OPCUG

Overview of the Transmission Control Protocol/Internet Protocol (TCP/IP) – how the Internet works

STEPHANE RICHARD

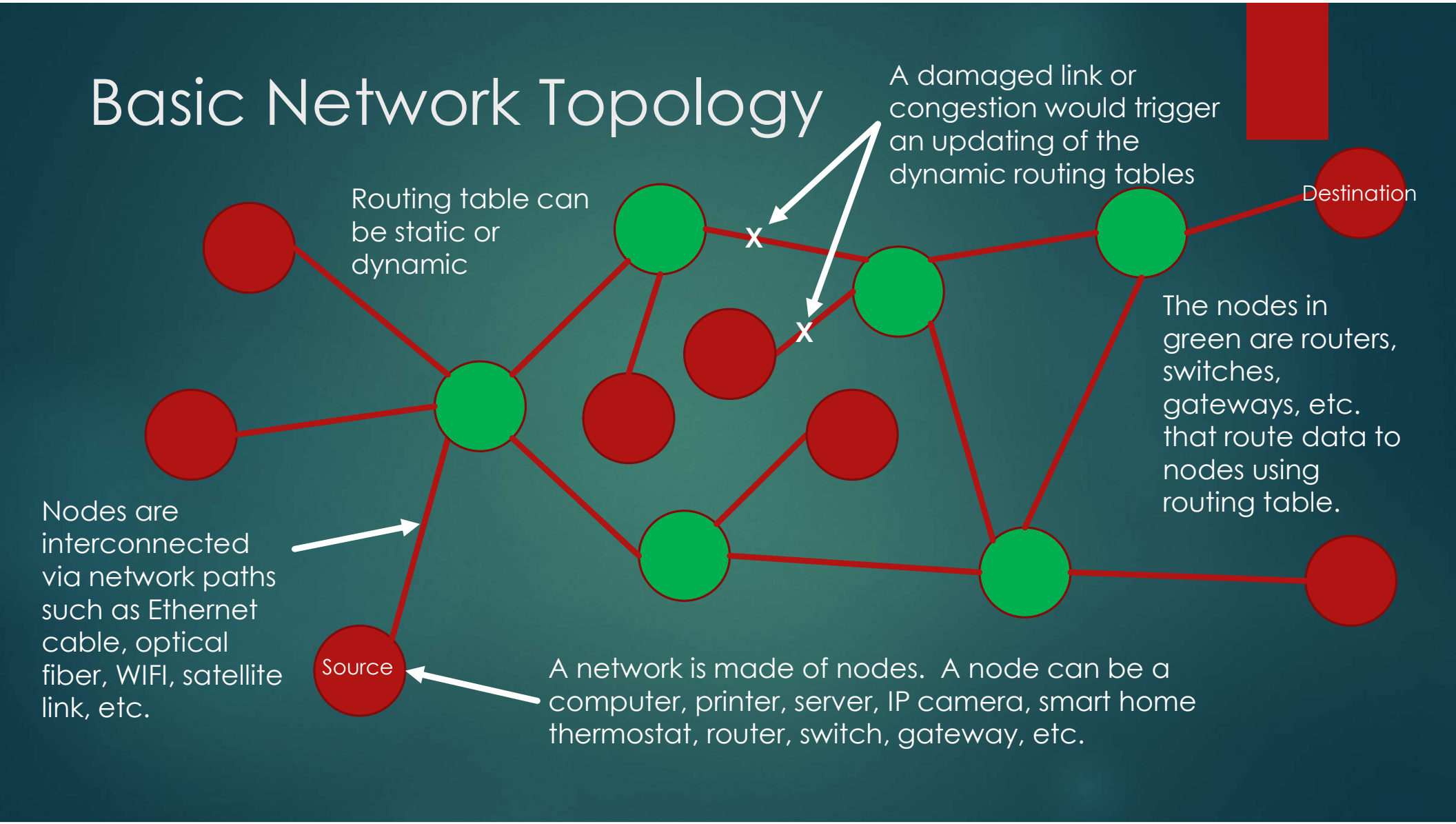
14 DECEMBER 2022

Content

- Network topology and Internet
- TCP/IP definitions and layers
- Layer 1 – Physical
- Layer 2 – Network
- Layer 3 – Transport
- Layer 4 – Application
- Miscellaneous Networking Topics

Network Topology and Internet

Basic Network Topology



What is the difference between a hub, router, switch and gateway?

- **Hub** – is the most basic networking device that connects multiple computers or other network devices. Unlike a network switch or router, a network hub has no routing tables or intelligence on where to send information and broadcasts all network data across each connection.

- **Router** – connects a network to different networks, ensuring that Internet traffic goes to the right networks or nodes.
- **Switch** – connect devices within a single network, transfer incoming and outgoing internet traffic between the connected devices.
- **Gateway** – regulate traffic between two or more dissimilar networks (e.g. security, protocol, etc.)

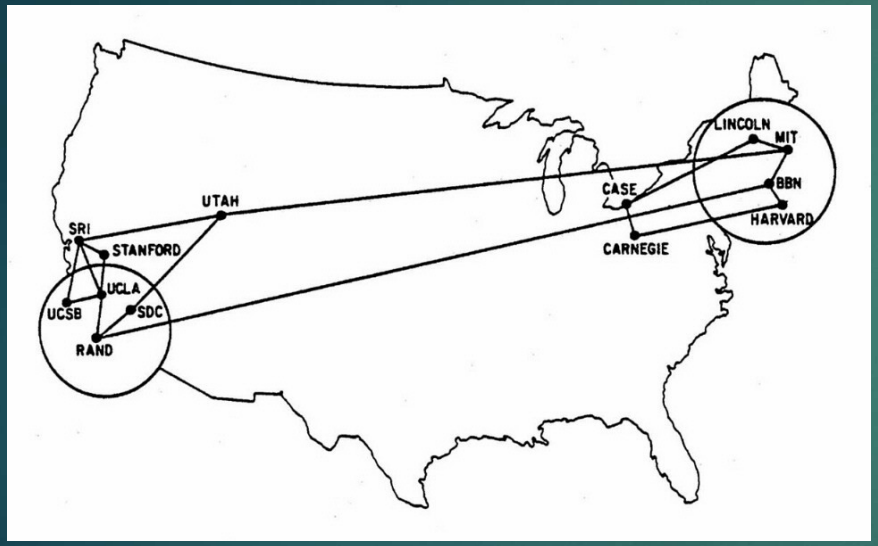
What is the Internet?

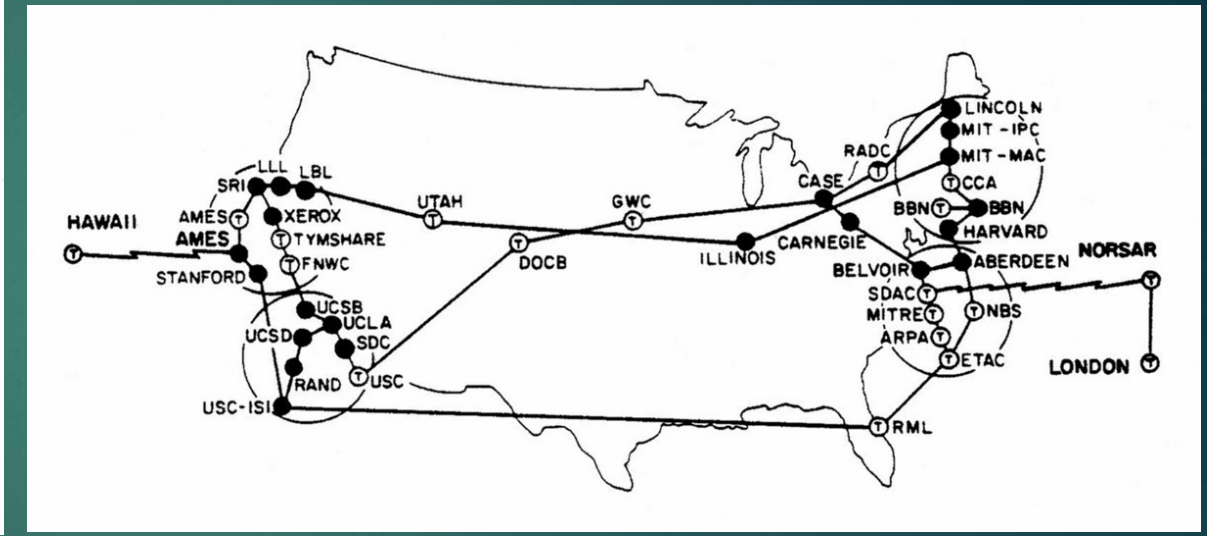
- The Internet is the global system of interconnected computer networks **that uses the Internet protocol suite (i.e., TCP/IP)** to communicate between networks and devices.
- Internet is a **network of networks** that consists of private, public, academic, business such as Internet Service Provider (ISP), and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies.
- The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW), electronic mail, telephony, video streaming, files sharing, gaming data, etc.

The History of the Internet

- Packet switching is **the transfer of small pieces of data across various networks**. These data chunks or "packets" allow for faster, more efficient data transfer.
- The origins of the Internet date back to the development of packet switching and research commissioned by the United States Department of Defense in the 1960s to enable time-sharing of computers.
- The primary precursor network, the ARPANET, initially served as a backbone for interconnection of regional academic and military networks in the 1970s with 13 nodes.
- The funding of the National Science Foundation Network as a new backbone in the 1980s, as well as private funding for other commercial extensions, led to worldwide participation in the development of new networking technologies, and the merger of many networks.
- The linking of commercial networks and enterprises by the early 1990s marked the beginning of the transition to the modern Internet, and **generated a sustained exponential growth** as generations of institutional, personal, and mobile computers were connected to the network.

