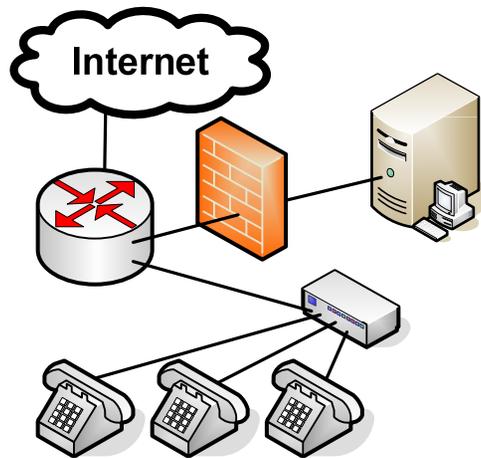


UNCLASSIFIED

Proposed Secure VoIP Communications System



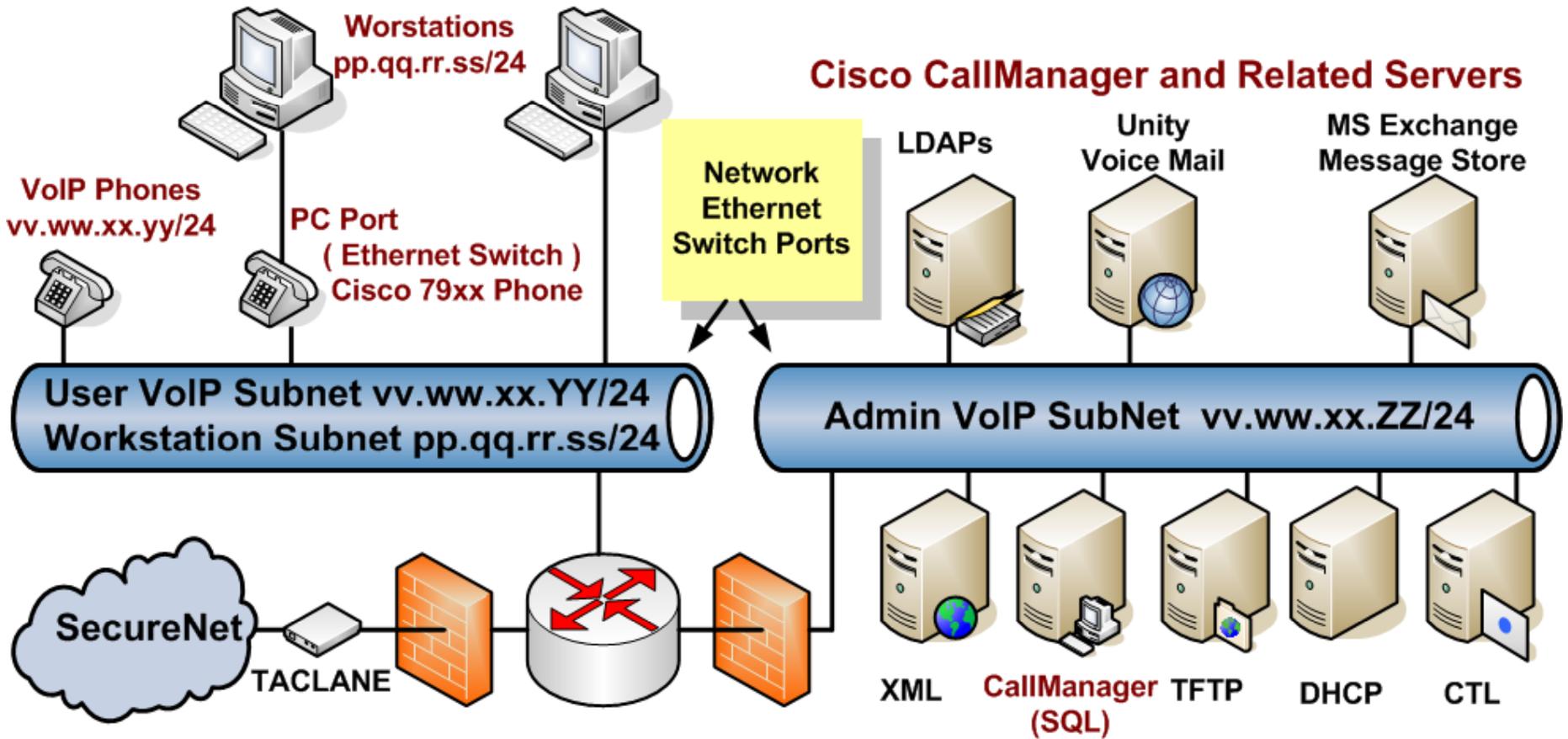
A Joint NLIT 2007 Presentation:

LANL: Karl Pommer

KCP: Tom Beechwood

LANL Publication: LA-UR-07-2730

Conceptual VoIP Deployment:



VoIP Phones for the Secure ICN:



7940G IP Phone

Display Call State Icons { 



Cisco 7960G IP Phone

Non-Secure,  Authenticated,



Cisco 7970G IP Phone

 Encrypted (AES-128) }



Cisco 7985G Video

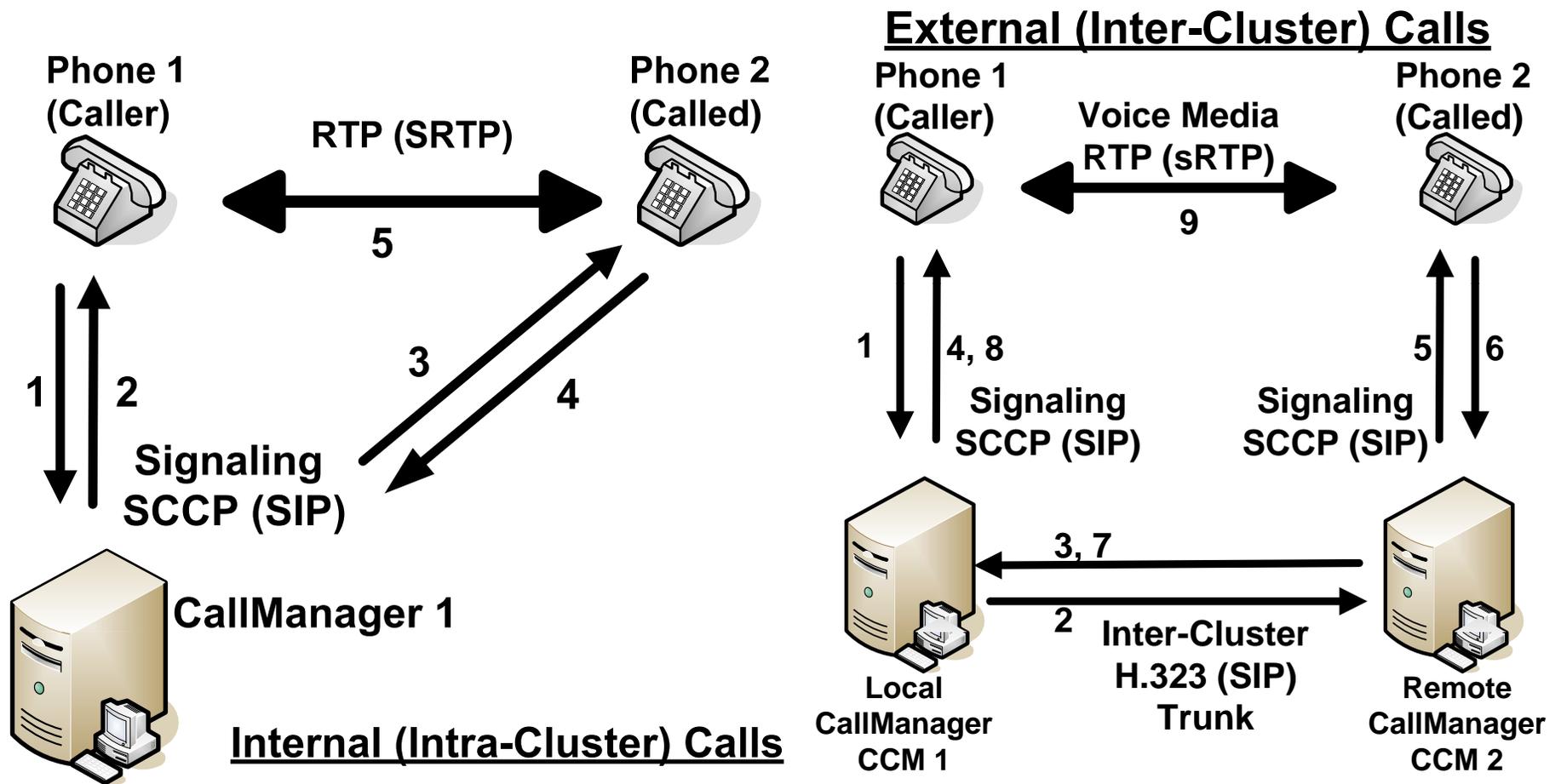
Non-Secure 
i.e. - No Authentication or Encryption

L-3 Communications IP-STE

Non-Secure 
 Secure (Type-1)



Internal & External VoIP Call:



TLS Used for Authentication & Encryption:

Transport Layer Security Protocol (TLS)

Communications Protocols							
+ OSI Model Level:		Data Format:	Protocol				
5 - 7			HTTP	SCCP	FTP	RTP	LDAP
4	Transport	Segments	TLS (Transmission Level Security)				
			TCP (Transport Control Protocol)				
3	Network	Packets	IP		ICMP	ARP	RARP
2	Data Link	Frames	Ethernet (IEEE 802.2 & 802.3)				
1	Physical	Bits	Based Standards				

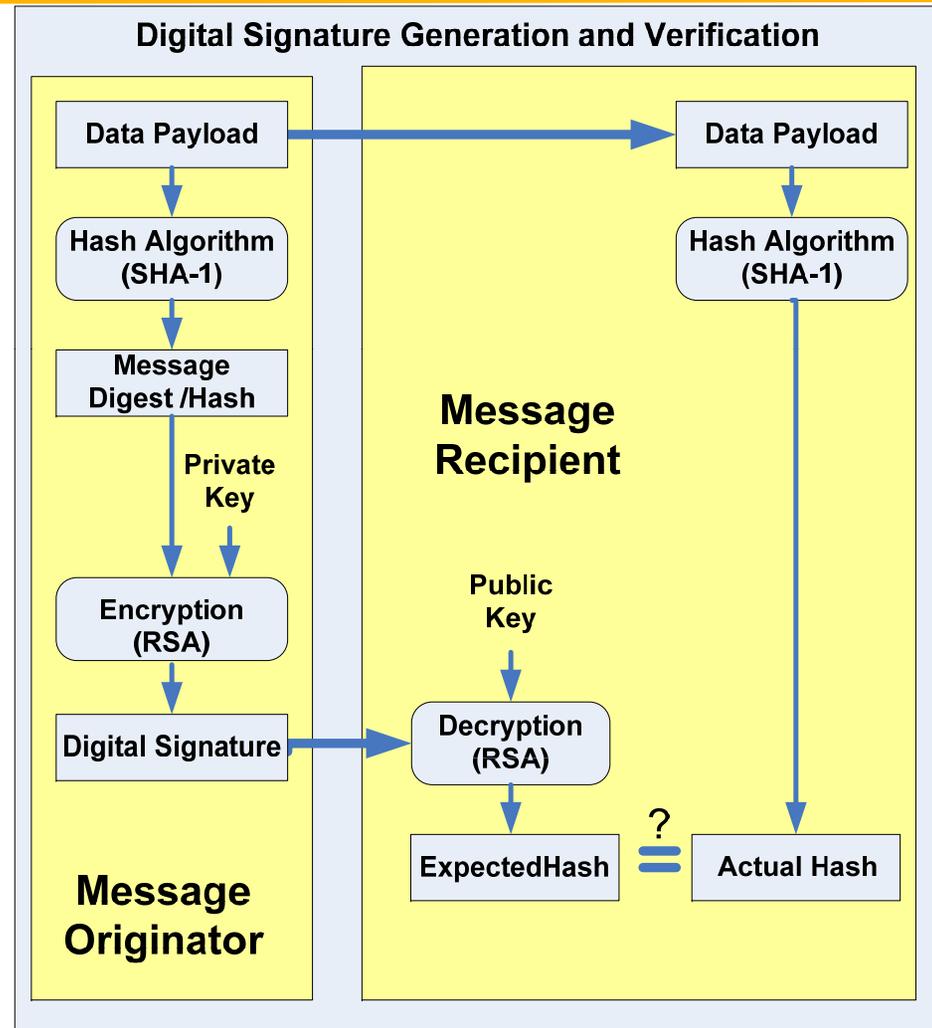
X.509 Certificate: Self-Signed / Certificate Authority:

X.509 Certificate for the Wells Fargo Certificate Authority			
Field:	Value:	Field:	Value:
Version	V3	Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.840.1.114171.903.1.11
Serial Number	39E4 979E		[1,1]Policy Qualifier Info: Policy Qualifier ID=CPS
Signature Algorithm	sha1RSA		Qualifier: http://www.wellsfargo.com/certpolicy
Issuer	CN = Wells Fargo Root Certificate Authority OU = Wells Fargo Certificate Authority O = Wells Fargo C = US		Basic Constraints
Valid from	Wednesday, October 11, 2000 9:41:28 AM	Thumbprint algorithm	sha1RSA
Valid to	Thursday, January 14, 2021 9:41:28 AM	Thumbprint (MDAC)	93E6 AB22 0303 B523 DA56 9EBA E4D1 D1CC FB65
Subject	CN = Wells Fargo Root Certificate Authority OU = Wells Fargo Certificate Authority O = Wells Fargo C = US	Friendly name	Wells Fargo Root Certificate Authority
Public Key	{RSA (2048 Bits)} 3082 010A 0282 0101 00D5 A833	Enhanced key usage (Property)	Server Authentication Client Authentication Secure Email

Digital Signatures:

Applications:

- X.509 Cert Thumbprints
- Packet Authentication



UNCLASSIFIED

Slide 6

TLS Based Client Server PKI Support:

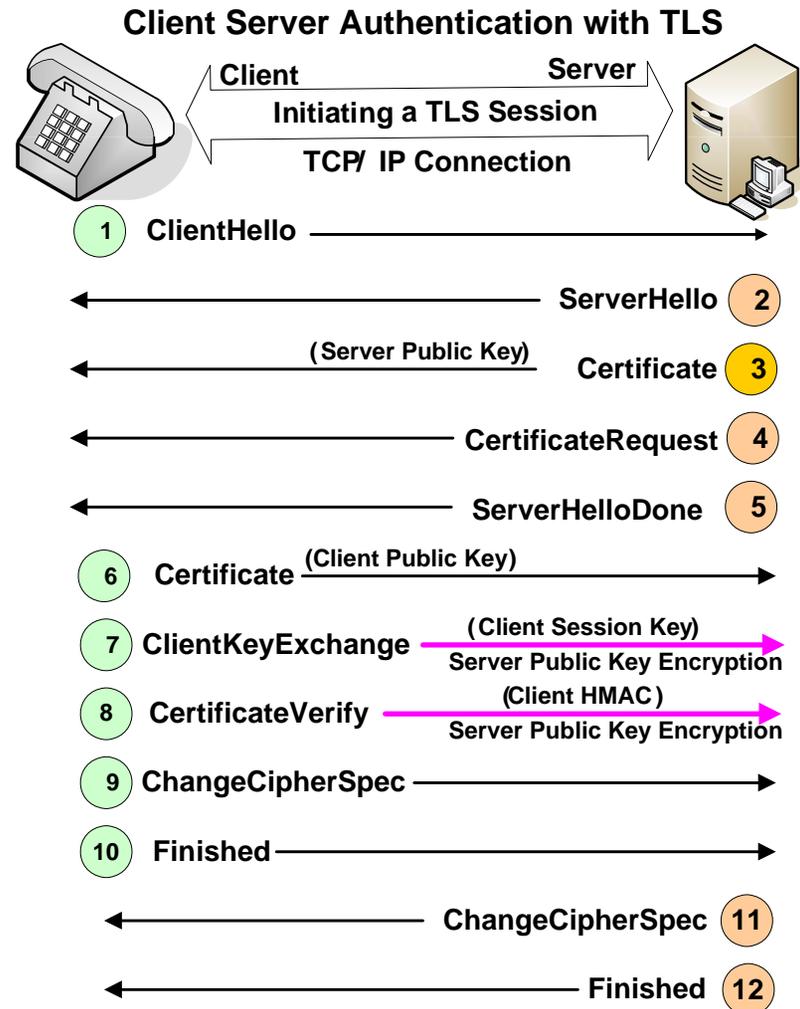
Key Events:

Tag #3 - Server sends X.509 Certificate to Client

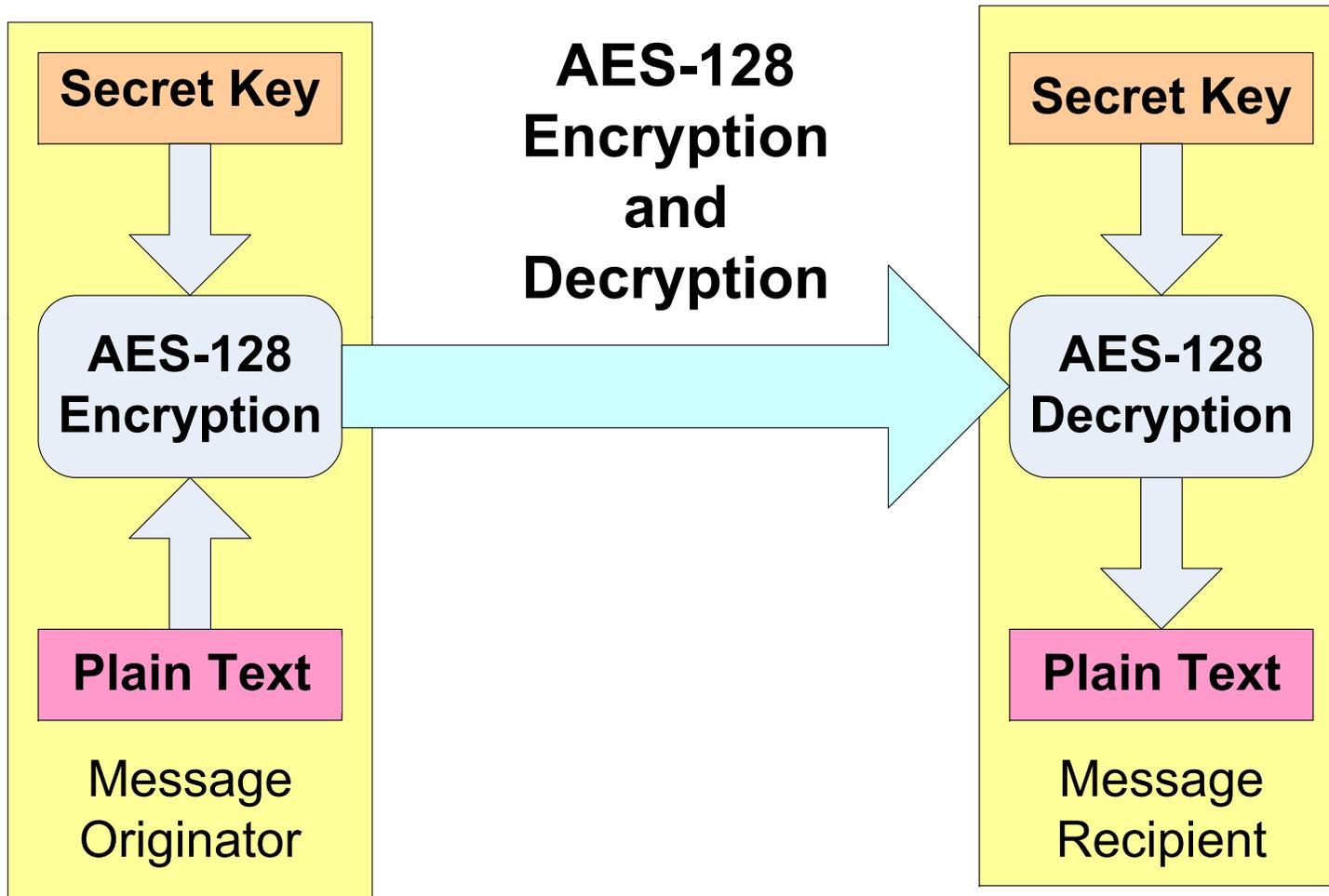
Tag #6 - Client sends X.509 Certificate to Server

