IV Foro de seguridad RedIRIS

SECURE WIRELESS LANS

José Casado Meléndez,

Systems Engineer, Public Sector Spain

Agenda

- WLAN Security Vulnerabilities and Threats
- WLAN Security Authentication and Encryption
- Wireless IDS
- Wireless NAC

WLAN Security Vulnerabilities and Threats

- Different forms of Vulnerabilities and Threats Exist

  Encryption Vulnerabilities: WEP

  Authentication Vulnerabilities: Shared-Key authentication, Dictionary attacks, and MITM attacks

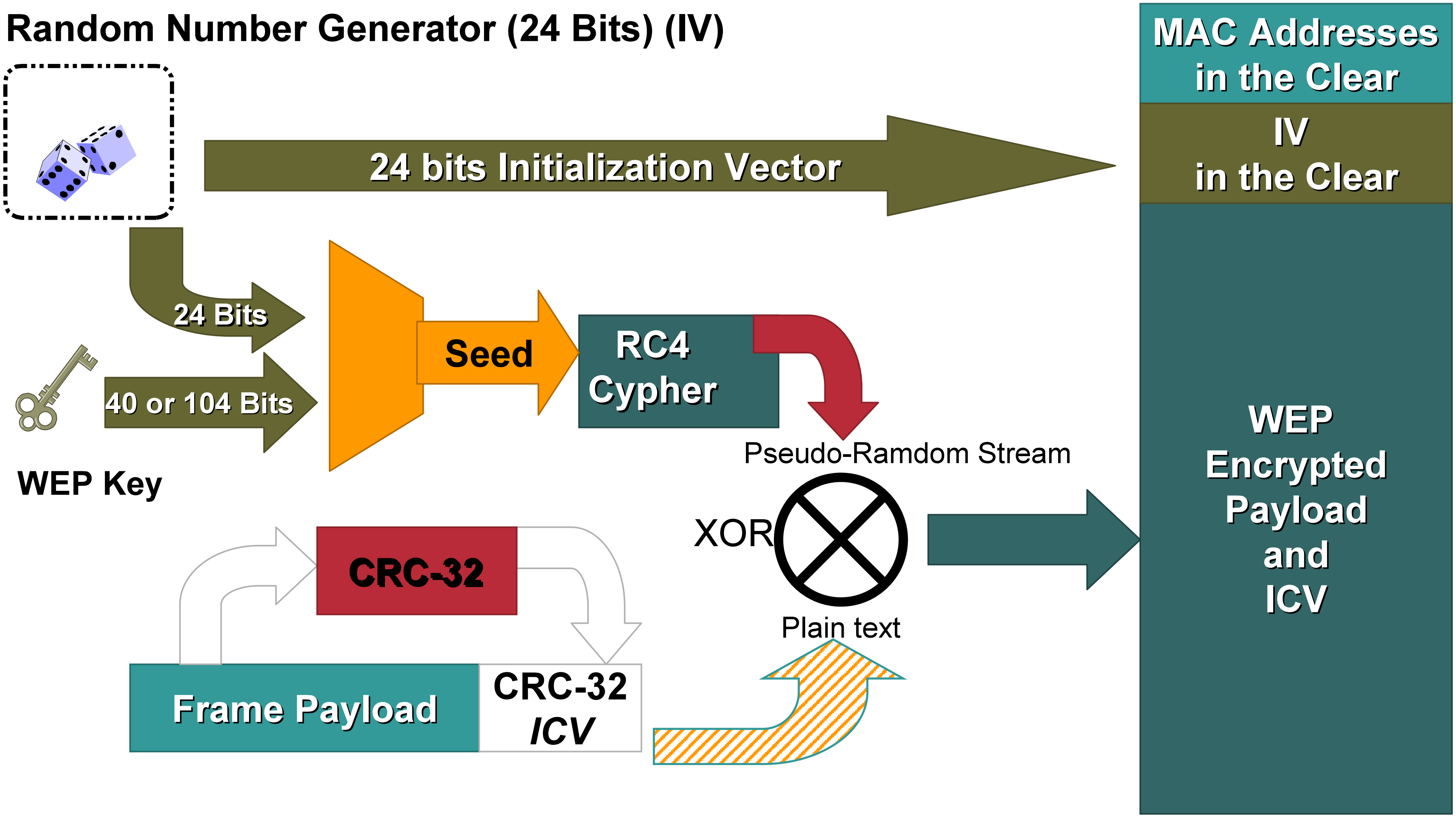
  WLAN Sniffing and SSID Broadcasting

  Address Spoofing: Mac-address spoofing and IP address spoofing (both hostile/outsider attacks as well as insider attacks)

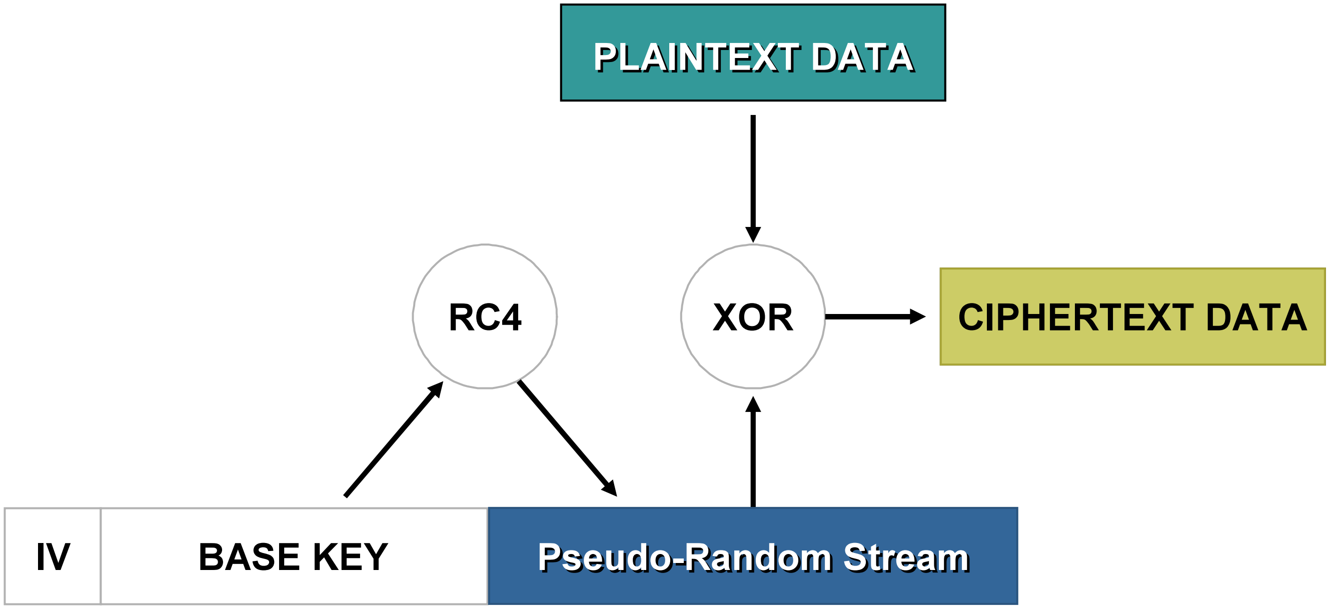
  Misconfigured APs and Clients

  Denial of Service (DoS) attacks: Using 802.11 deauthentication/ disassociation frames, RF jamming, etc.

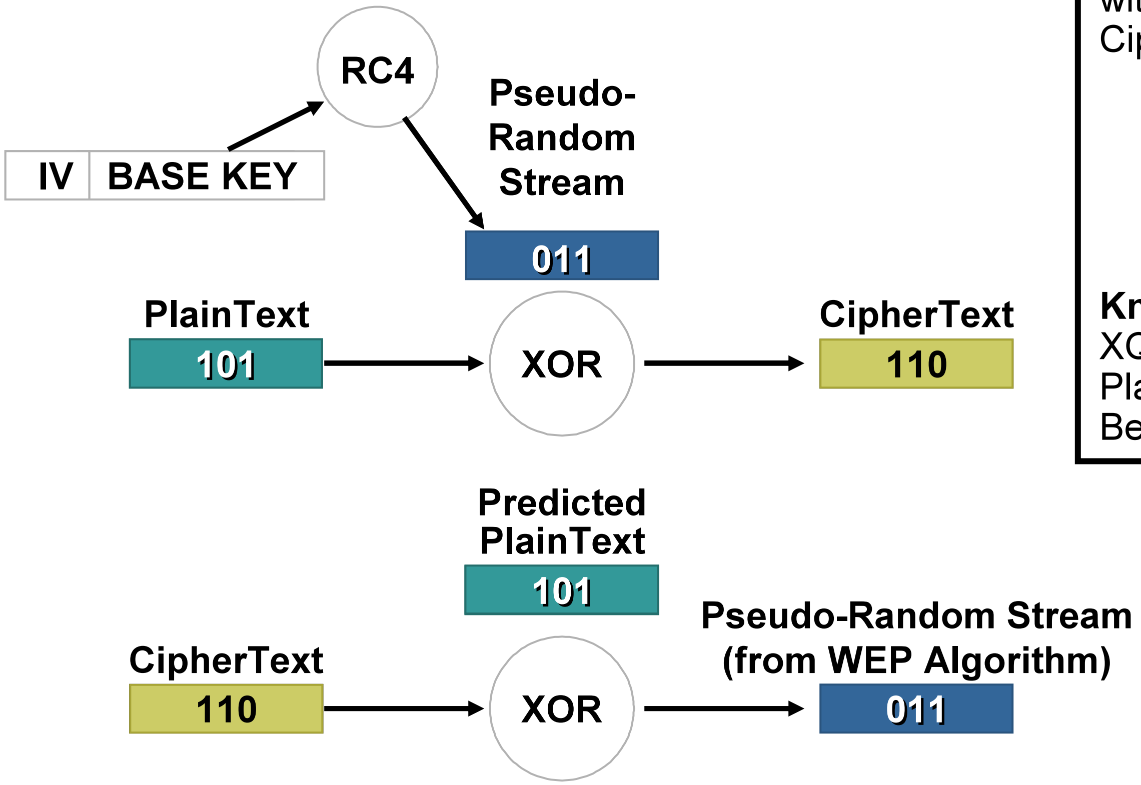
802.11 WEP Encryption


Random Number Generator (24 Bits) (IV)
24 bits Initialization Vector
MAC Addresses in the Clear
IV in the Clear
24 Bits
40 or 104 Bits
WEP Key
Seed
RC4 Cypher
Pseudo-Ramdom Stream
XOR
Plain text
WEP Encrypted Payload and ICV
CRC-32
Frame Payload
CRC-32 ICV

802.11 WEP Encryption—Algorithm



Known Plaintext Attack



RC4

IV | BASE KEY

Pseudo-Random Stream

011

PlainText

101

XOR

CipherText

110

Predicted PlainText

101

CipherText

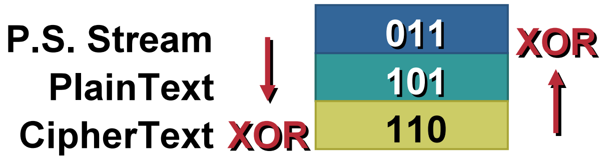
110

XOR

Pseudo-Random Stream (from WEP Algorithm)

011

Encryption: The Pseudo-Random Output from WEPs RC4 Cipher Is XQRed with the Plaintext Data to Produce the Ciphertext



P.S. Stream 011

PlainText 101

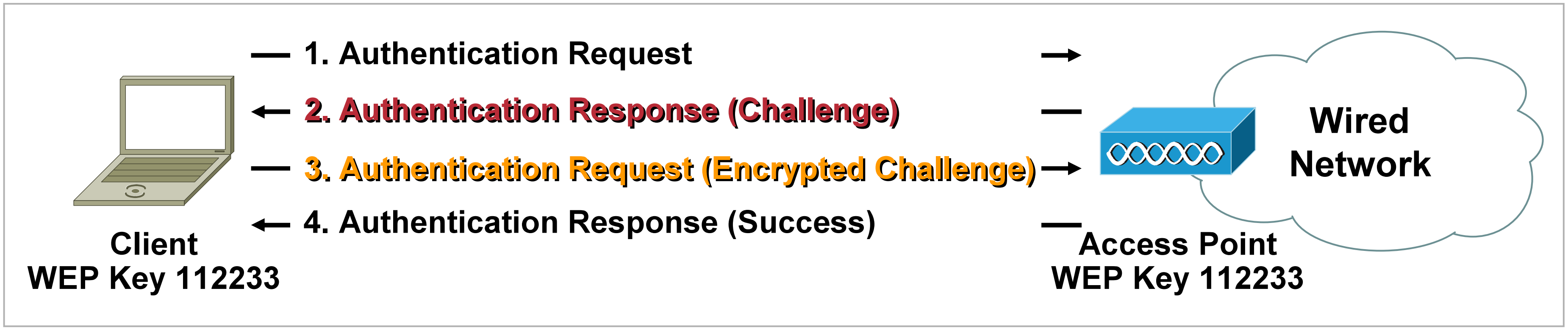
CipherText 110

XOR

XOR

Known Plaintext Attack: If Ciphertext Is XQRed with Known (or Guessed) Plaintext, the Stream Cipher Output Can Be Derived

Generating Known Plaintext—802.11 Shared Key Authentication



1. Authentication Request

2. Authentication Response (Challenge)

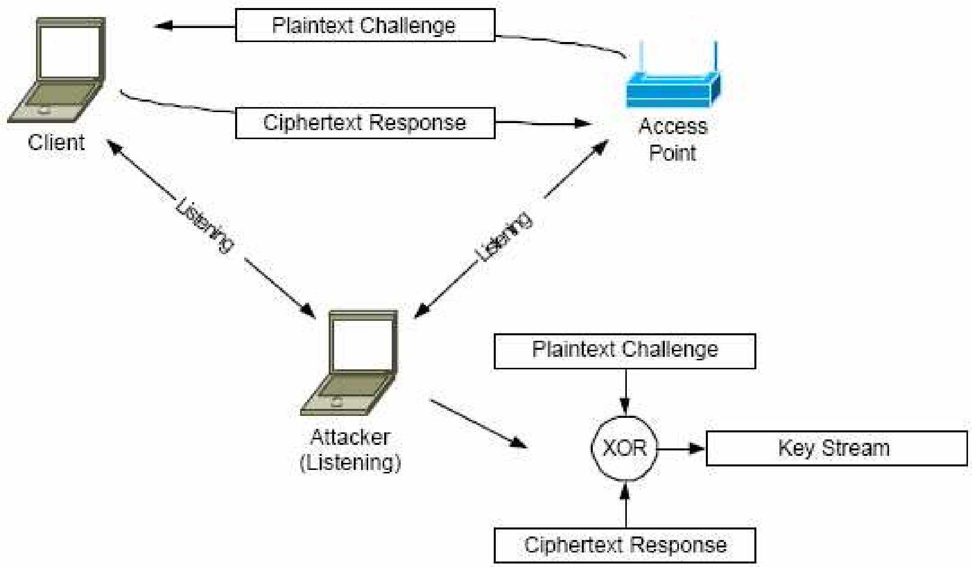
3. Authentication Request (Encrypted Challenge)

4. Authentication Response (Success)

Client
WEP Key 112233

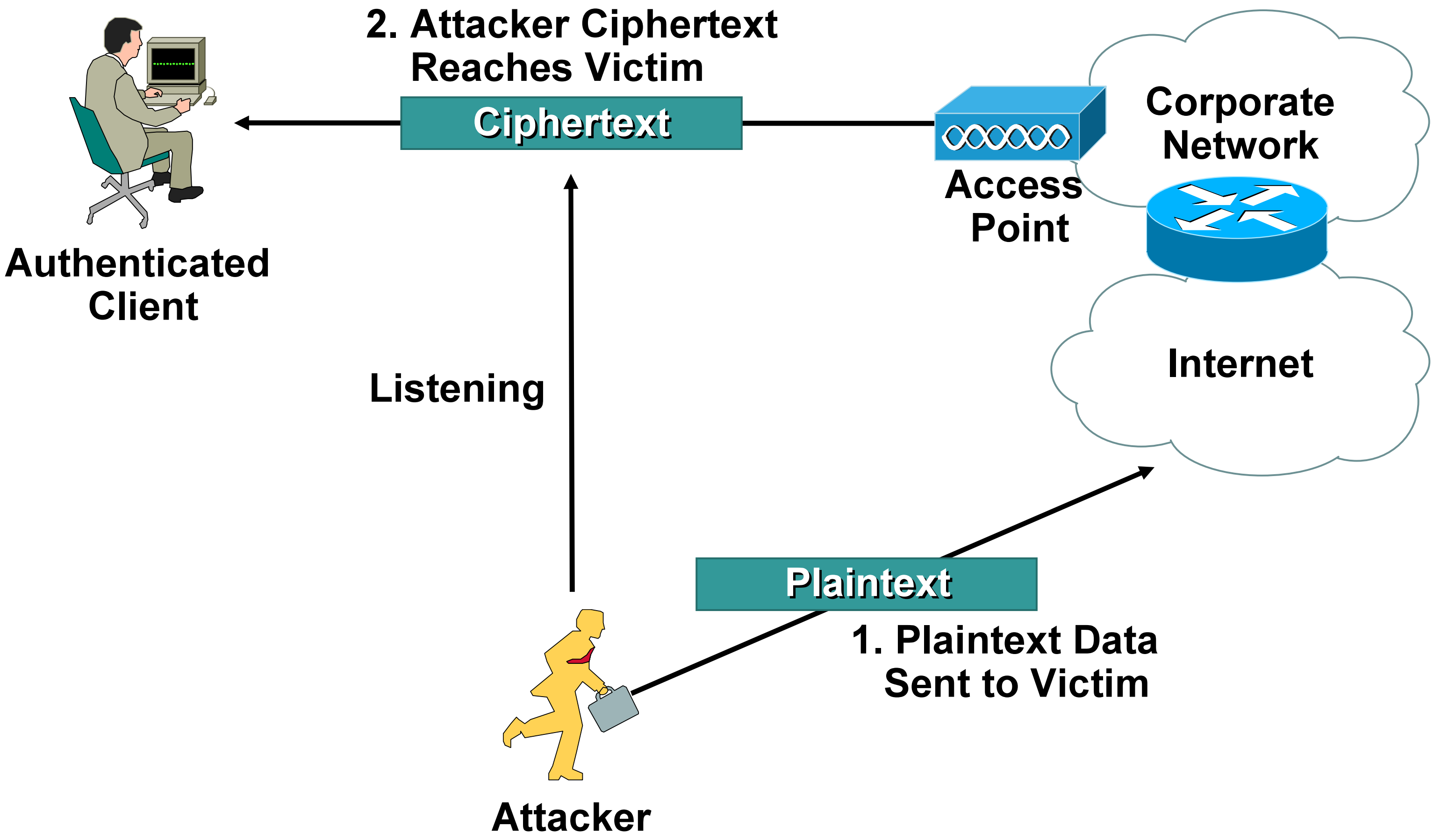
Access Point
WEP Key 112233

Wired Network



Shared Key Authentication Is Not Recommended

Generating Known Plaintext— Send Text Directly to Receiver



Agenda

- WLAN Security Vulnerabilities and Threats
- WLAN Security Authentication and Encryption
- Wireless IDS
- Wireless NAC

Basic Requirements to Secure Wireless LANs

- Encryption algorithm

  Mechanism to provide data privacy

- Message integrity

  Ensures data frames are tamper free and truly originate from the source address

- Authentication framework

  Framework to facilitate authentication messages between clients, access point, and AAA server

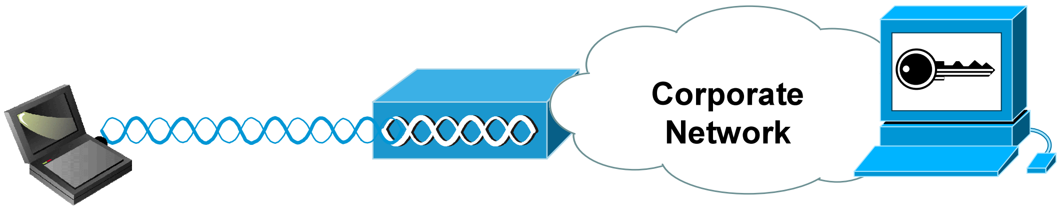
- Authentication algorithm

  Mechanism to validate client credentials

How does Extensible Authentication Protocol (EAP) authenticate clients?

WLAN Client | Access Point | RADIUS server

Client associates



Cannot send data until…

Data from client → ✗ Blocked by AP

…EAP authentication complete

EAP

802.1x | RADIUS

Client sends data

Data from client ✓ Passed by AP →

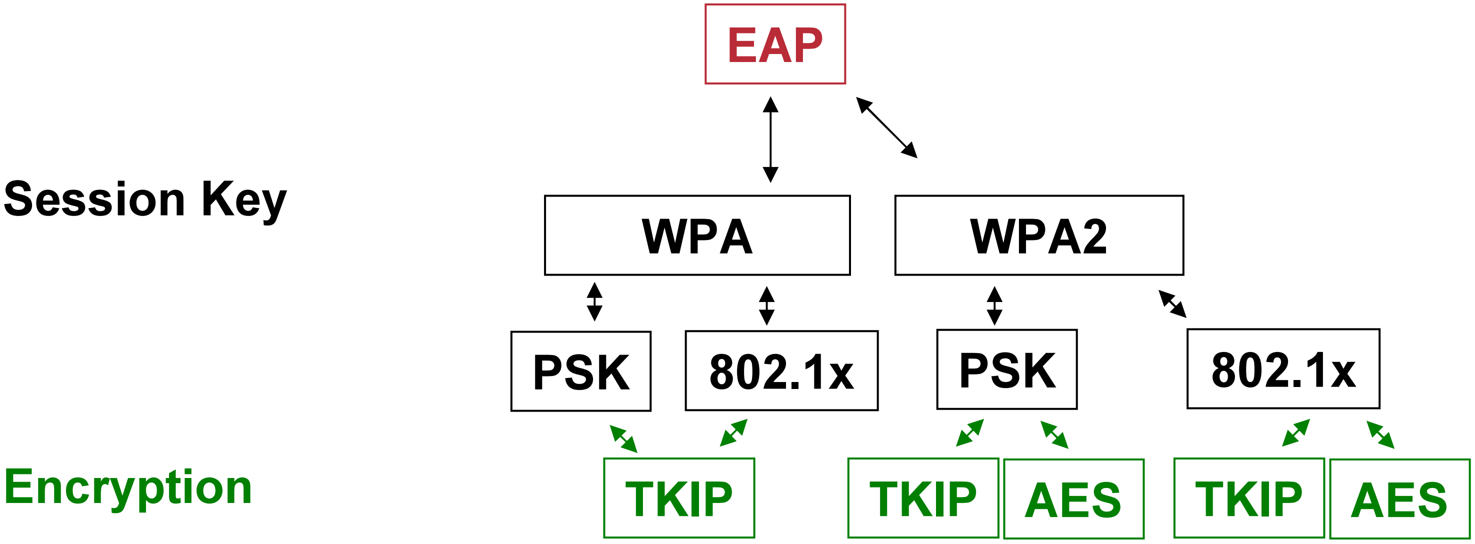
WPA Overview

- Interim standard that improves on WEP security prior to 802.11i
- Includes two authentication modes
    - 802.1X authentication
    - Pre-Shared Key (PSK)
- If using Temporal Key Integrity Protocol (TKIP) and 802.1X, this provides dynamic key encryption and mutual authentication that improve on the WEP encryption model
- If using Temporal Key Integrity Protocol (TKIP) and PSK, this provides dynamic key encryption and mutual authentication that does not require a RADIUS server
- Compatible with portions of the 802.11i drafts, including implementation of 802.1X and TKIP

WPA2 Overview

- New security standard developed by IEEE 802.11i task group
  - Robust Security Network (RSN) is IEEE equivalent to WPA2
- Generally uses Advanced Encryption Standard (AES) block ciphers with the Counter Mode-CBC MAC Protocol (CCMP) for encryption
  - Supports TKIP
- Generally uses 802.1x authentication methods
  - Supports PSK
- Comparable to WPA
  - Use the same authentication architecture, key distribution & key renewal
- Supports Proactive Key Caching (PKC)
- Supports pre-authentication (optional)

WPA2 versus WPA Context



EAP

Session Key

WPA

WPA2

PSK

802.1x

PSK

802.1x

Encryption

TKIP

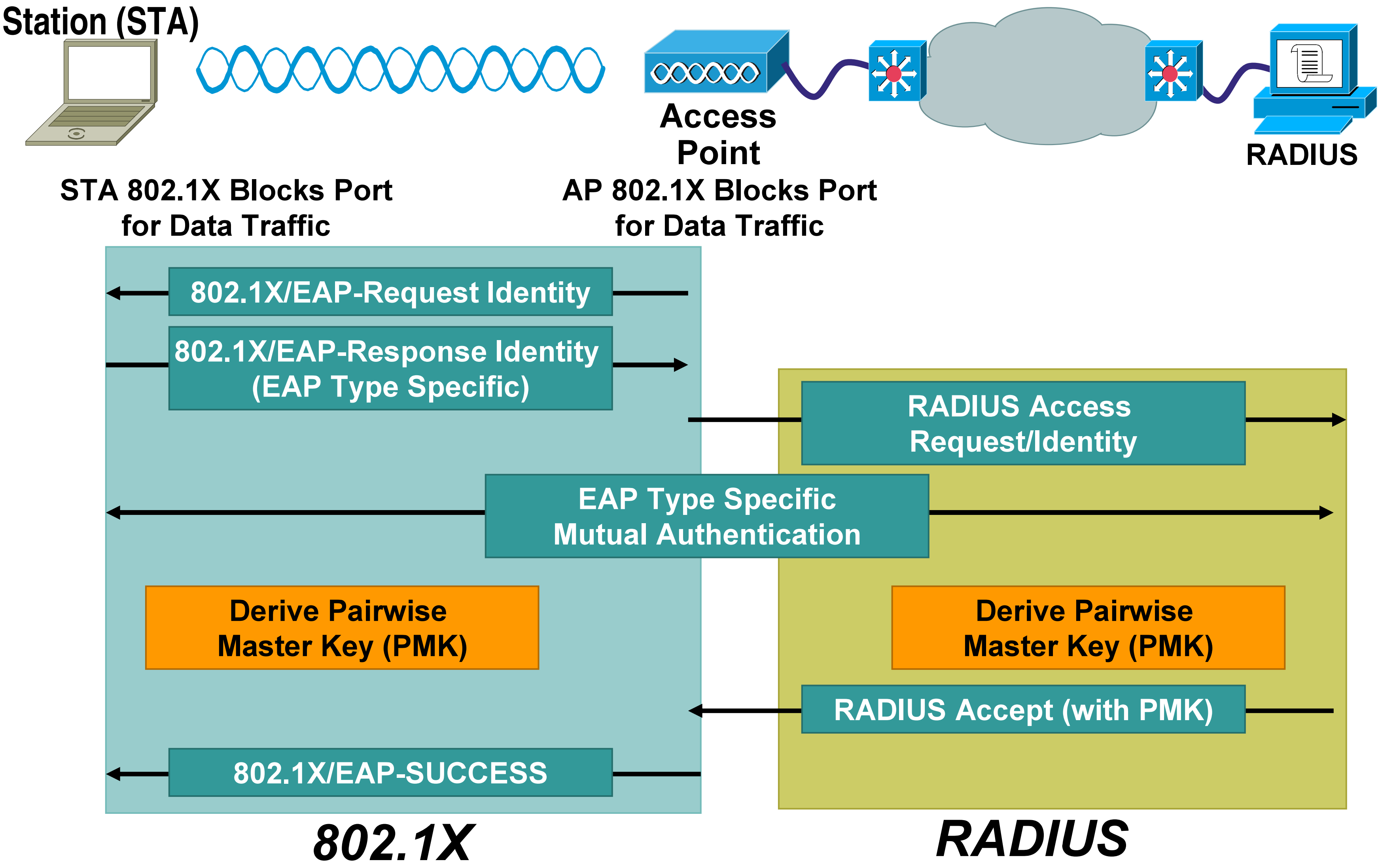
TKIP

AES

TKIP

AES

802.11i/WPA
EAP Authentication Overview



Station (STA)

Access Point

RADIUS

STA 802.1X Blocks Port for Data Traffic

AP 802.1X Blocks Port for Data Traffic

802.1X/EAP-Request Identity

802.1X/EAP-Response Identity (EAP Type Specific)

RADIUS Access Request/Identity

EAP Type Specific Mutual Authentication

Derive Pairwise Master Key (PMK)

Derive Pairwise Master Key (PMK)

RADIUS Accept (with PMK)

802.1X/EAP-SUCCESS

802.1X

RADIUS

WLAN Security Authentication and Encryption Summary

- WLAN Security encompasses both authentication and encryption and both components are mandated by WPA
- Care should be taken to ascertain that the chosen EAP authentication type employed is compatible with authentication database
- WPA provides both dynamic, per-packet keying in addition to key authentication/ message integrity
- WLAN Client capability/ availability must be considered when choosing WLAN authentication and encryption options

Agenda

- WLAN Security Vulnerabilities and Threats
- WLAN Security Authentication and Encryption
- Wireless IDS
- Wireless NAC

Agenda

- Wireless IDS Defined
- Cisco Wireless Intrusion Detection Solutions
    - WLAN Controller-based Architecture
    - Autonomous Access Point Architecture
    - Autonomous Access Point Architecture with Partner Integration

Problem Definition

- Traditional wired IDS focus on L3 and higher
- Nature of RF medium and wireless standards mandate IDS at the physical and data link layer
- RF medium vulnerabilities:

  Unlicensed spectrum subject to interference, contention

  Not contained by physical security boundaries
- Standards vulnerabilities:

  Unauthenticated management frames

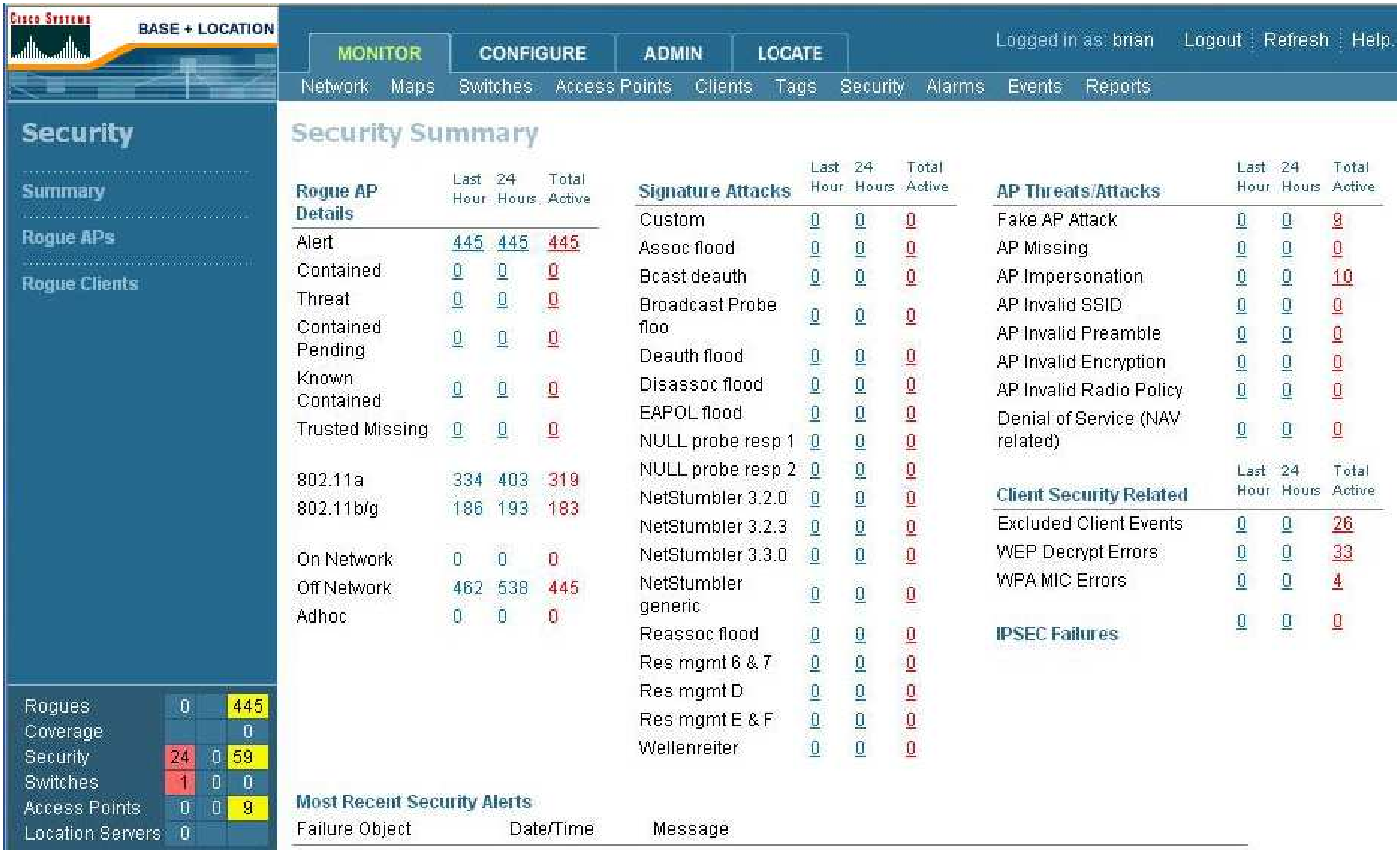
  Session hi-jacking, replay type attacks
- Wide availability of wireless hacking literature & tools

Wireless Intrusion Detection Systems

- Address RF related vulnerabilities
  - Detect, locate, mitigate rogue devices
  - Detect and manage RF interference
  - Detect reconnaissance if possible
- Address standards-based vulnerabilities
  - Detect management frame & hi-jacking style attacks
  - Enforce security configuration policies
- Complementary functionality:
  - Forensic analysis
  - Compliance reporting
- **Cisco has solutions to address WIDS requirements**

WIDS—WLAN Controller-based Architecture

Cisco WCS – Centralized Security Management



Security Summary

Rogue AP Details	Last Hour	24 Hours	Total Active
Alert	445	445	445
Contained	0	0	0
Threat	0	0	0
Contained Pending	0	0	0
Known Contained	0	0	0
Trusted Missing	0	0	0
802.11a	334	403	319
802.11b/g	186	193	183
On Network	0	0	0
Off Network	462	538	445
Adhoc	0	0	0

Signature Attacks	Last Hour	24 Hours	Total Active
Custom	0	0	0
Assoc flood	0	0	0
Bcast deauth	0	0	0
Broadcast Probe floo	0	0	0
Deauth flood	0	0	0
Disassoc flood	0	0	0
EAPOL flood	0	0	0
NULL probe resp 1	0	0	0
NULL probe resp 2	0	0	0
NetStumbler 3.2.0	0	0	0
NetStumbler 3.2.3	0	0	0
NetStumbler 3.3.0	0	0	0
NetStumbler generic	0	0	0
Reassoc flood	0	0	0
Res mgmt 6 & 7	0	0	0
Res mgmt D	0	0	0
Res mgmt E & F	0	0	0
Wellenreiter	0	0	0

AP Threats/Attacks	Last Hour	24 Hours	Total Active
Fake AP Attack	0	0	9
AP Missing	0	0	0
AP Impersonation	0	0	10
AP Invalid SSID	0	0	0
AP Invalid Preamble	0	0	0
AP Invalid Encryption	0	0	0
AP Invalid Radio Policy	0	0	0
Denial of Service (NAV related)	0	0	0

Client Security Related	Last Hour	24 Hours	Total Active
Excluded Client Events	0	0	26
WEP Decrypt Errors	0	0	33
WPA MIC Errors	0	0	4
IPSEC Failures	0	0	0

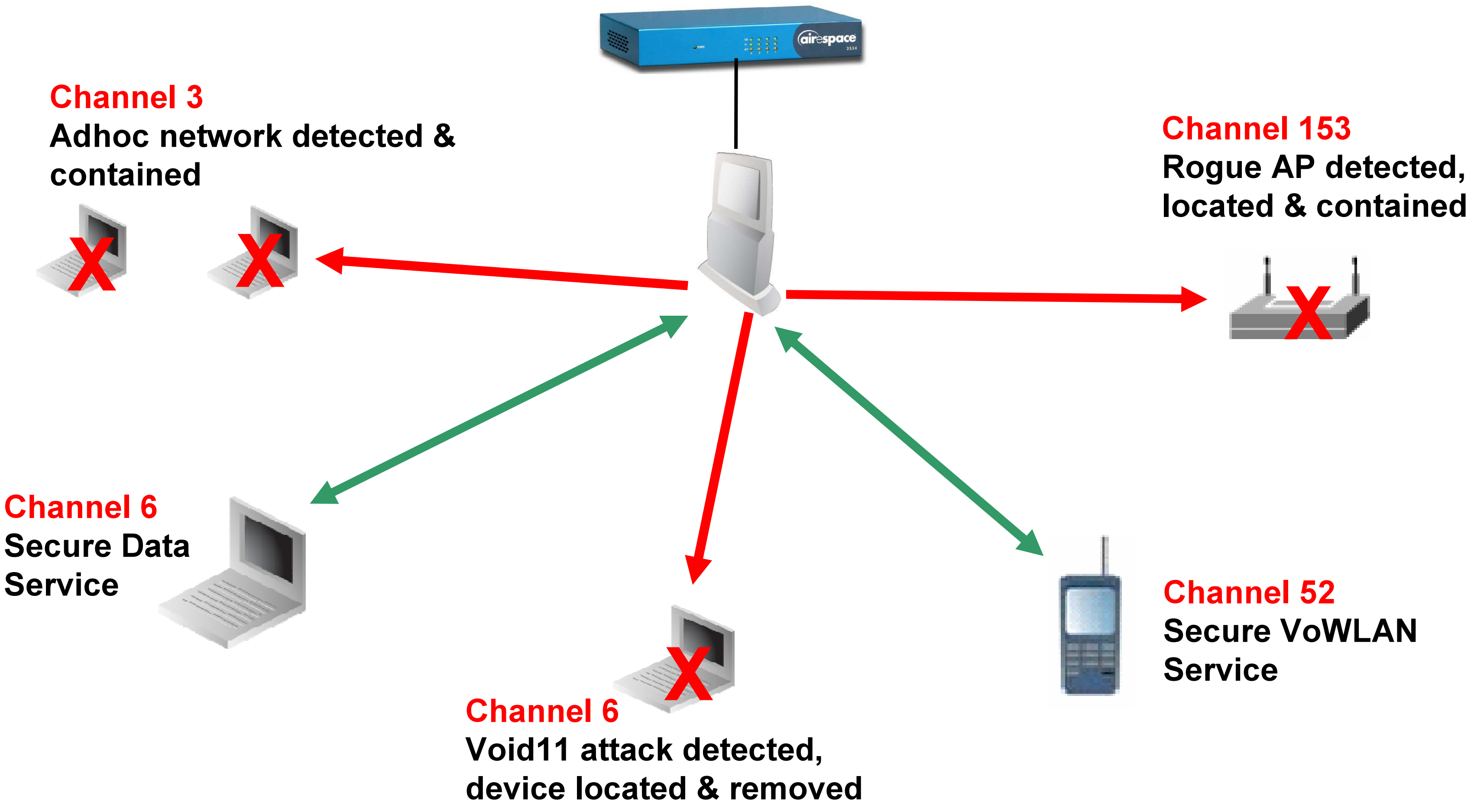
Most Recent Security Alerts

Failure Object	Date/Time	Message

Rogues	0		445
Coverage			0
Security	24	0	59
Switches	1	0	0
Access Points	0	0	9
Location Servers	0		

Simultaneous IDS Monitoring & 802.11 Service

Simultaneous multi-mode, multi-channel IDS Monitoring & 802.11 Service



Channel 3
Adhoc network detected & contained

Channel 153
Rogue AP detected, located & contained

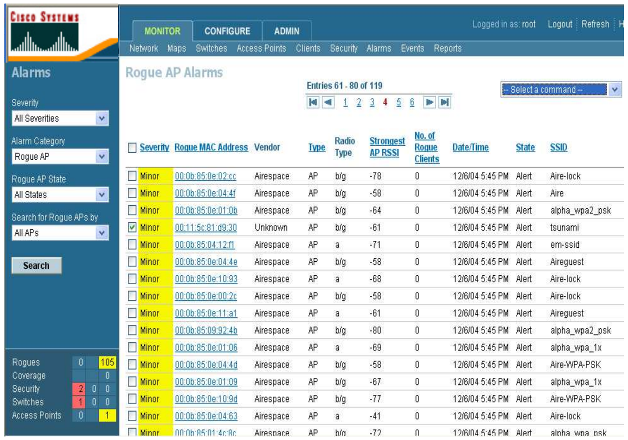
Channel 6
Secure Data Service

Channel 6
Void11 attack detected, device located & removed

Channel 52
Secure VoWLAN Service

IPS & Hi-res Location Tracking

1. Detect rogue or attack



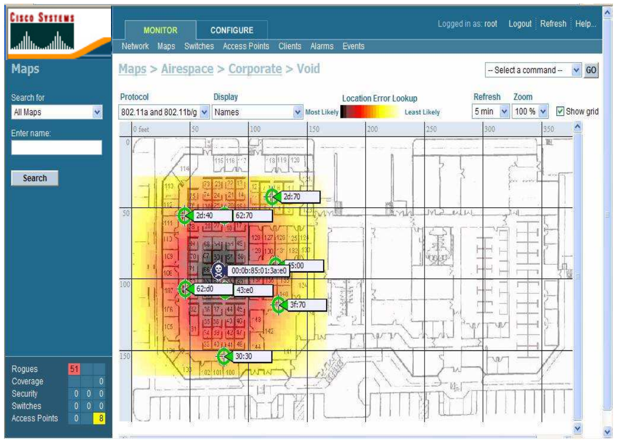
Rogue AP Alarms

Entries 61 - 80 of 119

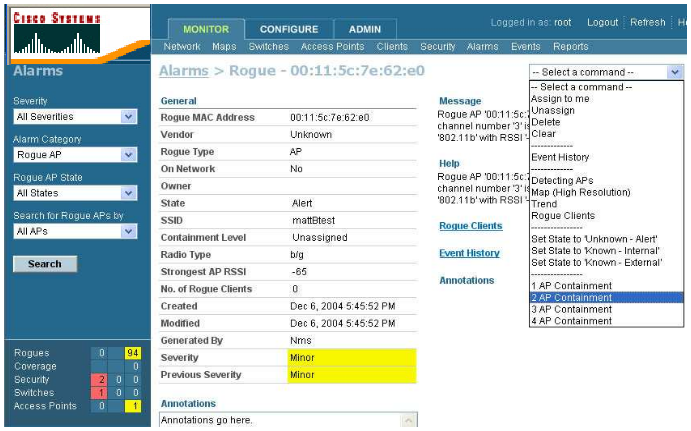
1 2 3 4 5 6

□	Severity	Rogue MAC Address	Vendor	Type	Radio Type	Strongest AP RSSI	No. of Rogue Clients	Date/Time	State	SSID
□	Minor	00:0b:85:0e:02:cc	Airespace	AP	b/g	-78	0	12/6/04 5:45 PM	Alert	Aire-lock
□	Minor	00:0b:85:0e:04:4f	Airespace	AP	b/g	-58	0	12/6/04 5:45 PM	Alert	Aire
□	Minor	00:0b:85:0e:01:0b	Airespace	AP	b/g	-64	0	12/6/04 5:45 PM	Alert	alpha_wpa2_psk
☑	Minor	00:11:5c:81:d9:30	Unknown	AP	b/g	-61	0	12/6/04 5:45 PM	Alert	tsunami
□	Minor	00:0b:85:04:12:f1	Airespace	AP	a	-71	0	12/6/04 5:45 PM	Alert	em-ssid
□	Minor	00:0b:85:0e:04:4e	Airespace	AP	b/g	-58	0	12/6/04 5:45 PM	Alert	Aireguest
□	Minor	00:0b:85:0e:10:93	Airespace	AP	a	-68	0	12/6/04 5:45 PM	Alert	Aire-lock
□	Minor	00:0b:85:0e:00:2c	Airespace	AP	b/g	-58	0	12/6/04 5:45 PM	Alert	Aire-lock
□	Minor	00:0b:85:0e:11:a1	Airespace	AP	a	-61	0	12/6/04 5:45 PM	Alert	Aireguest
□	Minor	00:0b:85:09:92:4b	Airespace	AP	b/g	-80	0	12/6/04 5:45 PM	Alert	alpha_wpa2_psk
□	Minor	00:0b:85:0e:01:06	Airespace	AP	a	-69	0	12/6/04 5:45 PM	Alert	alpha_wpa_1x
□	Minor	00:0b:85:0e:04:4d	Airespace	AP	b/g	-58	0	12/6/04 5:45 PM	Alert	Aire-WPA-PSK
□	Minor	00:0b:85:0e:01:09	Airespace	AP	b/g	-67	0	12/6/04 5:45 PM	Alert	alpha_wpa_1x
□	Minor	00:0b:85:0e:10:9d	Airespace	AP	b/g	-77	0	12/6/04 5:45 PM	Alert	Aire-WPA-PSK
□	Minor	00:0b:85:0e:04:63	Airespace	AP	a	-41	0	12/6/04 5:45 PM	Alert	Aire-lock
□	Minor	00:0b:85:01:4c:8c	Airespace	AP	b/g	-72	0	12/6/04 5:45 PM	Alert	alpha_wpa_psk

2. Locate attack & track device



3. Assess threat level & mitigate



Alarms > Rogue - 00:11:5c:7e:62:e0

General	
Rogue MAC Address	00:11:5c:7e:62:e0
Vendor	Unknown
Rogue Type	AP
On Network	No
Owner	
State	Alert
SSID	mattBtest
Containment Level	Unassigned
Radio Type	b/g
Strongest AP RSSI	-65
No. of Rogue Clients	0
Created	Dec 6, 2004 5:45:52 PM
Modified	Dec 6, 2004 5:45:52 PM
Generated By	Nms
Severity	Minor
Previous Severity	Minor

Annotations

Annotations go here.

Message

Rogue AP '00:11:5c:
channel number '3' is
'802.11b' with RSSI '-

Help

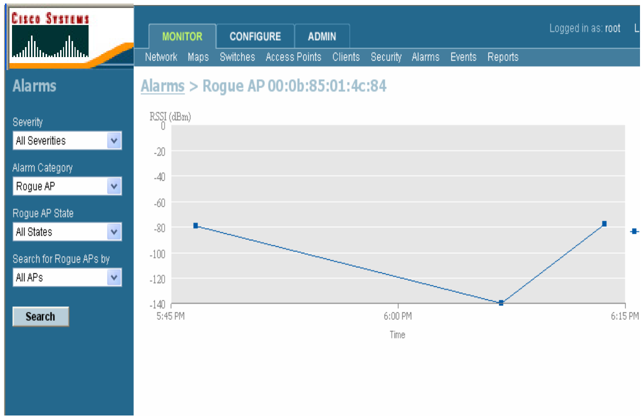
Rogue AP '00:11:5c:
channel number '3' is
'802.11b' with RSSI '-

Rogue Clients

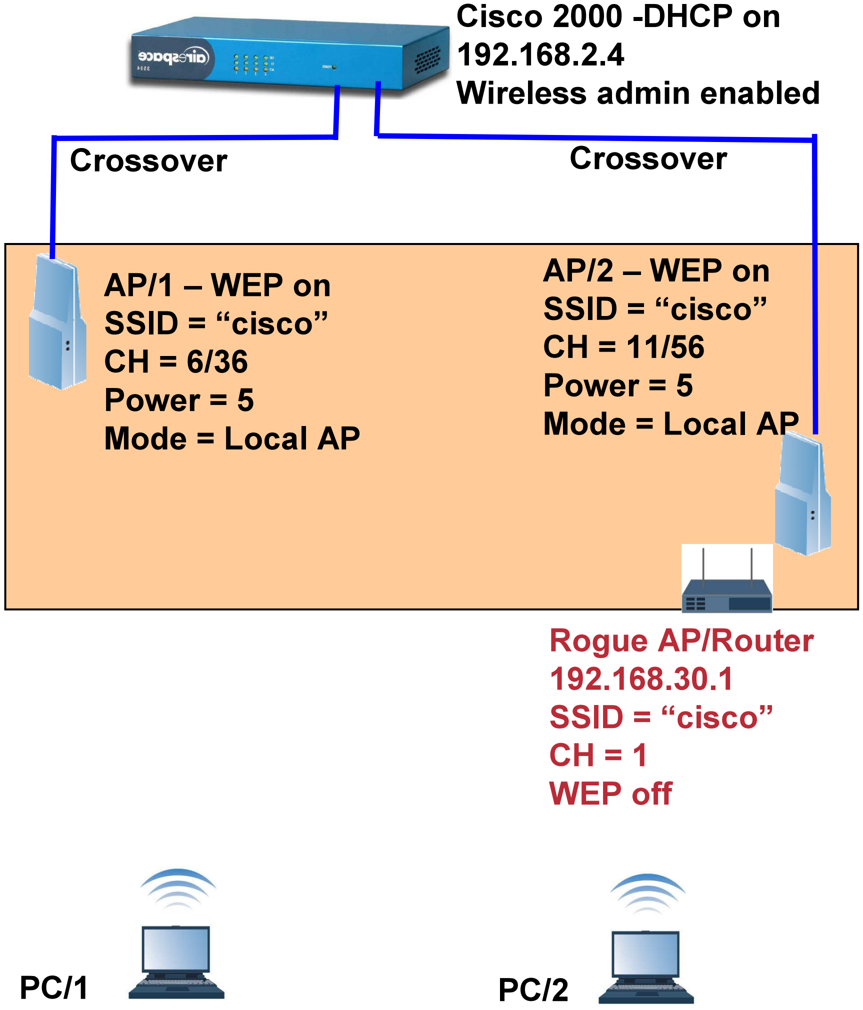
Event History

Annotations

4. Create Historical Reports



Detect, Locate & Contain Rogue AP Demo



Cisco 2000 -DHCP on
192.168.2.4
Wireless admin enabled

Crossover

Crossover

AP/1 – WEP on
SSID = “cisco”
CH = 6/36
Power = 5
Mode = Local AP

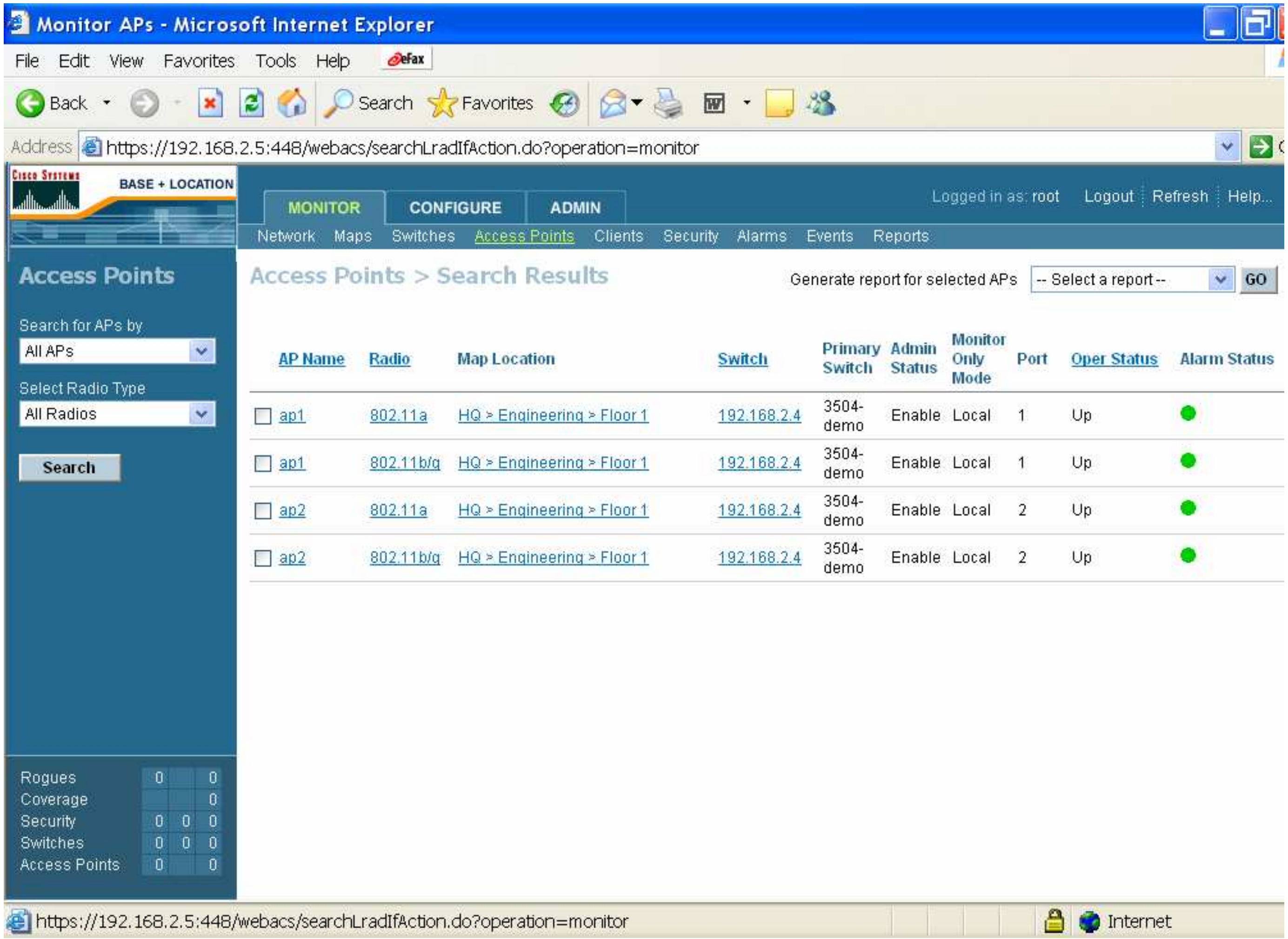
AP/2 – WEP on
SSID = “cisco”
CH = 11/56
Power = 5
Mode = Local AP

Rogue AP/Router
192.168.30.1
SSID = “cisco”
CH = 1
WEP off

PC/1
Associate to SSID “cisco”
Static IP = 192.168.2.5
SSID = “cisco”
WEP enabled
Running WCS

PC/2
Associate to rogue
192.168.30.10
SSID = “cisco”
WEP disabled

Verify APs are active: Monitor > Access Points


Monitor APs - Microsoft Internet Explorer
File Edit View Favorites Tools Help
eFax
Back
Search
Favorites
Address
BASE + LOCATION
MONITOR
CONFIGURE
ADMIN
Logout
Refresh
Help...
Network Maps Switches Access Points Clients Security Alarms Events Reports
GO
Search
Internet

Address: https://192.168.2.5:448/webacs/searchLradIfAction.do?operation=monitor

Logged in as: root

Access Points

Search for APs by: All APs

Select Radio Type: All Radios

Access Points > Search Results

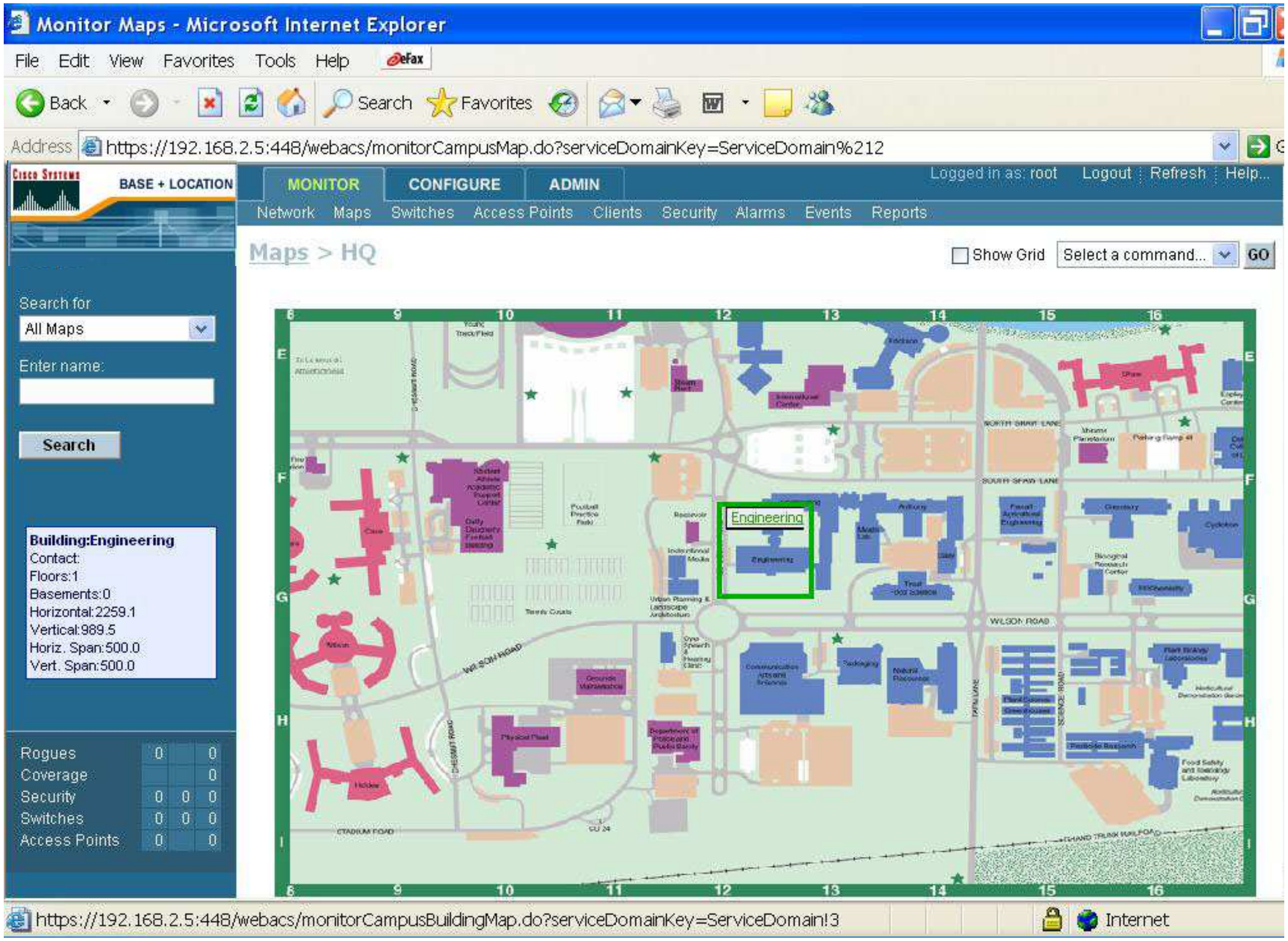
Generate report for selected APs: -- Select a report --

	AP Name	Radio	Map Location	Switch	Primary Switch	Admin Status	Monitor Only Mode	Port	Oper Status	Alarm Status
□	ap1	802.11a	HQ > Engineering > Floor 1	192.168.2.4	3504-demo	Enable	Local	1	Up	●
□	ap1	802.11b/g	HQ > Engineering > Floor 1	192.168.2.4	3504-demo	Enable	Local	1	Up	●
□	ap2	802.11a	HQ > Engineering > Floor 1	192.168.2.4	3504-demo	Enable	Local	2	Up	●
□	ap2	802.11b/g	HQ > Engineering > Floor 1	192.168.2.4	3504-demo	Enable	Local	2	Up	●

Rogues	0		0
Coverage			0
Security	0	0	0
Switches	0	0	0
Access Points	0		0

https://192.168.2.5:448/webacs/searchLradIfAction.do?operation=monitor

Map Campus > Building



Monitor Maps - Microsoft Internet Explorer
File Edit View Favorites Tools Help eFax
Back Search Favorites
Address
BASE + LOCATION
MONITOR CONFIGURE ADMIN
Logged in as: root Logout Refresh Help...
Network Maps Switches Access Points Clients Security Alarms Events Reports
Maps > HQ
□ Show Grid
Select a command...
GO
Search for
All Maps
Enter name:
Search
Engineering
WILSON ROAD
STADIUM ROAD
Internet

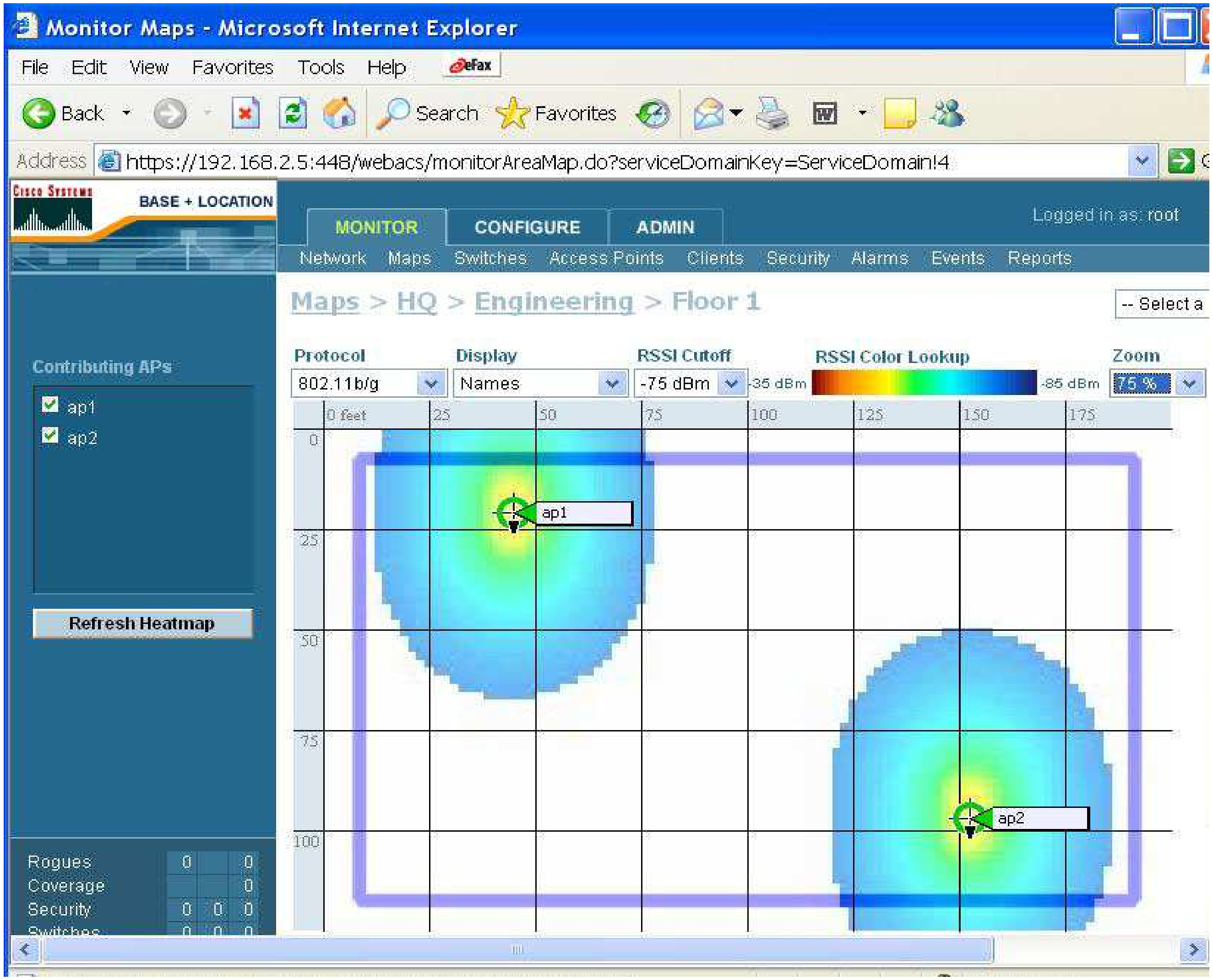
https://192.168.2.5:448/webacs/monitorCampusMap.do?serviceDomainKey=ServiceDomain%212

Building:Engineering
Contact:
Floors:1
Basements:0
Horizontal:2259.1
Vertical:989.5
Horiz. Span:500.0
Vert. Span:500.0

Rogues	0		0
Coverage			0
Security	0	0	0
Switches	0	0	0
Access Points	0		0

https://192.168.2.5:448/webacs/monitorCampusBuildingMap.do?serviceDomainKey=ServiceDomain!3

Map APs in Meeting Room



Address: https://192.168.2.5:448/webacs/monitorAreaMap.do?serviceDomainKey=ServiceDomain!4

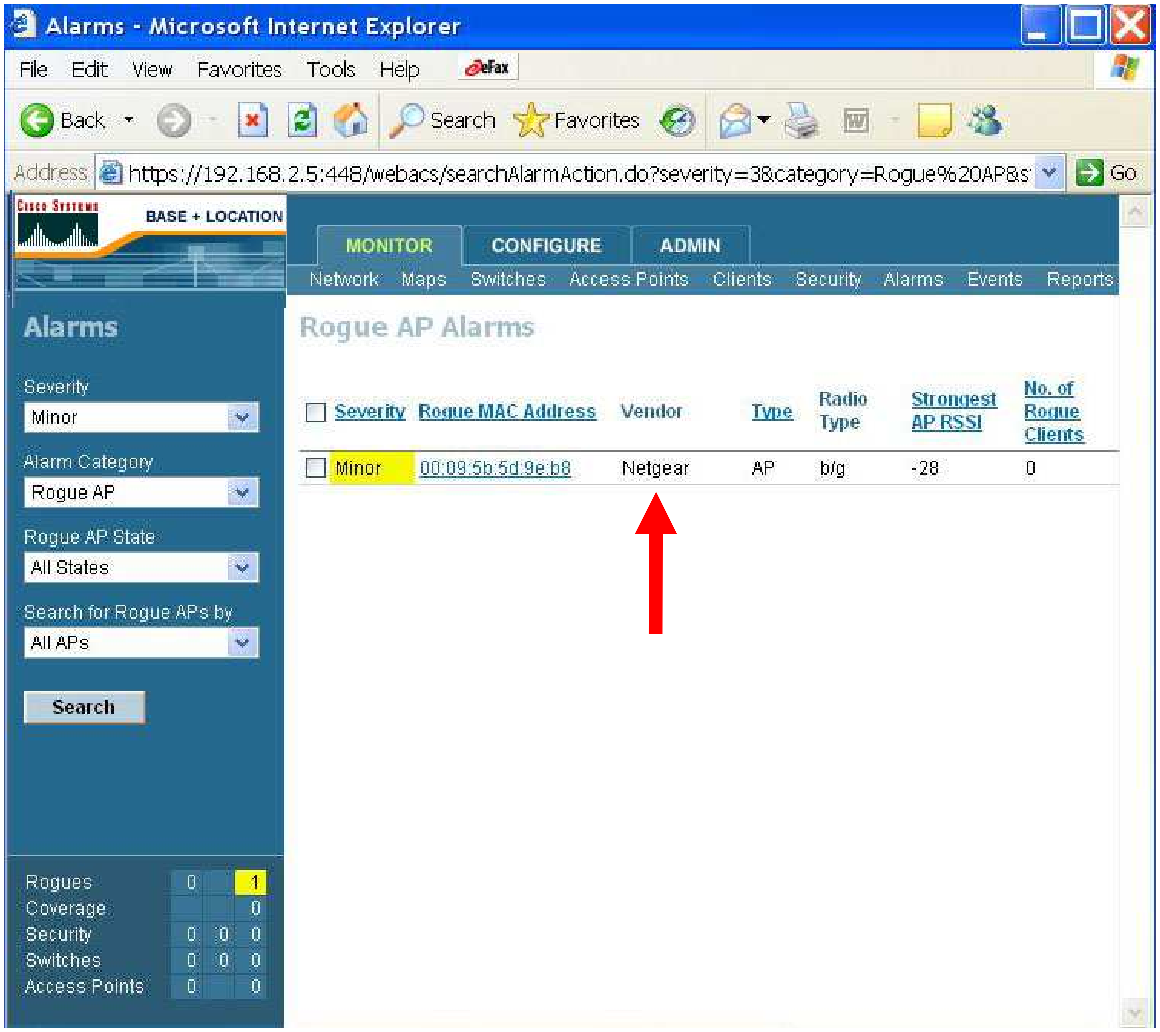
Maps > HQ > Engineering > Floor 1

Protocol: 802.11b/g
Display: Names
RSSI Cutoff: -75 dBm
RSSI Color Lookup: -35 dBm … -85 dBm
Zoom: 75 %

Contributing APs
☑ ap1
☑ ap2

Rogues	0	0
Coverage		0
Security	0 0	0

Show Rogue AP Alarm



Address: https://192.168.2.5:448/webacs/searchAlarmAction.do?severity=3&category=Rogue%20AP&s

Alarms

Severity: Minor

Alarm Category: Rogue AP

Rogue AP State: All States

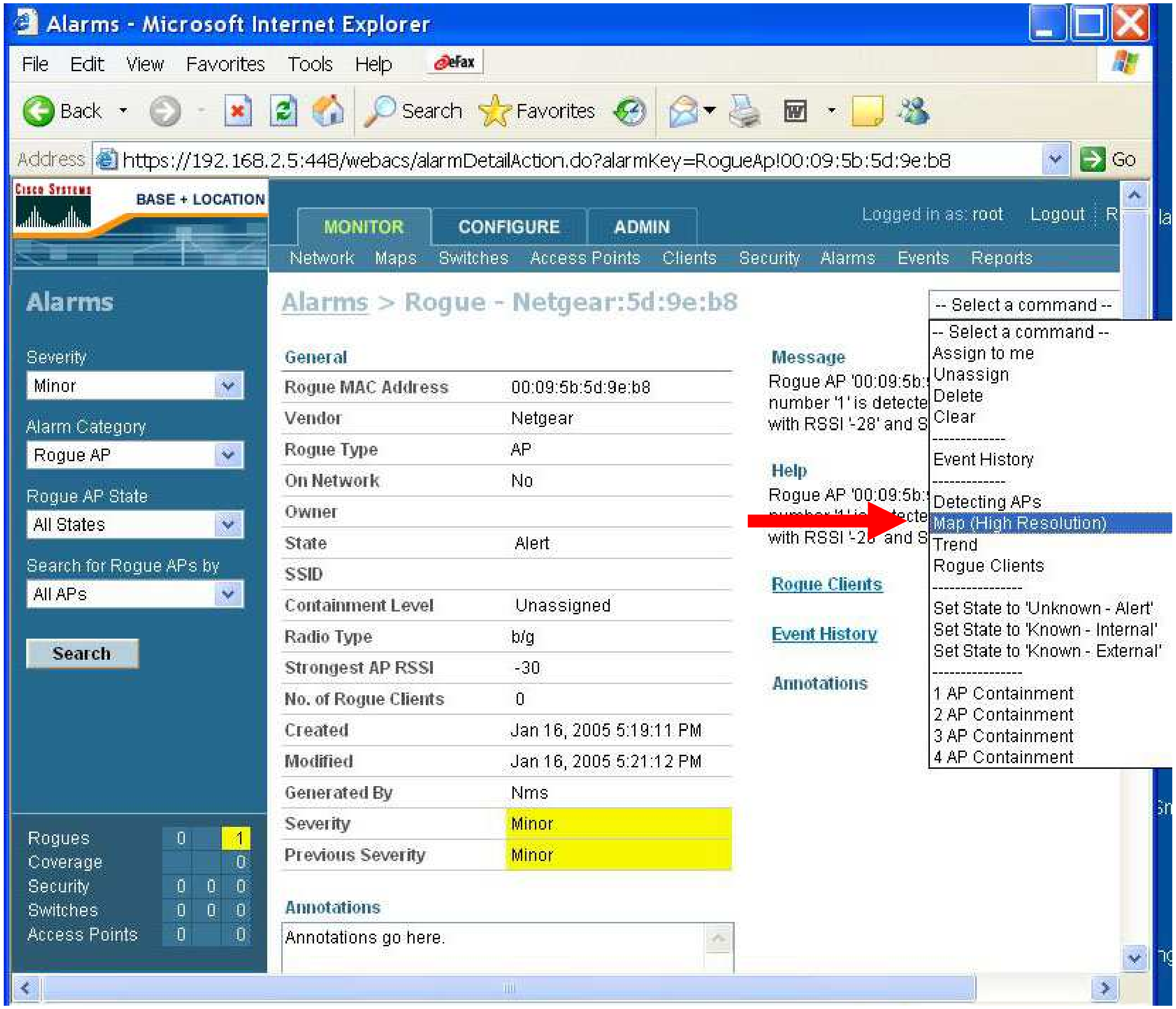
Search for Rogue APs by: All APs

Rogue AP Alarms

□ Severity	Rogue MAC Address	Vendor	Type	Radio Type	Strongest AP RSSI	No. of Rogue Clients
□ Minor	00:09:5b:5d:9e:b8	Netgear	AP	b/g	-28	0

Rogues	0		1
Coverage			0
Security	0	0	0
Switches	0	0	0
Access Points	0		0

Locate Rogue AP (High Resolution)



https://192.168.2.5:448/webacs/alarmDetailAction.do?alarmKey=RogueAp!00:09:5b:5d:9e:b8

Alarms

Severity: Minor

Alarm Category: Rogue AP

Rogue AP State: All States

Search for Rogue APs by: All APs

Rogues	0		1
Coverage			0
Security	0	0	0
Switches	0	0	0
Access Points	0		0

Alarms > Rogue - Netgear:5d:9e:b8

General	
Rogue MAC Address	00:09:5b:5d:9e:b8
Vendor	Netgear
Rogue Type	AP
On Network	No
Owner	
State	Alert
SSID	
Containment Level	Unassigned
Radio Type	b/g
Strongest AP RSSI	-30
No. of Rogue Clients	0
Created	Jan 16, 2005 5:19:11 PM
Modified	Jan 16, 2005 5:21:12 PM
Generated By	Nms
Severity	Minor
Previous Severity	Minor

Message

Rogue AP '00:09:5b:
number '1' is detecte
with RSSI '-28' and S

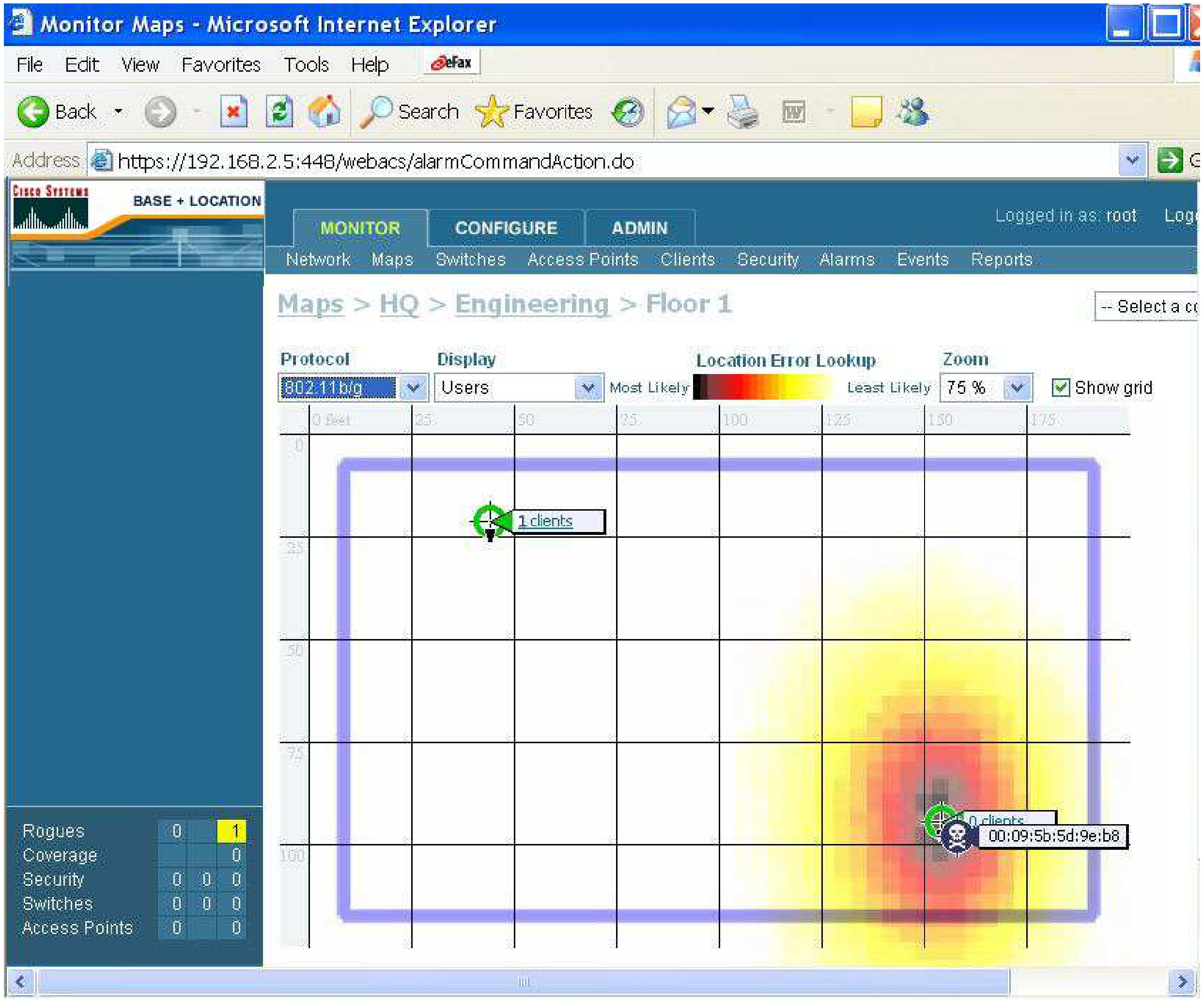
Help

Rogue AP '00:09:5b:
number '1' is detecte
with RSSI '-28' and S

Annotations

Annotations go here.

Map Rogue AP



Address: https://192.168.2.5:448/webacs/alarmCommandAction.do

Logged in as: root

Maps > HQ > Engineering > Floor 1

Protocol: 802.11b/g

Display: Users

Zoom: 75 %

☑ Show grid

1 clients

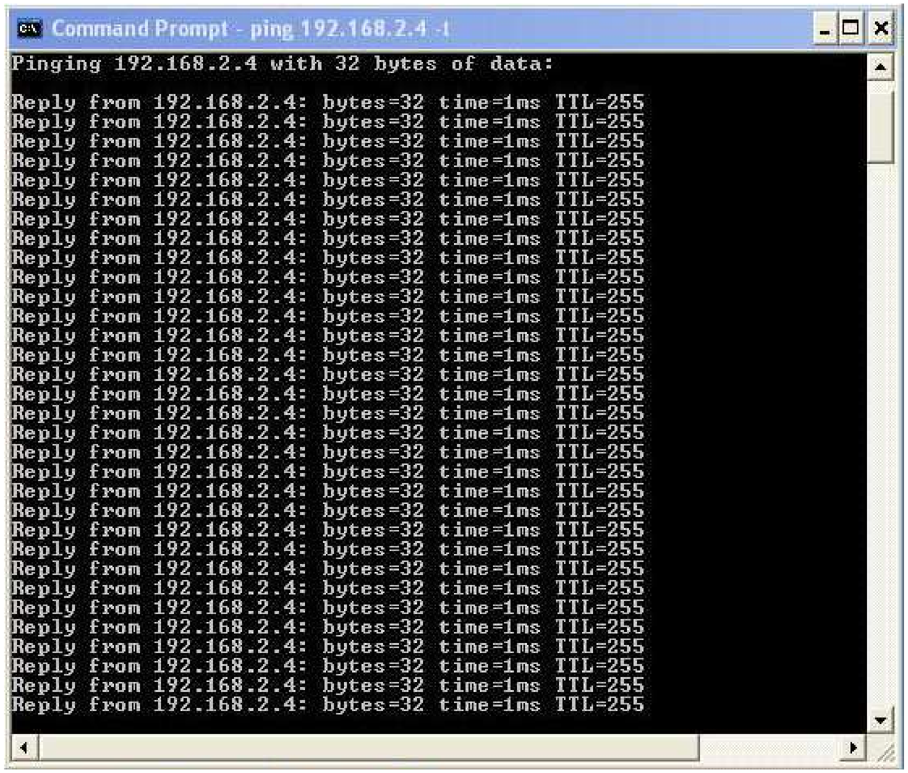
0 clients

00:09:5b:5d:9e:b8

Rogues	0		1
Coverage			0
Security	0	0	0
Switches	0	0	0
Access Points	0		0

Show Client Connection & Rogue Connection Up

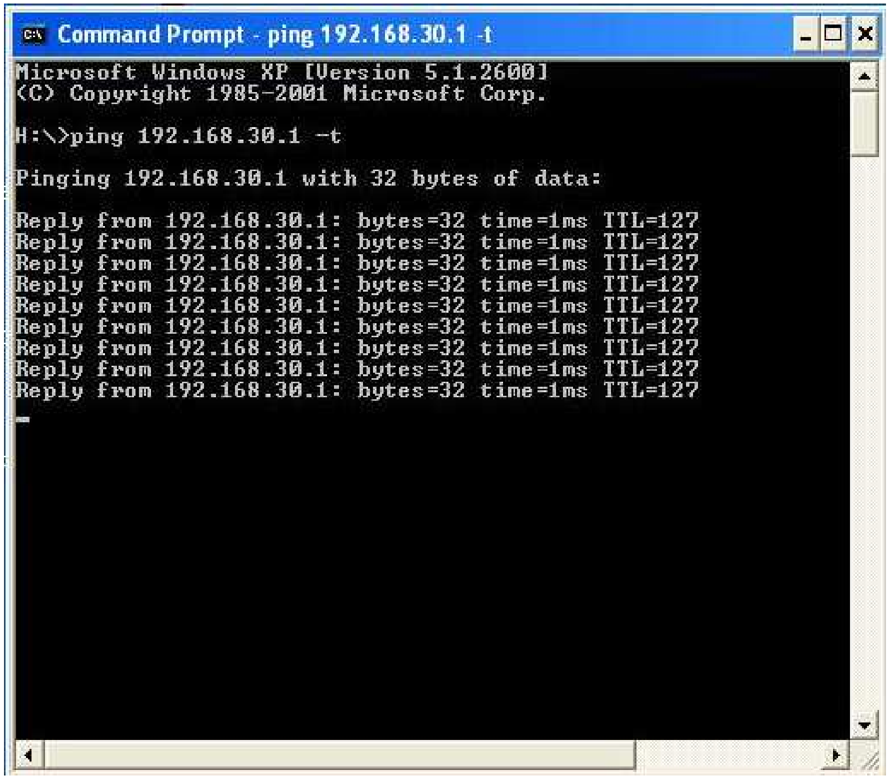
PC/1- Ping Cisco 2000 WLAN Controller 192.168.2.4



```
Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
```

PC/2 - Ping rogue AP/router 192.168.30.1



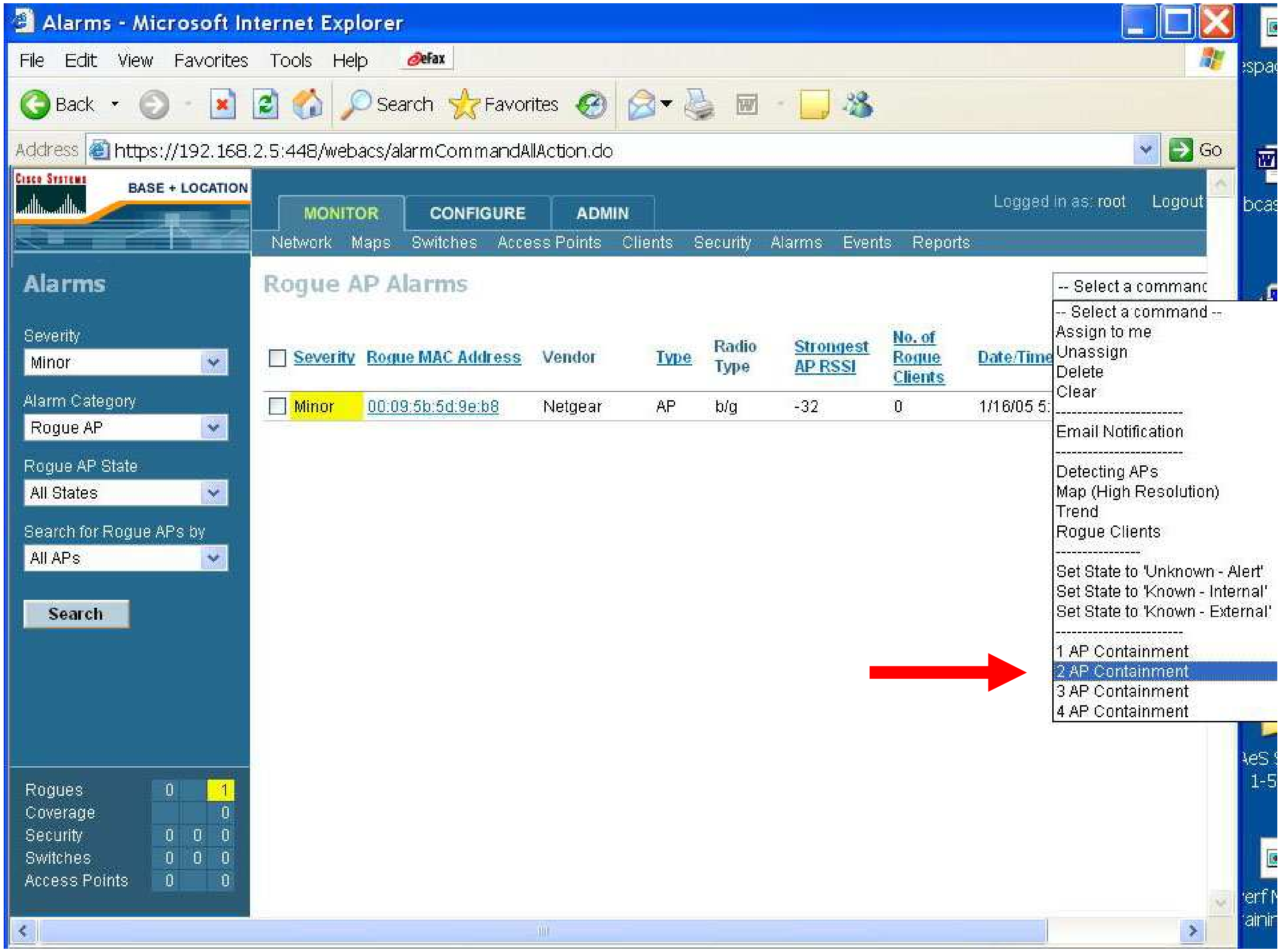
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

H:\>ping 192.168.30.1 -t

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
```

Show Manual Rogue Containment



Alarms - Microsoft Internet Explorer

Address https://192.168.2.5:448/webacs/alarmCommandAllAction.do

Logged in as: root

Alarms

Severity: Minor

Alarm Category: Rogue AP

Rogue AP State: All States

Search for Rogue APs by: All APs

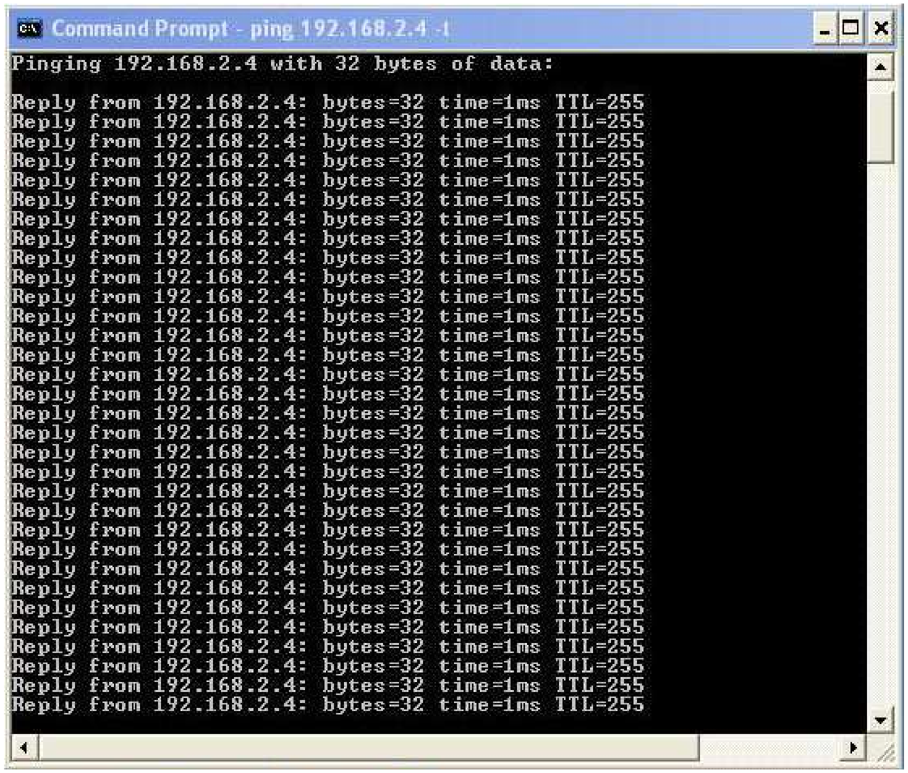
Rogues	0	1
Coverage		0
Security	0 0	0
Switches	0 0	0
Access Points	0	0

Rogue AP Alarms

☐ Severity	Rogue MAC Address	Vendor	Type	Radio Type	Strongest AP RSSI	No. of Rogue Clients	Date/Time
☐ Minor	00:09:5b:5d:9e:b8	Netgear	AP	b/g	-32	0	1/16/05 5:

Show Authorized Connected – Rogue Contained

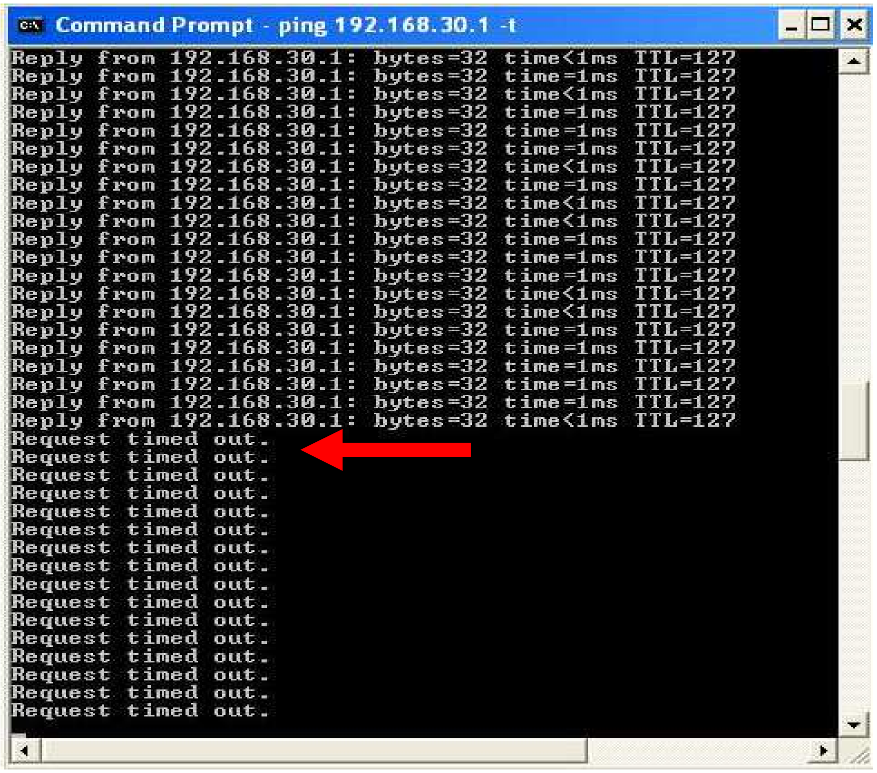
PC/1 – Still connected to Cisco 2000



```
Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
Reply from 192.168.2.4: bytes=32 time=1ms TTL=255
```

PC/2 – Rogue connection contained



```
Reply from 192.168.30.1: bytes=32 time<1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time<1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time<1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time<1ms TTL=127
Reply from 192.168.30.1: bytes=32 time<1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time<1ms TTL=127
Reply from 192.168.30.1: bytes=32 time<1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time<1ms TTL=127
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Agenda

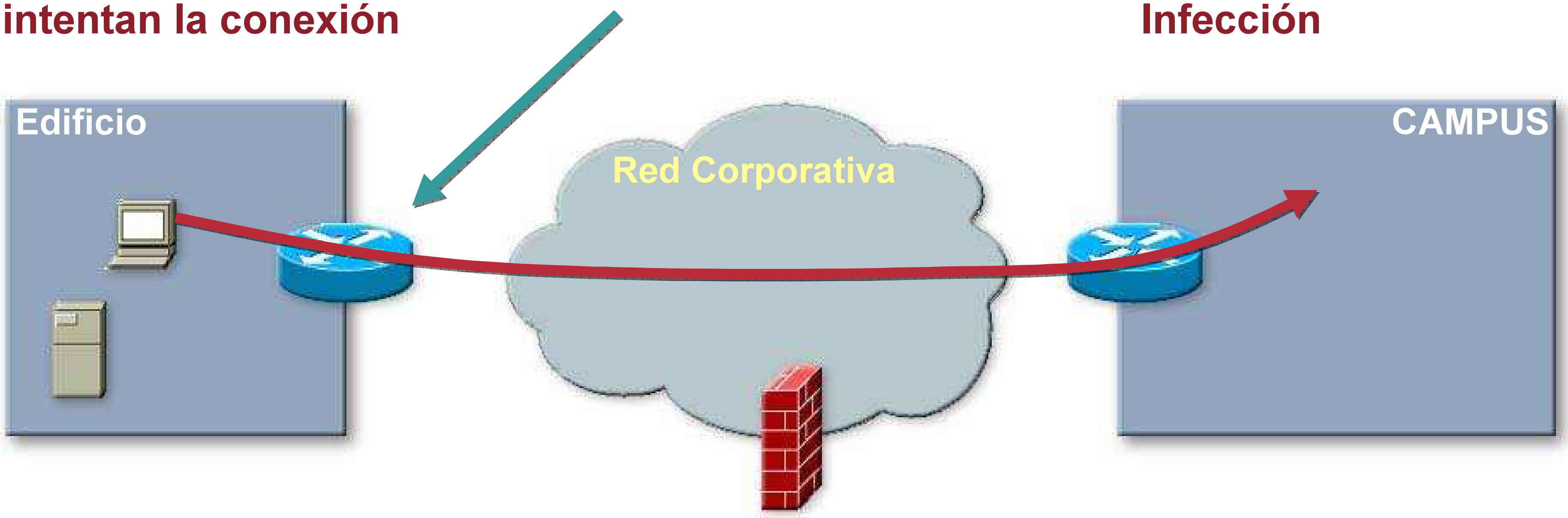
- WLAN Security Vulnerabilities and Threats
- WLAN Security Authentication and Encryption
- Wireless IDS
- Wireless NAC

¿Control de Admisión?

1. Clientes “Non-compliant” intentan la conexión

2. Conexión permitida

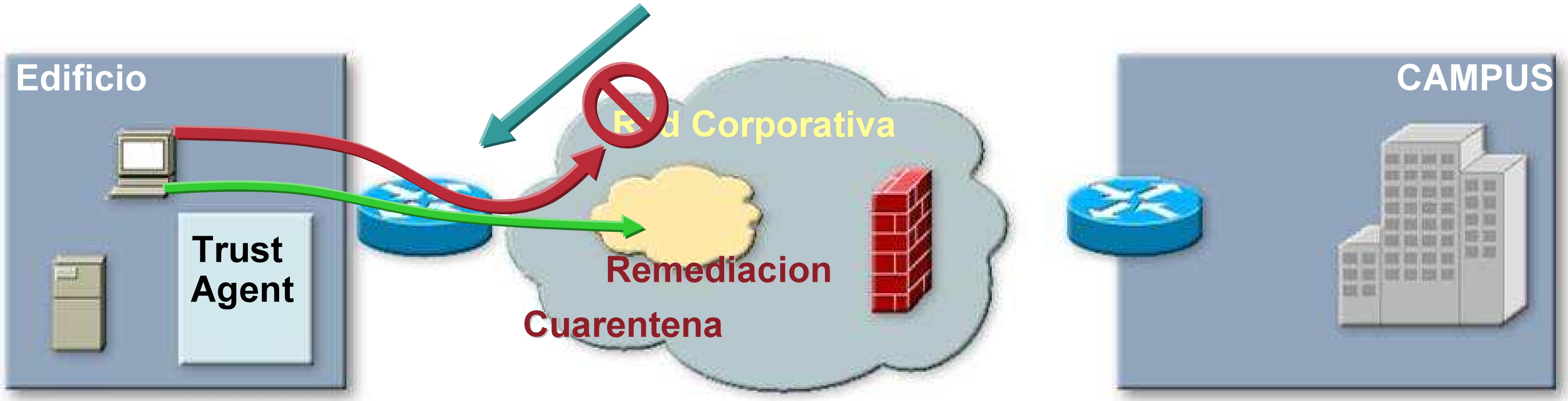
3. Extensión de la Infección



Control de Admisión:

Que hace

1. Clientes “Non-compliant” intentan la conexión
2. Cuarentena/ remediación
3. Contención de la infección



Cisco NAC : Dos modelos

NAC FRAMEWORK
Tradicional Cisco NAC

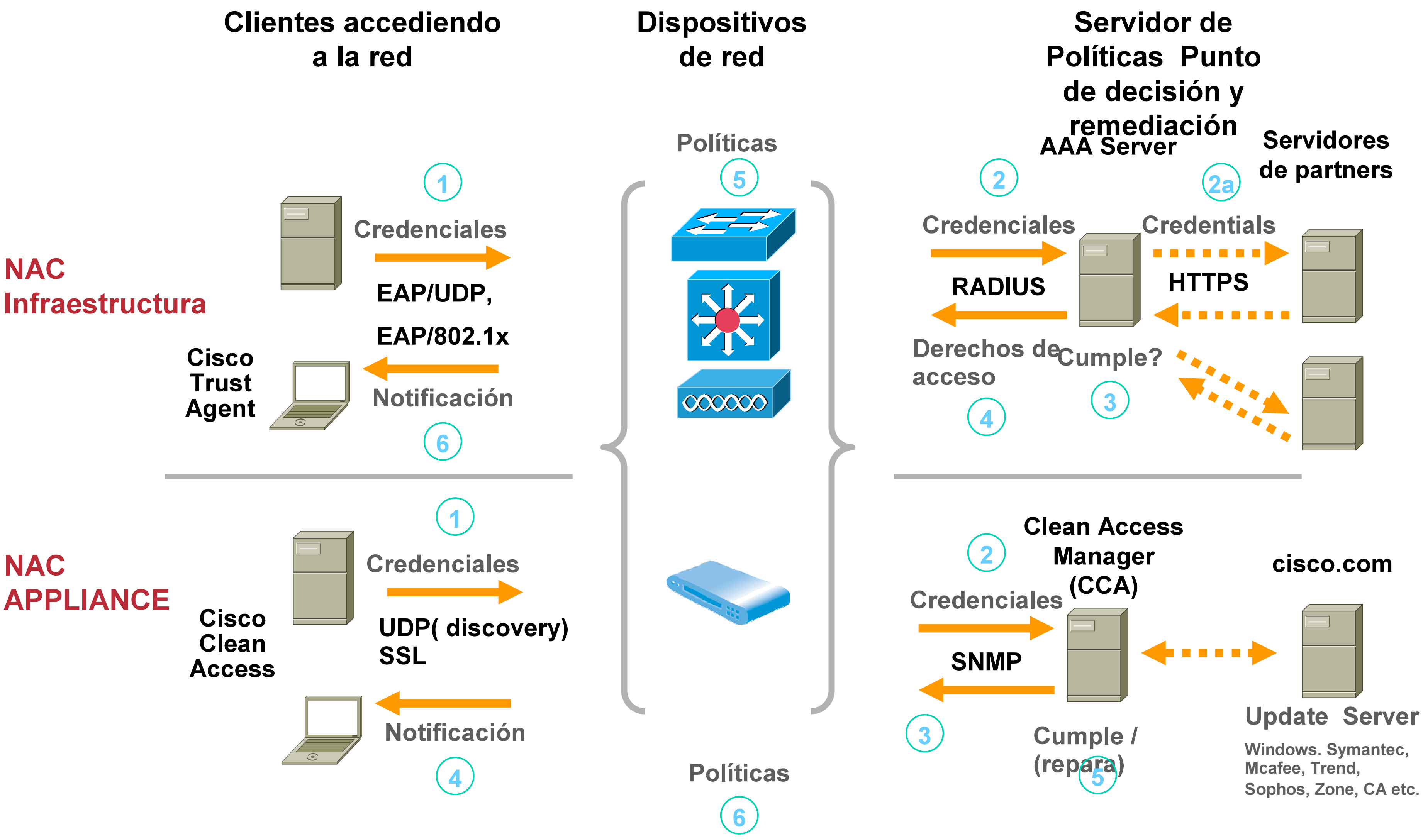
Solución integrada con todo el equipamiento Cisco

NAC APPLIANCE
Solución Cisco Clean Access

Solución autocontenida

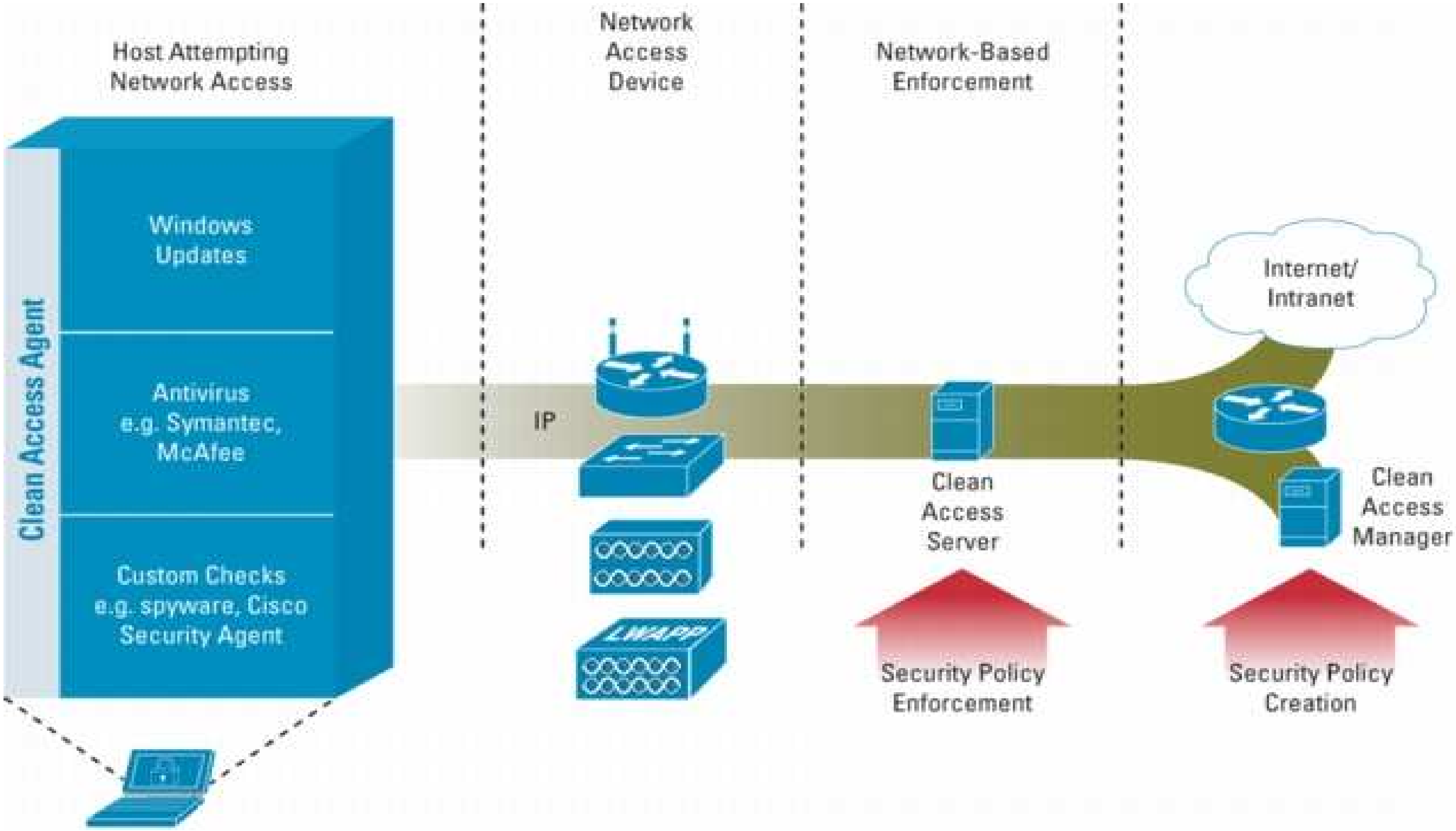
- **Aadaptación a las necesidades de cada cliente**

¿En que se diferencian?



NAC Appliance: Cisco Clean Access
Despliegue inalámbrico

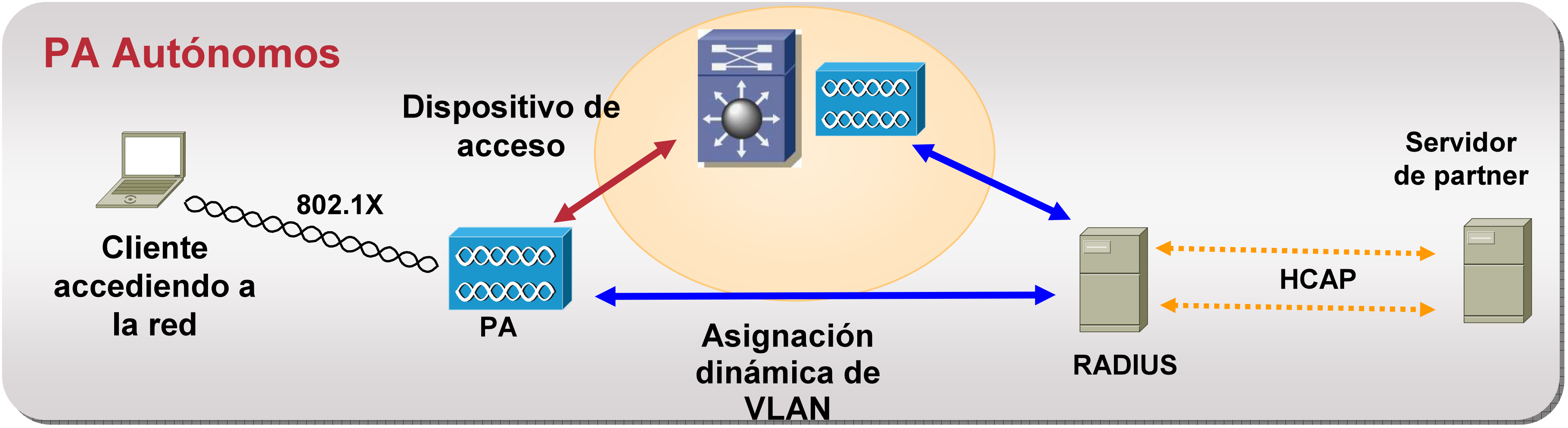
NAC Appliance Arquitectura en línea


Host Attempting Network Access
Network Access Device
Network-Based Enforcement
Clean Access Agent
Windows Updates
Antivirus e.g. Symantec, McAfee
Custom Checks e.g. spyware, Cisco Security Agent
IP
LWAPP
Clean Access Server
Internet/ Intranet
Clean Access Manager
Security Policy Enforcement
Security Policy Creation

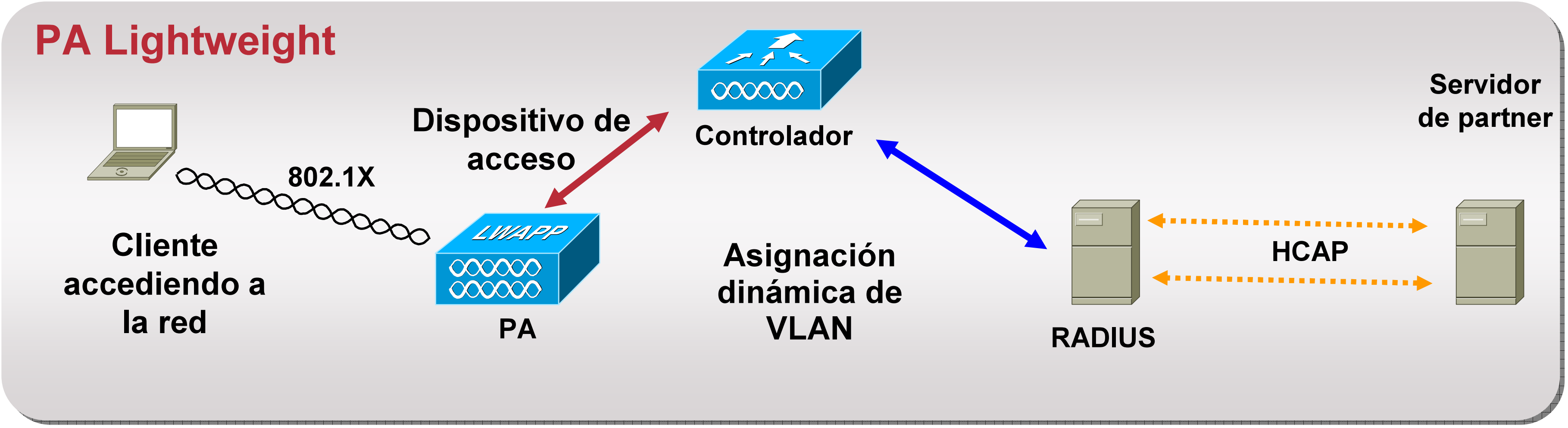
NAC Framework

Despliegue inalámbrico

PA Autónomos



PA Lightweight



Cisco Systems