Lab # 01

Objective

Introduction to networking and installation of network simulator.

Theory

Data Communication

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. **Delivery**. The system must deliver data to the correct destination.
2. **Accuracy**. The system must deliver the data accurately.
3. **Timeliness**. The system must deliver data in a timely manner.
4. **Jitter**. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

Components

1. **Message**. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. **Sender**. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. **Receiver**. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. **Transmission medium**. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
5. **Protocol**. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

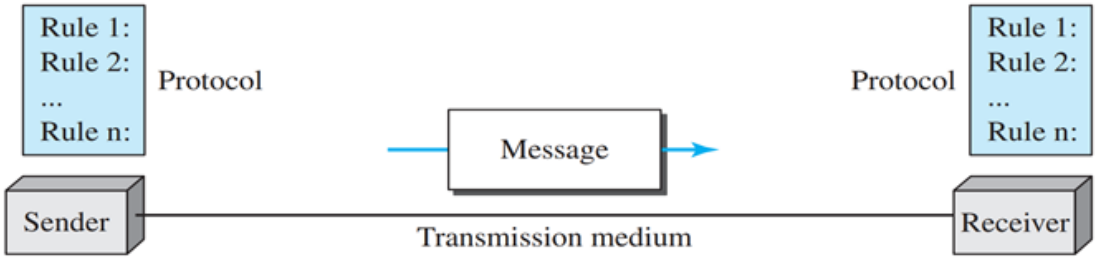


Figure 1 Components of Data Communication

Networks

A network is the interconnection of a set of devices capable of communication. In this definition, a device can be a host (or an end system as it is sometimes called) such as a large computer, desktop, laptop, workstation, cellular phone, or security system. A device in this definition can also be a connecting device such as a router, which connects the network to other networks, a switch, which connects devices together, a modem (modulator-demodulator), which changes the form of data, and so on. These devices in a network are connected using wired or wireless transmission media such as cable or air. When we connect two computers at home using a plug-and-play router, we have created a network, although very small.

Types of Networks

- **Local Area Network:** A local area network (LAN) is usually privately owned and connects some hosts in a single office, building, or campus. Each host in a LAN has an identifier, an address, that uniquely defines the host in the LAN. A packet sent by a host to another host carries both the source host's and the destination host's addresses.
- **Wide Area Network:** A wide area network (WAN) is also an interconnection of devices capable of communication. A WAN has a wider geographical span, spanning a town, a state, a country, or even the world. A WAN is normally created and run by communication companies and leased by an organization that uses it. We see two distinct examples of WANs today: point-to-point WANs and switched WANs.

Switching

An internet is a switched network in which a switch connects at least two links together. A switch needs to forward data from a network to another network when required. The two most common types of switched networks are circuit-switched and packet-switched networks.

Circuit-Switched Network

In a circuit-switched network, a dedicated connection, called a circuit, is always available between the two end systems; the switch can only make it active or inactive. Figure 2 shows a very simple switched network that connects four telephones to each end. We have used telephone sets instead of computers as an end system because circuit switching was very common in telephone networks in the past, although part of the telephone network today is a packet-switched network.

Packet-Switched Network

In a computer network, the communication between the two ends is done in blocks of data called packets. This allows us to make the switches function for both storing and forwarding because a packet is an independent entity that can be stored and sent later. Figure 3 shows a small packet-switched network that connects four computers at one site to four computers at the other site.

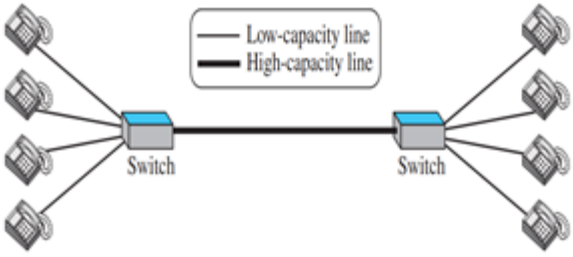


Figure 2 Circuit-Switched Network

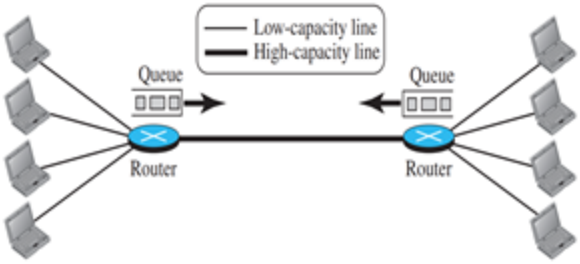


Figure 3 Packet-Switched Network

THE OSI MODEL

An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s. An ***open system*** is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable. The OSI model was intended to be the basis for the creation of the protocols in the OSI stack.

