CSET 150

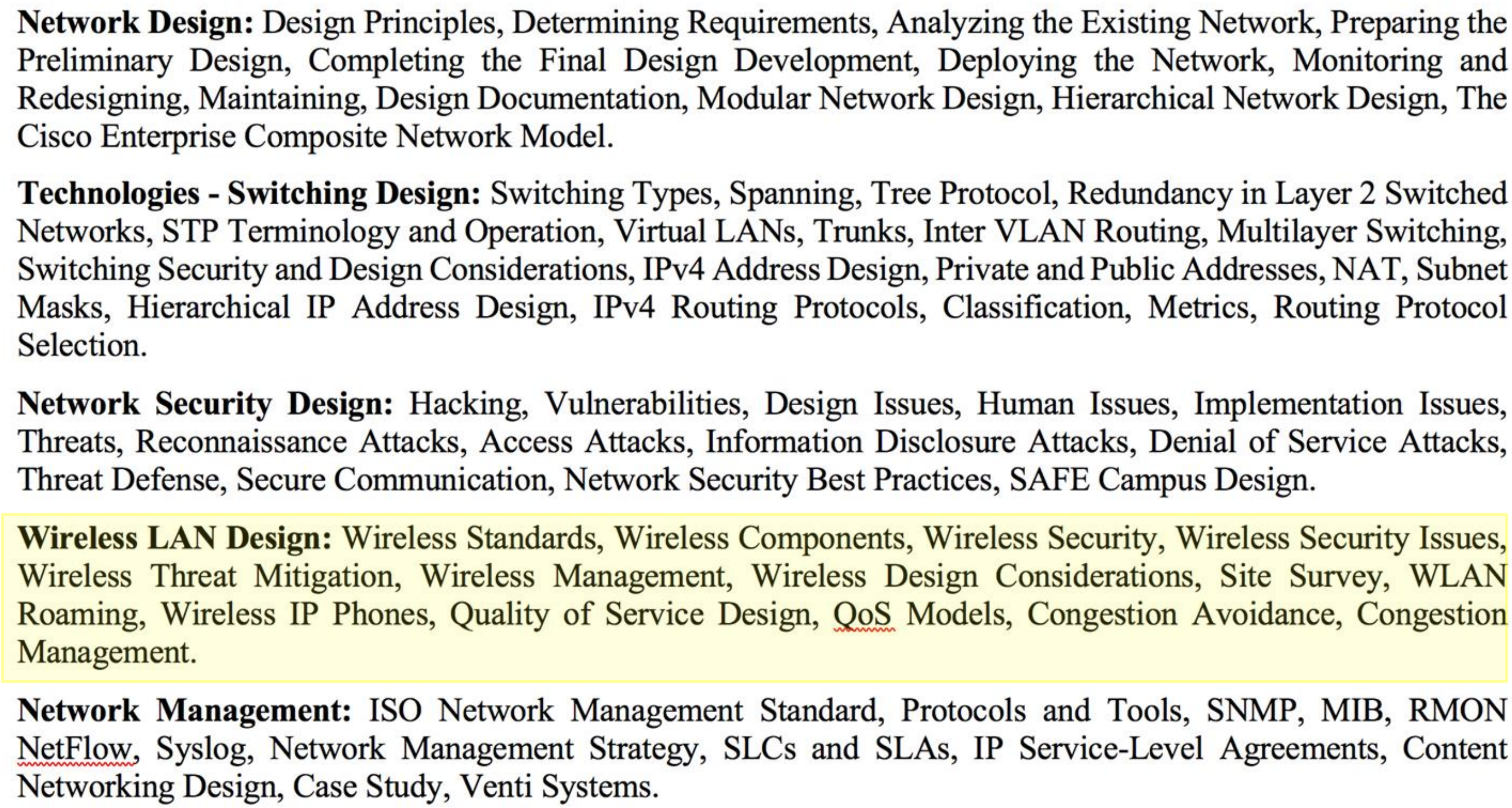
Network Design and Management

Evening Masters Edition

Dr. Mahboob Qaosar

Associate Professor, CSE, RU

COURSE CONTENTS



Network Design: Design Principles, Determining Requirements, Analyzing the Existing Network, Preparing the Preliminary Design, Completing the Final Design Development, Deploying the Network, Monitoring and Redesigning, Maintaining, Design Documentation, Modular Network Design, Hierarchical Network Design, The Cisco Enterprise Composite Network Model.

