CA169: Week 6

The Internet

OVERVIEW

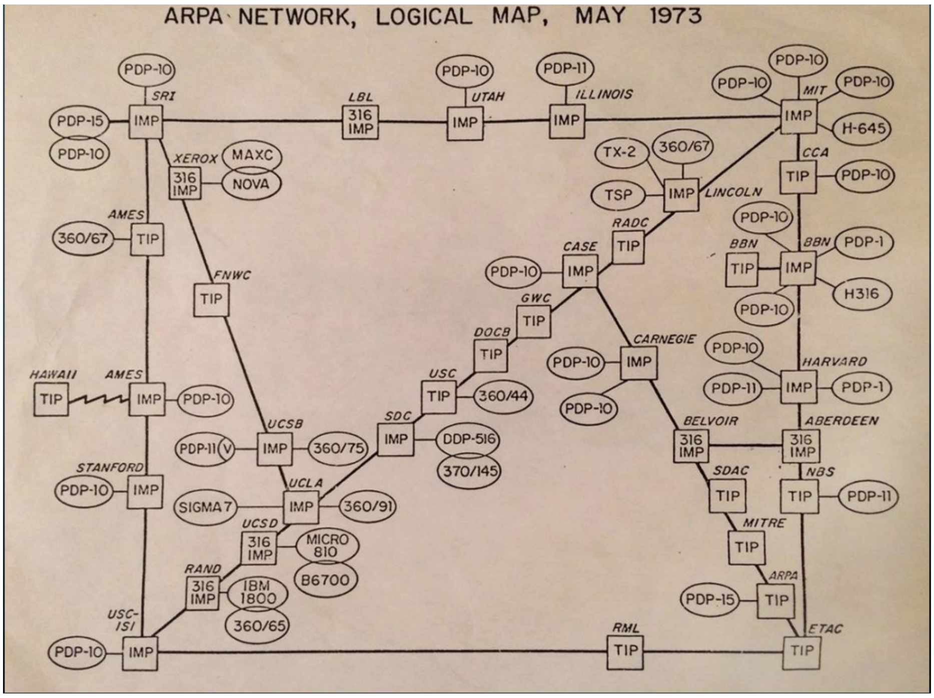
- History of the internet
- How the internet is structured
- Addressing & routing
- TCP & UDP

WHAT IS THE INTERNET?

- Global communication network
- Millions (if not billions) of computers connected
- Number of protocols to manage communications
- Websites ≠ Internet

HISTORY OF THE INTERNET

- Originally called the ARPANET in 1969
- ARPA became DARPA
- Developed during the cold war
- Linked universities & military installations



- ARPANET was the first packet switched network
- However it was only in America
- The network grew
- Other networks were created
- In order to create the internet they had to have a common form of communication
- By the end of the 1970s the transmission control protocol (TCP) was created
- This provided a common means of communication between computers
- Later on the Internet Protocol (IP) was added
- This is why we call it TCP/IP
- With TCP/IP the internet was globally connected
- However it was only used in universities for researchers to send data to one another
- They could read papers from the libraries of other organisations

THE HISTORY OF THE INTERNET – THE WORLD WIDE WEB

- In 1991 Tim Berners Lee invented the HTTP protocol
- HTTP stands for HYPERTEXT TRANSFER PROTOCOL
- This could be used to easily send data to any computer
- Along with HTTP , HTML was created
- HTML is the markup language used to create web pages
- Before HTML the internet was only used within a terminal
- HTML required a web browser to use
- Since then we are now on HTML5 & CSS3

INTERNETWORKING

- TCP/IP is the de-facto internet standard.
- Major issues to be addressed in Internetworking are…
    - Service type.
    - Addressing
    - Routing
    - QOS
    - Max. packet size
    - Flow & congestion control
    - Error reporting

SERVICE TYPE

- Connection oriented TCP
    - Provides reliable error free transport.
    - Utilises sliding window protocol.
- Connectionless UDP
    - Provides best effort datagram delivery.
    - Unreliable, packets may be discarded, not acknowledged.

ADDRESSING

- How do we address processes running on hosts ?
- How do we ensure unique addresses ?
- How do we map LAN addresses to TCP/IP addresses ?
- How do we interpret addresses ?
- How do we know where to send packets, i.e. route packets ?

