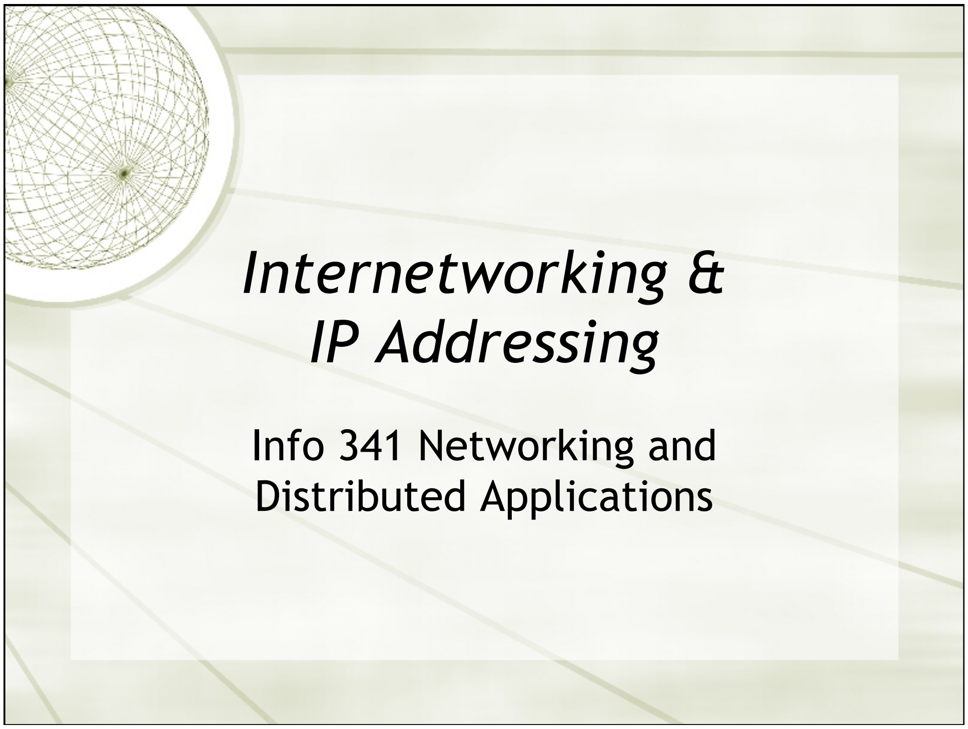
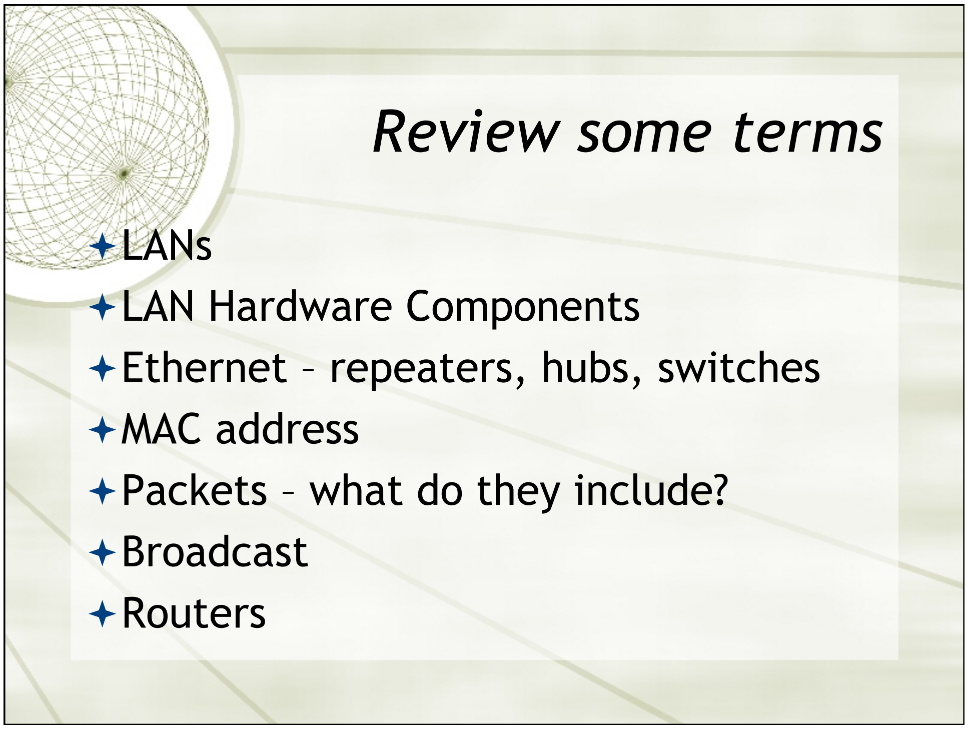


Internetworking & IP Addressing

Info 341 Networking and Distributed Applications



Review some terms

- LANs
- LAN Hardware Components
- Ethernet – repeaters, hubs, switches
- MAC address
- Packets – what do they include?
- Broadcast
- Routers

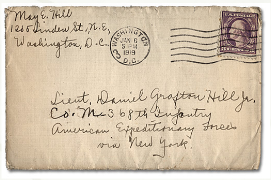
Protocols

- Protocol - an agreement about how endpoints will communicate
  - Protocols are an end-to-end concept
- Protocol Suite - a set of protocols that handle a full range of communication details and error handling (also called a ‘stack’)
  - Give me an example of a protocol we use in our daily lives?

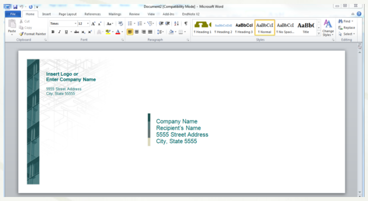
Protocols

- An agreed upon way to communicate
- Protocols establish rules for the communication to be successful
  - We use protocols in everyday life as well as on the Internet
  - Protocols may exists for years, even when other parts of the process or other technologies change

Example: Sending a letter through the US Post Office


May E. Hill
1265 Linden St, N.E.,
Washington, D.C.

Lieut. Daniel Grafton Hill Jr.
Co. M - 368th Infantry
American Expeditionary Forces
via New York.

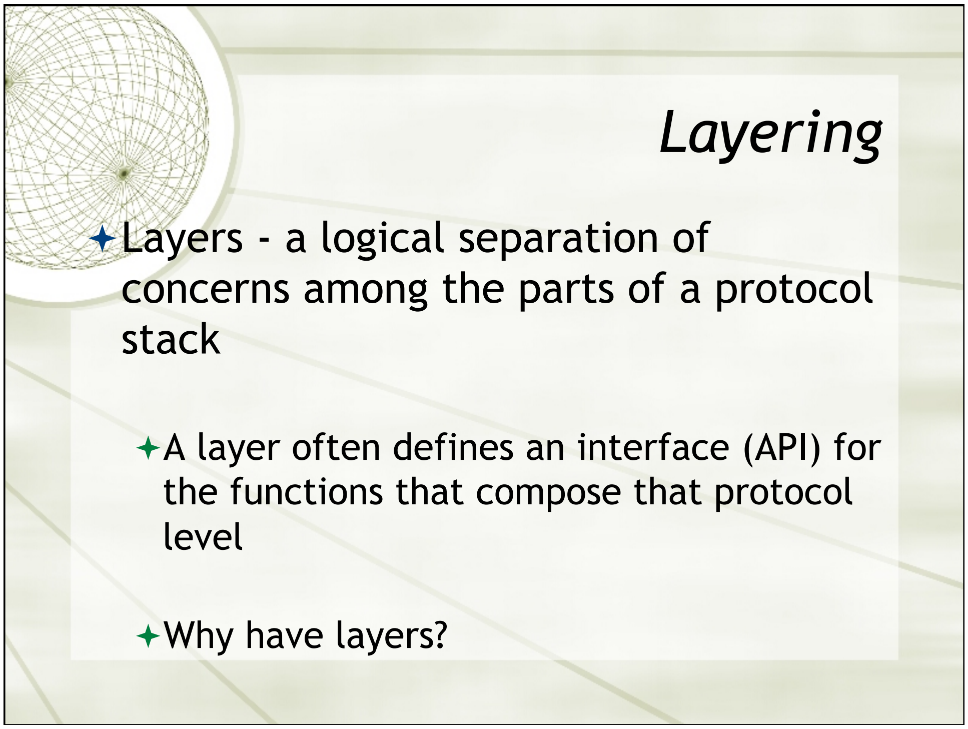


Insert Logo or
Enter Company Name

5555 Street Address
City, State 55555

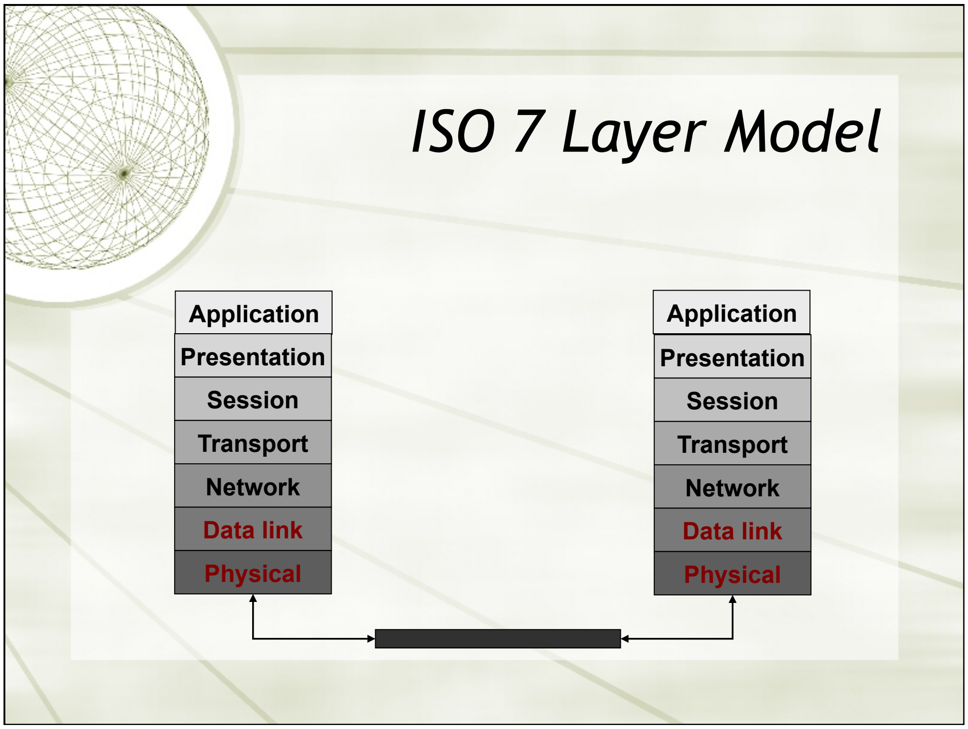
Company Name
Recipient’s Name
5555 Street Address
City, State 5555

What protocols are in use here? What’s missing or wrong in the two examples?



Layering

- Layers - a logical separation of concerns among the parts of a protocol stack
  - A layer often defines an interface (API) for the functions that compose that protocol level
  - Why have layers?



