatibility list on www.cisco.com



ASA Firewalls UC Features

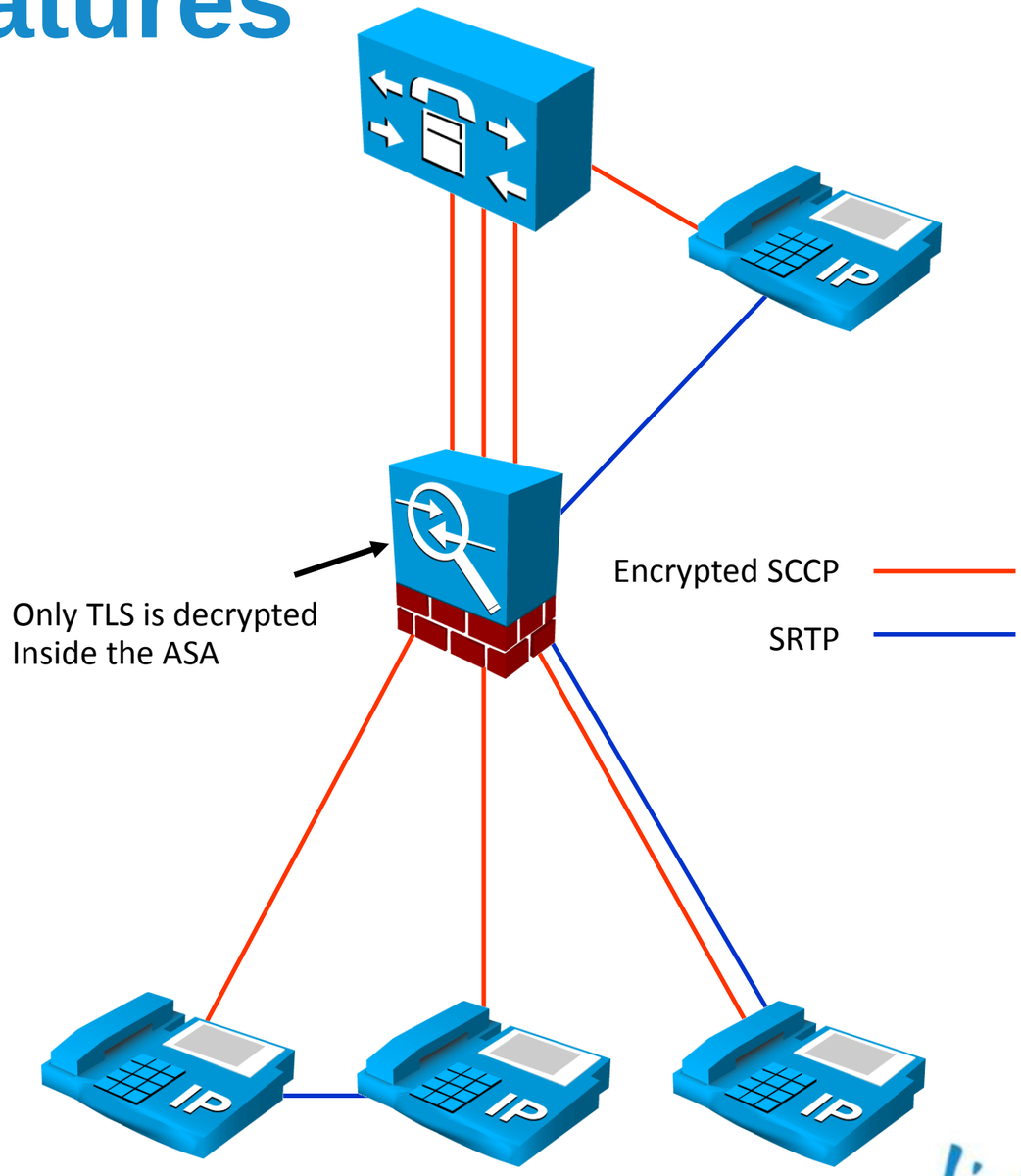
TLS Proxy

- Logical place to attack is with encryption
  - Just like HTTPS, attacking within TLS would hide the attack
  - All usual Firewalls have to use ACLs to get TLS through them
  - Inspection of signaling is usually lost
- This adds additional security and DoS protection when running TLS and SRTP with ASA version 8.0(2)

ASA Firewalls UC Features

TLS Proxy

- Each phone has its own TLS session to and from the ASA
- Ports needed for SRTP are open and closed based on signaling
- SRTP is not inspected at this point
- SRTP may or may not flow though the ASA, usual RTP flows will occur



