

Computer networking

In this section of notes you will learn the rudiments of networking, the components of a network and how to secure a network

James Tam

What This Section Will And Will Not Cover

- What we will talk about:
 - The principles of how a network functions, the different parts of a network and one way of securing a network.
- What we won't talk about:
 - The step-by-step process of building a network.
 - Typically you can find many sites that already provide this information:
 - E.g., <http://www.microsoft.com/windowsxp/using/networking/setup/default.msp>

James Tam

What Is Required For A Network

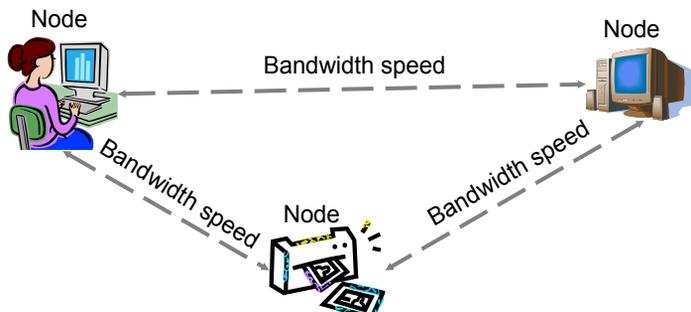
- 2+ computers
- The hardware and software needed to connect them



James Tam

Introducing Some Basic Parts Of A Network

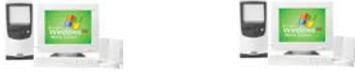
- Nodes:**
 - Hardware devices that are connected to the network (e.g., printers, computers)
- Bandwidth:**
 - Speed at which information transmits through the network
 - Maximum typically 10 – 100 Mbps



James Tam

What You Need For A Two Computer Network

- Two computers (obvious)



- A network adaptor for each computer



"NIC" (network interface card/controller)



USB to network adaptor

- It's hardware that acts as an interface between the computer and the network.
- It can be wired or wireless.
- Many new computers include this hardware (no need to buy a special component).

James Tam

What You Need For A Two Computer Network (2)

- Ethernet connection: a network cable.



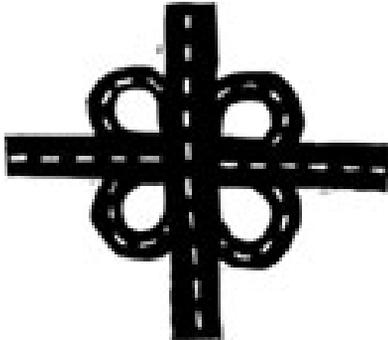
- Or as an alternative a cross-over cable can be used (looks physically identical to a regular network cable but allows the computers to be connected without the need for additional hardware e.g., hub, switch).
- Software to support the network connection (included in modern operating systems like Windows).

James Tam

What You Need For A Multi (3+) Computer Network



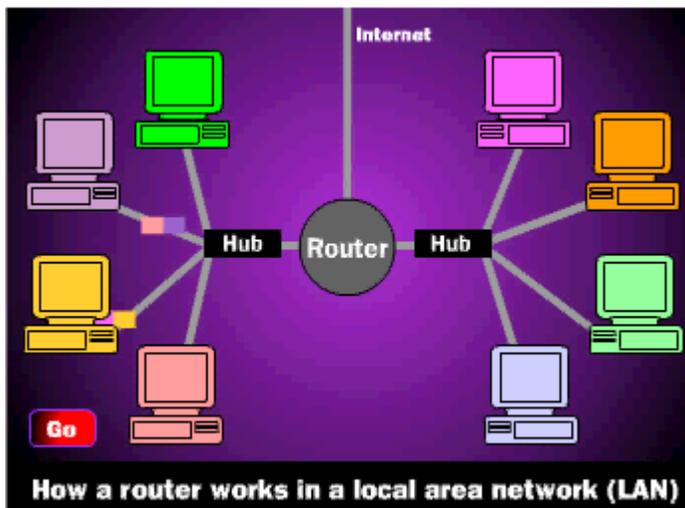
- The items mentioned for a 2 computer network
- Plus a network switch
 - Brings all of the connections together and routes information internally