ISO 7 Layer Model

Application

Presentation

Session

Transport

Network

Data link

Physical

Application

Presentation

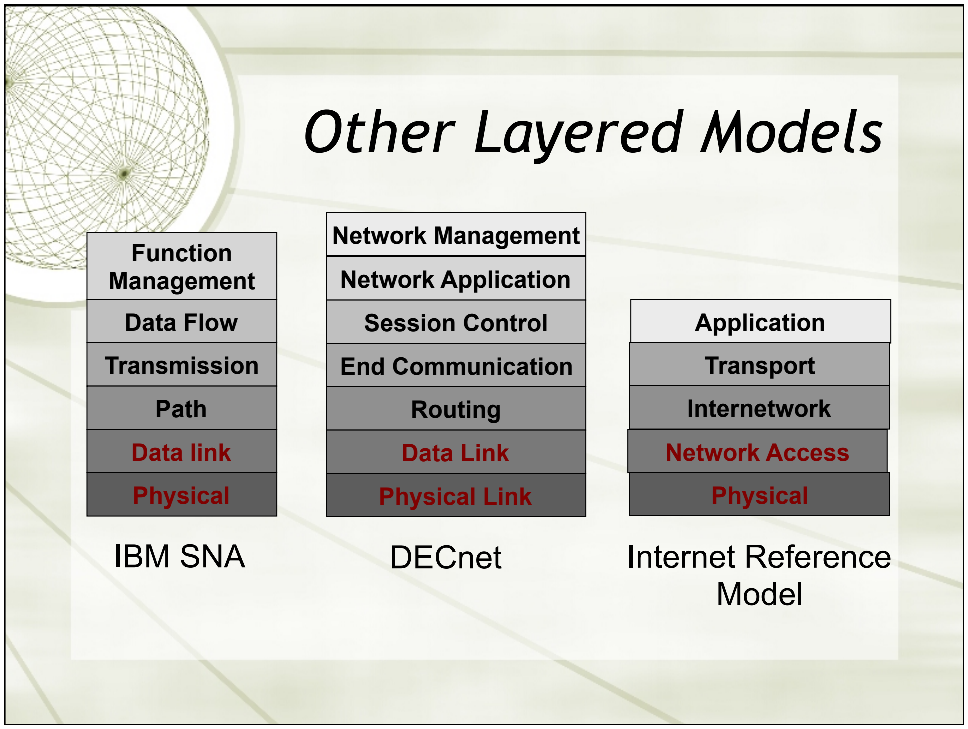
Session

Transport

Network

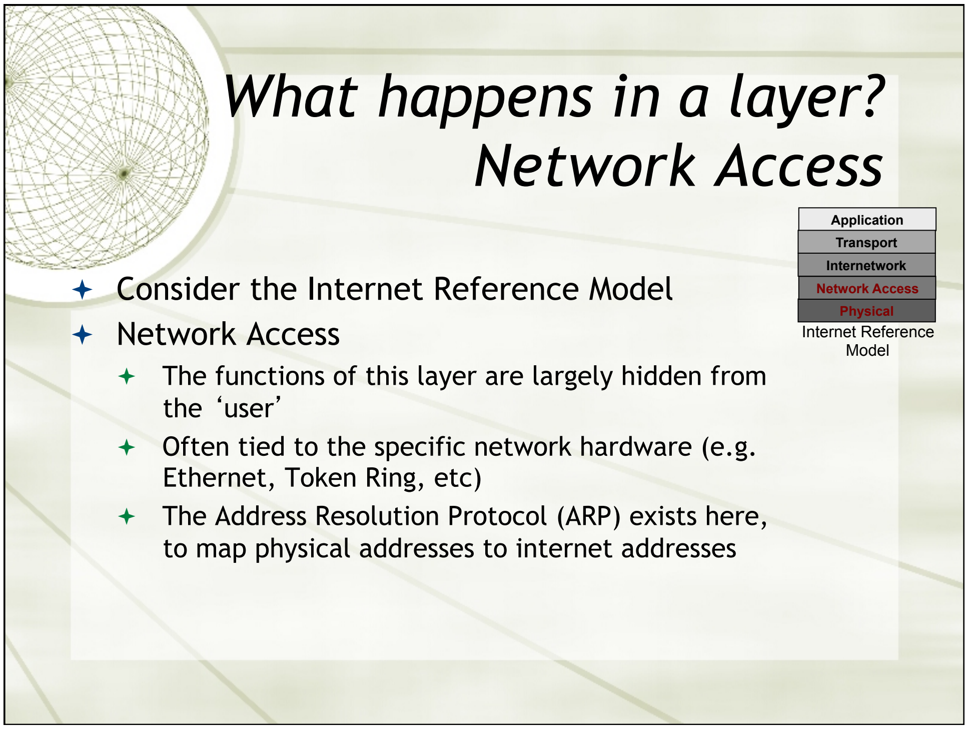
Data link

Physical



Other Layered Models

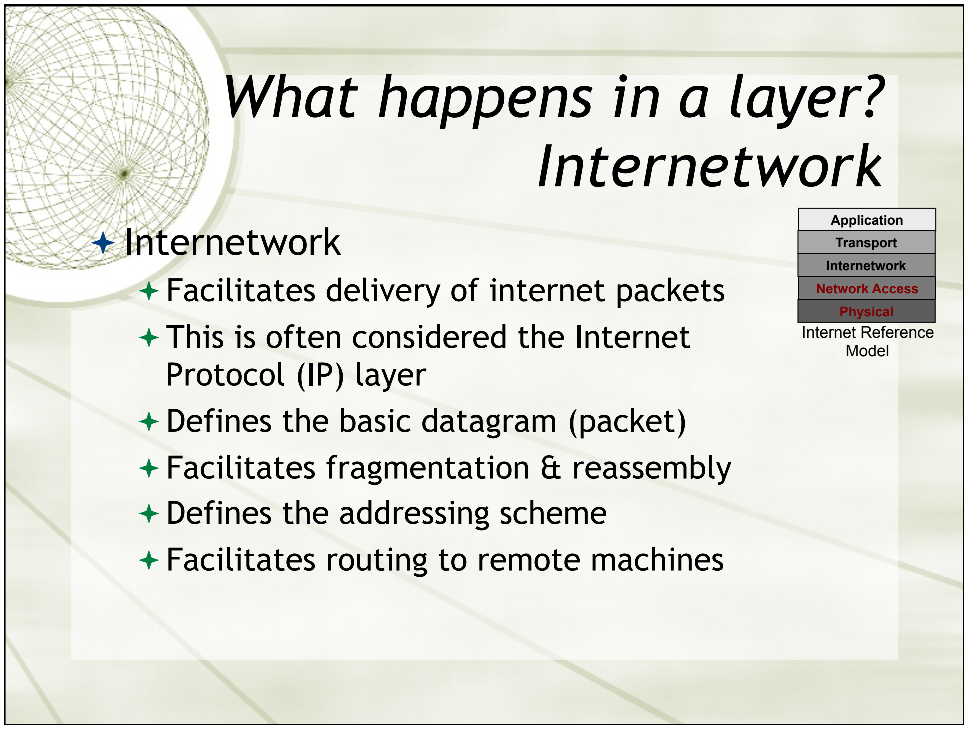
IBM SNA	DECnet	Internet Reference Model
	Network Management	
Function Management	Network Application	
Data Flow	Session Control	Application
Transmission	End Communication	Transport
Path	Routing	Internetwork
Data link	Data Link	Network Access
Physical	Physical Link	Physical



What happens in a layer? Network Access

- Consider the Internet Reference Model
- Network Access
  - The functions of this layer are largely hidden from the ‘user’
  - Often tied to the specific network hardware (e.g. Ethernet, Token Ring, etc)
  - The Address Resolution Protocol (ARP) exists here, to map physical addresses to internet addresses

Internet Reference Model
Application
Transport
Internetwork
Network Access
Physical

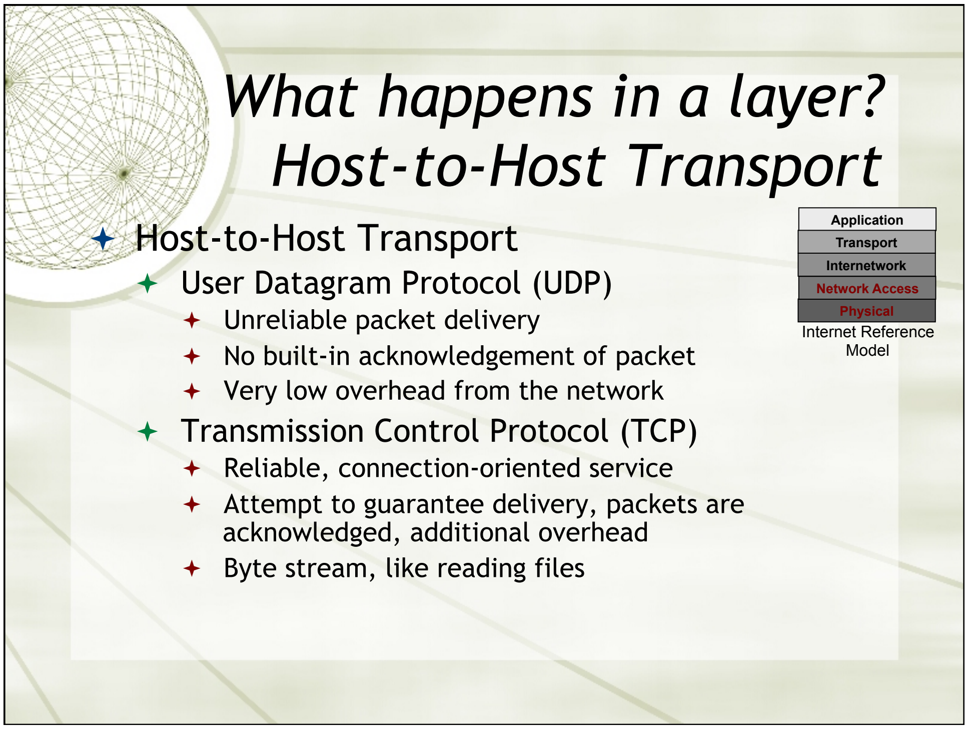


What happens in a layer? Internetwork

- Internetwork
  - Facilitates delivery of internet packets
  - This is often considered the Internet Protocol (IP) layer
  - Defines the basic datagram (packet)
  - Facilitates fragmentation & reassembly
  - Defines the addressing scheme
  - Facilitates routing to remote machines

Application
Transport
Internetwork
Network Access
Physical

Internet Reference Model

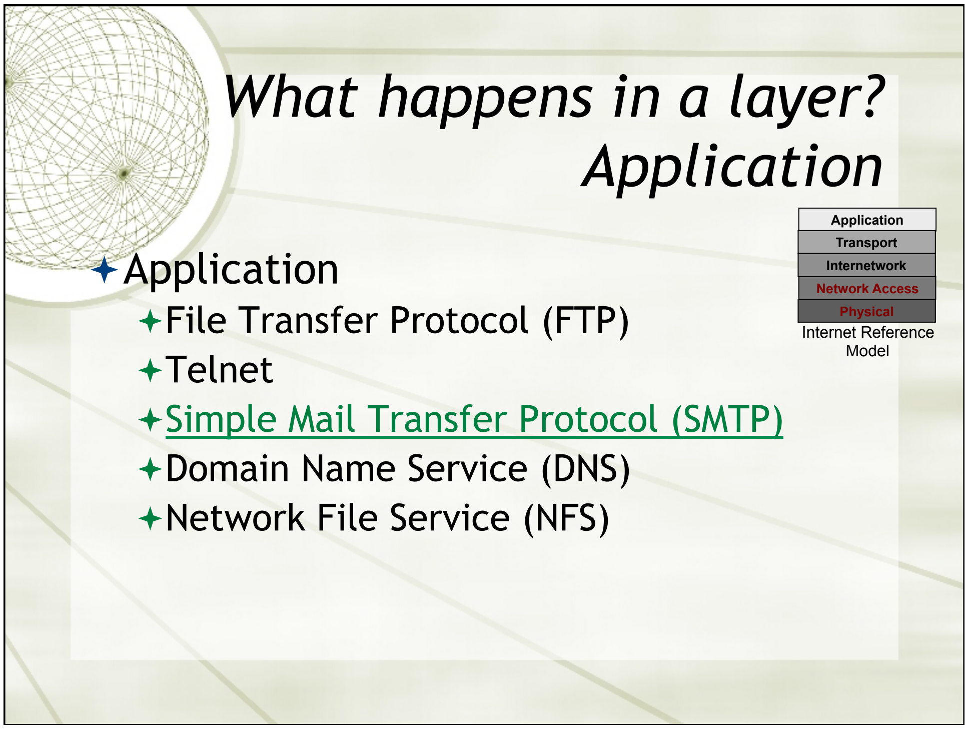


What happens in a layer? Host-to-Host Transport

- Host-to-Host Transport
  - User Datagram Protocol (UDP)
    - Unreliable packet delivery
    - No built-in acknowledgement of packet
    - Very low overhead from the network
  - Transmission Control Protocol (TCP)
    - Reliable, connection-oriented service
    - Attempt to guarantee delivery, packets are acknowledged, additional overhead
    - Byte stream, like reading files

Application
Transport
Internetwork
Network Access
Physical

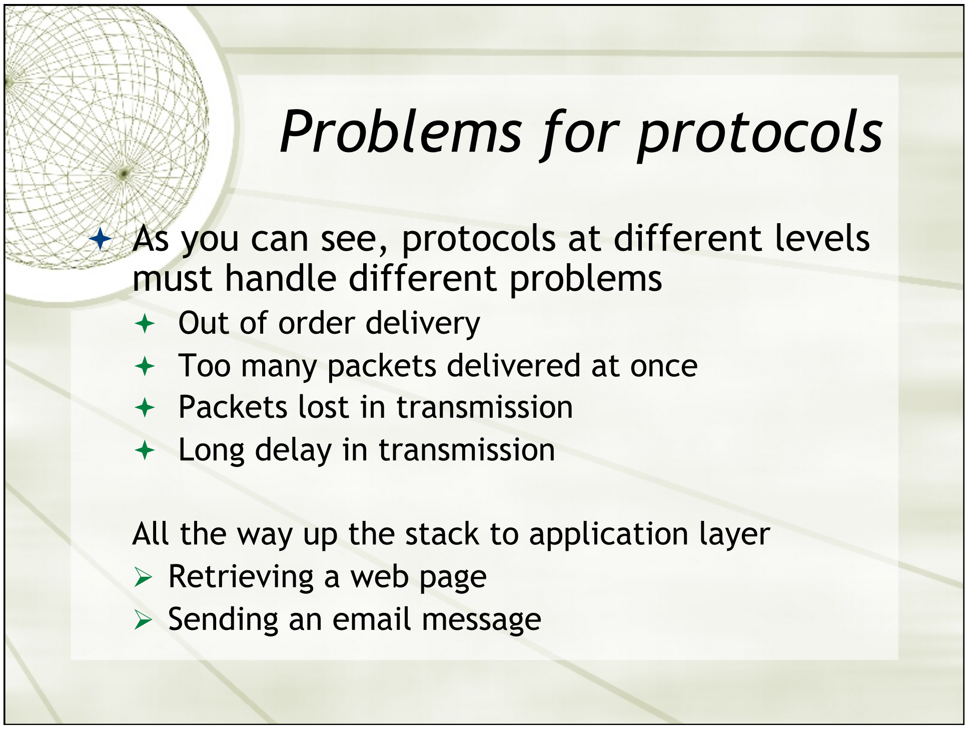
Internet Reference Model



What happens in a layer? Application

Application
Transport
Internetwork
Network Access
Physical
Internet Reference Model

- Application
  - File Transfer Protocol (FTP)
  - Telnet
  - Simple Mail Transfer Protocol (SMTP)
  - Domain Name Service (DNS)
  - Network File Service (NFS)



Problems for protocols

- As you can see, protocols at different levels must handle different problems
  - Out of order delivery
  - Too many packets delivered at once
  - Packets lost in transmission
  - Long delay in transmission

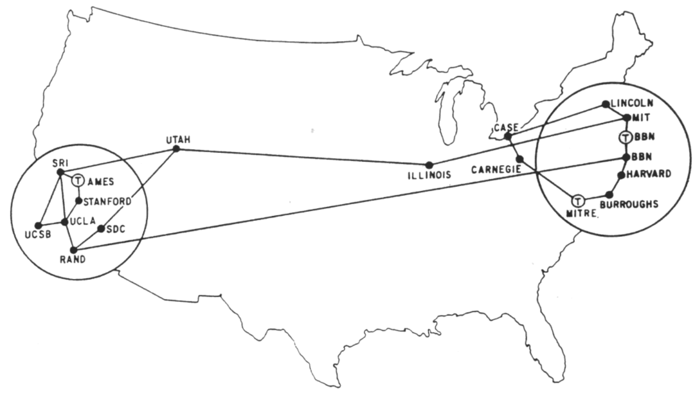
All the way up the stack to application layer

- Retrieving a web page
- Sending an email message

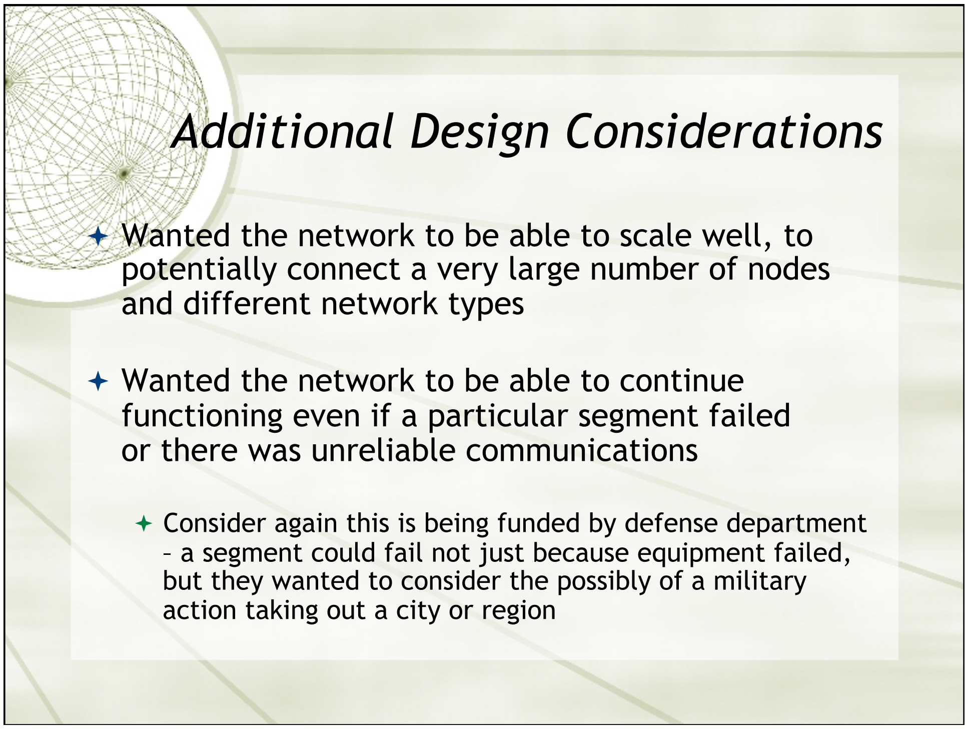
Internetworking

- Basic idea is a network of networks
  - An internetwork – internet
    - Note there is a difference between internet and Internet, why the distinction?
  - Different networks for different uses
  - Hide differences among networks
  - Combination of hardware and software
    - Software implements a virtual network
      - Addressing, protocols, etc
  - Most common Internetworking standard today TCP/IP

