



Instructor: Dr.Hanal ABUZANT

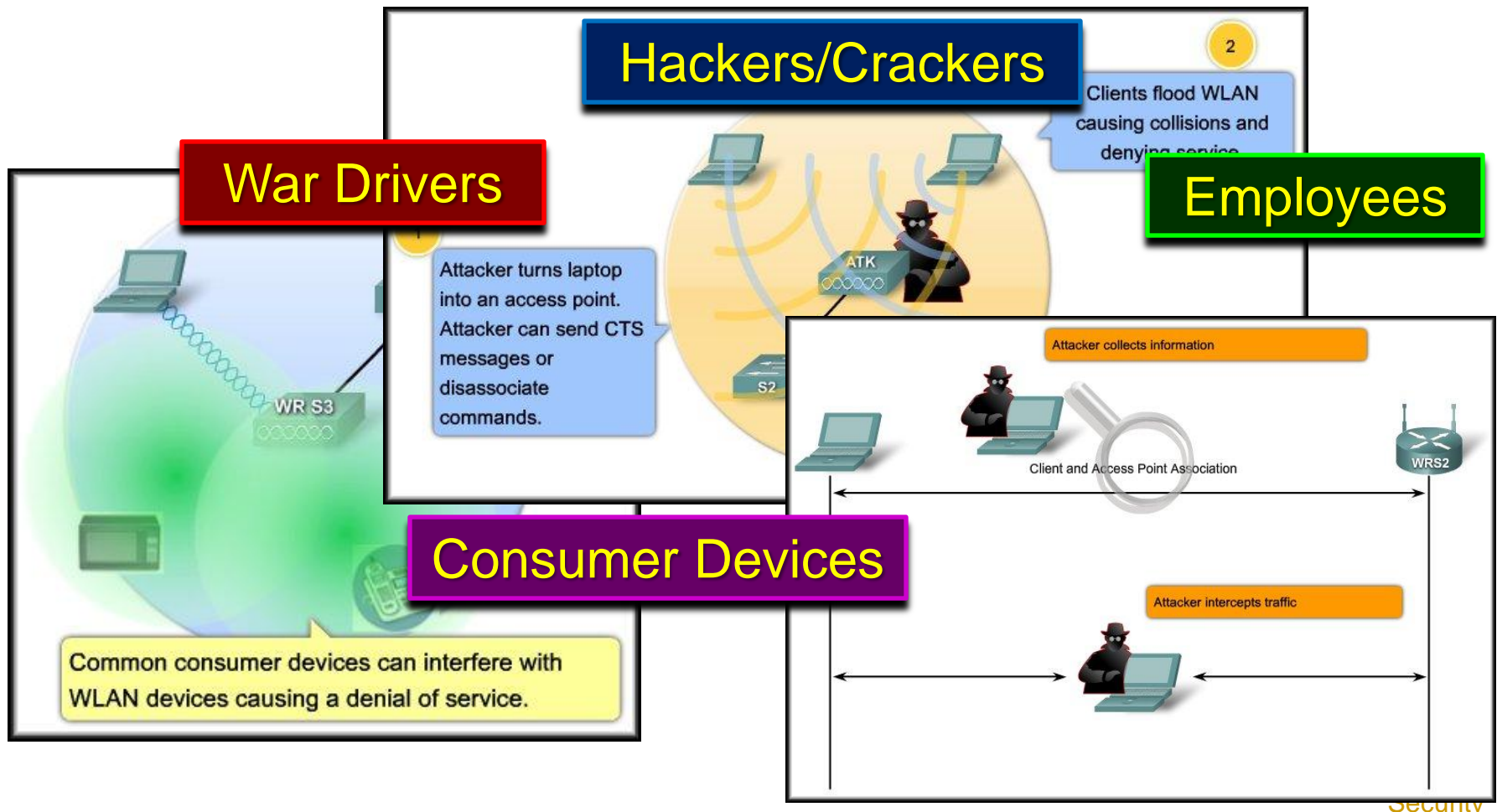
Security in Wireless Networks

Note for Instructors

- These presentations are the result of a collaboration among the instructors at St. Clair College in Windsor, Ontario.
- Thanks must go out to Rick Graziani of Cabrillo College. His material and additional information was used as a reference in their creation.
- If anyone finds any errors or omissions, please let me know at:
 - tdame@stclaircollege.ca.

Basic Wireless Concepts and Configuration

Wireless LAN Security



Wireless LAN Security

- Three Major Categories of Security Threats:
 - War Drivers:
 - War driving means driving around a neighborhood with a wireless laptop and looking for an unsecured 802.11b/g system.
 - Hackers/Crackers:
 - Malicious intruders who enter systems as criminals and steal data or deliberately harm systems.
 - Employees:
 - Set up and use Rogue Access Points without authorization. Either interfere with or compromise servers and files.

Threats to Wireless Security

- **War Drivers:**

- "War driving" originally referred to using a scanning device to find cellular phone numbers to exploit.
- War driving now also means driving around a neighborhood with a laptop and an 802.11b/g client card looking for an unsecured 802.11b/g system to exploit.
- Software is readily available.



WarDriving LogImporter v1.2.0 (beta)

File Help

Log File

Browse

C:\data\ImportData\3drun.csv

Load Data File

☐ First line is headers

Save Config

Clear Grid

Create Map

#	A	B	C	D	E	F	G	H	I	J
1	None	AdHoc	BW	00:38	0	6	9/30/...	9/30/...	39.14	-76.68
2	None	AdHoc	BW...	00:38...	0	6	9/30/...	9/30/...	39.11...	-76.69...
3	None	AdHoc	BW...	00:D2...	0	6	9/30/...	9/30/...	39.13...	-76.68...
4	None	AdHoc	BW...	00:03...	0	6	9/30/...	9/30/...	39.10...	-76.72...
5	None	AdHoc	BW...	00:68...	0	6	9/30/...	9/30/...	39.15...	-76.67...
6	None	Infrast...	My...	00:0F...	-90	6	9/30/...	9/30/...	39.14...	-76.68...
7	None	AdHoc	BW...	00:85...	0	6	9/30/...	9/30/...	39.10...	-76.72...
8	None	AdHoc	BW...	00:6D...	0	6	9/30/...	9/30/...	39.15...	-76.64...
9	None	Infrast...	link...	00:0F...	-90	6	9/30/...	9/30/...	39.10...	-76.69...
10	None	AdHoc	BW...	00:9F...	0	6	9/30/...	9/30/...	39.14...	-76.68...
11	None	AdHoc	BW...	00:08...	0	6	9/30/...	9/30/...	39.18...	-76.64...
12	None	Infrast...	link...	00:0F...	-90	6	9/30/...	9/30/...	39.14...	-76.68...
13	None	AdHoc	BW...	02:A6...	-90	6	9/30/...	9/30/...	0	0
14	None	AdHoc	BW...	00:09...	0	6	9/30/...	9/30/...	39.18...	-76.63...
15	None	Infrast...	Do...	00:0F...	-90	6	9/30/...	9/30/...	39.18...	-76.63...
16	None	AdHoc	BW...	00:D1...	0	6	9/30/...	9/30/...	39.11...	-76.69...
17	None	AdHoc	BW...	00:D2...	0	6	9/30/...	9/30/...	39.14...	-76.68...
18	None	AdHoc	BW...	00:6D...	0	6	9/30/...	9/30/...	39.18...	-76.63...
19	None	AdHoc	BW...	00:D2...	0	6	9/30/...	9/30/...	39.09...	-76.72...
20	None	AdHoc	BW...	00:6C...	0	6	9/30/...	9/30/...	39.09...	-76.71...
21	None	AdHoc	BW...	00:D4...	0	6	9/30/...	9/30/...	39.15...	-76.64...
22	None	Infrast...	klas...	00:06...	-90	6	9/30/...	9/30/...	39.18...	-76.63...
23	None	AdHoc	BW...	00:D3...	0	6	9/30/...	9/30/...	39.15...	-76.64...
24	None	AdHoc	BW...	00:06...	0	6	9/30/...	9/30/...	39.175	-76.63...
25	None	Infrast...	101...	00:0F...	-90	6	9/30/...	9/30/...	39.14...	-76.68...
26	None	Infrast...	link...	00:0F...	-90	6	9/30/...	9/30/...	39.18...	-76.63...

Data Map

A

Encryption

B

Mode

C

SSID

D

MAC

E

Signal

F

Chanel

G

First

H

Last

I

Latitude

J

Longitude

Pushpin symbols

No encryption

WEP

Other

1

2

0

Records: 132

d

Ultimate 14 dB Yagi



for long-range signal boosting
and serious WarDriving

10	None	AdHoc	BW...	00:9F...	0	6	9/30/...	9/30/...	39.14... -76.68...
11	None	AdHoc	BW...	00:08...	0	6	9/30/...	9/30/...	39.11... -76.69...
12	None	Infrast...	link...	00:0F...	-90	6	9/30/...	9/30/...	39.13... -76.68...
13	None	AdHoc	BW...	02:A6...	-90	6	9/30/...	9/30/...	39.10... -76.72...
14	None	AdHoc	BW...	00:09...	0	6	9/30/...	9/30/...	39.15... -76.67...
15	None	Infrast...	Do...	00:0F...	-90	6	9/30/...	9/30/...	39.14... -76.68...
16	None	AdHoc	BW...	00:D1...	0	6	9/30/...	9/30/...	39.10... -76.72...
17	None	AdHoc	BW...	00:D2...	0	6	9/30/...	9/30/...	39.15... -76.64...
18	None	AdHoc	BW...	00:6D...	0	6	9/30/...	9/30/...	39.10... -76.69...
19	None	AdHoc	BW...	00:D2...	0	6	9/30/...	9/30/...	39.14... -76.68...
20	None	AdHoc	BW...	00:6C...	0	6	9/30/...	9/30/...	39.18... -76.64...
21	None	AdHoc	BW...	00:D4...	0	6	9/30/...	9/30/...	39.14... -76.68...
22	None	Infrast...	klas...	00:06...	-90	6	9/30/...	9/30/...	39.14... -76.63...
23	None	AdHoc	BW...	00:D3...	0	6	9/30/...	9/30/...	0 0
24	None	AdHoc	BW...	00:06...	0	6	9/30/...	9/30/...	39.18... -76.63...
25	None	Infrast...	101...	00:0F...	-90	6	9/30/...	9/30/...	39.18... -76.63...
26	None	Infrast...	link...	00:0F...	-90	6	9/30/...	9/30/...	39.11... -76.69...

