TCP / IP

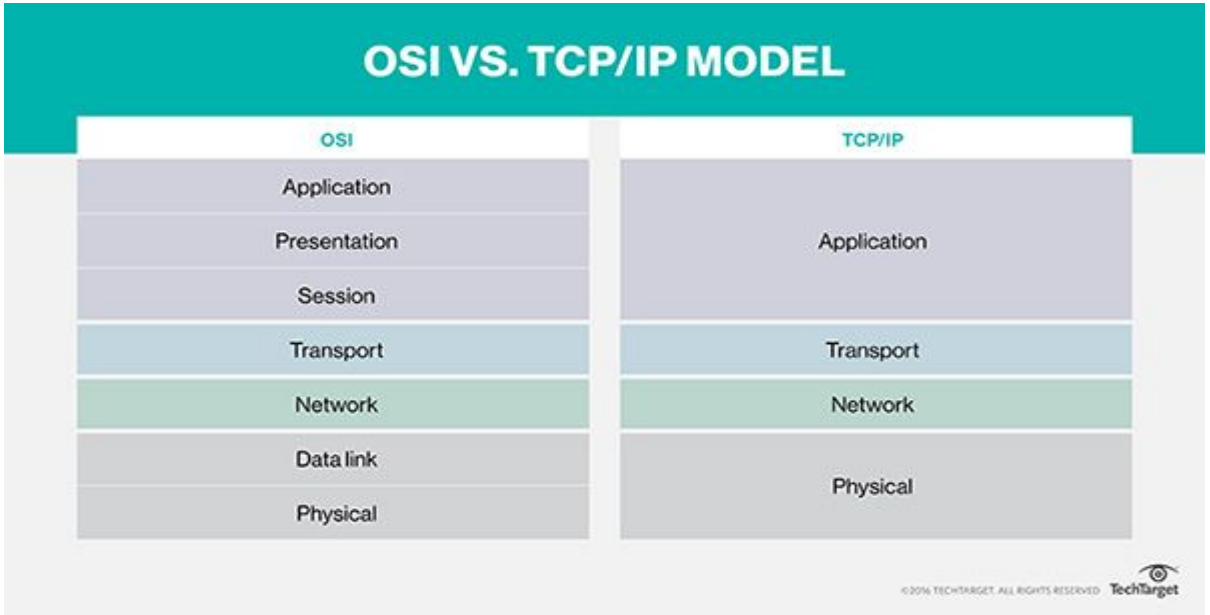
The protocol of the Internet.

TCP/IP

- Created in the 1970s by The Defense Research Project Agency (DARPA)
    - ARPANET
- ARPANET was a WAN the preceded the Internet
- TCP/IP was designed to be Robust
    - Traffic could be rerouted if there was a failure in the network

TCP/IP

- The protocol "sits" on top of an underlying Data Link protocol
  - IP Protocol is OSI Layer 3
  - Ethernet Frames are Layer 2
-

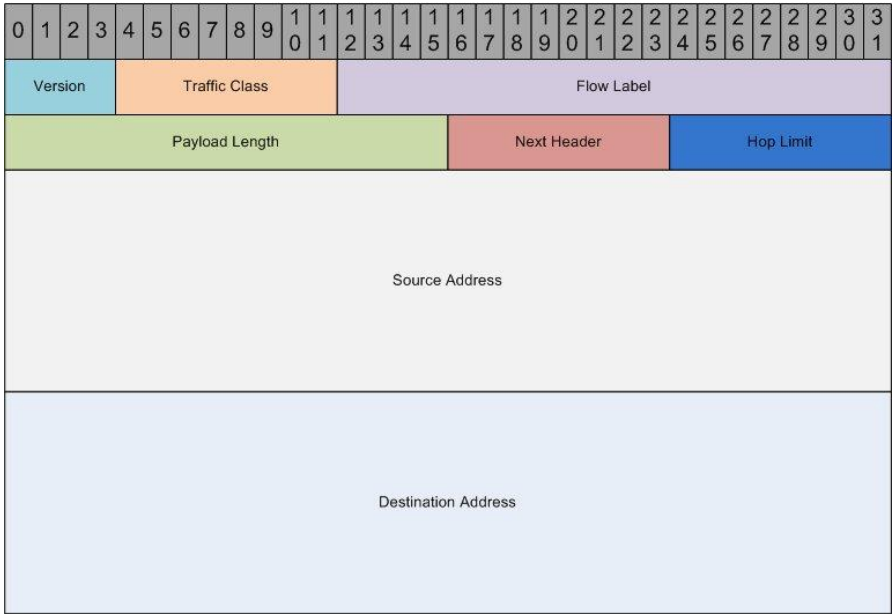


IP

- IP - Internet Protocol
- Network Layer Protocol
- Layer 3 Protocol - (OSI)
- Provides Fragmentation and reassembly of datagrams and error reporting.
- Best Effort Service
  - Loss
  - Reordering
  - Duplication
  - Delay
- IP Packets are delivered to the host (Not to the application)

