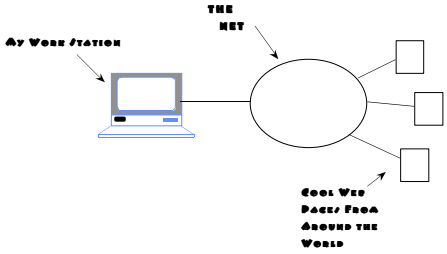
Technical Aspects of TCP/IP Networking

Charles Severance

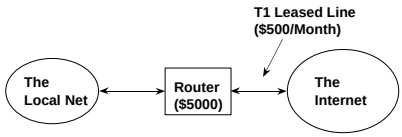
Network Terminology++

- Desk Area Network (DAN)
  - Camera, CPU, Mouse, Printer, Television, Stereo
- Local Area Network (LAN)
  - Limited by the physical length of a wire
- Building Area Network (BAN)
  - Multiple LANs tied together - performance/security
- Metro Area Network (MAN)
  - Multiple LAN/BANs tied together - no right of way
- Organization Area Network (OAN)
  - A network under control of one authority - Firewall?
- Wide Area Network (WAN)
  - Network uses long-lines typically from the phone co.
- Planet Area Network (PAN)
  - The Internet - A network of networks of networks

The View of the End User



View of the Network Administrator



We will cover each of these elements in some detail

TCP/IP Networking Model

- TCP/IP has a layered network model

Application Layer
Transport Layer (TCP) Error Correction Reliable Connection
Internetwork Layer (IP) WAN Connectivity Unreliable Datagram Service
Network Access Layer Physical Connection LAN Connection

A layered approach allows the problem of implementing a network to be broken into more managable sub problems.

For example, the IP layer is allowed to lose a packet if things go bad.

It is TCP's responsibility to store and retransmit the lost data.

Network Access Layer

- Responsible for physical connection
  - Shape
  - Size
  - Voltages
- Responsible for rules of how to put bits on the "wire"
- These are the building blocks for the network
- The goal of the physical layer is to move information across one "hop"

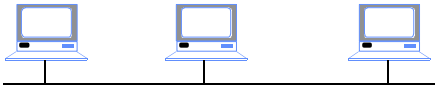
Example Physical Layers

- Local Area Network Standards
  - Ethernet (IEEE 802.3) (10Mb/sec - 100Mb/sec)
  - Token Ring (IEEE 802.4) (4Mb/sec-16Mb/sec)
  - FDDI (Fiber) (100Mb/sec)
  - CDDI (Copper) (100Mb/sec)
  - Packet Radio (3Mb/sec)
- Metro Area Network Standards
  - Cable TV (10Mb/sec)
  - Packet Radio (256Kb/sec)

Example Physical Layers

- Wide Area Network Standards
  - Leased Lines
    - » T3 - 45Mb/sec
    - » T1 - 1.544 Mb/sec
    - » 56 KB/sec
  - Dial-up
    - » ISDN - 128Kb/sec
    - » Modem - 28 Kb/sec
- These physical layer standards have different strengths and weaknesses and associated costs.
- To build an effective WAN it may be necessary to use several types of media

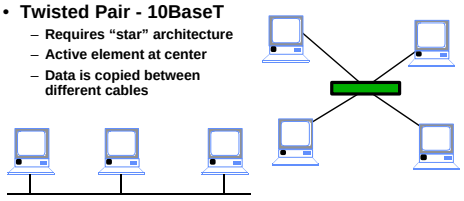
Ethernet/IEEE 802.3



Each interface has a unique serial number based on manufacturer
Broadcast packets are used to find other systems on the net
Each packet has a "protocol identifier"
IP
Appletalk
DECNET
Novell
Many protocols can co-exist on the same physical ethernet

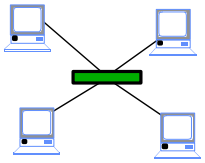
Ethernet Wiring Choices

- Coax - 10Base2
  - Allows "daisy chained" architecture
  - Physical "broadcast"
- Twisted Pair - 10BaseT
  - Requires "star" architecture
  - Active element at center
  - Data is copied between different cables

