



# **Network Protocol Analysis**

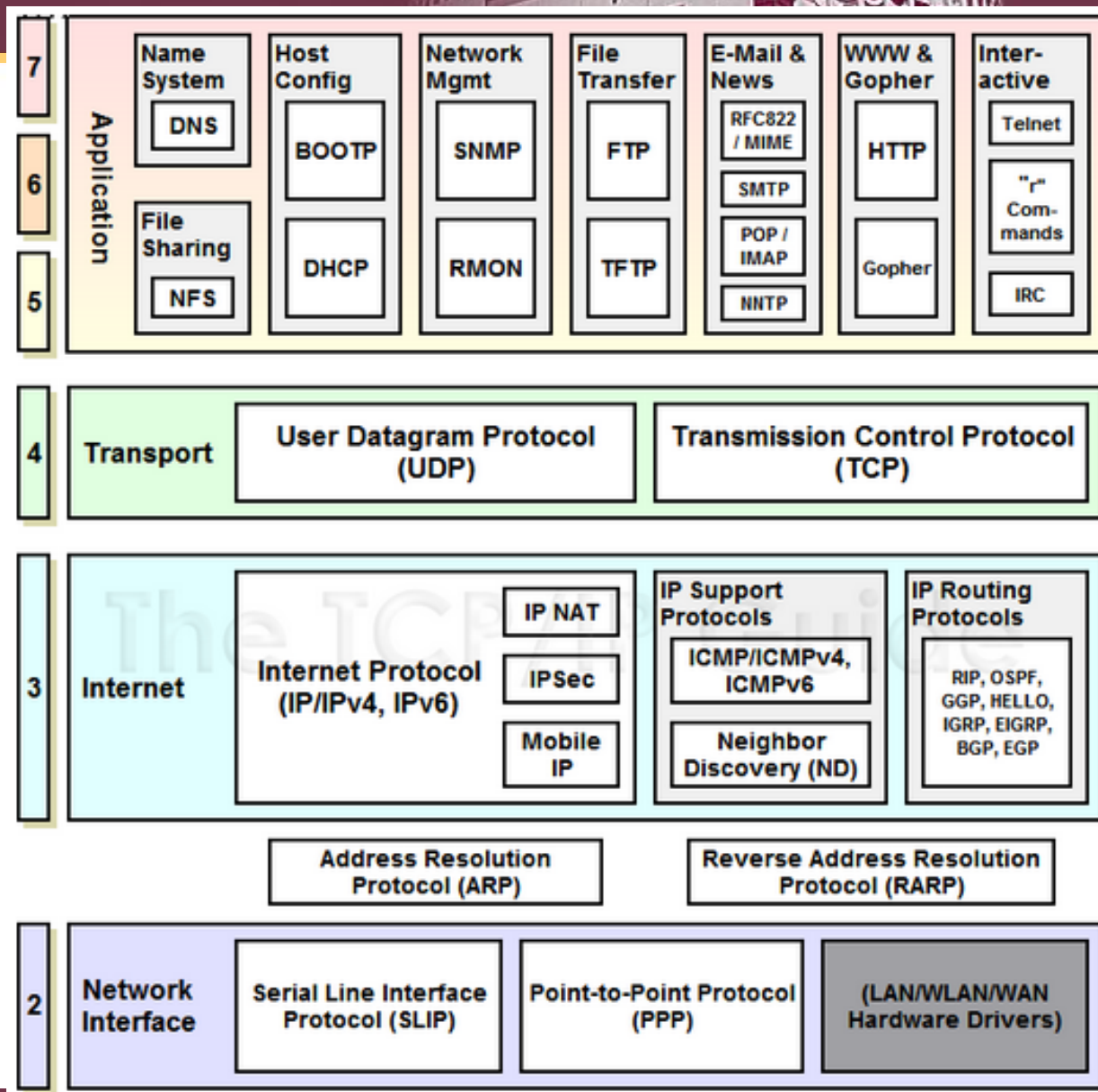
Chun-Jen (James) Chung

Arizona State University

# Protocol Analysis

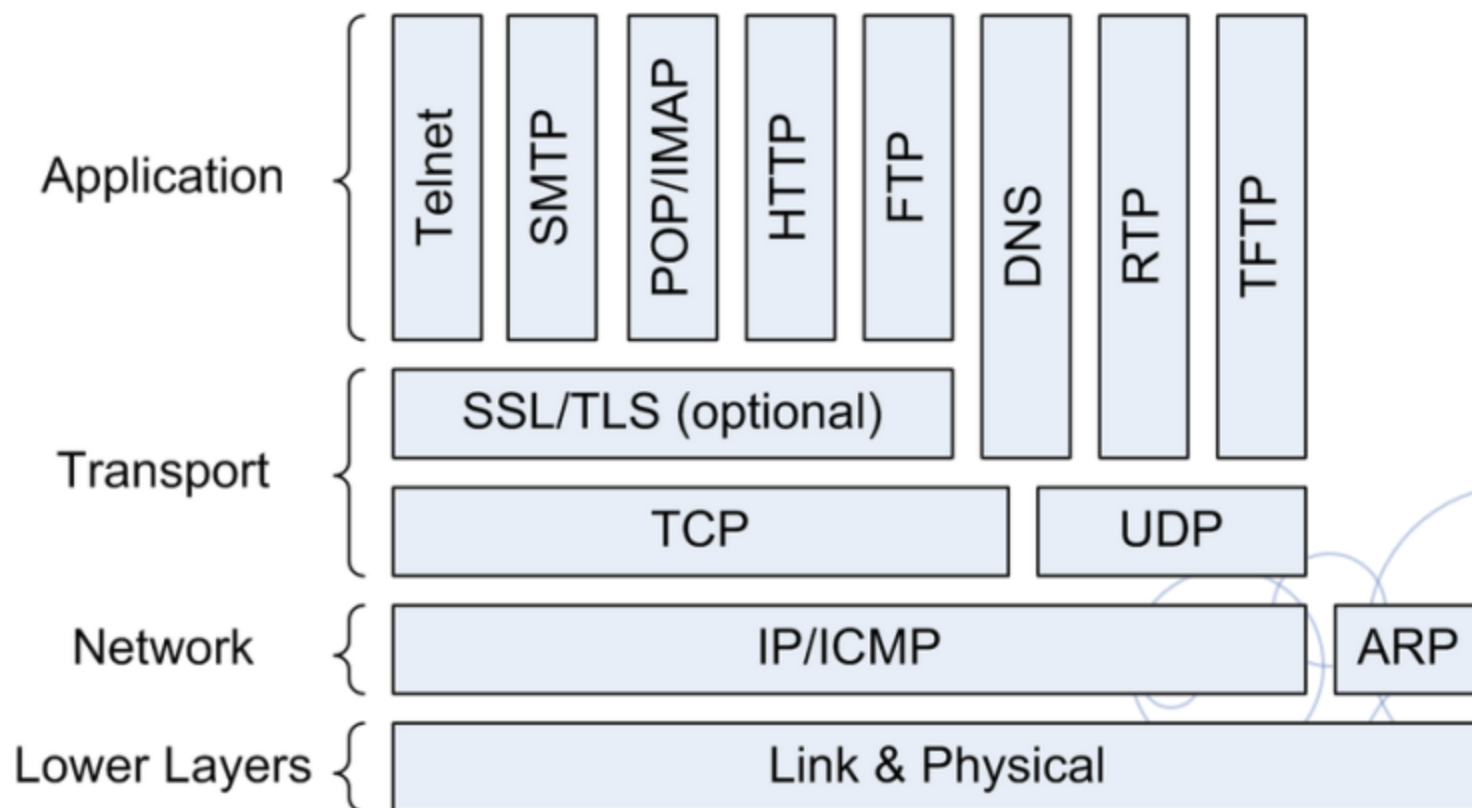
- Purpose: to identify and analyze network problems.
- What are problems?
  - Bad performance, unusual traffic/packets, malicious payload, and potential vulnerabilities
- How do we solve it?
  - Instrument the code :
    - difficult task, network programming skills required.
  - Use available tools: Ethereal, tcpdump/tshark, wireshark, etc.
  - Write your own tool: libpcap

