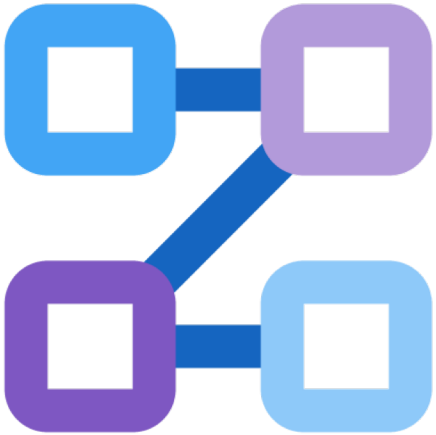
TCP/IP Fundamentals Crash Course

Michael J. Shannon

IT/Security Consultant, Instructor, and Author

History of Packet Switching

- The packet switching technology is represented by protocol suites and associated reference models
- TCP/IP finds its origins in the Arpanet reference model
- Architecture evolved from studies in methods for connecting multiple packet-switched networks



Sample Transport Protocol

322

600

FedEx Express USA Airbill

FedEx Tracking Number 8373 0209 7920

SPG13

Form I.D. No. 0215

Sender's Copy

NO POUCH NEEDED.
See back for peel and stick application instructions.

PULL AND RETAIN THIS COPY BEFORE AFFIXING TO THE PACKAGE.

1 From *Please print and press hard.*

Date

Sender's FedEx Account Number [redacted]

Sender's Name

Phone (616)

Company

Address

Dept./Floor/Suite/Room

City State ZIP 49423-3607

2 Your Internal Billing Reference OPTIONAL
First 24 characters will appear on invoice.

3 To

Recipient's Name

Phone ( )

Company

Address
To "HOLD" at FedEx location, print FedEx address. We cannot deliver to P.O. boxes or P.O. ZIP codes.

Address

Dept./Floor/Suite/Room

City State ZIP

Try online shipping at fedex.com

By using this Airbill you agree to the service conditions on the back of this Airbill and in our current Service Guide, including terms that limit our liability.

4a Express Package Service *Packages up to 150 lbs.* Delivery commitment may be later in some areas.

- FedEx Priority Overnight — Next business morning
- FedEx Standard Overnight — Next business afternoon
- FedEx First Overnight — Earliest next business morning delivery to select locations
- X FedEx 2Day — Second business day
- FedEx Express Saver — Third business day

FedEx Envelope rate not available. Minimum charge: One-pound rate

4b Express Freight Service *Packages over 150 lbs.* Delivery commitment may be later in some areas.

- X FedEx 1Day Freight* — Next business day
- FedEx 2Day Freight — Second business day
- FedEx 3Day Freight — Third business day

* Call for Confirmation:

5 Packaging * Declared value limit $500

- X FedEx Envelope*
- FedEx Pak* — Includes FedEx Small Pak, FedEx Large Pak, and FedEx Sturdy Pak
- Other

6 Special Handling Include FedEx address in Section 3.

- SATURDAY Delivery — Available ONLY for FedEx Priority Overnight and FedEx 2Day to select ZIP codes
- HOLD Weekday at FedEx Location — NOT Available for FedEx First Overnight
- HOLD Saturday at FedEx Location — Available ONLY for FedEx Priority Overnight and FedEx 2Day to select locations

Does this shipment contain dangerous goods? One box must be checked.

- No
- Yes — As per attached Shipper's Declaration
- Yes — Shipper's Declaration not required
- Dry Ice — Dry Ice, 9, UN 1845 ____ x ____ kg

Dangerous Goods (including Dry Ice) cannot be shipped in FedEx packaging.

- Cargo Aircraft Only

7 Payment *Bill to:* Enter FedEx Acct. No. or Credit Card No. below.

- Sender — Acct. No. in Section 1 will be billed.
- Recipient
- Third Party
- Credit Card
- Cash/Check

FedEx Acct. No. / Credit Card No. Exp. Date

Total Packages	Total Weight	Total Declared Value†
		$ .00

†Our liability is limited to $100 unless you declare a higher value. See back for details.

FedEx Use Only

8 Release Signature *Sign to authorize delivery without obtaining signature.*

Optional

Pioneers of Packet Switching

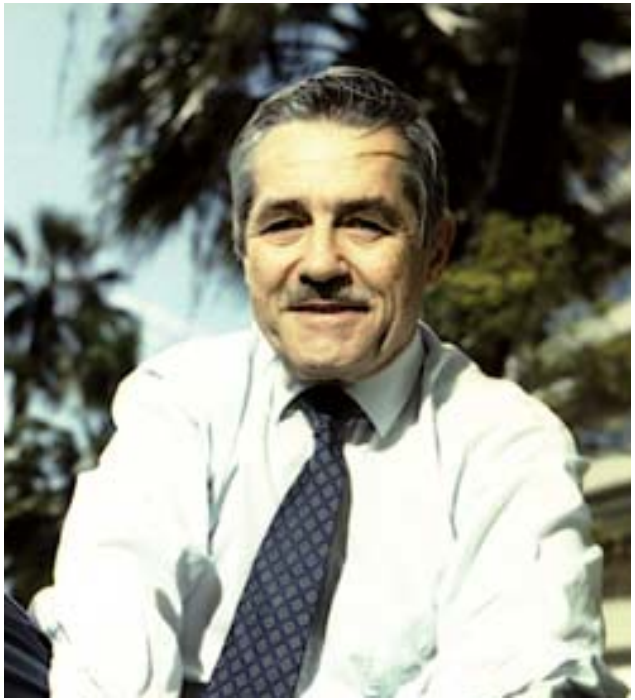
- Leonard Kleinrock

- Paul Baran

Pioneers of Packet Switching

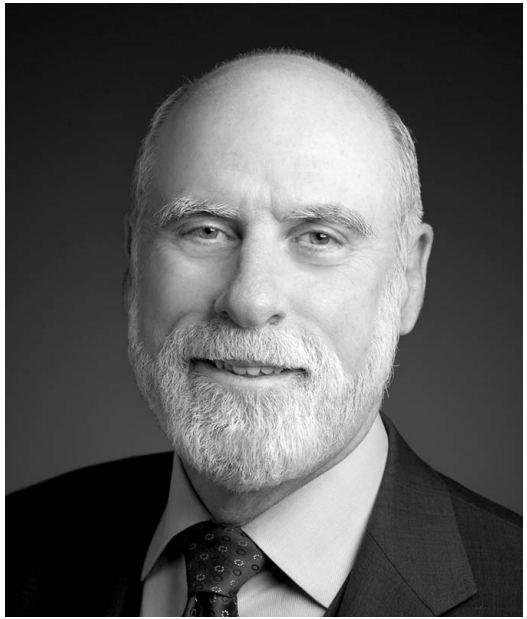
- Donald Davies

- Louis Pouzin



Pioneers of Packet Switching

- Vinton Cerf



- Jon Postel

Women Pioneers of Networking

- Heddy Lamarr

- Radia Perlman

TCP/IPv4 Timeline

- The early Internet and TCP/IP were developed together as part of the U.S. DARPA ARPAnet project in the 60's
- 1973 – a complete internetworking system for the ARPAnet officially began
- December 1974 – RFC 675 for early TCP
- March 1977 – TCP version 2
- 1978 through 1980 – TCP/IP version 3 was developed
- Early 1980's – many machines (UNIX) and networks started using TCP/IP version 4 on the ARPAnet

Base 10

- Base-10 systems are used in most modern civilizations and was the most common system for ancient civilizations, most likely because humans have 10 fingers
- Egyptian hieroglyphs dating back to 3000 B.C. show evidence of a decimal system

Hundred thousands	Ten thousands	thousands	hundreds	tens	ones
100000	10000	1000	100	10	1
			4	**5**	**7**

Binary Math

- Binary is a Base-2 system instead of Base-10
- There are 2 possible numbers 0 and 1 and the true value is based on their position in the system

512	256	128	64	32	16	8	4	2	1
2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
0	**1**	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**1**

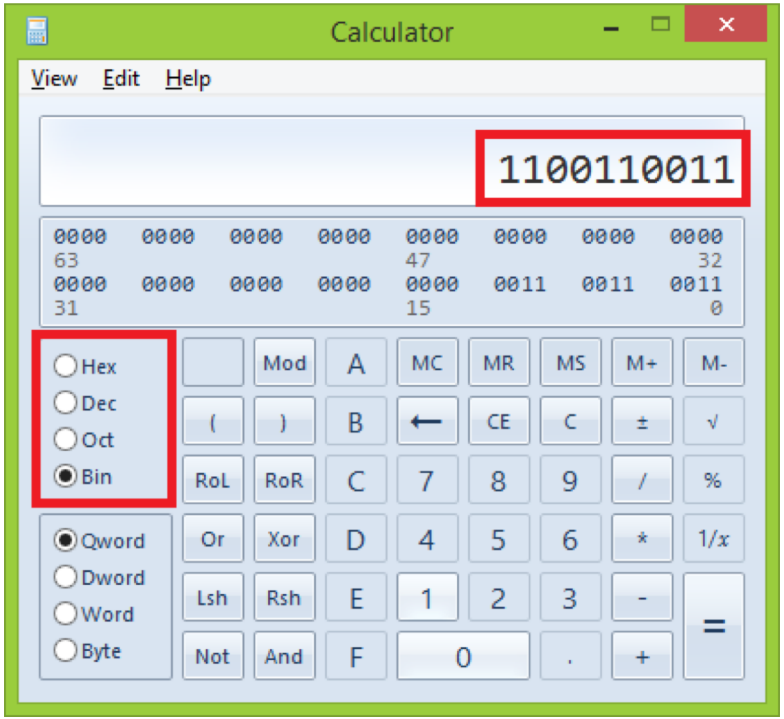
256 + 128 + 64 + 8 + 1 = 457

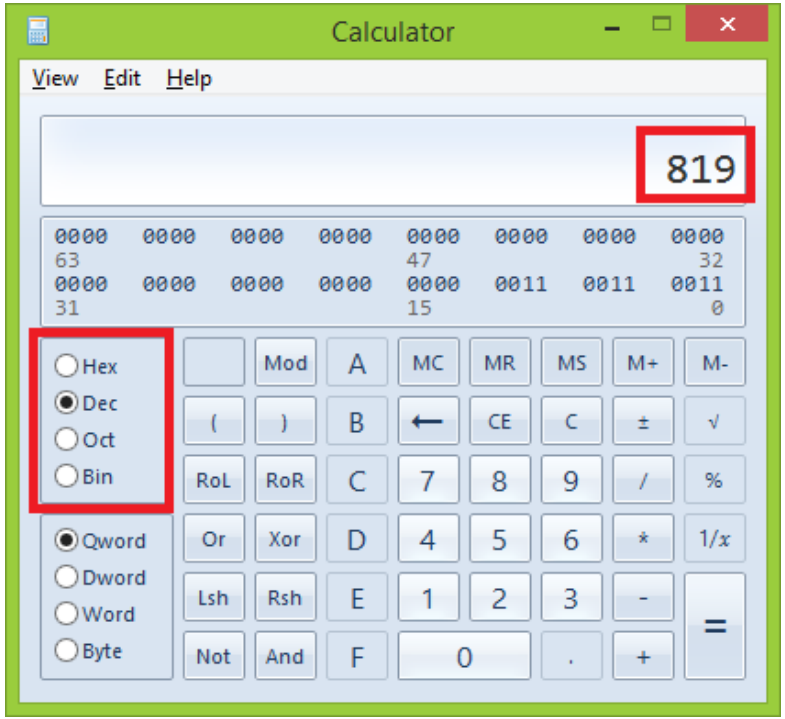
Some Binary Math Examples

512	256	128	64	32	16	8	4	2	1
2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

- **10 = 2**
- **101 = 5**
- **1001 = 9**
- **1100 = 12**
- **11011 = 27**
- **1001001 = 73**

Binary to Decimal





Hexadecimal Math

- Hexadecimal is Base-16 math
- Digits are 0-9, A, B, C, D, E, F (16 elements)

Hexadecimal:	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Decimal:	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**

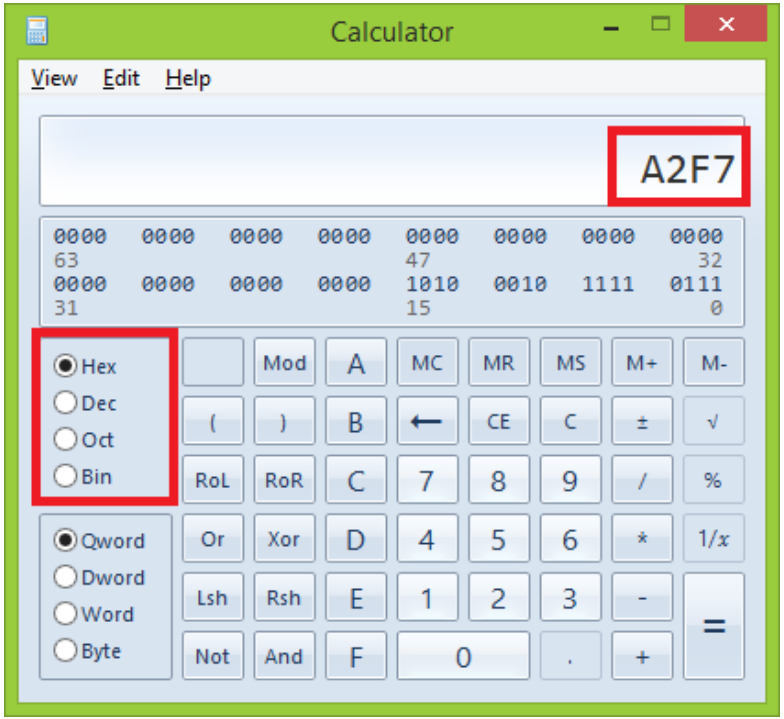
Hexadecimal Math

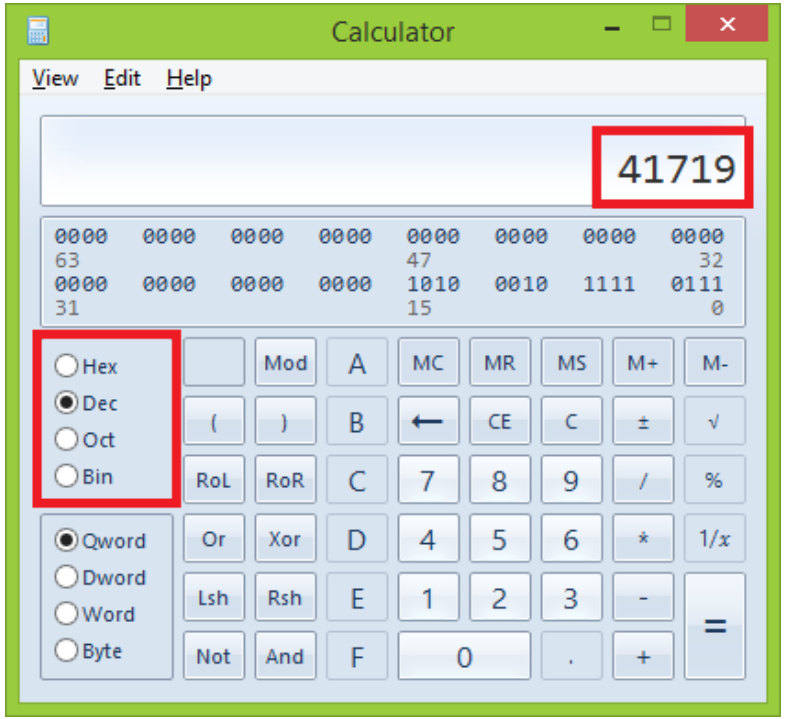
Hexadecimal:	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Decimal:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

