Understanding TCP/IP Model

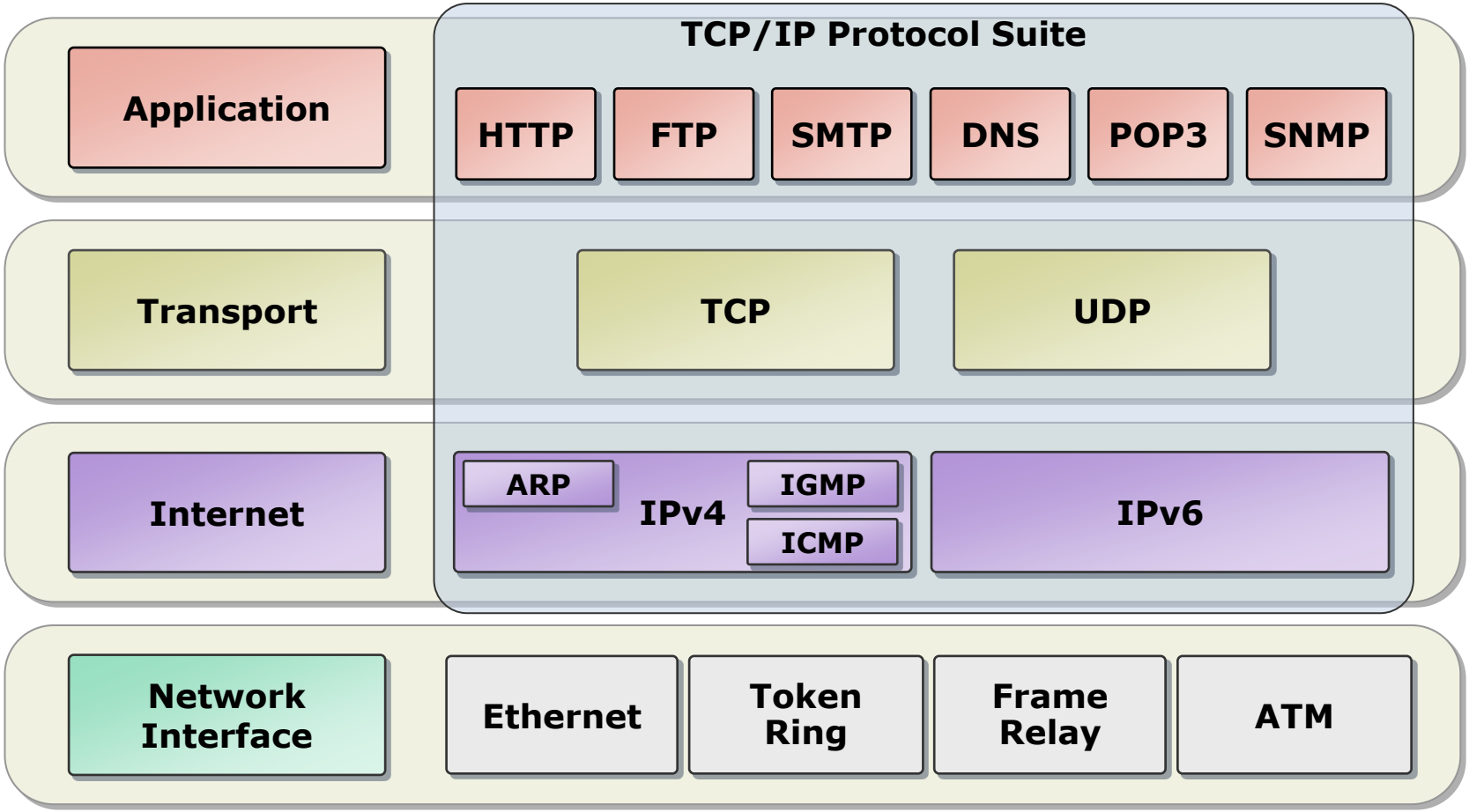
Module Overview

- Overview of TCP/IP
- Understanding IPv4 Addressing
- Understanding IPv6
- Name Resolution
- TCP Flow Control

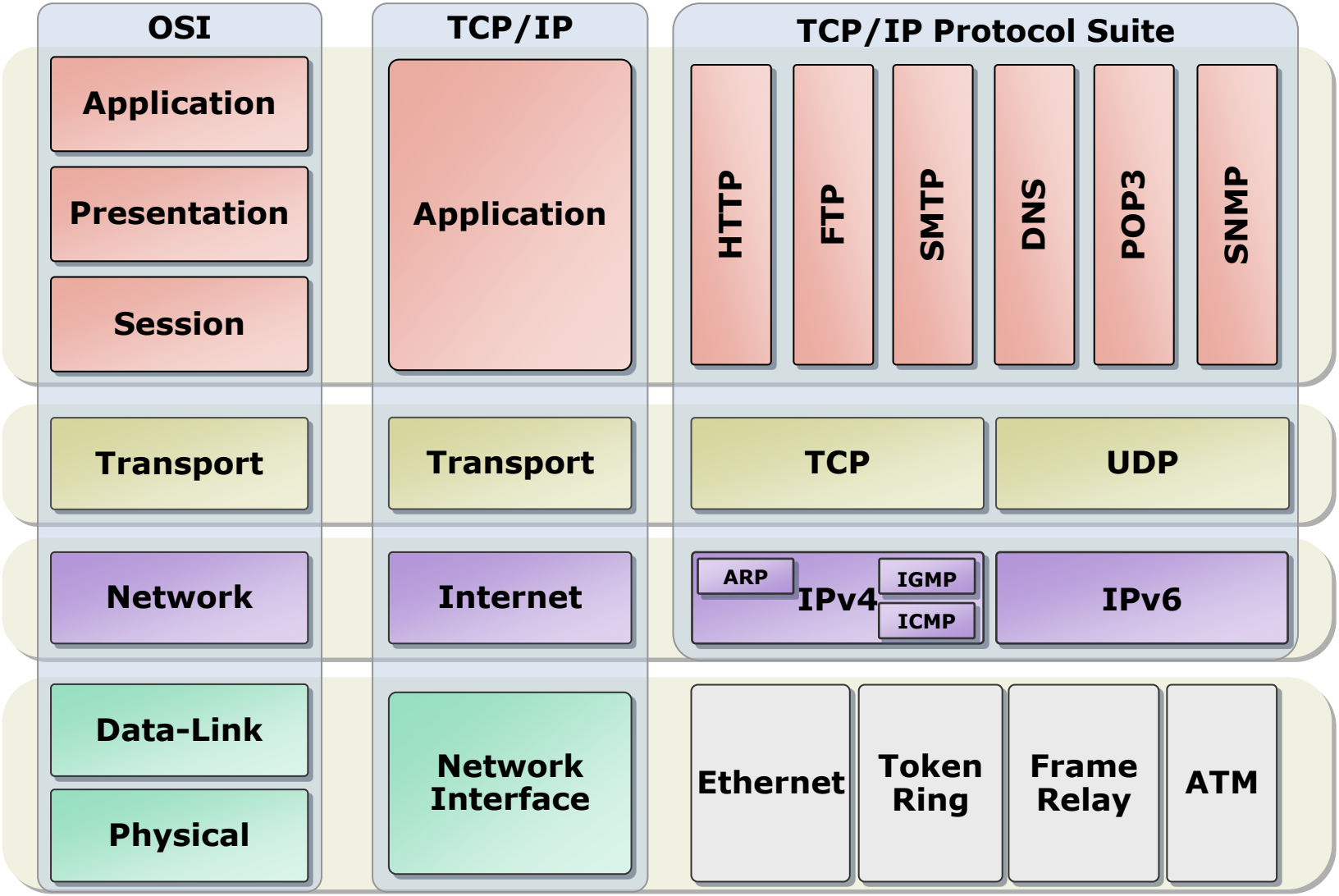
Overview of TCP/IP

- The TCP/IP Protocol Suite
- Protocols in the TCP/IP Suite
- TCP/IP Applications
- What Is a Socket?

