Topic 7 Notes

7.1 Wireless Markup Language

WAP uses **Wireless Markup Language** (WML), which includes the Handheld Device Markup Language (HDML) developed by Phone.com. WML can also trace its roots to **eXtensible Markup Language** (XML). A markup language is a way of adding information to your content that tells the device receiving the content what to do with it. The best-known markup language is Hypertext Markup Language (HTML). Unlike HTML, WML is considered a **meta language**. Basically, this means that in addition to providing predefined tags, WML lets you design your own markup language components. WAP also allows the use of standard Internet protocols such as UDP, IP and XML.

There are three main reasons why wireless Internet needs the Wireless Application Protocol:

i. Transfer speed
ii. Size and readability
iii. Navigation

Most cell phones and Web-enabled PDAs have data transfer rates of 14.4 Kbps or less. Compare this to a typical 56 Kbps modem, a cable modem or a DSL connection. Most Web pages today are full of graphics that would take an unbearably long time to download at 14.4 Kbps. Wireless Internet content is typically text-based in order to solve this problem.

The relatively small size of the LCD on a cell phone or PDA presents another challenge. Most Web pages are designed for a resolution of 640x480 pixels, which is fine if you are reading on a desktop or a laptop. The page simply does not fit on a wireless device's display, which might be 150x150 pixels. Also, the majority of wireless devices use monochrome screens. Pages are harder to read when font and background colors become similar shades of gray.

Navigation is another issue. You make your way through a Web page with points and clicks using a mouse; but if you are using a wireless device, you often use one hand to scroll keys.

WAP takes each of these limitations into account and provides a way to work with a typical wireless device.

Here's what happens when you access a Web site using a WAP-enabled device:

i. You turn on the device and open the mini browser.
ii. The device sends out a radio signal, searching for service.
iii. A connection is made with your service provider.
iv. You select a Web site that you wish to view.
v. A request is sent to a gateway server using WAP.
vi. The gateway server retrieves the information via HTTP from the Web site.
vii. The gateway server encodes the HTTP data as WML.
viii. The WML-encoded data is sent to your device.
ix. You see the wireless Internet version of the Web page you selected.

To create wireless Internet content, a Web site creates special text-only or low-graphics versions of the site. The data is sent in HTTP form by a Web server to a WAP gateway. This system includes the WAP encoder, script compiler and protocol adapters to convert the HTTP information to WML. The gateway then sends the converted data to the WAP client on your wireless device. What happens between the gateway and the client relies on features of different parts of the WAP protocol stack. The stack includes the following:

i. WAE - The Wireless Application Environment holds the tools that wireless Internet content developers use. These include WML and WMLScript, which is a scripting language used in conjunction with WML. It functions much like Javascript.
ii. WSP - The Wireless Session Protocol determines whether a session between the device and the network will be connection-oriented or connectionless. In a connection-oriented session, data is passed both ways between the device and the network; WSP then sends the packet to the Wireless Transaction Protocol layer. If the session is connectionless, commonly used when information is being broadcast or streamed from the network to the device, then WSP redirects the packet to the Wireless Datagram Protocol layer.
iii. WTP - The Wireless Transaction Protocol acts like a traffic cop, keeping the data flowing in a logical and smooth manner. It also determines how to classify each transaction request: Reliable two-way Reliable one-way Unreliable one-way The WSP and WTP layers correspond to Hypertext Transfer Protocol (HTTP) in the TCP/IP protocol suite.
iv. WTLS - Wireless Transport Layer Security provides many of the same security features found in the Transport Layer Security (TLS) part of TCP/IP. It checks data integrity, provides encryption and performs client and server authentication.
v. WDP - The Wireless Datagram Protocol works in conjunction with the network carrier layer. WDP makes it easy to adapt WAP to a variety of bearers because all that needs to change is the information maintained at this level.
vi. Network carriers - Also called bearers, these can be any of the existing technologies that wireless providers use, as long as information is provided at the WDP level to interface WAP with the bearer.

Once the information is received by the WAP client, it is passed to the **mini browser**. This is a tiny application built into the wireless device that provides the interface between the user and the wireless Internet. The mini browser does not offer anything more than basic navigation. Wireless Internet is still a long way from being a true alternative to the normal Internet. It is really positioned right now for people who need the ability to connect no matter where they are.