Agenda

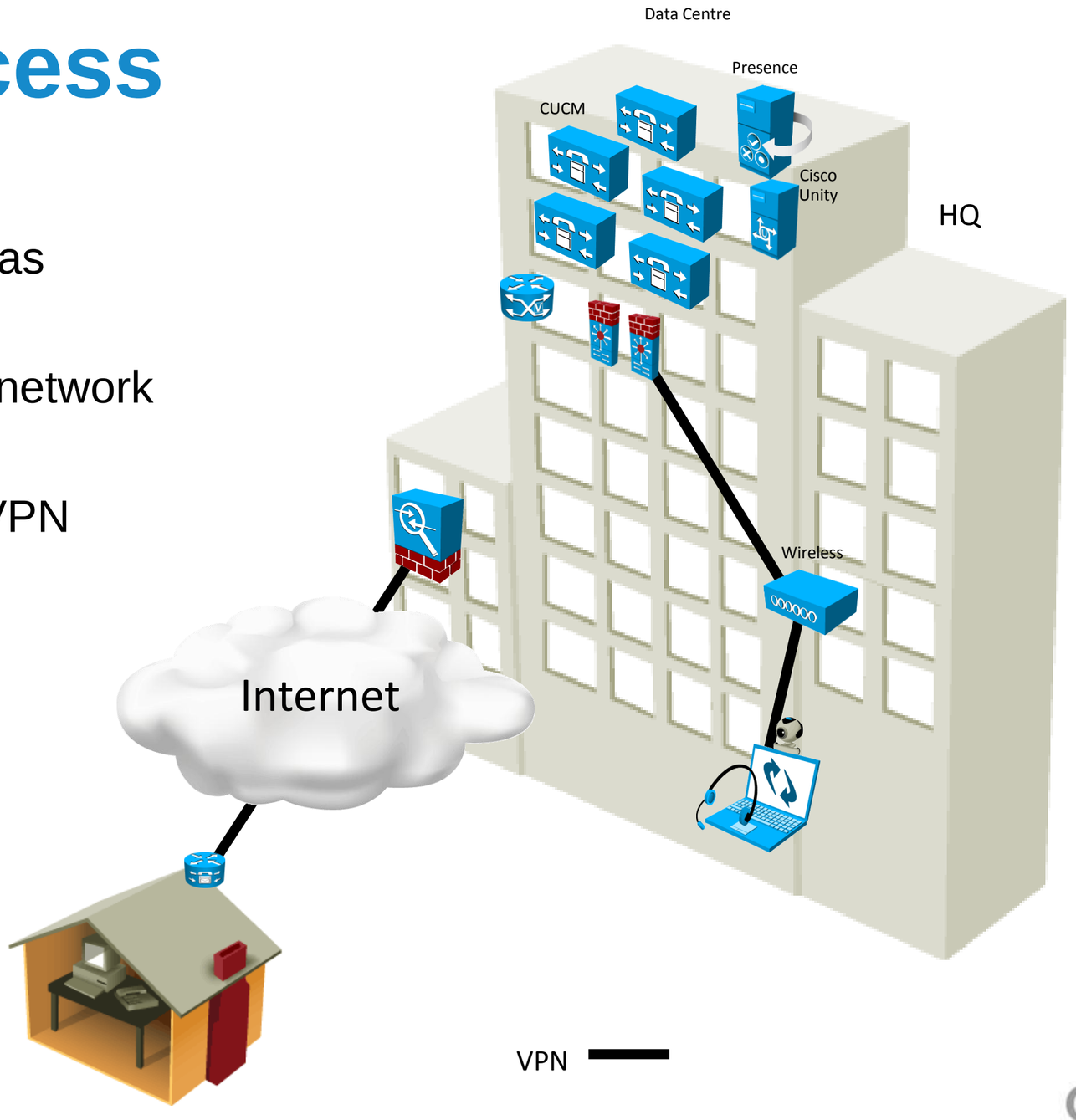
- Security Requirements for Unified Communications
- Unified Communications System Environment
- Defining Attacks on UC Systems
- Access Layer Security
- Endpoint Security
- Encryption
- Firewalls
- Secure Remote Access
- Security for IP PSTN
- Security for Video

Secure Remote Access

Remote Access

Network VPN

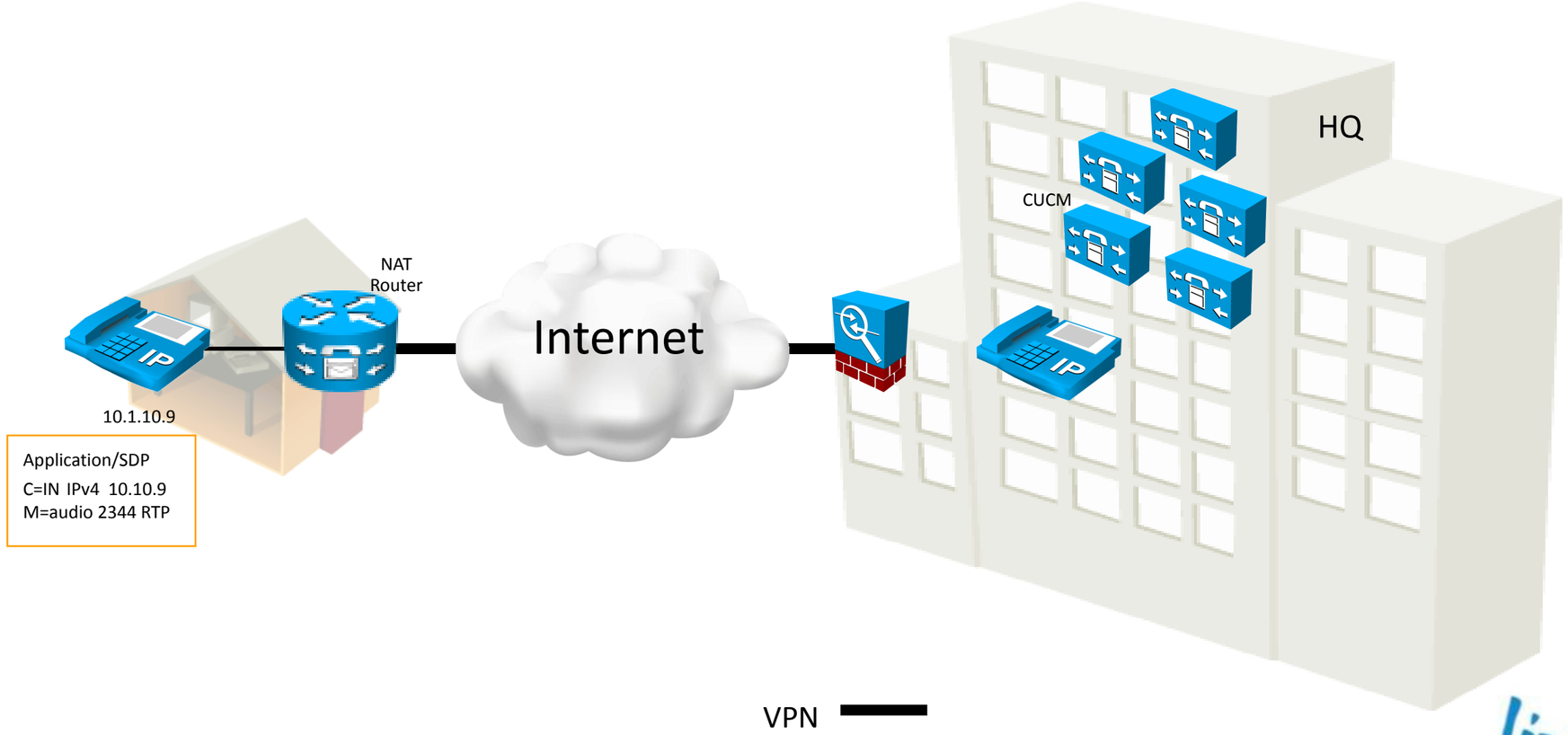
- The entire home user has a VPN for all traffic
- Extends the enterprise network to the users site
- Some companies use VPN for all softphones
  - This allows control of the flows to and from the voice side of the network