The TCP/IP Protocol Suite



Protocols in the TCP/IP Suite

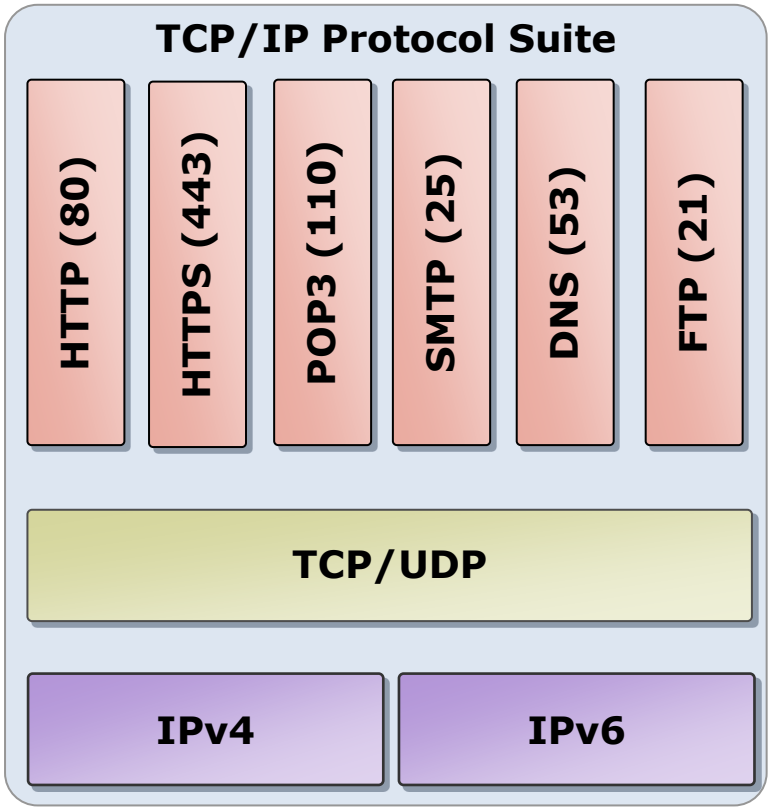


TCP/IP Applications

Some common application layer protocols are:

- **HTTP/HTTPS**
- **RPC over HTTP**
- **FTP**
- **RDP**
- **SMB**
- **SMTP**
- **POP3**

What Is a Socket?



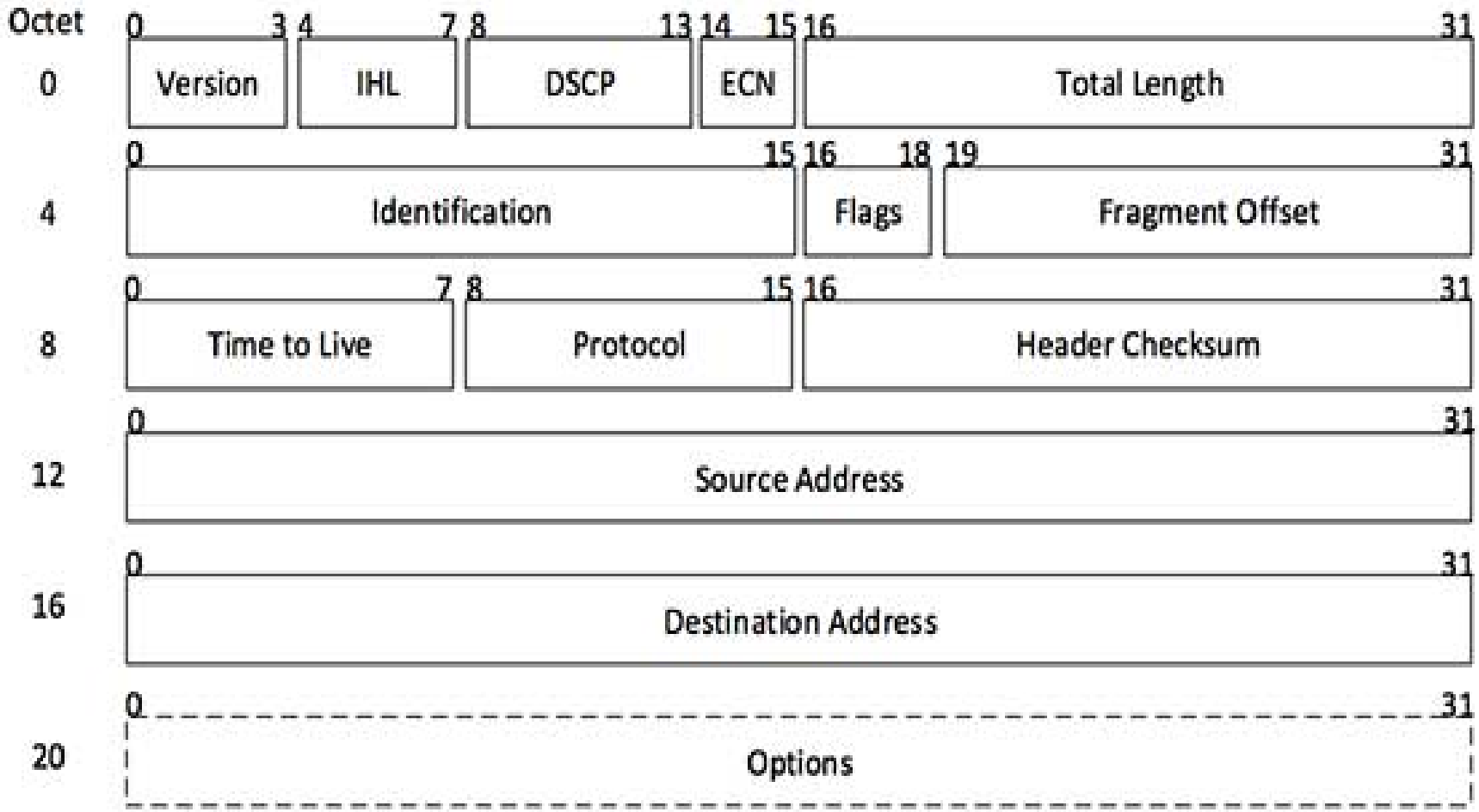
Understanding IPv4 Addressing

- What is IPv4
- IPv4 Packet Structure
- IPv4 Addressing Modes
- How Dotted Decimal Notation Relates to Binary Numbers
- Simple IPv4 Implementations
- How Bits Are Used in a Subnet Mask
- Implementing an IPv4 Subnetting Scheme

What is IPv4

- Stands for **Internet Protocol** and **v4** stands for **Version Four** (IPv4) consisting of 32-bit addresses
- Consists of 3 Parts
  - Network Part, Host Part and Subnet Part
- Works in any mode
- Permits encryption to keep up privacy and security
- Relies on network layer addresses to identify end-points on network
- World's supply of unique IP addresses is dwindling

IPv4 Packet Structure



IPv4 Packet Structure

Version	Version no. of Internet Protocol used
IHL	Internet Header Length; **Indicates the number of 32-bit blocks in the IPv4 header**. The size of this field is 4 bits
DSCP	Differentiated Services Code Point; Ensures that certain types of traffic that require a relatively uninterrupted flow of data get precedence over other kinds of traffic
ECN	Explicit Congestion Notification; It carries information about the congestion seen in the route.
Total Length	Length of entire IP Packet (including IP header and IP Payload).
Identification	If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to
Flags	As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'