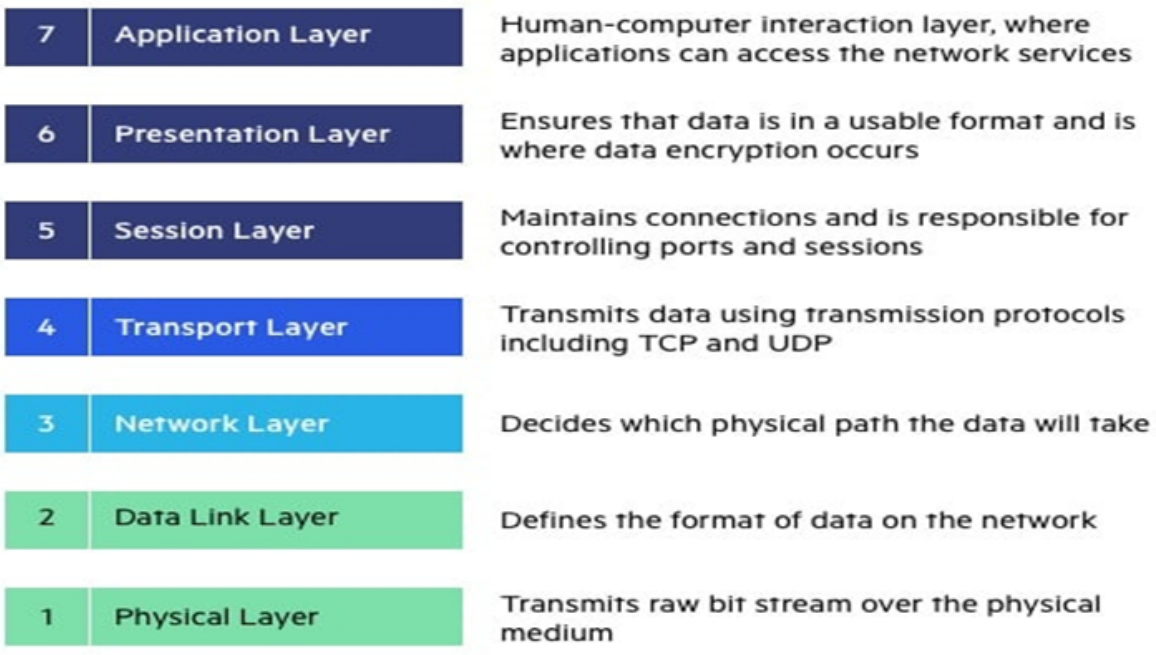


Figure 4 OSI Model

TCP/IP PROTOCOL SUITE

TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the Internet today. It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality. The term hierarchical means that each upper-level protocol is supported by the services provided by one or more lower-level protocols. The original TCP/IP protocol suite was defined as four software layers built upon the hardware. Today, however, TCP/IP is thought of as a five-layer model.

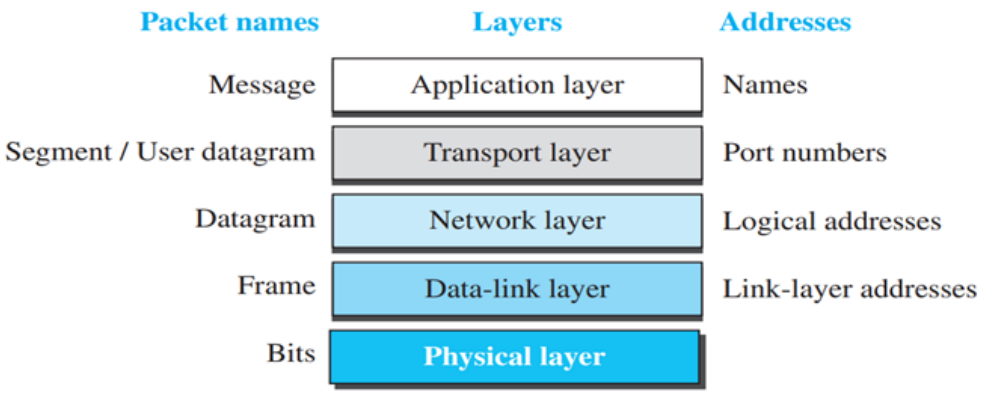


Figure 5 TCP/IP Model

Using logical connections makes it easier for us to think about the duty of each layer. The domain of duty of the top three layers is the internet, and the domain of duty of the two lower layers is the link.

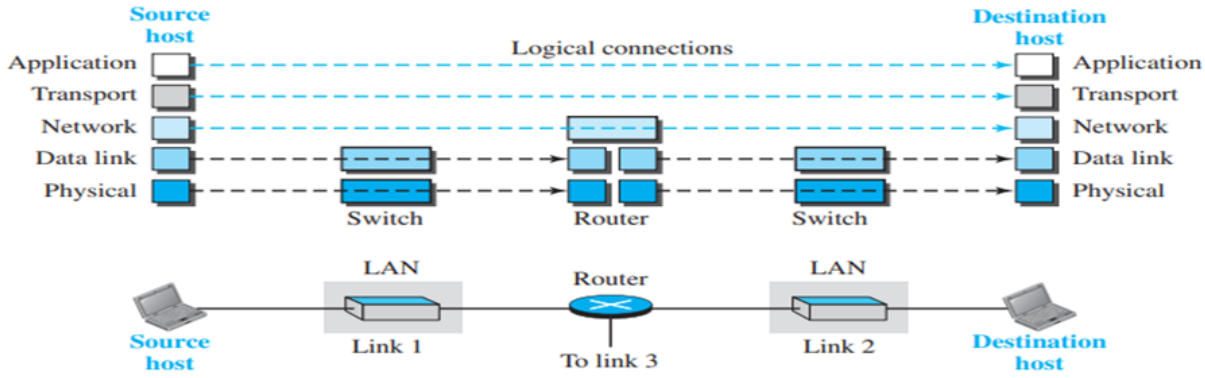


Figure 6 Logical connection between layers of TCP/IP Model

Encapsulation and De-encapsulation

One of the important concepts in protocol layering on the Internet is encapsulation/ de-encapsulation.