ROUTING

- Issues include …
- How does host determine address of router attached to its network.
- How does host select a particular router when sending a packet.
- How does router determine addresses of other routers attached to the same network
- How does router select another router to which to send packets given destination host address.

QUALITY OF SERVICE

- Issues include…
- Transit delay expected when delivering packets to destination.
- Security and privacy required.
- Cost of delivery.
- Probability of error.
- Priority of transfer.

MAXIMUM PACKET SIZE

- Prevailing conditions may determine size.
- High bit error-rates: smaller packets better.
- Large transit delay: large queuing delays at each intermediate router, reduces efficiency.
- Buffer requirements at routers may dictate that it is easier to store smaller than larger packets..
- Processing overheads used in processing large numbers of small packets are larger than processing smaller numbers of larger packets.

TCP/IP

- Four layer Architecture
- Developed in 1960's
- Open System
- Not just one protocol, whole family.
- Many programming interfaces available.
- Standardised protocol set.

INTERNET PROTOCOL

- Main protocol for the internet
- It's job is to send packets from one address to another
- There are two main protocols in use
- IPv4
- IPv6

INTERNET PROTOCOL - IPV4

- The main transport mechanism for the internet (at the moment)
- Made up of IP addresses
- Each address is 32 bits (4 bytes)
- 32 bits = 2^{32} addresses.
- Written as decimal dot notation
    - E.g. 136.206.48.94
- Each byte can range from 0-255
- First IP address = 0.0.0.0
- Last IP address = 255.255.255.255
- ~4 Billion IPv4 addresses!
- IPv4 addresses translate into binary
- 32 bits = 4 bytes = 4 sets of 8 binary digits
    - E.g. what is 153.206.48.94 in binary
-

153	206	48	94
10011001	11001110	00110000	01011110

BINARY (A REFRESHER)

- Base 2 number system (1's and 0's)
- We use Decimal – base 10 (0-9)
- There is also Octal – base 8 (0-7)
- Finally Hexadecimal – base 16 (0-9A-F)

BINARY TO DECIMAL

- Based on powers of two
- Exponents go right to left from 0
- Each exponent has base 2
- Multiply by binary (1or 0)
- Add them all together
- N.B. anything times 0 = 0
- Anything to the power of 0 = 1 (even $0^0 = 1$)

Binary	1	0	1	0
Exponent	3	2	1	0
	2^3	2^2	2^1	2^0
	$2^3 \times 1$	$2^2 \times 0$	$2^1 \times 1$	$2^0 \times 0$
	$(2^3 \times 1) + (2^2 \times 0) + (2^1 \times 1) + (2^0 \times 0)$			
	8 + 0 + 2 + 0			
	10			

- Convert 13 to binary
- Use whole number division
- Keep dividing the number by 2 and keep track of the remainder
- Stop once you reach 0
- Read the remainder from bottom to top

Equation	Answer	Remainder
$13 \div 2$	6 r 1	1
$6 \div 2$	3 r 0	0
$3 \div 2$	1 r 1	1
$1 \div 2$	0 r 1	1
0		

BACK TO IP ADDRESSES

- A machine can have many IP addresses
- An IP address can address only one NIC
- IP addresses broken into classes
  - A, B, C, D
- Class derived from the binary of the IP address

HOW TO FIND THE CLASS OF AN IP ADDRESS

- Convert the IP address into binary
- Look at where the first 0 is in the ip address
- If the first digit is 0 -> Class A
- Second digit -> Class B
- Etc..

Starting 0	Class
0	A
10	B
110	C
1110	D
1111	E

- What class is 192.168.0.0?
- Convert to binary
  - 11000000 . 10101000 . 00000000 . 00000000
- First 0 appears in the 3rd place Class C address

