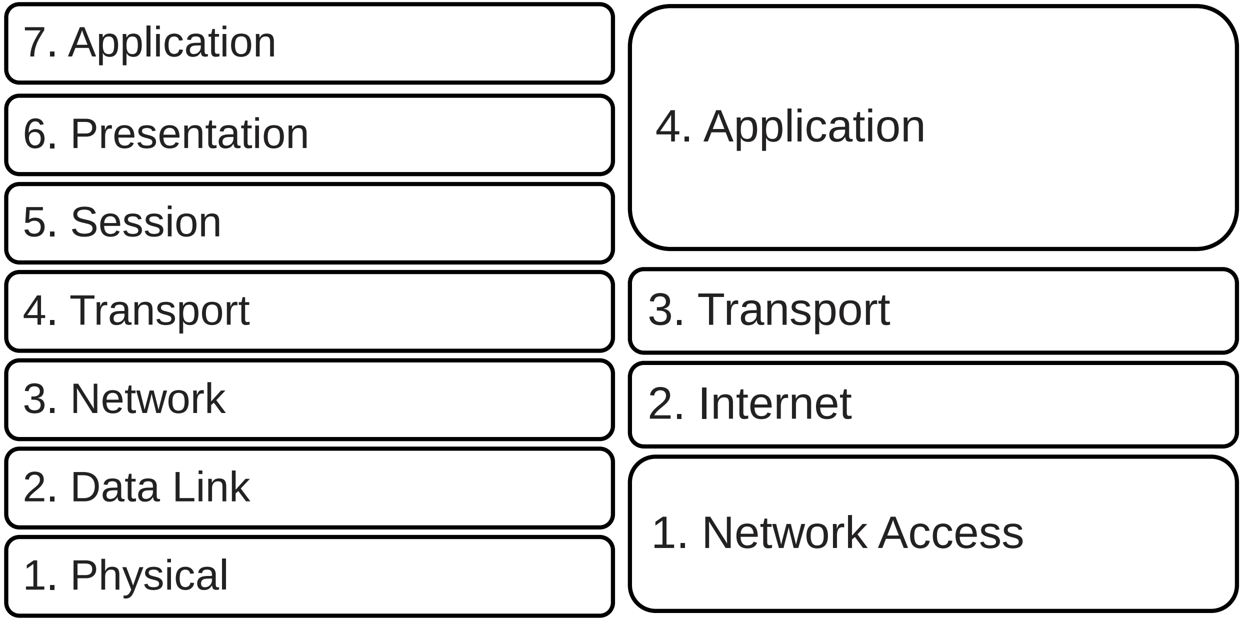
The TCP/IP Model



7. Application

6. Presentation

5. Session

4. Transport

3. Network

2. Data Link

1. Physical

4. Application

3. Transport

2. Internet

1. Network Access

Counting in Hex

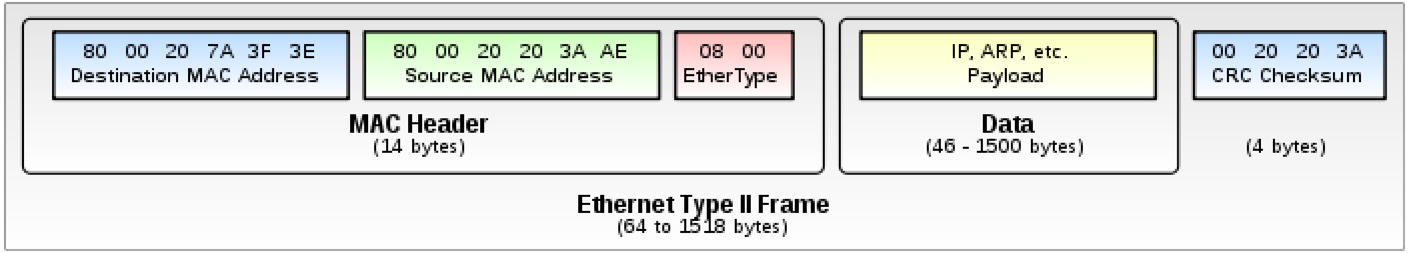
Decimal	Hex
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8

Decimal	Hex
9	9
10	A
11	B
12	C
13	D
14	E
15	F
16	10

Counting in Binary

Decimal	Hex	Binary
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111
16	10	00010000

