Session ID: VVT-2003

ENTERPRISE IP TELEPHONY SECURITY PRACTICES AND TECHNOLOGIES

Jason Halpern

Recuerde siempre:

Cisco.com

- Apagar su teléfono móvil/pager, o usar el modo “silencioso”.

- Completar la evaluación de esta sesión y entregarla a los asistentes de sala.

- Ser puntual para asistir a todas las actividades de entrenamiento, almuerzos y eventos sociales para un desarrollo óptimo de la agenda.

- Completar la evaluación general incluida en su mochila y entregarla el miércoles 8 de Junio en los mostradores de registración. Al entregarla recibirá un regalo recordatorio del evento.

What Are We Worried About?

- Toll fraud exploits—Same as a PBX
- Eavesdropping
  - With TDM: Requires knowledge and access to a specific pair of wires
  - With VoIP: Anywhere in the broadcast domain
- DoS, worms, and the virus-de-jour
  - Targeted or anonymous attacks against Windows
  - TCP vulnerabilities, L2/L3 exploits

- Rogue device insertion
- Reconnaissance
- Man-in-the-middle
- DHCP spoofing and starvation
- Various TCP vulnerabilities
- Lots more…

IP Telephony Security: Build It in Layers

Cisco CallManager

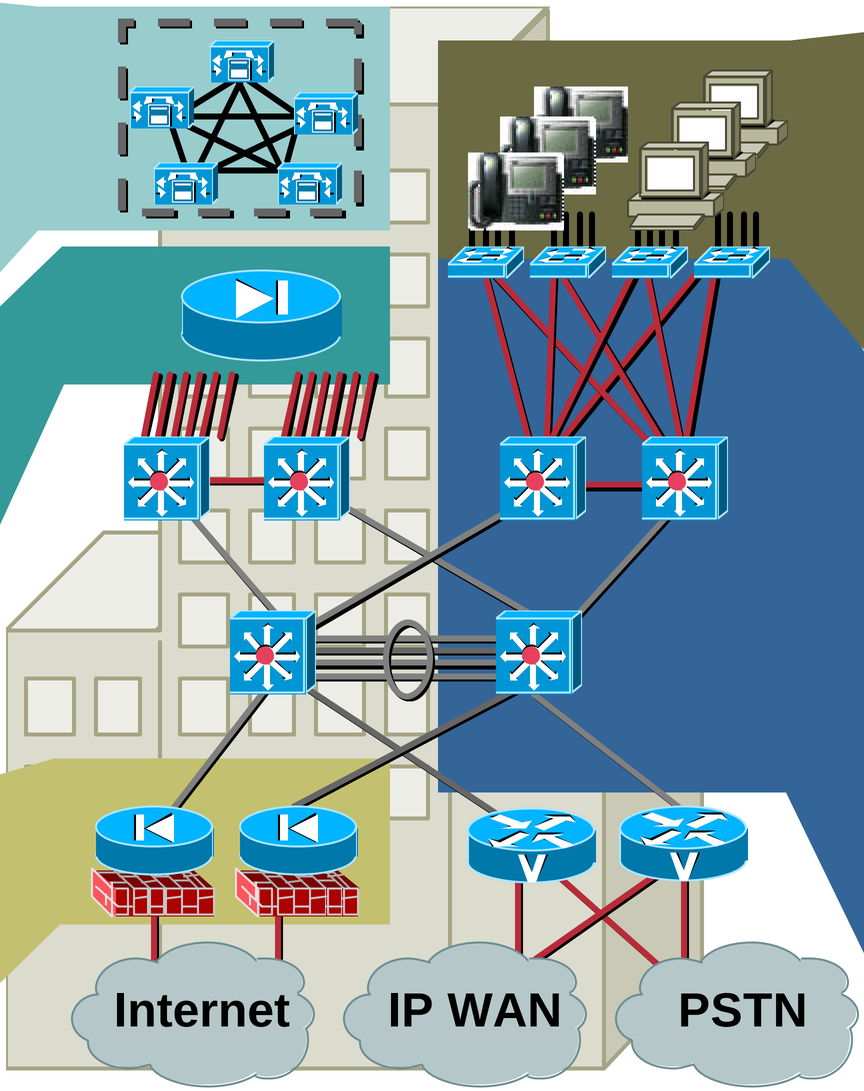
- Hardened OS
- Minimize Win2K services
- IPSec filters
- HIPS/anti-virus

Firewall or ACLs

- Allow only call control, LDAP, management
- Control source addresses

Outside World

- Voice over I-Net using V3PN
- IOS DoS tools
- Network IDS



Endpoints

- Separate voice and data VLANS
- Disable GARP and voice VLAN on PC port
- Authentication and Encryption

Campus Network

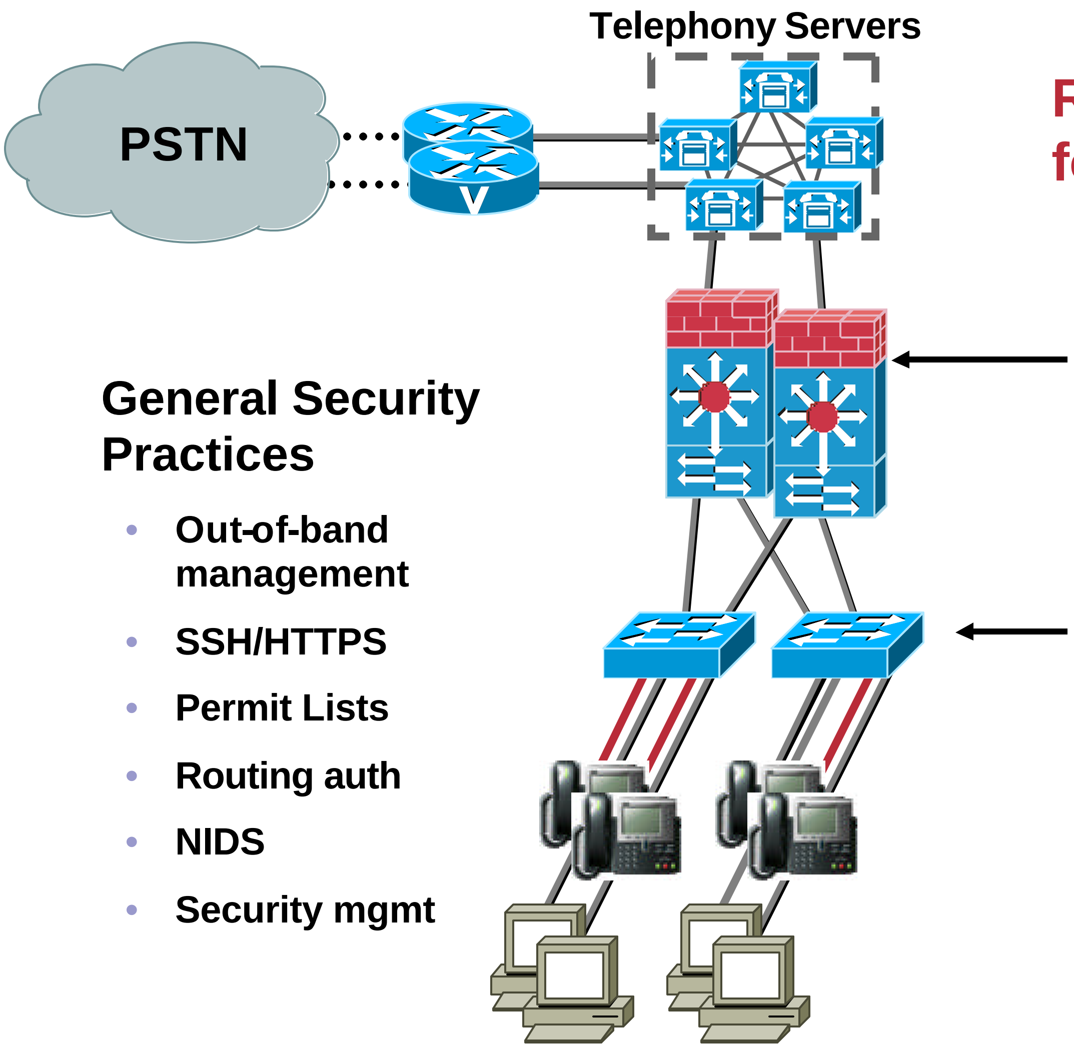
- High availability
- Layer 2/3 security
- IP filters between voice and data
- Policers
- Avoid NAT
- Secure access (OOB, TACACS+, SSH, Permit Lists)

Agenda

- Deployment Models for Secure IP Telephony
- Infrastructure Specifics for Voice
- Phone Protection
- OS Hardening
- Authentication and Encryption
- Toll Fraud Prevention
- How Does All of This Help?

DEPLOYMENT MODELS FOR SECURE IP TELEPHONY

Single Site



Refer to SAFE and SRND for All the Details

Firewall or ACL in Front of Telephony Servers with Rate Limiting

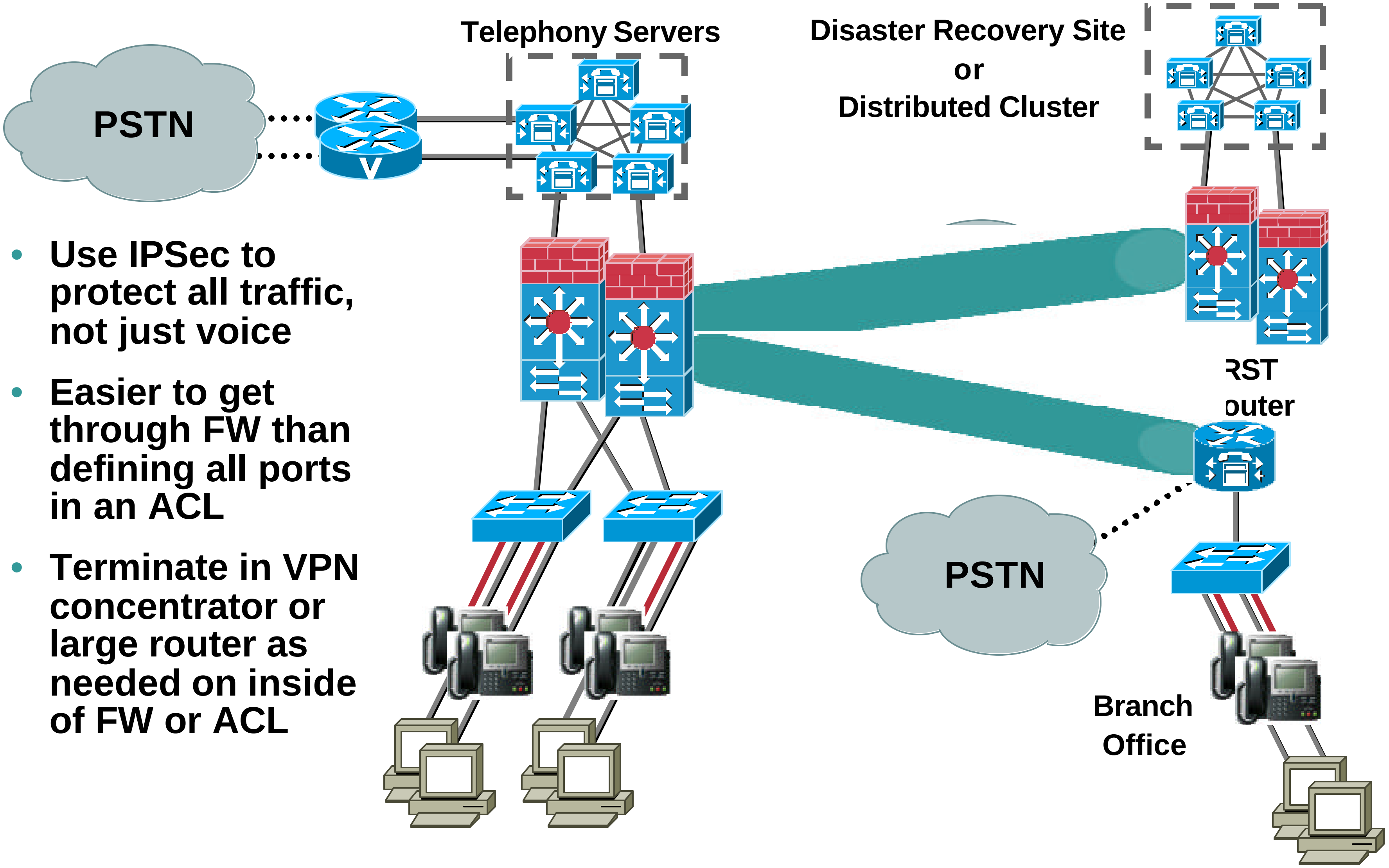
General Security Practices

- Out-of-band management
- SSH/HTTPS
- Permit Lists
- Routing auth
- NIDS
- Security mgmt

Layer 2 Best Practices

- Separate Voice/Data VLANs
- VACLs
- DHCP Snooping
- Dynamic ARP Inspection
- IP Source Guard
- Port Security
- Conditional QoS Trust

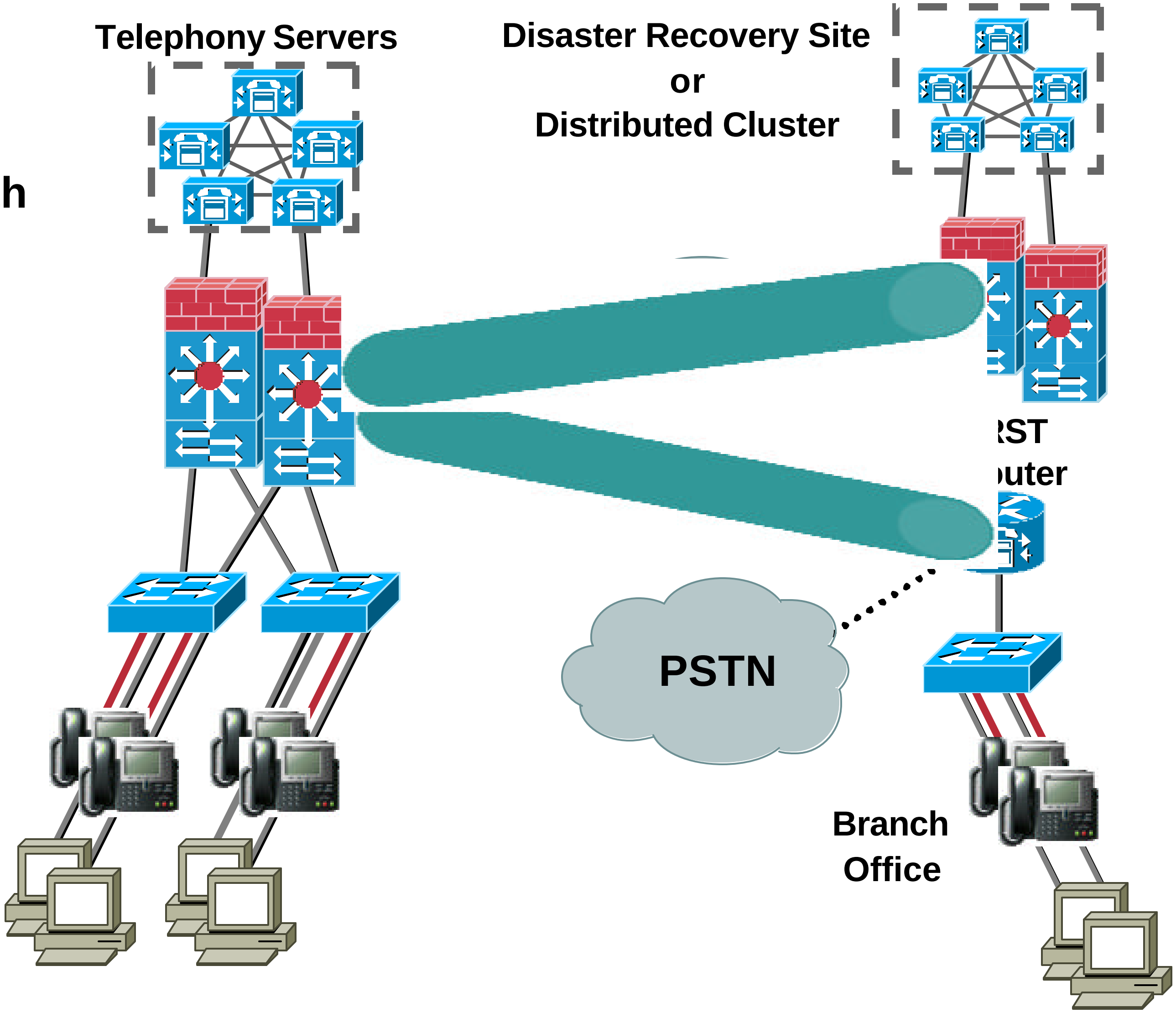
Connecting to a Branch Office or DR Site (1/2)