Save Config

Clear Grid

Create Map

Data Map

A Encryption
B Mode
C SSID
D MAC
E Signal
F Chanel
G First
H Last
I Latitude
J Longitude

Pushpin symbols

No encryption \$ 1

WEP \$ 2

Other \$ 0

Records: 132

d

Ultimate 14 dB Yagi

for lo
an



Totally and completely ILLEGAL!!!!!!!

Threats to Wireless Security

- Man-in-the-Middle Attacks:
 - Attackers select a host as a target and position themselves logically between the target and the router of the target.
 - In a wired LAN, the attacker needs to be able to physically access the LAN to insert a device logically into the topology.
 - With a WLAN, the radio waves emitted by access points can provide the connection.
 - Because access points act like Ethernet hubs, each NIC in a BSS hears all the traffic.
 - Attackers can modify the NIC of their laptop with special software so that it accepts all traffic.

Threats to Wireless Security

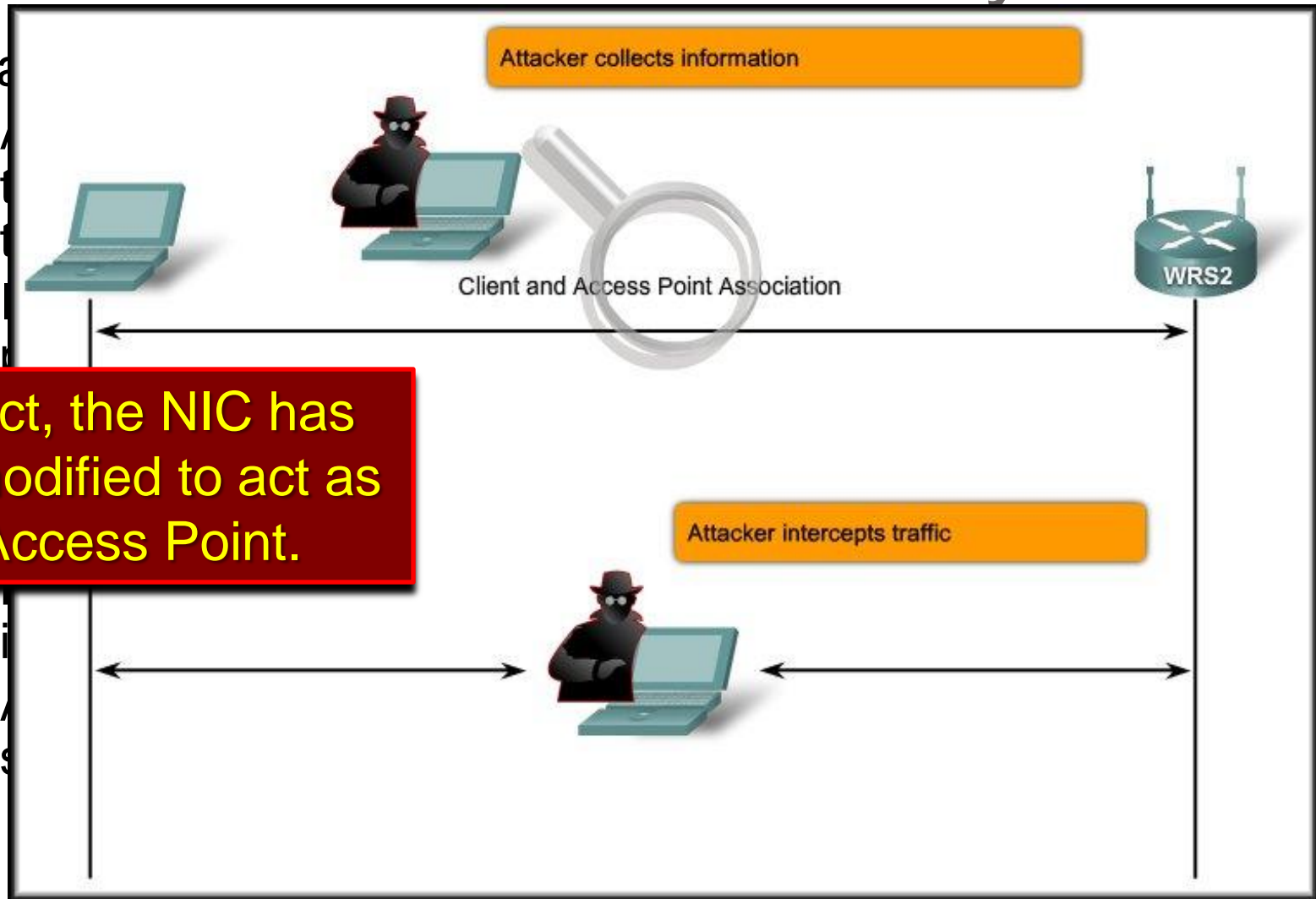
- Man-in-the-Middle

-

-

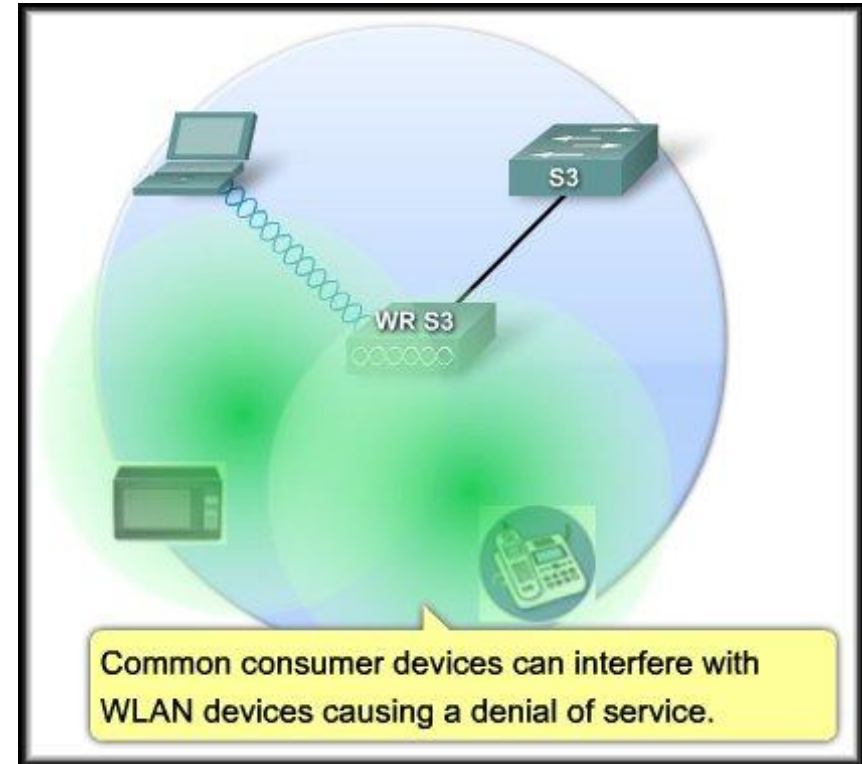
-

In effect, the NIC has been modified to act as an Access Point.



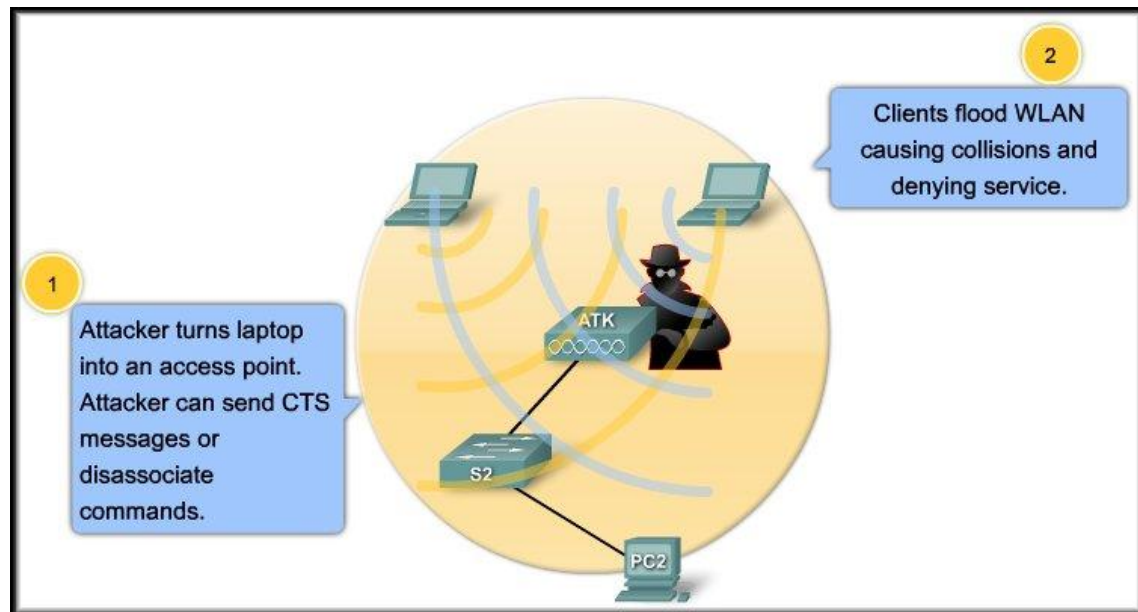
Threats to Wireless Security

- Denial of Service (DoS):
 - 802.11b/g WLANs use the unlicensed 2.4 GHz band.
 - This is the same band used by most baby monitors, cordless phones, and microwave ovens.
 - With these devices crowding the RF band, attackers can create noise on all the channels in the band with commonly available devices.