Technologies - Switching Design: Switching Types, Spanning, Tree Protocol, Redundancy in Layer 2 Switched Networks, STP Terminology and Operation, Virtual LANs, Trunks, Inter VLAN Routing, Multilayer Switching, Switching Security and Design Considerations, IPv4 Address Design, Private and Public Addresses, NAT, Subnet Masks, Hierarchical IP Address Design, IPv4 Routing Protocols, Classification, Metrics, Routing Protocol Selection.

Network Security Design: Hacking, Vulnerabilities, Design Issues, Human Issues, Implementation Issues, Threats, Reconnaissance Attacks, Access Attacks, Information Disclosure Attacks, Denial of Service Attacks, Threat Defense, Secure Communication, Network Security Best Practices, SAFE Campus Design.

Wireless LAN Design: Wireless Standards, Wireless Components, Wireless Security, Wireless Security Issues, Wireless Threat Mitigation, Wireless Management, Wireless Design Considerations, Site Survey, WLAN Roaming, Wireless IP Phones, Quality of Service Design, QoS Models, Congestion Avoidance, Congestion Management.

Network Management: ISO Network Management Standard, Protocols and Tools, SNMP, MIB, RMON NetFlow, Syslog, Network Management Strategy, SLCs and SLAs, IP Service-Level Agreements, Content Networking Design, Case Study, Venti Systems.

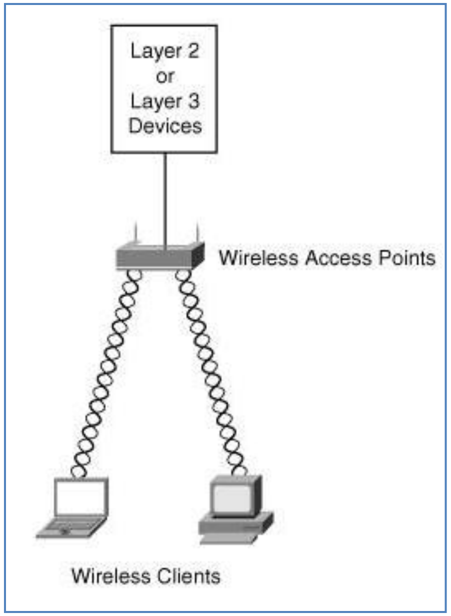
TYPES OF FRAMES

- In 802.11 …following types of frames are transferred over the airwaves:
  - **DATA FRAME:** Network traffic.
  - **CONTROL FRAME:**
    Frame controlling access to the medium, similar to a modem's analog connection control mechanism, with its
    Request To Send (RTS),
    Clear To Send (CTS), and
    acknowledgment (ACK) signals.
  - **MANAGER FRAME:**
    Frames similar to data frames, pertaining to the control of the current wireless transmission

WIRELESS COMPONENTS

- The main components of wireless networks are as follows:
  - Wireless access points
  - Wireless client devices