- 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

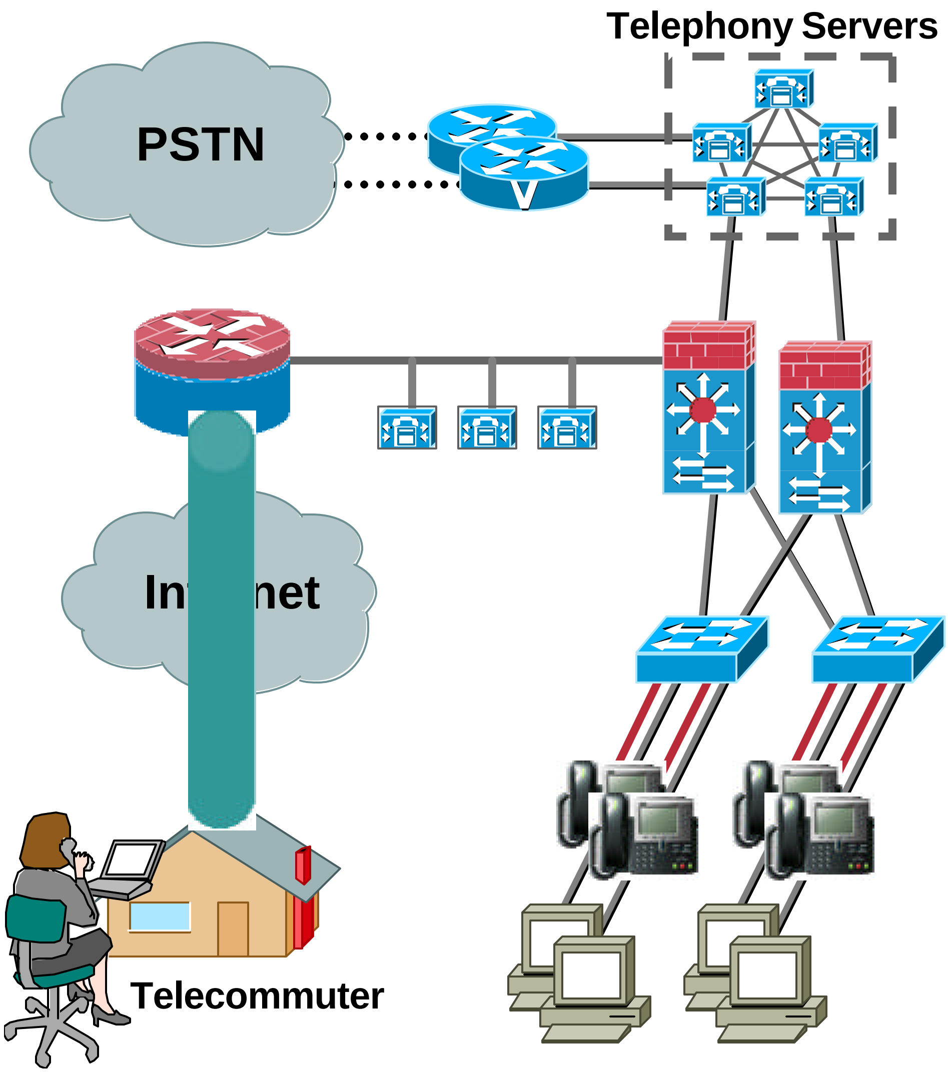
Connecting to a Branch Office or DR Site (2/2)

- **Remember to maintain bandwidth requirements for clustering-over-the-WAN**
  - **40ms maximum round-trip delay**
  - **Allow 900kbps for each 10,000 BHCA**
  - **Enough additional bandwidth to carry resulting calls in a failure situation**

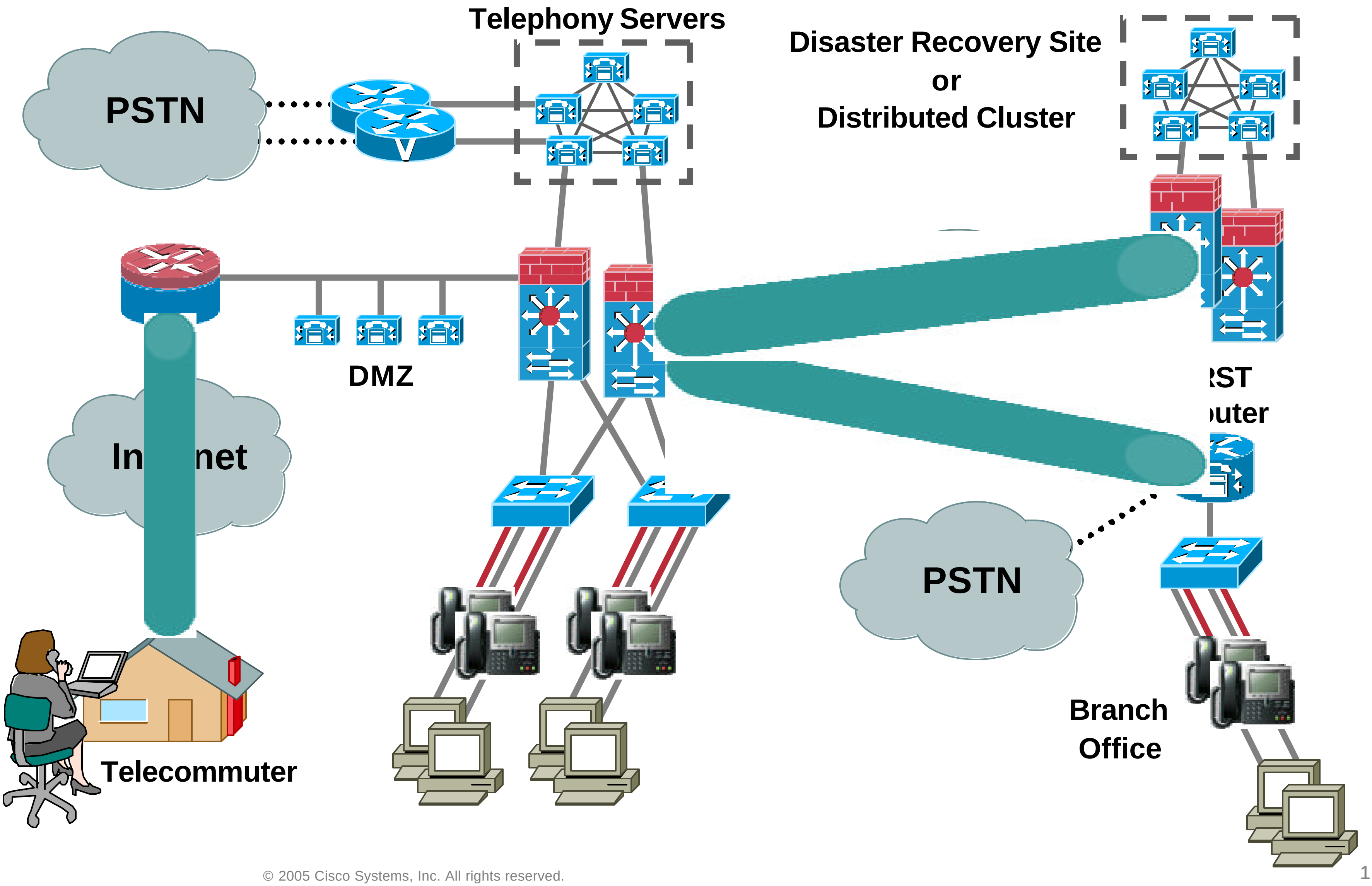


Connecting Telecommuters over the Internet

- 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



INFRASTRUCTURE SPECIFICS FOR VOICE

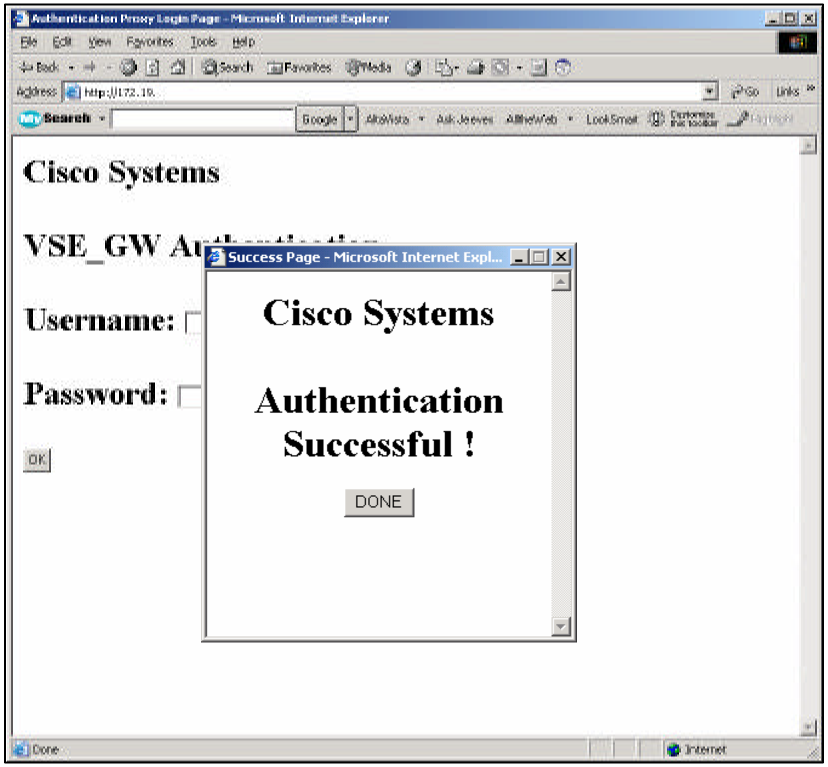
Firewall and NAT Voice ALGs

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 and 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!!!

Authentication Proxy

- Dynamic ACL in Cisco 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



Authentication Proxy Login Page - Microsoft Internet Explorer

Address http://172.19.

Cisco Systems

VSE_GW Au

Username: □

Password: □

OK

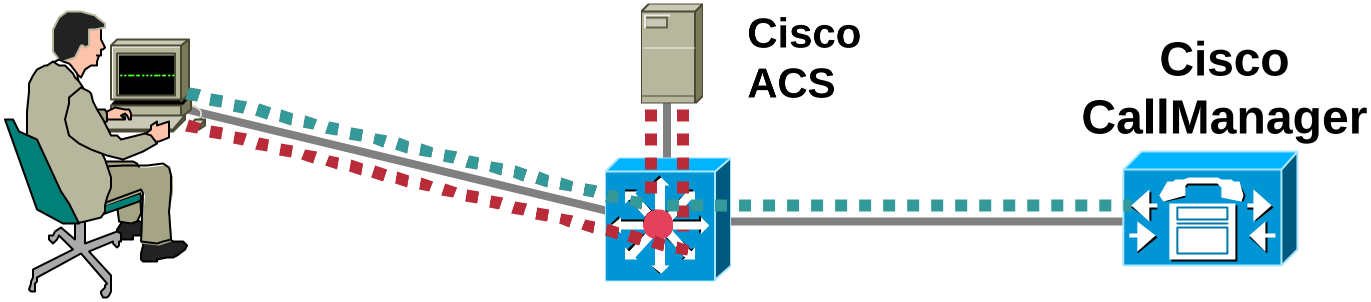
Success Page - Microsoft Internet Expl...

Cisco Systems

Authentication Successful !

DONE

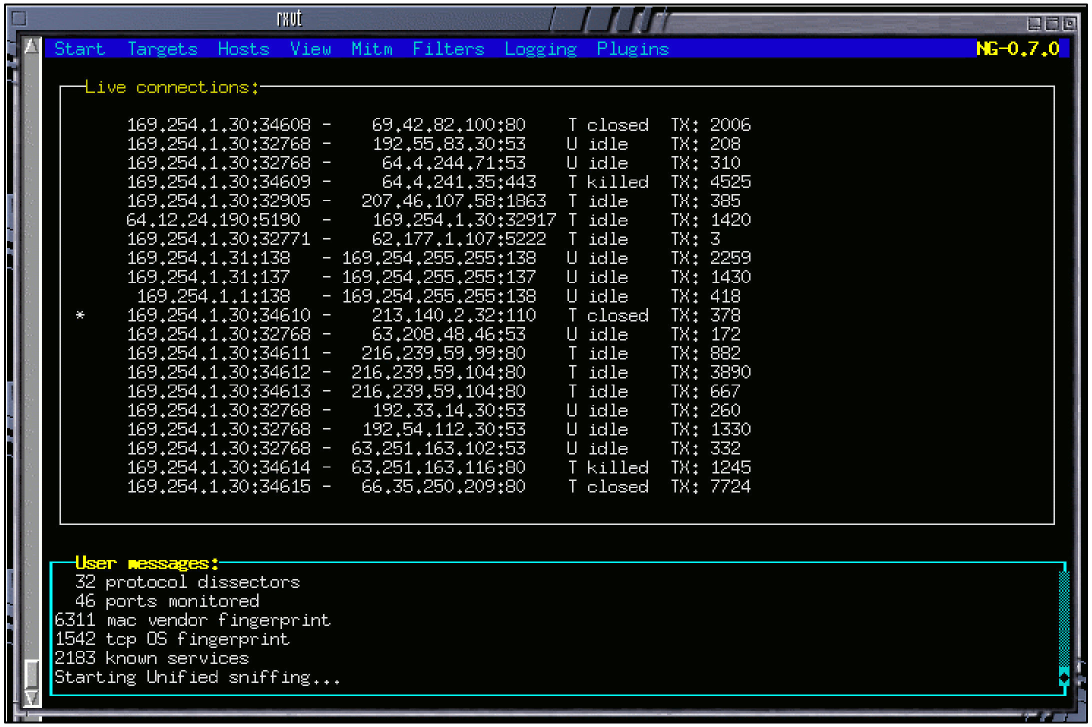
http://10.32.1.10/ccmadmin



Most Popular VoIP Hacker Tools

- Ettercap, dsniff—insert themselves as man-in-the-middle by sending gratuitous ARPs to opposing endpoints claiming to be the other end
    - Many other manifestations
- VOMIT (Voice over Misconfigured IP Telephony)
    - Converts TCPDump file to WAV file
- Nmap and nessus scan for open ports
- nemesis is a packet creation tool
- macof cam flooding
- Lots of others

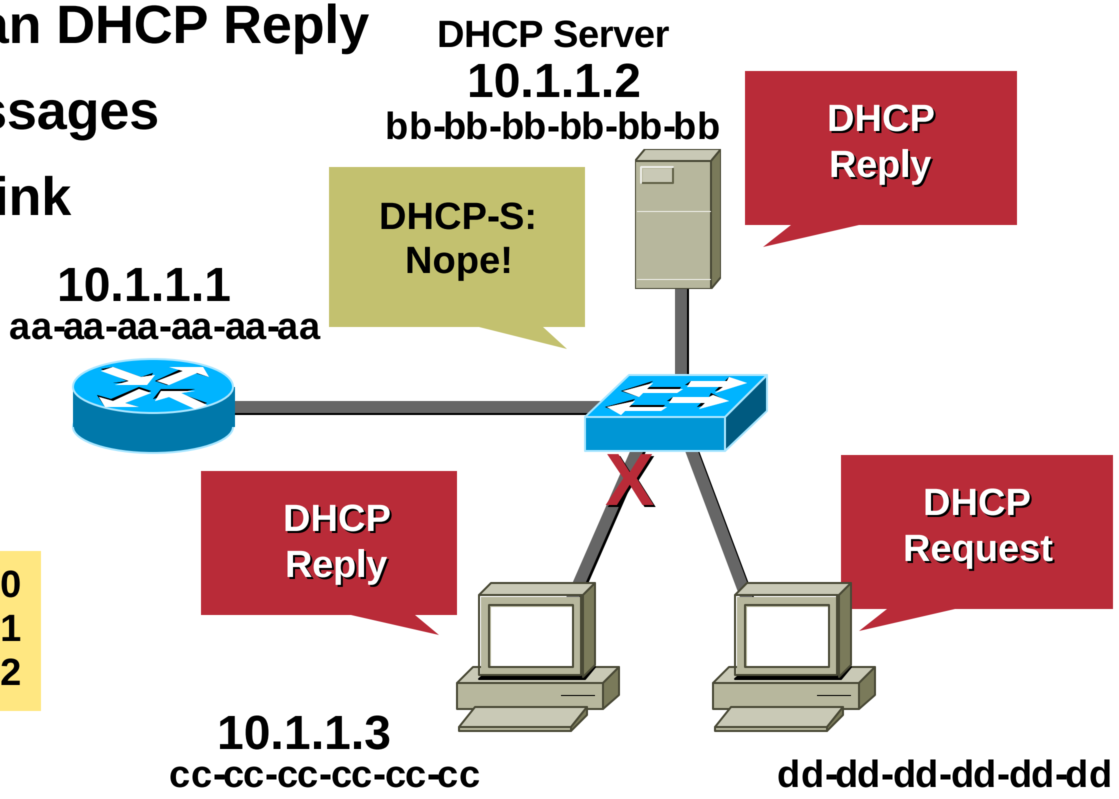
ettercap screenshot



```
Live connections:

     169.254.1.30:34608 -    69.42.82.100:80    T closed  TX: 2006
     169.254.1.30:32768 -    192.55.83.30:53    U idle    TX: 208
     169.254.1.30:32768 -     64.4.244.71:53    U idle    TX: 310
     169.254.1.30:34609 -     64.4.241.35:443   T killed  TX: 4525
     169.254.1.30:32905 -   207.46.107.58:1863  T idle    TX: 385
     64.12.24.190:5190  -    169.254.1.30:32917 T idle    TX: 1420
     169.254.1.30:32771 -    62.177.1.107:5222  T idle    TX: 3
     169.254.1.31:138   - 169.254.255.255:138   U idle    TX: 2259
     169.254.1.31:137   - 169.254.255.255:137   U idle    TX: 1430
      169.254.1.1:138   - 169.254.255.255:138   U idle    TX: 418
 *   169.254.1.30:34610 -    213.140.2.32:110   T closed  TX: 378
     169.254.1.30:32768 -    63.208.48.46:53    U idle    TX: 172
     169.254.1.30:34611 -   216.239.59.99:80    T idle    TX: 882
     169.254.1.30:34612 -  216.239.59.104:80    T idle    TX: 3890
     169.254.1.30:34613 -  216.239.59.104:80    T idle    TX: 667
     169.254.1.30:32768 -    192.33.14.30:53    U idle    TX: 260
     169.254.1.30:32768 -   192.54.112.30:53    U idle    TX: 1330
     169.254.1.30:32768 -  63.251.163.102:53    U idle    TX: 332
     169.254.1.30:34614 -  63.251.163.116:80    T killed  TX: 1245
     169.254.1.30:34615 -   66.35.250.209:80    T closed  TX: 7724

User messages:
  32 protocol dissectors
  46 ports monitored
6311 mac vendor fingerprint
1542 tcp OS fingerprint
2183 known services
Starting Unified sniffing...
```

Prevent DHCP Spoofing and Exhaustion (1/2)