Tag #7 - Client sends Shared Secret Session

**encrypted with
Public Key**



Encryption Algorithm for Cisco 79xx IP Phone:



Shared Secret Exchange (AES-128 Encryption):



Diffie-Hellman Shared Secret Key Exchange Algorithm

Cisco's Skinny Client Control Protocol (SCCP)

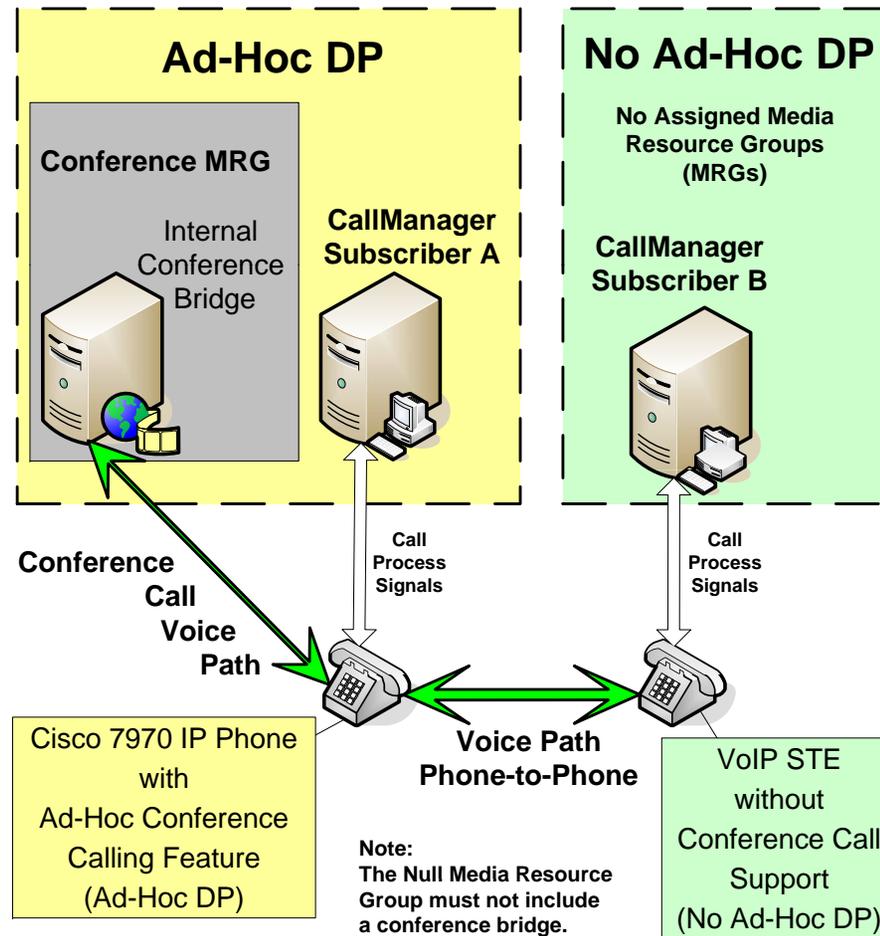


- | | | |
|---|--|---|
| <ol style="list-style-type: none"> 1. Generate large integer p.
Send p to Peer B.
Receive q.
Generate g. 2. Generate private key X_A 3. Generate public key
$Y_A = g^{X_A} \text{ mod } p$ 4. Send public key Y_A 5. Generate shared secret
number $ZZ = Y_B^{X_A} \text{ mod } p$ 6. Generate shared secret key
from ZZ (DES, 3DES, or AES) | \longleftrightarrow

\longleftrightarrow | <ol style="list-style-type: none"> 1. Generate large integer q.
Send q to Peer A.
Receive p.
Generate g. 2. Generate private key X_B 3. Generate public key
$Y_B = g^{X_B} \text{ mod } p$ 4. Send public key Y_B 5. Generate shared secret
number $ZZ = Y_A^{X_B} \text{ mod } p$ 6. Generate shared secret key
from ZZ (DES, 3DES, or AES) |
|---|--|---|

