CompTIA Network+

EXAM

N10-008

N10-008 Exam Domains

1.0 Networking Fundamentals	24%
2.0 Network Implementation	19%
3.0 Network Operations	16%
4.0 Network Security	19%
5.0 Network Troubleshooting	22%
Total	**100%**

Networking Fundamentals

DOMAIN 1.0

MODULE 1

Networking Fundamentals Topics

Intro to Networking

Common Terminology

OSI Model

DOD Model

TCP/IP

Network Topologies

Network Types and Characteristics

Intro to Networking

What is a Network?

Two or more computers connected together

The computers can be any type of computing device

The connection can be wired or wireless

Why Have a Network?

Share data

Remote communication

Share resources such as printers, faxes, databases, and services

Distribute a computing workload

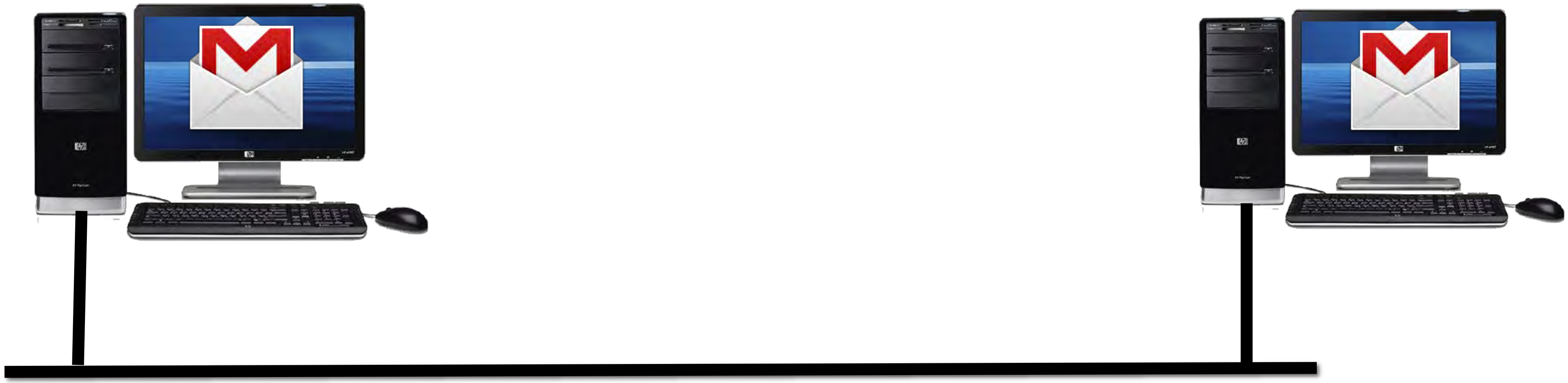
- Sensor – Monitor
- Client – Server
- Multiple facilities working together

Cost effectiveness and reliability

How Computers Communicate on a Network

Both Sides Need:

Applications that want to talk to each other

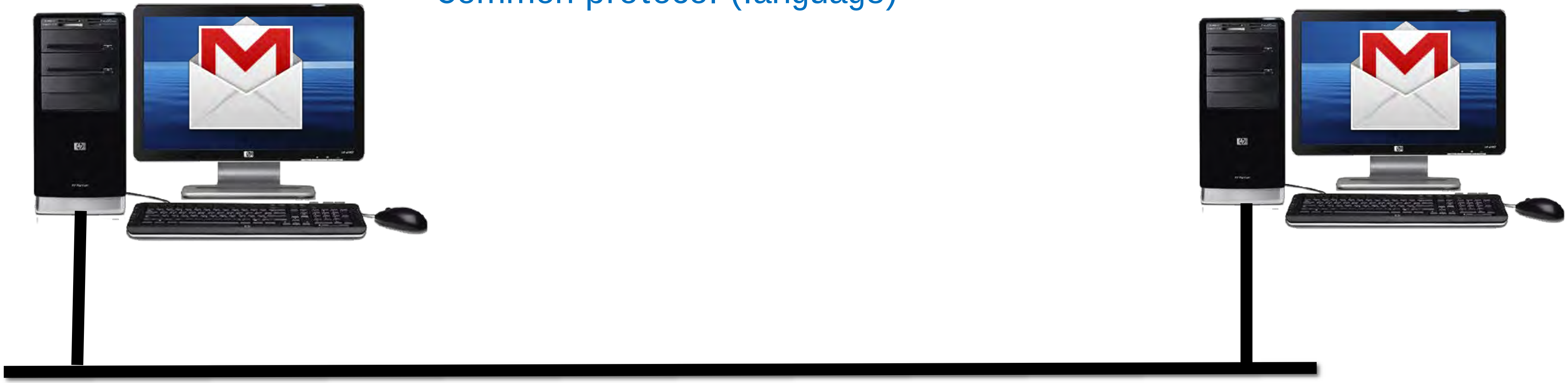


How Computers Communicate on a Network

Both Sides Need:

Applications that want to talk to each other

Common protocol (language)



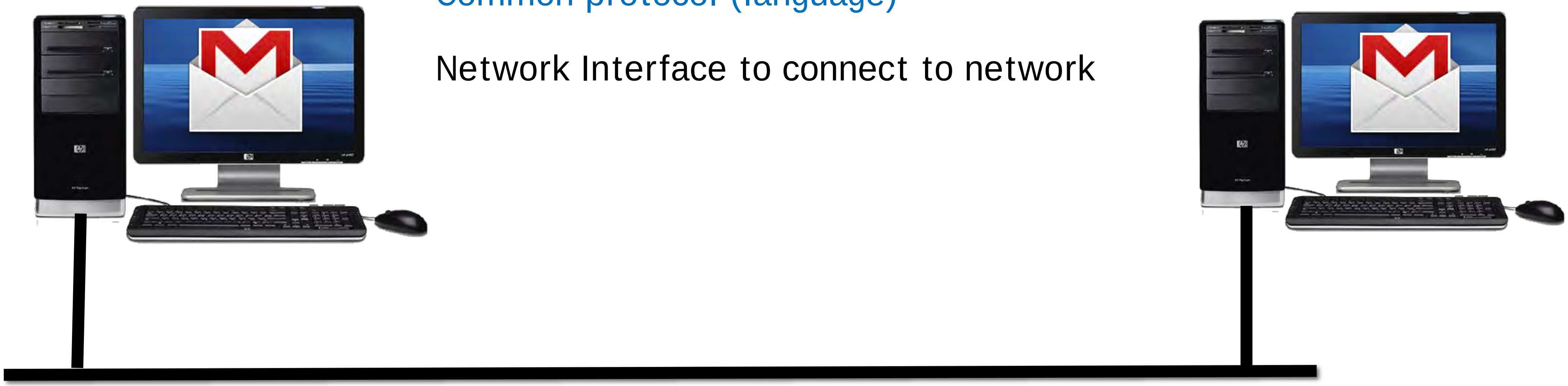
How Computers Communicate on a Network

Both Sides Need:

Applications that want to talk to each other

Common protocol (language)

Network Interface to connect to network



How Computers Communicate on a Network

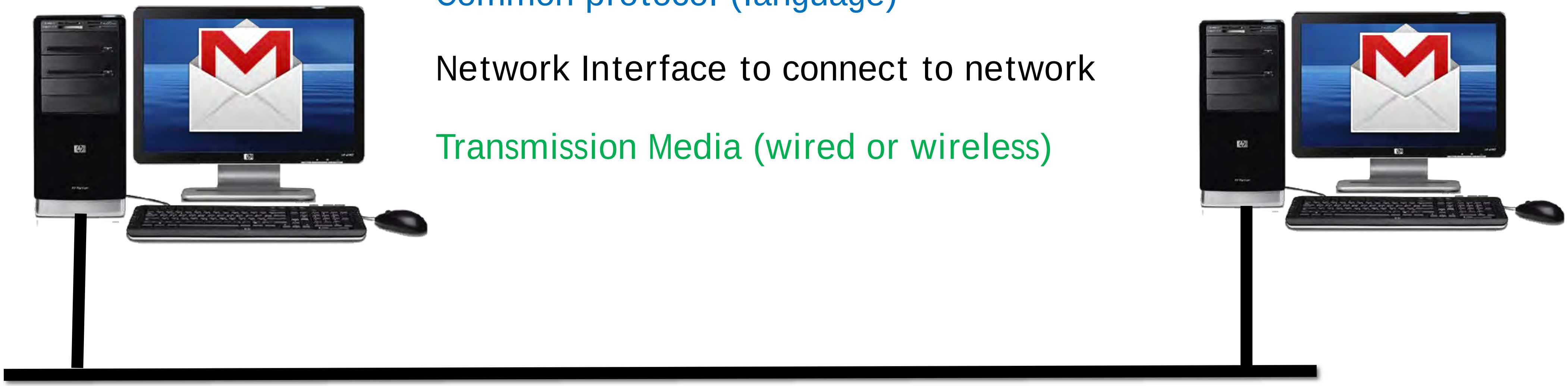
Both Sides Need:

Applications that want to talk to each other

Common protocol (language)

Network Interface to connect to network

Transmission Media (wired or wireless)



How Computers Communicate on a Network

Two hosts want to communicate

Host 1

Host 2

How Computers Communicate on a Network

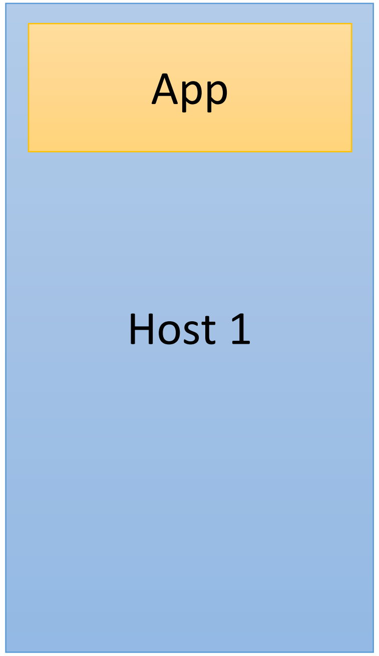
Usually, both hosts have applications that want to communicate

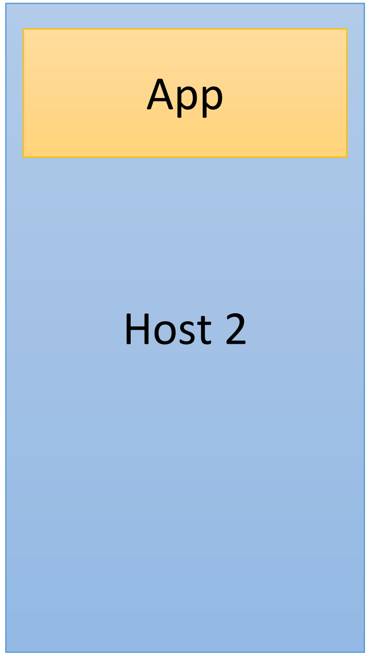
App
Host 1
App
Host 2

How Computers Communicate on a Network

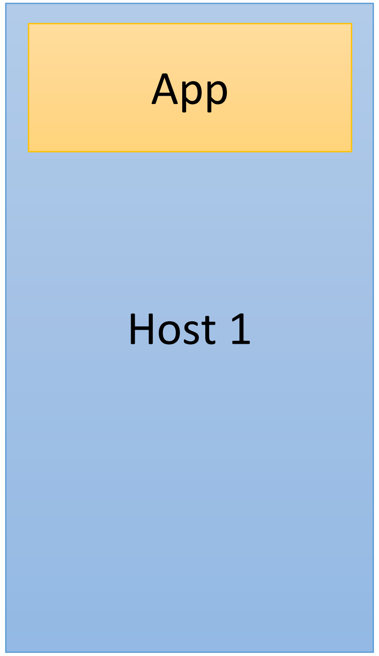
Usually, both hosts have applications that want to communicate

But most apps are not designed to use a network directly





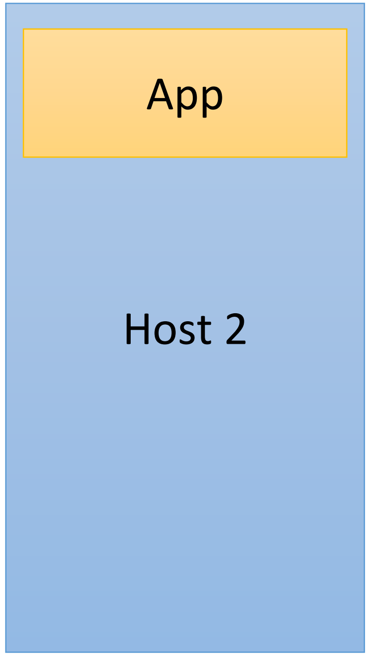
How Computers Communicate on a Network



Usually, both hosts have applications that want to communicate

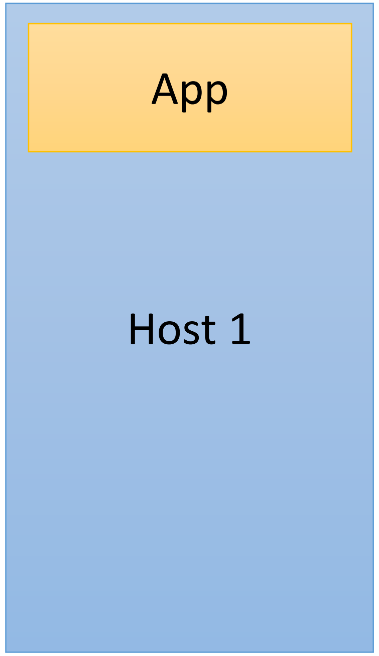
But most apps are not designed to use a network directly

They need the operating system with its networking services to help them

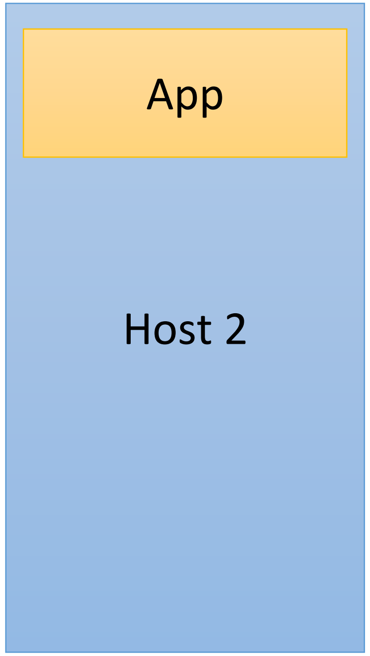


Basic Network Components

Networking has the following components:

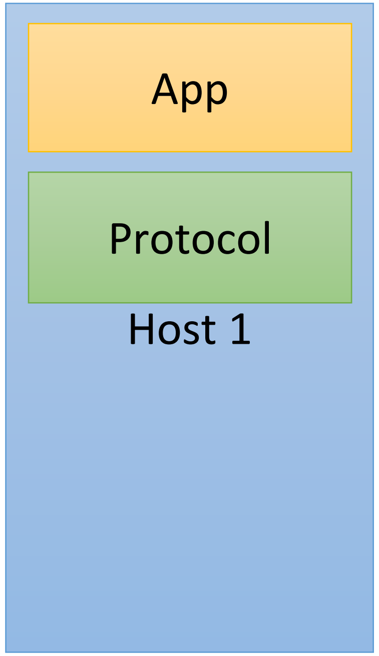


Applications that want to communicate



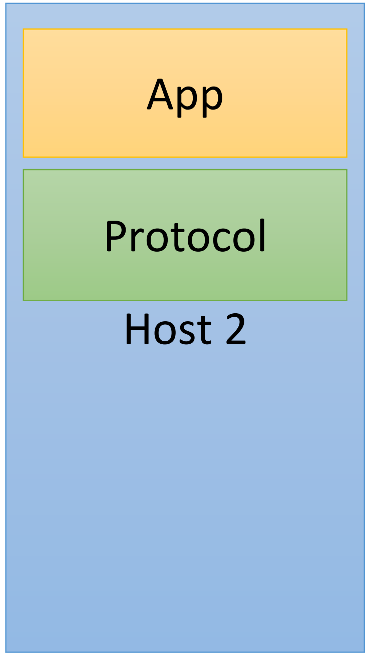
Basic Network Components

Networking has the following components:



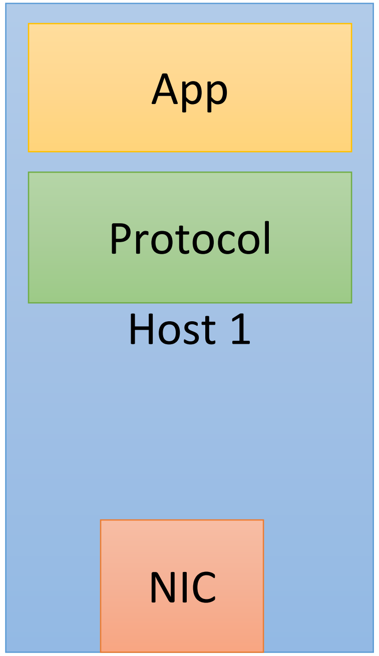
Applications that want to communicate

A common language (protocol)



Basic Network Components

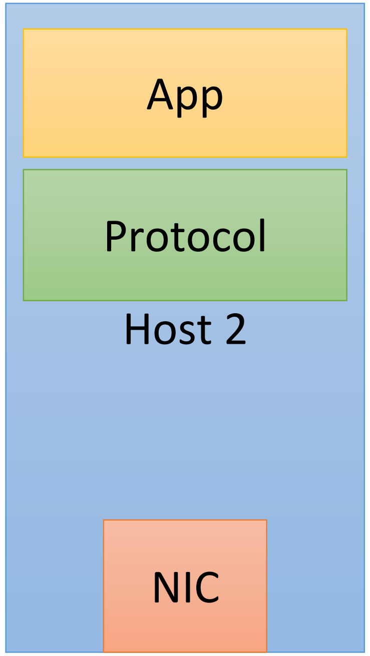
Networking has the following components:



Applications that want to communicate

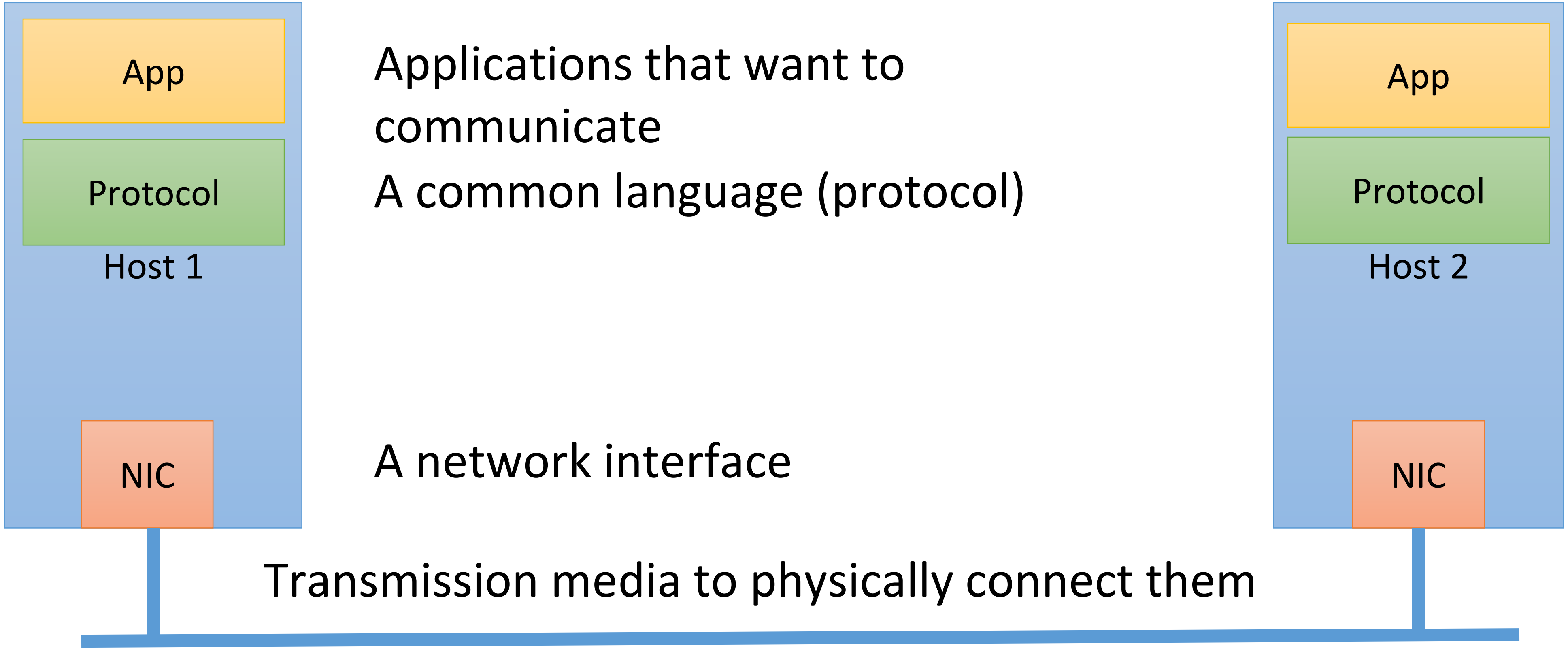
A common language (protocol)

A network interface



Basic Network Components

Networking has the following components:



Applications that want to communicate

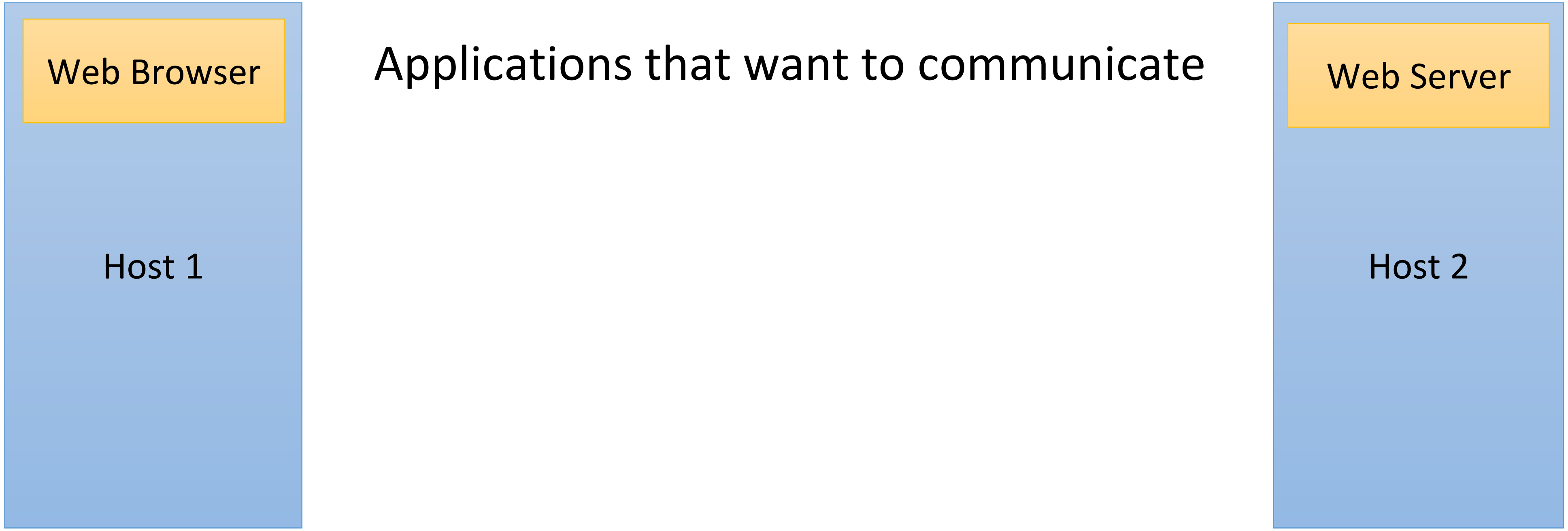
A common language (protocol)

A network interface

Transmission media to physically connect them

Basic Network Components

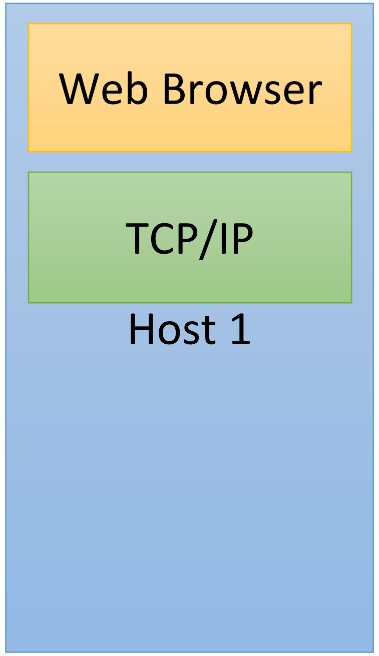
Let’s look again with examples:



Applications that want to communicate

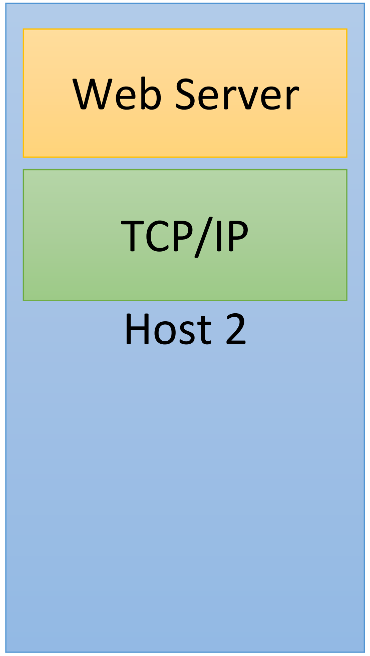
Basic Network Components

Let’s look again with examples:



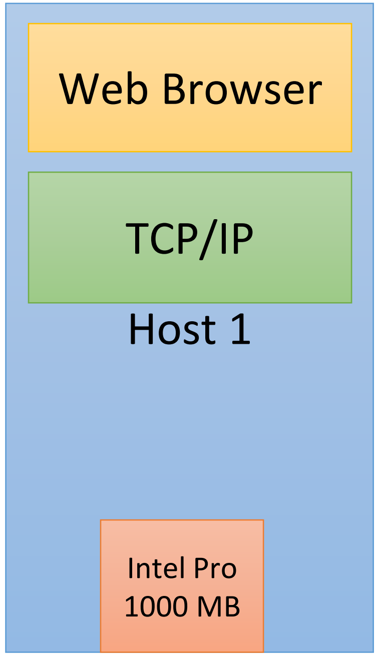
Applications that want to communicate

A common language (protocol)



Basic Network Components

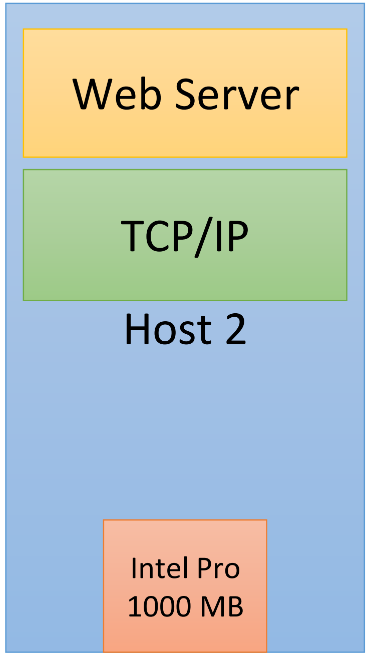
Let’s look again with examples:



Applications that want to communicate

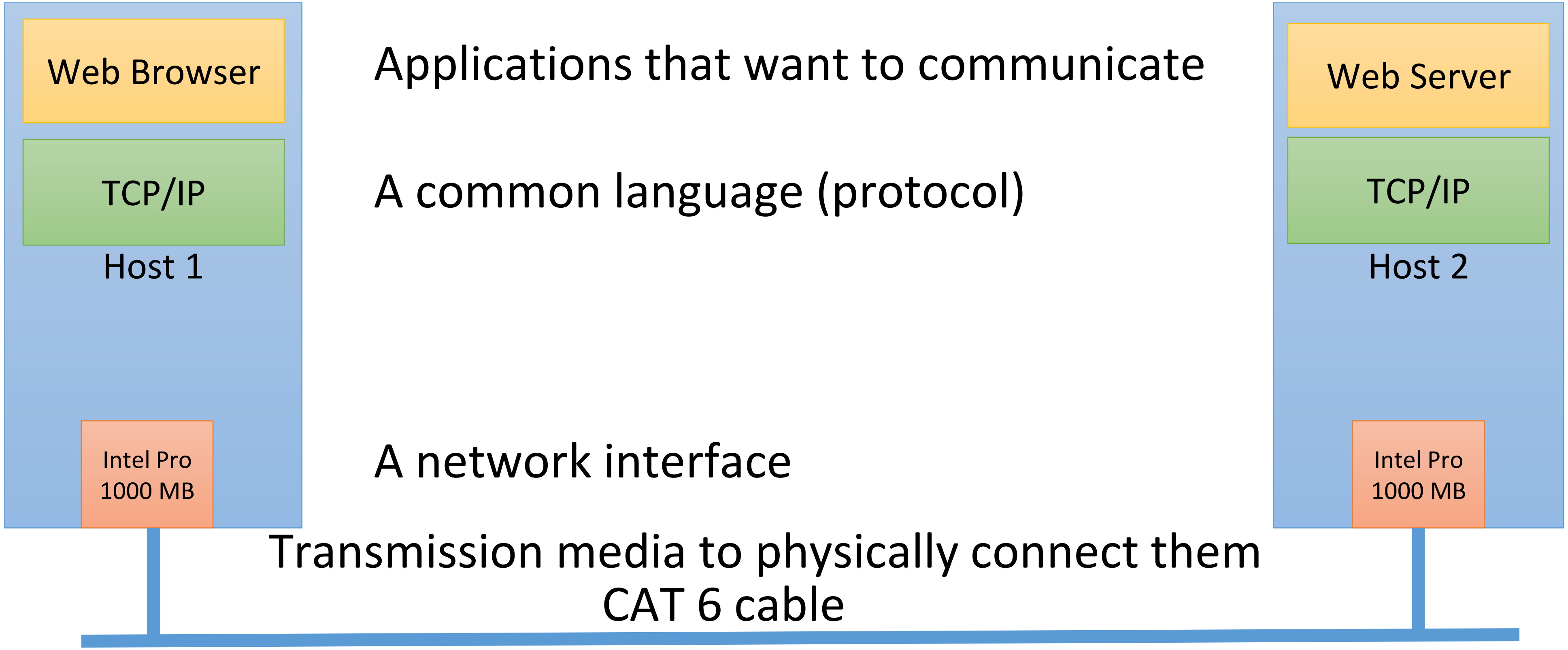
A common language (protocol)

A network interface



Basic Network Components

Let's look again with examples:



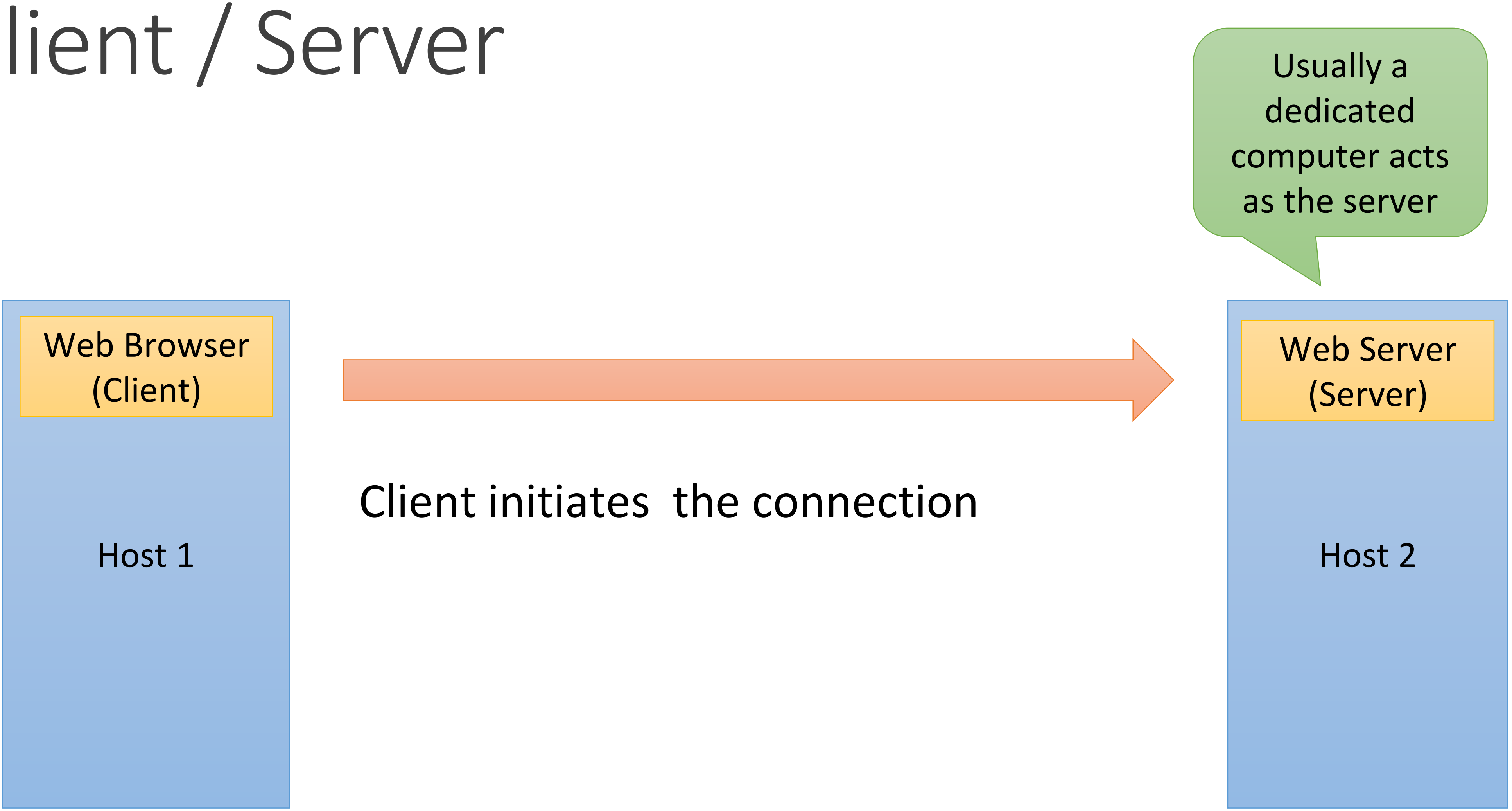
Applications that want to communicate

A common language (protocol)

A network interface

Transmission media to physically connect them
CAT 6 cable

Client / Server



Usually a dedicated computer acts as the server

Web Browser (Client)

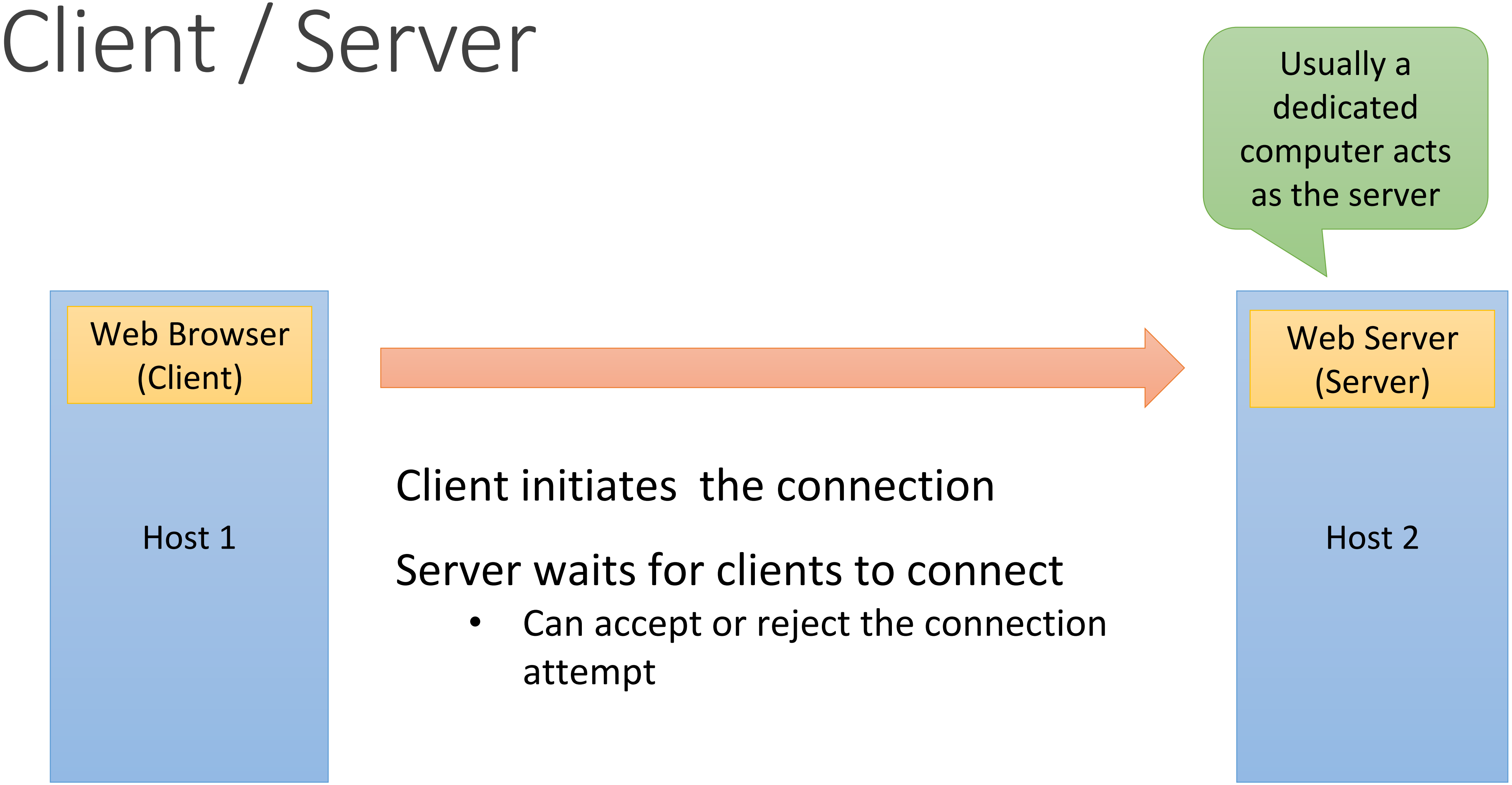
Host 1

Client initiates the connection

Web Server (Server)

Host 2

Client / Server

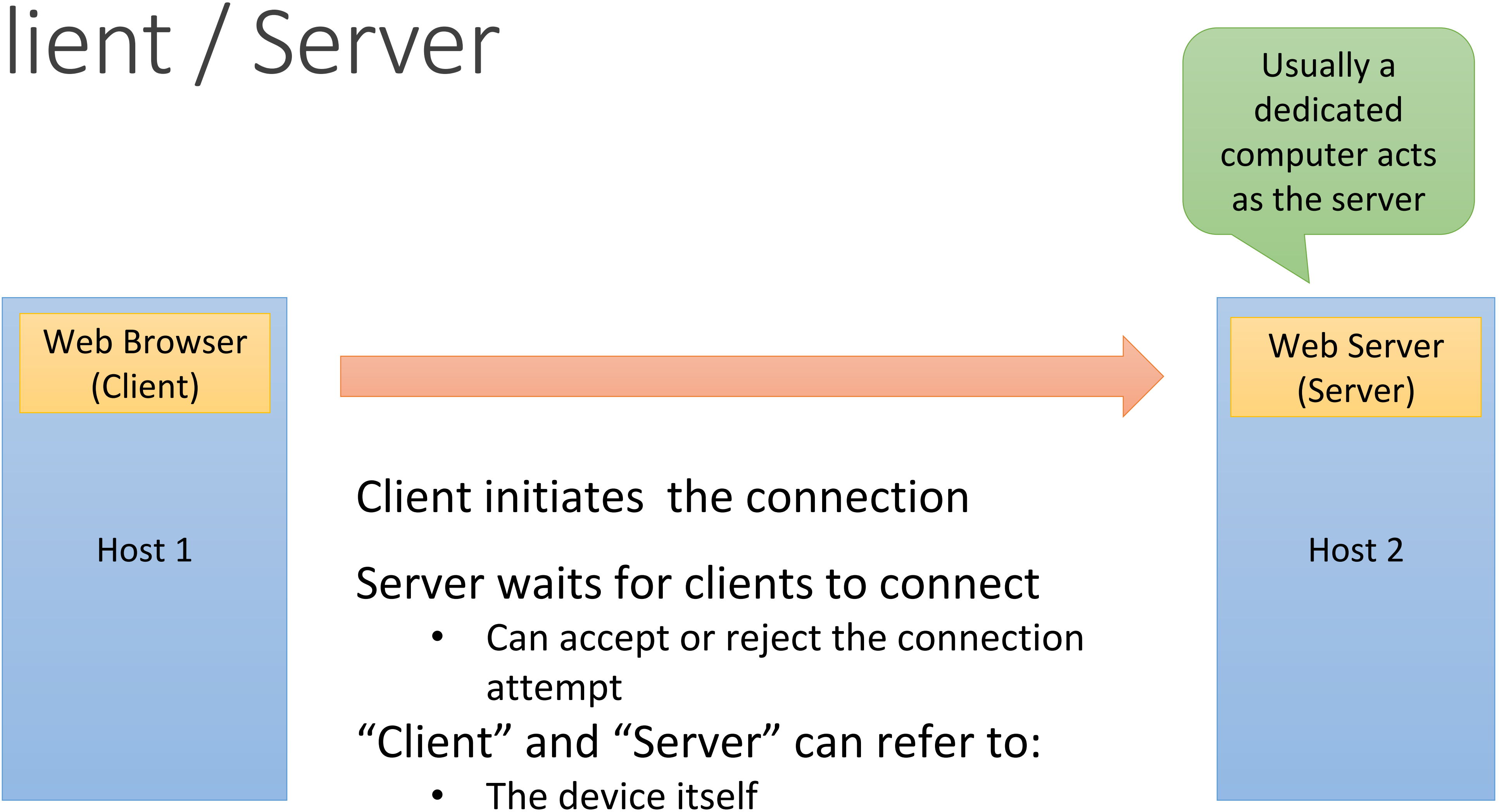


Client initiates the connection

Server waits for clients to connect

- Can accept or reject the connection attempt

Client / Server



Client initiates the connection

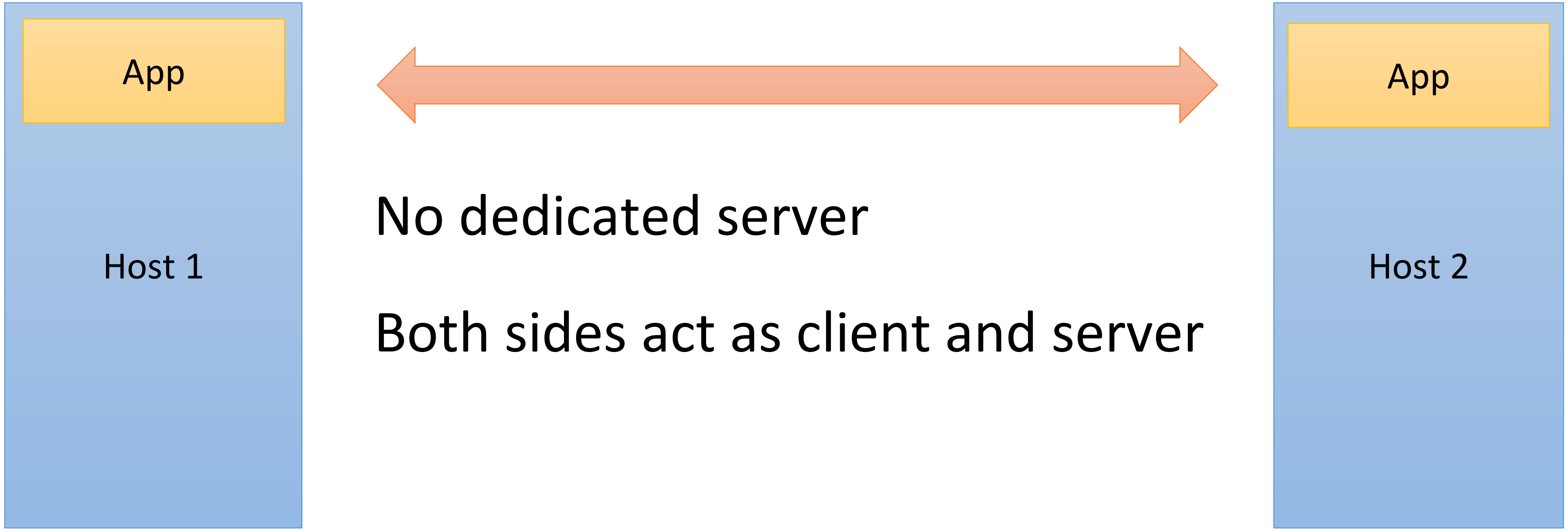
Server waits for clients to connect

- Can accept or reject the connection attempt

“Client” and “Server” can refer to:

- The device itself
- A process on the device

Peer-to-Peer



No dedicated server

Both sides act as client and server

Common Terminology

What is an IP Address?