A	2	F	7
16^3	16^2	16^1	16^0
10×16^3 = 40960	2×16^2 = 512	15×16^1 = 240	7×16^0 = 7

$$40960 + 512 + 240 + 7 = \mathbf{41719}$$

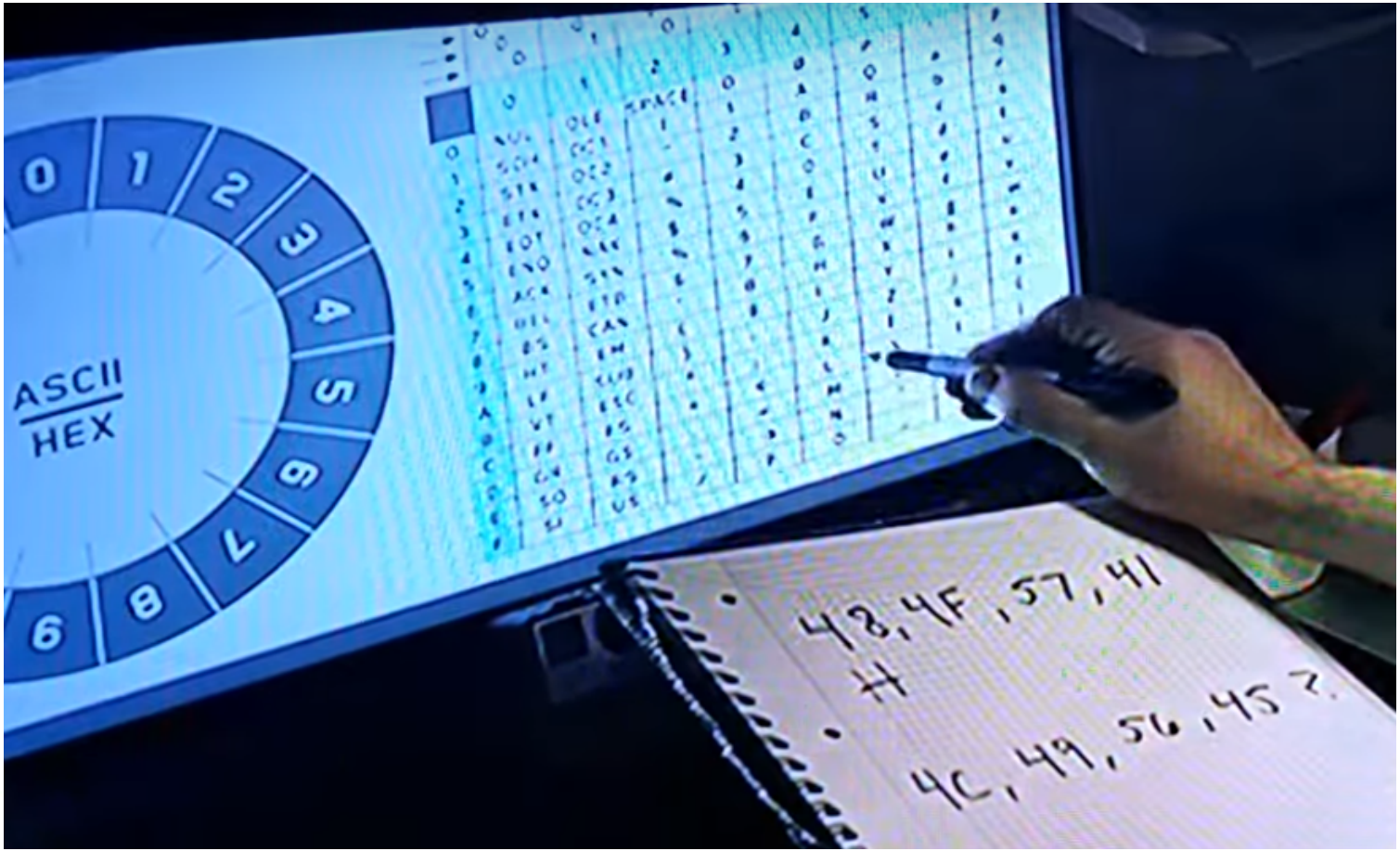
Hex to Decimal





Hexadecimal in “The Martian”

Hexadecimal in “The Martian”



ASCII Table

Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0	0		32	20	40	[space]	64	40	100	@	96	60	140	`
1	1	1		33	21	41	!	65	41	101	A	97	61	141	a
2	2	2		34	22	42	"	66	42	102	B	98	62	142	b
3	3	3		35	23	43	#	67	43	103	C	99	63	143	c
4	4	4		36	24	44	$	68	44	104	D	100	64	144	d
5	5	5		37	25	45	%	69	45	105	E	101	65	145	e
6	6	6		38	26	46	&	70	46	106	F	102	66	146	f
7	7	7		39	27	47	'	71	47	107	G	103	67	147	g
8	8	10		40	28	50	(	72	48	110	H	104	68	150	h
9	9	11		41	29	51	)	73	49	111	I	105	69	151	i
10	A	12		42	2A	52	*	74	4A	112	J	106	6A	152	j
11	B	13		43	2B	53	+	75	4B	113	K	107	6B	153	k
12	C	14		44	2C	54	,	76	4C	114	L	108	6C	154	l
13	D	15		45	2D	55	-	77	4D	115	M	109	6D	155	m
14	E	16		46	2E	56	.	78	4E	116	N	110	6E	156	n
15	F	17		47	2F	57	/	79	4F	117	O	111	6F	157	o
16	10	20		48	30	60	0	80	50	120	P	112	70	160	p
17	11	21		49	31	61	1	81	51	121	Q	113	71	161	q
18	12	22		50	32	62	2	82	52	122	R	114	72	162	r
19	13	23		51	33	63	3	83	53	123	S	115	73	163	s
20	14	24		52	34	64	4	84	54	124	T	116	74	164	t
21	15	25		53	35	65	5	85	55	125	U	117	75	165	u
22	16	26		54	36	66	6	86	56	126	V	118	76	166	v
23	17	27		55	37	67	7	87	57	127	W	119	77	167	w
24	18	30		56	38	70	8	88	58	130	X	120	78	170	x
25	19	31		57	39	71	9	89	59	131	Y	121	79	171	y
26	1A	32		58	3A	72	:	90	5A	132	Z	122	7A	172	z
27	1B	33		59	3B	73	;	91	5B	133	[	123	7B	173	{
28	1C	34		60	3C	74	<	92	5C	134	\	124	7C	174	|
29	1D	35		61	3D	75	=	93	5D	135	]	125	7D	175	}
30	1E	36		62	3E	76	>	94	5E	136	^	126	7E	176	~
31	1F	37		63	3F	77	?	95	5F	137	_	127	7F	177	

Hexadecimal in Networking

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Qualcomm Atheros AR956x Wireless Network Adapter
   Physical Address. . . . . . . . . : AC-B5-7D-4F-59-F4
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : ::cce8:3c9f:1e8b:c27a(Preferred)
   Temporary IPv6 Address. . . . . . : ::11d:daa6:5432:150e(Preferred)
   Link-local IPv6 Address . . . . . : fe80::cce8:3c9f:1e8b:c27a%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.20(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, December 2, 2019 8:55:28 AM
   Lease Expires . . . . . . . . . . : Monday, December 2, 2019 6:42:17 PM
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 95204733
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-52-40-24-30-65-EC-69-84-AF
   DNS Servers . . . . . . . . . . . : 208.180.42.68
                                       208.180.42.100
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

OSI Reference Model

Number	Name	Description
7	Application	To accomplish a networked user task
6	Presentation	Expressing and translating data formats
5	Session	To accommodate multiple session connections
4	Transport	Connecting multiple programs on same system
3	Network (or Internetwork)	Facilitate multihop communications across potentially different link networks
2	Link	Communication across a single link including media access control
1	Physical	Specifies connectors, data rates, and encoding bits

Some OSI Model Protocols

Number	Name	Example
7	Application	HTTP, FTP, SMTP, DNS, TELNET
6	Presentation	ASCII, PNG, MPEG, AVI, MIDI
5	Session	SSL/TLS, SQL, RPC, NFS
4	Transport	TCP, UDP, SPX, AppleTalk
3	Network (or Internetwork)	IP, IPX, ICMP, ARP, BGP, OSPF
2	Link	PPP/SLIP, Ethernet, Frame Relay, ATM
1	Physical	Binary transmission, encoding, bit rates, voltages

OSI Model Mnemonics

- **A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing
- **A**ll **P**roper **S**uitors **T**ell **N**o **D**evious **P**hrase

_____

- **P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way
- **P**lease **D**o **N**ot **T**ell **S**ecret **P**asswords **A**nytime
- **P**hysical **D**ata **N**etworks **T**ransport **S**ession **P**resentation **A**pplications

TCP/IP Reference Model

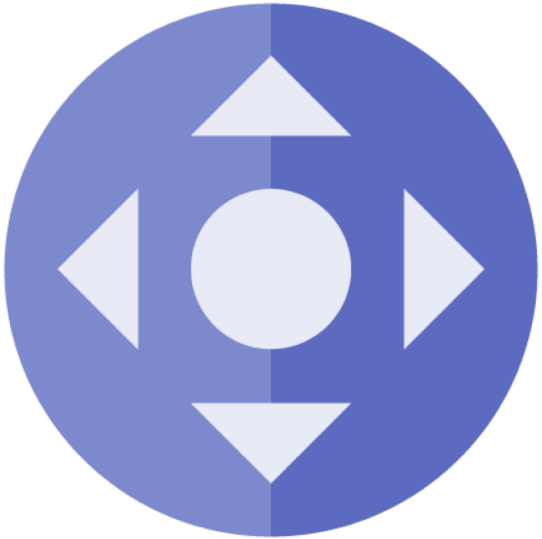
Number	OSI Name	TCP/IP Model
7	Application	**Application**
6	Presentation	
5	Session	
4	Transport	**Transport** (host-to-host)
3	Network (or Internetwork)	**Internet** (internetwork)
2	Link	**Network Access**
1	Physical	

The Link Layer 2 in a Nutshell

- Sends and receives IP datagrams for the IP service
- It also carries other support protocols like ARP for IPv4
- TCP/IP supports many Link Layer protocols
  - Ethernet wired LANs
  - 802.11 wireless LANs
  - Cable (DOCSIS) and DSL variants
  - Cellular technologies like WiMAX
  - Satellite technologies
- Point-to-Point Protocol (PPP) and its many variants helped TCP/IP run over many different layer 2 implementations

The Link Layer 2 in a Nutshell

- The most common Link layer protocol data unit (PDU) is called a “frame”
- They are often variable lengths where the upper bound is called the Maximum Transmission Unit (MTU) and is measured in Kilobytes.
- The behavior is governed my many IEEE 802 LAN/MAN standards:
  - 802.3, 802.1w, 802.3ae, 802.3bm-2015
  - 802.11g/n/ac, 802.11ax, 802.15.1
  - 802.1q and 802.1X



Layer 2 Frame Formats

Ethernet (802.3) Frame Format

7 bytes	1 byte	6 bytes	6 bytes	2 bytes	42 to 1500 bytes	4 bytes	12 bytes
Preamble	Start of Frame Delimiter	**Destination MAC Address**	**Source MAC Address**	Type	Data (payload)	CRC	Inter-frame gap

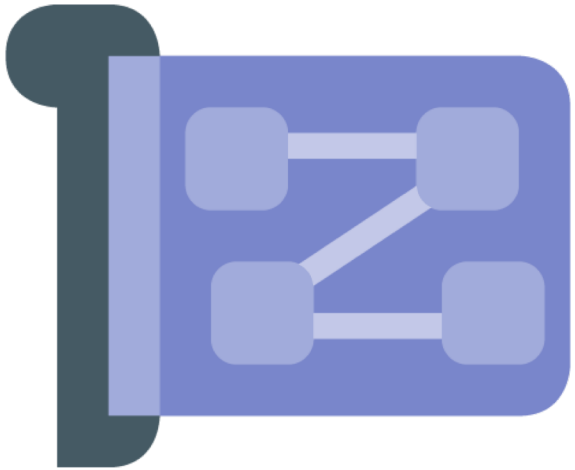
For TCP/IP communications, the payload for a frame is a packet

WiFi (802.11) Frame Format

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
Frame Control	Duration	MAC Address 1 (Destination)	MAC Address 2 (Source)	MAC Address 3 (Router)	Seq Control	MAC Address 4 (AP)	Data (payload)	CRC

Media Access Control (MAC) Address

- The IEEE 802 48-bit address MAC address comes from the original Xerox Ethernet addressing scheme
- It is represented in hex and is most commonly referred to as the EUI-48 identifier for addressing
- A Media Access Control (MAC) address is typically tied to a core connection device in your computer called the network interface card, or NIC



Media Access Control (MAC) Address

- A NIC converts data into an electrical signal that can be transmitted over the network
- Every commercially viable NIC has a hardware address that's known as a MAC
- Whereas IP addresses are linked with TCP/IP networking software stacks, a MAC address is linked to the hardware of logical or physical network adapters.

Media Access Control (MAC) Address

- Manufacturers all place a special number sequence (Organizationally Unique Identifier or OUI) that identifies them as the manufacturer
- The OUI is usually at the front of the address. For example, consider "00-14-22-01-23-45." The OUI for the manufacturer of this host is the first three octets—"00-14-22."
- **Dell**: 00-14-22, **Nortel**: 00-04-DC, **Cisco**: 00-40-96, **Belkin**: 00-30-BD

