TCP/IP Overview

Mohd Akram Khan, GCIH
Scientist 'B'

Agenda

Part 01

- OSI and TCP/IP Protocol Stack
- TCP/IP Layers
- TCP/IP Protocols

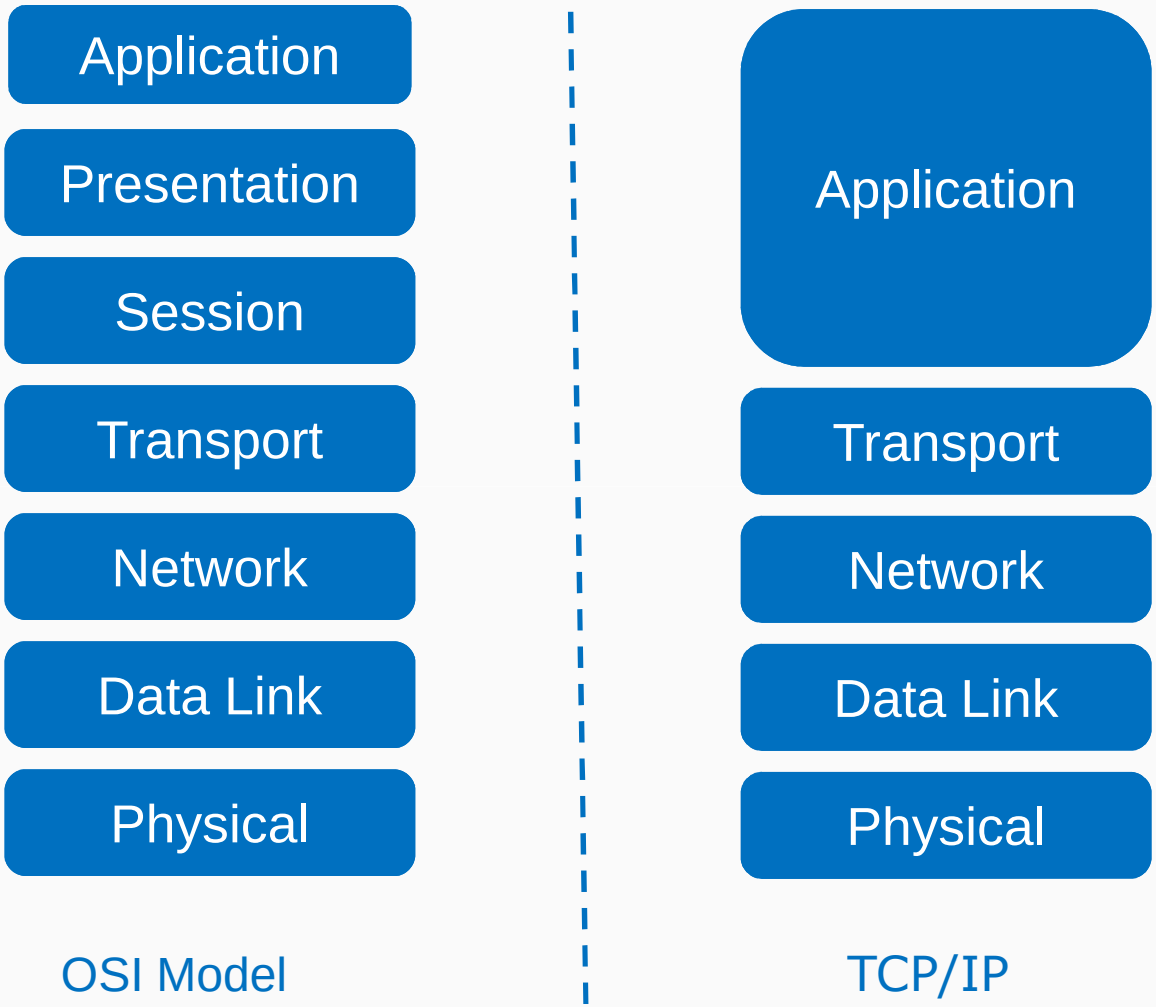
Part 02

- Network Traffic Analysis
- Traffic Analysis Approaches
- Network Flow
- Inline Monitoring
- Logs