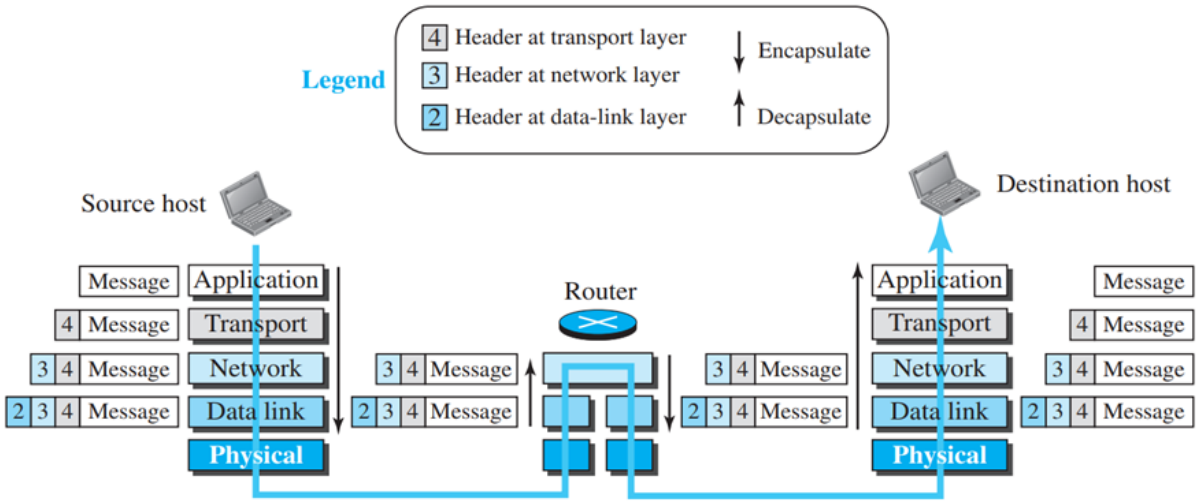


Figure 7 Encapsulation and De-encapsulation in TCP/IP Model

OSI versus TCP/IP

When we compare the two models, we find that two layers, session and presentation, are missing from the TCP/IP protocol suite. These two layers were not added to the TCP/IP protocol suite after the publication of the OSI model. The application layer in the suite is usually considered to be the combination of three layers in the OSI model, as shown below

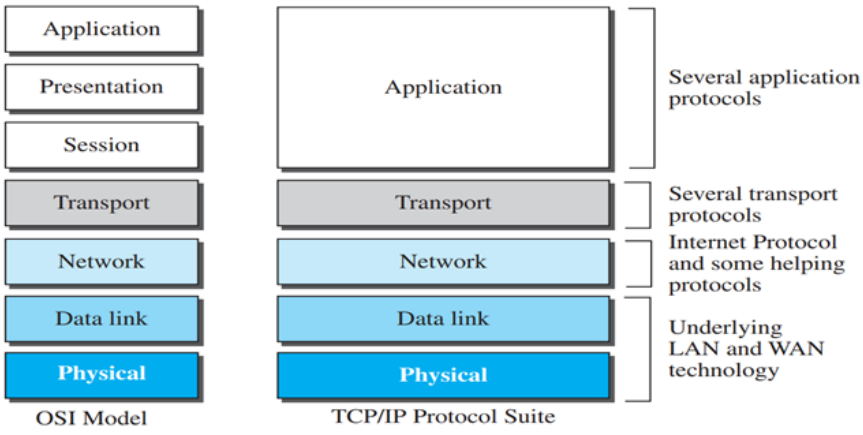


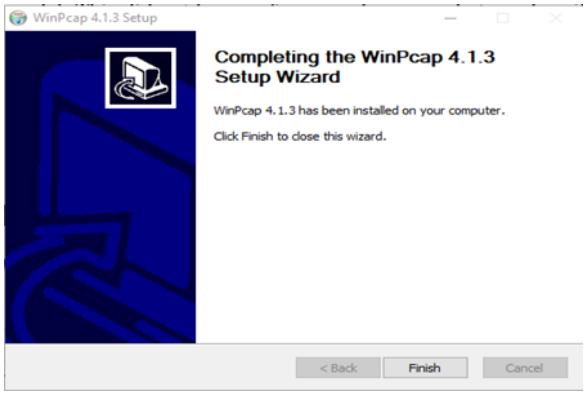
Figure 8. OSI Model vs TCP/IP

Two reasons were mentioned for this decision. First, TCP/IP has more than one transport-layer protocol. Some of the functionalities of the session layer are available in some of the transport-layer protocols. Second, the application layer is not only one piece of software. Many applications can be developed at this layer. If some of the functionalities mentioned in the session and presentation layers are needed for a particular application, they can be included in the development of that piece of software.

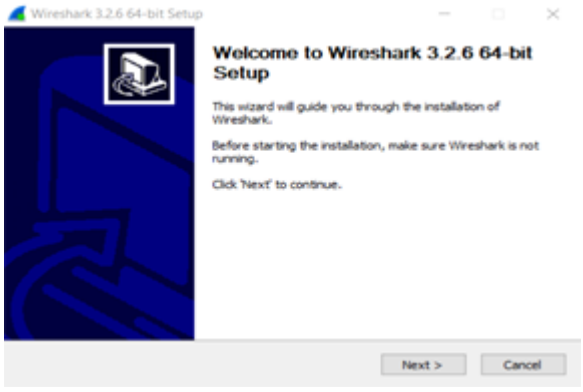
Network Simulator Setup

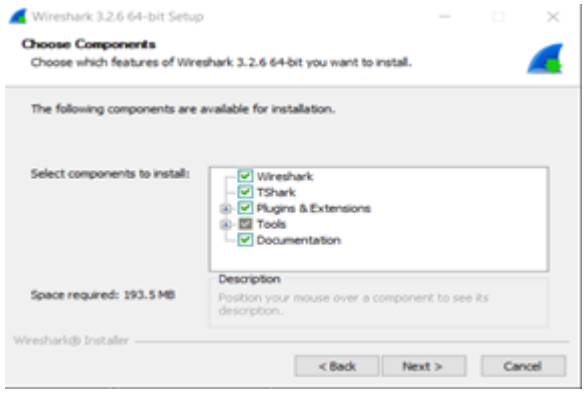
Before installing network simulator (eNSP) we need to **install the 3 prerequisites** required for eNSP

