CS 447/647

TCP/IP Networking

```
###[ Ethernet ]###
  dst       = FF:FF:FF:FF:FF:FF
  src       = aa:00:00:fb:6c:78
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = aa:00:00:fb:6c:78
     psrc      = 10.0.120.199
     hwdst     = 00:00:00:00:00:00
     pdst      = 10.0.120.1
```

News

Over 20 thousand servers have their iLO interfaces exposed to the internet, many with outdated and vulnerable versions of FW

Published: 2022-01-26

"A lot of devices and services we have seen during our research ***should never be connected to the public Internet at all***. As a rule of thumb, if you believe that "nobody would connect that to the Internet, really nobody", there are at least 1000 people who did. Whenever you think "that shouldn't be on the Internet but will probably be found a few times" it's there a few hundred thousand times. Like half a million printers, or a Million Webcams, or devices that have root as a root password."

http://census2012.sourceforge.net/paper.html

Hard Pass
@HardPass4

Hey @TraegerGrills - who the HELL sends a software update on thanksgiving?!?

7:03 AM · Nov 25, 2021

Read the full conversation on Twitter

9.7K Reply Share

Read 657 replies

What are the core Internet Protocols? (IP, ICMP, UDP, and ARP)

How is the Internet governed? (ICANN, ISOC and IGF)

How are standards developed? (RFC)

What are the 5 layers of the TCP/IP Model?

References

Goralski, W. (2017). The Illustrated Network: How TCP/IP works in a modern network. Amsterdam: Elsevier.

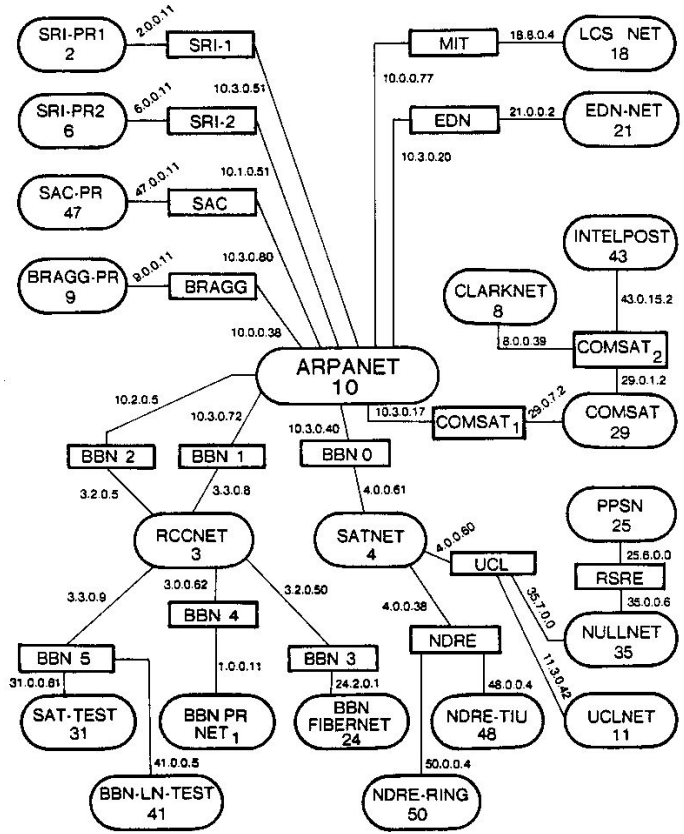
https://learning.oreilly.com/library/view/the-illustrated-network/9780128110287

TCP/IP Networking

- TCP/IP underpins the Internet
  - Web
  - Email
  - Zoom (TCP+UDP)
- TCP/IP is flexible
  - OS Independent
  - Hardware Independent
  - Works on any size or topology

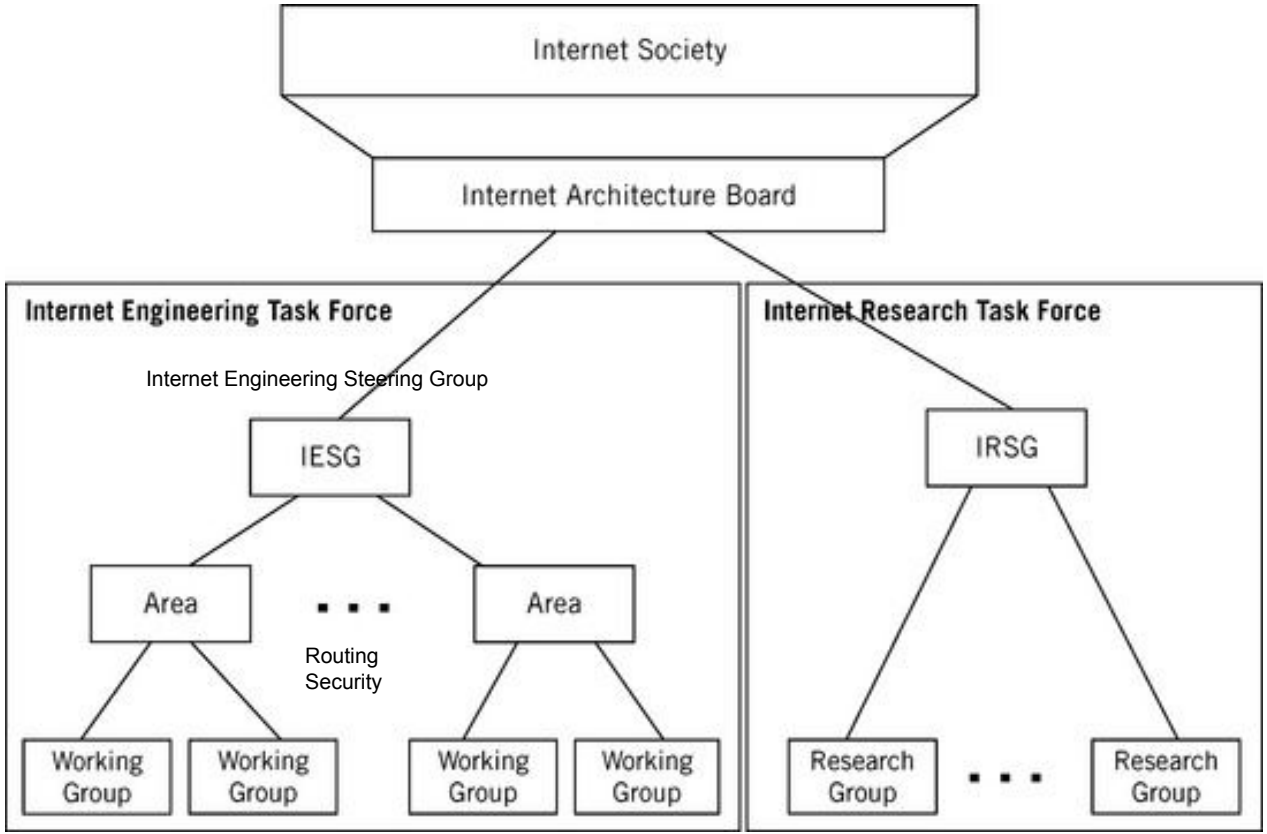
TCP/IP Networking & The Internet

- TCP/IP and the Internet have a shared history
  - TCP was created in 1974 by Vint Cerf
    - https://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf
- Progenitor was a network called ARPANET in 1969
  - In the 1980's in transitioned into the commercial Internet
- Collaboratively Managed
  - ICANN - Internet Corporation for Assigned Names and Numbers
    - Enforcement Capabilities
    - Controls the allocation of IPs, domains and protocol ports.
  - ISOC - Internet Society
    - Technical development through IETF - Internet Engineering Task Force
  - IGF - Internet Governance Forum
    - Created by the UN.
    - Used for policy-based discussions