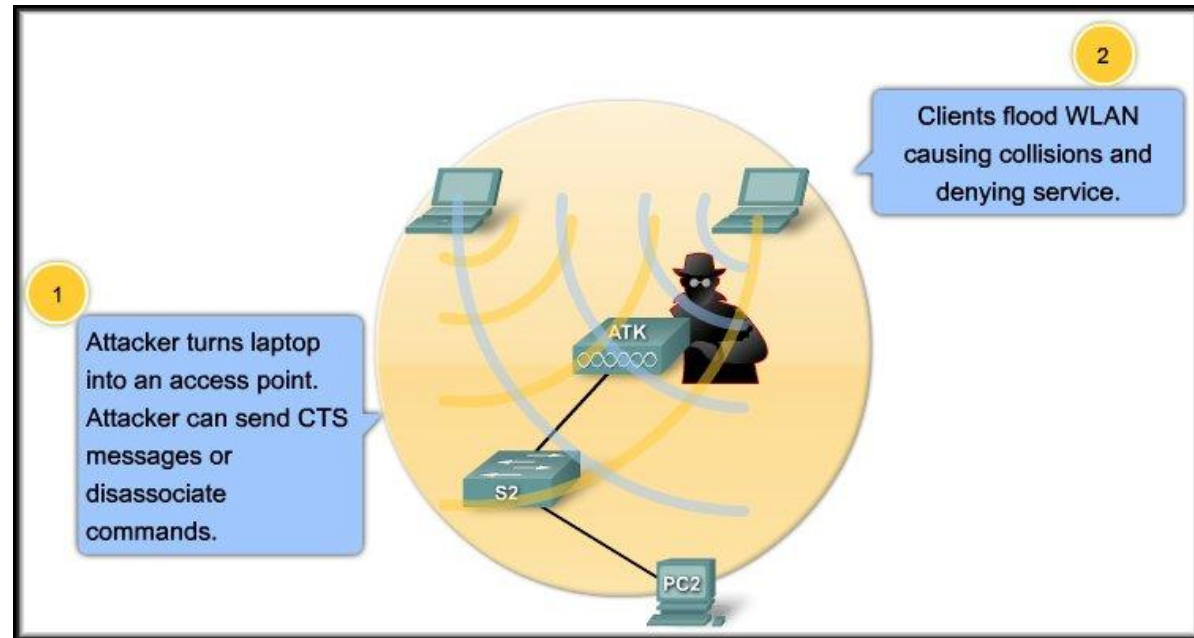
Threats to Wireless Security

- Denial of Service (DoS):
 - An attacker can turn a NIC into an access point.
 - The attacker, using a PC as an AP, can flood the BSS with clear-to-send (CTS) messages, which defeat the CSMA/CA function used by the stations.
 - The actual AP, floods the BSS with simultaneous traffic, causing a constant stream of collisions.



Threats to Wireless Security

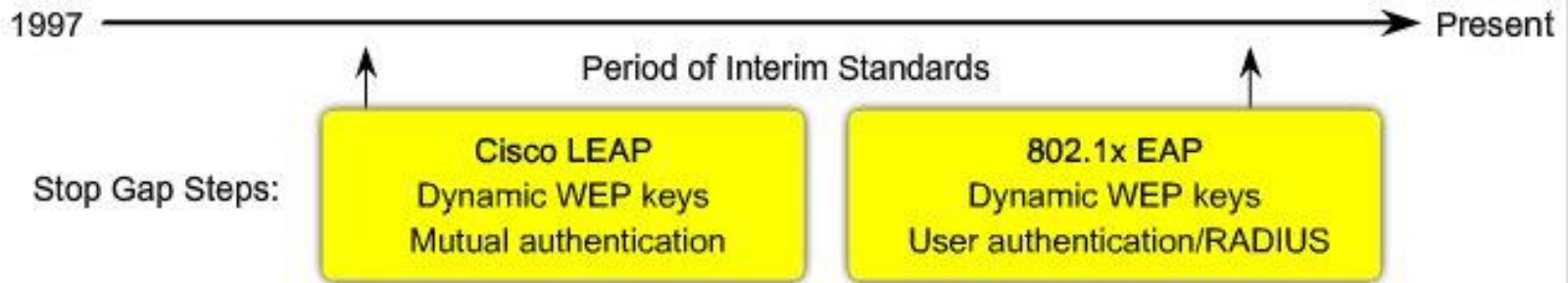
- Denial of Service (DoS):
 - Another DoS attack that can be launched in a BSS is when an attacker sends a series of disassociate commands that cause all stations to disconnect.
 - When the stations are disconnected, they immediately try to reassociate, which creates a burst of traffic.
 - The attacker sends another disassociate and the cycle repeats itself.



Wireless Security Protocols

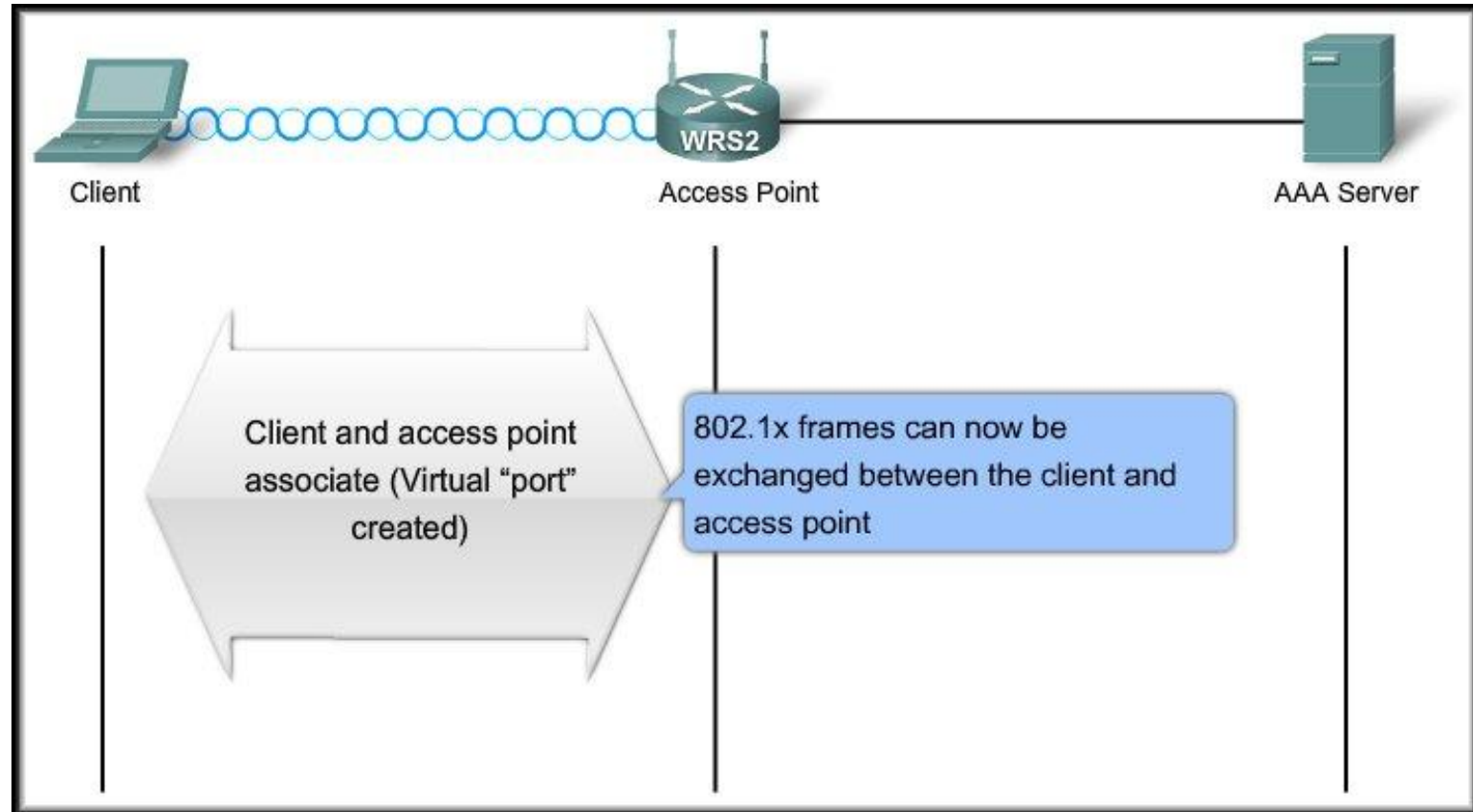
Major Stepping Stones to Secure WLAN

Open Access	First Generation Encryption	Interim	Present
SSID	WEP	WPA	802.11i/WPA2
<ul style="list-style-type: none"> No encryption Basic authentication Not a security handle 	<ul style="list-style-type: none"> No strong authentication Static, breakable keys Not scalable 	<ul style="list-style-type: none"> Standardized Improved encryption Strong, user-based authentication (e.g., LEAP, PEAP, EAP-FAST) 	<ul style="list-style-type: none"> AES Encryption Authentication: 802.1X Dynamic key management WPA2 is the Wi-Fi Alliance implementation of 802.11i



Authenticating to the Wireless LAN

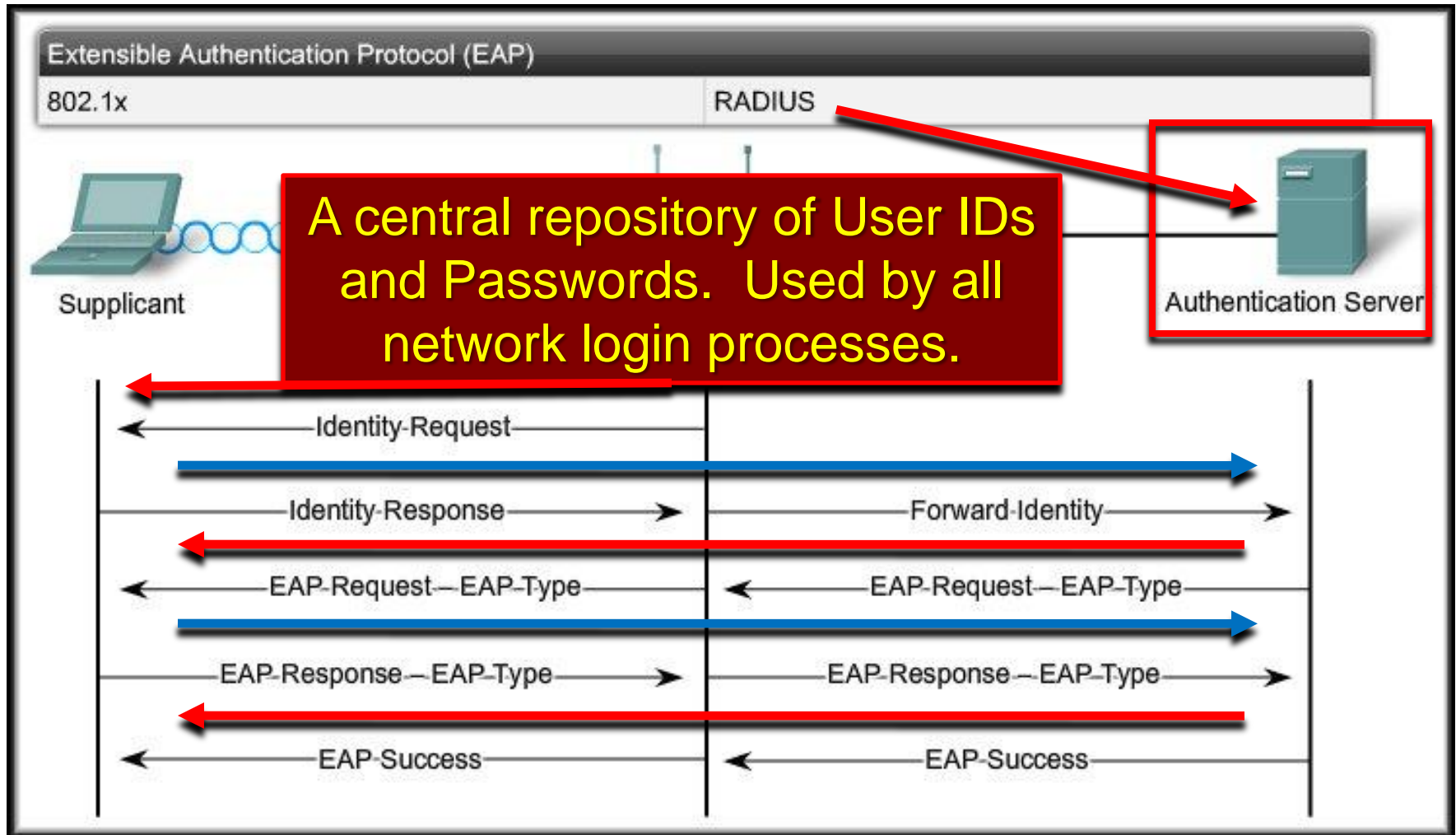
- In an open network, such as a home network, association may be all that is required to grant a client access to devices and services on the WLAN.