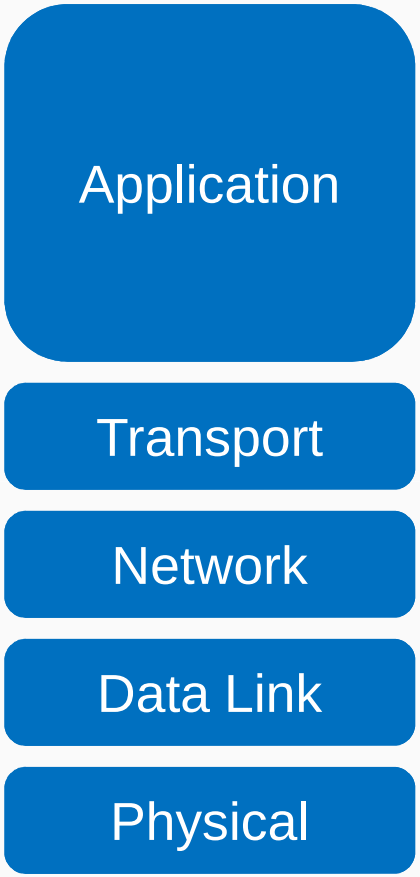
TCP/IP

- A highly standardized protocol used widely on the Internet
- Standards area available in the form of RFC documents
  - Request For Comments (RFC)
- Standards are overseen by the Internet Engineering Task Force (IETF)

OSI and TCP/IP



TCP/IP Layers



Handles the details of the particular Application

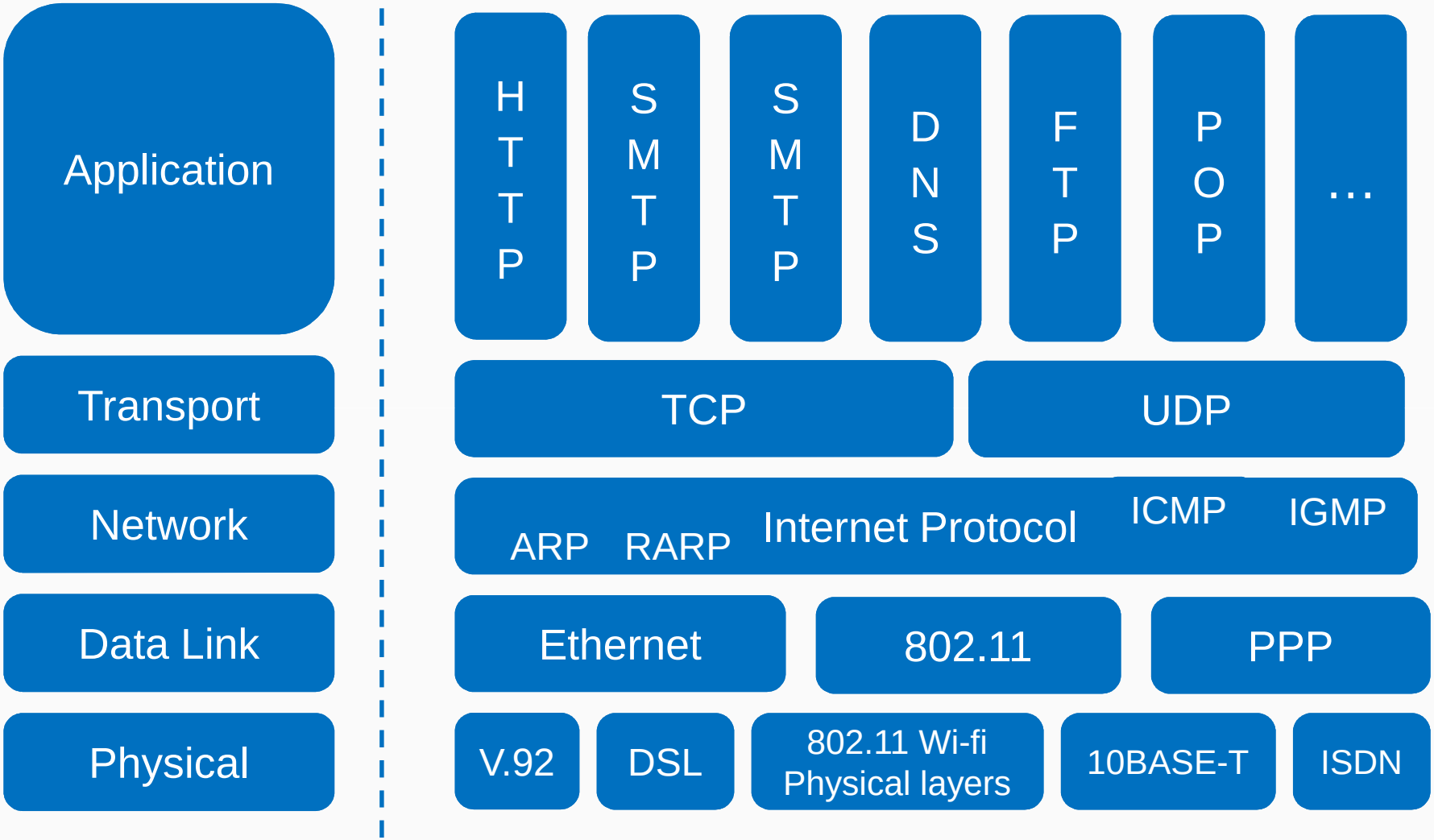
Data delivery, connection initiation, error control and sequence checking.