Ethernet Headers – Network Access Layer



80 00 20 7A 3F 3E
Destination MAC Address

80 00 20 20 3A AE
Source MAC Address

08 00
EtherType

MAC Header
(14 bytes)

IP, ARP, etc.
Payload

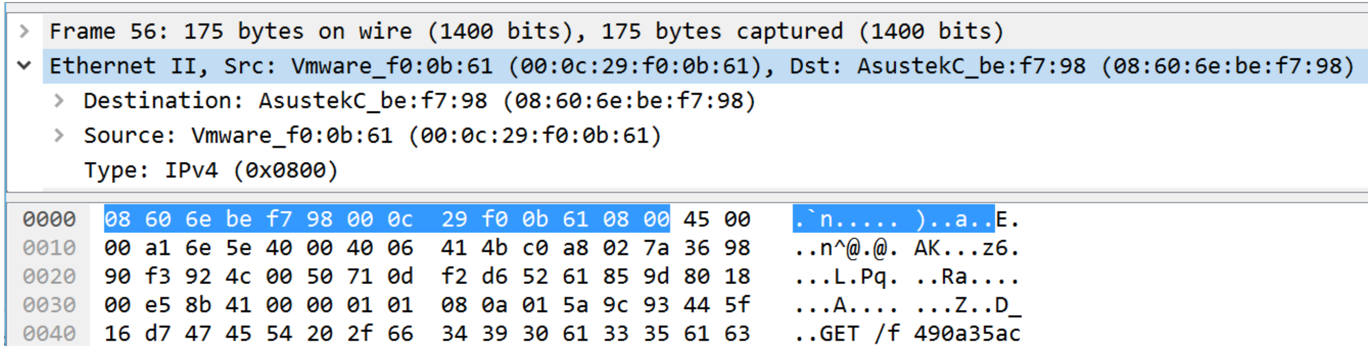
Data
(46 - 1500 bytes)

00 20 20 3A
CRC Checksum

(4 bytes)

Ethernet Type II Frame
(64 to 1518 bytes)

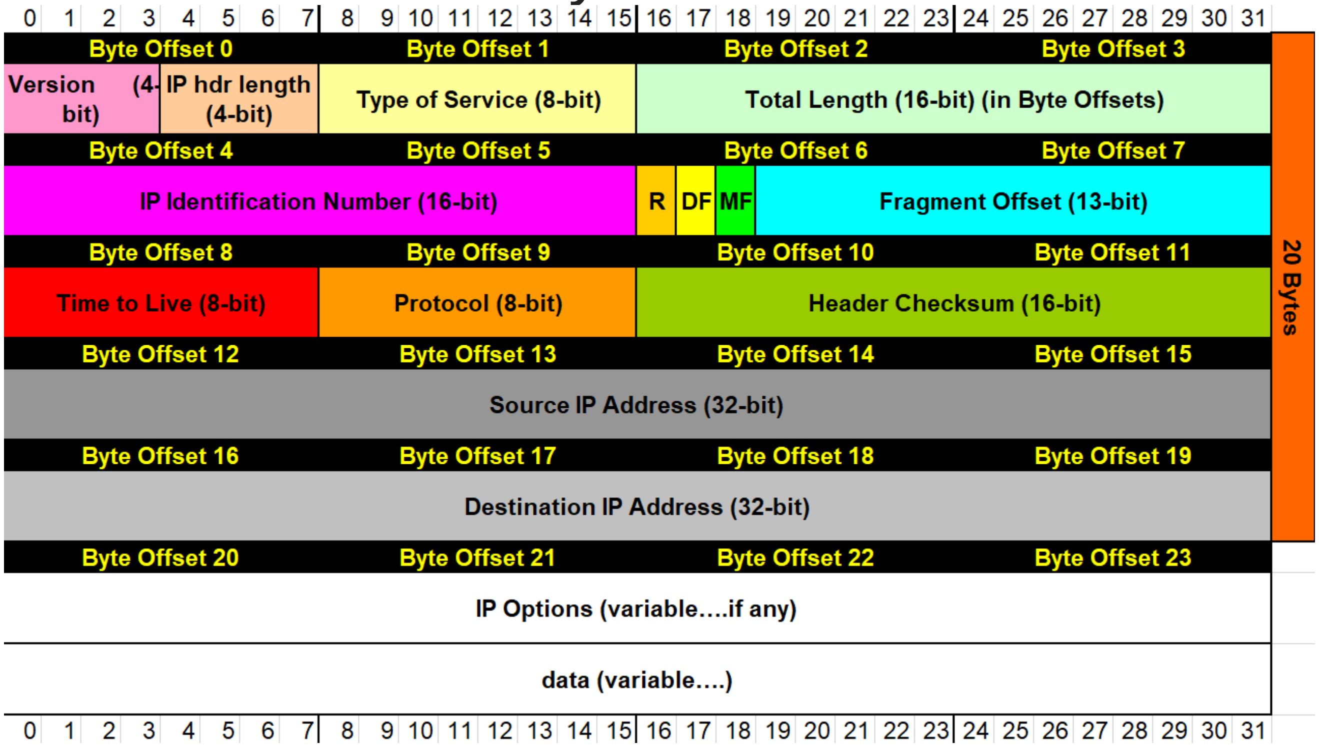
Source: https://en.wikipedia.org/wiki/Ethernet_frame



```
> Frame 56: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits)
v Ethernet II, Src: Vmware_f0:0b:61 (00:0c:29:f0:0b:61), Dst: AsustekC_be:f7:98 (08:60:6e:be:f7:98)
  > Destination: AsustekC_be:f7:98 (08:60:6e:be:f7:98)
  > Source: Vmware_f0:0b:61 (00:0c:29:f0:0b:61)
    Type: IPv4 (0x0800)

0000  08 60 6e be f7 98 00 0c  29 f0 0b 61 08 00 45 00   .`n..... )..a..E.
0010  00 a1 6e 5e 40 00 40 06  41 4b c0 a8 02 7a 36 98   ..n^@.@. AK...z6.
0020  90 f3 92 4c 00 50 71 0d  f2 d6 52 61 85 9d 80 18   ...L.Pq. ..Ra....
0030  00 e5 8b 41 00 00 01 01  08 0a 01 5a 9c 93 44 5f   ...A.... ...Z..D_
0040  16 d7 47 45 54 20 2f 66  34 39 30 61 33 35 61 63   ..GET /f 490a35ac
```