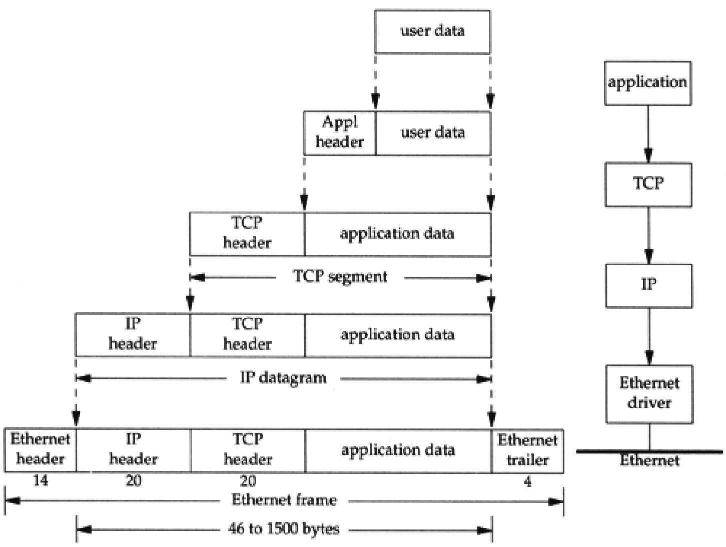
CLASSES, NETWORKS AND HOSTS

- Each class contains blocks of IP addresses called networks
- Each network contains a number of hosts
- These are the amount of machines that can be on the network.
- Class A – most hosts
- Class D – Least hosts

WHAT ABOUT CLASS E?

- Class E is a special class:
- It was never really defined what class E should be for
- It says reserved for "future use" (been reserved since the 90's)
- Most networks will ignore class E addresses (there are exceptions)
- Some addresses are reserved (e.g. 255.255.255.255 – broadcast)
- Some have been set aside for "Research"
- The US Military also took a few (214.x.x.x, 215.x.x.x)

TCP/IP ENCAPSULATION



Application

Tcp

ip

802.3

IP PACKET HEADER

<table>
<tr><td>4bit ver.</td><td colspan="2">4bit hdr L</td><td>8bit TOS</td><td colspan="2">16-bit total length (bytes)</td></tr>
<tr><td colspan="4">16-bit identification</td><td>3 bit flags</td><td>13 bit frag. offset</td></tr>
<tr><td colspan="2">8-bit TTL</td><td colspan="2">8-bit protocol</td><td colspan="2">16-bit header checksum</td></tr>
<tr><td colspan="6">32-bit source IP address</td></tr>
<tr><td colspan="6">32-bit destination IP address</td></tr>
<tr><td colspan="6">Options</td></tr>
<tr><td colspan="6">Data</td></tr>
</table>

IP HEADER DESCRIPTION

- Version: Currently V 4.
- Header Length: Specifies length of header as some fields are optional.
- Type of Service: This is the same as the QOS mentioned previously.
- Total length: Specifies the length of the datagram.
- Identification:Used to identify a set of datagrams which were formed from a single user message, but which got fragmented while traversing possibly several networks.
- D bit: Indicates that routers should not fragment a datagram i.e. Don’t fragment bit.
- M bit: Indicates that there are more fragments to follow in later datagrams.
- Fragment offset: Where this fragments fits into the original fragmented datagram
- Time to live: Datagram loses a life (or some time to live) on each hop across the internet. Datagram destroyed when time\lives run out. Prevents Datagrams from wandering endlessly.
- Header Checksum: Checks header only.
- IP addresses (Source, Destination): As described previously

IP ROUTING

- Central function of IP is routing along with fragmentation and re-assembly of data across an internet.
- Routing information organised in a hierarchy. With hosts and gateways involved.
- ARP address resolution protocol maps IP to Ethernet addresses, an Interior Gateway Protocol (IGP)
- Exterior Gateway Protocol (EGP) knows about other routers on the internet and can route from network to network.
- Distance Vector and Link State routing are most popular, Link State is superior.
- Subnet addressing may be performed on a group of related networks (owned by one organisation).
- More on Routing later...

SPECIAL IP ADDRESSES

- Some addresses are reserved for special use.
- IP address composed of all 0 means this host.
- Network part all 0, Host part not, host on this network.
- All 1s broadcast on LAN
- Host part 127.0.0.x is Loopback, useful for debugging.
- 192.168.0.0 and 10.0.0.0 are reserved by IANA and are private addresses
- 172.16.0.0 up to 173.31.255.255 are reserved /12 or 16 class B addresses also reserved.

CREATING SUBNETS

- Address space
  - [network#, host#]
  - [network#, subnet#, host#]
- Subnet mask used to find the host part of IP address and distinguish it from the NW part.

