Module 14

Wireless Fundamentals

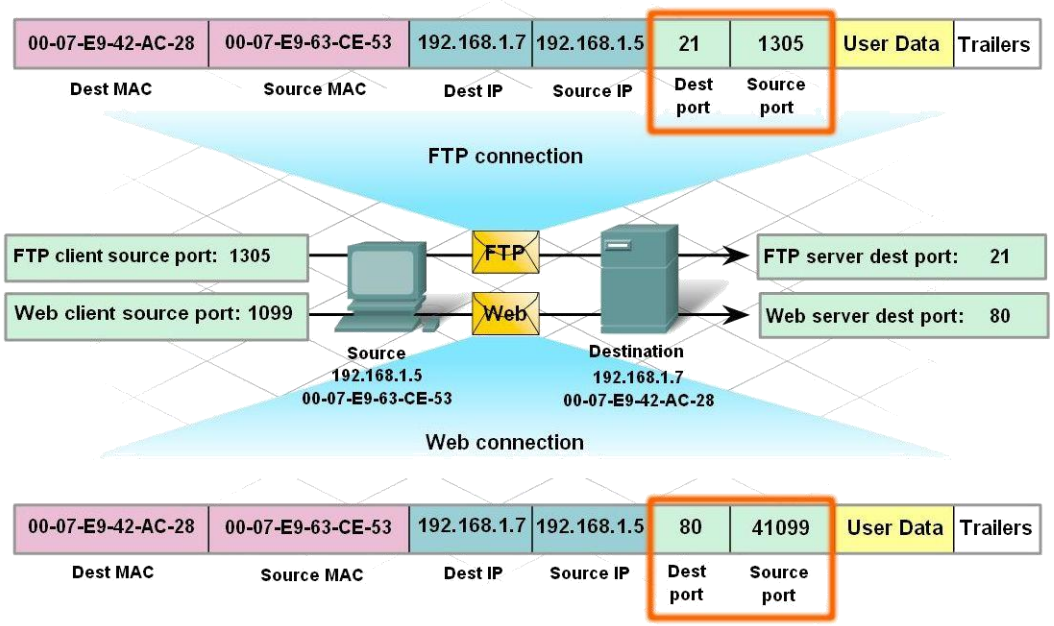
Objectives

1. Wireless and SOHOs
   A. 2.4 Explain common TCP and UDP ports, protocols and their purpose
   B. 2.5 Compare and contrast wireless networking standards and encryption types
   C. 2.6 Install, configure, and deploy a SOHO wireless/wired router using appropriate settings

PORTS AND PROTOCOLS

Port Numbers in Client-Server Conversations

The destination port number is used to determine which applications or protocol should be used to handle the incoming segment



Common Port Numbers

Destination Port	Protocol	Definition
20 & 21	FTP	File Transfer Protocol (20 for data; 21 for control)
23	TELNET	TELetype NETwork
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Service
69	TFTP	Trivial File Transfer Protocol
80	HTTP	Hypertext Transfer Protocol
110	POP3	Post Office Protocol version 3
143	IMAP4	Internet Message Access Protocol version 4
67	DHCP v4 Client	Dynamic Host Configuration Protocol (Client)
68	DHCP v4 Server	Dynamic Host Configuration Protocol (Server)
443	HTTPS	Hypertext Transfer Protocol Secure
3389	RDP	Remote Desktop Protocol