Remote Access

NAT and RTP

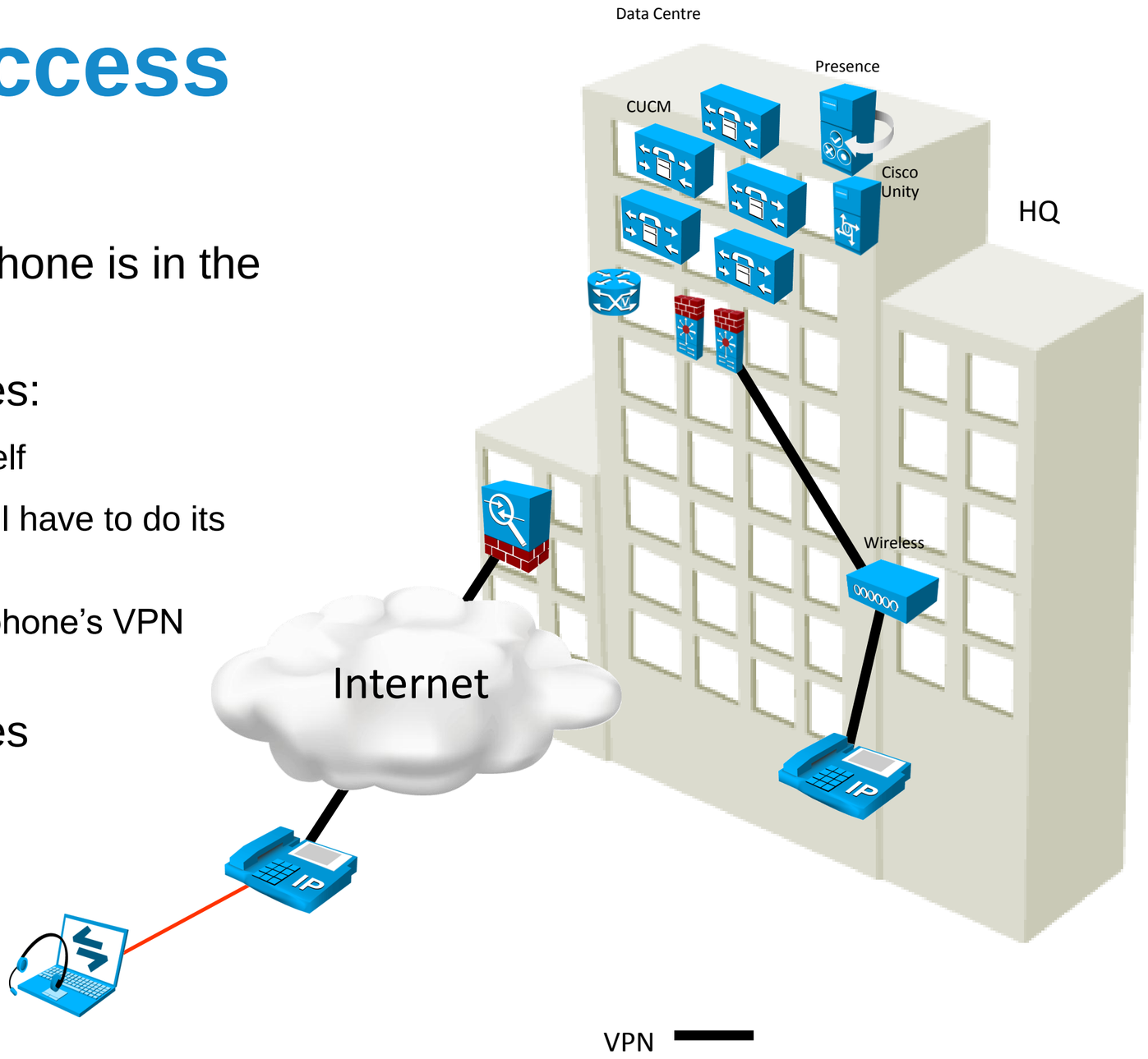
- NAT needs to translate the IP addresses in the signaling protocol
- ip nat service h225 | sccp | sip