Class	Format	Default subnet mask
A	nw.node.node.node	255.0.0.0
B	nw.nw.node.node	255.255.0.0
C	nw.nw.nw.node	255.255.255.0

SUBNETTING – WHY?

- Reduces Network traffic
  - Routers create smaller broadcast domains, more smaller domains limits the span of a broadcast.
- Optimizes NW performance
  - Less traffic, things run faster.
- Simplifies management
  - Easier to do fault analysis on a smaller self-contained NW than with a single huge NW
- Facilitates spanning of large geographical distances
  - Single large NW over large distance incurs big overhead of resources. Smaller NWs which keep much traffic local will incur less overhead over the long haul.

CIDR

- Classless Inter Domain Routing -
- Give the IP address space some breathing room!
- Basic idea: allocate the remaining IP addresses in variable-size blocks without regard to classes
  - original name: Supernetting, the opposite of Subnetting (sortof)
- A site needing 2000 addresses receives a block of 2408 addresses
  - i.e., 8 contiguous class C networks.
  - If need 8000 hosts, then allocate a block of 8192 addresses, i.e., 32 contiguous class C networks.

VARIABLE LENGTH SUBNET MASKS

- Only works with routing protocols which support CIDR
- Different masks on each router interface. Small number of bits for routers so they have few hosts, few routers. Keep big numbers for LANs
- Match required number of hosts to appropriate mask on each interface.
- Requires careful design so that blocks do not overlap
- Routes may be summarised, providing a hierarchy.

TCP SERVICES

- Provides connection-oriented, reliable, byte stream service.
- Segments passed to IP for routing, timer attached for each segment.
- Sliding window protocol utilised with go-back-n or selective-repeat for retransmission.
- All TCP segments acknowledged.
- TCP segments may arrive out of order, sliding window will sort order.
- TCP segments may be duplicated, duplicated are discarded.
- TCP provides flow control, no process\host will be swamped, helps avoid congestion.
- TCP utilised by many internet applications such as Telnet, Rlogin, FTP, E-mail, WWW Browsers.

TCP SEGMENT HEADER

<table>
<tr><td colspan="8">16-bit source port number</td><td>16-bit destination port number</td></tr>
<tr><td colspan="9">32-bit sequence number</td></tr>
<tr><td colspan="9">32-bit acknowledgement number</td></tr>
<tr><td>4bit hdr length</td><td>reserved</td><td>urg</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>16-bit window size</td></tr>
<tr><td colspan="8">16-bit TCP checksum</td><td>16-bit urgent pointer</td></tr>
<tr><td colspan="9">Options (if any)</td></tr>
<tr><td colspan="9">Data (if any)</td></tr>
</table>