MAC address on a Windows PC

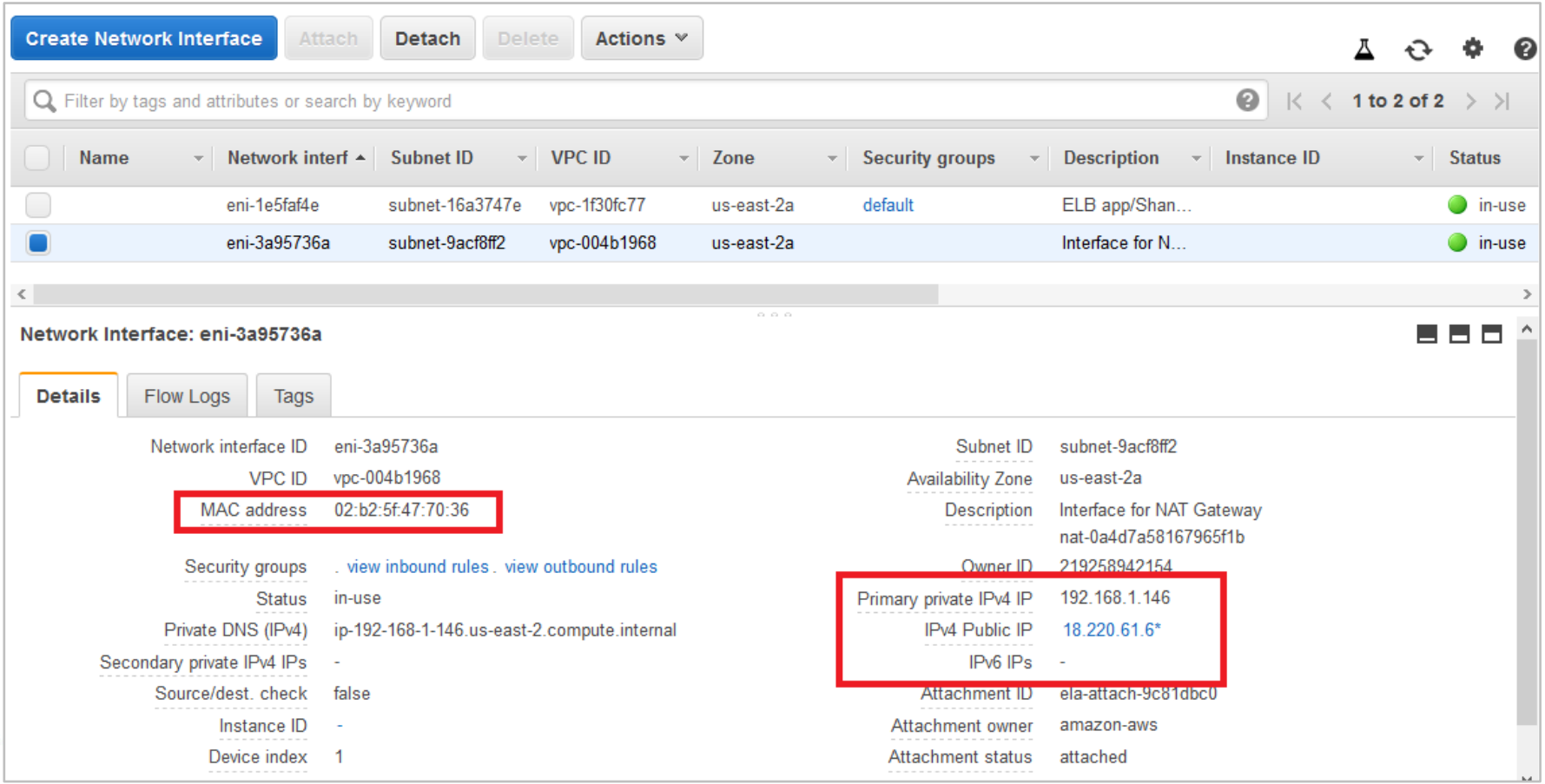
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Qualcomm Atheros AR956x Wireless Network Adapter
   Physical Address. . . . . . . . . : AC-B5-7D-4F-59-F4
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : ::cce8:3c9f:1e8b:c27a(Preferred)
   Temporary IPv6 Address. . . . . . : ::580a:d04f:89ce:921a(Preferred)
   Link-local IPv6 Address . . . . . : fe80::cce8:3c9f:1e8b:c27a%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.114(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, August 6, 2018 6:20:54 PM
   Lease Expires . . . . . . . . . . : Wednesday, August 8, 2018 3:04:36 PM
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 95204733
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-52-40-24-30-65-EC-69-84-AF
   DNS Servers . . . . . . . . . . . : 208.180.42.68
                                       208.180.42.100
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : peroot.com
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 30-65-EC-69-84-AF
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

Logical (Virtual) MAC addresses



Internet Protocol (IP)

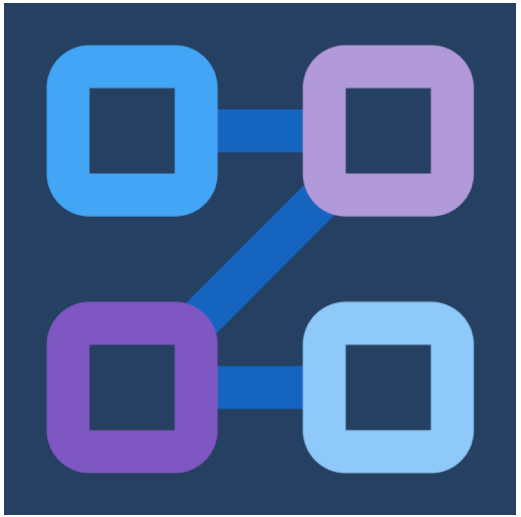
- The core protocol of the TCP/IP suite and the main protocol of the Network (internetwork) layer
- Main purpose is to provide internetwork datagram delivery services to layer 4 protocols like TCP and UDP
- Often uses layer 3 devices like routers, multilayer switches, load balancers, and firewall appliances to forward datagrams (packets)

Key Characteristics of IP

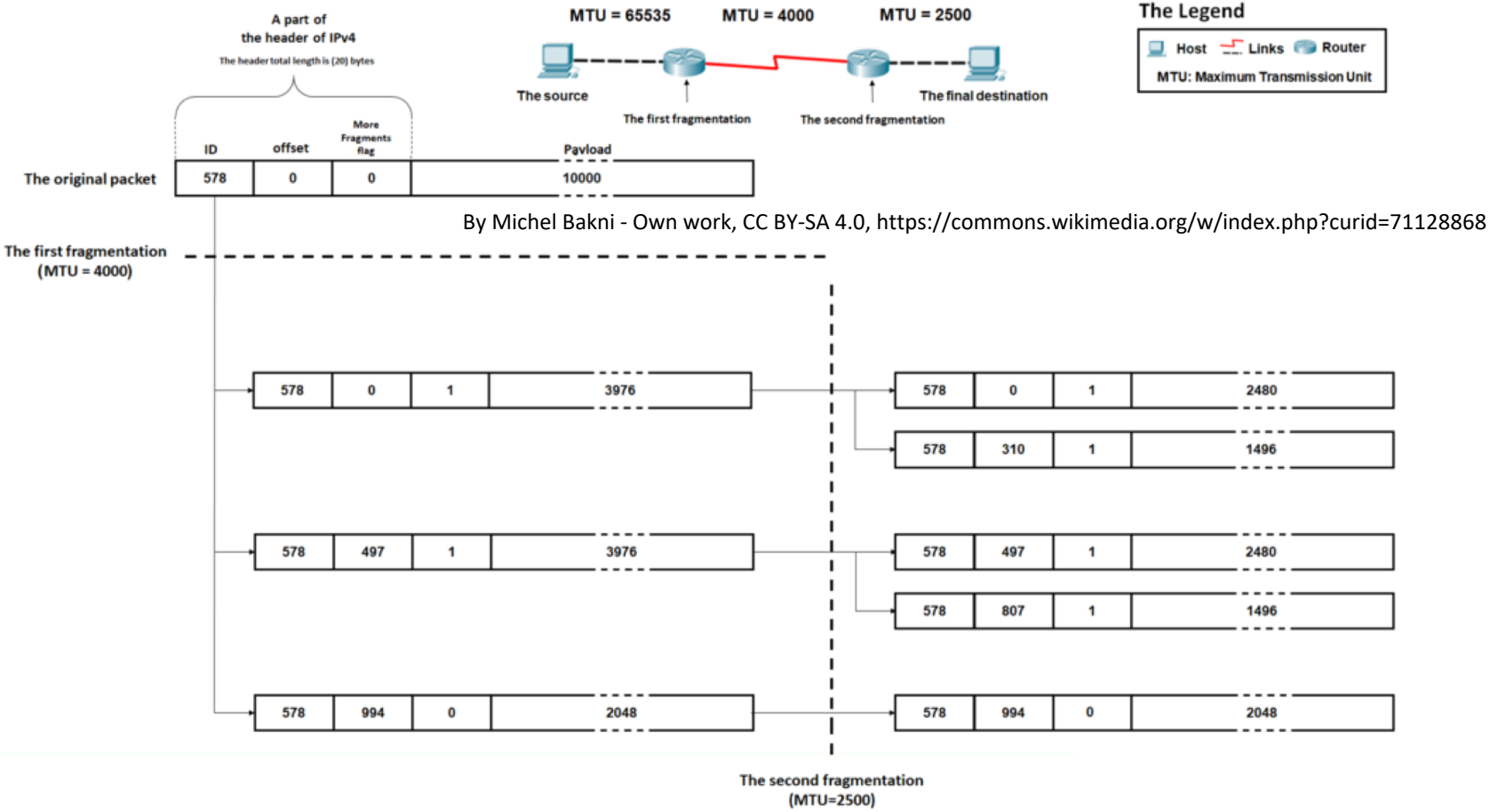
- Universal addressing
  - Defines addressing mechanism with IP version 4 and 6 addressing schemes
- Protocol independence
  - Works with both the Ethernet and the 802.11 wireless family
- Connectionless delivery
  - No handshake setup before transmission to remote host
- Unreliable and unacknowledged delivery
  - No tracking of datagrams

Main IP Protocol Functions

- Encapsulation and labeling of data from the upper application layers
- Formatting and identification
- Fragmentation and reassembly
- Routing and Internet delivery
  - Help comes from ICMP and dynamic routing protocols like RIP, OSPF, and BGP to name a few



IP Fragmentation



Main IP Protocol Versions

- The functions of IP were planned and designed well before the protocol suite was defined
- The original Transmission Control Program was eventually divided into Transmission Control Protocol (TCP) and Internet Protocol (IP)
- There were three previous versions of the original TCP; so when the split occurred, IP was called version 4
- **There were never IP versions 1, 2 or 3!**

What Happened to IP Version 5?

- Version 5 relates to an experimental TCP/IP protocol called the Internet Stream Protocol, Version 2, originally defined in RFC 1190
- Version 5 doesn’t technically exist, as it was intentionally skipped to avoid or rectify confusion
- This protocol never progressed, so it was bypassed in favor of IP version 6

Addressing Concepts

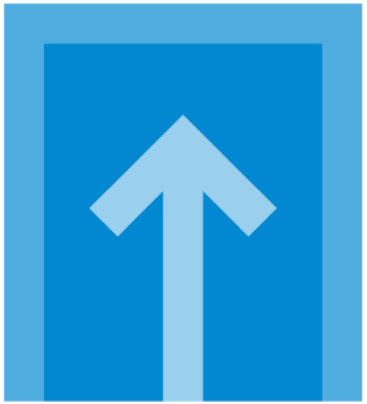
- When representing hosts on an internetwork, it is critical that coordinated, non-duplicate addresses are being used
- Every device on the network will have at least one IP address
- For most end-users, the addressing is typically shielded by the Domain Naming System (DNS), so friendly names are all that are referenced in practice:
  - **www.oreilly.com maps to 184.27.190.97**

Addressing Concepts

- Groups of assigned (allocated) IP addresses are assigned to users and organizations
- Various service providers (ISPs, ITSPs, and CSPs) typically provide addresses and routing services on the Internet
- The most common is the dotted-quad or dotted-decimal IPv4 address

Basic IP Address Structure

- IPv4 has a possible 4,294,967,296 addresses in the space
- Most of the space is **unicast** (also multicast and broadcast)
- When originally defined, every address had a network portion and a host portion and was grouped into one of the five classes (A, B, C, D, E)
- Public and Private (RFC 1918) addresses



IPv4 Address Examples

Dotted-Quad Representation	Binary Representation
1.2.3.4	00000001.00000010.00000011.00000100
10.0.0.255	00001010.00000000.00000000.11111111
128.16.1.15	10000000.00010000.00000001.00001111
255.255.255.255	11111111.11111111.11111111.11111111

The Subnet Mask

- The subnet mask as a configuration is rapidly being replaced with Classless Inter-domain Routing (CIDR)
- A bit assignment used by hosts (and routers) to partition the network portion of the address from the host portion in the IP address
- Where the network ends and host begins
- They are the same length as the corresponding address
  - 32 bits for IPv4
  - 128 bits for IPv6

Traditional Subnet Masking (obsolete)

128.16.1.15/24

Address	10000000.00010000.00000001.00001111	**128.16.1.15**
ANDing	11111111.11111111.11111111.00000000	**255.255.255.0**
Result	10000000.00010000.00000001.00000000	**128.16.1.0**

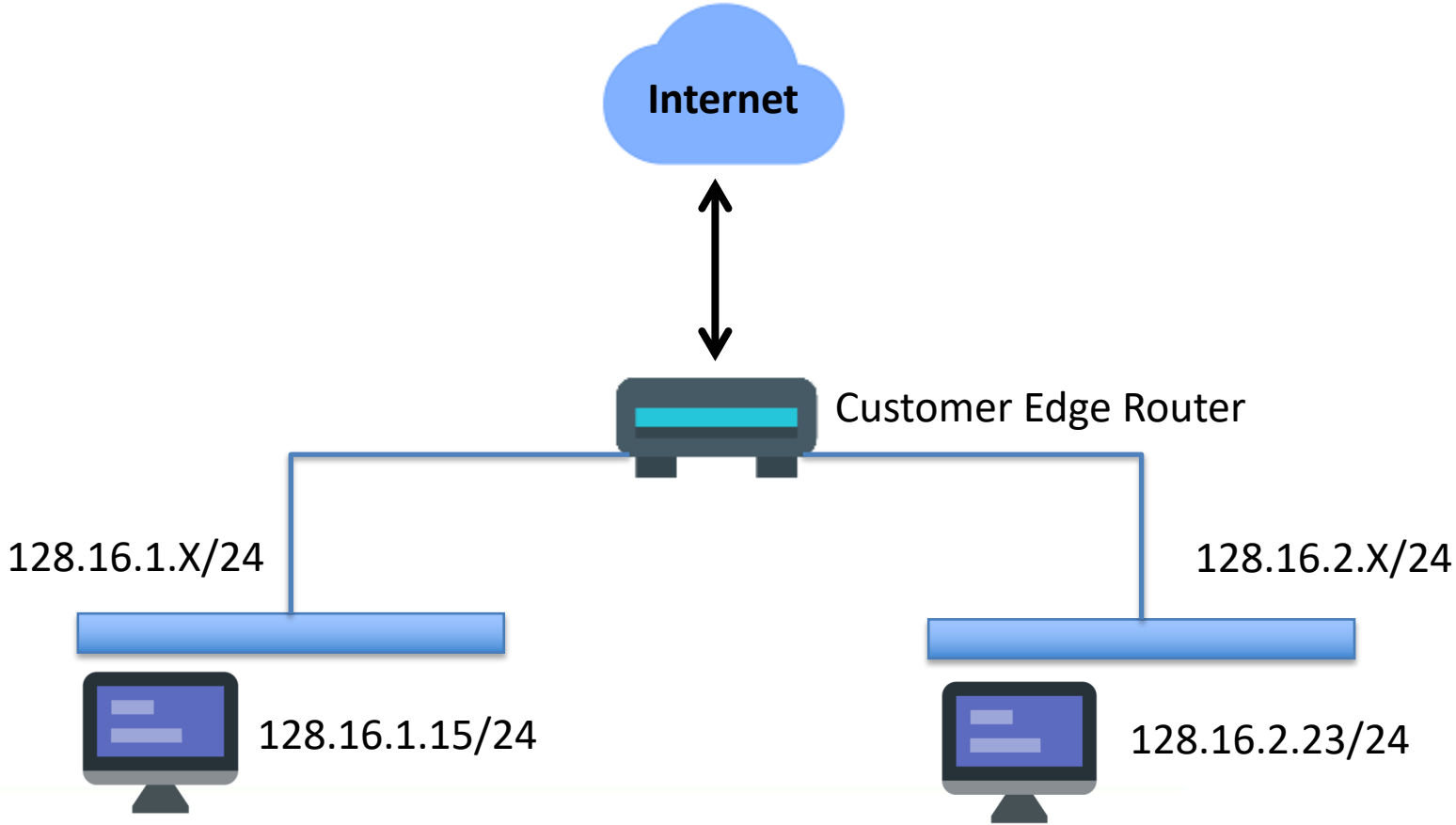
Classless inter-domain routing (CIDR)

- Compact method for representing IP addresses
- Sometimes called “Slash Notation”
- Eliminates the predefined partitioning of network and host numbers in the IP address
- The number of network (N) bits can be arbitrarily placed without regard to the legacy classes (A – E)
- For instance: the traditional Class C address 192.168.3.15 can be expressed as 192.168.3.15/24 or 192.168.3.15/16 or 192.168.3.15/23