IPv4 Packet Structure

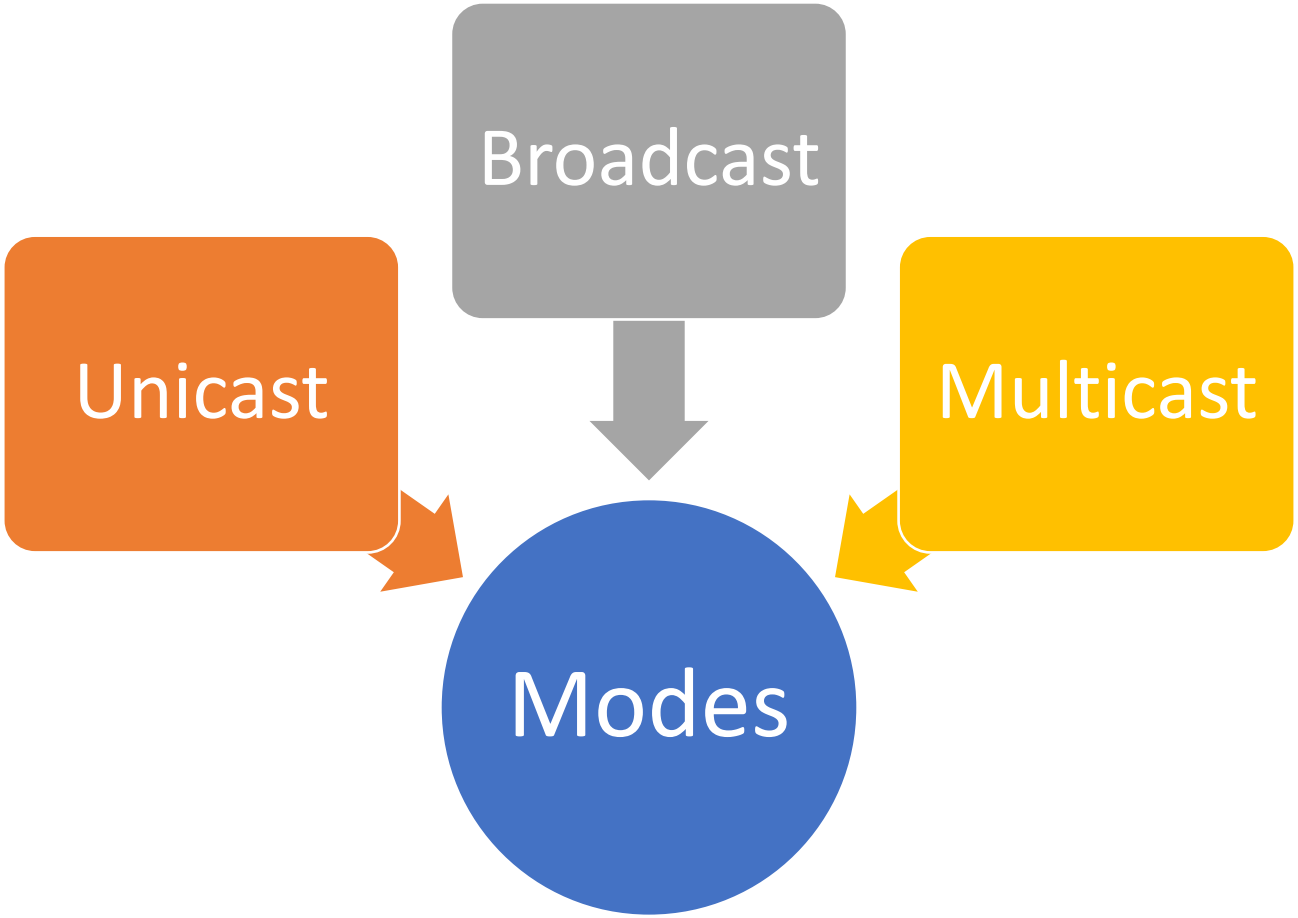
Fragment Offset	This offset tells the exact position of the fragment in the original IP Packet. The fragmentation offset value for the first fragment is always 0. The field is 13 bits wide. Max is (2^13 – 1) * 8 = 65528 offset
Time to Live	To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
Protocol	Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
Header Checksum	This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
Source Address	32-bit address of the Sender (or source) of the packet.
Destination Address	32-bit address of the Receiver (or destination) of the packet.
Options	This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

https://www.cloudshark.org/collections/WTRpgLI-GQSDfgzkQixICg

IPv4 Packet Structure - Example

```
▸ Frame 1: 680 bytes on wire (5440 bits), 680 bytes captured (5440 bits) on interface \Device\NPF_{62AEEC6F-7EEA-4EA
▸ Ethernet II, Src: Giga-Byt_9c:e2:71 (fc:aa:14:9c:e2:71), Dst: Cisco_7c:a2:8e (b0:aa:77:7c:a2:8e)
▾ Internet Protocol Version 4, Src: 10.56.100.2, Dst: 192.81.131.161
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
          0000 00.. = Differentiated Services Codepoint: Default (0)
          .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
      Total Length: 666
      Identification: 0x7088 (28808)
    ▾ Flags: 0x40, Don't fragment
          0... .... = Reserved bit: Not set
          .1.. .... = Don't fragment: Set
          ..0. .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 128
      Protocol: TCP (6)
      Header Checksum: 0x0000 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 10.56.100.2
      Destination Address: 192.81.131.161
    ▸ [Destination GeoIP: Fremont, US, ASN 63949, Akamai Connected Cloud]
▸ Transmission Control Protocol, Src Port: 64493, Dst Port: 80, Seq: 1, Ack: 1, Len: 626
▸ Hypertext Transfer Protocol
```

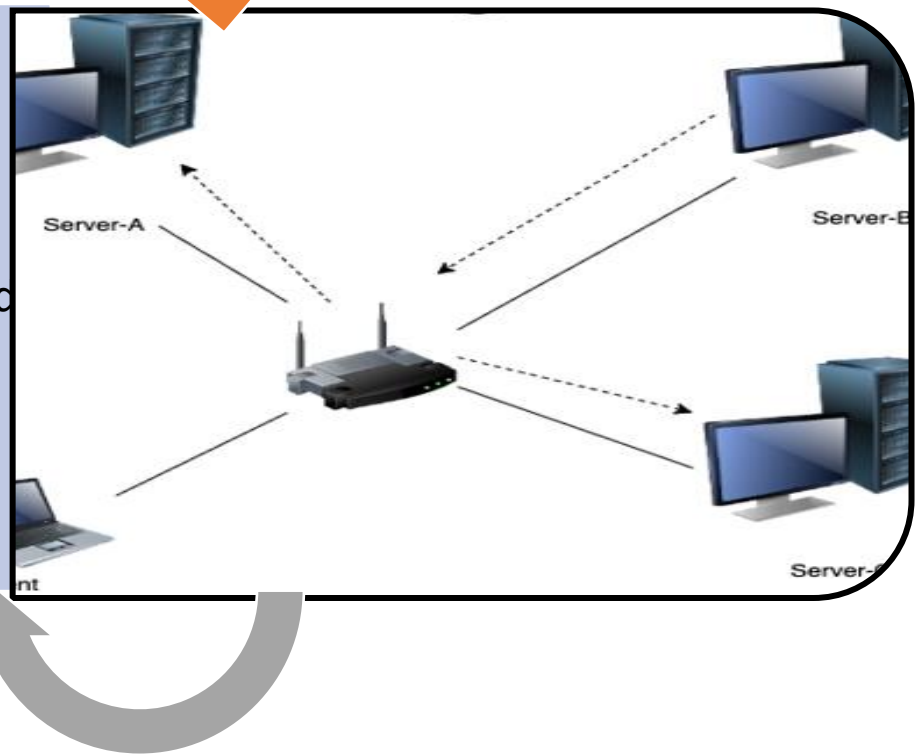
IPv4 Addressing Modes



IPv4 Addressing Modes

Unicast

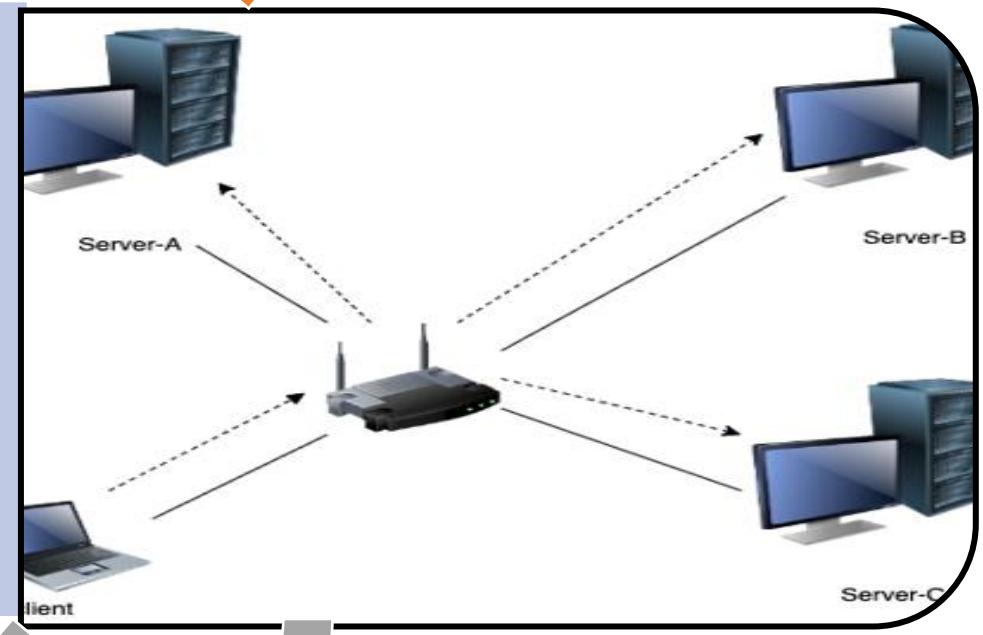
- Data sent to only one destination host
- Destination address field contains 32-bit address
- Client sends data to targeted server