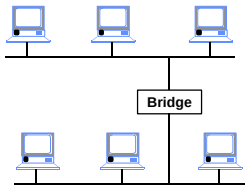


Ethernet Hubs

- In a star topology, some active network gear is necessary at the center of the network
- The simplest connection is using a hub
- A hub simply connects all of the stations together as if they were on a single physical wire
- All data is copied to all ports
- While any system is talking all others must wait



Ethernet Bridges

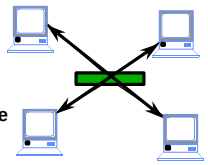


A bridge is "intelligent" network equipment which connects two Ethernet LANs. The Bridge copies packets from one network to another until it "learns" which systems are on which side of the bridge. Broadcasts must always be copied. Bridges keeps a list of which ethernet addresses are on which segment.

Bridges are a very nice simple solution because they require no configuration or management but they run out of table space or suffer from too much broadcast traffic when too many networks are interconnected.

Ethernet Switches

- In a star topology, the network gear at the center can also be a switch
- The switch maintains tables for each connection which are built similar to the bridge tables
- On a switch, traffic is only copied out to the ports for which the data is destined
- A switch allows all pairs of stations to communicate simultaneously at top speed



CSMA/CD - Ethernet Protocol

- Carrier Sense Media Access with Collision Detection
- Because the Ethernet network is shared, each station “hears” all traffic to avoid garbled messages, systems must observe “rules”
- Ethernet rules are simple
  - Listen for any traffic, wait until “silent”
  - Begin transmitting data
  - Listen for your own data
  - If you cannot hear your own data clearly, assume a collision, stop and wait before trying again
  - Each system waits a different amount of time to avoid “too much politeness”

Other Physical Layers

- This only describes Ethernet physical layer
  - Leased Lines - T1, T3
  - Fiber Optic - FDDI, ATM
- Each physical layer has complicated details
- The goal of a physical layer is to cross one “hop” reliably

Fiber Optic

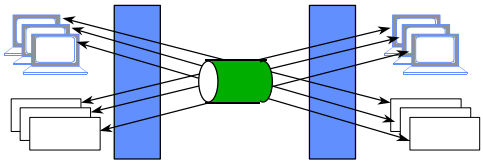
- Fiber Optic can be used in many ways
  - FDDI (Fiber Distributed Data Interface) - 1100Mb
  - ATM - Asynchronous Transfer Mode - 1Gb
  - Gigabit Ethernet - IEEE 802.3z - 1Gb
- Fiber Optic tends to be used for long physical distance applications
  - Total fiber capacity is > Tb/sec 10^{12}
  - Less susceptible to interference
  - Install once, then upgrade the equipment at either end to increase bandwidth

Internetwork Layer (IP)

- The goal of the Internetwork layer is to transport data from one end-user system to another end-user systems hopping across as many physical connections as necessary.
- Internetwork Layer provides a mechanism to connect many LANs together effectively
- IP is an *unreliable* datagram protocol
- Packets may arrive *out of order or not at all*
- IP is responsible for making connections between millions of computers worldwide without using broadcast packets

System to System IP

- Regardless of the number of connections between two systems, the traffic is transported across the internet as a single IP address - It is the responsibility of TCP to separate (de-multiplex) each stream on each system



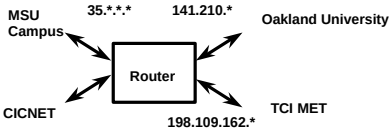
IP Addresses

- The IP address is the worldwide number which is associated with one particular workstation or server
- Every system which will send packets directly out across the Internet must have a unique IP address
- IP addresses are based on where station is connected
- IP addresses are controlled by a single organization - address ranges are assigned
- They are running out of space!