- 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

Prevent DHCP Spoofing and Exhaustion (2/2)

DHCP Snooping Supported On:

- **Catalyst 6000 IOS 12.2(17a)SX2, Catalyst OS 8.3(1)**
- **Catalyst 4000 IOS 12.1(12c)EW**
- **Catalyst 3750 12.1(19)EA1**

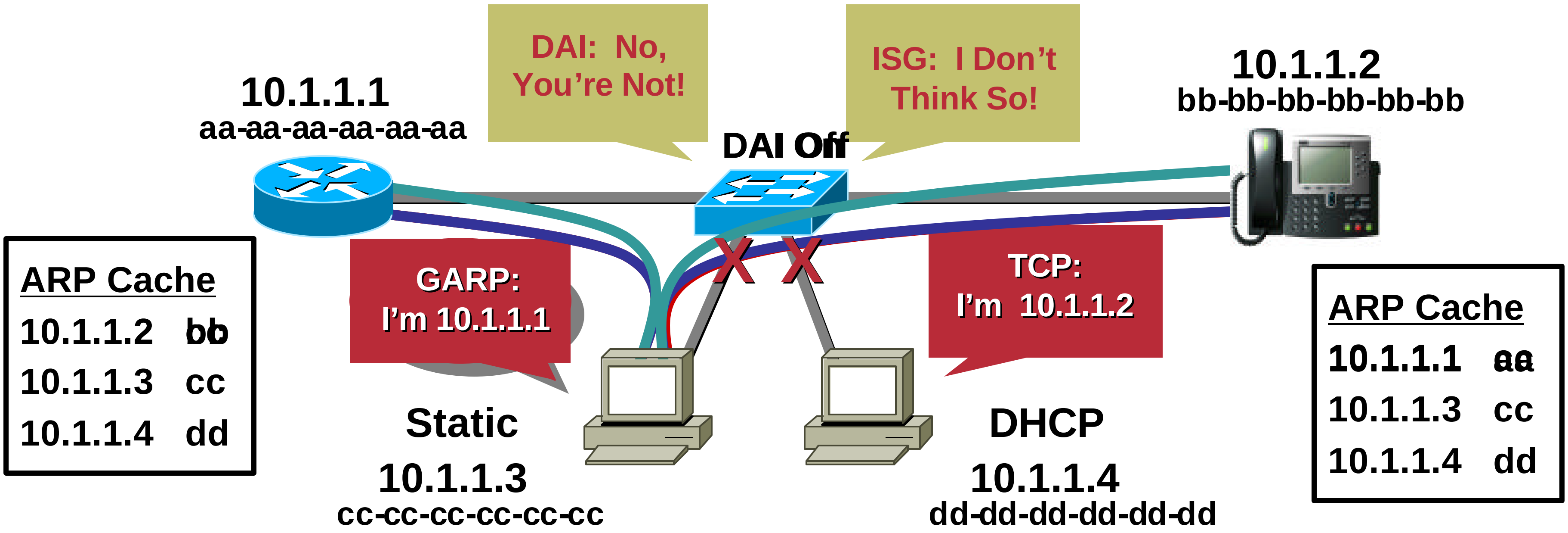
```
ip dhcp snooping
ip dhcp snooping vlan <id>

interface FastEthernet1/1
 ip dhcp snooping trust

interface FastEthernet1/2
 ip dhcp snooping limit rate 10
```

Stop Man-in-the-Middle Attacks (1/2)

- 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



ARP Cache

10.1.1.2	bb
10.1.1.3	cc
10.1.1.4	dd

ARP Cache

10.1.1.1	aa
10.1.1.3	cc
10.1.1.4	dd

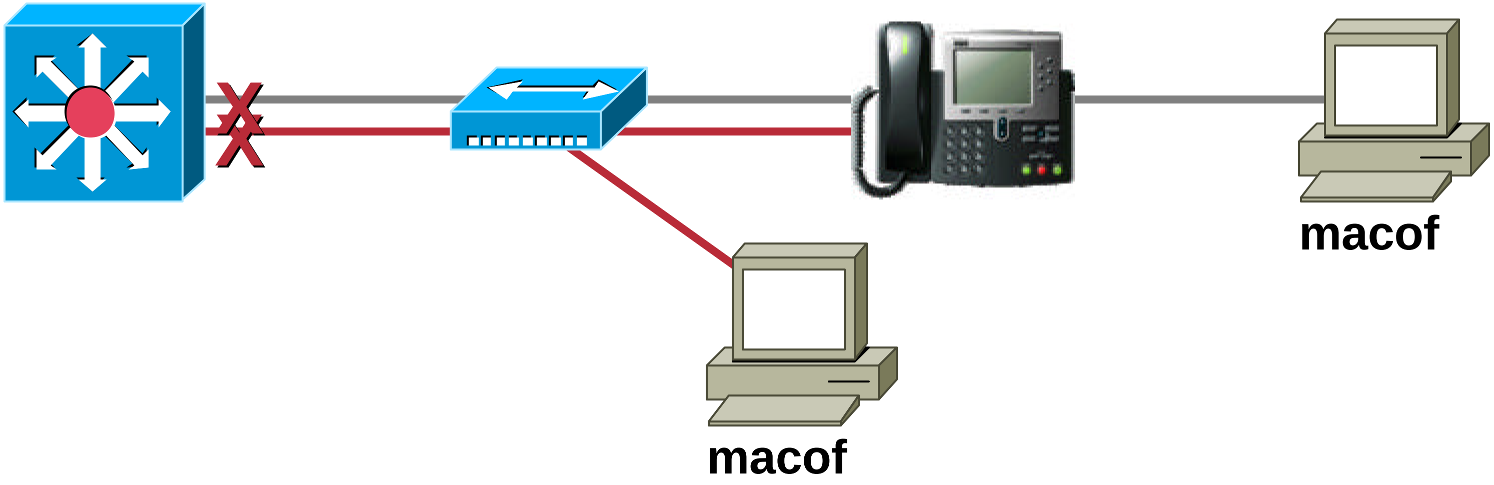
Stop Man-in-the-Middle Attacks (2/2)

DAI and IP Source Guard Supported On:

- Catalyst 6000 IOS 12.2(17a)SX2, Catalyst OS 8.3(1)
- Catalyst 4K IOS 12.1(19)EW
- Catalyst 3750 12.2(RLS3.5)SE (Summer ’04)

```
ip arp inspection vlan <id>
ip arp inspection validate src-mac ip

Interface FastEthernet1/0
 ip arp inspection trust

interface FastEthernet1/1
 ip arp inspection limit rate 10
 ip verify source vlan dhcp-snooping port-security
```

Prevent MAC Flooding Attacks



Limit Port to No More than 3 Mac Addresses

```
Interface FastEthernet1/1
 switchport port-security
 switchport port-security maximum 3
 switchport port-security aging time 1
 switchport port-security violation restrict
 switchport port-security aging type inactivity
```

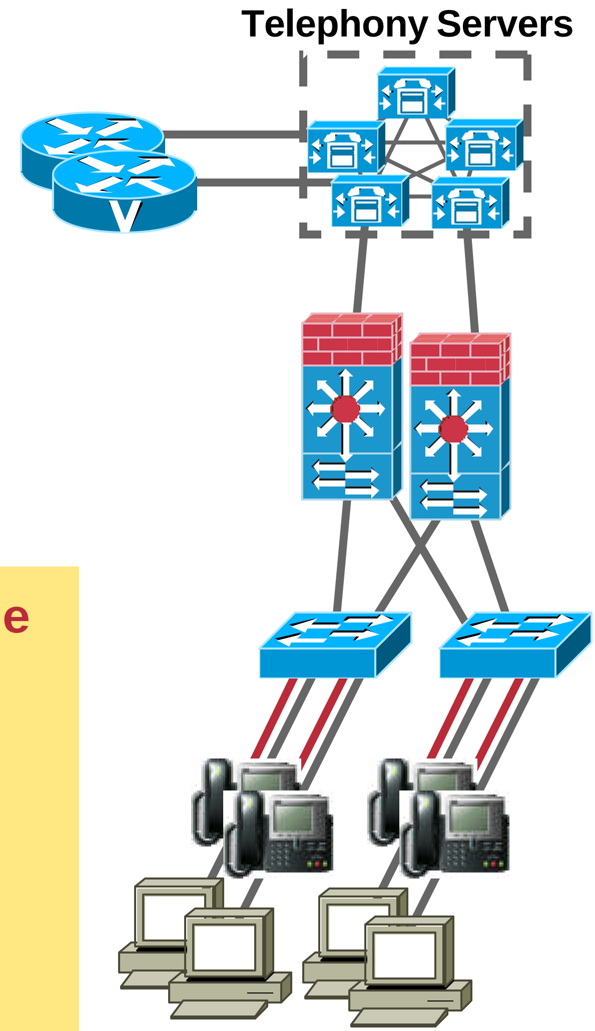
Why 3 macs?

- **Phone on data VLAN**
- **Phone on voice VLAN**
- **PC on data VLAN**

Use VACLs to 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!!!

```
permit udp <voice subnet> <mask> range
16384 32768 any range 16384 32768

permit udp <voice subnet> <mask> tftp
<server subnet> <mask>

permit tcp <voice subnet> <mask>
<server subnet> <mask>
```



CISCO IP PHONE PROTECTION

Stop Rogue Images from Entering Phones

- Signed firmware images

  Guaranteed from Cisco

  Unique signature for each phone model

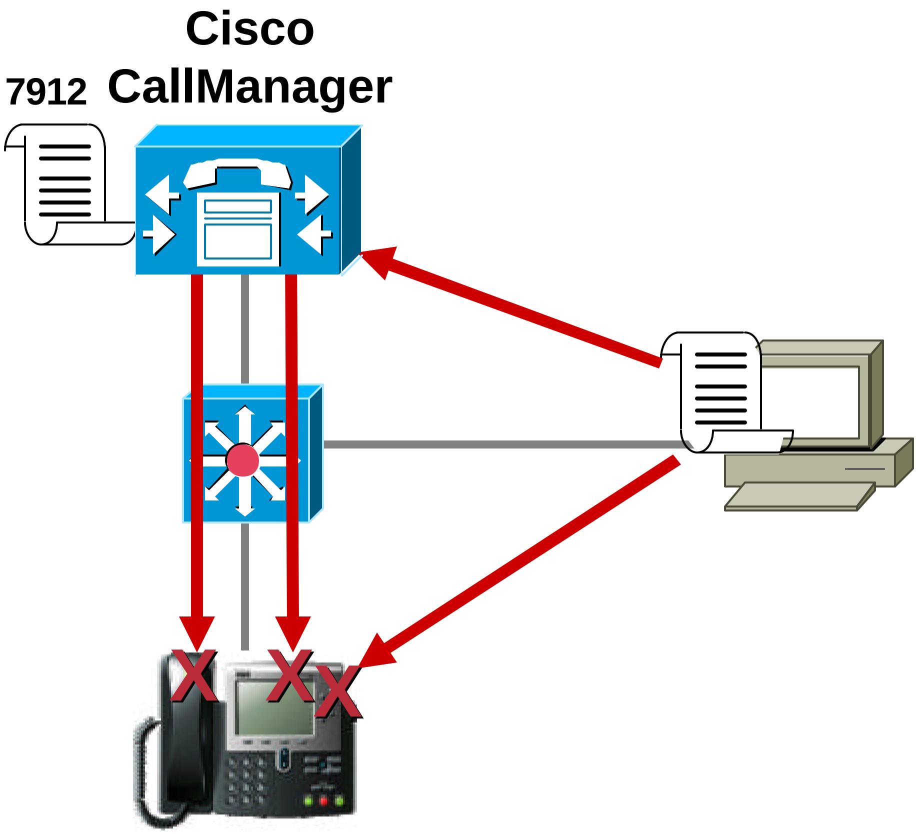
  Can't subvert security features!

  CCM 3.3(3)

- Signed config files

  7940, 7960 and 7970

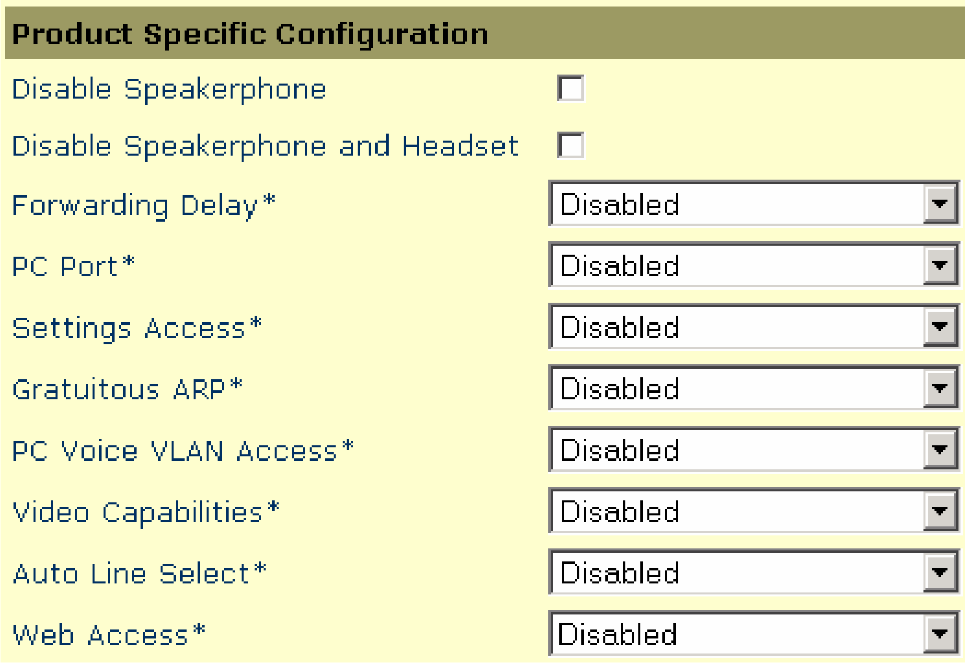
  CCM 4.0



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

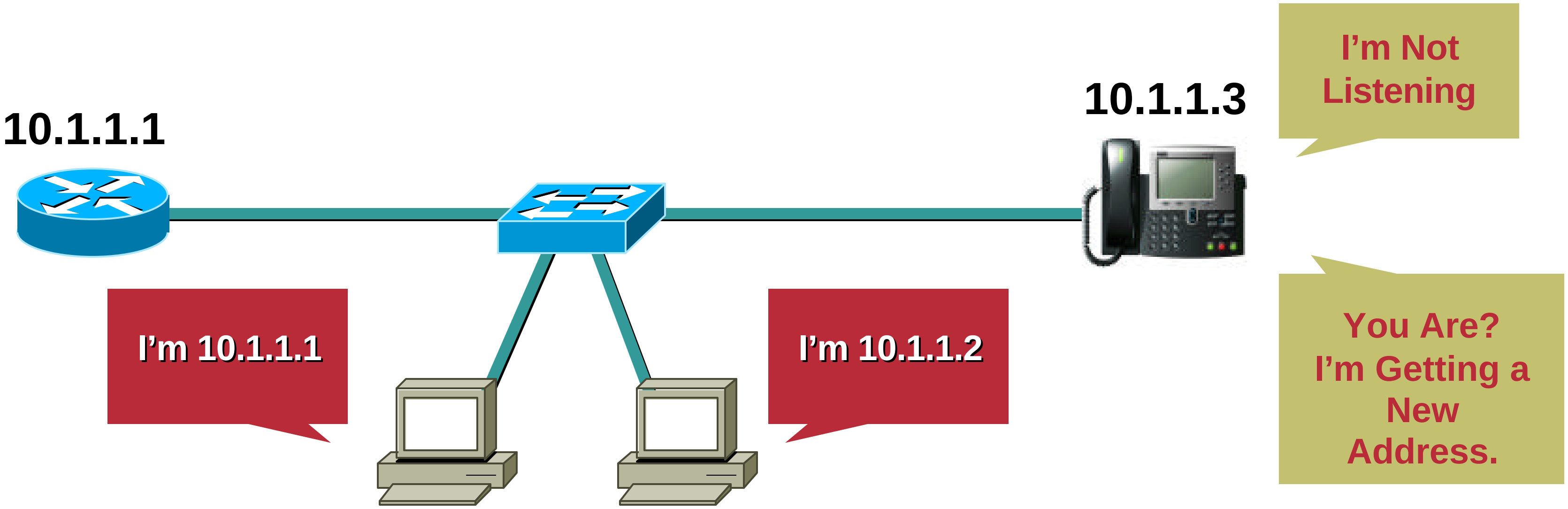
Disable Speakerphone	□
Disable Speakerphone and Headset	□
Forwarding Delay*	Disabled
PC Port*	Disabled
Settings Access*	Disabled
Gratuitous ARP*	Disabled
PC Voice VLAN Access*	Disabled
Video Capabilities*	Disabled
Auto Line Select*	Disabled
Web Access*	Disabled

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"