IPv4 Addressing Modes

Broadcast

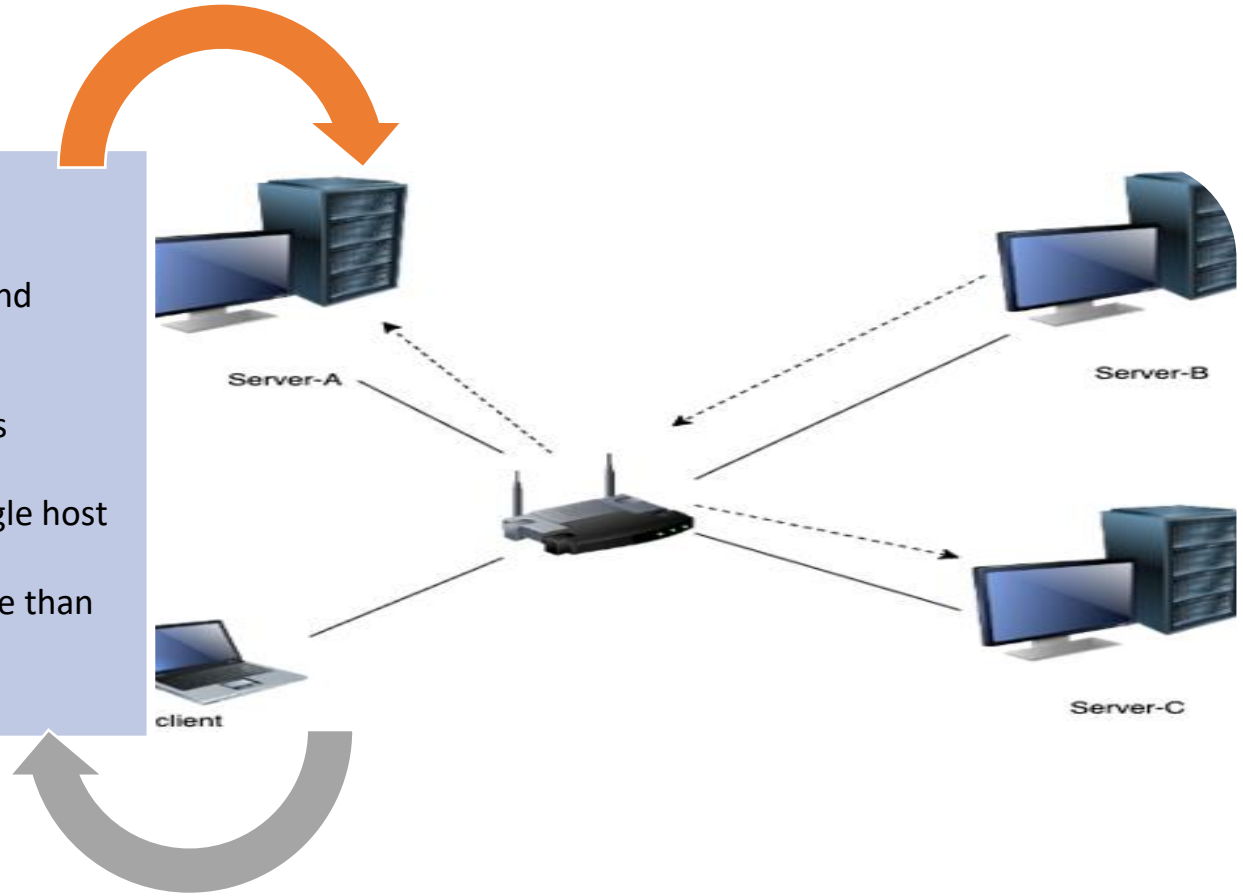
- The packet is addressed to all the hosts in the network segment
- The destination address field contains a special broadcast address (255.255.255.255)
- When a host/server sees the packet on the network, it is supposed to process the same
- The client sends the packet



