./



GENESIS – Networking Learning Report

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver. Rel. No.** | **Release Date** | **Prepared. By** | **Reviewed By** | **To be Approved** | **Remarks/Revision Details** |
| 1.0 | 21-12-20 | 1. Megha Annie George |  | Srinivas K |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Details**

**Contents**

[List of Figures 4](#_Toc59403535)

[List of Tables 4](#_Toc59403536)

[1 NETWORKING CONCEPTS 5](#_Toc59403537)

[1.1 NETWORK TOPOLOGIES 5](#_Toc59403538)

[1.1.1 MESH TOPOLOGY 5](#_Toc59403539)

[1.1.2 STAR TOPOLOGY 6](#_Toc59403540)

[1.1.3 BUS TOPOLOGY 6](#_Toc59403541)

[1.1.4 RING TOPOLOGY 7](#_Toc59403542)

[1.1.5 TREE TOPOLOGY 8](#_Toc59403543)

[1.1.6 HYBRID TOPOLOGY 8](#_Toc59403544)

[1.2 WIRED AND WIRELESS NETWORKS 9](#_Toc59403545)

[1.2.1 PAN 10](#_Toc59403546)

[1.2.2 LAN 11](#_Toc59403547)

[1.2.3 MAN 11](#_Toc59403548)

[1.2.4 WAN 12](#_Toc59403549)

[1.2.5 WLAN 12](#_Toc59403550)

[1.2.6 WI-FI 12](#_Toc59403551)

[1.2.7 WIMAX 13](#_Toc59403552)

[2 COMPONENTS 13](#_Toc59403553)

[2.1 HUB 13](#_Toc59403554)

[2.2 SWITCH 14](#_Toc59403555)

[2.3 ROUTER 14](#_Toc59403556)

[2.4 BRIDGE 14](#_Toc59403557)

[2.5 GATEWAY 15](#_Toc59403558)

[2.6 WIRELESS ACCESS POINTS 15](#_Toc59403559)

[3 PROTOCOLS 16](#_Toc59403560)

[3.1 OSI MODEL 16](#_Toc59403561)

[3.2 TCP 17](#_Toc59403562)

[3.3 UDP 19](#_Toc59403563)

[3.4 INTERNET PROTOCOL 20](#_Toc59403564)

[3.5 L2 PROTOCOLS 21](#_Toc59403565)

[3.6 L3 PROTOCOLS 22](#_Toc59403566)

[4 IP ADDRESSES 23](#_Toc59403567)

[4.1 IPV4 V/S IPV6 23](#_Toc59403568)

[4.2 NETWORK CLASSES IN IPV4 25](#_Toc59403569)

[4.2.1 CLASS A 25](#_Toc59403570)

[4.2.2 CLASS B 25](#_Toc59403571)

[4.2.3 CLASS C 25](#_Toc59403572)

[5 COLLEGE NETWORK 26](#_Toc59403573)

# List of Figures

Figure 1 MESH TOPOLOGY 5

Figure 2 STAR TOPOLOGY 6

Figure 3 BUS TOPOLOGY 6

Figure 4 RING TOPOLOGY 7

Figure 5 TREE TOPOLOGY 8

Figure 6 HYBRID TOPOLOGY 9

Figure 7 NETWORK HIERARCHY 10

Figure 8 PAN NETWORK 11

Figure 9 LAN NETWORK 11

Figure 10 MAN NETWORK 12

Figure 11 WAN NETWORK 12

Figure 12 NETWORK COMPONENTS HIERARCHY 13

Figure 13 HUB 14

Figure 14 SWITCH 14

Figure 15 ROUTER 14

Figure 16 BRIDGE 15

Figure 17 GATEWAY 15

Figure 18 WIRELESS ACCESS POINT 16

Figure 19 OSI MODEL 16

Figure 20 OSI MODEL - DATA UNIT 17

Figure 21 TCP 17

Figure 22 DATA FLOW IN TCP 18

Figure 23 TCP HEADER 18

Figure 24 UDP 19

Figure 25 DATA FLOW IN UDP 19

Figure 26 UDP HEADER 20

Figure 27 DATA FLOW IN INTERNET PROTOCOL SUITE 20

Figure 28 IP HEADER 21

Figure 29 IPV4 V/S IPV6 23

Figure 30 DIFFERENCE BETWEEN IPV4 & IPV6 24

Figure 31 IPV4 & IPV6 HEADER 24

Figure 32 NETWORK CLASSES 26

Figure 33 NETWORK CLASS MASK 26

Figure 34 COLLEGE NETWORK DESIGN 27

Figure 35 PING SCREENSHOT 28

# List of Tables

Table 1 MESH TOPOLOGY 5

Table 2 STAR TOPOLOGY 6

Table 3 BUS TOPOLOGY 7

Table 4 RING TOPOLOGY 8

Table 5 TREE TOPOLOGY 8

Table 6 HYBRID TOPOLOGY 9

Table 7 NETWORK TYPE 10

Table 8 L2 PROTOCOLS 21

Table 9 L3 PROTOCOLS 22

# NETWORKING CONCEPTS

## NETWORK TOPOLOGIES

The arrangement of a network which comprises of nodes and connecting lines via sender and receiver is referred as network topology.

### MESH TOPOLOGY

In mesh topology, every device is connected to another device via a particular channel.

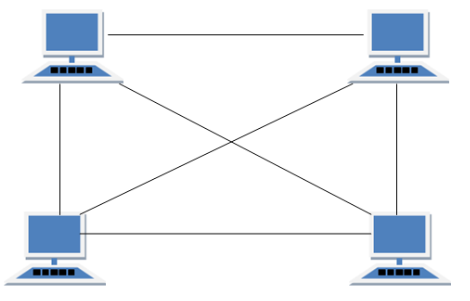


Figure MESH TOPOLOGY

Table MESH TOPOLOGY

|  |  |
| --- | --- |
| ADVANTAGES | DISADVANTAGES |
| * It is robust. * Fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links. * Provides security and privacy. | * Installation and configuration is difficult. * Cost of cables are high as bulk wiring is required, hence suitable for less number of devices. * Cost of maintenance is high. |

### STAR TOPOLOGY

In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node.

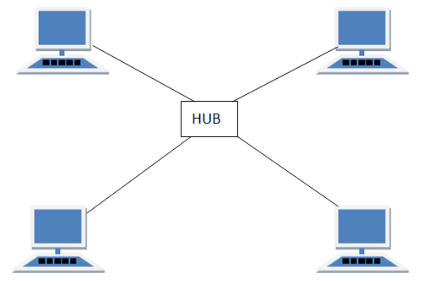


Figure STAR TOPOLOGY

Table STAR TOPOLOGY

|  |  |
| --- | --- |
| ADVANTAGES | DISADVANTAGES |
| * If N devices are connected to each other in star topology, then the number of cables required to connect them is N. So, it is easy to set up. * Each device require only 1 port i.e. to connect to the hub. | * If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down. * Cost of installation is high. * Performance is based on the single concentrator i.e. hub. |

### BUS TOPOLOGY

Bus topology is a network type in which every computer and network device is connected to single cable. No bi-directional feature is in bus topology.