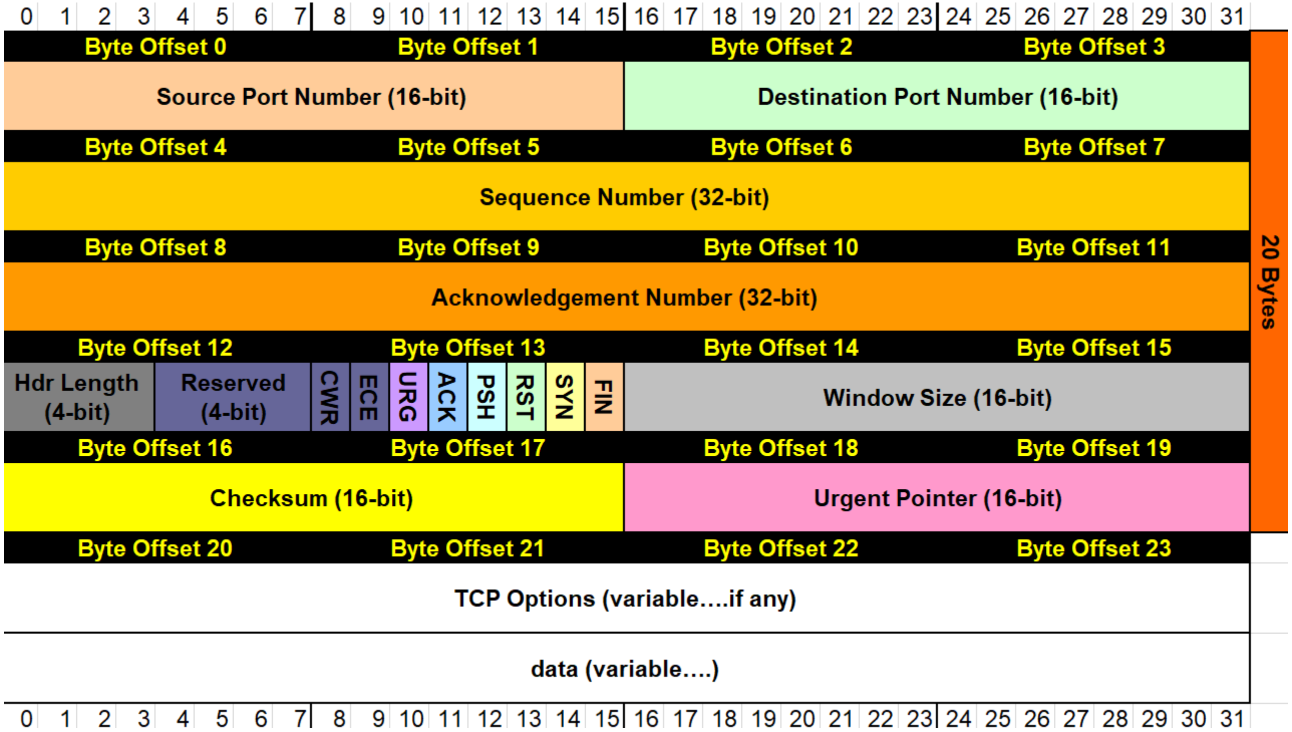
IPv4 Header – Internet Layer



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	
Byte Offset 0	Byte Offset 1	Byte Offset 2	Byte Offset 3	20 Bytes
Version (4-bit) IP hdr length (4-bit)	Type of Service (8-bit)	Total Length (16-bit) (in Byte Offsets)		
Byte Offset 4	Byte Offset 5	Byte Offset 6	Byte Offset 7	
IP Identification Number (16-bit)		R DF MF Fragment Offset (13-bit)		
Byte Offset 8	Byte Offset 9	Byte Offset 10	Byte Offset 11	
Time to Live (8-bit)	Protocol (8-bit)	Header Checksum (16-bit)		
Byte Offset 12	Byte Offset 13	Byte Offset 14	Byte Offset 15	
Source IP Address (32-bit)				
Byte Offset 16	Byte Offset 17	Byte Offset 18	Byte Offset 19	
Destination IP Address (32-bit)				
Byte Offset 20	Byte Offset 21	Byte Offset 22	Byte Offset 23	
IP Options (variable….if any)				
data (variable….)				
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	

