Lecture 3
Other Wireless Connections: Wi-Fi & 3G

More and more people are using laptop computers, smart cellphones, and personal digital assistants to access the internet through wireless networks, which use radio waves to transmit data. Indeed, 62% of all Americans are part of a wireless, mobile population.

Wi-Fi
Short for Wireless Fidelity, Wi-Fi is the name given to any of several standards—so-called 802.11 standards—set by the Institute of Electrical and Electronic Engineers (IEEE) for wireless transmission. Many airports, hotels, libraries, convention centers, and fast-food facilities offer so-called hotspots or access points, station that send and receive data to and from Wi-Fi networks. The hotspot can get its internet access from DSL, cable modem, T1 local area network, dial-up phone service, or any other method. Once the hotspot has the internet connection, it can broadcast it wirelessly. Laptops are commonly used for Wi-Fi internet connections; they must be equipped with the necessary Wi-Fi hardware, however.

Some cities are trying to use the technology to provide free or low-cost Internet access to residents. In the near future, wireless networking may become so widespread that you can access the Internet just about anywhere at any time, without using wires.

WiFi has a lot of advantages. Wireless networks are easy to set up and inexpensive. They’re also unobtrusive -- unless you’re on the lookout for a place to use your laptop, you may not even notice when you're in a hotspot.

What Is WiFi?
A wireless network uses radio waves, just like cell phones, televisions and radios do. In fact, communication across a wireless network is a lot like two-way radio communication. Here's what happens:

1. A computer's wireless adapter translates data into a radio signal and transmits it using an antenna.
2. A wireless router receives the signal and decodes it. The router sends the information to the Internet using a physical, wired Ethernet connection.

The process also works in reverse, with the router receiving information from the Internet, translating it into a radio signal and sending it to the computer's wireless adapter.
The radios used for WiFi communication are very similar to the radios used for walkie-talkies, cell phones and other devices. They can transmit and receive radio waves, and they can convert 1s and 0s into radio waves and convert the radio waves back into 1s and 0s.

**Walkie-Talkie**

- A walkie-talkie is a hand-held, portable, two-way radio transceiver. After the 2nd war, walkie-talkies spread to public safety and eventually commercial and jobsite work.

- Major characteristics include a half-duplex channel (only one radio transmits at a time, though any number can listen) and a "push-to-talk" (PTT) switch that starts transmission.

- Typical walkie-talkies resemble a telephone handset, possibly slightly larger but still a single unit, with an antenna mounted on the top of the unit.

But WiFi radios have a few notable differences from other radios:

- They transmit at frequencies of 2.4 GHz or 5 GHz. This frequency is considerably higher than the frequencies used for cell phones, walkie-talkies and televisions. The higher frequency allows the signal to carry more data.

- They use 802.11 networking standards, which come in several flavors:
  
  - **802.11a** transmits at 5 GHz and can move up to 54Mbps. It also uses orthogonal frequency-division multiplexing (OFDM), a more efficient coding technique that splits that radio signal into several sub-signals before they reach a receiver. This greatly reduces interference.
  
  - **802.11b** is the slowest and least expensive standard. For a while, its cost made it popular, but now it’s becoming less common as faster standards become less expensive. 802.11b transmits in the 2.4 GHz frequency band of the radio spectrum. It can handle up to 11 Mbps, and it uses complementary code keying (CCK) modulation to improve speeds.
  
  - **802.11g** transmits at 2.4 GHz like 802.11b, but it’s a lot faster -- it can handle up to 54 Mbps. 802.11g is faster because it uses the same OFDM coding as 802.11a.
  
  - **802.11n** is the newest standard that is widely available. This standard significantly improves speed and range. For instance, although 802.11g theoretically moves 54 Mbps, it only achieves real-world speeds of about 24 Mbps because of network congestion. 802.11n, however, reportedly can achieve speeds as high as 140 Mbps.
As long as they all have wireless adapters, several devices can use one router to connect to the Internet. This connection is convenient, virtually invisible and fairly reliable; however, if the router fails or if too many people try to use high-bandwidth applications at the same time, users can experience interference or lose their connections.

Radio spectrum

- **Radio spectrum** refers to the part of the electromagnetic spectrum corresponding to radio frequencies – that is, frequencies lower than around 300 GHz.
- Different parts of the radio spectrum are used for different radio transmission technologies and applications.
- Radio spectrum is typically government regulated in developed countries and, in some cases, is sold or licensed to operators of private radio transmission systems (for example, cellular telephone operators or broadcast television stations).

WiFi Hotspots

If you want to take advantage of public WiFi hotspots or start a wireless network in your home, the first thing you'll need to do is make sure your computer has the right device. Most new laptops and many new desktop computers come with built-in wireless transmitters. If your laptop doesn't, you can buy a **wireless adapter** that plugs into the PC card slot or USB port. Desktop computers can use USB adapters, or you can buy an adapter that plugs into the PCI slot inside the computer's case. Many of these adapters can use more than one 802.11 standard.

Once you've installed your wireless adapter and the drivers that allow it to operate, your computer should be able to automatically discover existing networks. This means that when you turn your computer on in a WiFi hotspot, the computer will inform you that the network exists and ask whether you want to connect to it. If you have an older computer, you may need to use a software program to detect and connect to a wireless network.

Being able to connect to the Internet in public hotspots is extremely convenient. Wireless **home networks** are convenient as well. They allow you to easily connect multiple computers and to move them from place to place without disconnecting and reconnecting wires.
Building a Wireless Network

If you already have several computers networked in your home, you can create a wireless network with a wireless access point. If you have several computers that are not networked, or if you want to replace your Ethernet network, you'll need a wireless router.