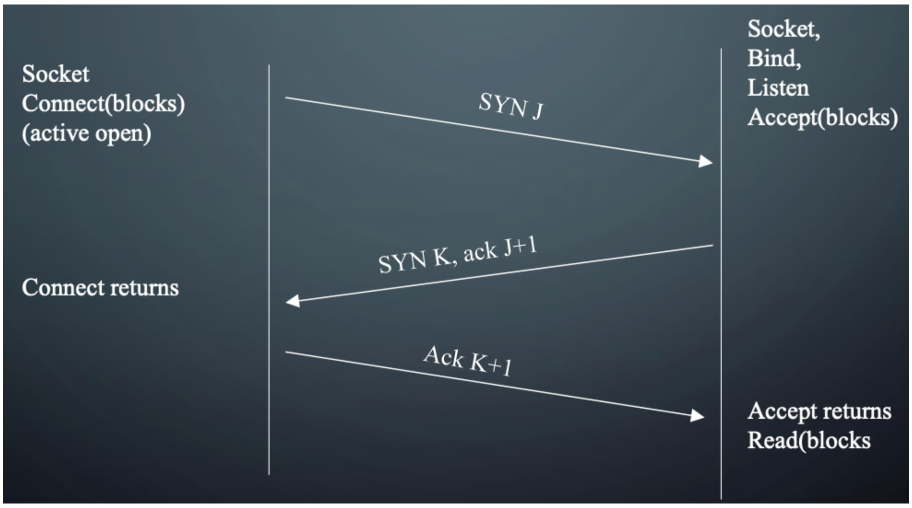
TCP HEADER DESCRIPTION

- Source Port and Destination Port identify transport end-points of connection.
- Sequence Number and Acknowledgement Number perform usual functions, Ack numbers next byte expected.
- TCP Header Length indicates number of 32 bit words in header. Length varies because of options.
- Not used. No bug fixes required !
- Six one bit flags…
- URGent pointer in use, used for indicating interrupts and offset from seq no. to urgent data.
- ACK bit used to indicate piggybacked acknowledgement.
- PSH requests that receiver does not buffer but to deliver.
- RST is reset connection, means problems !
- SYN used in conjunction with ACK to request connection.
- FIN release connection
- Window size used for variable-sized sliding window. Size of zero indicates a choke packet.
- Checksum checks header.
- Options field for things like specification of maximum TCP payload. Negotiated at startup lowest bid wins.
- A selective repeat instead of go-back-n sliding window protocol may be specified as an option.

TCP ADDRESSING

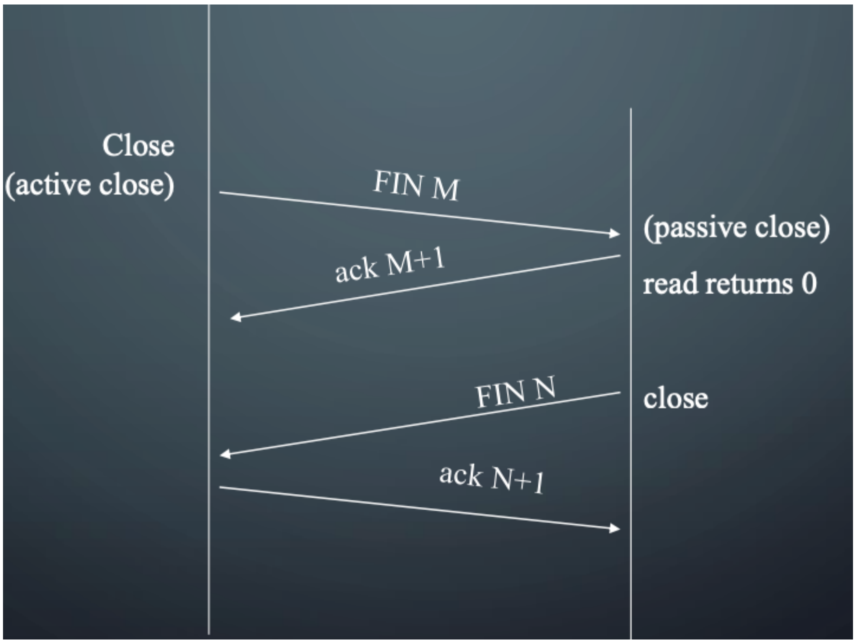
- TCP uses notion of Port Number to access transport endpoint on a single host.
- Many Ports may be in use simultaneously.
- Combination of IP address and port number uniquely identifies a port for process running on a particular machine.
- Process may even have several ports open.