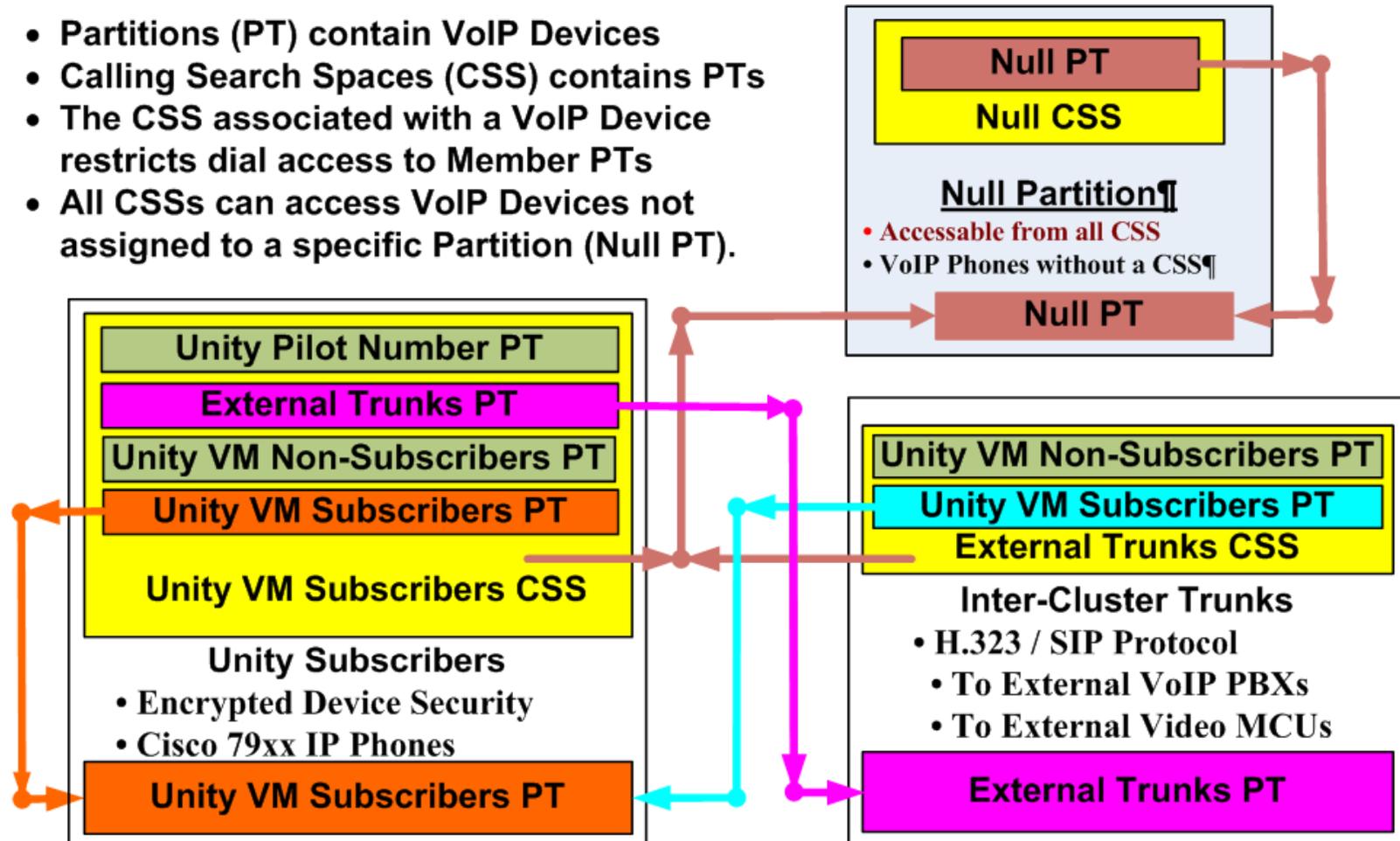
Allocating Resources – Conference Bridges:

Using Device Pools (DPs)

