



Secure Network Infrastructures for Unified Communications Deployments

Craig Sanderson
Solutions Manager—Cisco®
crsander@cisco.com

INTEROP®
THE LEADING BUSINESS TECHNOLOGY EVENT

Agenda

- Secure Unified Communications Overview
- Secure Unified Communications Best Practices
- Secure Unified Communications Infrastructure
 - Eavesdropping
 - Denial of Service



Secure Unified Communications

Overview

INTEROP[®]
THE LEADING BUSINESS TECHNOLOGY EVENT

True UC Security Requires a Secure Network and Secure Telephony

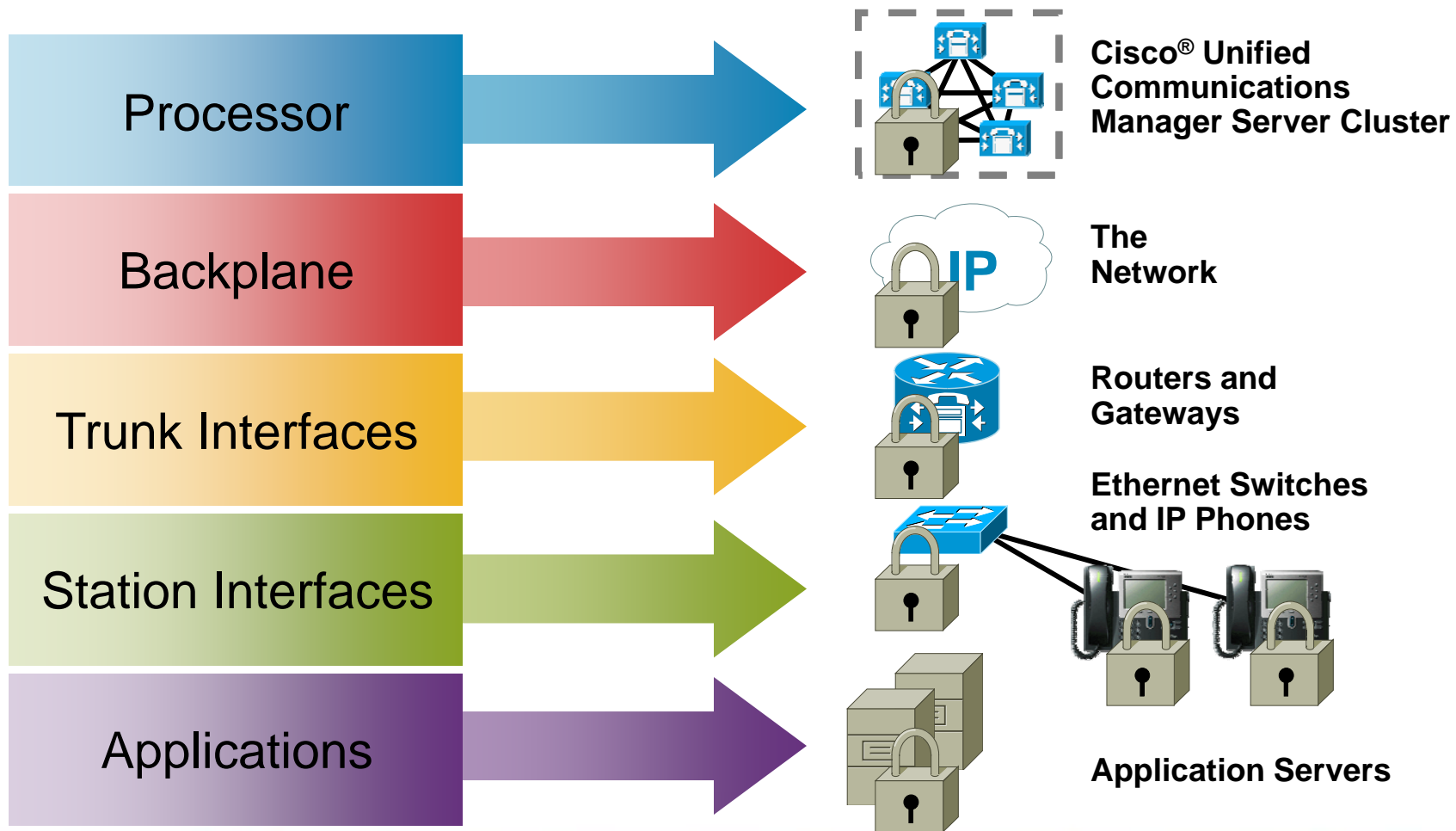
Secure Unified
Secure Network Communications Secure Telephony



“Organizations must focus on creating efficiencies across all aspects of UCC ownership including hygiene, compliance, integration, security, and identity and management.”
—Gartner, “Key Issues for Unified Communications and Collaboration,” March 2007