Three Way Handshake



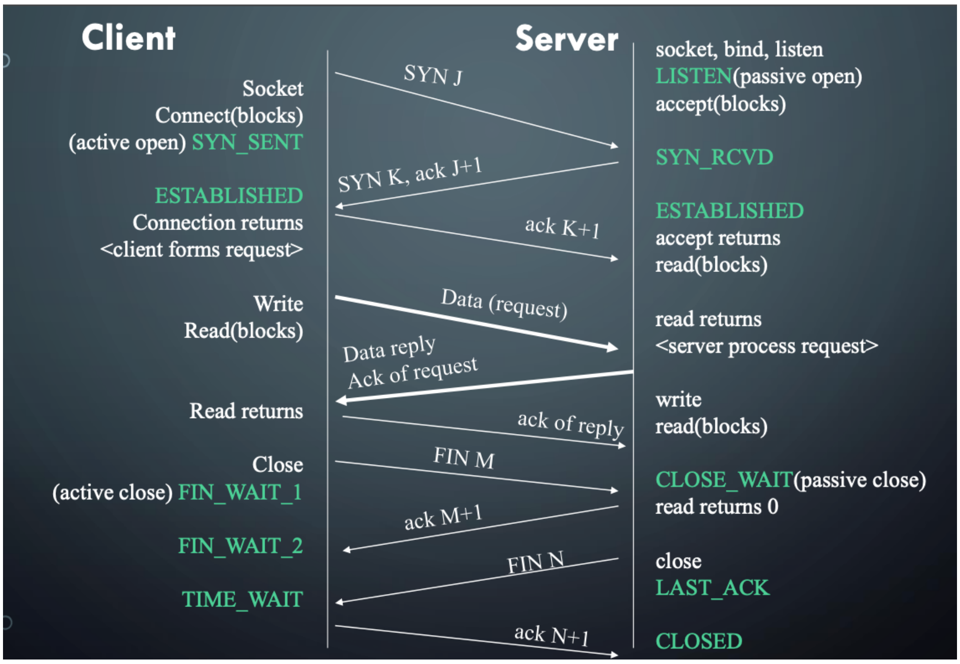
TCP CONNECTION TERMINATION

- If application calls close first, this is an active close.
- Sends FIN segment, meaning finished sending data.
- Server performs passive close.
- Clients FIN is ack'ed and sent to application as EOF, after any queued data to receive.
- When application receives its EOF, it will close its socket. TCP sends FIN.
- The server on receiving final FIN acks that FIN.



TCP CONNECTION & THE PACKETS

- A complete TCP connection involves many packet exchanges.
- Connection establishment
- Data transfer
- Connection termination
- TCP states are also shown as client and server enter them.

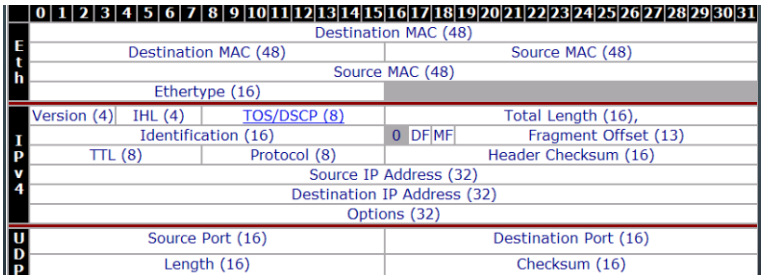


THE INTERACTIONS

- Once connection established, clients forms request for server.
- Server processes request and replies with piggybacked ack.
- Termination by client (active close)
- Waits 2MSL (Maximum Segment Lifetime) to deal with lost or wandering IP packets.
-

UDP

- The User Datagram Protocol. Its characteristics are:-
- Packet-oriented
- Connectionless
- Unreliable
- UDP adds almost nothing to the IP network layer over which it is transported. It just introduces the concept of a port (a concept it shares with TCP as we will soon see).
- A port is an abstraction which can be regarded as a transport-layer address (remember the role of the transport layer) which uniquely identifies a particular process (or endpoint) on the destination node
- The UDP header is very brief…



- The checksum is sometimes ignored…
- Most datalink layer protocols include some form of error-checking (e.g. Ethernet CRC)
- For some data types (e.g. VoIP), timely but (slightly) corrupt data is better than late but accurate data
- Services listen on well-known ports.
- DNS on UDP port 53
- Syslog on 514
- SIP on 5060 (e.g. whatsapp voice calls)
- These are administered by IANA (the Internet Assigned Numbers Authority) and the definitive list is maintained at http://www.iana.org/assignments/port-numbers
- Another good place to look these up is the /etc/services file on a Linux box or the %WinDir%\system32\drivers\etc\services file on Windows
- When a client wants to communicate with a UDP server, it starts by allocating a randomly-chosen UDP port > 1024.
- This will be the source UDP port.
- It will then transmit to the server on the destination port (e.g. one of the well-known ports mentioned on the previous slide).
- The server will reply with a UDP packet from the well-known port back to the port the client transmitted the request from
- The combination of (source IP address, source UDP port, destination IP address, destination UDP port) uniquely identifies this "session" (although the concept of a session is artificial with the connectionless UDP protocol)
- When the client transmits its packet to the server, it has no way to know if there actually is a service (i.e. process) listening on this port at the destination
- If not, the network (IP) layer on the server will return an ICMP "Port Unreachable" message