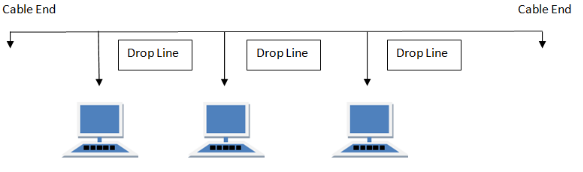


Figure BUS TOPOLOGY

Table BUS TOPOLOGY

|  |  |
| --- | --- |
| ADVANTAGES | DISADVANTAGES |
| * If N devices are connected to each other in bus topology, then the number of cables required to connect them is 1 which is known as backbone cable and N drop lines are required. * Cost of the cable is less as compared to other topology, but it is used to built small networks. | * If the common cable fails, then the whole system will crash down. * If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD etc. |

### RING TOPOLOGY

In this topology, it forms a ring connecting devices with its exactly two neighboring devices. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.

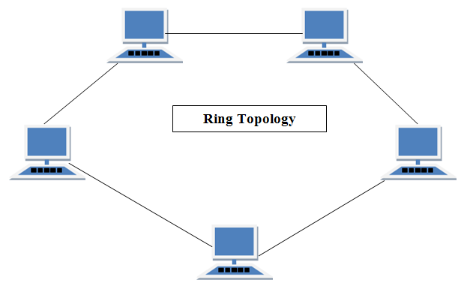


Figure RING TOPOLOGY

Table RING TOPOLOGY

|  |  |
| --- | --- |
| ADVANTAGES | DISADVANTAGES |
| * The possibility of collision is minimum in this type of topology. * Cheap to install and expand. | * Troubleshooting is difficult in this topology. * Addition of stations in between or removal of stations can disturb the whole topology. |

### TREE TOPOLOGY

This topology is the variation of Star topology. This topology has hierarchical flow of data.

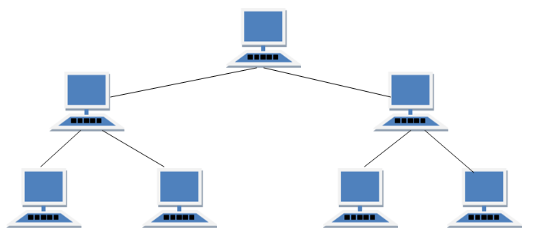


Figure TREE TOPOLOGY

Table TREE TOPOLOGY

|  |  |
| --- | --- |
| ADVANTAGES | DISADVANTAGES |
| * It allows more devices to be attached to a single central hub thus it increases the distance that is travel by the signal to come to the devices. * It allows the network to get isolated and to prioritize from different computers. | * If the central hub gets fails the entire system fails. * The cost is high because of cabling. |

### HYBRID TOPOLOGY

[Hybrid Topology is basically](https://www.educba.com/what-is-a-hybrid-topology/) a network topology comprising of two or more different types of topologies.

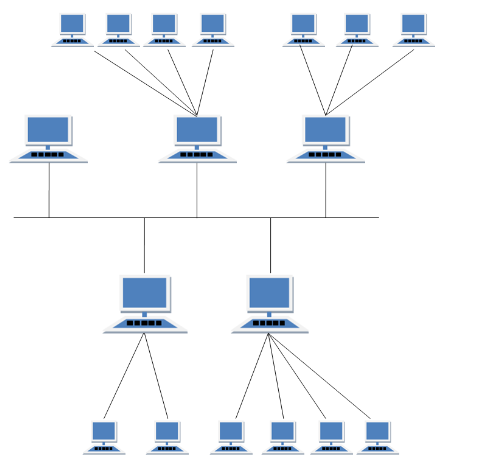


Figure HYBRID TOPOLOGY

Table HYBRID TOPOLOGY

|  |  |
| --- | --- |
| ADVANTAGES | DISADVANTAGES |
| * It is easy to troubleshoot and provides simple error detecting techniques. * It is a flexible network topology, making it quite effective. * It is scalable since the size can be made greater easily. | * If the central hub gets fails the entire system fails. * The cost is high because of cabling. |

## WIRED AND WIRELESS NETWORKS

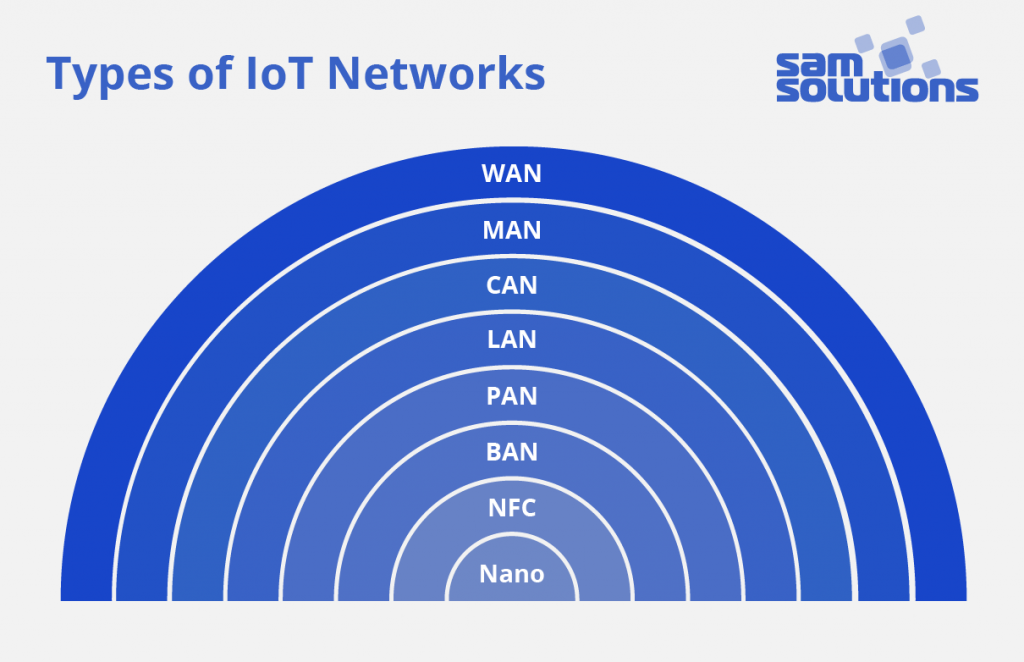


Figure NETWORK HIERARCHY

Table NETWORK TYPE

|  |  |  |  |
| --- | --- | --- | --- |
| NETWORK | SPEED | RANGE | EXAMPLE |
| PAN | 250 Kbps – 24 Mbps | < 10 m | Bluetooth |
| LAN | 100 Mbps / 1 Gbps / 10 Gbps | < 1 Km | Wi-Fi |
| MAN | ~ 50 Mbps | 50 – 100 Km | WiMAX |
| WAN | 20 Mbps / 50 Mbps / 100Mbps | 100 + Km | GSM, GPRS |

### PAN

PAN is a computer network formed around a person. It generally consists of a computer, mobile, or personal digital assistant. PAN can be used for establishing communication among these personal devices for connecting to a digital network and the internet.