7.2 The Evolution of Wireless Network Security

One of the first major complaints that arose from wireless networking was from the security community. Quite rightly, the complaint was that with RF signals being broadcast over the air, nothing can stop someone from reaching out and grabbing them. At least with wired networking, a person had to be physically connected to the same hubs or switches to be able to eavesdrop on a network conversation.

To deal with this issue, Wired Equivalent Privacy (WEP) was introduced. The goal of WEP was to provide the same level of privacy that you would have if you were still connected to a wired network. WEP involved two sets of mechanisms:

i. **Authentication**: You need to prove your identity before participating in the network.
ii. **Encryption**: You want everything you send over the airwaves to be encrypted.

The basis of WEP encryption is tied to an encryption key; today typically either 64-bit WEP or 128-bit WEP encryption keys are used. With 64-bit WEP, you use a 40-bit key that is joined with a 24-bit initialization vector (IV) to generate an RC4 (Rivest Cipher 4) stream cipher. A 128-bit WEP uses a 104-bit encryption key, which is then joined with the 24-bit IV to create the RC4 cipher.

While this gives you a quick and efficient way to encrypt and decrypt traffic at high speed, it has some serious flaws. Even if you cannot read the data, you can still capture data packets off a wireless network because they are just traveling over the air. One of the issues is that the IV must be unique for every packet that is sent over a time period, and because it is only 24 bits long, it can start repeating in as little as 5,000 packets, making it not as random or secure as it can be.

The goal of WEP was good, but as with a better-built mousetrap, you just end up with smarter mice. These days, WEP can be broken with readily available software in less than a minute. Given this, it is not considered reliably secure for networks. The Payment Card Industry (PCI), which sets standards for credit and debit card transactions, prohibits the use of WEP in any part of a credit card transaction.

Due to the limitations of WEP, Wi-Fi Protected Access (WPA) was developed. WPA uses most of the recommendations that are included in the IEEE 802.11i specification, which lays out security standards for wireless networks. WPA2 followed later, implementing all the IEEE 802.11i mandatory elements.

Rather than using a static encryption key, as is used with WEP, WPA uses the Temporal Key Integrity Protocol (TKIP), which can easily be implemented because it is a minor but effective upgrade to WEP. Rather than using a plain text IV, it combines the IV with a secret root key. It also implements a sequence counter, so all packets must arrive at the AP in the correct order or they are rejected. Finally, it provides a method of rekeying or updating the encryption key, neutralizing people trying to break the key.

There are still many documented attacks that can be successfully carried out on a WPA network using TKIP, and as such, it required additional updating. The implementation of AES (Advanced Encryption Standard) increased encryption to a level that is still considered to be the safest on the market.

7.3 Wireless Mesh Networks

Wireless mesh networks, an emerging technology, may bring the dream of a seamlessly connected world into reality. Wireless mesh networks can easily, effectively and wirelessly connect entire cities using inexpensive, existing technology. Traditional networks rely on a small number of wired access points or wireless hotspots to connect users. In a wireless mesh network, the network connection is spread out among dozens or even hundreds of wireless mesh nodes that "talk" to each other to share the network connection across a large area.

Mesh nodes are small radio transmitters that function in the same way as a wireless router. Nodes use the common Wi-Fi standards known as 802.11a, b and g to communicate wirelessly with users, and, more importantly, with each other.

Nodes are programmed with software that tells them how to interact within the larger network. Information travels across the network from point A to point B by hopping wirelessly from one mesh node to the next. The nodes automatically choose the quickest and safest path in a process known as dynamic routing.

The biggest advantage of wireless mesh networks -- as opposed to wired or fixed wireless networks -- is that they are truly wireless. Most traditional "wireless" access points still need to be wired to the Internet to broadcast their signal. For large wireless networks, Ethernet cables need to be buried in ceilings and walls and throughout public areas.