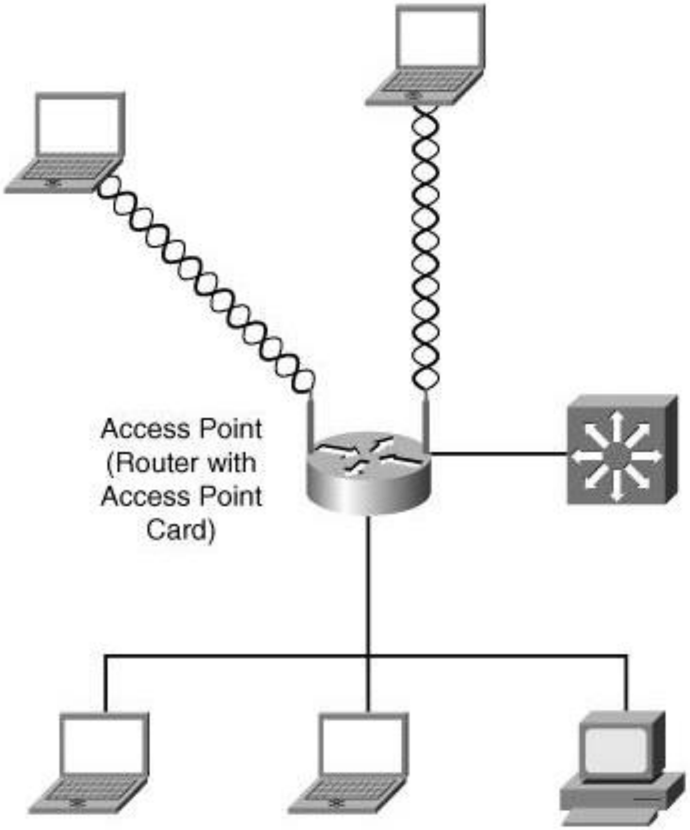
- **Wireless Access Points**
  - WAPs provide connectivity between wireless client devices and the wired network.



Wireless Access Points

- **Integrated Access Point**
  - The WAP does not need to be a stand-alone device.
  - Cisco offers integrated access point functionality for some small- to medium-business (SMB) routers
  - By installing a high-speed wireless interface card (HWIC) in Cisco 1800, 2800, or 3800 routers, customers can run concurrent routing, switching, and security services and include IEEE 802.11 wireless LAN functionality in a single platform.

WIRELESS ACCESS POINTS



WIRELESS CLIENT DEVICES

- Hardware:
  - ~~Wireless access points~~
  - Wireless client devices

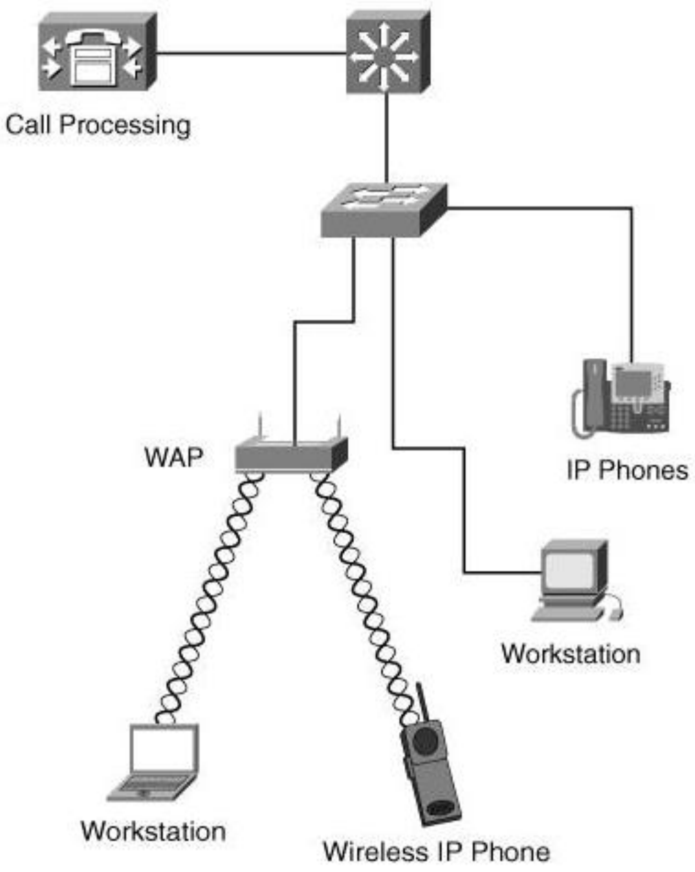
- **Wireless Client Devices**
  - A wireless client device is equipped with a wireless interface card (WIC), which the device uses to communicate over RF with WAPs.

Wireless Client Devices

- Wireless clients can be the following items:
  1. User workstations and laptops
  2. PDAs (tablets and smart phones)
  3. Wireless IP phones

- In addition to connecting to a WLAN access point, two wireless end stations can form an exclusive, point-to-point, wireless network without the intervention of an access point.
- This type of independent network is known as an ad-hoc network.

