Chapter 7

Basic Wireless Concepts and Configuration

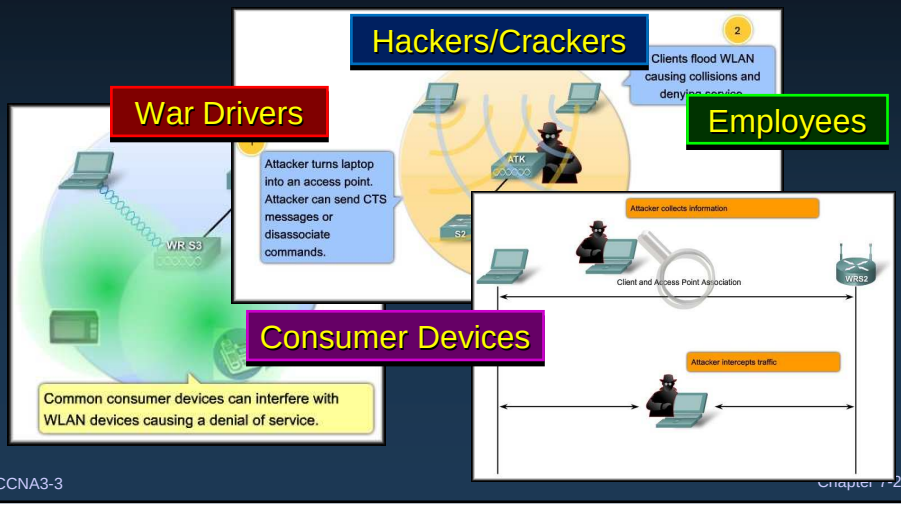
Part II

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



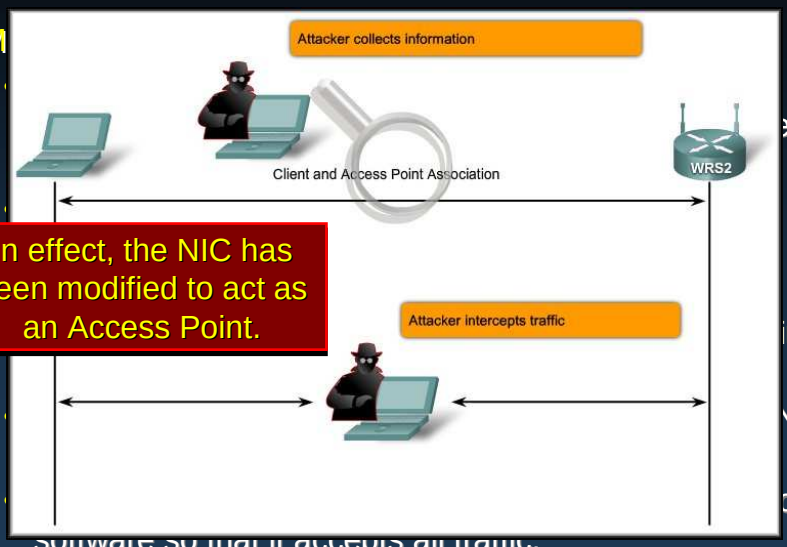
Wireless LAN Security

- 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

Threats to Wireless Security

- M



er of

into

nts

NIC

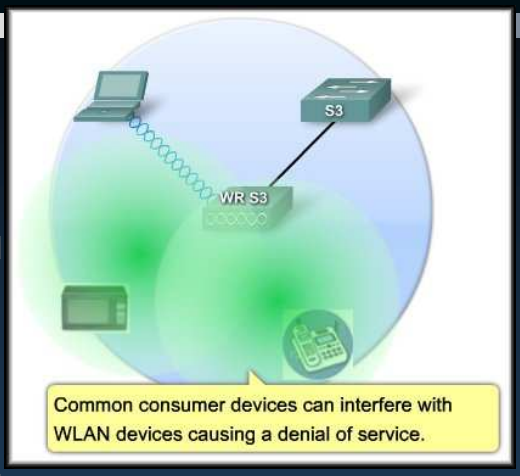
cial

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

software so that it accepts all traffic.