SRI-PR1
2
2.0.0.11
SRI-1
SRI-PR2
6
6.0.0.11
SRI-2
SAC-PR
47
47.0.0.11
SAC
BRAGG-PR
9
9.0.0.11
BRAGG
10.3.0.51
10.1.0.51
10.3.0.80
10.0.0.38
ARPANET
10
MIT
18.8.0.4
LCS NET
18
10.0.0.77
EDN
21.0.0.2
EDN-NET
21
10.3.0.20
INTELPOST
43
CLARKNET
8
43.0.15.2
8.0.0.39
COMSAT 2
29.0.1.2
COMSAT
29
29.0.7.2
10.3.0.17
COMSAT 1
10.2.0.5
10.3.0.72
10.3.0.40
BBN 2
BBN 1
BBN 0
3.2.0.5
3.3.0.8
4.0.0.61
RCCNET
3
SATNET
4
4.0.0.60
UCL
PPSN
25
25.6.0.0
RSRE
35.0.0.6
NULLNET
35
35.7.0.0
11.3.0.42
UCLNET
11
3.3.0.9
3.0.0.62
3.2.0.50
4.0.0.38
BBN 4
NDRE
BBN 5
BBN 3
31.0.0.61
1.0.0.11
24.2.0.1
48.0.0.4
SAT-TEST
31
BBN PR
NET 1
BBN
FIBERNET
24
NDRE-TIU
48
41.0.0.5
50.0.0.4
BBN-LN-TEST
41
NDRE-RING
50

Internet Governance

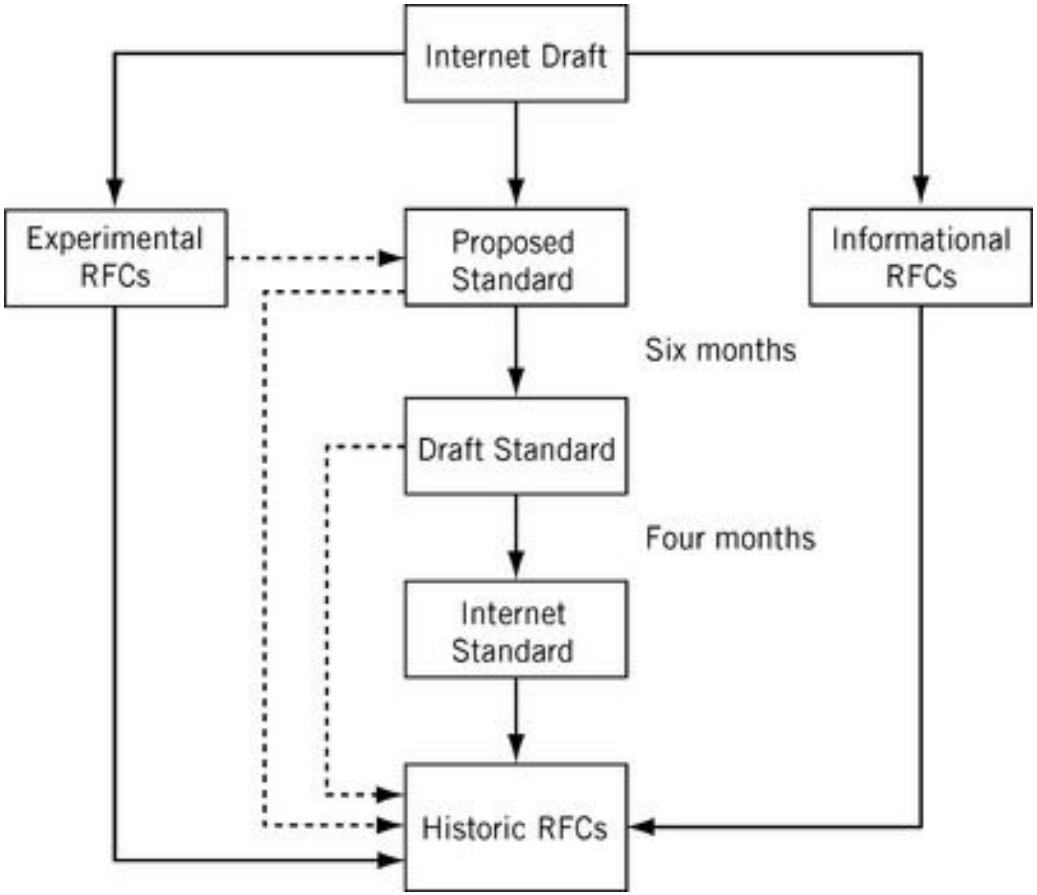
- Collaboratively Managed
  - ICANN - Internet Corporation for Assigned Names and Numbers
    - Enforcement Capabilities
    - Controls the allocation of IPs, domains and protocol ports.
  - ISOC - Internet Society
    - Technical development through IETF - Internet Engineering Task Force
  - IGF - Internet Governance Forum
    - Created by the UN.
    - Used for policy-based discussions

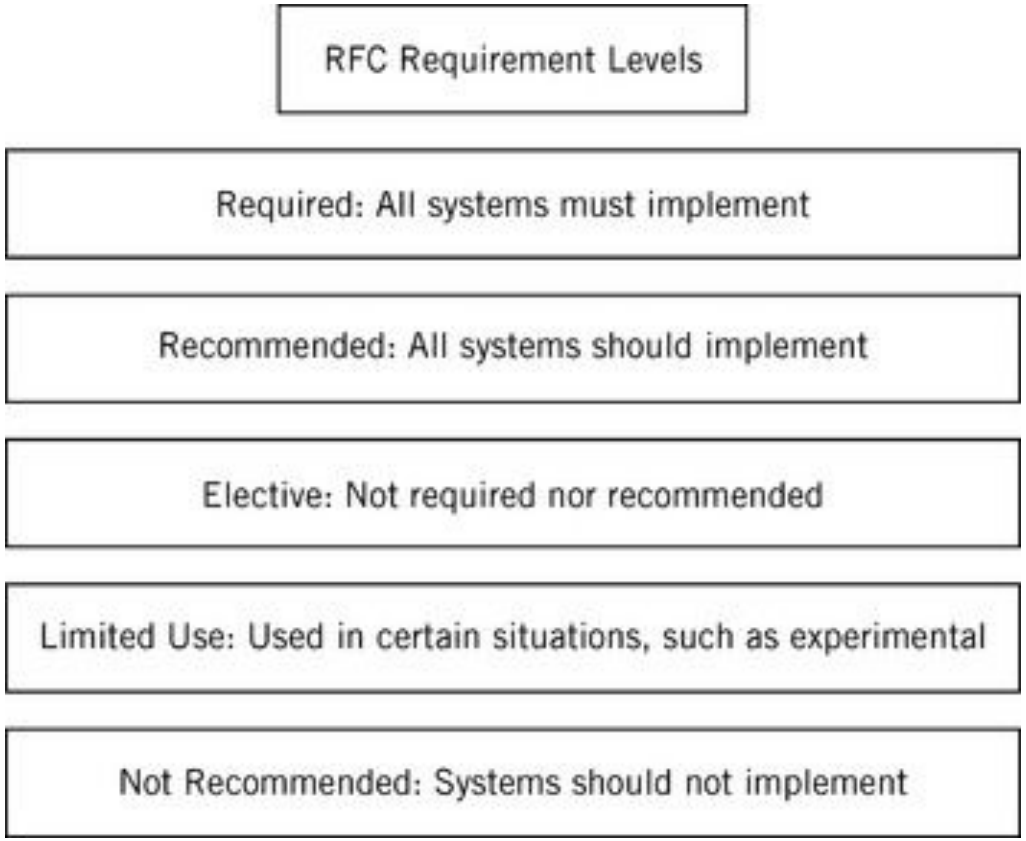


https://datatracker.ietf.org/wg/

Network standards and documentation

- RFCs - Request for Comments
  - Protocol Standards
    - TFTP, SMTP, HTTP, DNS, etc.
  - Proposed Changes
    - SMTP Require TLS Option - REQUIRETLS
      - https://www.rfc-editor.org/rfc/rfc8689.txt
  - Informational Bulletins
    - 50 years of RFCs
      - https://www.rfc-editor.org/rfc/rfc8700.txt
- RFCs can be assigned
  - BCP - Best Current Practice
    - Network Time Protocol Best Current Practices
  - STD - Standard
  - FYI - For Your Information