ARPANET 1970 and 1973





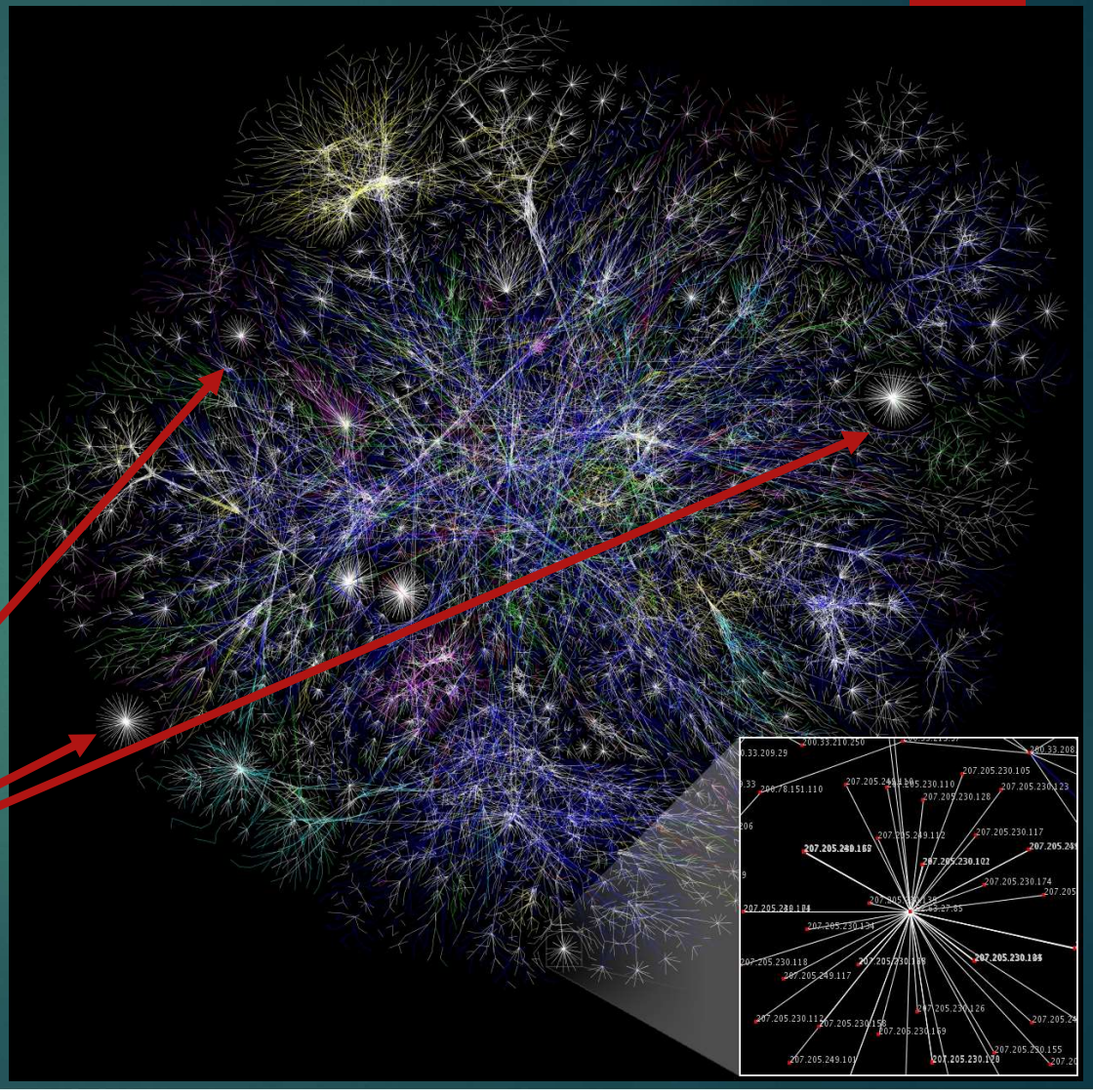
Internet network diagram in 2006

By The Opte Project - https://commons.wikimedia.org/w/index.php?curid=1538544

Graph color:

Asia Pacific
Europe/Middle East/Central Asia/Africa
North America
Latin American and Caribbean
RFC1918 Private IP Addresses
Unknown

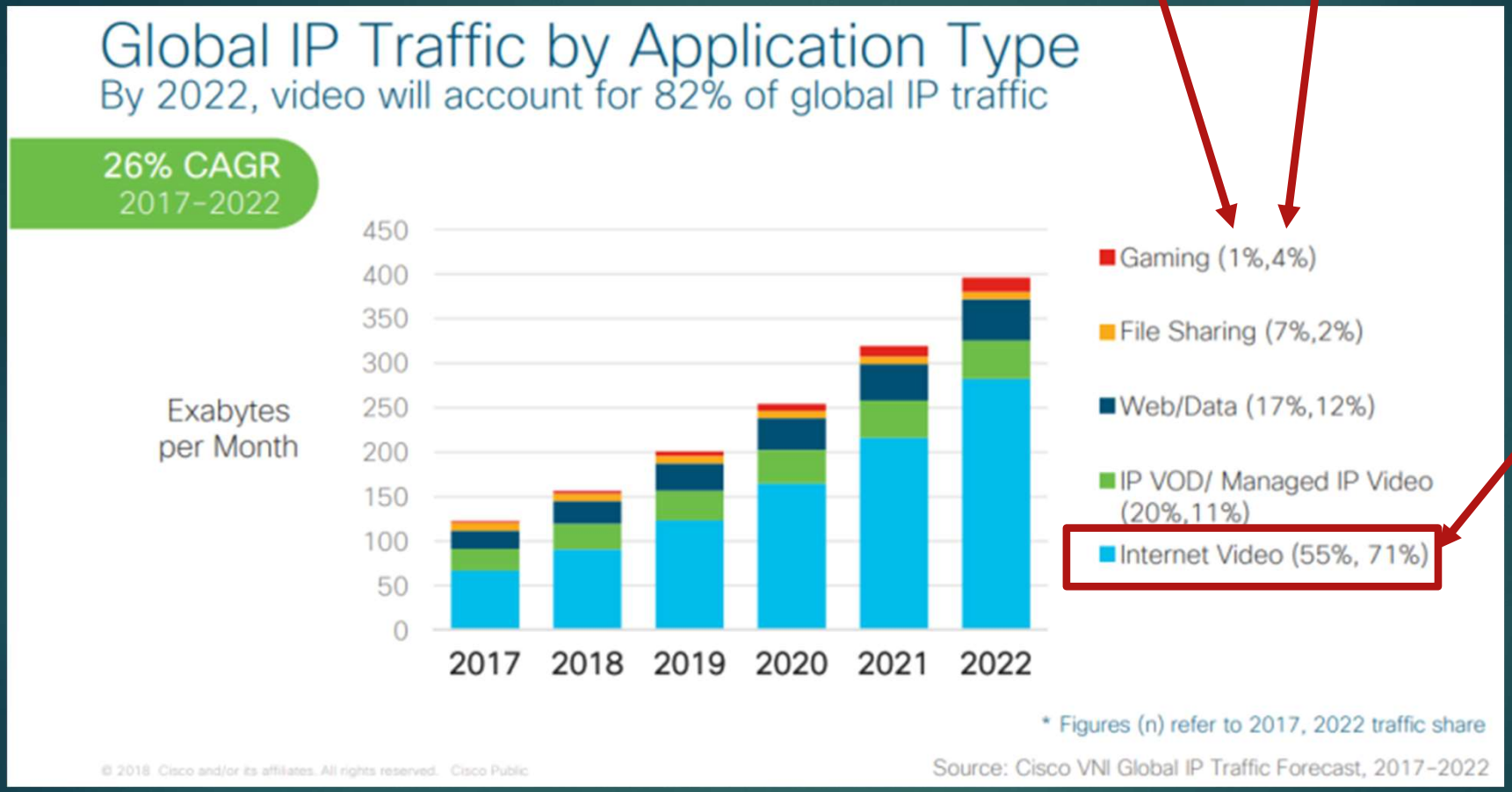
Notice the few stars with a single path to the Internet



Internet Backbone and core router

- The Internet backbone may be defined by the principal data routes between large, strategically interconnected computer networks and core routers of the Internet.
- A core router is a router designed to operate in the Internet backbone, or core. To fulfill this role, a router must be able to support multiple telecommunications interfaces of the highest speed in use in the core Internet and must be able to forward IP packets at full speed on all of them.
- These core routers are hosted by commercial, government, academic and other high-capacity network centers, as well as the Internet exchange points and network access points, that exchange Internet traffic between the countries, continents, and across the oceans.
- Internet Service Providers (ISPs) participate in Internet backbone traffic by privately negotiated interconnection agreements, primarily governed **by the principle of settlement-free peering**.
- In addition, the high degree of redundancy of today's network links and sophisticated real-time routing protocols provide alternate paths of communications for load balancing and congestion avoidance.

Photo of Core Router



Youtube and pornographic videos account for the vast majority (e.g., about 97%) of the "Internet Video" category.

TCP/IP Definitions

What is TCP/IP?

- TCP/IP stands for Transmission Control Protocol/Internet Protocol and is a suite of communication protocols used to interconnect network devices on the internet.
- The entire IP suite -- a set of rules and procedures -- is commonly referred to as TCP/IP.
- TCP and IP are the two main protocols, though others are included in the suite such as (not full list):
  - File Transfer Protocol (FTP) – to move data files
  - Simple Mail Transfer Protocol (SMTP), Post Office Protocol Version 3 (POP3), and Internet Message Access Protocol (IMAP) – for email
  - Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol over SSL/TLS (HTTPS) – for World Wide Web
  - and many more.

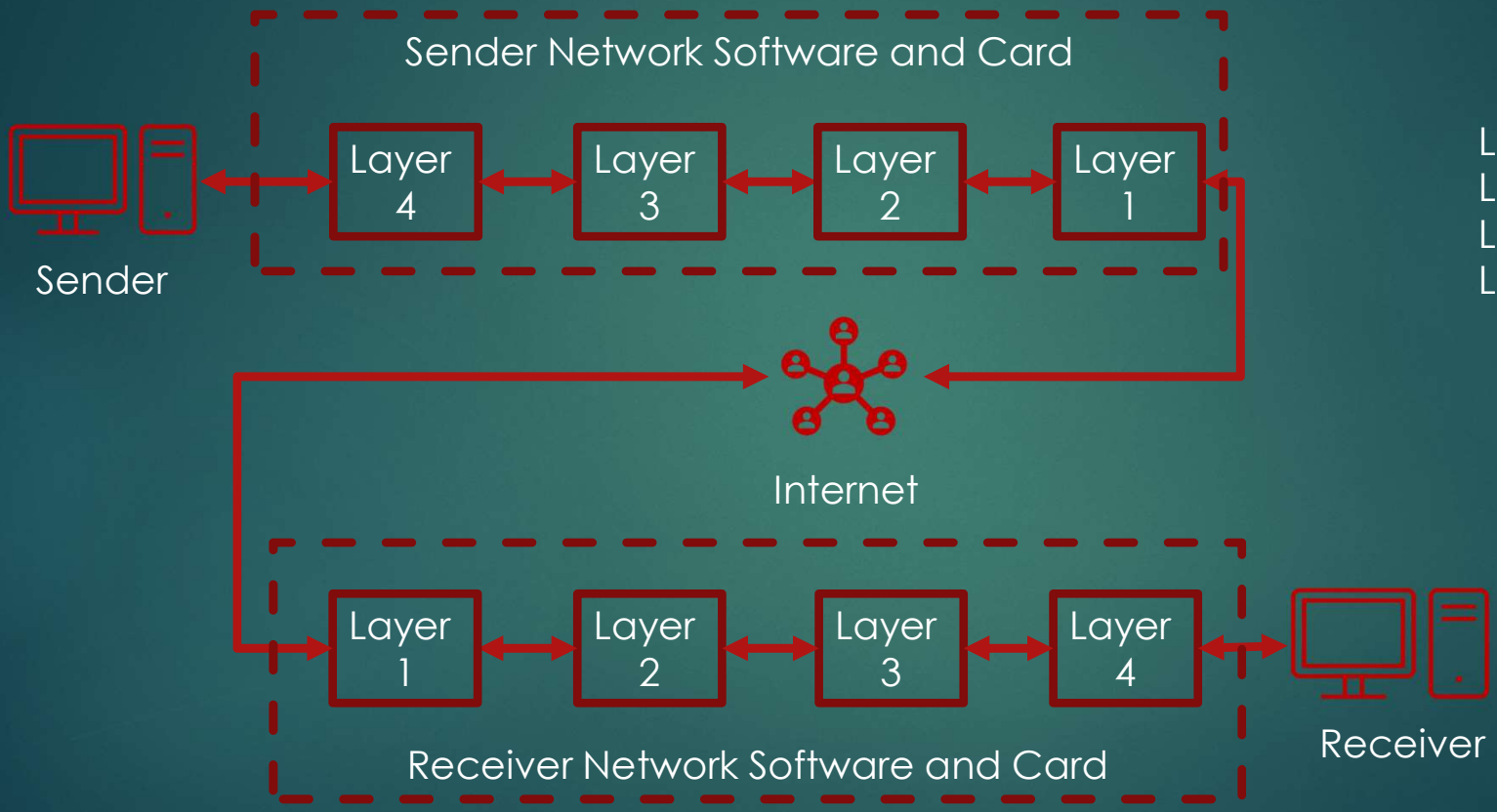
What is a layered network model?

- A layered network model use a number of layers with each layer responsible for specific tasks.
- It reduces the complexity of the problems from one large one to a number of smaller ones.
- It allows for the standardization of interfaces among layers.
- It facilitates modular engineering so engineers can work on one layer of the network model without being concerned with what happens at another layer.
- This modularity also accelerates the evolution of technology and eases the teaching and learning of networks.