INTEROP

Security in a Unified Communications World





Secure Unified Communications

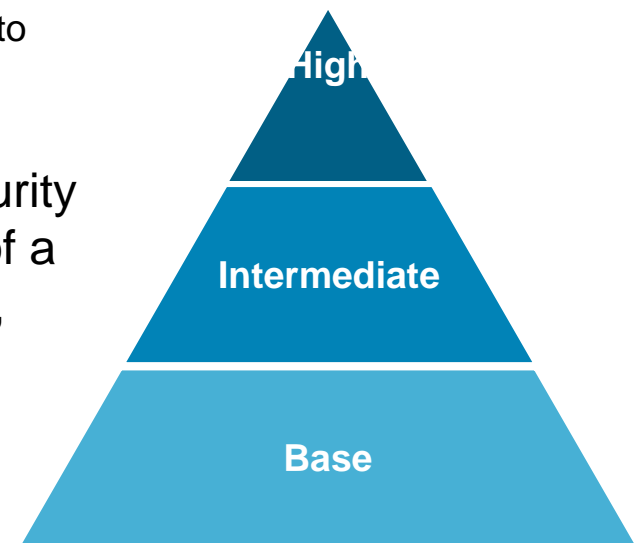
Best Practices

INTEROP[®]
THE LEADING BUSINESS TECHNOLOGY EVENT

Secure UC Threats and Risks

Best-Practice Approach to Evaluation UC Security Needs

- There is no definitive best practice for securing unified communications
- Determining what security is required and where starts with an understanding of the potential threats
- Threats must be evaluated in terms of corporate risk
 - Risk determines whether the implementation of security to mitigate the threat is justified
 - Risks can vary greatly between customers
- After a relevant risk is identified, review the security options available in the four main components of a UC system: call control, endpoints, applications, and infrastructure
- Use the Levels of Security model to evaluate the relative costs and effects of implementing a specific security feature