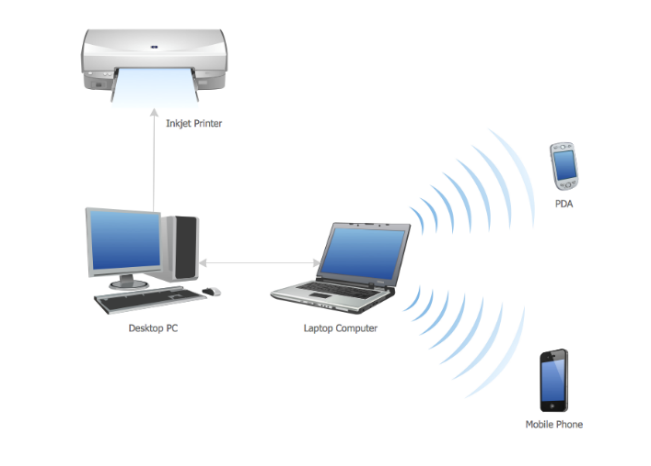


Figure PAN NETWORK

### LAN

A Local Area Network (LAN) is a group of computer and peripheral devices which are connected in a limited area such as school, laboratory, home, and office building. It is a widely useful network for sharing resources like files, printers, games, and other application.

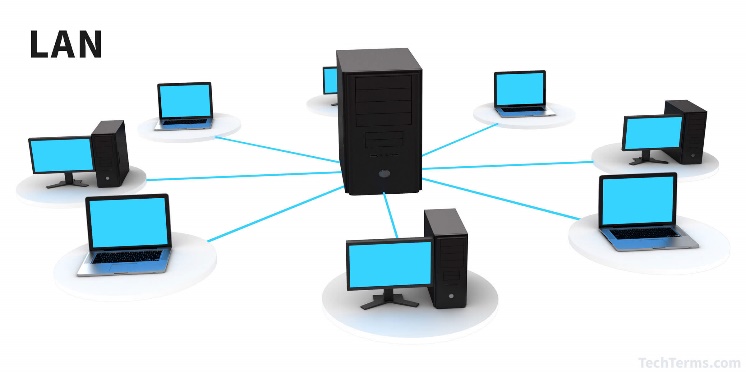


Figure LAN NETWORK

### MAN

A Metropolitan Area Network or MAN is consisting of a computer network across an entire city, college campus, or a small region. Depending upon the type of configuration, this type of network allows you to cover an area from several miles to tens of miles.

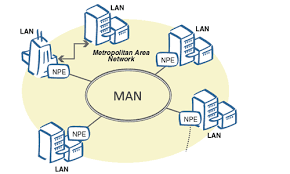


Figure MAN NETWORK

### WAN

WAN (Wide Area Network) is another important computer network that which is spread across a large geographical area. WAN network system could be a connection of a LAN which connects with other LAN's using telephone lines and radio waves. It is mostly limited to an enterprise or an organization.

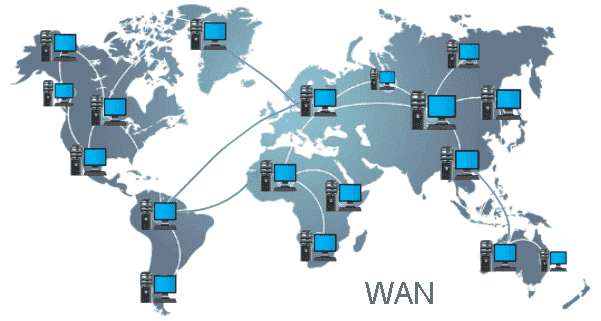


Figure WAN NETWORK

### WLAN

WLAN (Wireless Local Area Network) helps you to link single or multiple devices using wireless communication within a limited area like home, school, or office building. It gives users an ability to move around within a local coverage area which may be connected to the network. Today most modern day's WLAN systems are based on IEEE 802.11 standards.

### WI-FI

WI-FI is a family of [wireless network](https://en.wikipedia.org/wiki/Wireless_network) [protocols](https://en.wikipedia.org/wiki/Communication_protocol), based on the [IEEE 802.11](https://en.wikipedia.org/wiki/IEEE_802.11) family of standards, which are commonly used for [local area networking](https://en.wikipedia.org/wiki/Wireless_LAN) of devices and [Internet](https://en.wikipedia.org/wiki/Internet) access.

### WIMAX

Acronym for Worldwide Interoperability for Microwave Access. Based on Wireless MAN technology. A wireless technology optimized for the delivery of IP centric services over a wide area. A scalable wireless platform for constructing alternative and complementary broadband networks. A certification that denotes interoperability of equipment built to the IEEE 802.16 or compatible standard.

# COMPONENTS

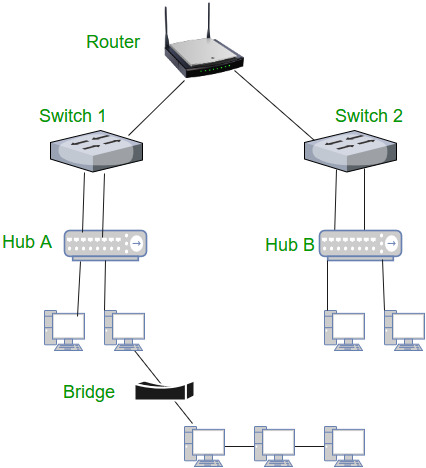


Figure NETWORK COMPONENTS HIERARCHY

## HUB

A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped. Hub consumes more bandwidth.



Figure HUB

## SWITCH

A switch is a hardware device that connects multiple devices on a computer network. The Switch contains the updated table that decides where the data is transmitted or not. Switch delivers the message to the correct destination based on the physical address present in the incoming message. A Switch does not broadcast the message to the entire network like the Hub. It increases the speed of the network.



Figure SWITCH

## ROUTER

A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network based on the information available in the routing table. A router works in a Layer 3 (Network layer) of the OSI Reference model. It determines the best path from the available paths for the transmission of the packet.



Figure ROUTER

## BRIDGE

A bridge interconnects two networks using the same technology (such as Ethernet or Arc net). A modern bridge reads the destination address of the received packet and determines whether the address is on the same segment of the network cables of the originating station. If the destination is on the other side of the bridge, the bridge transmits the packet into the traffic on that cable segment. Local bridges are used to connect two segments of the same LAN. Remote bridges are used to link local LAN cables to thin long-distance cables to link two physically separated network. Bridges are easy to install.



Figure BRIDGE

## GATEWAY

Two different networks can be connected using a gateway. For example, a [mainframe](https://ecomputernotes.com/fundamental/introduction-to-computer/mainframe) can be connected and accessible to a PC network using a gateway. Unlike routers, a gateway converts the format of the data sent between two networks. A router adds only addressing [information](https://ecomputernotes.com/fundamental/information-technology/what-do-you-mean-by-data-and-information) to the data packet. Routers never change the content of the message. However, a gateway identifies the protocols used in the networks, and recognize the data format and convert the message format into a suitable format to be accepted by the other network. Wide area networks often use gateways because there is many different networks present in a WAN.



Figure GATEWAY

## WIRELESS ACCESS POINTS

In [computer networking](https://en.wikipedia.org/wiki/Computer_networking_device), a wireless access point (WAP), or more generally just access point (AP), is a [networking hardware](https://en.wikipedia.org/wiki/Networking_hardware) device that allows other [Wi-Fi](https://en.wikipedia.org/wiki/Wi-Fi) devices to connect to a wired network. The AP connects to a [router](https://en.wikipedia.org/wiki/Router_(computing)) (via a wired network) as a standalone device, but it can also be an integral component of the router itself. An AP is differentiated from a [hotspot](https://en.wikipedia.org/wiki/Hotspot_(Wi-Fi)) which is a physical location where Wi-Fi access is available.