In a wireless mesh network, only one node needs to be physically wired to a network connection like a DSL Internet modem. That one wired node then shares its Internet connection wirelessly with all other nodes in its vicinity. Those nodes then share the connection wirelessly with the nodes

closest to them. The more nodes, the further the connection spreads, creating a wireless "cloud of connectivity" that can serve a small office or a city of millions.
Wireless mesh networks advantages include:

i. Using fewer wires means it costs less to set up a network, particularly for large areas of coverage.
ii. The more nodes you install, the bigger and faster your wireless network becomes.
iii. They rely on the same Wi-Fi standards (802.11a, b and g) already in place for most wireless networks.
iv. They are convenient where Ethernet wall connections are lacking -- for instance, in outdoor concert venues, warehouses or transportation settings.
v. They are useful for Non-Line-of-Sight (NLoS) network configurations where wireless signals are intermittently blocked. For example, in an amusement park a Ferris wheel occasionally blocks the signal from a wireless access point. If there are dozens or hundreds of other nodes around, the mesh network will adjust to find a clear signal.
vi. Mesh networks are "self-configuring;" the network automatically incorporates a new node into the existing structure without needing any adjustments by a network administrator.
vii. Mesh networks are "self-healing," since the network automatically finds the fastest and most reliable paths to send data, even if nodes are blocked or lose their signal.
viii. Wireless mesh configurations allow local networks to run faster, because local packets don't have to travel back to a central server.
ix. Wireless mesh nodes are easy to install and uninstall, making the network extremely adaptable and expandable as more or less coverage is needed.

The figure below shows how a wireless mesh network functions when sharing an Internet connection across a Local Area Network (LAN). As you see, only one node in the wireless mesh network needs to be directly wired to the Internet. That wired node shares the Internet connection wirelessly with the nearest cluster of nodes, which then share it with their nearest cluster of nodes and so on.

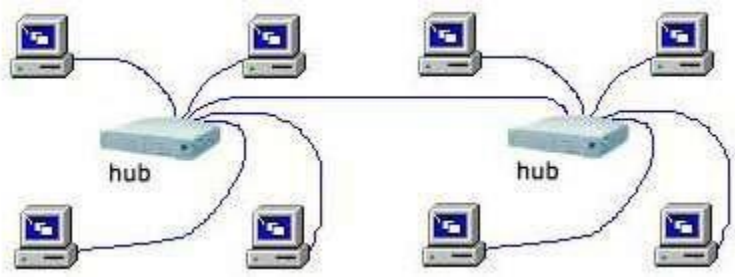

Fig 7.1: Wireless Mesh Technology

That means that each individual node doesn't need to be wired to anything. It only needs a power supply such as traditional AC plugs, batteries, or solar panels if outdoors. Outdoor nodes are encased in a weatherproof, protective shield and can be mounted anywhere including telephone pools, roofs, etc.

Wireless mesh networks are effective in sharing Internet connectivity because the more nodes that are installed, the further the signal can travel. And the more nodes you have, the stronger and faster the Internet connection becomes for the user. How does the Internet connection become stronger and faster?

i. If your laptop computer is in the broadcast range of four nodes, you're tapping into four times the bandwidth of one traditional wireless router.
ii. Distance plays a huge role in wireless signal strength. If you reduce the distance between your computer and the nearest wireless node by two, the signal strength is four times as strong.
iii. Nodes can also provide Internet connectivity to wired devices within the network like VoIP phones, video cameras, servers, and desktop workstations using traditional Ethernet cables. Most nodes come with two or more Ethernet ports, and through a technology called Power Over Ethernet (PoE), the node can provide power to stand-alone devices like surveillance cameras without having to plug the camera into an electrical outlet.

7.3.1 Applications for Wireless Mesh Networks

Cities and Municipalities

With wireless mesh networks, cities can connect citizens and public services over a widespread high-speed wireless connection. A growing number of downtown areas are installing public Wi-Fi hotspots. Mesh networks allow cities to inexpensively and simply link all those hotspots together to cover the entire municipality. Some advantages of municipal mesh networks include:

i. Commuters can check their e-mail on the train, in the park, at a restaurant.
ii. Public works officials can monitor the diagnostics of the city's power and water supply by installing wireless nodes in water treatment facilities, sewers and generators. There's no need to dig trenches to run cables.
iii. Public safety and emergency workers can access secure virtual networks within the larger network to keep communication lines open, even when regular phone or cellular service is down. With mesh nodes mounted on streetlights and stop lights, police and firefighters can remain connected to the network, even while moving.