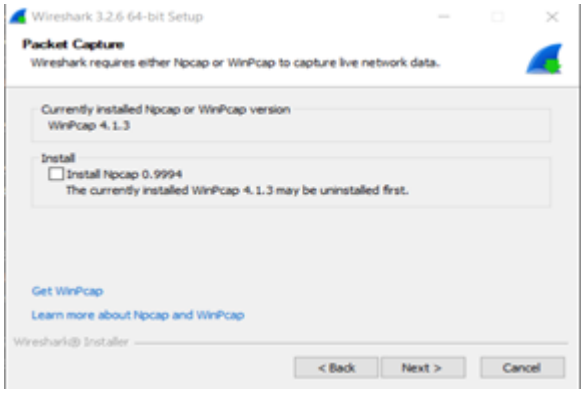
1. **Installing WinPcap Driver**



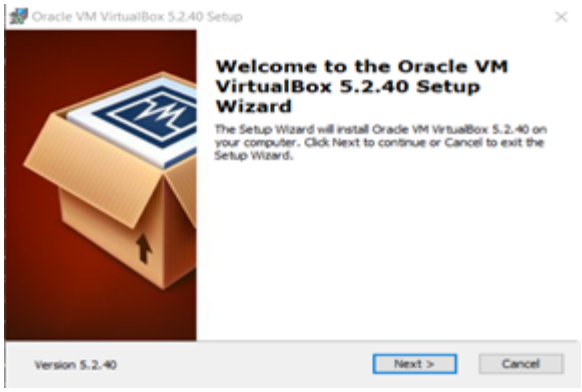
2. **Installing WireShark**



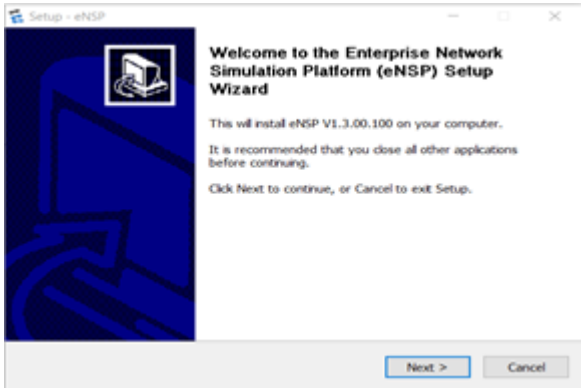


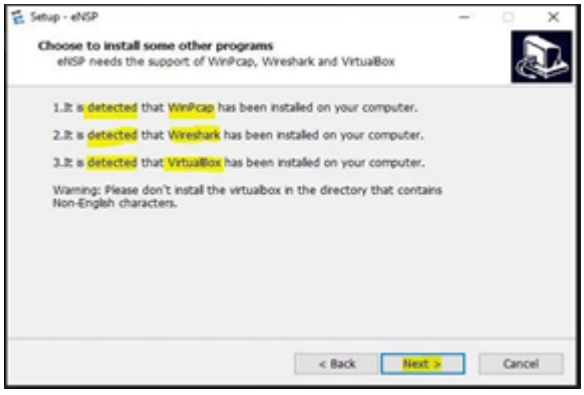


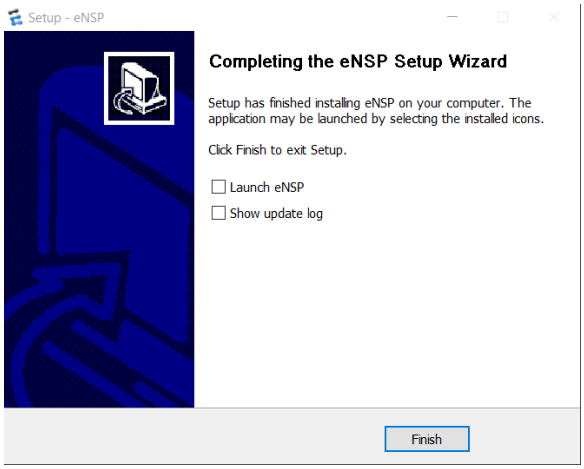
3. Installing Oracle VirtualBox



4. Installing eNSP







Lab # 02

Objective

Understand and calculate the IP Addresses and its subnetting.

Theory

Internet Protocol (IP)

The network layer in version 4 can be thought of as one main protocol and three auxiliary ones. The main protocol, Internet Protocol version 4 (IPv4), is responsible for packetizing, forwarding, and delivery of a packet at the network layer. The Internet Control Message Protocol version 4 (ICMPv4) helps IPv4 to handle some errors that may occur in the network-layer delivery. The Internet Group Management Protocol (IGMP) is used to help IPv4 in multicasting. The Address Resolution Protocol (ARP) is used to glue the network and data-link layers in mapping network-layer addresses to link-layer addresses

IPv4

IPv4 is an IP version widely used to identify devices on a network using an addressing system. It was the first version of IP deployed for production in the ARPANET in 1983. It uses a 32-bit address scheme to store 2^32 addresses which is more than 4 billion addresses. It is considered the primary Internet Protocol and carries 94% of Internet traffic.

