Computer Hardware & Networking& Server Configurations (H7E3 04)

UNIT 08:
Wireless Networking

Lecturer: Thilina Rajakaruna

BEng(SEng), SCQF Level 7(EQF 5)(SEng), SCQF Level 8(EQF 5)(SEng), PgDip(Edu)

Wireless technology

Why Wireless Communication

- Freedom from wires.
- No bunch of wires running from here and there.
- "Auto Magical" instantaneous communication without physical connection setup e.g.- Bluetooth, Wi-Fi.
- Global coverage
- Communication can reach where wiring is infeasible or costly

  E.g.- rural areas, buildings, battlefield, outer space.
- Stay connected, flexibility to connect multiple devices

Different Wireless Communication Media

01. Infrared
02. Bluetooth
03. Wi-Fi
04. Li-Fi
05. Wi-Max
06. Microwave
07. Radio wave
08. GPS

IR - Infrared

- Infrared signals may be used for short-distance connections. However, they are easily interrupted by bad weather or smoke, and offer a relatively slow method of connection, typically less than 10 Mbps.

- The IrDA (Infrared Data Association) standard for infrared devices was designed to allow devices such as PCs, PDAs and peripherals to communicate. It is not normally used for conventional LAN networking.

Bluetooth

- Bluetooth is designed for connecting computers and communications devices together directly over very short distances — typically up to 10 meters — using 2.4 GHz radio frequencies. It may be used to connect a laptop or PDA to a nearby network interface. The rate of data communications is 700 Kbps, which is relatively slow.

WI-FI (Wireless Fidelity)

- Unlike Bluetooth, Wi-Fi was designed specifically for computer networking. There are a range of 802.11 standards called 802.11a, 802.11b, 802.11g, 802.11n and 802.11ac.

- Defining the exact details of Wi-Fi radio communication. The links also use 2.4 GHz and 5 GHz frequencies. But run at rates up to 54 Mbps over short distances. Lower speed may be attained over distances up to 200 feet away.

- The latest Wi-Fi specification (802.11ac) promises speeds up to 1 Gbps.

The WLAN Standard: 802.11

The Institute of Electrical and Electronics Engineers (IEEE) is an organized group of engineers. They created the standard for WiFi technology which all wireless routers will follow. They called this standard 802.11. All wireless routers at the time were built around this standard. There was no letter designation, such as “G”, “N” or “AC”. This 802.11 standard was released in 1997

Protocol	Year Introduced	Maximum Data Transfer Speed	Frequency	Channel Bandwidth
802.11a	1999	54 Mbps	5 GHz	20 MHz
802.11b	1999	11 Mbps	2.4 GHz	20 MHz
802.11g	2003	54 Mbps	2.4 GHz	20 MHz
802.11n	2009	65 to 600 Mbps	2.4 or 5 GHz	20 and 40 MHz
802.11ac	2012	78 Mbps to 3.2 Gbps	5 GHz	20, 40, 80 and 160 MHz

802.11b

- IEEE expanded on the original 802.11 standard in July 1999, creating the *802.11b* specification. 802.11b supports bandwidth up to 11 Mbps, comparable to traditional Ethernet.

- 802.11b uses the same *unregulated* radio signaling frequency (2.4 GHz) as the original 802.11 standard. Vendors often prefer using these frequencies to lower their production costs. Being unregulated, 802.11b gear can incur interference from microwave ovens, cordless phones, and other appliances using the same 2.4 GHz range. However, by installing 802.11b gear a reasonable distance from other appliances, interference can easily be avoided.

- **Pros of 802.11b** - lowest cost; signal range is good and not easily obstructed

- **Cons of 802.11b** - slowest maximum speed; home appliances may interfere on the unregulated frequency band

802.11a

- While 802.11b was in development, IEEE created a second extension to the original 802.11 standard called *802.11a*.

- Because 802.11b gained in popularity much faster than did 802.11a, some folks believe that 802.11a was created after 802.11b. In fact, 802.11a was created at the same time. Due to its higher cost, 802.11a is usually found on business networks whereas 802.11b better serves the home market.

- 802.11a supports bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz. This higher frequency compared to 802.11b shortens the range of 802.11a networks. The higher frequency also means 802.11a signals have more difficulty penetrating walls and other obstructions.