Developing Countries

Wireless mesh networks are useful in countries without a widespread wired infrastructure, such as telephone service or even electricity. Solar-powered nodes can be connected to one cellular or satellite Internet connection, which could keep a whole village online.

Isolated Locations, Rugged Terrain

Even in developed countries, there are rugged locations too far off the grid for traditional high-speed Internet service providers. Wireless mesh networks are being considered for these areas. A series of nodes would be mounted from the nearest available wired access point out to the hard-to-reach area.

Education

Many colleges, universities and high schools are converting their entire campuses to wireless mesh networks. This solution eliminates the need to bury cables in old buildings and across campuses.

With dozens of well-placed indoor and outdoor nodes, everyone will be connected all the time. Mesh networks also have the capacity to handle the high-bandwidth needs required by students who need to download large files.

Healthcare
Many hospitals are spread out through clusters of densely constructed buildings that were not built with computer networks in mind. Wireless mesh nodes can sneak around corners and send signals short distances through thick glass to ensure access in every operating room, lab and office. The ability to connect to the network is crucial as more doctors and caregivers maintain and update patient information -- test results, medical history, even insurance information -- on portable electronic devices carried from room to room.

Hospitality
High-speed Internet connectivity at hotels and resorts has become the rule, not the exception. Wireless mesh networks are quick and easy to set up indoors and outdoors without having to remodel existing structures or disrupt business.

Temporary Venues
Construction sites can capitalize on the easy set-up and removal of wireless mesh networks. Architects and engineers can stay wired to the office, and Ethernet-powered surveillance cameras can decrease theft and vandalism. Mesh nodes can be moved around and supplemented as the construction project progresses. Other temporary venues like street fairs, outdoor concerts and political rallies can set-up and tear down wireless mesh networks in minutes.

Warehouses
There is simply no effective way to keep track of stock and shipping logistics without the types of Ethernet-enabled handheld scanners used in modern warehouses. Wireless mesh networks can ensure connectivity throughout a huge warehouse structure with little effort.

Future Applications
The U.S. military, which helped develop wireless mesh technology, foresees a day when thousands of microchip-size mesh nodes can be dropped onto a battlefield to set up instant scouting and surveillance networks. Information can be routed to both ground troops and headquarter personnel.

Carmakers and telecom companies are working to develop **Intelligent Transport Systems (ITS)** powered by street and highway-based wireless mesh networks. Using an automated network of surveillance cameras and in-car sensors, public safety officials can tightly monitor traffic accidents and dangerous road conditions.

Chipmakers and network software developers like Ember Corporation already sell automated home and automated building solutions that employ mesh networks to control and remotely monitor surveillance systems, climate control and entertainment systems. The future applications for wireless mesh networks are limited only by our imaginations.