Following are the features of IPv4:

- Connectionless Protocol
- Allow creating a simple virtual communication layer over diversified devices
- It requires less memory, and ease of remembering addresses
- Already supported protocol by millions of devices
- Offers video libraries and conferences

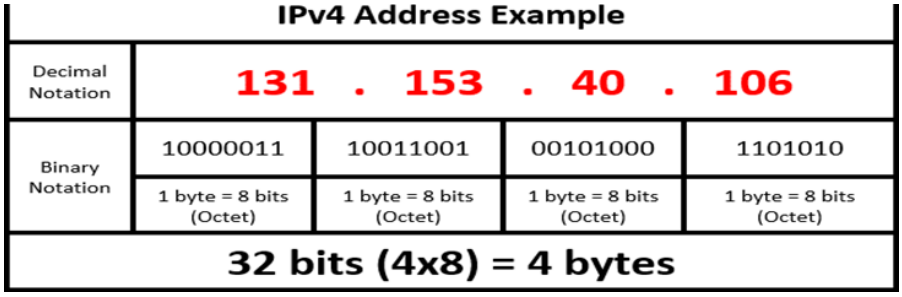


Figure 1. IPV4

IPv6

IPv6 is the most recent version of the Internet Protocol. This new IP address version is being deployed to fulfill the need for more Internet addresses. It was aimed to resolve issues that are associated with IPv4. With 128-bit address space, it allows 340 undecillion unique address space. IPv6 is also called IPng (Internet Protocol next generation).
Here are the features of IPv6:

- Hierarchical addressing and routing infrastructure
- Stateful and Stateless configuration
- Support for quality of service (QoS)
- An ideal protocol for neighboring node interaction

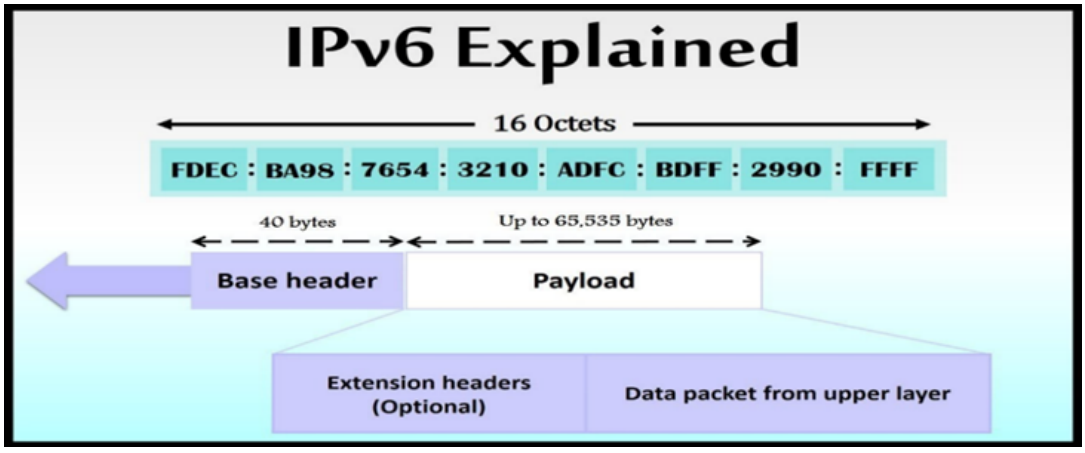


Figure 2. IPV6

Key Differences Between IPv4 and IPv6

IPv4 & IPv6 are both IP addresses that are binary numbers. IPv4 is a 32-bit binary number, and IPv6 is a 128-bit binary number address. IPv4 addresses are separated by periods, while IPv6 addresses are separated by colons. Both IP addresses are used to identify machines connected to a network. In principle, they are almost similar, but they are different in how they work.

Private and Public IP Addressing

The main difference between public and private IP addresses is how far they reach, and what they're connected to.
A **public IP address** identifies you to the wider internet so that all the information you're searching for can find you.
A **private IP address** is used within a private network to connect securely to other devices within that same network.

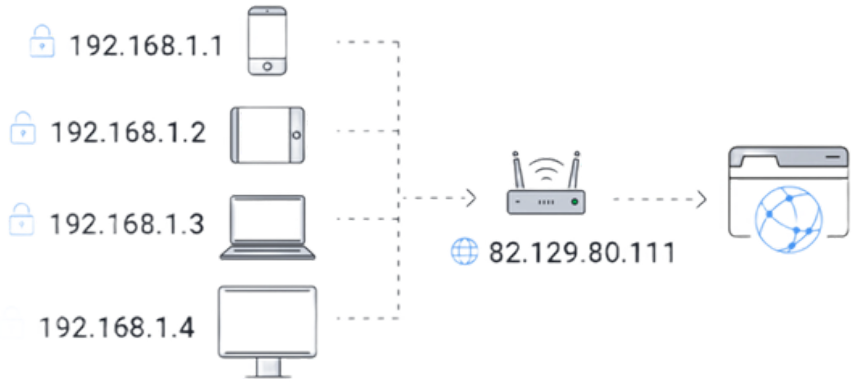


Figure 3. Public and Private IP Addressing

Private and Public IP Address Ranges

Your private IP address exists within specific private IP address ranges reserved by the Internet Assigned Numbers Authority (IANA) and should never appear on the internet. There are millions of private networks across the globe, all of which include devices assigned **private IP addresses** and the public IP address range encompasses every number *not* reserved for the private IP range.