Authenticating to the Wireless LAN

- In networks that have stricter security requirements, an additional authentication or login is required to grant clients such access.
- This login process is managed by the Extensible Authentication Protocol (EAP).

Authenticating to the Wireless LAN



Wireless Encryption

- Two Encryption Mechanisms:

TKIP – Temporal Key Integrity ~~Key~~ Protocol

- Encrypts by adding increasingly complex bit coding to each packet
- Based on same cipher (RC4) as WEP

AES – Advanced Encryption Standard

- New cipher used in 802.11i
- Based on TKIP with additional features that enhances the level of provided security

- TKIP is the encryption method certified as Wi-Fi Protected Access (WPA).
 - Provides support for legacy WLAN equipment by addressing the original flaws associated with the 802.11 WEP encryption method.
 - Encrypts the Layer 2 payload.
 - Message integrity check (MIC) in the encrypted packet that helps ensure against a message tampering.

Wireless Encryption

- Two Encryption Mechanisms:

TKIP – Temporal Key Integrity ~~Key~~ Protocol

- Encrypts by adding increasingly complex bit coding to each packet
- Based on same cipher (RC4) as WEP

AES – Advanced Encryption Standard

- New cipher used in 802.11i
- Based on TKIP with additional features that enhances the level of provided security

- The AES encryption of WPA2 is the preferred method.
 - WLAN encryption standards used in IEEE 802.11i.
 - Same functions as TKIP.
 - Uses additional data from the MAC header that allows destination hosts to recognize if the non-encrypted bits have been tampered with.
 - Also adds a sequence number to the encrypted data header.

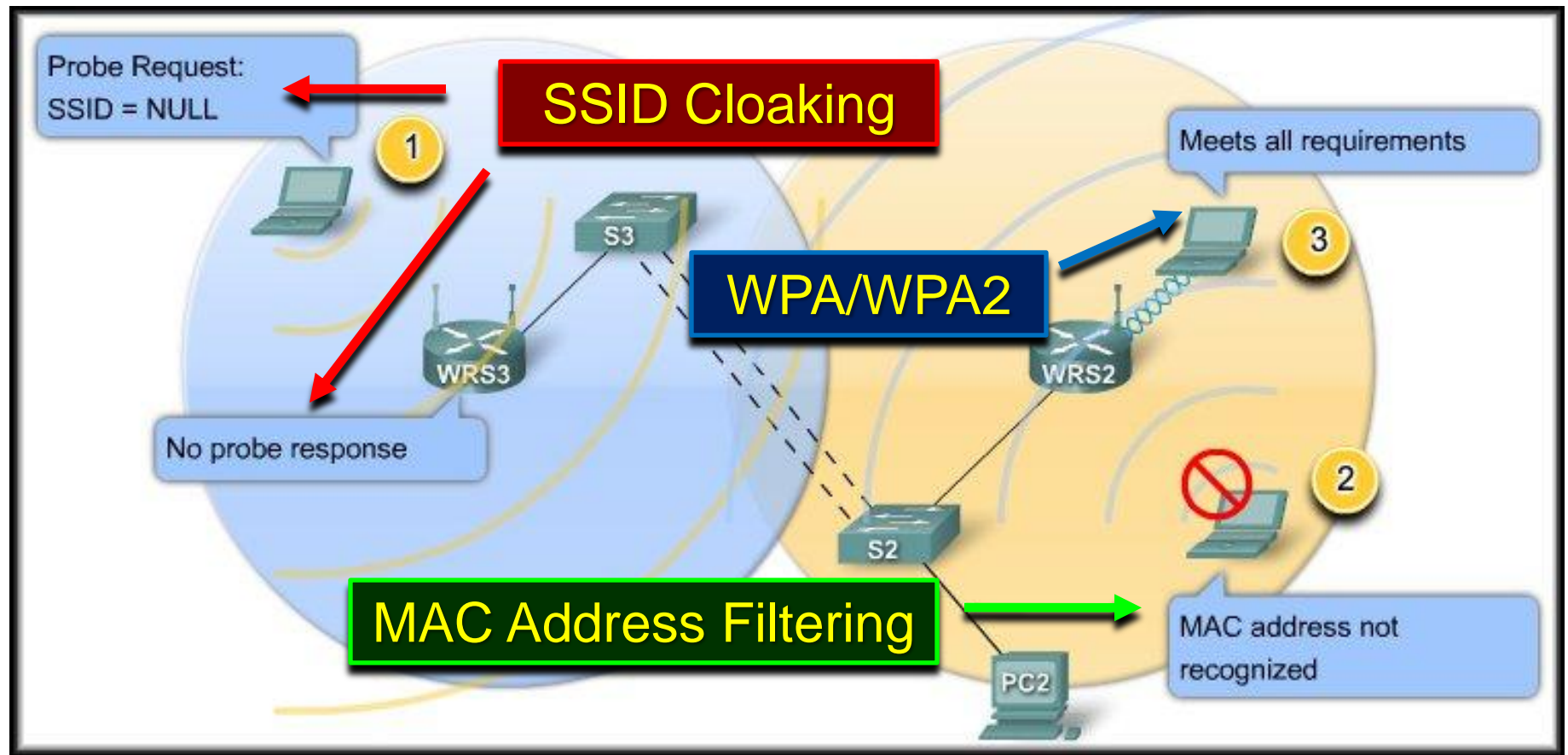
Wireless Encryption

- *When you configure Linksys access points or wireless routers you may not see WPA or WPA2.*
 - Instead you may see references to something called pre-shared key (PSK).
- Types of PSKs:
 - PSK or PSK2 with TKIP is the same as WPA.
 - PSK or PSK2 with AES is the same as WPA2.
 - PSK2, without an encryption method specified, is the same as WPA2.

Controlling Access to the Wireless LAN

- When controlling access, the concept of depth means having multiple solutions available.
 - Three step approach:
 - SSID cloaking:
 - Disable SSID broadcasts from access points.
 - MAC address filtering:
 - Tables are manually constructed on the access point to allow or disallow clients based on their physical hardware address.
 - WLAN Security:
 - Implement WPA or WPA2.

Controlling Access to the Wireless LAN



Controlling Access to the Wireless LAN

- An additional consideration is to configure access points that are near outside walls of buildings to transmit on a lower power setting than other access points closer to the middle of the building.
- This is to merely reduce the RF signature on the outside of the building.
 - Anyone running an application such as Netstumbler, Wireshark, or even Windows XP can map WLANs.

Basic Wireless Concepts and Configuration

Configuring Wireless LAN Access

The screenshot shows the 'Basic Wireless Settings' page in a web browser. The page is titled 'LINKSYS A Division of Cisco Systems, Inc.' and has a navigation bar with 'Wireless', 'Setup', 'Security', and 'Status' tabs. The 'Wireless' tab is selected, and the 'Basic Wireless Settings' sub-tab is active. The page contains several configuration fields: 'Network Mode' (a dropdown menu), 'Network Name (SSID)' (a text input field), 'Radio Band' (a dropdown menu), 'Wide Channel' (a dropdown menu), 'Standard Channel' (a dropdown menu), and 'SSID Broadcast' (radio buttons for 'Enabled' and 'Disabled').

Numbered callouts highlight the following steps:

1. Click on the 'Wireless' tab in the navigation bar.
2. Click on the 'Basic Wireless Settings' sub-tab.
3. Select network mode from the 'Network Mode' dropdown menu.
 - MixedBG-Mixed
 - Wireless-B Only
 - Wireless-G Only
 - Wireless-N Only
 - Disabled
4. Change default SSID in the 'Network Name (SSID)' text input field.
5. Set RF Channels by selecting 'Radio Band' and 'Wide Channel'.
6. Select SSID Broadcast option by choosing 'Enabled' or 'Disabled'.

Buttons at the bottom of the page include 'Save Settings' and 'Cancel Changes'.