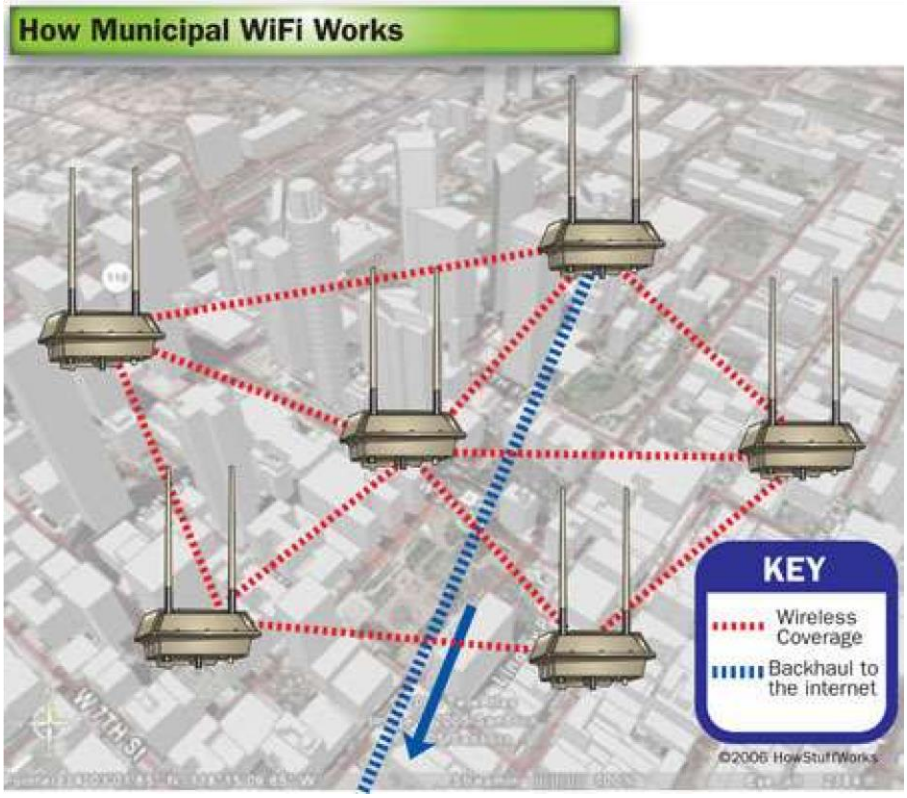

Fig 7.2: Municipal Wi-Fi

7.4 Wireless Internet Cards

Walk into any coffee shop and you'll see scores of people pecking away at their laptop computers. If you feel like everywhere you go -- from college campuses and libraries to Starbucks and McDonald's -- has wireless connectivity, you're not alone. Currently, 241,506 **Wi-Fi hot spots** are scattered throughout 134 countries, and some of those "spots" are entire cities.

These hot spots usually connect to the larger Internet community by wires or cables and broadcast the Internet signal wirelessly to individual computers using radio frequencies. Many personal computers pick up that signal using a wireless Internet card, a small device about the size of a credit card.

Wireless Internet cards, also known as Local Area Network, or LAN cards, are one of the many types of adapter cards that add capabilities to your computer. Other adapter cards can enable teleconferencing, improve sound systems or download photos from a digital camera.

Wireless Internet cards come in several forms. Different cards exist for laptops, desktops and PDAs. Many computers come with one preinstalled, but they can also be purchased relatively inexpensively and self-installed or simply inserted into a slot on the side of the computer.

The sheer number of Wi-Fi hot spots has made wireless Internet cards even more desirable. Initially used mostly in homes or businesses so that multiple people could share an Internet connection, they are a hot commodity for anyone with a computer, especially with entire cities going wireless.

7.4.1 Wireless Internet Cards for Laptops, Desktops and PDAs

Cards labeled as **PCI** refer to the specific language the card uses to communicate with the computer's central processor. PCI stands for **Peripheral Component Interconnect**, which is an industry standard that refers to the way an attached device talks to the computer through a central pathway called the **bus**. PCI network adapters come in many different shapes and sizes called **form factors**. Two common form factors are the **mini PCI**, which is a wireless network card that comes embedded inside a laptop computer, and the **PCI wireless adapter card** for desktops. Since a desktop computer's bus is located inside the computer, wireless Internet cards for desktops have to be installed inside the unit, and most computers come with one preinstalled. If you want an external Internet adapter, you need to look for one that connects through the USB.

Other labels include the **PC Card** or **Express Card** designations. Whereas PCI wireless network adapters communicate through a computer's bus, PC Card adapters just fit into a slot on the side and are used mainly in laptops because of their thin design. The newer Express Card technology has gradually been replacing PC Card adapters.

The PC Card and Express Card designations come from **PCMCIA**, the **Personal Computer Memory Card International Association**, which is the organization that developed a standard network adapter using the PC form factor. You'll sometimes see these cards labeled as PCMCIA cards. Regardless of the name, they all insert into a slot on the laptop's side, and typically stick out a little bit to better transmit and receive signals with their built-in Wi-Fi antennas. You also can buy USB keys that plug in to use as wireless adapters. These devices, which resemble the memory sticks or flash drives you stick into an available USB port on the side of your computer, seem to be an increasingly popular choice.

Yet another type of wireless Internet card exists for PDAs. For people who haven't yet jumped on the BlackBerry bandwagon, there is **WCF**. **Wireless CompactFlash** cards, like PC Cards, fit into a slot on the side or back of a PDA and enable it to communicate with the Internet.