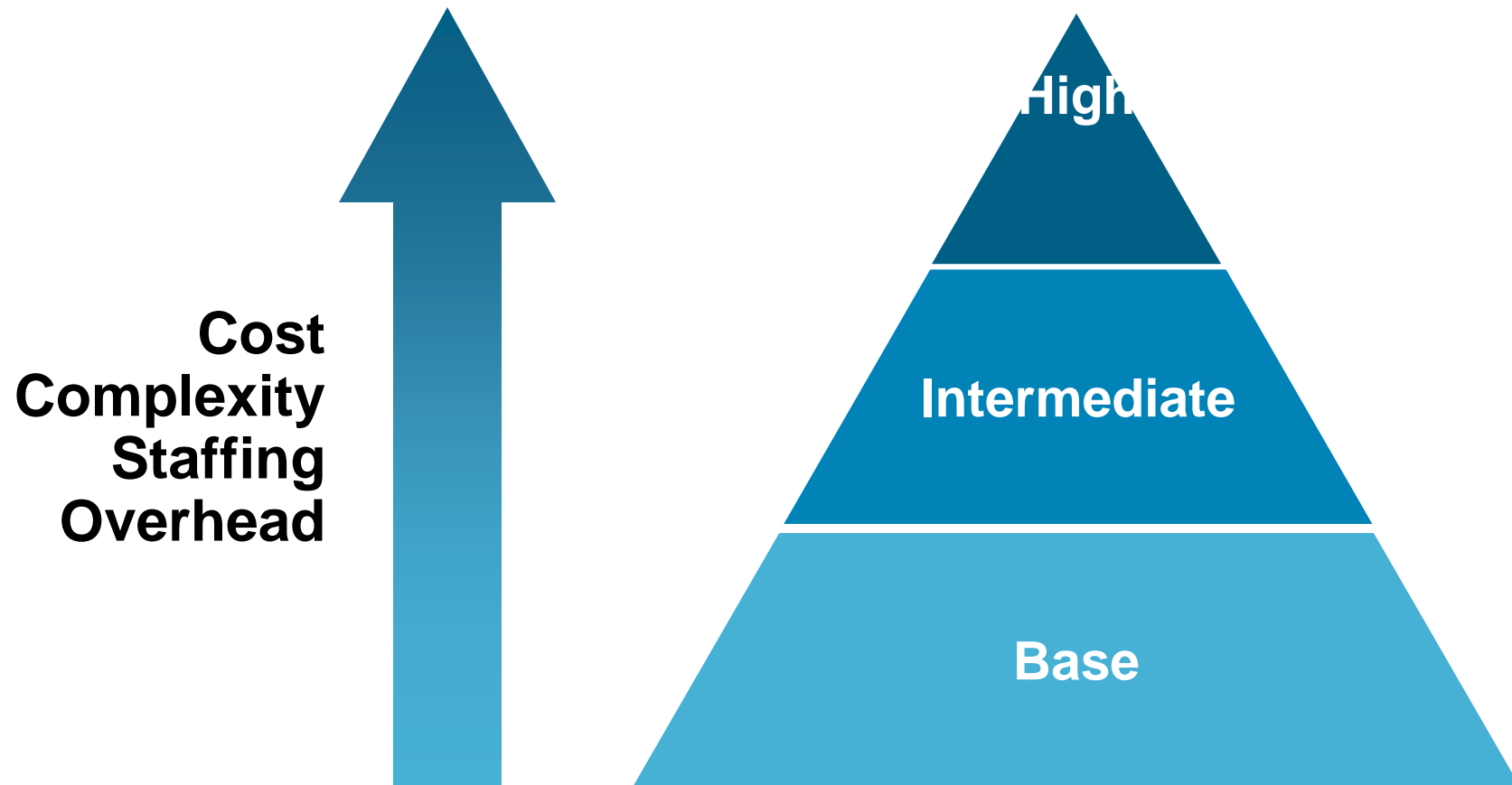


Secure UC Threats and Risks

Examples

- Eavesdropping
 - Listening to or recording audio or video conversations
 - Risk: Loss of privacy (regulatory concerns and reputation)
- Denial of Service (Internal)
 - Loss of service
 - Risk: Loss of productivity and safety and security problems (E911)
- Compromised System Integrity
 - Hacker control of applications or call control infrastructure
 - Risk: Financial (toll fraud), data theft, and regulatory concerns (loss of privacy)
- Compromised UC Clients (such as soft phones)
 - Hacker control of platforms that are UC clients
 - Risk: Financial (toll fraud), data theft (for example, customer information on Cisco IP Contact Center (IPCC) agent desktop)

Security Levels





Secure Unified Communications

Network Infrastructure Security

Eavesdropping

Denial of Service


INTEROP[®]

THE LEADING BUSINESS TECHNOLOGY EVENT

The Good News: Many Risks Can Be Mitigated by Capabilities You Already Have in the Network

1

Included as Features in the UC System (example: Transport Layer Security [TLS])




2

Included in Networking Products (example: VLAN)



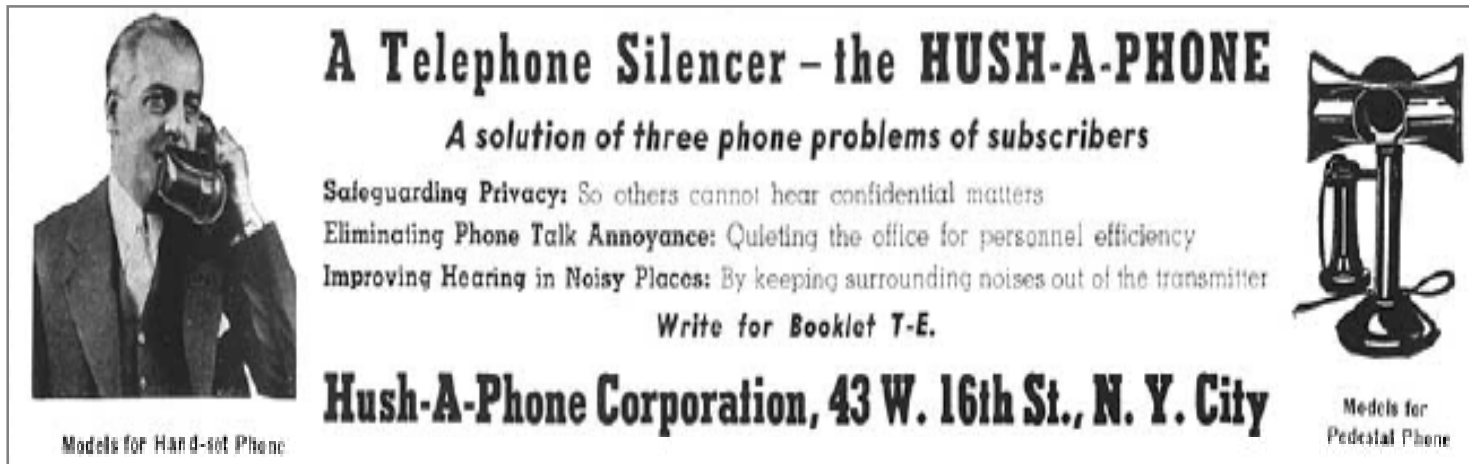
3

Features You Should Use Anyway (example: Firewall and Intrusion Prevention System [IPS])



Eavesdropping

- Privacy and confidentiality are concerns in both traditional private branch exchanges (PBXs) and UC
- Access to the media flow is the key to eavesdropping attacks
 - Many ways to achieve this
 - Many ways to prevent this—not just encryption



A Telephone Silencer – the HUSH-A-PHONE

A solution of three phone problems of subscribers

Safeguarding Privacy: So others cannot hear confidential matters
Eliminating Phone Talk Annoyance: Quieting the office for personnel efficiency
Improving Hearing in Noisy Places: By keeping surrounding noises out of the transmitter

Write for Booklet T-E.

Hush-A-Phone Corporation, 43 W. 16th St., N. Y. City

Models for Hand-set Phone

Models for Pedestal Phone

Unified Communications Encryption Options

	IPSec	SSL	TLS/SRTP (Native Phone Encryption)
Typical Deployment	Remote Access or Site-to-Site	Remote Access	Campus Network to Call Control System
Typical Client Platform	Softphone on a PC	Softphone on a PC	Hard Phone
Typical Head End Platform	VPN Device	VPN Device	Call Control System

Why did the Unified Communications vendors use TLS/SRTP?

- Low packet overhead
- No TCP re-transmission
- No user interaction required
- No client key management
- Separate signal/media paths

Eavesdropping

Why Not Just Encrypt Calls Using TLS/SRTP?

