

Lecture (06)

Wireless Networks

Dr. Ahmed M. ElShafee

Dr. Ahmed ElShafee, ACU Fall 2013, Network I

Introduction

- A *wireless network* is a network that uses radio signals rather than direct cable connections to exchange information.
- A wireless network is often referred to as a *WLAN*, for *wireless local area network*.
- The term *Wi-Fi* is often used to describe wireless networks, although it technically refers to just one form of wireless networks: the 802.11b/g/n standards.
- A wireless network has a name, known as a *SSID*.
- SSID stands for *service set identifier* Each of the computers that belong to a single wireless network must have the same SSID.

Dr. Ahmed ElShafee, ACU Fall 2013, Network I

Revision

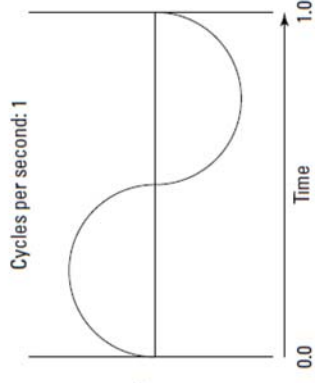
Waves and frequencies

- *radio* consists of electromagnetic waves that are sent through the atmosphere.
- radio receivers can pick them up and convert them into sounds, images, or — in the case of wireless networks — data.
- Radio waves are actually cyclical waves of electronic energy (Electromagnetic) that repeat at a particular rate, called the *frequency*
- The measure of a frequency is *cycles per second*, which indicates how many complete cycles the wave makes in one second

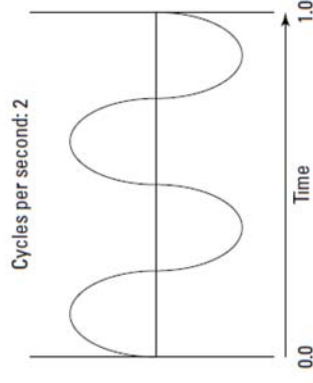
Dr. Ahmed ElShafee, ACU Fall 2013, Network I

- Wireless networks can transmit over any of several channels.
- In order for computers to talk to each other, they must be configured to transmit on the same channel.
- The simplest type of wireless network consists of two or more computers with wireless network adapters.
- This type of network is called an *ad-hoc mode network*.
- A more complex type of network is an *infrastructure mode network*.
- All this really means is that a group of wireless computers can be connected not only to each other, but also to an existing cabled network via a device called a *wireless access point*, or AP.

Dr. Ahmed ElShafee, ACU Fall 2013, Network I



- *cycles per second* is usually referred to as *Hertz*, abbreviated *Hz*.
- 1 Hz is one cycle per second. Incidentally, when the prefix *K* (for *kilo*, or 1,000), *M* (for *mega*, 1 million), or *G* (for *giga*, 1 billion) is added to the front of *Hz*.



Dr. Ahmed ElShafee, ACU Fall 2013, Network I

3

Dr. Ahmed ElShafee, ACU Fall 2013, Network I

Wavelength and antennas

- A term related to frequency is *wavelength*.
- Radio waves travel at the speed of light.
- The term *wavelength* refers to how far the radio signal travels with each cycle.

$$F = C/\lambda$$

- the wavelength decreases as the frequency increases.
- The wavelength of a typical AM radio station broadcasting at 580 KHz is about 500 meters.
- For a TV station broadcasting at 100 MHz, it's about 3 meters.
- For a wireless network broadcasting at 2.4 GHz, the wavelength is about 12 centimeters.

Dr. Ahmed ElShafee, ACU Fall 2013, Network I

4

Dr. Ahmed ElShafee, ACU Fall 2013, Network I

- Transmitters can be tuned to broadcast radio waves at a certain frequency.
- Likewise, receivers can be tuned to receive radio waves at a certain frequency, ignoring waves at other frequencies.
- That's why you can tune the radio in your car to listen to dozens of different radio stations: Each station broadcasts at its own frequency.

- It turns out that the shorter the wavelength, the smaller the antenna needs to be in order to adequately receive the signal.
- higher frequency transmissions need smaller antennas.