A number that identifies a node on the network

Can be changed

- User configures a different address in network settings
- Device automatically obtains a new address when connected to a different network

A device can have more than one IP address

- One per interface
- Alternate IP addresses on the same interface

Each IP address must be unique on the network so there is no conflict

Analogous to a phone number

Examples:

IPv4 - 192.168.1.10

IPv6 - 2601:140:8780:43f0:2d1e:9ebb:92f0:d6e9

What is a MAC Address?

The physical address of the network interface

- Also known as the “Burned In Address” (BIA)
- Does not change

Assigned by the NIC vendor

One per interface

Analogous to a cell phone MEID or IMEI number, or a device serial number

Examples: BC-85-56-F3-13-02, BC:85:56:F3:13:02, BC85.56F3.1302

What are Source and Destination?

Source is the node that is transmitting/sending

Destination is the intended recipient of the transmission

A Client and Server take turns transmitting to each other

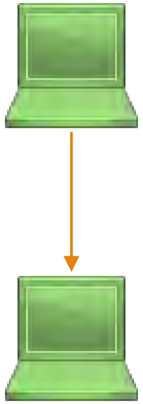
- Thus they alternate between being source and destination

What is a Unicast, Multicast, Broadcast?

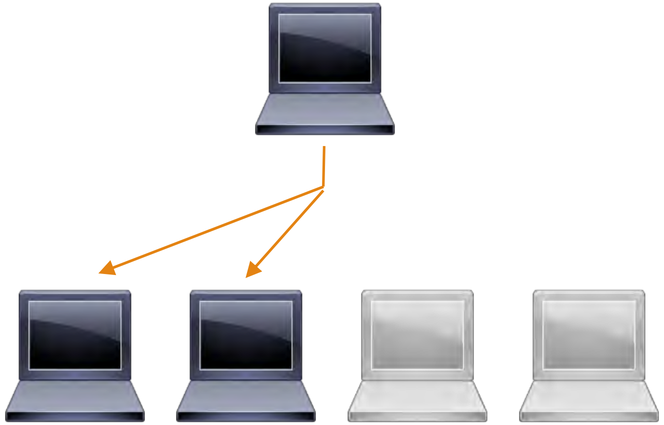
A node transmits a packet on the network

Depending on the destination address, one or more nodes will receive the packet

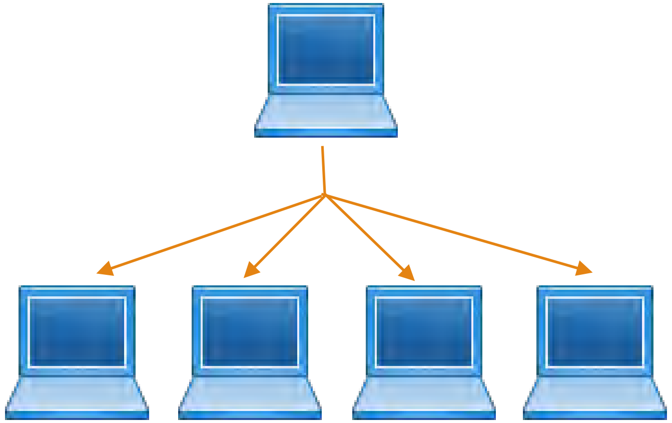
Unicast
One to one



Multicast
One to Some



Broadcast
One to All



What is a Protocol?

Set of rules or “language” for communication

Can exist at any level/layer of networking

A host will use several protocols to make a connection on the network

What is a Port?

A number that represents an application (process) on the network

Assigned by the operating system

Every process that accesses the network has its own unique port number on that device

What is a Socket?

A socket is a port that is in use

It is a combination of protocol, IP address, and port

This combination uniquely identifies the connection on the network

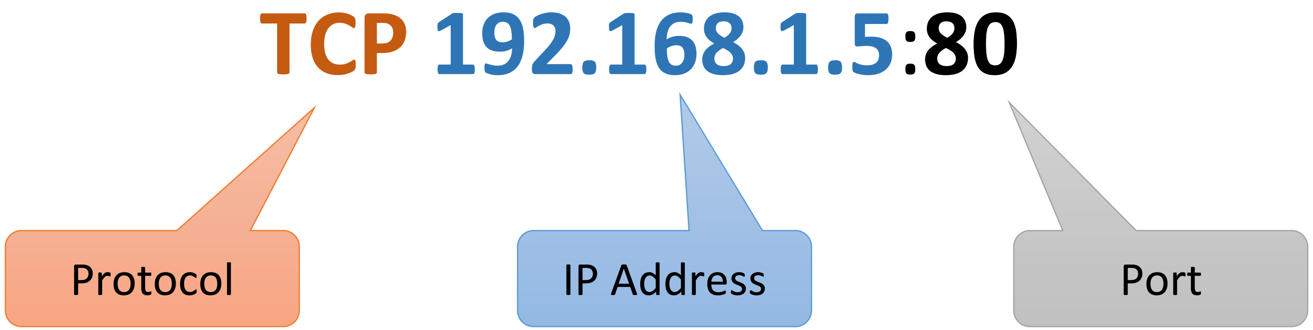
What is a Socket?

A socket is a port that is in use

It is a combination of protocol, IP address, and port

This combination uniquely identifies the connection on the network

Example:



TCP 192.168.1.5:80

Protocol

IP Address

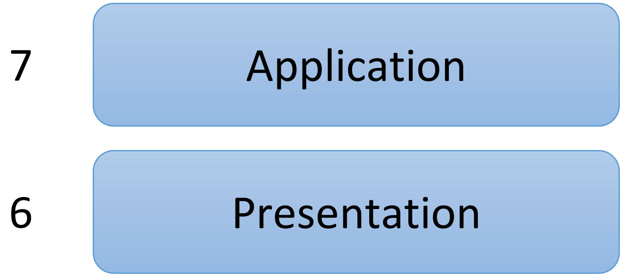
Port

OSI Model

OSI Model

7 Application

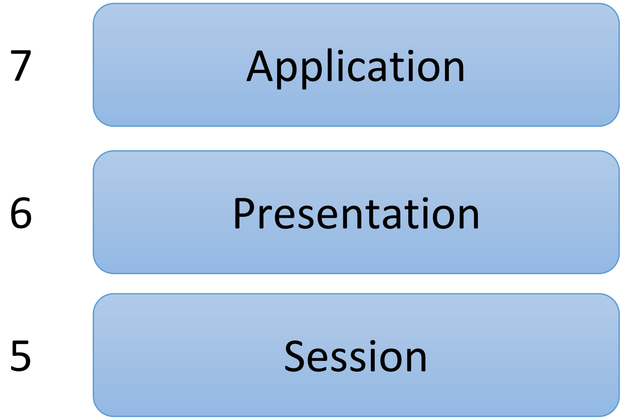
OSI Model



7 Application

6 Presentation

OSI Model

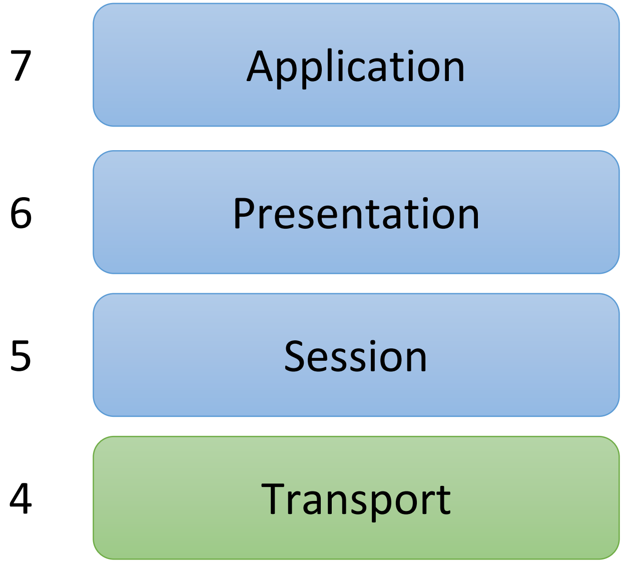


7 Application

6 Presentation

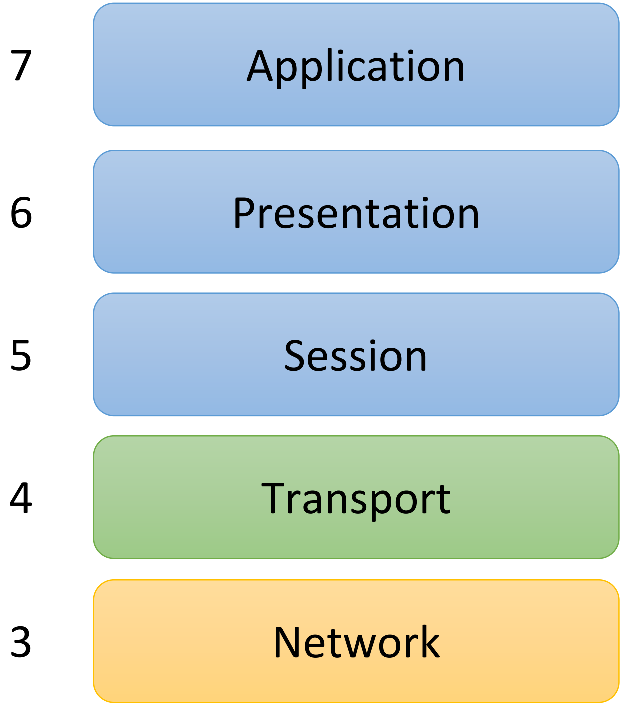
5 Session

OSI Model



7	Application
6	Presentation
5	Session
4	Transport

OSI Model



7 Application

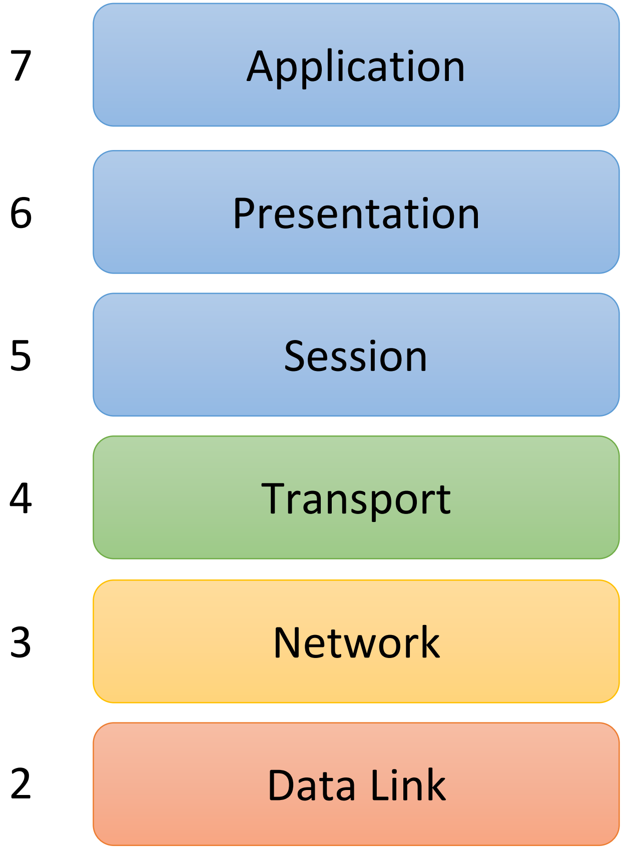
6 Presentation

5 Session

4 Transport

3 Network

OSI Model



7 Application

6 Presentation

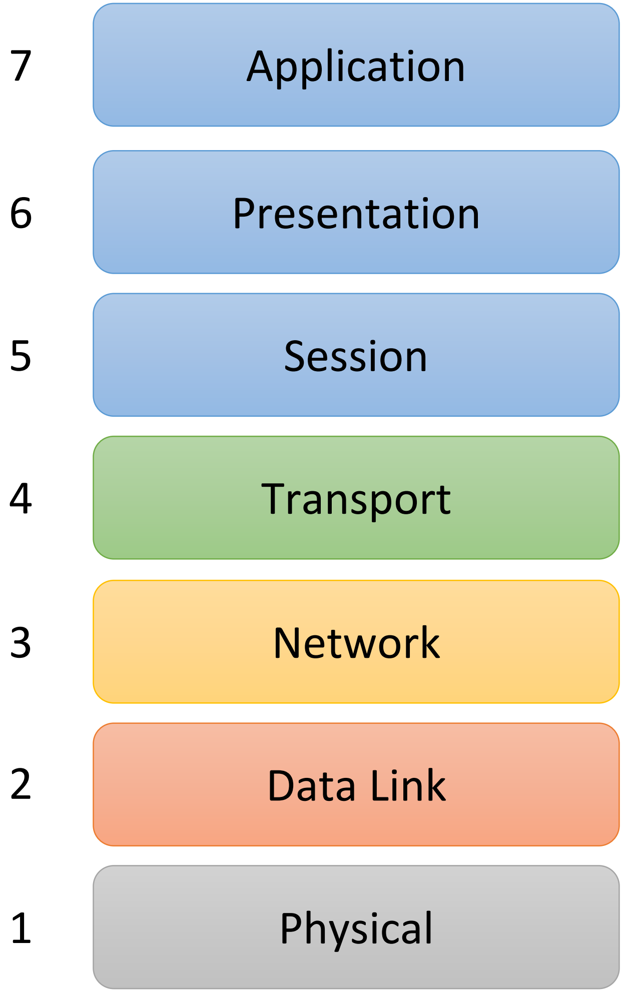
5 Session

4 Transport

3 Network

2 Data Link

OSI Model



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

Protocol Data Unit (PDU)

A specific block of information transferred over a network

This term is used in reference to the OSI model, describing the data at each layer:

- Application = data
- Presentation = data
- Session = data
- Transport = segment (TCP), datagram (UDP)
- Network = packet
- Data Link = frame
- Physical = bit

Layer 7 – Application Layer

"Customer service counter" that applications use to request network services

User can typically interact at this layer

Applications connect by speaking a language (protocol)

Common Layer 7 protocols include:

- SMTP, POP3, IMAP4, HTTP, HTTPS, RDP, DNS, DHCP, SMB, NFS, FTP, TFTP, Telnet, SSH, SIP, NTP, SNMP, LDAP

Firewalls, proxies

At this layer, data is called "data"

Layer 6 – Presentation Layer

Both sides agree on a common data format

User may or may not be able to interact with this layer

- Might be prompted to install a browser plugin to watch a video

At this layer, data is stilled called “data”

Common formats include:

- Multimedia formats – JPG, PNG, GIF, MP3, MP4, MKV, MOV, WAV, PDF…
- Encryption algorithm and bit size – DES, AES, MD5, SHA-1, 160 bit, 128 bit…
- Compression – H.264, H.263, MPEG-4, MPEG-2, AAC,
- Character sets – ASCII, Unicode, EBCDIC

Firewalls

Layer 5 – Session Layer

Keeps separate conversations separate

It is here that a host has the first concept of communicating with another host

Usually done by assigning ports (source and destination) to a conversation

Can also be NetBIOS named pipes or Unix sockets

Firewalls, packet filtering routers, multi-layer switches

SOCKS proxies

At this layer, data is stilled called "data"

Layer 4 – Transport Layer

Pivotal layer – abstracts the mechanics of the network from the higher layers

Starts, manages, and tears down the session

First layer to encapsulate the data payload with a header

TCP, UDP

Firewalls, packet filtering routers, multi-layer switches

Layer 4 – Transport Layer (cont’d)

TCP:

- Breaks up data into manageable pieces for transmission
- Adds sequence numbers to each segment for reassembly at other end
- Embeds the source and destination ports into its header
- Establishes the session with a handshake
- Provides error correction and flow control during session
- Tears down session with a handshake

Data is called a “Segment”

UDP:

- Embeds the source and destination ports into its header
- Depends on the application for session establishment, management, payload length, error correction, flow control, and tear down

Data is called a “Datagram”

Layer 3 – Network Layer

Encapsulates Layer 4 into a packet

Adds a logical address (usually IP address)

diagnostic like ping

Chooses the best route

multi casting

IP, ICMP, IGMP

Routers, Firewalls, multi-layer switches

Data at this layer is called a “packet”

Layer 2 – Data Link Layer

also a frame

Adds a physical source and destination address

Encapsulates Layer 3 packet into a frame

- Adds both a header and trailer

Formats the frame to be suitable for transmission media

Checks incoming frames for errors

- Discards frames that do not pass a simple cyclical redundancy check (CRC)
- Depends on Layer 4 to retransmit discarded data

Has two sub layers:

- Logical Link Control (LLC) – describes the Layer 3 payload
- Media Access Control (MAC) – adds the physical addresses

ARP, Ethernet, Token Ring, PPP, HDLC, Frame Relay

Switches, bridges

Data at this layer is called a “frame”

Layer 1 – Physical Layer

Data at this layer is called “bits”

Actual transmission of the frame as 1’s and 0’s

All electrical and mechanical aspects of the transmission

Includes connectors, wiring types, wireless technologies, baseband, broadband, modulation, speed, bandwidth, clock rate, voltages, frequencies, power levels…

Hubs, repeaters, patch panels, network interface cards, RJ-45, STP, UTP, thicknet/thinnet coax, CAT 3/5/5e/6/6a/7, fiber optic, 2.4/5 GHz, Wi-Fi channels, ZigBee, Z-Wave, infrared and other wireless technologies

Data Encapsulation / Decapsulation

Encapsulation

Layers 4, 3, 2 on the sender add a header

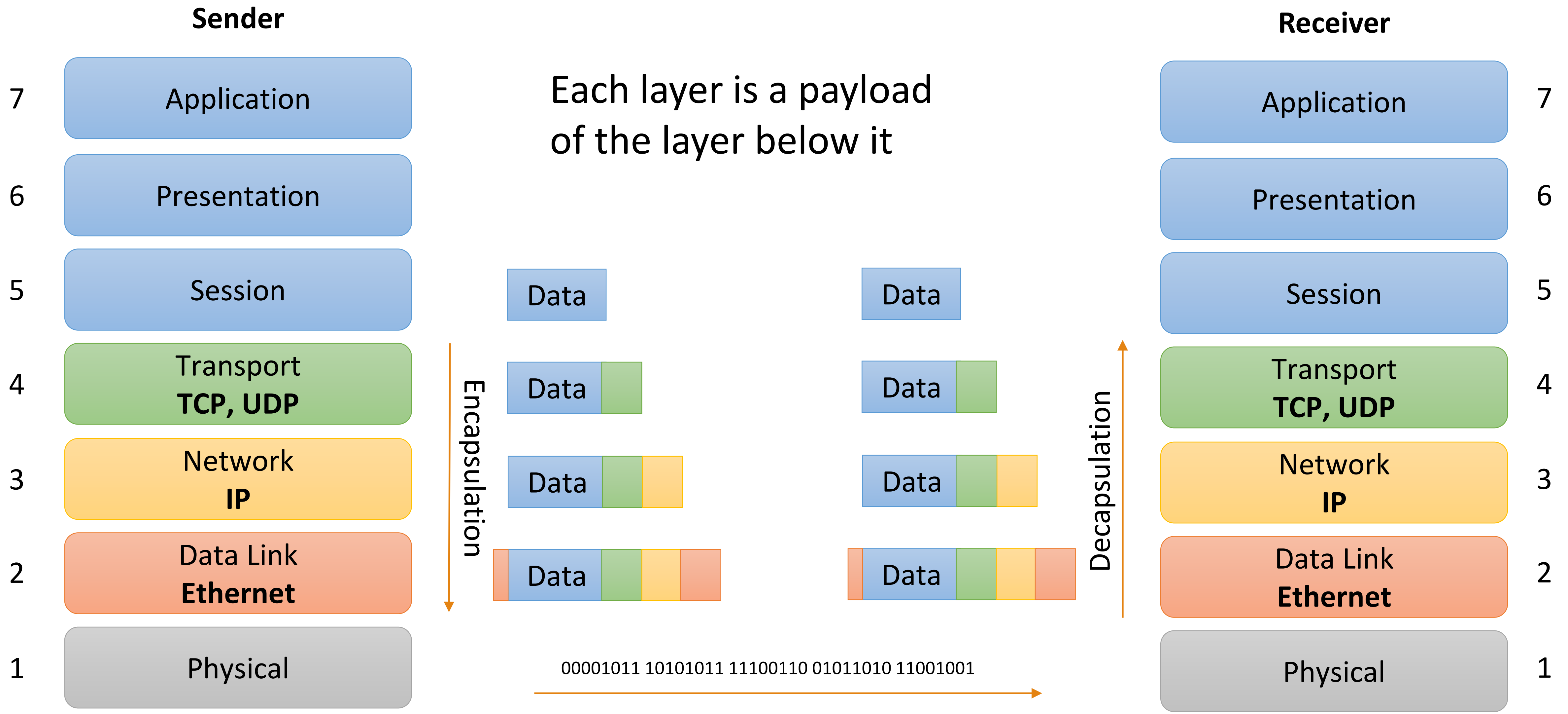
- Description of the data and/or protocol
- Layer 2 also adds a trailer

Decapsulation:

Corresponding layers on the receiver remove the header

- Refer to the information in the header/trailer
- Pass the PDU up to the next layer

OSI Encapsulation/Decapsulation



Each layer is a payload of the layer below it

OSI Model Summary

7	Application	Customer service counter for app to request network services	HTTP, HTTPS, FTP, TFTP, SMTP, POP3, IMAP4, SMB, NFS, RDP, LDAP, DNS, DHCP, SSH, Telnet, SNMP …
6	Presentation	Both sides agree on common data format	All encryption, multimedia formats, character sets, encryption
5	Session	Keep separate conversations separate	Ports, named pipes, NetBIOS, RPC
4	Transport	Establish, manage, tear down a connection	TCP, UDP
3	Network	Add logical address, choose the best route	IP, ICMP, IGMP
2	Data Link	Format the data for transmission, add physical address	LAN and WAN protocols, ARP
1	Physical	Actually transmit packet as 1's and 0's	All physical and electrical characteristics of connectors and transmission media

DoD Model

What is the DoD Model?