- Because 802.11a and 802.11b utilize different frequencies, the two technologies are incompatible with each other. Some vendors offer hybrid *802.11a/b* network gear, but these products merely implement the two standards side by side (each connected devices must use one or the other).

- **Pros of 802.11a** - fast maximum speed; regulated frequencies prevent signal interference from other devices

- **Cons of 802.11a** - highest cost; shorter range signal that is more easily obstructed

802.11g

- In 2002 and 2003, WLAN products supporting a newer standard called *802.11g* emerged on the market. 802.11g attempts to combine the best of both 802.11a and 802.11b. 802.11g supports bandwidth up to 54 Mbps, and it uses the 2.4 Ghz frequency for greater range. 802.11g is backwards compatible with 802.11b, meaning that 802.11g access points will work with 802.11b wireless network adapters and vice versa.

- **Pros of 802.11g** - fast maximum speed; signal range is good and not easily obstructed
- **Cons of 802.11g** - costs more than 802.11b; appliances may interfere on the unregulated signal frequency

802.11n

- *802.11n* (also sometimes known as "Wireless N") was designed to improve on 802.11g in the amount of bandwidth supported by utilizing multiple wireless signals and antennas (called *MIMO* technology) instead of one. Industry standards groups ratified 802.11n in 2009 with specifications providing for up to 300 Mbps of network bandwidth. 802.11n also offers somewhat better range over earlier Wi-Fi standards due to its increased signal intensity, and it is backward-compatible with 802.11b/g gear.

- **Pros of 802.11n** - fastest maximum speed and best signal range; more resistant to signal interference from outside sources

- **Cons of 802.11n** - standard is not yet finalized; costs more than 802.11g; the use of multiple signals may greatly interfere with nearby 802.11b/g based networks.

802.11ac

- The newest generation of Wi-Fi signaling in popular use, 802.11ac utilizes dual band wireless technology, supporting simultaneous connections on both the 2.4 GHz and 5 GHz Wi-Fi bands. 802.11ac offers backward compatibility to 802.11b/g/n and bandwidth rated up to 1300 Mbps on the 5 GHz band plus up to 450 Mbps on 2.4 GHz.

Li-Fi (Light Fidelity)

- Light Fidelity or Li-Fi is a Visible Light Communications (VLC) system running wireless communications travelling at very high speeds.

- Li-Fi uses common household LED (light emitting diodes) lightbulbs to enable data transfer, boasting speeds of up to 224 gigabits per second.

- The term Li-Fi was coined by University of Edinburgh Professor Harald Haas during a TED Talk in 2011. Haas envisioned light bulbs that could act as wireless routers.

How it works

- Li-Fi and Wi-Fi are quite similar as both transmit data electromagnetically. However, Wi-Fi uses radio waves while Li-Fi runs on visible light.

- As we now know, Li-Fi is a Visible Light Communications (VLC) system. This means that it accommodates a photo-detector to receive light signals and a signal processing element to convert the data into 'stream-able' content.

- An LED lightbulb is a semi-conductor light source meaning that the constant current of electricity supplied to an LED lightbulb can be dipped and dimmed, up and down at extremely high speeds, without being visible to the human eye.

- For example, data is fed into an LED light bulb (with signal processing technology), it then sends data (embedded in its beam) at rapid speeds to the photo-detector (photodiode).

- The tiny changes in the rapid dimming of LED bulbs is then converted by the 'receiver' into electrical signal.

- The signal is then converted back into a binary data stream that we would recognize as web, video and audio applications that run-on internet enables devices.

Wi-Max (IEEE 802.16)

- Wi-MAX (Worldwide Interoperability for Microwave Access) is essentially a variation of Wi-Fi that has better performance over longer distances. Theoretically it can broadcast at 70 Mbps for 30 miles distance but real-world tests suggest that 0.5 – 2 Mbps over 3–5 miles is more typical.

Radio and Microwave Transmission

RADIO TRANSMISSION:- easily generated, Omni-directional , travel long distance , easily penetrates buildings.