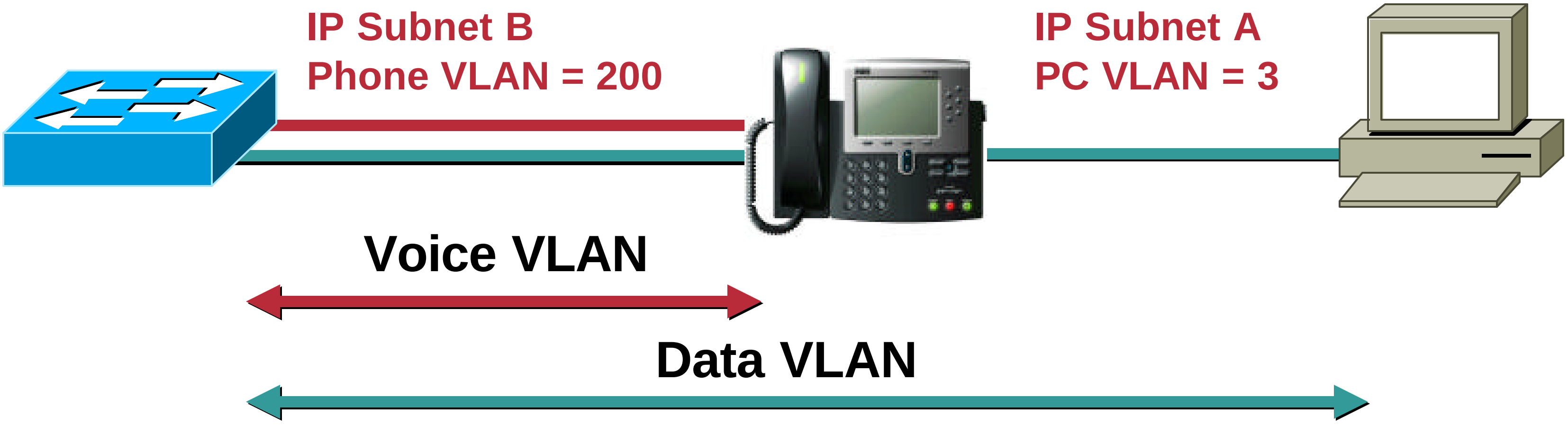
Better to do this in layer two



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

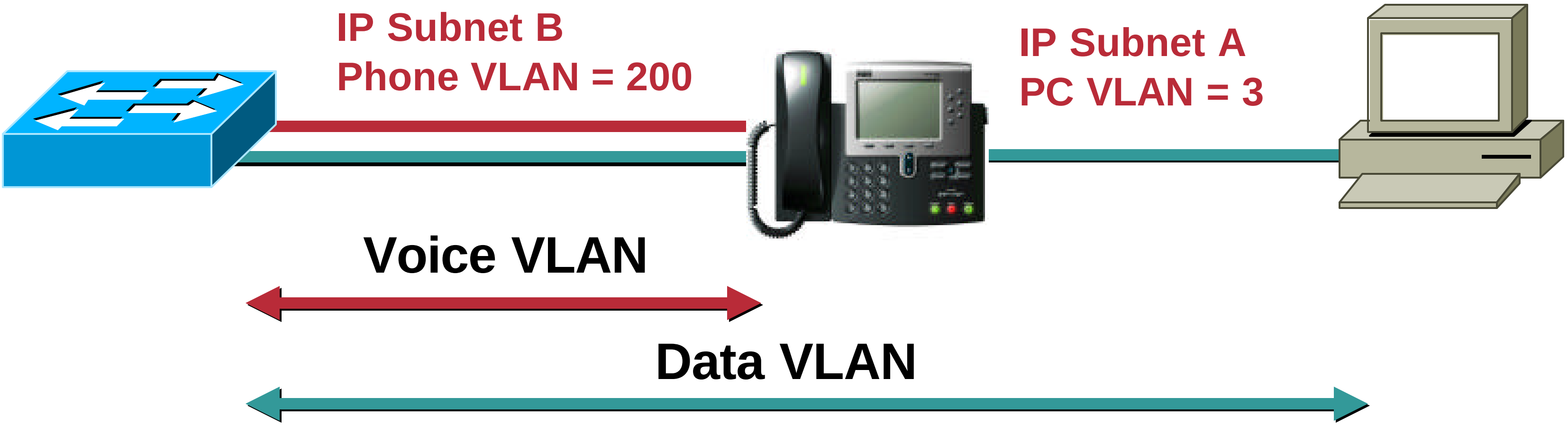
Successfully Stops VOMIT



Block PC Access to Voice VLAN

Differences Between Phone Model Implementations

- 7940 and 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



SECURING THE WINDOWS OPERATING SYSTEM

Hardened Windows Operating System

- Windows-2000 Server OS shipped by default, and downloadable from www.cisco.com
- Same OS build used for seven applications:

  Cisco CallManager, Emergency Responder, Conference Connection, Personal Assistant, IPCC Express, IP/IVR, and ISN

- Every version gets incrementally more secure:

  Registry, IP stack, file system, permissions, middleware apps, disable unused services, etc.

  Release Notes provide details

Security Patch and Hotfix Policy

- Cisco monitors several sites such as Microsoft, CERT, and SANS for new vulnerabilities
- Any applicable patch deemed Severity 1 or Critical is tested and posted to www.cisco.com within 24 hours as hotfixes
- All applicable patches are consolidated and posted once per month as incremental service releases
- Waiting for MS Software Update Service 2.0
- Email alias tells you when new patches are available
- http://www.cisco.com/warp/public/779/largeent/software_patch.html

Blaster Patch Was Available on www.cisco.com Three Weeks Before It Hit the Internet!

Sasser Patch Was Available on www.cisco.com Two Weeks Before It Hit the Internet!

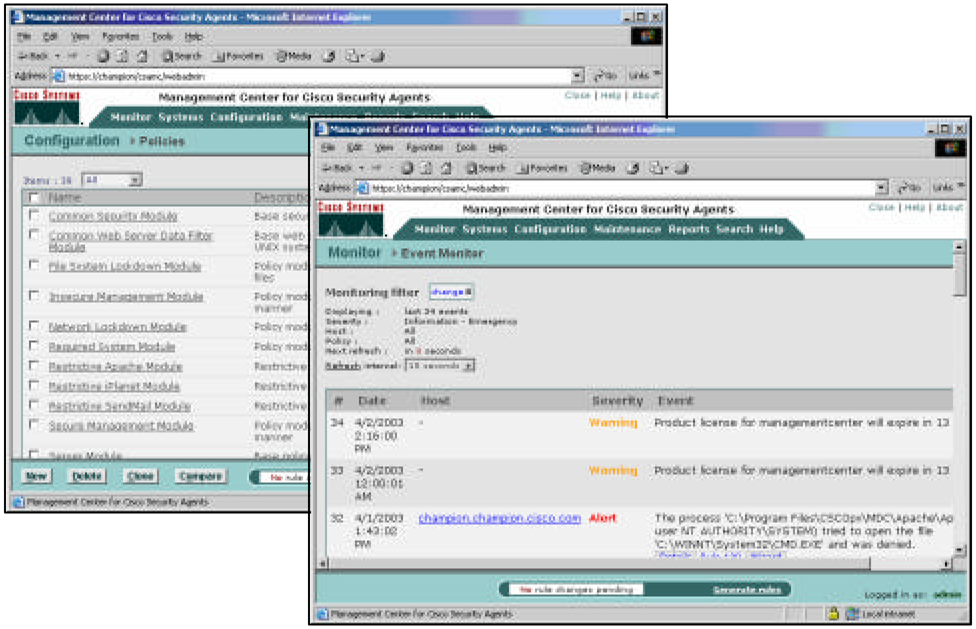
Anti-Virus Software

- Cisco doesn't sell it, bundle it, include it or OEM it, but we do recommend you run it!!!
- McAfee VirusScan Enterprise 4.5, 7.0 and 7.1
- Symantec Corporate Edition 7.61, 8.0 and 8.1
- Trend Micro ServerProtect5

Disable Heuristic Scanning—
If Not, 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
- VMS centrally administers managed agents with distributed, autonomous policy enforcement
- Effective against existing and previously unseen attacks
- Stopped Slammer, Nimda and Code Red sight unseen with out-of-the-box policies


Management Center for Cisco Security Agents - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://champion/csamc/webadmin
Go Links
Cisco Systems
Close | Help | About
Monitor Systems Configuration Maintenance Reports Search Help
New Delete Clone Compare
No rule changes pending
Generate rules
Logged in as: admin
Management Center for Cisco Security Agents
Local intranet

Management Center for Cisco Security Agents

Configuration › Policies

Items : 16 All

Name	Description
Common Security Module	Base secu
Common Web Server Data Filter Module	Base web UNIX syste
File System Lockdown Module	Policy mod files
Insecure Management Module	Policy mod manner
Network Lockdown Module	Policy mod
Required System Module	Policy mod
Restrictive Apache Module	Restrictive
Restrictive iPlanet Module	Restrictive
Restrictive SendMail Module	Restrictive
Secure Management Module	Policy mod manner
Server Module	Base polic

Monitor › Event Monitor

Monitoring filter change

Displaying : last 34 events
Severity : Information - Emergency
Host : All
Policy : All
Next refresh : in 8 seconds
Refresh interval: 10 seconds

#	Date	Host	Severity	Event
34	4/2/2003 2:16:00 PM	-	Warning	Product license for managementcenter will expire in 13
33	4/2/2003 12:00:01 AM	-	Warning	Product license for managementcenter will expire in 13
32	4/1/2003 1:43:02 PM	champion.champion.cisco.com	Alert	The process 'C:\Program Files\CSCOpx\MDC\Apache\Ap user NT AUTHORITY\SYSTEM) tried to open the file 'C:\WINNT\System32\CMD.EXE' and was denied.

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

- Additional password restrictions, event logs, NTLM auth., registry settings, file and IIS ACLs, deletes un-needed files and 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 Cisco 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 and iLO passwords
  - Disable iLO if not used
- Remove everyone group from share permissions
- Details in the OptionalSecurity Readme

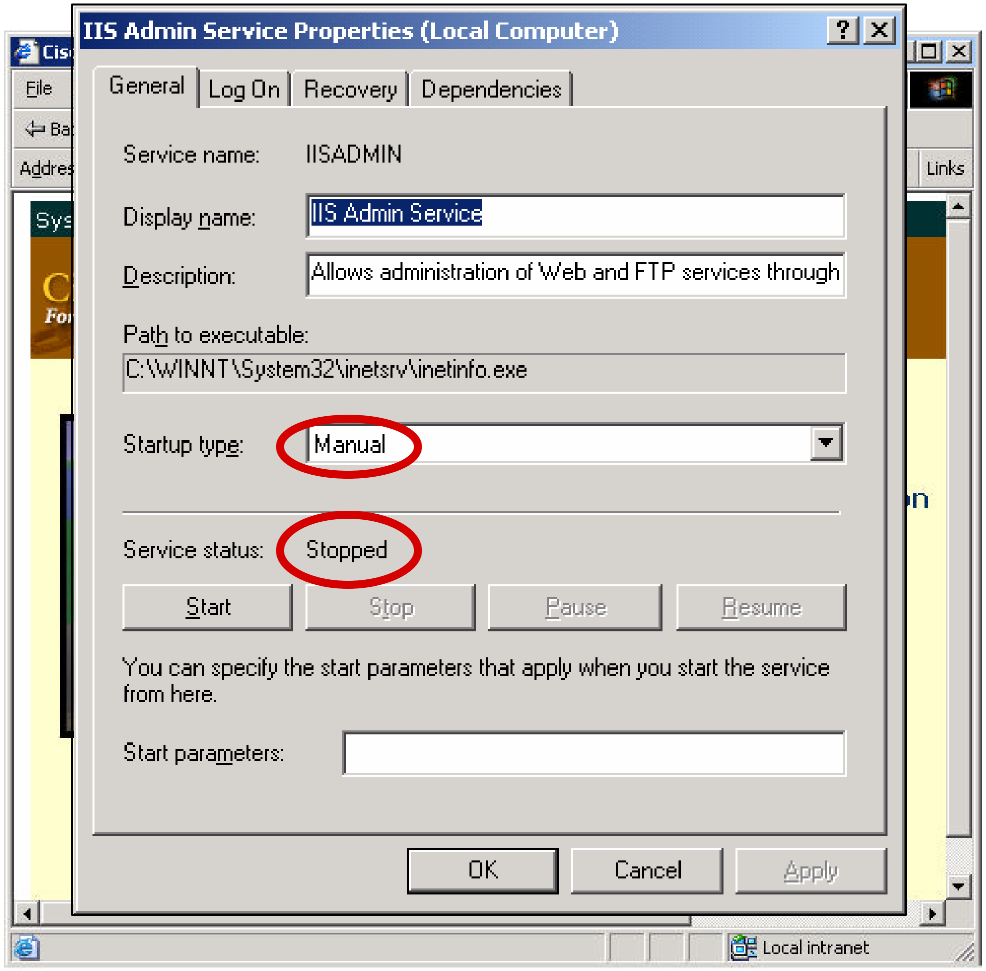
Protect Cisco CallManager from Unwanted Access

IP Security Filter—Blocks Fixed Windows and SQL Ports

- Extra layer of protection from worms, viruses, and hackers
- Provided script makes it easy—in C:\Utils
- Apply IP addresses, subnets, or local hosts for full access—include servers for third-party apps (billing, management, etc.)
- Packets from any other address blocks SMB, ICMP (in but not out), Netbios, NTP, SNMP, and SQL
- HTTP, Terminal Services and VNC not blocked
- Found in local security policy
- Not to be confused with TCP Filters

Protect Windows Against Common Exploits

- **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**



IIS Admin Service Properties (Local Computer)

Service name: IISADMIN

Display name: IIS Admin Service

Description: Allows administration of Web and FTP services through

Path to executable:
C:\WINNT\System32\inetsrv\inetinfo.exe

Startup type: Manual

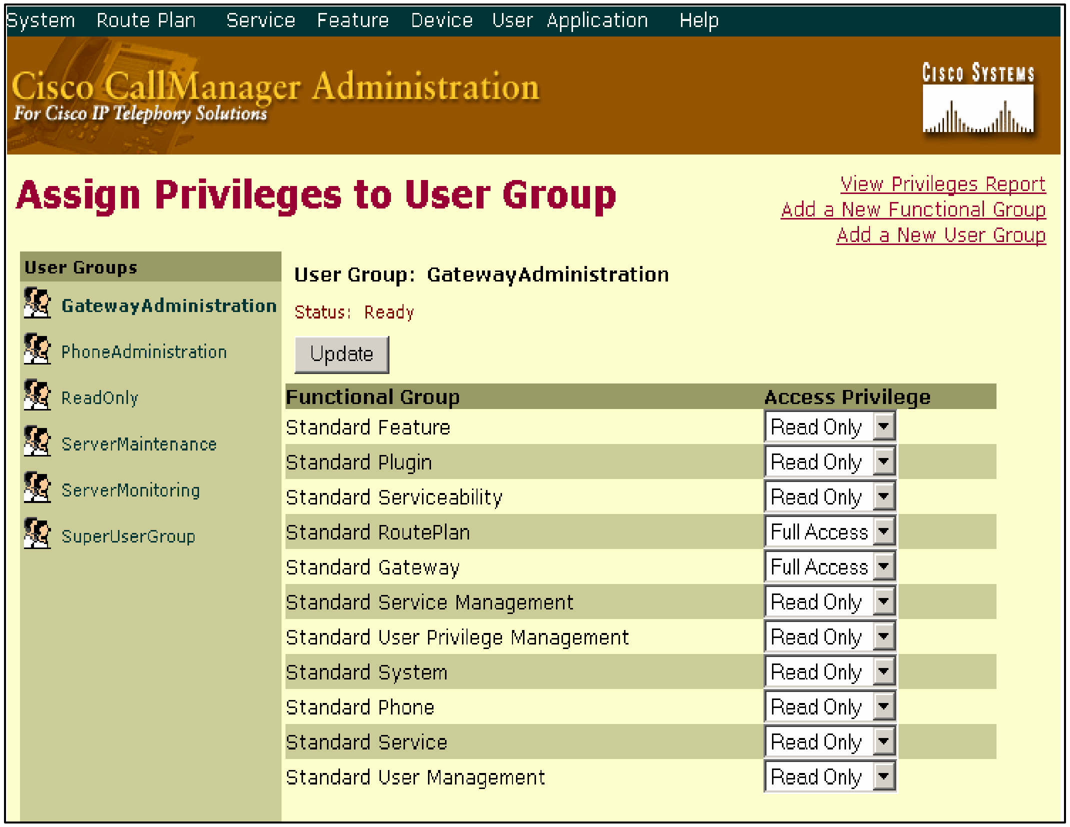
Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Limit Access to Admin Webpages

- **Multi-Level Admin (MLA) limits access by user ID**
- **Users are defined in LDAP directory**
- **Users are placed in User Groups**
- **User Groups are placed in Functional Groups**
- **Functional Groups have access to individual webpages**
  - **Read/write**
  - **Read-only**
  - **No access**



Assign Privileges to User Group

User Groups
- GatewayAdministration
- PhoneAdministration
- ReadOnly
- ServerMaintenance
- ServerMonitoring
- SuperUserGroup

User Group: GatewayAdministration

Status: Ready

Functional Group	Access Privilege
Standard Feature	Read Only
Standard Plugin	Read Only
Standard Serviceability	Read Only
Standard RoutePlan	Full Access
Standard Gateway	Full Access
Standard Service Management	Read Only
Standard User Privilege Management	Read Only
Standard System	Read Only
Standard Phone	Read Only
Standard Service	Read Only
Standard User Management	Read Only

OS Security Taboos (1/2)

Security Settings That Are Not Recommended

- Shutdown if unable to write security log—Not ideal for a strategic application
- Account lockout after N failed login attempts—Breaks low-level service accounts
- Crash control—Disabling Dr. Watson crash dumps adds complexity to forensic troubleshooting
- Convert D: from FAT to NTFS—“Same Server Recovery” won’t work
- Clear page file at reboot—Reboots can take 30 minutes or longer
- A few other odds and ends—check the OptionalSecurity Readme in the C:\Utils\SecurityTemplates directory

OS Security Taboos (2/2)

Security Settings That Should Not Be Done in Any Circumstance

- DON'T join an AD domain*
  - Role-based admin not supported
  - AD group policies—9.3 * 10^157 permutations
- DON'T delete, disable or rename any service accounts—processes, like CCM or SQL, won't run
- DON'T set CMOS power on password—server won't boot after power failure until PW is entered
- DON'T change permissions—high probability that CCM will break
- DON'T install un-approved agents or third-party applications