- Why not just use TLS/SRTP encryption?
 - Breaks most firewalls as they cannot inspect the signaling (more on this later)
 - Performance impact on the call control system
 - Provides a back channel to bypass network security infrastructure (soft phones)
 - Makes requirements such as call recording more difficult
- Encryption is often an option but not necessarily the solution
- Do you encrypt calls on your existing PBX?

Eavesdropping

Using the Network

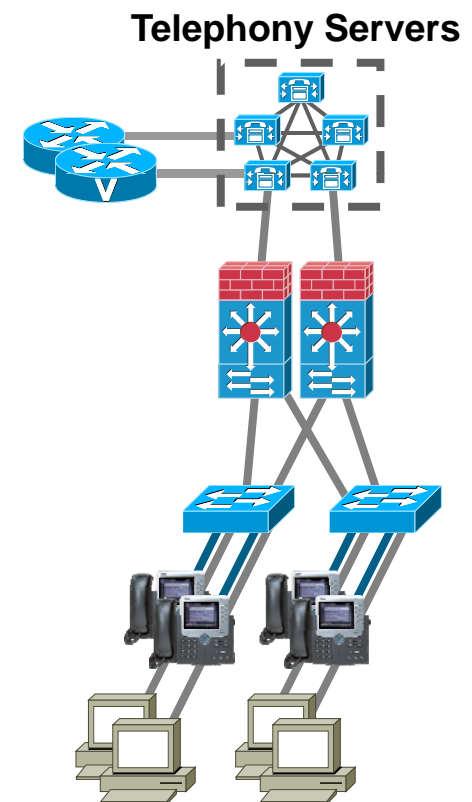
- **Baseline**
 - Basic access control lists (ACLs)
 - Separate voice and data VLANs
 - No static IEEE 802.1q trunks
- **Intermediate**
 - Dynamic port security
 - Dynamic Host Configuration Protocol (DHCP) snooping
 - Dynamic Address Resolution Protocol (ARP) inspection
 - IP Source Guard
- **Advanced**
 - IEEE 802.1x for phone and PC authentication



Eavesdropping

Separate Voice and Data VLANs with VLAN ACLs

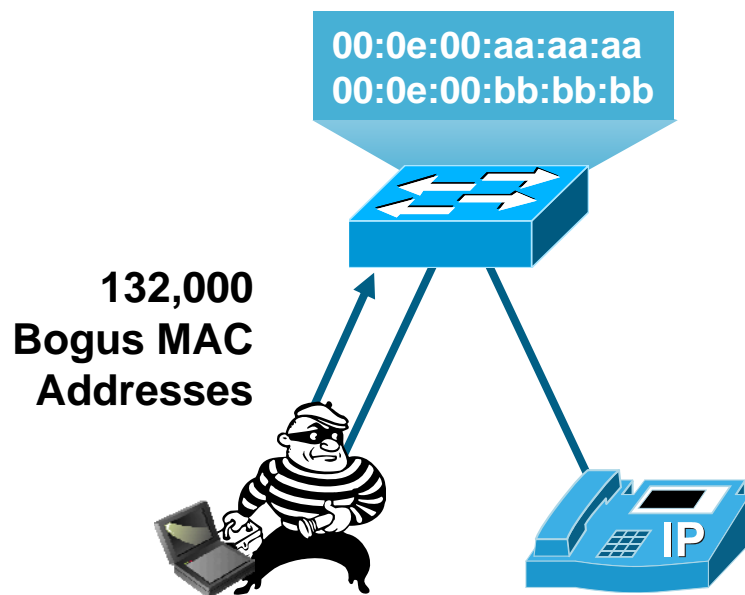
- Separate Voice and Data VLAN
 - Simplifies address management
 - Easier to apply security policy to a specific VLAN
- VLAN Access Control Lists (VACLs)
 - Phones only need to send RTP to each other and a small number of TCP and UDP protocols to servers
 - Phones have no reason to send TCP or ICMP to each other
 - Stops all TCP and ICMP attacks against the phones



Note: Soft phones that run on PCs undermine this architecture

Eavesdropping: MAC Flooding Attacks

What Happens If an Attacker Floods Your Infrastructure with False MAC Addresses?