The Original ARPANet

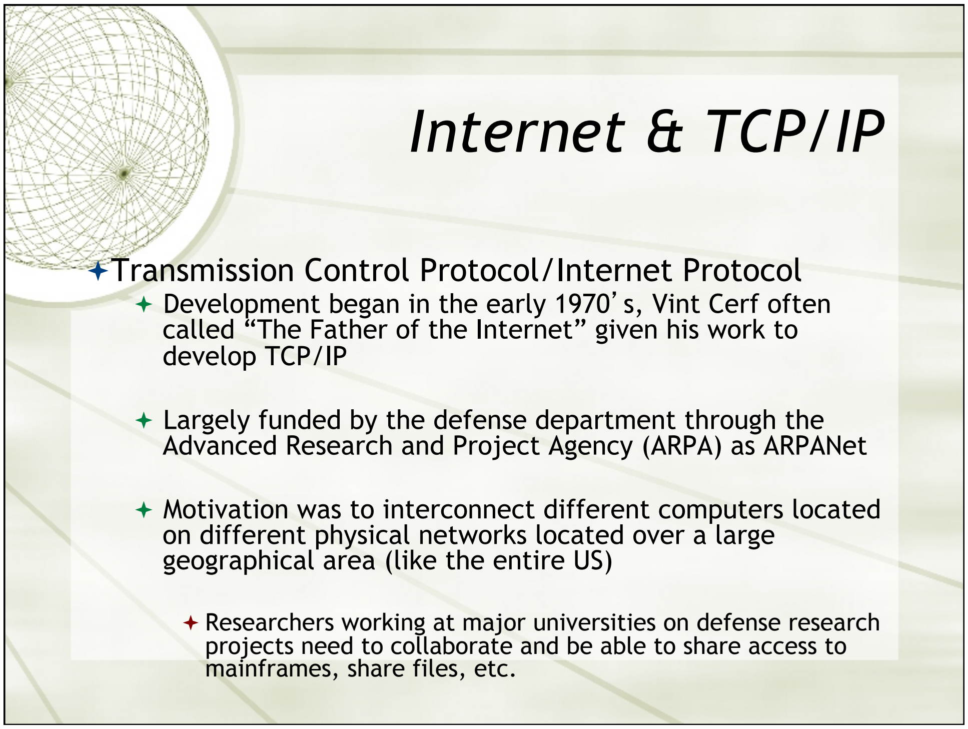


MAP 4 September 1971



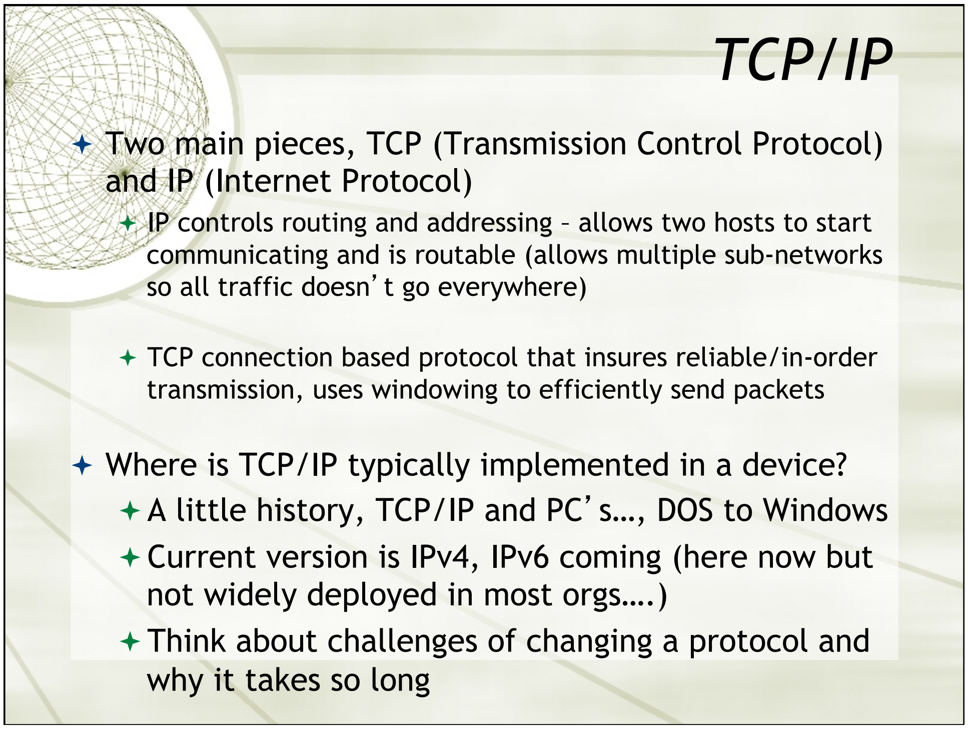
Additional Design Considerations

- Wanted the network to be able to scale well, to potentially connect a very large number of nodes and different network types
- Wanted the network to be able to continue functioning even if a particular segment failed or there was unreliable communications
  - Consider again this is being funded by defense department – a segment could fail not just because equipment failed, but they wanted to consider the possibly of a military action taking out a city or region



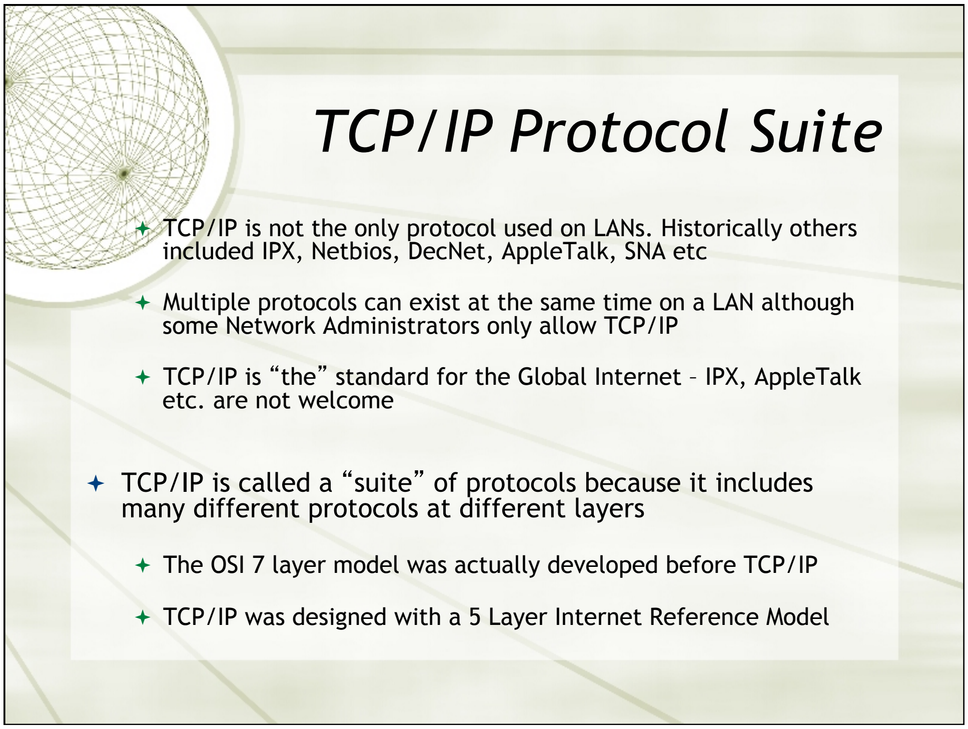
Internet & TCP/IP

- Transmission Control Protocol/Internet Protocol
  - Development began in the early 1970's, Vint Cerf often called "The Father of the Internet" given his work to develop TCP/IP
  - Largely funded by the defense department through the Advanced Research and Project Agency (ARPA) as ARPANet
  - Motivation was to interconnect different computers located on different physical networks located over a large geographical area (like the entire US)
    - Researchers working at major universities on defense research projects need to collaborate and be able to share access to mainframes, share files, etc.



TCP/IP

- Two main pieces, TCP (Transmission Control Protocol) and IP (Internet Protocol)
  - IP controls routing and addressing – allows two hosts to start communicating and is routable (allows multiple sub-networks so all traffic doesn’t go everywhere)
  - TCP connection based protocol that insures reliable/in-order transmission, uses windowing to efficiently send packets
- Where is TCP/IP typically implemented in a device?
  - A little history, TCP/IP and PC’s…, DOS to Windows
  - Current version is IPv4, IPv6 coming (here now but not widely deployed in most orgs….)
  - Think about challenges of changing a protocol and why it takes so long

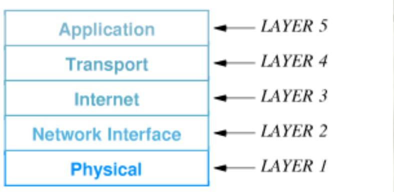


TCP/IP Protocol Suite

  - TCP/IP is not the only protocol used on LANs. Historically others included IPX, Netbios, DecNet, AppleTalk, SNA etc
  - Multiple protocols can exist at the same time on a LAN although some Network Administrators only allow TCP/IP
  - TCP/IP is “the” standard for the Global Internet – IPX, AppleTalk etc. are not welcome
- TCP/IP is called a “suite” of protocols because it includes many different protocols at different layers
  - The OSI 7 layer model was actually developed before TCP/IP
  - TCP/IP was designed with a 5 Layer Internet Reference Model

TCP/IP Layering Model

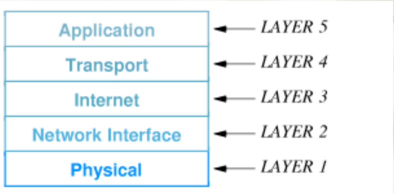
- Physical – basic network hardware
- Network Interface – how to organize data into frames and how frames are transmitted
- Internet – the format of packets sent across an Internet and how packets are forwarded through routers
- Transport – Insure reliable delivery (TCP)
- Application – There may be many application level protocols, each defines how that application uses the network
    - Telnet, FTP, HTTP, SMTP, are all application level protocols



Application ← LAYER 5
Transport ← LAYER 4
Internet ← LAYER 3
Network Interface ← LAYER 2
Physical ← LAYER 1

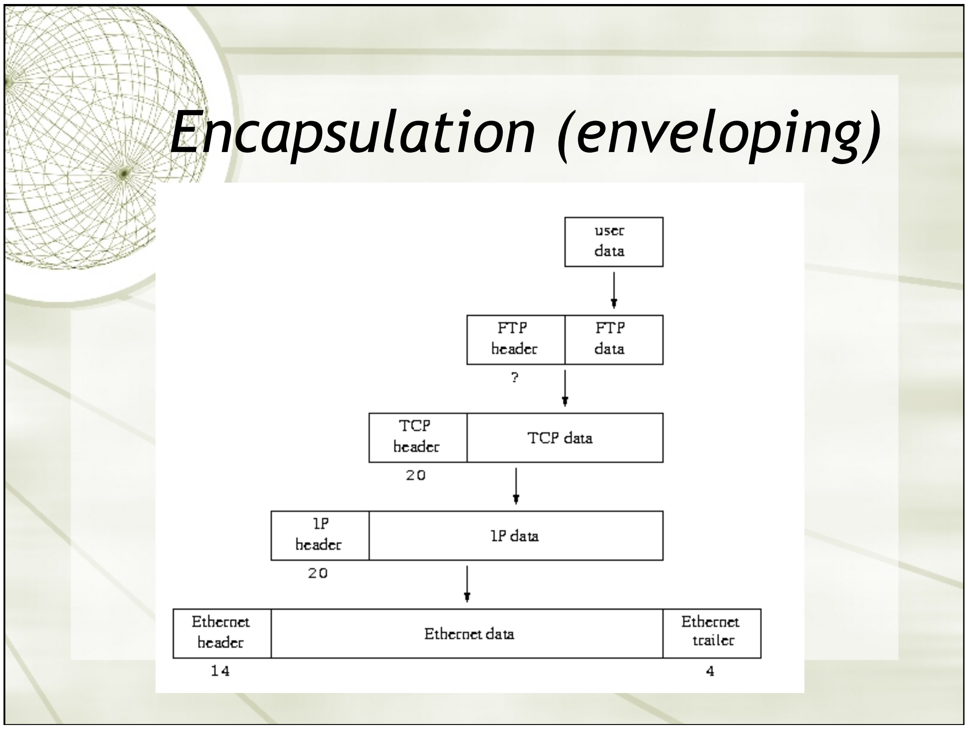
Refresher: Ethernet hardware and layers

- Repeaters, simple hubs
    - Layer 1 devices
- Bridges, Switches
    - Layer 2 devices
- Routers, “Layer 3” Switches
    - Layer 3 devices

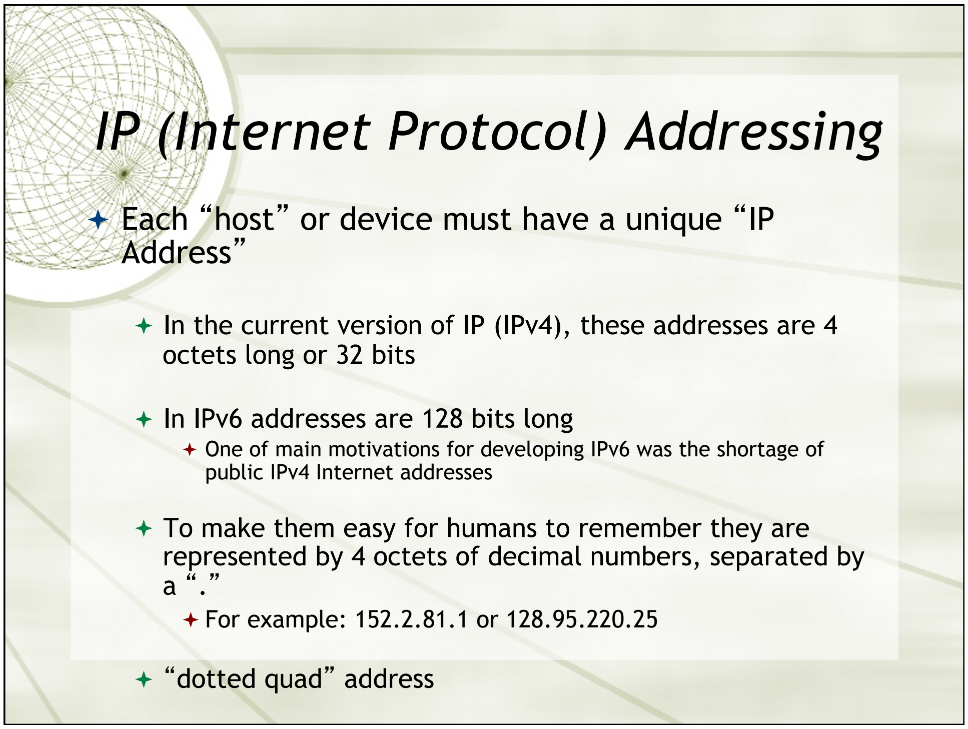


Application ← LAYER 5
Transport ← LAYER 4
Internet ← LAYER 3
Network Interface ← LAYER 2
Physical ← LAYER 1

Refresher: What’s the difference between an ethernet hub and a switch?