Remote Access

Phone VPN

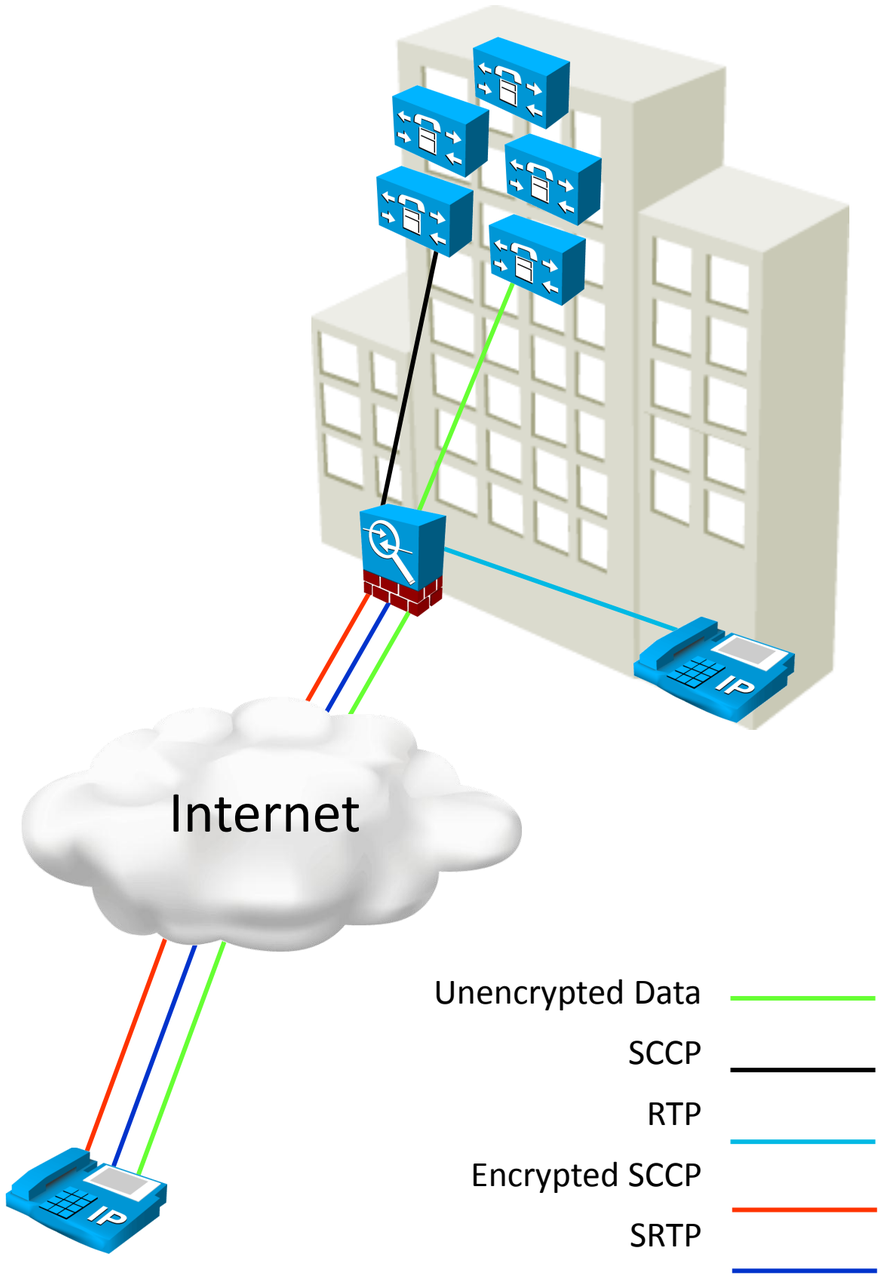
- All traffic from the phone is in the VPN
- The phone only does:
  - Traffic to and from itself
  - The PC plugged in will have to do its own VPN
  - VXC clients can join phone's VPN tunnel
- VPN for hard phones
  - CUCM 8.x



Remote Access

Phone Proxy

- ASA phone proxy can be used for remote users
- Only has encryption for remote users for TLS and SRTP
- All other messages to and from the phone are unencrypted
- By default, all other services are disabled that are not encrypted—Directory lookup, services, etc.
- Can be encrypted or not encrypted on the inside of the enterprise
- ASA 8.04



Agenda

- Security Requirements for Unified Communications
- Unified Communications System Environment
- Defining Attacks on UC Systems
- Access Layer Security
- Endpoint Security
- Encryption
- Firewalls
- Secure Remote Access
- Security for IP PSTN
- Security for Video