Responsible for data addressing, transmission, and packet fragmentation and reassembly.

Specifies procedures for transmitting data across the network, including how to access the physical medium.

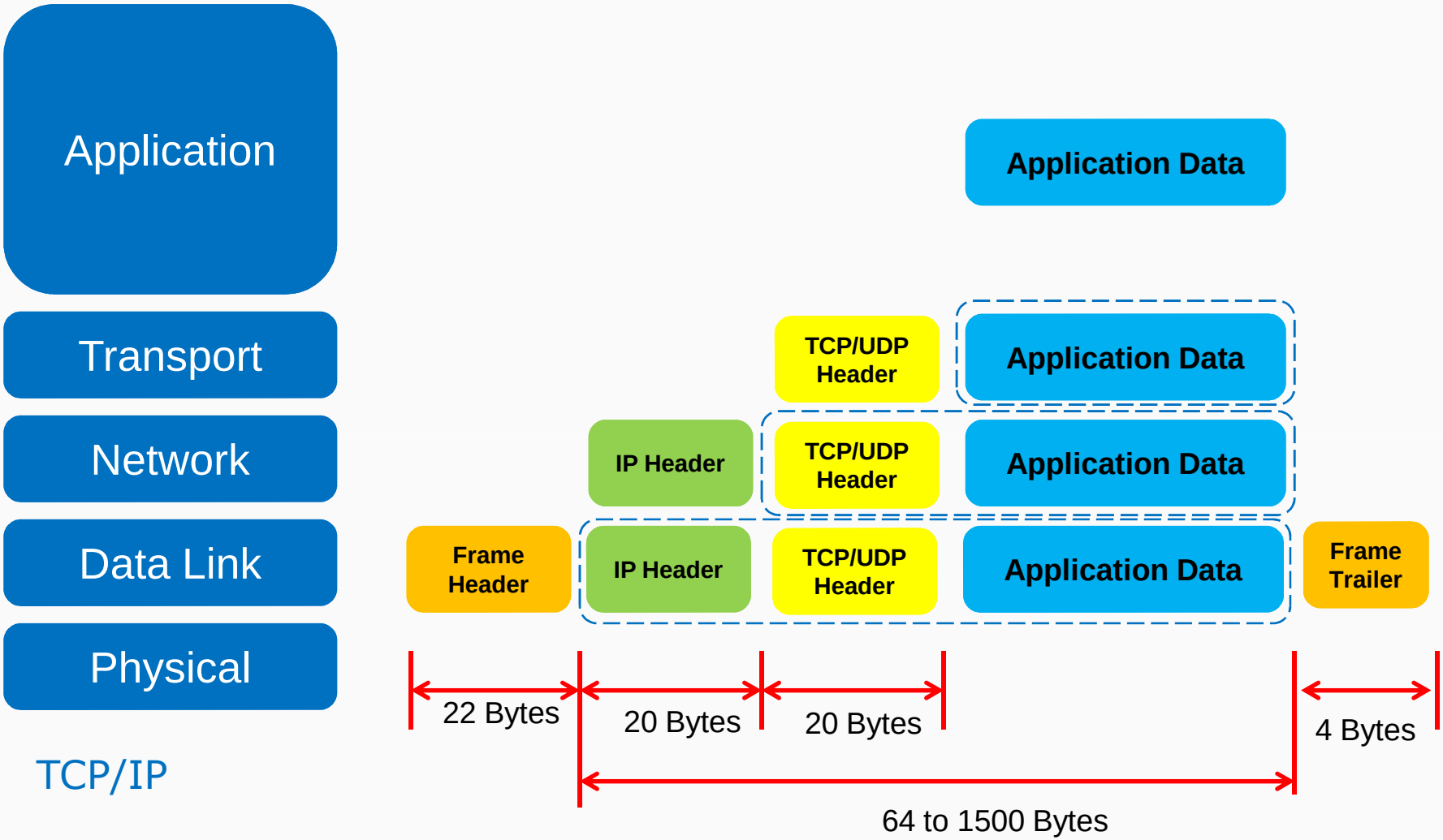
Interface, Medium specification, Encoding, Signaling, Data Transmission and Reception