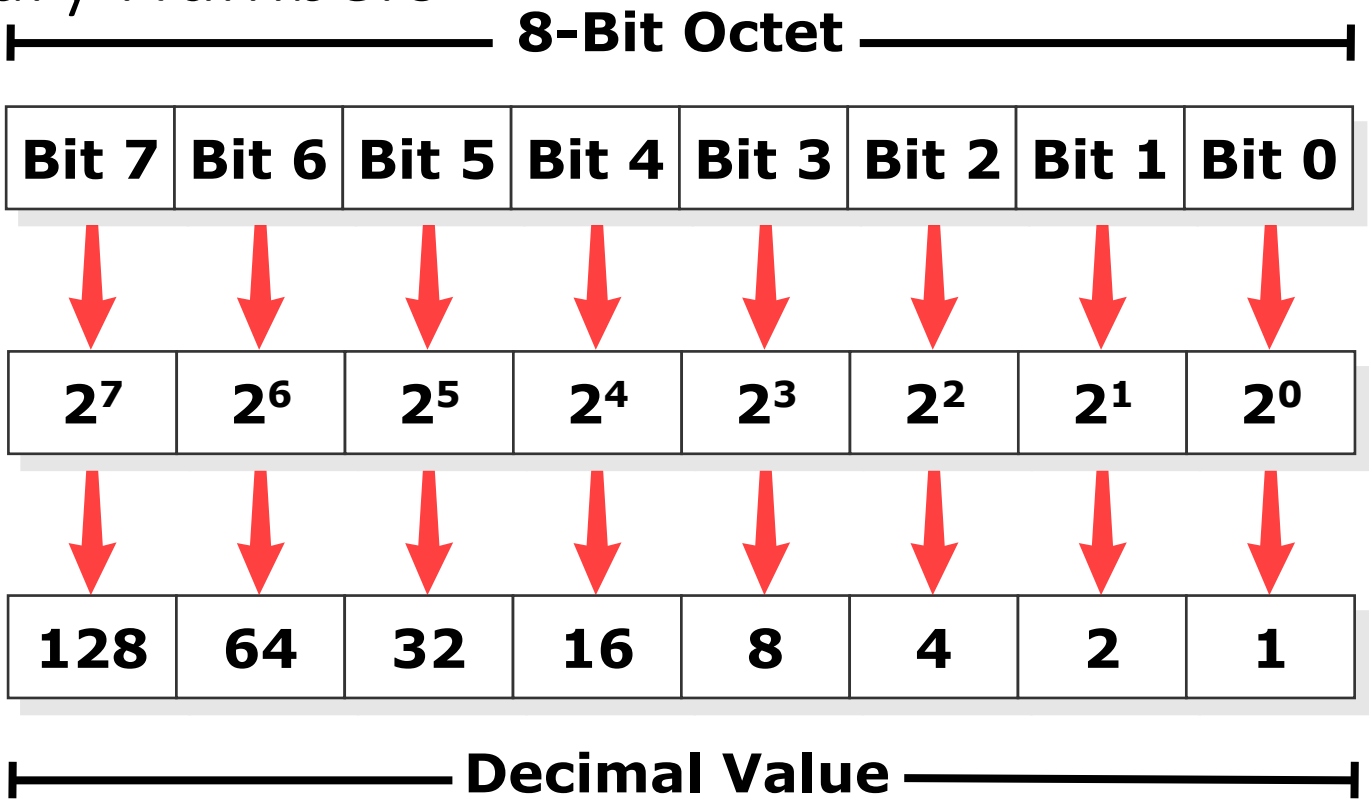
IPv4 Addressing Modes

Multicast

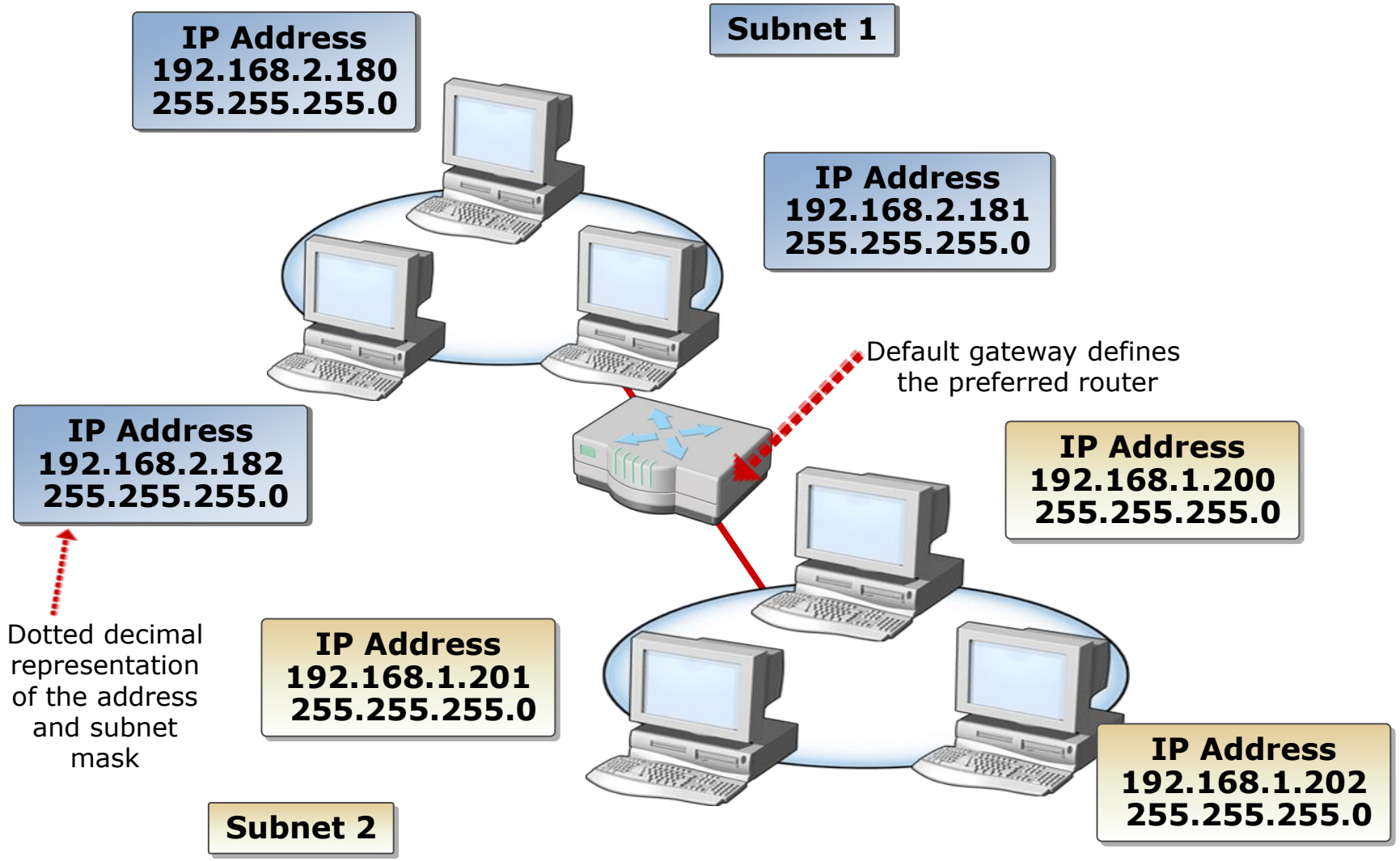
- Combination of unicast and broadcast modes
- Destination address field contains a special address (224.x.x.x)
- Neither destined to a single host nor all the hosts
- Can be processed by more than one hosts/servers



How Dotted Decimal Notation Relates to Binary Numbers



An IPv4 configuration identifies a computer to other computers on a network

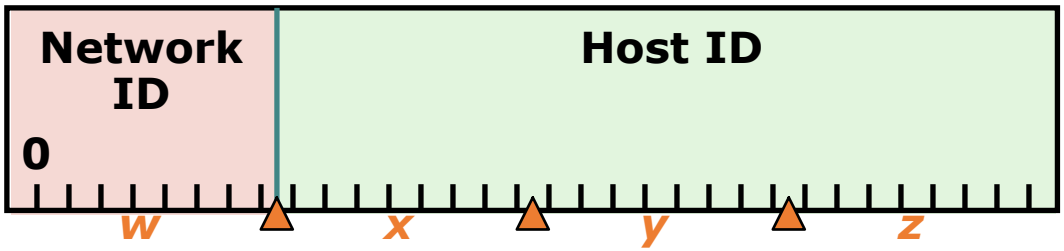


Simple IPv4 Implementations

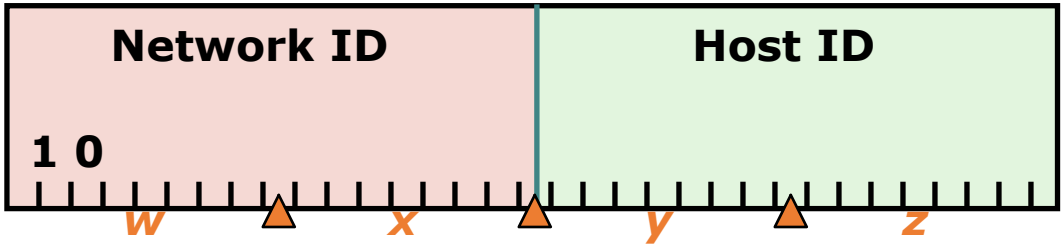
Class	Public IP Range	Private IP Range	Subnet Mast	Networks	Hosts
Class A	1.0.0.0 to 127.0.0	10.0.0.0 to 10.255.255.255	255.0.0.0	127	1,67,77,214
Class B	128.0.0.0 – 191.255.0.0	172.16.0.0 - 172.31.255.255	255.255.0.0	16,382	65,534
Class C	192.0.0.0 to 223.255.255	192.168.0.0 to 192.168.255.255	255.255.255.0	20,97,150	254

Simple IPv4 Implementations

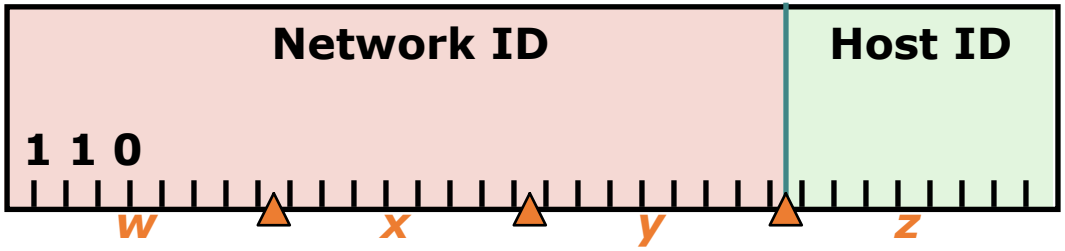
Class A
Large Network



Class B
Medium Network

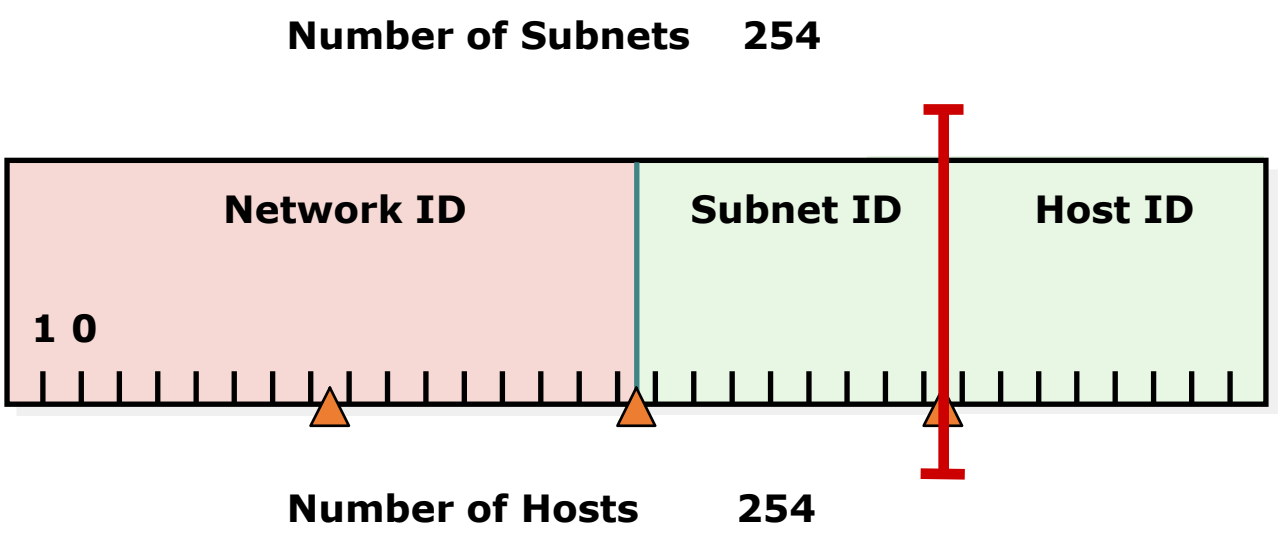


Class C
Small Network



How Bits Are Used in a Subnet Mask

Class B Address with Subnet



Implementing an IPv4 Subnetting Scheme

When you subdivide a network into subnets, create a unique ID for each subnet derived from the main network ID