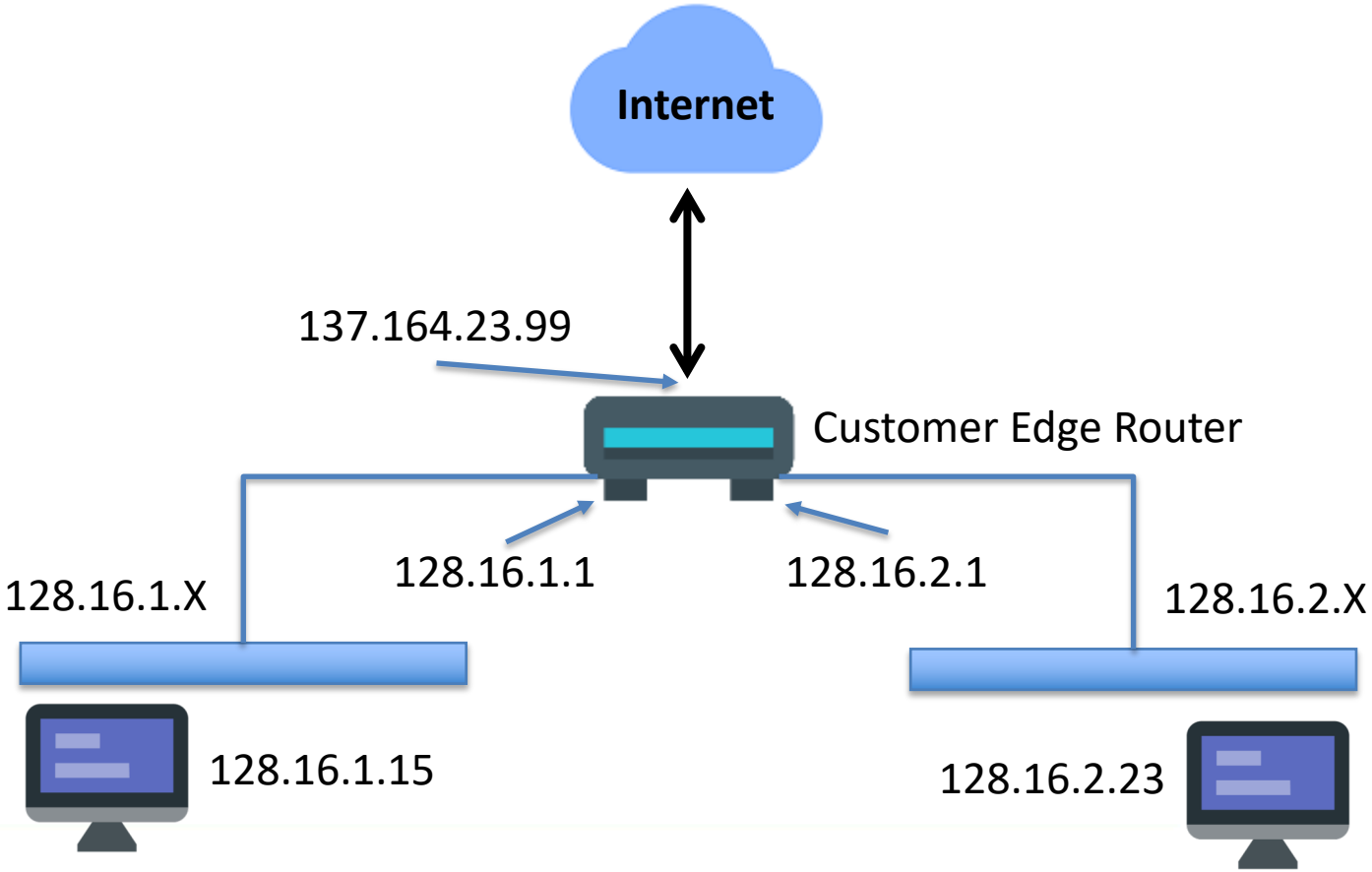
Subnetting Examples

Dotted-Decimal	Prefix Length	Binary Expression
128.0.0.0	/1	10000000 00000000 00000000 00000000
255.0.0.0	/8	11111111 00000000 00000000 00000000
255.192.0.0	/10	11111111 11000000 00000000 00000000
255.255.0.0	/16	11111111 11111111 00000000 00000000
255.255.254.0	/23	11111111 11111111 11111110 00000000
255.255.255.192	/27	11111111 11111111 11111111 11100000
255.255.255.255	/32	11111111 11111111 11111111 11111111

Addressing the Local Area Network



Addressing the Local Area Network



RFC 1918 Private Addresses

- Hosts within enterprises that use IP can be partitioned into three categories

1. Hosts that need network layer access outside the enterprise - Hosts in this category require IP addresses that are globally unambiguous (unique)
2. Hosts that do not require access to hosts in other enterprises or the Internet at large
3. Hosts that need access to a limited set of outside services which can be handled by mediating gateways

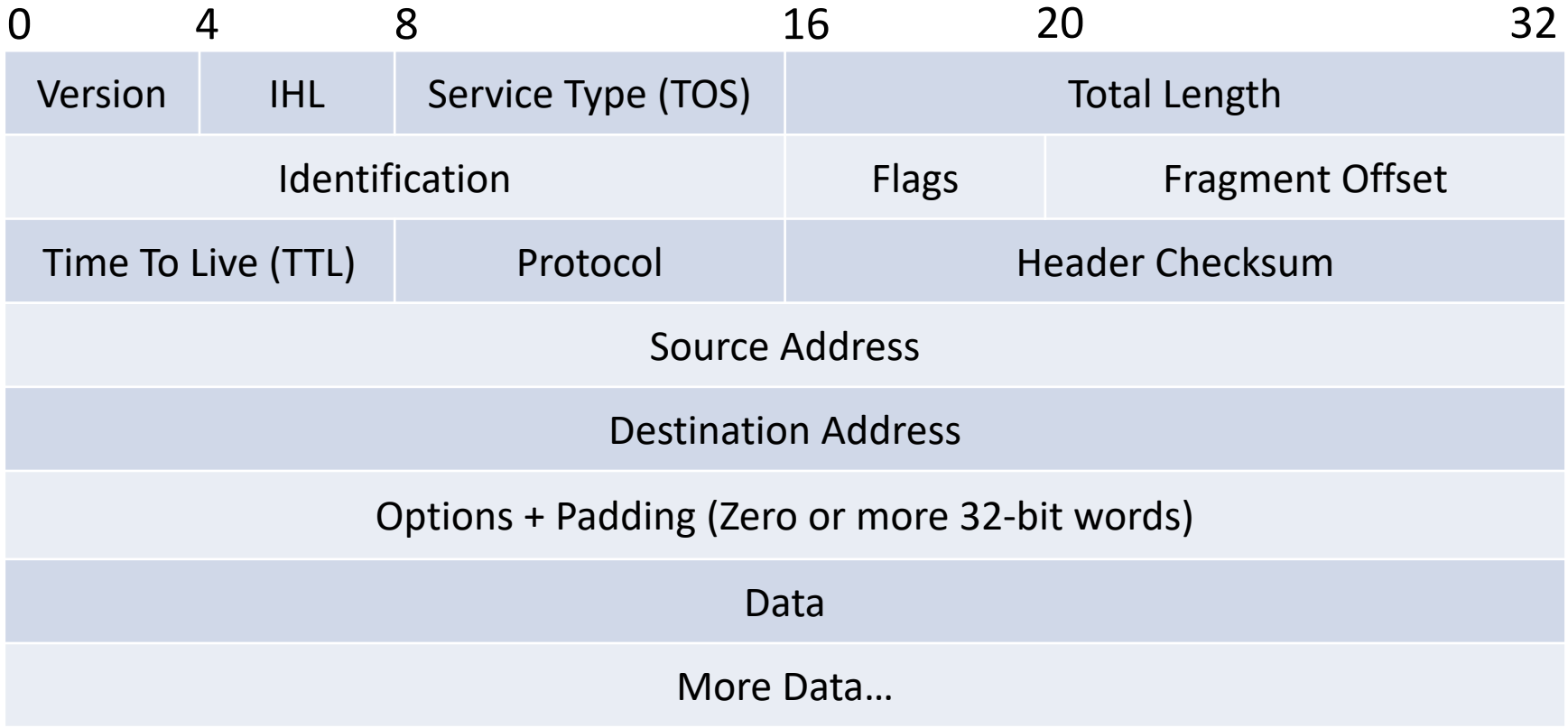
RFC 1918 Private Addresses

- The Internet Assigned Numbers Authority (IANA) reserved these three blocks of the IP space for private internets address space:
- **10.0.0.0 - 10.255.255.255 (10/8 prefix)**
- **172.16.0.0 - 172.31.255.255 (172.16/12 prefix)**
- **192.168.0.0 - 192.168.255.255 (192.168/16 prefix)**

Special-Use IPv4 Addresses (in CIDR)

CIDR Prefix	Special Use	RFC
0.0.0.0/8	Source address of Hosts on local network only	1122
10.0.0.0/8	Private networks only	1918
127.0.0.0/8	Loopback (same host) and 127.0.0.1 is most common	1122
169.254.0.0/16	Link-Local APIPA addresses	3927
172.16.0.0/12	Private networks only	1918
192.168.0.0/16	Private networks only	1918
224.0.0.0/4	IPv4 multicast range (previously Class D)	5771
255.255.255.255	Local network broadcast address	922

IP version 4 Header



IP Datagram Characteristics

Field Name	Size (bytes)	Description
Version	1/2 (4 bits)	***Version:*** Identifies the version of IP used to generate the datagram. For IPv4, this is of course the number 4. The purpose of this field is to ensure compatibility between devices that may be running different versions of IP. In general, a device running an older version of IP will reject datagrams created by newer implementations, under the assumption that the older version may not be able to interpret the newer datagram correctly.
IHL	1/2 (4 bits)	***Internet Header Length (IHL):*** Specifies the length of the IP header, in 32-bit words. This includes the length of any options fields and padding. The normal value of this field when no options are used is 5 (5 32-bit words = 5*4 = 20 bytes). Contrast to the longer *Total Length* field below.
TOS	1	***Type Of Service (TOS):*** A field designed to carry information to provide quality of service features, such as prioritized delivery, for IP datagrams. It was never widely used as originally defined, and its meaning has been subsequently redefined for use by a technique called *Differentiated Services (DS)*. See below for more information.
TL	2	***Total Length (TL):*** Specifies the total length of the IP datagram, in bytes. Since this field is 16 bits wide, the maximum length of an IP datagram is 65,535 bytes, though most are much smaller.
Identification	2	***Identification:*** This field contains a 16-bit value that is common to each of the fragments belonging to a particular message; for datagrams originally sent unfragmented it is still filled in, so it can be used if the datagram must be fragmented by a router during delivery. This field is used by the recipient to reassemble messages without accidentally mixing fragments from different messages. This is needed because fragments may arrive from multiple messages mixed together, since IP datagrams can be received out of order from any device.

IP Datagram Characteristics

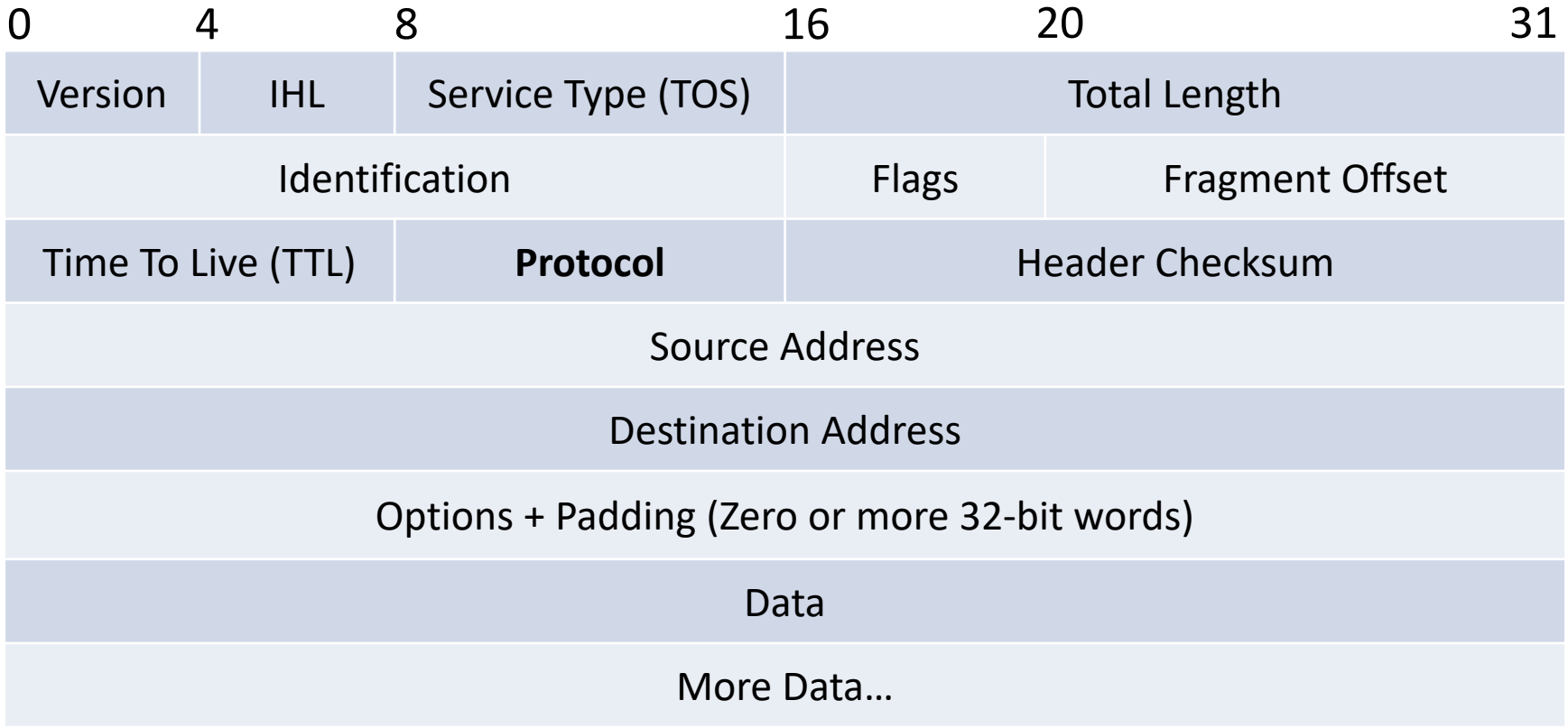
<table>
<tr>
<td>Flags</td>
<td>3/8
(3 bits)</td>
<td>
<table>
<tr><th>Subfield Name</th><th>Size (bytes)</th><th>Description</th></tr>
<tr><td>Reserved</td><td>1/8 (1 bit)</td><td>Reserved: Not used.</td></tr>
<tr><td>DF</td><td>1/8 (1 bit)</td><td>Don't Fragment: When set to 1, specifies that the datagram should not be fragmented. Since the fragmentation process is generally "invisible" to higher layers, most protocols don't care about this and don't set this flag. It is, however, used for testing the maximum transmission unit (MTU) of a link.</td></tr>
<tr><td>MF</td><td>1/8 (1 bit)</td><td>More Fragments: When set to 0, indicates the last fragment in a message; when set to 1, indicates that more fragments are yet to come in the fragmented message. If no fragmentation is used for a message, then of course there is only one "fragment" (the whole message), and this flag is 0. If fragmentation is used, all fragments but the last set this flag to 1 so the recipient knows when all fragments have been sent.</td></tr>
</table>
</td>
</tr>
<tr>
<td>Fragment Offset</td>
<td>1 5/8
(13 bits)</td>
<td>Fragment Offset: When fragmentation of a message occurs, this field specifies the offset, or position, in the overall message where the data in this fragment goes. It is specified in units of 8 bytes (64 bits). The first fragment has an offset of 0.</td>
</tr>
<tr>
<td>TTL</td>
<td>1</td>
<td>Time To Live (TTL): Short version: Specifies how long the datagram is allowed to "live" on the network, in terms of router hops. Each router decrements the value of the TTL field (reduces it by one) prior to transmitting it. If the TTL field drops to zero, the datagram is assumed to have taken too long a route and is discarded.</td>
</tr>
</table>