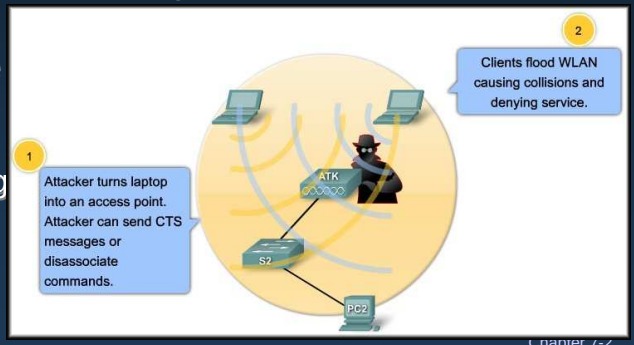
Threats to Wireless Security

- 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.



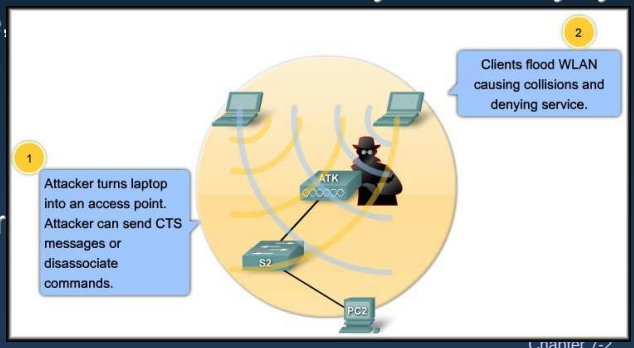
Threats to Wireless Security

- 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

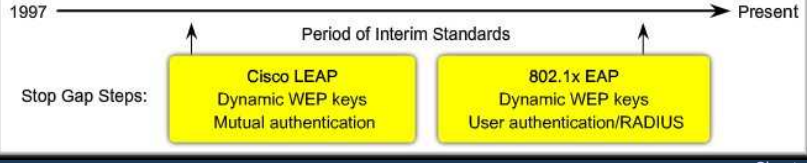
- **Denial of Service (DoS):**
  - Another DoS attack that can be launched in a BSS is when an attacker sends a **series of disassociate commands** that cause all stations to disconnect.
  - When the stations are disconnected, they immediately try to reassociate, which creates a burst of traffic.
  -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



Wireless Security Protocols

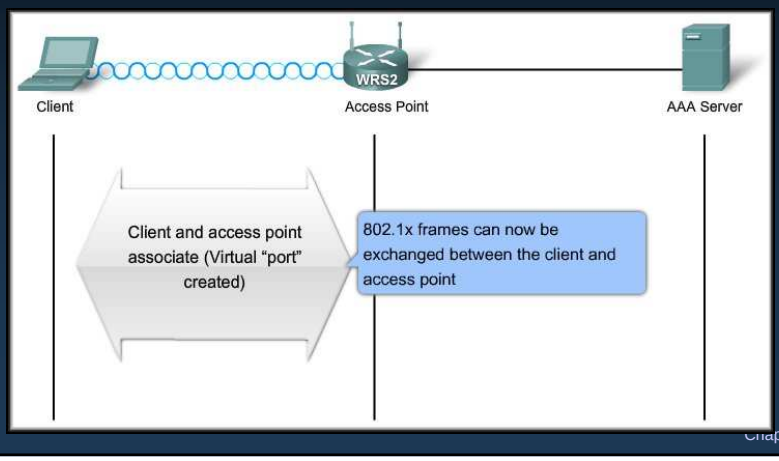
Major Stepping Stones to Secure WLAN

Open Access	First Generation Encryption	Interim	Present
SSID	WEP	WPA	802.11i/WPA2
• No encryption • Basic authentication • Not a security handle	• No strong authentication • Static, breakable keys • Not scalable	• Standardized • Improved encryption • Strong, user-based authentication (e.g., LEAP, PEAP, EAP-FAST)	• AES Encryption • Authentication: 802.1X • Dynamic key management • WPA2 is the Wi-Fi Alliance implementation of 802.11i