Spectrums, FCC, and ETSI

- The term *spectrum* refers to a continuous range of frequencies on which radio can operate.
- In the United States, the Federal Communications Commission (FCC) governs spectrum usage and allocation.
- In Europe and MENA, ETSI governs spectrum usage and allocation.
- radio spectrum is devised into dozens of small ranges called *bands* and restricted certain uses to certain bands.
- For example, AM radio operates in the band from 535 KHz to 1,700 KHz.

Popular Bands of the Radio Spectrum

Band	Use
535 KHz–1,700 KHz	AM radio
5.9 MHz–26.1 MHz	Short wave radio
26.96 MHz–27.41 MHz	Citizens Band (CB) radio
54 MHz–88 MHz	Television (VHF channels 2 through 6)
88 MHz–108 MHz	FM radio
174 MHz–220 MHz	Television (VHF channels 7 through 13)
470 MHz–806 MHz	Television (UHF channels)
806 MHz–890 MHz	Cellular networks
900 MHz	Cordless phones
1850 MHz–1990 MHz	PCS cellular
2.4 GHz–2.4835 GHz	Cordless phones and wireless networks (802.11b and 802.11g)
4 GHz–5 GHz	Large dish satellite TV
5 GHz	Wireless networks (802.11a)
11.7 GHz–12.7 GHz	Small dish satellite TV

802.11

- The most popular standards for wireless networks are the IEEE 802.11 standards.
- These standards are essential wireless Ethernet standards and use many of the same networking techniques that the cabled Ethernet standards (in other words, 802.3)
- The 802.11 standards address the bottom two layers of the IEEE seven-layer model: The Physical layer and the data link layer.
- Note that TCP/IP protocols apply to higher layers of the model.
- As a result, TCP/IP runs just fine on 802.11 networks.

OSI TCP/IP

Application		Application
Presentation		
Session		
Transport		Transport
Network		Internetwork
Data Link		Network Interface
Physical		

- The original 802.11 standard was adopted in 1997.
- Two additions to the standard, 802.11a and 802.11b, were adopted in 1999.
- The latest and greatest versions are 802.11g and 802.11n.

802.11 Variations

Standard	Speeds	Frequency
802.11a	Up to 54 Mbps	5 GHz
802.11b	Up to 11 Mbps	2.4 GHz
802.11g	Up to 54 Mbps	2.4 GHz
802.11n	Up to 300Mbps (but most devices are in the 100Mbps range)	2.4GHz

Ranges

- The maximum range of an 802.11g wireless device indoors is about 100 meters.
- Although the normal range for 802.11g is 100 meters , the range may be less in actual practice.
- Obstacles such as solid walls, bad weather, cordless phones, microwave ovens, nuclear reactors, all can conspire together to reduce the effective range of a wireless adapter.
- Also, wireless networks tend to slow down when the distance increases.
- 802.11g network devices claim to operate at 54 Mbps, but they usually achieve that speed only at ranges of 30 meters or less.

Wireless Network Adapters

- The wireless network adapter is similar to the network interface card (NIC) that's used for a standard Ethernet connection.
- However, instead of having a cable connector on the back, a wireless network adapter has an antenna.



Wireless Access Points

- *wireless access point*, also known as a *AP*.
- AP actually performs two functions:
 - First, it acts as a central connection point for all your computers that have wireless network adapters.
 - In effect, the AP performs essentially the same function as a hub or switch performs for a wired network.
 - Second, the AP links your wireless network to your existing wired network so that your wired computer and your wireless computers get along like one big happy family.