IP Datagram Characteristics

Protocol	1	

Value (Hexadecimal)	Value (Decimal)	Protocol
00	0	Reserved
01	1	ICMP
02	2	IGMP
03	3	GGP
04	4	IP-in-IP Encapsulation
06	6	TCP
08	8	EGP
11	17	UDP
32	50	Encapsulating Security Payload (ESP) Extension Header
33	51	Authentication Header (AH) Extension Header

IP version 4 Header



IP Datagram Characteristics

Header Checksum	2	***Header Checksum:*** A checksum computed over the header to provide basic protection against corruption in transmission. This is not the more complex CRC code typically used by data link layer technologies such as Ethernet; it's just a 16-bit checksum. It is calculated by dividing the header bytes into words (a word is two bytes) and then adding them together. The data is not checksummed, only the header. At each hop the device receiving the datagram does the same checksum calculation and on a mismatch, discards the datagram as damaged.
Source Address	4	***Source Address:*** The 32-bit IP address of the originator of the datagram. Note that even though intermediate devices such as routers may handle the datagram, they do not normally put their address into this field—it is always the device that originally sent the datagram.
Destination Address	4	***Destination Address:*** The 32-bit IP address of the intended recipient of the datagram. Again, even though devices such as routers may be the intermediate targets of the datagram, this field is always for the ultimate destination.
Options	Variable	***Options:*** One or more of several types of options may be included after the standard headers in certain IP datagrams.
Padding	Variable	***Padding:*** If one or more options are included, and the number of bits used for them is not a multiple of 32, enough zero bits are added to "pad out" the header to a multiple of 32 bits (4 bytes).
Data	Variable	***Data:*** The data to be transmitted in the datagram, either an entire higher-layer message or a fragment of one.

IP Version 6

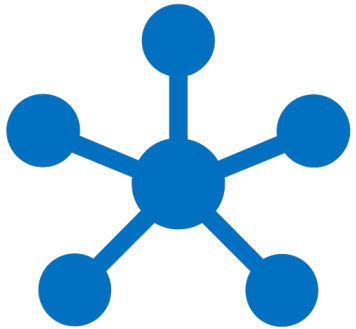
- IPv6 was intended to replace the widely used IPv4 that is considered the backbone of the modern Internet
- IPv6 is often referred to as the "next generation Internet" because of its expanded capabilities and its growth through recent large-scale deployments
- Uses a 128-bit hexadecimal address instead of a 24-bit dotted decimal

IPv6 Design Goals

- Larger (128-bit) address space
- Hierarchical addressing
- Better multicast support
- Easier autoconfiguration and renumbering
- More efficient datagram format
- Better QoS and Security
- Updated processes for fragmentation and reassembly
- Modernized support for routing
- Effective transition techniques
- Eliminates cumbersome technologies (like NAT and ARP)

IPv6 Addressing

- The format is X:X:X:X:X:X:X:X, where each X is a 16-bit hexadecimal field
- The leading zeros in each field are optional (010F can be written as 10F)
- A field that contains all zeros (0000) can be written as 0
- Successive fields of zeros can be represented as a double colon (::) but only once in an address

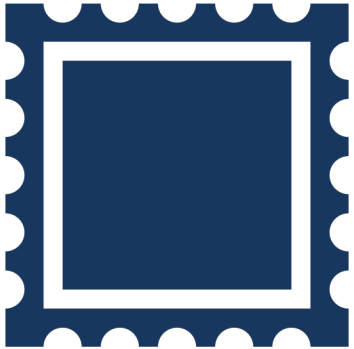


IPv6 Addressing

- The use of the double-colon technique makes many addresses very small
- For example - FF02:0:0:0:0:0:0:2 can be expressed as FF02::2
- The unspecified address is written as a double colon because it contains only zeros.

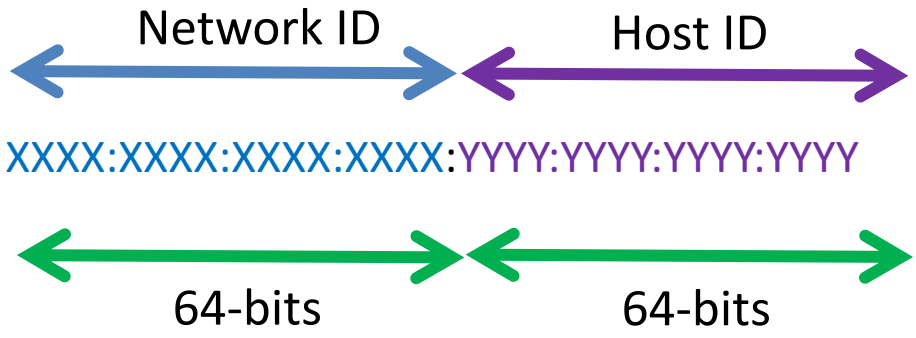
IPv6 Address Types

- **Unicast**: Unicast addresses are used in a one-to-one host scenario
- **Multicast**: Identifies a group of interfaces. Traffic is sent to multiple destinations at the same time. An interface may belong to any number of multicast groups.
- **Anycast**: An IPv6 anycast address is assigned to an interface on more than one node. It is routed to the nearest interface that has this address
- **No broadcast address support – uses multicast addresses**



IPv6 Unicast Addresses

- An IPv6 unicast address normally uses 64 bits for the network ID and 64 bits for the host ID
- The network ID is administratively-assigned and the host ID can be configured manually or autoconfigured



Assigning IPv6 Addresses

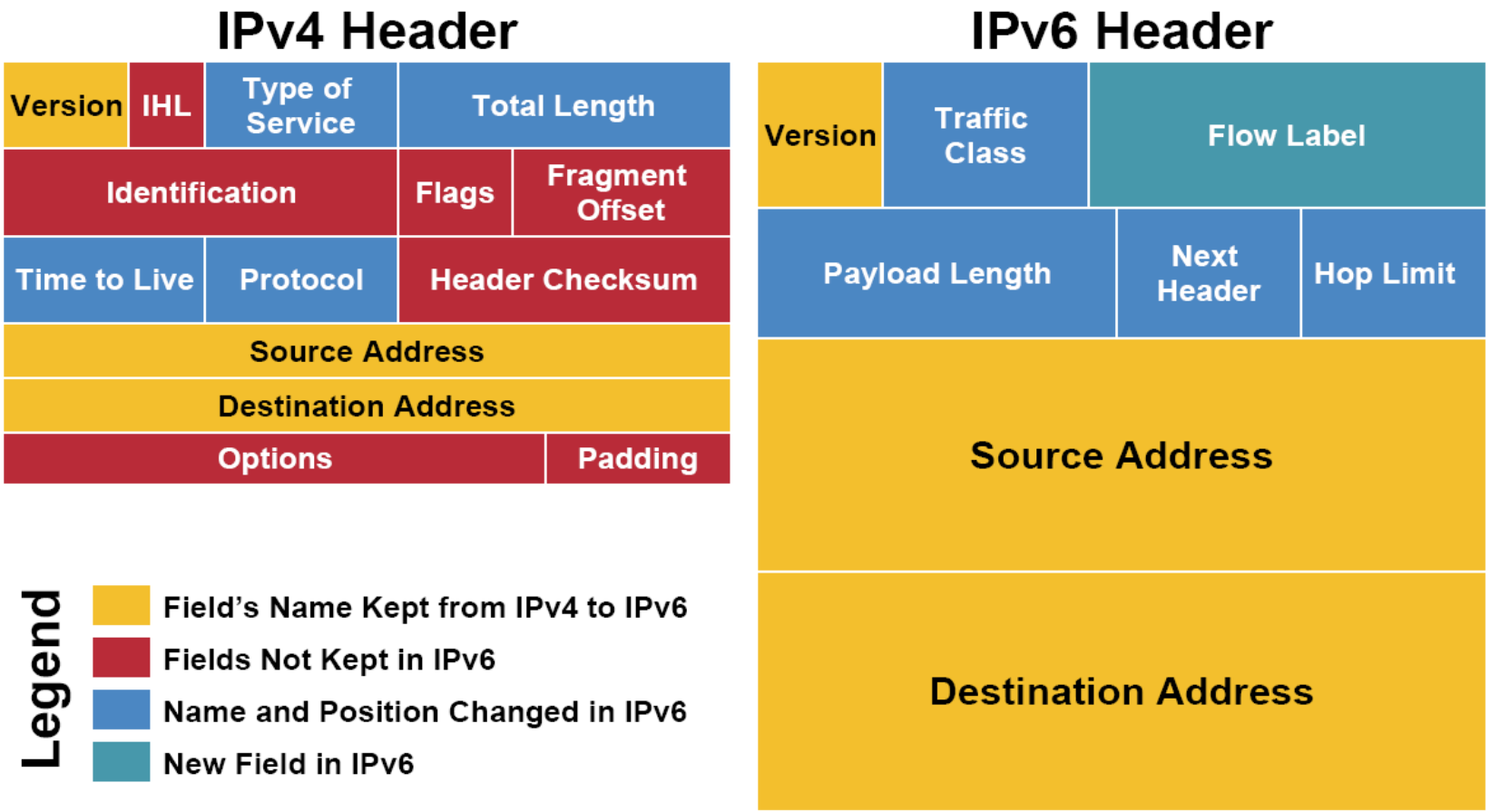
There are three methods for assigning IPv6 addresses:

- Manual
- Stateful Autoconfiguration (using a DHCPv6 server)
- **Stateless Autoconfiguration (SLAAC)**

Stateless Autoconfiguration

- Uses neighbor discovery to find routers and then dynamically create IPv6 addresses
- You must connect the host to a network that uses at least one IPv6-capable router that will send advertisement messages to the link
- The connected IPv6 nodes can self-configure with an IPv6 address and routing parameters without further human intervention (RFC 2462)

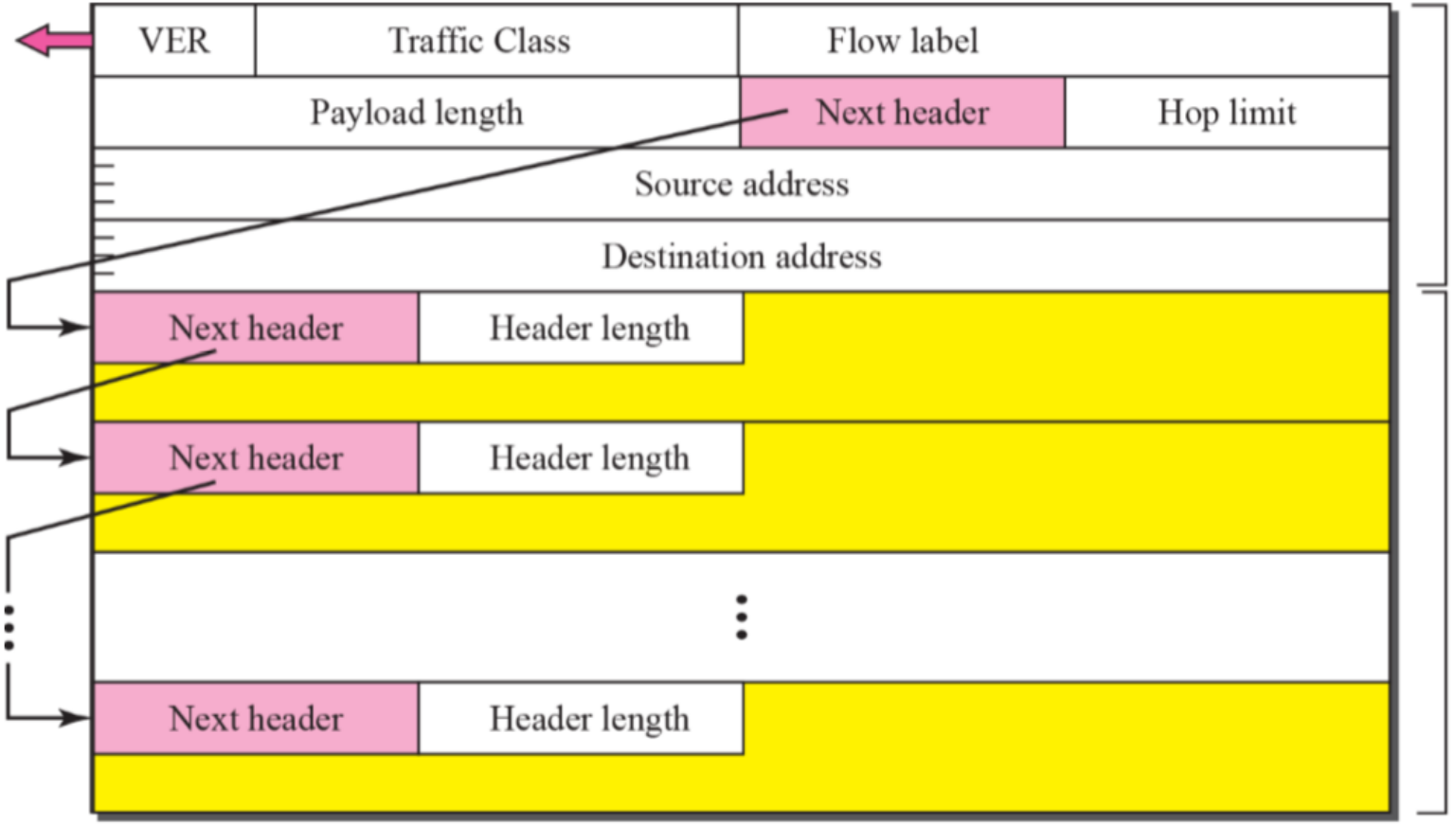
The IPv6 Header



IPv6 Extension Headers

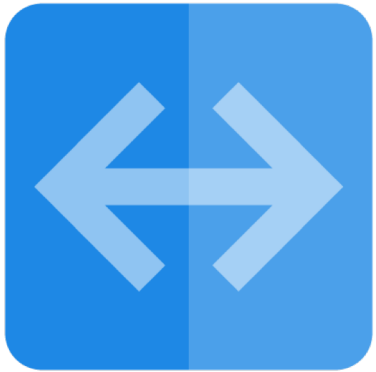
- IPv6 uses two distinct types of headers: The regular IPv6 Header and IPv6 Extension Headers
- The extension headers, if there are any, follow the original 8 fields
- The number of extension headers is not fixed, so the total length of the extension header chain is variable

IPv6 Extension Headers



Common Use Cases for EH

- Hop-by-Hop EH is used for the support of Jumbo-grams
- Destination EH is used in IPv6 Mobility
- Routing EH is used in IPv6 Mobility and in Source Routing
- Fragmentation EH is critical
- Mobility EH is used in support of Mobile IPv6 service
- Authentication EH and Encapsulating Security Payload EH