IPv4 vs IPv6


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Version
Length
ToS/DSCP/ECN
Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address

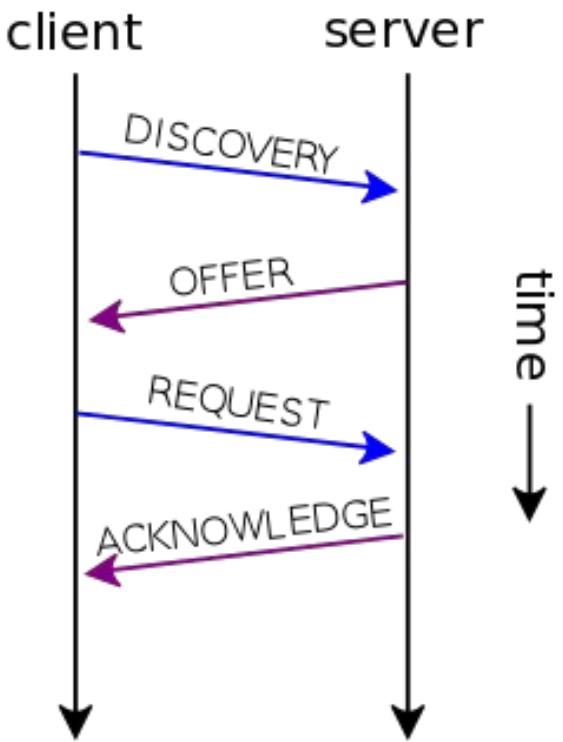
IP Address

- All hosts on the internet have at least one IP Address
  - The IP Address Identifies the host interface
  - A host may have more than one interface
- The addresses are typically presented in dotted decimal notation
  - a.b.c.d
  - 192.168.1.1
- The maximum address length is 32 bits (4 bytes or 4 octets)
- 32 bit address length means there are 2^{32} possible addresses
  - 4,294,967,296
  - Some blocks are reserved for private addresses (~18 Million)
  - Multicast addresses ~270 Million

Host Address Assignments

- Static
  - Manually assigned by user or administration
  - Need to keep track of what addresses have been assigned
  - Best for servers
- Dynamic
  - Automatically assigned at boot type
  - DHCP
    - Dynamic Host Configuration Protocol
  - Machine requests an address from DHCP server at boot time
  - DHCP server assigns and keeps track of assigned IP Addresses
    - Provides information necessary from computer to operate on the network
  - Lease Time is the amount of time a computer can keep the address before it must be renewed.
    - Shorter lease times are better on networks with transient users (ie guest networks)