Protocols

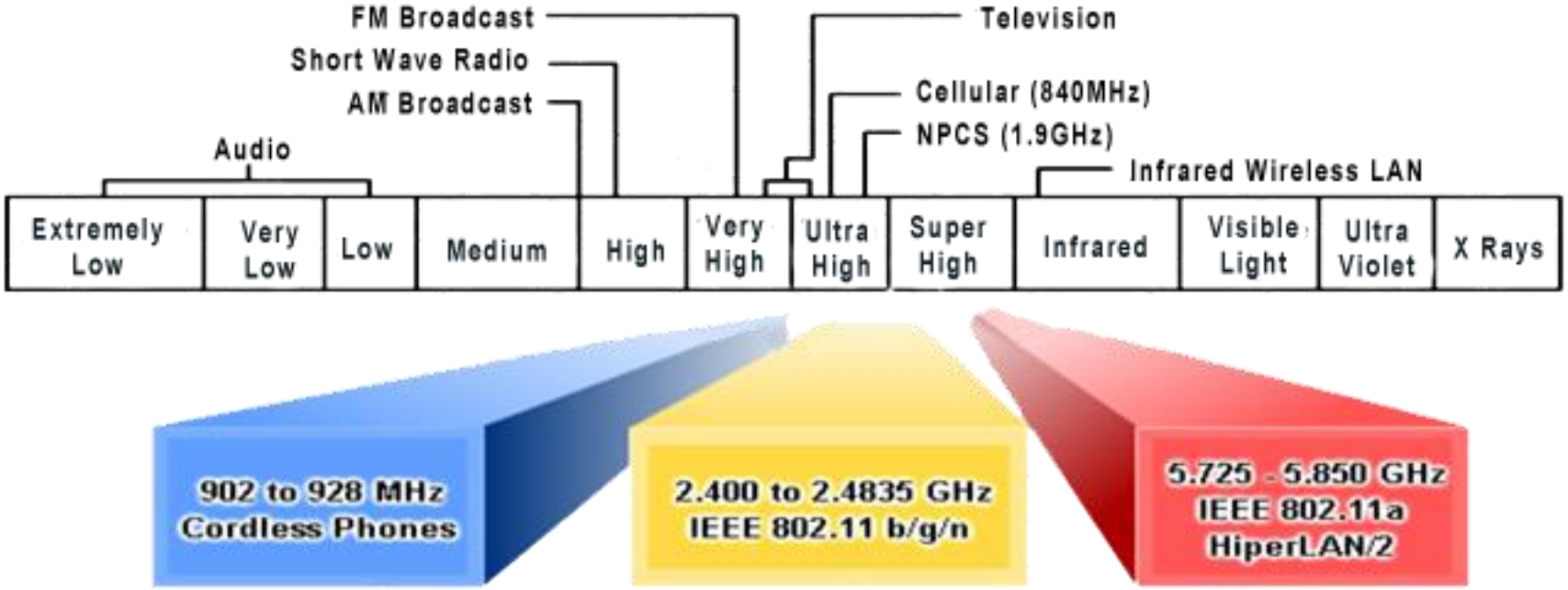
Protocol	Name	Definition
DHCP	Dynamic Host Configuration Protocol	Service to automatically assign IP address information to requesting clients.
DNS	Domain Name Service	Service to translate domain names into IP addresses.
LDAP	Lightweight Directory Access Protocol	Services to provide any organized set of records or directory to a requesting client.
SNMP	Simple Network Management Protocol	Used to monitor network-attached devices for conditions that warrant administrative attention.
SMB	Server Message Block	Used for providing shared access to files, printers, and authenticated communications between nodes on a network.
CIFS	Common Internet File System	Another name for SMB.
SSH	Secure Shell	Used for secure data communication between two networked computers.
SFTP	Secure File Transfer Protocol	Provides secure file access, file transfer, and file management functionality.
FTP	File Transfer Protocol	Used to transfer authenticated files from one host to another host over a TCP-based network.
TFTP	Trivial File Transfer Protocol	Used to transfer unauthenticated files from one host to another host over a TCP-based network.

A **Protocol** is a set of rules used to exchange information between computing systems.

WIRELESS

Wireless Technologies

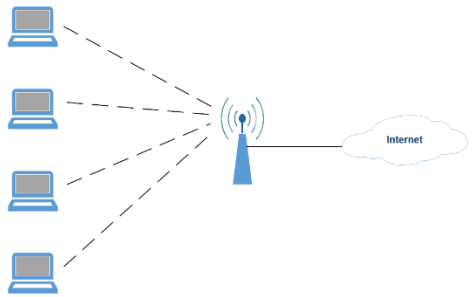
Uses infrared light and radio frequency transmissions as its signally technologies



Wireless LAN (WLAN)

Advantages:

1. Mobility = easy connection of both stationary and mobile clients
2. Scalability = ease of adding additional devices
3. Flexibility = anytime, anywhere connectivity
4. Cost Savings = inexpensive to install
5. Reliability = easy to install



Wireless Topologies

1. WPAN - devices dedicated to a single host
2. WLAN - used to extend the boundaries of the local wired network
   A. IEEE 802.11 standards
3. WWAN – covers extremely large areas
   A. Technologies such as Code Division Multiple Access (CDMA) or Global System for Mobile Communication (GSM)