IPv4 vs. IPv6

Version 4	Version 6
2^{32} address space	2^{128} address space
Dotted decimal format	Hexadecimal notation
DHCP dynamic addressing	SLAAC and DHCPv6
Header has 20 bytes and 13 fields	Header has 40 bytes and 8 fields
Variable header length	Fixed header length
Header options (obsolete)	Header extensions
Header checksum	No header checksum

IPv4 vs. IPv6

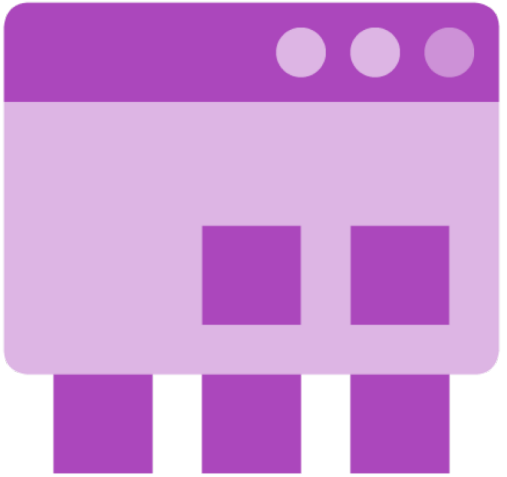
Version 4	Version 6
Packet size: 576 bytes required, fragmentation optional	Packet size: 1280 bytes required without fragmentation
Packet fragmentation: Routers and sending hosts	Packet fragmentation: Sending hosts only
IPv4 was never designed to be secure	Has native encryption and authentication
IPsec optional	IPsec mandatory
Non-equal geographical distribution (>50% USA)	No geographic limitations

The OSI Layer 4

Number	OSI Name	TCP/IP Model
7	Application	Application
6	Presentation	
5	Session	
4	**Transport**	**Transport (host-to-host)**
3	Network (or Internetwork)	Internet (internetwork)
2	Link	Network Interface (link)
1	Physical	Hardware*

Transport (Host-To-Host) Layer

- Enables end-to-end communication over internetworks
- Logical connections (ports) are made between hosts in a reliable (connection-oriented TCP) or unreliable manner (connectionless UDP)
- TCP/IP identifies the source and destination application process or service

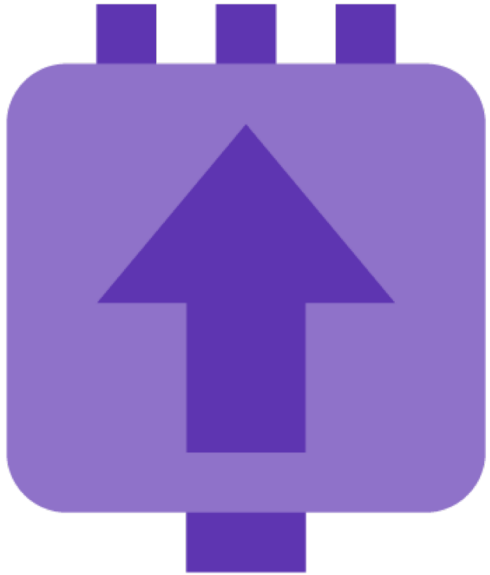


Transport (Host-To-Host) Layer

- Transmission Control Protocol (TCP) ensures reliable and flow-controlled delivery of data using IP
- User Datagram Protocol (UDP) is a more efficient, streamlined version of TCP that sends data between hosts without the reliability flow management techniques of TCP
- The TCP/IP transport layer includes specific functionality of the OSI Session layer 5 as well

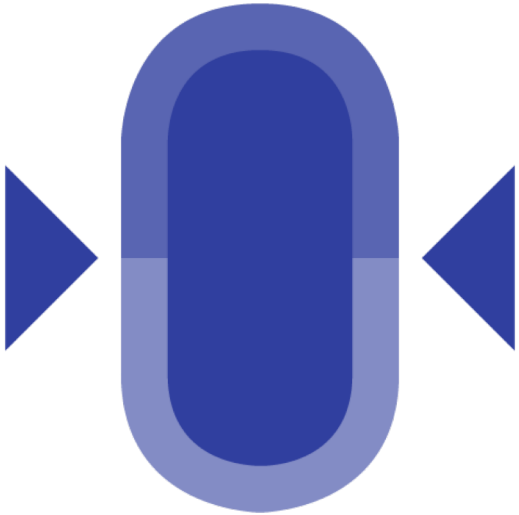
TCP Characteristics

- Connection-oriented
- Stream-oriented
- Bidirectional transport
- Allows multiple connections
- Reliable and acknowledged
- Unstructured data
- Managed data flow



TCP Functionality

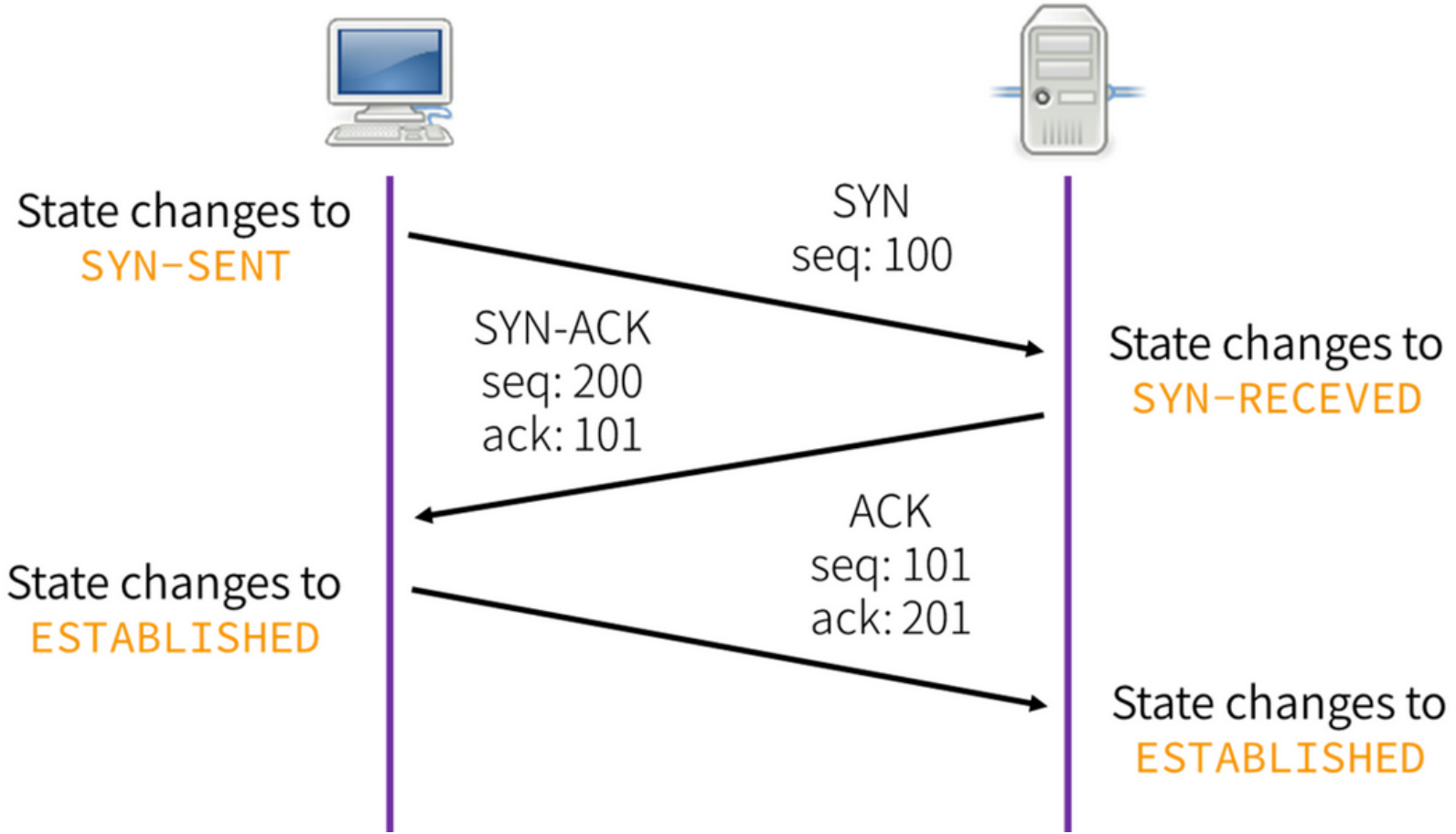
- Addressing and multiplexing
- Connection handling
- Packaging and managing data
- Transferring data
- Providing reliability and transmission quality
- Providing flow control
- Congestion avoidance



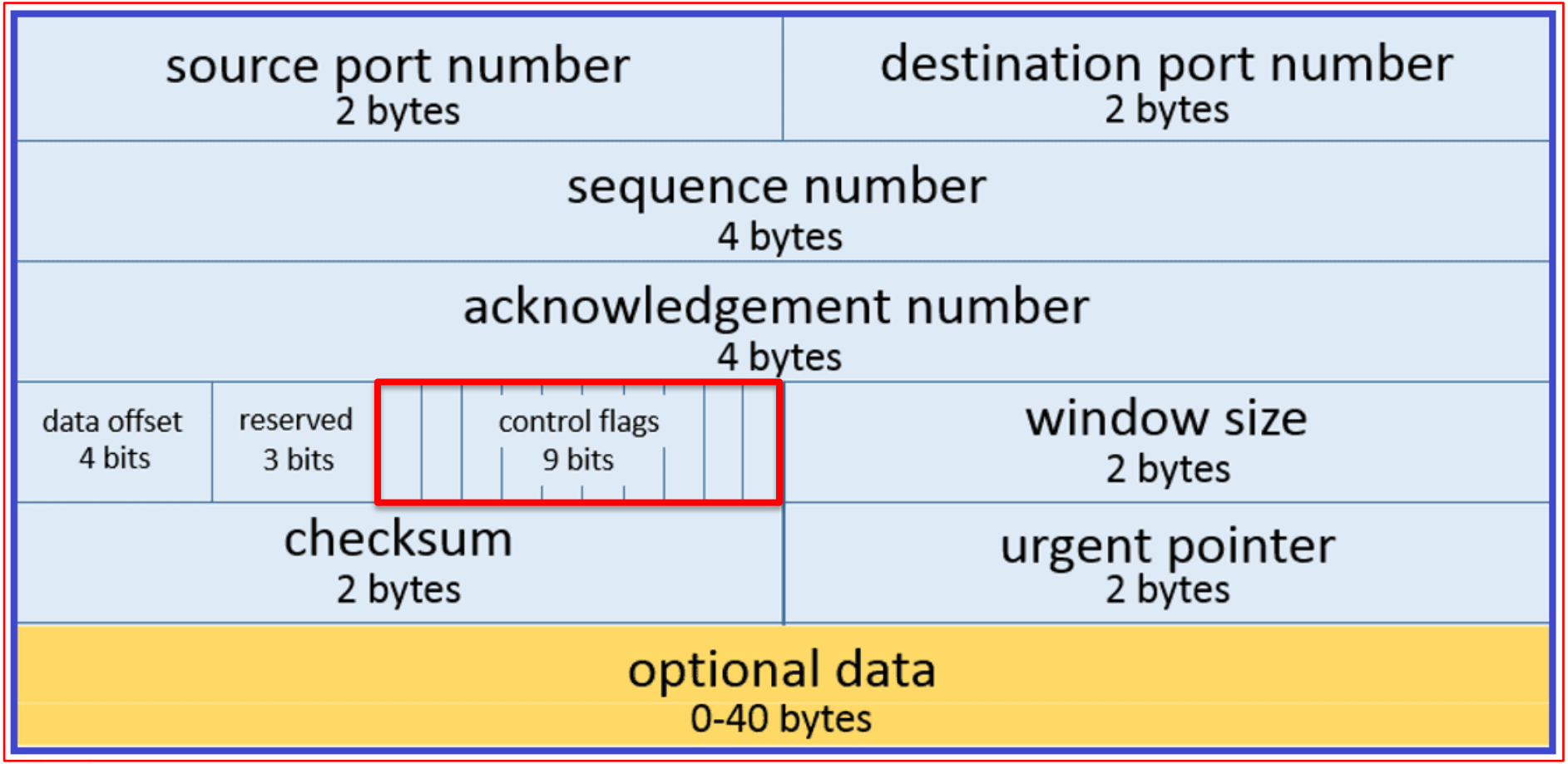
What TCP Doesn’t Do

- It doesn’t determine how applications actually use TCP
- Does not natively ensure privacy or authenticity
- TCP sends data as a continuous stream of segments instead of as discrete messages – the application decides where one message begins and ends
- TCP doesn’t guarantee the delivery of segments – it only provides reliability by detecting failed transport and resending segments

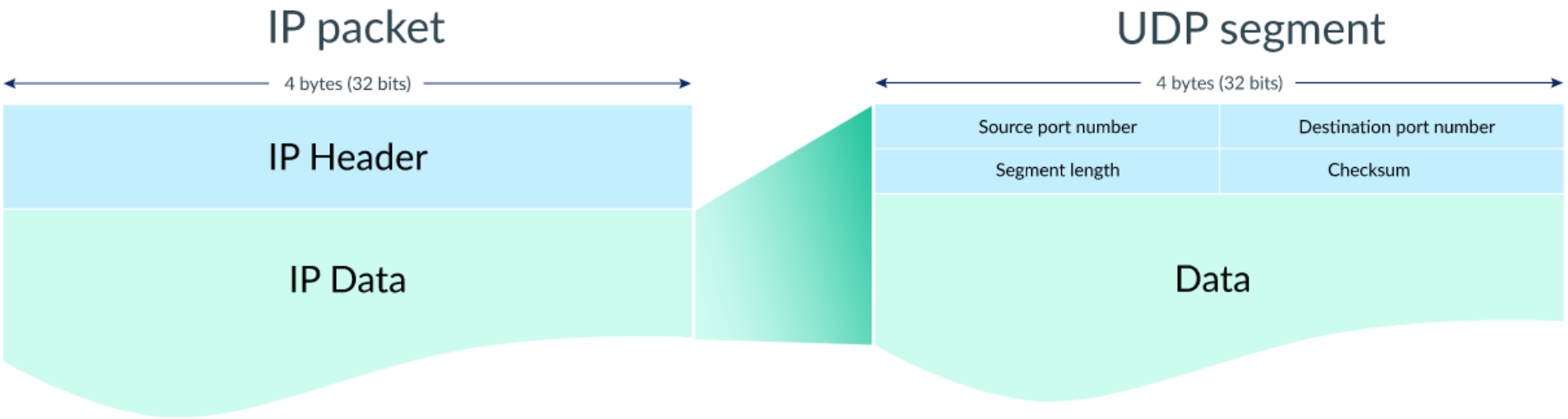
The 3-Way TCP Handshake



The TCP Header

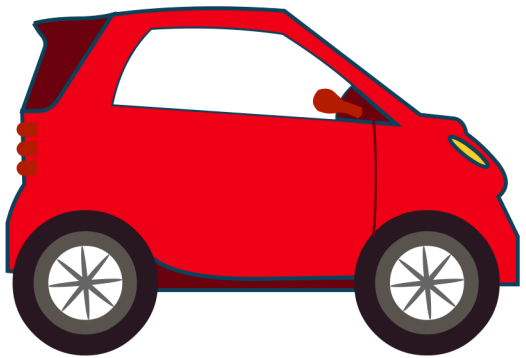


User Datagram Protocol (UDP)