PROBLEMS:-

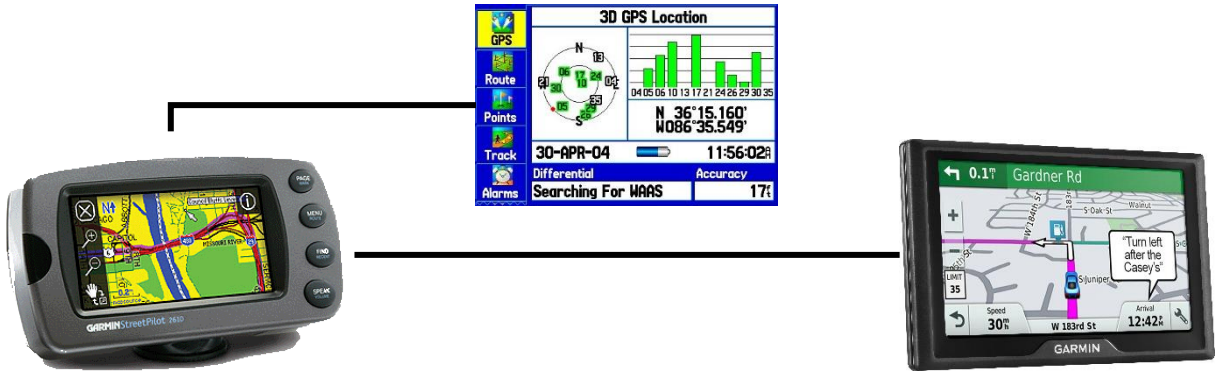
frequency dependent , relatively low bandwidth for data communication , tightly licensed by government.

MICROWAVE TRANSMISSION:- widely used for long distance communication , relatively inexpensive.

PROBLEMS:-

don't pass through buildings , weather and frequency dependent

GPS (Global Positioning System)



- The Global Positioning System (GPS) is a satellite-based navigation system made up of a network of 24 satellites placed into orbit by the U.S. Department of Defense. GPS was originally intended for military applications, but in the 1980s, the government made the system available for civilian use. GPS works in any weather conditions, anywhere in the world, 24 hours a day. There are no subscription fees or setup charges to use GPS.

Wireless Security

The Difference Between WEP, WPA, and WPA2 Wi-Fi Passwords

Even if you know you need to secure your Wi-Fi network (and have already done so), you probably find all the encryption acronyms a little bit puzzling. Read on as we highlight the differences between encryption standards like WEP, WPA, and WPA2 – and why it matters which acronym you slap on your home Wi-Fi network.

What Does It Matter?

- You did what you were told to do, you logged into your router after you purchased it and plugged it in for the first time, and set a password. What does it matter what the little acronym next to the security encryption standard you chose was? As it turns out, it matters a whole lot: as is the case with all encryption standards, increasing computer power and exposed vulnerabilities have rendered older standards at risk. It's your network, it's your data, and if someone hijacks your network for their illegal hijinks, it'll be the police knocking on your door. Understanding the differences between encryption protocols and implementing the most advanced one your router can support (or upgrading it if it can't support current gen secure standards) is the difference between offering someone easy access to your home network and sitting secure.

WEP, WPA, and WPA2: Wi-Fi Security Through the Ages

- Since the late 1990s, Wi-Fi security algorithms have undergone multiple upgrades with outright depreciation of older algorithms and significant revision to newer algorithms. A stroll through the history of Wi-Fi security serves to highlight both what's out there right now and why you should avoid older standards.

Wired Equivalent Privacy (WEP)

- Wired Equivalent Privacy (WEP) is the most widely used Wi-Fi security algorithm in the world. This is a function of age, backwards compatibility, and the fact that it appears first in the encryption type selection menus in many router control panels.

- WEP was ratified as a Wi-Fi security standard in September of 1999. The first versions of WEP weren't particularly strong, even for the time they were released, because U.S. restrictions on the export of various cryptographic technology led to manufacturers restricting their devices to only 64-bit encryption. When the restrictions were lifted, it was increased to 128-bit. Despite the introduction of 256-bit WEP encryption, 128-bit remains one of the most common implementations.