*AD Plug-in for LDAP Directory Is Supported as an Alternative Directory

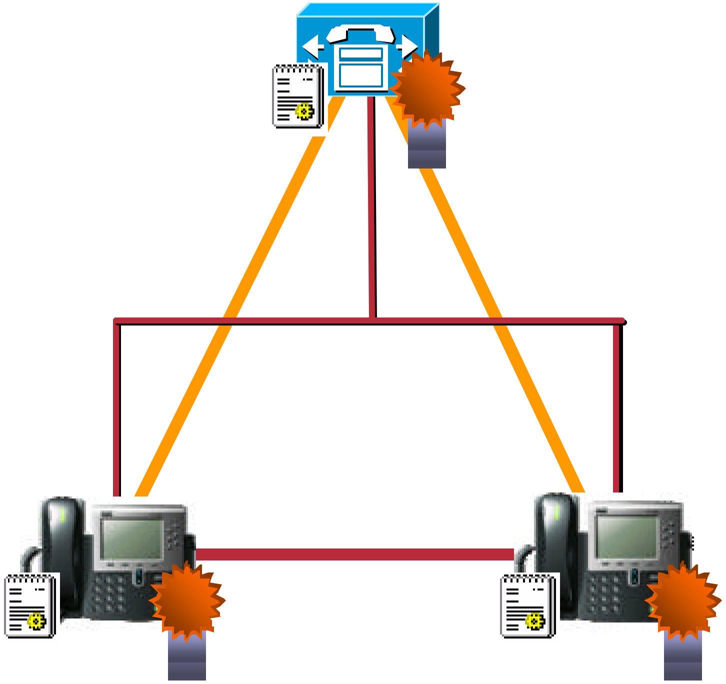
OS Hardening Summary

- Hardened OS
- Patches and hotfixes kept up to date
- Anti-virus
- Cisco Security Agent
- Optional security settings
  - Optional security script
  - Manual settings for your environment
  - Disable unused services
  - Apply IIS and IP security filters

CISCO IP TELEPHONY AUTHENTICATION AND ENCRYPTION

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

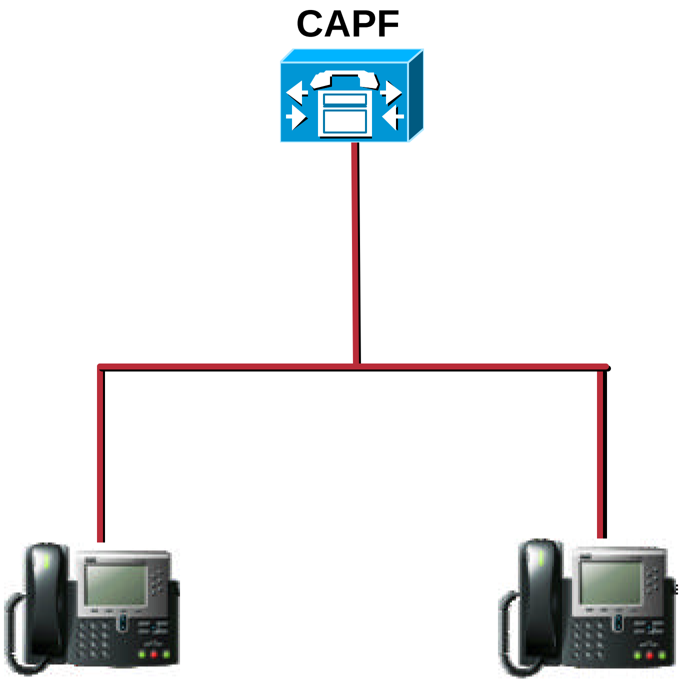


In Cisco CallManager 4.0,

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

Public Key/Private Key Pair

- Every device has a Public Key/Private Key pair
- Derived and stored 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



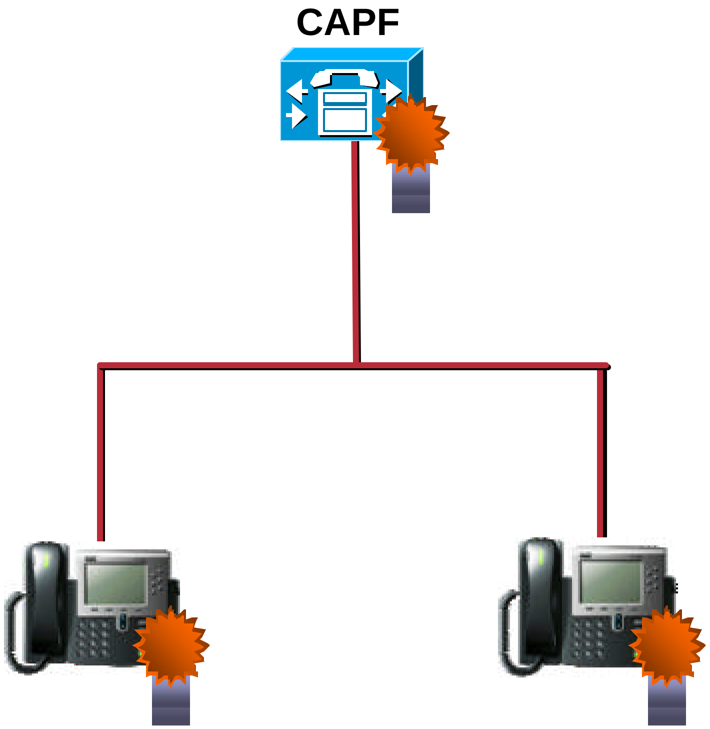
X.509v3 Certificates

- **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

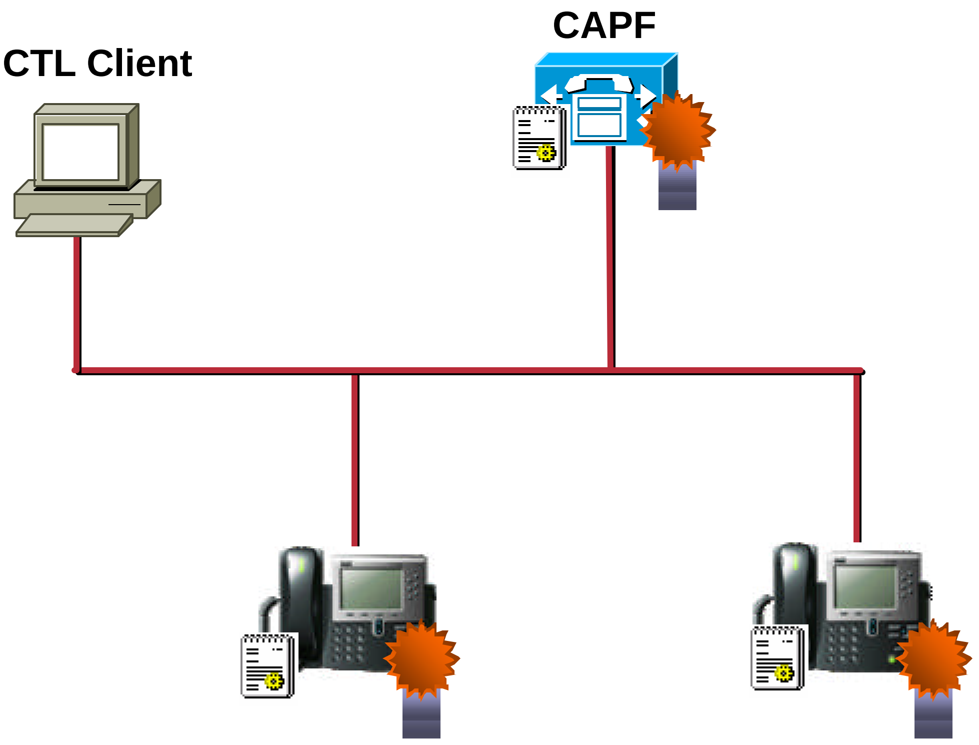


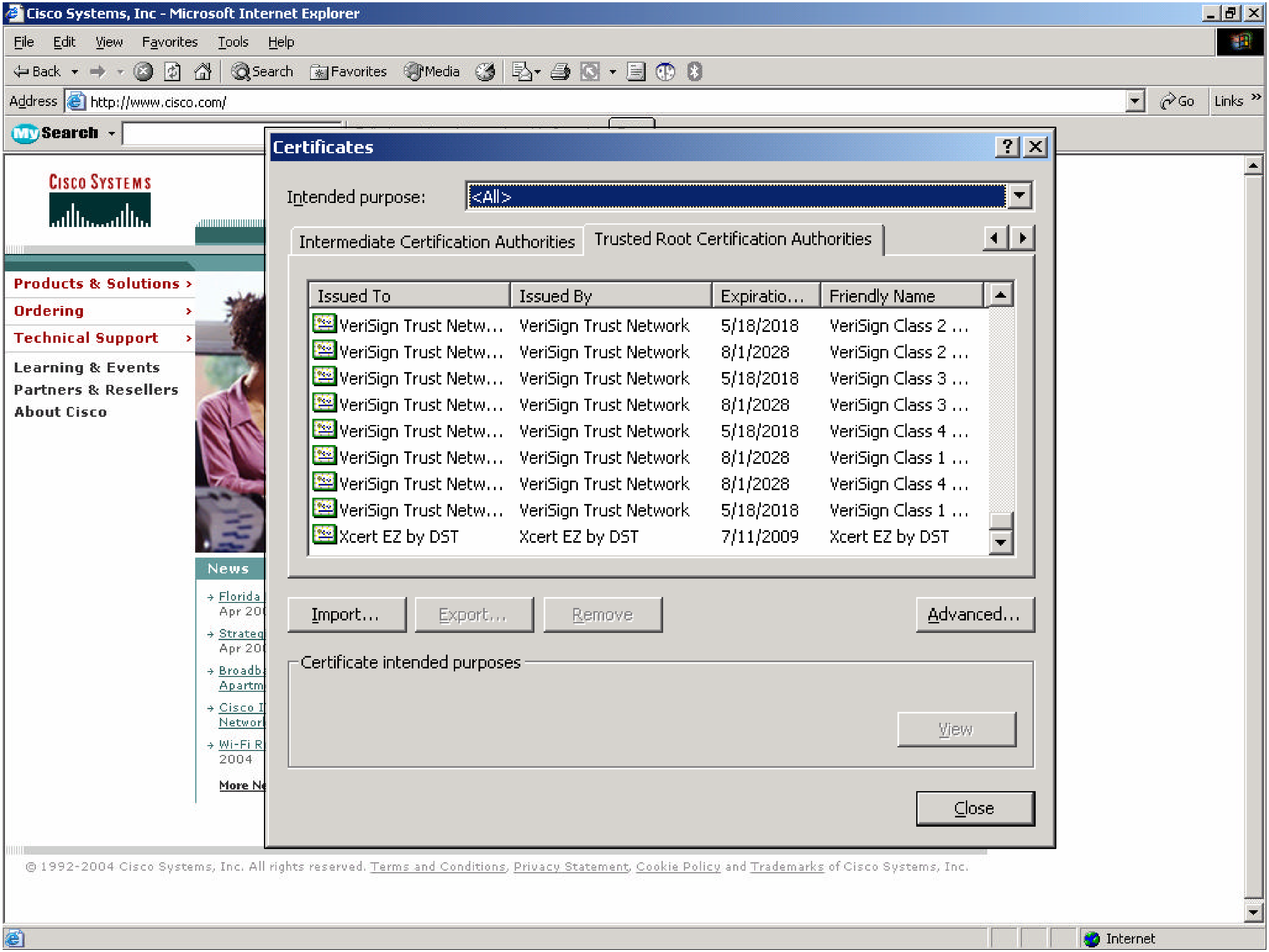
Certificate Trust List

- Certificate Trust List contains list of trusted devices—CCM, TFTP, CAPF
- Similar to Trusted Root CAs in IE
- Generated by CTL client
- Downloaded to phone during TFTP
- All phones in a cluster have the same CTL file
- CCM has a dynamic CTL file

  Populated during TLS registration

  Contained in OpenSSL database




Cisco Systems, Inc - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.cisco.com/
Go Links
My Search
Cisco Systems
Products & Solutions
Ordering
Technical Support
Learning & Events
Partners & Resellers
About Cisco
News
Certificates
Intermediate Certification Authorities
Trusted Root Certification Authorities
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close
Internet

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
VeriSign Trust Netw...	VeriSign Trust Network	5/18/2018	VeriSign Class 2 ...
VeriSign Trust Netw...	VeriSign Trust Network	8/1/2028	VeriSign Class 2 ...
VeriSign Trust Netw...	VeriSign Trust Network	5/18/2018	VeriSign Class 3 ...
VeriSign Trust Netw...	VeriSign Trust Network	8/1/2028	VeriSign Class 3 ...
VeriSign Trust Netw...	VeriSign Trust Network	5/18/2018	VeriSign Class 4 ...
VeriSign Trust Netw...	VeriSign Trust Network	8/1/2028	VeriSign Class 1 ...
VeriSign Trust Netw...	VeriSign Trust Network	8/1/2028	VeriSign Class 4 ...
VeriSign Trust Netw...	VeriSign Trust Network	5/18/2018	VeriSign Class 1 ...
Xcert EZ by DST	Xcert EZ by DST	7/11/2009	Xcert EZ by DST

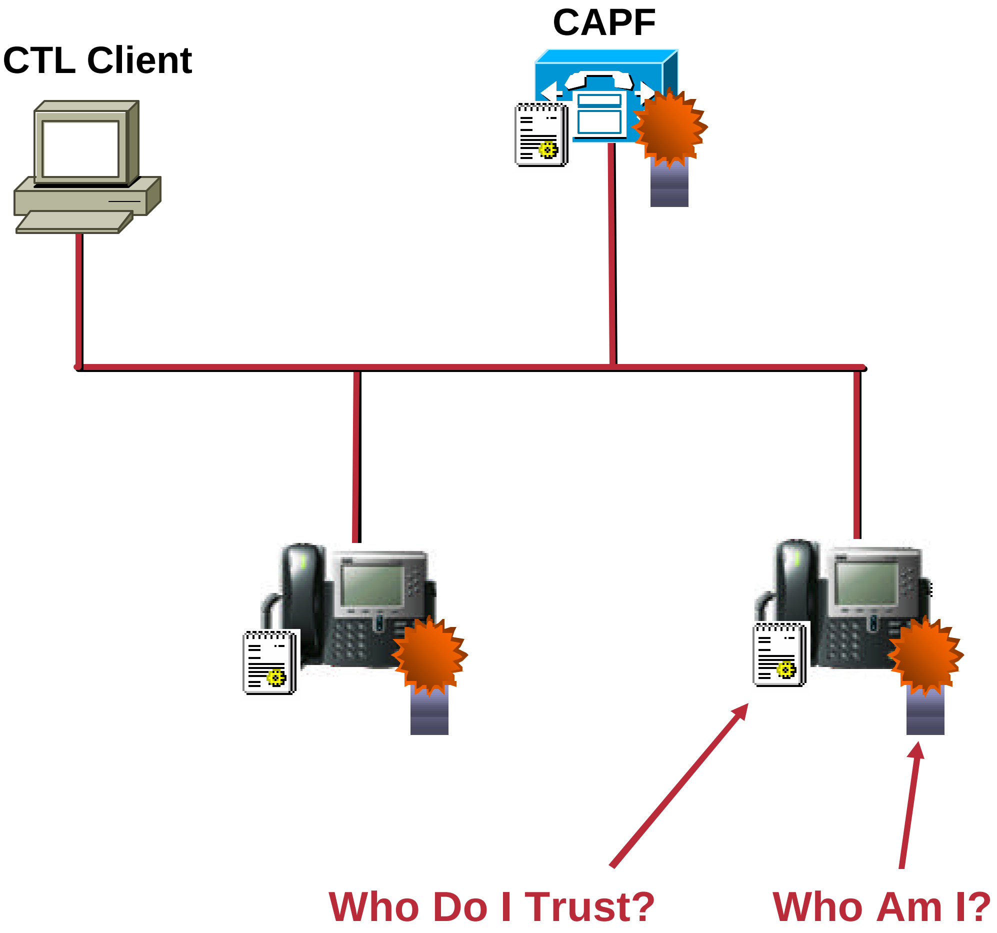
© 1992-2004 Cisco Systems, Inc. All rights reserved. Terms and Conditions, Privacy Statement, Cookie Policy and Trademarks of Cisco Systems, Inc.

Certificate Trust List

- Certificate Trust List contains list of trusted devices
- Similar to Trusted Root CAs in IE
- 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

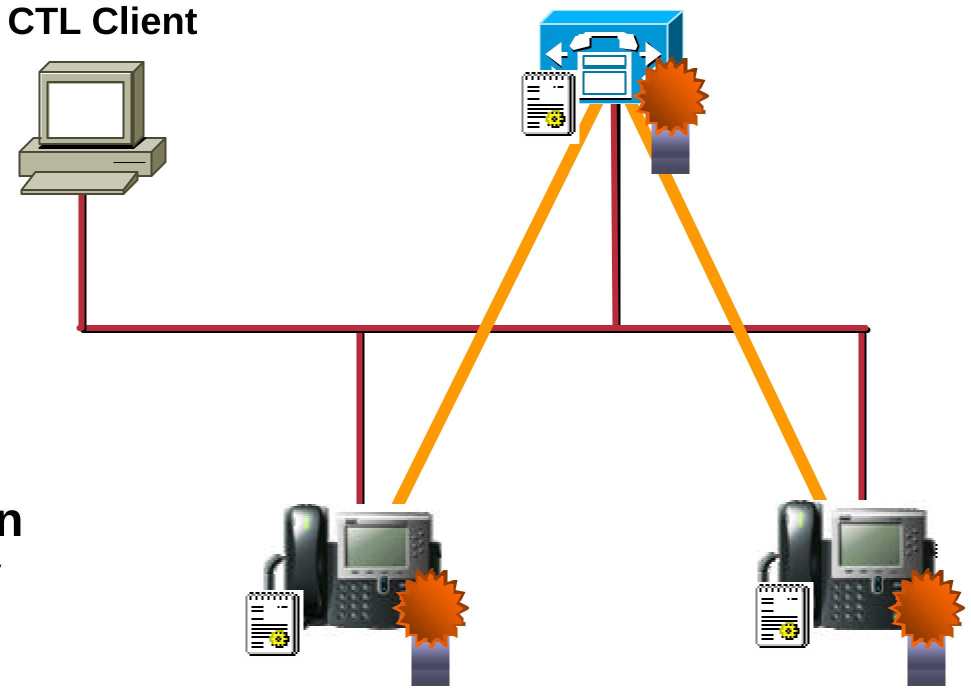
  Contained in OpenSSL database



TLS: Transport Layer Security

Cisco Uses TLS for Secure Signaling Between CCM and IP Phones

- Bidirectional exchange of certificates for mutual authentication
- RSA signatures
- HMAC-SHA-1 authentication tags insure packet integrity
- AES-128-CBC encryption protects session keys, DTMF tones and other data*

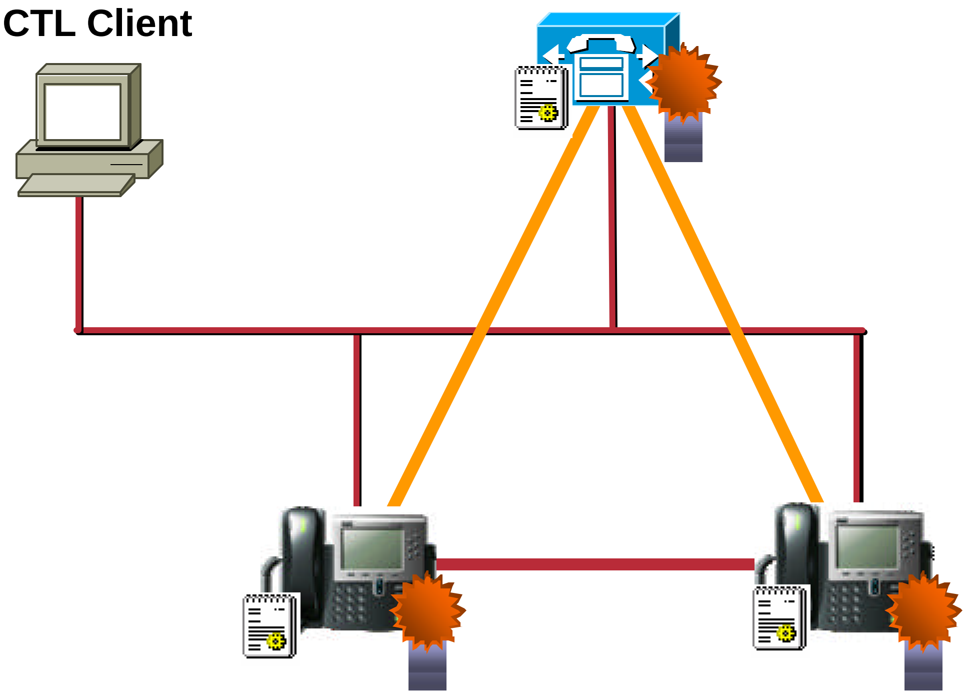


TLS Has a 20–25% Hit on Cisco CallManager Performance

* 7970 Only at This Time

SRTP: Secure RTP

- SRTP is the transport for authenticated and encrypted media
- IETF RFC3711
- Uses HMAC-SHA-1 for authentication and AES-128-CM for encryption
- Keys derived in CCM—sent to phones over TLS
- Currently only supported on 7970
- Over time, SRTP will role out to a broad range of phones, gateways and applications



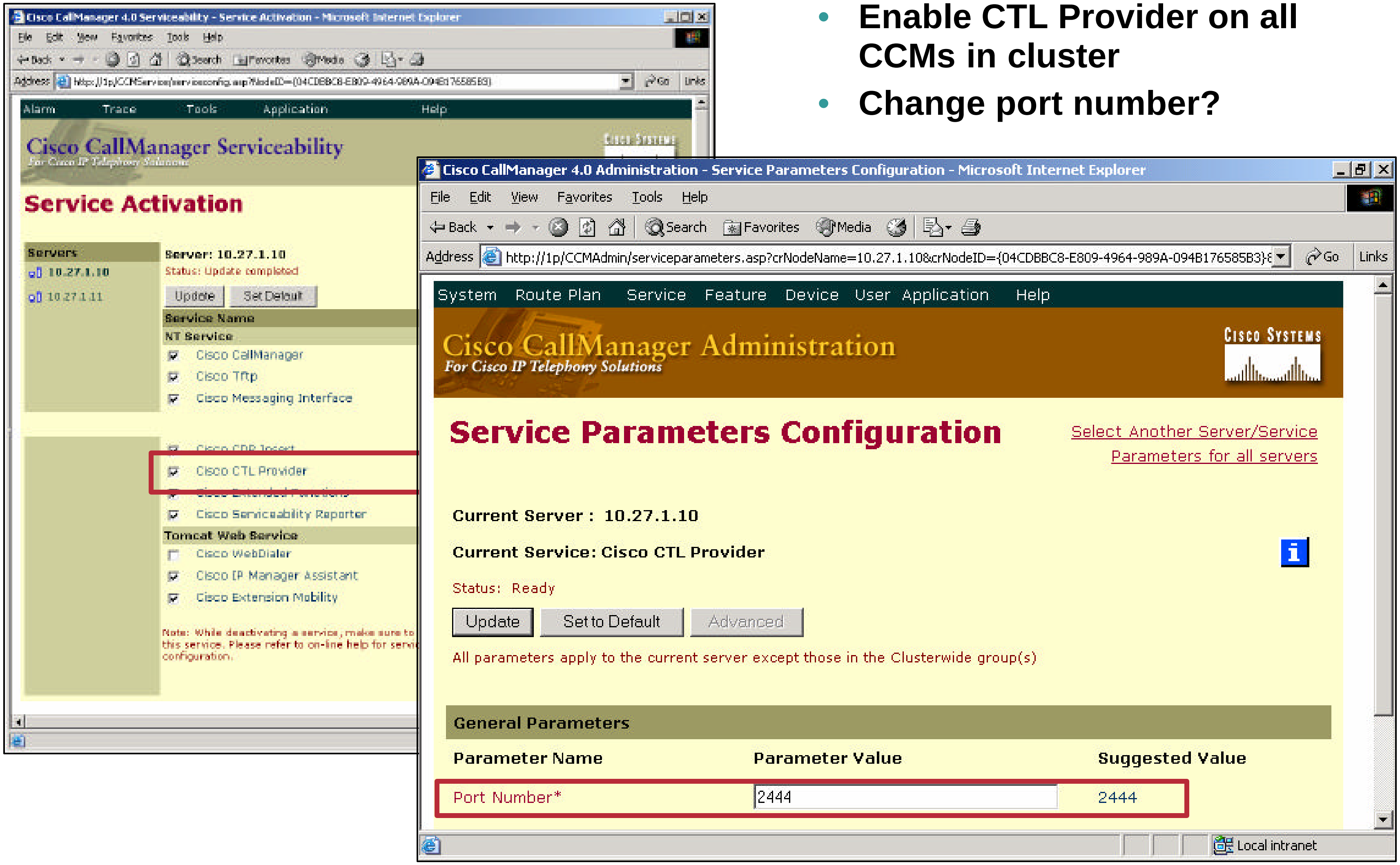
SRTP Packets Add 15 Microseconds to Latency and Are 4–7 Bytes Bigger than RTP Packets

CONFIGURING CISCO IPT

AUTHENTICATION AND ENCRYPTION

CISCO CALLMANAGER 4.0

Step 1:
Activate CTL Provider in Service Activation



Cisco CallManager 4.0 Serviceability - Service Activation - Microsoft Internet Explorer

Address: http://1p/CCMService/serviceconfig.asp?NodeID={04CDBBC8-E809-4964-989A-094B176585B3}

File Edit View Favorites Tools Help
Back Search Favorites Media
Go Links
Alarm Trace Tools Application Help
Cisco CallManager Serviceability
For Cisco IP Telephony Solutions
Cisco Systems

Service Activation

Servers
- 10.27.1.10
- 10.27.1.11

Server: 10.27.1.10

Status: Update completed

Service Name

NT Service
- ☑ Cisco CallManager
- ☑ Cisco Tftp
- ☑ Cisco Messaging Interface
- ☑ Cisco CDR Insert
- ☑ Cisco CTL Provider
- ☑ Cisco Extended Functions
- ☑ Cisco Serviceability Reporter

Tomcat Web Service
- □ Cisco WebDialer
- ☑ Cisco IP Manager Assistant
- ☑ Cisco Extension Mobility

Note: While deactivating a service, make sure to this service. Please refer to on-line help for servi configuration.

Cisco CallManager 4.0 Administration - Service Parameters Configuration - Microsoft Internet Explorer

Address: http://1p/CCMAdmin/serviceparameters.asp?crNodeName=10.27.1.10&crNodeID={04CDBBC8-E809-4964-989A-094B176585B3}&

File Edit View Favorites Tools Help
Back Search Favorites Media
Go Links
System Route Plan Service Feature Device User Application Help
Cisco CallManager Administration
For Cisco IP Telephony Solutions
Cisco Systems

Service Parameters Configuration

Select Another Server/Service
Parameters for all servers

Current Server : 10.27.1.10

Current Service: Cisco CTL Provider

Status: Ready

All parameters apply to the current server except those in the Clusterwide group(s)

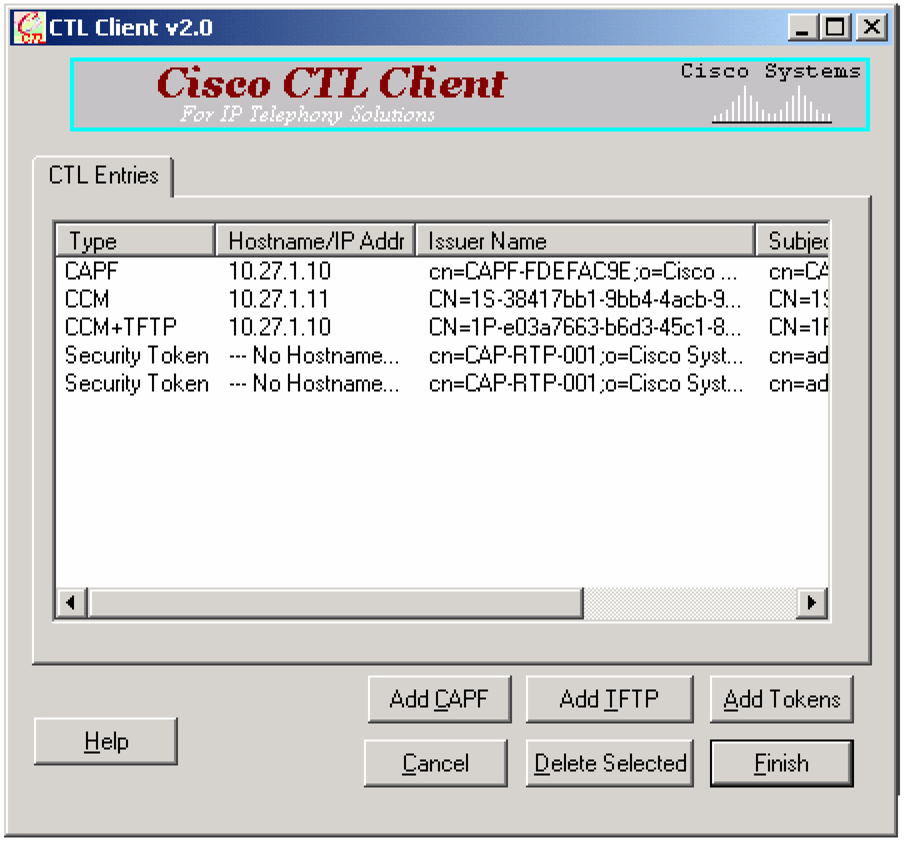
General Parameters

Parameter Name	Parameter Value	Suggested Value
Port Number*	2444	2444

- Enable CTL Provider on all CCMs in cluster
- Change port number?

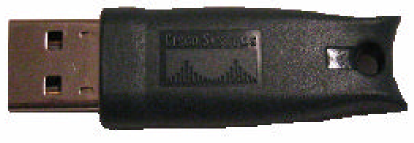
Step 2:
Install CTL Client on Windows Workstation

- Windows application
  - Smart Card Services must be running on target machine *
  - Download from CCM Plug-ins
  - Runs on admin workstation—Win-2K or greater
- Requires 2+ USB eTokens
  - 2 eTokens first time
  - 1 eToken thereafter
- Sets Cluster Security Mode
- Creates ctlfile.tlv
  - Uploaded to all CCMs defined in CTL Client
  - Downloaded to phones by TFTP

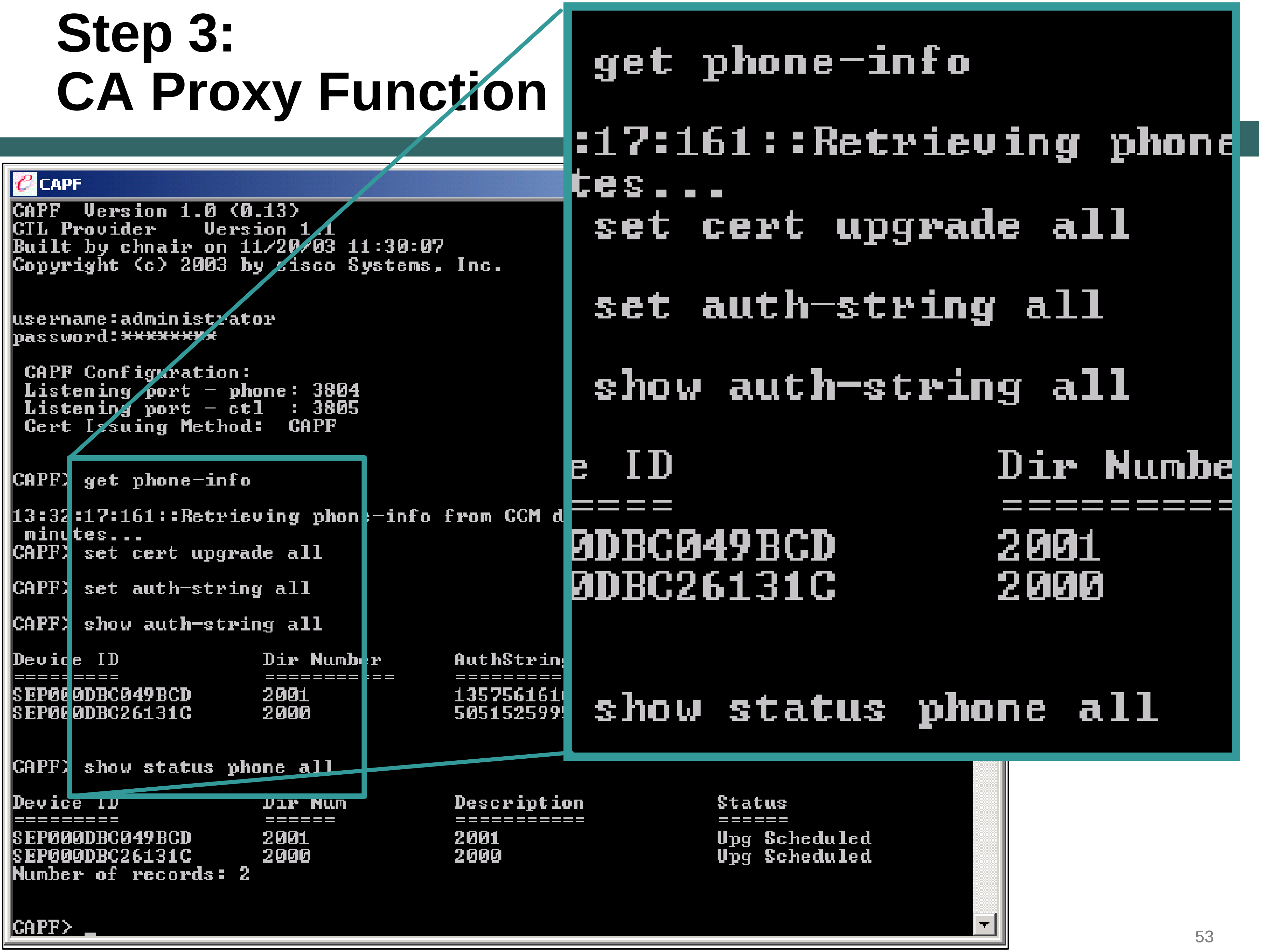


Type	Hostname/IP Addr	Issuer Name	Subjec
CAPF	10.27.1.10	cn=CAPF-FDEFAC9E;o=Cisco ...	cn=CA
CCM	10.27.1.11	CN=1S-38417bb1-9bb4-4acb-9...	CN=1
CCM+TFTP	10.27.1.10	CN=1P-e03a7663-b6d3-45c1-8...	CN=1
Security Token	--- No Hostname...	cn=CAP-RTP-001;o=Cisco Syst...	cn=ad
Security Token	--- No Hostname...	cn=CAP-RTP-001;o=Cisco Syst...	cn=ad

***Enable Smart Card Services**
Start > Programs > Administrative Tools > Services
Right Click Smart Card, choose Properties
Automatic > Apply, Start > OK



Step 3:
CA Proxy Function



```
CAPF  Version 1.0 (0.13)
CTL Provider    Version 1.1
Built by chnair on 11/20/03 11:30:07
Copyright (c) 2003 by Cisco Systems, Inc.


username:administrator
password:*********

 CAPF Configuration:
 Listening port - phone: 3804
 Listening port - ctl  : 3805
 Cert Issuing Method:  CAPF


CAPF> get phone-info

13:32:17:161::Retrieving phone-info from CCM d
 minutes...
CAPF> set cert upgrade all

CAPF> set auth-string all

CAPF> show auth-string all

Device ID            Dir Number      AuthStrin
=========            ===========     =========
SEP000DBC049BCD      2001            135756161
SEP000DBC26131C      2000            505152599


CAPF> show status phone all

Device ID            Dir Num         Description       Status
=========            =======         ===========       ======
SEP000DBC049BCD      2001            2001              Upg Scheduled
SEP000DBC26131C      2000            2000              Upg Scheduled
Number of records: 2


CAPF> _
```

```
get phone-info

:17:161::Retrieving phone
tes...
 set cert upgrade all

 set auth-string all

 show auth-string all

e ID              Dir Numbe
====              ==========
0DBC049BCD        2001
0DBC26131C        2000


 show status phone all
```

Pending Improvements to CAPF

Yep, It’s Ugly!!! Next Up

- GUI-based
  - Moved to CCM admin pages
  - BAT supported
- Three modes of authentication
  - Auth string—just like today
  - Existing MIC or LSC
  - Null push, with appropriate warning

Step 4:
Set the Cluster-Wide Security Mode

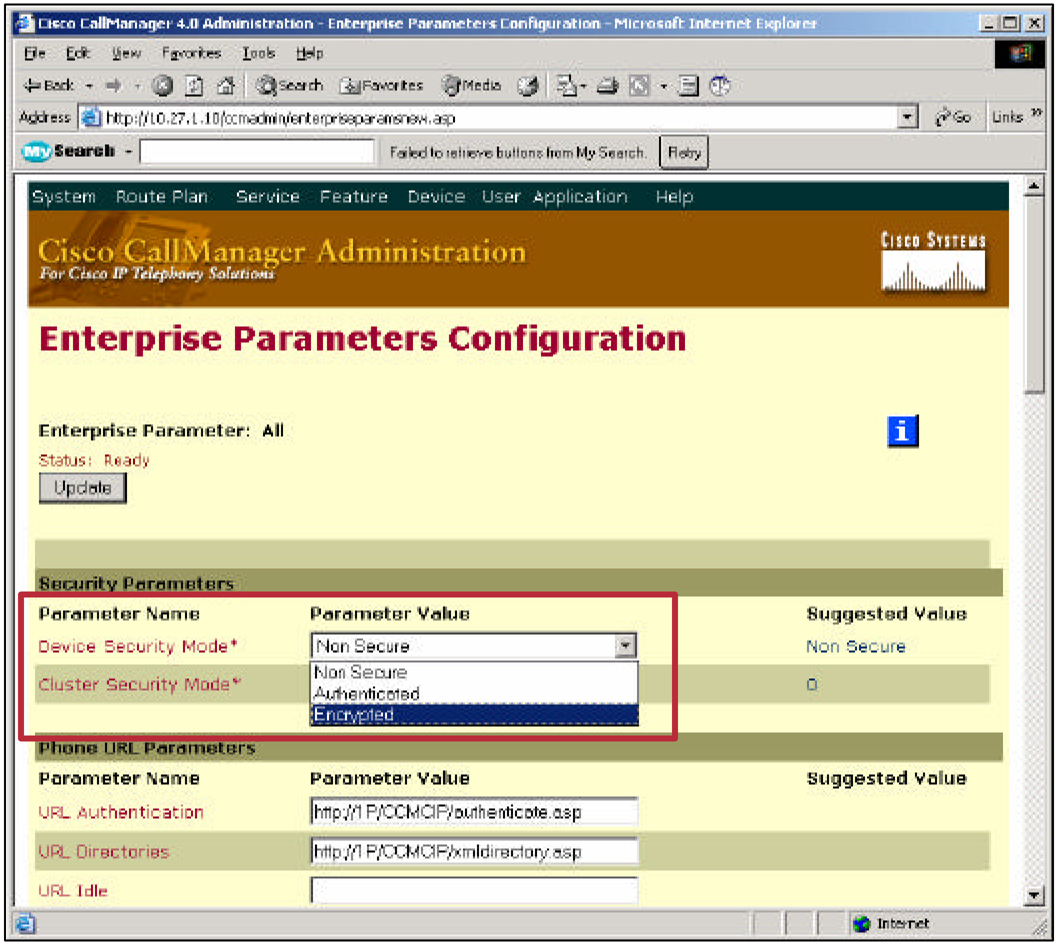
- **Sets the security mode for EVERY endpoint in the network:**

  Non-Secure

  Authenticated

  Encrypted

- **Each device will use it's highest capability**


Cisco CallManager 4.0 Administration - Enterprise Parameters Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.27.1.10/ccmadmin/enterpriseparamsnew.asp
Go Links
My Search
Failed to retrieve buttons from My Search.
Retry
System Route Plan Service Feature Device User Application Help
Cisco CallManager Administration
For Cisco IP Telephony Solutions
Cisco Systems
Internet

Enterprise Parameters Configuration

Enterprise Parameter: All

Status: Ready

Update

Security Parameters

Parameter Name	Parameter Value	Suggested Value
Device Security Mode*	Non Secure Non Secure Authenticated Encrypted	Non Secure
Cluster Security Mode*		0

Phone URL Parameters

Parameter Name	Parameter Value	Suggested Value
URL Authentication	http://1 P/CCMCIP/authenticate.asp	
URL Directories	http://1 P/CCMCIP/xmldirectory.asp	
URL Idle		

(Picture Abridged)

Step 4:
OR, Set Security Setting on Phone

- **On the phone configuration page, set it to**

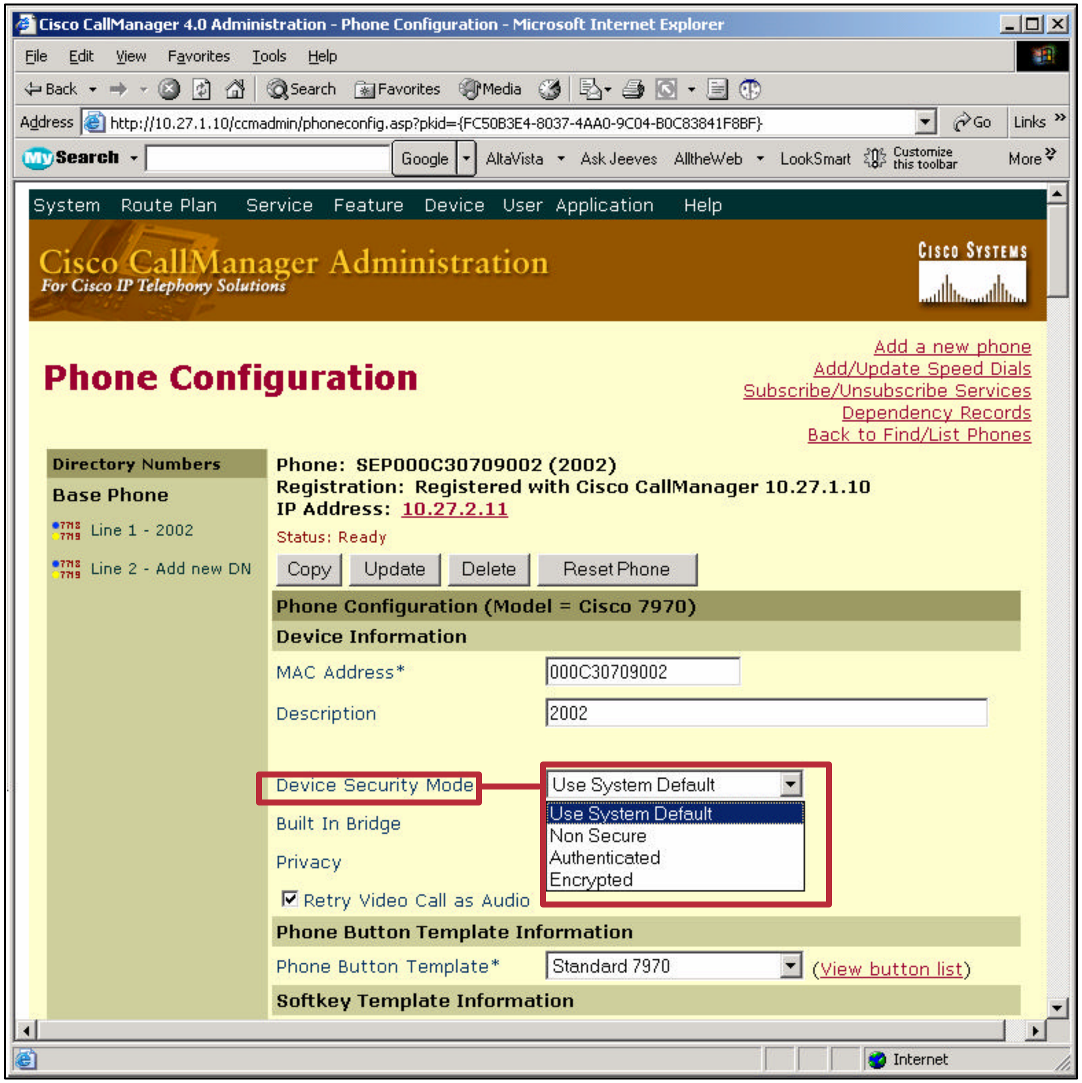
  Use System Default

  Non-Secure

  Authenticated

  Encrypted

- **Note: 7940 and 7960 do not list Encrypted as an option**


Cisco CallManager 4.0 Administration - Phone Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.27.1.10/ccmadmin/phoneconfig.asp?pkid={FC50B3E4-8037-4AA0-9C04-B0C83841F8BF}
Go Links
My Search Google AltaVista Ask Jeeves AlltheWeb LookSmart Customize this toolbar More
System Route Plan Service Feature Device User Application Help
Cisco CallManager Administration
For Cisco IP Telephony Solutions
Cisco Systems
Add a new phone
Add/Update Speed Dials
Subscribe/Unsubscribe Services
Dependency Records
Back to Find/List Phones
Directory Numbers
Base Phone
Line 1 - 2002
Line 2 - Add new DN
Copy
Update
Delete
Reset Phone
Internet

Phone Configuration

Phone: SEP000C30709002 (2002)
Registration: Registered with Cisco CallManager 10.27.1.10
IP Address: 10.27.2.11
Status: Ready

Phone Configuration (Model = Cisco 7970)

Device Information

MAC Address* 000C30709002

Description 2002

Device Security Mode Use System Default

- Use System Default
- Non Secure
- Authenticated
- Encrypted

Built In Bridge

Privacy

☑ Retry Video Call as Audio

Phone Button Template Information

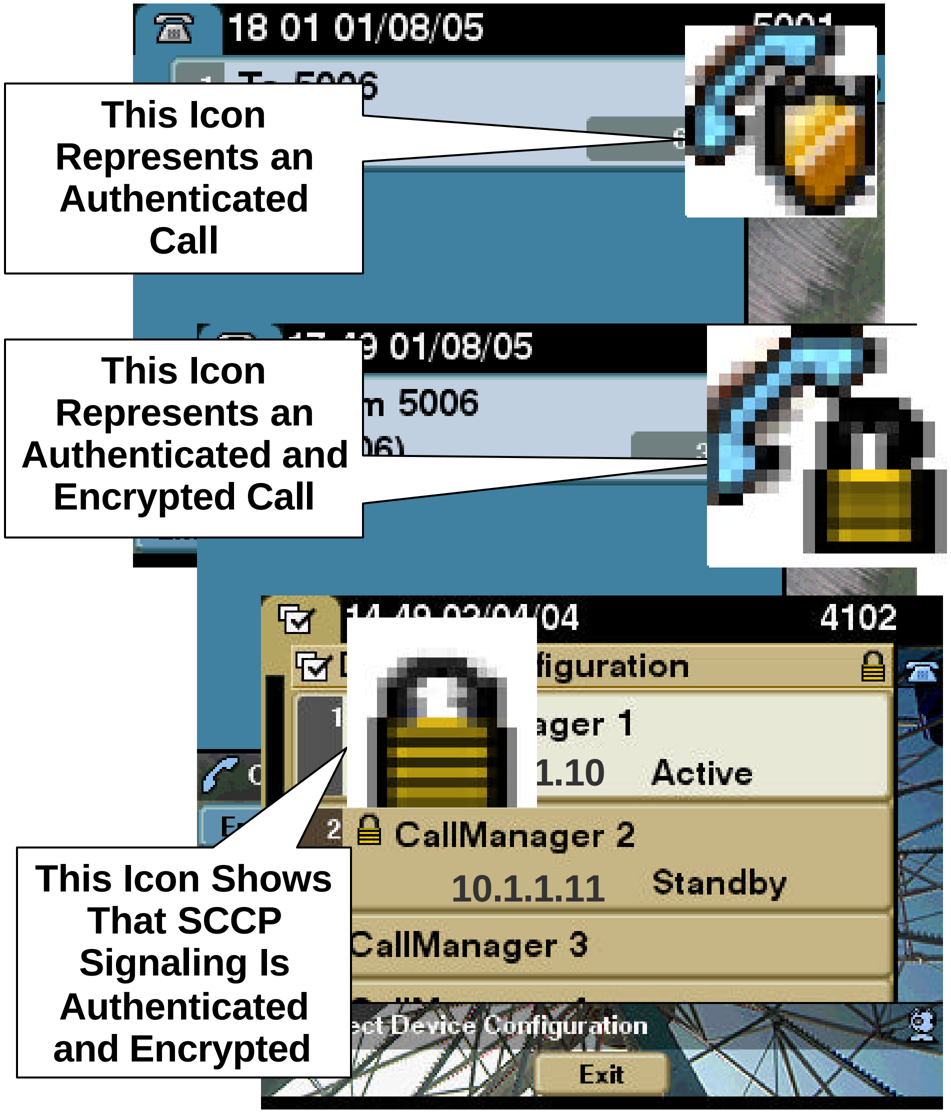
Phone Button Template* Standard 7970 (View button list)

Softkey Template Information

(Picture Abridged)

Authentication and Encryption Summary

- “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



This Icon Represents an Authenticated Call

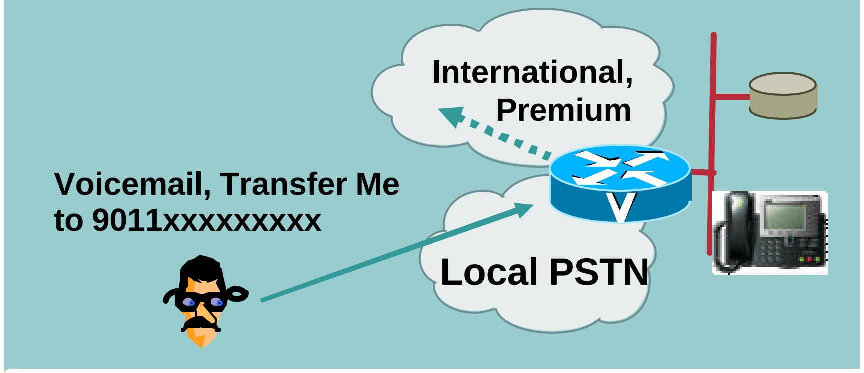
This Icon Represents an Authenticated and Encrypted Call

This Icon Shows That SCCP Signaling Is Authenticated and Encrypted

CISCO CALLMANAGER TOLL FRAUD PREVENTION

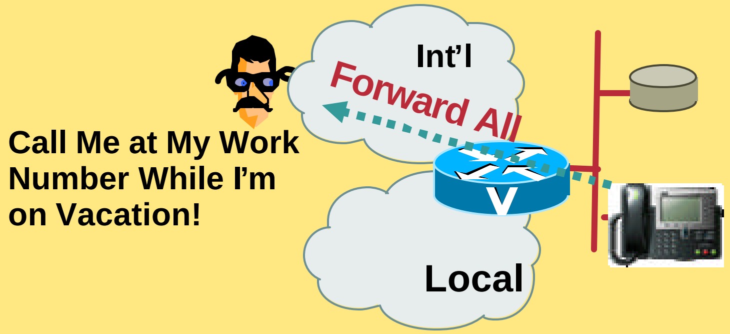
Exploits of Toll Fraud

Toll Fraud 1: Transfer from Voicemail



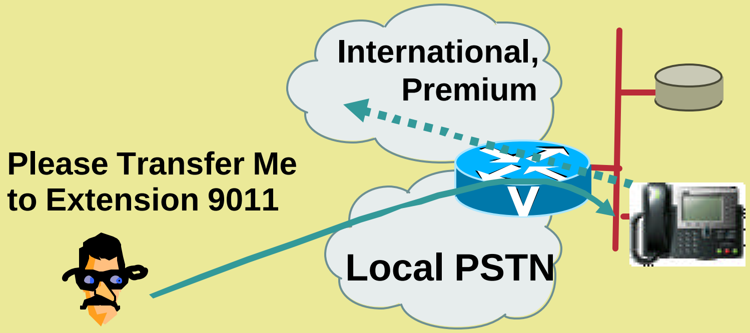
Voicemail, Transfer Me to 9011xxxxxxxxx

Toll Fraud 2: Call Forward All



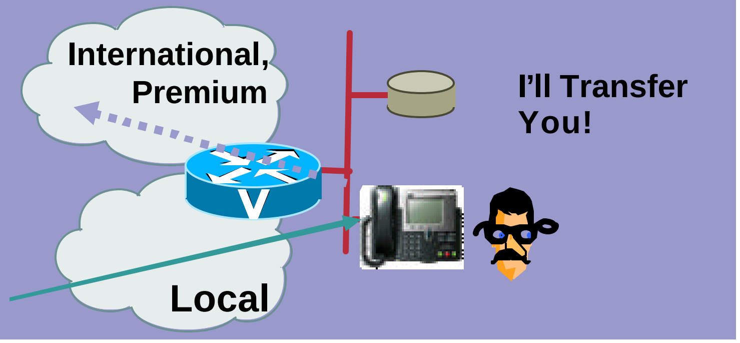
Call Me at My Work Number While I'm on Vacation!

Toll Fraud 3: Social Engineering



Please Transfer Me to Extension 9011

Toll Fraud 4: Inside Facilitators



I'll Transfer You!

Prevent Authenticated User Toll Fraud

- Exploits of Call Forward All:

  Forward work phone to home phone, have relatives call toll-free number for office, transferred to home

  Forward work phone to hotel in foreign country while on vacation; have friends from home call for free!

  Need to make an international call from home? Use the web to forward your work phone to desired number, then call your work phone

  Forward All CSS stops these exploits

- Exploits of Voicemail (similar to Call Forward All)

  Restricted CSS on VM ports block these

Prevent External Transfer

- **Prevents users from transferring 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)

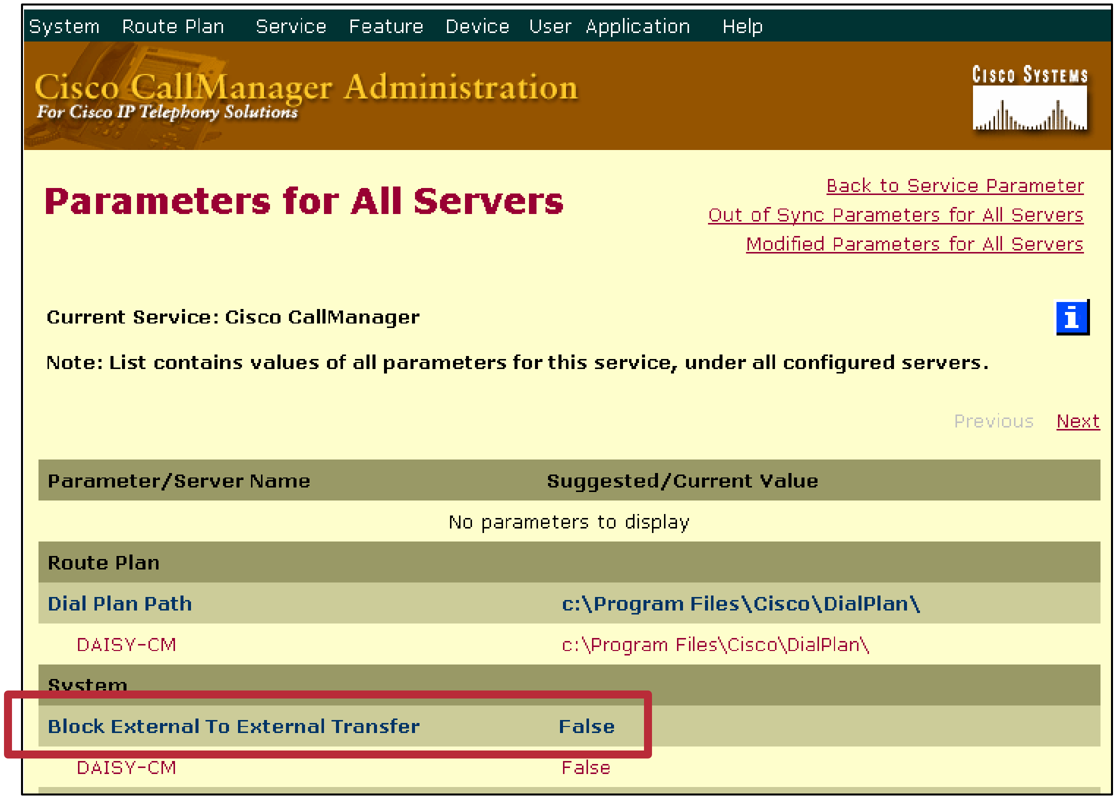
- **External devices:**

  H323 Gateway device

  MGCP FXO trunk

  MGCP T1/E1 trunk

  Inter-cluster trunk



Parameters for All Servers

Back to Service Parameter
Out of Sync Parameters for All Servers
Modified Parameters for All Servers

Current Service: Cisco CallManager

Note: List contains values of all parameters for this service, under all configured servers.

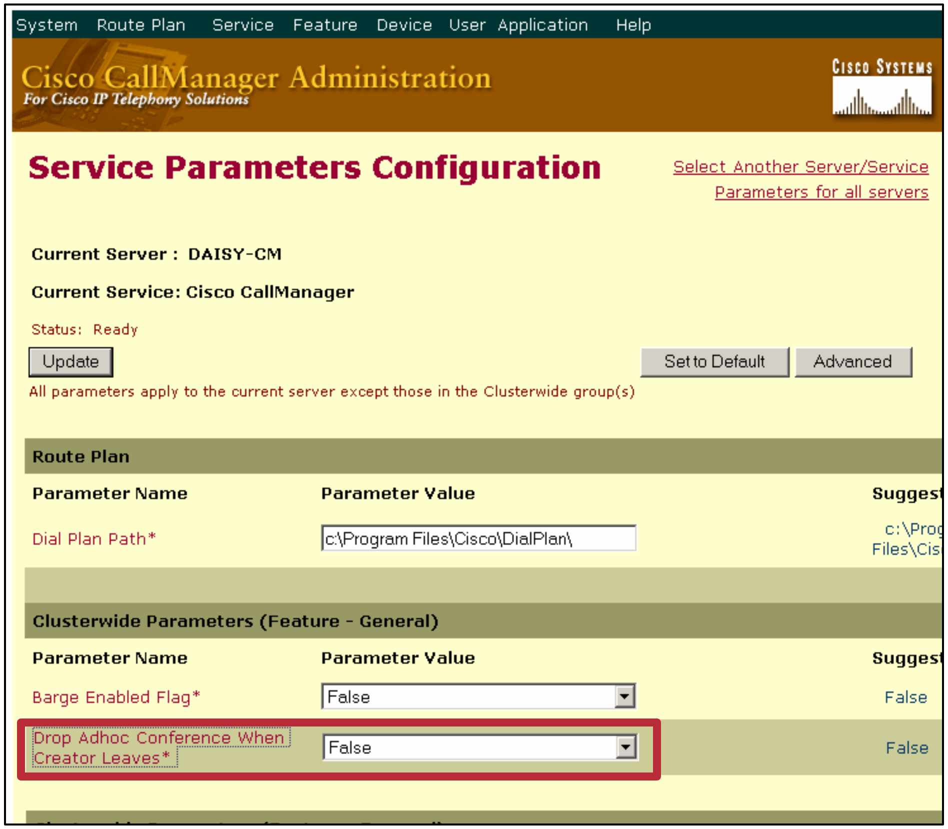
Previous Next

Parameter/Server Name	Suggested/Current Value
No parameters to display	
Route Plan	
Dial Plan Path	c:\Program Files\Cisco\DialPlan\
DAISY-CM	c:\Program Files\Cisco\DialPlan\
System	
Block External To External Transfer	False
DAISY-CM	False

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



Service Parameters Configuration

Select Another Server/Service
Parameters for all servers

Current Server : DAISY-CM

Current Service: Cisco CallManager

Status: Ready

All parameters apply to the current server except those in the Clusterwide group(s)

Route Plan

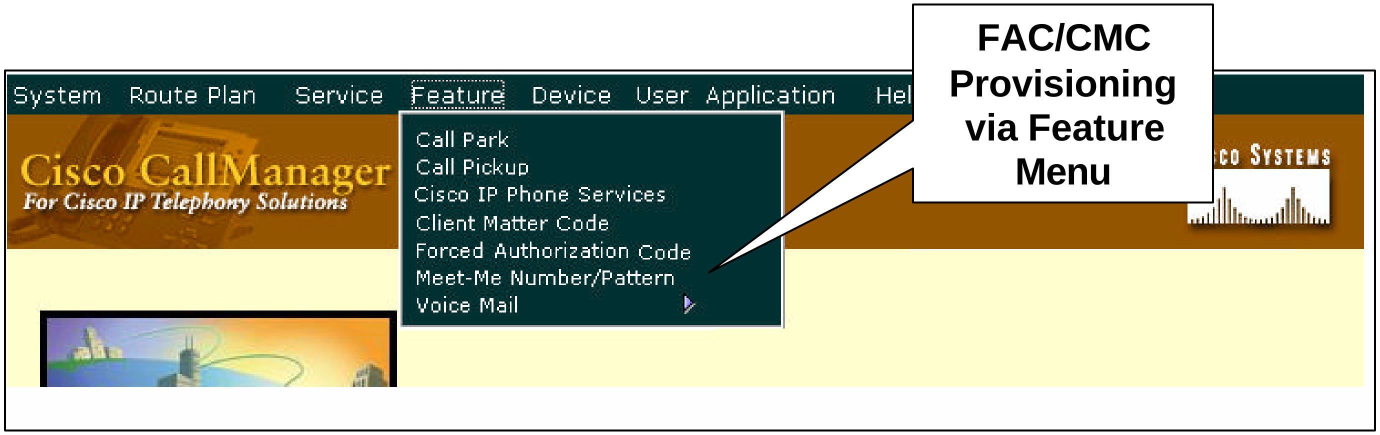
Parameter Name	Parameter Value	Suggest
Dial Plan Path*	c:\Program Files\Cisco\DialPlan\	c:\Prog Files\Cis

Clusterwide Parameters (Feature - General)

Parameter Name	Parameter Value	Suggest
Barge Enabled Flag*	False	False
Drop Adhoc Conference When Creator Leaves*	False	False

In CCM 3.3(4)

Forced Authorization Codes and Client Matter Codes



FAC/CMC Provisioning via Feature Menu

- 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

Cisco.com

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

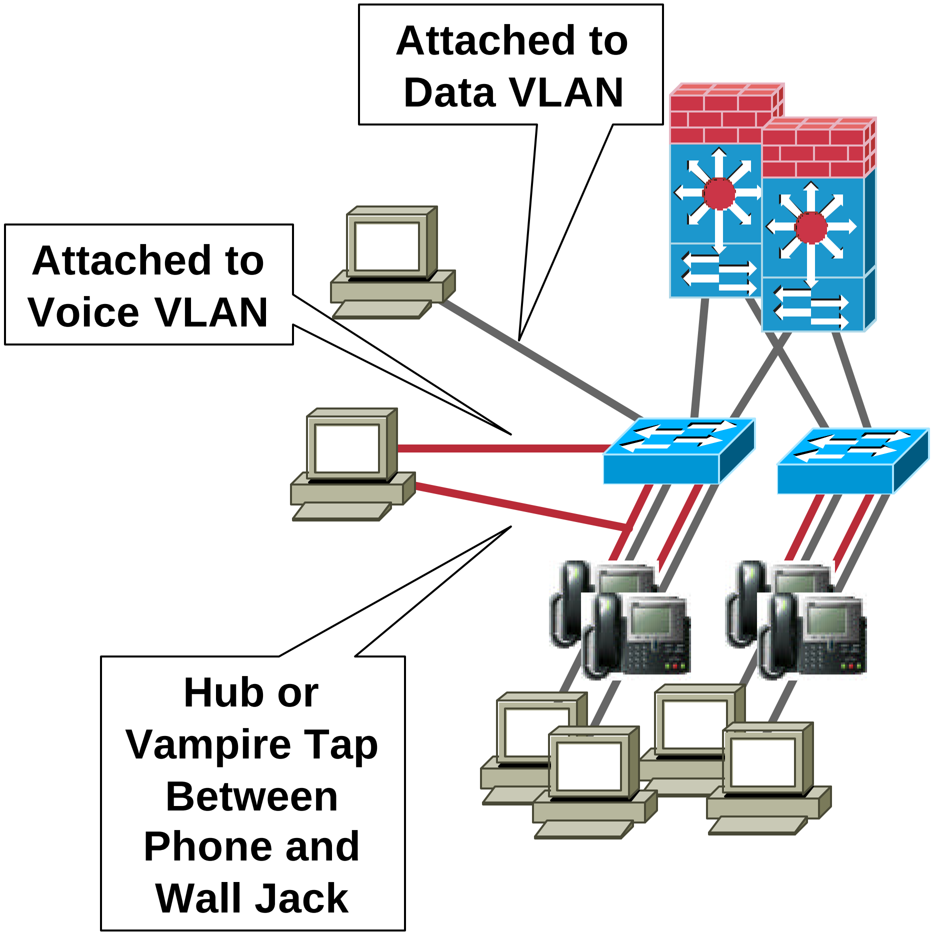
Research the problem for your particular area

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 and Nevis	869	9.1869xxxxxxx
St. Lucia	758	9.1758xxxxxxx
St. Vincent and the Grenadines	784	9.1784xxxxxxx
Toll Charge	900 976	9.1900xxxxxxx 9.1976xxxxxxx
Trinidad and Tobago	868	9.1868xxxxxxx
Turks and Caicos Is	649	9.1649xxxxxxx
U.S. Virgin Islands	340	9.1242xxxxxxx

HOW DOES ALL OF THIS HELP?

Mitigating Attacks Against Endpoints

- Blocking PC access to voice VLAN stops eavesdropping attacks (VOMIT)
- DAI and Source Guard prevent man-in-the-middle attacks or traffic interception (ettercap, dsniff)
- VACLs stopped 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)



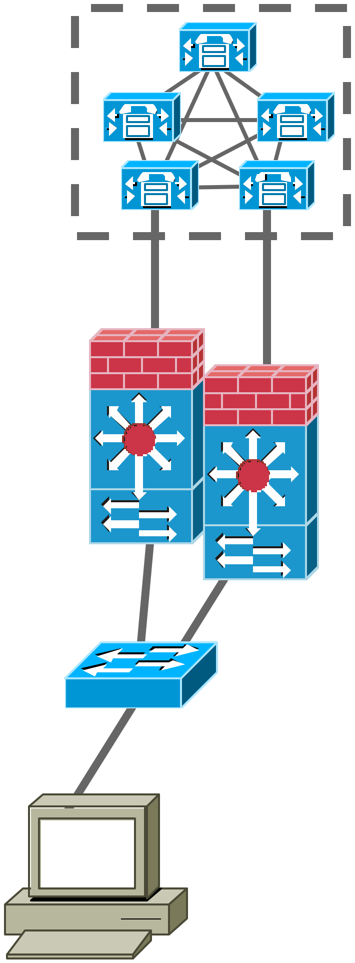
Attached to Data VLAN

Attached to Voice VLAN

Hub or Vampire Tap Between Phone and Wall Jack

Mitigating Attacks Against Servers

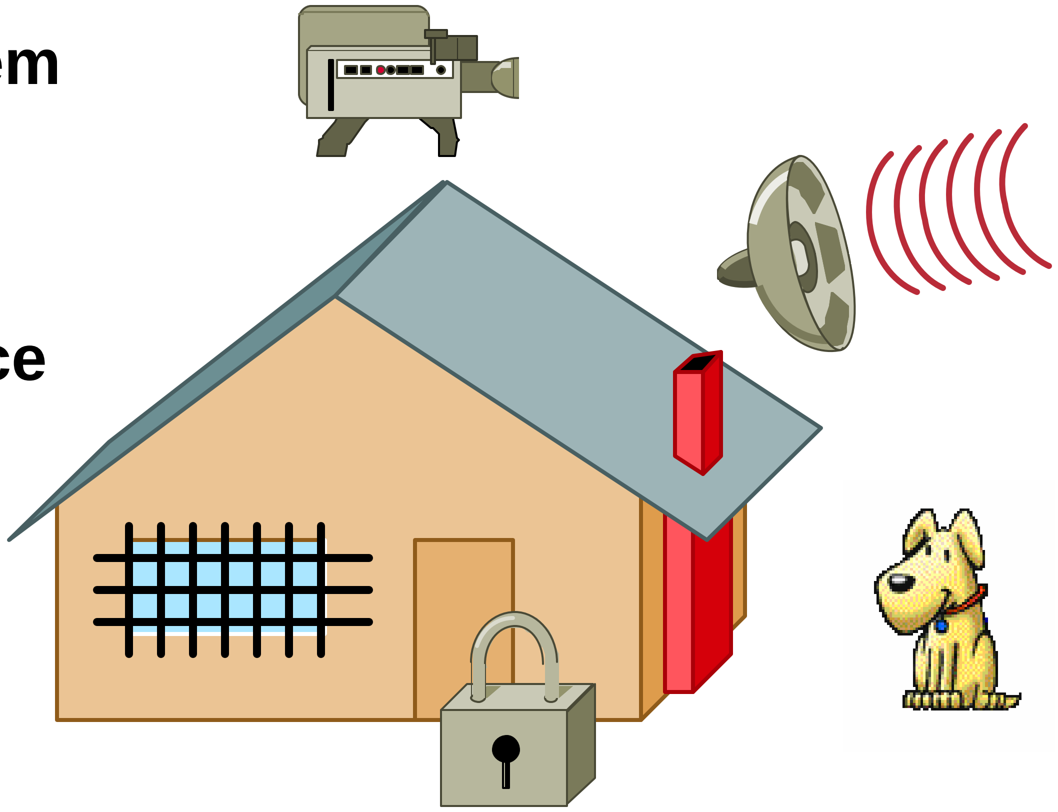
- **FW, ACL and VACL prevent targeted TCP and UDP attacks and port scans**
- **Authentication proxy limits access to vulnerable ports at L3**
- **Rate limiting prevents DoS and DDoS attacks on signaling ports to servers**
- **Common Windows exploits thwarted by hardened OS**
- **Targeted and anonymous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



How Do You Secure Your Home?

- Lock the doors
- Get a dog
- Install an alarm system
- Fortify with bars and gates
- Use video surveillance

It All Depends on Your Situation



How Do You Secure Your Voice Network?

	OPEN	BETTER	BEST
Isolate Servers	Open	ACLs	Firewalls and 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 and L1/L2 Toggles	Authentication and Encryption
Network Connectivity	Open	VACLs, Ignore GARP	DHCP Snooping, DAI, ISG
Forensic Information	Open	Syslog	NIDS/VMS/CWSIM

It All Depends on Your Situation

Complete Your Online Session Evaluation!

Por favor, complete el formulario de evaluación.

Muchas gracias.

Session ID: VVT-2003

**ENTERPRISE IP TELEPHONY
SECURITY PRACTICES AND TECHNOLOGIES**

Cisco Systems®