Private	Public
Class A: 10.0.0.0 — 10.255.255.255	Class A: 1.0.0.0 — 9.255.255.255 11.0.0.0 — 126.255.255.255
Class B: 172.16.0.0 — 172.31.255.255	Class B: 128.0.0.0 — 172.15.255.255 172.32.0.0 — 191.255.255.255
Class C: 192.168.0.0 — 192.168.255.255	Class C: 192.0.0.0 — 192.167.255.255 192.169.0.0 — 223.255.255.255

Subnet Mask

A subnet mask is a 32-bit number created by setting host bits to all 0s and setting network bits to all 1s. In this way, the subnet mask separates the IP address into the network and host addresses.

The "255" address is always assigned to a broadcast address, and the "0" address is always assigned to a network address. Neither can be assigned to hosts, as they are reserved for these special purposes.

The IP address, subnet mask and gateway or router comprise an underlying structure—the Internet Protocol—that most networks use to facilitate inter-device communication.

When organizations need additional sub networking, subnetting divides the host element of the IP address further into a subnet. The goal of subnet masks is simply to enable the subnetting process. The phrase "mask" is applied because the subnet mask essentially uses its own 32-bit number to mask the IP address.

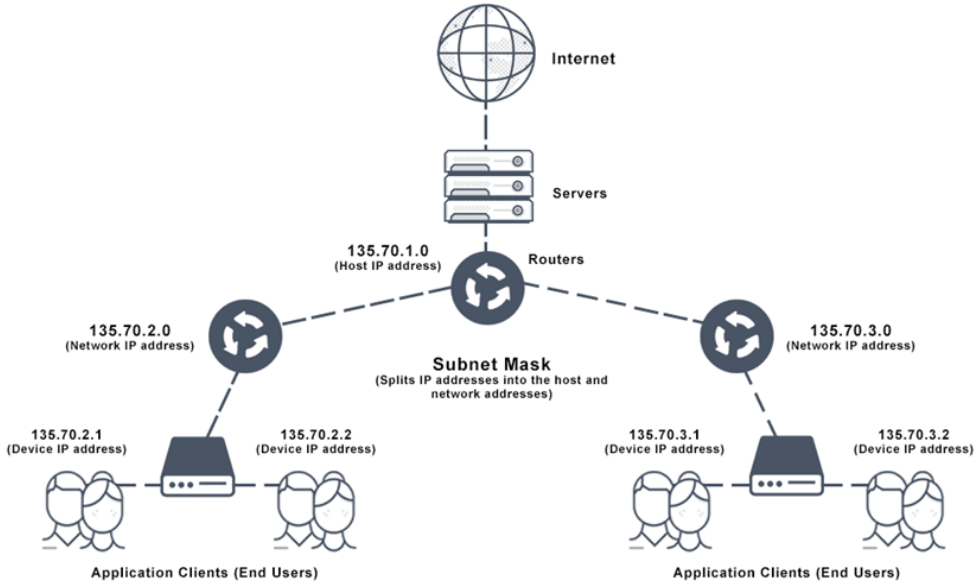


Figure 4. Subnet Mask

VLSM

VLSM stands for Variable Length Subnet Mask where the subnet design uses more than one mask in the same network which means more than one mask is used for different subnets of a single class A, B, C or a network. It is used to increase the usability of subnets as they can be of variable size. It is also defined as the process of subnetting of a subnet.

Earlier, it was required to use the same subnet mask across the network. This was called classful networking. With increase in complexity of networks and decrease in available IP addresses it became obvious that classful networking causes waste of valuable IP addresses. To understand how, consider Figure 1. The largest subnet requires 30 host addresses. So, across the network a mask of /27 is used, which gives 30 hosts per subnet. You will notice that in every subnet except the subnet attached to RouterD, some host addresses will remain unused. In particular, 28 host addresses are wasted for each link between the routers. In total this network wastes 118 addresses and uses 92 addresses.

To avoid wasting of IP addresses, classless networking was introduced by way of VLSM. VLSM allows you to use different subnet masks across the network for the same class of addresses. For example, a /30 subnet mask, which gives 2 host addresses per subnet, can be used for point-to-point links between routers. Figure 6 shows how VLSM can be used to save address space in the network shown in Figure 5.