14

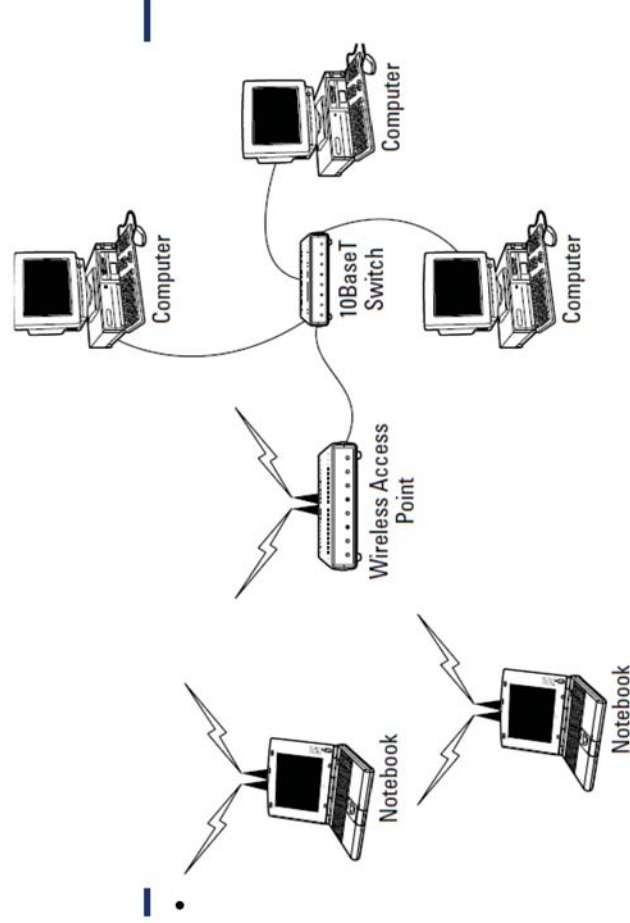
Dr. Ahmed ElShafee, ACU Fall 2013, Network I

Infrastructure mode

- When you set up a wireless network with an access point, you are creating an *infrastructure mode* network.
- It's called *infrastructure mode* because the access point provides a permanent infrastructure for the network.
- The access points are installed at fixed physical locations, so the network has relatively stable boundaries.
- Whenever a mobile computer comes into the range of one of the access points, it has come into the sphere of the network and can connect.

15

Dr. Ahmed ElShafee, ACU Fall 2013, Network I



Wireless Network

10BaseT Network

16

Dr. Ahmed ElShafee, ACU Fall 2013, Network I

- An access point and all the wireless computers that are connected to it are referred to as a *Basic Service Set*, or *BSS*.
- Each BSS is identified by a *Service Set Identifier*, or *SSID*.
- When you configure an access point, you specify the SSID that you want to use.
- The SSID is often a generic name such as *wireless*, or it can be a name that you create.

17

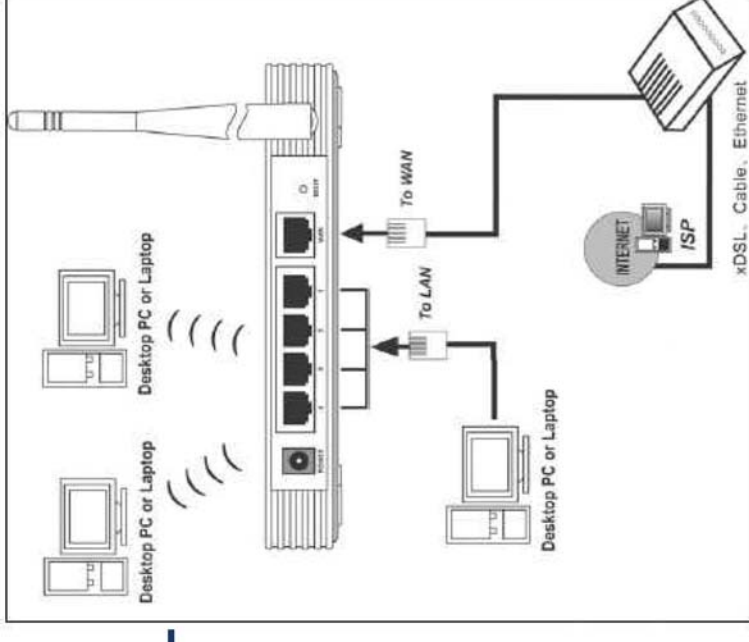
Dr. Ahmed ElShafee, ACU Fall 2013, Network I

Multifunction WAPs

- Wireless access points often include other built-in features.
- For example, some access points double as Ethernet hubs or switches, In that case, the access point will have more than one RJ-45 port.
- In addition, some access points include broadband cable or DSL firewall routers that enable you to connect to the Internet.

٢١

Dr. Ahmed ElShafee, ACU Fall 2013, Network I



٢٢

Roaming

- You can use two or more wireless access points to create a large wireless network in which computer users can roam from area to area and still be connected to the wireless network.
- As the user moves out of the range of one access point, another access point automatically picks up the user and takes over without interrupting the user's network service.