Developed by the US Department of Defense

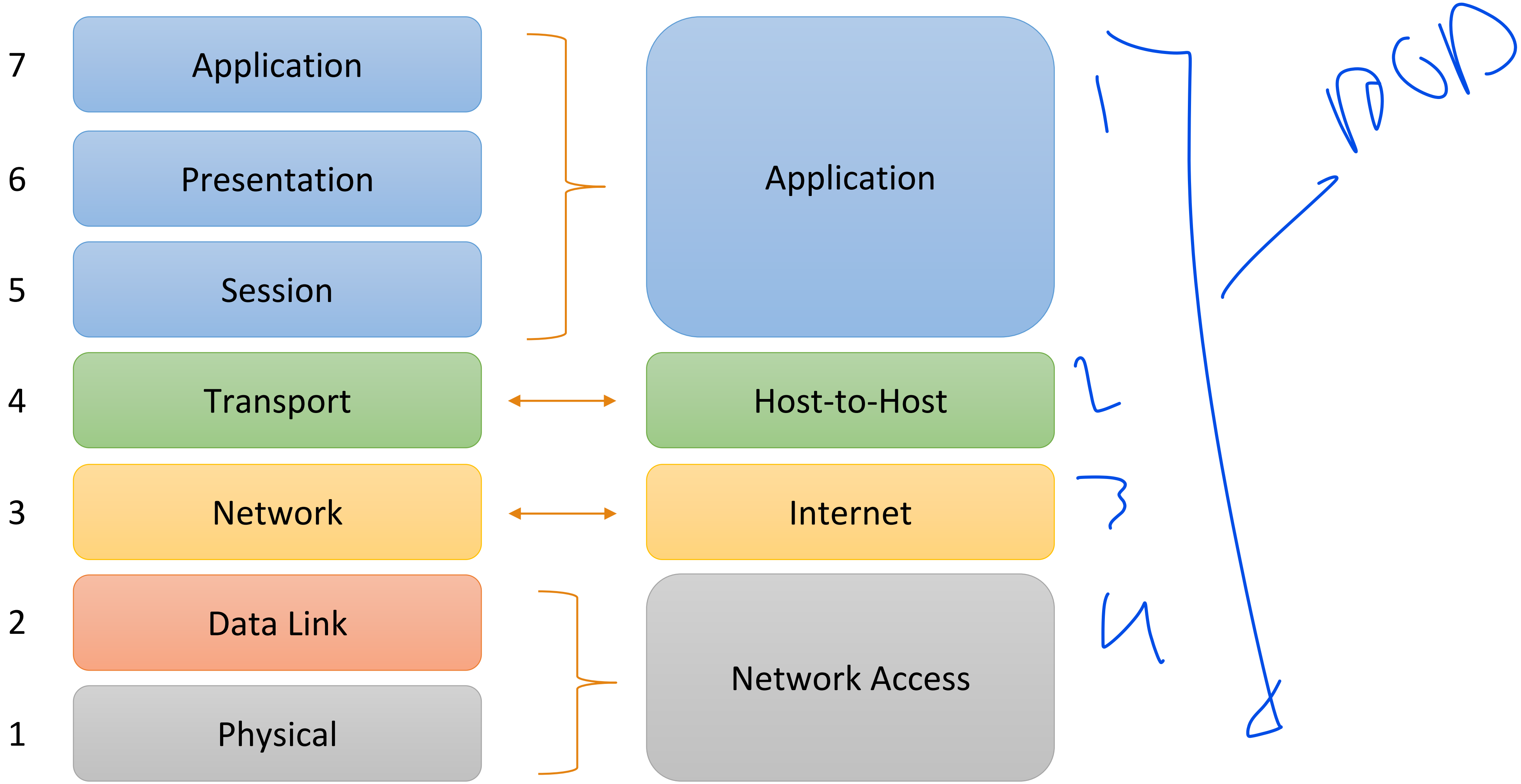
4 layer model

Its layers map to the OSI model

Sometimes referred to as the TCP/IP Model

- Specifically uses the TCP/IP suite

OSI – DoD Layer Mapping



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

Application

Host-to-Host

Internet

Network Access

TCP/IP Suite

Transmission Control Protocol / Internet Protocol

Protocols of the DoD Model

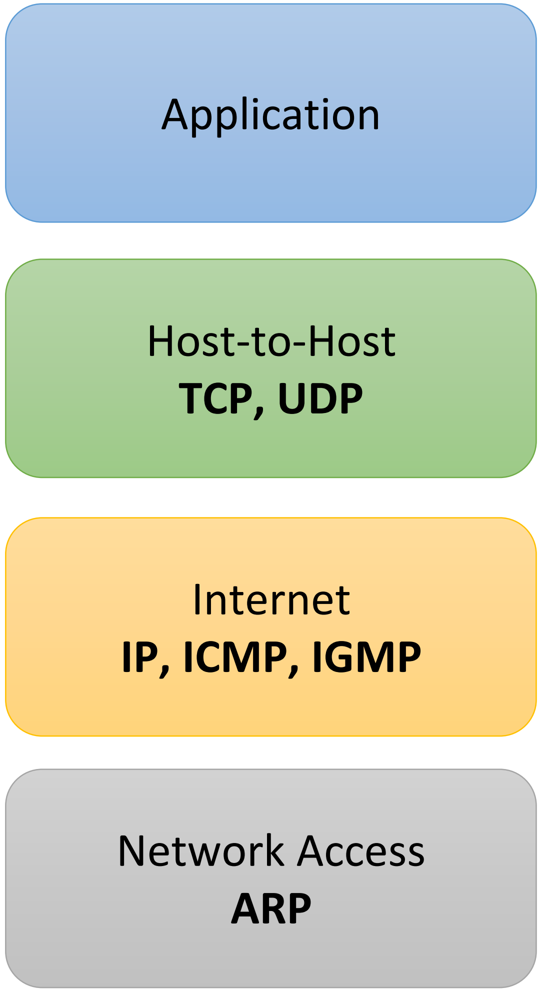
6 core protocols:

- TCP, UDP, IP, ICMP, IGMP, ARP

All but ARP have an IANA assigned protocol number (protocol ID)

Number

Many auxiliary protocols also exist at the various layers



Application

- Data Payload

Host-to-Host **TCP, UDP**

- Session Establishment / Management
- Sequencing

Internet **IP, ICMP, IGMP**

- Logical Addressing
- Routing

Network Access **ARP**

- Physical Addressing
- Framing/CRC/MTU
- Actual transmission

What is a Connection-Oriented Protocol?

Attempts to ensure reliability and completeness of transmission

Uses a handshake to create and end a session
- Like sending registered mail

Keeps track of the conversation

Ensures that the other side is responding
- Is the other side acknowledging received packets?
- Resends packets that are not acknowledged
- Acknowledgements and resends add overhead and slow the conversation

Responds to requests from the other side
- Receiver informs sender how many packets it can receive at a time
- Sender speeds up or slows down the transmission rate accordingly

Used when reliability is more important than performance

What is a Connectionless Protocol?

Makes no attempt to ensure completeness of the transmission

No handshake

- Does not even know or care if the recipient is online or offline
- Like sending post cards

Expects higher level protocols or the app to request resends if some of the data did not arrive

- Assumes lost packets are not important or will be re-transmitted

Used when performance is more important than reliability

Connection-Oriented vs Connectionless

Connection-Oriented	Connectionless
TCP	UDP, IP, ICMP, IGMP, ARP
Handshake to set up / tear down session	No handshake
Flow control / error correction	No flow control / no error correction
"Reliable" → Not to 100%	"Unreliable" or "best effort" No guarantee
Focus on receiving all the data	Focus on speed/performance
Used for transferring files: - web pages - emails - file transfers - video-on-demand - remote control	- Used for communications that are time sensitive, and/or can tolerate some loss: - Realtime voice and video - SNMP, DNS, DHCP

TCP, UDP, IP

Transmission Control Protocol (TCP)

Host-to-host Layer (Layer 4) protocol

Payload of IP

Embeds source and destination ports in its header

Provides reliable, connection-oriented communication over IP networks between two endpoints

Connection oriented

- Attempts to guarantee delivery

Transmission Control Protocol (TCP)(cont'd)

Data is broken into smaller segments

- Identified by sequence #

Uses a receive window (sliding window)

- Tells the sender how big the receiver's buffer is from segment to segment

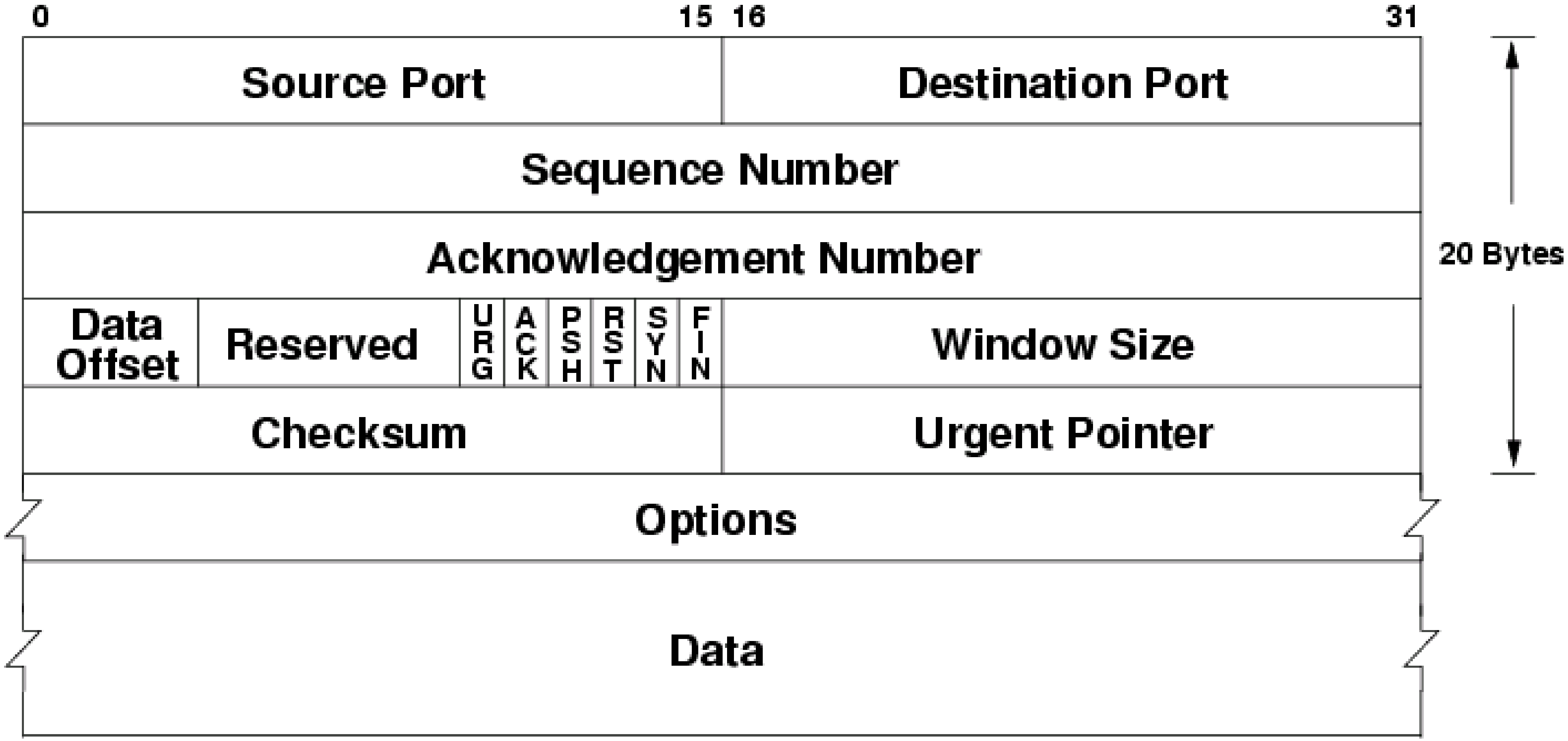
Session established by three-way handshake (SYN – SYN/ACK – ACK)

this is the three way hand shake

Session closed by a four-way handshake (FIN-ACK-FIN-ACK)

Protocol ID 6

TCP Header



0 15 16 31

Source Port | Destination Port

Sequence Number

Acknowledgement Number

Data Offset | Reserved | URG | ACK | PSH | RST | SYN | FIN | Window Size

Checksum | Urgent Pointer

Options

Data

20 Bytes

TCP Flags

Indicate the purpose of the TCP segment

Every TCP segment will have at least one flag raised

	Flag	Description
urgent	URG	Tells receiver to prioritize this data
	ACK	Acknowledge All TCP segments (except very first and last will have an ACK)
push	PSH such as log in	Tells receiver to directly send this data to the application
	RST	Tells receiver that the sender has abruptly ended the conversation
	SYN	Used in 3-way handshake to start conversation
	FIN	Used in 4-way handshake to end conversation

User Datagram Protocol (UDP)

TCP’s “Little Brother”

Host-to-Host Layer (Layer 4) protocol

Connectionless (“unreliable” or “best effort”)

A payload of IP

Embeds source and destination ports in its header

No session establishment

User Datagram Protocol (UDP) (cont’d)

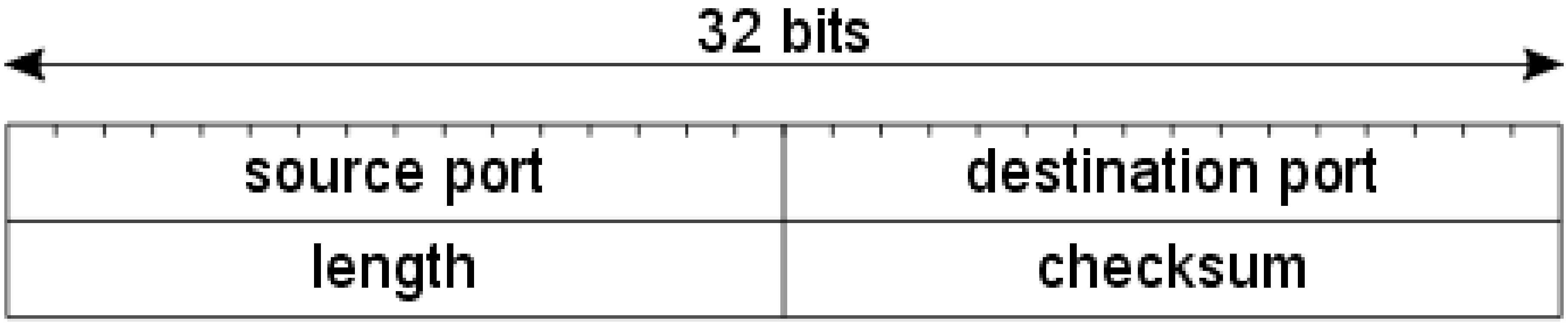
This protocol sends short packets of data, called datagrams

Ideal for network applications where latency is critical but loss is not:

- Gaming, real-time voice and video
- SNMP, DNS queries and DHCP
- Some applications (especially voice) use various techniques to make up for any loss

Protocol ID 17

UDP Header



32 bits

source port	destination port
length	checksum

Internet Protocol (IP)

Internet Layer (Layer 3) connectionless protocol

Can be a payload of nearly any link-layer protocol

Protocol ID 4

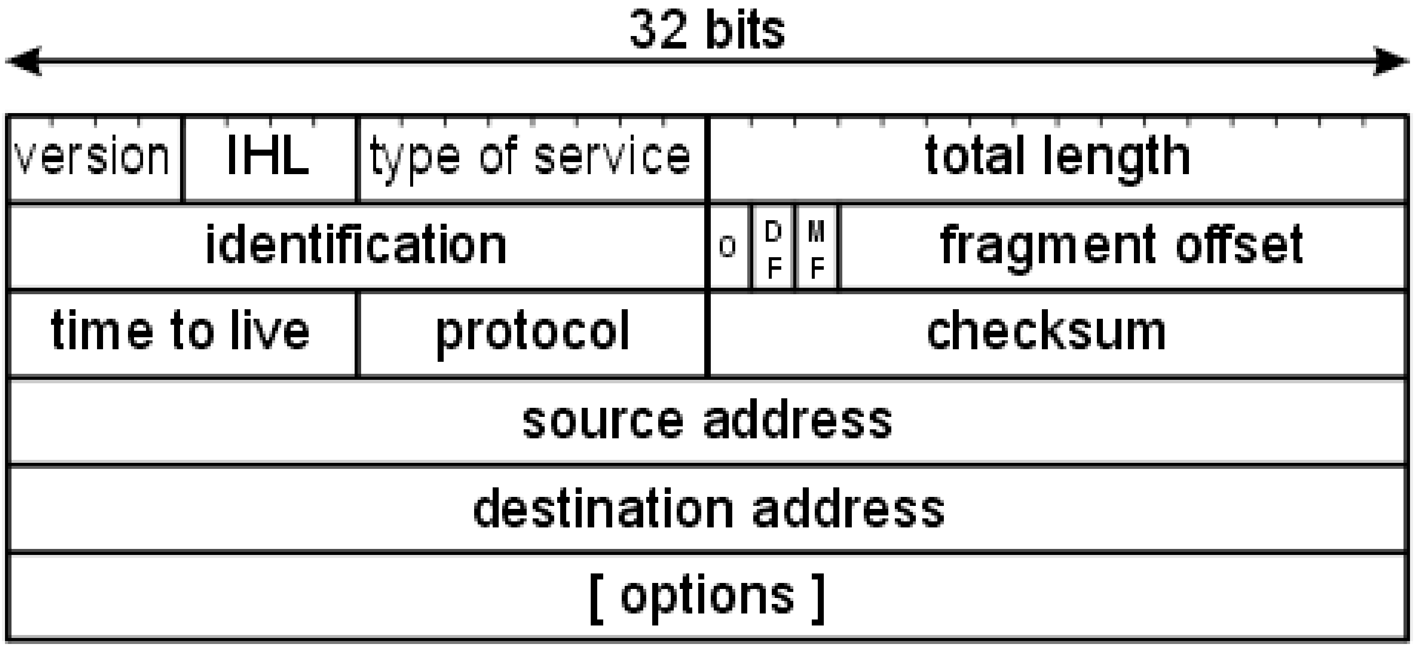
IPv4:

- Still most widely used version
- Uses 32-bit logical addressing to identify source and destination host
- Address examples: 10.0.0.207, 172.16.54.3, 207.45.168.4, 198.32.8.75

IPv6:

- Allows longer addressing and vast improvements over IPv4
- Steadily gaining in popularity and use
- Address examples: 2601:140:8780:43f0::4762, fe80::10:18ff:fe12:2001