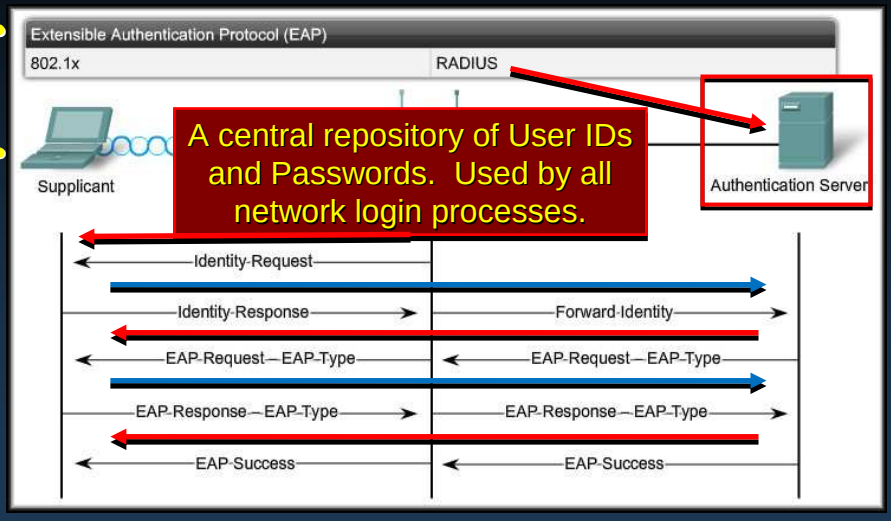
Authenticating to the Wireless LAN

- 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

-
-



Wireless Encryption

- Two Encryption Mechanisms:

TKIP – Temporal Key Integrity ~~Key~~ Protocol	AES – Advanced Encryption Standard
• Encrypts by adding increasingly complex bit coding to each packet • Based on same cipher (RC4) as WEP	• 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	AES – Advanced Encryption Standard
• Encrypts by adding increasingly complex bit coding to each packet • Based on same cipher (RC4) as WEP	• 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.

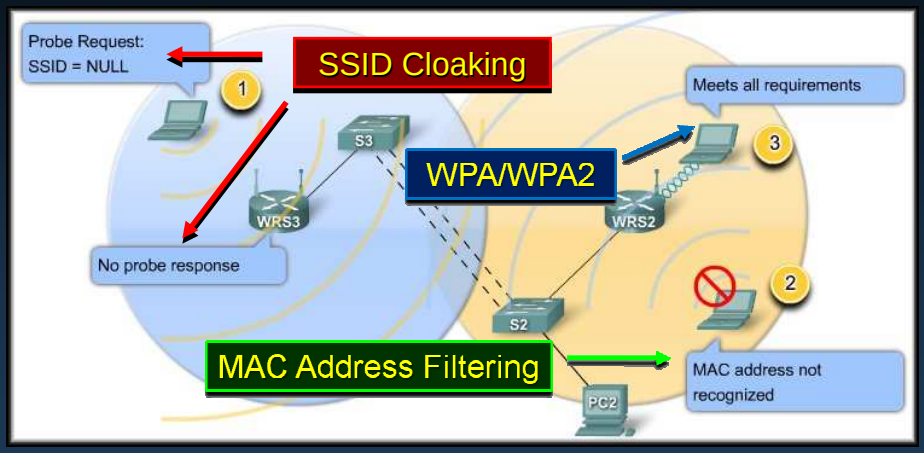
Wireless Encryption

- *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.

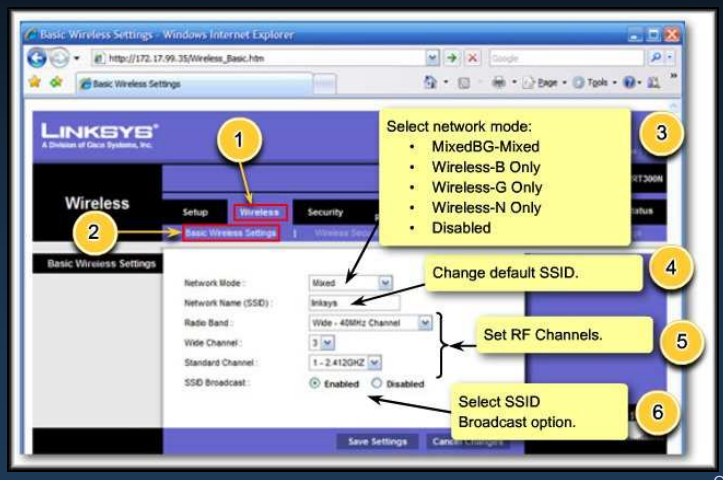
Controlling Access to the Wireless LAN



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.