James Tam

Router

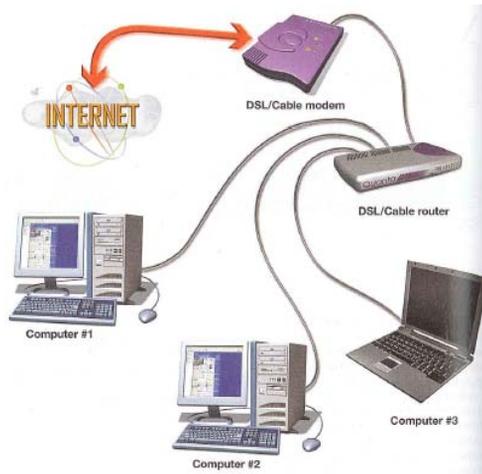
- Used to *connect multiple networks*.



James Tam

Router (2)

- Routers can also be used to share a broadband connection (referred to as DSL/cable routers)

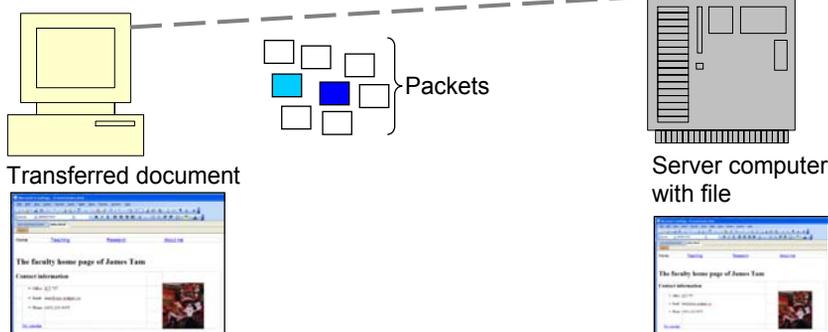


From "Technology in Action" by Evans, Martin and Poatsy

James Tam

Transmitting Information On A Network

- Information is broken down into parts (packets).

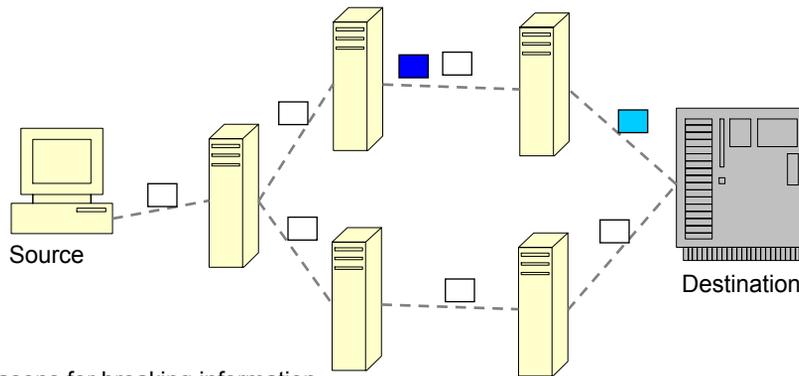


- The packets are sent over the network.
- When the packets reach their destination they are reassembled into their original forms.

James Tam

Transmitting Information Over A Network (2)

- The route taken can vary from packet-to-packet:



Reasons for breaking information into packets:

1. Speed
2. Stability

James Tam

Types Of Network Connections

- Wired
 - Twisted pair: typically used for home or small networks although the fastest ones now rival fiber optic in terms of speed.
 - Fiber optic: used for larger networks when a lot of data is transmitted.
 - Power -line networks: uses existing electrical wiring to transmit network information.
- Wireless
 - Typically use the Wi-Fi protocol for transmitting information