IPv4 Header



32 bits

version | IHL | type of service | total length

identification | o | D F | M F | fragment offset

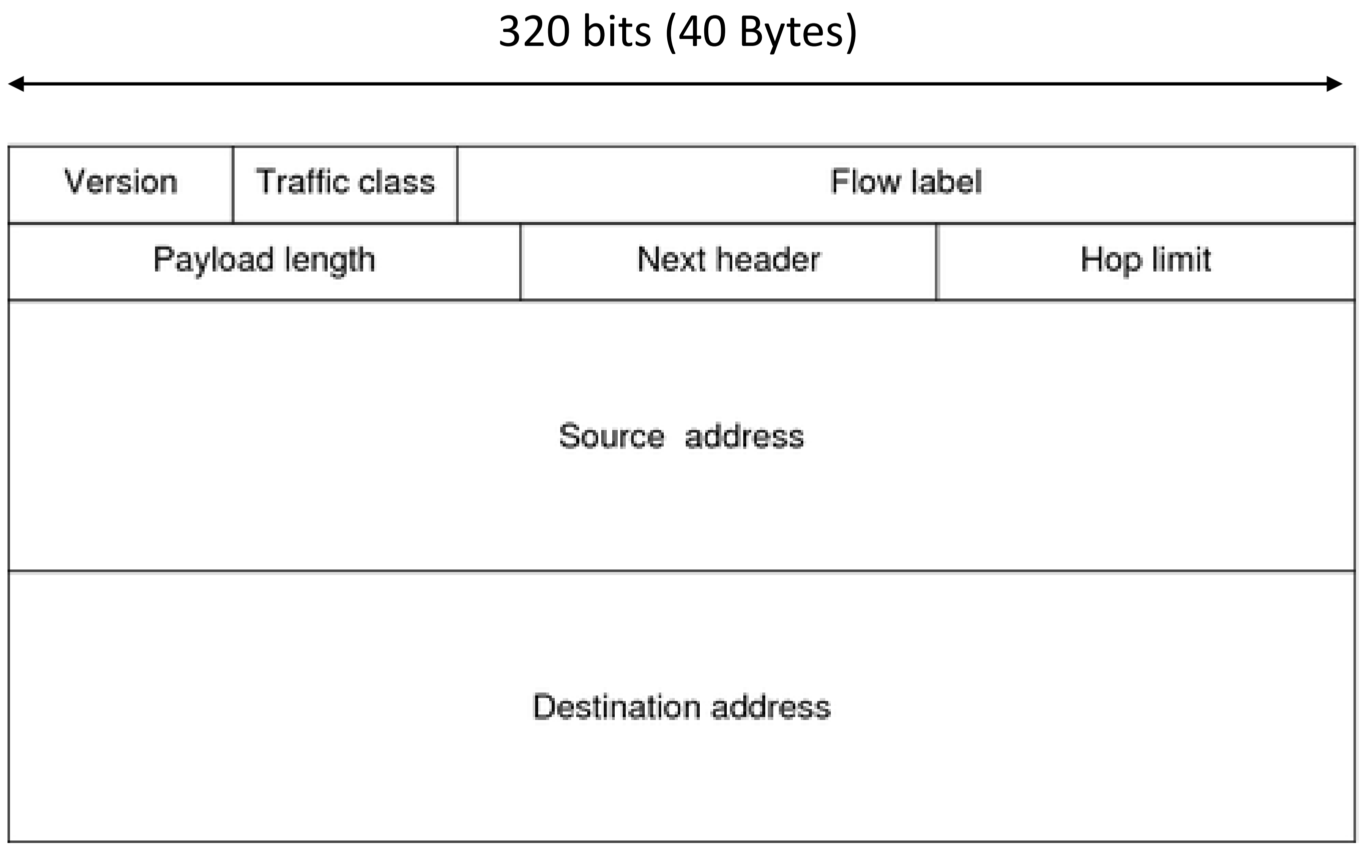
time to live | protocol | checksum

source address

destination address

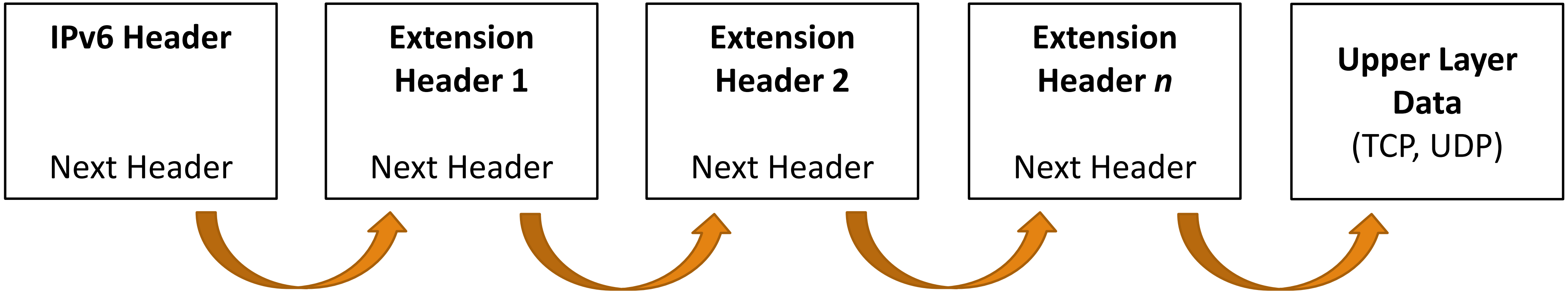
[options]

IPv6 Header



320 bits (40 Bytes)

IPv6 Header Extensions



IPv6 Header

Next Header

Extension Header 1

Next Header

Extension Header 2

Next Header

Extension Header *n*

Next Header

Upper Layer Data

(TCP, UDP)

ICMP, IGMP, ARP

Internet Control Message Protocol (ICMP)

An error-reporting protocol used by network devices (e.g. routers) to generate error messages and manage traffic flow

Layer 3 payload of IP

Any IP network device can send and receive ICMP messages

Used by PING application

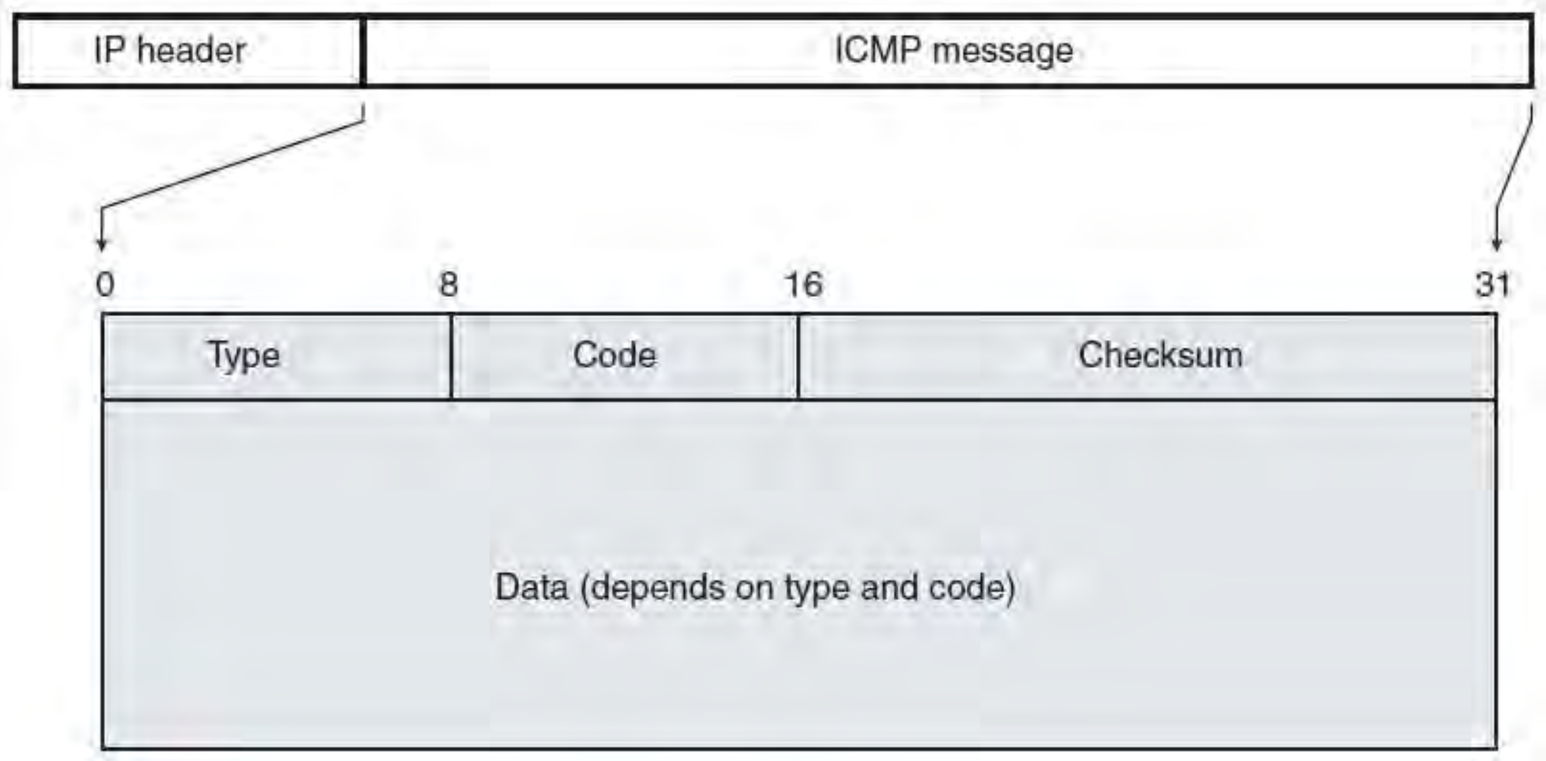
Protocol ID 1

ICMP Message Codes

ICMP uses different codes to identify the purpose of the message:

- Echo request
- Echo reply
- Destination unreachable
- Source quench
- Redirect
- Router solicitation
- Router advertisement
- Time exceeded

ICMP Message Format



Applications that Use ICMP

PING

- An application that uses ICMP to prove Layer 3 connectivity
- NOT a protocol – do not confuse with ICMP

Traceroute

- Stream of ICMP echo requests OR UDP datagrams with limited TTL
- Router that discards the expired packet and sends Expired in Transit message while identifying itself
- Microsoft traceroute application is called **tracert**

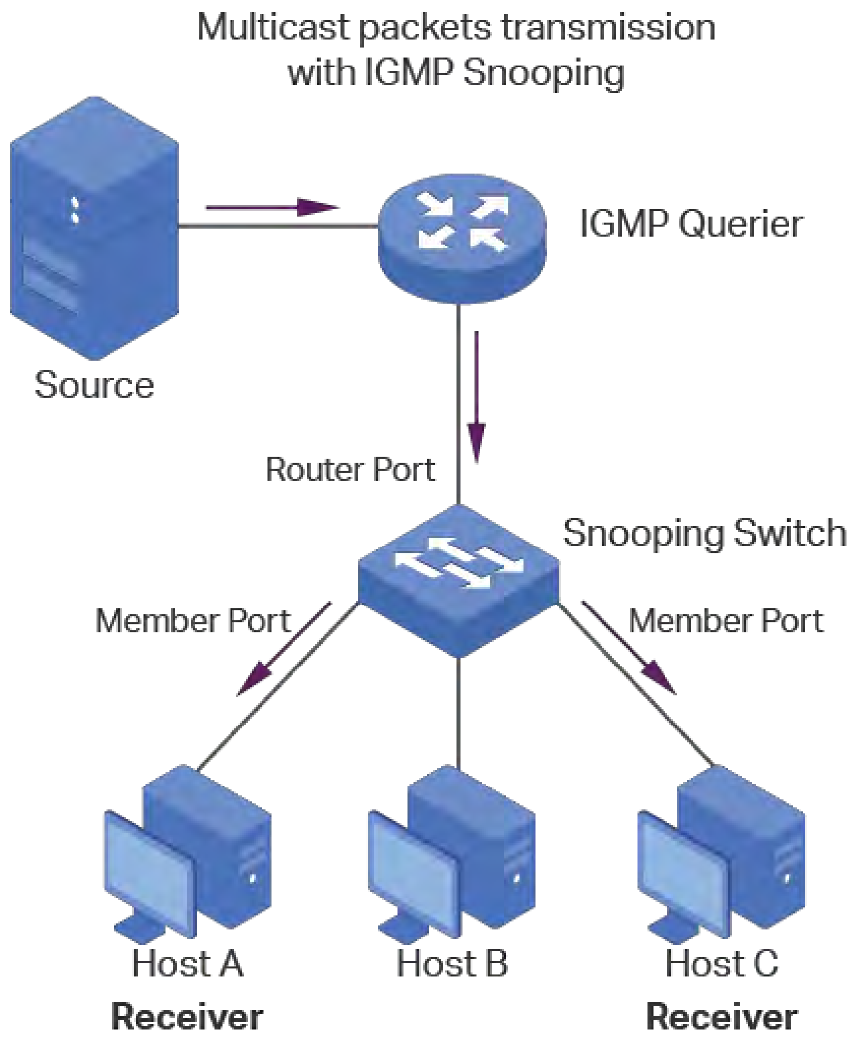
Internet Group Management Protocol (IGMP)

Used by hosts to notify routers that they are still interested in receiving multicasts from upstream server

- Routers do not forward multicasts by default
- Host must let upstream router know that it wants the multicast

Protocol ID 2

IGMP Operation

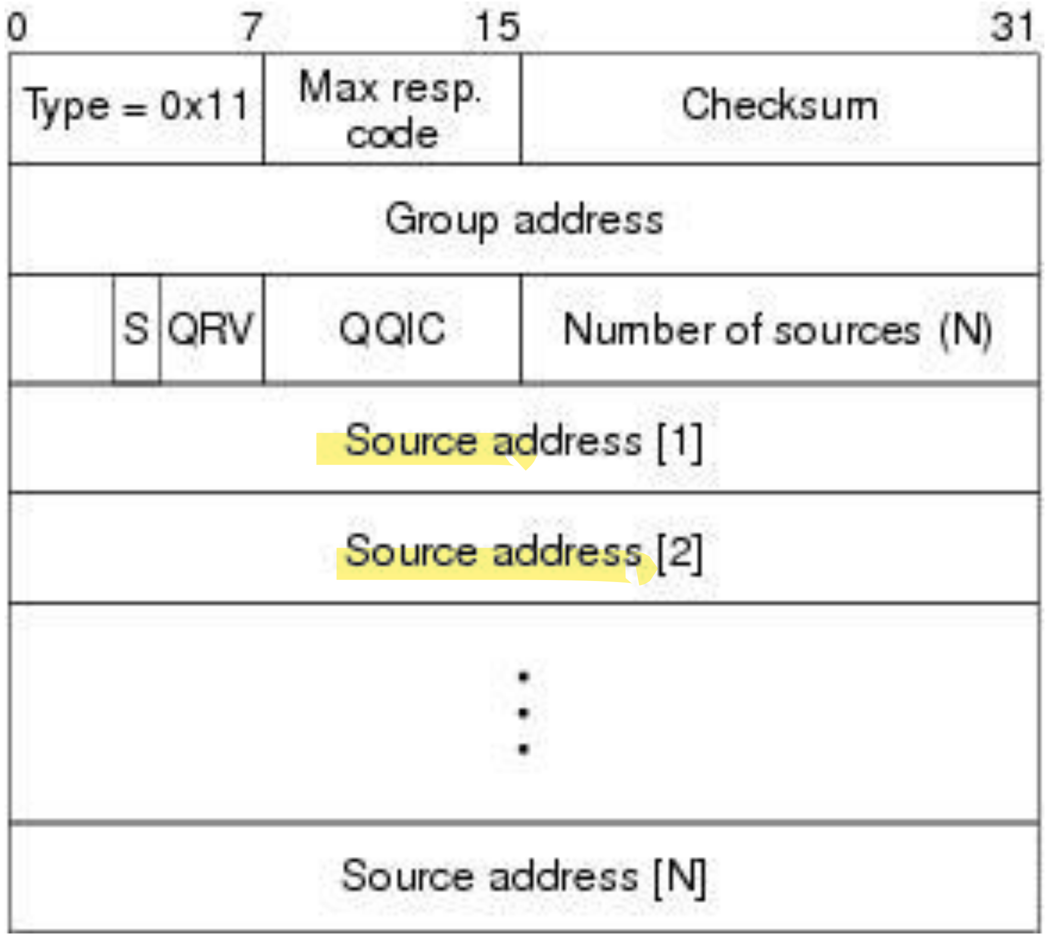


Router needs to know if downstream devices still want the transmission

Switch listens for IGMP requests from hosts – only forwards IGMP to hosts that request it

Hosts that want to receive the multicast send IGMP messages up to the router

IGMP Packet Format



0		7	15	31
Type = 0x11			Max resp. code	Checksum
Group address				
	S	QRV	QQIC	Number of sources (N)
Source address [1]				
Source address [2]				
⋮				
Source address [N]				

Address Resolution Protocol (ARP)

Network Access Layer (Layer 2) connectionless protocol

Used to map MAC addresses to IP addresses

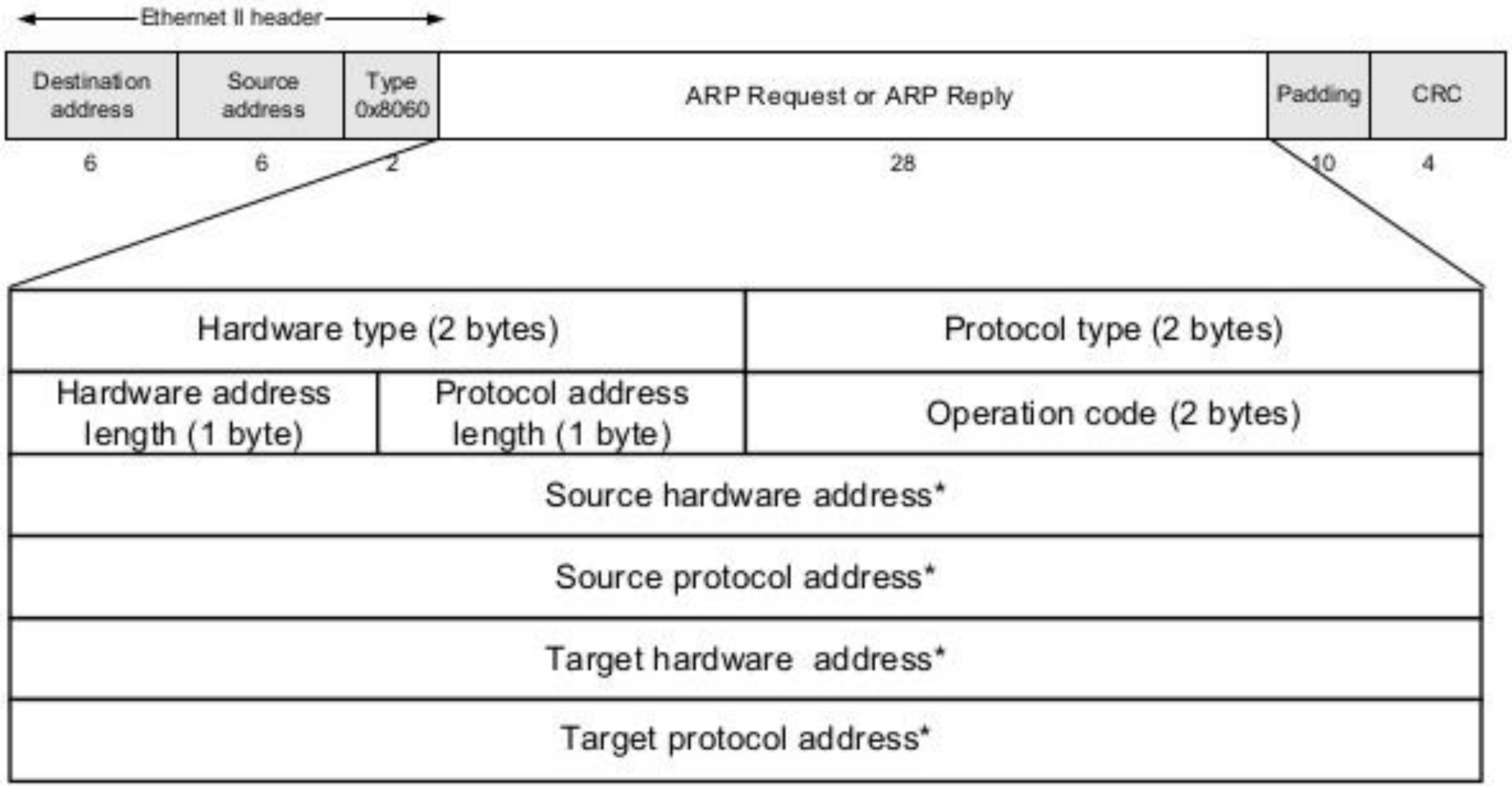
Sends Layer 2 broadcast (FFFFFFFFFFFF) querying all listening nodes to identify which one is using the specified IP address

Mappings are temporarily stored in the device’s ARP cache

Used in Ethernet and Wi-Fi networks

Does not have an assigned protocol number

ARP Message Format



Ethernet II header

Destination address	Source address	Type 0x8060	ARP Request or ARP Reply	Padding	CRC
6	6	2	28	10	4

Hardware type (2 bytes)		Protocol type (2 bytes)
Hardware address length (1 byte)	Protocol address length (1 byte)	Operation code (2 bytes)
Source hardware address*		
Source protocol address*		
Target hardware address*		
Target protocol address*		

Network Topologies

Network Topology

Describes the layout of a network

Determines how devices connect and communicate

Topologies are either physical or logical

- Physical – actual physical layout/physical connections between devices on a network
- Logical – how data moves from one device to another