Security for IP PSTN

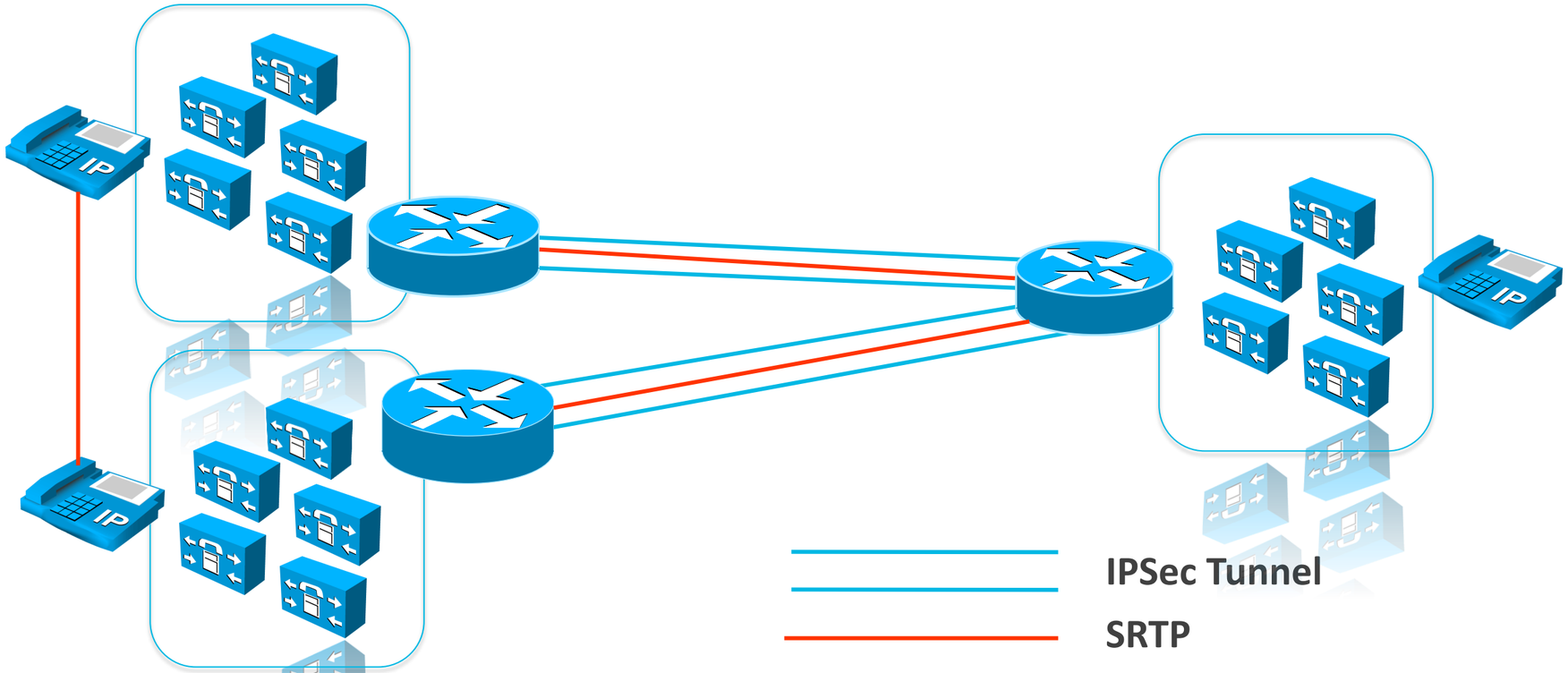
IP PSTN Trunks Security

- Secure Signaling and SRTP can be configured for SIP and H323 Trunks
  - SRTP security keys are sent in clear
  - SRTP requires signaling encryption
- SIP Trunk security supports TLS
  - Simpler to deploy
  - Less resource intensive
- H323 requires IPSec for signaling security
  - IPSec Tunnels should be set up in the network infrastructure (router/ASA)

IP PSTN

H323 Trunks

- H323 requires IPSec for signaling security
  - IPSec Tunnels should be set up in the network infrastructure (router/ASA)



IP PSTN

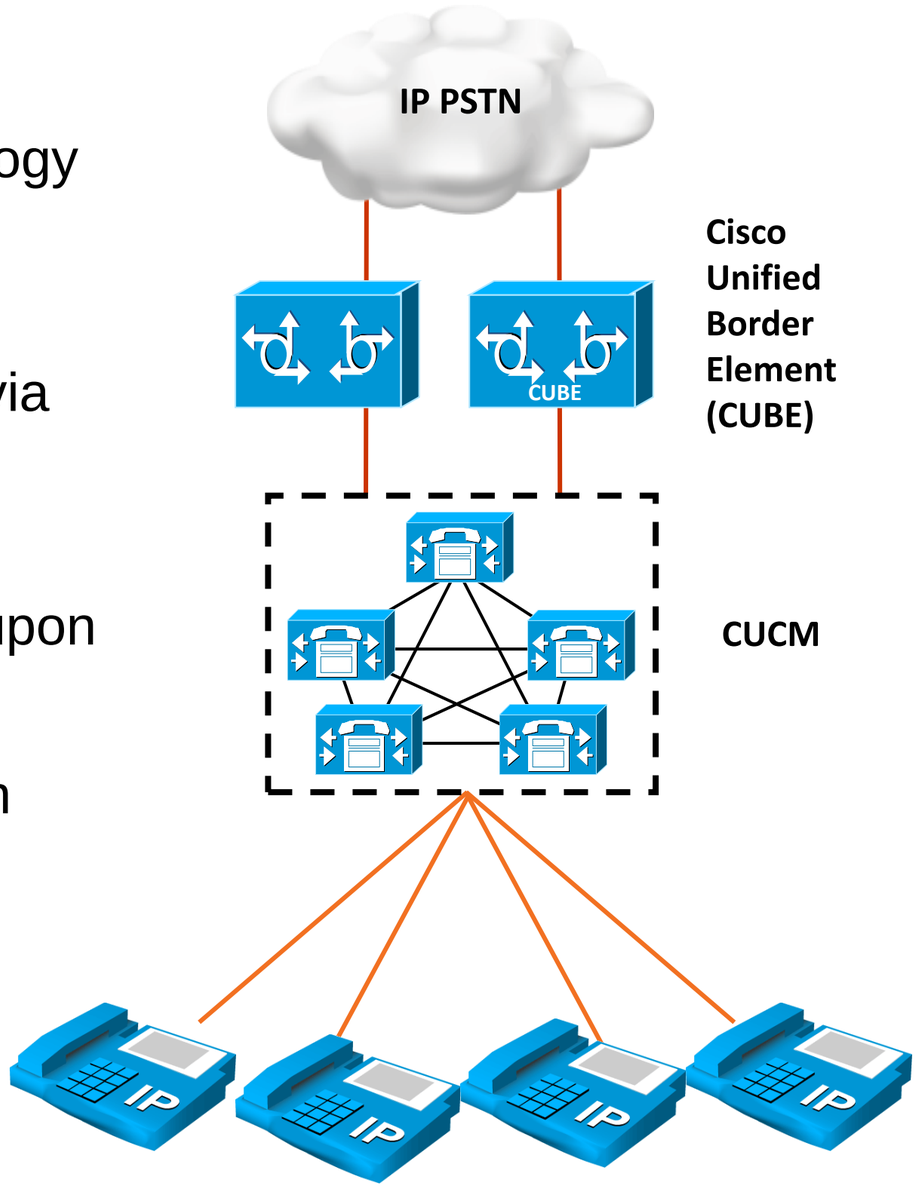
SIP Trunks

- Digest Authentication can be enabled in the SIP Line or Trunk Security Profile
- Client / Server Model
  - CUCM can only be server for SIP lines
  - CUCM can be client or server on SIP trunk
- Server Challenges, Client responds
  - Client needs to prove knowledge of the password without giving it to the server