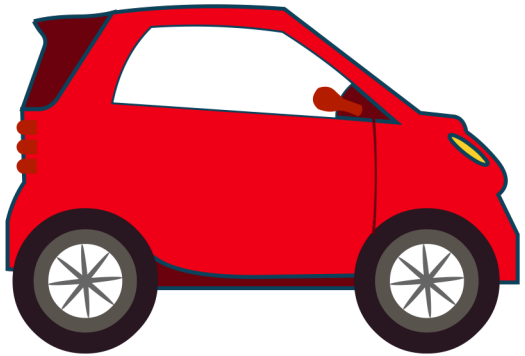
UDP Use Cases

- Typically used for real time applications which can not tolerate uneven delays between sections of a received message.
- Simple request response communication when size of data is small and there is less concern about flow and error control
- Suitable for multicasting as UDP supports packet switching
- UDP is used for some routing update protocols



UDP Use Cases

- The following application layer services uses UDP as a transport layer protocol:
  - NTP (Network Time Protocol)
  - DNS (Domain Name Service)
  - BOOTP, DHCP
  - TFTP, RTSP, RIP



QUIC

- The QUIC UDP Internet Connection (QUIC) is a newer transport protocol which was standardized by a Google working group in July 2016
- It reduces latency compared to using TCP
  - TCP is implemented in operating system kernels, and middlebox firmware, making significant changes to TCP is next to impossible.
  - Since QUIC is built on top of UDP, it suffers from no such limitations (Similar to TCP+TLS+HTTP/2 implemented on UDP)
  - A requirement is that all data is encrypted with TLS 1.3

QUIC

- In HTTP/3, the future replacement for HTTP/2, QUIC will completely replace TCP going forward
- LiteSpeed (as opposed to Apache and Nginx so far) is currently the only web server to fully implement QUIC, and as a result, HTTP/3

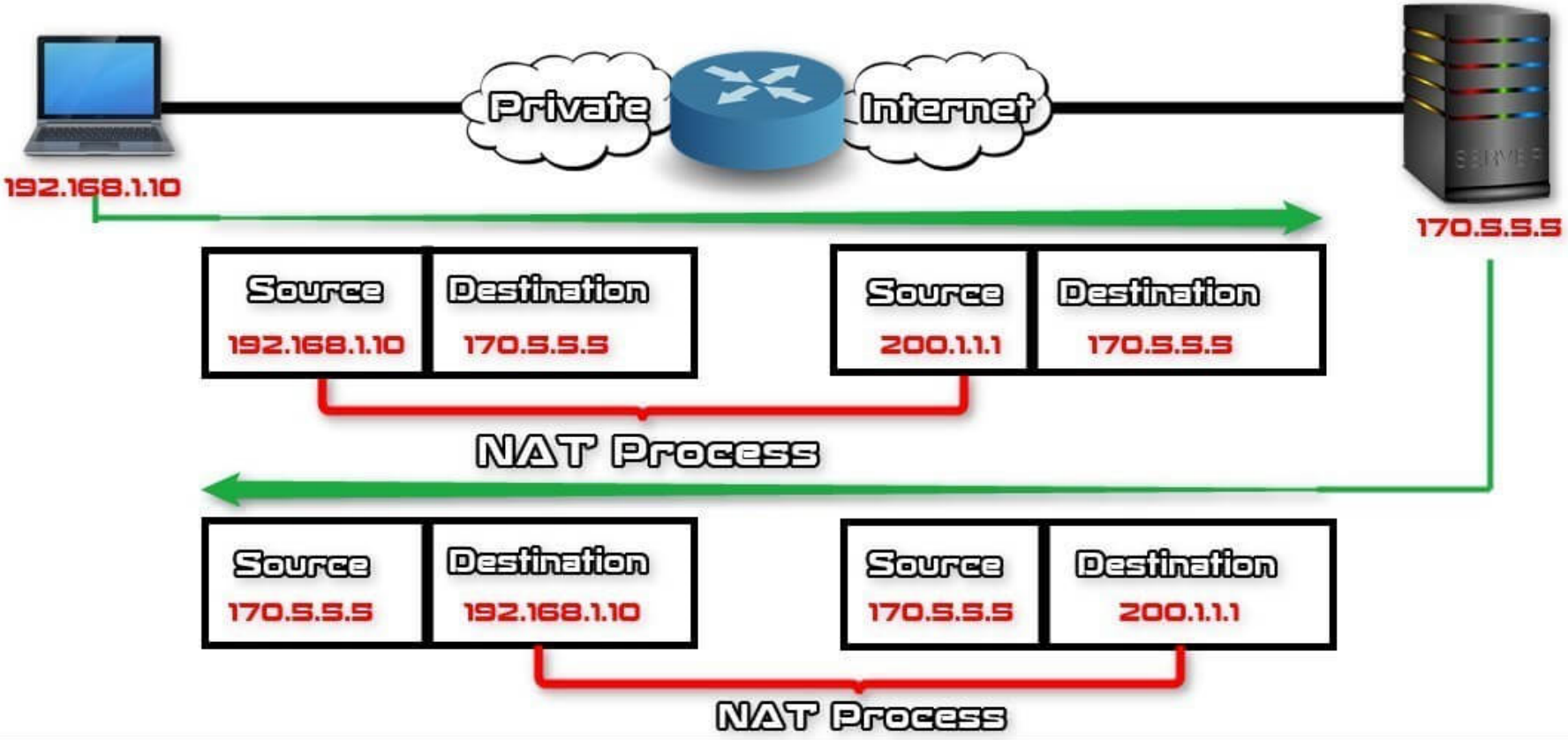
Common L4 Port Numbers

- 20 – FTP data
- 21 – FTP control
- 22 – SSH remote login
- 23 – TELNET
- 25 – Simple Mail Transport Protocol (SMTP)
- 49 – TACACS+
- 67 BOOTPS (server)
- 68 BOOTPC (client)
- 69 – TFTP
- 80 – HTTP
- 88 – Kerberos
- 110 – POP3
- 123 – Network Time Protocol
- 137 to 139 – NetBIOS
- 161 – SNMP
- 179 – Border Gateway Protocol (BGP)
- 443 – HTTP over SSL/TLS (HTTPS)
- 546 – DHCPv6 client
- 547 – DHCPv6 server

Key TCP/IP Services - NAT

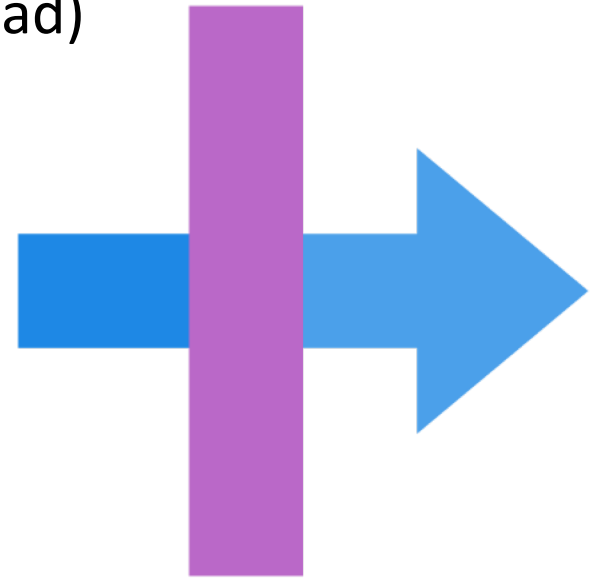
- IP Network Address Translation (NAT) allows an enterprise to set up a LAN of RFC 1918 private addresses while still allowing access to the public internet
- A NAT-capable edge router or firewall translate private to public and vice-versa
- Can allow for greater flexibility and address sharing
- Can provide security by hiding internal address scheme
- Can create problems with some security protocols and applications as well as affect performance

Key TCP/IP Services - NAT



Common Types of NAT

- Static NAT
- Dynamic NAT
- Port Address Translation (PAT – overload)
- Dynamic PAT
- Bidirectional NAT (Twice NAT)



NAT vs. PAT

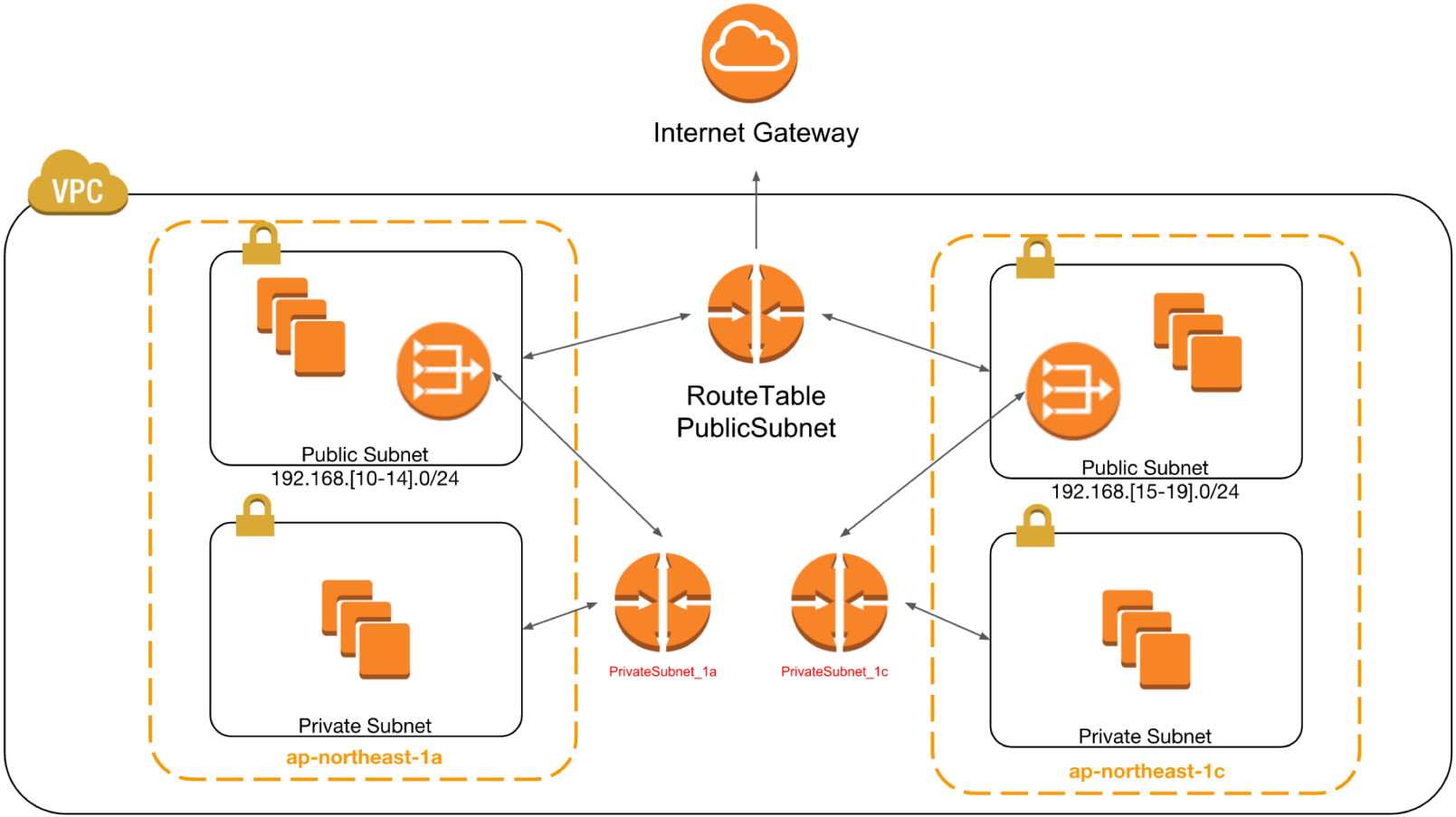
NAT

Inside Global Address Pool	Inside Local Address
209.165.200.226	192.168.10.10
209.165.200.227	192.168.10.11
209.165.200.228	192.168.10.12
209.165.200.229	192.168.10.13

PAT

Inside Global Address	Inside Local Address
209.165.200.226:1444	192.168.10.10:1444
209.165.200.226:1445	192.168.10.11:1444
209.165.200.226:1555	192.168.10.12:1555
209.165.200.226:1556	192.168.10.13:1555

NAT Gateways at AWS



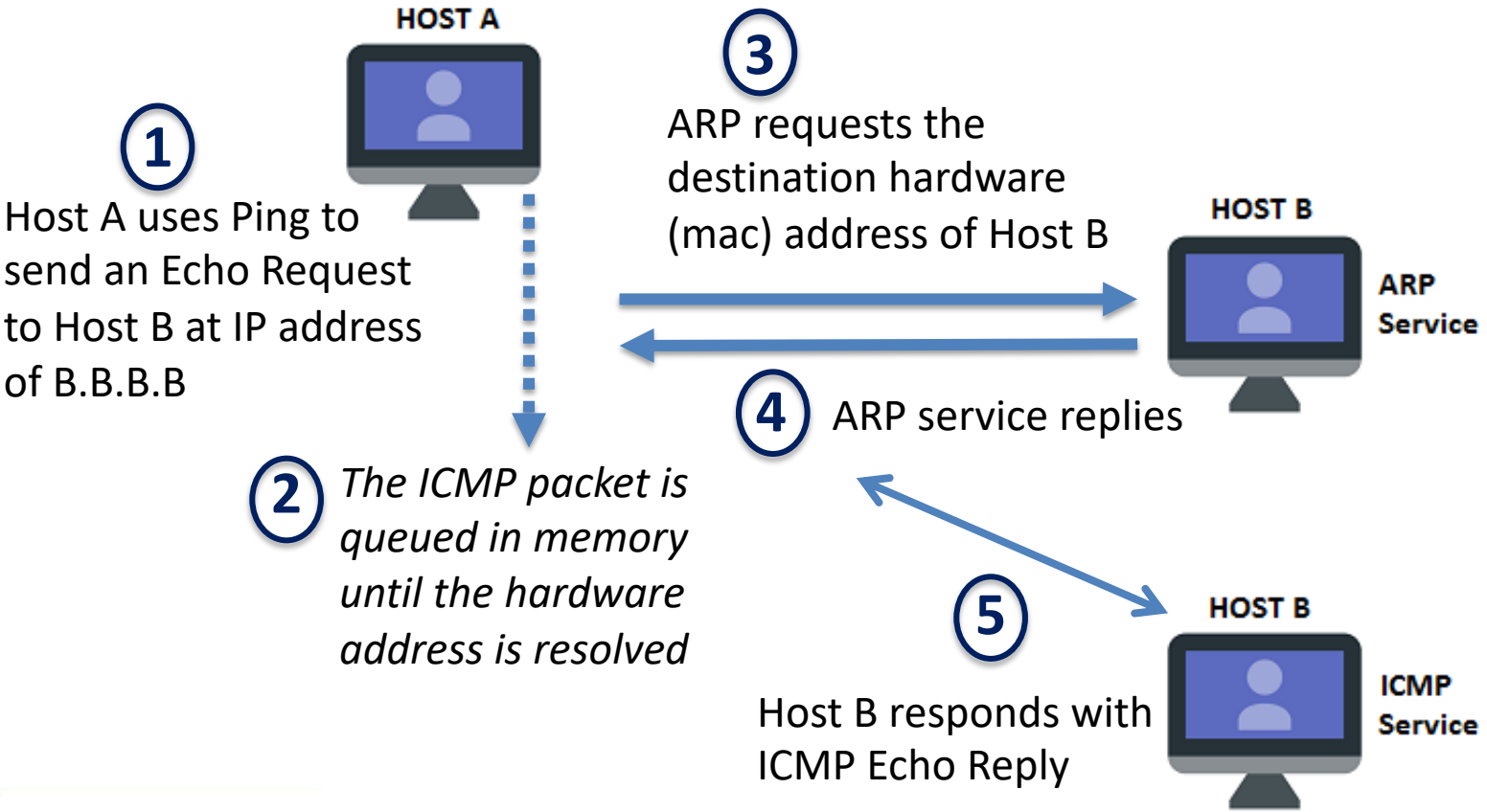
Address Resolution Protocol (ARP)