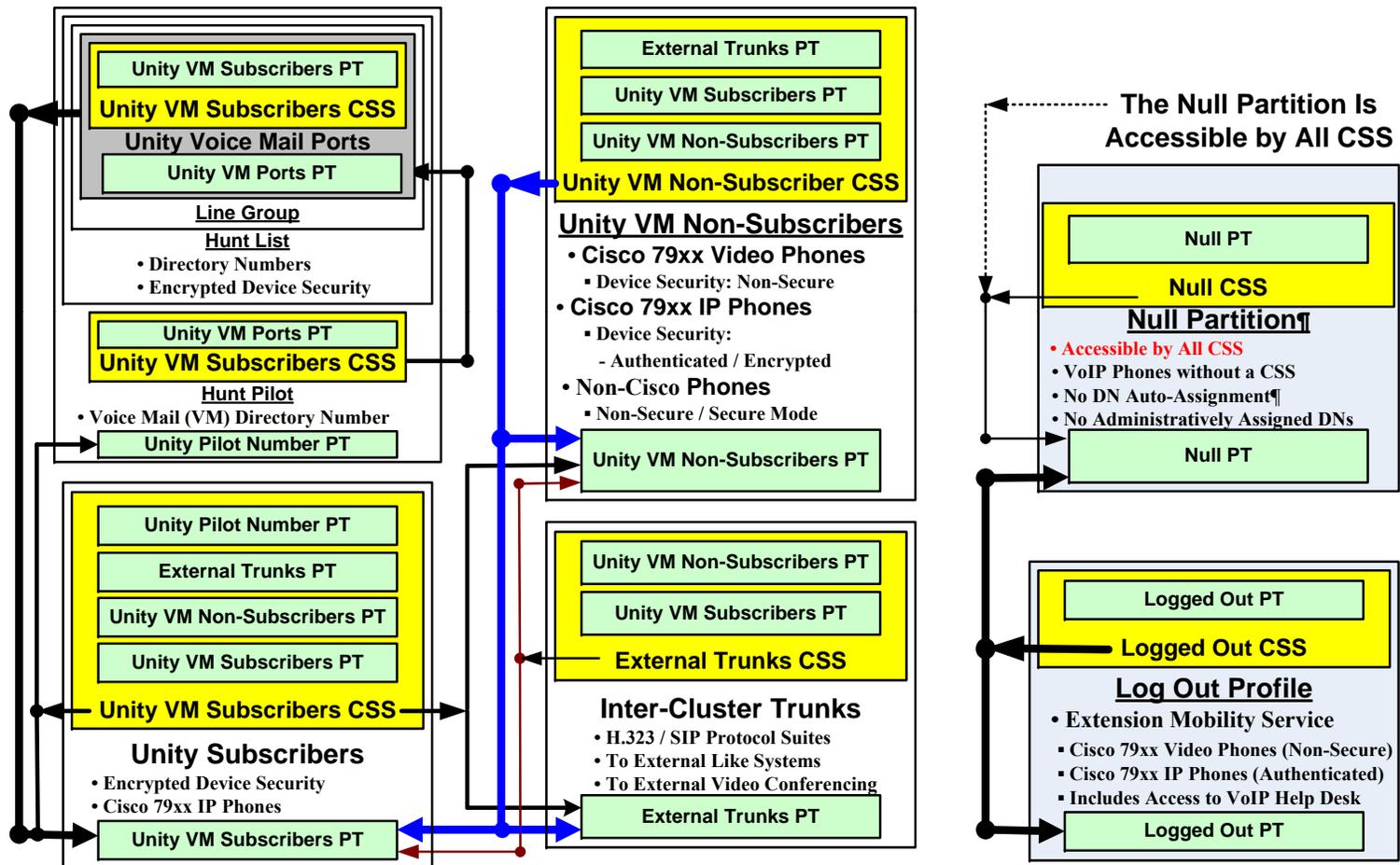


Dial Restrictions Using Calling Search Spaces:

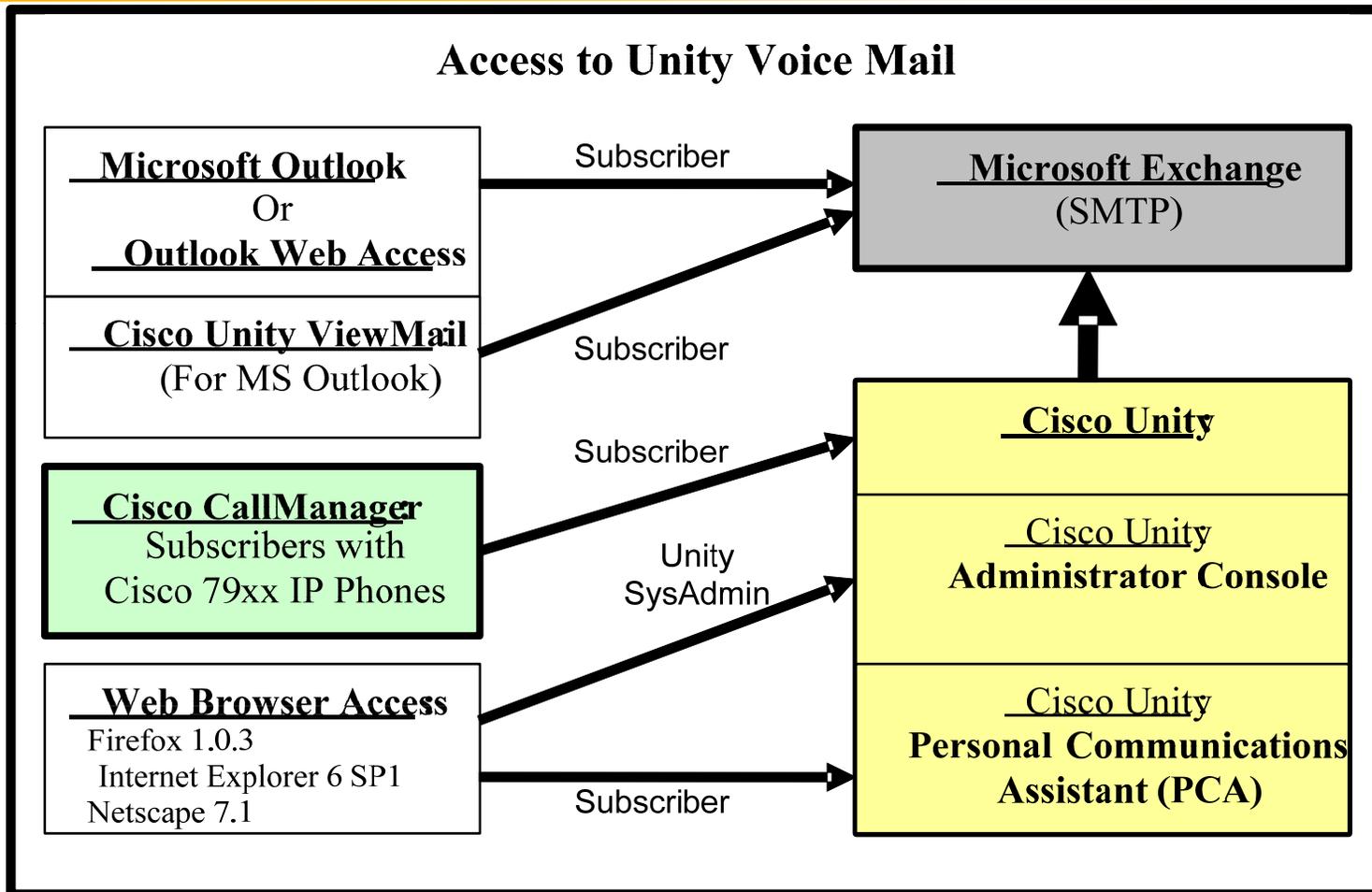
- Partitions (PT) contain VoIP Devices
- Calling Search Spaces (CSS) contains PTs
- The CSS associated with a VoIP Device restricts dial access to Member PTs
- All CSSs can access VoIP Devices not assigned to a specific Partition (Null PT).