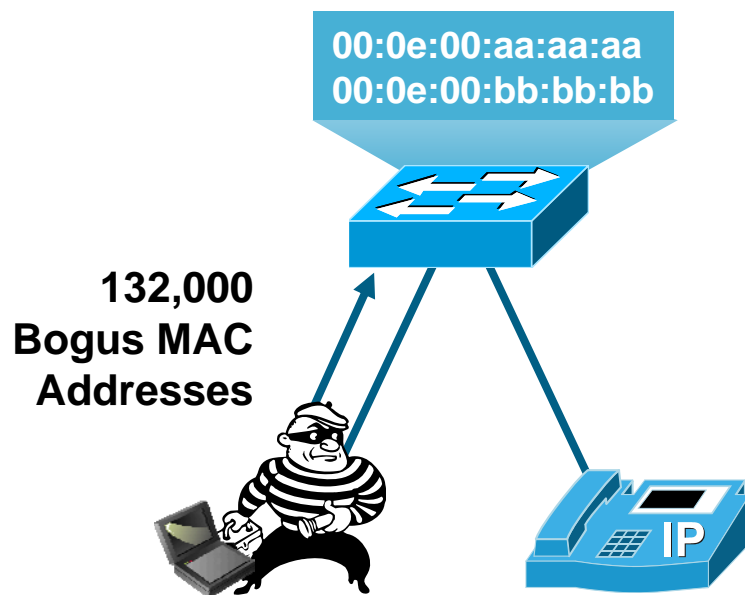


Problem

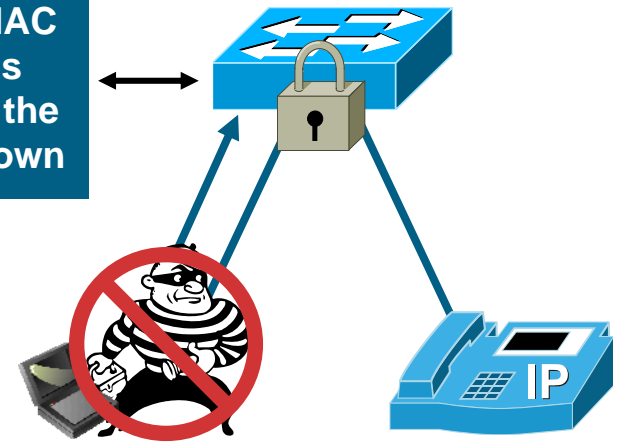
- Switches learn new MAC addresses from frames they receive on their ports
- When the MAC table is full, by default switches replace the oldest addresses (those of your phones) with the newest addresses (false MAC addresses)
- When packets are sent to the legitimate devices, the result is a flood to all ports
- Attacker listens to calls and all unencrypted data passwords

Countermeasures for MAC Attacks

Port Security Limits the Number of MAC Addresses on an Interface



Only One MAC
Address Is
Allowed on the
Port: Shutdown



Solution

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

Eavesdropping: DHCP Attack Types

Rogue DHCP Server Attack

- What can the attacker do if the attacker is the DHCP server?

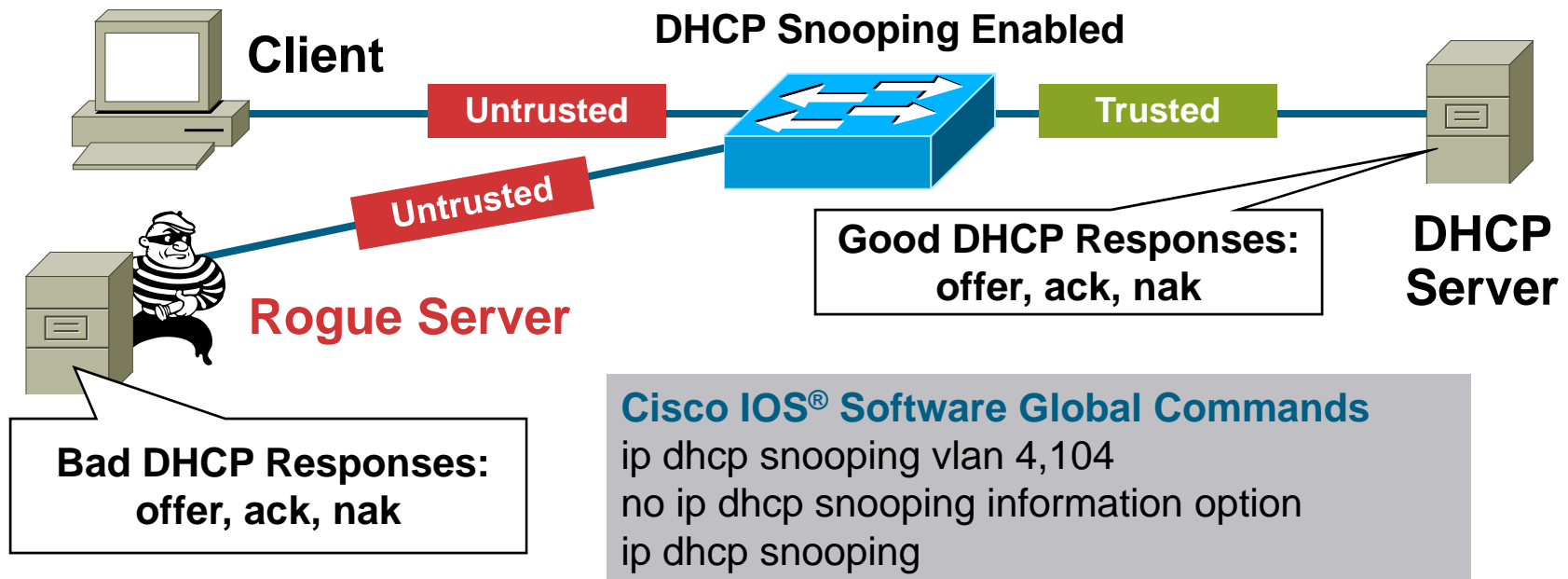
```
IP Address: 10.10.10.101
Subnet Mask: 255.255.255.0
Default Routers: 10.10.10.1
DNS Servers: 192.168.10.4, 192.168.10.5
Lease Time: 10 days
```

