



# IPC Networking

Cisco Systems Korea

S.E ( [whchoi@cisco.com](mailto:whchoi@cisco.com) )

# IPC Network

...



**Smart, Simple, and  
Secure Communications**

1. Smart :

.

2. Simple :

.

3. Secure :

...

# IP Telephony



## IPT Server

IPT Server

IPT Server

가

## Infra

DDoS, Worm

Infra

## EndPoint

IPT  
IPT

# IPT End-Point



# Host Storm-Control

## Infra



50Mbps/1500Byte Traffic  
(4000 ~ 5000 PPS )

G.711  
64Kbps / 128byte Traffic  
(50~100PPS )

G.711 & Data  
(4000 ~ 5000 PPS )



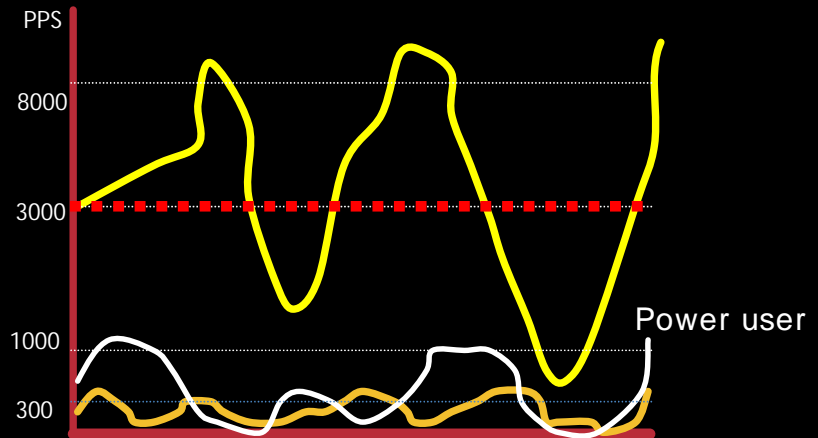
50Mbps/64Byte Traffic  
( 10,000 PPS )

G.711  
64Kbps / 128byte Traffic  
(50~100PPS )

G.711 & Data  
(10,000 PPS )

# Host Storm-Control

Infra



- Storm Control PPS Limit !!!

Storm Control PPS      Enable



Action : 800 PPS



SNMP Trap Log



Blocking



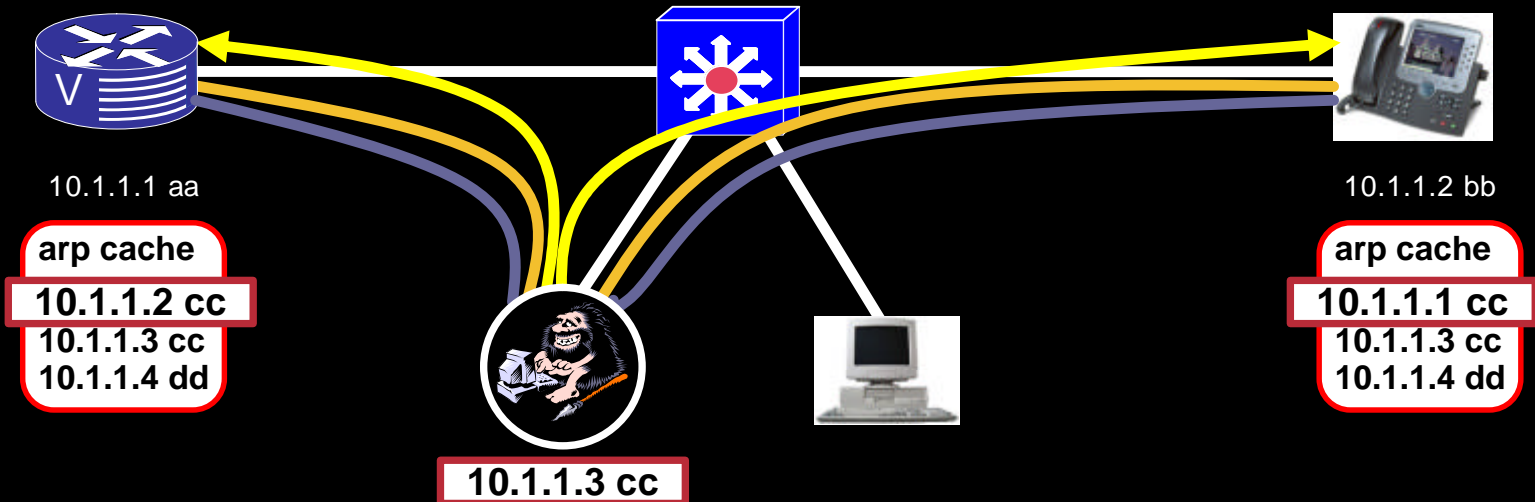
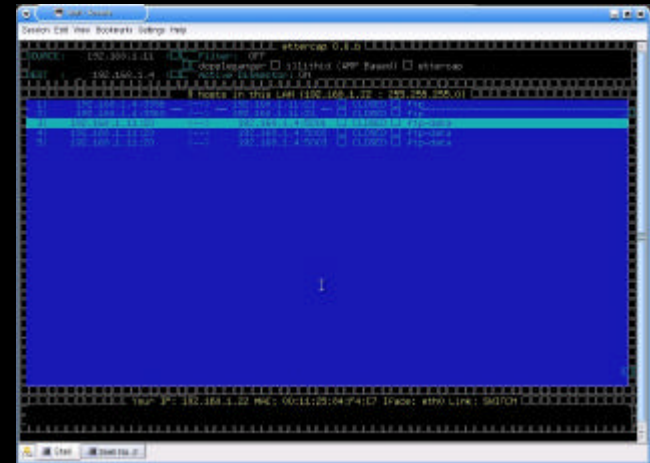
Shutdown

Forwarding

Enable

# IPT PC DHCP Snooping & DAI

- ❖ MITMA(Man In The Middle Attack)
  - Voice Call : Packet sniffing
- ❖ VOMIT(Voice Over Misconfig IP Telephony)
  - : TCP Dump WAV file
- ❖ MAC Flooding
  - MAC Address  
Infra 가



# IPT PC DHCP Snooping & DAI

## ❖ DHCP Snooping

- DHCP IP

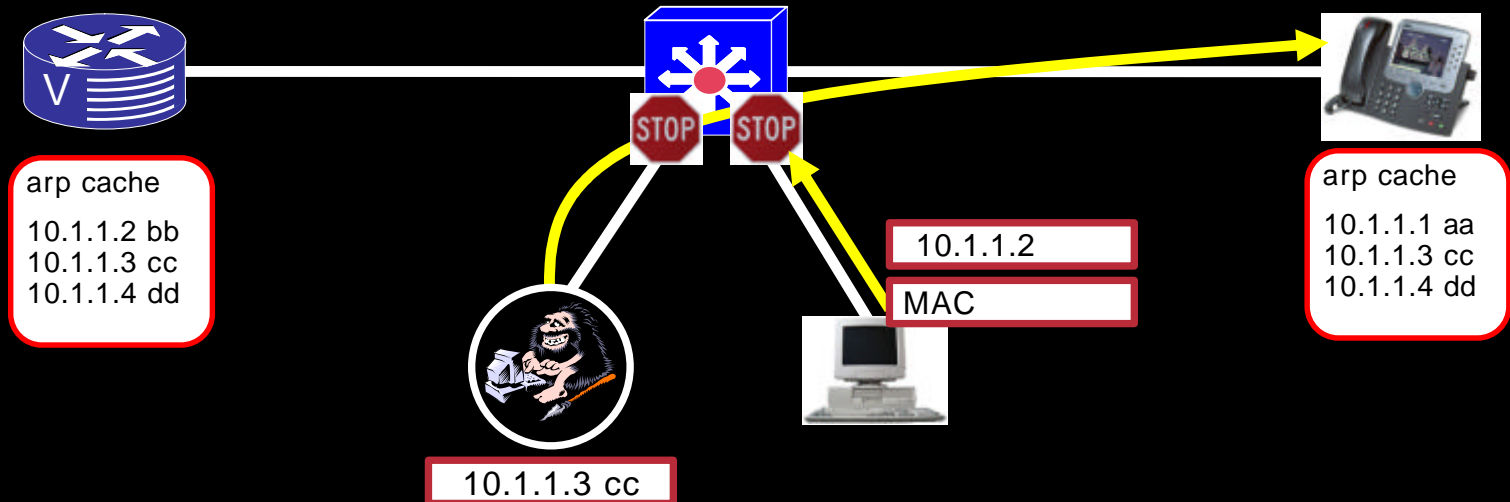
## ❖ ARP Inspection

- ARP Inspection

Voice Call 가 가 ( )

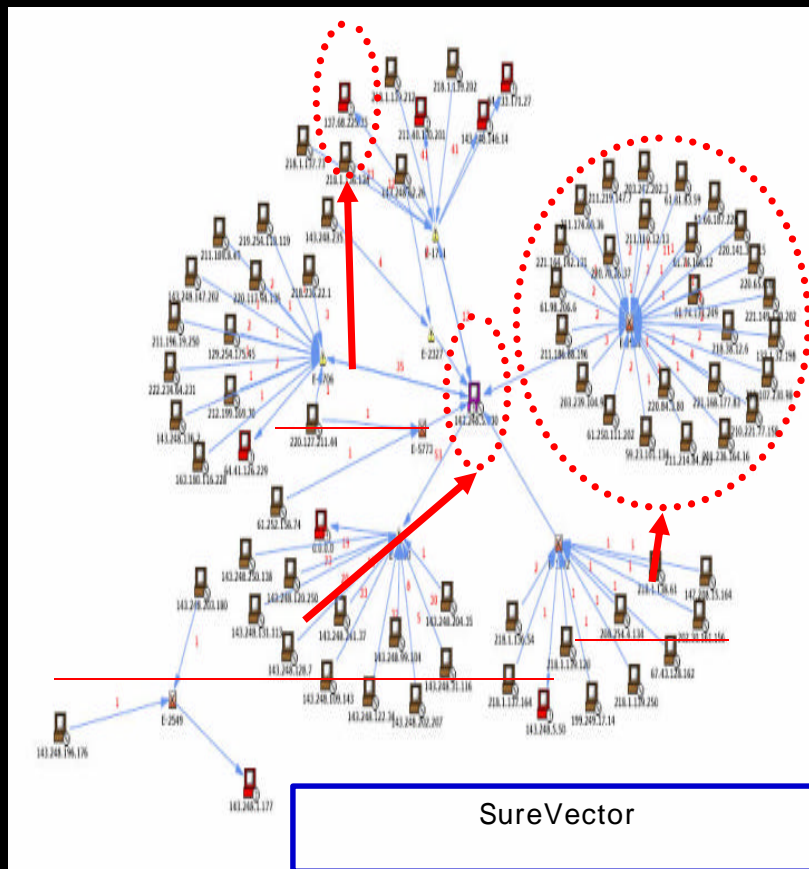
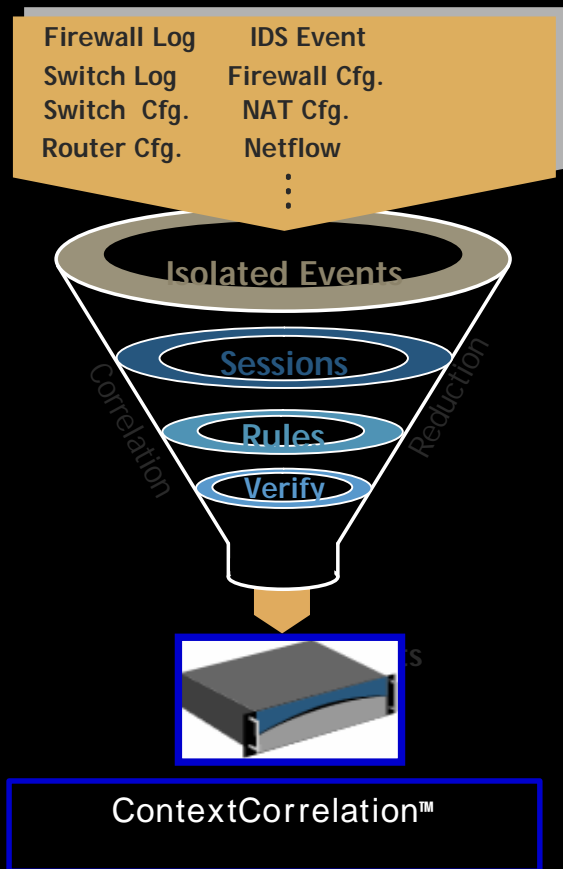
## ❖ Port Security

- MAC Address

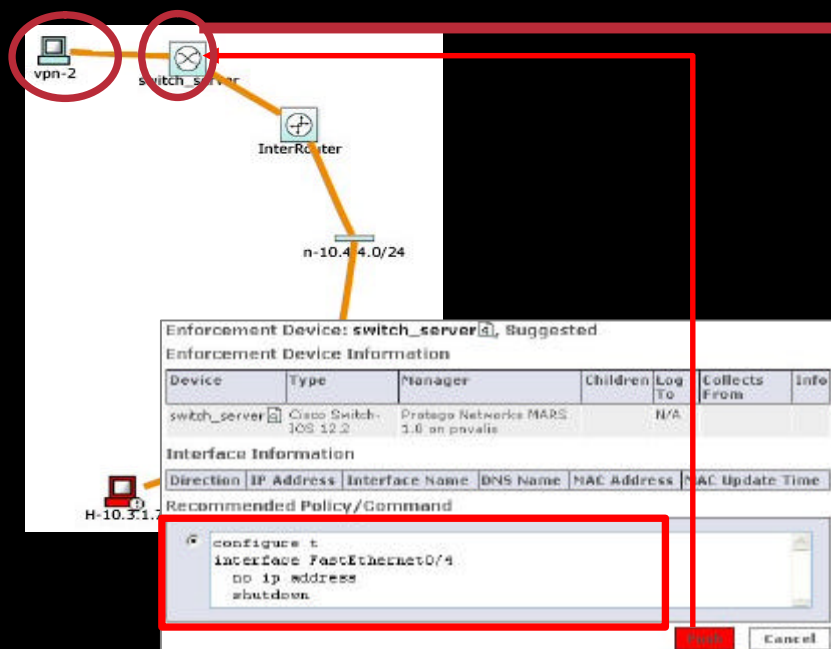




# CS-MARS + CCM



# CS-MARS + CCM



## Product Specific Configuration

Disable Speakerphone	<input type="checkbox"/>
Disable Speakerphone and Headset	<input type="checkbox"/>
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

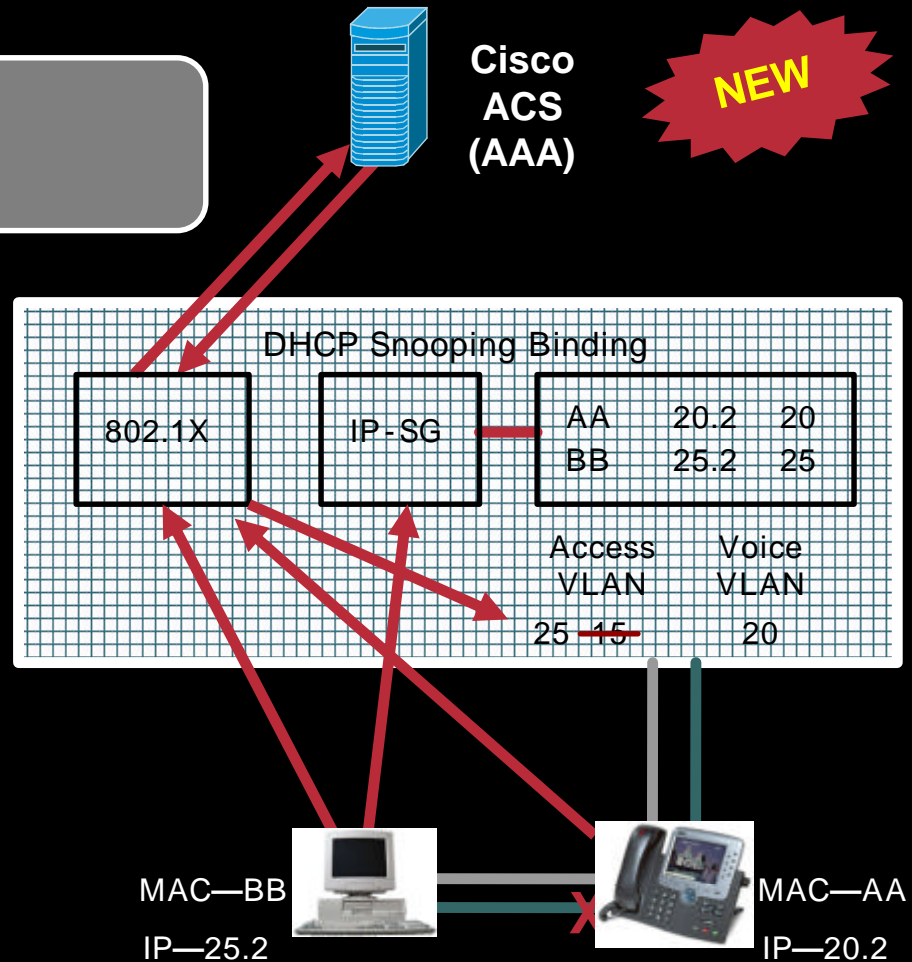
CCM  
CCM

Port Blocking  
PC Port

powered by cisco.  
**voicecomm**  
**2005**

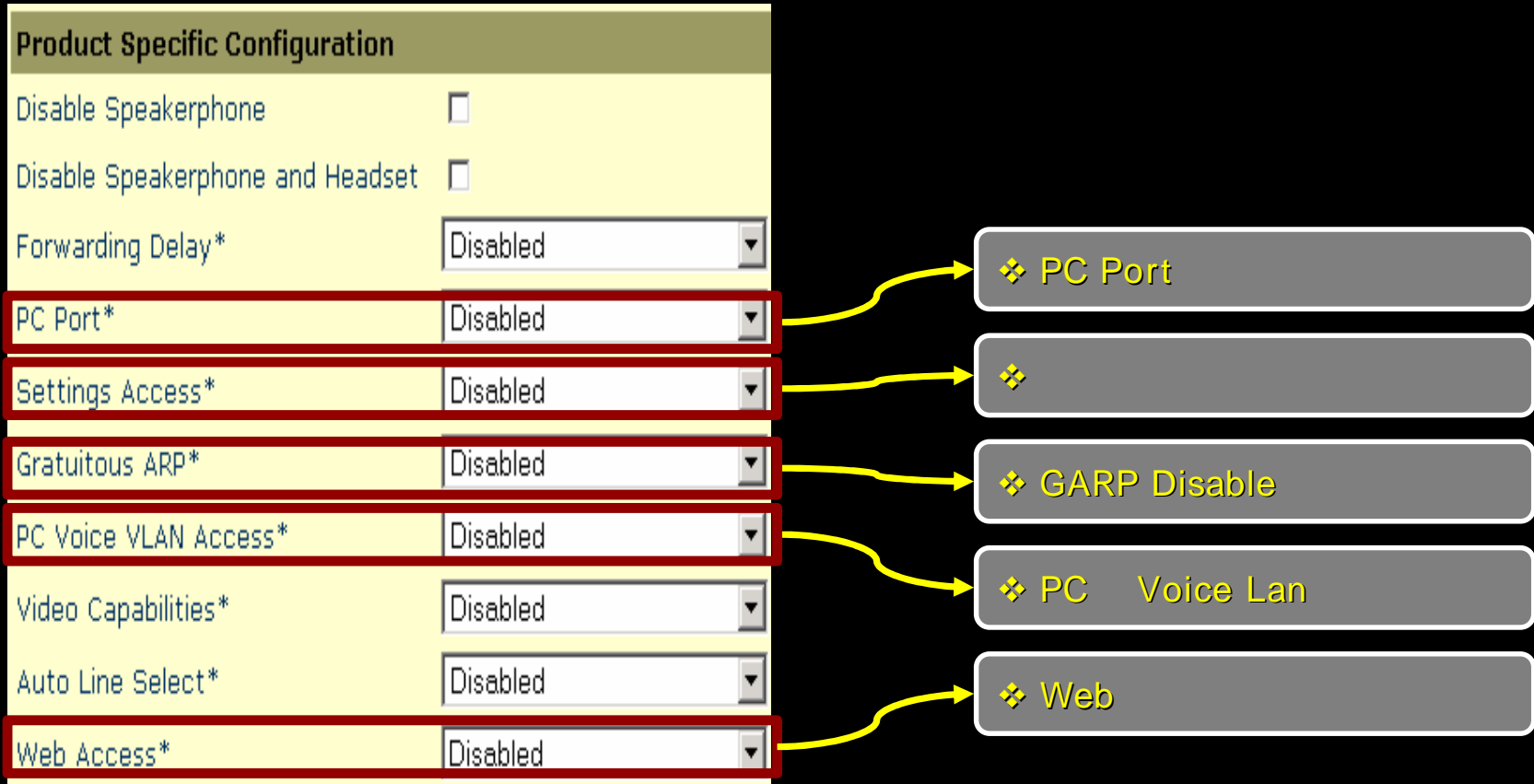
# Cisco ACS (AAA)

1. PC EAPOL - Logon—  
phone watche
2. AAA
3. Vlan ID
4. PC DHCP IP
5. DHCP snooping binding
6. IP-SG monitor
7. PC가 Voice Vlan
8. PC , phone EAPOL -  
Logoff



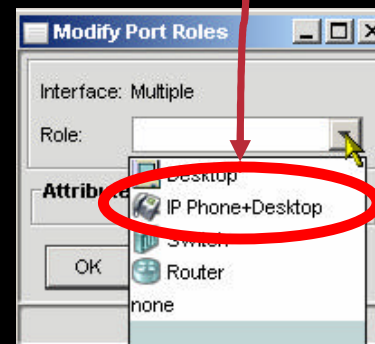
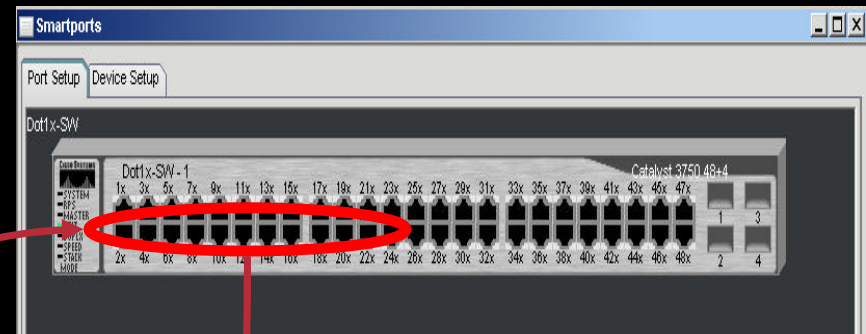
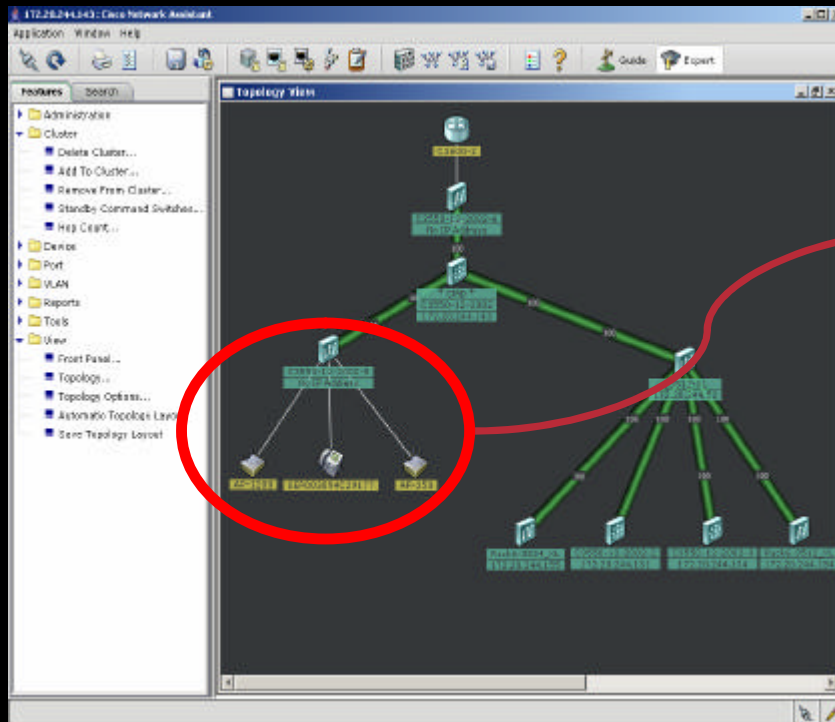
# IPT Phone Layer 1/2

## Feature



# CNA PC IPC

poweredbycisco.  
**voicecomm**  
**2005**



One-Click

# IPT Server



# Call Manager

-



Web

E-mail

App

File System  
Registry  
COM Object  
Web  
Memory  
Code

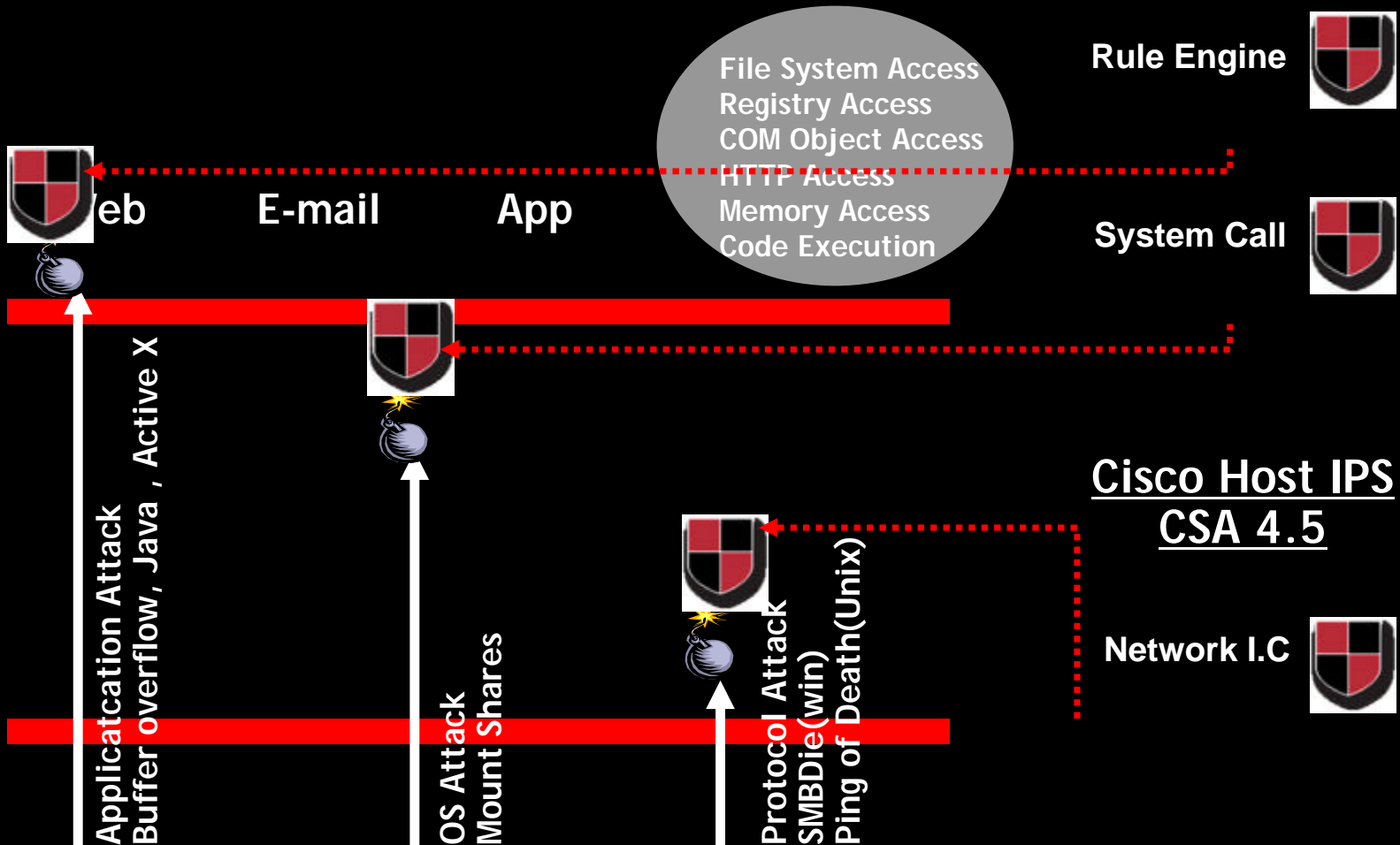
System Call

Host OS (Windows or Unix)

Network Protocol Stack

Network I.C

# Call Manager

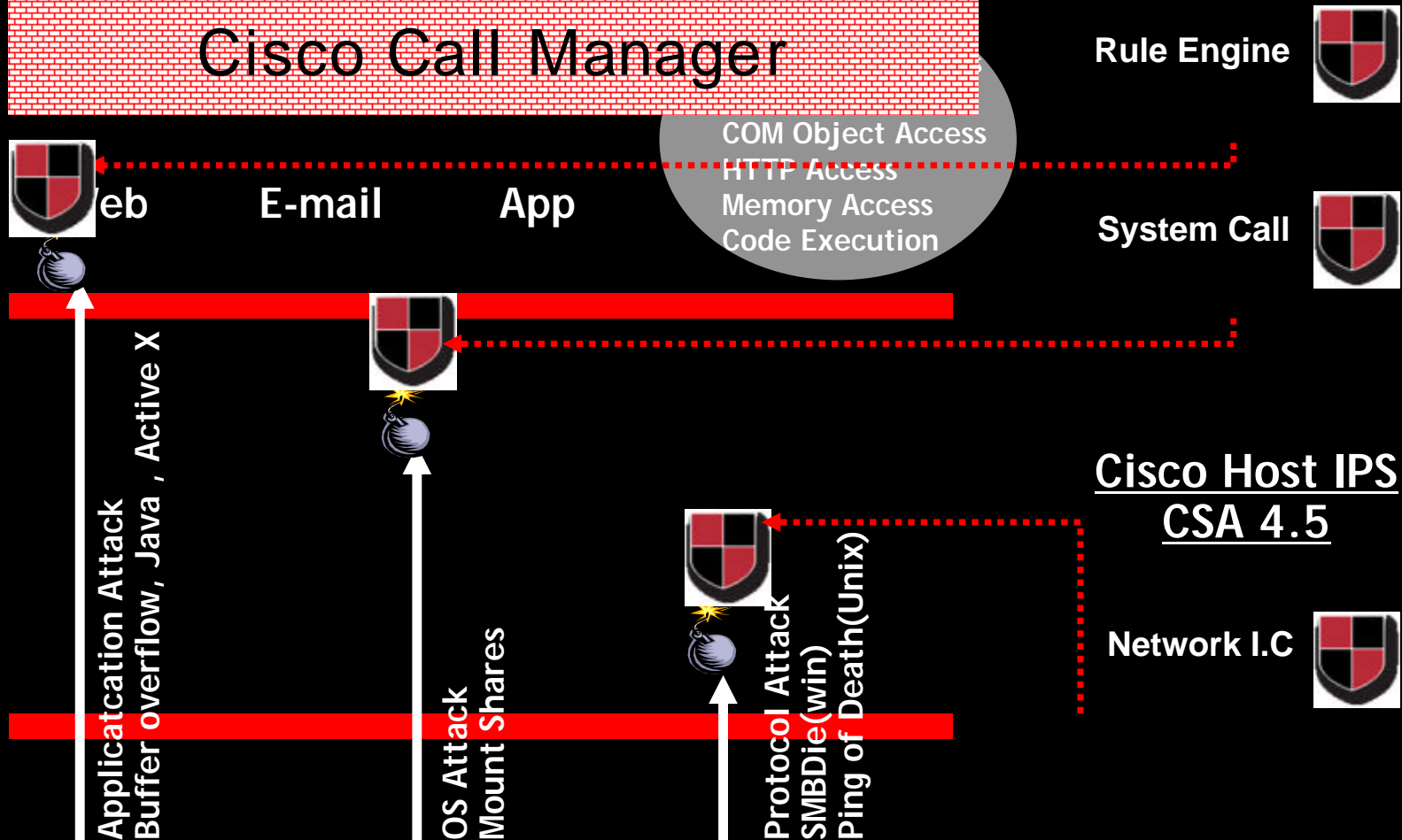




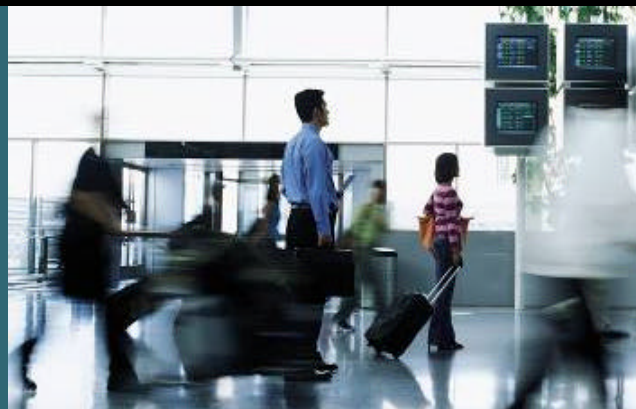
# Call Manager

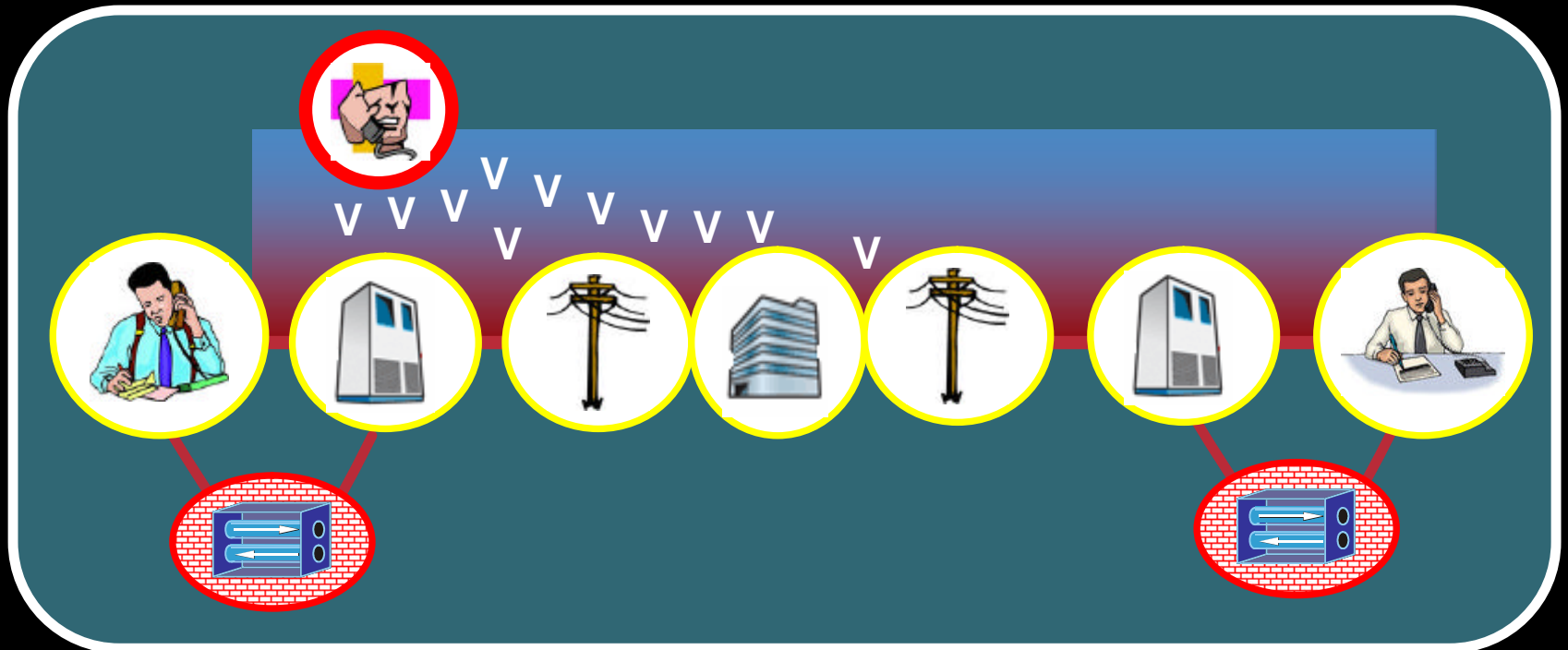


## Cisco Call Manager



,

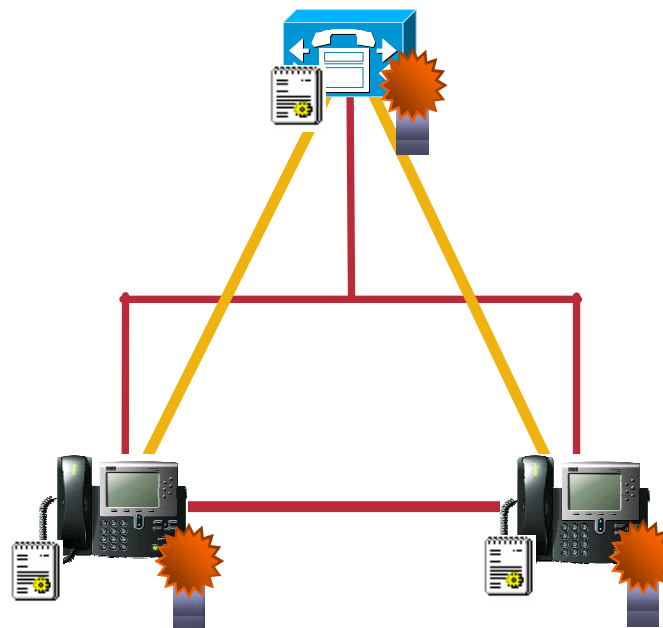




가 ...  
→ ???  
→ , 가...

- ❖ X.509 v3
  - Cisco CCM
  - CAPF (Cisco Authority Proxy Function)
- ❖ TLS
  - CCM Phone SSL v3
  - Call
- ❖ SRTP
  - RFC 3711 Secure RTP
  - Phone Call CCM

→ ,



# Voice



Wireshark - Ethereal

File Edit View Go Capture Analysis Statistics Help

Filter:  Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	11.1.10.50	11.1.10.152	SKINNY	CallSetupMessage
2	0.000099	11.1.10.50	11.1.10.152	SKINNY	SelectSoftkeyMessage
3	0.000116	11.1.10.50	11.1.10.152	SKINNY	DisplayPromptStatusMessage
4	0.000194	11.1.10.50	11.1.10.152	SKINNY	DisplayPhoneOffMessage
5	0.000249	11.1.10.50	11.1.10.152	SKINNY	CallInfoMessage
6	0.000294	11.1.10.50	11.1.10.152	SKINNY	SetLampMessage
7	0.000277	11.1.10.50	11.1.10.152	SKINNY	SetRingMessage
8	0.000341	11.1.10.50	11.1.10.50	TCP	3339 > 2000 [ACK] Seq=0 Ack=610 Win=7608 Len=0
9	4.489650	11.1.10.152	11.1.10.50	SKINNY	AudioStreamMessage
10	4.489755	11.1.10.152	11.1.10.50	SKINNY	OffhookMessage
11	4.486032	11.1.10.50	11.1.10.152	TCP	2000 > 3339 [ACK] Seq=620 Ack=38 Win=64855 Len=0
12	4.104302	11.1.10.50	11.1.10.152	SKINNY	SetRingMessage
13	4.104390	11.1.10.50	11.1.10.152	SKINNY	SetSpeakerModeMessage
14	4.104448	11.1.10.50	11.1.10.152	SKINNY	SetLampMessage
15	4.104532	11.1.10.50	11.1.10.152	SKINNY	CallStartMessage
16	4.104633	11.1.10.50	11.1.10.152	SKINNY	ActivateCallPlanMessage
17	4.104731	11.1.10.50	11.1.10.152	SKINNY	SetRingMessage
18	4.104779	11.1.10.50	11.1.10.152	SKINNY	StopRingMessage

Frame 1 (50 bytes on wire, 38 bytes captured)  
 Ethernet II, Src: 08:00:0c:0b:0a:bc, Dst: 08:0f:33:fc:a2:92  
 Internet Protocol, Src Addr: 11.1.10.50 (11.1.10.50), Dst Addr: 11.1.10.152 (11.1.10.152)  
 Transmission Control Protocol, Src Port: 2000 (2000), Dst Port: 3339 (3339), Seq: 0, Ack: 0, Len: 36  
 Source port: 2000 (2000)  
 Destination port: 3339 (3339)  
 Sequence number: 0 (relative sequence number)  
 Next sequence number: 36 (relative sequence number)  
 Acknowledgment number: 0 (relative ack number)  
 Header Length: 20 bytes  
 Flags: 0x0018 (PSH, ACK)  
 Window size: 64860  
 Checksum: 0x979b (correct)  
 Skinny client control protocol

Packet Length: 50 bytes, 38 bytes captured on interface eth0

## Call Signaling

Wireshark - Ethereal

File Edit View Go Capture Analysis Statistics Help

Filter:  Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
9	2.118234	11.1.10.152	11.1.10.50	TCP	3706 > 2443 [PSH, ACK] Seq=0 Ack=49 Win=8192 Len=49
10	2.102290	11.1.10.50	11.1.10.152	TCP	2443 > 3706 [PSH, ACK] Seq=0 Ack=49 Win=8192 Len=49
11	2.102356	11.1.10.50	11.1.10.152	TCP	2443 > 3706 [PSH, ACK] Seq=51 Ack=49 Win=8192 Len=49
12	2.102396	11.1.10.50	11.1.10.152	TCP	2443 > 3706 [PSH, ACK] Seq=94 Ack=49 Win=8192 Len=49
13	2.102540	11.1.10.50	11.1.10.152	TCP	2443 > 3706 [PSH, ACK] Seq=243 Ack=49 Win=8192 Len=49
14	2.102600	11.1.10.50	11.1.10.152	TCP	2443 > 3706 [PSH, ACK] Seq=204 Ack=49 Win=8192 Len=12
15	2.102661	11.1.10.50	11.1.10.152	TCP	2443 > 3706 [PSH, ACK] Seq=257 Ack=49 Win=8192 Len=82
16	2.102680	11.1.10.50	11.1.10.152	TCP	2443 > 3706 [PSH, ACK] Seq=318 Ack=49 Win=8192 Len=41
17	2.102650	11.1.10.50	11.1.10.152	TCP	2443 > 3706 [PSH, ACK] Seq=379 Ack=49 Win=8192 Len=51
18	2.111821	11.1.10.50	11.1.10.152	TCP	2443 > 3706 [PSH, ACK] Seq=411 Ack=49 Win=8192 Len=60
19	2.111890	11.1.10.50	11.1.10.152	TCP	2443 > 3706 [PSH, ACK] Seq=501 Ack=49 Win=8192 Len=61
20	2.112026	11.1.10.50	11.1.10.152	TCP	2443 > 3706 [PSH, ACK] Seq=562 Ack=49 Win=8192 Len=21
21	2.114991	11.1.10.50	11.1.10.152	TCP	2443 > 3706 [PSH, ACK] Seq=683 Ack=49 Win=8192 Len=13
22	2.115005	11.1.10.50	11.1.10.152	TCP	2443 > 3706 [PSH, ACK] Seq=1006 Ack=49 Win=8192 Len=62
23	2.115120	11.1.10.50	11.1.10.152	TCP	2443 > 3706 [PSH, ACK] Seq=1097 Ack=49 Win=8192 Len=13
24	2.115180	11.1.10.50	11.1.10.152	TCP	2443 > 3706 [PSH, ACK] Seq=1150 Ack=49 Win=8192 Len=82
25	2.115298	11.1.10.50	11.1.10.152	TCP	2443 > 3706 [PSH, ACK] Seq=1211 Ack=49 Win=8192 Len=421
26	2.115354	11.1.10.152	11.1.10.50	TCP	3706 > 2443 [ACK] Seq=48 Ack=683 Win=8192 Len=0

Frame 9 (105 bytes on wire, 103 bytes captured)  
 Ethernet II, Src: 08:0f:33:fc:a2:92, Dst: 08:00:0c:0b:0a:bc  
 Internet Protocol, Src Addr: 11.1.10.152 (11.1.10.152), Dst Addr: 11.1.10.50 (11.1.10.50)  
 Transmission Control Protocol, Src Port: 3706 (3706), Dst Port: 2443 (2443), Seq: 0, Ack: 0, Len: 49  
 Source port: 3706 (3706)  
 Destination port: 2443 (2443)  
 Sequence number: 0 (relative sequence number)  
 Next sequence number: 49 (relative sequence number)  
 Acknowledgment number: 0 (relative ack number)  
 Header Length: 20 bytes  
 Flags: 0x0018 (PSH, ACK)  
 Window size: 8192  
 Checksum: 0x4d1c (correct)  
 Data (49 bytes)

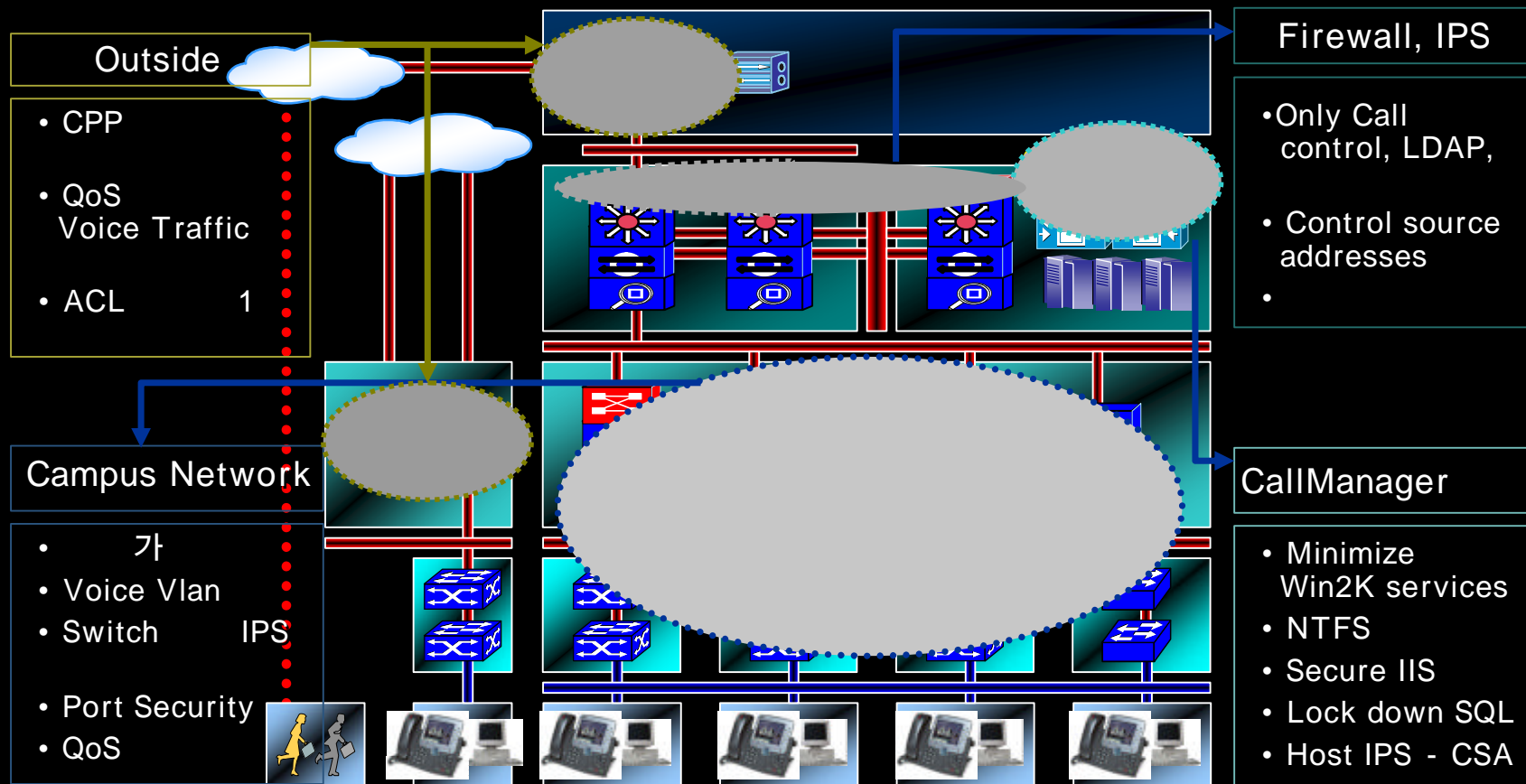
Packet Length: 105 bytes, 103 bytes captured on interface eth0

## Call Signaling

# IPC Vision



# IPC





## 1. Smart Security

—

## 2. Simple Config

- CNA , CCM , CS-MARS

## 3. Secure, Secure, Secure...

, — ,



# CISCO SYSTEMS