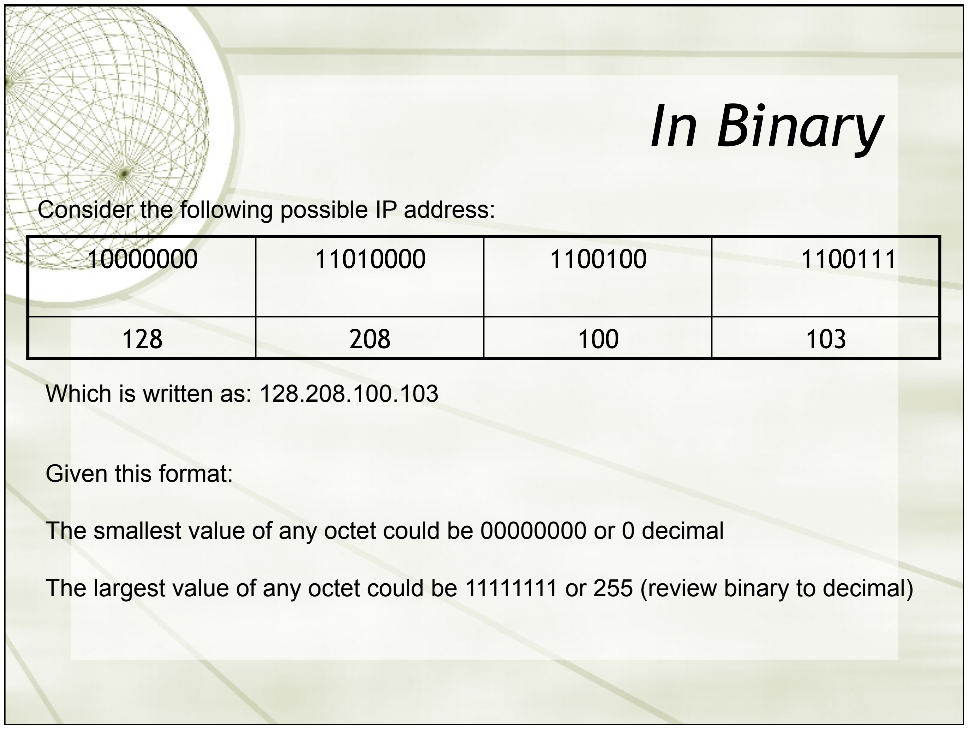


Encapsulation (enveloping)



IP (Internet Protocol) Addressing

- Each “host” or device must have a unique “IP Address”
  - In the current version of IP (IPv4), these addresses are 4 octets long or 32 bits
  - In IPv6 addresses are 128 bits long
    - One of main motivations for developing IPv6 was the shortage of public IPv4 Internet addresses
  - To make them easy for humans to remember they are represented by 4 octets of decimal numbers, separated by a “.”
    - For example: 152.2.81.1 or 128.95.220.25
  - “dotted quad” address



In Binary

Consider the following possible IP address:

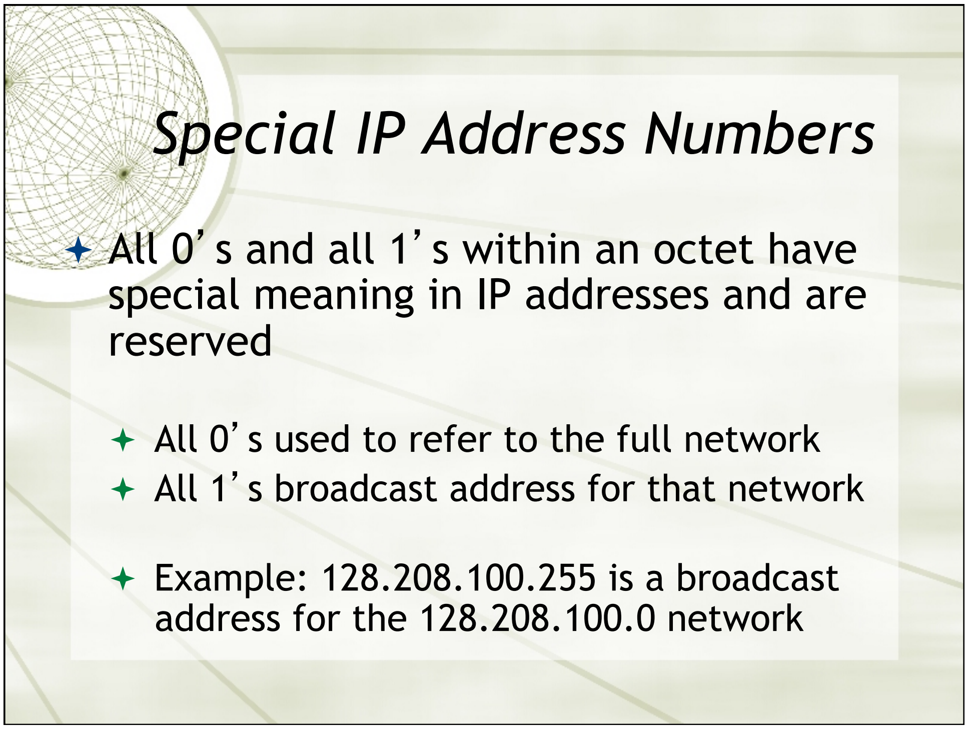
10000000	11010000	1100100	1100111
128	208	100	103

Which is written as: 128.208.100.103

Given this format:

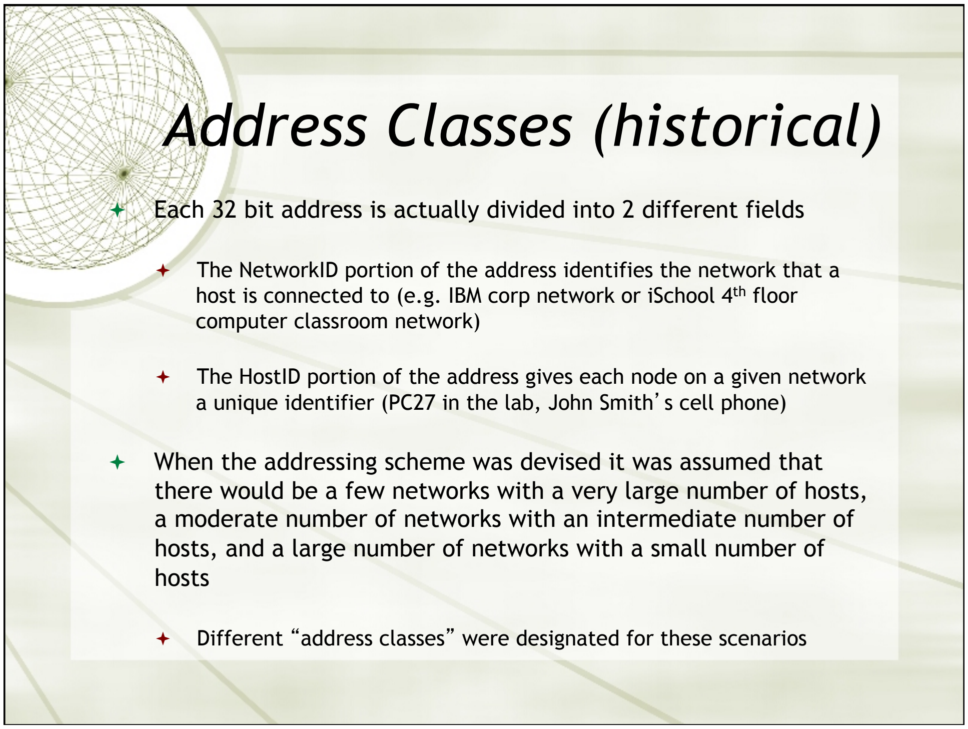
The smallest value of any octet could be 00000000 or 0 decimal

The largest value of any octet could be 11111111 or 255 (review binary to decimal)



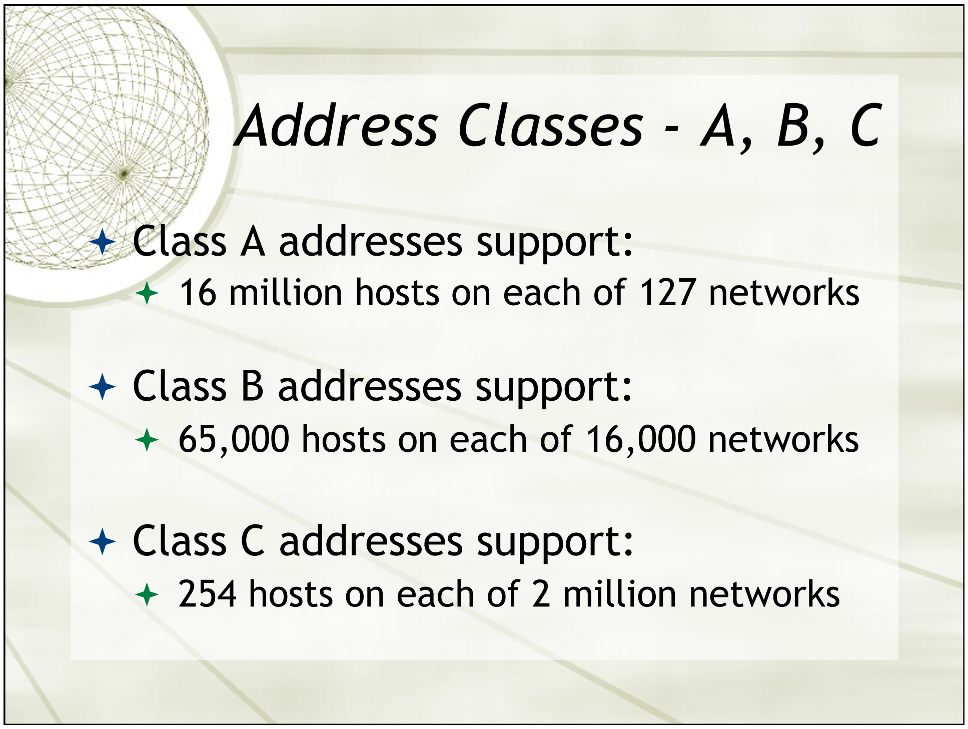
Special IP Address Numbers

- All 0's and all 1's within an octet have special meaning in IP addresses and are reserved
  - All 0's used to refer to the full network
  - All 1's broadcast address for that network
  - Example: 128.208.100.255 is a broadcast address for the 128.208.100.0 network



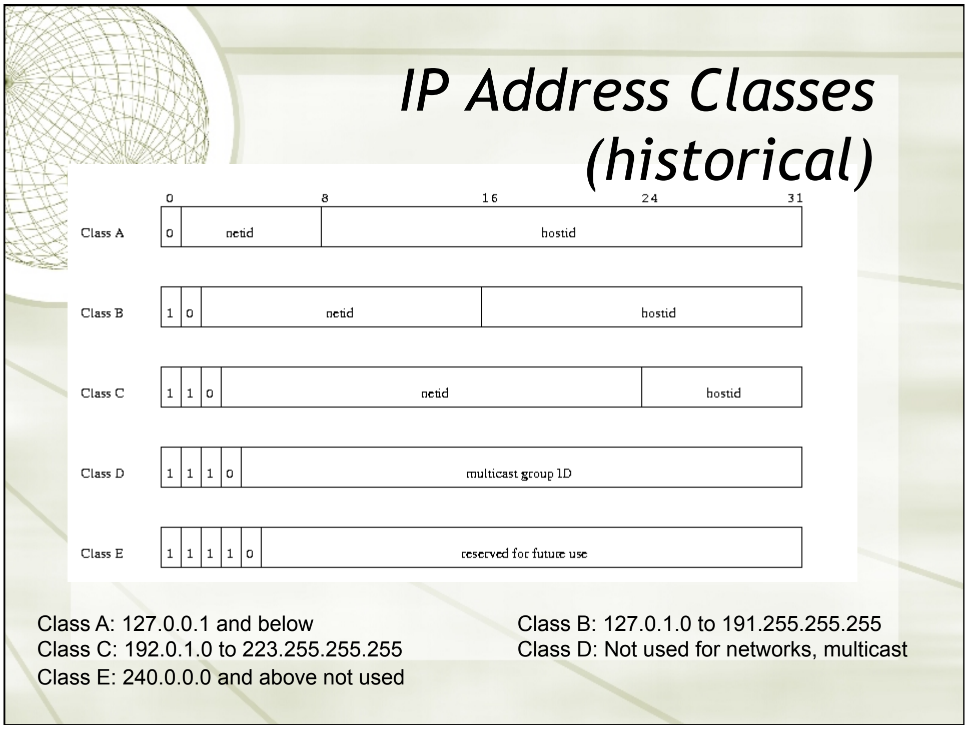
Address Classes (historical)

- Each 32 bit address is actually divided into 2 different fields
  - The NetworkID portion of the address identifies the network that a host is connected to (e.g. IBM corp network or iSchool 4th floor computer classroom network)
  - The HostID portion of the address gives each node on a given network a unique identifier (PC27 in the lab, John Smith's cell phone)
- When the addressing scheme was devised it was assumed that there would be a few networks with a very large number of hosts, a moderate number of networks with an intermediate number of hosts, and a large number of networks with a small number of hosts
  - Different "address classes" were designated for these scenarios