Figure WIRELESS ACCESS POINT

# PROTOCOLS

## OSI MODEL

OSI stands for Open Systems Interconnection. It is a 7-layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

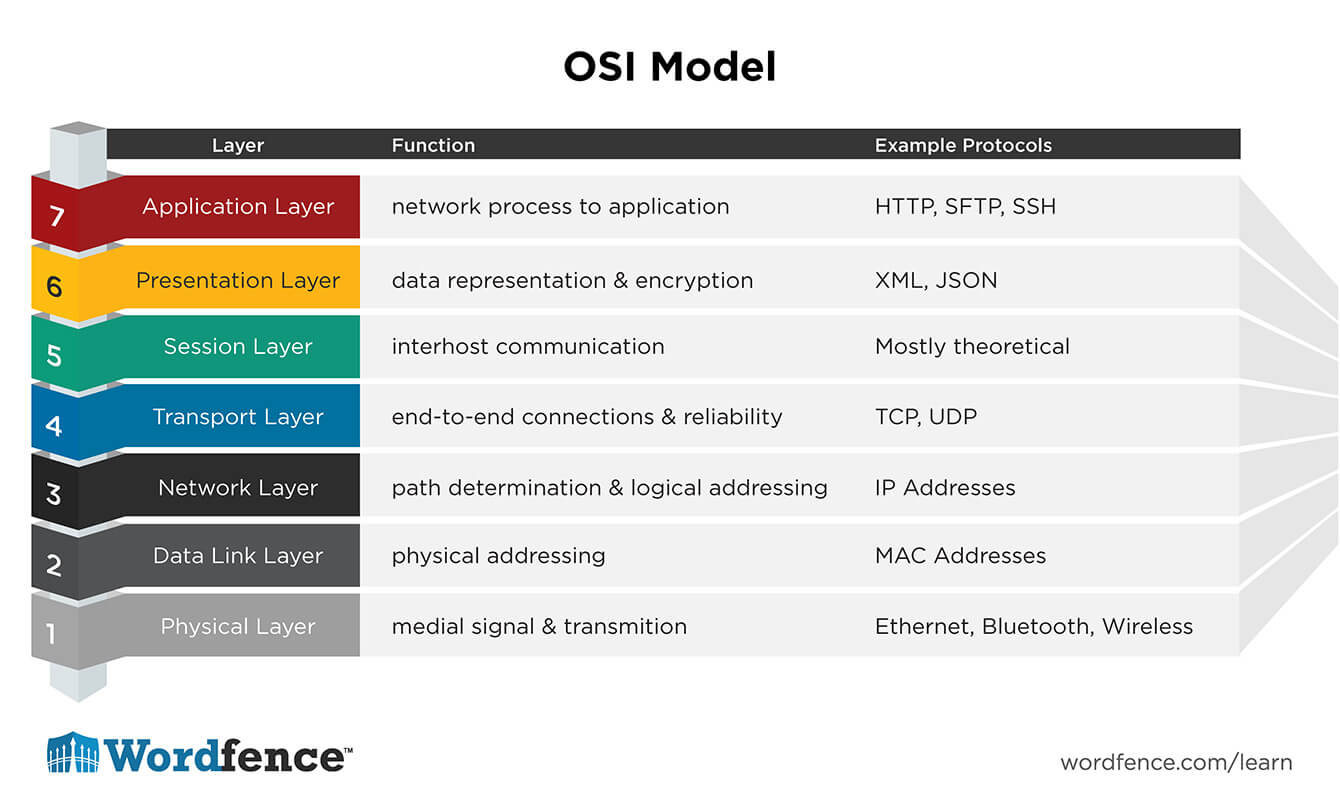


Figure OSI MODEL

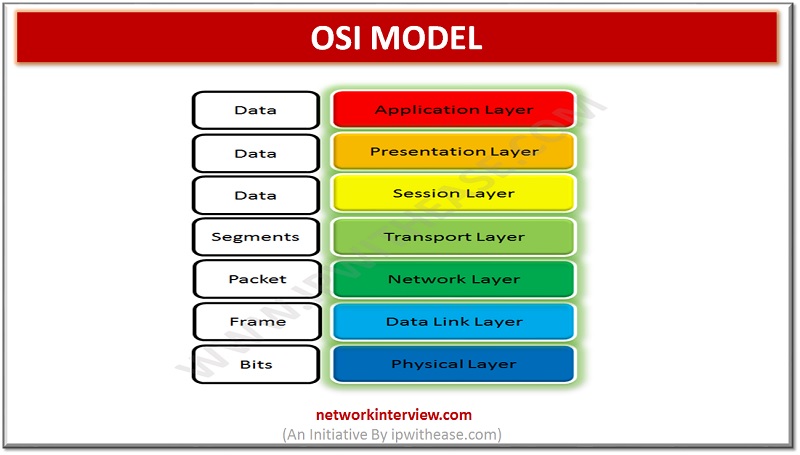


Figure OSI MODEL - DATA UNIT

## TCP

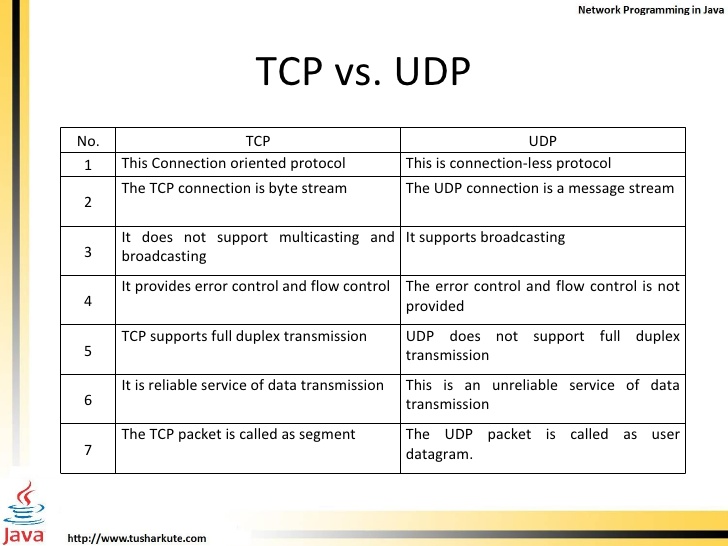


Figure TCP

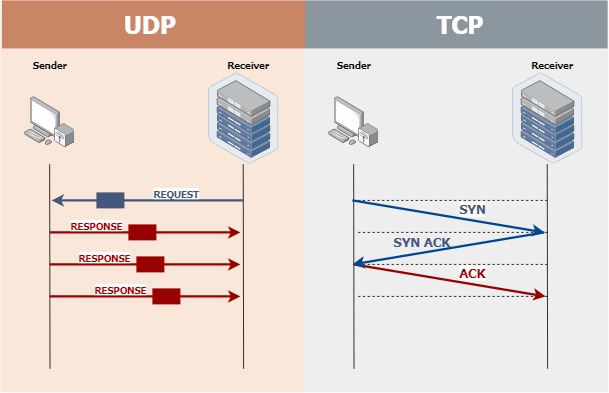


Figure DATA FLOW IN TCP

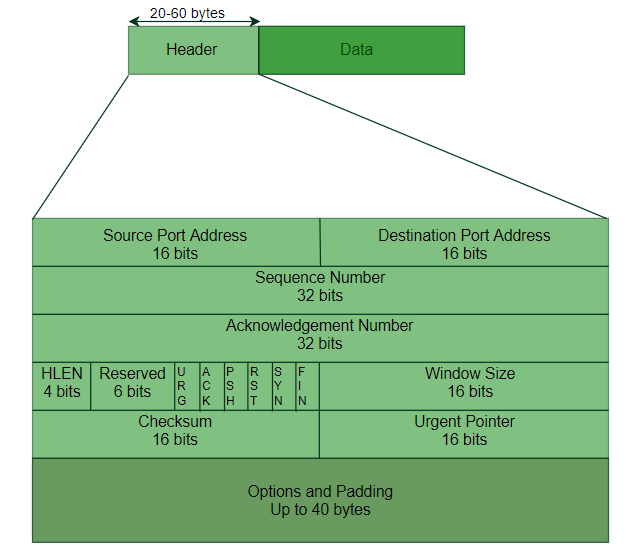


Figure TCP HEADER

## UDP

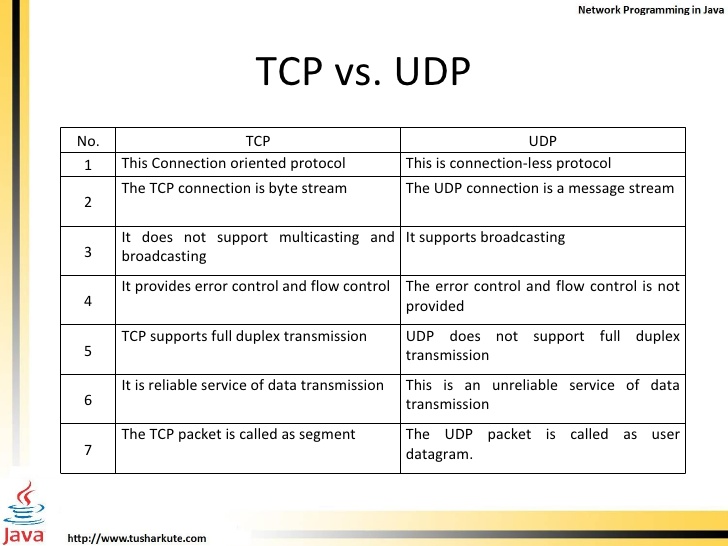


Figure UDP

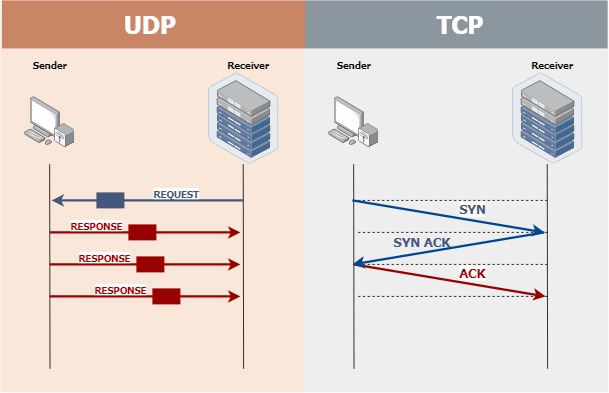


Figure DATA FLOW IN UDP

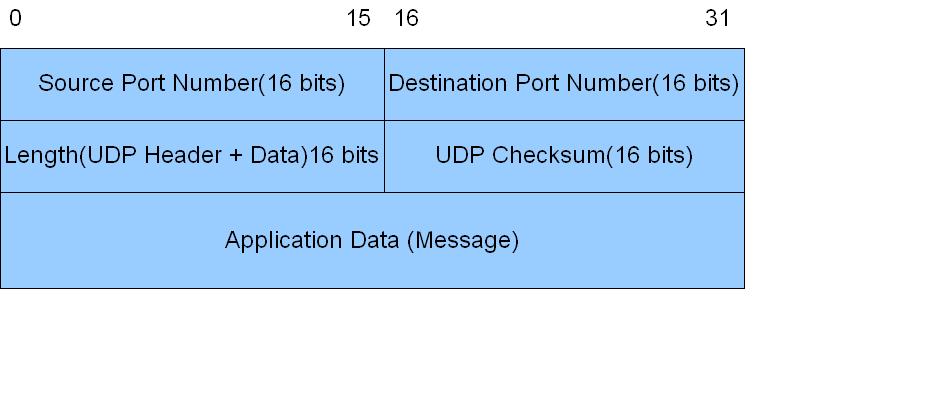


Figure UDP HEADER

