Networks

Connecting Computers
- Computers use networks to communicate
  - like people use telephones or the postal service
- Requires either some sort of cable …
  - point-to-point links connect exactly 2 computers
    - dial-up, ADSL
  - broadcast networks connect multiple computers
    - or radio waves
    - WLAN, GPRS (cell phone)

Measures for connection speed
- **Bandwidth** is the amount of data transferred per unit time
  - usually measured in megabits per second (Mbit/s)
  - high is good
- **Latency** is the time between the departure of data from the sender and its arrival at the receiver
  - usually measured in milliseconds (ms)
  - low is good
- These are not equivalent, e.g. your car
- Driving CDs to school in your car is high bandwidth
  - (10 CDs*650MB/CD*8Bits/Byte)/(15min*60)=900Mbit/s
  - way faster than cable modem (~3Mbit/s)
- Driving an essay to school in your car is high latency
  - takes 15min, way slower than dial-up (~30s)

Ethernet
- Invented by Dr. Robert Metcalfe in 1970 at Xerox Palo Alto Research Center
- Allows group of computers to communicate in a Local Area Network (LAN)

Ethernet protocol
- Ethernet uses a system where each computer listens to the cable before sending anything through the network
- Information or data is broken into packets
- If network is clear computer will transmit or send the data until it arrives at the destination without colliding with any other packet

Collision detection
- Carrier Sense Multiple Access/Collision Detection (CSMA/CD)
- If any device attached to a network, such as file servers, printers, or workstations is sending data on the cable computer will wait and try again when the line is clear
How to connect 100,000,000 computers?

- It is virtually impossible to run a single wire across the world to connect all computers.
- Solution: Connect each computer only to a few others and pass on data from one to the next until it reaches its destination.

Terminology

- A network topology describes the way computers are connected in a network.
- Switching is the process of reading data from one connection and sending on another one.
- The process of directing data to the correct destination in the network is called routing.
- To be sent across a network, data is split into packets.
- A hop is the traversal of a single connection between two computers by a packet.
- Computers in a network are called hosts or nodes.

Network Topology

- Restricted by how many other nodes each node is connected to.
- Diameter of a network is the maximum number of hops it takes to get from one host to any other.
- Bisection is the maximum number of connections that can be removed without splitting the network into two.
- Small networks use regular topologies.
  - named topologies that describe the “shape” of the network, such as tree, ring and star.
- Most large network topologies are irregular.
  - combination of regular topologies.

Ring

- 2 connections per host.
- 12 links total.
- Diameter is 6.

Torus

- 4 connections per host.
- 24 links total.
- Diameter is 3.

Star

- 11 connections at center host.
- One connection at all other hosts.
- 11 links total, diameter is 2.

Networks are often a combination of regular topologies.
**Finding a path**

- To send a packet to a known destination every computer along the path must know where to send the packet next.
- In **circuit switching** this information is determined for the entire path before the first packet leaves the sender. This is how the telephone system works.
- In **packet switching** each computer determines the next destination whenever a packet arrives.
- Allows packets exchanged between same sender and receiver to take different paths.
- Can always send data on least used connection.

**Packets**

- Contain information about the sender’s address, the receiver’s address, and some amount of data.
- Like letters or postcards.
- Long documents are split into multiple packets before they are transmitted and reassembled upon arrival.

**Packet switched ethernet**

- Split shared line into **segments**.
  - Broadcast within segments.
  - Packet switching across segments.
- Segments are connected to **switches**, computers within segments are connected to **hubs**.
- Data sent within one segment is not seen on others.
  - Multiple hosts can communicate at the same time, as long as they are on different segments.
  - Switched ethernet also prevents sniffing (we’ll get to that).
- Most large eternets are switched.
  - E.g. Duke computer clusters.

**Switched ethernet network**

- Internet/Internet

  - An internet is a collection of interconnected networks.
    - Wide Area Network (WAN).
    - Gateways, routers, backbones, switching.
  - The **Internet** is the largest example of an internet.

**The Internet**

- “The information superhighway” - transports vast amounts of information from point to point at high speeds along telephone lines, cables, satellites and microwave links.
- Web browser – your “window to the Internet”.
- Internet service provider (ISP)
  - Companies that allow you to connect to their computers.
    - Which in turn are connected to the Internet.
- Routers
  - Computers that direct information to its destination.
- Internet backbone
  - Phone lines and cables.
- Network service providers (NSPs).
- Network access points (NAPs).
How the Internet works

- A **protocol** defines what packets exchanged in networks look like and how they are processed
- All computers on the Internet use **IP** (the Internet Protocol)
- To define a destination every host needs an address
  - IP addresses consist of four 8 bit numbers that uniquely identify a host: 152.3.233.7
- IP addresses are easy to process in programs, but hard to remember
  - Humans normally use domain names: **www.duke.edu**
  - The domain name service (DNS) translates domain name into IP addresses

TCP/IP

- There is no TCP/IP protocol, they are two different protocols
- IP allows all computers to exchange packets by defining a “common language” and addressing scheme
  - IP is best-effort – it does not guarantee that packets arrive at their destination
  - IP packets will not always arrive in the order they were sent
  - IP packets carry no information what application they belong to
- TCP, the Transmission Control Protocol, uses IP to sent packets and
  - puts them in the original order (in-order-delivery)
  - makes sure no packets are lost, by keeping to ask the sender for missing ones (reliability)
  - distinguishes packets for different applications by assigning every program a unique port