Here Is Your Configuration

- What do you see as a potential problem with incorrect information?
 - Wrong default gateway: Attacker is the gateway
 - Wrong DNS server: Attacker is Domain Name System (DNS) server
 - Wrong IP address: Attacker launches denial-of-service (DoS) attack

Countermeasures for DHCP Attacks

Rogue DHCP Server = DHCP Snooping



DHCP Snooping **Untrusted** Client

Interface Commands

```
no ip dhcp snooping trust (Default)  
ip dhcp snooping limit rate 10 (pps)
```

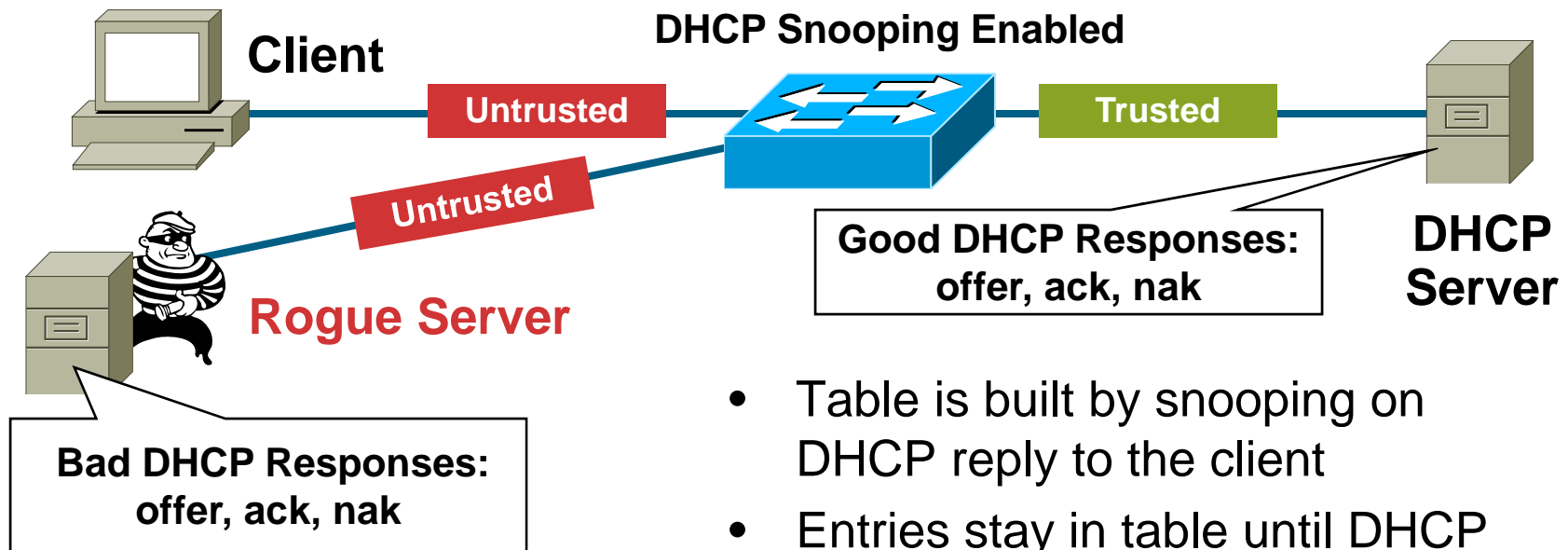
DHCP Snooping **Trusted** Server or Uplink

Interface Commands

```
ip dhcp snooping trust
```

Countermeasures for DHCP Attacks

Rogue DHCP Server = DHCP Snooping



- Table is built by snooping on DHCP reply to the client
- Entries stay in table until DHCP lease time expires