Address Classes - A, B, C

- Class A addresses support:
  - 16 million hosts on each of 127 networks
- Class B addresses support:
  - 65,000 hosts on each of 16,000 networks
- Class C addresses support:
  - 254 hosts on each of 2 million networks



IP Address Classes (historical)

0 8 16 24 31

Class A	0	netid	hostid			
Class B	1	0	netid	hostid		
Class C	1	1	0	netid	hostid	
Class D	1	1	1	0	multicast group ID	
Class E	1	1	1	1	0	reserved for future use

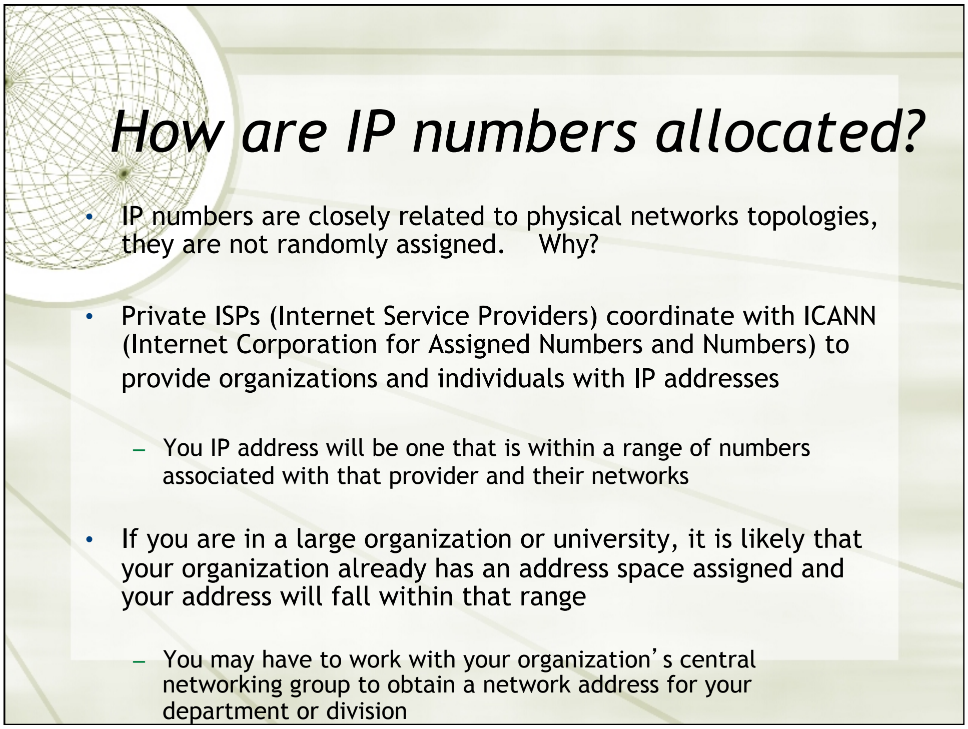
Class A: 127.0.0.1 and below

Class B: 127.0.1.0 to 191.255.255.255

Class C: 192.0.1.0 to 223.255.255.255

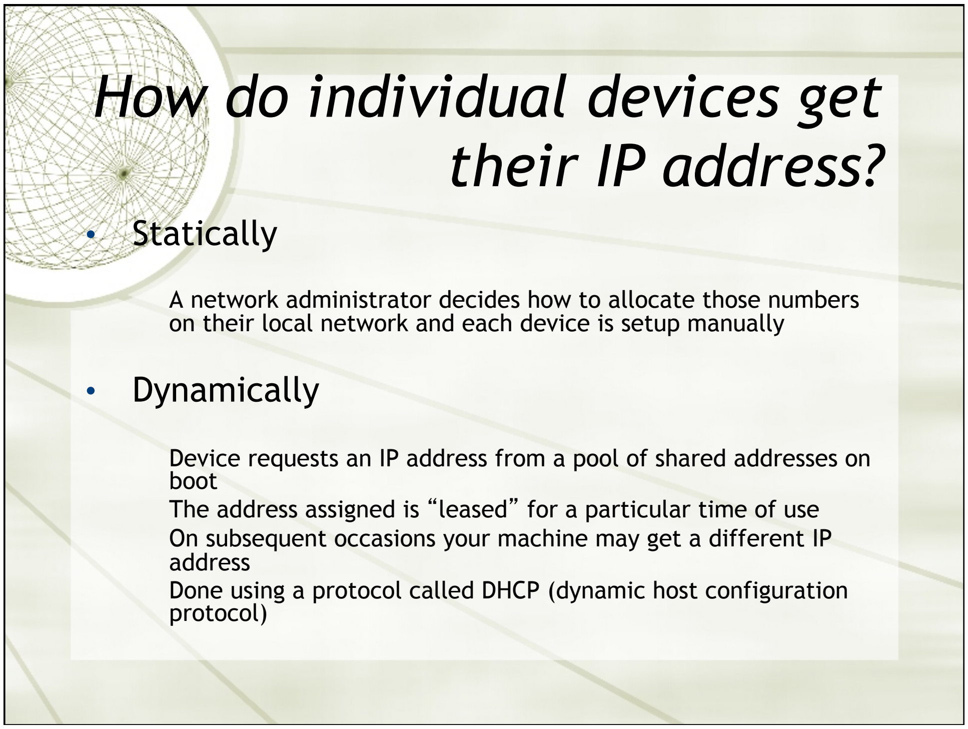
Class D: Not used for networks, multicast

Class E: 240.0.0.0 and above not used



How are IP numbers allocated?

- IP numbers are closely related to physical networks topologies, they are not randomly assigned. Why?
- Private ISPs (Internet Service Providers) coordinate with ICANN (Internet Corporation for Assigned Numbers and Numbers) to provide organizations and individuals with IP addresses
  - You IP address will be one that is within a range of numbers associated with that provider and their networks
- If you are in a large organization or university, it is likely that your organization already has an address space assigned and your address will fall within that range
  - You may have to work with your organization's central networking group to obtain a network address for your department or division



How do individual devices get their IP address?

- Statically

  A network administrator decides how to allocate those numbers on their local network and each device is setup manually

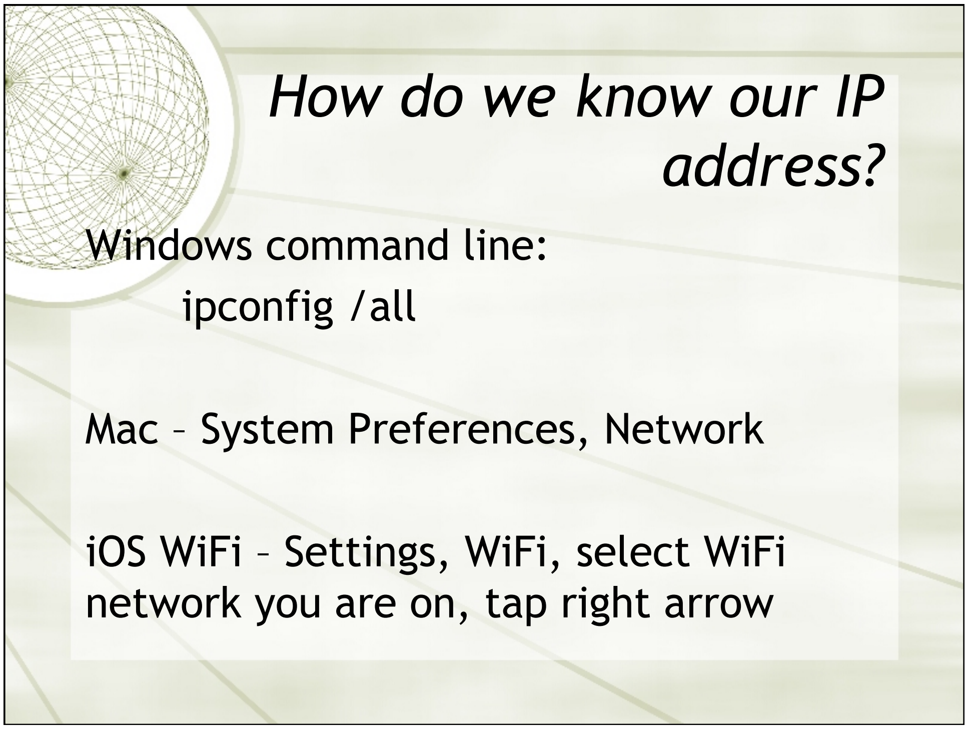
- Dynamically

  Device requests an IP address from a pool of shared addresses on boot

  The address assigned is "leased" for a particular time of use

  On subsequent occasions your machine may get a different IP address

  Done using a protocol called DHCP (dynamic host configuration protocol)



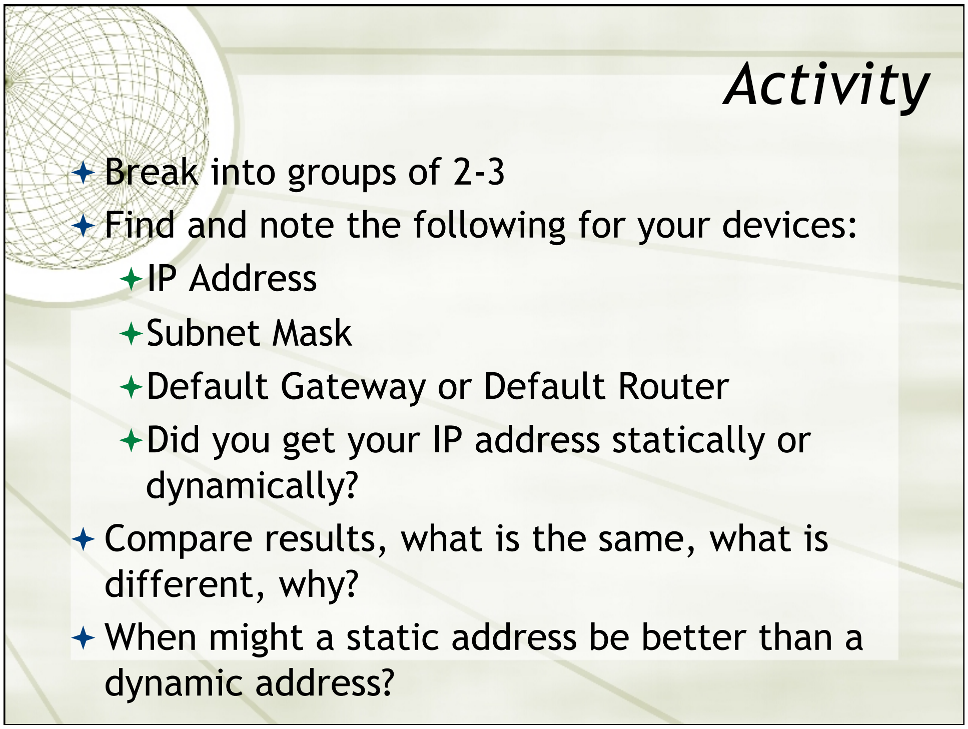
How do we know our IP address?

Windows command line:

```
ipconfig /all
```

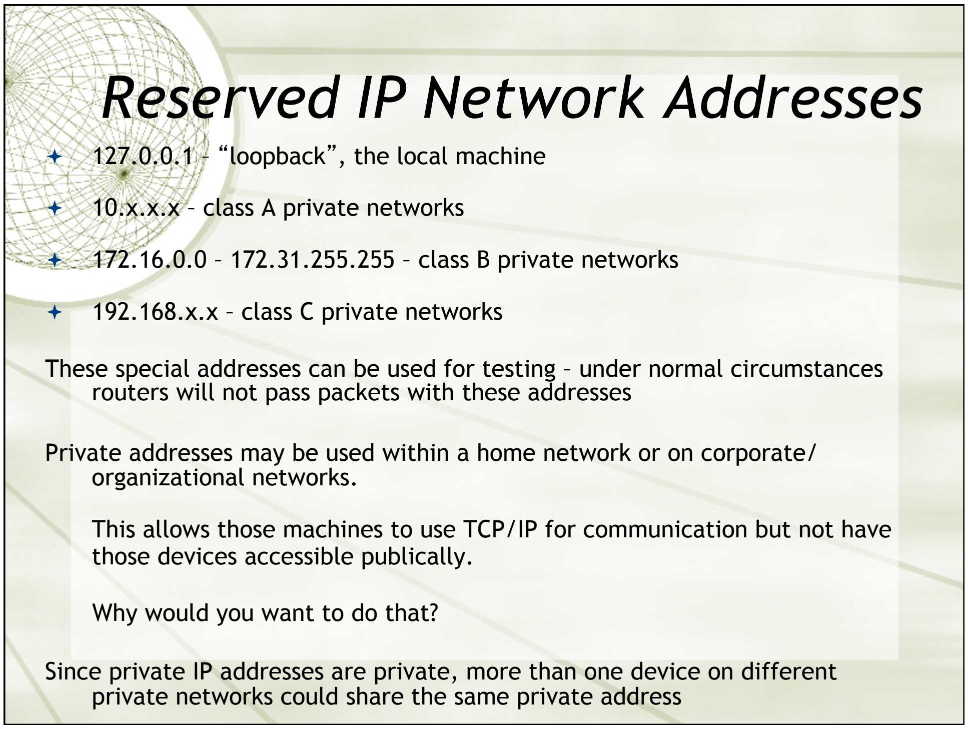
Mac – System Preferences, Network

iOS WiFi – Settings, WiFi, select WiFi network you are on, tap right arrow



Activity

- Break into groups of 2-3
- Find and note the following for your devices:
  - IP Address
  - Subnet Mask
  - Default Gateway or Default Router
  - Did you get your IP address statically or dynamically?
- Compare results, what is the same, what is different, why?
- When might a static address be better than a dynamic address?