IP PSTN

SIP Trunks

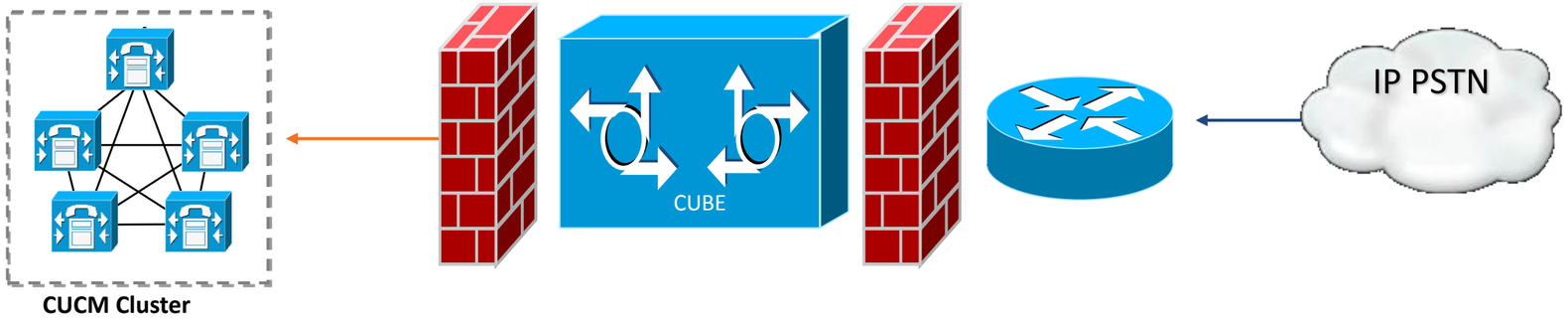
- Security demarcation via topology hiding and SIP signaling and media inspection
- Troubleshooting demarcation via B2BUA, i.e. SIP session termination and reorigination
- Call admission control (CAC) upon entry to network
- SIP Registration Authentication



IP PSTN

CUBE

- CUBE in DMZ
- Firewall placement for Protocol Inspection
  - Protection against rogue/malformed SIP packets
- SIP Trunk Registration
  - Digest Authentication
  - Hostname validation



IP PSTN

SIP TLS and SRTP

- Secure Interworking with UCME, CUBE, and Gateways
- The X.509 Subject Name field in the SIP Trunk Security profile – matches the name on a certificate and authorises it use with the Trunk
- The Certificate authenticates the remote trunk to a server / cluster

SIP IP PSTN

Toll Fraud

- Enable SIP Trunk Registration
- Enable SIP Digest Authentication
- TLS encrypted SIP and SRTP
- Change SIP port 5060 to a different value
- Use explicit destination patterns and dial peers
- Use Host name validation feature
  - Validate initial SIP Invites with FQDN host name in the Request URI

Agenda

- Security Requirements for Unified Communications
- Unified Communications System Environment
- Defining Attacks on UC Systems
- Access Layer Security
- Endpoint Security
- Encryption
- Firewalls
- Secure Remote Access
- Security for IP PSTN
- Security for Video