A wireless router allows you to use wireless signals or Ethernet cables to connect your computers to one another, to a printer and to the Internet. Most routers provide coverage for about 100 feet (30.5 meters) in all directions. If your home is very large, you can buy inexpensive range extenders or repeaters to increase your router's range.

As with wireless adapters, many routers can use more than one 802.11 standard. 802.11b routers are slightly less expensive, but because the standard is older, they're slower than 802.11a, 802.11g and 802.11n routers. Most people select the 802.11g option for its speed and reliability.

Once you plug in your router, it should start working at its default settings. Most routers let you use a Web interface to change your settings. You can select:

- **The name of the network, known as its service set identifier (SSID)** -- The default setting is usually the manufacturer's name.
- **The channel that the router uses** -- Most routers use channel 6 by default. If you live in an apartment and your neighbors are also using channel 6, you may experience interference. Switching to a different channel should eliminate the problem.
• **Your router's security options** -- Many routers use a standard, publicly available sign-on, so it's a good idea to set your own username and password.

Security is an important part of a home wireless network, as well as public WiFi hotspots. If you set your router to create an open hotspot, anyone who has a wireless card will be able to use your signal. Most people would rather keep strangers out of their network, though. Doing so requires you to take a few security precautions.

It's also important to make sure your security precautions are current. The Wired Equivalency Privacy (WEP) security measure was once the standard for WAN security. The idea behind WEP was to create a wireless security platform that would make any wireless network as secure as a traditional wired network. But hackers discovered vulnerabilities in the WEP approach, and today it's easy to find applications and programs that can compromise a WAN running WEP security.

To keep your network private, you can use one of the following methods:

• **WiFi Protected Access** (WPA) is a step up from WEP and is now part of the 802.11i wireless network security protocol. It uses temporal key integrity protocol (TKIP) encryption.

As with WEP, WPA security involves signing on with a password. Most public hotspots are either open or use WPA or 128-bit WEP technology, though some still use the vulnerable WEP approach.

TKIP was designed as a solution to replace WEP without requiring the replacement of legacy hardware. This was necessary because the breaking of WEP had left WiFi networks without viable link-layer security, and a solution was required for already deployed hardware.

• **Media Access Control** (MAC) address filtering is a little different from WEP or WPA. It doesn't use a password to authenticate users -- it uses a computer's physical hardware. Each computer has its own unique MAC address. MAC address filtering allows only machines with specific MAC addresses to access the network. You must specify which addresses are allowed when you set up your router.

This method is very secure, but if you buy a new computer or if visitors to your home want to use your network, you'll need to add the new machines' MAC addresses to the list of approved addresses. The system isn't foolproof. A clever hacker can **spoof** a MAC address -- that is, copy a known MAC address to fool the network that the computer he or she is using belongs on the network.

**3G**

3G, which stands for “third generation,” is loosely defined as high-speed wireless technology that does not need access points because it uses the existing cellphone system. This technology, which is found in many smartphones and PDAs that are
capable of delivering downloadable video clips and high-resolution games, is being provided.

An especially notable development during this time is the smartphone (for example, the iPhone, and the Android family), combining the abilities of a PDA with a mobile phone, leading to widespread demand for mobile internet connectivity. 3G has also introduced the term "mobile broadband" because its speed and capability make it a viable alternative for internet browsing, and USB Modems connecting to 3G networks are becoming increasingly common.

Applications of 3G

The bandwidth and location information available to 3G devices gives rise to applications not previously available to mobile phone users. Some of the applications are:

- Mobile TV
- Video on demand
- Video Conferencing
- Telemedicine
- Location-based services
- Global Positioning System (GPS).

4G

- **4G** is the fourth generation of mobile communications standards. It is a successor of the third generation (3G) standards.
- A 4G system provides mobile ultra-broadband Internet access, for example to laptops with USB wireless modems, to smartphones, and to other mobile devices.
- Recently, Android and Windows-enabled cellular devices have fallen in the 4G category.
- One base advantage of 4G is that it can, at any point of travelling time, provide an internet data transfer rate higher than any existing cellular services (*excluding* broadband and Wi-Fi connections).

4G applications:

- mobile web access
- IP telephony
- gaming services
- high-definition mobile TV
- video conferencing
- 3D television.
Internet Access Providers: Three Kinds
As we mentioned, in addition to having an access device and a means of connection, to get on the internet you need to go through an internet access provider. There are three types of such providers: internet service providers, commercial online services, and wireless internet service providers.

INTERNET SERVICE PROVIDERS (ISPs): (ISP) is a company that connects online users through their communications lines to the company’s server, which links them to the internet via another company’s network access points. Examples are EarthLink. There are also some free ISPs. Free ISPs are ISPs which provide service free of charge. Many free ISPs display advertisements while the user is connected; like commercial television, in a sense they are selling the users’ attention to the advertiser. Other free ISPs, often called freenets, are run on a nonprofit basis, usually with volunteer staff.

COMMERCIAL ONLINE SERVICES: is a members-only company that provides not only internet access but other specialized content as well, such as news, games, and financial data. The two best-known subscriber-only commercial online services are AOL (America Online) and MSN (Microsoft Network).

WIRELESS INTERNET SERVICE PROVIDERS: (WISP) enables users with computers containing wireless modems—mostly laptops/notebooks—and web-enabled mobile smartphones and PDAs to gain access to the internet. Examples are T-Mobile, and Verizon.