By using subnets, you can:

- **Use a single network address across multiple locations**
- **Reduce network congestion by segmenting traffic**
- **Overcome limitations of current technologies**

Determining Subnet Addresses

When determining subnet addresses you should:

- Choose the number of subnet bits based on the number of subnets required
- Use 2^n to determine the number of subnets available from n bits

For five locations, the following three subnet bits are required:

- 5 locations = 5 subnets required
- 2^2 = 4 subnets (not enough)
- 2^3 = 8 subnets

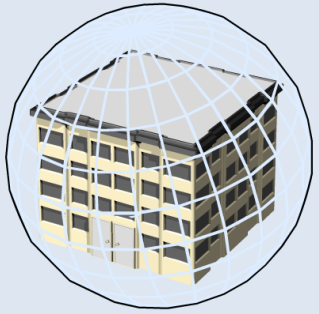
Public and Private IPv4 Addresses

Public

- **Required by devices and hosts that connect directly to the Internet**
- **Must be globally unique**
- **Routable on the Internet**
- **Must be assigned by IANA**

Private

- **Nonroutable on the Internet**
- **Can be locally assigned by organization**
- **Must be translated to access the Internet**



Understanding IPv6

- Benefits of Using IPv6
- The IPv6 Address Space

Benefits of Using IPv6

Benefits of using IPv6 compared to IPv4

- ✓ **Larger address space**
- ✓ **More efficient routing**
- ✓ **Simpler host configuration**
- ✓ **Built-in security**
- ✓ **Better prioritized delivery support**
- ✓ **Redesigned headers**

The IPv6 Address Space

Address Syntax:

- **128-bit address in binary:**

```
00100000000000010000110110111000000000
00000000000000010111100111011
00000010101010100000000011111111111
11100010100010011100010110 10
```

- **128-bit address divided into 16-bit boundaries:**

```
0010000000000001  0000110110111000
0000000000000000  0010111100111011
0000001010101010  0000000011111111
1111111000101000  1001110001011010
```

- **Each 16-bit block converted to HEX (base 16):**

```
2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A
```

- **Further simplify by removing leading zeros:**

```
2001:DB8:0:2F3B:2AA:FF:FE28:9C5A
```

Compressing Zeros:

- **Some types of addresses can contain many zeros**
- **A contiguous sequence of 16-bit blocks set to 0 can be compressed using the double colon "::"**
- **Link-local:**

```
FE80:0:0:0:2AA:FF:FE9A:4CA2
```

  - **Can be compressed down to:**

```
FE80::2AA:FF:FE9A:4CA2
```

- **Multicast:**

```
FF02:0:0:0:0:0:0:2
```

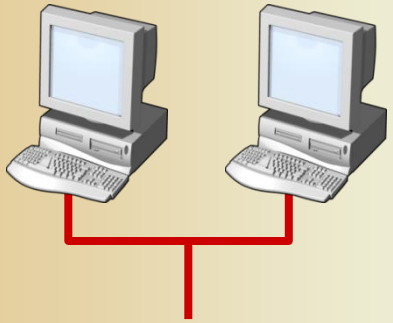
  - **Can be compressed down to:**

```
FF02::2
```

Name Resolution

- Configuring a Computer Name
- What Is DNS?
- DNS Zones and Records
- How Internet DNS Names Are Resolved

Configuring a Computer Name

Name	Description
 **Host name**	• Up to 255 characters in length • Can contain alphabetic and numeric characters, periods, and hyphens • Part of FQDN
 **NetBIOS name**	• Represent a single computer or group of computers • 15 characters used for the name • 16th character identifies service • Flat namespace

What Is DNS?

DNS is a service that manages the resolution of host names to IP addresses:

- **Resolve host names to IP addresses**
- **Locate domain controllers and global catalog servers**
- **Used to resolve IP addresses to host names**
- **Used to locate mail servers during e-mail deliver**

DNS Zones and Records

A DNS zone is a specific portion of DNS namespace that can contain DNS records

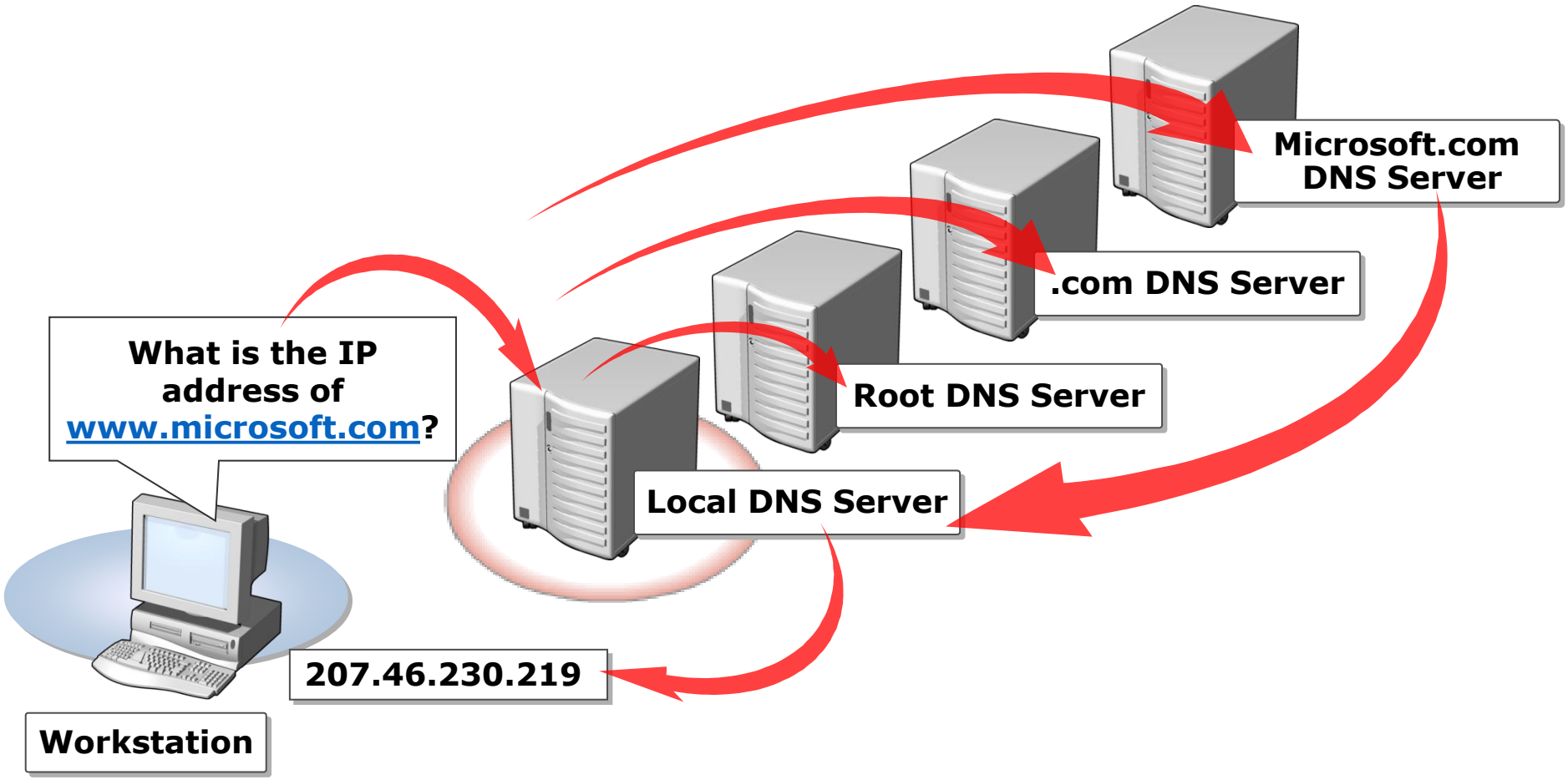
Records in forward lookup zones include:

- **A**
- **SRV**
- **MX**
- **CNAME**

Records in reverse lookup zones include:

- **PTR**

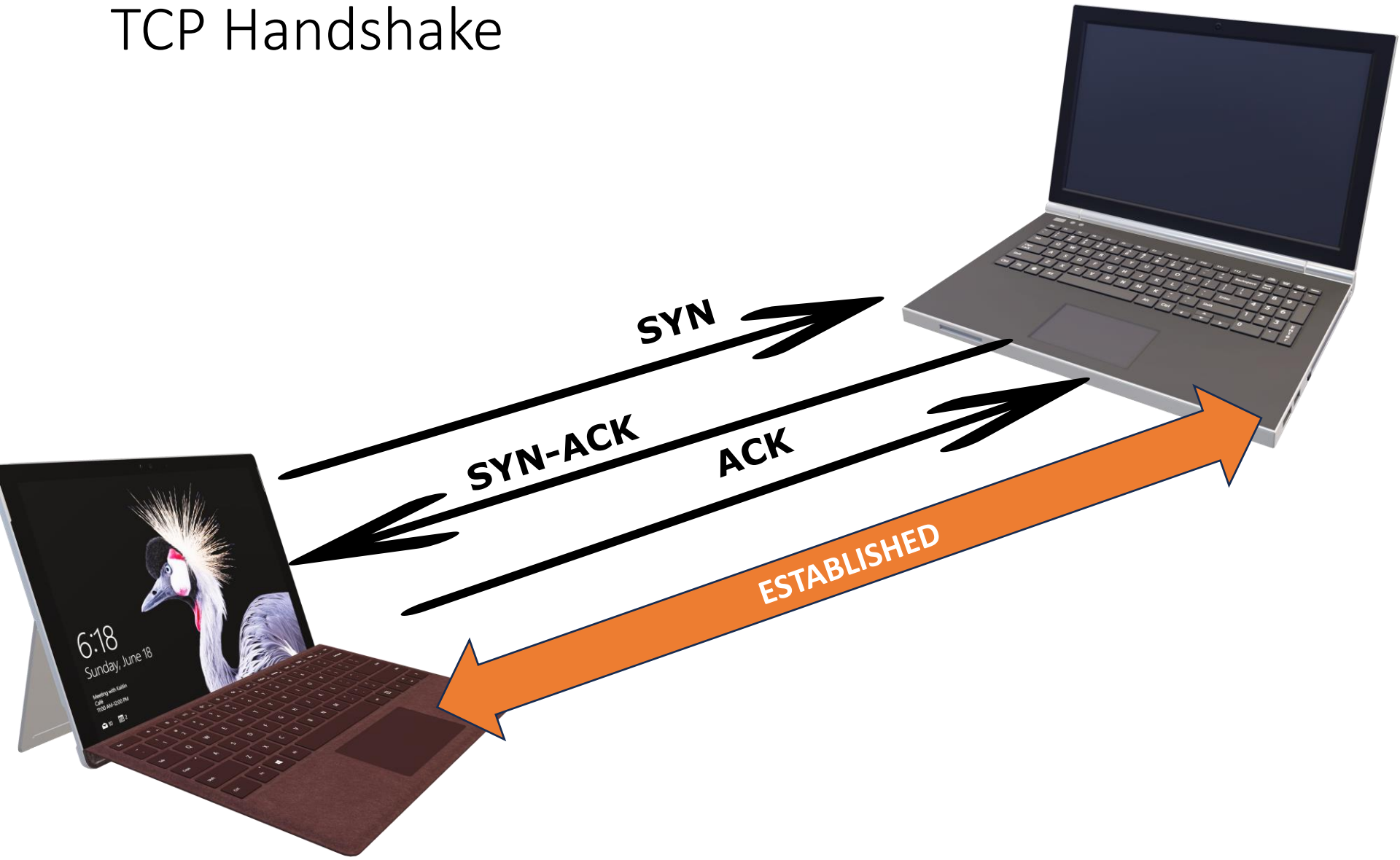
How Internet DNS Names Are Resolved



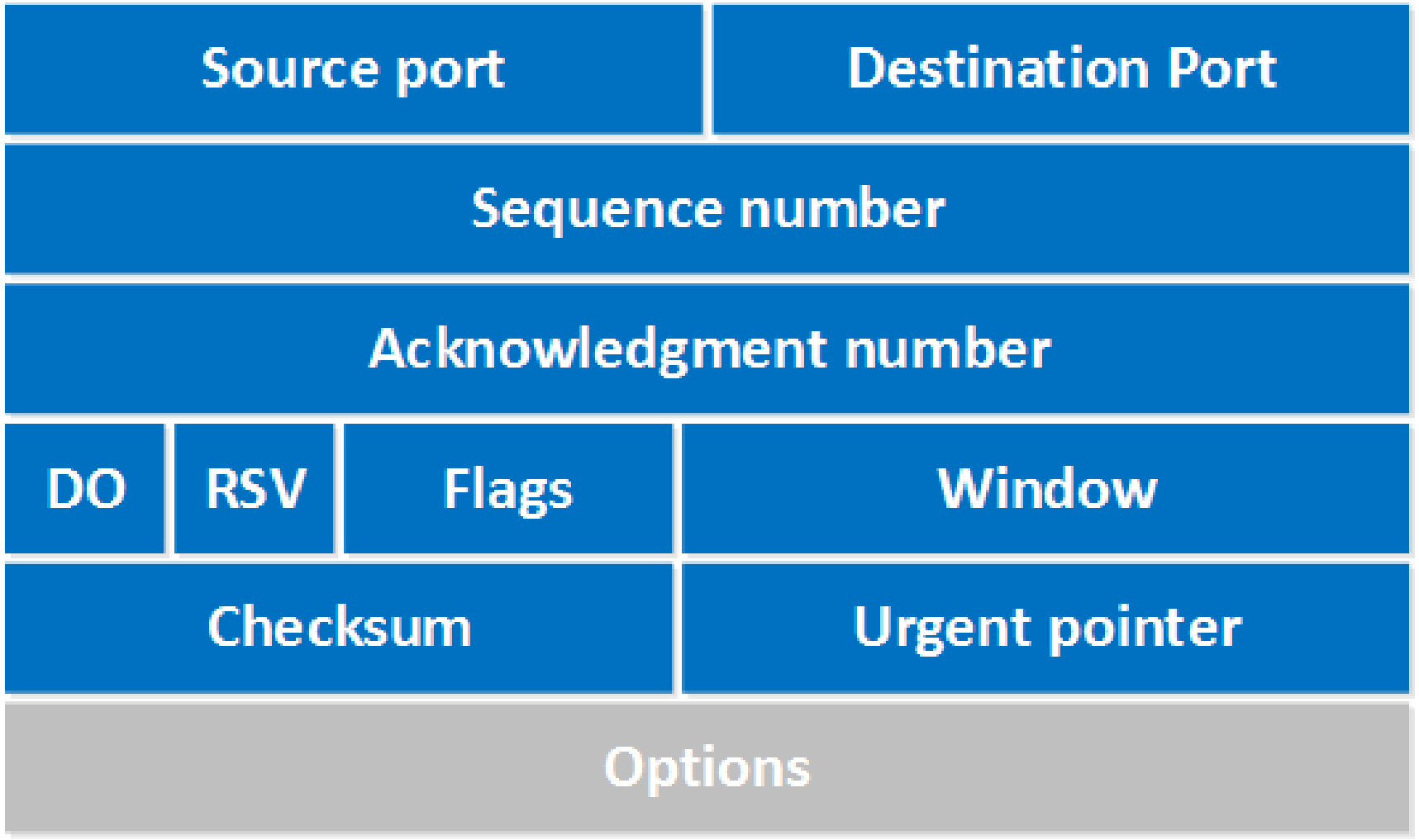
TCP Flow

- TCP Handshake
- TCP Packet Structure
- HTTP – GET Request Frame

TCP Handshake



TCP Packet Structure



TCP Packet Structure

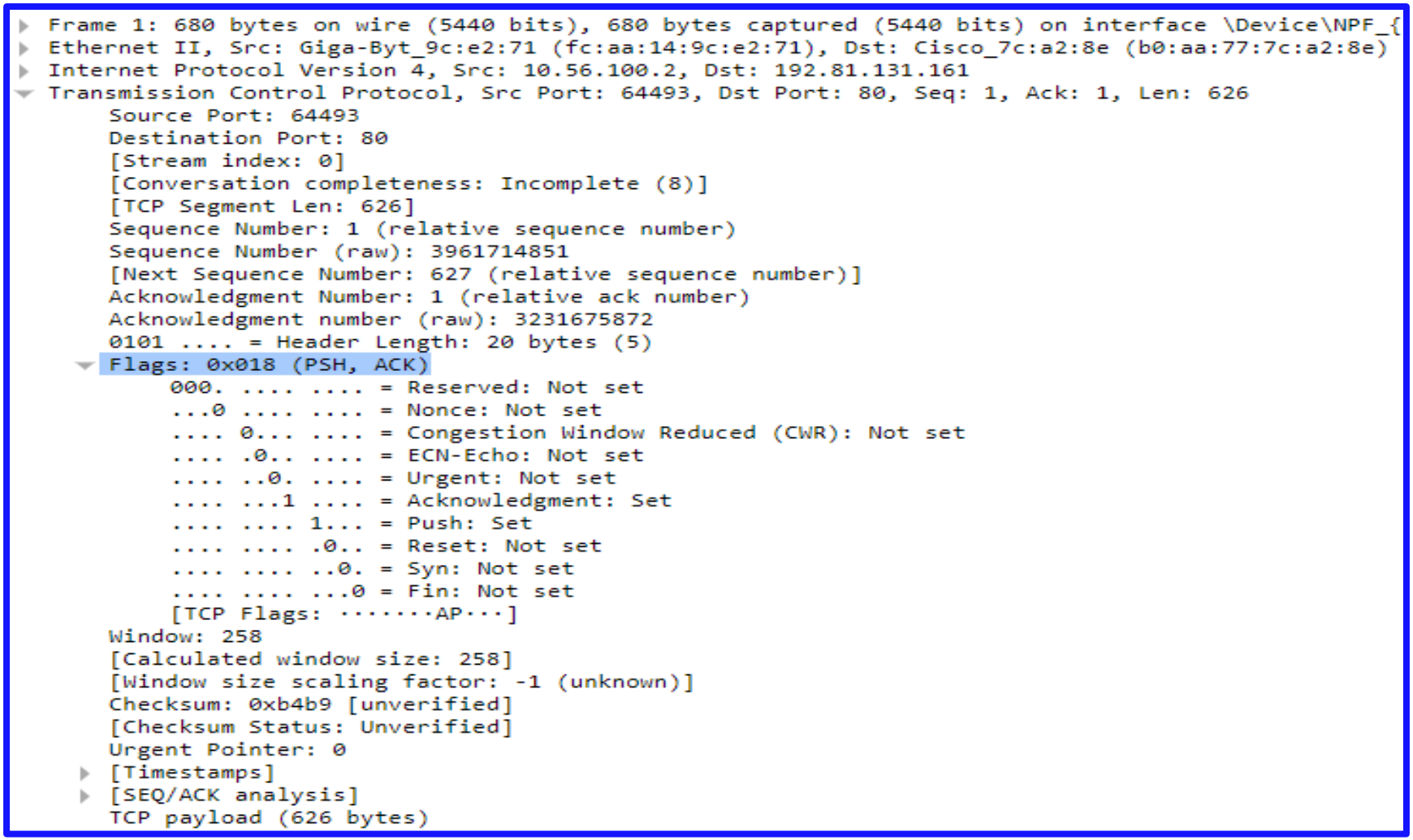
Source Port	This is a 16 bit field identifying the source port
Destination Port	16 bit field identifying the destination port
Sequence Number	32-bit field identifying how much data is sent
Acknowledgement Number	32-bit field which increments the sequence number by 1, used to request the next sequence
DO	4-bit Identifies the data start location - Data Offset
RSV	3-bit field Reserved and unused

PORTS					
System Ports	**0-1023**	**User Ports**	**1024 – 49151**	**Private/Dynamic Ports**	**49152-65535**

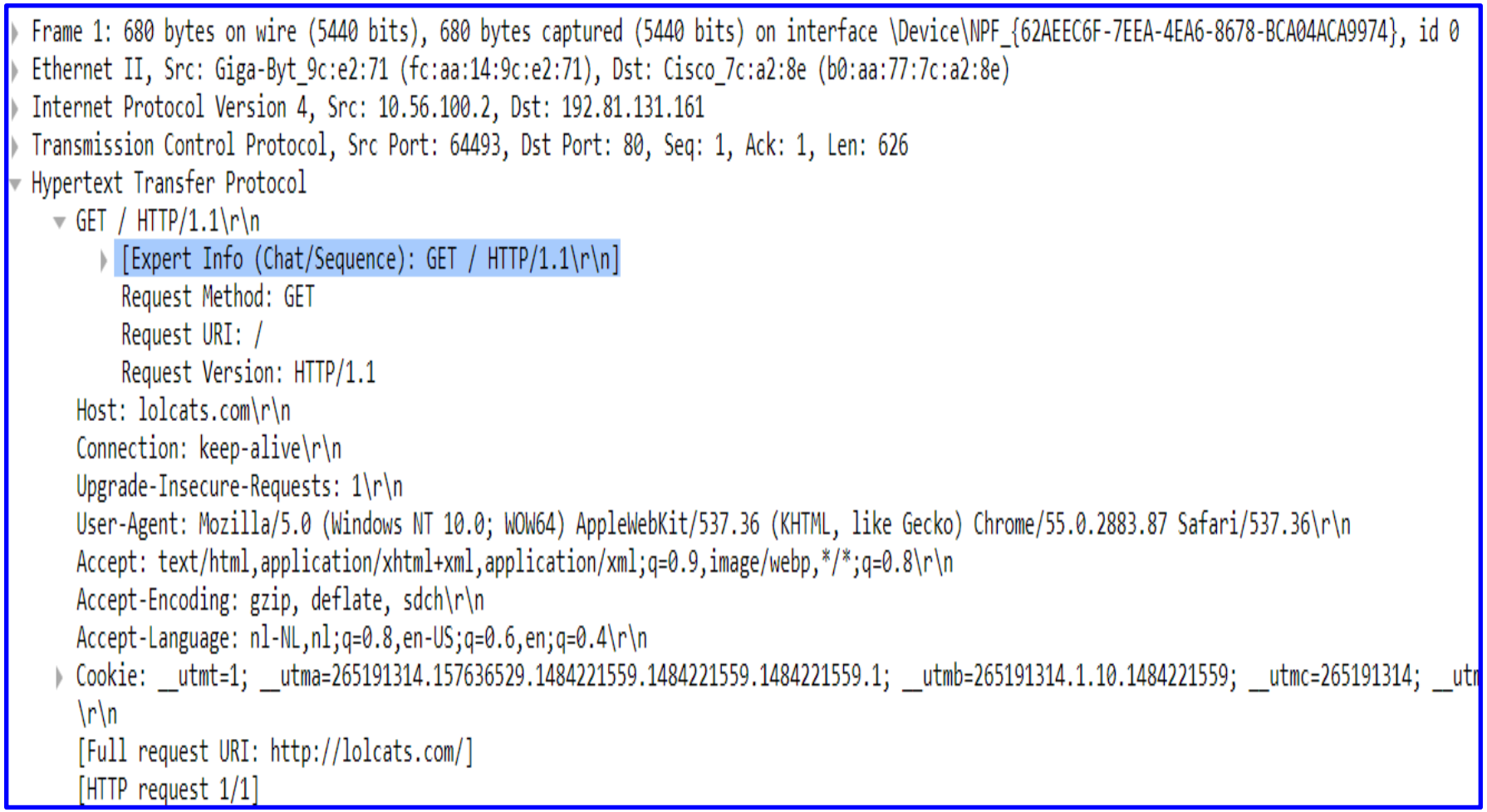
TCP Packet Structure

Flags	9-bits for flags **(NONCE, CWR, ECE)**
	URG – Urgent
	ACK: used for the acknowledgment.
	PSH: this is the push function
	RST: this resets the connection
	SYN: Used for the initial three way handshake
	FIN: this finish bit is used to end the TCP connection
Window	16-bit field specifies how many bytes the receiver is willing to receive
Checksum	16 bits are used for a checksum to check if the TCP header is OK or not
Urgent Pointer	these 16 bits are used when the URG bit has been set, the urgent pointer is used to indicate where the urgent data ends
Options	this field is optional and can be anywhere between 0 and 320 bits

TCP Packet Structure - Wire



HTTP-GET Request Frame



Windows Network Commands

- **ARP**
- **GETMAC**
- **IPCONFIG**
- **PING**
- **TRACERT**
- **NETSTAT**
- **NSLOOKUP**
- **ROUTE**
- **PATHPING**
- **NETSH**
- **HOSTNAME**
- **TASKLIST**
- **NET**
- **NBTSTAT**