Reserved IP Network Addresses

- 127.0.0.1 – "loopback", the local machine
- 10.x.x.x – class A private networks
- 172.16.0.0 – 172.31.255.255 – class B private networks
- 192.168.x.x – class C private networks

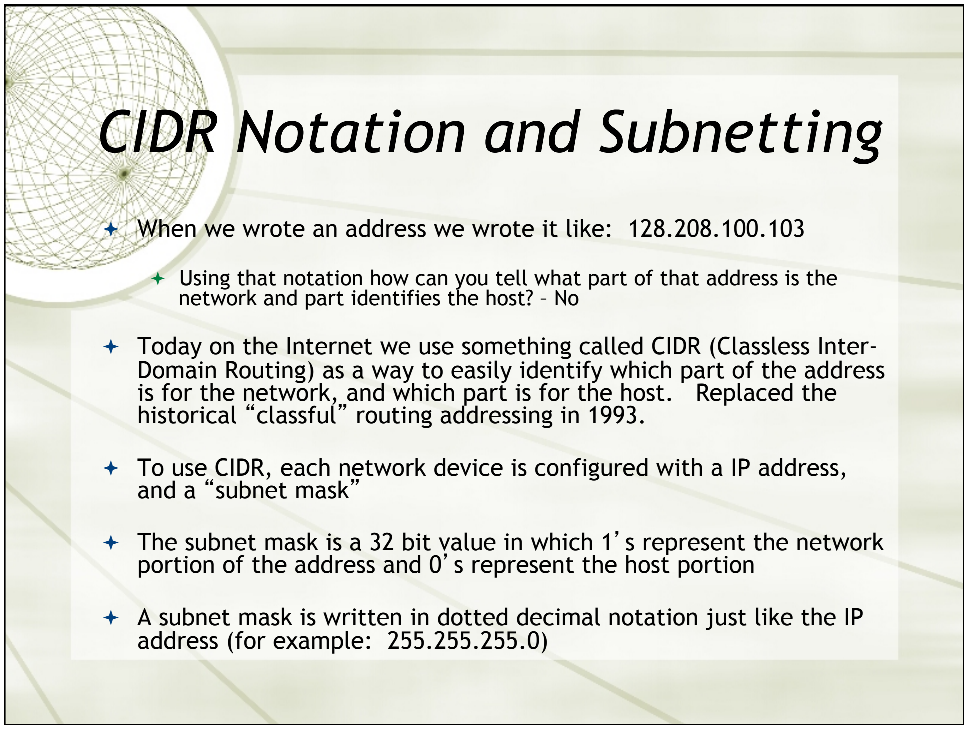
These special addresses can be used for testing – under normal circumstances routers will not pass packets with these addresses

Private addresses may be used within a home network or on corporate/ organizational networks.

This allows those machines to use TCP/IP for communication but not have those devices accessible publically.

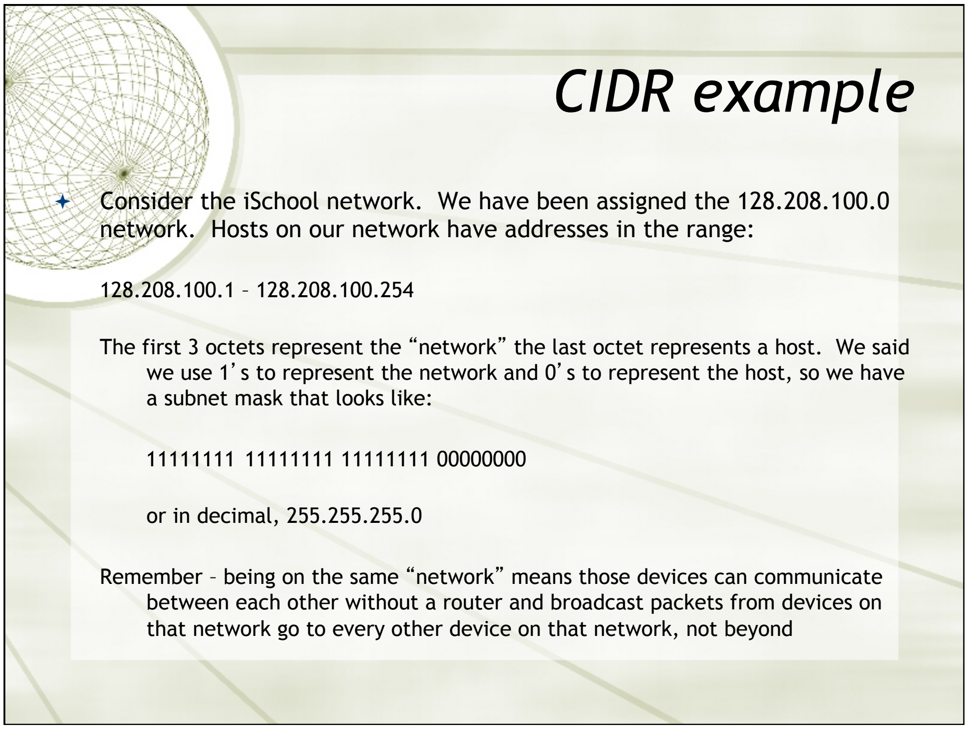
Why would you want to do that?

Since private IP addresses are private, more than one device on different private networks could share the same private address



CIDR Notation and Subnetting

- When we wrote an address we wrote it like: 128.208.100.103
  - Using that notation how can you tell what part of that address is the network and part identifies the host? – No
- Today on the Internet we use something called CIDR (Classless Inter-Domain Routing) as a way to easily identify which part of the address is for the network, and which part is for the host. Replaced the historical "classful" routing addressing in 1993.
- To use CIDR, each network device is configured with a IP address, and a "subnet mask"
- The subnet mask is a 32 bit value in which 1's represent the network portion of the address and 0's represent the host portion
- A subnet mask is written in dotted decimal notation just like the IP address (for example: 255.255.255.0)



CIDR example

- Consider the iSchool network. We have been assigned the 128.208.100.0 network. Hosts on our network have addresses in the range:

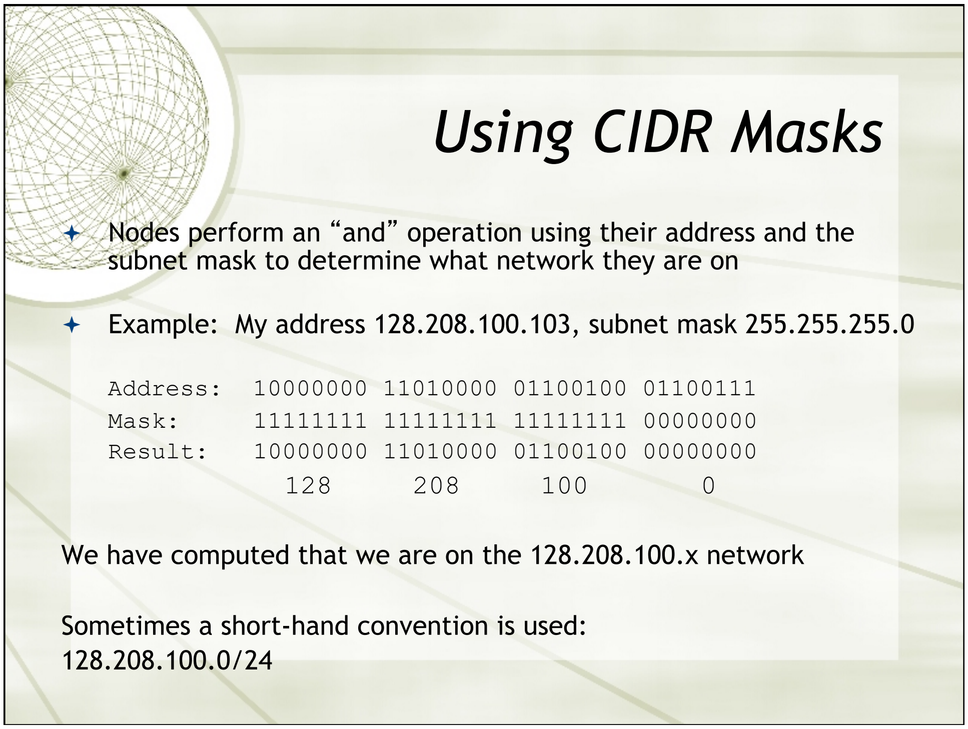
128.208.100.1 – 128.208.100.254

The first 3 octets represent the "network" the last octet represents a host. We said we use 1's to represent the network and 0's to represent the host, so we have a subnet mask that looks like:

11111111 11111111 11111111 00000000

or in decimal, 255.255.255.0

Remember – being on the same "network" means those devices can communicate between each other without a router and broadcast packets from devices on that network go to every other device on that network, not beyond



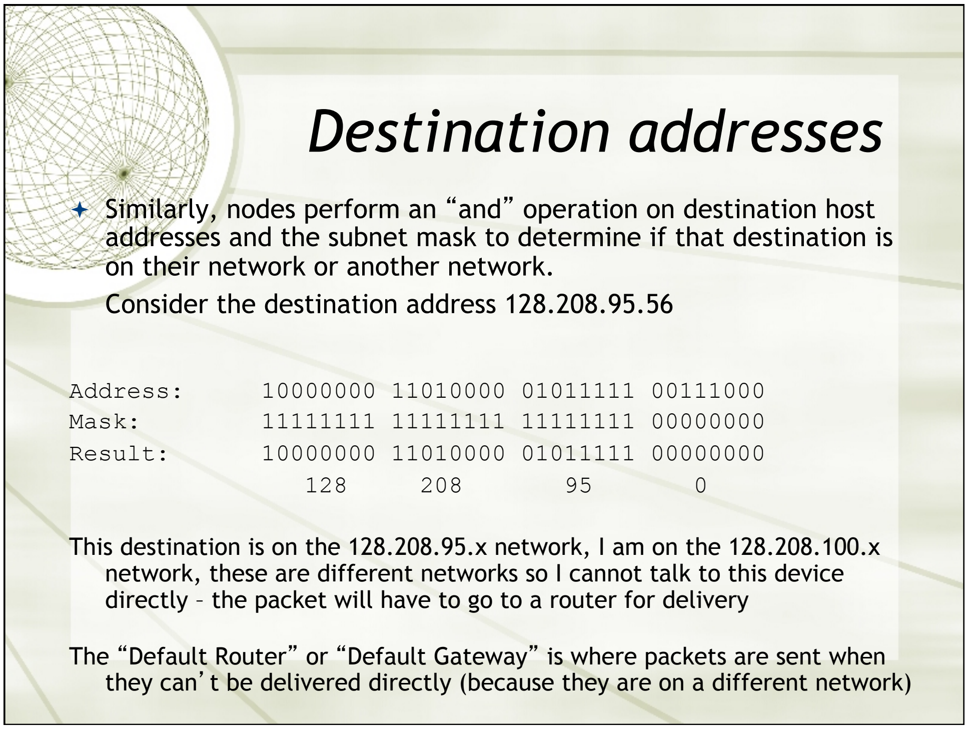
Using CIDR Masks

- Nodes perform an “and” operation using their address and the subnet mask to determine what network they are on
- Example: My address 128.208.100.103, subnet mask 255.255.255.0

```
Address:  10000000 11010000 01100100 01100111
Mask:     11111111 11111111 11111111 00000000
Result:   10000000 11010000 01100100 00000000
            128      208      100        0
```

We have computed that we are on the 128.208.100.x network

Sometimes a short-hand convention is used:
128.208.100.0/24



Destination addresses

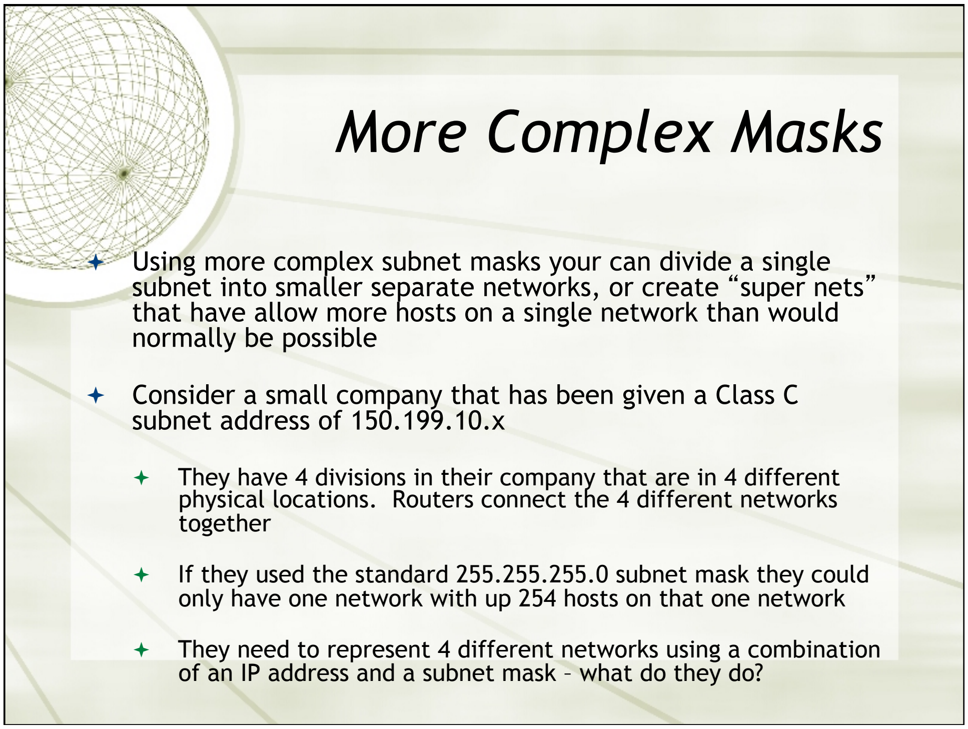
- Similarly, nodes perform an “and” operation on destination host addresses and the subnet mask to determine if that destination is on their network or another network.

  Consider the destination address 128.208.95.56

```
Address:      10000000 11010000 01011111 00111000
Mask:         11111111 11111111 11111111 00000000
Result:       10000000 11010000 01011111 00000000
                 128      208       95       0
```

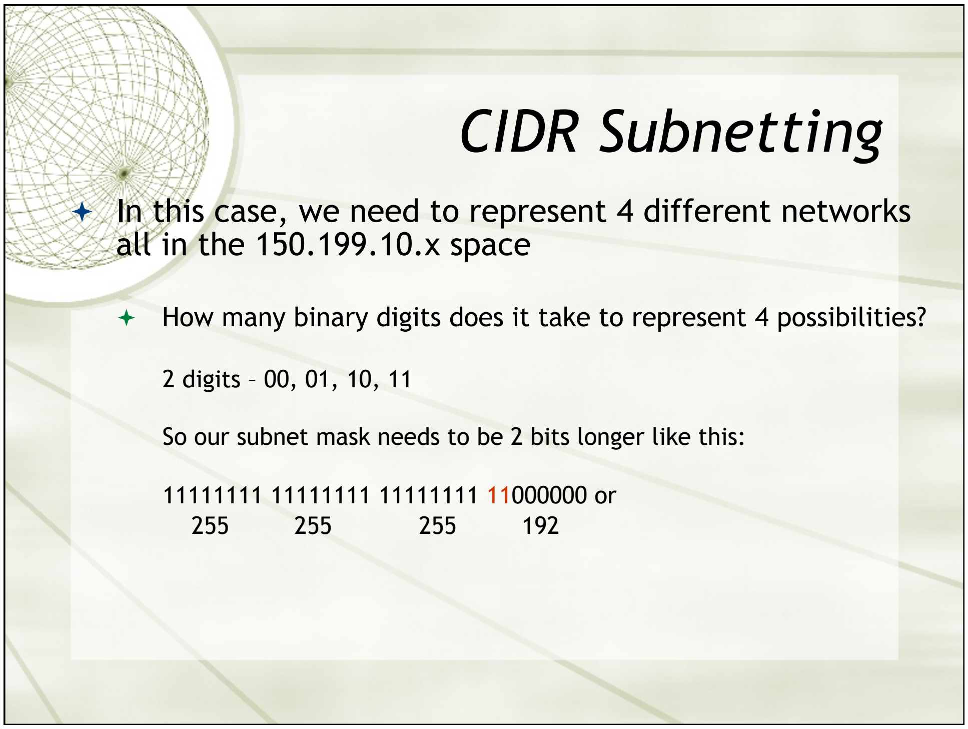
This destination is on the 128.208.95.x network, I am on the 128.208.100.x network, these are different networks so I cannot talk to this device directly – the packet will have to go to a router for delivery

The “Default Router” or “Default Gateway” is where packets are sent when they can’t be delivered directly (because they are on a different network)



More Complex Masks

- Using more complex subnet masks your can divide a single subnet into smaller separate networks, or create “super nets” that have allow more hosts on a single network than would normally be possible
- Consider a small company that has been given a Class C subnet address of 150.199.10.x
  - They have 4 divisions in their company that are in 4 different physical locations. Routers connect the 4 different networks together
  - If they used the standard 255.255.255.0 subnet mask they could only have one network with up 254 hosts on that one network
  - They need to represent 4 different networks using a combination of an IP address and a subnet mask – what do they do?