http://wiki.gnhlug.org/twiki2/pub/Www/IpReference/Packet_Headers_Subnet_Breakdown.xls

TCP Header



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

Byte Offset 0 | Byte Offset 1 | Byte Offset 2 | Byte Offset 3

Source Port Number (16-bit) | Destination Port Number (16-bit)

Byte Offset 4 | Byte Offset 5 | Byte Offset 6 | Byte Offset 7

Sequence Number (32-bit)

Byte Offset 8 | Byte Offset 9 | Byte Offset 10 | Byte Offset 11

Acknowledgement Number (32-bit)

Byte Offset 12 | Byte Offset 13 | Byte Offset 14 | Byte Offset 15

Hdr Length (4-bit) | Reserved (4-bit) | CWR | ECE | URG | ACK | PSH | RST | SYN | FIN | Window Size (16-bit)

Byte Offset 16 | Byte Offset 17 | Byte Offset 18 | Byte Offset 19

Checksum (16-bit) | Urgent Pointer (16-bit)

20 Bytes

Byte Offset 20 | Byte Offset 21 | Byte Offset 22 | Byte Offset 23

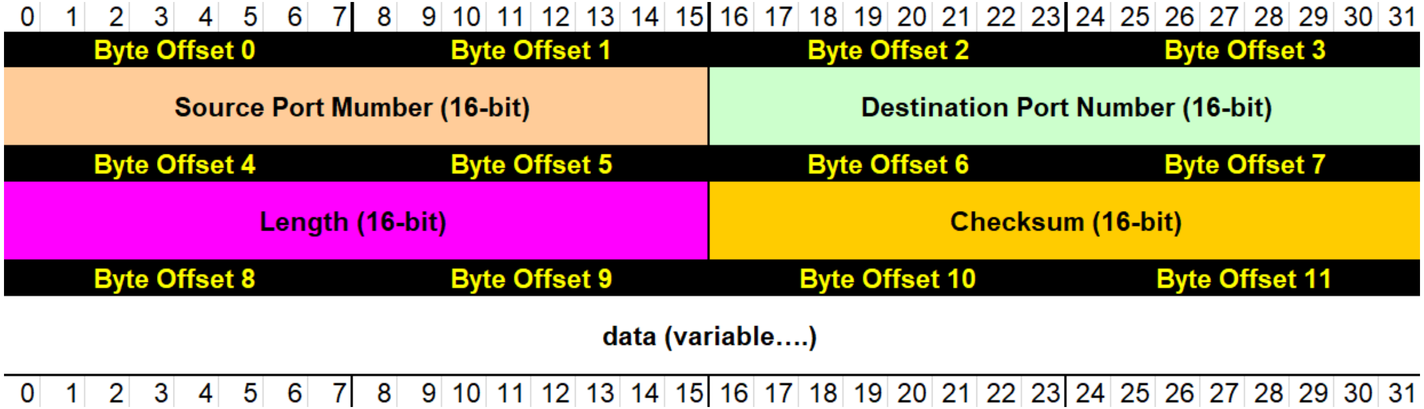
TCP Options (variable….if any)