# TCP/IP Protocol Suite in OSI

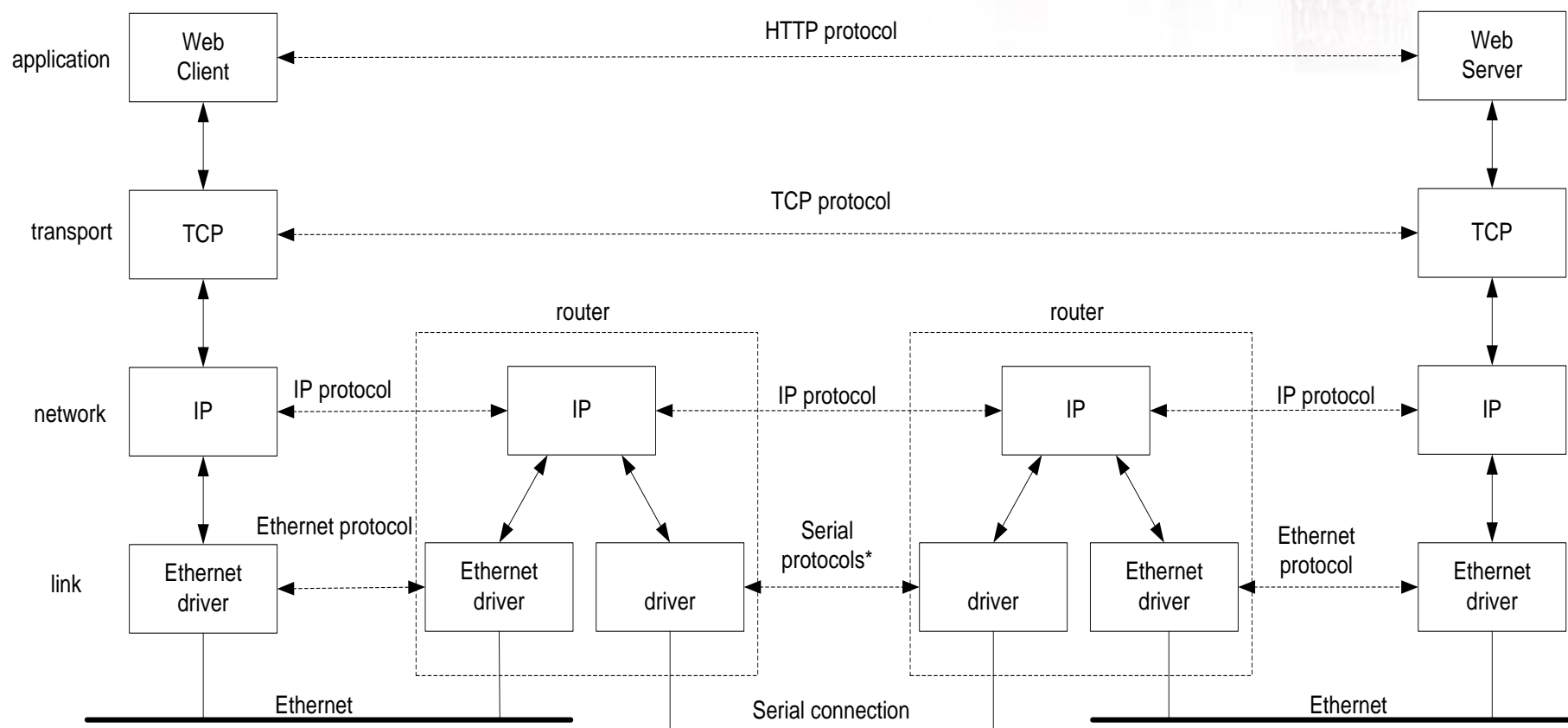


Courtesy of tcpipguide.com

# TCP/IP (4 layer model)



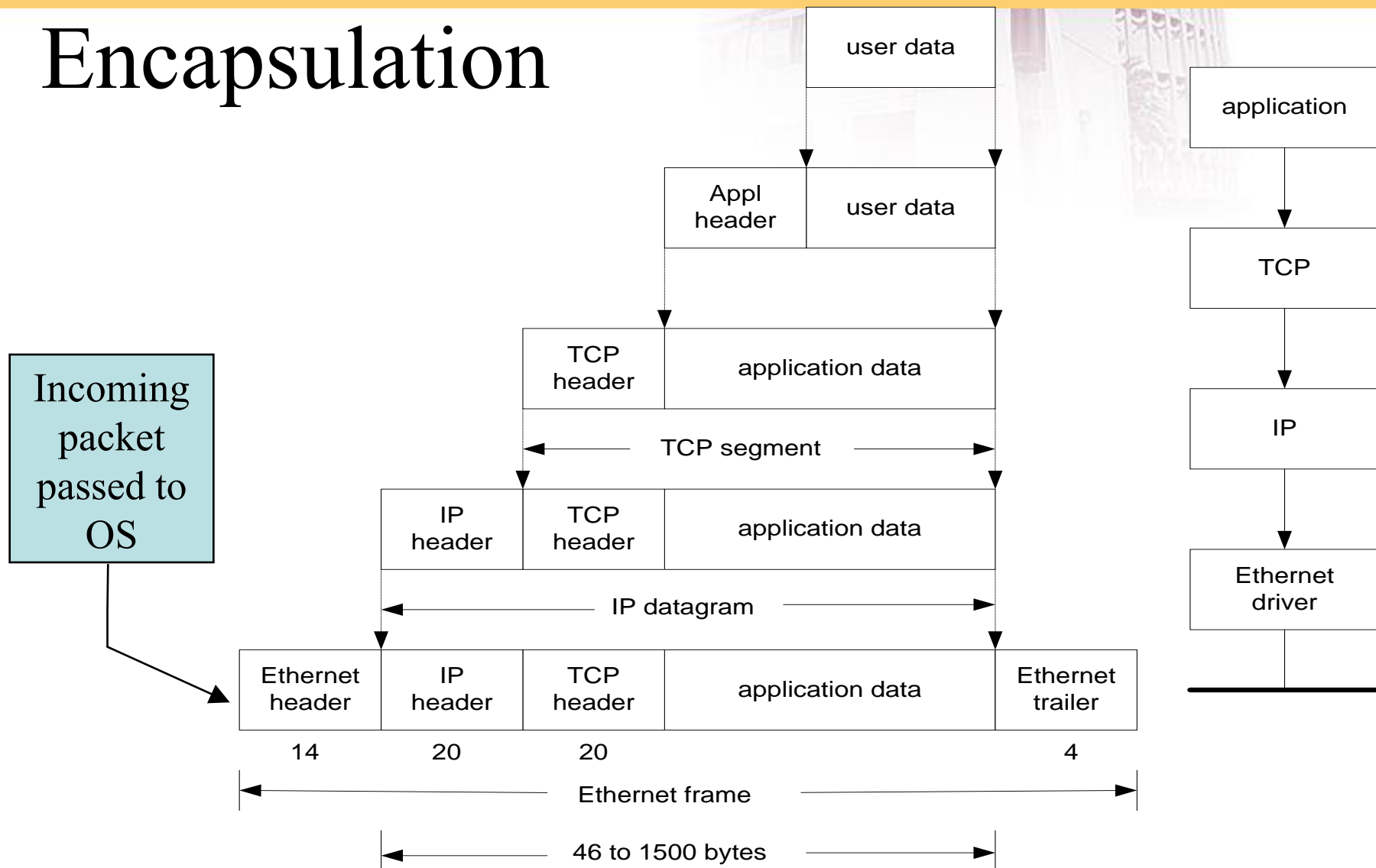