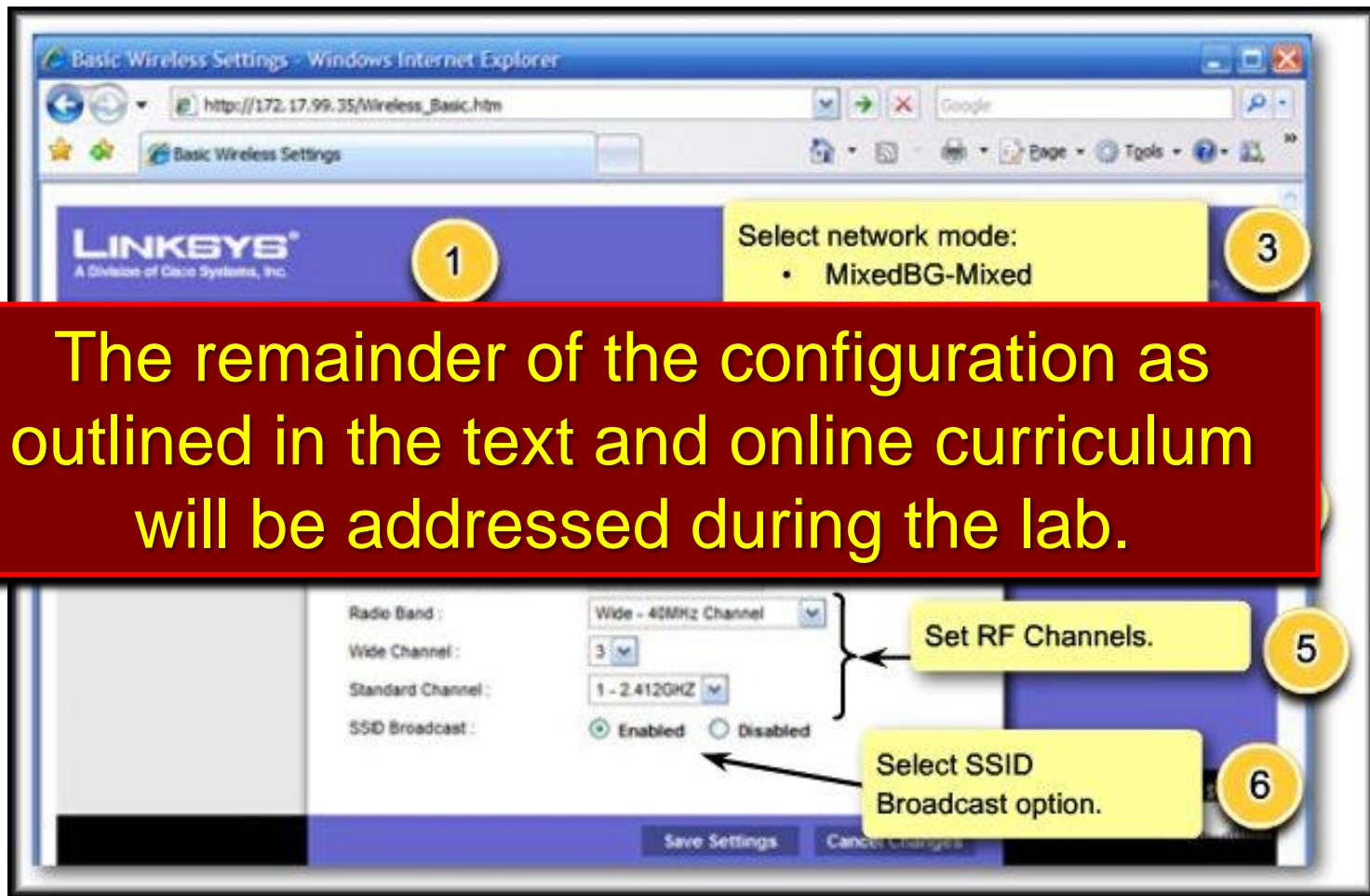
Configuring the Wireless Access Point

- In this topic, you will learn:
 - How to configure a wireless access point.
 - How to set the SSID.
 - How to enable security.
 - How to configure the channel.
 - How to adjust the power settings.
 - How to back up and restore the configuration.

Configuring the Wireless Access Point

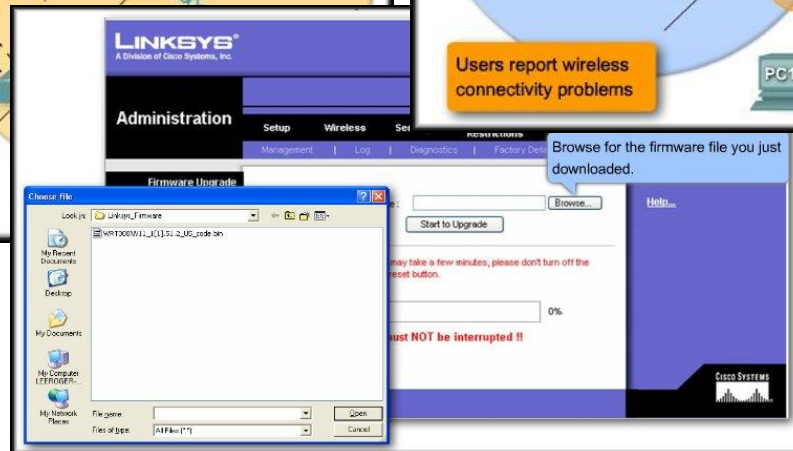
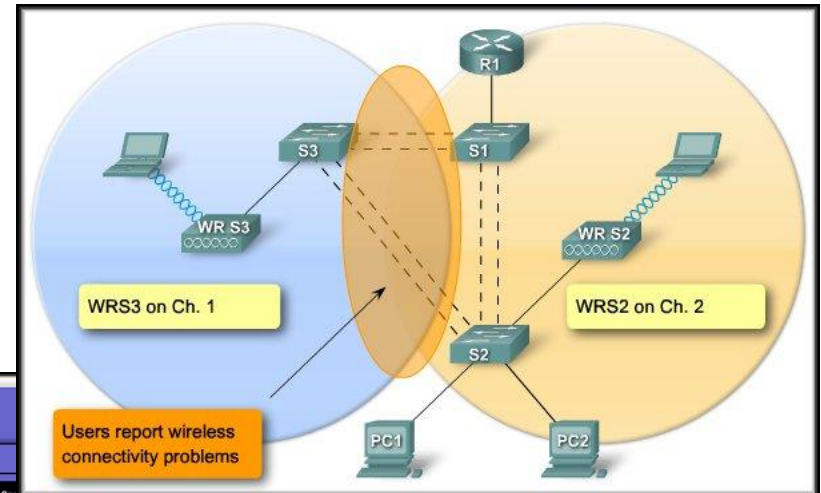
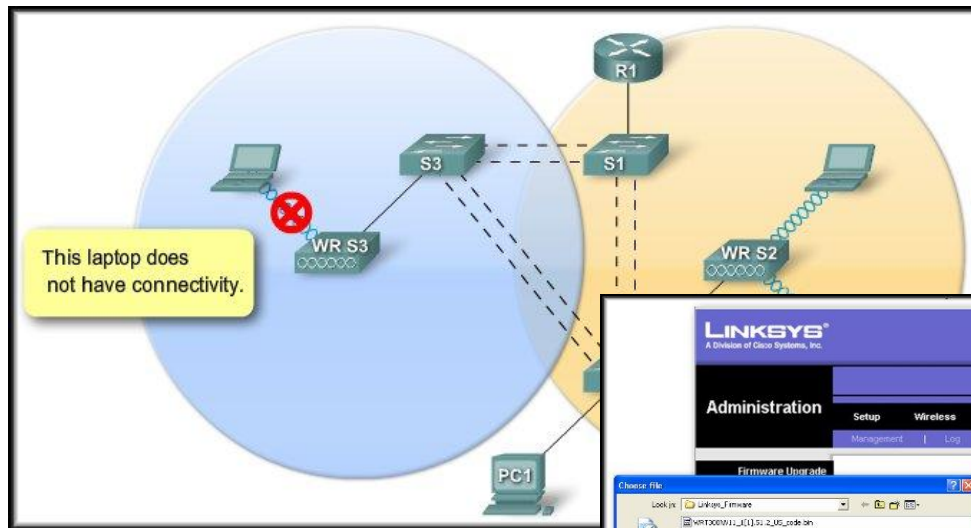
- The basic approach to wireless implementation, as with any basic networking, is to configure and test incrementally.
 - Verify the existing network and Internet access for the wired hosts.
 - Start the WLAN implementation process with a single access point and a single client, without enabling wireless security.
 - Verify that the wireless client has received a DHCP IP address and can ping the local wired default router and then browse to the external Internet.
 - Finally, configure wireless security with WPA2.
 - Use WEP only if the hardware does not support WPA.

Configuring the Wireless Access Point

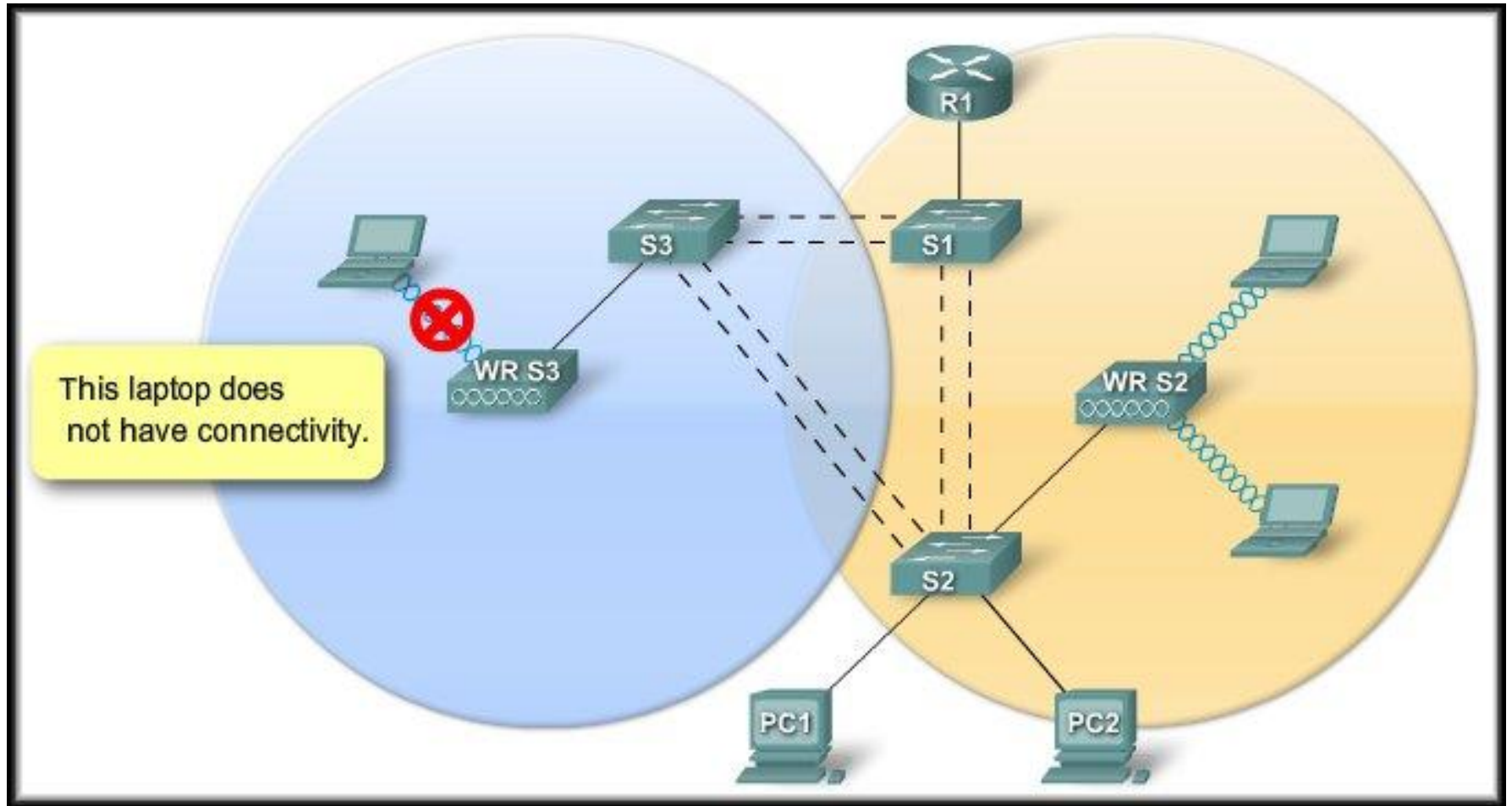


Basic Wireless Concepts and Configuration

Troubleshooting Simple WLAN Problems



A Systematic Approach



A Systematic Approach

Eliminate the User's PC as the source of the problem.