The 4 layers of the TCP/IP model

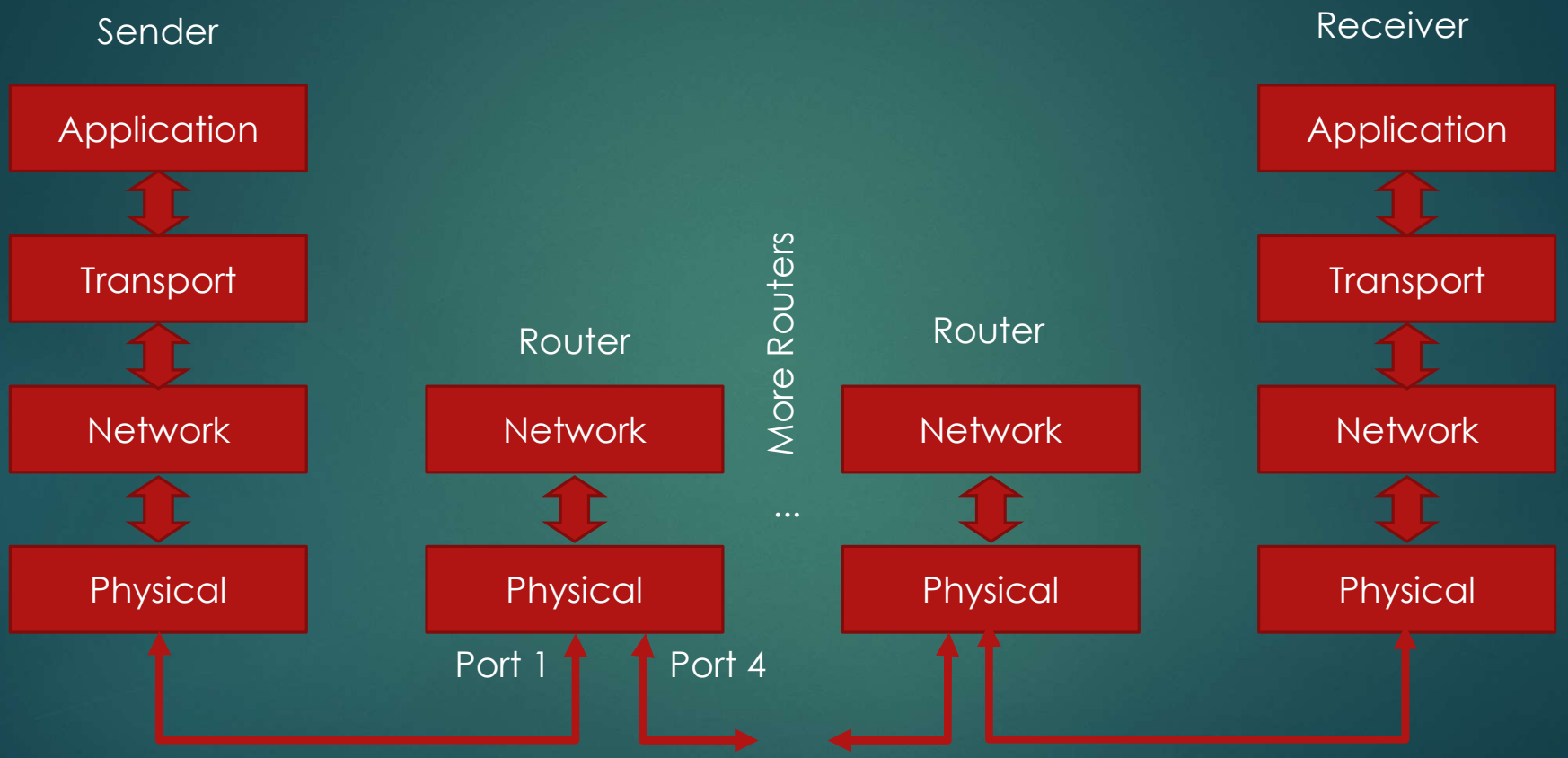
1. **Physical layer (also known as the network interface layer or data link layer)**: consists of protocols (such as Ethernet) that operate only on a link -- the network component that interconnects nodes in the network.
2. **Network layer (also called the internet layer)**: transport the packets or datagram across the network using the Internet Protocol (IP).
3. **Transport layer**: is responsible for maintaining end-to-end communications across the network.
4. **Application layer**: provides applications with standardized data exchange. Its protocols include HTTP, HTTPS, FTP, POP3, SMTP and many more. At the application layer, the payload is the actual application data.

The TCP/IP Model Process



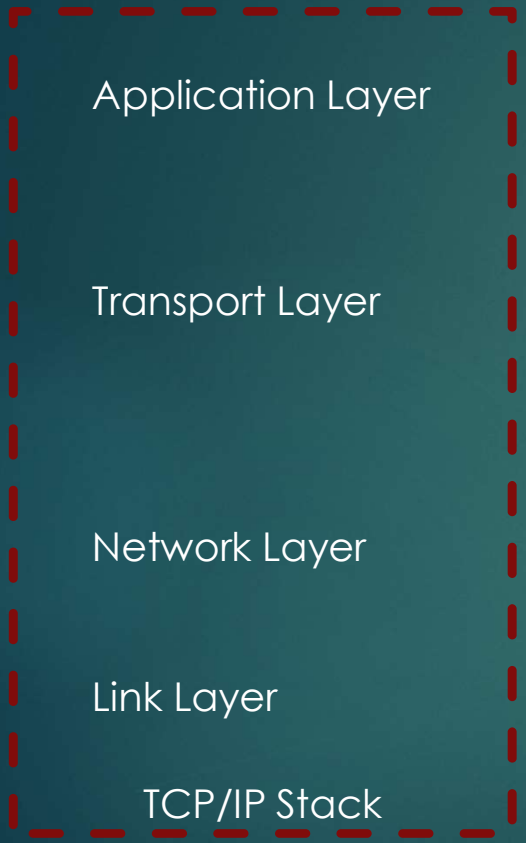
Layer 4 Application
Layer 3 Transport
Layer 2 Network
Layer 1 Physical

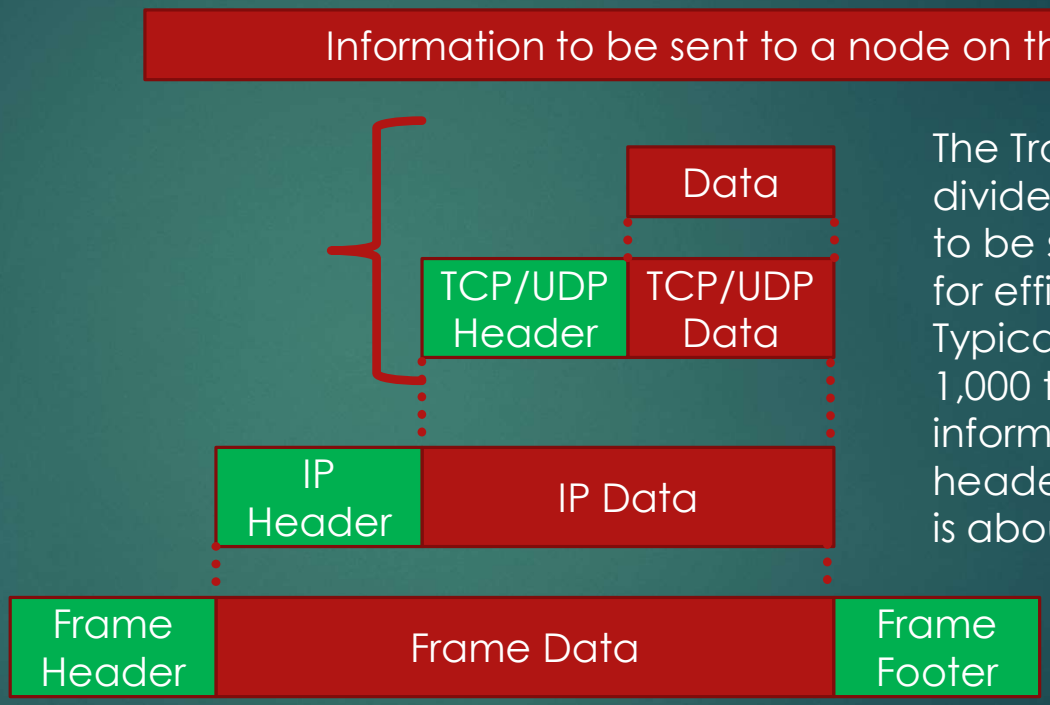
Another view of the TCP/IP Process



Routing table will determine which port will be used on the router

TCP/IP Layers/Stack - Header and Footer





The Transport layer divides the information to be sent into packets for efficient routing. Typically, a packet holds 1,000 to 1,500 bytes of information. The header/footer overhead is about 5%.

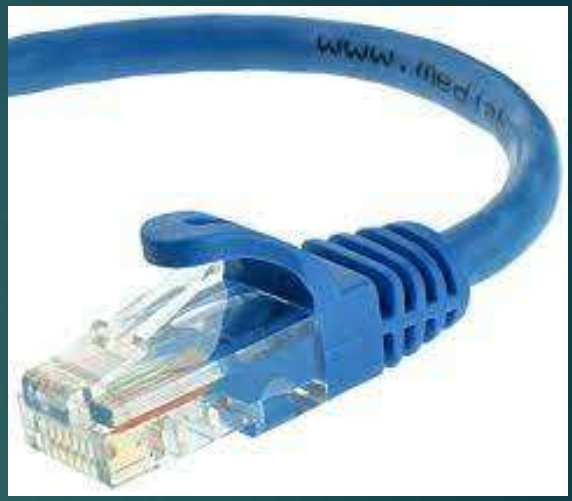
Layer 1 - Physical

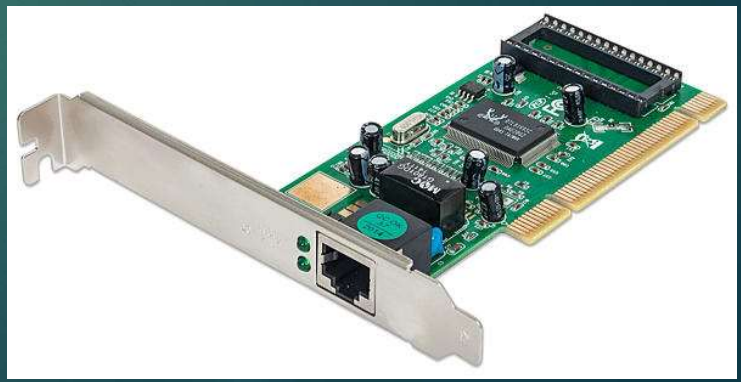
OPERATES ON A SINGLE LINK

Physical Layer – example of hardware

- This layer is all about connecting two nodes together using a media such as copper wire, pure silica (glass), atmosphere – i.e. radio wave, etc.
- Example of hardware:
  - Ethernet
  - Wireless Fidelity (WIFI)
  - Fiber Distributed Data Interface (FDDI)
  - Microwave wireless broadband
  - Elon Musk satellite internet constellation Starlink
  - And others, but will focus on the list shown

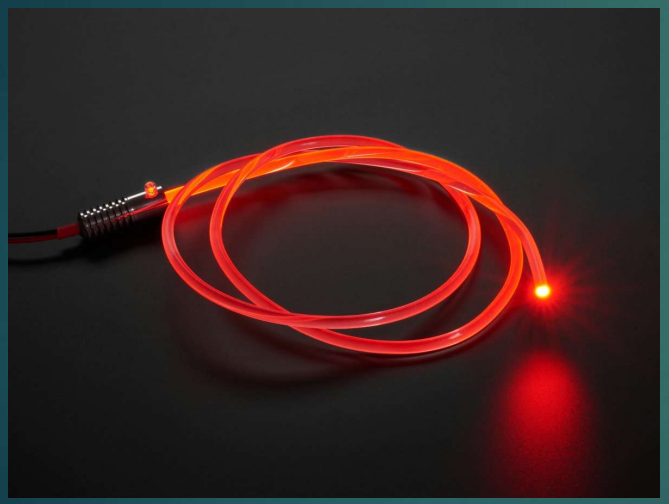
Physical Layer – Ethernet (up to 90 m)