DHCP

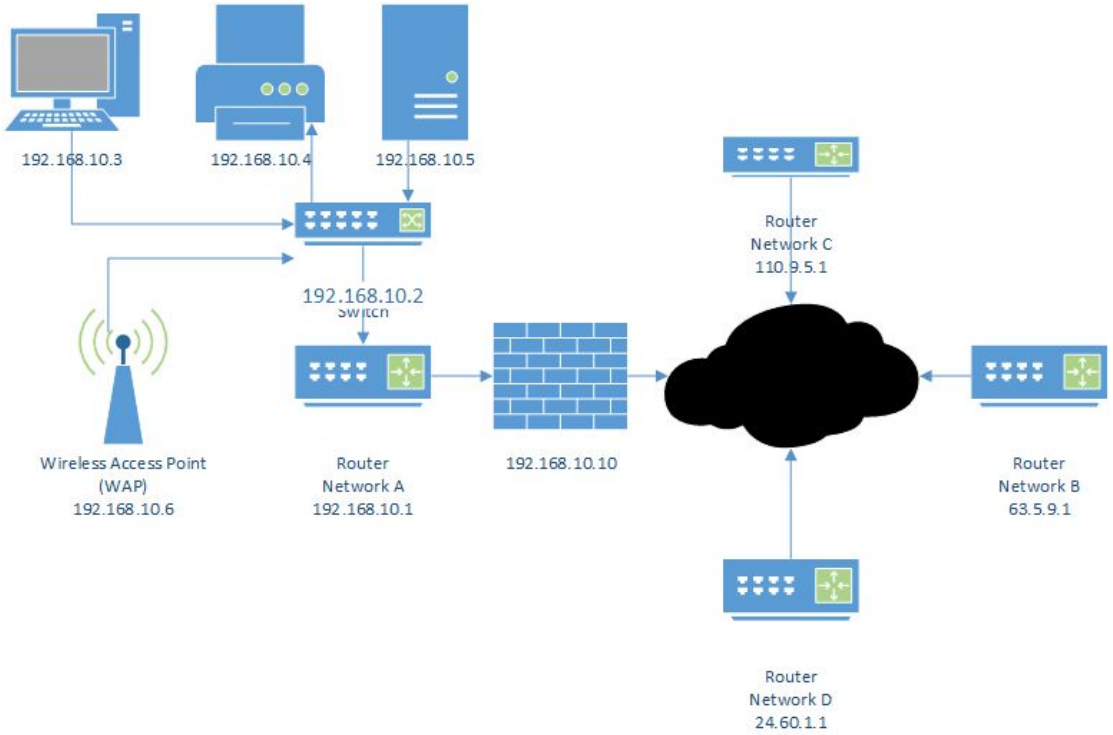


- Client machine sends a broadcast discover request on the LAN
- Server responds to client with an offer of an IP Address.
- Client sends a request back to the offering server for the IP Address
- DHCP Server responds with an Acknowledgment
- DHCP Servers listen on port 67 and respond on port 68
- At OSI layer 3 the requests and offers are broadcast.
- At layer 2, the offer is Unicast

Default Gateway or Router

- The default gateway is the router that connects your network to other networks.
- On your iPad the default gateway is a setting called router

An IP Network



Common Tools
ipconfig / ifconfig

- Use to determine IP address on computer / host
- ipconfig - Windows
- ifconfig - Most other Operating Systems

- Can you find the IP address on your iPad?
  - Take a picture of your iPad IP settings at school
  - Take a picture of your iPad IP settings at home
  - Submit them.

IP Address Subnet

- An IP address contains two parts:
  - The high order bits are the Network Address
  - The Low order bits are the Host
    - Each computer or device is a host
- The original design of IPv4 permitted a maximum of 256 network identifiers.
- The system was redesigned to have "Network Classes" or Classful Networking
  - Subnet Mask
    - Class A - 255.0.0.0 (/8)
    - Class B - 255.255.0.0 (/16)
    - Class C - 255.255.255.0 (/24)
    - Class D - Reserved for Multiclass Addresses(224.0.0.0 - 239.0.0.0)
    - Class E - Reserved (240.0.0.0)/4
- IP Address 255.255.255.255 -> Broadcast Address

IP Address Subnet
-It's about the bits

- The subnet mask setting is used to filter out the network from the host
  - 255.255.255.0 - Subnet Mask
  - 192.168.10.100 - IP Address
  - X.X.X.Y
  - Since all of the bits in the first 3 parts of the address are filtered out by the subnet mask - They are the Network Identifier - 192.168.10
  - The Host Identifier is 100
- What is the IP address of your computer?
- What is the Subnet Mask of your computer?
  - ipconfig - Windows
  - ifconfig - Unix / Linux

http://www.subnet-calculator.com/

A quick look at your subnet mask

255.255.224.0

1111 1111 . 1111 1111 . 1110 0000 . 0000 0000

N N S H H

There are 8 possible subnets where the mask matches the hosts
starting with:

000 - 192.168.0.0 - 192.168.31.255
001 - 192.168.32.0 - 192.168.63.255
010 - 192.168.64.0 - 192.168.95.255
011 - 192.168.96.0 - 192.168.127.255
100 - 192.168.128.0 - 192.168.159.255
101 - 192.168.160.0 -192.168.191.255

Common Tools
Ping / Tracert / traceroute

- Ping sends an ICMP message to a remote host to "test" if it is there.
  - Try "ping www.google.com"

- TraceRt / traceroute
  - determines the path traffic will take to get to a remote host
  - try "tracert www.google.com"
- Some systems block ICMP messages and although the server is there, you may not get a response.

DNS

- Domain Name System
- Telephone Directory of the Internet
- Used to resolve and internet host name to an IP Address
- www.kellenberg.org = 107.20.218.54
- DNS is on Port 53

Tools - nslookup

- Open a command prompt and type nslookup
  - set type=A
    - A is a host record
    - kellenberg.org
    - www.kellenberg.org
    - kmhs-media
      - Try this at home?
      - What is the IP Address when you try at home?
  - set type=mx
    - mx is Mail Exchanger - the server that processes email
    - look up kellenberg.org mx record

IP / DHCP / DNS

- We've covered three protocols so far
  - IP
    - Internet Protocol - Layer 3 on the OSI model (layer two on the TCP/IP Model)
  - DNS
    - Domain Name System
    - Resolves Host Names to IP Addresses
    - DNS Servers Listen on Port 53
  - DHCP
    - Dynamic Host Configuration Protocol
    - Clients are automatically assigned an IP Address