DHCP Snooping Binding Table

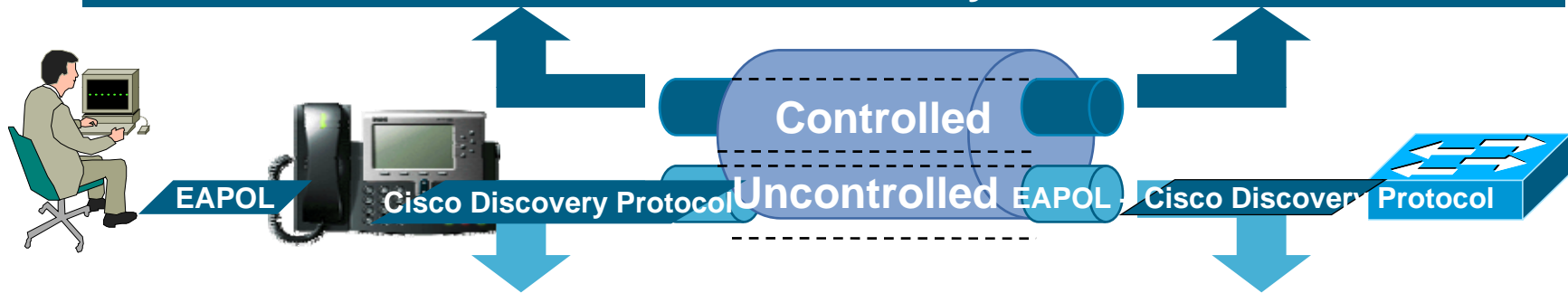
```
sh ip dhcp snooping binding
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:03:47:B5:9F:AD	10.120.4.10	193185	dhcp-snooping	4	FastEthernet3/18

IEEE 802.1x and Hard Phones

Review

The Controlled Port Is Open Only When the Device Connected to the Port Has Been Authorized by IEEE 802.1X



Uncontrolled port provides a path for Extensible Authentication Protocol over LAN (EAPOL) and Cisco® Discovery Protocol traffic **only**

- Cisco Discovery Protocol or Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) assigns devices to voice or data VLAN
- IEEE 802.1x optionally applied to either VLAN using multi-VLAN authentication capability
- IEEE 802.1x authentication can be applied to the phone, the PC, or the user using the PC
- IEEE 802.1x is an advanced feature because of the complexity of deployment and operation

Denial of Service (DoS)

- Any incident that prevents an authorized user from using the unified communications service
 - Making a call
 - Receiving an IM chat session
- DoS protection is not just about protecting the UC infrastructure
- Denial of network connectivity and service is essentially DoS
- Many of the features available in the network to protect against eavesdropping also help reduce the risk of DoS

Denial of Service (DoS)

Using the Network

- **Baseline**
 - VLAN Separation and ACLs
 - Spanning Tree Protection
 - Bridge Protocol Data Unit (BPDU) Guard and Root Guard
- **Intermediate**
 - Dynamic Port Security
 - DHCP Snooping
 - Dynamic ARP Inspection
 - IP Source Guard
 - Network and Firewall Rate Limiting
- **Advanced**
 - Advanced Quality of Service (QoS)
 - Firewalls and Intrusion Prevention



Denial of Service (DoS)

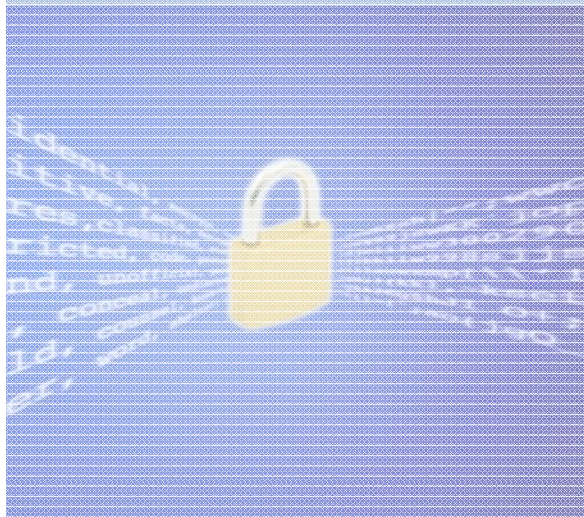
BPDU Guard and Root Guard

- If the campus network fails
 - No outbound calls: What about E911 calls?
 - No internal calls
 - In fact, no dial tone at all
- The most common cause of campus network failures are Spanning Tree Protocol loops
 - End user plugs in a hub to two different switch ports in a conference room
- BPDU Guard prevents rogue switches on the network and mitigates accidental Spanning Tree Protocol loops
- Root Guard protects the Spanning Tree Protocol root on a Layer 2 infrastructure and mitigates Spanning Tree Protocol loops and Spanning Tree Protocol convergence when switches are added to a network
- Both features have negligible effect on performance and are relatively easy to configure—yet few customers implement them

The Good News: Many Risks Can Be Mitigated by Capabilities You Already Have in the Network

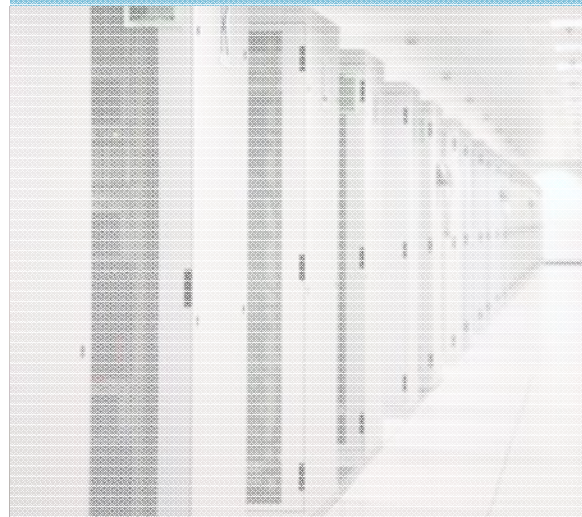
1

Included as Features in the UC System (example: Transport Layer Security [TLS])




2

Included in Networking Products (example: VLAN)



3

Features You Should Use Anyway (example: Firewall and Intrusion Prevention System [IPS])