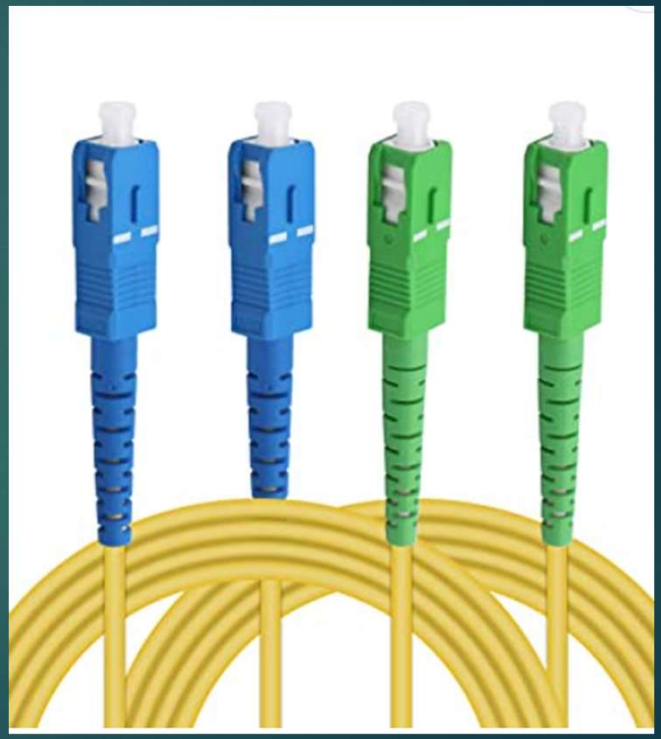




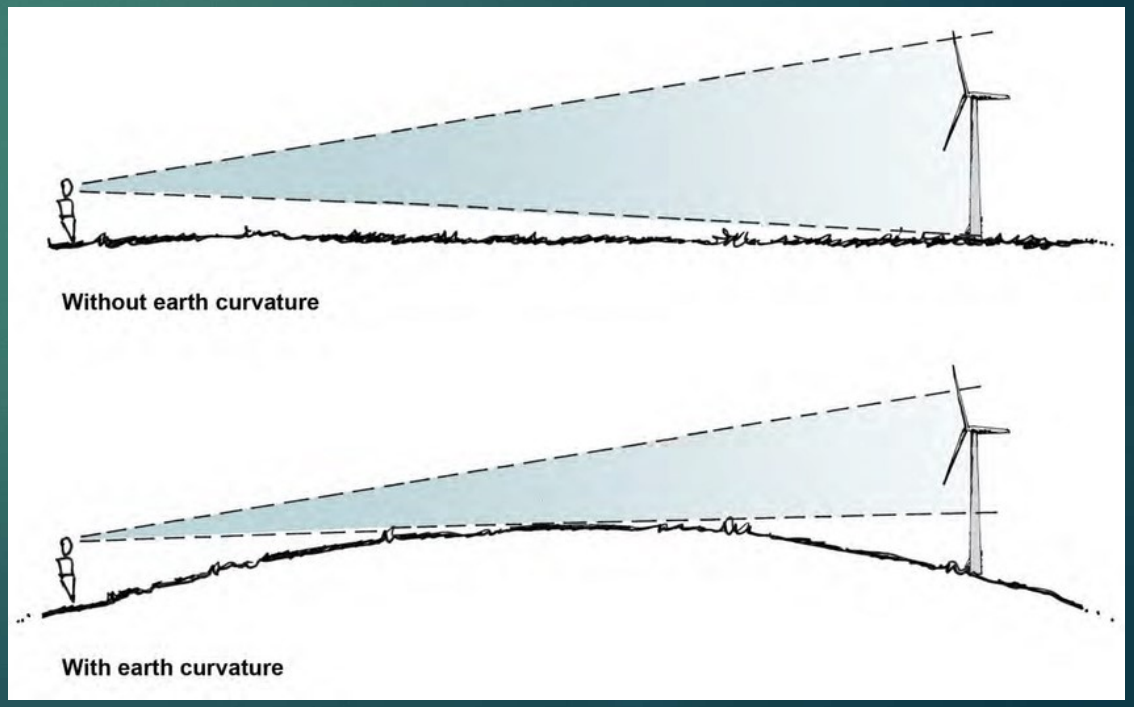
Physical Layer – WIFI (distance 45 m indoor)

Physical Layer – Fiber Distributed Data Interface (FDDI) (distance 200 km)

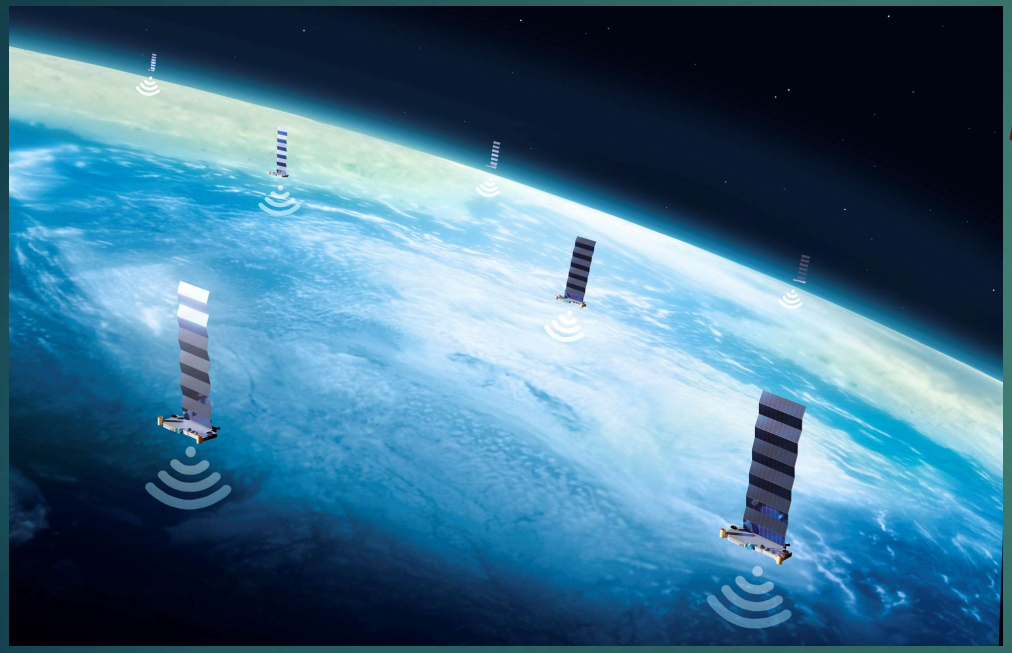




Physical Layer - Microwave wireless broadband (distance of about 50 km – curvature of the Earth – needs taller antenna for greater distance)



Physical Layer – Elon Musk Starlink (550 km – altitude of satellites)



Space segment. Current constellation is about 2,300 satellites (largest in the world), but the full constellation will have 12,000 satellites...

Ground Segments connected to the Internet

User Terminal

Layer 2 - Network

TRANSPORTS THE DATA PACKETS ACROSS THE NETWORK

Network Layer Protocol

- The Network Layer principally uses the Internet Protocol (IP).
- IP is connection less:
  - No state related to IP packets is maintained either on the source, intermediate, or the destination nodes (**aka end-to-end principle**).
- IP is unreliable:
  - **It not guaranteed that an IP packets will get delivered to the destination**.
  - **It also does not assure proper sequencing or avoidance of duplicate delivery of packets.**
- If an IP packet encounters some error at the destination or at some intermediate host (while traveling from source to destination) then **the IP packet is generally discarded** and an error message is sent back to the source.
- IP packets may not use the same network paths while travelling from the source node to the destination node.
- There are organizations that managed the allocation of IP addresses and there are reserved IP addresses that can be used for specific purposes.

Internet Assigned Numbers Authority (IANA)

- They are responsible for global coordination of the Internet Protocol (IP) addressing systems, as well as the Autonomous System Numbers used for routing Internet traffic:
  - AFRINIC: Africa Region
  - APNIC: Asia/Pacific Region
  - ARIN: Canada, USA, and some Caribbean Islands
  - LACNIC: Latin America and some Caribbean Islands
  - RIPE NCC: Europe, the Middle East, and Central Asia

Network Layer Internet Protocol (IP) Header

- There are two versions of the IP header currently in use:
  - IP Version 4 (IPv4)
  - IP Version 6 (IPv6)
- This begs the question - what happened to IPv5?
  - IP Version 5 (IPv5) was an experimental protocol developed in the 1980s and was never widely deployed.

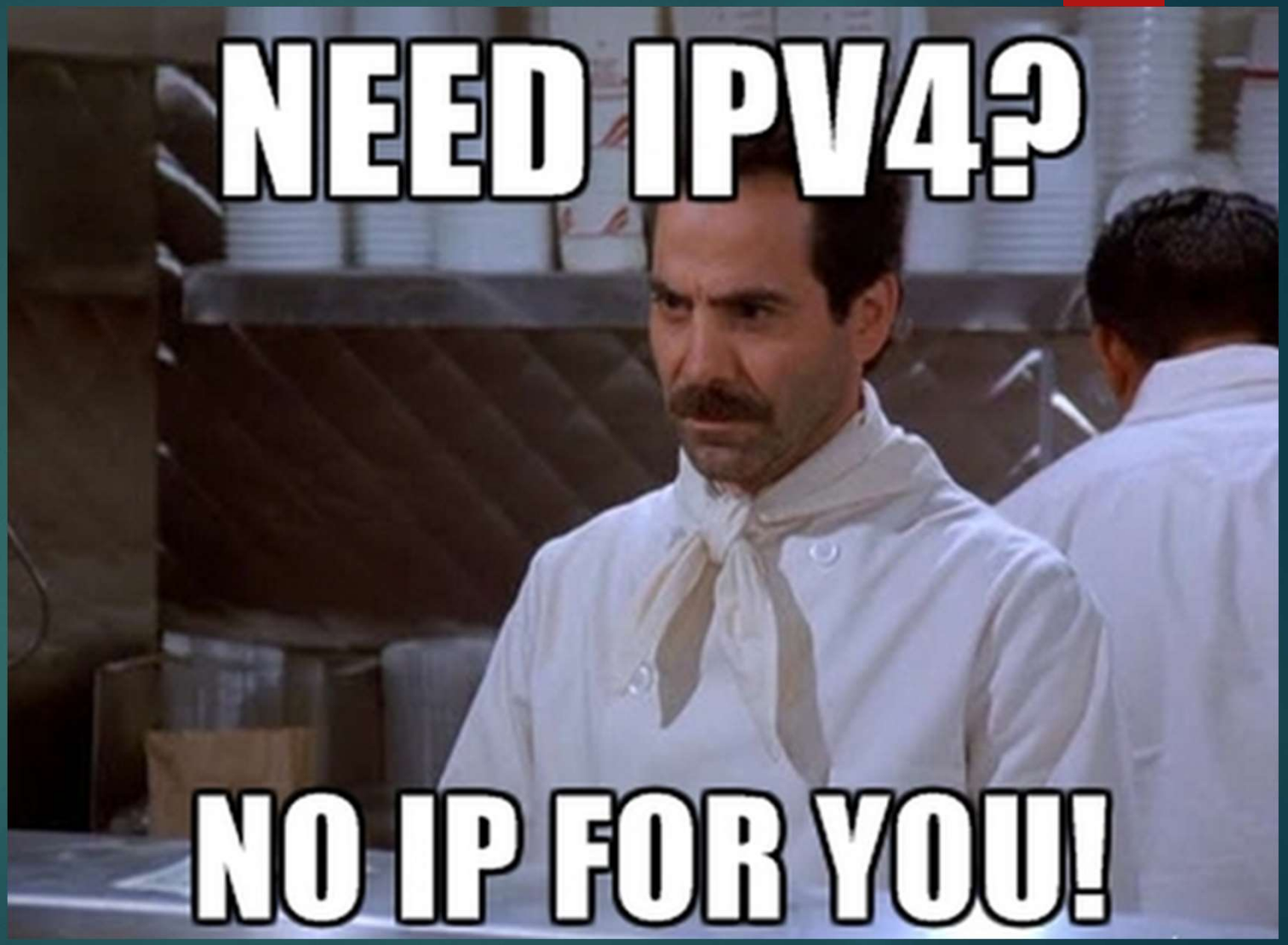
IPv4 Overview

- IPv4 uses 32-bit addresses which limits the address space to 4,294,967,296 (2^{32}) or about 4.3 billion addresses.
- IPv4 addresses may be represented in any notation expressing a 32-bit integer value.
- They are most often written in **dot-decimal notation**, which consists of four octets (8 bits, 0 to 255) of the address expressed individually in decimal numbers and separated by periods.
- For example, dot-decimal IP address 192.0.2.235 represents the 32-bit decimal number 3,221,226,219, which in hexadecimal format is 0xC00002EB. Hexadecimal is a numbering system using a base 16, i.e. digit 0, 1, 2, ..., 9, A, B, C, D, E and F.