# Network inter-connection



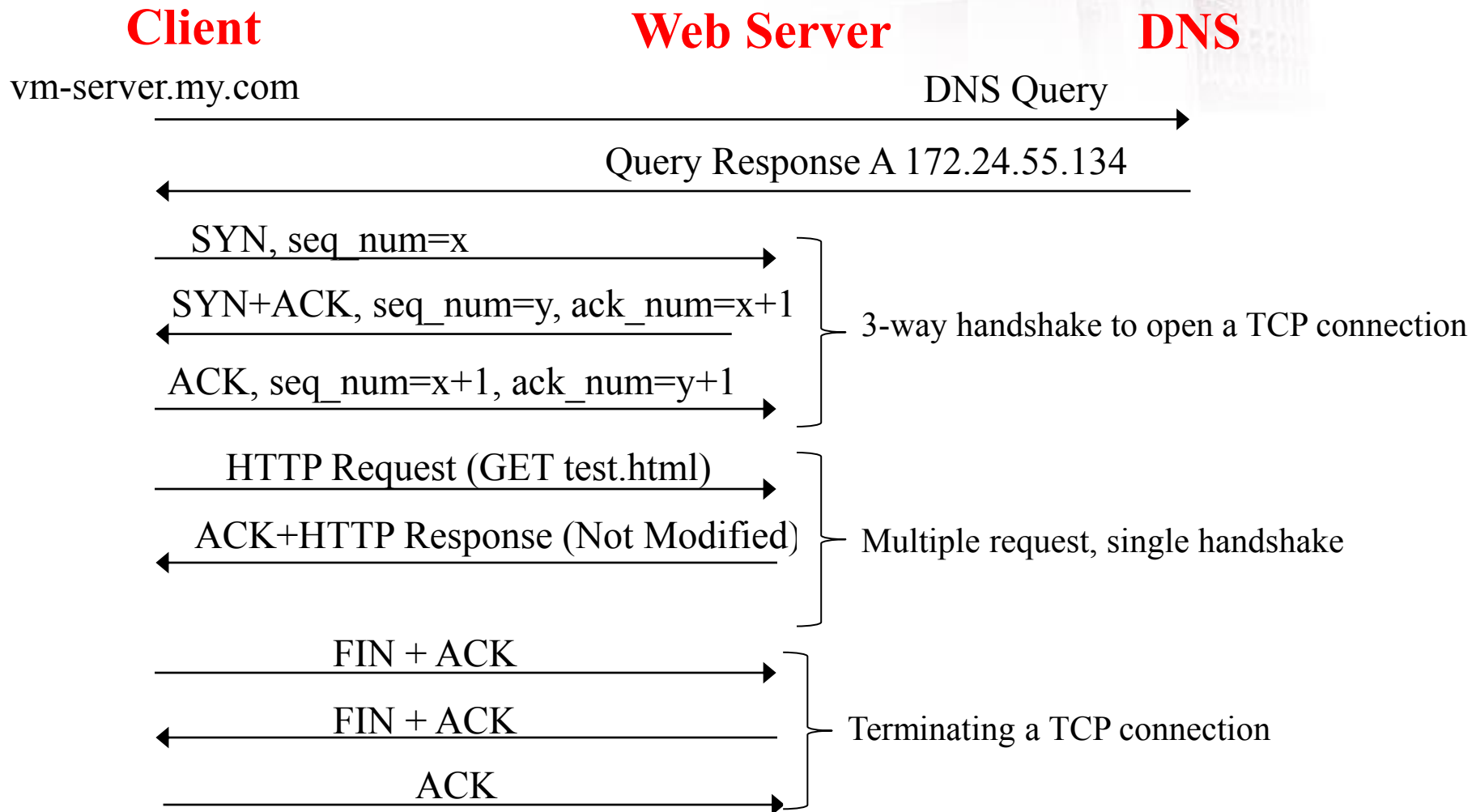
Two networks connected with two routers

\* (Cisco support: EIA/TIA-232, EIA/TIA-449, V.35, X.21 and EIA-530 etc.)