Physical and logical topologies need not be the same

Point-to-Point

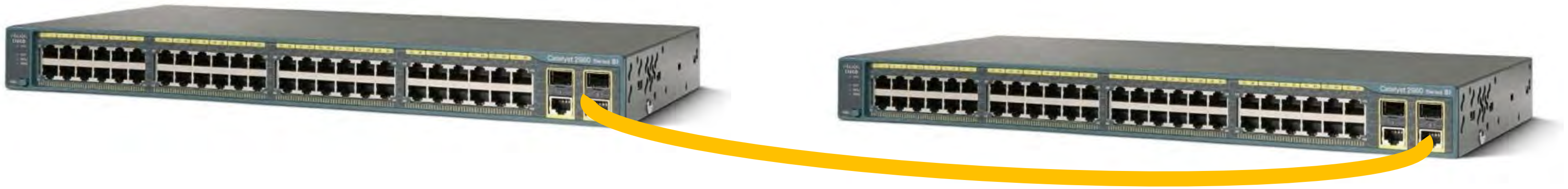
Only two nodes on a link

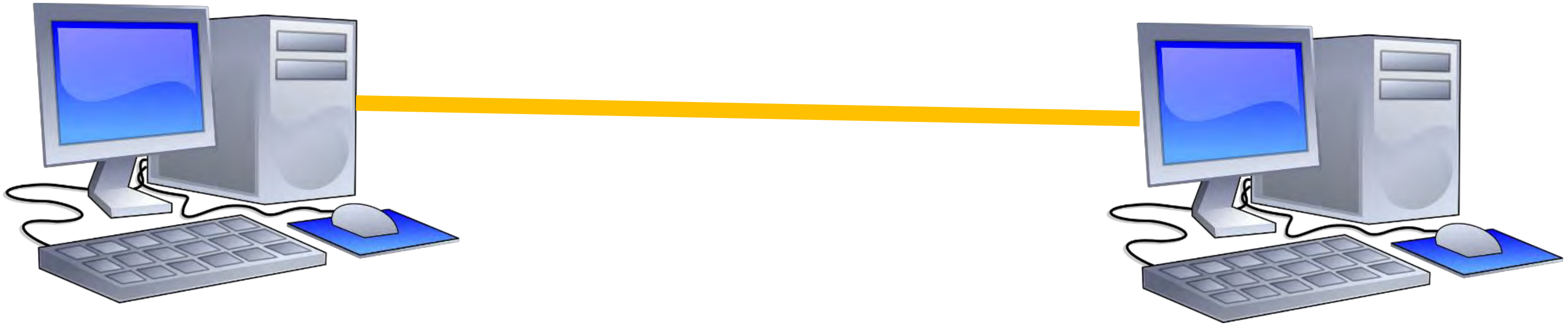
Examples:

- WAN link between two locations
- Line-of-sight wireless between two buildings
- Uplink/trunk link between two switches
- Two PCs connected by a crossover cable

ot is only intresterd in the end point as iys only connected to it

Point-to-Point Topology Examples





Bus

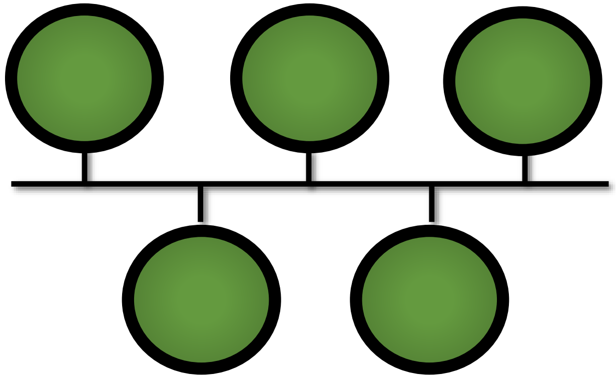
Comprised of a single cable that all devices tap into

Cable ends have to be specially terminated so signal does not reflect back onto bus

Original Ethernet networks used a bus topology

If the main cable breaks the network goes down

- It can be difficult to troubleshoot



Star

most coomonly used no w

Network devices are connected to a central device/node called a hub

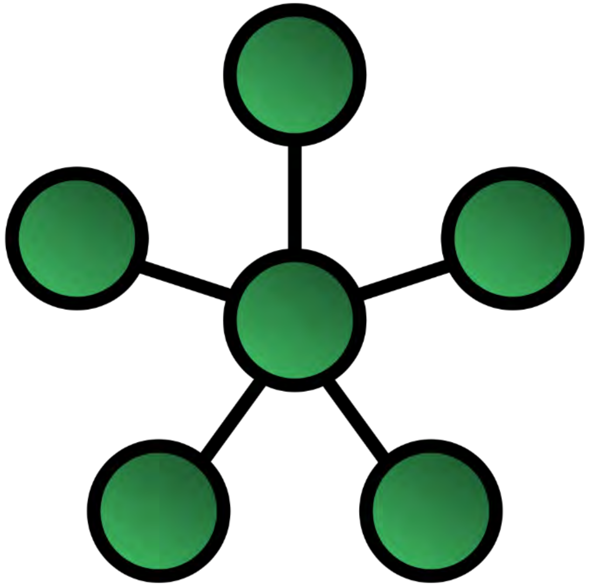
Nodes communicate across the network by passing data through the hub

Also known as:

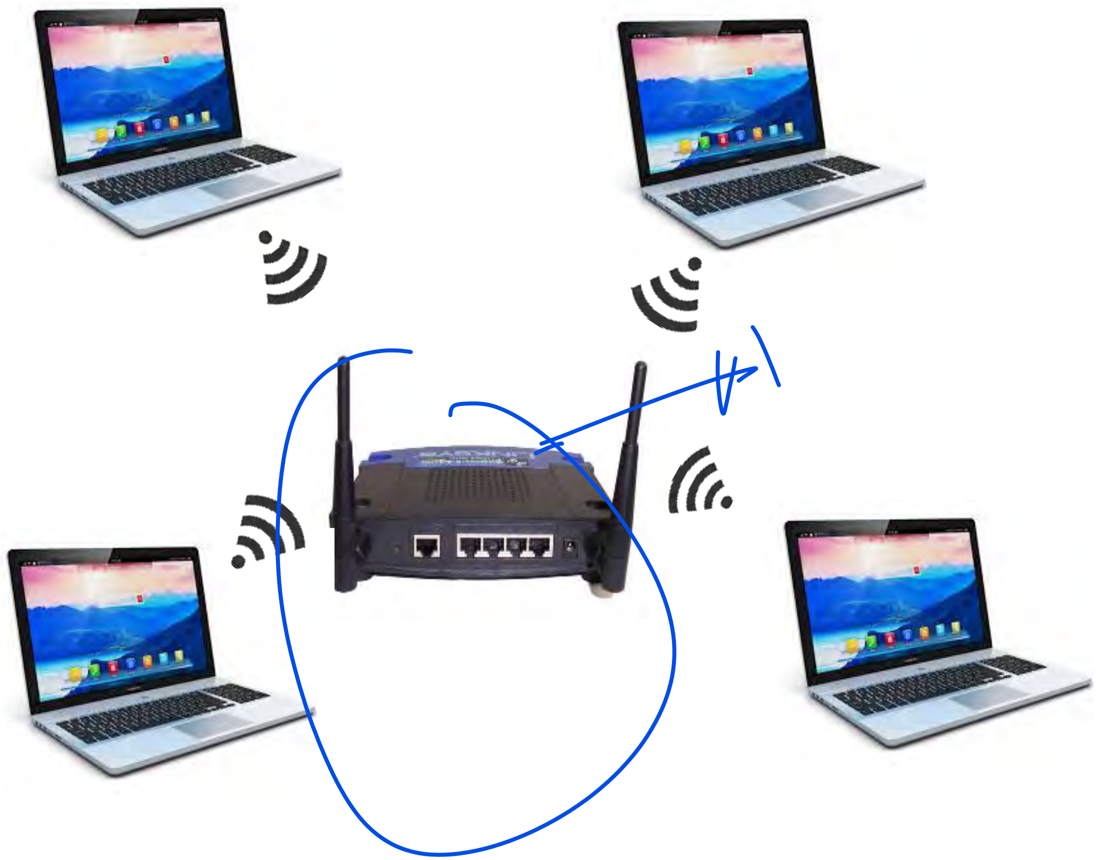
- Hub-and-Spoke
- Point-to-multipoint (WANs or wireless)

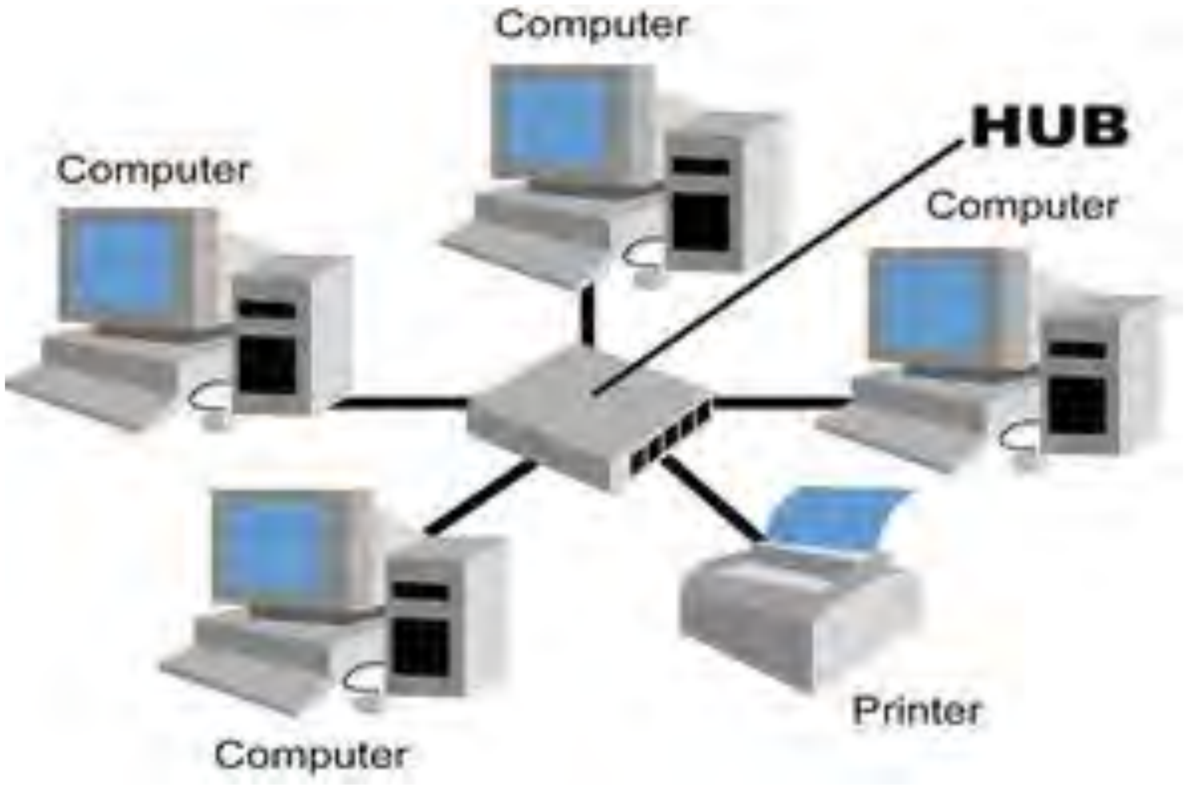
Advantage – if one device or link malfunctions, the remainder of network still functions

Disadvantage - if the hub fails, the whole network goes down

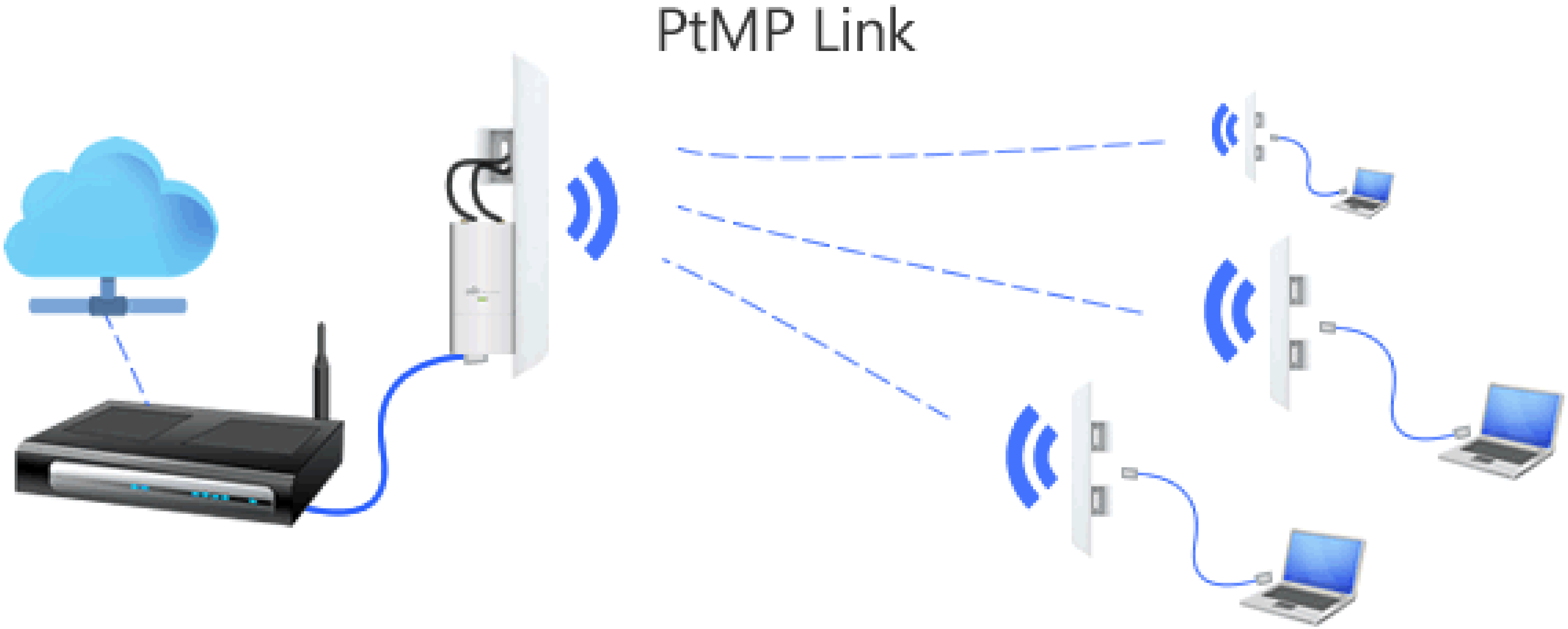


Star Topology Examples





Point-to-Multipoint Wireless Example



Ring

Network devices are arranged in a loop

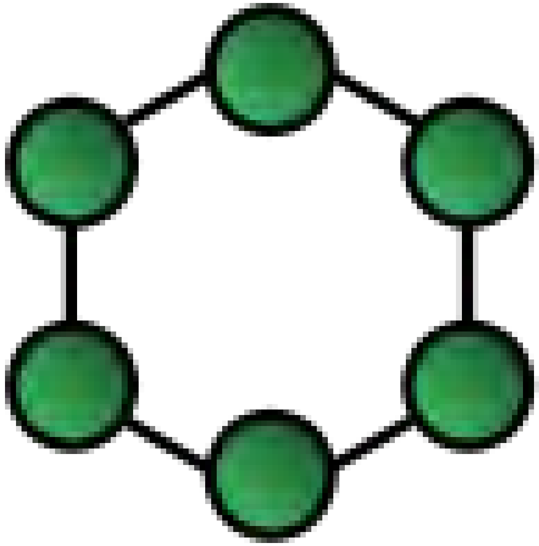
Each node acts as a repeater

Advantage:

- Regenerates signal when passing data through each device
- Thus can support a larger network

Disadvantage:

- Can be slower than star
- If one device goes down all of devices will be impacted

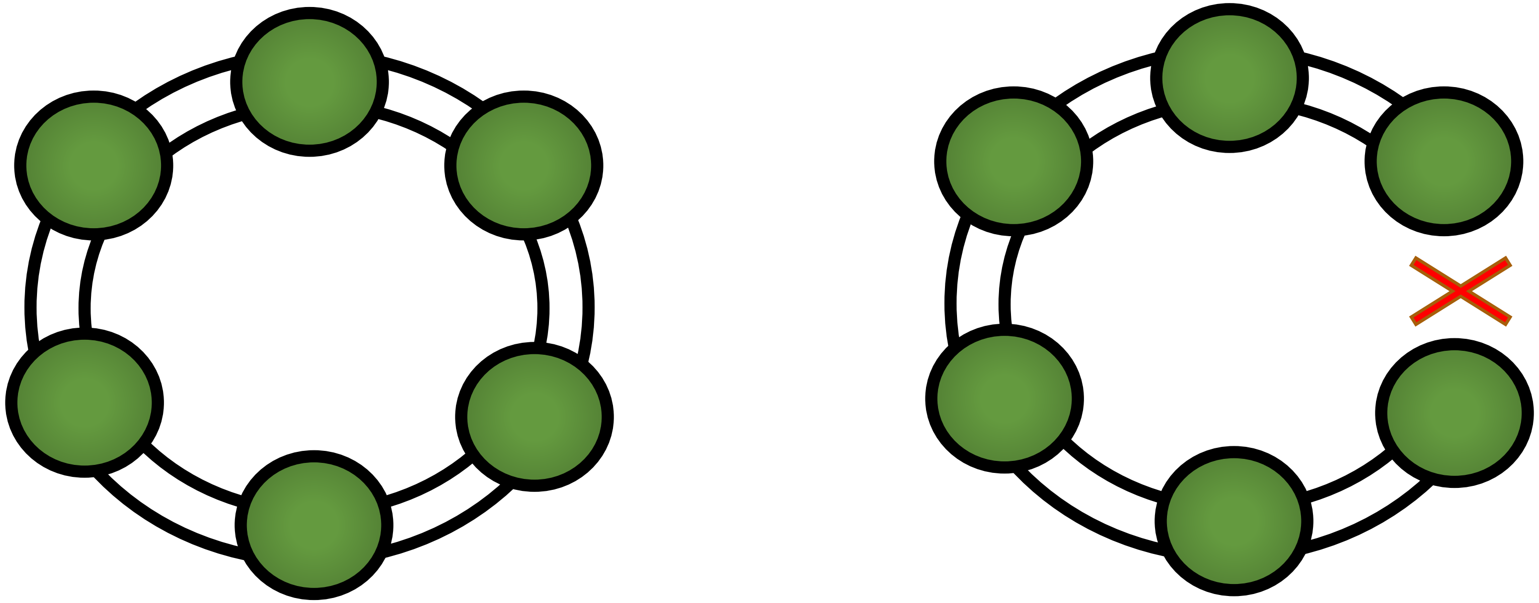


Dual Ring

Used in FDDI MANs

Redundant rings provide fault tolerance

If the rings are broken at one point, nodes on either side use both rings to close the loop



Mesh

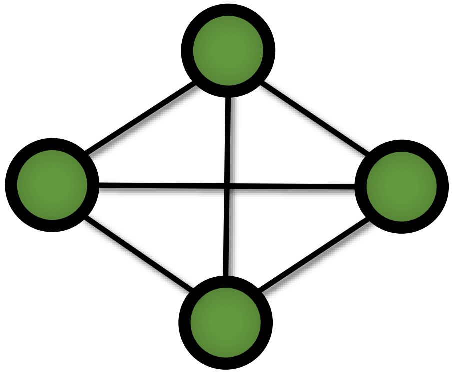
Nodes are connected to more than one node

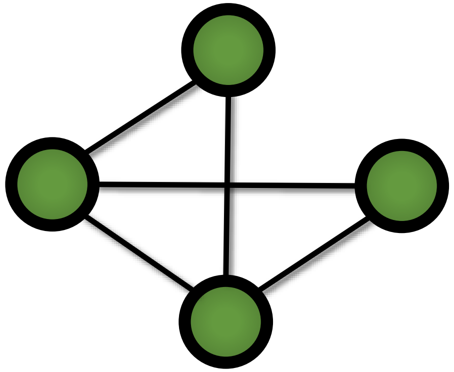
- Redundancy
- Fault tolerance

Can be thought of as a redundant star

Two types of mesh topologies:

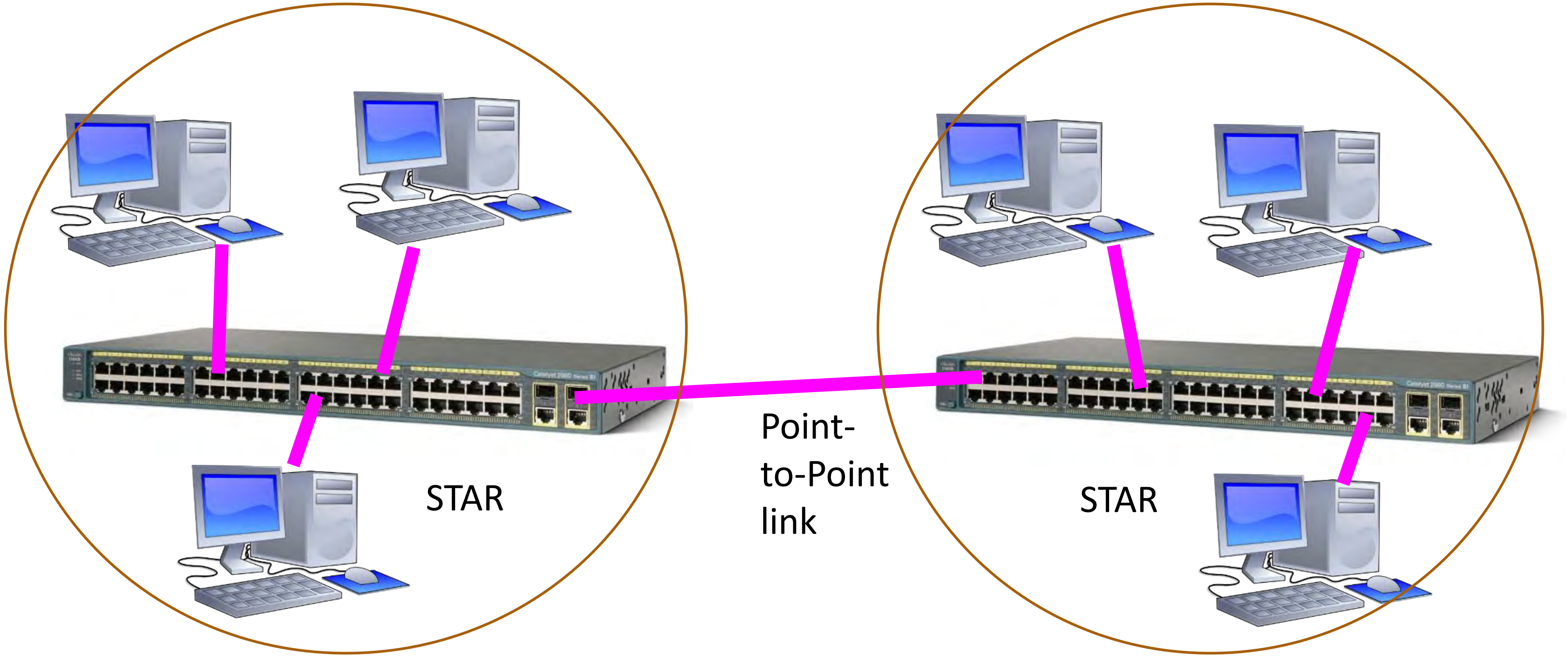
- Full mesh - Every node connects to every other node
  - Full redundancy
  - Expensive, but good for backbone (core) network
- Partial mesh – Some nodes have links to more than one node
  - Is less expensive with less redundancy
  - Good for devices that connect to backbone network