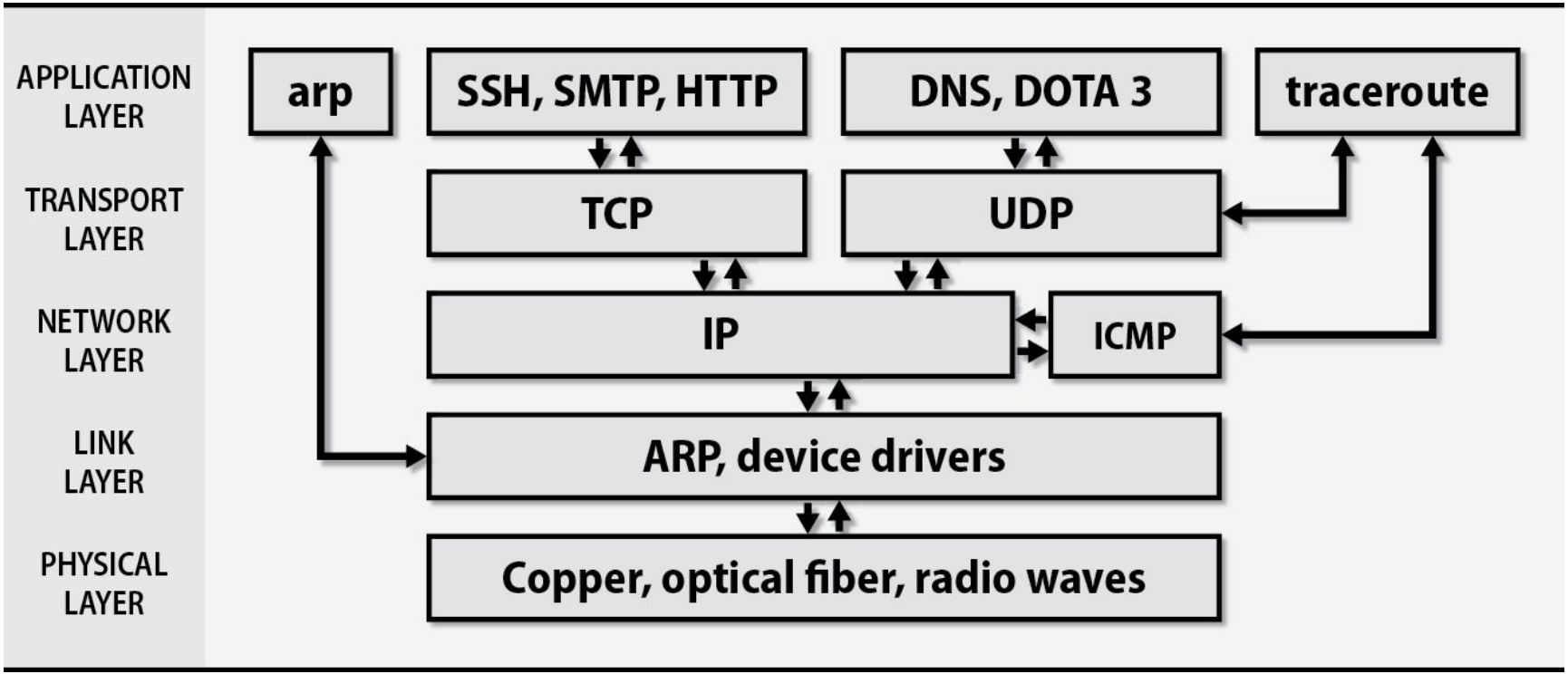

Internet Draft
Experimental RFCs
Proposed Standard
Informational RFCs
Six months
Draft Standard
Four months
Internet Standard
Historic RFCs

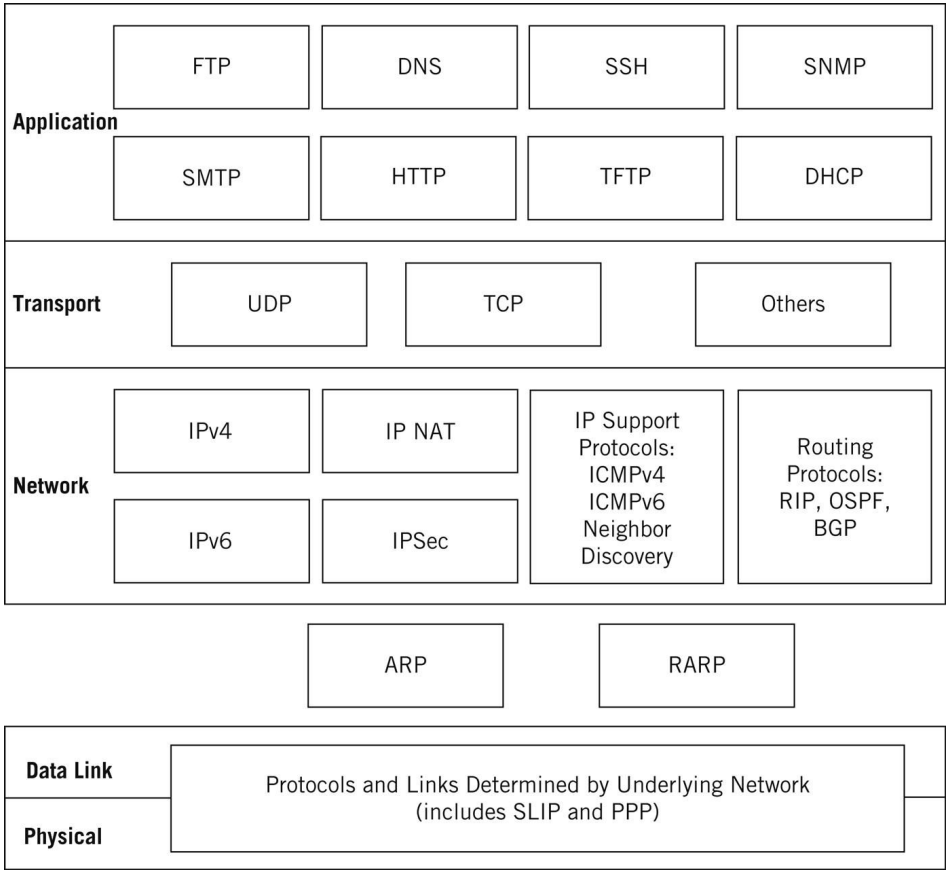

RFC Requirement Levels
Required: All systems must implement
Recommended: All systems should implement
Elective: Not required nor recommended
Limited Use: Used in certain situations, such as experimental
Not Recommended: Systems should not implement

