Basic Home Networking

DSL/Cable

The two most popular means of acquiring high speed Internet access within your home are DSL and Cable. For the most part the standard user won't see much difference between the two but let's take a moment for a quick comparison:

- Speed: Cable typically has a higher speed than DSL but sees more variance in speeds depending on traffic
- Security: Comparable
- Satisfaction: Comparable, though DSL providers typically rate higher in reliability

Either product will deliver an Internet connection that will serve the purposes of today's class.

DNS

DNS, or the Domain Name System, allows us to access web sites and network resources using names accessible to human beings. Each computer requires a DNS server to allow it to connect to websites. This can be viewed through the Control Panel→Network→Local Area Connection→Internet Protocol properties.
The DNS server is typically assigned automatically and only needs to be changed if the computer is having difficulties finding it or if you wish to customize how you travel around the Internet. [OpenDNS is an excellent example of these options]

TCP/IP

The TCP/IP protocols are, loosely speaking, a means of addressing and organizing network resources. Typically computers are automatically assigned a TCP/IP address, though if you like you can specify the addresses within your network. Other resources (for example, printers) can be assigned a network address, depending on how they are set up – we'll discuss in more detail in the next section. While the address assigned can indicate problems to computer technicians, typically the key thing you need to remember about TCP/IP addresses is that they need to be unique. If two resources in the same network have identical addresses one of them will be unable to connect.

Sharing Resources

The reason we go to the trouble to create networks is so multiple computers can share resources. This can mean many things; printers, files, software, etc. Before sharing resources your computer must be part of a workgroup or domain. This is set in the Control Panel→System properties (demonstrated in class.) The sharing of resources is controlled through the item's properties screen (reached by right-clicking and choosing "Properties") or by selecting "sharing" or "share with" from the right-click menu. When

allowing sharing deciding what level of permission to allow becomes an important choice. This decision is based on how much freedom you want to give the other users.

Wireless Networking

Wireless networks, in many respects work exactly like wired networks. The same data is passed, the same connections are made, etc. The difference is, of course, that one involves data moving across wires, and the other involves using radio waves to transmit data.

What changes when we send data through the air instead of over wires? First, speeds decrease. Where speed over wires has reached 10 Gbps (10,000 Mbps), wireless speeds have, thus far, topped out at 248 Mbps. It is important to note that these speeds are theoretical maximums and that under typical circumstances, you would see speeds slower than are listed above.

802.11

The 802.11 standard, as handed down by the IEEE (Institute of Electrical and Electronics Engineers), handles standardization of what is known as a WLAN (wireless local area network). The IEEE is a professional organization known for being one of the leading standard making organizations in the world. By providing standardized technical specifications, the IEEE helps to ensure that products from different manufacturers work together.

The 802.11 standard has several subcategories, each of which define a different protocol for wireless LAN communication.

802.11b

802.11b provides for maximum speeds of 11 Mbps in an indoor range of approximately 38 meters.

802.11a

802.11a provides for maximum speeds of 54 Mbps in an indoor range of approximately 35 meters.

802.11g

802.11g provides for maximum speeds of 54 Mbps in an indoor range of approximately 38 meters.

802.11n

802.11n provides for speeds up to 248 Mbps with an indoor range up to 70 meters. This is obviously a significant upgrade from previous versions of the 802.11 standard, however, the typical speeds one would be likely to see using an 802.11 network will be significantly slower (estimated at 74 Mbps) than the maximum.

Security

When working with a wireless network, it should also be mentioned that you are not as secure as when working on a wired network. The reason for this is that when using wires, in order to intercept any data, someone would have to be physically connected to those wires somehow. Whereas with a wireless network, someone would only need to be in the area of the wireless broadcast to potentially intercept your data.

WEP vs. WPA

There are ways to make up for this decrease in security. The first is WEP.

WEP (Wired Equivalent Privacy) is an authentication protocol that aims to provide security similar to that of a wired network.
The most common implementation of WEP is the use of a Shared Key. The way this works is that both the access point and the computer connecting to the access point are given a key (password). When the computer attempts to connect to the network, the computer asks the access point to authenticate it. The access point then sends a challenge message to the computer. It is then the computer's task to send back that same message, encrypted using the shared key. The access point then decrypts the message using the key it has. The decrypted message should match the message the access point sent to begin with. At this point, all the messages sent between these two points will be encrypted using the WEP key used to authenticate the computer in the first place.
The second, and more secure way to use WEP is called Open System authentication. In this mode, there is no true authentication. The computer is allowed to associate with the access point, and then the data is encrypted using the key that each should have been given. If the correct key is not shared, the two will not communicate properly. The reason Open System authentication is more secure is that it is possible to get the WEP key if the authentication traffic is intercepted. By not having that traffic in the first place, Open System authentication proves to be more secure.

WPA (Wi-Fi Protected Access) is another security measure, created by the Wi-Fi Alliance in response to weaknesses with WEP. WPA is more secure, relying on keys that change dynamically, and more robust encryption methods. To the user, however, WPA works in a very similar fashion as the Shared Key implementation of WEP.