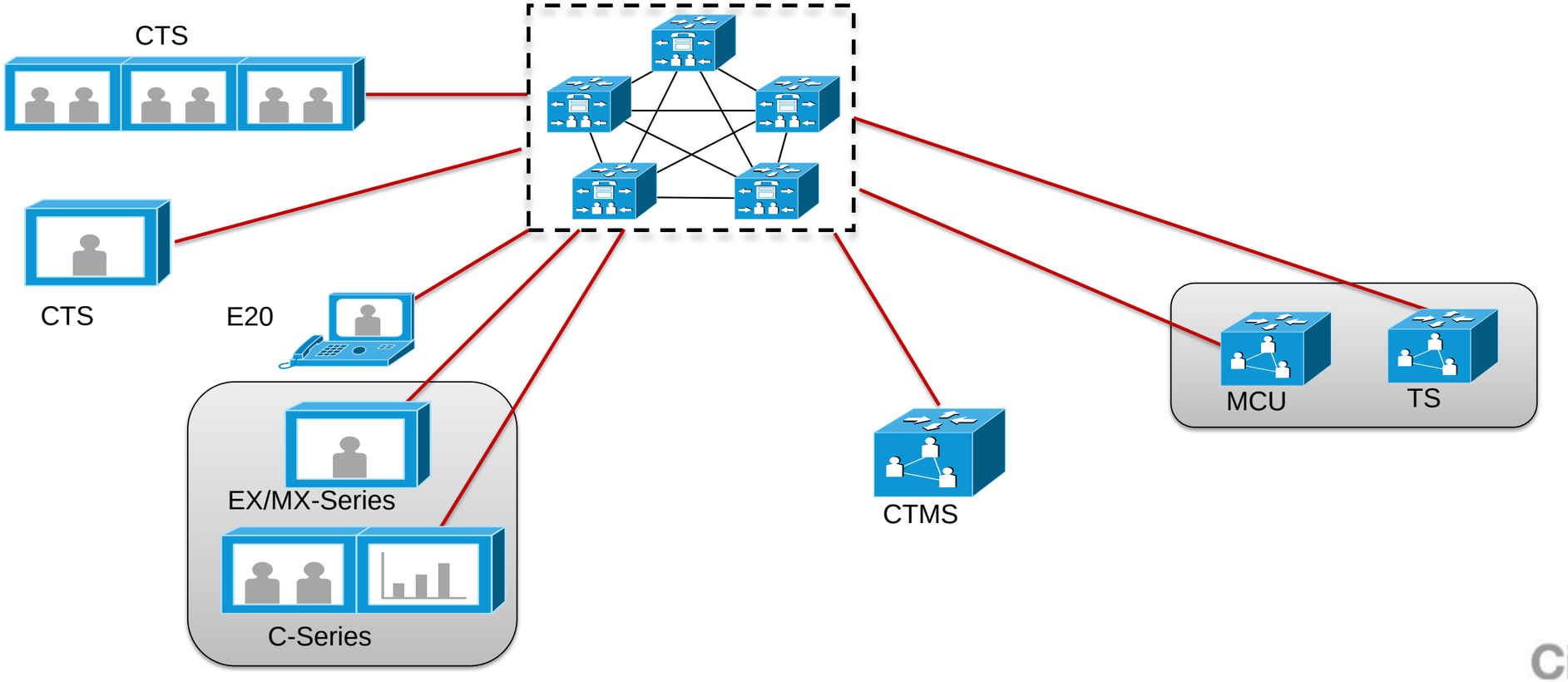
Security for Video

CUCM, CTS, VCS Integration

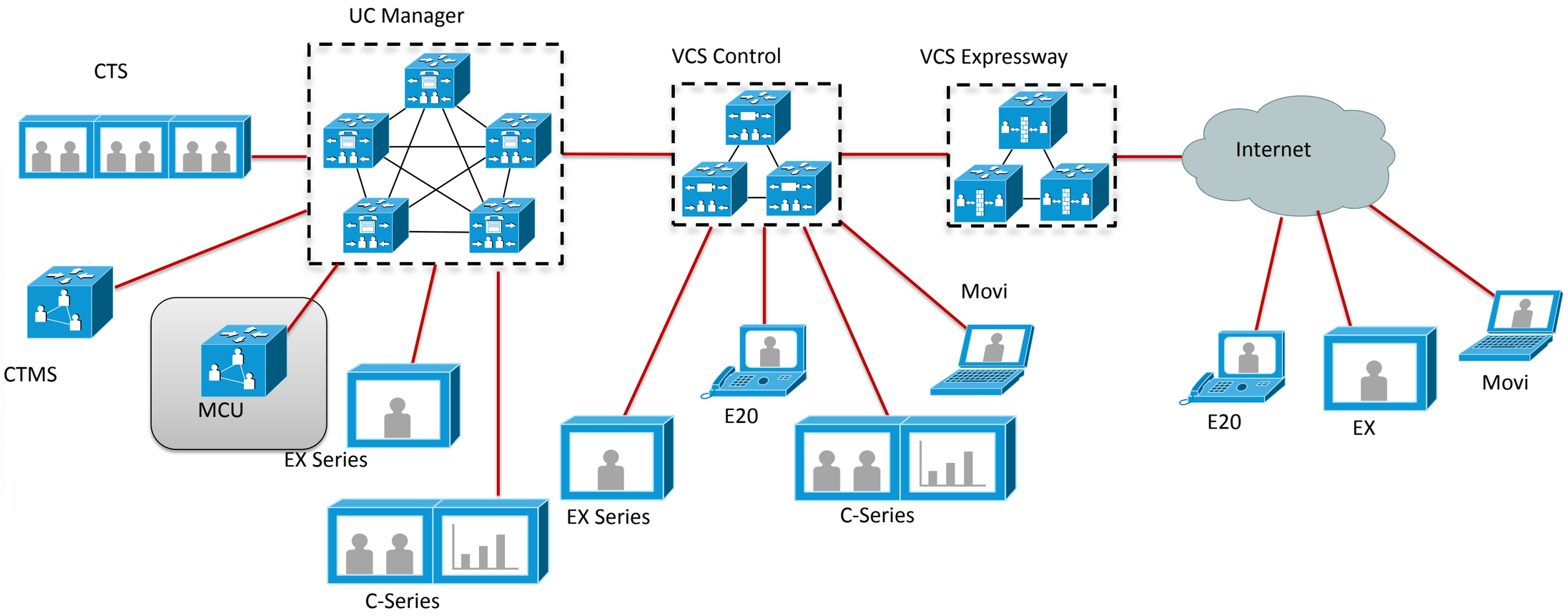
- SIP TLS Trunk integration
  - CUCM – VCS
  - CUCM – CTS
- Support for video SRTP in CUCM 9.0
  - 99XX and 89XX IP Phones
  - EX/MX/C-Series
- LSCs for natively registered Tandberg endpoints
  - SIP only
- CTS Endpoints support both TLS/SRTP and DTLS/SRTP