Deploying Wireless IP Phones



WIRELESS SECURITY

- **Wireless Security Issues**
  - A main issue with wireless communication is unauthorized access to network traffic or, more precisely, the watching, displaying, and logging of network traffic, also known as **sniffing**.
  - Contrary to a wired network, where a hacker would need to be **physically located** at the corporate premises to gain access through a network drop, with a wireless network, the intruder can access the network from a location outside the corporate building
  - Wireless equipment tends to ship with open access. Not only is traffic propagated in clear text, but WAPs also voluntarily broadcast their identity, known as **Service Set Identifiers (SSIDs)**

WIRELESS THREAT MITIGATION

- Wireless network security can be classified into the following three categories:
  1. Basic wireless security
  2. Enhanced wireless security
  3. Wireless intrusion detection

BASIC WIRELESS SECURITY

- **Basic Wireless Security**
  - Basic wireless security is provided by the following built-in functions:
    1. SSIDs
    2. Wired Equivalent Privacy (WEP)
    3. Media Access Control (MAC) address verification

SSIDs

- Service Set Identifiers ⇨ SSID
- An SSID is a code that identifies membership with a WAP.
- All wireless devices that want to communicate on a network must have their SSID set to the same value as the WAP SSID to establish connectivity with the WAP.
- By default, a WAP broadcasts its SSID every few seconds.
- This broadcast can be stopped so that a drive-by hacker can't automatically discover the SSID and hence the WAP.
- However, because the SSID is included in the beacon of every wireless frame, it is easy for a hacker equipped with sniffing equipment to discover the value and fraudulently join the network
- **Beacon Frame**
  - The WAP periodically advertises SSID and other network information using a special 802.11 management frame known as a beacon.

WIRED EQUIVALENT PRIVACY (WEP)

- WEP can be used to alleviate the problem of SSID broadcasts by encrypting the traffic between the wireless clients and WAPs.
- Joining a wireless network using WEP is referred to as , where the WAP sends a challenge to the wireless client who must return it encrypted.
- If the WAP can decipher the client's response, the WAP has the proof that the client possesses valid keys and therefore has the right to join the wireless network.
- WEP comes in two encryption strengths: 64-bit and 128-bit.

MAC Address Verification

- To further wireless security, a network administrator could use MAC address filtering, in which the WAP is configured with the MAC addresses of the wireless clients that are to be permitted access.
- Unfortunately, this method is also not secure because frames could be sniffed to discover a valid MAC address, which the hacker could then spoof.