IPv4 Address Space Exhaustion (also known as IPcalypse)

- In the 1980s, it became apparent that the pool of available IPv4 addresses was depleting at a rate that was not initially anticipated in the original design of the Internet protocol in the 1970s.
- The main market forces that accelerated address depletion included the rapidly growing number of Internet users, who increasingly used mobile computing devices, such as laptop computers, personal digital assistants (PDAs), and smart phones with IP data services.
- Starting in the 1990s, it started to get real bad...

On 24 September 2015 American Registry for Internet Numbers (ARIN) declared exhaustion of the ARIN IPv4 addresses pool.



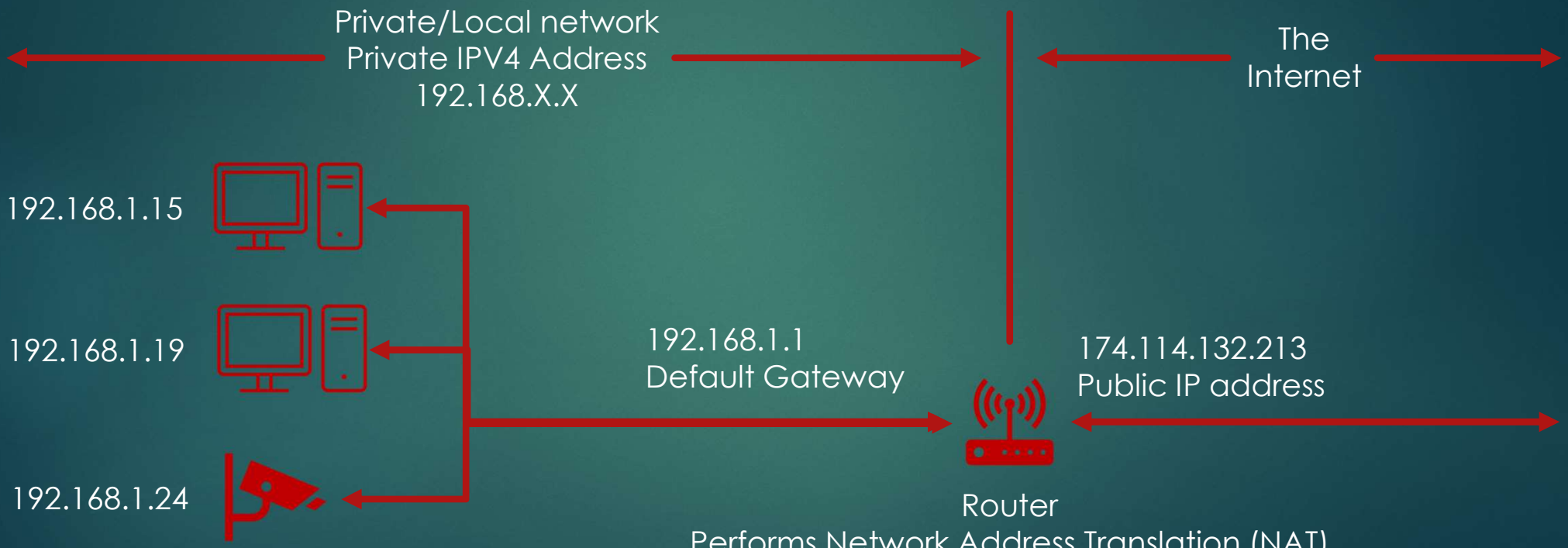
Solutions to IPcalypse

- The threat of exhaustion motivated the introduction of:
  - In 1996 - RFC1918 Private address and Network Address Translation (NAT):
    - More on Private address and NAT on the next few slides.
    - NAT breaks the end-to-end principle.
  - In 2012 - IPv6

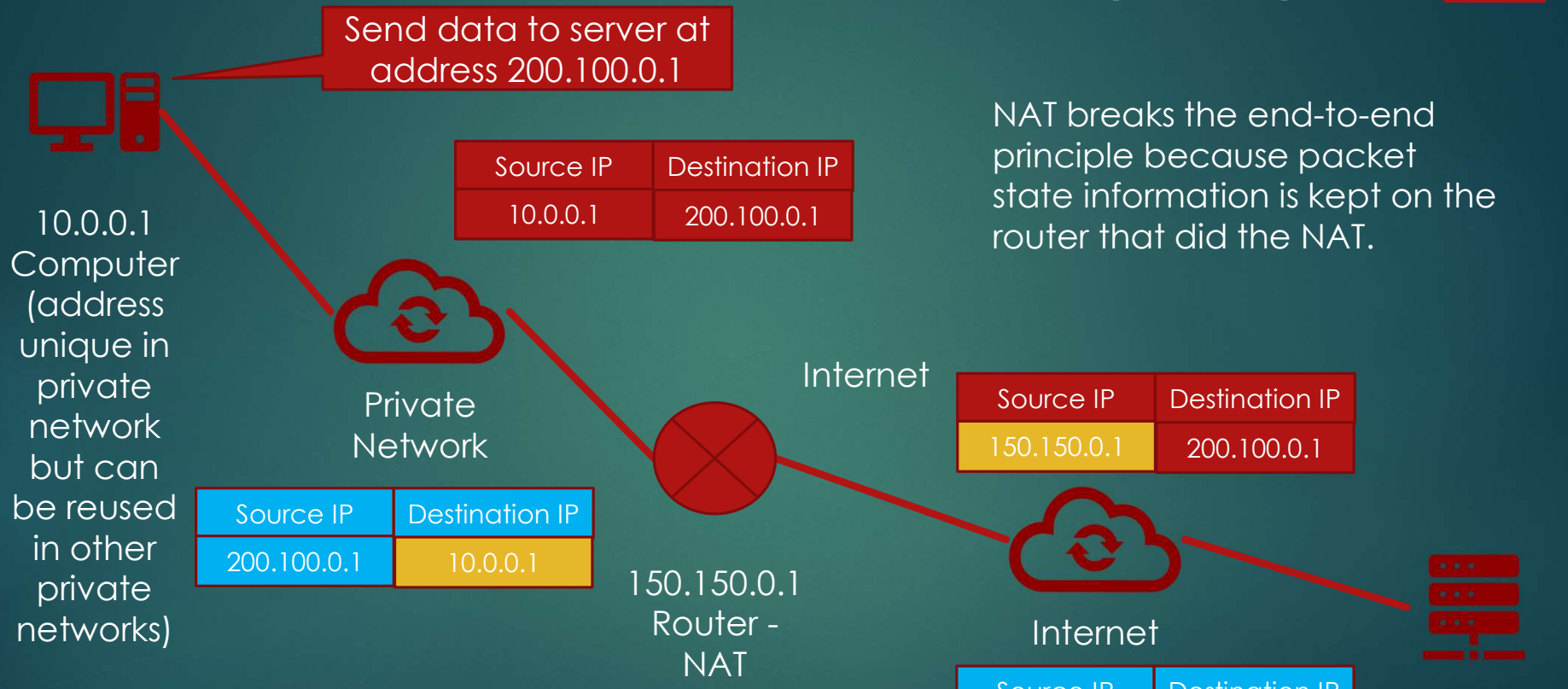
Private versus Public IPv4 addresses

Private IPv4 Address	Public IPv4 Address
Private IP address ranges: 10.0.0.0 to 10.255.255.255 (very large network) 172.16.0.0 to 172.31.255.255 (large) 192.168.0.0 to 192.168.255.255 (medium)	Any IP address not included in the reserved private IP address ranges
Free	Not free
Assigned by your network device (e.g. WIFI router) to your specific device within a private network	Assigned and controlled by your Internet Service Provider (ISP) or IANA
Found via your device's internal settings	Found by Googling: "What is my IP address?"
A non-unique address that may be reused by other devices in other private networks	A unique address never reused by other devices on the internet

Example of IPv4 Private versus Public IP addresses



Network Address Translation (NAT)



NAT breaks the end-to-end principle because packet state information is kept on the router that did the NAT.

Router modify the packet, keep log of source address and port (source generate random port), and destination address and port