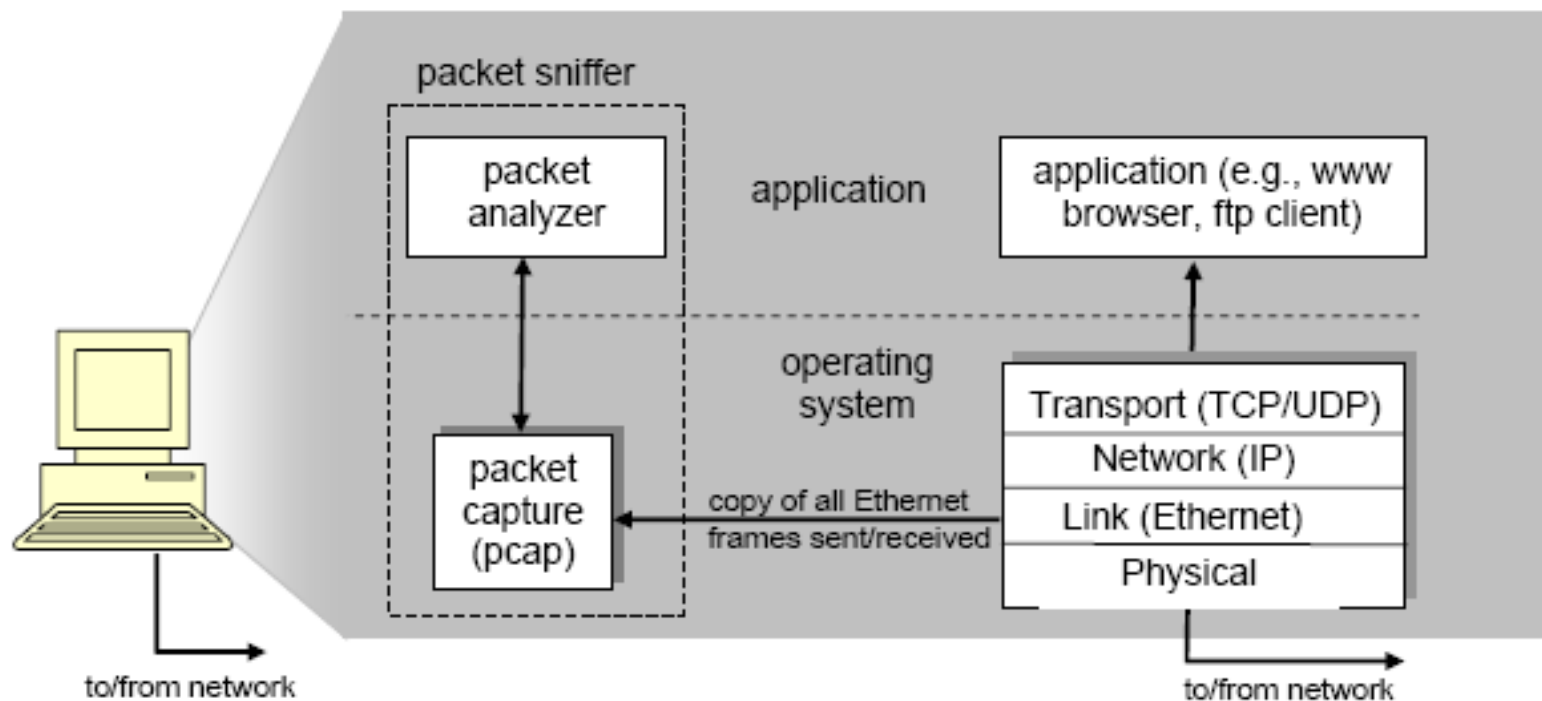
# Encapsulation



# WWW Request/Response Example



# Wireshark System Overview





Select interface  
Set options  
Start live capture

Display filter

Listing of captured packets

Details of selected packet header

packet content

Nc	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.24.55.6	172.24.55.196	DNS	76	Standard query A vm-server.my.com
2	0.001461	172.24.55.196	172.24.55.6	DNS	125	Standard query response A 172.24.55.134
3	0.001822	172.24.55.6	172.24.55.134	TCP	74	33176 > http [SYN] Seq=0 Win=14600 Len=0 MSS
4	0.003653	172.24.55.134	172.24.55.6	TCP	74	http > 33176 [SYN, ACK] Seq=0 Ack=1 Win=1448
5	0.003689	172.24.55.6	172.24.55.134	TCP	66	33176 > http [ACK] Seq=1 Ack=1 Win=14720 Len
6	0.003888	172.24.55.6	172.24.55.134	HTTP	458	GET /test.html HTTP/1.1
7	0.004602	172.24.55.134	172.24.55.6	TCP	66	http > 33176 [ACK] Seq=1 Ack=393 Win=15616 L
8	0.005225	172.24.55.134	172.24.55.6	HTTP	275	HTTP/1.1 304 Not Modified
9	0.005245	172.24.55.6	172.24.55.134	TCP	66	33176 > http [ACK] Seq=393 Ack=210 Win=15744
10	0.172238	172.24.55.6	172.24.55.134	HTTP	369	GET /favicon.ico HTTP/1.1
11	0.173911	172.24.55.134	172.24.55.6	HTTP	568	HTTP/1.1 404 Not Found (text/html)
12	0.173937	172.24.55.6	172.24.55.134	TCP	66	33176 > http [ACK] Seq=696 Ack=712 Win=16768
13	5.002729	fa:16:3e:39:28:a9	fa:16:3e:2d:a9:7c	ARP	42	Who has 172.24.55.6? Tell 172.24.55.4

Frame 6: 458 bytes on wire (3664 bits), 458 bytes captured (3664 bits)

- Ethernet II, Src: fa:16:3e:2d:a9:7c (fa:16:3e:2d:a9:7c), Dst: fa:16:3e:39:28:49 (fa:16:3e:39:28:49)
- Internet Protocol Version 4, Src: 172.24.55.6 (172.24.55.6), Dst: 172.24.55.134 (172.24.55.134)
- Transmission Control Protocol, Src Port: 33176 (33176), Dst Port: http (80), Seq: 1, Ack: 1, Len: 392
- Hypertext Transfer Protocol

```

0000  fa 16 3e 39 28 49 fa 16 3e 2d a9 7c 08 00 45 00  ..>9(I.. >-.|..E.
0010  01 bc 99 46 40 00 40 06 d9 38 ac 18 37 06 ac 18  ...F@.@. .8..7...
0020  37 86 81 98 00 50 41 1f 23 12 01 ab 60 79 80 18  7....PA. #...`y..
0030  00 73 c8 6b 00 00 01 01 08 0a 00 19 ba 55 00 1e  .s.k.... ..U..
0040  a8 c3 47 45 54 20 2f 74 65 73 74 2e 68 74 6d 6c  ..GET /t est.html
    
```



The image shows two Wireshark dialog boxes. The 'Wireshark: Capture Options' dialog is in the foreground, and the 'Wireshark: Capture Interfaces' dialog is in the background.

**Wireshark: Capture Options**

- Interface: eth0
- IP address: 172.24.55.6, fe80::f816:3eff:fe2d:a97c
- Link-layer header type: Ethernet
- Buffer size: 1024 KiB
- ☒ Capture packets in promiscuous mode
- ☐ Capture packets in monitor mode
- ☐ Capture packets in pcap-ng format
- ☐ Limit each packet to 65535 bytes
- Capture Filter: host 172.24.55.134
- Capture File(s): File: [ ] Browse...
  - ☐ Use multiple files
  - ☒ Next file every 1 megabyte(s)
  - ☐ Next file every 1 minute(s)
  - ☐ Ring buffer with 2 files
  - ☐ Stop capture after 1 file(s)
- Stop Capture ...
  - ☒ ... after 20 packet(s)
  - ☐ ... after 1 megabyte(s)
  - ☐ ... after 1 minute(s)

**Wireshark: Capture Interfaces**

Device	Description	IP	Packets	Packets/s	Stop
eth0		172.24.55.6	0	0	Start Options
any	Pseudo-device that captures on all interfaces	unknown	0	0	Start Options
lo		127.0.0.1	0	0	Start Options

Buttons: Help, Close

Arrows point from the 'host 172.24.55.134' filter and the '20 packet(s)' stop time to the corresponding text in the list on the right.

- Capture all packets that contain a host address of: 134.193.6.58 as either source or destination
- Capture packets for 20 seconds and then stop.