٢٣

Dr. Ahmed ElShafee, ACU Fall 2013, Network I

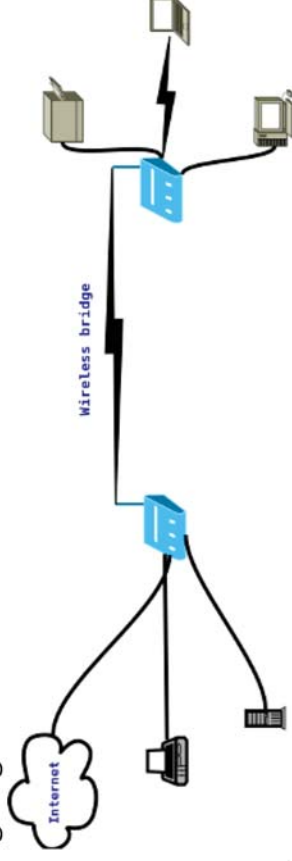
- A multifunction access point that's designed to serve as an Internet gateway for home networks .
 - 802.11b wireless access enables users to connect their PCs wireless
 - A four-port 10/100 MHz switch that I can connect up to four computers to via twisted-pair cable.
 - A DSL/cable router that connect user network to internet.
- This enables all the computers on the network (cabled and wireless) to access the Internet.

٢٤

Dr. Ahmed ElShafee, ACU Fall 2013, Network I

Wireless bridging

- Another use for wireless access points is to bridge separate subnets that can't easily be connected by cable.
- Connect one of the access points to the first, network and the other access point to the second network.
- Then, configure both access points to operate in bridge mode giving each AP the MAC of the other AP.

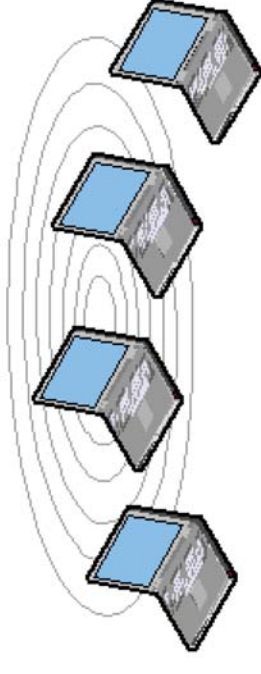


Y.3

Ad-hoc networks

- A wireless access point is not necessary to set up a wireless network.
- Any time two or more wireless devices come within range of each other, they can link up to form an *ad-hoc network*.
- All of the computers within range of each other in an ad-hoc network are called an *Independent Basic Service Set*, or *IBSS*.

AD HOC CLIENT TO CLIENT



Y.4

Configuring a Wireless Access Point

- **Enable/Disable:** Enables or disables the device's wireless access point functions.
- **SSID:** The Service Set Identifier used to identify the network.
- **Allow broadcast SSID to associate?** Disables the access point's periodic broadcast of the SSID.
- Normally, the access point regularly broadcasts its SSID so that wireless devices that come within range can detect the network and join in.
- For a more secure network, you can disable this function.
- Then, a wireless client must already know the network's SSID in order to join the network.

- **Channel:** Lets you select 1 of 11 channels on which to broadcast.
- All the access points and computers in the wireless network should use the same channel.
- **WEP (security):** Lets you use a security protocol called *wired equivalent privacy*.
- **DHCP configuration:** it's common for the access point to also be the DHCP server for the entire network.

Y.5

Y.6

Securing a Wireless Network

- Wired networks are so secure that no one can gain access to the network if only he is physically connect to your network.
- on the other hand wireless networks are totally open, in which anyone within range of your wireless transmissions can log on.
- The goal of securing a wireless network is to find the happy medium between these two extremes that meets the access and risk-management needs of the organization.
- Wireless connections has important security issues to keep the intruders from accessing, reading and modifying the network traffic.
- We need an algorithm which provides the same level of security that physical wired does.

٢٩

Dr. Ahmed ElShafee, ACU Fall 2013, Network I

WEP

- WEP –(Wired Equivalent Privacy)
 - part of the IEEE 802.11 specification
- Goal
 - make the Wi-Fi network at least as secure as a wired LAN.
 - Encrypt data transmitted to prevent the attackers from getting the information or change it.
- Services
 - access control to the network.
 - message confidentiality.
 - message integrity and authenticity.