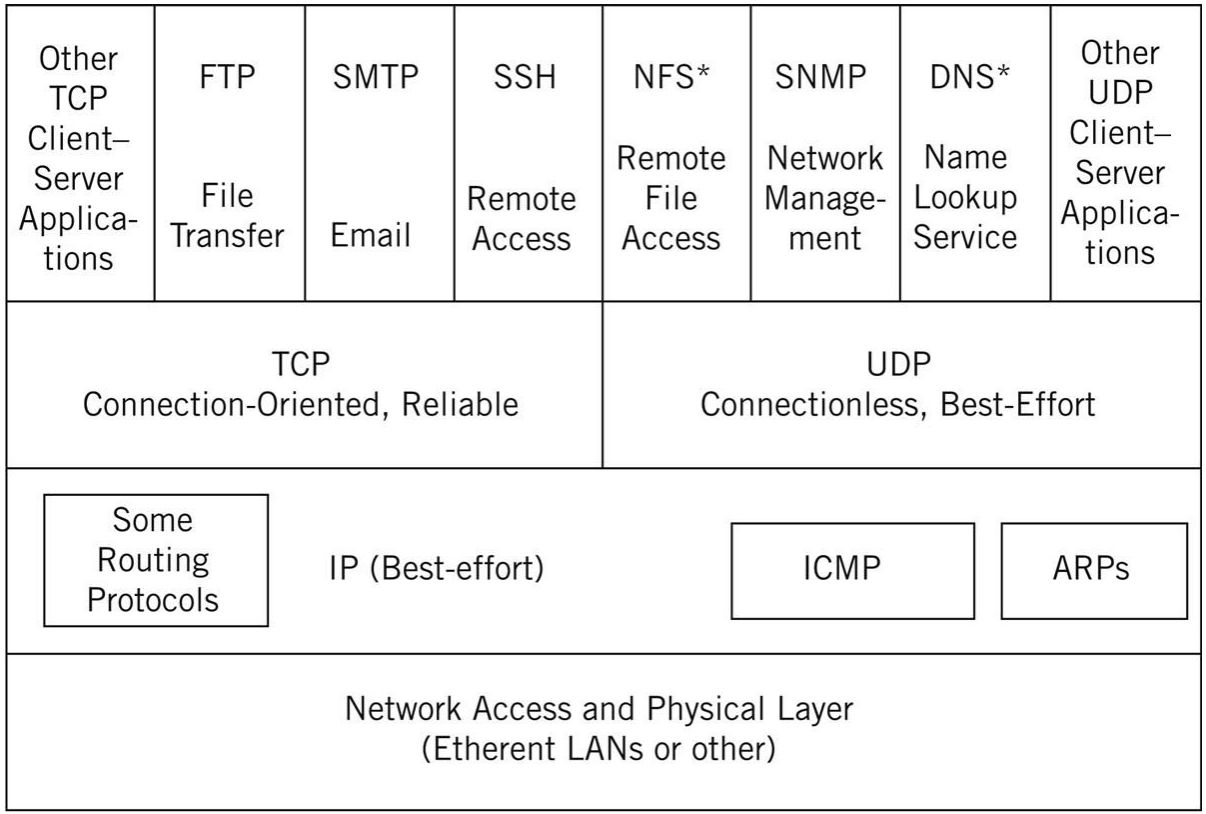
Networking Basics - Protocol Suite

- IP - Internet Protocol
  - Routes data from one machine to another
- ICMP - Internet Control Message Protocol
  - Low-level support for IP error message, routing and debugging
  - ping, traceroute
- ARP - Address Resolution Protocol
  - Translates IP to hardware address (MAC)
- UDP - User Datagram Packet
  - Unreliable one-way delivery
- TCP - Transmission Control Protocol
  - Reliable full-duplex and error corrected conversations

TCP/IP Layering model




Application
FTP
DNS
SSH
SNMP
SMTP
HTTP
TFTP
DHCP
Transport
UDP
TCP
Others
Network
IPv4
IP NAT
IP Support Protocols: ICMPv4 ICMPv6 Neighbor Discovery
Routing Protocols: RIP, OSPF, BGP
IPv6
IPSec
ARP
RARP
Data Link
Physical
Protocols and Links Determined by Underlying Network (includes SLIP and PPP)



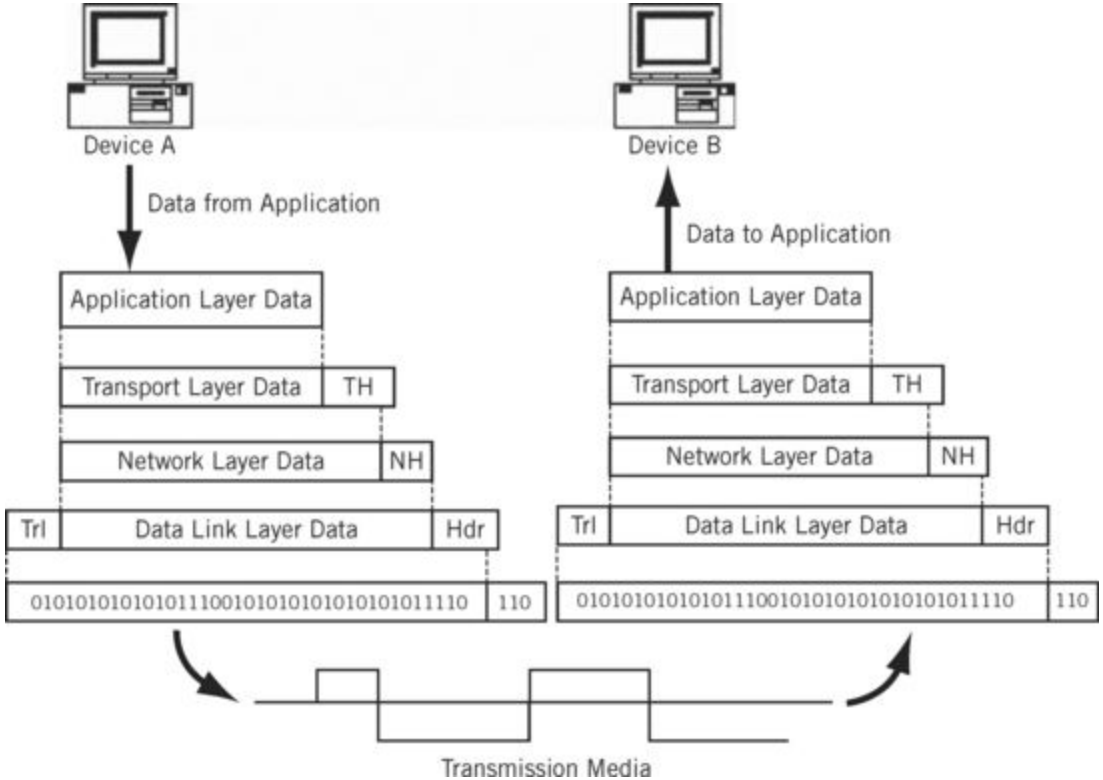
*In some instances, NFS and DNS use TCP.

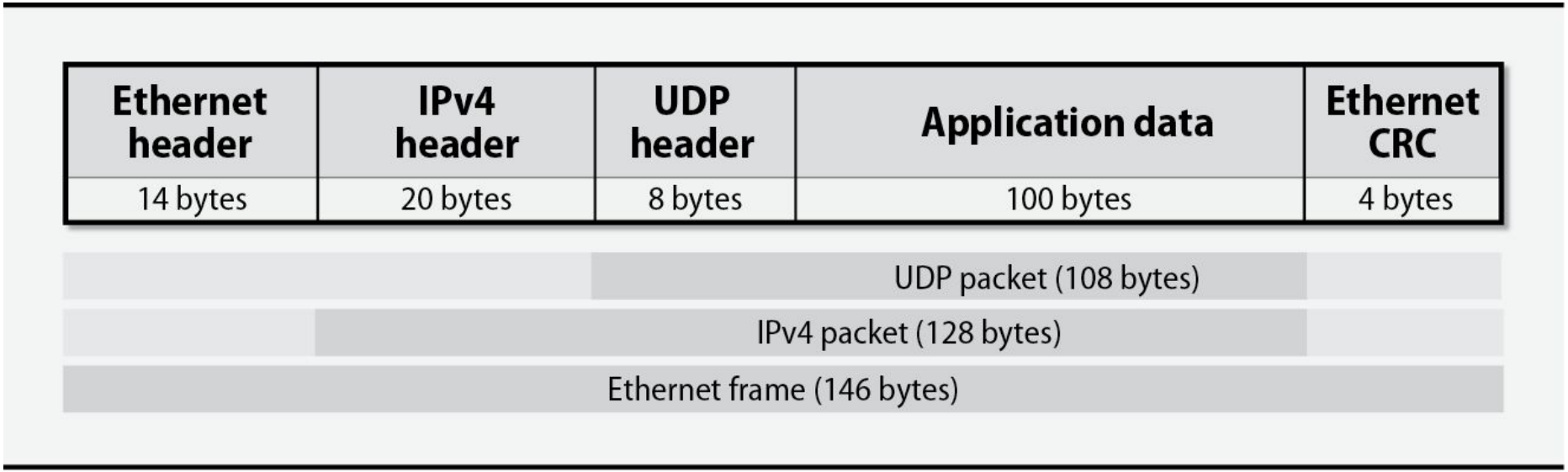
IPv4 and IPv6

- IPv4
  - 32 bit addresses
  - 4,294,967,296 addresses
  - NAT - Network Address Translation
- IPv6
  - 128 bit addresses
  - IPsec - built in authentication and encryption
  - No checksum
  - 30% of google.com visits
- Adoption of IPv6 is slow
  - Amazon, Bing, Wordpress, craigslist
  - Waiting for services to be IPv6 only
  - Cleaned up version of IPv4
    - Python2
      - 2010 to 2020