data (variable….)

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

http://wiki.gnhlug.org/twiki2/pub/Www/IpReference/Packet_Headers_Subnet_Breakdown.xls

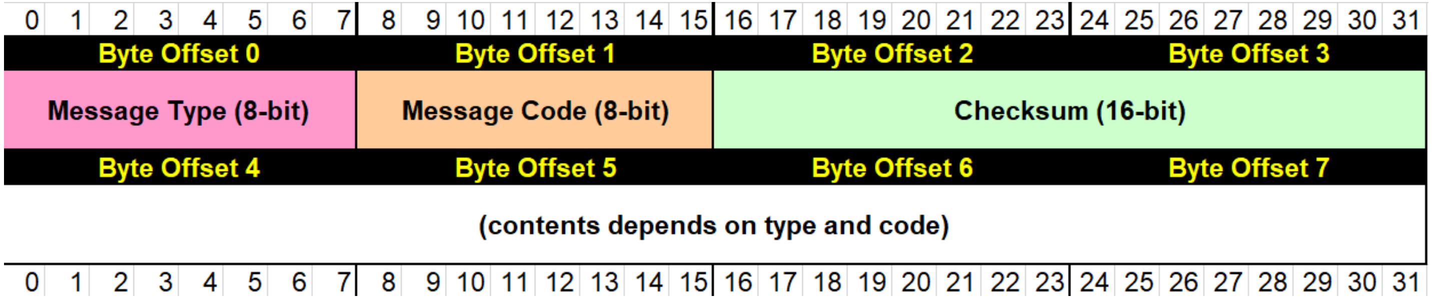
UDP Header



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
Byte Offset 0	Byte Offset 1	Byte Offset 2	Byte Offset 3
Source Port Mumber (16-bit)		Destination Port Number (16-bit)	
Byte Offset 4	Byte Offset 5	Byte Offset 6	Byte Offset 7
Length (16-bit)		Checksum (16-bit)	
Byte Offset 8	Byte Offset 9	Byte Offset 10	Byte Offset 11
data (variable....)			
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

http://wiki.gnhlug.org/twiki2/pub/Www/IpReference/Packet_Headers_Subnet_Breakdown.xls