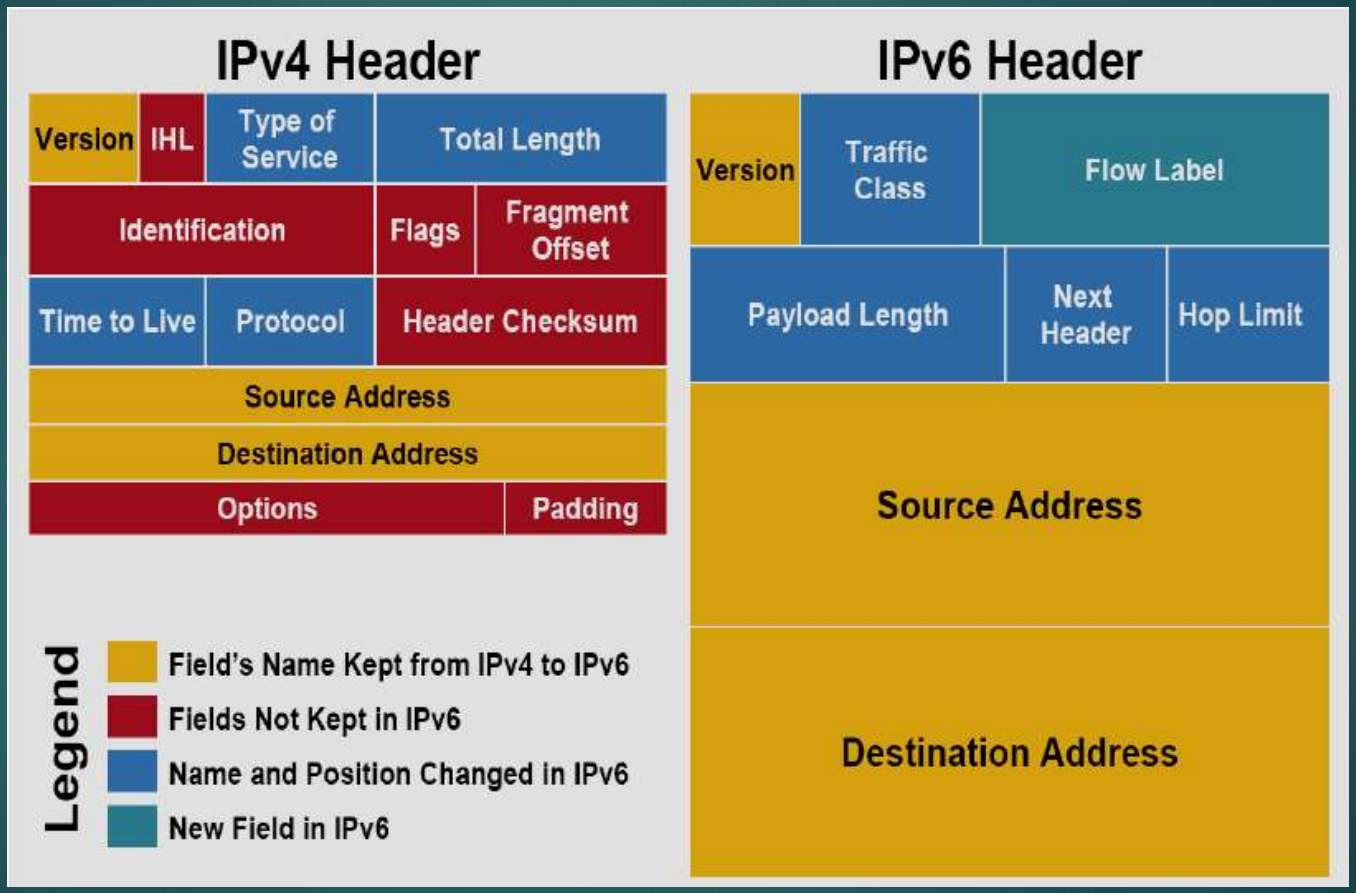
IPv6 Overview

- Instead of using 32 bits address like in the IPv4, IPv6 uses 128 bits address.
- IPv6 has 2^{128} addresses, so 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses
- An IPv6 address has the following format: **y:y:y:y:y:y:y:y** where y is called a segment (8 segments in total) and can be any **lower case hexadecimal** value between 0 and ffff (16 bits). The segments are separated by colons - not periods. Example of an IPv6 address is 2001:0db8:85a3:0000:0000:0000:0370:7334.
- Shortening IPv6 addresses:
  - Omit Leading zeros in group:
    - 2001:0db8:85a3:0000:0000:0000:0370:7334 to 2001:db8:85a3:0:0:0:370:7334
  - Zero Compression, a double colon (::) can replace a single, contiguous string **of one or more groups** consisting of all 0s. It can only be used once:
    - 2001:db8:85a3:0:0:0:370:7334 to 2001:db8:85a3::370:7334

IPv6 Overview Cont'd

- A % followed by a string added to an IPv6 address is called the scope ID. This is used to identify the interface to which a local address belongs. Example:
  - 2001:db8:85a3::370:7334%3
  - Windows uses the scope ID in its IPv6 addresses
- IPv6 address space corresponds to 655,570,793,348,866,943,898,599 addresses for every square meter of the Earth's surface.
- For IPv4, it is one address per 125,729 square meter.
- About 80% of the IPv6 address space has not been allocated.

IPv4 Header versus IPv6 Header

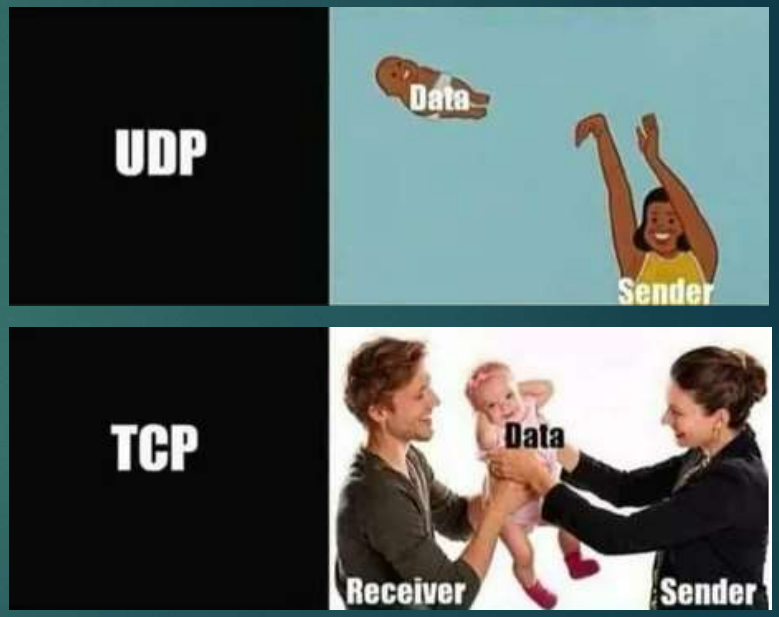


Layer 3 - Transport Layer

MAINTAINS END-TO-END COMMUNICATIONS ACROSS THE NETWORK

Transport Layer Protocols

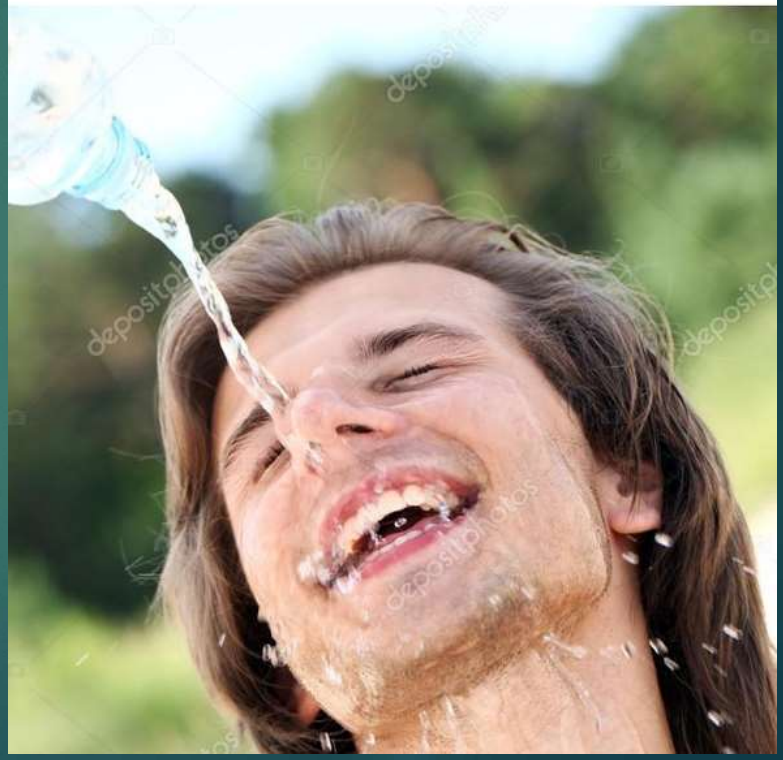
- The Transport Layer typically utilizes two major protocols to move information:
  - User Datagram Protocol (UDP)
  - Transmission Control Protocol (TCP)
- UDP is a connectionless protocol that **contains no reliability, flow-control, or error-recovery functions**. Because of its simplicity, UDP headers contain fewer bytes and consume less network overhead than TCP.
- TCP is a connection-oriented protocol that provides **full-duplex, acknowledged, and flow-controlled service to upper-layer protocols**. It moves data in a stream of data packets. Sequence numbers identify packets within that stream. TCP can also support numerous simultaneous upper-layer conversations.



Another way to look at TCP versus UDP

TCP

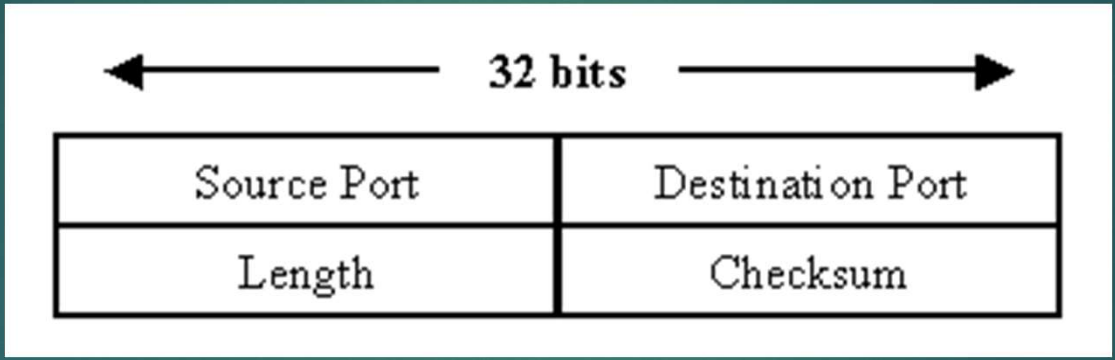
UDP



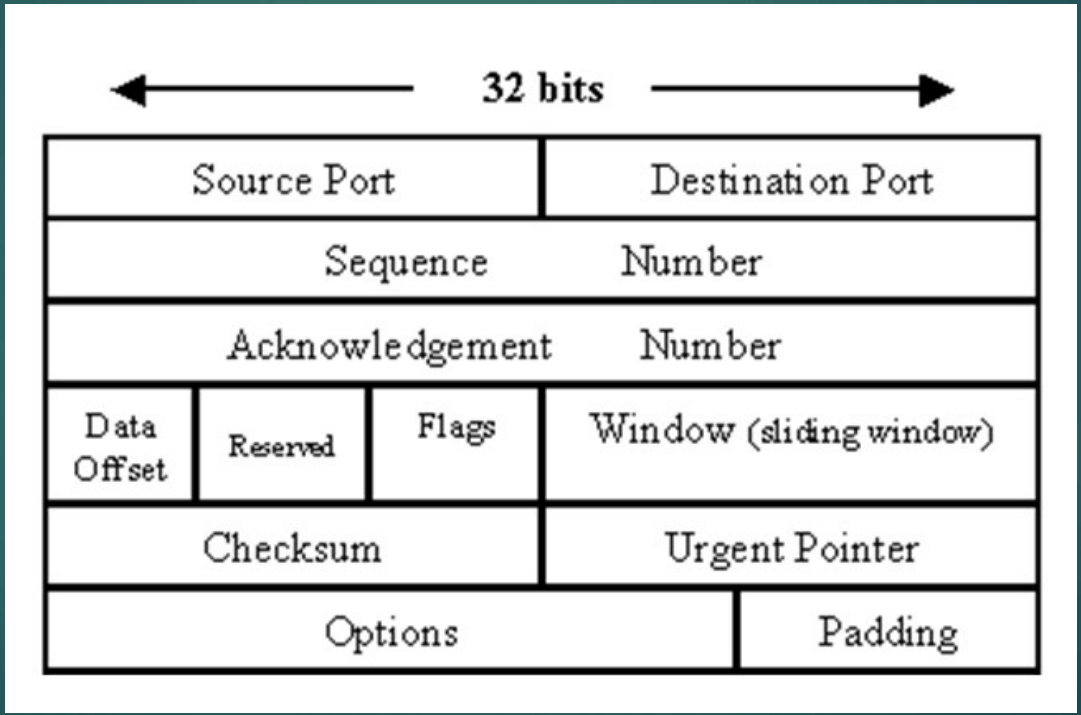
Ports and sockets

- A port is a number used to uniquely identify a transaction over a network by specifying both the host, and the service. They are necessary to differentiate between many different services, such as web service (HTTP), mail service (SMTP), file transfer (FTP), and many more.
- To connect to a server, you need its IP address and also need to indicate which service you want to communicate with, so that the data is sent to the appropriate application. The port number serves to uniquely identify that service on a particular host.
- A port number uses 16 bits and so can therefore have a value from 0 to 65,535 decimal.
- For example, the HTTP protocol uses port 80.
- A socket is the combination of an IP address plus a port number.