This laptop does not have connectivity.

Network configuration.
Can it connect to a wired network?
Is the NIC O.K?
Are the proper drivers loaded?
Do the security settings match?

How far is the PC from the Access Point?
Check the channel settings.
Any interference from other devices?

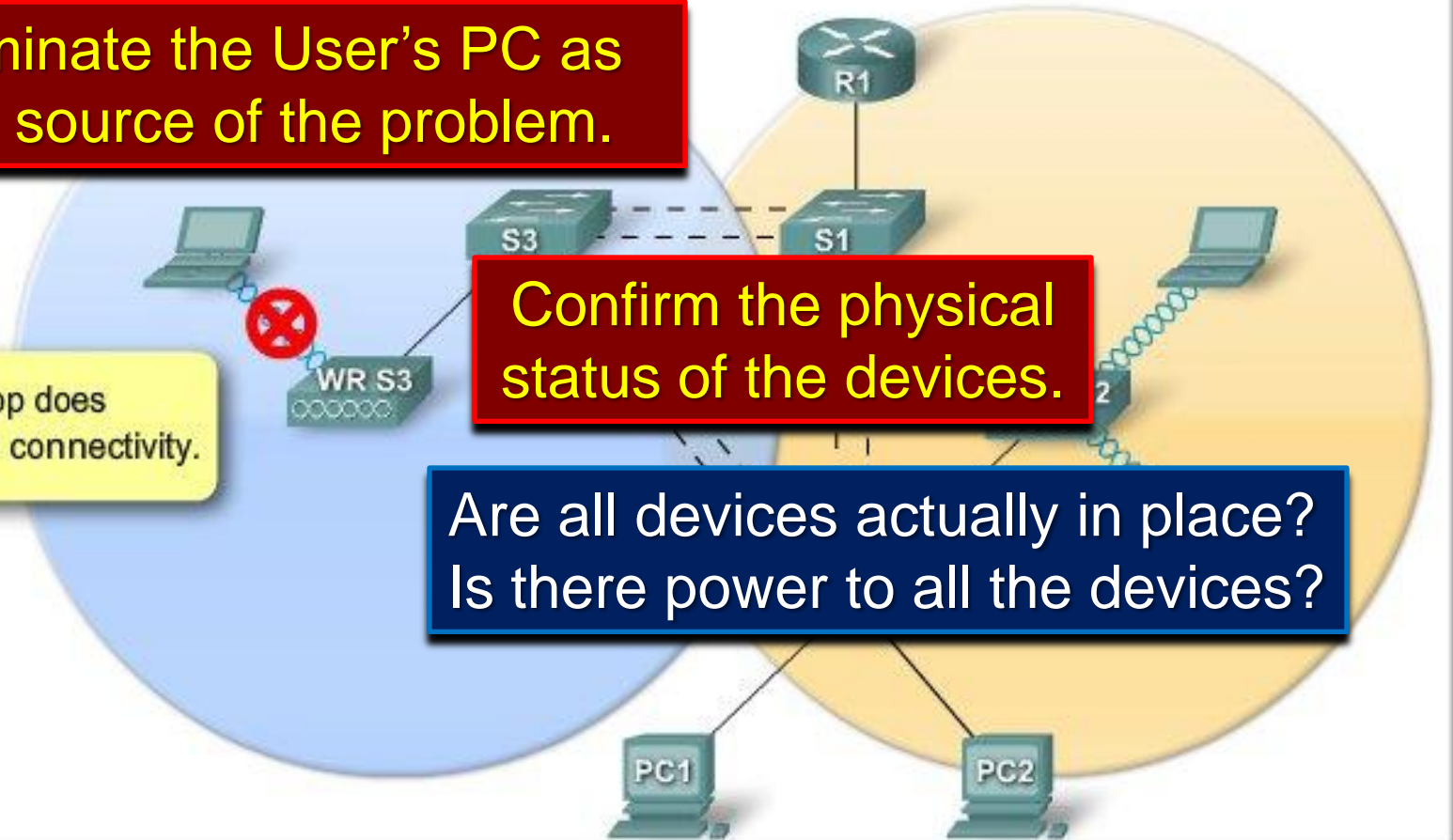
A Systematic Approach

Eliminate the User's PC as the source of the problem.

This laptop does not have connectivity.

Confirm the physical status of the devices.

Are all devices actually in place?
Is there power to all the devices?



A Systematic Approach

Eliminate the User's PC as the source of the problem.

This laptop does not have connectivity.

Confirm the physical status of the devices.

Inspect the wired links.

Cables damaged or missing?
Can you ping the AP from a cabled device?

A Systematic Approach

Eliminate the User's PC as the source of the problem.

This laptop does not have connectivity.

Confirm the physical status of the devices.

Inspect the wired links.

If all of this fails, perhaps the AP is faulty or the configuration is in error. The AP may also require a firmware upgrade.