Configuring Wireless LAN Access



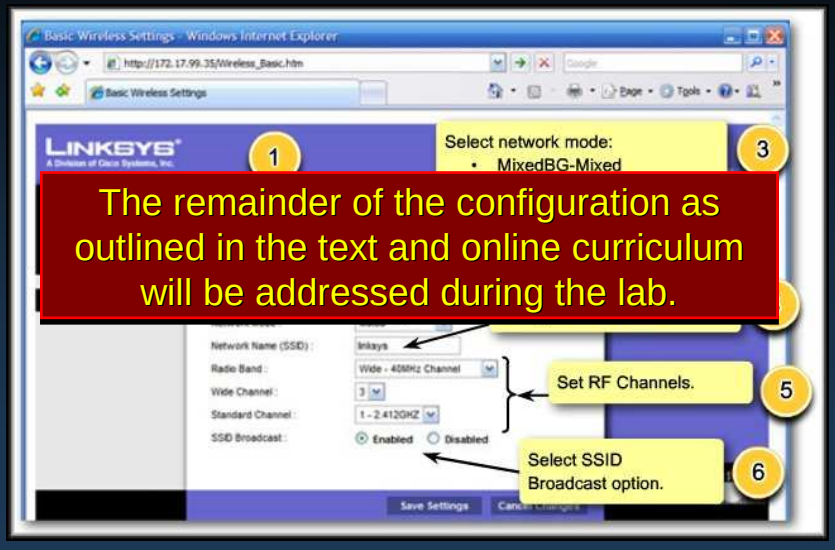
Configuring the Wireless Access Point

- 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.

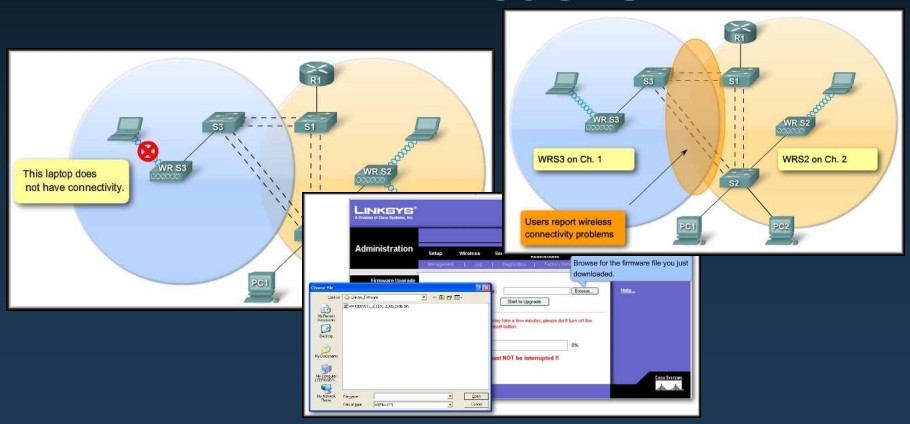
Configuring the Wireless Access Point

- 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.