	WPAN	WLAN	WWAN
Standards	Bluetooth v2.0+	IEEE 802.11 a/b/g/n/ac	GSM, GPRS, CDMA
Speed	<3 Mbps	1 Mbps – 1 Gbps	10-384 Kbps
Range	Short	Medium	Long
Applications	Peer-to-Peer Device-to-Device	Home, Small Business, and Enterprise Networks	PDAs, Mobile Phones, Cellular Access

4. Each uses a higher power output to increase its coverage

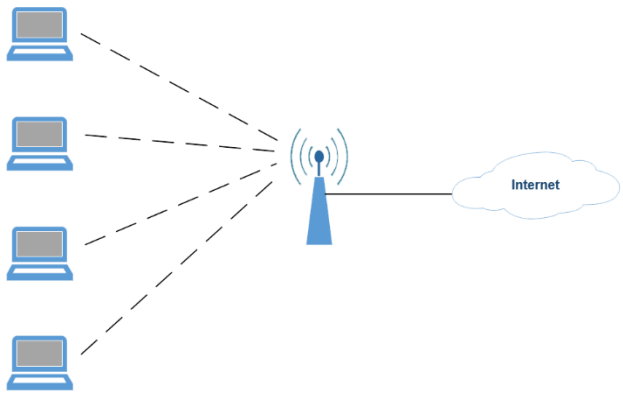
Wireless LAN Standards

Allow users to connect wireless hosts to other hosts or services on a wired Ethernet network

Standard	Release Date	Frequency	Data Rate (Max)	Max Range*
802.11	July 1997	2.4 GHz	2 Mbps	Undefined
802.11a	October 1999	5 GHz	54 Mbps	50 m
802.11b	October 1999	2.4 GHz	11 Mbps	100 m
802.11g	June 2003	2.4 GHz	54 Mbps	100 m
802.11n	April 2007	2.4 GHZ or 5 GHz	540 Mbps	250 m
802.11ac	2014	2.4 GHZ or 5 GHz	1 Gbps	Undefined
*The maximum range may vary greatly under different conditions.				

Components and Structure of a WLAN

1. **Access Points** control access between a wired and a wireless network
2. A **wireless bridge** connect two networks with a wireless link
3. Wireless clients are commonly referred to as a **STA** or **Station**



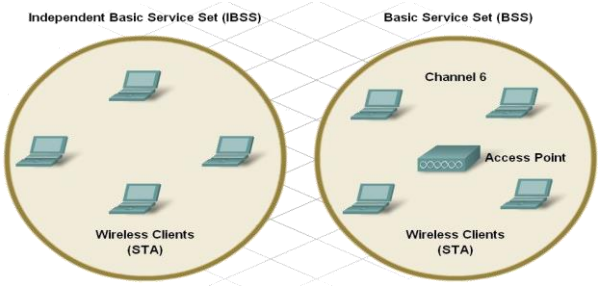
Service Set Identifier (SSID)

1. Name that identifies a wireless network
2. Case-sensitive, alpha-numeric string that is up to 32-characters
3. Tells a wireless device to which WLAN it belongs
4. All wireless devices on the same WLAN must have the same SSID
5. Sent in the header of all frames transmitted over the WLAN

Wireless Modes

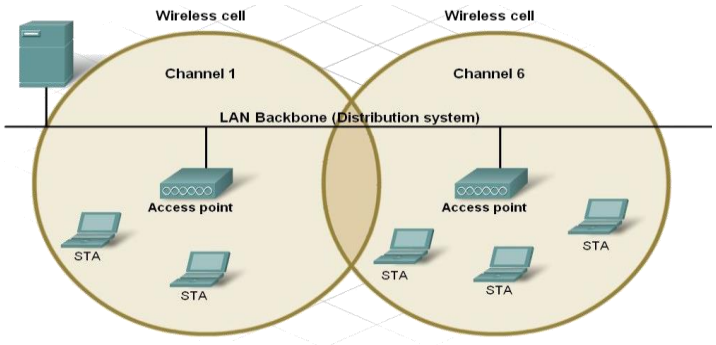
Two wireless modes:

1. **Ad-hoc Mode -** created by connecting clients in a peer-to-peer network. Does not use an AP
   A. **Independent Basic Service Set** (IBSS)
2. **Infrastructure Mode** - The AP controls all communications and ensures that all STAs have equal access to the medium
   A. **Basic Service Set** (BSS) – uses a single AP
   B. **Extended Service Set** (ESS) uses multiple APs, each being an separate BSS



