Internetworking & IP Addressing

Info 341 Networking and Distributed Applications

Protocols

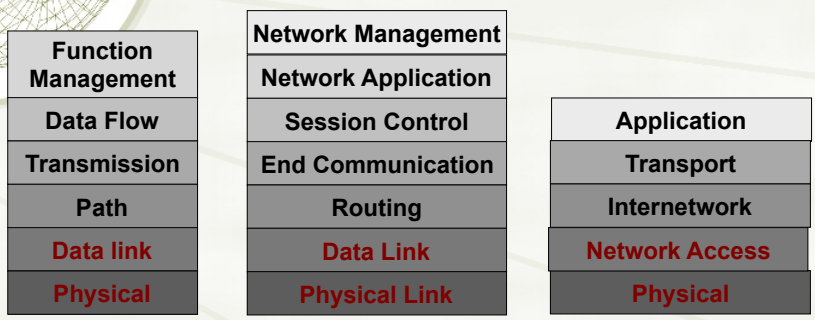
- Protocol - an agreement about how endpoints will communicate
  - Protocols are an end-to-end concept
- Protocol Suite - a set of protocols that handle a full range of communication details and error handling (also 'stack')

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

ISO 7 Layer Model

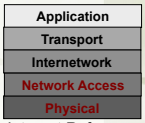
Other Layered Models



IBM SNA | DECnet | Internet Reference Model

What happens in a layer? Network Access

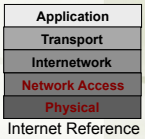
- Consider the Internet Reference Model
- Network Access
  - The functions of this layer are largely hidden from the 'user'
  - Often tied to the specific network hardware (e.g. Ethernet, Token Ring, etc)
  - The Address Resolution Protocol (ARP) exists here, to map physical addresses to internet addresses



Internet Reference Model

What happens in a layer? Internetwork

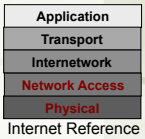
- Internetwork
  - Facilitates delivery of internet packets
  - This is often considered the Internet Protocol (IP) layer
  - Defines the basic datagram (packet)
  - Facilitates fragmentation & reassembly
  - Defines the addressing scheme
  - Facilitates routing to remote machines



Internet Reference Model

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

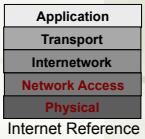
- Host-to-Host Transport
  - User Datagram Protocol (UDP)
    - Unreliable packet delivery
    - No built-in acknowledgement of packet
    - Very low overhead from the network
  - Transmission Control Protocol (TCP)
    - Reliable, connection-oriented service
    - Attempt to guarantee delivery, packets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



Internet Reference Model

What happens in a layer? Application

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



Internet Reference Model

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

Protocol Techniques

- Packet Sequencing
  - Out of order delivery
  - Packet Delay
  - Packet Duplication
- Reliable Delivery
  - Packet loss
- Sliding Window
  - Flow control

Packet Sequencing

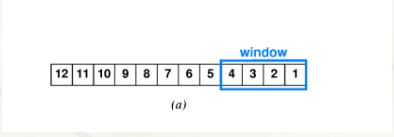
- A sequencing number in each packet, maintains the order for reconstruction
  - When a packet is received the sequence number is checked with a list of those already received

Reliable Delivery

- Acknowledgement with Retransmission
  - An "ACK" packet is sent to acknowledge a packet that is 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

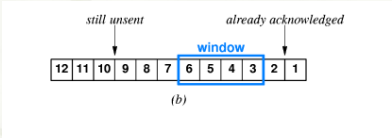
Sliding Window

- Improve efficiency, prevent overruns
  - Define a window size, send that many packets right away



