LAN

Remember that a Local Area Network (LAN) is a small network as you might have in a home or business.

LAN

To have a LAN, we need a way for the computers to communicate with each other.

Though it is possible to connect computers in a line or ring so that each passes on information to the next, most real LANs communicate through a central device, the *router*. Each computer needs a device that can communicate with this device – a network card.

We are using the term router to mean any computer whose job is to guide packets when there is more than one direction to go. In fact, there are technically routers, hubs, and switches. Any packet sent through a hub is sent to every machine it is connected to, which is a waste of bandwidth. A switch, on the other hand, knows the addresses of the computers it is attached to, and can send a message only to the correct destination. A router's job is to send packets between networks. So, technically, the "router" in a LAN is usually a device that integrates a router and a switch, so that it can deal with the local computers and also talk to outside networks.

A router is either wired, in which case Ethernet cables are used to connect computers to the router, or wireless, in which case it can communicate either through wireless signals (wi-fi) or cables. A wireless router is sometimes called a wireless access point. The

network cards in the computers on the LAN must match the router – a wifi router is no good if the computers don't have wifi.

To talk to the internet, a LAN generally also needs a *modem*. In some cases, this might be integrated into the same device as the router.

Security

A firewall is a program whose job is to control what information is allowed into or out of a system. This is usually done by packet filtering – based on information in a packet, a firewall might not allow that packet into a system, if it were sent from an IP address known to be owned by criminals, or out of a system, if it came from the port number of a program that is not allowed to talk to computers outside the LAN. More advanced firewalls may filter at the transport layer, using more information on the packets, or at the application layer, using information about specific application protocols.

Individual computers can run their own firewall programs, many routers have firewall programs built in, and a business might buy a separate machine whose one job is to run the firewall.

Note that while a firewall might stop spyware from getting onto a system (if it came from a known criminal source) or disrupt the working of malware – it might stop spyware from sending keylogged information to a criminal, for example – its job is not to detect or remove malware; that's what antivirus programs are for.

If we are using wifi for our LAN, there are other security issues, because information sent over wifi travels through the air and right through walls. This means that a computer outside your

house could connect to your router and become part of your network, so that anything it did would come from the IP address given to you by your ISP, and it could potentially look at files you have shared among the computers on your network.

However, stopping incoming connections is not the the biggest security issue involved in wireless networks. Just as outside persons can send packets in through your walls, all your packets are constantly sent *out* as well, and can be read by any other computer in range. So it would be easy for the data you send and receive, such as user names and passwords and bank account numbers, to be read by strangers.

One approach to wireless security is MAC filtering. Each network card has an ID number called the Media Access Control address, which can be used to identify it. Most routers can do MAC filtering; you enter the MAC addresses of all your computers, and the router will not allow any machine not on that list to join the network[1]. Notice that this only addresses the problem of computers joining the network; it has no effect on who can read the packets.

WEP (Wired Equivalent Privacy) is another approach. In WEP, each computer must provide a password to connect to the network, and every packet sent over the network is encrypted before being sent, so that if it is intercepted it is harder to read. WEP passwords are relatively short, and WEP encryption is fairly weak, which means it is very easy to defeat. WEP has been replaced by WPA (Wifi Protected Access) which uses longer passwords to keep computers from joining the network and more complex encryption so that packets are difficult to read by outsiders.

---

[1] Which works well until a computer lies about its MAC address, which is easy to do.

Internet Access

To get internet access, our computers must communicate with computers at an ISP. There are various ways this connection can be made.

The speed at which information travels is described in terms of bandwidth – how much data can travel over a connection in a set amount of time[2]. Data sent from a computer is an upload, while data sent to a computer is a download. Most ISPs offer more bandwidth for download than upload; this makes sense: typically a personal computer is uploading very small messages – requests sent to servers – while downloading large files from servers.

Latency describes the delay in a message being sent from one machine to another. Various problems could cause delays, for instance having to travel a longer distance, or go through more routers along the way. A connection might have high bandwidth, meaning that the data is traveling fast while it is moving, but also high latency, meaning many delays, in which case we would probably feel the connection was slow.

Local IP Addresses

When you connect to the internet, you get an IP address from your ISP. However, you need not connect to an ISP to have a home LAN that allows your computers to talk to each other. And since your ISP would charge you for extra IP addresses, we need a way for computers on a LAN to get IP addresses they can use locally, and a way for multiple computers to share the single IP address from the ISP.

---

[2] A common unit is mbps – mega *bits* per second. Consider why a company selling the service might use a unit an eighth the size of how we usually measure files…

A Dynamic Host Configuration Protocol (DHCP) server follows the rules of the IP to assign IP addresses to computers. Your ISP's DHCP assigns you an IP address when you connect; this is your public IP address. Certain ranges of IP addresses have been set aside for use on LANs, and cannot be used on the internet at large. These are called local IP addresses. When a computer joins your LAN, your router's DHCP server assigns it a local IP address. This can be done statically or dynamically. Your computer uses a local IP address exactly as it would a public one.