Internet ≠ WWW

- The Internet is an **infrastructure** that is used by different services that exchange data using TCP/IP
  - WWW (World Wide Web)
  - email
  - Instant messaging (ICQ, AIM, …)
  - Chat (IRC)
  - File transfer (FTP)
  - File sharing (Napster, Gnutella, eDonkey, Kazaa)
  - …

Domain names

- Domain names are organized back to front
  - Top Level Domain (TLD) - the last piece (**www.duke.edu**)
    - there are generic TLDs, such as .com, .org, .biz, .info, .aero, .net, .edu
    - and country TLDs: .jp (Japan), .it (Italy), .at (Austria)
  - The piece before the TLD (**www.duke.edu**) has to be registered by anyone wanting to use that domain
    - registration managed by different organizations for different TLDs
    - e.g. VeriSign for .com
  - The remainder (**www.duke.edu**) often specifies a service, but does not have to
    - can be arbitrarily many pieces here (**www.acpub.duke.edu**)
  - Internet Assigned Numbers Authority (IANA) assigns IP addresses and coordinates management of domain names

Important tools

- **nslookup** translates domain names into IP addresses
- **whois** prints information about the owner of a domain
- **ping** determines if a computer on the internet is reachable, i.e. running and receiving messages
  - find out if a connection is working
- **tracerout** prints the path taken by packets from the local computer to another computer (on Windows it is called tracert)
  - find where a connection is broken
  - explore network topology from a single host

Internet security

- In the early days the Internet was used by few people that knew each other
  - security not an issue
- Today millions of people use the Internet and security has become a problem
  - For the most part communication on the internet is anonymous
    - hard to determine sender of an email, owner of a webpage or chat partner
  - Commercial transactions (like online shopping) make Internet crime profitable
Bad things happening on the Internet

- Spam is unsolicited email, e.g., ads for Viagra™, Cialis™
- Scams is spam with fraudulent intent, e.g., "Nigeria" scam
- Email viruses are little programs that spread via email
  - disguised as normal attachment
  - most viruses require the user to click on them, but some are started by just viewing the mail
- Worms are programs that spread through the Internet by infiltrating computers
  - use bugs in the operating system or server software to gain control of a computer
  - need no human intervention to spread
  - spread faster than viruses
  - Slammer worm infected >50000 hosts in 10 minutes

More bad things

- Denial of Service (DoS) attacks prevent a service from doing its work by flooding it with useless requests
- Defacements are modifications of web pages by hackers
- Trojan horses are seemingly useful programs that have hidden malicious functions
  - SpyWare is a special kind of Trojan horse with the purpose of collecting information about the user
- BackDoors secretly give hackers access to a computer
  - often installed by viruses or as part of a Trojan horse
- Sniffers can read all traffic routed through a computer or sent on a broadcast network
  - used to search for passwords or other sensitive information
  - do not work on switched Ethernet used today
  - big problem for wireless LANs

The email problem

- Although every email message carries a sender address in the "From" field it is impossible to verify where it came from, because the sender is never verified
  - forging an email sender address is easy
- Virtually impossible to track down the true source of email
  - email can be read by anybody who has access to the mail server or a connection the mail is sent over
- Use encryption to authenticate and protect email
  - S/MIME in Outlook, PGP

IP Spoofing

- Like email IP packet carry a sender address
  - ...and like email the sender can be easily forged
- Most protocols require multiple requests and responses
  - if a host sends a packet with a forged sender address it won’t see the reply, because it is sent to the true owner of the IP address
- Must be able to monitor outgoing traffic from victim
  - hosts along the route between the victim and the true owner of the false IP address can do this
  - hosts in the same broadcast network as the victim can do this

IP spoofing example

Victim 154.67.8.5

Router 154.67.8.6

Server 148.30.2.1

From 154.67.8.5 To 148.30.2.1
What’s the quote for Yahoo?

From 154.67.8.5 To 148.30.2.1
Yahoo is $60

From 154.67.8.5 To 148.30.2.1
Yahoo is $30

Attacker 154.67.8.4

Victim wants to connect to server and sends request
Attacker sees connect because it is broadcast

Attacker replies with a forged reply
Server also replies
Forged message arrives first
Victim ignores server’s reply, because it has already seen a reply
How hackers attack

- **Port scanners** can determine what kind of networking software is running on a computer and if it is a potential target
  - e.g. nmap
- **Security scanners** test a computer for known security problems, bugs and backdoors
  - e.g. Nessus
- **Exploits** are small programs that use bugs to give a hacker control over a system
- **Root kits** hide the presence of a hacker from the user and allow him/her to take control over a computer even after bugs are fixed

Making the Internet Secure

- **Firewalls** protect computers from unwanted accesses by filtering all incoming packets and allowing only certain services
  - often included in (wireless) routers
  - sometimes prevent programs from working e.g. ICQ, Quake, Napster
  - no protection from viruses
- **Intrusion Detection System (IDS)** monitor network traffic for suspicious activity to detect attacks
  - e.g. snort
- Many internet protocols have been extended to use encryption and authentication
  - Prevents sniffing and IP spoofing
  - https for secure forms on WWW
  - smtps and imaps for email

References

- [http://www.zone-h.org](http://www.zone-h.org)
- [http://www.insecure.org](http://www.insecure.org)
- [http://www.securityfocus.com](http://www.securityfocus.com)
- [http://hoaxbusters.ciac.org](http://hoaxbusters.ciac.org)
- [http://vil.mcafee.com](http://vil.mcafee.com)