## INTERNET PROTOCOL

The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. It also defines addressing methods that are used to label the datagram with source and destination information.

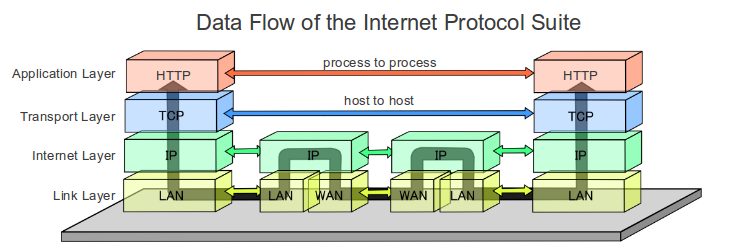


Figure DATA FLOW IN INTERNET PROTOCOL SUITE

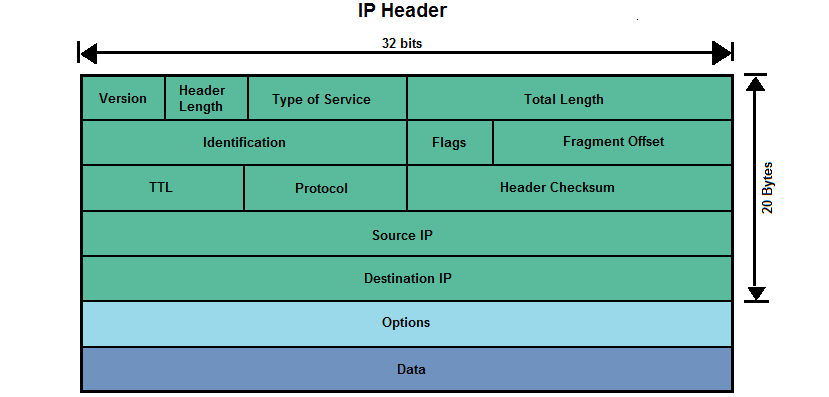


Figure IP HEADER

## L2 PROTOCOLS

Layer 2 contains two sublayers:

* Logical link control (LLC) sublayer, which is responsible for managing communications links and handling frame traffic.
* Media access control (MAC) sublayer, which governs protocol access to the physical network medium. By using the MAC addresses that are assigned to all ports on a switch, multiple devices on the same physical link can uniquely identify one another.