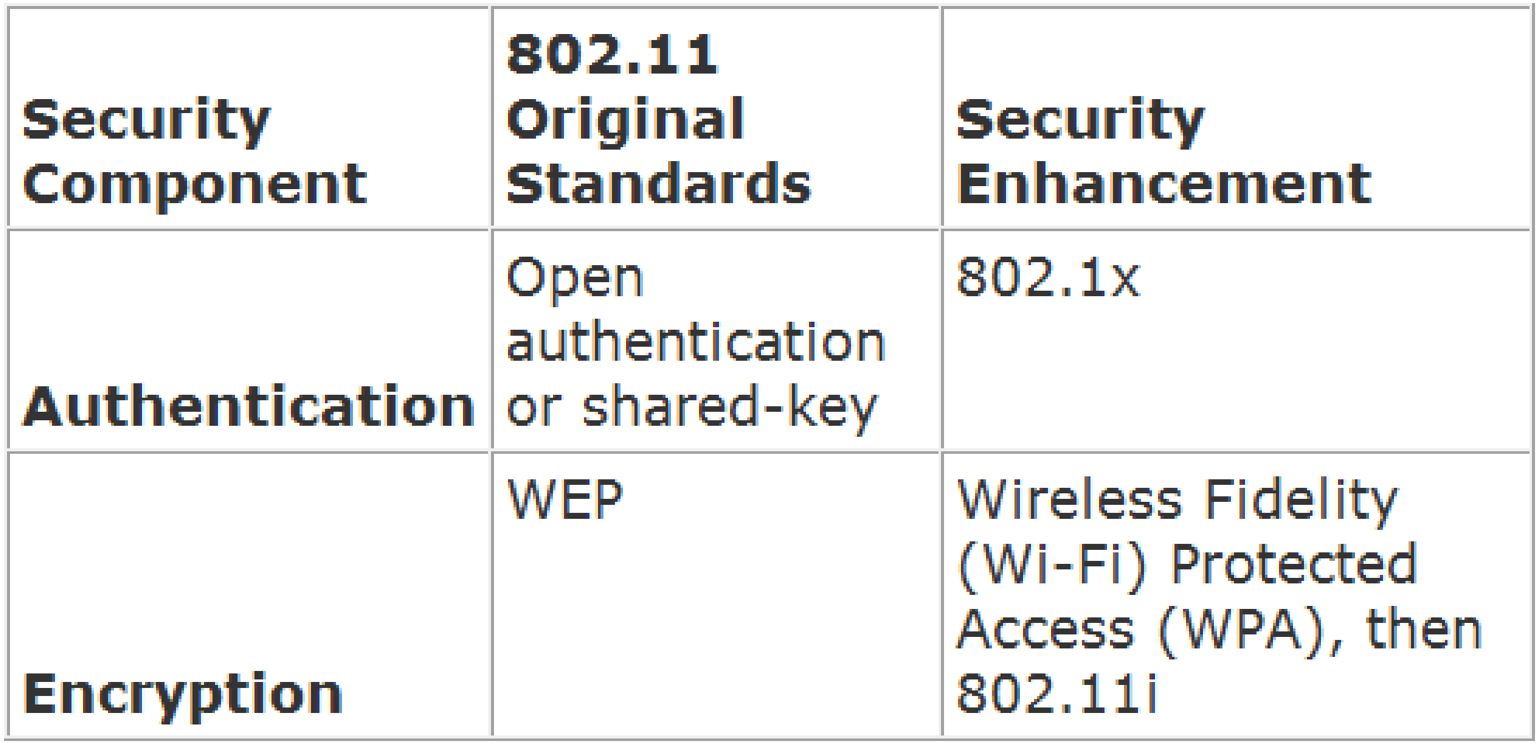
Enhanced Wireless Security

- Wireless network security can be classified into the following three categories:

  1. ~~Basic wireless security~~
     - SSIDs
     - Wired Equivalent Privacy (WEP)
     - Media Access Control (MAC) address verification