Packet Encapsulation

- Hardware
  - Ethernet, token ring, Infiniband, Omni-path
- Data travels as packets
  - Max length is dictated by the link layer (2)
  - Packet header has source and destination
  - Checksums, protocol options
  - Handling instructions (TTL)
  - Payload
- Encapsulation
  - Packets are added to by each layer by the sender
  - Each layer is removed by the receiver

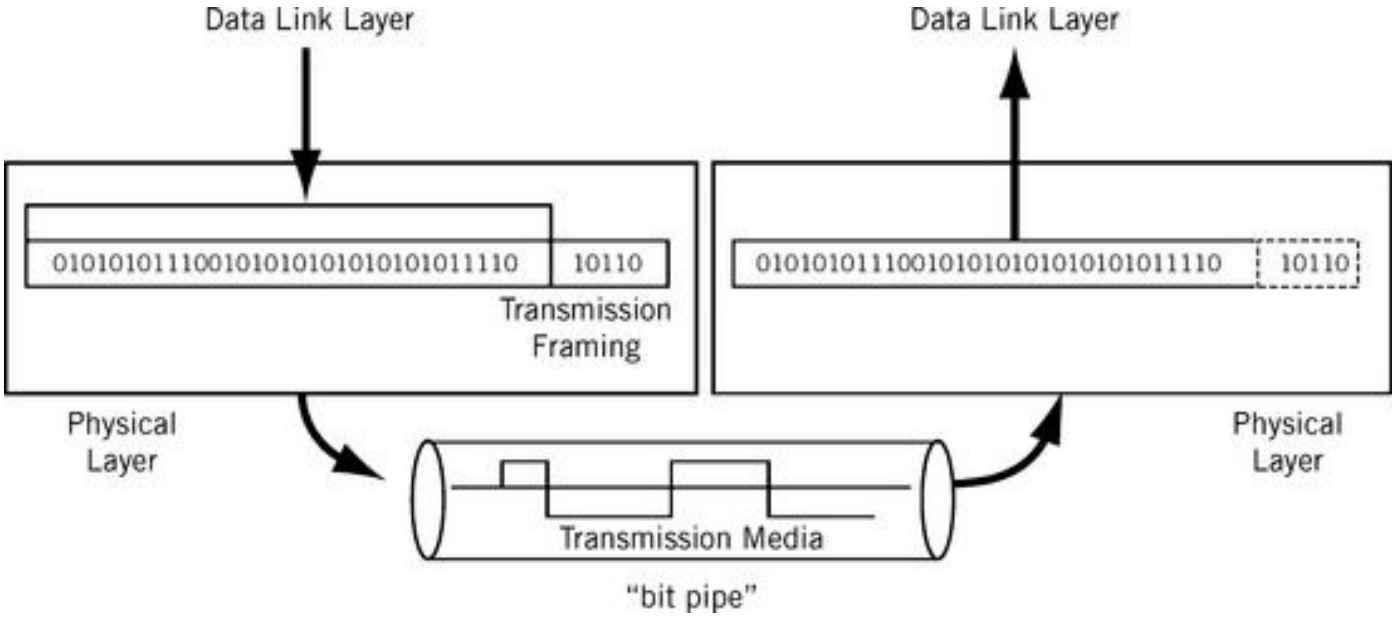

Device A
Device B
Data from Application
Data to Application
Application Layer Data
Transport Layer Data
TH
Network Layer Data
NH
Trl
Data Link Layer Data
Hdr
0101010101010111001010101010101011110
110
Transmission Media


Ethernet header
IPv4 header
UDP header
Application data
Ethernet CRC
14 bytes
20 bytes
8 bytes
100 bytes
4 bytes
UDP packet (108 bytes)
IPv4 packet (128 bytes)
Ethernet frame (146 bytes)

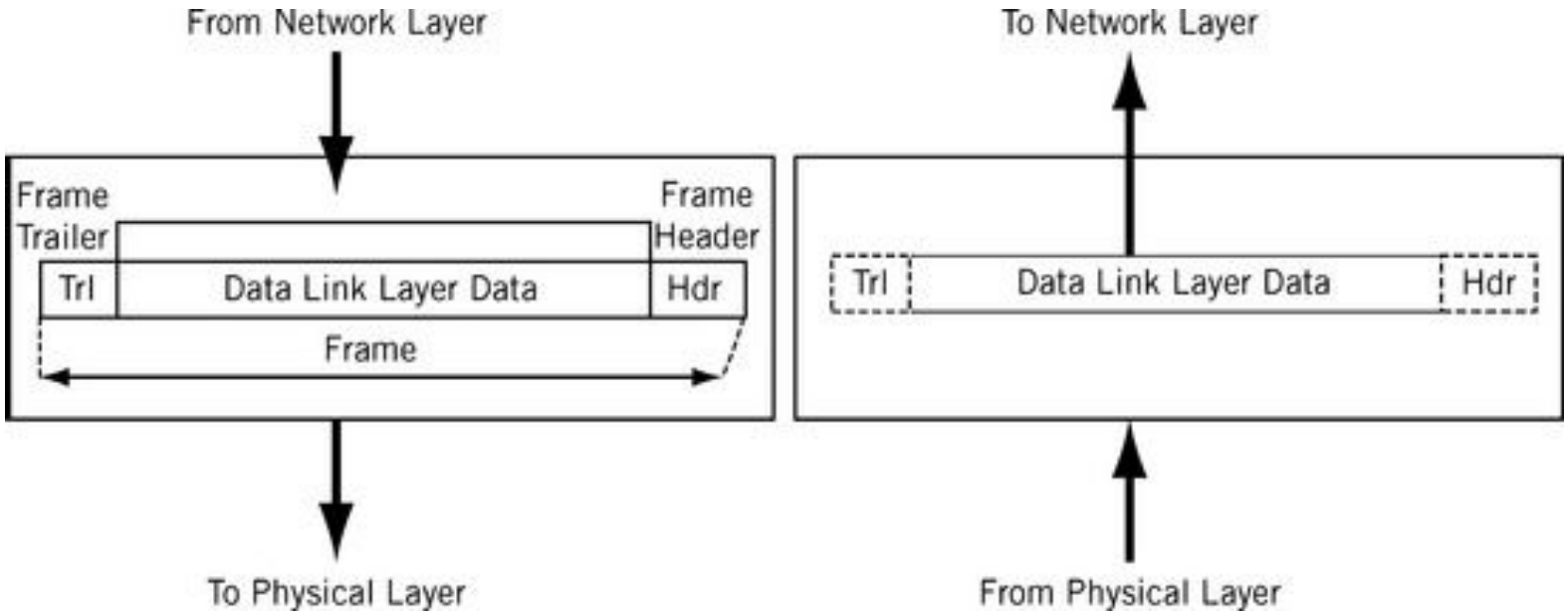
Ethernet Framing

- Adding extra bits to a packet
- Link layer adds headers to packets
  - Header contains addresses
  - Checksums
- Link layer adds separators between packets
- Two parts of link layer
  - Media Access Control - Deals with hardware, puts packets onto the wire
  - Logical Link Control - Ethernet framing