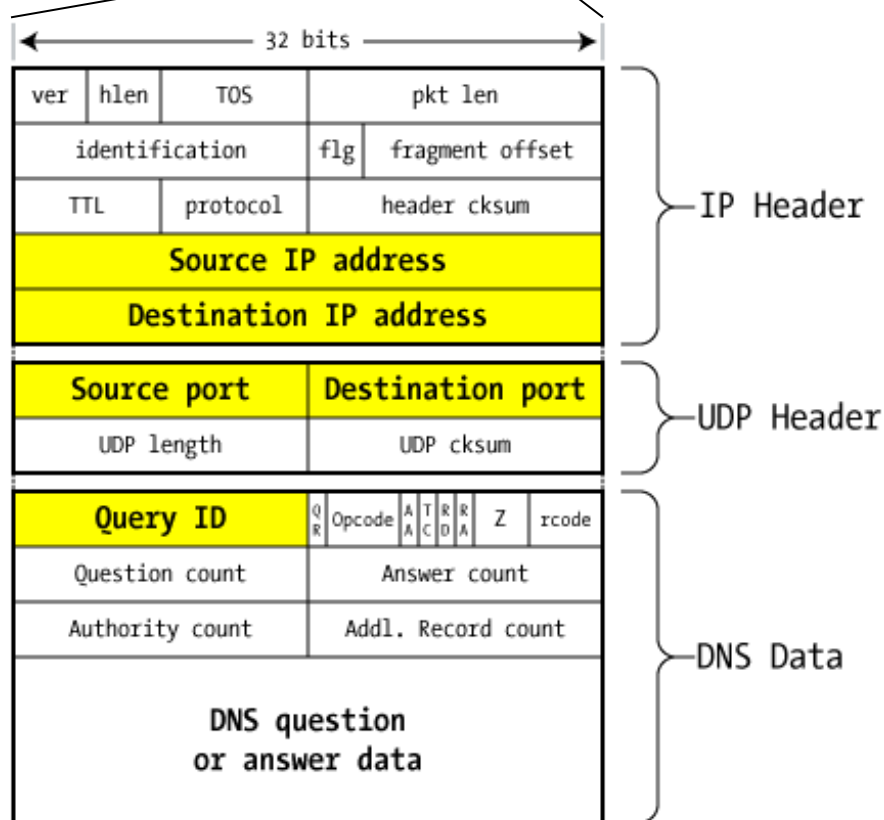
# Sample Filters

- Capture Filter: (protocol)(direction)(hosts)(value)(logic op)(other)
  - `dst host 134.193.6.58`
  - `dst host 134.193.6.58 and dst port 12345`
  - `src host 134.193.15.9 && dst net 216.92.131.0`
  - `host 134.193.6.58 and ip proto tcp`
  - `dest host 134.193.6.58 && ip proto icmp`
- Display Filter:  
(protocol).(string1).(string2)(compare op)(value)(logic op)(other)
  - `dns || tcp`
  - `ip.addr == 10.0.1.1`
  - `ip.src != 10.1.2.3 or ip.dst != 10.4.5.6`
  - `tcp.port == 22`
  - `tcp.dstport == 25`
  - `tcp.flags.syn == 0x02`

# Ethernet Frame and DNS Packet on the wire

Ethernet  
Frame

Preamble	Destination MAC address	Source MAC address	Type/Length	User Data	Frame Check Sequence (FCS)
8	6	6	2	46 - 1500	4



# Well-known common ports

Port	TCP/UDP	Protocol Direction	Description	Additional Info
23	TCP	Inbound/Outbound	Telnet for <u>mgmt</u> port	
22	TCP	Inbound/Outbound	SSH for <u>mgmt</u> port	Also used for <u>SoL</u> to CiMC
80	TCP	Inbound	HTTP to <u>mgmt</u> port	
443	TCP	Inbound	HTTPS to <u>mgmt</u> port	
161	UDP	Inbound	SNMP Poll	
162	UDP	Outbound	SNMP Trap	
623	UDP	Inbound	IPMI to CiMC	
2068	TCP	Inbound	KVM	
69	UDP	Outbound	TFTP	File Transfer
1812/1813	UDP	Outbound	RADIUS	Authentication
49	TCP	Outbound	TACACS	Authentication
389	TCP	Outbound	LDAP	Directory Authentication
123	TCP	Outbound	NTP	Time Sync
25	TCP	Outbound	SMTP	Call Home
514	UDP	Outbound	Syslog	External logging
53	UDP	Outbound	DNS	Name Resolution
115/20	TCP	Outbound	SFTP	File Transfer

# DNS Query Packet

```
▶ Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
▼ Ethernet II, Src: fa:16:3e:2d:a9:7c (fa:16:3e:2d:a9:7c), Dst: fa:16:3e:39:28:49 (fa:16:3e:39:28:49)
  ▶ Destination: fa:16:3e:39:28:49 (fa:16:3e:39:28:49)
  ▶ Source: fa:16:3e:2d:a9:7c (fa:16:3e:2d:a9:7c)
  Type: IP (0x0800)
▶ Internet Protocol Version 4, Src: 172.24.55.6 (172.24.55.6), Dst: 172.24.55.196 (172.24.55.196)
▼ User Datagram Protocol, Src Port: 54355 (54355), Dst Port: domain (53)
  Source port: 54355 (54355)
  Destination port: domain (53)
  Length: 42
  ▶ Checksum: 0xc736 [validation disabled]
▼ Domain Name System (query)
  \[Response In: 2\]
  Transaction ID: 0x691a
  ▶ Flags: 0x0100 (Standard query)
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
▼ Queries
  ▼ vm-server.my.com: type A, class IN
    Name: vm-server.my.com
    Type: A (Host address)
    Class: IN (0x0001)
```

# DNS Response Packet

```
▶ Frame 2: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits)
▶ Ethernet II, Src: fa:16:3e:39:28:49 (fa:16:3e:39:28:49), Dst: fa:16:3e:2d:a9:7c (fa:16:3e:2d:a9:7c)
▶ Internet Protocol Version 4, Src: 172.24.55.196 (172.24.55.196), Dst: 172.24.55.6 (172.24.55.6)
▼ User Datagram Protocol, Src Port: domain (53), Dst Port: 54355 (54355)
    Source port: domain (53)
    Destination port: 54355 (54355)
    Length: 91
    ▶ Checksum: 0x5751 [validation disabled]
▼ Domain Name System (response)
    [Request In: 1]
    [Time: 0.001461000 seconds]
    Transaction ID: 0x691a
    ▶ Flags: 0x8580 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 1
    ▶ Queries
    ▼ Answers
        ▶ vm-server.my.com: type A, class IN, addr 172.24.55.134
    ▼ Authoritative nameservers
        ▶ my.com: type NS, class IN, ns ns.my.com
    ▼ Additional records
        ▶ ns.my.com: type A, class IN, addr 172.24.55.196
```