The Transport Layer User Datagram Protocol (UDP) Header



The Transport Layer Transmission Control Protocol (TCP) Header

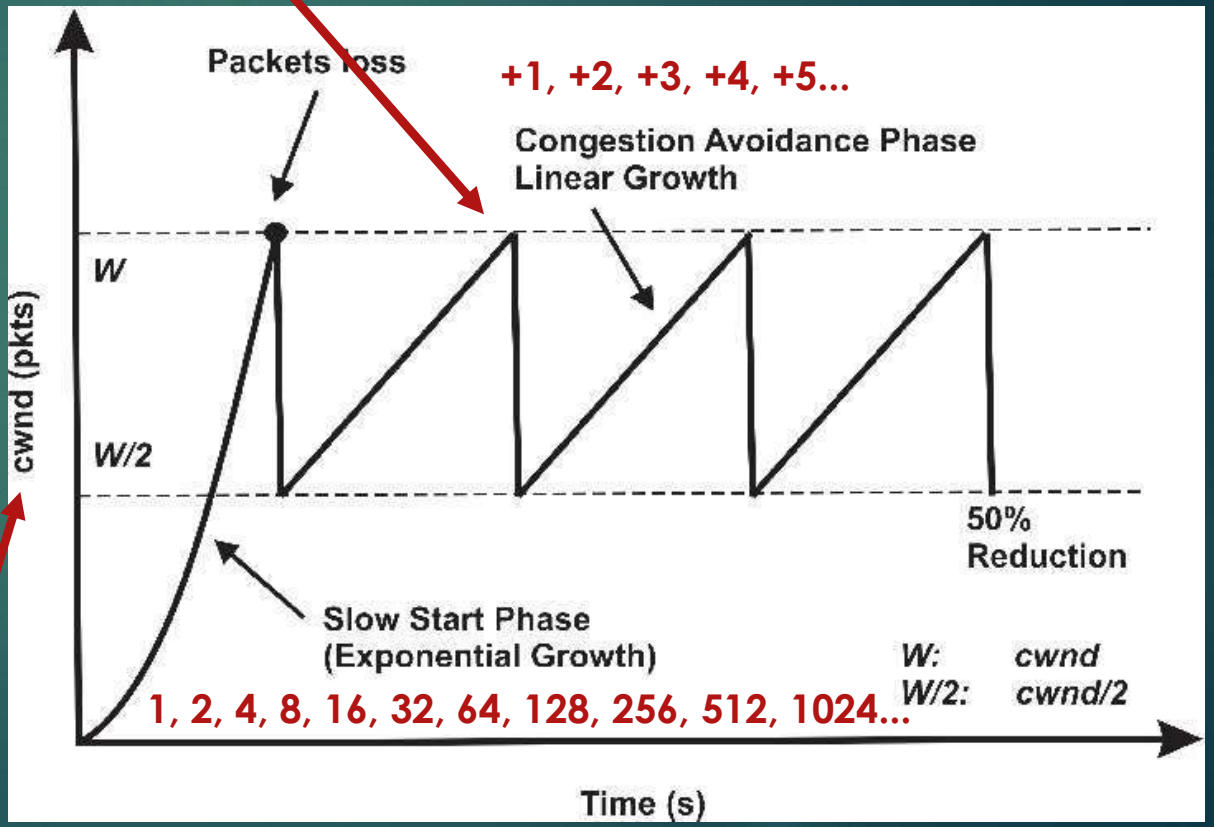


TCP Slow Start

- Why is my download speed not constant?
  - It is because of the TCP slow start algorithm.
- TCP slow start is an algorithm which balances the speed of a network connection. Slow start gradually increases the amount of data transmitted until it finds the network's maximum carrying capacity and then reduces the amount of data by 50%.

cwnd means Congestion Window

In real life, this value is probably not the same all the time, it varies with the network conditions.



Layer 4 - Application

PROVIDES APPLICATIONS WITH STANDARDIZED DATA EXCHANGE

Application protocols

- There are many application protocols and only three are going to be briefly presented:
  - Hypertext Transfer Protocol (HTTP)
  - Domain Name System (DNS)
  - Dynamic Host Configuration Protocol (DHCP)

Hypertext Transfer Protocol (HTTP)

- The Hypertext Transfer Protocol (HTTP) is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems.
- HTTP is the foundation of data communication for the World Wide Web (WWW), where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.
- Development of HTTP was initiated by Tim Berners-Lee at CERN in 1989 and summarized in a simple document describing the behavior of a client and a server using the first HTTP protocol version.
- Its secure variant named HTTPS is used by more than 79% of websites (as of May 2022).

HTTP Transaction Example

Request

GET / HTTP/1.1

Host: www.example.com

User-Agent: Mozilla/5.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-GB,en;q=0.5

Accept-Encoding: gzip, deflate, br

Connection: keep-alive

Reply

HTTP/1.1 200 OK

Date: Mon, 23 May 2005 22:38:34 GMT

Content-Type: text/html; charset=UTF-8

Content-Length: 155

Last-Modified: Wed, 08 Jan 2003 23:11:55 GMT

Server: Apache/1.3.3.7 (Unix) (Red-Hat/Linux)

ETag: "3f80f-1b6-3e1cb03b"

Accept-Ranges: bytes

Connection: close

```
<html>
  <head>
    <title>An Example Page</title>
  </head>
  <body>
    <p>Hello World, this is a very simple HTML document.</p>
  </body>
</html>
```

There are many other HTML tags such as tags that link to another web page, display an image, etc.

Domain Name System (DNS)

- The IP protocols use numerical addresses.
- Domain Name System (DNS) map human-friendly domain names to the numerical IP addresses computers need to use the internet.
- An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses.
- For example, the domain name www.example.com translates to the addresses IPv4 93.184.216.34 and IPv6 2606:2800:220:1:248:1893:25c8:1946.
- The DNS can be quickly and transparently updated, allowing a service's location on the network to change without affecting the end users, who continue to use the same hostname.

Dynamic Host Configuration Protocol (DHCP)

- The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks **for automatically assigning IP addresses and other communication parameters** to devices connected to the network.
- This how your cable modem gets its Public IP address and other parameters from your ISP and your network devices (e.g., computer, camera, etc.) get their Private IP addresses and other parameters from your router.
- This technology eliminates the need for individually configuring network devices manually, and consists of two network components, a centrally installed network DHCP server and client instances of the protocol stack on each computer or device.
- When connected to the network, and periodically thereafter, a client requests a set of parameters from the DHCP server using the DHCP protocol.

Miscellaneous Network Topics

Miscellaneous Network Topics

- TCP/IP versus the Open Systems Interconnection (OSI) model
- How does the internet handles IPv4 and IPv6?
- Does IPv6 needs NAT?
- Should I turn on both IPv4 and IPv6?
- What is a Temporary IPv6 Addresses?
- What is a Link-local IPv6 Address?
- How to tell if my Windows computer is using IPv4 or IPv6, or both?
- Trace Route – a fun command to try

TCP/IP versus the Open Systems Interconnection (OSI) model

TCP/IP Model	OSI Model
4. Application	7. Application
	6. Presentation
	5. Session
3. Transport	4. Transport
2. Network	3. Network
1. Link	2. Data-Link
	1. Physical

How does the internet handles IPv4 and IPv6?

- IPv4/IPv6 co-existence can take one of three forms:
  - **Dual stacks**: where your network hardware runs IPv4 and IPv6 simultaneously, Windows uses this method.
  - **Tunnel one protocol within another**: this means taking IPv6 packets and encapsulating them in IPv4 packets or vice versa.
  - **Network Address Translation-Protocol Translation (NAT-PT)**: software or a device translates IPv6 packets into IPv4 packets.
- With dual stacks, your computers, routers, switches, and other devices run both protocols, but IPv6 will be the preferred protocol.
- The downside of using IPv6 is that most legacy networking hardware, servers and software don't support IPv6.

Does IPv6 needs NAT?
Should I turn on both IPv4 and IPv6?

- Does IPv6 needs NAT?
  - No, IPv6 native connectivity can exist between nodes on both private networks behind firewalls as well as across the Internet.
- Should I turn on both IPv4 and IPv6?
  - Yes, it is better to keep both IPv4 and IPv6 addresses enabled. However, you may have IPv6 connectivity to the internet, but the host you are trying to reach does not. The Windows application will figure this out while using the DNS and fallback to IPv4, but there will be a few seconds delay. If this happen often, you may want to disable IPv6 on your router and Windows will use IPv4.
  - As of March 2022, according to Google, the IPv6 adoption rate globally is around 34%, but in the U.S. it's at about 46%. Carrier networks and ISPs have been the first group to start deploying IPv6 on their networks, with mobile networks leading the charge.

What is a Temporary IPv6 Addresses?

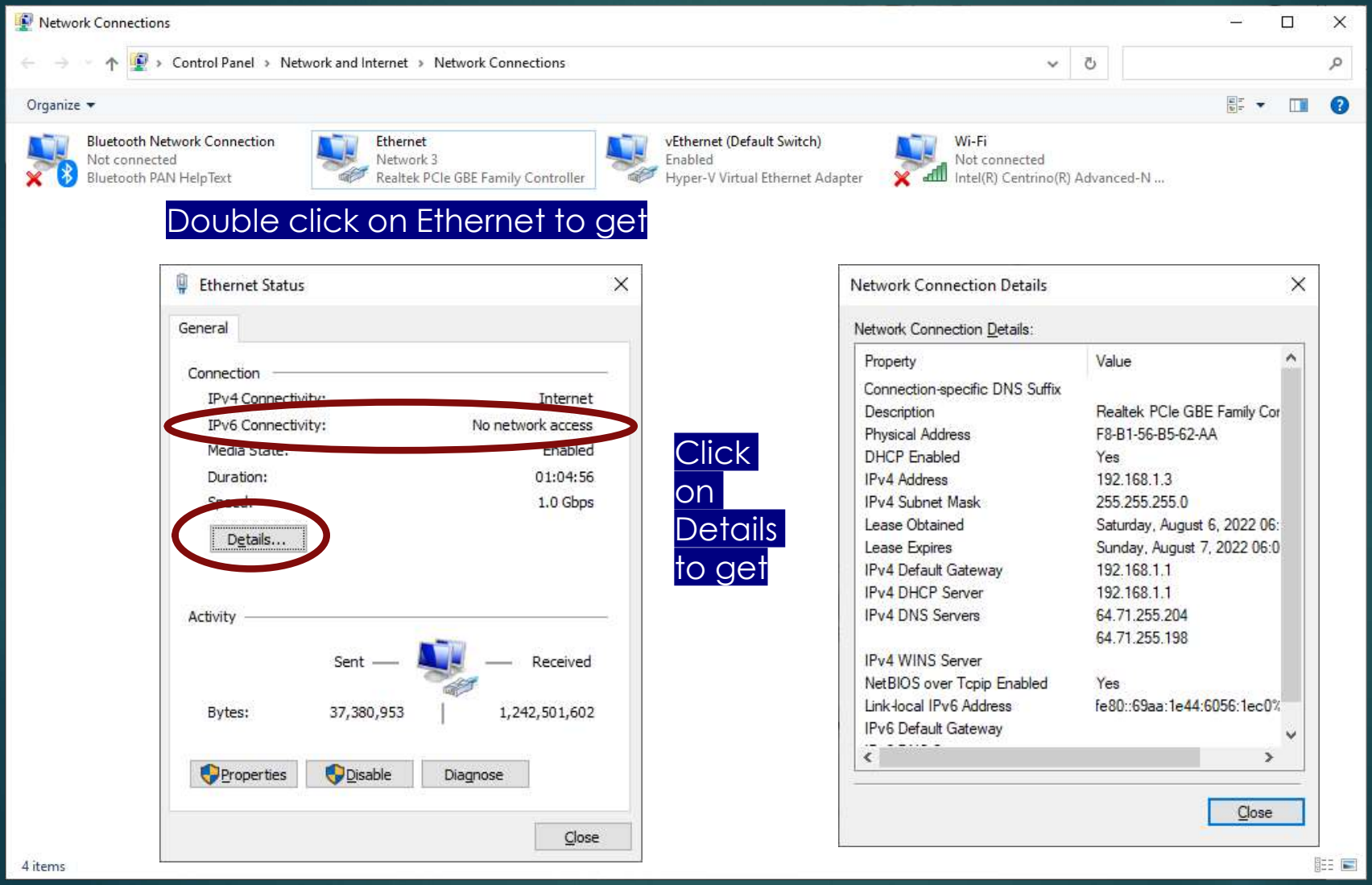
- A temporary IPv6 address includes a randomly generated 64-bit number as the interface ID, instead of an interface's Media Access Control (MAC) address.
- You can use temporary addresses for any interfaces on an IPv6 node that you want to keep anonymous.
- It's completely normal to have multiple IPv6 addresses on one device. A device generates new 64 bits every once in a while and uses that in the IPv6 address.
- Because new addresses are generated regularly the addresses are marked as temporary interfaces.