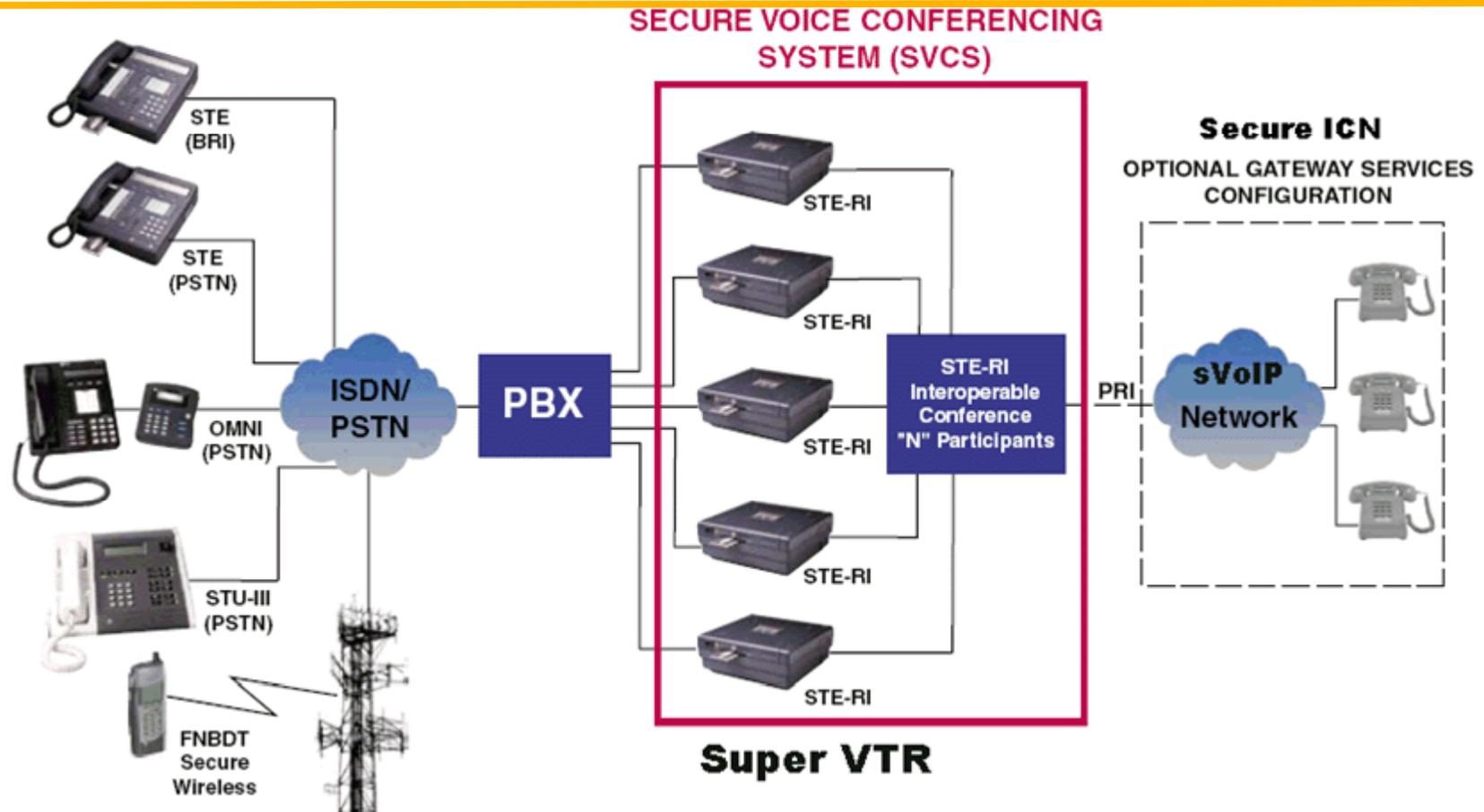
Call Flow with Calling Search Spaces (CSS):



Security Layer 1 - Voice Mail (VoIP & Web):



Something New for Discussion: STE Portal



Basic Security Threats:

High Threat Level: Knowledgeable inside personnel motivated to gather or destroy sensitive information.

Solution: 1. Secure ICN Administrative Controls

- Prohibited Workstation Software
- Unused Port Controls
- Network Controls

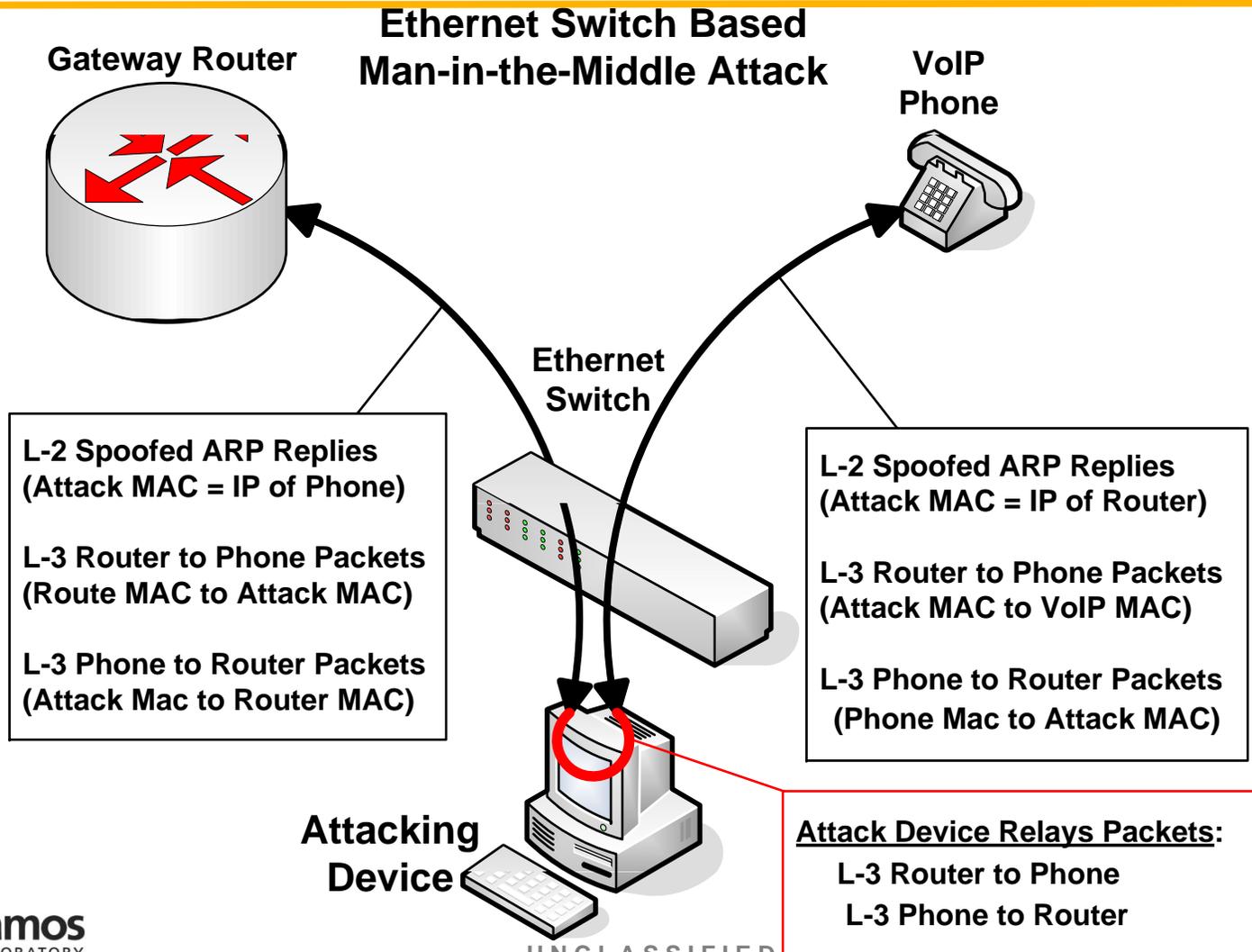
2. CallManager & Unity Administrative controls

3. User Training & VoIP Support Staff

Low Threat Level: Unauthorized personnel motivated to gather or destroy sensitive information.