# TCP connection request

- ▶ Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
- ▶ Ethernet II, Src: fa:16:3e:2d:a9:7c (fa:16:3e:2d:a9:7c), Dst: fa:16:3e:39:28:49 (fa:16:3e:39:28:49)
- ▶ Internet Protocol Version 4, Src: 172.24.55.6 (172.24.55.6), Dst: 172.24.55.134 (172.24.55.134)
- ▼ Transmission Control Protocol, Src Port: 33176 (33176), Dst Port: http (80), Seq: 0, Len: 0
  - Source port: 33176 (33176)
  - Destination port: http (80)
  - [Stream index: 1]
  - Sequence number: 0 (relative sequence number)
  - Header length: 40 bytes
  - ▶ Flags: 0x002 (SYN)
    - Window size value: 14600
    - [Calculated window size: 14600]
  - ▶ Checksum: 0xc6eb [validation disabled]
  - ▼ Options: (20 bytes)
    - Maximum segment size: 1460 bytes
    - TCP SACK Permitted Option: True
    - ▶ Timestamps: TSval 1686101, TSecr 0
    - No-Operation (NOP)
    - ▶ Window scale: 7 (multiply by 128)

# TCP connection response

```
▶ Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▶ Ethernet II, Src: fa:16:3e:39:28:49 (fa:16:3e:39:28:49), Dst: fa:16:3e:2d:a9:7c (fa:16:3e:2d:a9:7c)
▶ Internet Protocol Version 4, Src: 172.24.55.134 (172.24.55.134), Dst: 172.24.55.6 (172.24.55.6)
▼ Transmission Control Protocol, Src Port: http (80), Dst Port: 33176 (33176), Seq: 0, Ack: 1, Len: 0
  Source port: http (80)
  Destination port: 33176 (33176)
  [Stream index: 1]
  Sequence number: 0      (relative sequence number)
  Acknowledgement number: 1    (relative ack number)
  Header length: 40 bytes
▶ Flags: 0x012 (SYN, ACK)
  Window size value: 14480
  [Calculated window size: 14480]
▶ Checksum: 0x9d15 [validation disabled]
▼ Options: (20 bytes)
  Maximum segment size: 1460 bytes
  TCP SACK Permitted Option: True
▶ Timestamps: TSval 2009283, TSecr 1686101
  No-Operation (NOP)
▶ Window scale: 7 (multiply by 128)
▶ [SEQ/ACK analysis]
```

# Initial HTTP request for page

```
▶ Frame 6: 458 bytes on wire (3664 bits), 458 bytes captured (3664 bits)
▶ Ethernet II, Src: fa:16:3e:2d:a9:7c (fa:16:3e:2d:a9:7c), Dst: fa:16:3e:39:28:49 (fa:16:3e:39:28:49)
▶ Internet Protocol Version 4, Src: 172.24.55.6 (172.24.55.6), Dst: 172.24.55.134 (172.24.55.134)
▶ Transmission Control Protocol, Src Port: 33176 (33176), Dst Port: http (80), Seq: 1, Ack: 1, Len: 392
▼ Hypertext Transfer Protocol
  ▶ GET /test.html HTTP/1.1\r\n ← Request Line
    Host: vm-server.my.com\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    If-Modified-Since: Wed, 29 Jan 2014 04:36:38 GMT\r\n
    If-None-Match: "15c4c-54-4f1147c98f662"\r\n
    \r\n
    [Full request URI: http://vm-server.my.com/test.html]
    ← Blank line separates header and body
    ← Request Message body
```

Request Headers

HTTP Request Methods: GET, POST, PUT,...

# Initial HTTP response

```
▶ Frame 8: 275 bytes on wire (2200 bits), 275 bytes captured (2200 bits)
▶ Ethernet II, Src: fa:16:3e:39:28:49 (fa:16:3e:39:28:49), Dst: fa:16:3e:2d:a9:7c (fa:16:3e:2d:a9:7c)
▶ Internet Protocol Version 4, Src: 172.24.55.134 (172.24.55.134), Dst: 172.24.55.6 (172.24.55.6)
▶ Transmission Control Protocol, Src Port: http (80), Dst Port: 33176 (33176), Seq: 1, Ack: 393, Len: 209
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 304 Not Modified\r\n ← Status Line
    Date: Wed, 29 Jan 2014 04:39:03 GMT\r\n
    Server: Apache/2.2.22 (Ubuntu)\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "15c4c-54-4f1147c98f662"\r\n
    Vary: Accept-Encoding\r\n
    \r\n
    ← Blank line separates header and body
    ← Request Message body
```

- The status code is a 3-digit number: 1xx (Informational), 2xx (Success), 3xx (Redirection), 4xx (Client Error), 5xx (Server Error).
- 304 Not Modified: In response to the If-Modified-Since conditional GET request, the server notifies that the resource requested has not been modified.

# Client's TCP SYN Packet

3	0.001822	172.24.55.6	172.24.55.134	TCP	74	33176 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM
4	0.003653	172.24.55.134	172.24.55.6	TCP	74	http > 33176 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=146
5	0.003689	172.24.55.6	172.24.55.134	TCP	66	33176 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=168610
6	0.003888	172.24.55.6	172.24.55.134	HTTP	458	GET /test.html HTTP/1.1
7	0.004602	172.24.55.134	172.24.55.6	TCP	66	http > 33176 [ACK] Seq=1 Ack=393 Win=15616 Len=0 TSval=2009
8	0.005225	172.24.55.134	172.24.55.6	HTTP	275	HTTP/1.1 304 Not Modified
9	0.005245	172.24.55.6	172.24.55.134	TCP	66	33176 > http [ACK] Seq=393 Ack=210 Win=15744 Len=0 TSval=16

- ▶ Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
- ▶ Ethernet II, Src: fa:16:3e:2d:a9:7c (fa:16:3e:2d:a9:7c), Dst: fa:16:3e:39:28:49 (fa:16:3e:39:28:49)
- ▶ Internet Protocol Version 4, Src: 172.24.55.6 (172.24.55.6), Dst: 172.24.55.134 (172.24.55.134)
- ▼ Transmission Control Protocol, Src Port: 33176 (33176), Dst Port: http (80), Seq: 0, Len: 0

Source port: 33176 (33176)

Destination port: http (80)

[Stream index: 1]

Sequence number: 0 (relative sequence number)

Header length: 40 bytes

Client's sequence number, c\_sn=0

- ▶ Flags: 0x002 (SYN)

Window size value: 14600

[Calculated window size: 14600]

- ▶ Checksum: 0xc6eb [validation disabled]

- ▶ Options: (20 bytes)

# Server's TCP SYN+ACK Packet

3	0.001822	172.24.55.6	172.24.55.134	TCP	74	33176 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM
4	0.003653	172.24.55.134	172.24.55.6	TCP	74	http > 33176 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460
5	0.003689	172.24.55.6	172.24.55.134	TCP	66	33176 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=168610
6	0.003888	172.24.55.6	172.24.55.134	HTTP	458	GET /test.html HTTP/1.1
7	0.004602	172.24.55.134	172.24.55.6	TCP	66	http > 33176 [ACK] Seq=1 Ack=393 Win=15616 Len=0 TSval=2009
8	0.005225	172.24.55.134	172.24.55.6	HTTP	275	HTTP/1.1 304 Not Modified
9	0.005245	172.24.55.6	172.24.55.134	TCP	66	33176 > http [ACK] Seq=393 Ack=210 Win=15744 Len=0 TSval=16