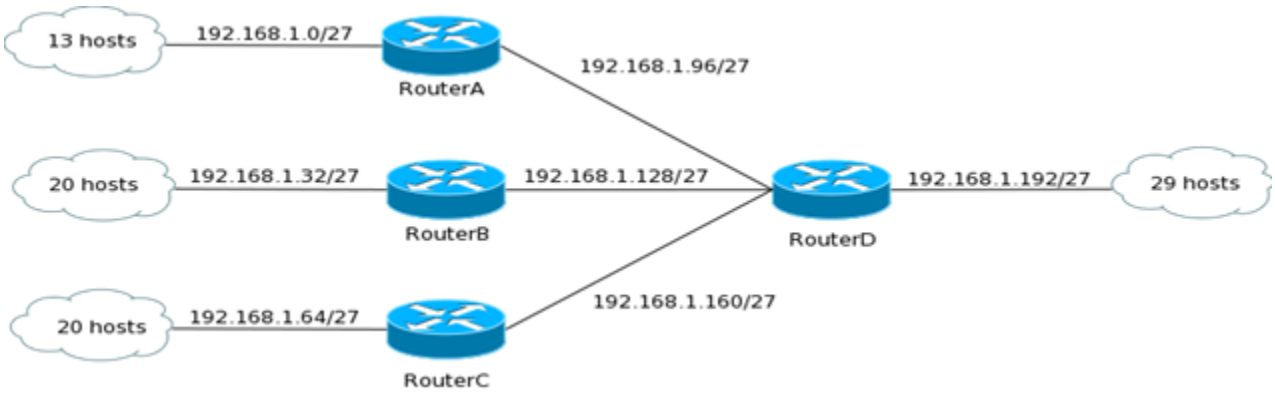


Figure 5. Without VLSM

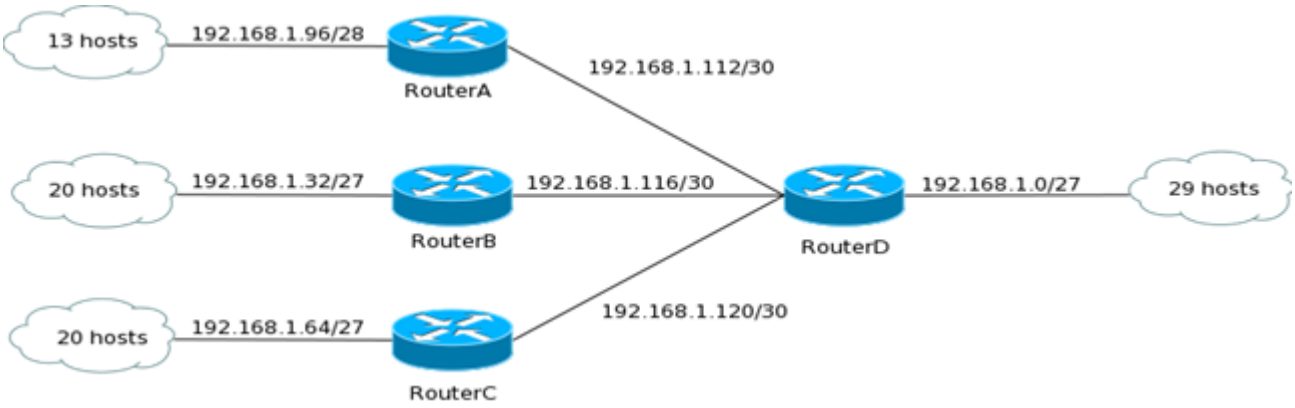


Figure 6. With VLSM

Subnetting and Supernetting

- **Subnetting**

  Subnetting is the procedure to divide the network into sub-networks or small networks.

- **Supernetting**

  Supernetting is the procedure to combine the small networks into larger space.

In subnetting, Network address bits are increased. On the other hand, in supernetting, Host address bits are increased. Subnetting is implemented via Variable-length subnet masking, while supernetting is implemented via Classless interdomain routing.