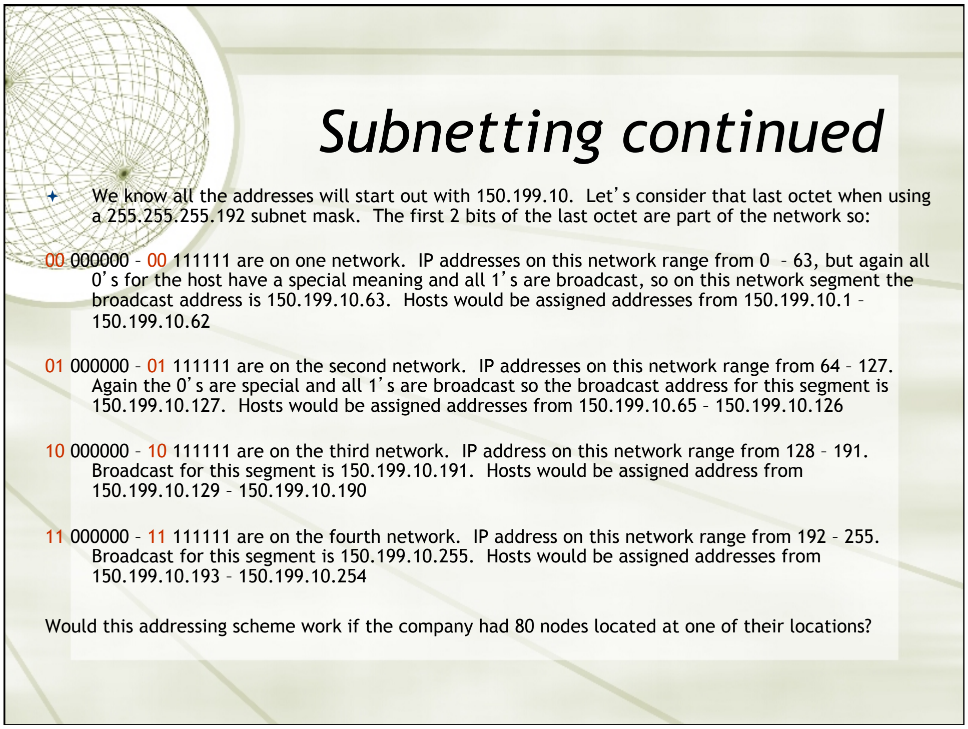
CIDR Subnetting

- In this case, we need to represent 4 different networks all in the 150.199.10.x space
  - How many binary digits does it take to represent 4 possibilities?

    2 digits – 00, 01, 10, 11

    So our subnet mask needs to be 2 bits longer like this:

```
11111111 11111111 11111111 11000000 or
   255      255       255      192
```



Subnetting continued

- We know all the addresses will start out with 150.199.10. Let's consider that last octet when using a 255.255.255.192 subnet mask. The first 2 bits of the last octet are part of the network so:

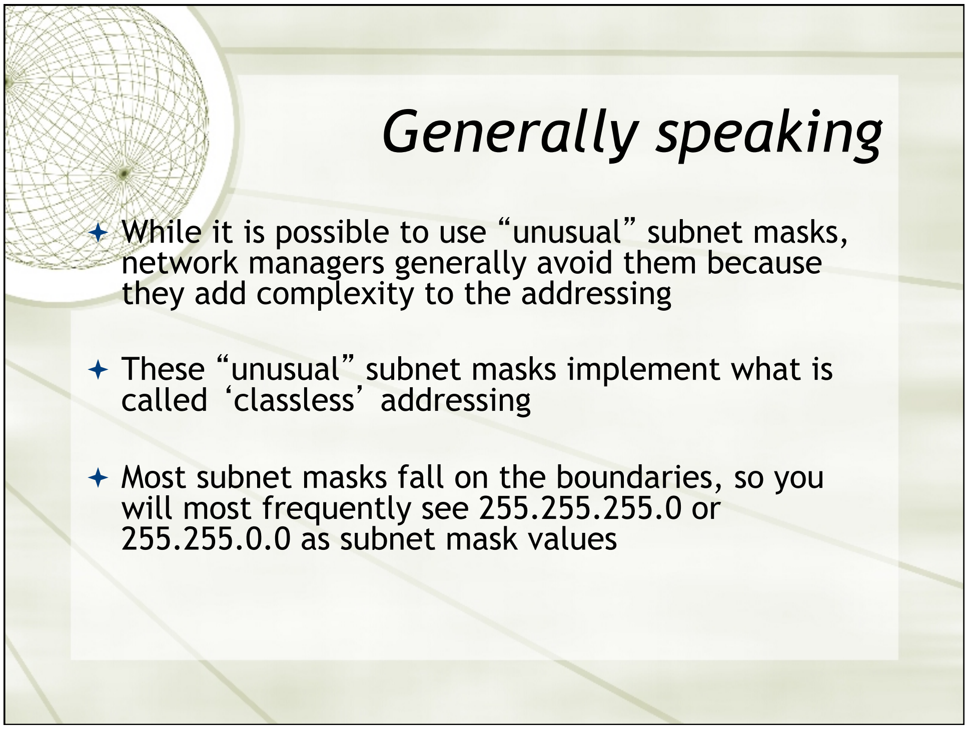
00 000000 – 00 111111 are on one network. IP addresses on this network range from 0 – 63, but again all 0's for the host have a special meaning and all 1's are broadcast, so on this network segment the broadcast address is 150.199.10.63. Hosts would be assigned addresses from 150.199.10.1 – 150.199.10.62

01 000000 – 01 111111 are on the second network. IP addresses on this network range from 64 – 127. Again the 0's are special and all 1's are broadcast so the broadcast address for this segment is 150.199.10.127. Hosts would be assigned addresses from 150.199.10.65 – 150.199.10.126

10 000000 – 10 111111 are on the third network. IP address on this network range from 128 – 191. Broadcast for this segment is 150.199.10.191. Hosts would be assigned address from 150.199.10.129 – 150.199.10.190

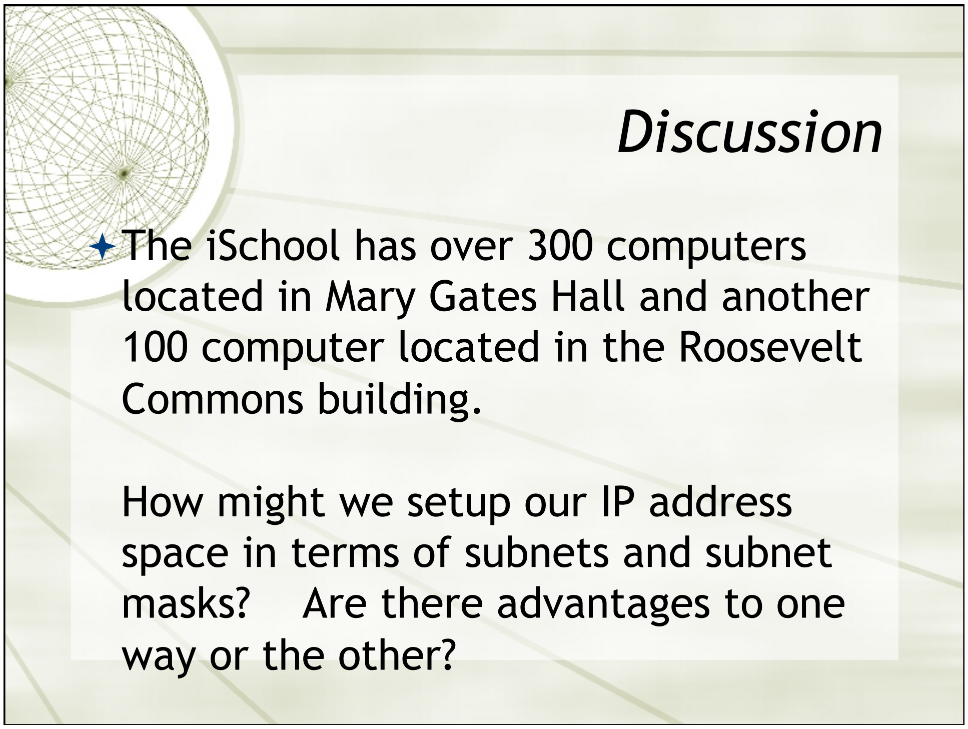
11 000000 – 11 111111 are on the fourth network. IP address on this network range from 192 – 255. Broadcast for this segment is 150.199.10.255. Hosts would be assigned addresses from 150.199.10.193 – 150.199.10.254

Would this addressing scheme work if the company had 80 nodes located at one of their locations?



Generally speaking

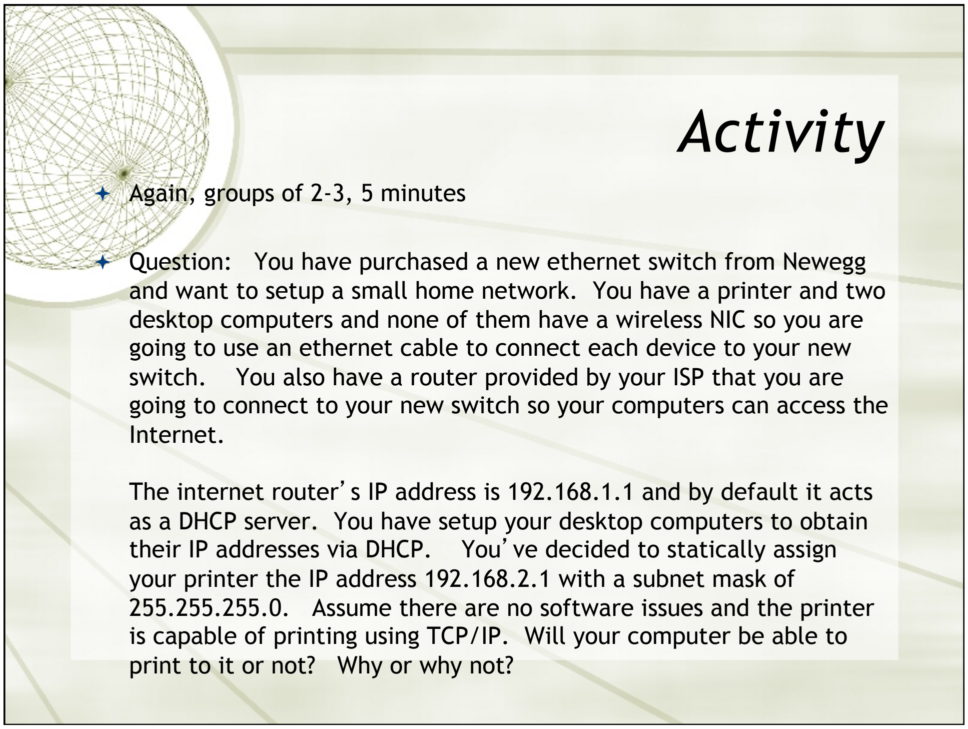
- While it is possible to use "unusual" subnet masks, network managers generally avoid them because they add complexity to the addressing
- These "unusual" subnet masks implement what is called 'classless' addressing
- Most subnet masks fall on the boundaries, so you will most frequently see 255.255.255.0 or 255.255.0.0 as subnet mask values



Discussion

- The iSchool has over 300 computers located in Mary Gates Hall and another 100 computer located in the Roosevelt Commons building.

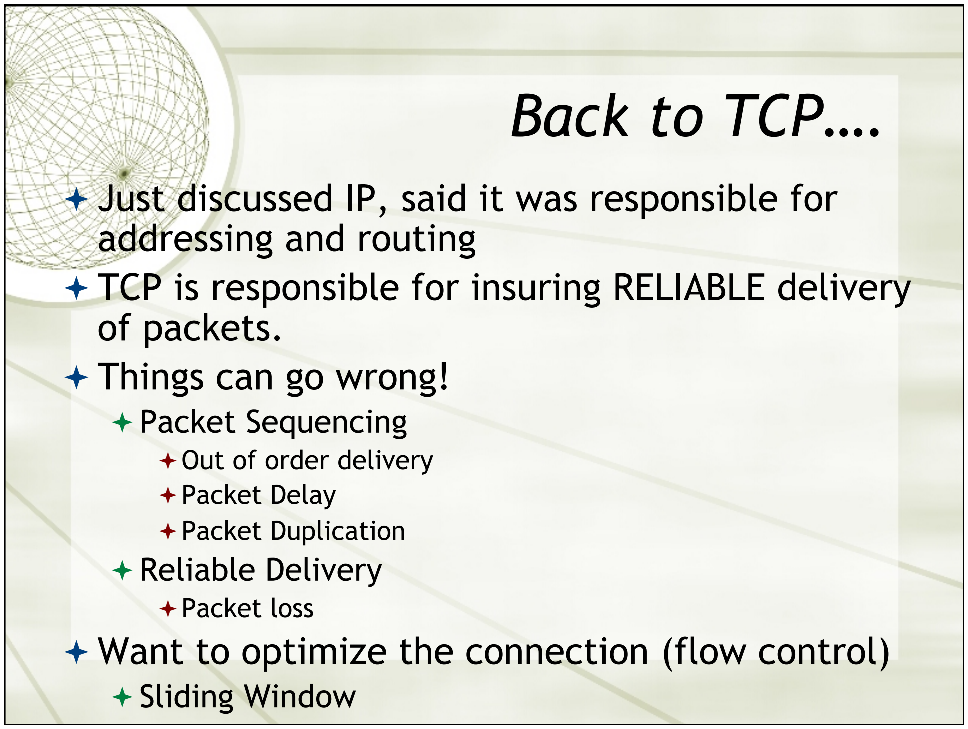
  How might we setup our IP address space in terms of subnets and subnet masks? Are there advantages to one way or the other?