TCP/IP Protocols



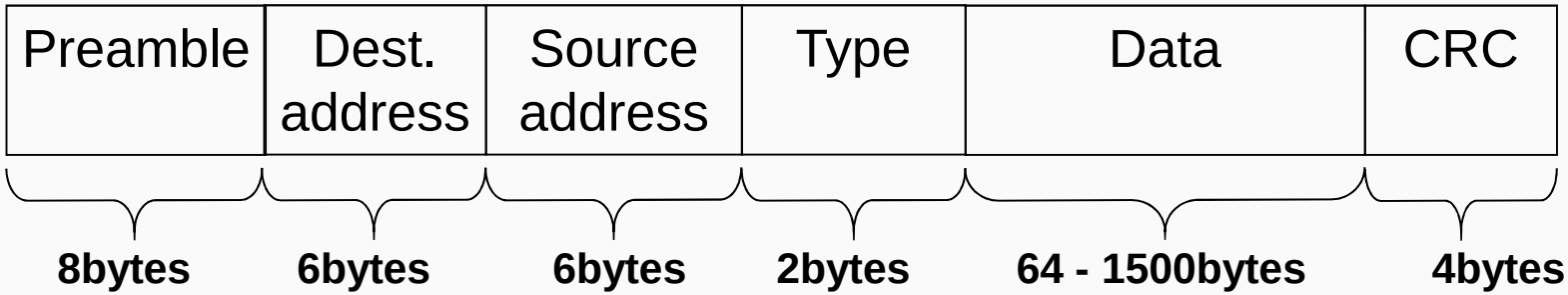
TCP/IP Protocols

Packet Encapsulation



Ethernet

- Computer to Computer communication
- Interface has unique 48 bit long address MAC address
  example: 00-26-15-55-5a-c6



ARP : Address Resolution Protocol

- ARP/RARP provides mapping

  32bit IP address ⟷ 48bit MAC address

  192.168.1.1 ⟷ 00-26-15-55-5a-c6

- ARP cache

  contains mappings from IP addresses to MAC addresses

Protocol

1. ARP request broadcast on Ethernet
2. Destination host responds ARP with MAC Address

Source	Destination	Protocol	Info
GemtekTe_a6:b6:17	Broadcast	ARP	Who has 192.168.1.1? Tell 192.168.1.5
Teracom_55:5a:c6	GemtekTe_a6:b6:17	ARP	192.168.1.1 is at 00:26:15:55:5a:c6