7.4.2 Comparing Wireless Internet Connection Cards

You'll need to pay attention to several things when purchasing a wireless Internet card, such as the networking standard that the card uses. For example, **802.11b**, which used to be the dominant Wi-Fi standard, is meant for wireless networks operating in the 2.4-gigahertz range. It supports a bandwidth of 11 megabits of data per second. The bandwidth refers to how much data can be transferred in a set amount of time. The higher the number, the faster the rate of transfer. So **802.11g** and **802.11n**, which send data over the Internet at speeds of 54 and 140 megabits per second, respectively, are going to stream your video faster than the clunkier 802.11b standard.

Paying attention to the network standard on the card you purchase is important because you need it to be able to communicate with the other wireless products you'll be using. For instance, if your home network uses the 2.4-gigahertz frequency, and you buy a card that just works in the 5gigahertz range, you'll be out of luck. However, if you buy a card that is Wi-Fi-certified for the same frequency band and with the same features (such as encryption codes) of the other products you'll be using, you're good to go. If you want a card that works on different frequencies, you can get a **dual-band** one, which will be compatible with all Wi-Fi-certified products.

In addition, don't forget to look at the card's transfer rate, range and the operating system it requires. Also, consider whether you want a card with an external or internal antenna. Last but not least is security. Wireless networks are notoriously easier to hack into than wired ones, which means you have to take extra measures to protect yourself. The Wi-Fi Alliance suggests always connecting through a trusted provider that uses encryption technologies, enabling security if you have your

own network and buying products that are Wi-Fi-certified for **Wi-Fi Protected Access (WPA)**. Wireless technology shows no signs of stopping its quest to allow you to check your e-mail anytime, anywhere. Soon you may even be able to surf the net while flying at 30,000 feet (9,144 meters).

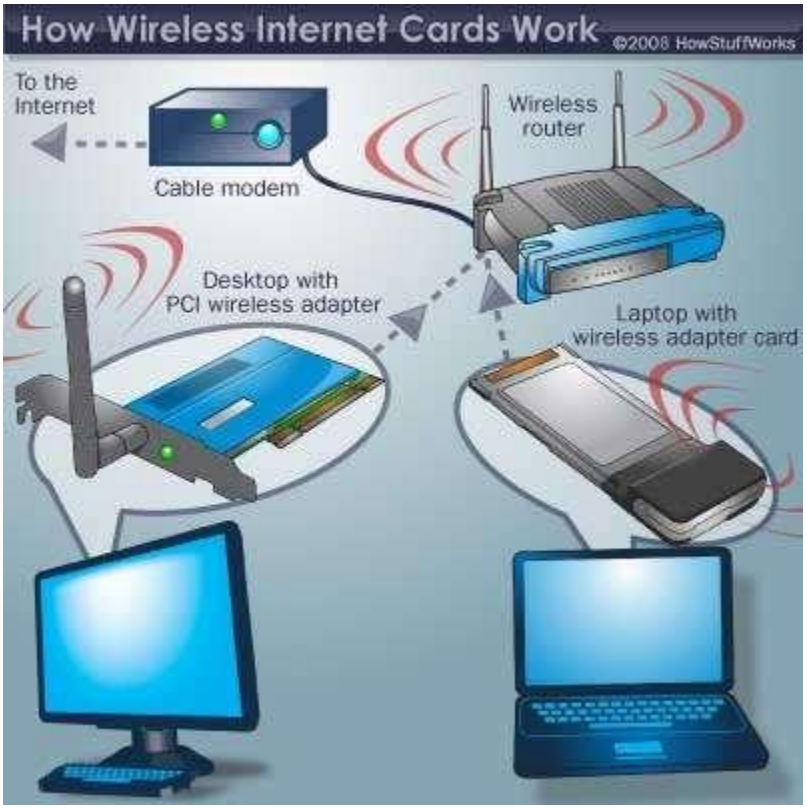

Fig 7.3: Wireless Internet Cards

7.5 Wireless Internet Background

To understand the mechanism behind wireless Internet cards, you first have to grasp how the wireless Internet itself works. Rather than transmitting data through a phone line, digital subscriber line (DSL) or high-speed cable, a wireless Internet network transmits data the same way that radios and cell phones do: radio waves.