- Despite revisions to the algorithm and an increased key size, over time numerous security flaws were discovered in the WEP standard and, as computing power increased, it became easier and easier to exploit them. As early as 2001 proof-of-concept exploits were floating around and by 2005 the FBI gave a public demonstration (in an effort to increase awareness of WEP's weaknesses) where they cracked WEP passwords in minutes using freely available software.

- Despite various improvements, work- arounds, and other attempts to shore up the WEP system, it remains highly vulnerable and systems that rely on WEP should be upgraded or, if security upgrades are not an option, replaced. The Wi-Fi Alliance officially retired WEP in 2004.

Wi-Fi Protected Access (WPA)

- Wi-Fi Protected Access was the Wi-Fi Alliance's direct response and replacement to the increasingly apparent vulnerabilities of the WEP standard. It was formally adopted in 2003, a year before WEP was officially retired. The most common WPA configuration is WPA-PSK (Pre-Shared Key). The keys used by WPA are 256-bit, a significant increase over the 64-bit and 128-bit keys used in the WEP system.

- Some of the significant changes implemented with WPA included message integrity checks (to determine if an attacker had captured or altered packets passed between the access point and client) and the Temporal Key Integrity Protocol (TKIP). TKIP employs a per-packet key system that was radically more secure than fixed key used in the WEP system. TKIP was later superseded by Advanced Encryption Standard (AES).

- Despite what a significant improvement WPA was over WEP, the ghost of WEP haunted WPA. TKIP, a core component of WPA, was designed to be easily rolled out via firmware upgrades onto existing WEP-enabled devices. As such it had to recycle certain elements used in the WEP system which, ultimately, were also exploited.

- WPA, like its predecessor WEP, has been shown via both proof-of-concept and applied public demonstrations to be vulnerable to intrusion. Interestingly the process by which WPA is usually breached is not a direct attack on the WPA algorithm (although such attacks have been successfully demonstrated) but by attacks on a supplementary system that was rolled out with WPA, Wi-Fi Protected Setup (WPS), designed to make it easy to link devices to modern access points.

Wi-Fi Protected Access II (WPA2)

- WPA has, as of 2006, been officially superseded by WPA2. One of the most significant changes between WPA and WPA2 was the mandatory use of AES algorithms and the introduction of CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) as a replacement for TKIP (still preserved in WPA2 as a fallback system and for interoperability with WPA).

- Currently, the primary security vulnerability to the actual WPA2 system is an obscure one (and requires the attacker to already have access to the secured Wi-Fi network in order to gain access to certain keys and then perpetuate an attack against other devices on the network). As such, the security implications of the known WPA2 vulnerabilities are limited almost entirely to enterprise level networks and deserve little to no practical consideration in regard to home network security.

- Unfortunately, the same vulnerability that is the biggest hole in the WPA armor, the attack vector through the Wi-Fi Protected Setup (WPS), remains in modern WPA2-capable access points. Although breaking into a WPA/WPA2 secured network using this vulnerability requires anywhere from 2-14 hours of sustained effort with a modern computer, it is still a legitimate security concern and WPS should be disabled (and, if possible, the firmware of the access point should be flashed to a distribution that doesn't even support WPS so the attack vector is entirely removed).

Wireless AP Configuration

Purchase a wireless router

- Purchase a wireless router. Routers come in all shapes and sizes. Compare features to find the router that is right for you. If you have more area that you need to cover, or have lots of walls in your home, you'll need a router that offers the option of upgrading antenna(s) with high gain types - if not supplied in the box. If more than one wireless device will be connecting at the same time at different speeds, a MiMo type router is recommended, otherwise the speed for all devices will drop the highest supported by all at that time.

- All modern routers should support 802.11n, or Wireless-N. This is the most stable, offers the fastest speeds and is backwards compatible with older standards such as 802.11g.

Connecting the Hardware

- Connect your router to your modem. Routers and wireless routers enable you to share your broadband internet connection with multiple devices. To do so, you will need to connect your broadband modem to the router. For best results, place your router near your modem.

- Connect the router and the modem with an Ethernet cable. Most routers come packaged with a short Ethernet cable that you can use for this.

- Connect the modem to the WAN/Internet port on your router. It is usually offset, and may be a different color from the LAN ports.