  2. Enhanced wireless security
  3. Wireless intrusion detection

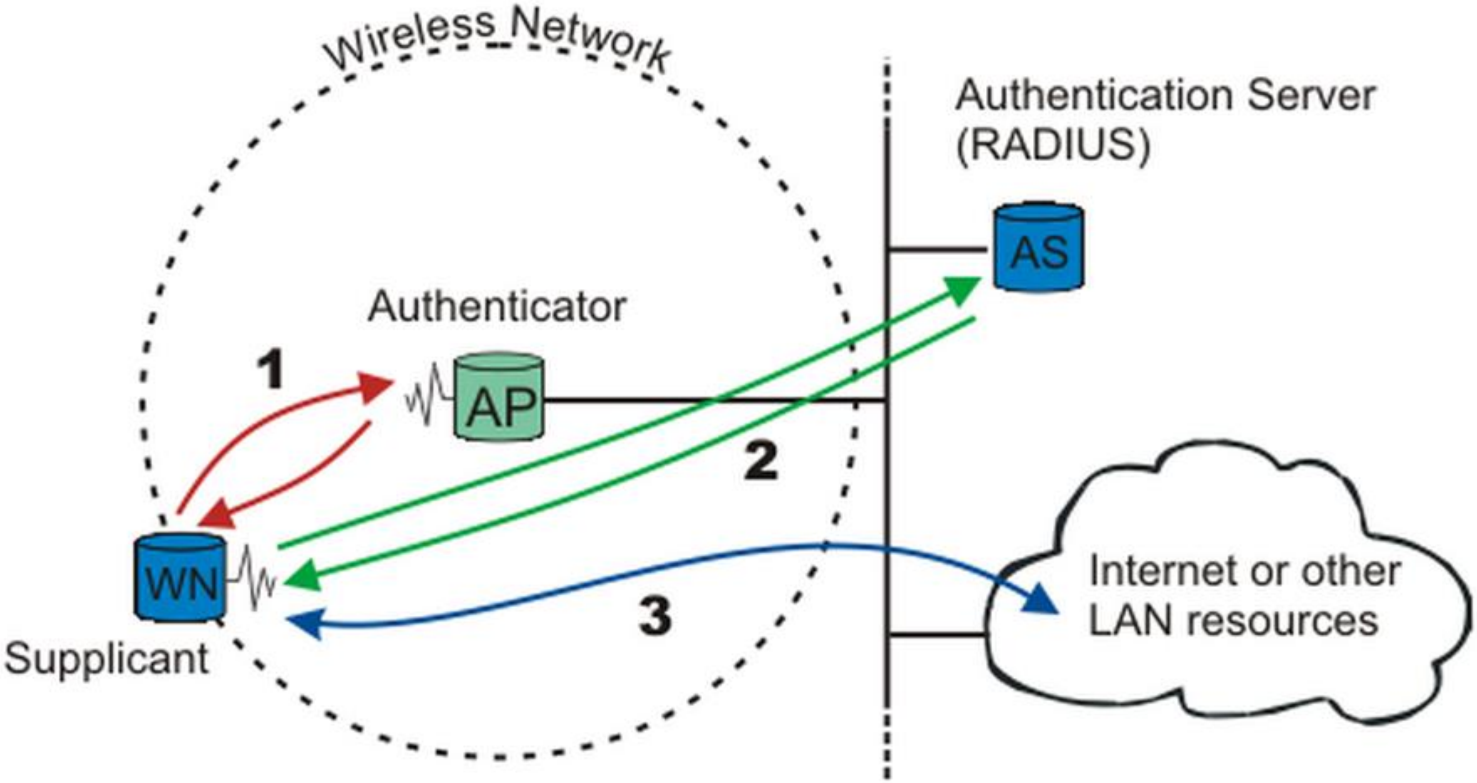
ENHANCED WIRELESS SECURITY



Security Component	802.11 Original Standards	Security Enhancement
Authentication	Open authentication or shared-key	802.1x
Encryption	WEP	Wireless Fidelity (Wi-Fi) Protected Access (WPA), then 802.11i

Enhanced Wireless Security

- **802.1x**
  - IEEE 802.1x is a port-based network access control standard.
  - It provides per-user, per-session, mutual strong authentication, not only for wireless networks but also for wired networks, if need be.



802.1x

- A wireless node must be authenticated before it can gain access to other LAN resources

1. When a new wireless node (WN) requests access to a LAN resource, the access point (AP) asks for the WN's identity.
   - *No other traffic than EAP is allowed before the WN is authenticated.*
   - Extensible Authentication Protocol, or EAP
2. After the identity has been sent, the authentication process begins.
   - The protocol used between the Supplicant and the Authenticator is EAP
   - The Authenticator re-encapsulates the EAP messages to RADIUS format, and passes them to the Authentication Server.
   - Remote Authentication Dial In User Service (RADIUS)
3. After a successful authentication, the Supplicant is granted access to other LAN resources/Internet