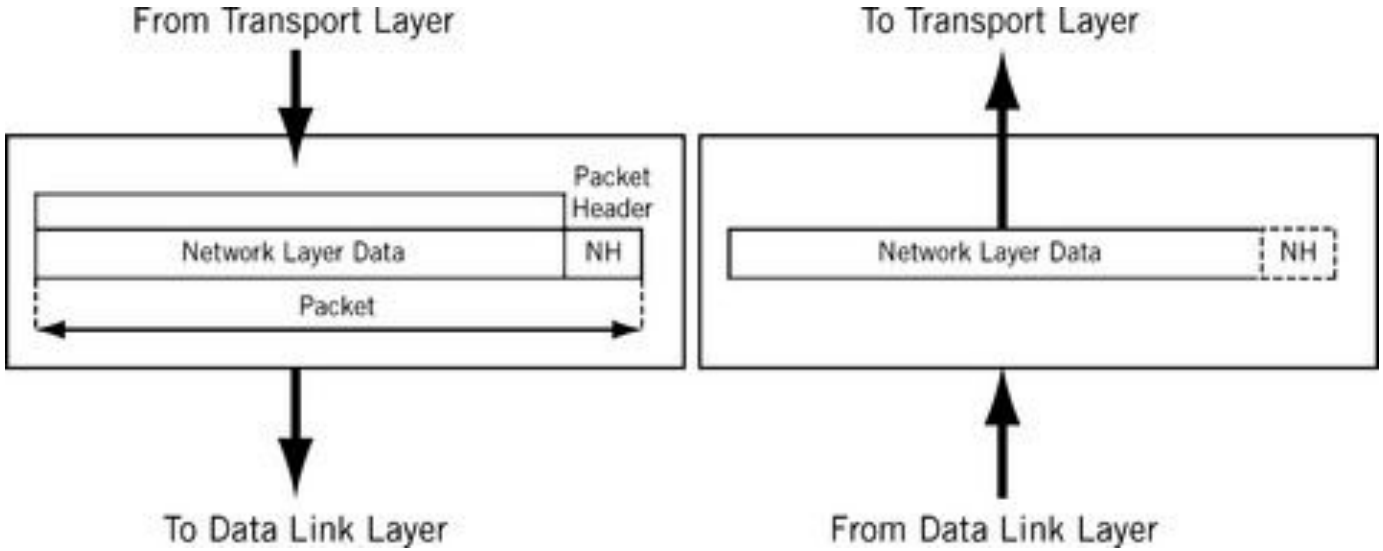
Physical


Data Link Layer
Data Link Layer
01010101110010101010101010111110
10110
Transmission
Framing
01010101110010101010101010111110
10110
Physical
Layer
Physical
Layer
Transmission Media
"bit pipe"

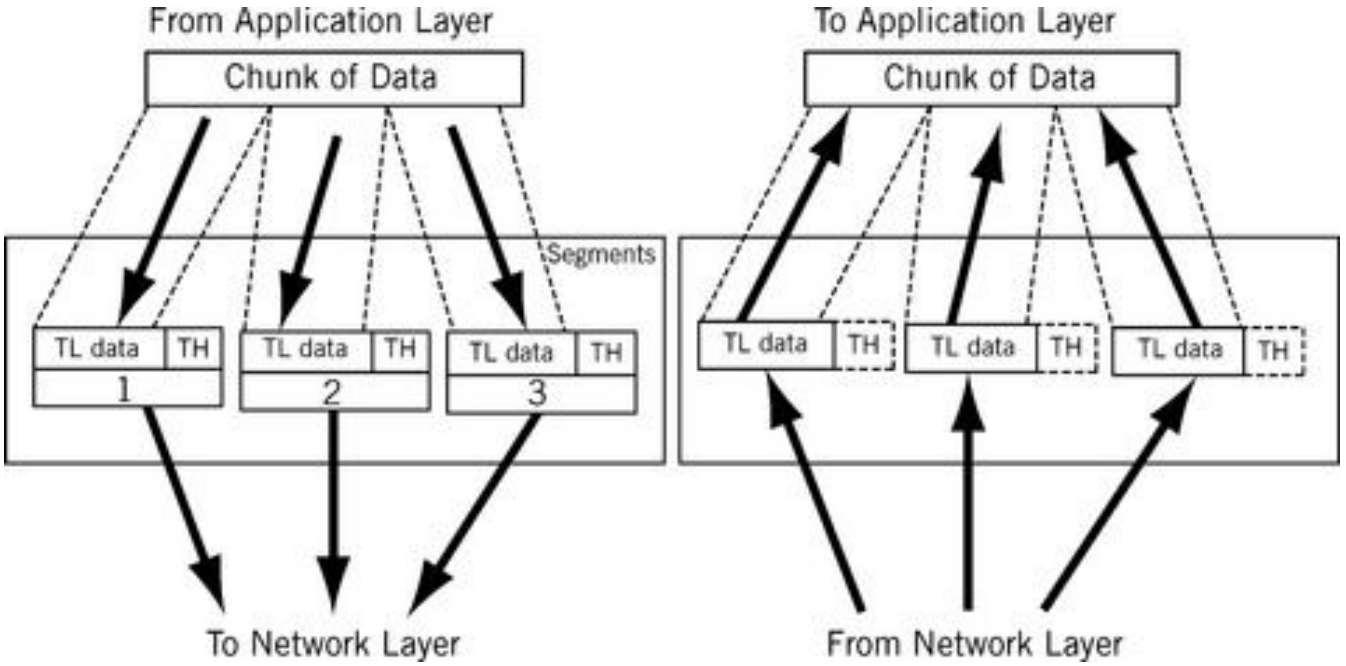
Data Link


From Network Layer
Frame
Trailer
Frame
Header
Trl
Data Link Layer Data
Hdr
Frame
To Physical Layer
To Network Layer
Trl
Data Link Layer Data
Hdr
From Physical Layer

Network


From Transport Layer
Packet Header
Network Layer Data
NH
Packet
To Data Link Layer
To Transport Layer
Network Layer Data
NH
From Data Link Layer

Transport


From Application Layer
Chunk of Data
Segments
TL data
TH
1
TL data
TH
2
TL data
TH
3
To Network Layer
To Application Layer
Chunk of Data
TL data
TH
TL data
TH
TL data
TH
From Network Layer

Maximum Transfer Unit

- Packet size is limited
  - Hardware
    - E1000 - 16,298 bytes
  - Protocol
    - Ethernet - 1500 bytes

Network type	Maximum transfer unit
Ethernet	1,500 bytes (1,492 with 802.2 framing)
IPv6 (all hardware)	At least 1,280 bytes at the IP layer
Token ring	Configurable [a]
Point-to-point WAN links (T1, T3)	Configurable, often 1,500 or 4,500 bytes

a. Common values are 552; 1,064; 2,088; 4,508; and 8,232. Sometimes 1,500 to match Ethernet.

MTU

- IPv4 Packets are split to conform to the MTU
  - Test with
    - ping -s 4500 google.com
- Fragmentation happens in-flight by routers
  - IPv6 moves this to the sender
- Lowest MTU link can be found with “do not fragment” flag
  - ICMP error response
    - Contains network info for lowest-MTU link
- TCP does automatic MTU discover
  - UDP does not

Packet Addressing

- MAC Address
  - Hardware
- IPv4 and IPv6 addresses
  - Software
- **Hostnames**
  - Humans

Hostnames

- Domain Name System (DNS)
  - A - IPv4
  - AAAA - IPv6
  - PTR - IP to Hostname aka. Reverse lookup
- /etc/hosts (Windows: C:\Windows\System32\drivers\etc\hosts)
  - *IP hostname hostname1 hostname2*
- Lookup with dig
  - dig A google.com
  - dig A cse.unr.edu @8.8.8.8
  - dig A cse.unr.edu @134.197.5.1

Ports

- IP is an address. IE: 127.0.0.1
- Port is a communication channel for an application
  - 1 - 65,535
- IP + Port = Socket
  - 127.0.0.1:80 = HTTP
- /etc/services defines common network services
  - grep daytime /etc/services
- Ports < 1024 reserved for root

IPv4 Address Classes

Class	1st byte[a]	Format	Comments
A	1-127	N.H.H.H	Very early networks, or reserved for DoD
B	128-191	N.N.H.H	Large sites, usually subnetted, were hard to get
C	192-223	N.N.N.H	Were easy to get, often obtained in sets
D	224-239	–	Multicast addresses, not permanently assigned
E	240-255	–	Experimental addresses

a. The value 0 is special and is not used as the first byte of regular IP addresses. The value 127 is reserved for the loopback address.