Network Address Translation

Local IP addresses are fine for use on a LAN, but to talk to other computers on the internet, we must use a public IP address. Network Address Translation is a process that allows several computers to share a single public IP address by translating the addresses in packet headers coming in and out of a LAN. From the rest of the internet, it will look like there is a single computer at that public IP address.

Any packet being sent out to the internet from a computer on the LAN will have been originally created with the computer's local IP address and the program's port set as the *From* address for the packet.

When the packet reaches the router, it must change this *From* address to the public IP address, which is the only address we have that is valid for use on the internet. So the router is going to lie about where the packet came from.

But probably some other computer will be responding to this packet – it might be a request to a server for a web page or email – and several other computers on the LAN may be awaiting responses to the packets they have sent as well. So the router

needs a way to keep track of the lies it has told so that it will know who to give each reply to when it arrives.

So, the router will make up a port number to stand for the combination of local IP address and local port number, and record this in a table. It puts this made up port number on the packet along with the public IP address as the *From* address. Then the packet can be sent out.

Any packet arriving at our router from the internet is actually intended for some port on one of the local computers. The router can't figure out which one it is for based on the *To* IP address alone – that's just the public address we're all hiding behind. Instead, it looks at the *To* port number. That will be a port number the router made up earlier and recorded in the table.

Looking it up in the table, the router can find the combination of local IP address and port number, to see which computer and which program on the computer this packet was actually intended for. Then it changes the *To* address on the packet and gives it to the correct recipient.

So, anything outgoing has the *From* address translated from local to public, and a port number made up and recorded in a table. Anything incoming has its *To* address translated from public to local by looking up the port number in the table.

Types of ISP connection

One way to connect to an ISP is by using lines that already existed for other types of communication, such as phone lines.

Dial-up internet access works by making a phone call. Originally, all phone lines were analog, so information sent from a computer had to be translated from digital to analog to go on the phone

line and then from analog to digital at the other end. A device to do this translation was called a modulator-demodulator, or *modem*. Although other forms of internet access did not require the analog/digital translation, the name modem has stuck for a device that formats data for sending to and from an ISP.

Dial-up internet access was often paid for by the minute, as it could only be used while making a phone call to the ISP's computers.

Most analog telephone lines have been replaced with digital lines, which allows data to be sent without translation to analog and also allows the line to be used for more than one purpose at the same time – it can be used for internet traffic and for making phone calls simultaneously.

Digital Subscriber Line (DSL) is one form of internet access over digital phone lines. It is an *always-on connection*, in which the household maintains connection to the ISP all the time, rather than having to connect only when access is needed.

Another form of communication line already in place is *cable*, used for cable television. Part of the bandwidth of a cable line can be used for internet access. In a neighborhood or apartment building, there is typically a shared box, with lines from many homes coming together. From a house to this box, the full bandwidth of the cable is available to each customer; from the box onward, the bandwidth of the connection is shared with everyone else in the neighborhood using cable internet. For this reason, cable internet tends to slow down at times of peak usage, when the bandwidth is being used by more people.

Recently companies have put new fiber optic cables in the ground to provide dedicated internet connections to customers generally. This is used for FiOs internet service. Similar to cable, in FiOs,

lines from several houses come together to share bandwidth, although FiOs companies say that their system involves less sharing of bandwidth than cable.

Fiber optic lines are certainly higher-bandwidth than basic cable lines. For this reason, many cable internet companies have been replacing the lines in their regional networks with fiber optic as well.

For those who need and can afford a dedicated connection that is not shared, there is the *Leased Line* – a customer pays to have a communication line laid directly from them to their ISP. These tend to be used by schools and businesses. The bandwidth of a leased line is not shared with other customers, and unlike other forms of ISP access, as much of the bandwidth can be used for upload or for download as the customer needs. This is ideal for campuses, where there are many individual computers downloading from outside servers, but there is also a mail server and a web server uploading to clients off-campus.

Rather than using existing or new communication lines, another option is to simply send the information through the air.

In some places, the only option is *satellite* internet. A customer's computer sends data through a satellite dish, which bounces it off a satellite in orbit and back down to a dish at their ISP. This is an example of a connection that has high bandwidth but also high latency because the data has such a long distance to travel.

For Cellular Data, towers that can send and receive signals are placed every few miles, and as long as a computer is close enough to send a signal to one tower, the data can be sent from tower to tower until it reaches the ISP.

There are several standards for cellular data, but don't be confused by the terms 3G, 4G, etc; the G is short for generation,

so it simply means a particular system’s 3rd version, 4th version, etc.