٣٠

Dr. Ahmed ElShafee, ACU Fall 2013, Network I

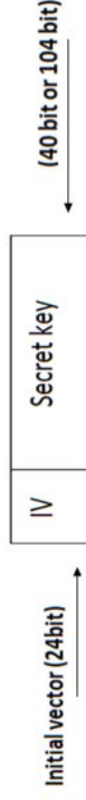
- usage
 - Protect wireless communication from eavesdropping.
 - Prevent unauthorized access to wireless network
- Goals and services
 - Access Control
 - Ensure that your wireless infrastructure is not used.
 - Data Integrity
 - Ensure that your data packets are not modified in transit.
 - Confidentiality
 - Ensure that the contents of your wireless traffic is not learned

٣١

Dr. Ahmed ElShafee, ACU Fall 2013, Network I

Operation

- WEP uses encryption algorithm called RC4
- The key divided in two parts



- There are two kinds of WEP
 - 1) WEP 64 (40 bit + 24 bit).
 - 2) WEP 128 (104 bit + 24 bit).

٣٢

Dr. Ahmed ElShafee, ACU Fall 2013, Network I

Example

KSU K=6Bh, S=73h, U=75h

Plaintext 01101011 01110011 01110101

key stream 01101100 10010111 01101111

Cipher text 00000111 11100100 00011010

٣٢

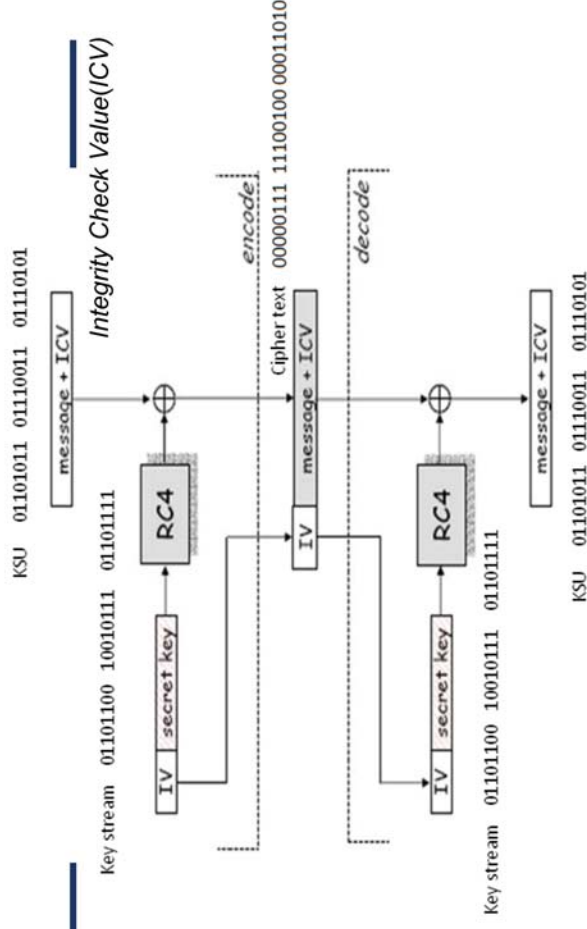
Dr. Ahmed ElShafee, ACU Fall 2013, Network I

The reason of Transition to WPA

- The same IV can be used more than once.
- The secret key is common in WEP.
- The key that WEP uses is short .
- Most users usually do not change their keys.

٣٣

Dr. Ahmed ElShafee, ACU Fall 2013, Network I



٣٤

Dr. Ahmed ElShafee, ACU Fall 2013, Network I

WPA

- WPA –(Wi-Fi Protected Access).
- WPA use the TKIP and depends on RC4.
- The key in WPA consist of 128 bit and 48 bit for initial victor.