Table L2 PROTOCOLS

|  |  |
| --- | --- |
| PROTOCOL | DESCRIPTION |
| LLDP (Link layer discovery protocol) | LLDP is vendor neutral, and is commonly used as a component in network management and network monitoring applications. |
| CDP (Cisco Discovery Protocol) | CDP is a Cisco proprietary protocol that support the IEEE 802.1ab version of LLDP, and is primarily used to share information between directly connected Cisco devices. |
| IP route | This command contains information from the IP routing table that can be used to forward a packet through the best path towards its destination. |
| FDB (Forwarding database) | FDB stores MAC addresses of the discovered devices and their respective ports. This protocol is preferred for discovering switches. |
| ARP (Address Resolution Protocol) | ARP maps dynamic IP (Layer 3) with MAC addresses (Layer 2). ARP translates 32-bit addresses to 48-bit and vice versa, and is preferred by IPv4 devices. |
| MLT (Multi-link trucking Protocol) | MLT provides high-speed, fault tolerant connection between servers, switches and routers by grouping all ethernet links into a single logical ethernet link. |
| CAN (Controller area network) | CAN facilitates communication between the applications of microcontrollers and their devices without relying on a host computer. |
| PPP (Point-to-Point Protocol) | PPP allows you to establish communication between two routers without the help of a host. |

## L3 PROTOCOLS

L3(Layer3) does routing, logical addressing, packet sequencing and provide interfacing with TCP or UDP.

Table L3 PROTOCOLS

|  |  |
| --- | --- |
| PROTOCOL | DESCRIPTION |
| CLNP (Connectionless Networking Protocol)  IPX (Internetwork Packet Exchange) |  |
| NAT (Network Address Translation) |  |
| ICMP (Internet Control Message Protocol) |  |
| OSPF (Open Shortest Path First (v1 and v2)) |  |
| RIP (Routing Information Protocol (v1 and v2)) |  |
| IPSEC |  |
| IP (Internet Protocol) |  |
| HSRP (Hot Standby Router protocol) |  |