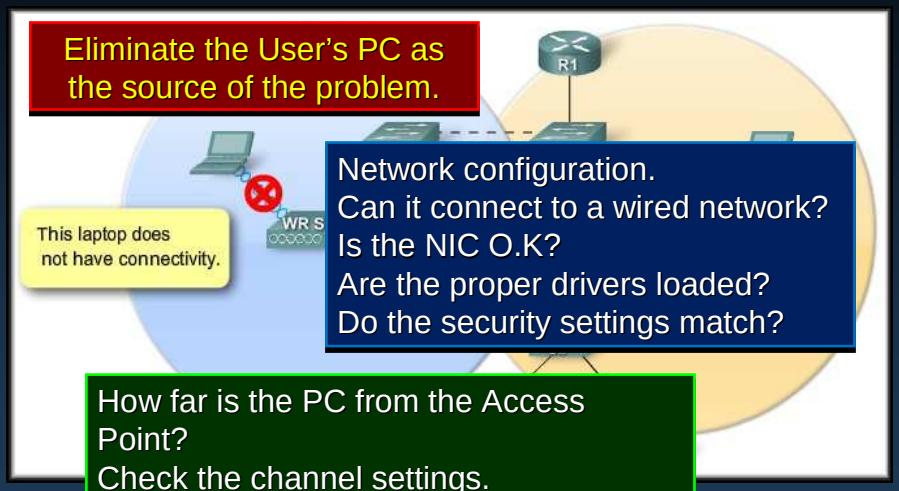
Configuring the Wireless Access Point



Troubleshooting Simple WLAN Problems



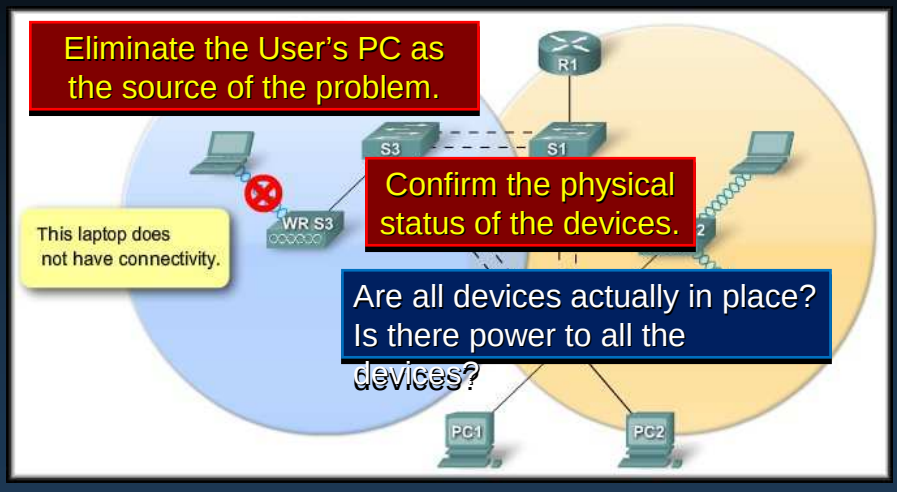
Eliminate the User's PC as the source of the problem.



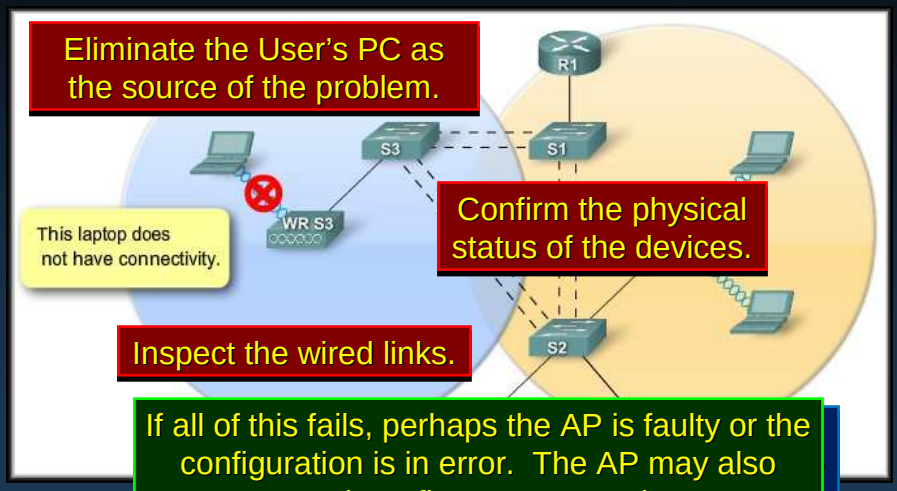
Network configuration.
Can it connect to a wired network?
Is the NIC O.K?
Are the proper drivers loaded?
Do the security settings match?