- ARP is a protocol used by IPv4 to map IP network addresses to the hardware addresses used by a data link protocol
- ARP functions below the Network layer as an interface between that layer and the Link layer
- There are four types of ARP messages:
  - ARP request
  - ARP reply
  - RARP request
  - RARP reply

Address Resolution Protocol (ARP)

- To reduce the number of requests, a client typically caches resolved addresses for a short period of time
- The ARP cache is of a finite size and can fill up (flood attack), therefore it is periodically flushed of all entries
- This deletes unused entries and frees up space in the cache as well as stops the unsuccessful attempts to contact hosts which are not currently running

ARP in Action



Internet Control Message Protocol (ICMP)

- IP is unreliable and doesn't guarantee delivery, so ICMP is the feedback mechanism offering feedback about network problems
- IP also doesn’t offer a direct method for collecting diagnostic information
- It resides somewhere between the Transport and Network layers
- ICMP provides error messages and informational messages

ICMP Characteristics

- ICMP definitely affects network operations in both positive and negative ways
- Many border routers and firewalls will block most, if not all, ICMP messages
- However, if blocked, diagnostic tools like ping and traceroute will not work
- There are a number of Types and Codes and only a few are commonly used

Common ICMPv4 Messages

Name	Type	E/I	Description
Echo Reply	0	I	Ping reply that returns data
Destination Unreachable	3	E	Unreachable host/protocol
Redirect	5	E	Alternate gateway should be used
Echo	8	I	Ping request (data optional)
Time Exceeded	11	E	Resource exhausted (TTL decremented)
Parameter Problem	12	E	Malformed packet or header

Ping

- The basic purpose of ping is to verify the following metrics:
  - Reachability
  - RTT
  - Packet loss
- The Ping program uses the ICMP Echo Request (Type 8) and Echo Reply (Type 0)

Ping

```
Switch# ping 10.10.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/5 ms
Switch# ping 10.10.1.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.20, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
Switch# ping 10.10.1.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/20/99 ms
```

Traceroute (successful)

```
C:\>tracert w3.pok.ibm.com

Tracing route to w3.pok.ibm.com [222.222.222.222]

over a maximum of 30 hops:

  1     2 ms     2 ms     1 ms  locbldsamp1.pok.ibm.com
[222.222.222.222]

  2     6 ms     7 ms     6 ms  locbldsamp2.pok.ibm.com
[222.222.222.222]

  3    15 ms     9 ms    14 ms  w3.pok.ibm.com [222.222.222.222]

Trace complete.

C:\>
```

Traceroute (unsuccessful)

```
C:\>tracert testcase.boulder.ibm.com

Tracing route to testcase.boulder.ibm.com [222.222.222.222]

over a maximum of 30 hops:

  1     2 ms     1 ms     2 ms  locbldsamp1.pok.ibm.com
[222.222.222.222]

  2    20 ms     8 ms     6 ms  locbldsamp2.pok.ibm.com
[222.222.222.222]

  3    16 ms    10 ms     7 ms  222.222.222.222

  4     *        *        *     Request timed out.

  5     *        *        *     Request timed out.

  6     *
```

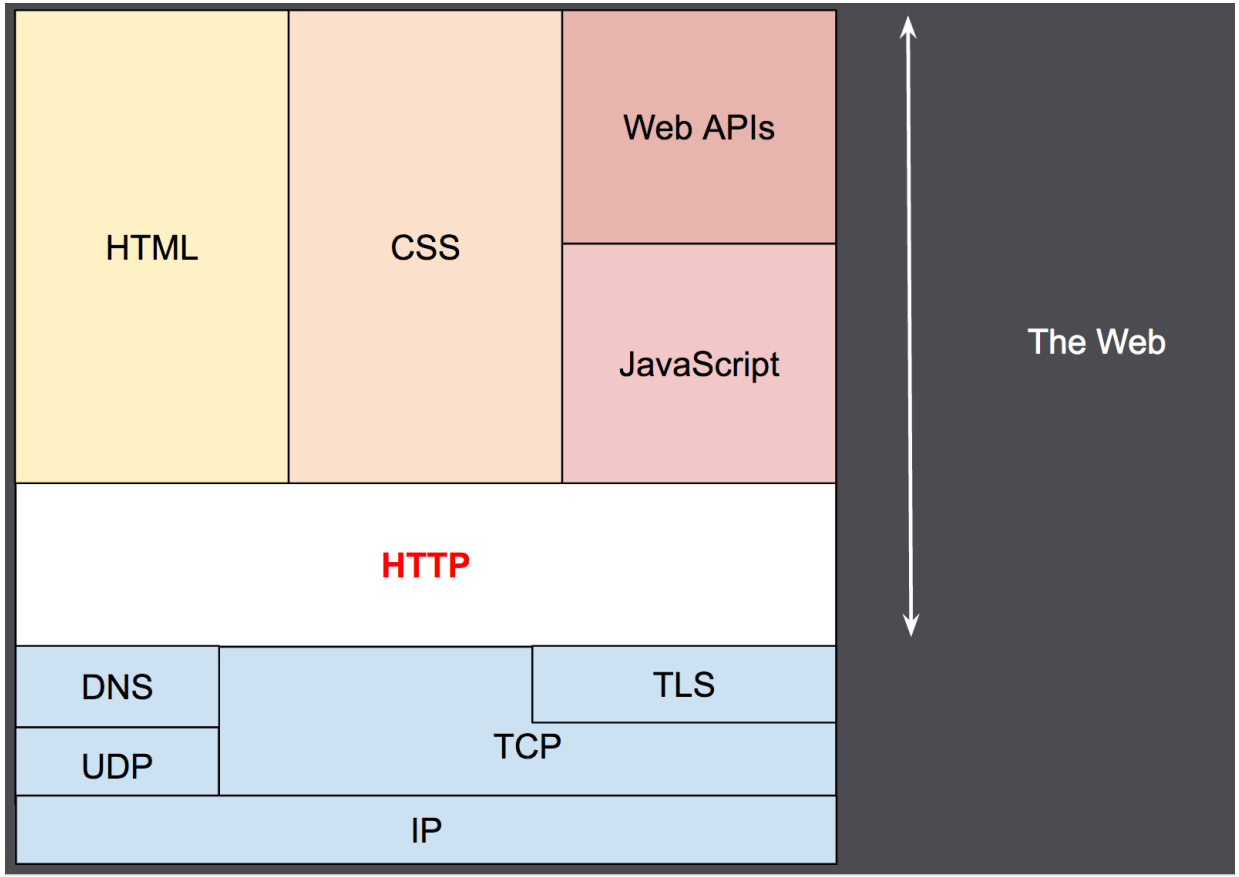
The Hypertext Transfer Protocol (HTTP)

- It is the foundation of any data exchange on the World Wide Web
- HTTP enables the fetching of resources, such as HTML documents from servers
- It is a TCP-port 80 client-server protocol, which means requests are initiated by the recipient, usually the Web browser
- Uses request and response headers
- The best- known and most widely deployed version is HTTP/1.1 although HTTP/3 has been fully defined

HTTP/S

- The Internet of today does the following:
  - The text format for displaying hypertext documents (HTML)
  - Software browsers to display the documents
  - A simple protocol for exchanging documents
  - A server that grants access to the documents (the HTTP daemon (HTTPD)
- HTTP/S is HTTP over SSL/TLS for secure transmission on TCP port 443
- Today SSL should never be used on public web servers – only Transport Layer Protocol (TLS)

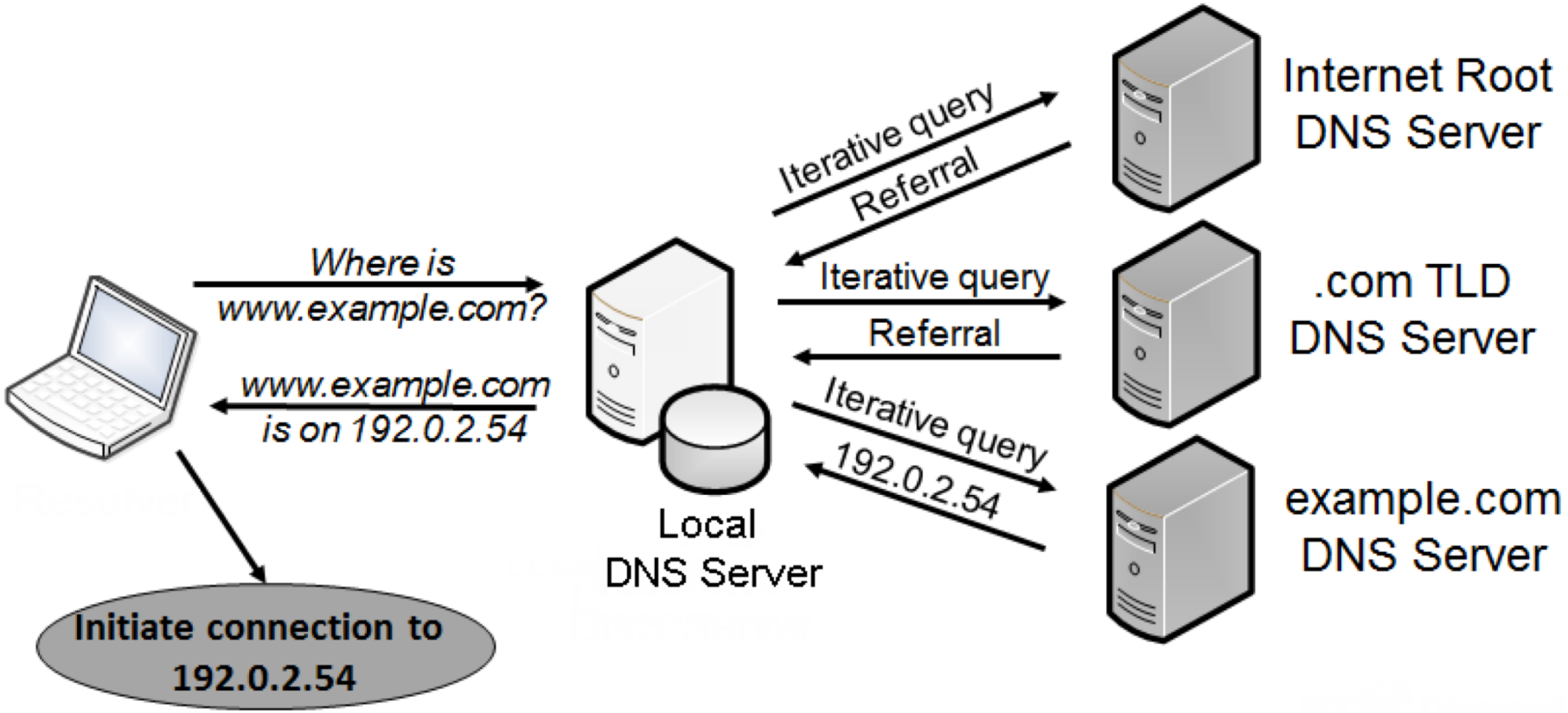
HTTP/S



Domain Name System (DNS)

- DNS offers convenient and efficient method for mapping human-readable names to machine-readable IP addresses
- Without DNS one would have to remember many node numbers – hundreds or more
- Uses a globally distributed database that is highly automated
- Many newer security mechanisms have been introduced

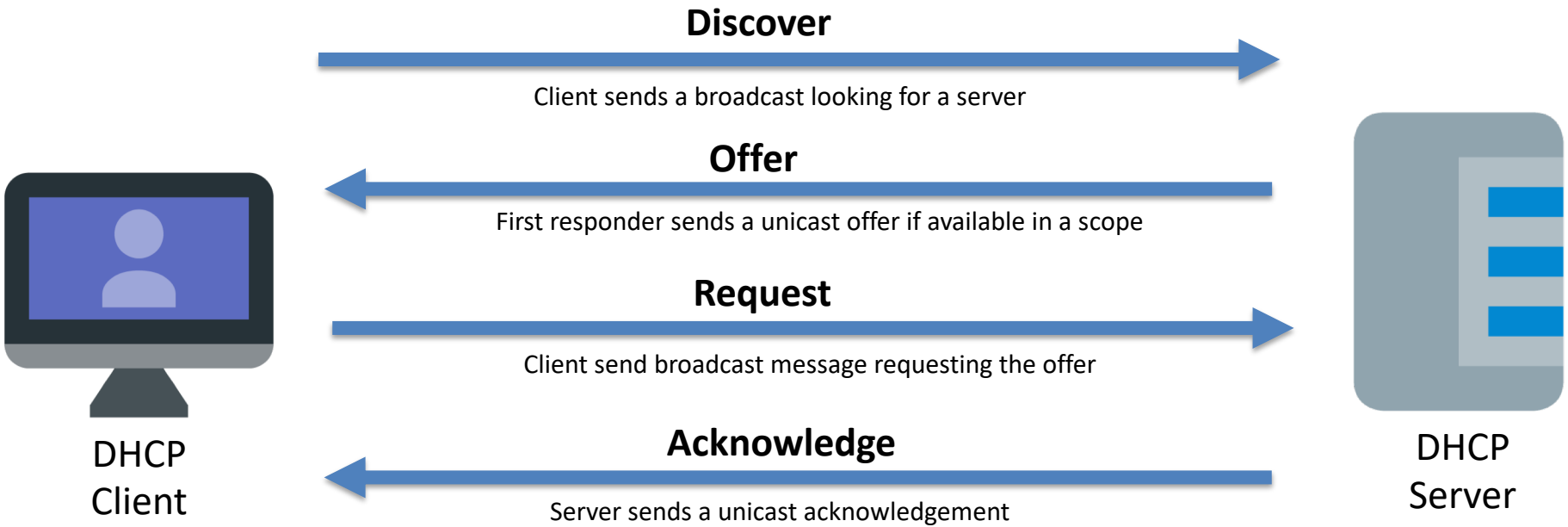
DNS Query Resolution



Dynamic Host Configuration Protocol

- DHCP reduces the administrative burden of assigning IP addresses and other configuration information to endpoints in wired and wireless networks
- The endpoints “lease” configurations from “scopes” on DHCP servers that push out settings based on VLAN membership
- Centralized policy can be used to ensure consistent settings across the entire organization

The DHCP “DORA” Process



Border Gateway Protocol (BGP)

- BGP is one of the original foundational routing protocols of the Internet
  - Complex
  - Scalable
  - Reliable
  - Secure
  - TCP-based
- EBGP is a part of the BGP that is used for exchanging routes between different autonomous systems (AS)

Border Gateway Protocol (BGP)

- An autonomous system is a collection of networks under a single technical administration domain
- BGP provides the routing between these autonomous systems
- BGP can be an internal or external protocol although OSPF, RIP, and EIGRP are more common IGPs

Border Gateway Protocol (BGP)

- Reliable updates using TCP port 179
- Can be IGP or EGP
- Customers exchange routed with ISP
- ISPs trade routed with other ISPs

- Highly scalable
- Security through peer authentication and route filtering
- Supports advanced routing policies and manipulation between peers

Get Wireshark!