- Connect any devices you want to hard wire with CAT 5 (or better) Ethernet cables. If you have computers that are close, or a video game console or TV, you can connect them to the router via Ethernet. This will result in a more stable and faster connection, and doesn't require any extra configuration.

Connecting Your Router To Broadband Providers

- Connect at least one computer via Ethernet. You will need at least one computer connecting via Ethernet cable in order to adjust your router settings. You can disconnect this computer afterwards if you want to connect wirelessly.
- When you power on the router, it will only create its wi-fi network, and the device will be connected to the router's wi-fi connection, not the internet. To connect the router to the internet, with some internet providers (i.e. GTPL in India), it is required to register router's MAC address to the internet service provider's website.
- MAC of the router can be found printed on router or in the documents etc.
- Go to the internet service provider's website. Log in with the username and password provided by the internet service provider and go to MAC address update option. one can see their existing laptop/pc's MAC address there. Add the router's MAC address there and save it. This process means that the router is authorized to use the internet provide by the broadband company.

Configuring the Router

- Find the IP address of the router. If this is a new installation or new router, determine the default IP address that may be printed on a label affixed to the router or in the documentation. If you can't find the router's IP address anywhere, you can do a web search for the router model to see what the default address is.
- IP addresses are formatted as four groups of up to three digits, separated by periods. Most default IP addresses are 192.168.1.1, 192.168.0.1,192.168.2.1 or 192.168.100.1
- Open a web browser on the computer that is connected to the router. Enter in the IP address of the router into the address bar and press Enter. Your browser will attempt to connect to the router's configuration menu.
- If your router came with an installation disc, you can run the configuration program from that instead. It will accomplish many of the same functions.

- Enter your username and password. In order to access the configuration page, you will need to be on the router's IP address and enter a valid username and password at the prompt. Most routers have a basic account set up that you will need to use to log on. This varies from model to model, but should be printed on the router or in the documentation.

  - The most typical username is “admin”.
  - The most typical passwords are “admin” and “password”.
  - Many routers will only require a username and a blank password, and some allow you to leave all fields blank.

- If you can’t figure out the correct IP address, your username or password, search for your router model online to see what the default login is. If it has been changed, press the Reset button on the back of the router for 10 (to 30+ seconds as dictated in the instructions for the router model) to restore factory defaults and try again.

- Open the Wireless Settings. When you log in to your router, you will be taken to the router's main menu or status screen. There will be several options to choose from. The Internet section can usually be left at default settings, unless you received specific instructions from your internet service provider. The Wireless section will allow you to set up your wireless network.
- Enter a name for your wireless network. In the Wireless section, you should see a field labeled SSID or Name. Enter a unique name for your wireless network. This is what other devices will see when scanning for networks.
- Check the box to enable SSID broadcast. This will essentially "turn on" the wireless network so that it may be readily seen by anyone in range of the signal. *See the Tips section below for additional information on the SSID setting.
- Choose a security method. Choose from the list of available security options. For the best security, choose WPA2-PSK as the encryption method. This is the most difficult security to crack, and will give you the most protection from hackers and intruders.

- Create a passphrase. Once you've chosen your security method, enter in a passphrase for the network. This should be a difficult password, with a combination of letters, numbers, and symbols. Don't use any passwords that could be easily deduced from your network name or from knowing you.

- Save your settings. Once you are finished naming and securing your wireless network, click the Apply or Save button. The changes will be applied to your router, which may take a few moments. Once the router has finished resetting, your wireless network will be enabled.

- Change your router's username and password from the default. Once you have your network configured, you should change the username and password that you use to access your router. This will help protect your router from unauthorized changes. You can change these from the Administration section of the router configuration menu.

- Block sites. If you want to prevent devices that are connected to your network from accessing certain websites, you can use built-in blocking tools to restrict access. These can be found in the Security/Block section of the router.

- You can usually block by specific domain names, or by keywords.

Connecting the Devices

- Connect a computer, tablet, or smartphone to the wireless network. Scan for the wireless network with the SSID you provided above. On any device that supports wireless networks, you should see your new network as long as you are within range of the router. Select it and you will be prompted for the passphrase.

- Enter your wireless passphrase. Once you enter the passphrase, your device will be automatically connected to the wireless network. The network will be stored in your devices memory and will automatically connect whenever you are within range.