# IP ADDRESSES

## IPV4 V/S IPV6

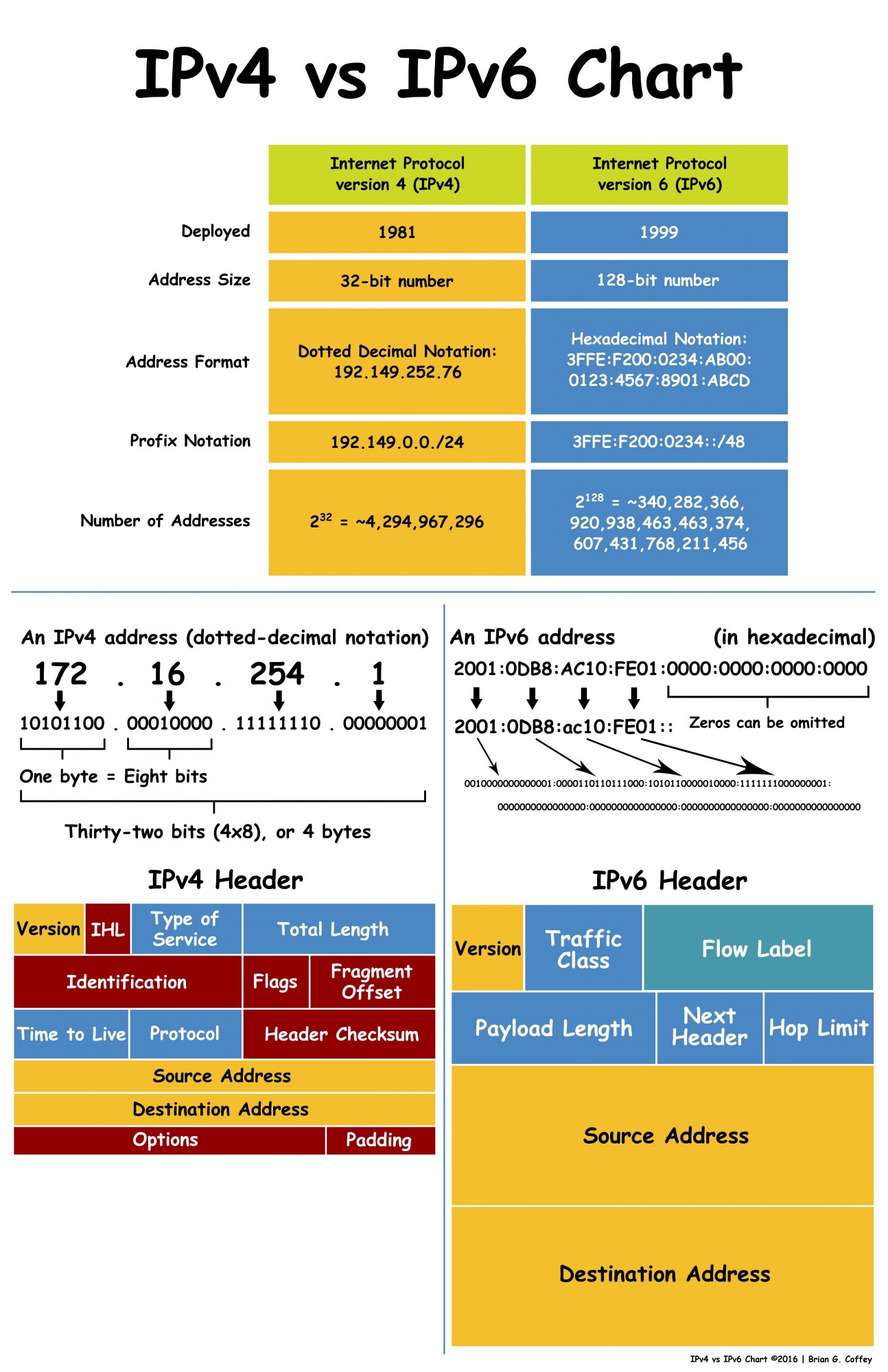


Figure IPV4 V/S IPV6

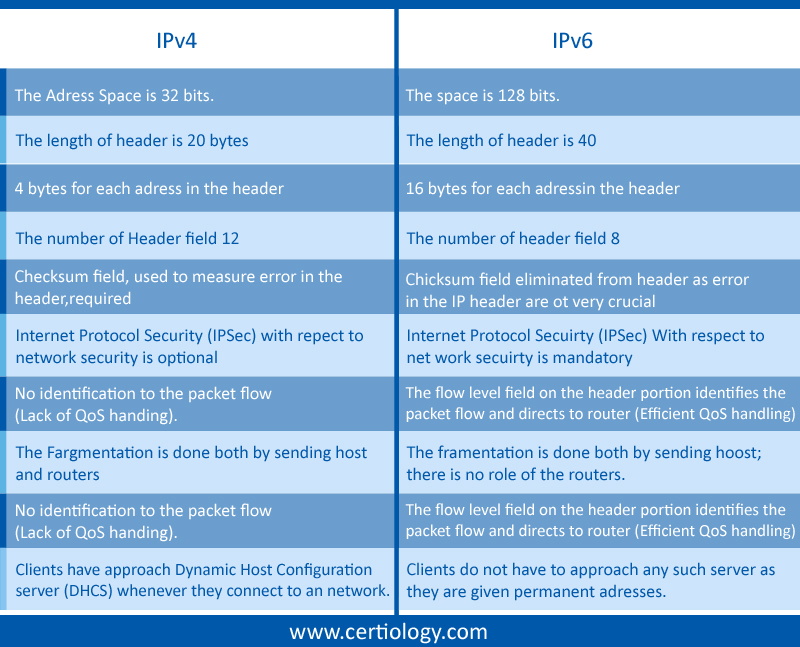


Figure DIFFERENCE BETWEEN IPV4 & IPV6

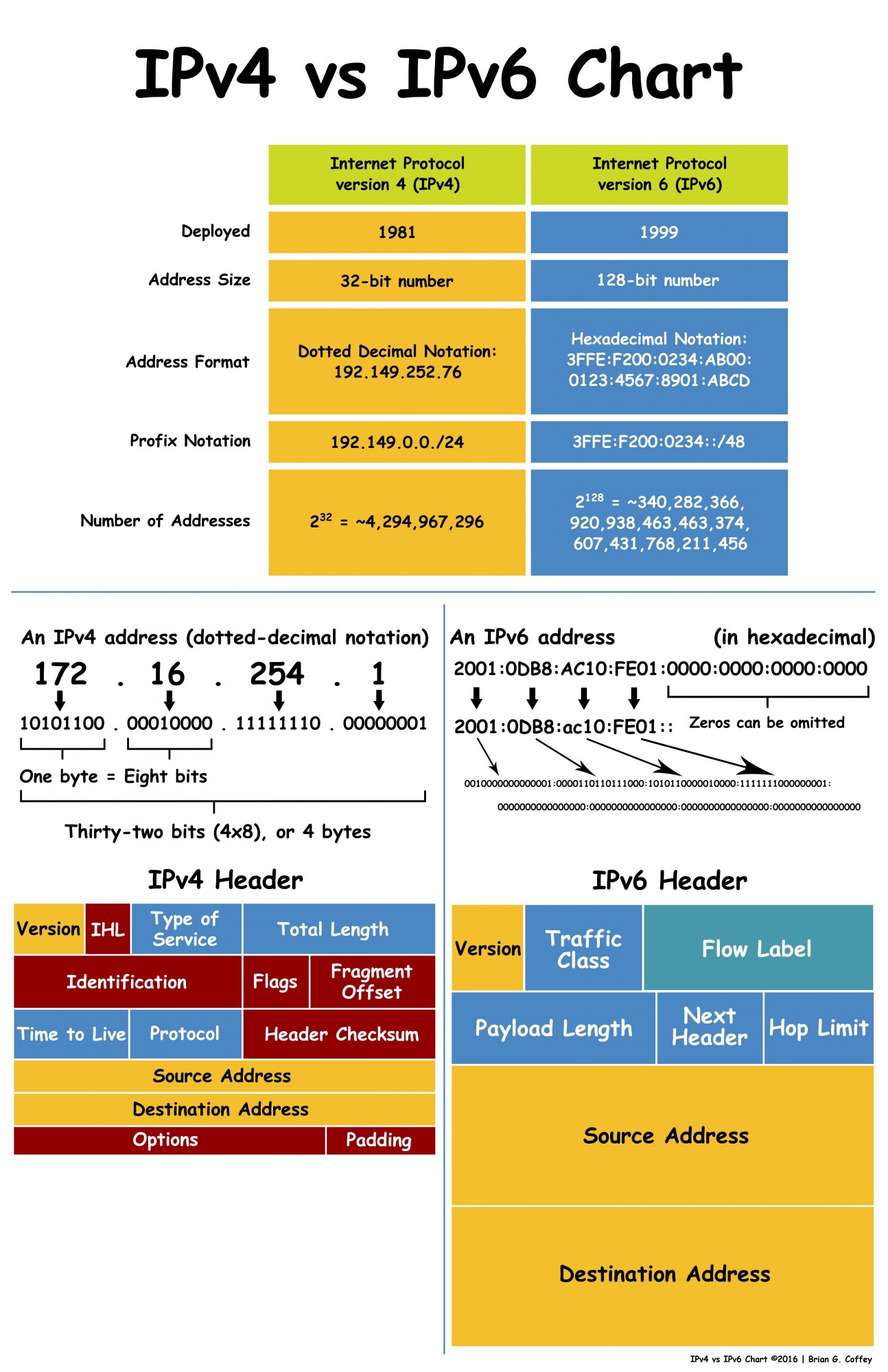


Figure IPV4 & IPV6 HEADER

## NETWORK CLASSES IN IPV4

The first step in planning for IP addressing on your network is to determine which network class is appropriate for your network. After you have done this, you can take the crucial second step: obtain the network number from the InterNIC addressing authority.

Currently there are three classes of TCP/IP networks. Each class uses the 32-bit IP address space differently, providing more or fewer bits for the network part of the address. These classes are class A, class B, and class C.

### CLASS A

A class A network number uses the first eight bits of the IP address as its "network part." The remaining 24 bits comprise the host part of the IP address. The values assigned to the first byte of class A network numbers fall within the range 0-127. Consider the IP address 75.4.10.4. The value 75 in the first byte indicates that the host is on a class A network. The remaining bytes, 4.10.4, establish the host address. The InterNIC assigns only the first byte of a class A number. Use of the remaining three bytes is left to the discretion of the owner of the network number. Only 127 class A networks can exist. Each one of these numbers can accommodate up to 16,777,214 hosts.

### CLASS B

A class B network number uses 16 bits for the network number and 16 bits for host numbers. The first byte of a class B network number is in the range 128-191. In the number 129.144.50.56, the first two bytes, 129.144, are assigned by the InterNIC, and comprise the network address. The last two bytes, 50.56, make up the host address, and are assigned at the discretion of the owner of the network number. Class B is typically assigned to organizations with many hosts on their networks.

### CLASS C

Class C network numbers use 24 bits for the network number and 8 bits for host numbers. Class C network numbers are appropriate for networks with few hosts--the maximum being 254. A class C network number occupies the first three bytes of an IP address. Only the fourth byte is assigned at the discretion of the network owners. The first byte of a class C network number covers the range 192-223. The second and third each cover the range 1- 255. A typical class C address might be 192.5.2.5. The first three bytes, 192.5.2, form the network number. The final byte in this example, 5, is the host number.