IP: Internet Protocol

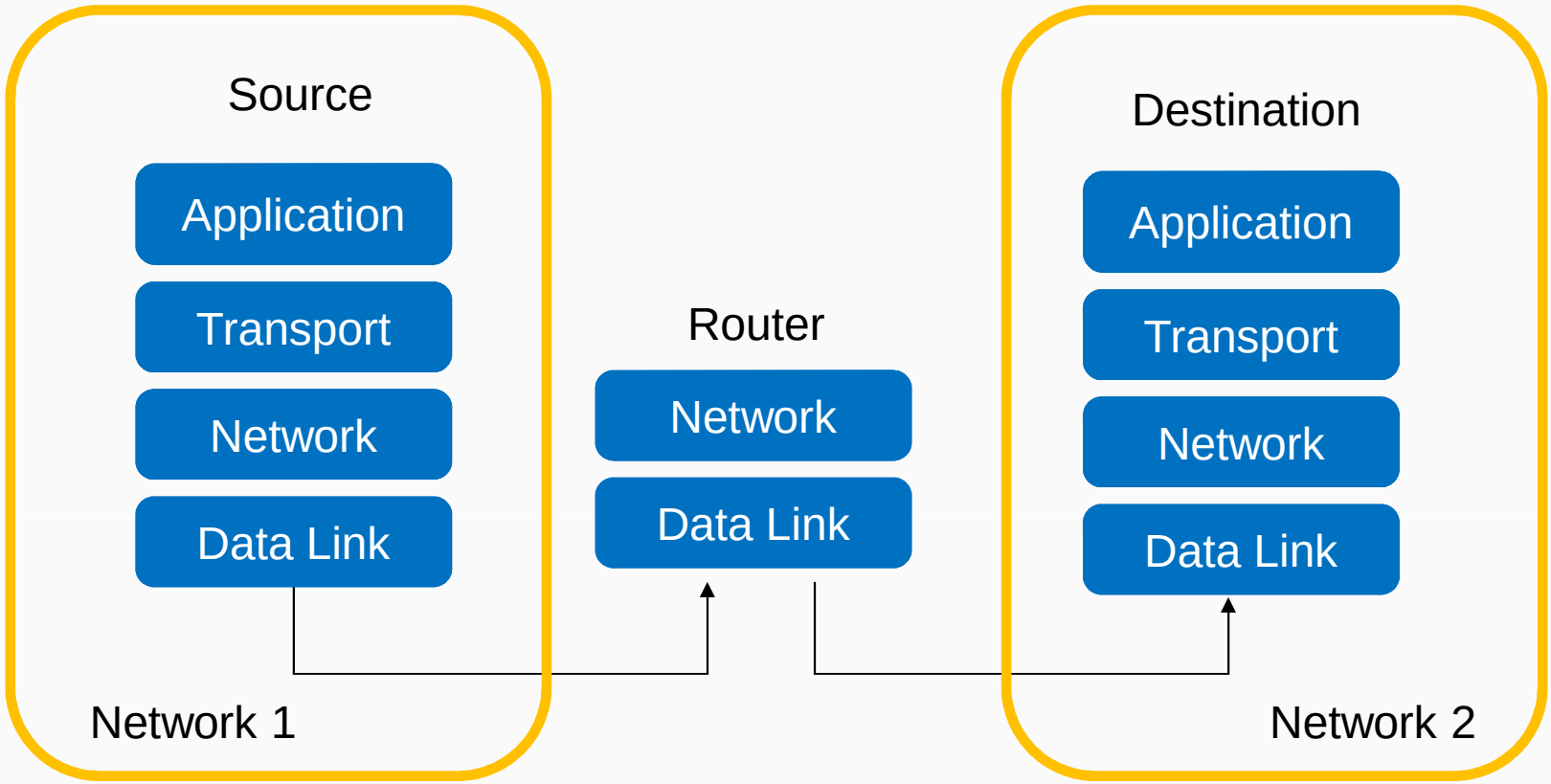
- Packaging
  - Fragmentation and Reassembly
- Addressing
  - Unique 32 bit IP Address
- Routing
  - Best-effort connectionless IP packet transfer:
  - no setup, routed independently, robust, out of order, duplicate, or lose of packet

IP Header

IP Header: 4500002800a2400039062857ca8d8c9cc0a80105

```
Internet Protocol, Src: 202.141.140.156 (202.141.140.156), Dst: 192.168.1.5 (192.168.1.5)
  Version: 4
  Header length: 20 bytes
⊟ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..0. = ECN-Capable Transport (ECT): 0
    .... ...0 = ECN-CE: 0
  Total Length: 40
  Identification: 0x00a2 (162)
⊟ Flags: 0x02 (Don't Fragment)
    0.. = Reserved bit: Not Set
    .1. = Don't fragment: Set
    ..0 = More fragments: Not Set
  Fragment offset: 0
  Time to live: 57
  Protocol: TCP (0x06)
⊟ Header checksum: 0x2857 [correct]
    [Good: True]
    [Bad : False]
  Source: 202.141.140.156 (202.141.140.156)
  Destination: 192.168.1.5 (192.168.1.5)
```