Components and Structure of a WLAN

1. Channels are created by dividing up the available RF spectrum
2. Each channel is capable of carrying a different conversation
3. Uses an access method called **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**
   A. Creates a reservation on the channel
   B. While a reservation is in place, no other device may transmit on the channel



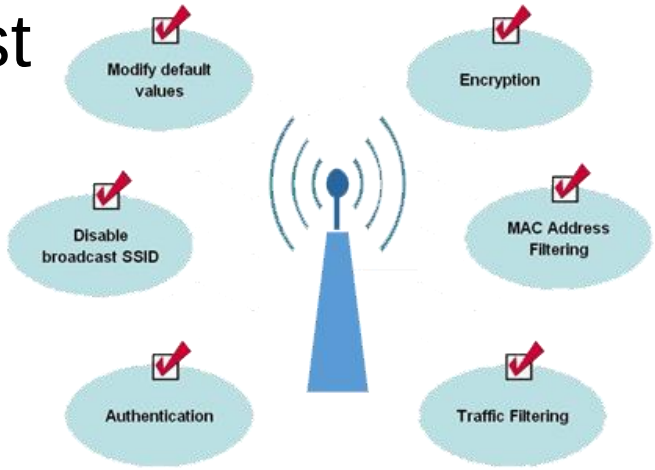
INSTALL, CONFIGURE AND DEPLOY A WIRELESS NETWORK

Planning the WLAN

1. A **site survey** – process of evaluating a network solution to deliver the required coverage, data rates, network capacity, roaming capacity, and quality of service
2. Factors that affect the number of access points needed:
   A. The size of the building
   B. The number of solid interior walls in the building
   C. The present high voltage equipment (i.e. microwave ovens)
   D. Existing implementations
   E. Bandwidth requirements
3. **Total Cost of Ownership** (TCO)

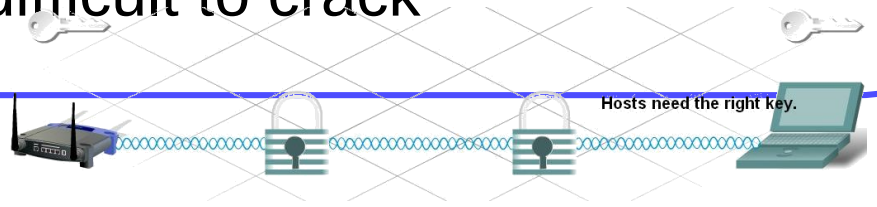
Wireless LAN Security

1. Important because wireless inherently allows easy access
2. Strategies:
   A. Change the default IP, username and password
   B. Disable the SSID broadcast
   C. Apply strong encryption
   D. Apply authentication
   E. Apply MAC filters
   F. Apply traffic filtering



Encryption

1. The encoding of wireless data to prevent intercepted data from being read by a hacker
2. Encryption methods:
   - **A. (WEP) Wired Equivalency Protocol**
     - Uses key lengths of 64 and 128 bits
   - **B. (WPA) Wi-Fi Protected Access**
     - Uses encryption keys from 64 bits up to 256 bits
     - Generates new dynamic keys each time a client establishes a connection with the AP
     - Considered more secure than WEP because it is significantly more difficult to crack



Encryption

1. **AES** (**Advanced Encryption Standard**)
   A. Adopted and used worldwide
   B. The algorithm described by AES is a symmetric-key algorithm
2. **TKIP** (**Temporal Key Integrity Protocol**)
   A. Used in the IEEE 802.11
   B. Designed to replace WEP without requiring the replacement of legacy hardware

Authentication

Authentication methods:

1. **Open**
   A. does not require a secret word
   B. Used on APs by default
2. **Extensible Authentication Protocol (EAP)**
   A. require an encrypted secret word
   B. Uses two-way authentication
3. **Pre-shared keys (PSK)**
   A. require an encrypted secret word
   B. Uses one-way authentication

MAC Address and Traffic Filtering

1. **MAC address filtering**
   A. Uses the MAC address to identify which devices are allowed to connect to the wireless network
2. **Traffic filtering**
   A. Allows a network administrator to block undesirable traffic from entering or leaving the wireless network

Summary

In this module we discussed:

1. Common ports and protocols
2. Types of wireless
3. Wireless topologies
4. Wireless standards
5. Wireless equipment
6. Wireless modes
7. Wireless configuration