James Tam

Twisted Pair Network Connections

- The transmitting wire consists of a collection of paired wires

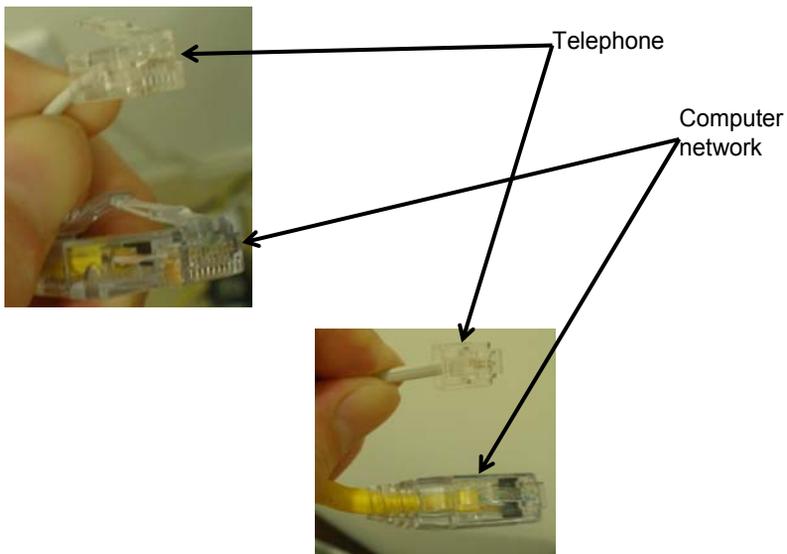


Category "Cat"	Max bandwidth
Category 5	100 Mbps
Category 5E	100 – 1000 Mbps (1 Gbps)
Category 6	1000 Mbps (1 Gbps)

James Tam

Twisted Pair Network Connections (2)

- The ends look similar to but are larger than telephone cables.



James Tam

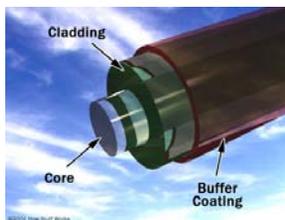
Twisted Pair Network Connections (3)

- Pros:
 - Mature proven technology: stable with a great deal of choice
- Cons:
 - Rewiring of an existing home may be expensive (although new homes – North America - often have Cat 5 wiring through out the house).
- Typical range ~300'

James Tam

Fiber Optic Network Connections

- Unlike twisted pair and coaxial connections which use electricity, fiber optic connections use light.

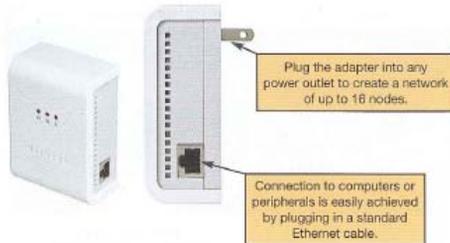


- Pros:
 - Fast transmissions (~100 Mbps – 30 Gbps) with few errors
 - Very long range connections are possible (~62 miles)
 - Typically used for large networks where there's a high volume of information transmitted
- Cons:
 - Expensive

James Tam

Power-Line Network Connections

- Rather than requiring new wires to network equipment, this type of network uses existing power lines.



- Transmission rates: 200 Mbps

James Tam

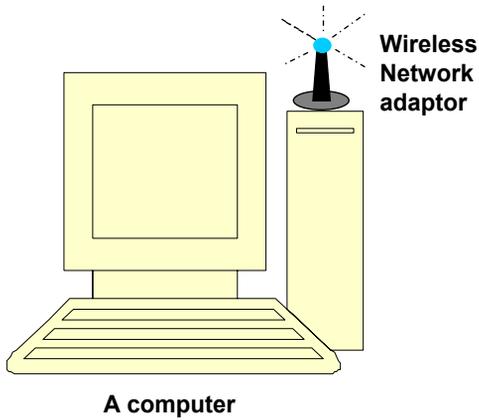
Power-Line Connections (2)

- Pros:
 - Easy to set up.
 - No new wiring needed, flexibility in the layout of nodes.
- Cons:
 - An entire power outlet must be used (power bars cannot be used).
 - Performance can be affected by power usage.