IP Routing

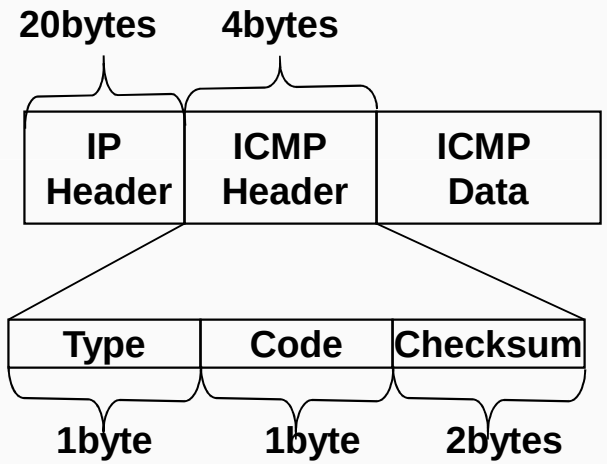


- Routing Table
  - Destination IP address
  - IP address of a next-hop router

ICMP : Internet Control Message Protocol

- Handles errors and control information for IP
  - Report problems with delivery of IP Datagrams
  - ping, traceroute

ICMP Message



Types and Codes

- Echo Request (type=8, code=0)
- Echo Reply(type=0, code=0)
- Destination Unreachable(type=3, code=0)
- Time Exceeded(type=11, code=0) :
  Time-to-Live =0

```
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0 ()
  Checksum: 0x5552 [correct]
  Identifier: 0x0001
  Sequence number: 9 (0x0009)
Data (32 bytes)
  Data: 6162636465666768696A6B6C6D6E6F707172737475767761...
  [Length: 32]
```

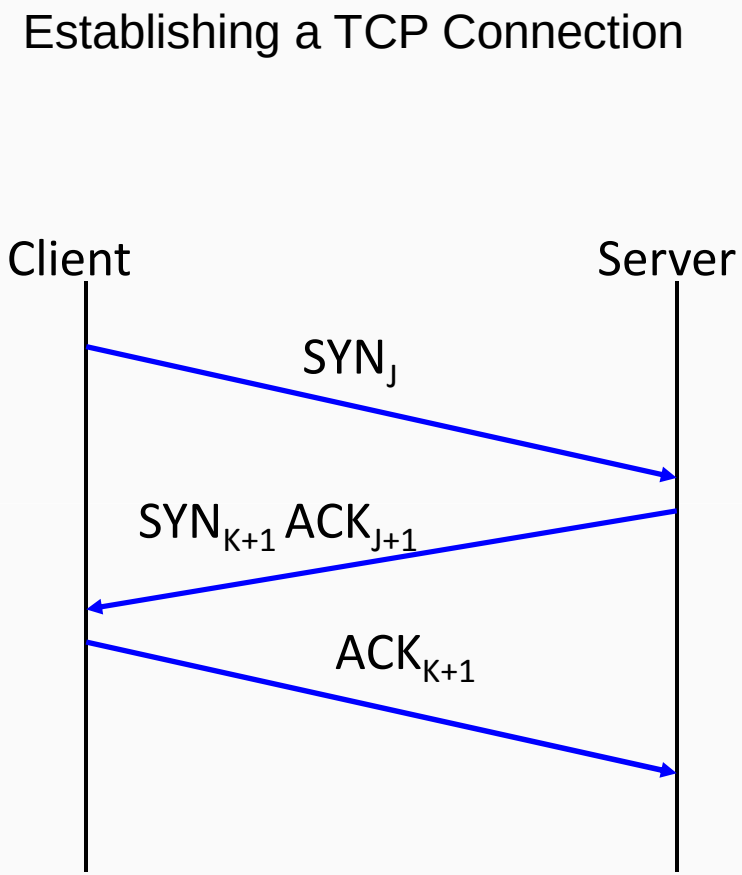
```
Info
Echo (ping) request
Echo (ping) reply
```