IP Addresses and Network Numbers

- A range of IP addresses is assumed to be on a single "physical network" from the point of view of the Internet
  - Class A: 1-127.*.*.*
    - » 127 networks, 16 Million hosts per network
    - » 35.8.2.42 serv1.cl.msu.edu
    - » 36.56.0.10 stanford.edu
  - Class B: 128-191.0-255.*.*
    - » 16,065 networks, 65,025 hosts per network
    - » 141.210.10.11 mars.acs.oakland.edu
  - Class C: 192-223.0-255.0-255.*
    - » 2,015,775 networks, 255 hosts per network
    - » 198.109.162.6 www.tcimet.net

Internet Protocol (IP) Router

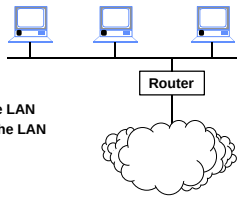


An IP Router does not have to know where every system is connected. All that is necessary is to know "which way" will get the packet closer. Because of this the table is quite small and can handle an unlimited number of systems.

However the router can only route IP - Not Ethernet. Because of this Novell/Appletalk, etc cannot be sent through an IP router directly.

Simple Router

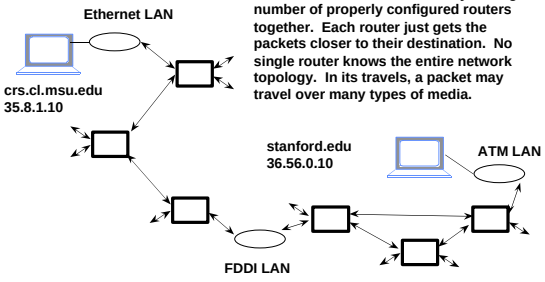
- Each organization has a router which acts as a "gateway" to to the Internet
- This router is connected to the LAN and also has a WAN or LAN connection
- The configuration of this router is simple
  - Network number for the LAN
  - Its own IP address on the LAN



Backbone Router

- A router with multiple connections must maintain a table with the best routes to all possible network numbers
- The closer a router is to the core of the internet, the more difficult this becomes
- These routes can change as links go up or down, or traffic patterns change
- These routers have special protocols to update these "routing tables" dynamically
  - RIP - Routing Information Protocol
  - EGP - Exterior Gateway Protocol

An IP Internetwork



An IP Internetwork is created by linking a number of properly configured routers together. Each router just gets the packets closer to their destination. No single router knows the entire network topology. In its travels, a packet may travel over many types of media.

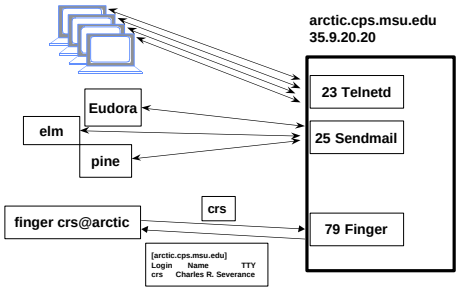
Transport Layer (TCP)

- The responsibility of the transport layer is to present a reliable end-to-end pipe to the application
- Data either arrives in the proper order or the connection is closed
- TCP keeps buffers in the sending and destination system to keep data which has arrived out of order or to retransmit if necessary
- TCP provides individual connections between applications

Application Layer

- The Application layer uses the reliable TCP connections to accomplish useful work over the network
  - client-server applications
  - standard applications
    - » telnet (port 23)
    - » mail (port 25)
    - » finger (port 79)
    - » ftp (port 21)
- Each application uses a "port" and a protocol
- Each port can have many connections
- On a UNIX system type netstat -a