٣٥

Dr. Ahmed ElShafee, ACU Fall 2013, Network I

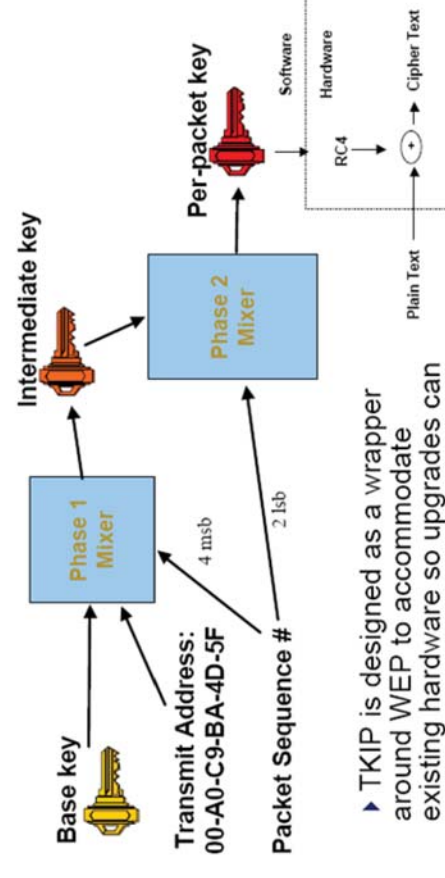
TKIP (Temporal Key Integrity Protocol)

- TKIP is a security protocol used in the IEEE 802.11 wireless networking standard.
- TKIP was a solution to replace WEP without requiring the replacement of legacy hardware.
- TKIP implement three new security features

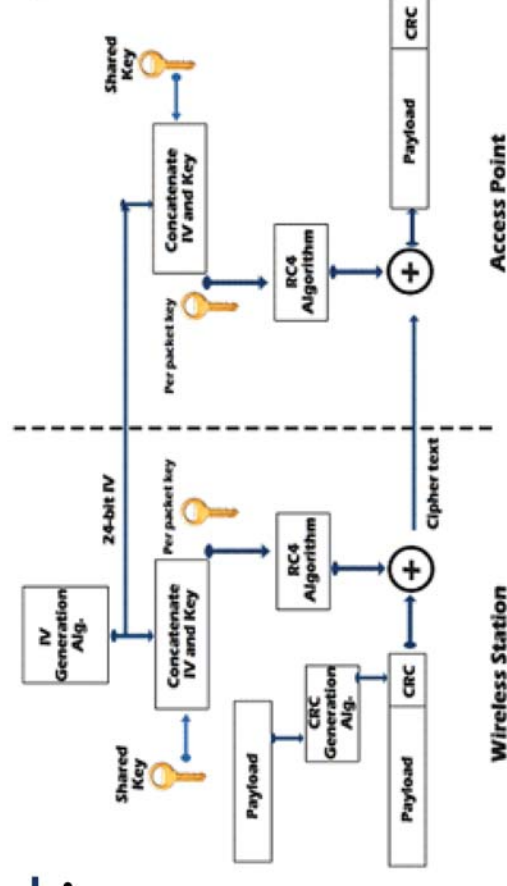
- First, TKIP implements a key mixing function.

- Second, WPA implements a sequence counter to protect against replay attacks.

TKIP Design



- TKIP is designed as a wrapper around WEP to accommodate existing hardware so upgrades can be made



802.11i or WPA2

- WPA addressed problems with WEP, but still had room for improvement.
- Implements new encryption algorithm, No use of RC4.
- Uses Advanced Encryption Standard algorithm (AES)
 - Variable key sizes of 128, 192 and 256 bits.
 - Much harder to decrypt than WPA or WEP.
- Not compatible with old (WPA, & WEP) devices
 - Requires new chip sets.

- comparison between protocols

	WEP	WPA	WPA2
Encryption algorithm	RC4	RC4	AES
Key re-generation	None	Dynamic session keys	Dynamic session keys
Key distribution	Manually typed into each device	Automatic distribution available	Automatic distribution available

MAC address filtering

- MAC address filtering allows you to specify a list of MAC addresses for the devices that are allowed to access the network.
- If a computer with a different MAC address tries to join the network via the access point, the access point will deny access.

Summary

- security has always been considered important for Wi-Fi.
- WEP is weak against security attacks.
- TKIP provides a quick way to upgrade firmware and fix many of the flaws => WPA
- WAP2 use AES encryption and message integrity check but requires new hardware.

Placing your access points outside the firewall

- The most effective security technique for wireless networking is to place all your wireless access points *outside* of your firewall.
- That way, all network traffic from wireless users will have to travel through the firewall to access the network.
- As you can imagine, doing this can significantly limit network access for wireless users.
- To get around those limitations, you can enable a virtual private network (VPN) connection for your wireless users.
- The VPN will allow full network access to authorized wireless users.

Thanks,..
See you next week (ISA),...