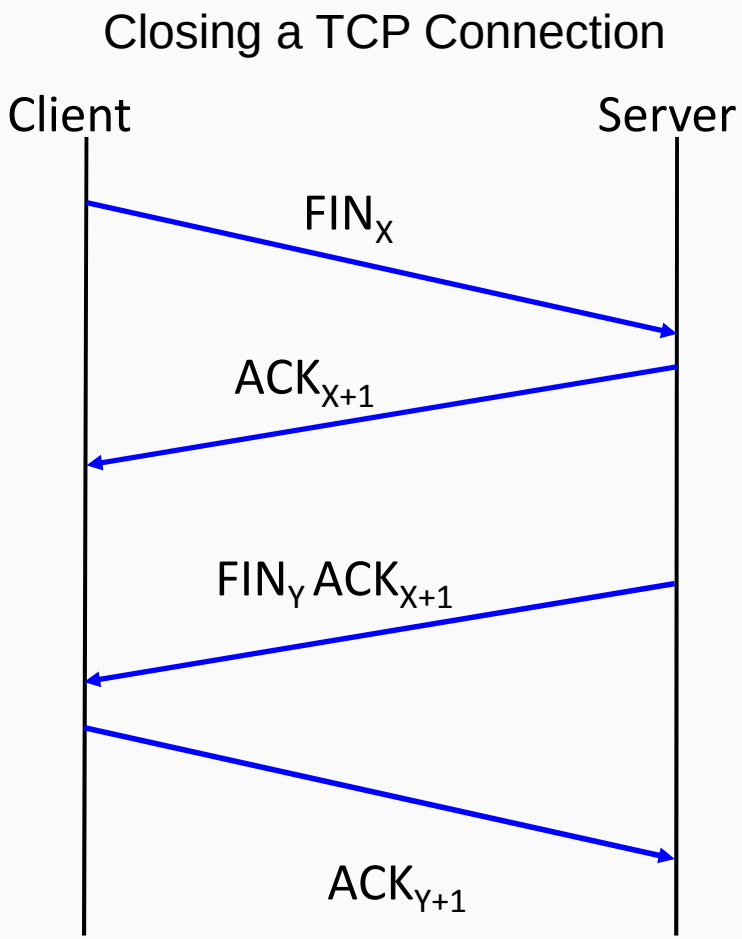
TCP: Transmission Control Protocol

- Connection-Oriented, Reliable, Byte Stream Service
  - Connection establishment/release
  - Sequence number, acknowledgement, retransmission, timeout (RTT)
    - Sliding window protocol
  - Flow control/Congestion control

- Operation
  1. Set up connection
  2. Transfer data
  3. Close connection

Establishing a TCP Connection





TCP Header

```
Transmission Control Protocol, Src Port: 63889 (63889), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
  Source port: 63889 (63889)
  Destination port: http (80)
  [Stream index: 24]
  Sequence number: 1    (relative sequence number)
  Acknowledgement number: 1    (relative ack number)
  Header length: 20 bytes
⊟ Flags: 0x10 (ACK)
    0... .... = Congestion Window Reduced (CWR): Not set
    .0.. .... = ECN-Echo: Not set
    ..0. .... = Urgent: Not set
    ...1 .... = Acknowledgement: Set
    .... 0... = Push: Not set
    .... .0.. = Reset: Not set
    .... ..0. = Syn: Not set
    .... ...0 = Fin: Not set
  Window size: 17160 (scaled)
⊞ Checksum: 0x900e [validation disabled]
⊟ [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 66]
    [The RTT to ACK the segment was: 0.000028000 seconds]
```

UDP: User Datagram Protocol

- Unreliable and connectionless
  - Data may be lost, duplicated and reordered..
  - Used for the transmission of small amount of data
  - Accuracy is not desired
  - No connection establishment overhead
  - Faster compared to TCP

```
User Datagram Protocol, Src Port: 60163 (60163), Dst Port: domain (53)
  Source port: 60163 (60163)
  Destination port: domain (53)
  Length: 41
⊟ Checksum: 0x9bb1 [validation disabled]
```

Application Layer Protocols

- Provide services that can be used by applications / softwares / users
- New protocols are continuously evolving
  - E.g. HTTP, DNS, FTP, Telnet, SMTP, POP3, IMAP, SNMP etc.