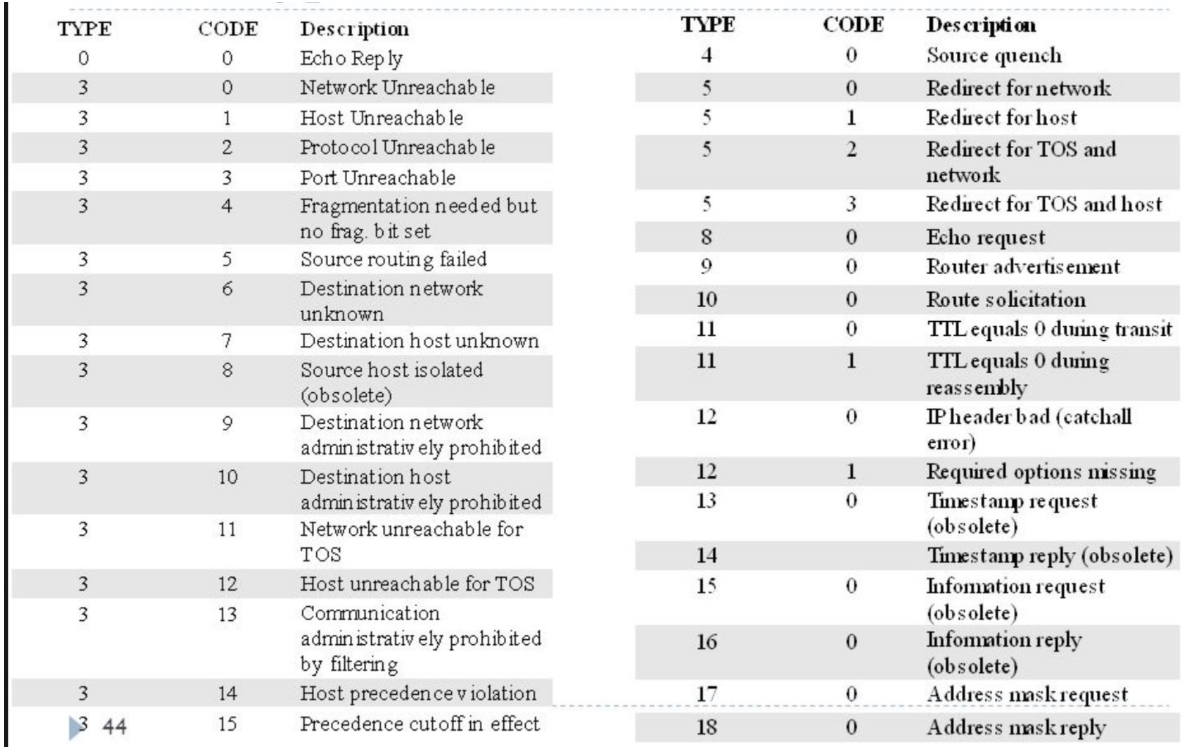
ICMP Header



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
Byte Offset 0								Byte Offset 1								Byte Offset 2								Byte Offset 3							
Message Type (8-bit)								Message Code (8-bit)								Checksum (16-bit)															
Byte Offset 4								Byte Offset 5								Byte Offset 6								Byte Offset 7							
(contents depends on type and code)																															
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

http://wiki.gnhlug.org/twiki2/pub/Www/IpReference/Packet_Headers_Subnet_Breakdown.xls

ICMP Header



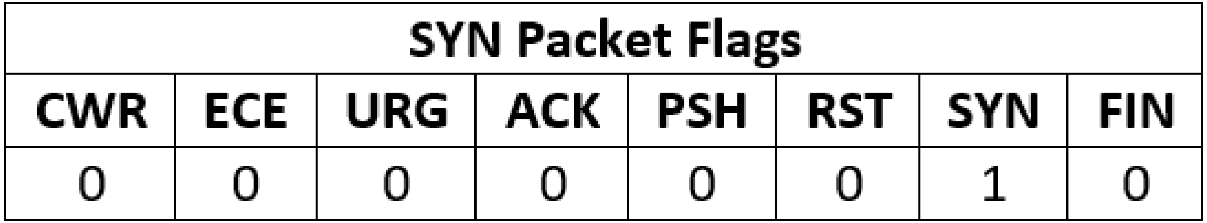
TYPE	CODE	Description
0	0	Echo Reply
3	0	Network Unreachable
3	1	Host Unreachable
3	2	Protocol Unreachable
3	3	Port Unreachable
3	4	Fragmentation needed but no frag. bit set
3	5	Source routing failed
3	6	Destination network unknown
3	7	Destination host unknown
3	8	Source host isolated (obsolete)
3	9	Destination network administratively prohibited
3	10	Destination host administratively prohibited
3	11	Network unreachable for TOS
3	12	Host unreachable for TOS
3	13	Communication administratively prohibited by filtering
3	14	Host precedence violation
3 44	15	Precedence cutoff in effect

TYPE	CODE	Description
4	0	Source quench
5	0	Redirect for network
5	1	Redirect for host
5	2	Redirect for TOS and network
5	3	Redirect for TOS and host
8	0	Echo request
9	0	Router advertisement
10	0	Route solicitation
11	0	TTL equals 0 during transit
11	1	TTL equals 0 during reassembly
12	0	IP header bad (catchall error)
12	1	Required options missing
13	0	Timestamp request (obsolete)
14		Timestamp reply (obsolete)
15	0	Information request (obsolete)
16	0	Information reply (obsolete)
17	0	Address mask request
18	0	Address mask reply

http://slideplayer.com/slide/6252793/

TCP Flags (Byte 13)

- Byte 13 in the TCP header contains control flags
- Help manage the TCP conversation