IPv4 Subnetting

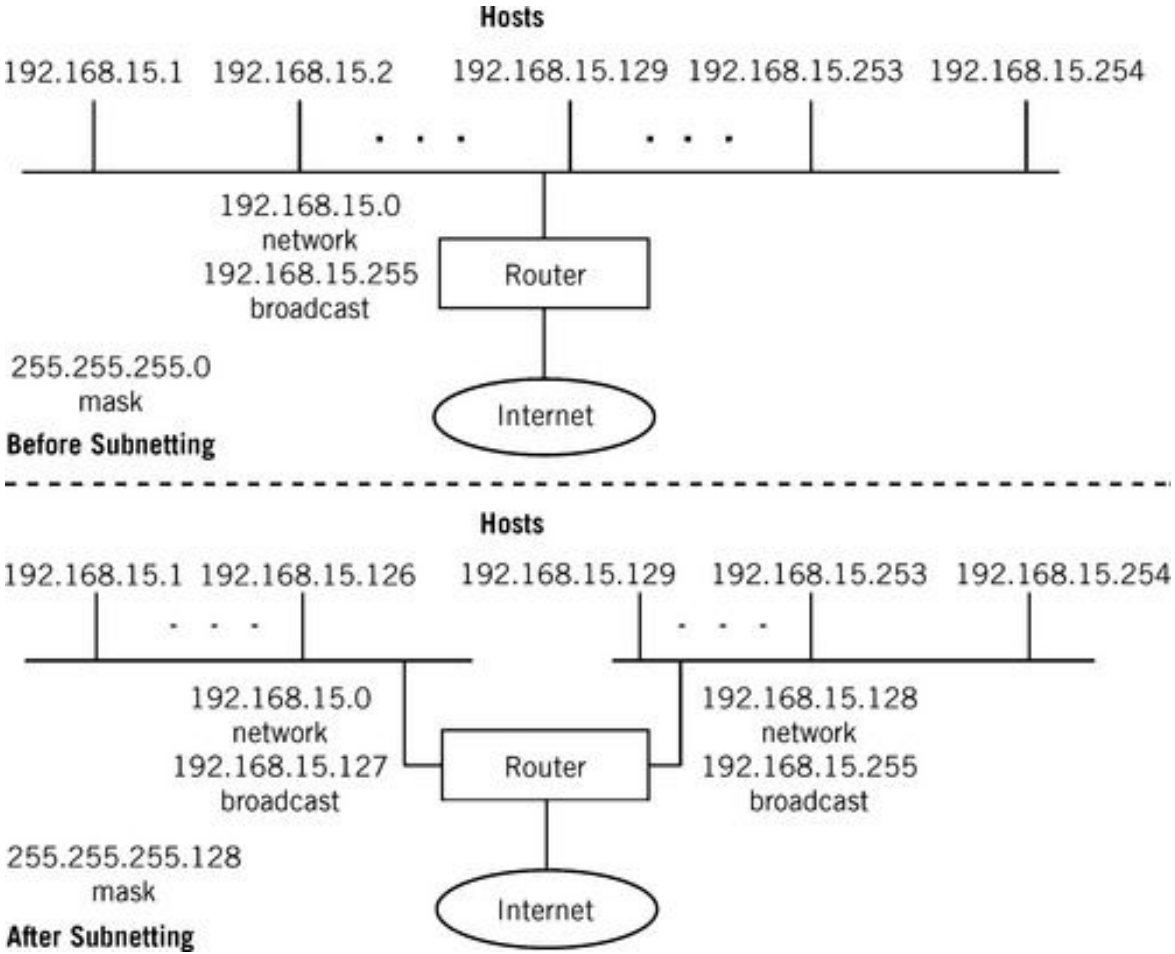
Class A	Network	Host	Host	Host	CIDR
Subnet Mask	255	0	0	0	/8

Class B	Network	Network	Host	Host	CIDR
Subnet Mask	255	255	0	0	/16

Class C	Network	Network	Network	Host	CIDR
Subnet Mask	255	255	255	0	/24

IP address	Netmask	Network	Broadcast
128.138.243.100/16	255.255.0.0	128.138.0.0	128.138.255.255
128.138.243.100/24	255.255.255.0	128.138.243.0	128.138.243.255
128.138.243.100/26	255.255.255.192	128.138.243.64	128.138.243.127

192 = 1100 0000


Hosts
192.168.15.1
192.168.15.2
192.168.15.129
192.168.15.253
192.168.15.254
192.168.15.0
network
192.168.15.255
broadcast
Router
255.255.255.0
mask
Internet
Before Subnetting
Hosts
192.168.15.1
192.168.15.126
192.168.15.129
192.168.15.253
192.168.15.254
192.168.15.0
network
192.168.15.127
broadcast
192.168.15.128
network
192.168.15.255
broadcast
Router
255.255.255.128
mask
Internet
After Subnetting

IPv4 Subnetting

apt install ipcalc

```
root@cs447-newellz2-server ~# ipcalc 192.168.15.0/25
Address:   192.168.15.0          11000000.10101000.00001111.0 0000000
Netmask:   255.255.255.128 = 25  11111111.11111111.11111111.1 0000000
Wildcard:  0.0.0.127             00000000.00000000.00000000.0 1111111
=>
Network:   192.168.15.0/25       11000000.10101000.00001111.0 0000000
HostMin:   192.168.15.1          11000000.10101000.00001111.0 0000001
HostMax:   192.168.15.126        11000000.10101000.00001111.0 1111110
Broadcast: 192.168.15.127        11000000.10101000.00001111.0 1111111
Hosts/Net: 126                    Class C, Private Internet
```

Classless Inter-Domain Routing (CIDR)

- Splitting networks for routing purposes
- Example

Site has been given a block of eight class C addresses numbered 192.144.0.0 through 192.144.7.0

- 1 network of length /21 with 2,046 hosts, netmask 255.255.248.0
- 8 networks of length /24 with 254 hosts each, netmask 255.255.255.0
- 16 networks of length /25 with 126 hosts each, netmask 255.255.255.128
- 32 networks of length /26 with 62 hosts each, netmask 255.255.255.192

Address Allocation

Name	Site	Region covered
ARIN	arin.net	North America, part of the Caribbean
APNIC	apnic.net	Asia/Pacific region, including Australia and New Zealand
AfriNIC	afrinic.net	Africa
LACNIC	lacnic.net	Central and South America, part of the Caribbean
RIPE NCC	ripe.net	Europe and surrounding areas

Special forms of IPv4 Addressing

Special Address	NetID	HostID	Example	Use
Network itself	Non-0	All zeros (0s)	192.168.14.0	Used by routers: on a host, means "some host," but it is not used.
Directed broadcast	Non-0	All ones (1s)	192.168.14.255	Destination only: used by routers to send to all host on this network.
Limited broadcast	All 1s	All 1s	225.255.255.255	Destination only: direct broadcast when NetID is not known.
This host on this network	All 0s	All 0s	0.0.0.0	Source only: used when host does not know its IPv4 address.
Specific host on this network	All 0s	Non-0	0.0.0.46	Destination only: defined, but not used
Loopback	127	Any	127.0.0.0	Destination only: packet is not sent out onto network.