- ▶ Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
- ▶ Ethernet II, Src: fa:16:3e:39:28:49 (fa:16:3e:39:28:49), Dst: fa:16:3e:2d:a9:7c (fa:16:3e:2d:a9:7c)
- ▶ Internet Protocol Version 4, Src: 172.24.55.134 (172.24.55.134), Dst: 172.24.55.6 (172.24.55.6)
- ▶ Transmission Control Protocol, Src Port: http (80), Dst Port: 33176 (33176), Seq: 0, Ack: 1, Len: 0

Source port: http (80)

Destination port: 33176 (33176)

[Stream index: 1]

Sequence number: 0 (relative sequence number)

Acknowledgement number: 1 (relative ack number)

Header length: 40 bytes

- ▶ Flags: 0x012 (SYN, ACK)

Window size value: 14480

[Calculated window size: 14480]

- ▶ Checksum: 0x9d15 [validation disabled]

- ▶ Options: (20 bytes)

- ▶ [SEQ/ACK analysis]

Server's sequence number, s\_sn = 0

Acknowledge client's packet, ack=c\_sn+1=1

# Client's ACK Packet

3	0.001822	172.24.55.6	172.24.55.134	TCP	74	33176 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM
4	0.003653	172.24.55.134	172.24.55.6	TCP	74	http > 33176 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=146
5	0.003689	172.24.55.6	172.24.55.134	TCP	66	33176 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=168610
6	0.003888	172.24.55.6	172.24.55.134	HTTP	458	GET /test.html HTTP/1.1
7	0.004602	172.24.55.134	172.24.55.6	TCP	66	http > 33176 [ACK] Seq=1 Ack=393 Win=15616 Len=0 TSval=2009
8	0.005225	172.24.55.134	172.24.55.6	HTTP	275	HTTP/1.1 304 Not Modified
9	0.005245	172.24.55.6	172.24.55.134	TCP	66	33176 > http [ACK] Seq=393 Ack=210 Win=15744 Len=0 TSval=16

- ▶ Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
- ▶ Ethernet II, Src: fa:16:3e:2d:a9:7c (fa:16:3e:2d:a9:7c), Dst: fa:16:3e:39:28:49 (fa:16:3e:39:28:49)
- ▶ Internet Protocol Version 4, Src: 172.24.55.6 (172.24.55.6), Dst: 172.24.55.134 (172.24.55.134)
- ▼ Transmission Control Protocol, Src Port: 33176 (33176), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0

Source port: 33176 (33176)

Destination port: http (80)

[Stream index: 1]

Sequence number: 1 (relative sequence number)

Acknowledgement number: 1 (relative ack number)

Header length: 32 bytes

client's sequence number,  $c\_sn+1 = 1$

Acknowledge server's packet,  $ack=s\_sn+1=1$

- ▶ Flags: 0x010 (ACK)

Window size value: 115

[Calculated window size: 14720]

[Window size scaling factor: 128]

- ▶ Checksum: 0xc6e3 [validation disabled]

- ▶ Options: (12 bytes)

# HTTP Request Packet

3	0.001822	172.24.55.6	172.24.55.134	TCP	74	33176 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK PERM
4	0.003653	172.24.55.134	172.24.55.6	TCP	74	http > 33176 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=146
5	0.003689	172.24.55.6	172.24.55.134	TCP	66	33176 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=168610
6	0.003888	172.24.55.6	172.24.55.134	HTTP	458	GET /test.html HTTP/1.1
7	0.004602	172.24.55.134	172.24.55.6	TCP	66	http > 33176 [ACK] Seq=1 Ack=393 Win=15616 Len=0 TSval=20092
8	0.005225	172.24.55.134	172.24.55.6	HTTP	275	HTTP/1.1 304 Not Modified
9	0.005245	172.24.55.6	172.24.55.134	TCP	66	33176 > http [ACK] Seq=393 Ack=210 Win=15744 Len=0 TSval=168

- ▶ Frame 6: 458 bytes on wire (3664 bits), 458 bytes captured (3664 bits)
- ▶ Ethernet II, Src: fa:16:3e:2d:a9:7c (fa:16:3e:2d:a9:7c), Dst: fa:16:3e:39:28:49 (fa:16:3e:39:28:49)
- ▶ Internet Protocol Version 4, Src: 172.24.55.6 (172.24.55.6), Dst: 172.24.55.134 (172.24.55.134)
- ▼ Transmission Control Protocol, Src Port: 33176 (33176), Dst Port: http (80), Seq: 1, Ack: 1, Len: 392

Source port: 33176 (33176)

Destination port: http (80)

[Stream index: 1]

Sequence number: 1 (relative sequence number)

[Next sequence number: 393 (relative sequence number)]

Acknowledgement number: 1 (relative ack number)

Header length: 32 bytes

▶ Flags: 0x018 (PSH, ACK)

Window size value: 115

[Calculated window size: 14720]

[Window size scaling factor: 128]

▶ Checksum: 0xc86b [validation disabled]

$c\_sn = 1$ , since no data has been transmitted since the last packet.

$n\_sn = sn + len$

$ack = 1$ , since no data has been received from server, either.

# ACK from Server

3	0.001822	172.24.55.6	172.24.55.134	TCP	74	33176 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM
4	0.003653	172.24.55.134	172.24.55.6	TCP	74	http > 33176 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460
5	0.003689	172.24.55.6	172.24.55.134	TCP	66	33176 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=168610
6	0.003888	172.24.55.6	172.24.55.134	HTTP	458	GET /test.html HTTP/1.1
7	0.004602	172.24.55.134	172.24.55.6	TCP	66	http > 33176 [ACK] Seq=1 Ack=393 Win=15616 Len=0 TSval=20092
8	0.005225	172.24.55.134	172.24.55.6	HTTP	275	HTTP/1.1 304 Not Modified
9	0.005245	172.24.55.6	172.24.55.134	TCP	66	33176 > http [ACK] Seq=393 Ack=210 Win=15744 Len=0 TSval=168610

- ▶ Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
- ▶ Ethernet II, Src: fa:16:3e:39:28:49 (fa:16:3e:39:28:49), Dst: fa:16:3e:2d:a9:7c (fa:16:3e:2d:a9:7c)
- ▶ Internet Protocol Version 4, Src: 172.24.55.134 (172.24.55.134), Dst: 172.24.55.6 (172.24.55.6)
- ▶ Transmission Control Protocol, Src Port: http (80), Dst Port: 33176 (33176), Seq: 1, Ack: 393, Len: 0

Source port: http (80)

Destination port: 33176 (33176)

[Stream index: 1]

Sequence number: 1 (relative sequence number)

Acknowledgement number: 393 (relative ack number)

Header length: 32 bytes

▶ Flags: 0x010 (ACK)

Window size value: 122

[Calculated window size: 15616]

[Window size scaling factor: 128]

▶ Checksum: 0x0270 [validation disabled]

▶ Options: (12 bytes)

▶ [SEQ/ACK analysis]

s\_sn= 1, since no data has been transmitted since the last packet.