Solution: Mitigate using existing physical access controls.

Insider Threat: Man-in-the-Middle-Attack





VoIP Risk Mitigation Best Practices:

Description of Threats:

- Unauthorized Access
- Digital Snooping / Electronic Eavesdropping
- Denial of Service
- System Failure / Security Controls Failure
- Malicious Software / Code

The Kansas City Plant is operated and managed by Honeywell Federal Manufacturing & Technologies, LLC, for the NNSA.

Tom Beechwood tbeechwood@kcp.com



Slide 17



Major Category: Unauthorized Access

Threat	<ul style="list-style-type: none"> - Default Password - Guest Account
Vulnerability	Default password provides access to CallManager Operating System.
Recommended Mitigation	Remove Guest Account. Upon setup, change the default password of the CallManager servers to a strong password.
Probability Before Mitigation	High
Probability After Mitigation	Low

The Kansas City Plant is operated and managed by Honeywell Federal Manufacturing & Technologies, LLC, for the NNSA.





Major Category: Unauthorized Access

Threat	HTTP attack
Vulnerability	Unsecured web server interfaces / services
Recommended Mitigation	Use HTTPS. Restrict use of web interface to administrator accounts. Allow no remote access.
Probability Before Mitigation	Medium
Probability After Mitigation	Low



Major Category: Digital Snooping / Electronic Eavesdropping: #1

Threat	ARP Cache Poisoning (Enables rerouting of voice and data traffic)
Vulnerability	Capability for unauthorized physical connection to the network.
Recommended Mitigation	Keep all components of the system in areas with restricted physical access. Disable all unused network connections to this VoIP network. This includes the VoIP phone's PC port when possible. Configure the phones to support the authorized Security Level.
Probability Before Mitigation	Low
Probability After Mitigation	Low



Major Category:
Digital Snooping / Electronic Eavesdropping: #2

Threat	Phone Traffic → Attacker
Vulnerability	Netmask vulnerability.
Recommended Mitigation	<ul style="list-style-type: none"> -Keep phones in secure locations or require login for multi-user and multi-person security areas. - CallManager will only interoperate with known MAC addresses with known IP addresses. Includes - Administrative software and unused port controls.
Probability Before Mitigation	Medium
Probability After Mitigation	Low



Major Category:
Digital Snooping / Electronic Eavesdropping: #3

Threat	Man-in-the-Middle Attack: DHCP server insertion
Vulnerability	Reliance on DHCP server for IP addresses.
Recommended Mitigation	- Monitor the network for the presence of Rogue DHCP servers. - Static IP Addresses for all Major VoIP Components
Probability Before Mitigation	Medium
Probability After Mitigation	Low



Major Category: Denial of Service #1

Threat	CPU Resource Attack (without any account information)
Vulnerability	Capability for remote terminal access to the server.
Recommended Mitigation	Keep CallManager Operating System patches up to date. Provide firewall or access list controls to restrict network access to CallManager server. Monitor the voice network for DOS attacks.
Probability Before Mitigation	Medium
Probability After Mitigation	Low



Major Category: Denial of Service #2

Threat	Password Account lockout
Vulnerability	System lockout after several incorrect login attempts.
Recommended Mitigation	CallManager and Unity Related Servers will be kept in a Vault or Vault Type Room with restricted access to the console port. Remote Browser / Terminal access to the CallManager, Unity and related servers will be restricted via the use of firewall controls and user logins.
Probability Before Mitigation	Medium
Probability After Mitigation	Low

The Kansas City Plant is operated and managed by Honeywell Federal Manufacturing & Technologies, LLC, for the NNSA.





Major Category: Security Controls Failure

Threat	Unstable System
Vulnerability	Software bugs.
Recommended Mitigation	Keep backups and restore the prior working version of the system.
Probability Before Mitigation	Low
Probability After Mitigation	Low



Major Category: Malicious Software / Code

Threat	Server Compromised
Vulnerability	Computer system/ network vulnerabilities
Recommended Mitigation	Implement virus protection software on servers. Locate servers behind a firewall in a Vault or Vault Type Room. Provide the phone protections provided for the authorized Security Level. Only allow authorized users access to the system.
Probability Before Mitigation	Low (System is physically isolated from external networks.)
Probability After Mitigation	Low



Conclusion and Recommendations

This VoIP system is a logically isolated network within a closed system.

Connections to the internet or external telephone systems are encrypted.

Administrative access is only available through the firewall protected servers, which are strongly password-protected.

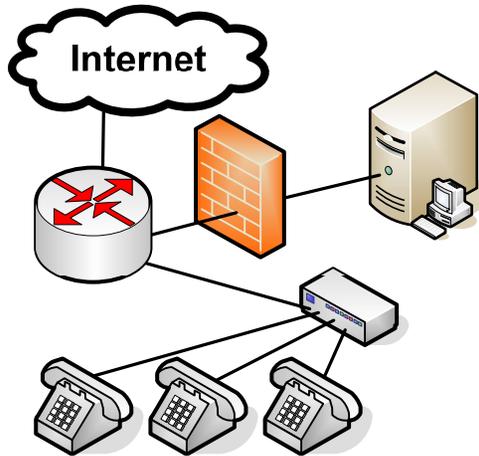
System components are either kept in a Vault or Vault Type Rooms under rigid access controls to protect physical access to the system.

The risk of confidentiality, integrity, or availability problems is low.

The most likely risk is an accidental denial of service attack from another machine on the same closed system. Not a problem (Not mission-critical).

Questions & Answers:

Proposal: Secure VoIP Communications System



A Joint NLIT 2007 Presentation:

LANL: Karl Pommer

KCP: Tom Beechwood

The End