WIRELESS DESIGN CONSIDERATIONS

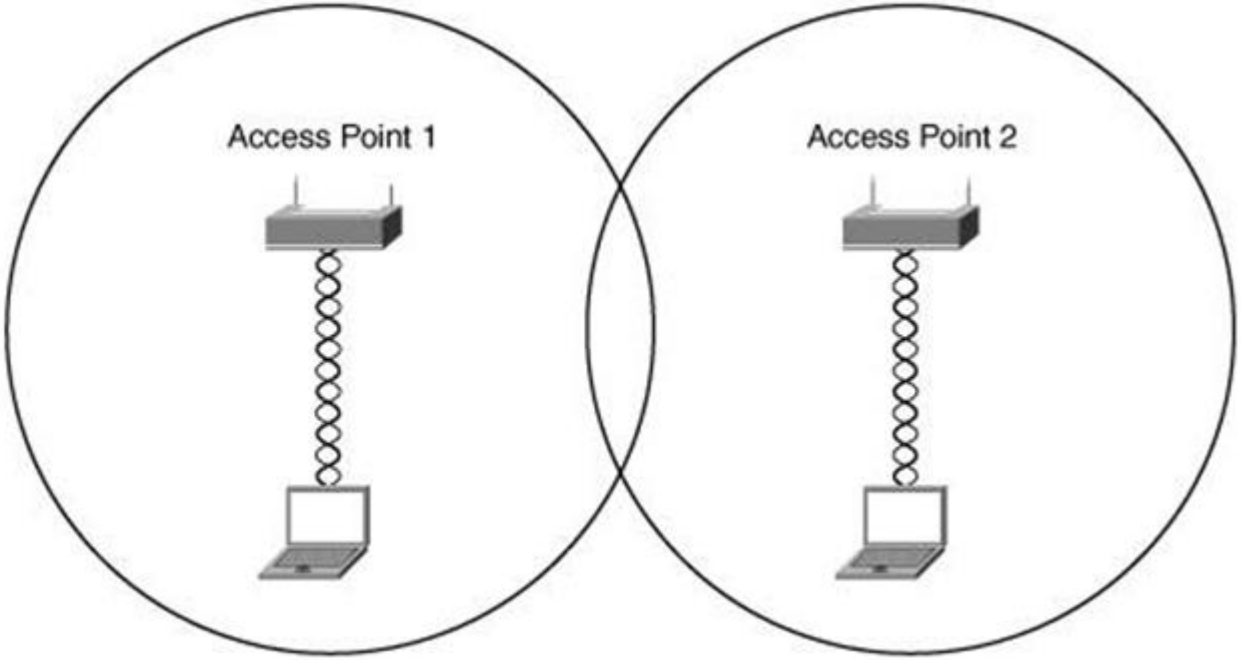
- Some items that should be considered when designing and provisioning a wireless network:

1. **Site Survey**
2. **WLAN Roaming**
3. **Point-to-Point Bridging**

Site Survey

- You should ask the following questions:
  - Which **wireless system** is best suited for the application?
    - b/g/n ?
  - Does a **line-of-sight requirement** exist between antennas?
  - Where should the WAP be located so that it is **as close as possible to clients?**
  - What potential sources of interference are in this building?
  - Should any federal, provincial, or local regulations and legislation be considered in this deployment?