Hybrid

Any combination of the various topologies to create a larger network



Network Types

Local Area Network (LAN)

Limited to a small geographical region

- A floor, building, or small campus

Uses LAN-based or dual-use network protocols/technologies

- Ethernet
- Wireless
- Token Ring
- ATM

One organization usually owns all of the equipment/infrastructure

Metropolitan Area Network (MAN)

A network that connects users with computer resources in a geographic area or region

- Typically around a town/municipality (5 - 50 km)
- Larger than a LAN
- Smaller than a WAN

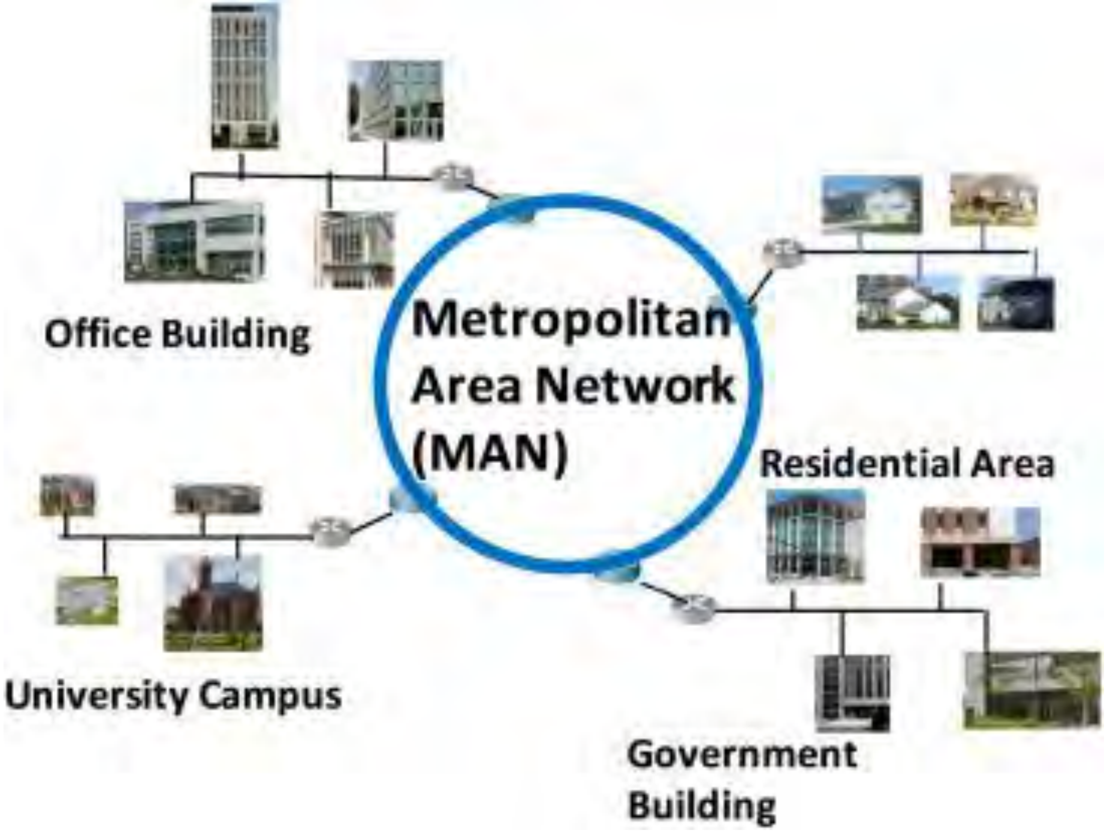
Uses MAN-specific protocols

LAN (high) speed on fiber optic cable

Often used by companies to connect multiple sites around town

Typically owned by a consortium of users

- Or a single provider that sells the service to users



MAN Protocols

Asynchronous Transfer Mode (ATM)

Fiber Distribution Data Interface (FDDI)

Switched Multi-megabit Data Service (SMDS)

Multiprotocol Label Switching (MPLS)

Metropolitan Ethernet (Metro Ether)

Wide Area Network (WAN)

Connects remote locations

- Across towns, states, even continents
- Owned by one or more service providers

Likely to use different network protocols in various network segments

Customers pay for the provider to connect their remote offices

Traditionally much slower than LANs or MANs

The Internet is the largest example of a WAN

The Internet is the Ultimate WAN

Comprised of thousands of telecom networks all connected together

When a telecom provides Internet service, it is called an “ISP” (Internet Service Provider)

ISPs are identified by their Autonomous System (AS) Number

Permits billions of devices and people to communicate across the globe

Wireless LAN (WLAN)

Uses Wi-Fi instead of Ethernet to connect devices

Can be connected to an Ethernet LAN

Personal Area Network (PAN)

A computer network organized around an individual person

Set up for personal use only

Can include a computer, phone, printer, tablet, wearables, and other personal devices

Can use many technologies (wired or wireless)

- Traditionally was Bluetooth-based (802.15)
- Can also include other wireless technologies

Also known as a piconet

Campus Area Network (CAN)

A large LAN, covering a campus of buildings

Likely to have a high-speed fiber optic backbone

Smaller MAN networks are sometimes referred to as “CANs”

Storage Area Network (SAN)

Most commonly used storage architecture in business

Specialized network segment connects servers to centralized, dedicated storage devices

Provides high performance and low latency

Can use:

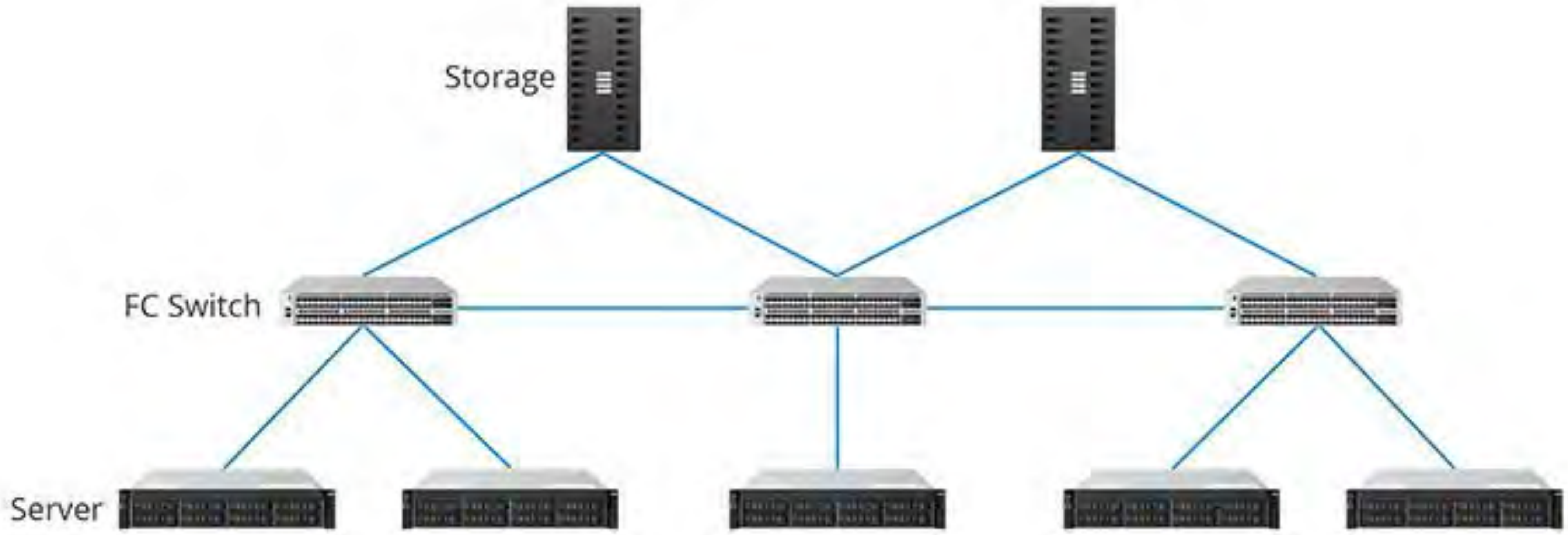
- Specialized fibre channel cable and switches
- Existing Ethernet network

Can span multiple sites

Can play an important role in Business Continuity

- Important data is all in one place
- Easier to secure, back up, recover, and manage

Typical SAN Architecture



Network Characteristics

What are Baseband and Broadband?

Baseband

- Data signal is placed directly on transmission medium
  - Generally, transmission medium can only carry one signal at a time
- Distance limited by quality of transmission medium and original signal strength
- Most LAN transmissions are baseband
- Analogous to sound carried on a microphone cable or speaker wire

Broadband

- Digital data signal is “piggy-backed” (modulated) on top of a more powerful analog carrier signal
  - Multiple carrier frequencies allow multiple signals to share the same transmission medium
- Distance is limited by strength of the carrier signal and type of transmission medium
- DSL and cable modem

Multiprotocol Label Switching (MPLS)

Internal network used by service providers to:

- Create private WAN links for customers
- Connect data centers to branch offices

Not a service, but a routing technique

- Directs traffic from one node to the next based on short path labels instead of long network addresses
- Used to speed up the flow of traffic in a network and to ensure reliable packet delivery of data packets

Operates between traditional OSI Layer 2 and 3

- Sometimes referred to as Layer 2.5 protocol

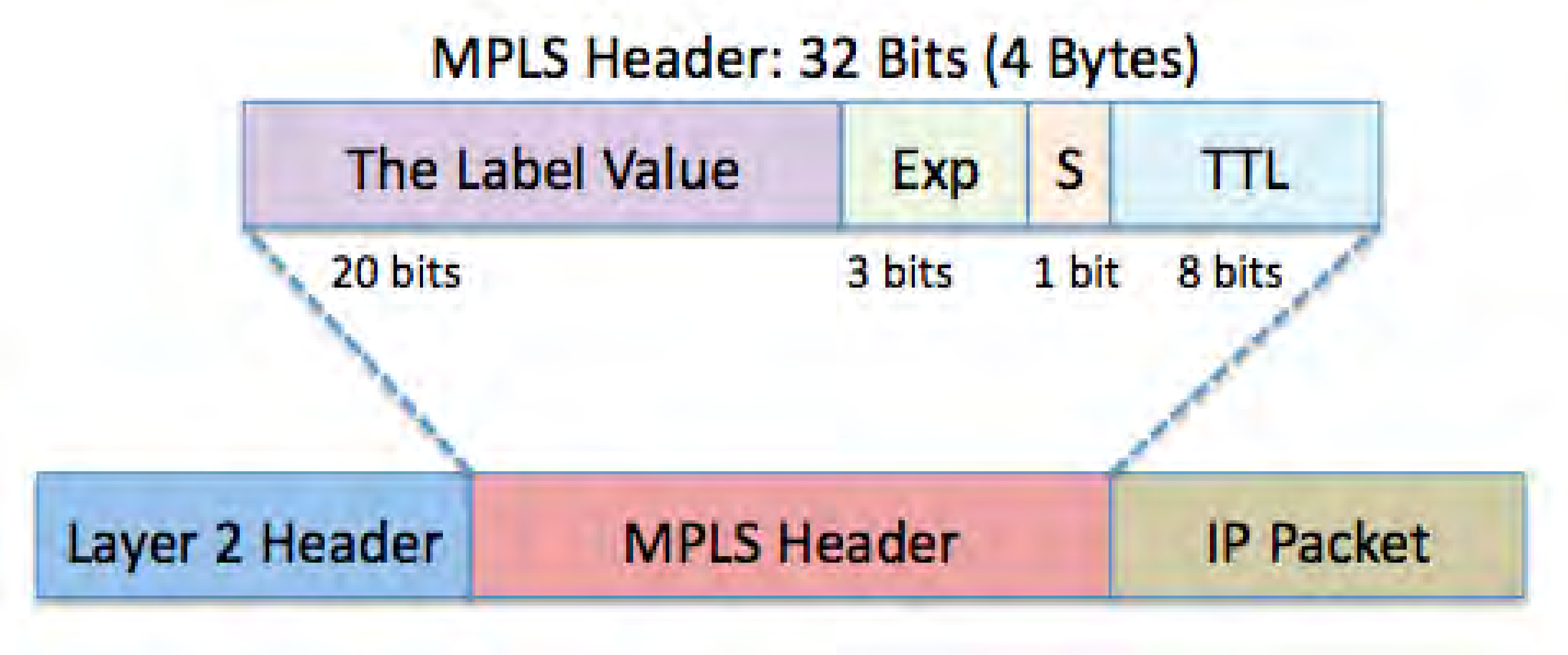
A trusted go-to connectivity option for organizations for decades

- Still in use today

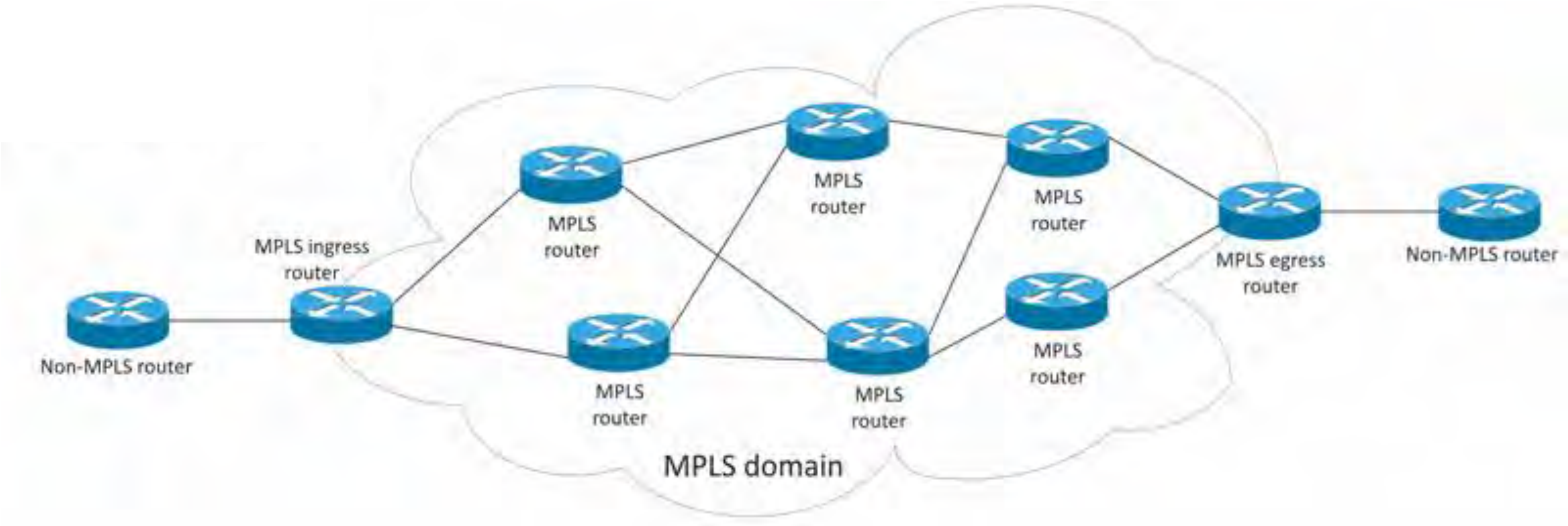
MPLS Process

1. The packet enters an MPLS network (domain)
2. The first router (ingress router) performs a traditional route table lookup
3. Instead of finding a next-hop, it finds the final destination router
4. Then it finds a pre-determined path from “here” to that final router
5. Based on this information, the router applies a “label” (or “shim”) to the packet
6. The other routers along the path use the label to forward the packet to the next router in the path
   - No need to perform any additional IP lookups
   - They know what the path should be, and keep the packet on that path
7. The final router removes the label
8. The packet is delivered to the destination via normal IP routing

MPLS Header


MPLS Header: 32 Bits (4 Bytes)
The Label Value
Exp
S
TTL
20 bits
3 bits
1 bit
8 bits
Layer 2 Header
MPLS Header
IP Packet

MPLS Domain Example



MPLS Advantages

Much faster than traditional routing

Reliable and secure

Built-in traffic engineering

Can have pre-calculated backup routes handy

Offers customers a private connection with end-to-end QoS

Works with IP, ATM, Frame Relay, Ethernet or SONET

MPLS providers also can deliver more comprehensive service-level agreements than providers that offer connectivity over public links

MPLS Disadvantages

Solutions are geographically limited to locations where dedicated MPLS circuits are available

Complex

Time-consuming to manage

Somewhat inflexible

Costly to upgrade and scale

High bandwidth usage compared to the newer SD-WAN

Software Defined WAN (SD-WAN)

SD-WAN is a software-defined approach to managing the WAN

The latest incarnation of WAN technology, primarily for enterprises

Evolved out of MPLS

Developed to address some of the limitations of traditional WANs

More economical and flexible than MPLS

Traditional WAN Challenges

Traditionally, users connected back to the corporate data center (“back haul”) to access business applications

- If you want to centrally apply and manage organizational policies, you have to route the traffic to the corporate LAN, even if it is ultimately destined to go back out to the Internet or a cloud service
- Results in delayed response times and poor network performance

MPLS not originally designed to handle cloud-based SaaS and IoT traffic

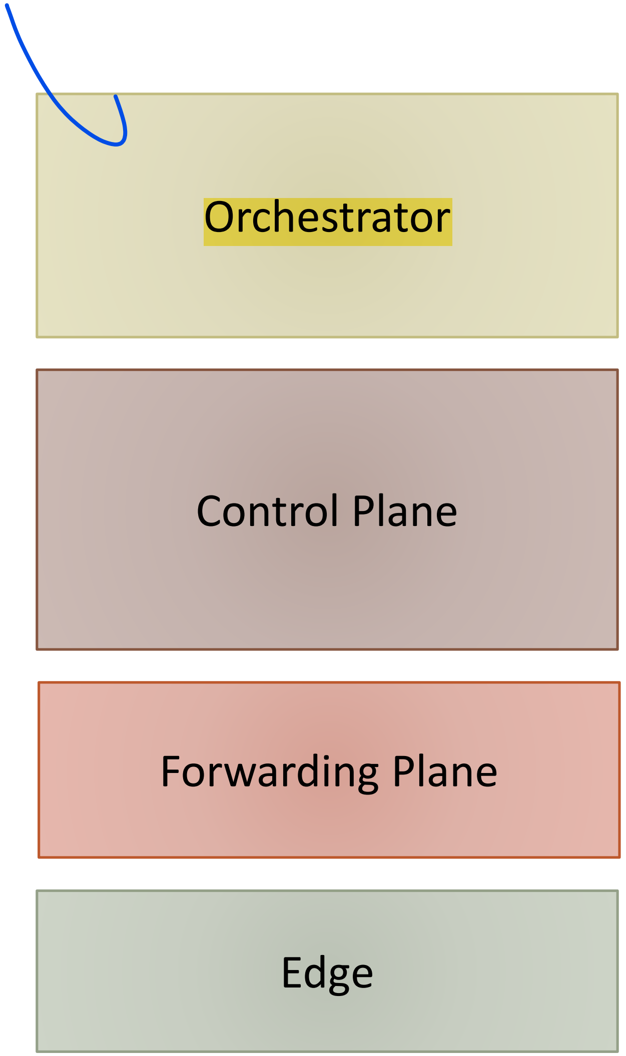
- Cloud-based SaaS allows users to connect to the same apps from anywhere, using their local ISP
- The problem is, you don’t have centralized control over who connects to what and how

Configuration in traditional WAN architecture is distributed

- Housed locally on individual physical routers
- Changes and new deployments are time consuming
- Configuration usually done manually on a per-device basis by on-site IT engineers

SD-WAN Architecture

optional



Optional master software that coordinates multiple SD-WANs

- Automates onboarding new networks and devices into the entire SD-WAN fabric
- Makes it easy for admins and customers to set overarching policy and service requirements
- Directs and coordinates the control planes of participating SD-WANs
- Typically includes a self-service portal for customers and admins

Centralized software that manages the SDWAN

- Takes direction from the orchestrator
- Coordinates underlying networks into a single WAN
- Allows admins to see and manage all traffic through a single pane-of-glass
- Continuously monitors, making real-time routing decisions
- Simultaneously deploys configuration and policy to underlying networks

The physical part of the SD-WAN

- Comprised of existing WANs from various operators
- MPLS, 4G/5G/LTE, broadband Internet, etc.