A Systematic Approach

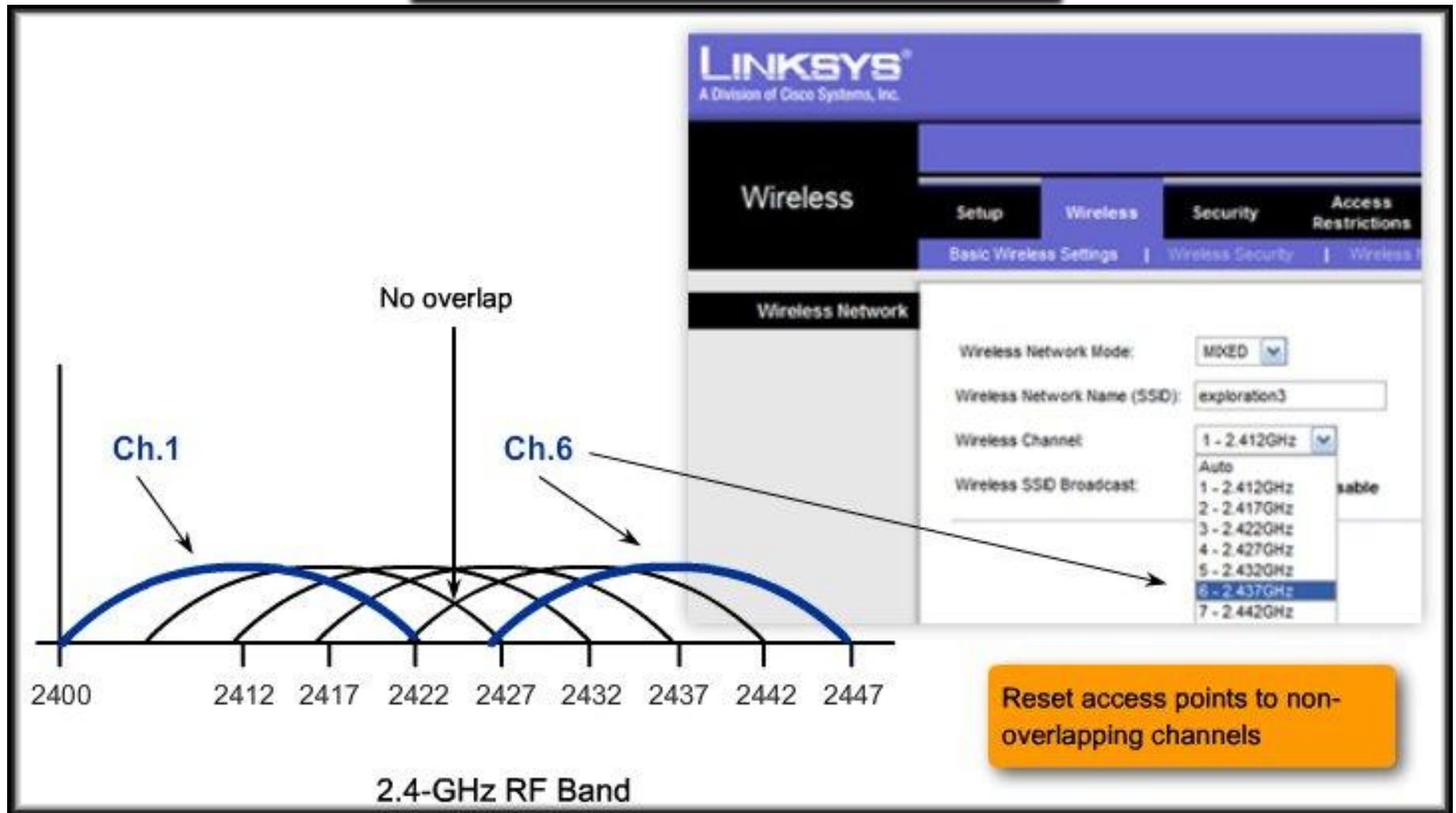
Updating the Access Point

Download
Select the Firmware
Run the Upgrade

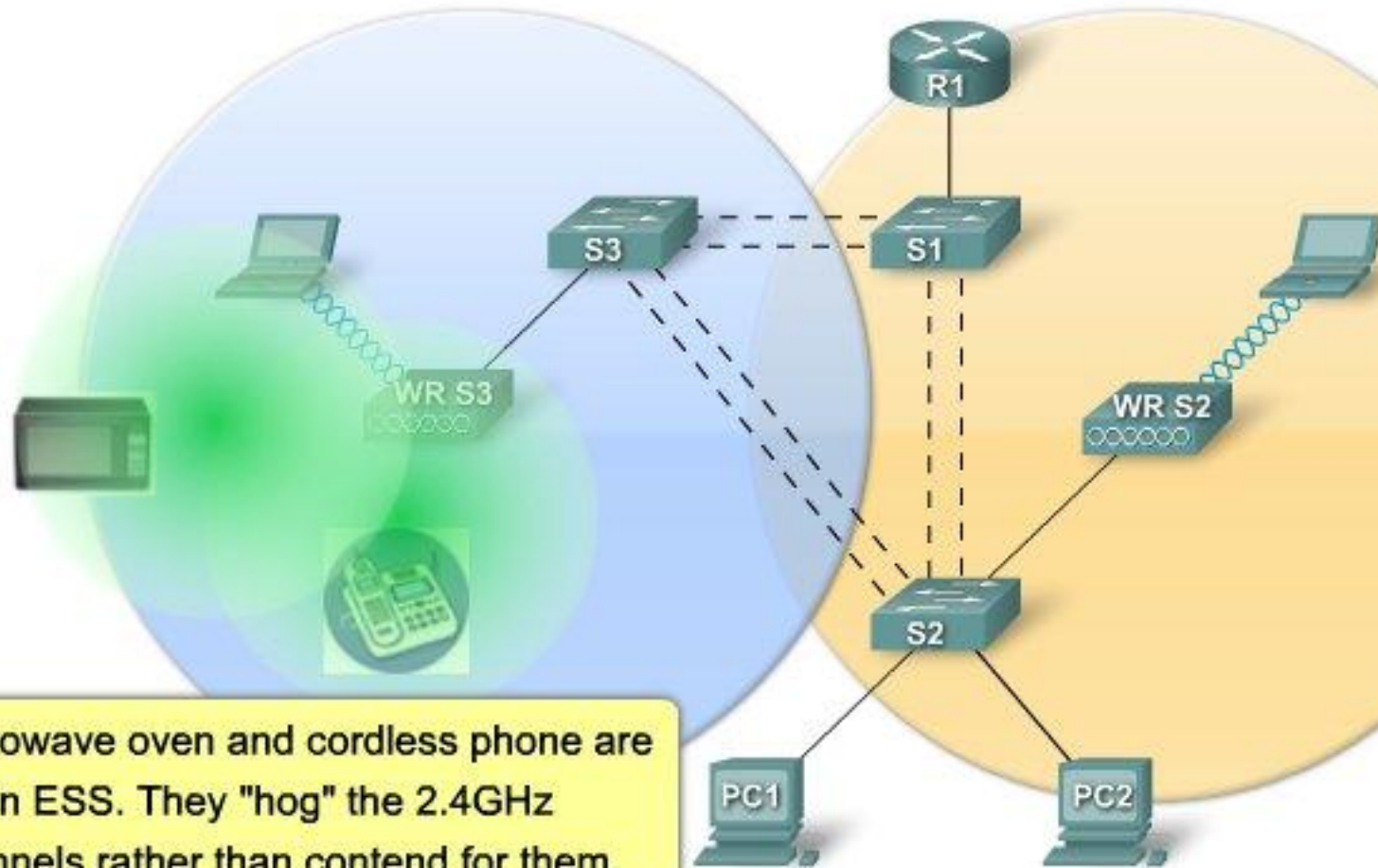
The screenshot displays the Linksys Administration web interface. The 'Firmware Upgrade' section is active, showing a 'Browse...' button and a 'Start to Upgrade' button. A file explorer window is open, showing the selected firmware file 'WRT300M11_1(1.51.2_US_code.bin)'. A callout bubble points to the 'Browse...' button with the text 'Browse for the firmware file you just downloaded.' A red box at the bottom contains the warning: 'DO NOT upgrade the firmware unless you are experiencing problems with the access point or the new firmware has a feature you want to use.'

A Systematic Approach

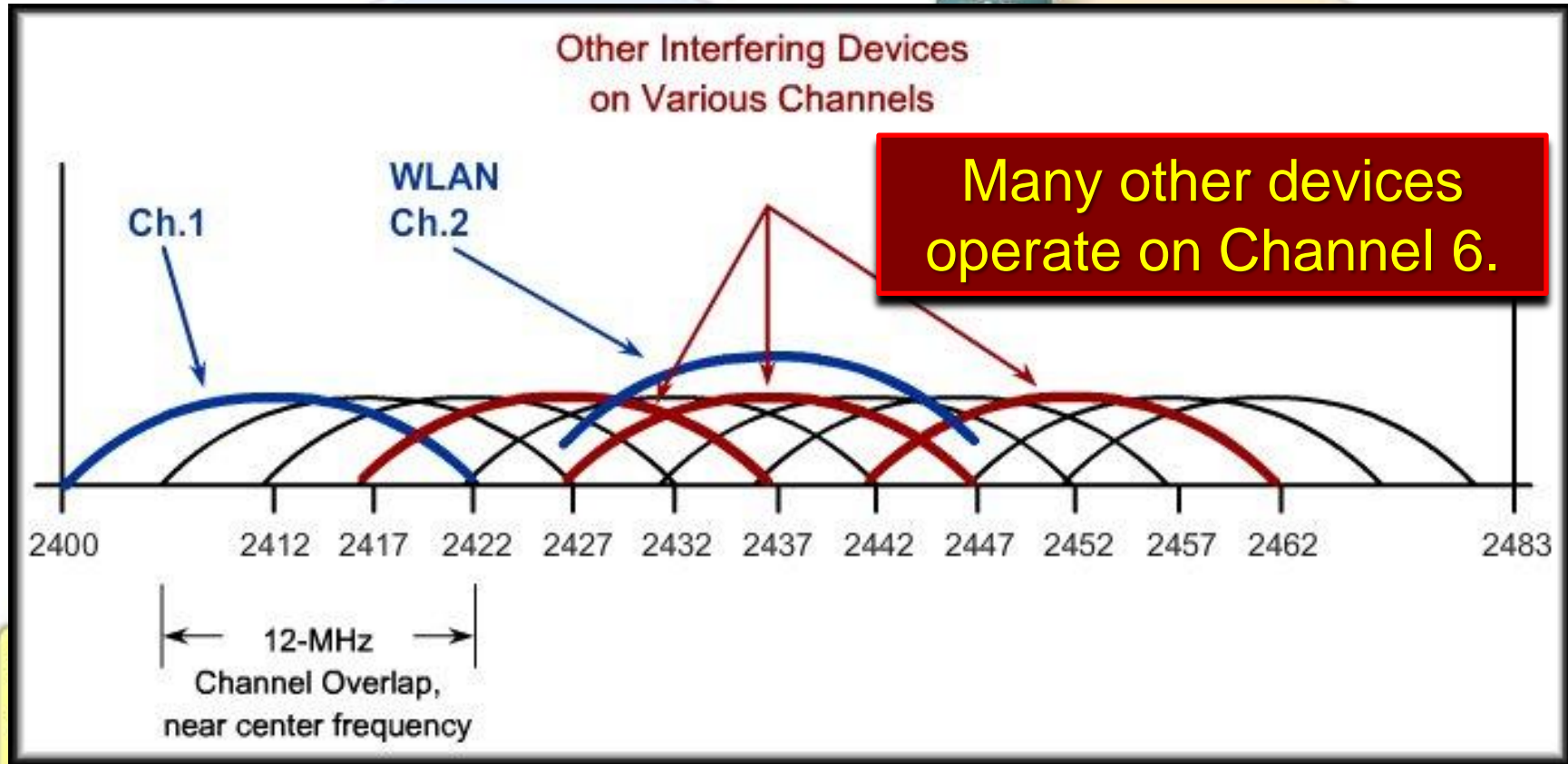
Incorrect Channel Settings



RF Interference Issues



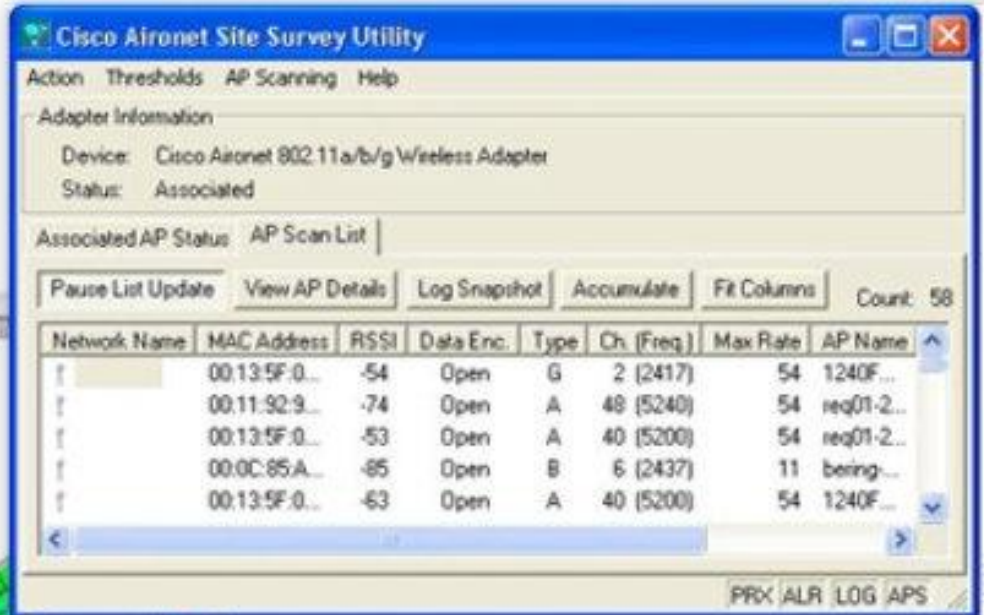
RF Interference Issues



channels rather than contend for them.