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

A Systematic Approach



A Systematic Approach

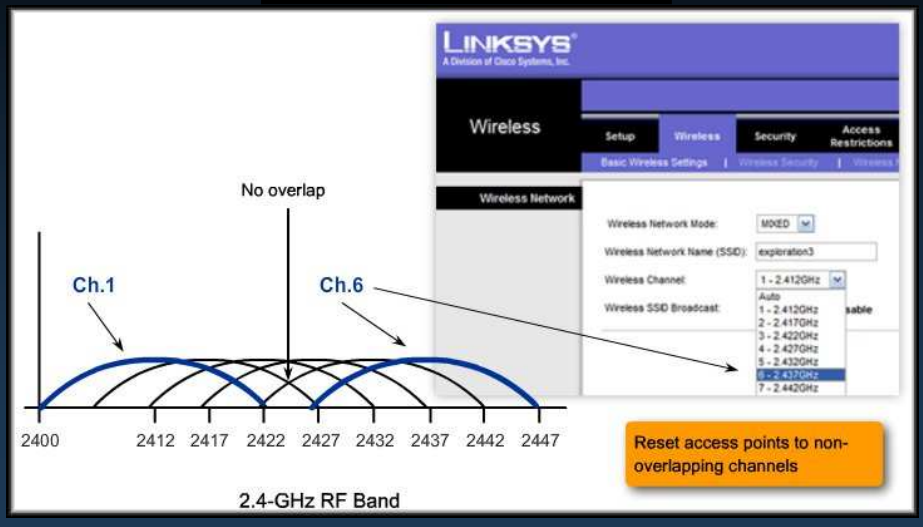


A Systematic Approach

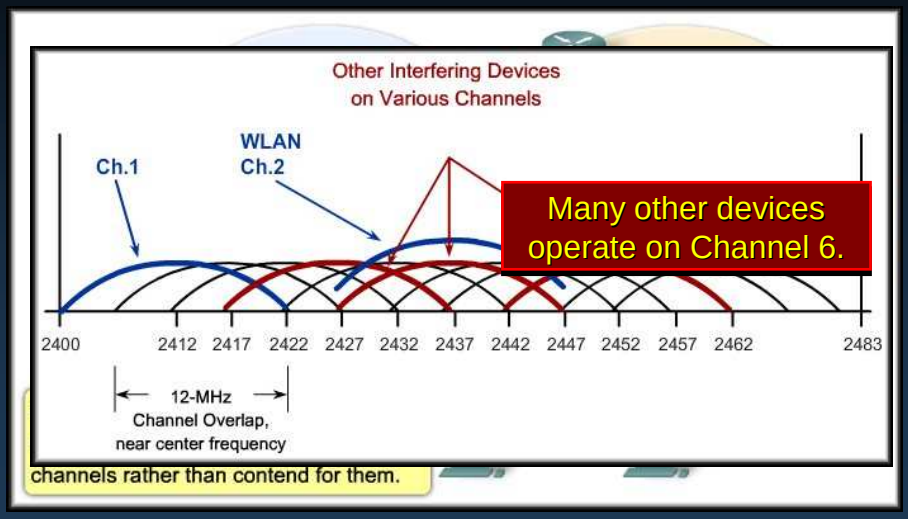
Updating the Access Point

A Systematic Approach

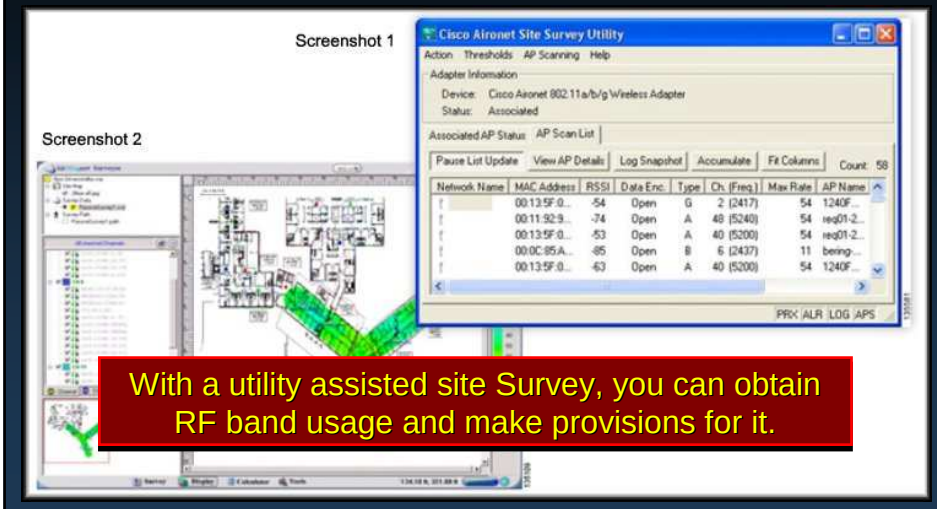
Incorrect Channel Settings



RF Interference Issues

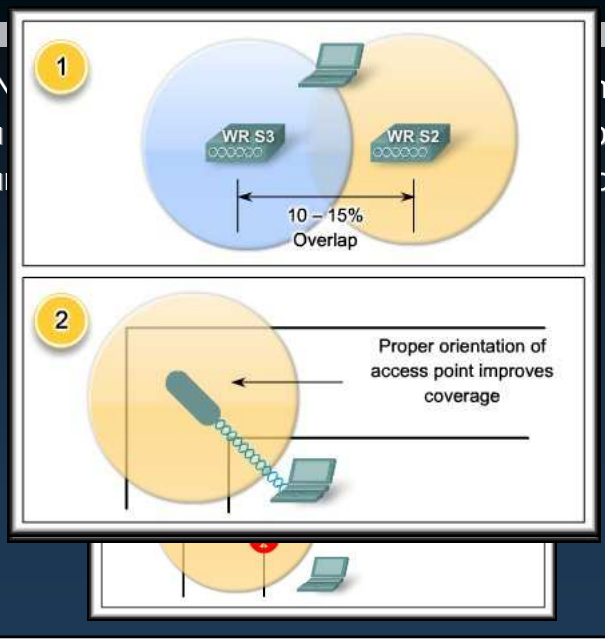


RF Interference Issues



Access Point Placement

- A WLAN
  - You
  - You



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

-