Hyper Text Transfer Protocol (HTTP)

- Stateless Transaction Protocol

  Each transaction creates a new connection

<u>Protocol</u>

1. Request

   Method (GET/POST/PUT etc.) <URL>

   <Data>

2. Response

   Response Code (200,302,404,500 etc)

   <Data>

```
GET / HTTP/1.1
Host: www.cert-in.org.in
Connection: keep-alive
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.11 (
Safari/535.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: JSESSIONID=759EF8BE8CB4C5A32ADC0F8B73714695;
K_V_D_JSESSIONID=jbiimlnfjeonebkghpjgmchcjpbapmjfoknjojobhdgogphkgll

HTTP/1.1 200 OK
Date: Thu, 01 Mar 2012 17:37:20 GMT
Content-type: text/html;charset=ISO-8859-1
Content-length: 369
Set-cookie: JSESSIONID=A9EBDE670B670975D632EBBB294C933E; Path=/
Set-Cookie:  K_V_D_JSESSIONID=hcgiemankffnaomdonkmcnpmomkcifooaefnbbl
Path=/

<html>
.<head>
..<TITLE>Indian - Computer Emergency Response Team</TITLE>
.</head>
.<frameset framespacing="0" border="0" frameborder="0" rows="0,*">
..<frame name="top_frame" target="contents" src="about:blank"
...frameborder="no" scrolling="no">
..<frame name="test" src="./s2cMainServlet?pageid=PUBWEL01"
...frameborder="no" scrolling="yes">
.</frameset>
```

Hyper Text Transfer Protocol (HTTP)

- Common Request Methods

  GET, POST, OPTIONS, HEAD, PUT

- Response Codes

  Informational :100

  Success :200

  Redirection :300

  Client Error :400

  Server Error :500

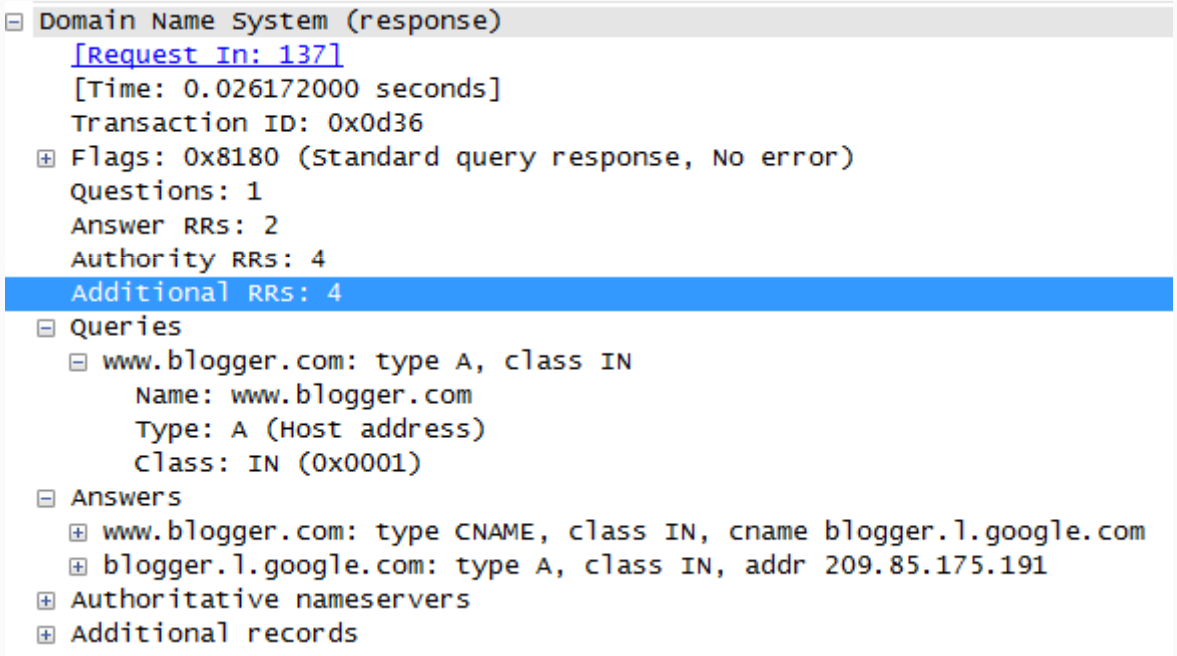
DNS: Domain Naming System

- Resolves domain names to IP addresses and vice versa
- Uses UDP for normal operations

1. DNS Query

2. DNS Query Response

Source	Destination	Protocol	Info
192.168.1.5	192.168.1.1	DNS	Standard query A www.blogger.com
192.168.1.1	192.168.1.5	DNS	Standard query response CNAME blogger.l.google.com A 209.85.175.191



Thank You