RF Interference Issues

Screenshot 1



Cisco Aironet Site Survey Utility

Action Thresholds AP Scanning Help

Adapter Information

Device: Cisco Aironet 802.11a/b/g Wireless Adapter

Status: Associated

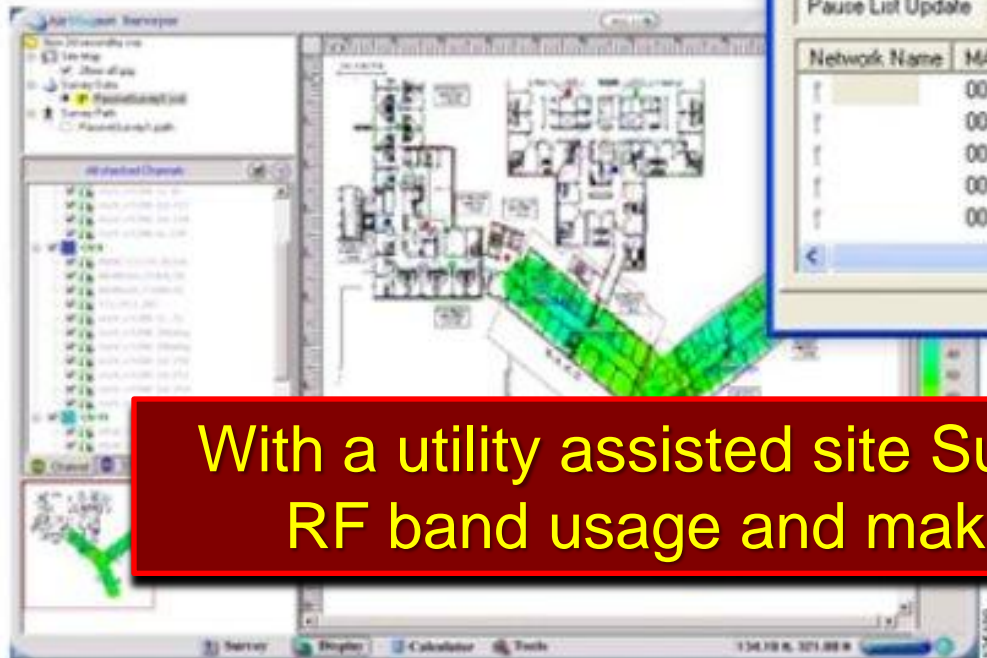
Associated AP Status AP Scan List

Pause List Update View AP Details Log Snapshot Accumulate Fit Columns Count: 58

Network Name	MAC Address	RSSI	Data Enc.	Type	Ch. (Freq)	Max Rate	AP Name
	00:13:5F:0...	-54	Open	G	2 (2417)	54	1240F...
	00:11:92:9...	-74	Open	A	48 (5240)	54	reg01-2...
	00:13:5F:0...	-53	Open	A	40 (5200)	54	reg01-2...
	00:0C:85:A...	-65	Open	B	6 (2437)	11	being...
	00:13:5F:0...	-63	Open	A	40 (5200)	54	1240F...

PRX ALR LOG APS

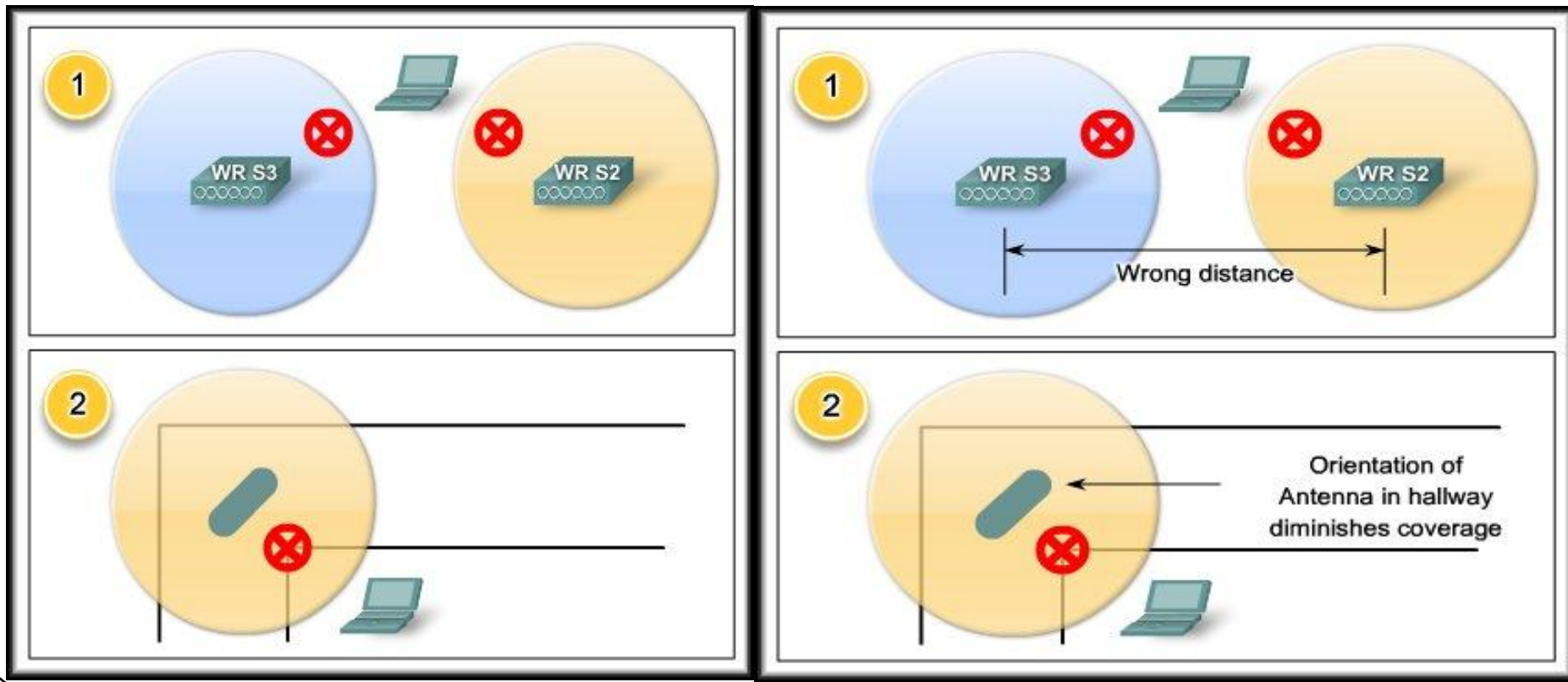
Screenshot 2



With a utility assisted site Survey, you can obtain RF band usage and make provisions for it.

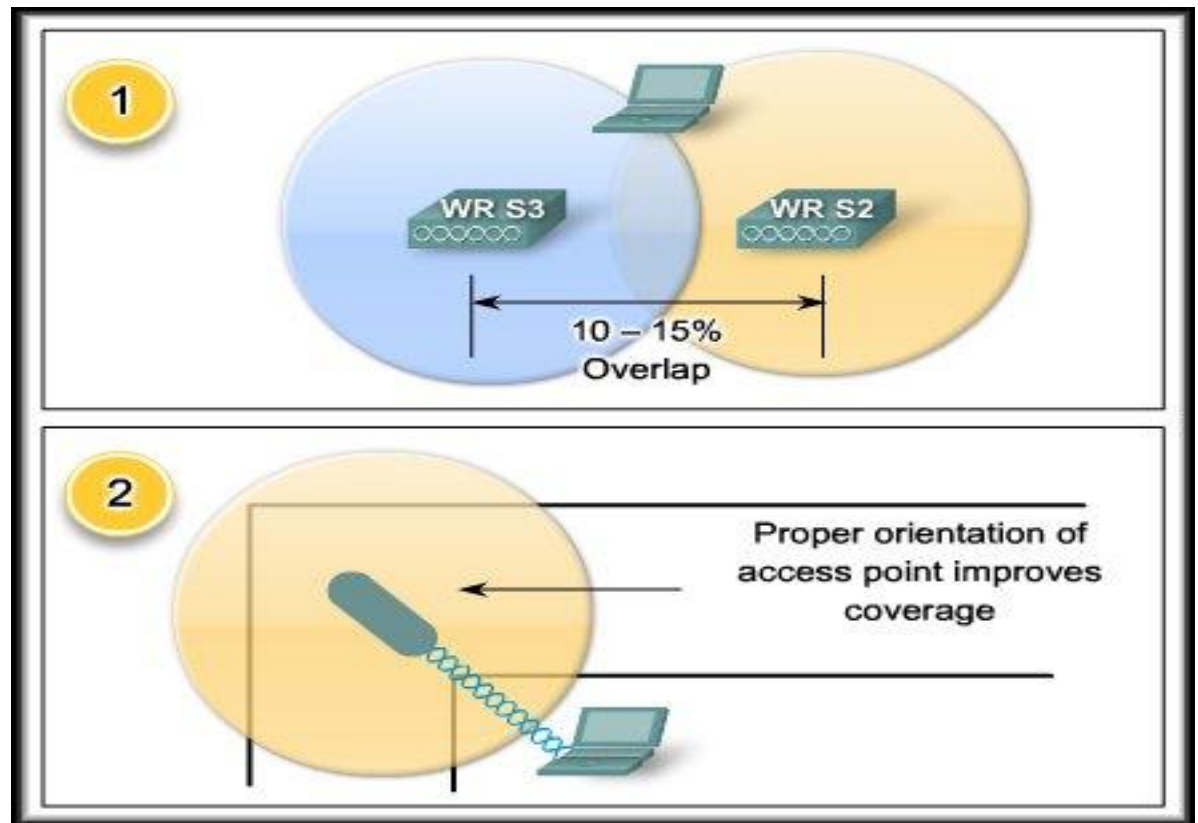
Access Point Placement

- A WLAN that just did not seem to perform like it should.
 - You keep losing association with an access point
 - Your data rates are much slower than they should be.



Access Point Placement

- A WLAN that just did not seem to perform like it should.
 - You keep losing association with an access point
 - Your data rates are much slower than they should be.



Access Point Placement

- **Some additional specific details:**
 - Not mounted closer than 7.9 inches (20 cm) from the body of all persons.
 - Do not mount the access point within 3 feet (91.4 cm) of metal obstructions.
 - Install the access point away from microwave ovens.
 - Always mount the access point vertically..
 - Do not mount the access point outside of buildings.
 - Do not mount the access point on building perimeter walls, unless outside coverage is desired.
 - When mounting an access point in the corner of a right-angle hallway intersection, mount it at a 45-degree angle.

Authentication and Encryption

1. Wrong encryption type set on client

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Security Mode: PSK2 Personal

Encryption: AES

Pre-shared Key: AES TKIP

Remember, **all devices connecting to an access point** must use the same security type as the one configured on the access point.

2. Wrong cre

Network key:

Confirm network key:

Pre-shared Key:

Key Renewal: 3600

Access point expects 32 characters in key

3. Some problem, other than encryption is at fault