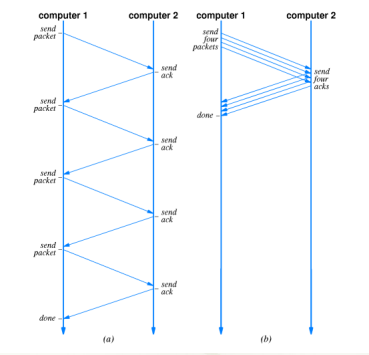
Sliding Window

- As ACKs come in, slide the window and send additional packets



Sliding Window

- Improves throughput



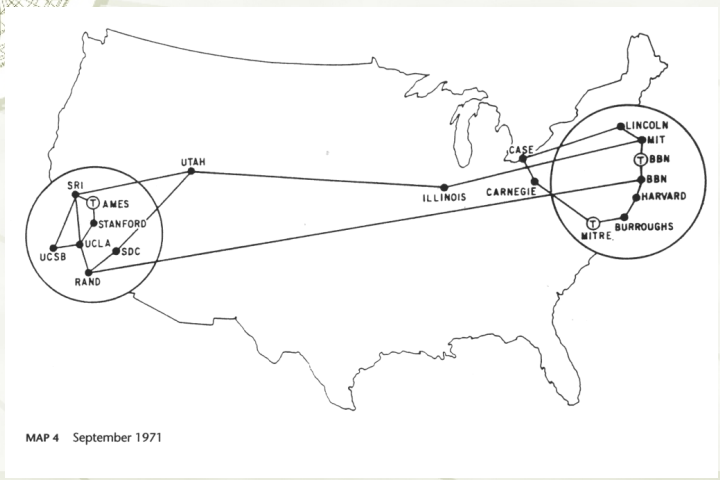
Internetworking

- Basic idea is a network of networks
  - An internetwork - internet
  - Different networks for different use
  - Hide differences among networks
  - Combination of hardware and software
    - Software implements a virtual network
      - Addressing, protocols, etc
  - Most common Internetworking standard TCP/IP

Internet & TCP/IP

- Transmission Control Protocol/Internet Protocol
  - Development began in the early 1970's
  - 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.

The Original ARPANet



Additional Design Considerations

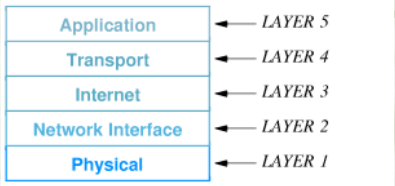
- Wanted the network to be able to scale well, to potentially connect a very large number of nodes and different network types
- Wanted the network to be able to continue functioning even if a particular segment failed or there was unreliable communications
  - Consider again this is being funded by 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

TCP/IP Protocol Suite

- What is a protocol?
  - An end-to-end agreement about how to communicate
  - TCP/IP is not the only protocol used on LANs. Others include IPX, Netbios, DecNet, AppleTalk, others
  - Multiple protocols can exist at the same time on a LAN although some Network Administrators only allow TCP/IP
- 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

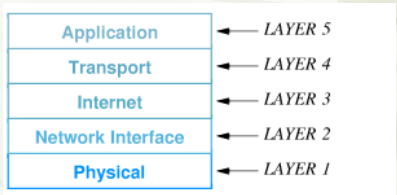
TCP/IP Layering Model

- 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

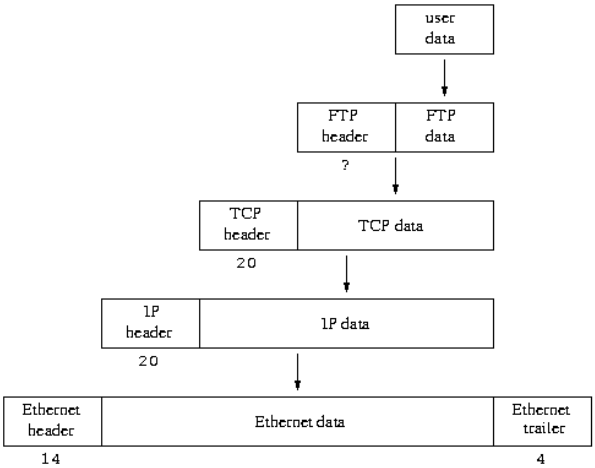


Ethernet hardware and layers

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



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
  - 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