TelePresence endpoints with CUCM

- Native registration requires CUCM 8.6
- TLS/SRTP support requires CUCM 9.0



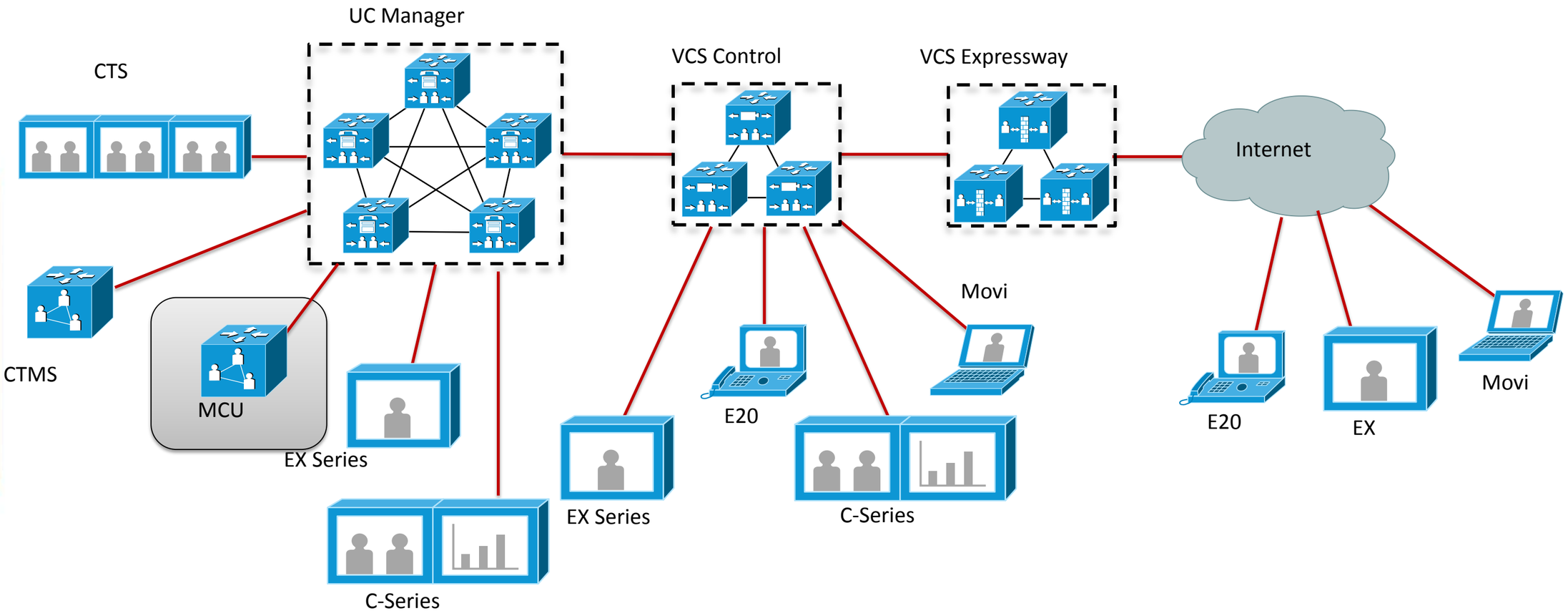
CUCM – VCS Integration



Secure CUCM – VCS Certificate Management

- CUCM needs to trust the Cisco VCS server certificate
  - Upload VCS certificate to CUCM trust store
- Configure the SIP Trunk Security profile on CUCM
  - Update the CUCM SIP Trunk to VCS to use TLS
- Configure the VCS neighbour zone to CUCM to use TLS
- Upload callmanager certificate to VCS identity store
- Ensures signaling encryption
  - Media encryption is negotiated between endpoints
- Using External CA
  - Eliminates need for manual certificate handling

CUCM – VCS Integration



Secure CUCM – VCS Integration

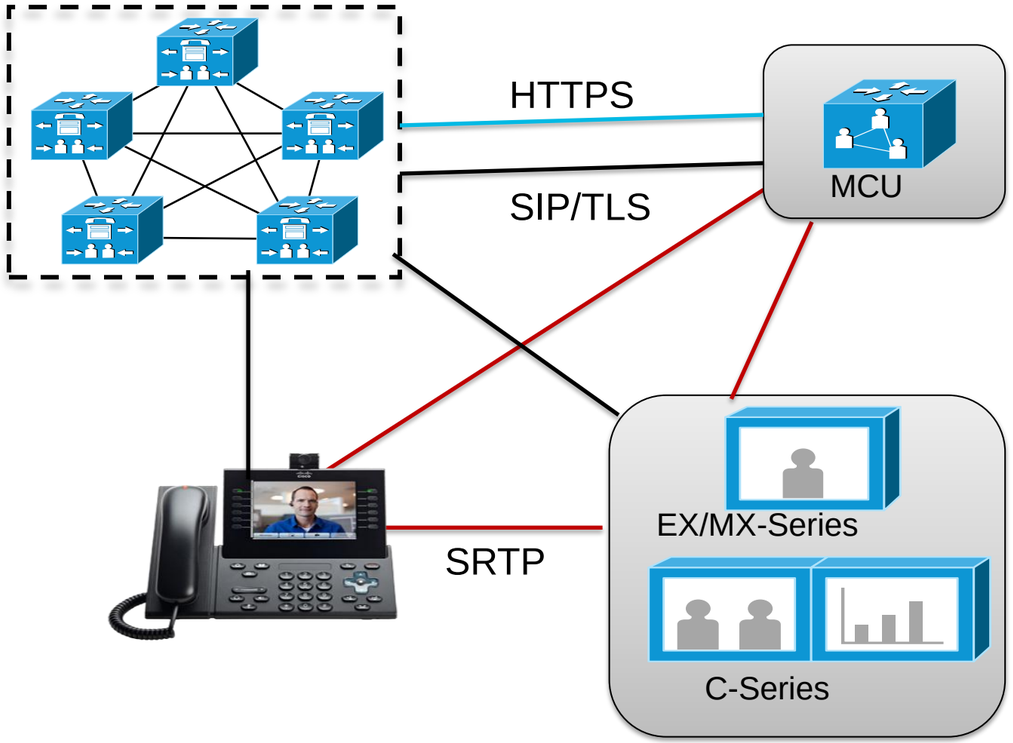
- Security Configuration Requirements:
  - CUCM 8.6(2) and later
  - VCS 7.1 and later
- The TelePresence endpoints registered to CUCM should be running in secure mode
- Cisco VCS and CUCM must be connected through secure SIP TLS trunk
- Assign the CUCM "vcs-interop" SIP Normalisation script
  - Choose vcs-interop in the Normalisation Script window while configuring the trunk profile in CUCM

Secure Codian – CUCM Integration

- CUCM 8.6.1 release introduced support for Cisco TelePresence (Codian) MCU as ad-hoc conference resource on CUCM
- CUCM 9.0 introduces security features for conferencing using this MCU
  - SIP signaling security between CUCM and MCU.
  - Media (audio/video) encryption between endpoints and MCU.
  - Security (HTTPS) on HTTP interface between CUCM and MCU
- 9.3.1 firmware required for sRTP video support on 89XX, 99XX

Secure CUCM – MCU Deployment

- TLS/SRTP support requires CUCM 9.0
- MCU Version 4.3
- Supports SIP TLS and HTTPS between CUCM and MCU
- Supports SRTP between video endpoints and MCU



Secure CUCM - MCU Deployment

- For TLS connection between CUCM and MCU, certificates need to be exchanged on both sides
- Upload CallManager Certificates to the MCU trust store
- MCU allows only one certificate file to be uploaded in its trust store
- For multiple CUCM nodes to have TLS connection with MCU, concatenate individual CallManager certificates into a single file, and upload to MCU trust store
- Upload MCU certificate to the CallManager trust-store

Review

- Policy has to drive security
- Once policy is set, apply correct security
- Choose which security is needed where
  - In the network
  - In the application
- Test security features in a lab if possible
  - Allows you to better understand what is being turned on
  - Gain experience on how to troubleshoot issues

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

Don't forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww