

# Ch. 8 – Seguridad

Cisco Fundamentals of Wireless LANs version 1.2

Nora Sánchez  
ITESM CEM



# Introducción

## Objetivos del Capítulo

1. Fundamentos de seguridad
2. Tecnologías básicas de seguridad en WLAN
3. Configuración básica de seguridad en WLAN
4. Autenticación empresarial en WLAN
5. Cifrado empresarial en WLAN
6. Otros servicios empresariales de seguridad

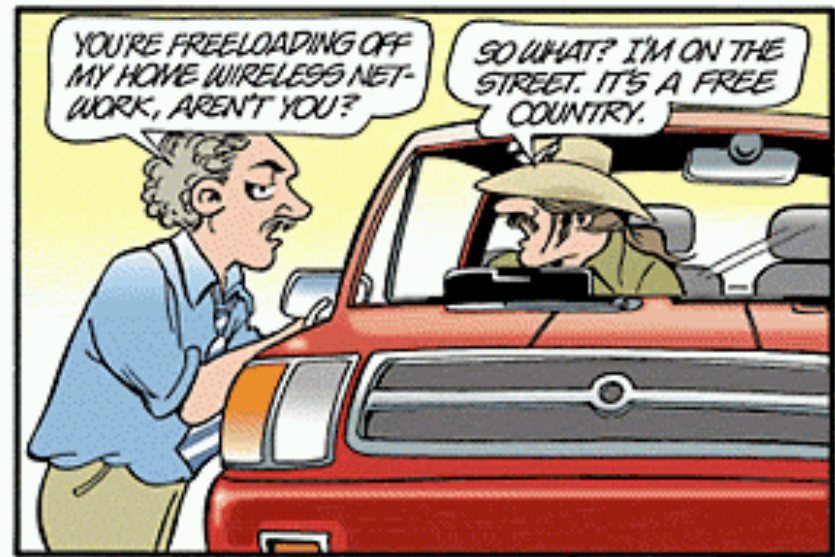
- ◆ **Las metas de la seguridad en redes** son mantener integridad, proteger confidencialidad y garantizar disponibilidad.
- ◆ El incremento exponencial de las redes, incluyendo tecnologías inalámbricas, ha incrementado los riesgos de seguridad.
- ◆ Muchos de estos riesgos se deben a *hacking* así como al uso inadecuado de recursos de red.

# Fundamentos de Seguridad



# ¿Qué es la seguridad?

- ◆ **Seguridad** usualmente se refiere a asegurar que los usuarios puedan realizar sólo las tareas a las que están autorizados y que puedan obtener sólo la información que tienen autorizada obtener



# ¿Qué es la seguridad?

## Balanceo entre

### Acceso transparente

- ◆ Conectividad
- ◆ Desempeño
- ◆ Facilidad de uso
- ◆ Administrable
- ◆ Disponibilidad

### Seguridad

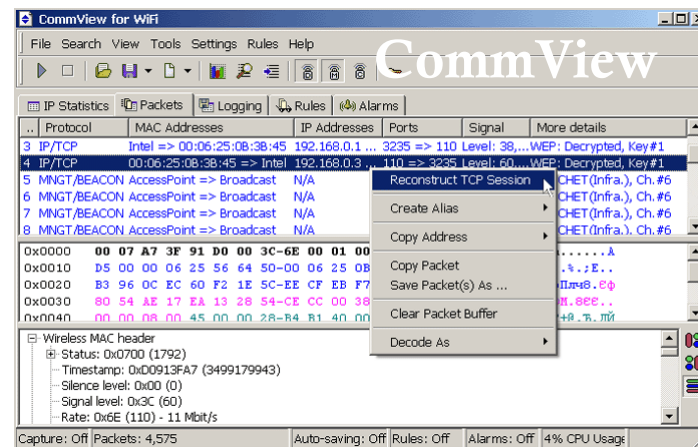
- ◆ Autenticación
- ◆ Autorización
- ◆ Contabilidad
- ◆ Certeza
- ◆ Confidencialidad
- ◆ Integridad de datos





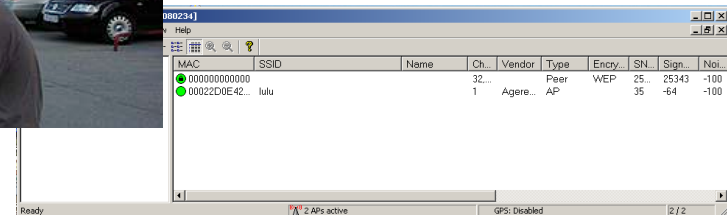
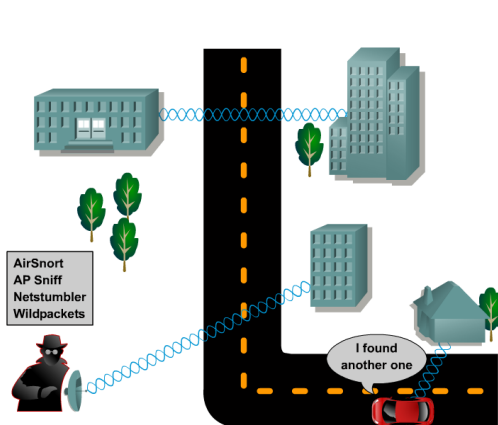
# Vulnerabilidades en WLANs

- WLANs son vulnerables a ataques especializados
  - Ataques que explotan las debilidades tecnológicas del estándar 802.11
  - Ataques a debilidades en la configuración
  - Muchos usuarios dejan los parámetros que ya vienen preconfigurados



# Amenazas a las WLANs

- Existen cuatro clases principales de amenazas a la seguridad inalámbrica:
  - Amenazas no estructuradas:
    - Individuos usan herramientas de *hackeo* ya disponibles
  - Amenazas estructuradas:
    - Hackers* altamente motivados y que son técnicamente competentes
  - Amenazas externas:
    - Lograr entrar a la red desde lugares externos
  - Amenazas internas:
    - Representan entre el 60 y 80% de incidentes reportados



# Fundamentos de Seguridad



- ◆ Los métodos de ataques a inalámbricas pueden descomponerse en tres categorías:
  - ◆ Reconocimiento
  - ◆ Ataque de acceso
  - ◆ Negación de Servicio (DoS)

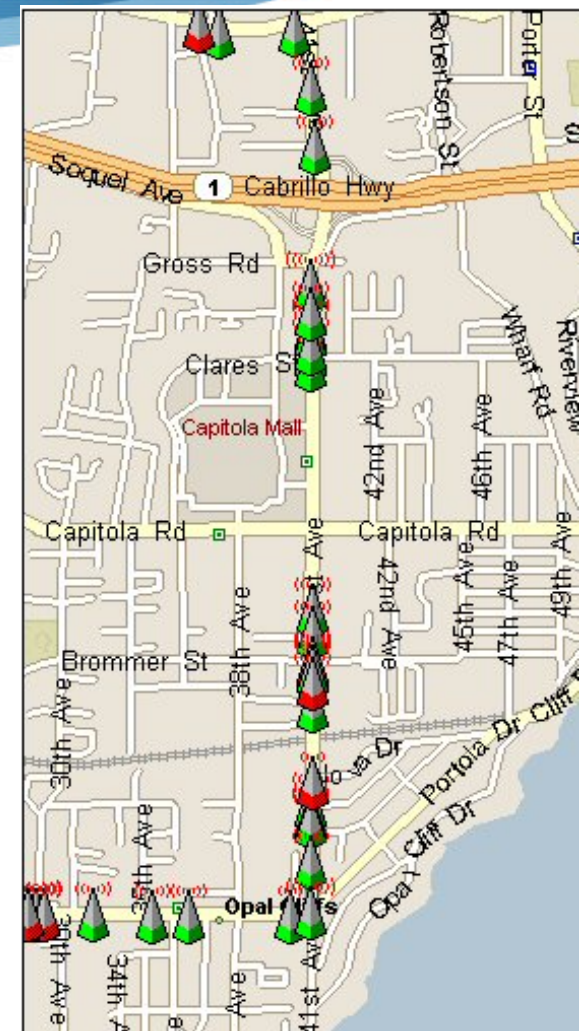
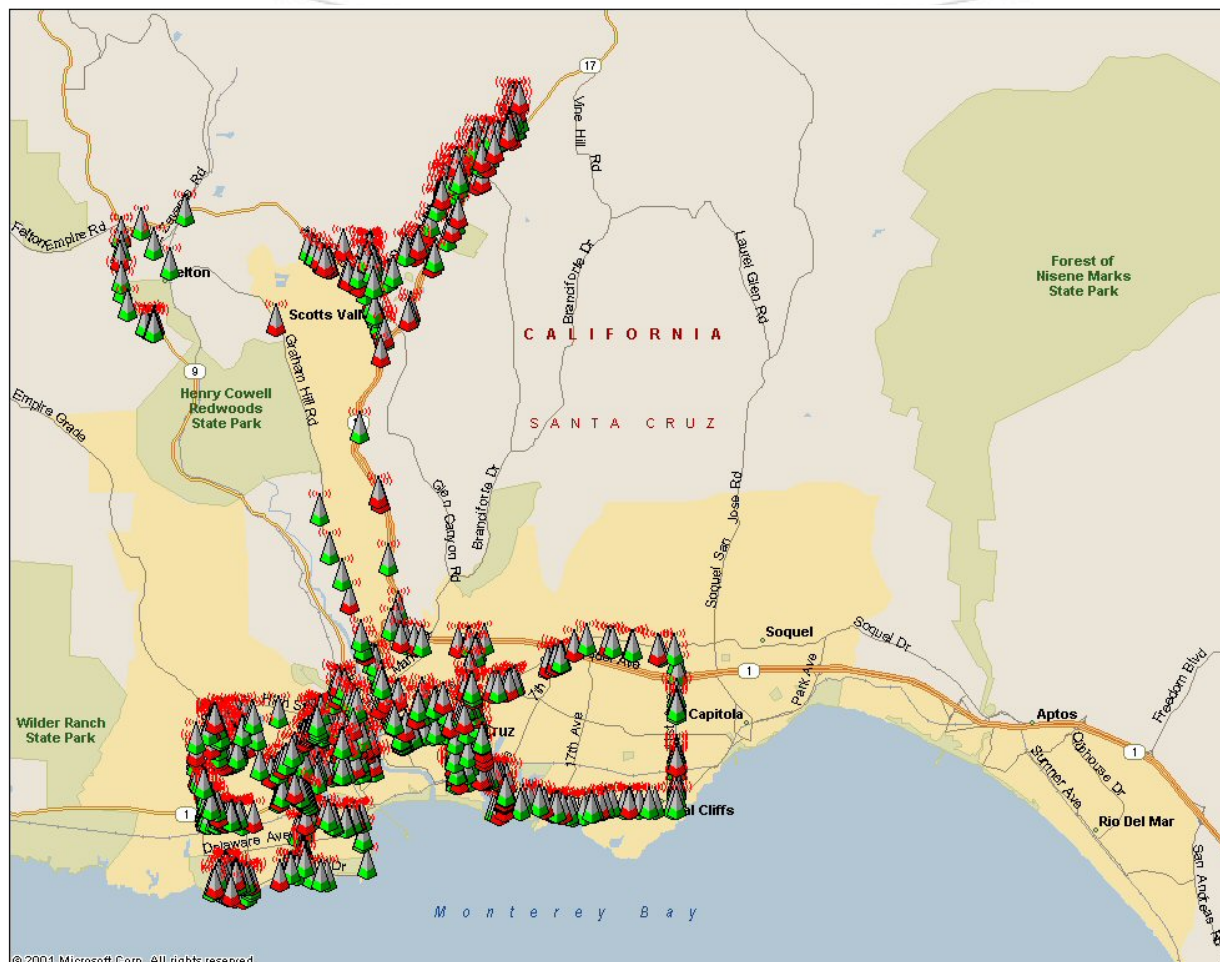


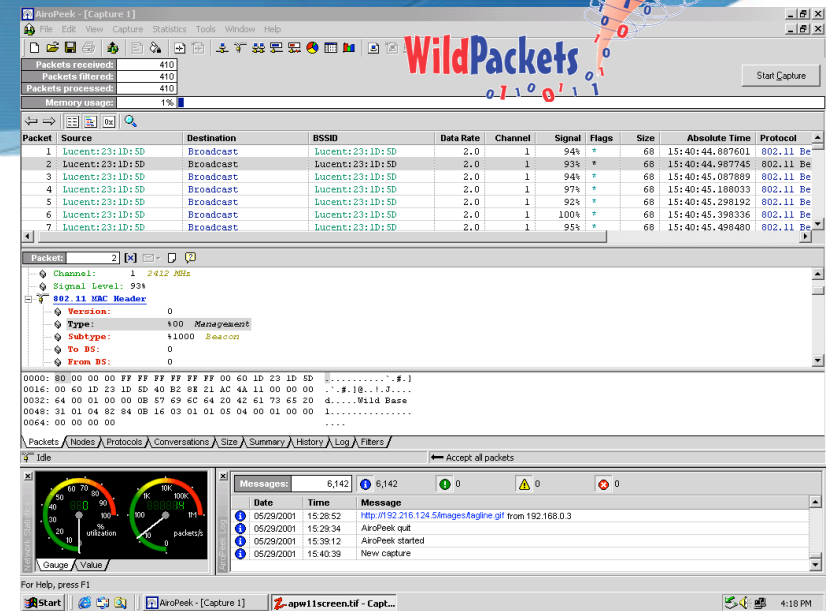
# Reconocimiento



- ◆ **Reconocimiento** es el descubrimiento no autorizado y mapeo de sistemas, servicios o vulnerabilidades.
  - ◆ No es usualmente ilegal más que sólo en algunos países.
- ◆ También conocido como recolección de información y usualmente precede a un ataque de acceso o de negación de servicio.
- ◆ También conocido como *wardriving*.

# Reconocimiento – Mapas de *Wardriving*





- Analizadores de protocolos comerciales:
  - AiroPeek (by WildPackets)
  - AirMagnet
  - Sniffer Wireless
  - **AirPCap**
- Analizadores de protocolos gratuitos:
  - Wireshark
  - Kismet
  - tcpdump
- Las utilerías pueden ser pasivas o activas



# Acceso

- Acceso al sistema es la habilidad de un intruso no autorizado a ganar acceso a un dispositivo para el cual el intruso no tenía una cuenta o password
- Usualmente involucra ejecutar un *script de hackeo* o una herramienta que explota vulnerabilidades conocidas del sistema o aplicación que está siendo atacada
- Incluye
  - Explotación de passwords débiles o no existentes
  - Explotación de servicios tales como HTTP, FTP, SNMP, CDP, y Telnet.

The screenshot shows the AirSnort application window. At the top, there's a menu bar with 'File', 'Edit', 'Settings', and 'Help'. Below the menu bar, there are several configuration fields: 'scan' (checked), 'channel' (set to 10), 'Network device' (set to eth1), 'Card type' (set to Orinoco (orinoco\_cs)), '40 bit crack breadth' (set to 11), and '128 bit crack breadth' (set to 1). Below these fields is a table with the following columns: C, BSSID, Name, WEP, Last Seen, Last IV, Chan, Packets, Encrypted, Interesting, PW: Hex, and PW: ASCII. The table contains two rows of data. The first row has 'X' in the 'C' column, '00:60:1D:1E:B5:5B' in 'BSSID', 'AENA pruebas' in 'Name', 'Y' in 'WEP', '5A:43:49' in 'Last Seen', '10' in 'Chan', '5432303' in 'Packets', '5344593' in 'Encrypted', '1520' in 'Interesting', '6D:65:6C:6F:6E' in 'PW: Hex', and 'melon' in 'PW: ASCII'. The second row has '00:60:1D:F0:BD:4A' in 'BSSID', 'AENA pruebas' in 'Name', 'Y' in 'WEP', '85:78:00' in 'Last Seen', '10' in 'Chan', '142255' in 'Packets', '25056' in 'Encrypted', '87' in 'Interesting', and empty fields for 'PW: Hex' and 'PW: ASCII'. At the bottom of the window, there are three buttons: 'Start', 'Stop', and 'Clear'. The 'AirSnort' logo is also visible in the bottom left corner.

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	PW: Hex	PW: ASCII
X	00:60:1D:1E:B5:5B	AENA pruebas	Y	5A:43:49		10	5432303	5344593	1520	6D:65:6C:6F:6E	melon
	00:60:1D:F0:BD:4A	AENA pruebas	Y	85:78:00		10	142255	25056	87		

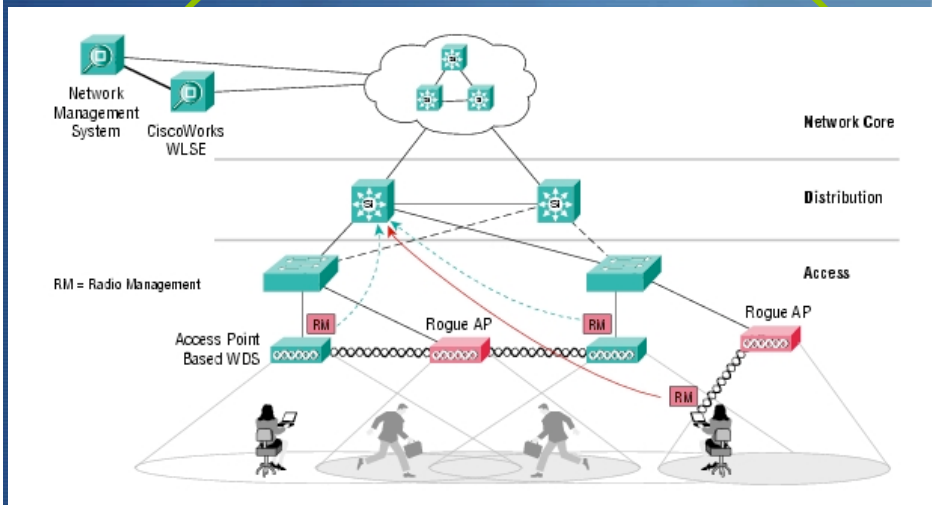


# Acceso – Ataque del AP pícaro

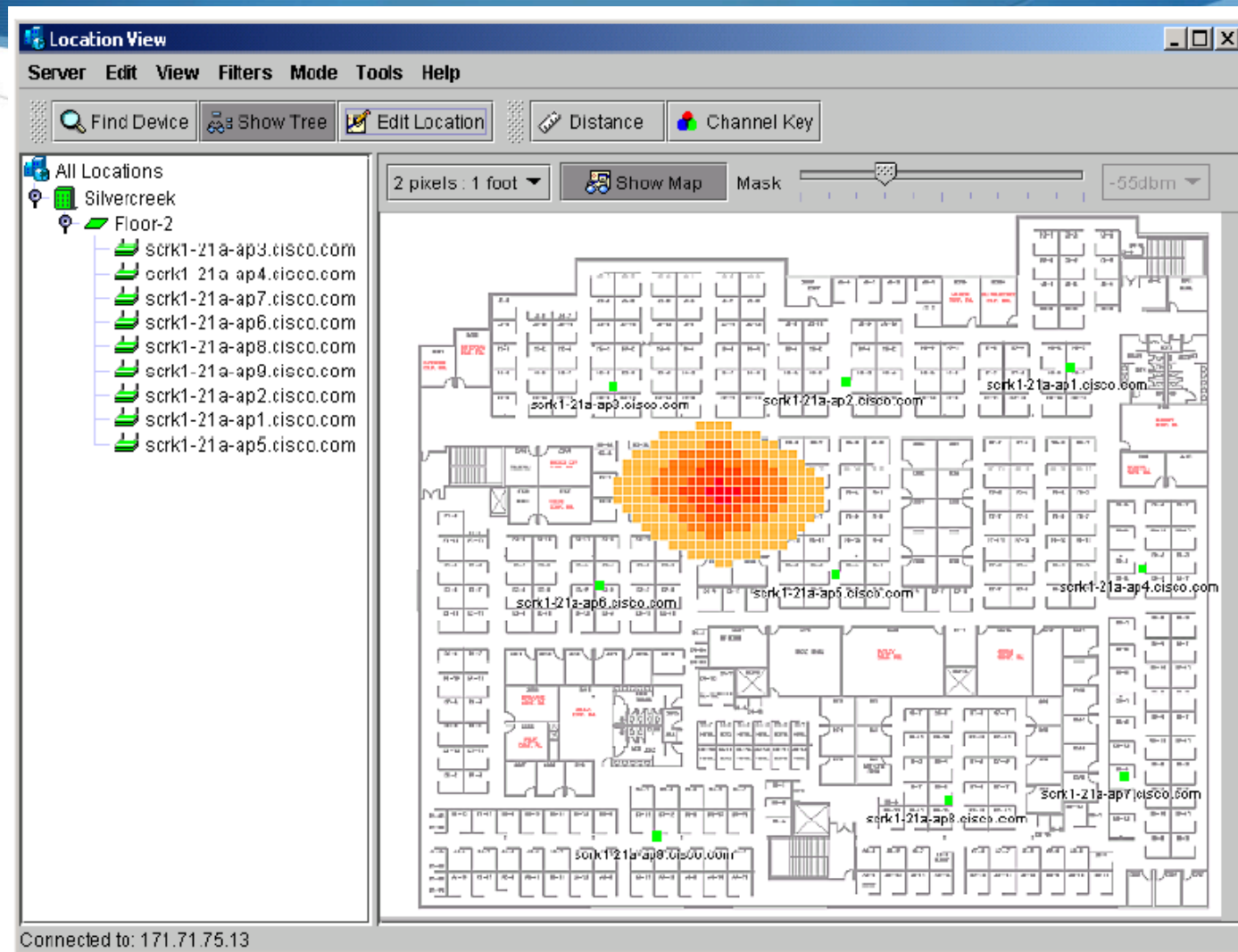
Muchos clientes se asociarán al AP de señal más fuerte. Si un AP no autorizado tiene una señal más fuerte, los clientes se asociarán a él.

El **AP pícaro** tendrá acceso al tráfico de red de todos los clientes asociados.

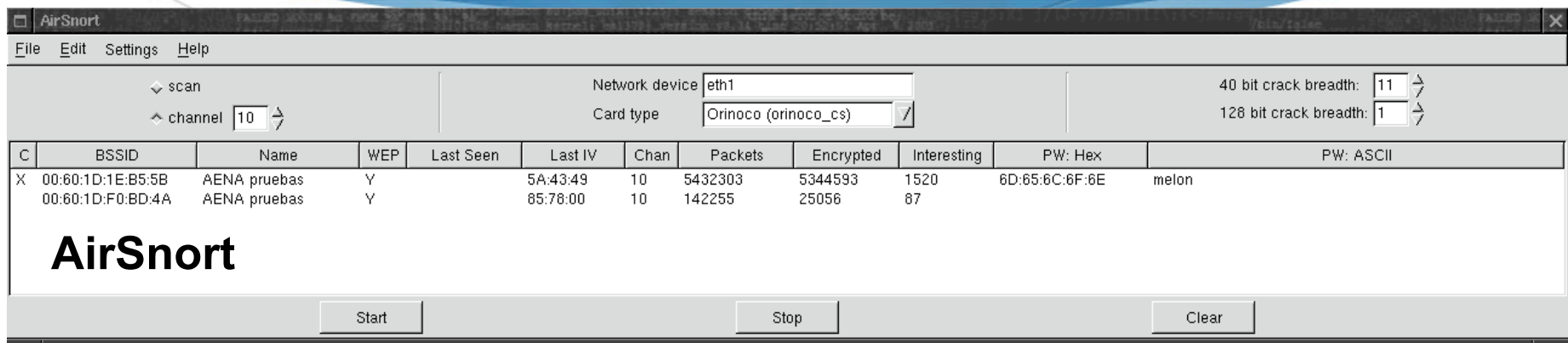
También puede utilizar ARP e IP spoofing para engañar a los clientes para que le envíen sus password o información confidencial.



# CiscoWorks WLSE detecta AP pícaros



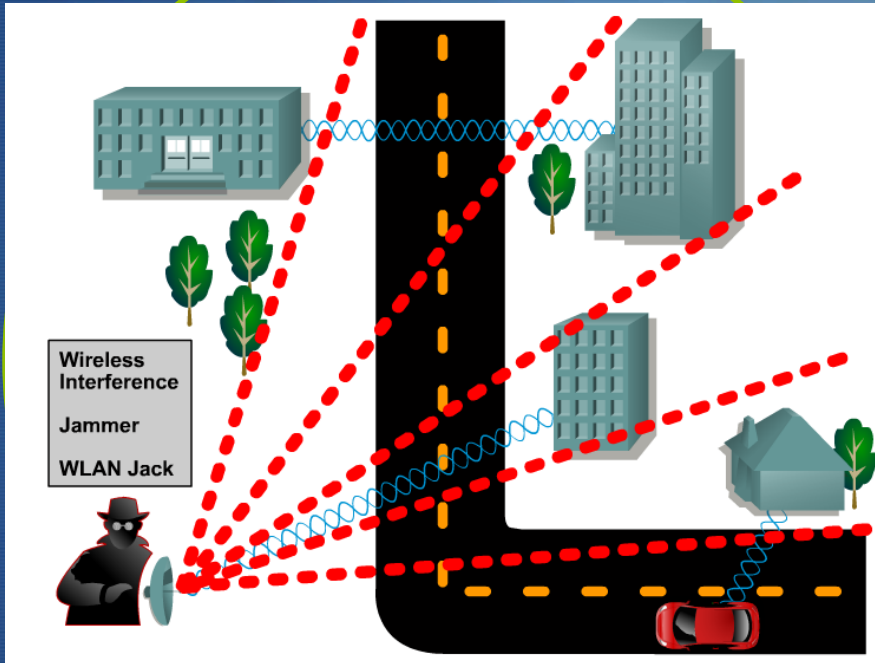
# Acceso – Ataques a Wired Equivalent Privacy (WEP)



- ◆ Ataques contra WEP incluyen:
  - ◆ Bit Flipping, Replay Attacks, y recolección de IV débiles
- ◆ Muchos ataques WEP attacks no han sido liberados del laboratorio pero se encuentran bien documentados
- ◆ AirSnort captura Vectores de Inicialización débiles para determinar la llave WEP que está siendo utilizada

# Negación de Servicio (DoS)

**DoS** es cuando un atacante deshabilita o corrompe las redes inalámbricas, sistemas o servicios, con la intención de negar el servicio a usuarios autorizados.





```
#./wlan_jack
Wlan Jack: 802.11b DOS attack.

Usage: ./wlan_jack -b <bssid> [ -v <victim address> ] [ -c <channel number> ] [
-i <interface name> ]
    -b:  bssid, the mac address of the access point (e.g. 00:de:ad:be:ef:00)
    -v:  victim mac address, defaults to broadcast address.
    -c:  channel number (1-14) that the access point is on, defaults to current.
    -i:  the name of the AirJack interface to use (defaults to aj0).

#./wlan_jack -b 00:06:25:53:cb:2c -c 1 -i aj0
Wlan Jack: 802.11 DOS utility.
```

Jacking Wlan...-█

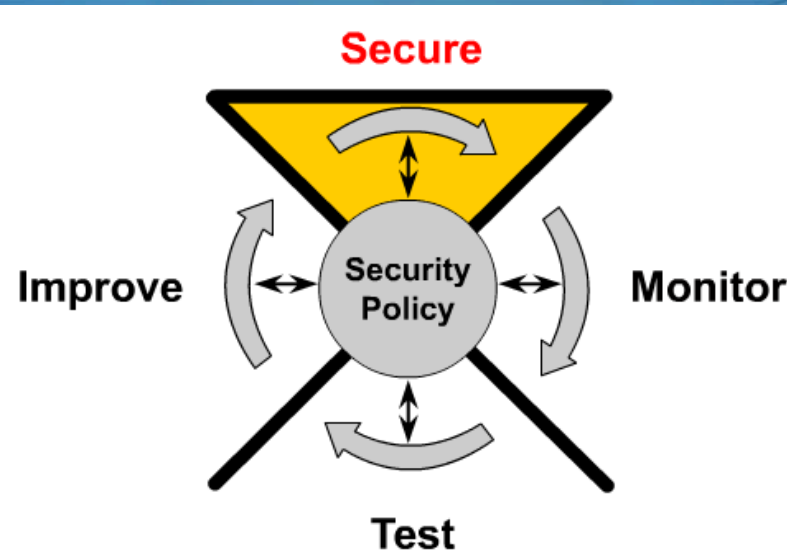
Source	Destination	BSSID	Data R...	Cha...	Signal	Flags	Size	Absolute Time	Protocol
00:40:96:58:37:AF	Broadcast	00:40:96:58:37:AF	1.0	1	70%	*	30	03:57:59.011112	802.11 Deauth
00:40:96:58:37:AF	Broadcast	00:40:96:58:37:AF	1.0	1	77%	*	30	03:57:59.011459	802.11 Deauth
00:07:85:92:1B:A9	Broadcast	Broadcast	1.0	1	90%	*	44	03:57:59.024358	802.11 Probe Req
00:40:96:58:37:AF	00:07:85:92:1B:A9	00:40:96:58:37:AF	1.0	1	98%	*	91	03:57:59.025430	802.11 Probe Rsp
	00:40:96:58:37:AF		1.0	1	100%	#	14	03:57:59.025739	802.11 Ack
00:07:85:92:1B:A9	Broadcast	Broadcast	1.0	1	100%	*	44	03:57:59.062400	802.11 Probe Req
00:40:96:58:37:AF	00:07:85:92:1B:A9	00:40:96:58:37:AF	1.0	1	98%	*	91	03:57:59.063523	802.11 Probe Rsp
	00:40:96:58:37:AF		1.0	1	100%	#	14	03:57:59.063758	802.11 Ack
00:40:96:58:37:AF	00:07:85:92:1B:A9	00:40:96:58:37:AF	1.0	1	88%	*	91	03:57:59.065134	802.11 Probe Rsp
00:07:85:92:1B:A9	Broadcast	Broadcast	1.0	1	81%	*	44	03:57:59.100279	802.11 Probe Req
00:40:96:58:37:AF	00:07:85:92:1B:A9	00:40:96:58:37:AF	1.0	1	96%	*	91	03:57:59.101339	802.11 Probe Rsp
00:40:96:58:37:AF	Broadcast	00:40:96:58:37:AF	1.0	1	79%	*	30	03:57:59.113531	802.11 Deauth
00:40:96:58:37:AF	Broadcast	00:40:96:58:37:AF	1.0	1	77%	*	30	03:57:59.113932	802.11 Deauth
00:07:85:92:1B:A9	Broadcast	Broadcast	1.0	1	72%	*	44	03:57:59.138173	802.11 Probe Req
00:40:96:58:37:AF	00:07:85:92:1B:A9	00:40:96:58:37:AF	1.0	1	79%	*	91	03:57:59.139230	802.11 Probe Rsp

- Wlan Jack, envía paquetes de des-asociación falsos, que desconectan a clientes 802.11 del punto de acceso.

# Tecnologías Básicas de Seguridad para WLAN



# El proceso de seguridad en WLAN



- Una **política de seguridad inalámbrica** efectiva trabaja para garantizar que los recursos de red de una organización se encuentran protegidos de sabotaje y de acceso inapropiado, lo que incluye acceso intencional o accidental.
- Todas las características de la seguridad inalámbrica debe ser configuradas de acuerdo a lo establecido en la política de seguridad de una organización.

# Primera generación de seguridad inalámbrica

## Métodos antiguos de seguridad en WLANs

SSID

Autenticación controlada por MAC

- ◆ Muchas WLANs utilizan el SSID como una forma básica de seguridad.
- ◆ Algunas WLANs controlan el acceso a través del filtrado de MAC



# AP: “Permitir cualquier SSID”

- ◆ Muchos APs tienen dos opciones
  - ◆ "SSID broadcast"
  - ◆ "Allow any SSID"
- ◆ Algunas vienen habilitadas de manera predeterminada para facilitar el establecimiento de la red inalámbrica
- ◆ "Allow any SSID"
  - ◆ habilita al AP para aceptar el acceso de un cliente que envía un SSID vacío
- ◆ "SSID broadcast"
  - ◆ Envía paquetes de señalización que contienen el SSID
- ◆ El deshabilitar estas opciones no garantiza la seguridad de la red. Un analizador de protocolos inalámbrico puede capturar un SSID válido de una red funcional
- ◆ SSIDs no deben ser utilizados como función de seguridad

# AP: "Allow any SSID"

350 Series Properties - [test]

System Parameters | RF Network | Advanced (Infrastructure) | Network Security

Client Name:

SSID1:

SSID2:

SSID3:

Power Save Mode: ☐ Wake Mode) ☐ Power Savings) ☐ Save Mode)

Network Type: ☐ Ad Hoc ☒ Infrastructure

Global Radio0-802.11B SSID Properties

Set Guest Mode SSID: tsunami

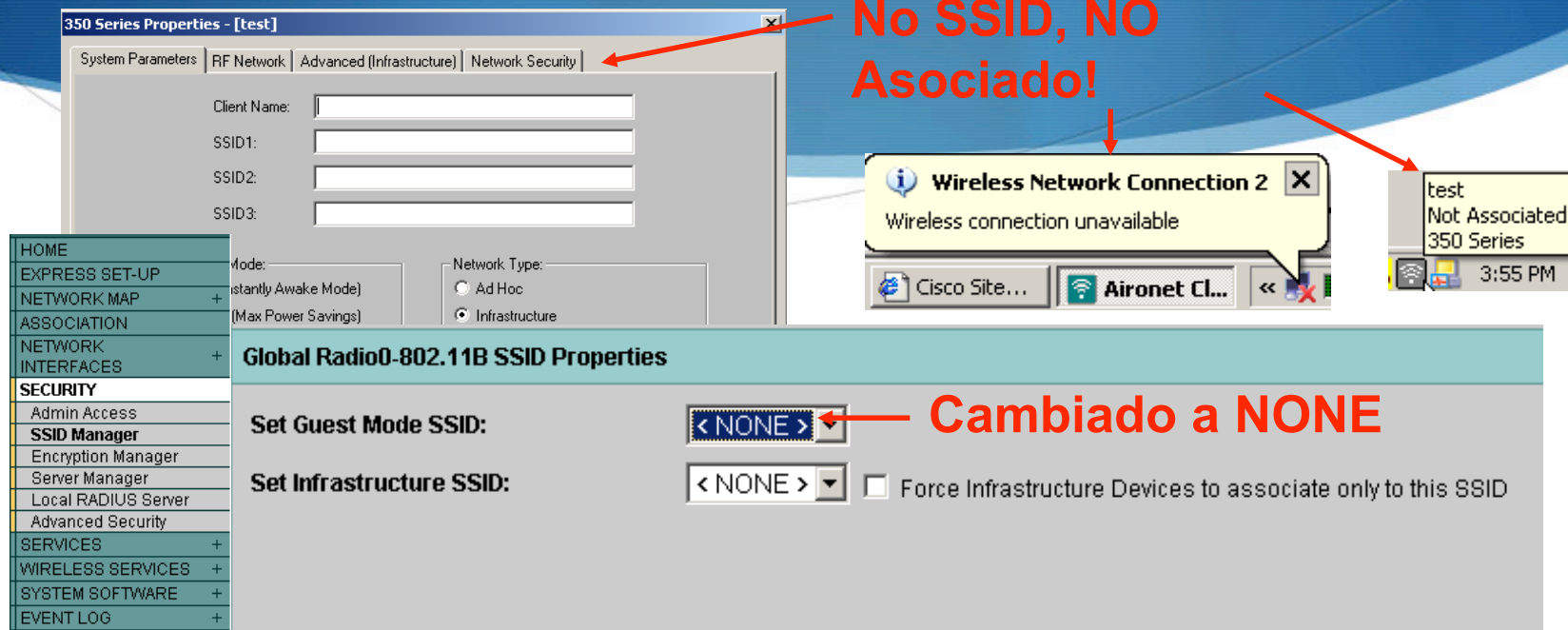
Set Infrastructure SSID: < NONE > ☐ Force Infrastructure Devices to associate only to this SSID

Wireless Network Connection 2 (tsunami)  
Speed: 11.0 Mbps  
Signal Strength: Excellent

test  
tsunami  
Associated  
Excellent  
11 Mbps  
350 Series  
192.168.1.100

- ◆ **Guest Mode SSID**
  - ◆ Si se quiere que el AP permita asociaciones de dispositivos cliente que no especifican un SSID en sus configuraciones, se puede establecer un guest SSID.
- ◆ El AP incluye el SSID en su señalización.
- ◆ Por default, el SSID predeterminado del AP, tsunami, se encuentra en guest mode.
- ◆ Para mantener la red segura, se deben deshabilitar los SSID en modo guest.

# AP: "Do NOT allow any SSID"



- Colocar el Guest Mode SSID en NONE, no permitirá asociar a clientes que no especifican un SSID.
- Recuerda, no es difícil obtener el SSID, así que esto no debe ser una medida de seguridad.
- El **siguiente paso** debe ser configurar WEP, WPA, u otra autenticación/ encriptación en el AP.
- No se puede tener el mismo SSID establecido como Guest Mode y autenticación/ encriptación.**

# Wired Equivalent Privacy (WEP)

The image shows two overlapping windows from a network configuration utility. The top window, labeled 'AP', is for configuring the Access Point. It has sections for 'Transmit Key' (with radio buttons for 'Encryption Key 1' and 'Encryption Key 2'), 'Encryption Key (Hexadecimal)' (with two input fields, the first containing ten dots), and 'Key Size' (a dropdown menu showing '40 bit', '40 bit' (highlighted), and '128 bit'). The bottom window, labeled 'ACU', is for configuring the Access Client Unit. It has a table for keys with columns 'Already Set?', 'Transmit Key', and 'WEP Key Size'. The first row is checked and has '40' selected. Below the table is a 'Key Entry Method' section with 'Hexadecimal (0-9, A-F)' selected. Both windows have 'OK', 'Cancel', and 'Help' buttons at the bottom.

Already Set ?	Transmit Key	WEP Key Size
<input checked="" type="checkbox"/>	WEP Key 1: <input type="text"/>	40 <input checked="" type="radio"/> 128 <input type="radio"/>
<input type="checkbox"/>	WEP Key 2: <input type="text"/>	<input type="radio"/> <input type="radio"/>
<input type="checkbox"/>	WEP Key 3: <input type="text"/>	<input type="radio"/> <input type="radio"/>
<input type="checkbox"/>	WEP Key 4: <input type="text"/>	<input type="radio"/> <input type="radio"/>

Key Entry Method: ☒ Hexadecimal (0-9, A-F) ☐ ASCII Text

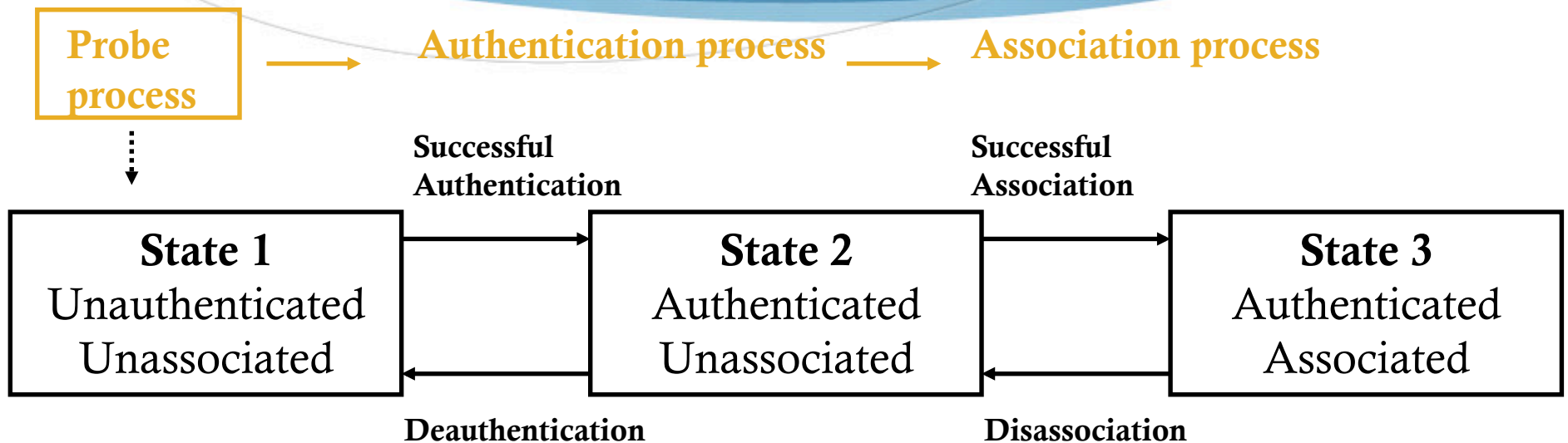
128 bit WEP es mejor conocido como 104 bit WEP.

La Llave 1 debe ser la misma en ambos equipos

- El estándar **IEEE 802.11** incluye WEP para proteger a usuarios autorizados de una WLAN de analizadores de protocolos
- El estándar IEEE 802.11 especifica una llave de 40-bit, para que WEP pueda ser exportado mundialmente.
- La mayoría de los fabricantes lo extendió a 128 bits o más.
- Cuando se **utiliza WEP**, tanto el cliente como el punto de acceso deben tener la misma llave WEP.
- WEP está basado en **Rivest Cipher 4 (RC4)**.



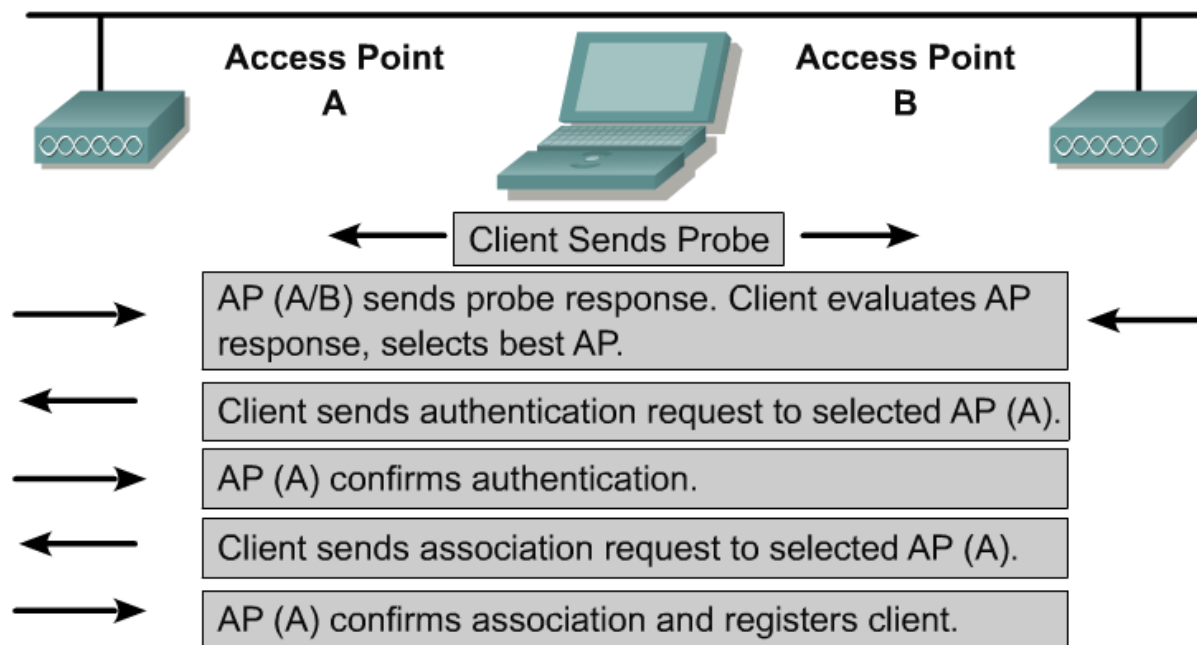
# Autenticación y asociación



- ◆ Métodos de autenticación definidos por el estándar:
  - ◆ Autenticación abierta
  - ◆ Autenticación por llave compartida

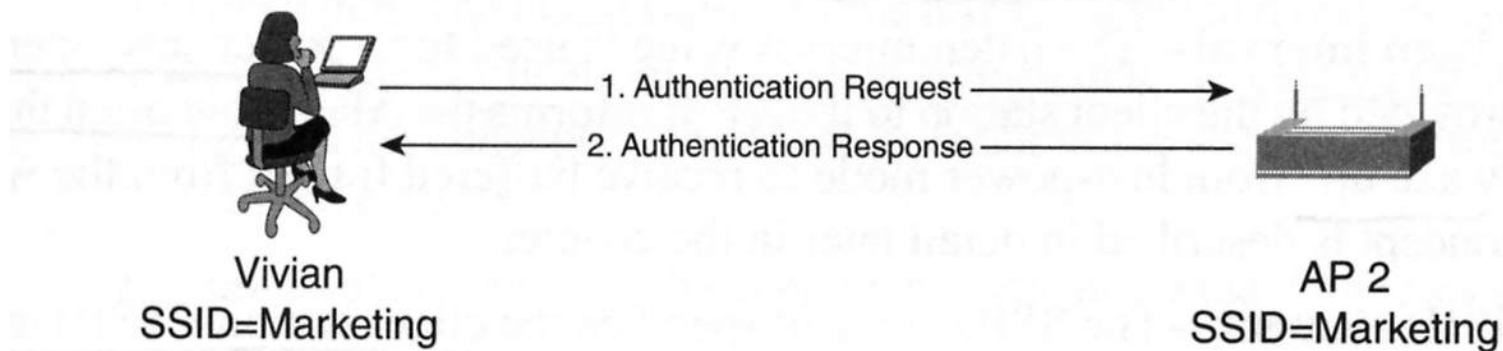
# Autenticación abierta

- Autenticación abierta = autenticación nula
- No hay verificación por parte de los dispositivos



# Proceso de autenticación (Repaso)

## *The Authentication Process*

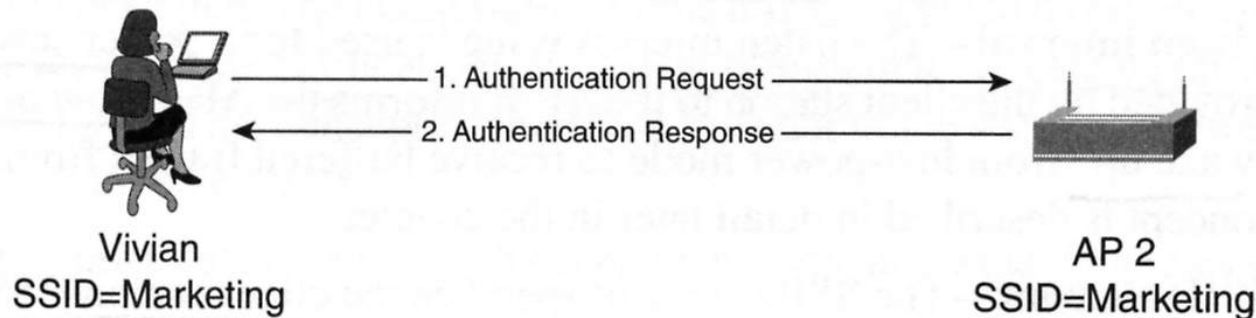


- ◆ En una red alambrada, la autenticación es proveída implícitamente por el cable físico de la PC al switch
- ◆ Autenticación es el proceso de asegurar que las estaciones intentando asociarse con ella red tienen permiso de hacerlo
- ◆ 802.11 especifica dos tipos de autenticación:
  - ◆ **Open-system**
  - ◆ Shared-key (utiliza WEP)

# Proceso de autenticación – Sistema abierto (repaso)

- ◆ Sistema de autenticación abierta = “no autenticación”
- ◆ Es el único método requerido por el estándar 802.11
- ◆ El cliente y la estación intercambian tramas de autenticación

## *The Authentication Process*



## *Frame Format of the Authentication Frame*

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Authentication Algorithm Numer Field	Authentication Transaction Sequence Numer Field	Status Code Field	Challenge Text IE (Optional)
---------------	----------	----	----	-------	------------------	--------------------------------------	---	-------------------	------------------------------



# Proceso de autenticación – Sistema abierto (Repaso)

- ◆ El cliente:
  - ◆ Coloca **Authentication Algorithm Number** en 0 (open-system)
  - ◆ Coloca **Authentication Transaction Sequence Number** en 1
- ◆ El AP:
  - ◆ Coloca **Authentication Algorithm Number** en 0 (open-system)
  - ◆ Coloca **Authentication Transaction Sequence Number** en 2
  - ◆ **Status Code** colocado en 0 (Successful)

Duration	= 213 (in microseconds)
Destination Address	= Station 0006D7863845
Source Address	= Station Aironet482745
Basic Service Set ID	= Aironet482745
Sequence Control	= 0x00B0
...Sequence Number	= 0x00B (11)
...Fragment Number	= 0x0 (0)
Authentication algorithm number = 0 (Open System)	
Authentication transaction sequence number = 2	
Status code	= 0 (Successful)

# Autenticación abierta

HOME
EXPRESS SET-UP
NETWORK MAP +
ASSOCIATION
NETWORK INTERFACES +
SECURITY
Admin Access
SSID Manager
Encryption Manager
Server Manager
Local RADIUS Server
Advanced Security
SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +

## Authentication Settings

### Methods Accepted:

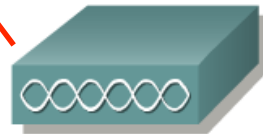
- ☒ Open Authentication: < NO ADDITION >
- ☐ Shared Authentication: < NO ADDITION >
- ☐ Network EAP: < NO ADDITION >

ASSOCIATION
NETWORK INTERFACES +
SECURITY
Admin Access
SSID Manager
Encryption Manager
Server Manager
Local RADIUS Server
Advanced Security
SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +

## Security: Encryption Manager - Radio0-802.11B

### Encryption Modes

- ☒ None
- ☐ WEP Encryption Optional
- ☐ Cipher WEP 128 bit
- Cisco Compliant TKIP Features:



- Autenticación abierta típica en AP y Cliente sin llaves WEP



350 Series Properties - [test]

System Parameters | RF Network | Advanced (Infrastructure) | Network Security

Network Authentication

☐ Wi-Fi Protected Access (WPA)

☒ None ☐ LEAP ☐ Host Based EAP (802.1x)

☐ Allow Fast Roaming (CKM)

☐ Allow Association to both WPA and non-WPA authenticators

Data Encryption

☒ None ☐ Static WEP ☐ TKIP ☐ Dynamic WEP

☐ Allow Association to Mixed Cells

Access Point Authentication

☒ Open ☐ Shared Key

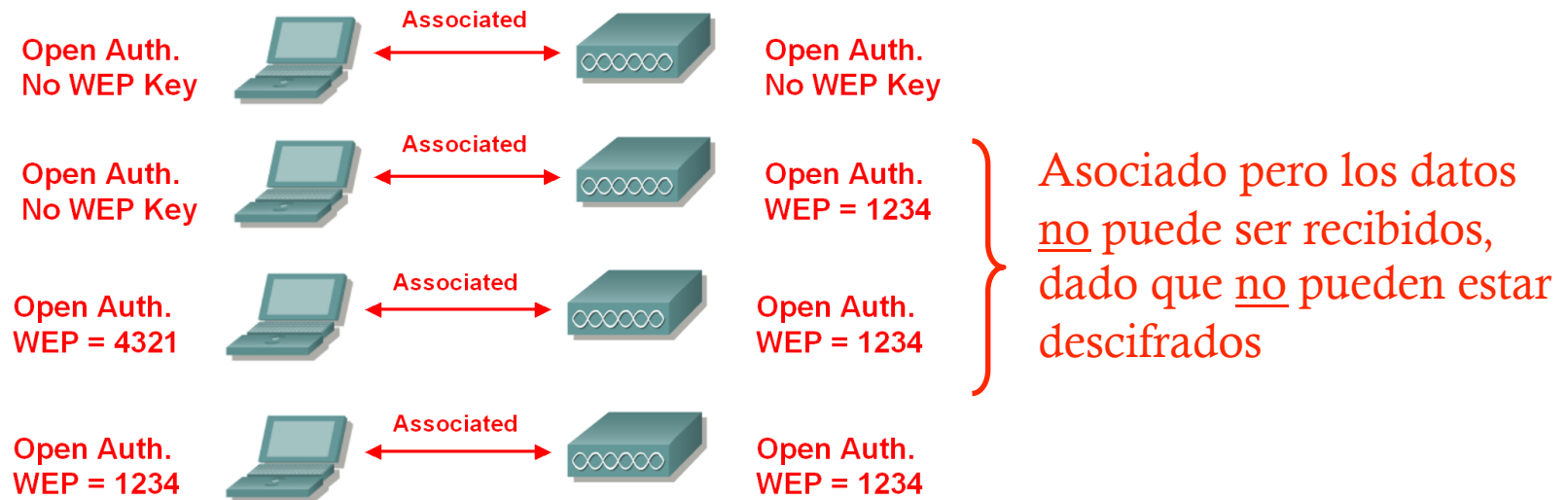
OK Cancel Help

# Autenticación abierta y WEP

- ◆ Recordemos los tres pasos para Asociación:
  - ◆ Escanéo
  - ◆ Autenticación
  - ◆ Asociación
- ◆ Un cliente se puede asociar con un AP, pero usamos WEP para enviar paquetes de datos cifrados
- ◆ Autenticación y encriptación de datos son dos cosas diferentes
  - ◆ Autenticación – ¿Tiene el cliente permiso para asociarse al AP?
  - ◆ Cifrado – Cifra los campos de datos (payload) e ICV (Integrity Check Value) de la MAC de 802.11, no los otros campos.
- ◆ Un cliente se puede asociar utilizando autenticación abierta, pero cifrar los datos intercambiados a través de WEP



# Autenticación abierta y WEP



- En algunas configuraciones, un cliente puede asociarse al AP y tener una llave WEP incorrecta o no tener una
  - El AP debe ser configurado para permitir esto.
- El encabezado no es cifrado con WEP solo la parte de datos



# Autenticación abierta – Cifrado WEP opcional (AP)

Association

Clients: 0Repeaters: 0

View: ☒ Client ☒ Repeater

Radio802.11B

SSID tsunami :

Device Type	Name	IP Address	MAC Address	State
-	-	192.168.1.103	0030.6520.d060	Associated

ASSOCIATION

NETWORK INTERFACES

SECURITY

Admin Access

SSID Manager

Encryption Manager

Server Manager

Local RADIUS Server

Advanced Security

SERVICES

WIRELESS SERVICES

SYSTEM SOFTWARE

EVENT LOG

Security: Encryption Manager - Radio0-802.11B

Encryption Modes

☐ None

☒ WEP Encryption 

Optional

Cisco Compliant TKIP Features: ☐ Enable MIC ☐ Enable Per Packet Keying

☐ Cipher 

WEP 128 bit

Encryption Keys

Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<div>••••••••••</div>	40 bit

HOME

EXPRESS SET-UP

NETWORK MAP

ASSOCIATION

NETWORK INTERFACES

SECURITY

Admin Access

SSID Manager

Encryption Manager

Server Manager

Local RADIUS Server

Advanced Security

SERVICES

WIRELESS SERVICES

SYSTEM SOFTWARE

EVENT LOG

Authentication Settings

Methods Accepted:

☒ Open Authentication: 

< NO ADDITION >

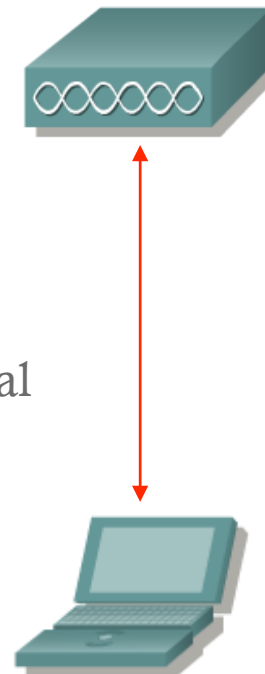
☐ Shared Authentication: 

< NO ADDITION >

☐ Network EAP: 

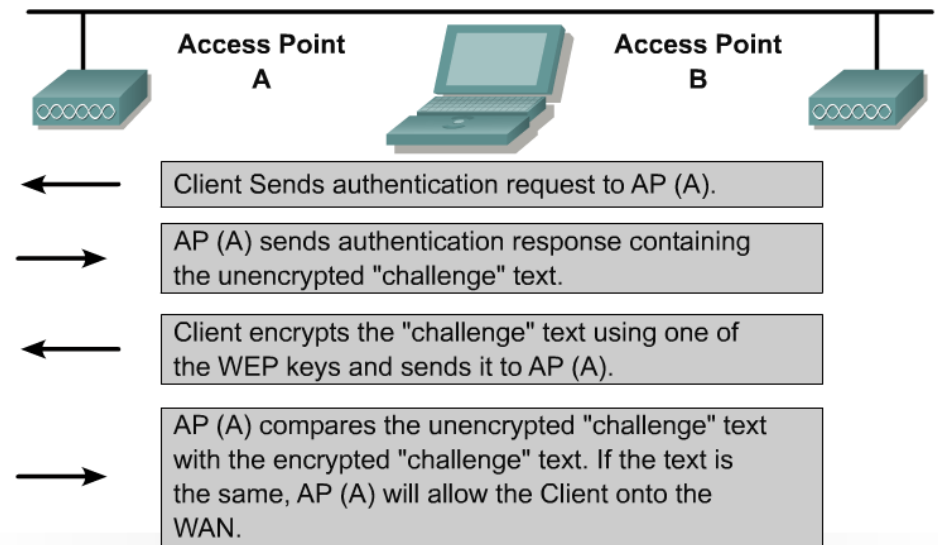
< NO ADDITION >

- 802.11 permite a los clientes asociarse a un AP.
- Cisco AP debe tener cifrado WEP como Opcional
- La asociación será exitosa si:
  - Llave WEP igual
  - Llave WEP no igual
  - No llave WEP



# Proceso de autenticación – llave compartida

- **Llave compartida** requiere que el cliente y el punto de acceso compartan una misma llave WEP
- Un AP utilizando autenticación con llave compartida envía un texto *challenge* hacia el cliente
- Si el cliente no tiene o tiene la llave incorrecta fallará el proceso de autenticación
- El cliente no podrá asociarse al AP.



# Proceso de autenticación – Llave compartida (Repaso)

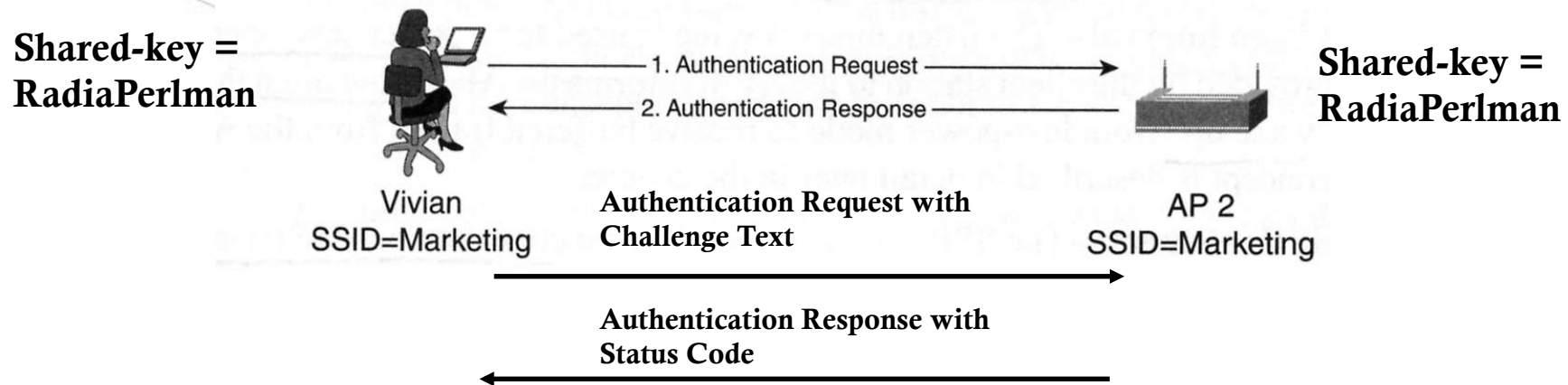
*Frame Format of the Authentication Frame*

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Authentication Algorithm Numer Field	Authentication Transaction Sequence Numer Field	Status Code Field	Challenge Text IE (Optional)
---------------	----------	----	----	-------	------------------	--------------------------------------	---	-------------------	------------------------------

- Utiliza WEP (Wired Equivalent Privacy) y sólo puede ser utilizado por productos que soporten WEP
- 802.11 requiere que todas las estaciones que soporten WEP también soporten autenticación por llave compartida

# Proceso de autenticación – Llave compartida (Repaso)

*The Authentication Process*



- WEP es un algoritmo de cifrado, no un método de autenticación
- Autenticación con llave compartida utiliza WEP y sólo puede ser utilizado en clientes y APs que implementen WEP
- Requiere que una llave sea distribuida a todos los clientes

# Proces de autenticación – Llave compartida (Repaso)

*Frame Format of the Authentication Frame*

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Authentication Algorithm Numer Field	Authentication Transaction Sequence Numer Field	Status Code Field	Challenge Text IE (Optional)
---------------	----------	----	----	-------	------------------	--------------------------------------	---	-------------------	------------------------------

- ◆ El cliente:
  - ◆ Coloca Authentication Algorithm Number en 1 (shared-key)
  - ◆ Coloca Authentication Transaction Sequence Number en 1
- ◆ El AP:
  - ◆ Coloca Authentication Algorithm Number en 1 (shared-key)
  - ◆ Coloca Authentication Transaction Sequence Number en 2
  - ◆ Status Code en 0 (Successful)
  - ◆ Challenge Text
- ◆ El cliente:
  - ◆ Coloca Authentication Algorithm Number en 1 (shared-key)
  - ◆ Coloca Authentication Transaction Sequence Number en 3
  - ◆ Challenge Text
- ◆ El AP:
  - ◆ Coloca Authentication Algorithm Number en 1 (shared-key)
  - ◆ Coloca Authentication Transaction Sequence Number en 4
  - ◆ Status Code en 0 (Successful)



# Proceso de autenticación

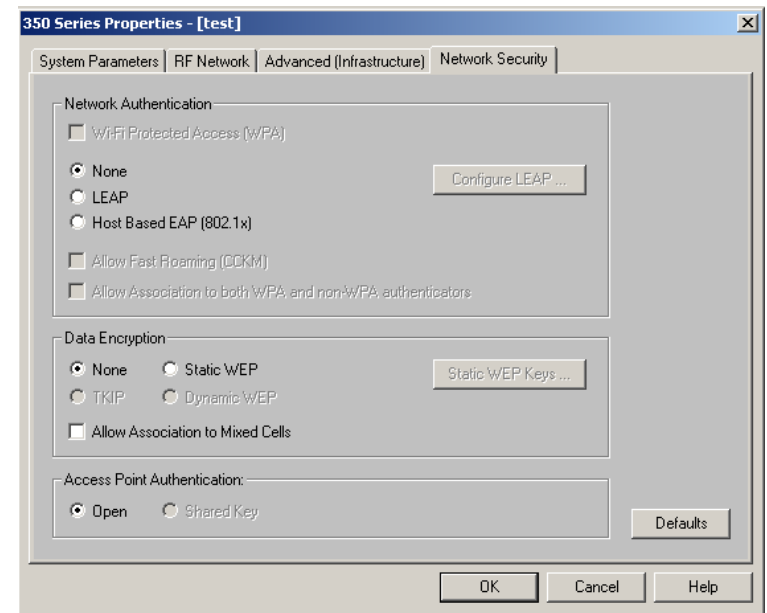
- Autenticación
  - Open-System
  - Shared-Key (WEP)

Cifrado

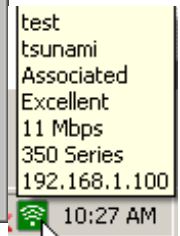
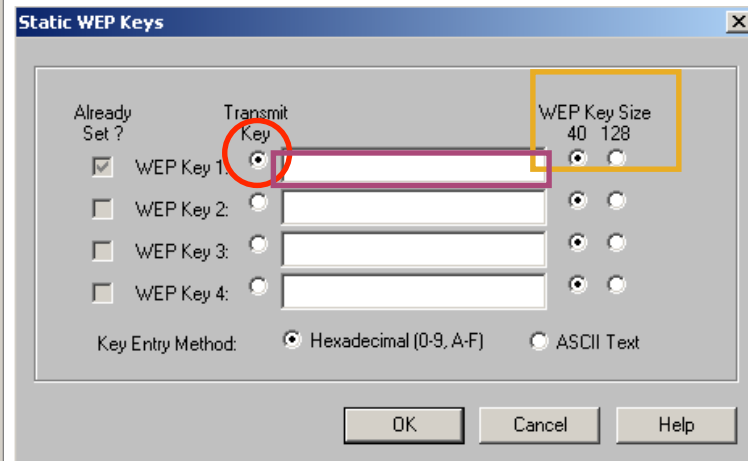
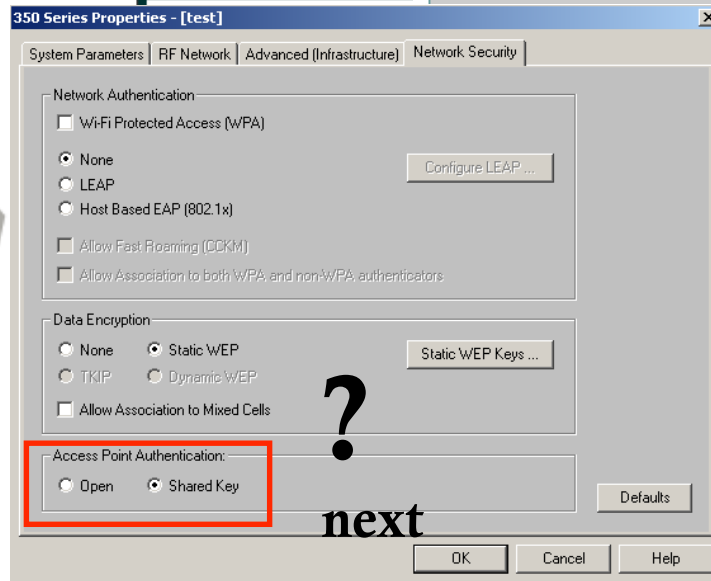
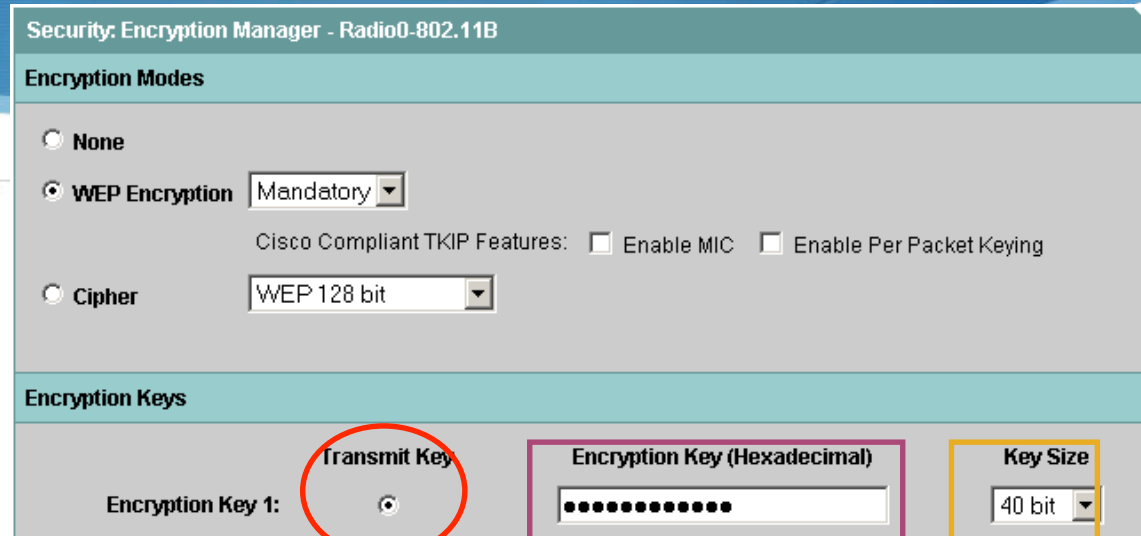
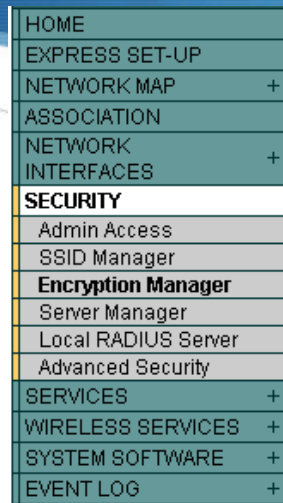
Ninguno

WEP

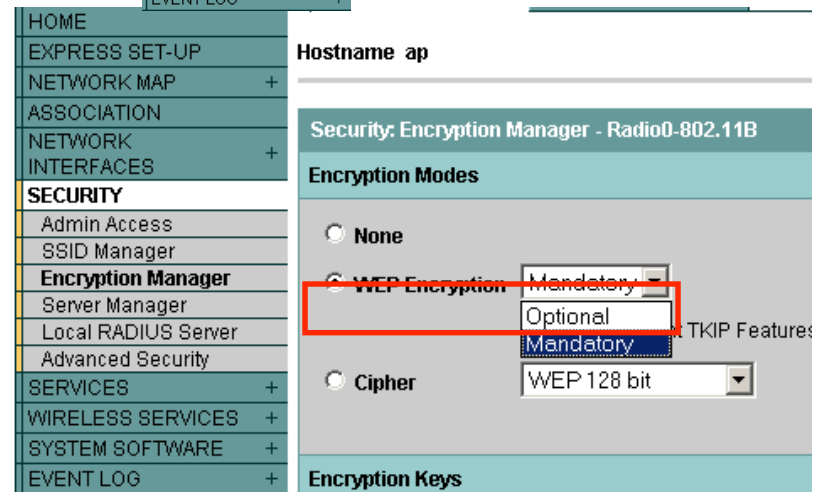
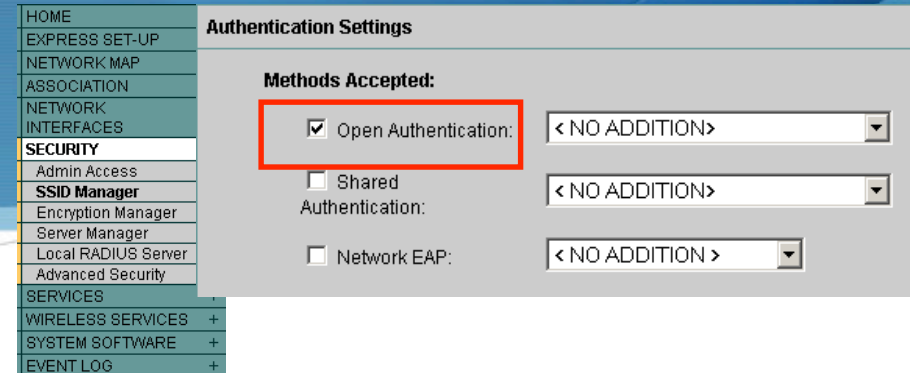
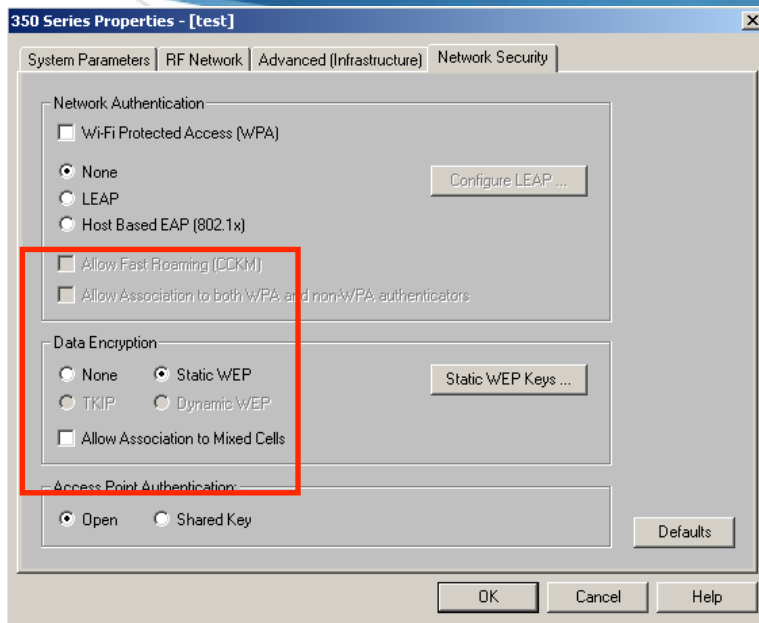
solo



# Proceso de autenticación – Llave compartida



# En resumen



- ◆ Cliente
  - ◆ Usa autenticación abierta en el cliente (no usa WEP, envío de *challenge* durante la asociación).
  - ◆ Usa WEP cifrado de datos
- ◆ AP
  - ◆ Usa autenticación abierta
  - ◆ Usa cifrado WEP obligatorio, Dispositivos que no usen WEP no se podrán comunicar