A Wi-Fi hot spot, usually a wireless router or access point, first receives information from the Internet the old-fashioned way: through wires. It then translates that data from the binary form (the computer code of 1s and 0s) into radio waves. Next it broadcasts those radio waves into the surrounding area. Wireless signals typically travel between 75 feet and 150 feet (23 meters and 46 meters). In a wide-open area with no obstacles, however, they have been known to transmit up to 1,000 feet (305 meters) and, with optimal conditions, even a mile (1.6 kilometers).

Wireless Internet cards within the range of the radio signal pick it up using a tiny antenna and translate it back into binary code for your computer to read. The process also works in the opposite direction, with the card translating your computer's information into radio waves to send to the router, where it is put back into binary form and sent to the Internet over the wires.

The radio communication used by wireless networks is slightly different from that of radios and cell phones. For instance, wireless Internet cards are designed to work at higher frequencies to handle more data -- typically either 2.4 gigahertz or 5 gigahertz. In addition, the cards and the routers can communicate on one of three different frequency channels. In cases where many people are using the wireless signal, like an airport crowded with business travelers, the cards and the routers can also jump between channels to reduce interference.

Wireless cards operate under networking standards that are a variation of the basic 802.11 standard. These standards were developed by the Institute of Electrical and Electronics Engineers to differentiate between the various technologies. The 802.11b and 802.11g standards are the most common, while the faster 802.11n, which was recently released, is not as widespread.

Although Wi-Fi radio signals have some benefits over regular radio signals, they are still subject to interference by physical obstacles. Interference happens when a signal is hampered by distance or a physical obstacle. For instance, microwaves and many cordless phones operate in the same frequency used by some Wi-Fi networks, so you might notice a slowdown in your service if you're trying to warm your latte while you sign on. Likewise, if you move to another room or if an elephant comes to stand between you and the hot spot, the signal could be lost.

Don't worry if you don't have your own wireless network at home or at work. You can purchase prepaid wireless Internet cards in the U.S. from companies such as T-Mobile, which allow you access to all the T-Mobile hot spots. This can get kind of pricey, though, so you may want to kick in the cash to set up your own network or find a local spot that advertises a free Wi-Fi connection.

7.6 Wireless Networks

The easiest, least expensive way to connect the computers in your home is to use a wireless network, which uses radio waves instead of wires. The absence of physical wires makes this kind of network very flexible. For example, you can move a laptop from room to room without fiddling with network cables and without losing your connection. The downside is that wireless connections are generally slower than Ethernet connections and they are less secure unless you take measures to protect your network.

If you want to build a wireless network, you'll need a wireless router. Signals from a wireless router extend about 100 feet (30.5 meters) in all directions, but walls can interrupt the signal. Depending on the size and shape of your home and the range of the router, you may need to purchase a range extender or repeater to get enough coverage.

You'll also need a wireless adapter in each computer you plan to connect to the network. You can add printers and other devices to the network as well. Some new models have built-in wireless communication capabilities, and you can use a wireless Ethernet bridge to add wireless capabilities to devices that don't. Any devices that use the Bluetooth standard can also connect easily to each other within a range of about 10 meters (32 feet), and most computers, printers, cell phones, home entertainment systems and other gadgets come installed with the technology.

If you decide to build a wireless network, you'll need to take steps to protect it -- you don't want your neighbors hitchhiking on your wireless signal. Wireless security options include:

i. Wired Equivalency Privacy (WEP)
ii. Wi-Fi Protected Access (WPA)
iii. Media Access Control (MAC) address filtering

You can choose which method (or combination of methods) you want to use when you set up your wireless router. The IEEE has approved each of these security standards, but studies have proven

that WEP can be broken into very easily. If you use WEP, you may consider adding Temporal Key Integrity Protocol (TKIP) to your operating system. TKIP is a wrapper with backward compatibility, which means you can add it to your existing security option without interfering with its activity. Think of it like wrapping a bandage around a cut finger -- the bandage protects the finger without preventing it from carrying out its normal functions.

Revision questions

1. What is a Wireless Markup Language?
2. What is a wireless Mesh Network?
3. What are the applications for Wireless Mesh Networks?
4. Describe Wireless Internet Cards used in wireless communication
5. What security measures can be used in a wireless network?