What is a Link-local IPv6 Address?

- IPv6 link-local addresses are addresses that can be used to communicate with nodes (hosts and routers) on an attached link. Packets with those addresses are not forwarded by routers.
- Link-local addresses are designed to be used for addressing on a single link for purposes such as automatic address configuration, neighbor discovery, or in the absence of routers. It also may be used to communicate with other nodes on the same link.
- A link-local address is automatically assigned.

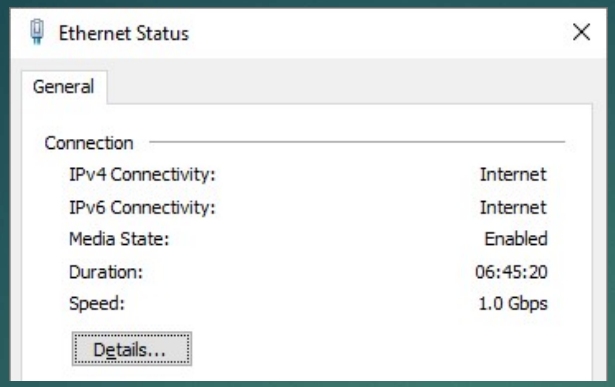
How to tell if my Windows computer is using IPv4 or IPv6, or both?

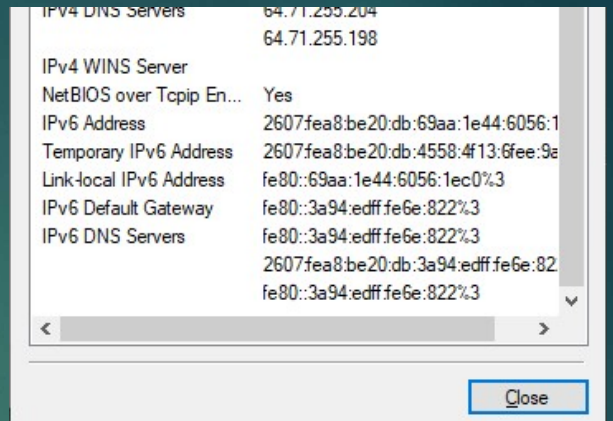
- If IPv6 is not available, Windows will use IPv4.
- If both IPv4 and IPv6 are available, IPv6 will be used first.
- How to tell if Windows has IPv4 and IPv6 connectivity to the Internet:
  - Click the Windows Start menu, click search.
  - Type ncpa.cpl and click it in the list of found items.
  - You should get a windows similar to the one shown on the next slide.

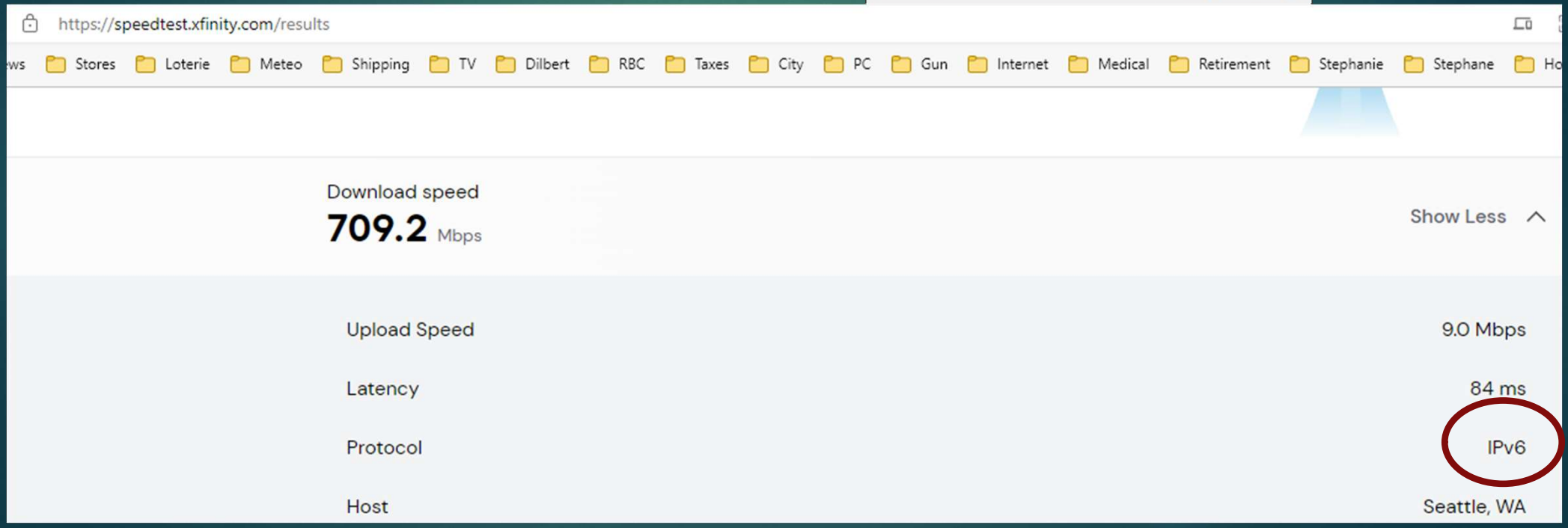


I have an IPv6 address, but no IPv6 connectivity to the Internet. It was working before, but I recently change my WIFI router to a Netgear Orbi. I checked the router settings and discovered that its default setting is to have IPv6 disabled.

After getting from Rogers the settings for my Netgear Router to enable IPv6, I am getting this status (no PC or router reboots):

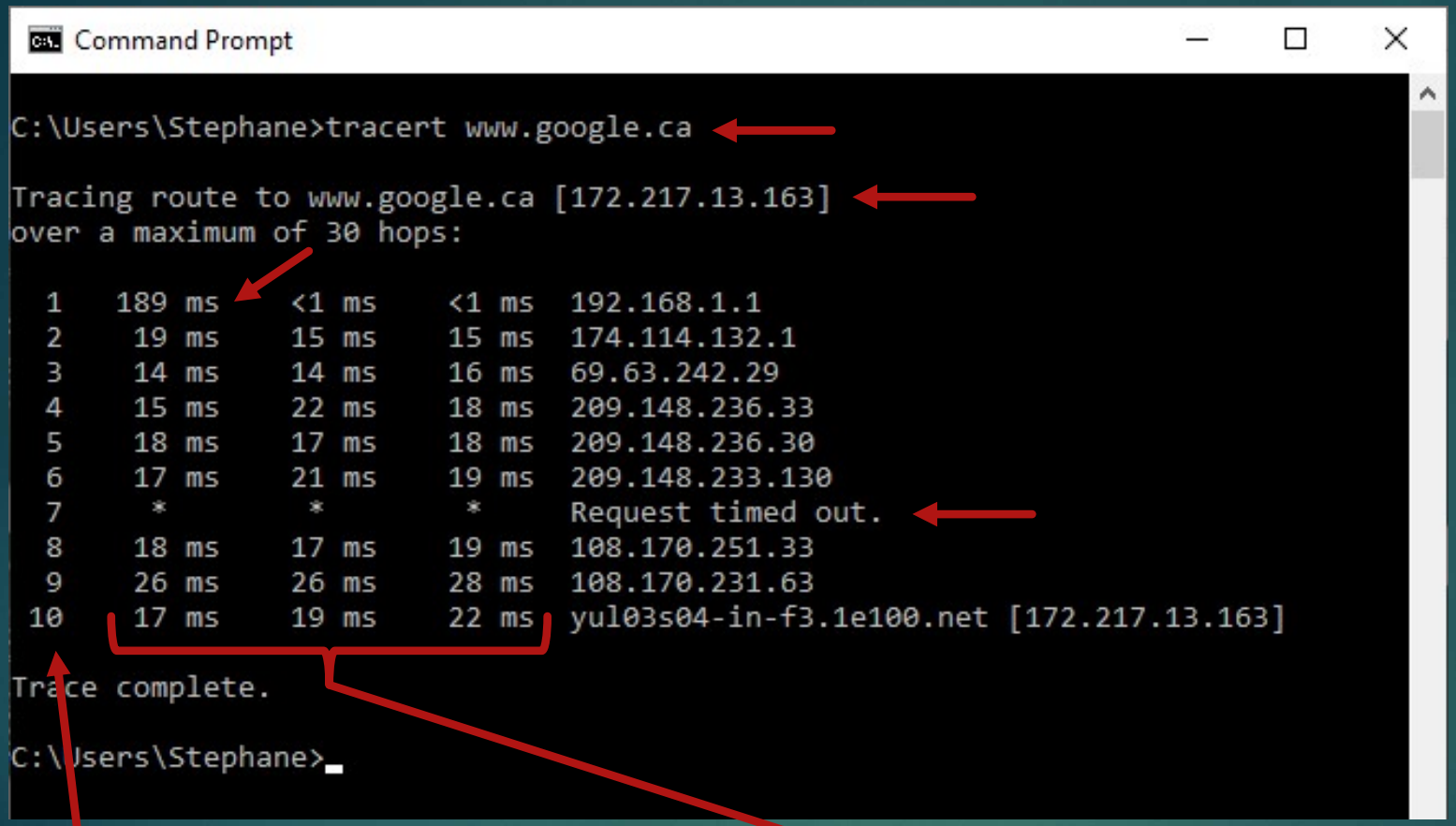






Trace Route – a fun command to try

- Open a Windows Command Prompt.
- In the Command Prompt window, type 'tracert' followed by the destination, either an IP Address or a Domain Name, and press Enter.
- The command will return the hops discovered to reach the destination and for each hop will return the IP address and transit time (in milliseconds).
- Fun story: More than 25 years ago, I was using my Ottawa FreeNet account to access my work account, **both physically located in Ottawa**:
  - The communication was very slow.
  - I used the trace route command and discovered that my data packets were travelling to Montreal, Washington DC, Boston, Toronto...
- Lets find out the output of tracert for my computer to connect to www.google.ca.



You can use the web page https://www.iplocation.net/ip-lookup to get information about an IP address. For example, 172.217.13.163 is owned by Google LLC and is located in Mountain View California. So, while the URL ends with .ca, the physical server is in the US.

Hop #

The next three columns display the round trip time (RTT) for your packet to reach that point and return to your computer. There are three columns because the traceroute sends three separate signal packets. This is to display consistency, or a lack thereof, in the route.

After listening to this presentation, you should be able to understand this discussion between a manager and an employee…

You should recognize this address as a Public IPv4 Address

127.0.0.1 is the IP address of the local computer. This IP address allows the machine to connect to and communicate with itself. Therefore, localhost (127.0. 0.1) is used to establish an IP connection to the same device used by the end-user.

It is not an IPv4 nor IPv6 address. It is a Media Access Control (MAC) address which is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment. The format is six groups of two hexadecimal digits.


Any
Questions