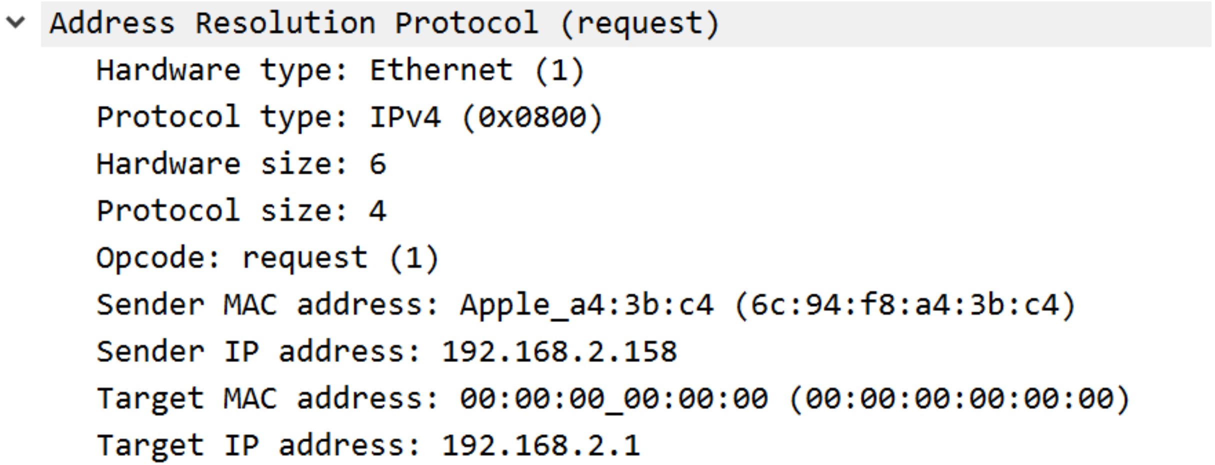
SYN Packet Flags							
CWR	ECE	URG	ACK	PSH	RST	SYN	FIN
0	0	0	0	0	0	1	0

Translate - tr

- Replaces single character
- tr ‘a’ ‘b’ : replace a with b
- tr -s ‘ ‘ : squeeze repeating characters
- tr -d ‘:‘ : delete character
- Very handy before cut

Address Resolution Protocol (ARP) Format

Hardware Type (Word)	Protocol Type (Word)	Hardware Size (Byte)	Protocol Size (Byte)	Opcode (Word)	Sender MAC (6 Bytes)	Sender IP (4 Bytes)	Target MAC (6 Bytes)	Target IP (4 Bytes)



```
⌄ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Apple_a4:3b:c4 (6c:94:f8:a4:3b:c4)
    Sender IP address: 192.168.2.158
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.2.1
```

Common External Ports

- Good egress filtering should block most external traffic
- Permitted traffic should go through an intermediary
  - TCP:80 (HTTP)
  - TCP:443 (SSL)
  - UDP:123 (NTP)
    - Should be blocked
  - UDP:53 (DNS)

Common Internal TCP Ports

- 22 (SSH)
- 445 (SMB)
- 88 (Kerberos)
- 135 (DCE/RPC)
- 389 (LDAP)
- 636 (LDAPS)
- 993 (IMAPS)

Common Internal TCP Ports

- 80 (HTTP)
- 443 (HTTPS)
- 8080 (Alternate HTTP)
- 8443 (Alternate HTTPS)
- Ephemeral ports (RPC)

Common Internal UDP Ports

- 53 (DNS)
- 5355(LLMNR)
- 123(NTP)

Alerts

- Many sources
  - Intrusion Detection System
  - Intrusion Prevention System
  - Web Application Firewall
- Signatures are not always great
- Places to start
  - Use the source port

Continued Analysis

- Work forward for post infection
  - Find binary files for analysis
  - Identify command and control traffic
- Work backward to find the origin
  - Often starts with legitimate sites

Useful Techniques

- Wireshark display filters
  - dns || http.request.full_uri || ssl.handshake.certificate
- Find “odd” URLs
  - Long alphanumeric strings that are not words
  - Directed outside of domain
  - Use “referer” to work backwards
  - Find redirection call in calling page (URL string)

Automated Tools

- Virustotal.com
  - Binaries or pcaps
- Sandboxes
  - https://zeltser.com/automated-malware-analysis/