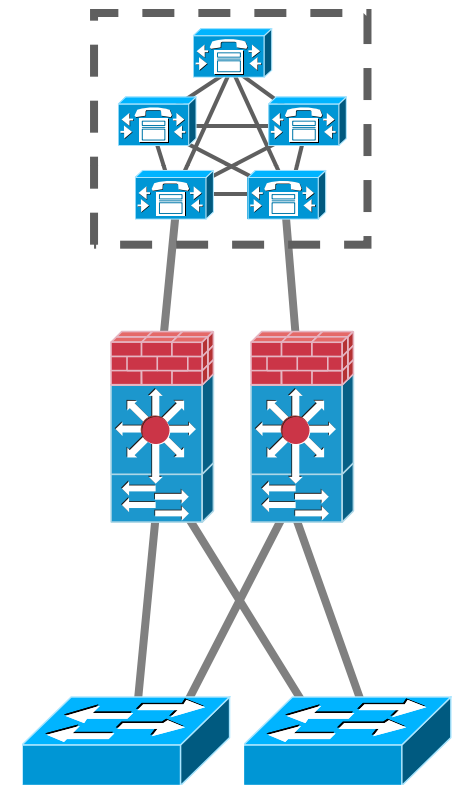
Place a Firewall or ACL in Front of Telephony Servers

Why Use a Firewall?

- Network mechanism is needed to isolate and protect telephony servers
 - Protocol conformance
 - Registration protection
 - DoS protection
- Service filtering mechanism is needed
 - For example, prevent IM over SIP
 - Filter blacklisted numbers or users

Why Not Use ACLs?

- ACLs can open up the signaling ports but cannot inspect the signal and protect the call processor
- ACLS must open all possible RTP ports



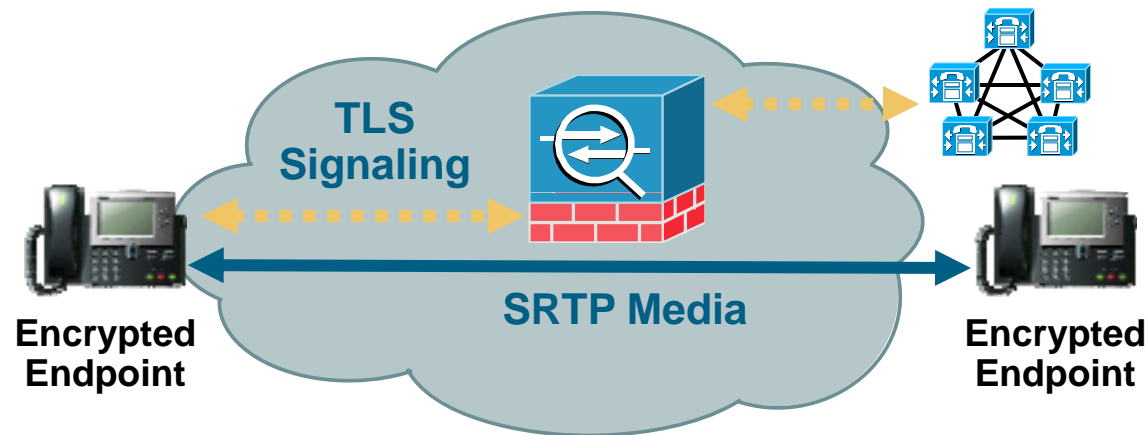
Large Enterprise Customer Challenge

Solving the Firewall and Encryption Integration Problem

- Customer security policy mandates
 - All servers, including Cisco® Unified Communications Manager server, must be firewalled to protect against DoS, provide system integrity, etc.
 - Certain end users must have all phone calls encrypted (to prevent eavesdropping)
- Firewalls need to inspect the signaling traffic to
 - Open media pinholes
 - Apply protocol conformance
 - Apply application inspection and control (AIC)
- Encrypted calls must encrypt the signaling (transparent LAN service [TLS]) because Cisco Unified Communications Manager sends the media encryption keys to phones through the signaling
- Problem: Two primary security functions cannot coexist or integrate
- Customer options: Choose encryption or firewalling, but not both
- Customer requirement: Network-to-UC-application integration

Encrypted Voice Security Solution

Security, UC, and Network Integration



Any Cisco® voice and video communications encrypted with SRTP or TLS can now be inspected by Cisco ASA 5500 Adaptive Security Appliances:

- Maintains integrity and confidentiality of call while enforcing security policy through advanced SIP and SCCP firewall services
- TLS signaling is terminated and inspected and then re-encrypted for connection to the destination (using integrated hardware encryption services for scalable performance)
- Dynamic port is opened for SRTP-encrypted media stream and automatically closed when call ends

Summary

- To know what you need to secure your unified communications infrastructure, you must understand your organizational risk
- Policy and process are just as important, if not more so, than technology and platform features
- To secure unified communications, you must consider call control, endpoints, applications, and—of course—the network
- The network infrastructure has a number of security functions that can secure both voice and data
- As security becomes more of a concern, the capability of network and security platforms to integrate as a system will become more critical



Secure Network Infrastructures for Unified Communications Deployments

Craig Sanderson
Solutions Manager—Cisco®
crsander@cisco.com

INTEROP®
THE LEADING BUSINESS TECHNOLOGY EVENT



INTEROP