Network Address Translation

- Made to deal with IPv4 exhaustion
- Private address spaces
- Border router translates between private and public

IP class	From	To	CIDR range
Class A	10.0.0.0	10.255.255.255	10.0.0.0/8
Class B	172.16.0.0	172.31.255.255	172.16.0.0/12
Class C	192.168.0.0	192.168.255.255	192.168.0.0/16

Routing

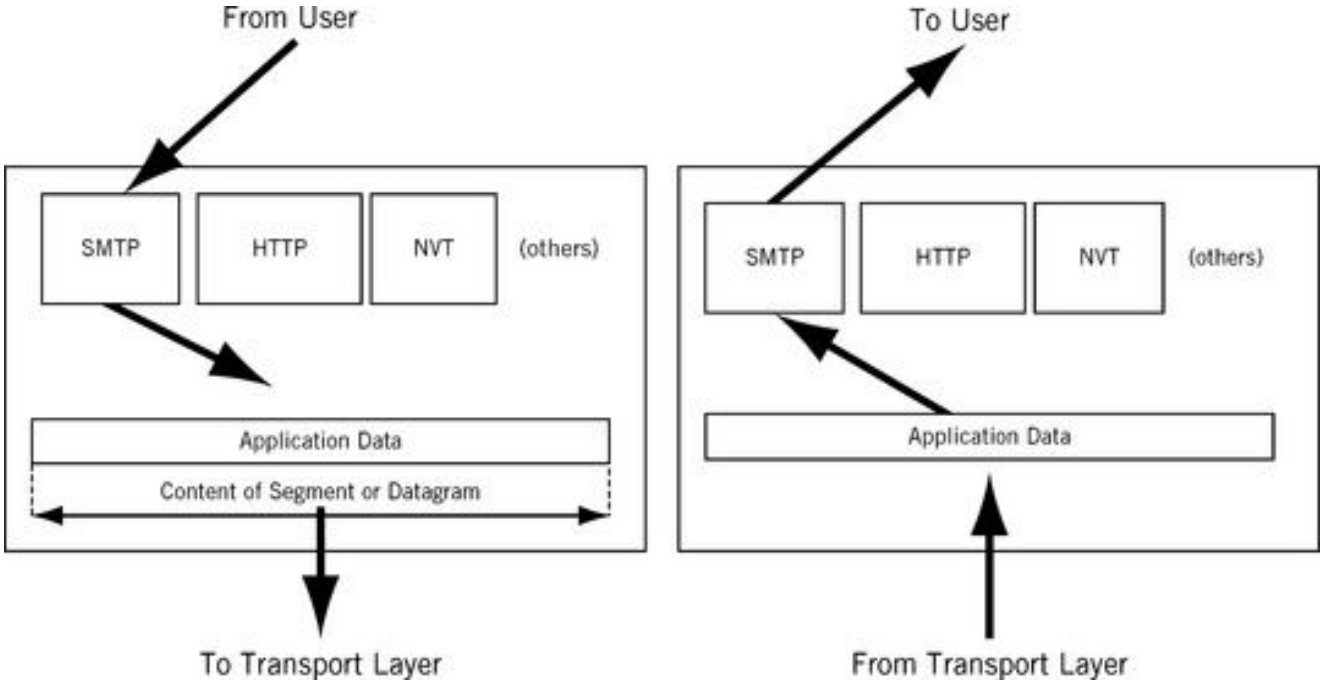
- Direct a packet to its destination
  - To reach network A
    - Send packets through machine C
  - Default route
    - Often the gateway assigned by DHCP

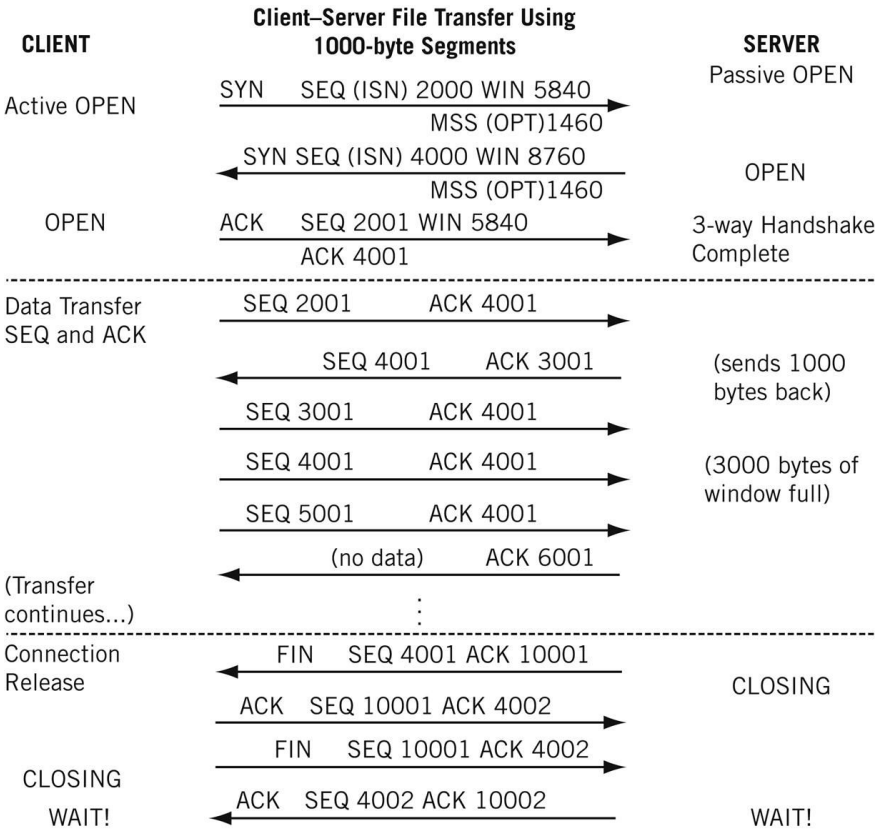
ip route show

```
ip route add 132.236.220.64/26 via 132.236.212.6 dev eth1
ip route add default via 132.236.227.1 dev eth0
```

Dynamic Host Control Protocol

- Enables automatic
  - IP Address
  - Netmask
  - Gateway
  - DNS Server configuration
- Offers a lease
  - Expires after a configurable amount of time
  - Must be renewed
- Software
  - isc-dhcp-server
  - dnsmasq - simple


From User
SMTP
HTTP
NVT
(others)
Application Data
Content of Segment or Datagram
To Transport Layer
To User
SMTP
HTTP
NVT
(others)
Application Data
From Transport Layer


Client–Server File Transfer Using 1000-byte Segments
CLIENT
SERVER
Passive OPEN
Active OPEN
SYN SEQ (ISN) 2000 WIN 5840
MSS (OPT)1460
SYN SEQ (ISN) 4000 WIN 8760
MSS (OPT)1460
OPEN
OPEN
ACK SEQ 2001 WIN 5840
ACK 4001
3-way Handshake Complete
Data Transfer SEQ and ACK
SEQ 2001 ACK 4001
SEQ 4001 ACK 3001
(sends 1000 bytes back)
SEQ 3001 ACK 4001
SEQ 4001 ACK 4001
(3000 bytes of window full)
SEQ 5001 ACK 4001
(no data) ACK 6001
(Transfer continues...)
Connection Release
FIN SEQ 4001 ACK 10001
CLOSING
ACK SEQ 10001 ACK 4002
FIN SEQ 10001 ACK 4002
CLOSING
ACK SEQ 4002 ACK 10002
WAIT!
WAIT!

Basic Network Configuration

```
ip link set eth0 up

ip add 192.168.47.20/24 dev eth0

ip route add default via 192.168.47.1

# Setup DNS Modify

/etc/resolv.conf

/etc/systemd/resolved.conf
```