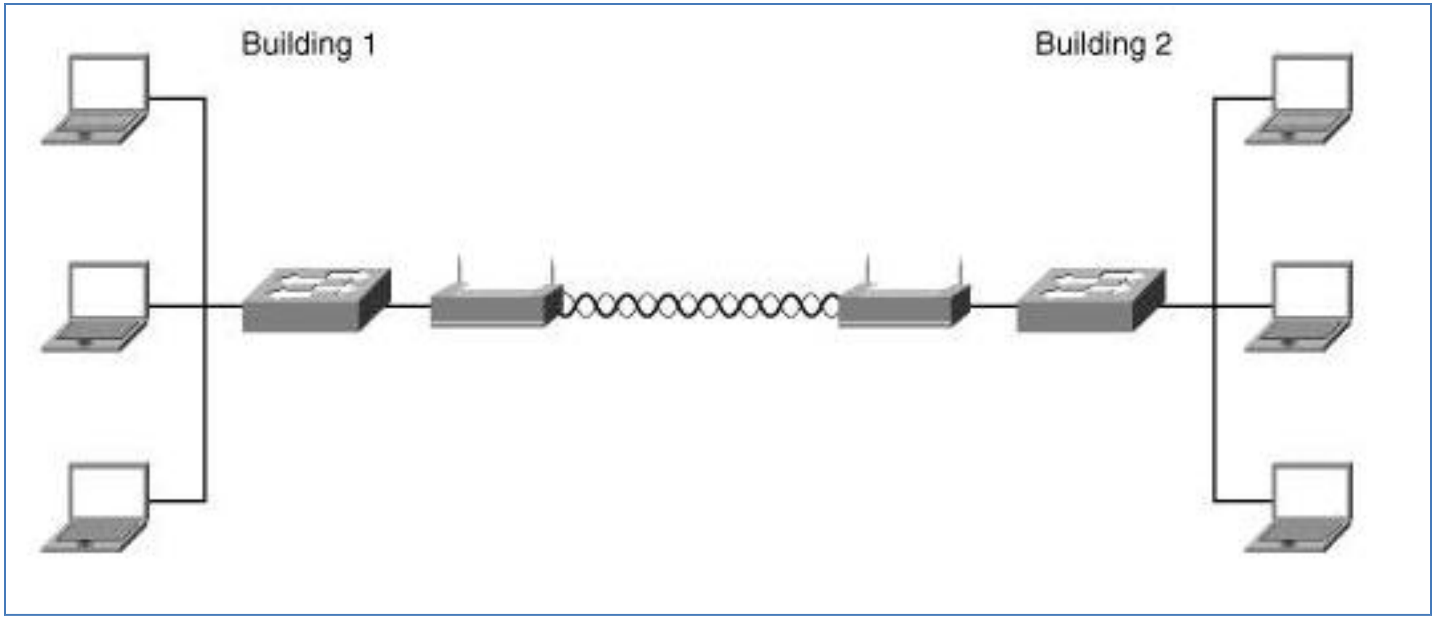
WLAN Roaming



- Could be Layer2 or Layer 3.
- This problem could be more easily solved with rudimentary planning and by using non-overlapping channels.
- Channels 1, 6, and 11 do not overlap

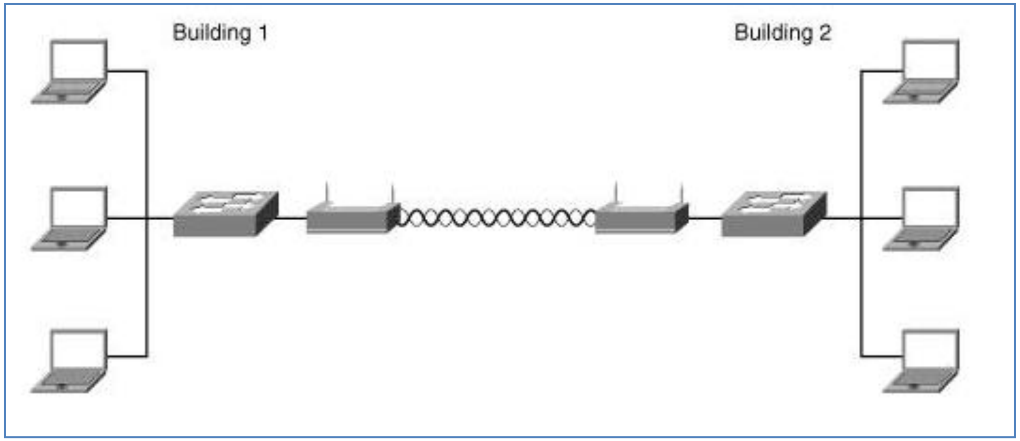
Point-to-Point Bridging

- It is not always feasible to run a network cable between two buildings to join their respective LANs.
- If the two buildings are a reasonable distance apart and preferably in direct **line of sight** with each other, wireless bridges can be configured.



POINT-TO-POINT BRIDGING

- It takes two WAPs to create one logical two-port bridge.
- In this mode, WAPs are operating in a **dedicated point-to-point bridge mode** and therefore are no longer operating as wireless access points for clients.



DESIGN CONSIDERATIONS FOR WIRELESS IP PHONES

- a system administrator should conduct another site survey.
- Another consideration for wireless IP phones is roaming.
  - Its need to be Layer2 Roaming
  - With Layer 2 roaming, devices keep their IP address and therefore the changing to another switch would not be noticeable by users.
  - Layer 3 roaming would mean that a device would have to change its IP address; this would mean an interruption in the user's connection.
  - If the connection was to a wireless IP phone, the call would be disconnected; this scenario would likely be **unacceptable** to users