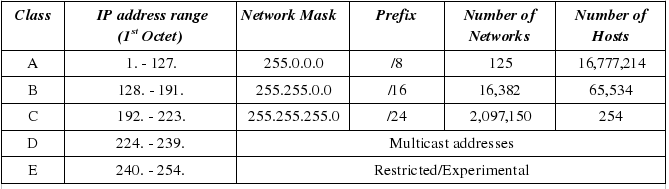


Figure NETWORK CLASSES

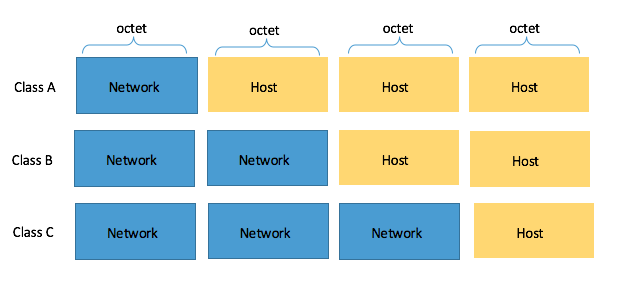


Figure NETWORK CLASS MASK

# COLLEGE NETWORK

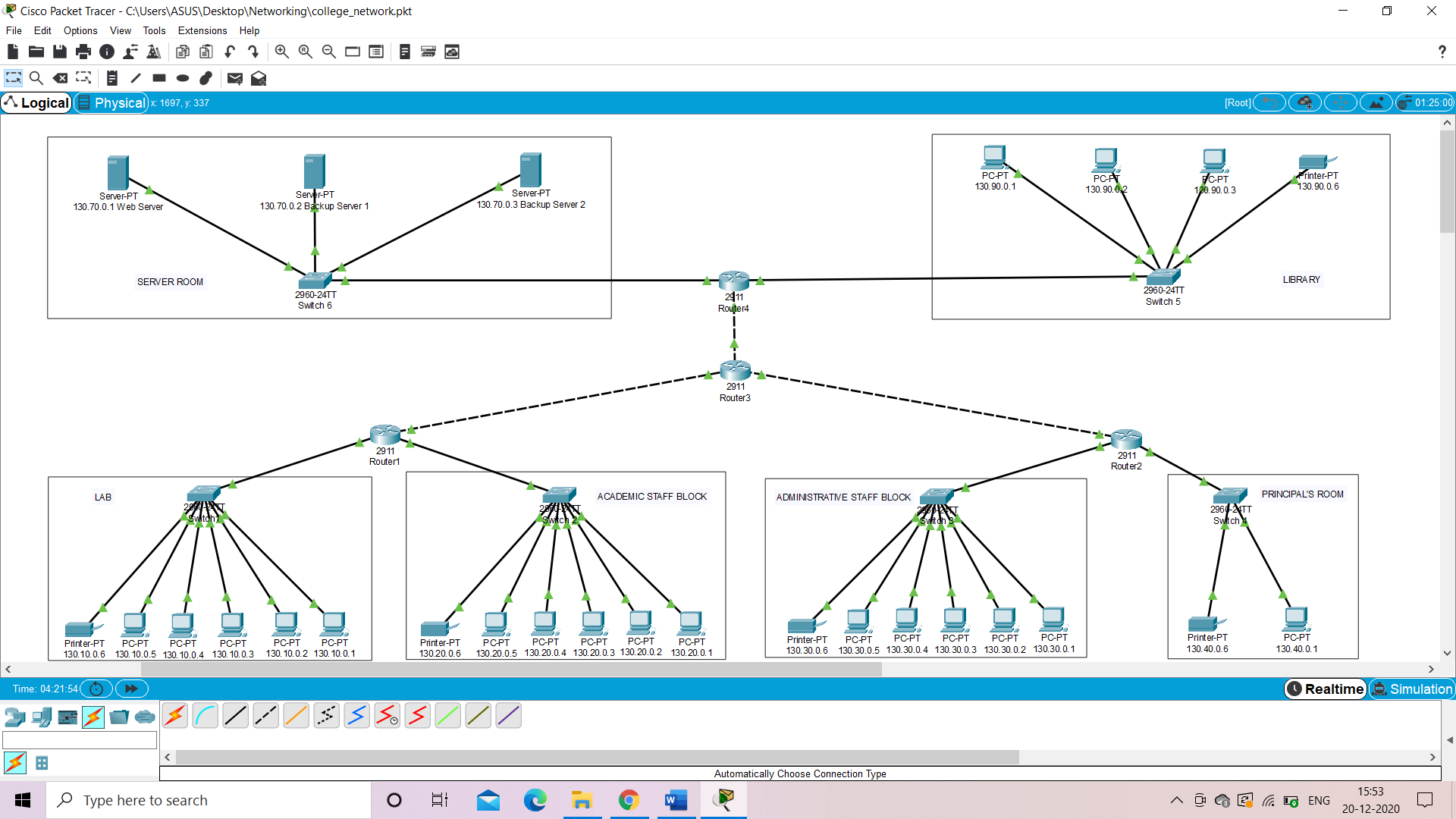


Figure COLLEGE NETWORK DESIGN

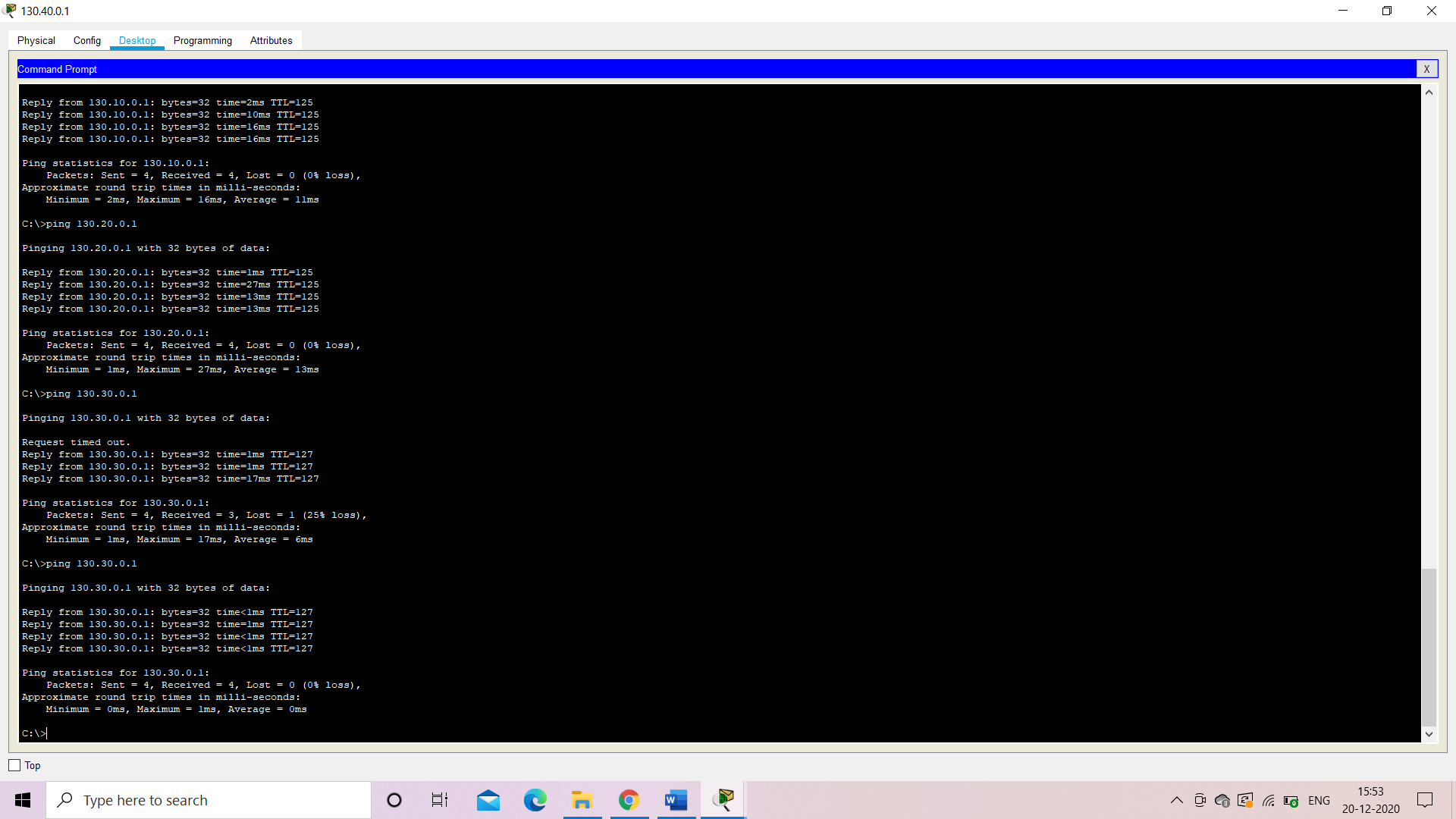


Figure PING SCREENSHOT