ack=len(payload in the client's request) + 1

# HTTP Response Packet

3	0.001822	172.24.55.6	172.24.55.134	TCP	74	33176 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM
4	0.003653	172.24.55.134	172.24.55.6	TCP	74	http > 33176 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=146
5	0.003689	172.24.55.6	172.24.55.134	TCP	66	33176 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=168610
6	0.003888	172.24.55.6	172.24.55.134	HTTP	458	GET /test.html HTTP/1.1
7	0.004602	172.24.55.134	172.24.55.6	TCP	66	http > 33176 [ACK] Seq=1 Ack=393 Win=15616 Len=0 TSval=20092
8	0.005225	172.24.55.134	172.24.55.6	HTTP	275	HTTP/1.1 304 Not Modified
9	0.005245	172.24.55.6	172.24.55.134	TCP	66	33176 > http [ACK] Seq=393 Ack=210 Win=15744 Len=0 TSval=168

Frame 8: 275 bytes on wire (2200 bits), 275 bytes captured (2200 bits)  
 Ethernet II, Src: fa:16:3e:39:28:49 (fa:16:3e:39:28:49), Dst: fa:16:3e:2d:a9:7c (fa:16:3e:2d:a9:7c)  
 Internet Protocol Version 4, Src: 172.24.55.134 (172.24.55.134), Dst: 172.24.55.6 (172.24.55.6) **Payload length**  
 Transmission Control Protocol, Src Port: http (80), Dst Port: 33176 (33176), Seq: 1, Ack: 393, Len: 209  
 Source port: http (80)  
 Destination port: 33176 (33176)  
 [Stream index: 1]  
 Sequence number: 1 (relative sequence number)  
 [Next sequence number: 210 (relative sequence number)]  
 Acknowledgement number: 393 (relative ack number)  
 Header length: 32 bytes  
 Flags: 0x018 (PSH, ACK) **Ack number remains the same**  
 Window size value: 122  
 [Calculated window size: 15616]  
 [Window size scaling factor: 128]  
 Checksum: 0x374a [validation disabled]  
 Options: (12 bytes)

# ACK from Client

3	0.001822	172.24.55.6	172.24.55.134	TCP	74	33176 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM
4	0.003653	172.24.55.134	172.24.55.6	TCP	74	http > 33176 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=146
5	0.003689	172.24.55.6	172.24.55.134	TCP	66	33176 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=168610
6	0.003888	172.24.55.6	172.24.55.134	HTTP	458	GET /test.html HTTP/1.1
7	0.004602	172.24.55.134	172.24.55.6	TCP	66	http > 33176 [ACK] Seq=1 Ack=393 Win=15616 Len=0 TSval=2009
8	0.005225	172.24.55.134	172.24.55.6	HTTP	275	HTTP/1.1 304 Not Modified
9	0.005245	172.24.55.6	172.24.55.134	TCP	66	33176 > http [ACK] Seq=393 Ack=210 Win=15744 Len=0 TSval=16

Frame 9: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)  
 Ethernet II, Src: fa:16:3e:2d:a9:7c (fa:16:3e:2d:a9:7c), Dst: fa:16:3e:39:28:49 (fa:16:3e:39:28:49)  
 Internet Protocol Version 4, Src: 172.24.55.6 (172.24.55.6), Dst: 172.24.55.134 (172.24.55.134)  
 Transmission Control Protocol, Src Port: 33176 (33176), Dst Port: http (80), Seq: 393, Ack: 210, Len: 0

Source port: 33176 (33176)

Destination port: http (80)

[Stream index: 1]

Sequence number: 393 (relative sequence number)

Acknowledgement number: 210 (relative ack number)

Header length: 32 bytes

Flags: 0x010 (ACK)

Window size value: 123

[Calculated window size: 15744]

[Window size scaling factor: 128]

Checksum: 0xc6e3 [validation disabled]

Options: (12 bytes)

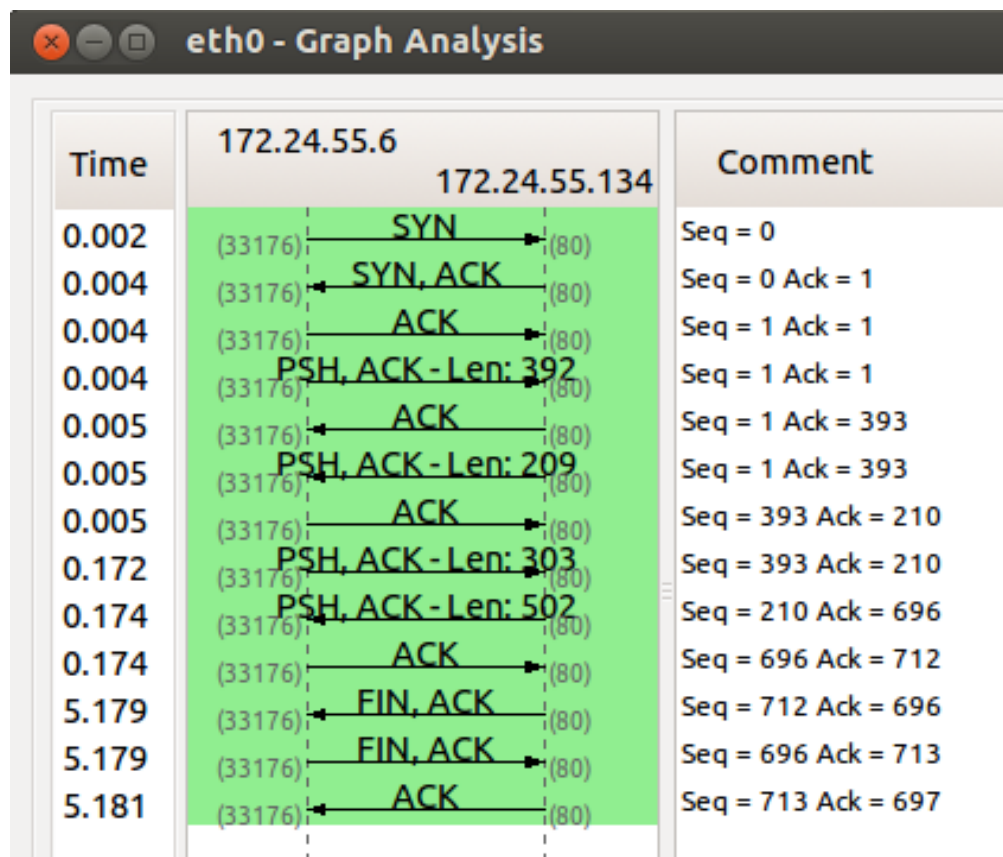
[SEQ/ACK analysis]

$c\_sn = c\_sn + 1$

$ack = len(\text{payload in the server's response}) + 1$

# TCP Flow

In Wireshark, **Statistics > Flow Graph...**, select **TCP flow** and click **OK**.



# Protocol Analysis Process

- Identify the problem “symptoms”
  - What appears to be happening / not happening that is a concern
  - Identify the machines (hosts) involved
  - Identify the protocols involved
  - Set up capture filters to define what packets will be gathered.
  - Capture and analyze packets.

# Summary

- Review a popular Internet Service
- Overview of Wireshark
- Packet Analysis of Internet service communications