Where network endpoints reside

- Clients, servers, storage, customer firewall
- Can be a provider's cloud, branch office, company headquarters, datacenter, teleworker's home

SD-WAN Control and Forwarding Functions

Control Plane ("overlay")

- Centralized software application
- Creates a virtual network ("overlay") on top of the physical circuits ("underlay")
- Monitors all circuits in the underlay
- Controls routing decisions in real-time
- Continuously chooses the fastest and best-performing available route
- Creates tunnels for traffic to move across the underlay
  - Tunneling protocols are typically GRE, mGRE, IPSEC or Secure Vector Routing (SVR)

Forwarding Plane ("Underlay")

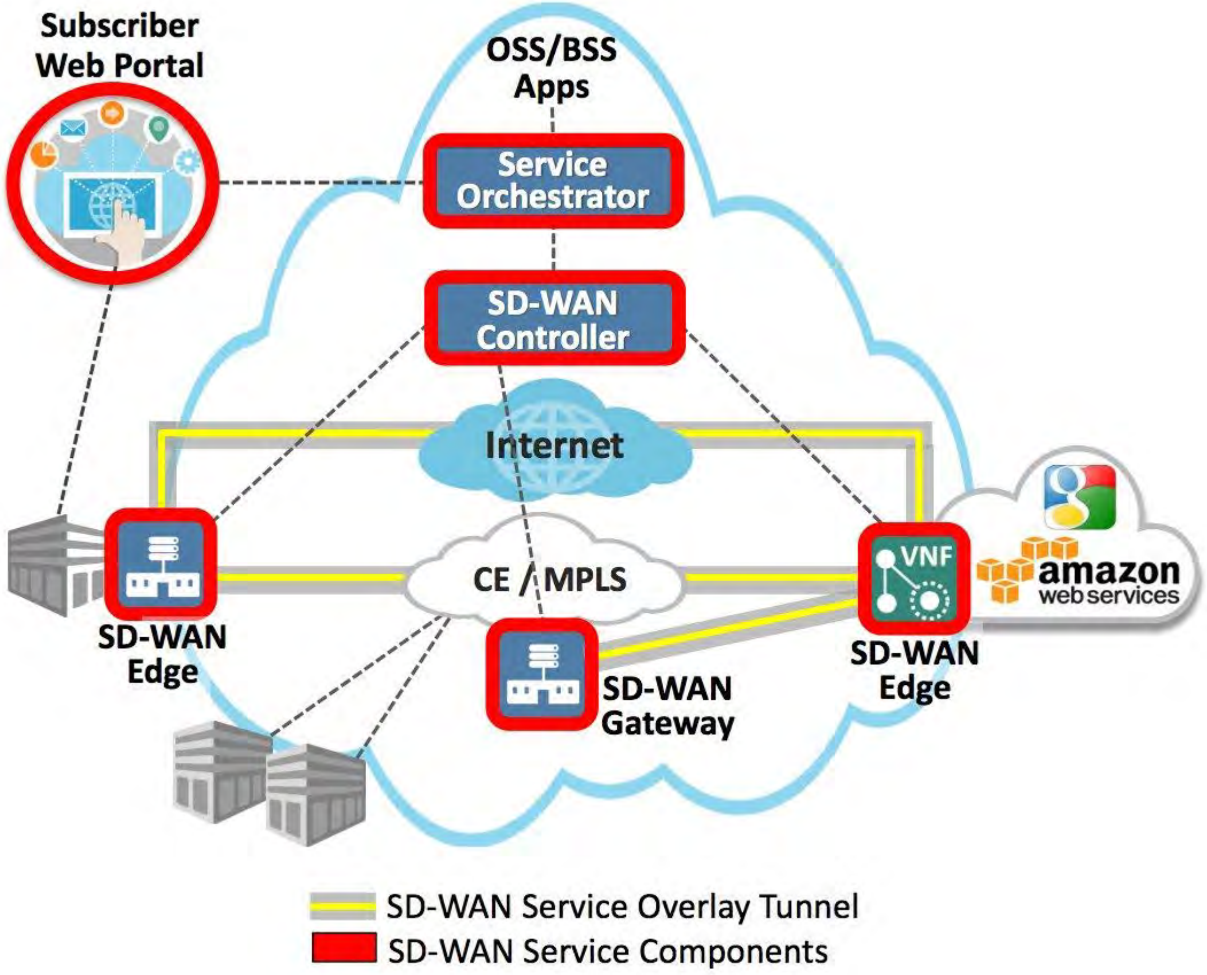
- Physical infrastructure including switches, routers, and links
- Tunneled traffic is moved across any combination of traditional networks
  - MPLS, cellular, broadband Internet
- Traffic is routed based on policies created by network administrators

SD-WAN Example

OSS = Operational Support System

BSS = Business Support System

CE = Customer Edge



SD-WAN Advantages

Dramatic savings over traditional WANS

Constantly, dynamically choosing the best route

Can use cheaper circuits that still maintain the desired performance and security

Increased network visibility for IT administrators

More control over endpoints

Enables connections between geographically remote sites

Reduces hardware dependencies

Eliminates lock-in to service provider solutions

SD-WAN Disadvantages

Without a good orchestrator, can be complex to adopt

Solutions often lack natively integrated security

- Can put organizations at risk for cyberattacks

Multipoint Generic Routing Encapsulation (mGRE)

Point-to-multipoint ***tunneling*** between routers

- Originally, GRE was point-to-point

Allows a single GRE interface to support multiple IPsec tunnels.

Packets are encapsulated (hidden) inside IP packets

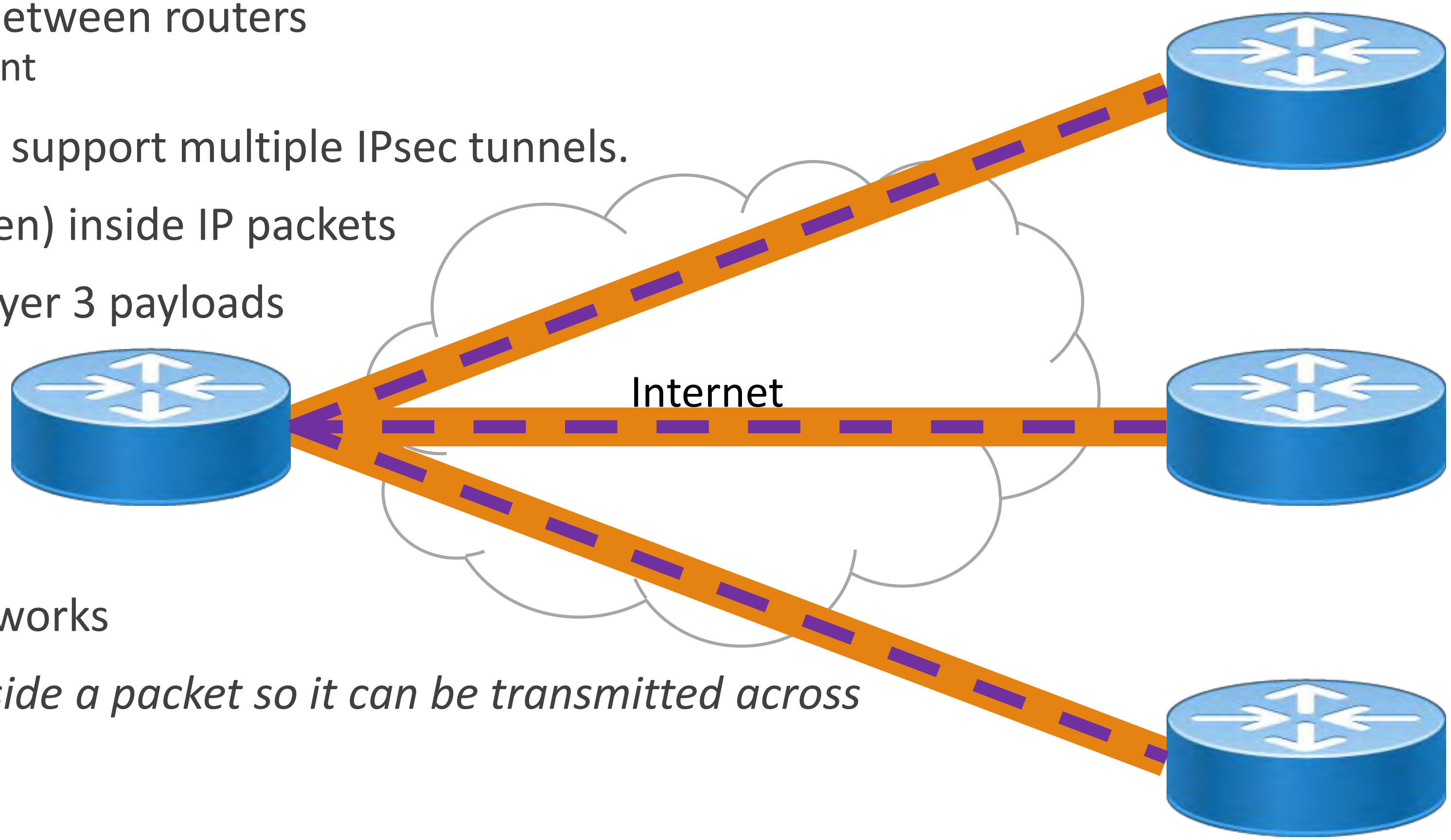
Hidden packets can be other Layer 3 payloads

- Multicasting
- IPv6
- IPv4

Encryption can be added

Used in MPLS and SD-WAN networks

Tunneling = *to hide a packet inside a packet so it can be transmitted across a certain type of network*



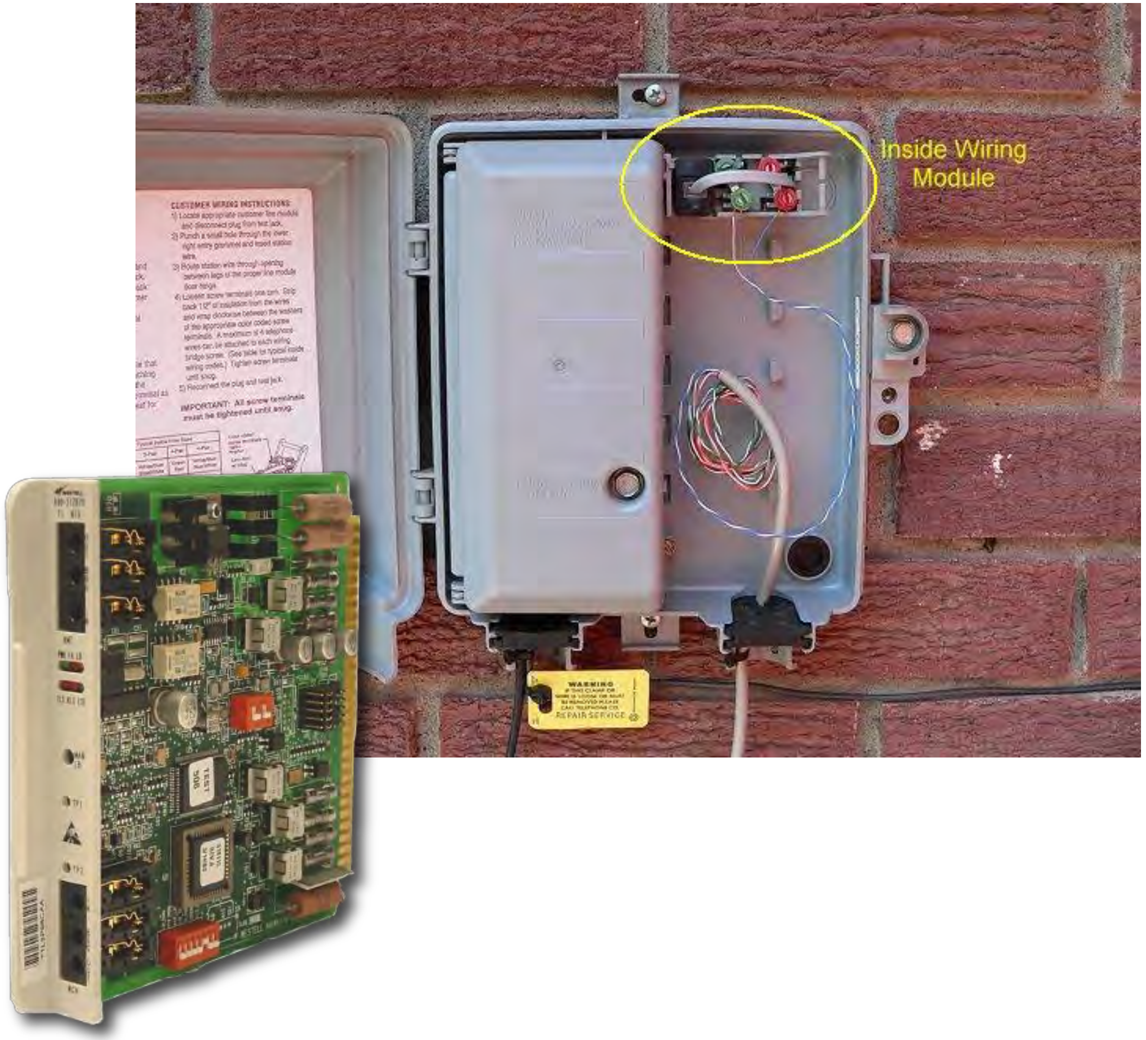
Service-related Entry Point

Demarcation

- Where outside phone/Internet service connects to inside wiring
- At home – outside jack
- At business – telco room/wiring closet (sometimes server room)
- Aka “demark”

Smart Jack

- Placed between demark and customer wiring
  - Business installations
- Creates a loopback for signal to return to telecom
- Used for remote line diagnostics



Virtual Networks

Network (and its attached devices) are not physical

- Software processes inside a host computer
- Like a little world inside the host
- Virtual machines connect to virtual networks inside the host

Connectivity can be restricted to inside the host, or allowed to connect to the outside world

Can also be hosted in a provider's cloud

- Connected to across the Internet or VPN by outside devices

Virtual Network Concepts

vSwitch

- Provides switch functionality to virtual machines (VMs)
- A host can have many vSwitches, connecting groups of VMs together

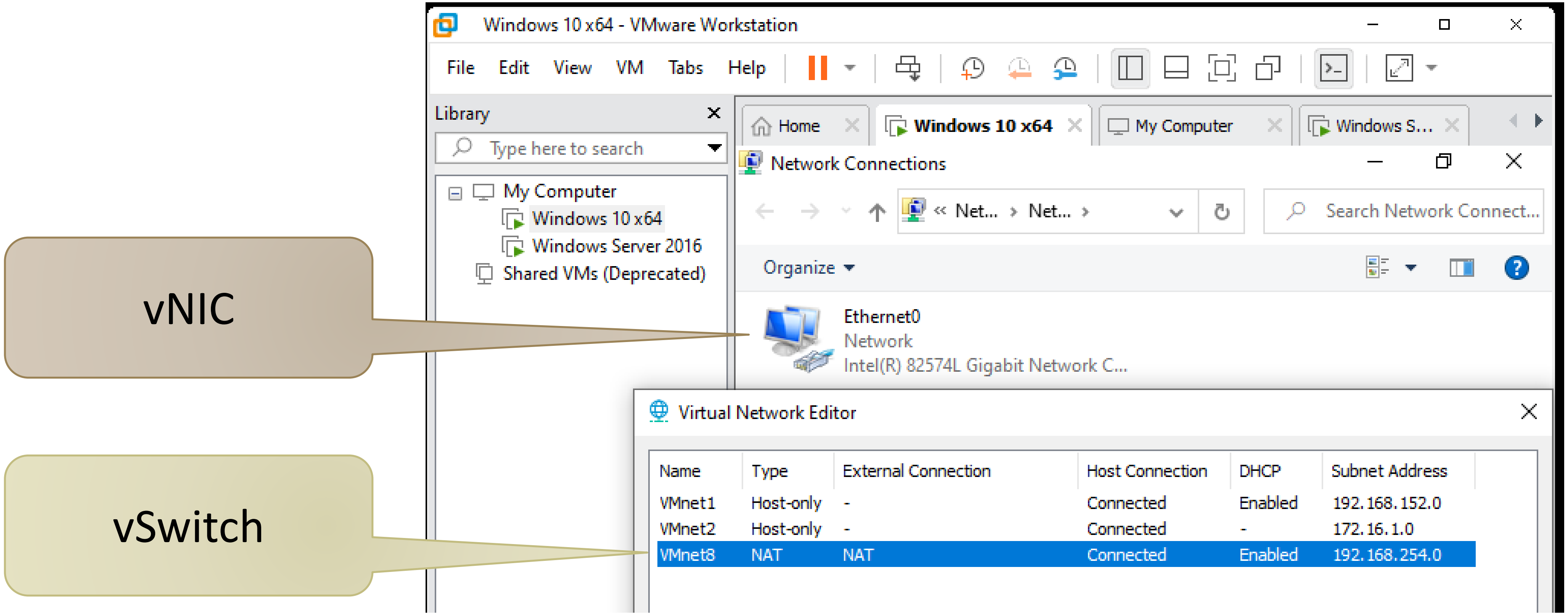
Virtual network interface card (vNIC)

- The “network interface” that allows a VM to connect to a vSwitch

Hypervisor

- A layer of functionality in the host that allows virtual devices to share the host’s physical hardware

Host-based Virtual Network Example



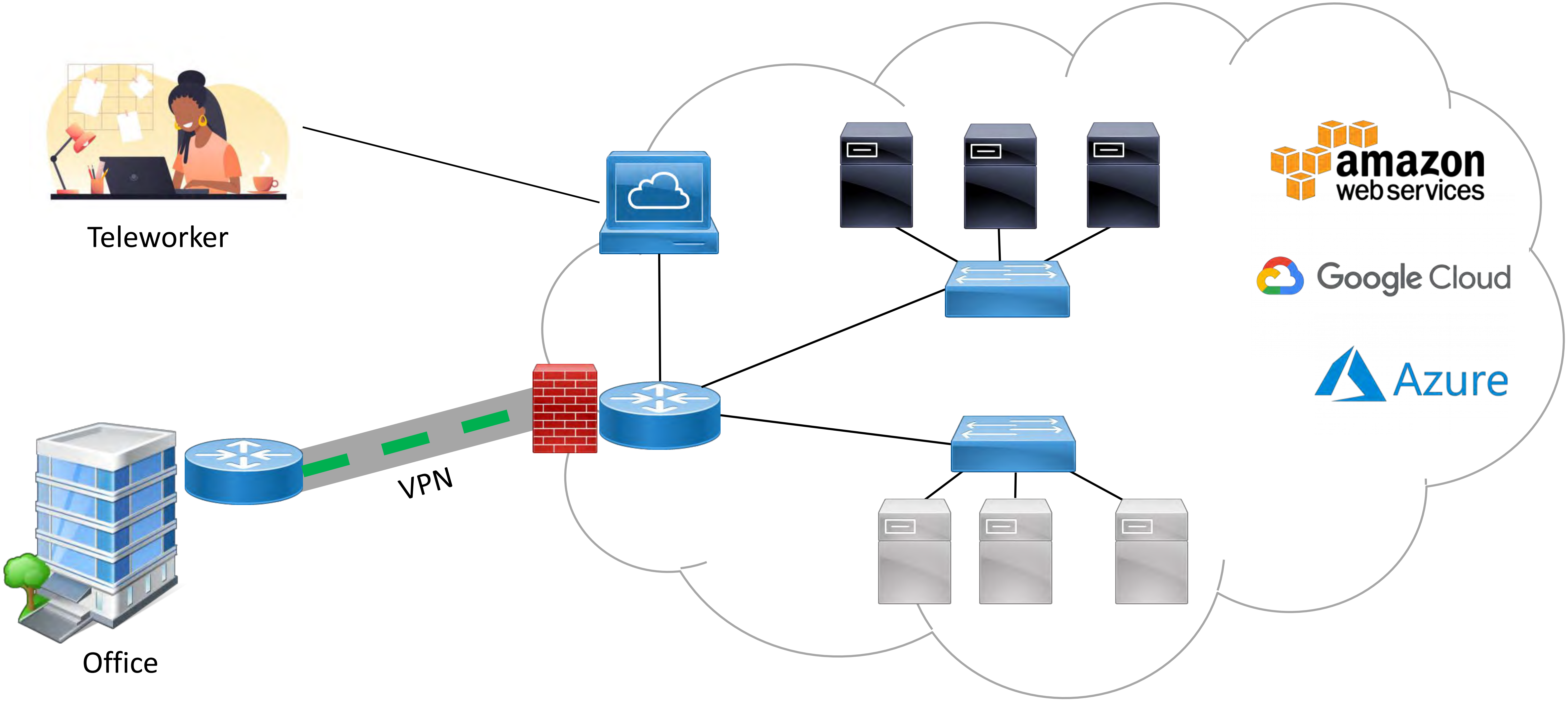
vNIC

vSwitch

Ethernet0
Network
Intel(R) 82574L Gigabit Network C...

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	192.168.152.0
VMnet2	Host-only	-	Connected	-	172.16.1.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.254.0

Cloud-based Virtual Network



Provider Links

Link Type	Description	Typical Max Speed
Satellite	• Used where other connection types not available • One satellite covers a large area • Originally high latency, now dramatically reduced using AI	Hundreds of gigabits
Digital subscriber line (DSL)	• Uses existing telephone landline • Carries traditional Point-to-Point dialup protocol over ATM • Requires special modem & user authentication • PPP over Ethernet at customer site	Download 45 mb/s Upload 7 mb/s
Cable	• Uses existing cable TV network • Transmit and receive data carried on two premium TV channels	300 mb/s
Leased line	• Dedicated to a single customer • Primary Rate ISDN, T3, T1, or fractional T1 • PPP or HDLC	1.544 mb/s 44.736 mb/s
Metro-optical	Optical fiber connecting to provider's MAN	100 mb/s