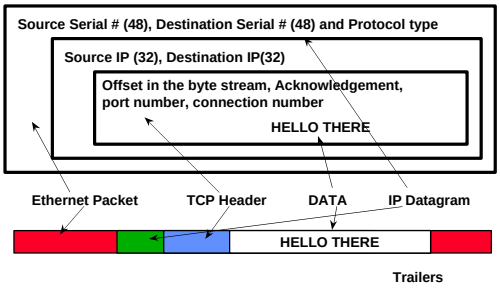
Ports and Applications



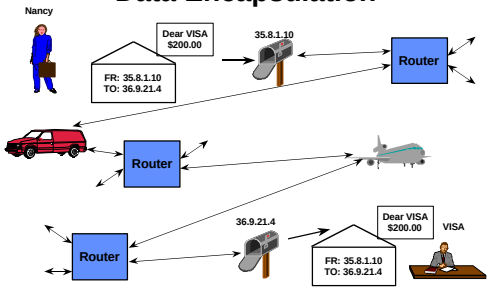
Application Layer Standards

- Often a document called RFC (request for Comments) is written for each application
  - http://ds.internic.net/ds/dspg1intdoc.html
  - http://ds.internic.net/rfc/rfc1288.txt (Finger RFC)
- RFC's are all available on-line and can be searched

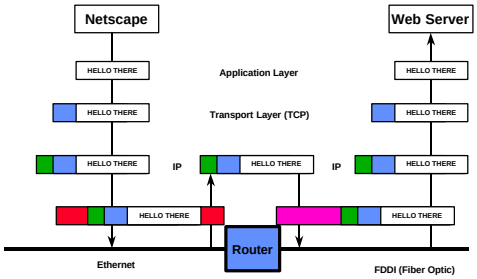
Data Encapsulation



Data Encapsulation



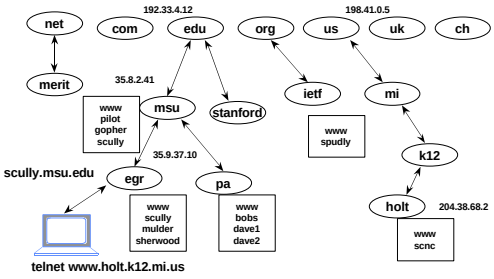
Data Encapsulation



The Domain Name System

- In order to make the use of network addresses more convenient and flexible, each system connected to the Internet also has one or more logical addresses.
- For example: clunix.msu.edu
- Unlike IP addresses, the domain address have no routing information - they are organized based on administrative unit
- There are no limitations on the mapping from domain addresses to IP addresses

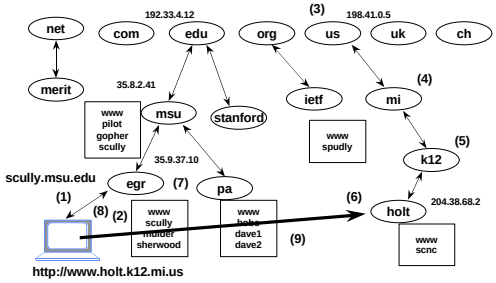
Domain Name Hierarchy



Domain Name Resolution

- The act of looking up a logical name and finding a physical IP address is called Domain Name Resolution
- There is a hierarchy of domain name servers
- Each client system uses one domain name server which in turn queries up and down the hierarchy to find the address
- If your server does not know the address, it goes up the hierarchy possibly to the top and works its way back down

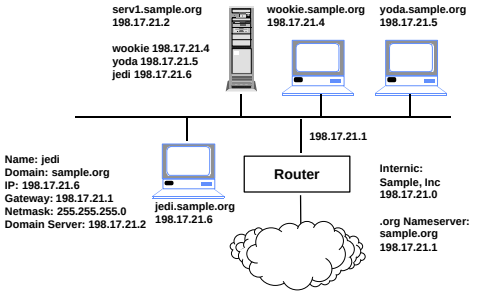
Domain Name Resolution



The View From a Client

- Each client must know the following information:
  - Their own IP address
  - The address of the gateway
  - The network mask - Indicates which IP address are local and which IP addresses are remote.
  - The address of the domain name server for the client

Sample Network - 198.17.21.0



Conclusion

- This does not yet qualify you to be a TCP/IP administrator - but it hopefully gives you some ideas
- Excellent text: TCP/IP Network Adminstration, O'Reilly & Associates, Craig Hunt, ISBN-0-937175-82-X