Activity

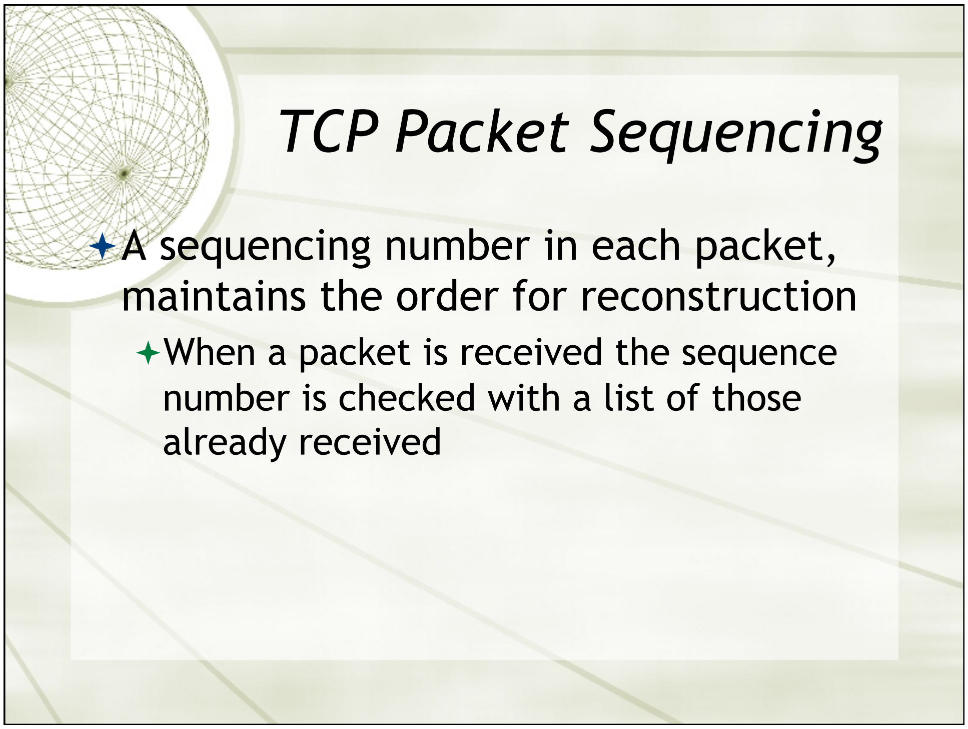
- Again, groups of 2-3, 5 minutes
- Question: You have purchased a new ethernet switch from Newegg and want to setup a small home network. You have a printer and two desktop computers and none of them have a wireless NIC so you are going to use an ethernet cable to connect each device to your new switch. You also have a router provided by your ISP that you are going to connect to your new switch so your computers can access the Internet.

  The internet router's IP address is 192.168.1.1 and by default it acts as a DHCP server. You have setup your desktop computers to obtain their IP addresses via DHCP. You've decided to statically assign your printer the IP address 192.168.2.1 with a subnet mask of 255.255.255.0. Assume there are no software issues and the printer is capable of printing using TCP/IP. Will your computer be able to print to it or not? Why or why not?



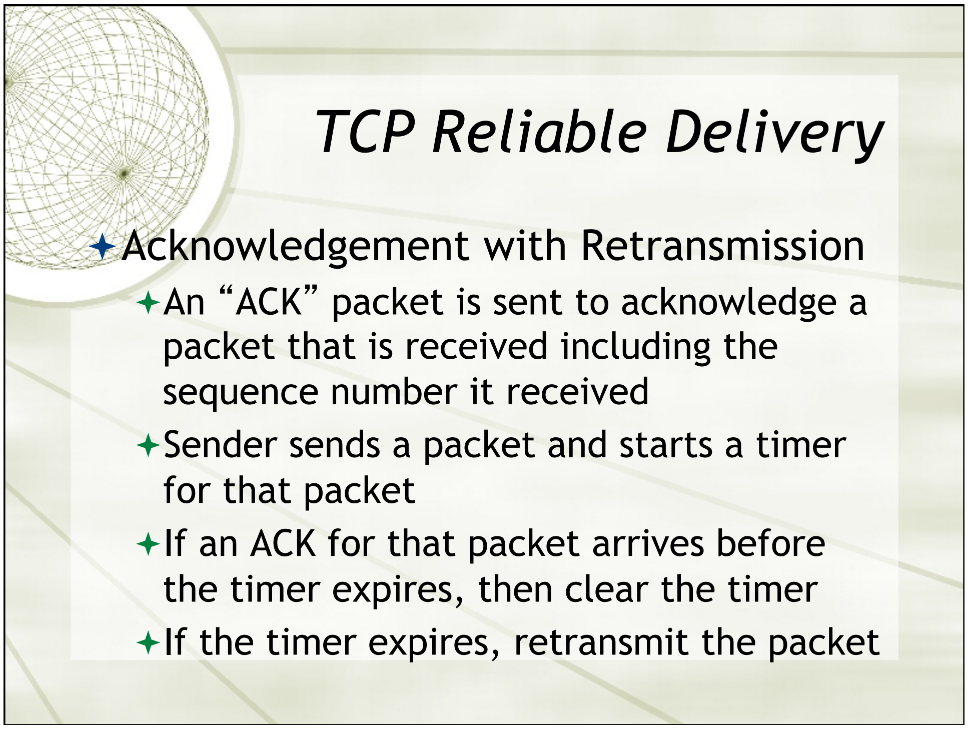
Back to TCP….

- Just discussed IP, said it was responsible for addressing and routing
- TCP is responsible for insuring RELIABLE delivery of packets.
- Things can go wrong!
  - Packet Sequencing
    - Out of order delivery
    - Packet Delay
    - Packet Duplication
  - Reliable Delivery
    - Packet loss
- Want to optimize the connection (flow control)
  - Sliding Window



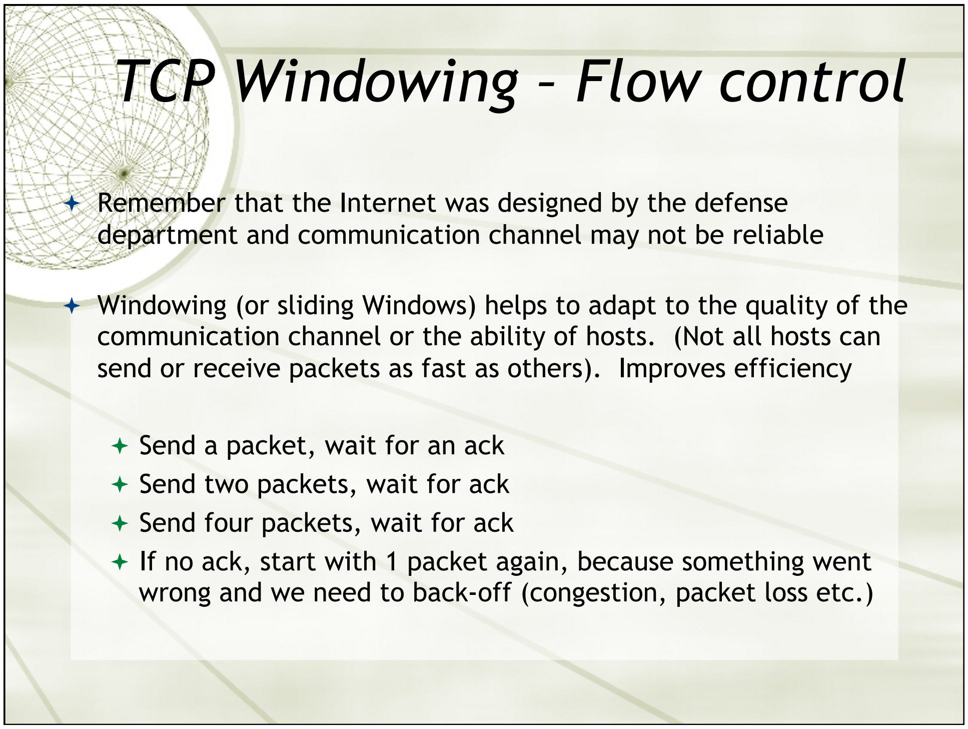
TCP Packet Sequencing

- A sequencing number in each packet, maintains the order for reconstruction
  - When a packet is received the sequence number is checked with a list of those already received



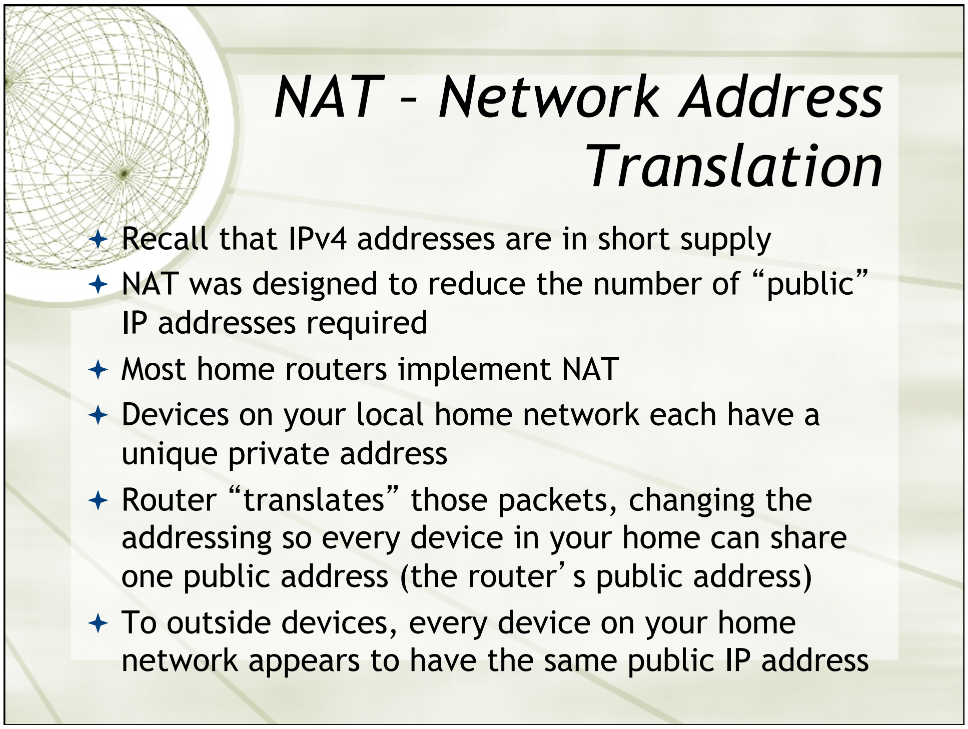
TCP Reliable Delivery

- Acknowledgement with Retransmission
  - An “ACK” packet is sent to acknowledge a packet that is received including the sequence number it received
  - Sender sends a packet and starts a timer for that packet
  - If an ACK for that packet arrives before the timer expires, then clear the timer
  - If the timer expires, retransmit the packet



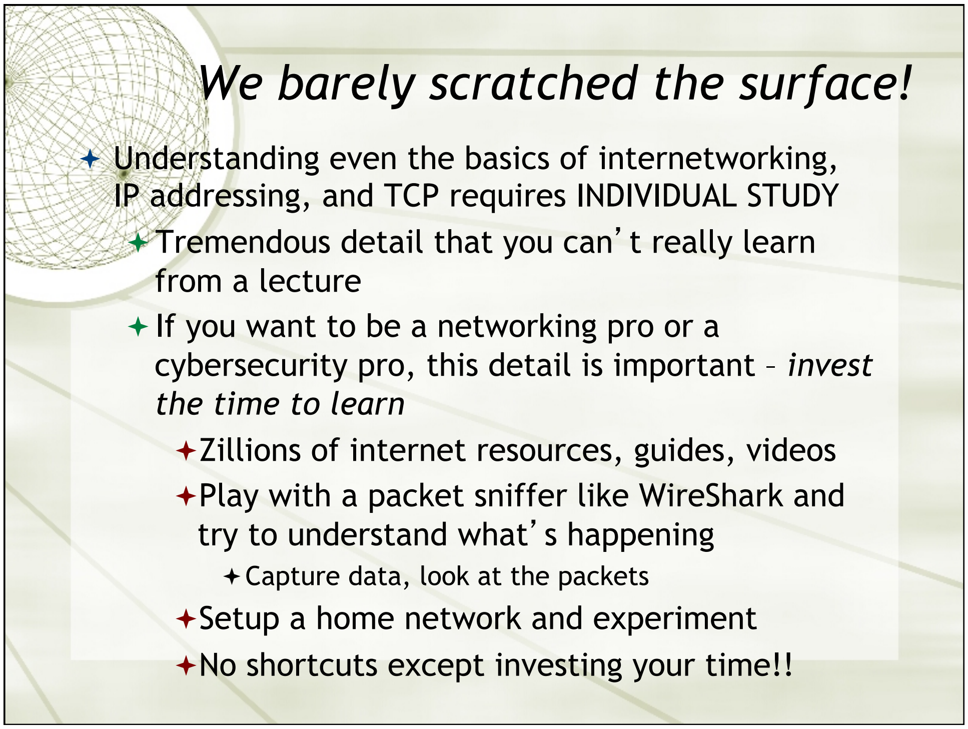
TCP Windowing – Flow control

- Remember that the Internet was designed by the defense department and communication channel may not be reliable
- Windowing (or sliding Windows) helps to adapt to the quality of the communication channel or the ability of hosts. (Not all hosts can send or receive packets as fast as others). Improves efficiency
  - Send a packet, wait for an ack
  - Send two packets, wait for ack
  - Send four packets, wait for ack
  - If no ack, start with 1 packet again, because something went wrong and we need to back-off (congestion, packet loss etc.)



NAT – Network Address Translation

- Recall that IPv4 addresses are in short supply
- NAT was designed to reduce the number of "public" IP addresses required
- Most home routers implement NAT
- Devices on your local home network each have a unique private address
- Router "translates" those packets, changing the addressing so every device in your home can share one public address (the router's public address)
- To outside devices, every device on your home network appears to have the same public IP address



We barely scratched the surface!

- Understanding even the basics of internetworking, IP addressing, and TCP requires INDIVIDUAL STUDY
  - Tremendous detail that you can't really learn from a lecture
  - If you want to be a networking pro or a cybersecurity pro, this detail is important – *invest the time to learn*
    - Zillions of internet resources, guides, videos
    - Play with a packet sniffer like WireShark and try to understand what's happening
      - Capture data, look at the packets
    - Setup a home network and experiment
    - No shortcuts except investing your time!!