James Tam

Wireless Network Connections

- The network is connected via radio waves.
- The general requirements for setting up a wireless network are similar but not identical to a wired network:



James Tam

Types Of Wireless Network Connections

- All are based on the 802.11 standard (also known as Wi-Fi) for wireless transmissions

Transmission protocol	Maximum bandwidth
802.11g	52 Mbps
802.11n	540 Mbps

James Tam

Wired Vs. Wireless Networks

- **Wired:**

- Speed (faster for many)
- Security
- Less likely to be affected by interference

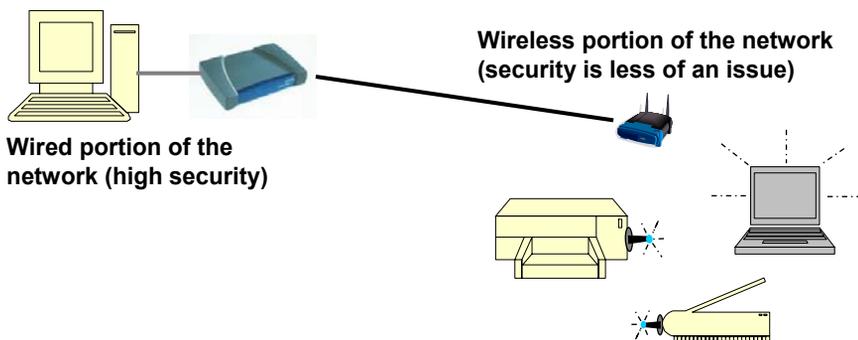
- **Wireless:**

- Convenience

James Tam

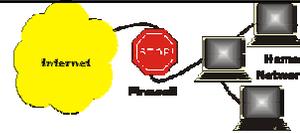
Mixed Networks

- To balance the strengths of wired networks vs. the strength of wireless networks a network can mix-and-match between wired and wireless connections.



James Tam

Firewall



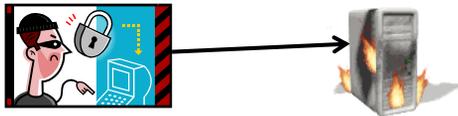
- It's *one way* of protecting a network.
- Protects the network against things coming into the network:
 - Certain type of connections to your computer can be disabled e.g., transfer of files to/from your computer.
 - Connections may be made only by certain users or only within a certain period of time e.g., file transfer only possible for today or only possible for login name 'tam'
- Some may screen outgoing data

James Tam

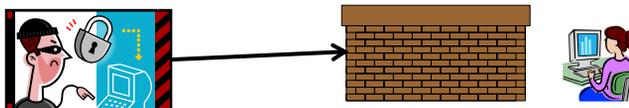
Firewalls (2)

- Firewalls may be implemented as software or hardware
- Software based firewalls:
 - Easy to set up and inexpensive (e.g., Windows comes with one built in)
- Hardware based firewalls:
 - Your computer can be attacked if it can be located on the Internet

No firewall: your computer has been located



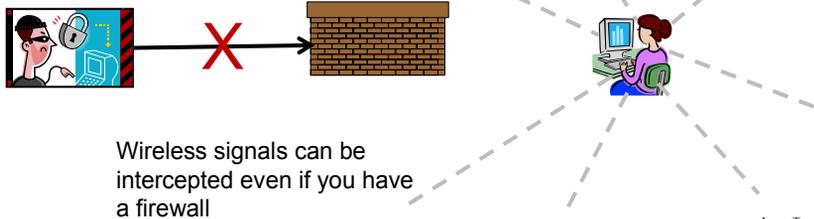
Hardware firewall: only the firewall is visible



James Tam

A Firewall Will NOT Make You Invulnerable!

- Firewalls cannot protect against carelessness. If YOU choose to allow a malicious program to have access to your computer then the firewall may still be bypassed. (This is an example of “Social Engineering” and will be discussed further in the section on computer security).
- Also if your firewall is secure and your wireless signals are not secure then someone else may be able to ‘sniff’ out private information from the wireless signals on your network.



After This Section You Should Now Know

- What is a computer network
- What are some of the benefits of networking computers
- What's needed to network computers
- The role of a switch in a network
- The purpose of a router in a computer network
- How is information transmitted on a network in the form of packets
- The characteristics of common wired and wireless networks
- How a firewall can be used to secure a network as well as the things that they can't protect