*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

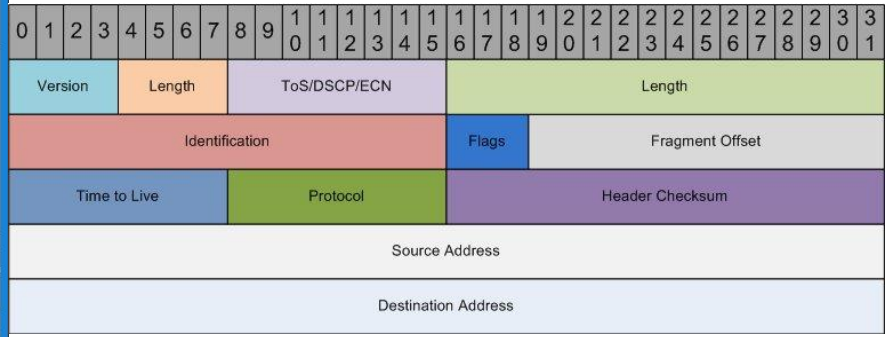
Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination
1	0.000000	Micro-St_85:e4:c7	Broadcast
2	0.012644	BrocadeC_2f:a3:c0	cf:4e:24:2f:a3:c0
3	0.051700	HewlettP_3f:ed:4d	Broadcast
4	0.207632	52.55.206.11	192.168.8.67
5	0.207632	52.55.206.11	192.168.8.67
6	0.207693	192.168.8.67	52.55.206.11
7	0.207790	192.168.8.67	52.55.206.11
8	0.207838	192.168.8.67	52.55.206.11
9	0.211443	192.168.8.67	52.55.206.11
10	0.220193	52.55.206.11	192.168.8.67
11	0.220231	192.168.8.67	52.55.206.11
12	0.223466	52.55.206.11	192.168.8.67
13	0.223546	192.168.8.67	52.55.206.11
14	0.223843	192.168.8.67	52.55.206.11
15	0.235986	52.55.206.11	192.168.8.67
16	0.235987	52.55.206.11	192.168.8.67
17	0.236497	192.168.8.67	52.55.206.11
18	0.236753	192.168.8.67	52.55.206.11
19	0.247198	fe80::e9db:164b:8d9a:4e2e	ff02::1:2
20	0.248548	52.55.206.11	192.168.8.67
21	0.292169	HewlettP_3f:ed:4c	Broadcast

> Frame 8: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: Microsof_96:3b:79 (58:82:a8:96:3b:79), Dst: BrocadeC_91:ac:6c (74:8e:f8:91:ac:6c)
> Internet Protocol Version 4, Src: 192.168.8.67, Dst: 52.55.206.11
> Transmission Control Protocol, Src Port: 51867, Dst Port: 443, Seq: 32, Ack: 342, Len: 0

```
0000  74 8e f8 91 ac 6c 58 82  a8 96 3b 79 08 00 45 00   t....lX. ..;y..E.
0010  00 28 50 4d 40 00 80 06  00 00 c0 a8 08 43 34 37   .(PM@... .....C47
0020  ce 0b ca 9b 01 bb 9c 73  55 f7 53 a3 62 c6 50 11   .......s U.S.b.P.
0030  00 fe cb 48 00 00                                  ...H..
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 30 · Displayed: 30 (100.0%) | Profile: AirPCap



Netstat

- Netstat is a command we issue to see what sessions are open on our computer as well as what ports processes are listening on
  - netstat
  - netstat -a
  - netstat -o

There's no place like 127.0.0.1

Remember - IP Packets

- IP - Internet Protocol
- Network Layer Protocol
- Layer 3 Protocol - (OSI)
- Provides Fragmentation and reassembly of datagrams and error reporting.
- Best Effort Service
  - Loss
  - Reordering
  - Duplication
  - Delay
- IP Packets are delivered to the host (Not to the application)

Now we need to move data

Transport Protocols on top of IP (Layer 4 of OSI Model)

- User Datagram Protocol (UDP)
  - Data Checksum
  - Best-Effort
- Transmission Control Protocol (TCP)
  - Data Checksum
  - Reliable byte-stream delivery
  - Flow and Congestion Control

Ports

- Ports identify the destination Application of the packets / datagram
- A host may have several applications listening on different ports
  - Two applications may not listen on same port
- Port is a 16 bit (2 byte) identifier in the TCP or UDP header
  - port 0 - 65535
- Well Known Ports
  - 25 - SMTP - eMail
  - 80 - http - www
  - 443 - https - secure www
  - 23 - Telnet
  - https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Netstat - Review

- Netstat is a command we issue to see what sessions are open on our computer as well as what ports processes are listening on
  - netstat
  - netstat -a
  - netstat -o

  - https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
    - Netstat -a > netstat.txt
    - Use the list of well known ports, identify all ports under 3000
    - Submit via eBackpack