Special IP Address Numbers

- 0 and 255 have special meanings in IP addresses
  - 0 and 255 are reserved for special purposes
  - Example: 128.208.100.255 is a broadcast address for the 128.208.100.x network
- Devices have addresses from 1-254

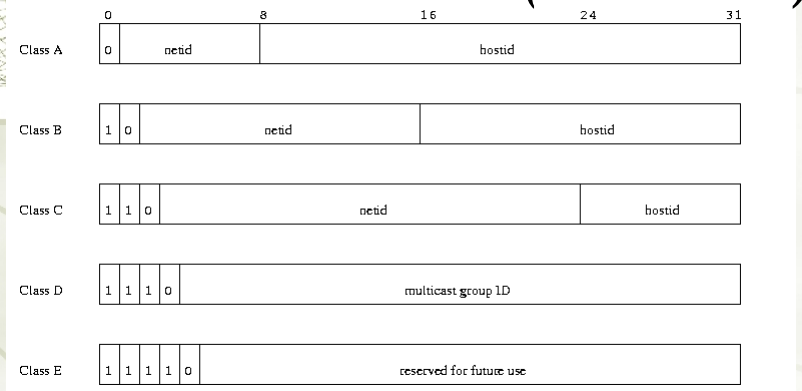
Address Classes (historical)

- Each 32 bit address is actually divided into 2 different fields
  - The NetID portion of the address identifies the network that a host is connected to
  - The HostID portion of the address gives each node on a given network a unique identifier
- 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)



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

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

CIDR Notation

- 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
- 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.x 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

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

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

More Complex Masks

- 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

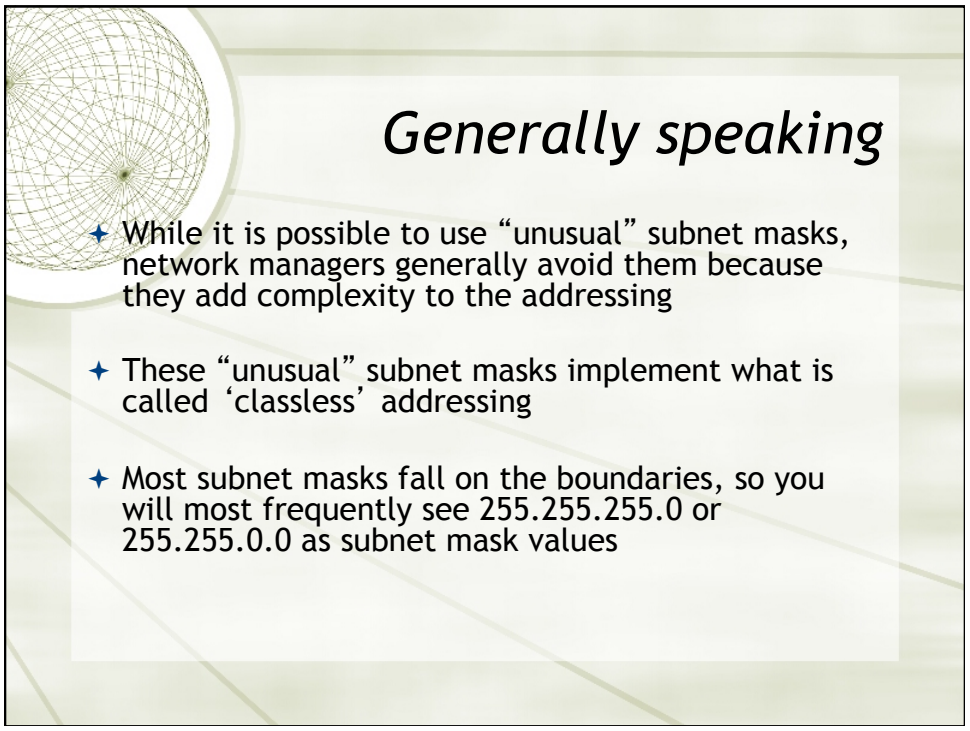
- We know all the addresses will start out with 150.199.10. Let's consider that last octet when using a 255.255.255.192 subnet mask. The first 2 bits of the last octet are part of the network so:

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


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