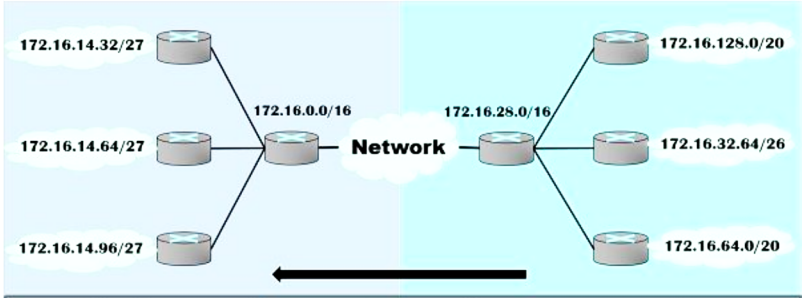


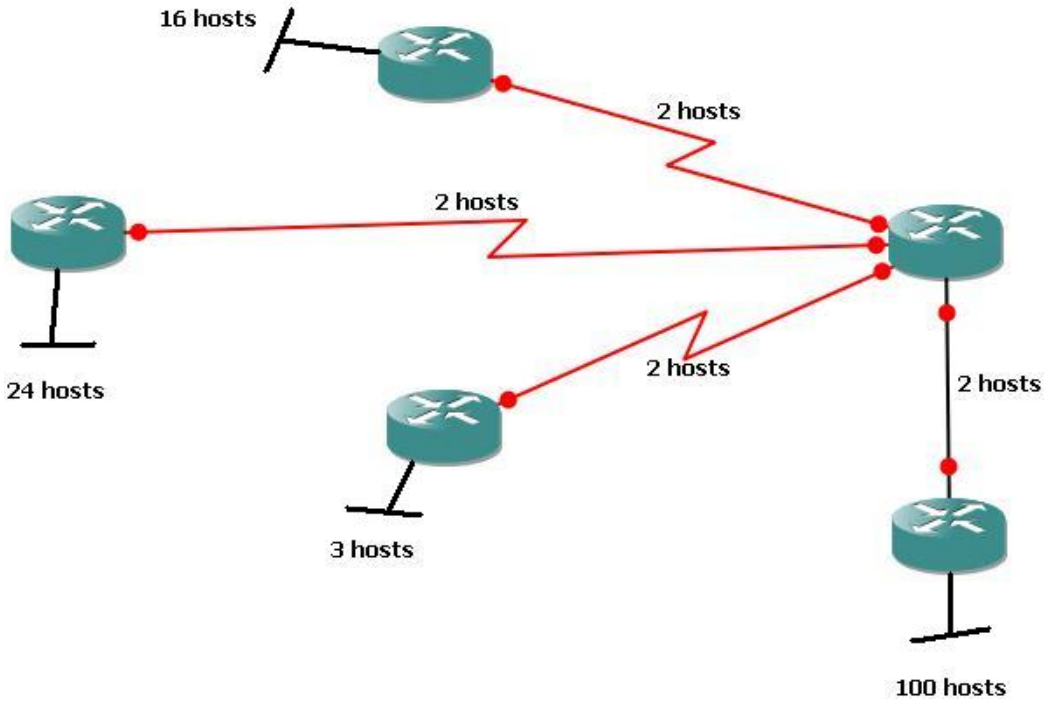
Figure 7. Subnetting vs Supernetting

Differences between Subnetting and Supernetting

	Subnetting	Supernetting
1.	Subnetting is the procedure to divide the network into sub networks.	While supernetting is the procedure of combining the small networks.
2.	In subnetting, Network address bits are increased.	While in supernetting, Host address bits are increased.
3.	In subnetting, the mask bits are moved towards the right.	While in supernetting, the mask bits are moved towards the left.
4.	Subnetting is implemented via Variable-length subnet masking.	While supernetting is implemented via Classless interdomain routing.
5.	In subnetting, Address depletion is either reduced or removed.	It is used to simplify the routing process.

Lab Task (Lab # 02):

Calculate the VLSM (IPs) using the Available Subnet – 24.23.5.0/24. Then implement in the following scenario with eNSP.



Lab # 03

Objective

Mac Addresses, ARP and Switching.

Theory

Address Resolution Protocol (ARP)

The network Address Resolution Protocol (ARP) is a procedure for mapping a dynamic IP address to a permanent physical machine address in a local area network (LAN). The physical machine address is also known as a media access control (MAC) address.

The job of ARP is essentially to translate 32-bit addresses to 48-bit addresses and vice versa. This is necessary because IP addresses in IP version 4 (IPv4) are 32 bits, but MAC addresses are 48 bits.

ARP works between Layers 2 and 3 of the Open Systems Interconnection model (OSI model). The MAC address exists on Layer 2 of the OSI model, the data link layer. The IP address exists on Layer 3, the network layer.

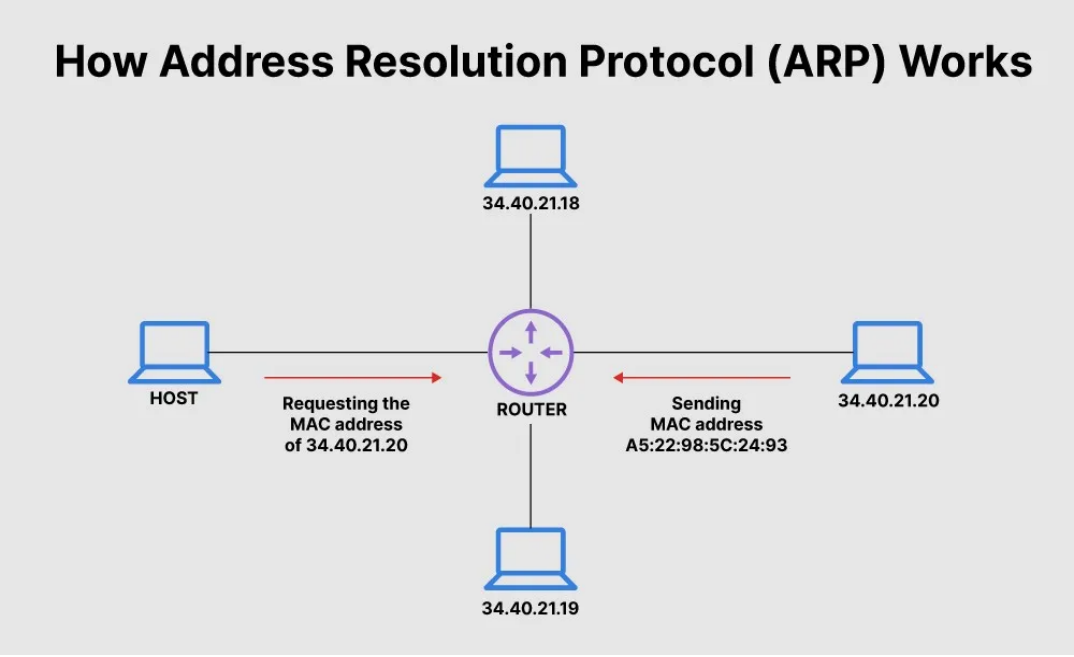


Figure 1. Working of ARP

There are four types of arp messages that may be sent by the arp protocol. These are identified by four values in the "operation" field of an arp message. The types of message are:

1. ARP-Request (Broadcast, source IP address of the requester)
2. ARP-Reply (Unicast to requester, the target)

Types of ARP

There are different versions and use cases of ARP. Let us take a look at a few.

Proxy ARP

Proxy ARP is a technique by which a proxy device on a given network answers the ARP request for an IP address that is not on that network. The proxy is aware of the location of the traffic's destination and offers its own MAC address as the destination.

Gratuitous ARP

Gratuitous ARP is almost like an administrative procedure, carried out as a way for a host on a network to simply announce or update its IP-to-MAC address. Gratuitous ARP is not prompted by an ARP request to translate an IP address to a MAC address.

Reverse ARP (RARP)

Host machines that do not know their own IP address can use the Reverse Address Resolution Protocol (RARP) for discovery.

Inverse ARP (IARP)

Whereas ARP uses an IP address to find a MAC address, IARP uses a MAC address to find an IP address.

Media Access Control Address (MAC Address)

A MAC address is a hardware identification number that uniquely identifies each device on a network. The MAC address is manufactured into every network card, such as an Ethernet card or Wi-Fi card, and therefore cannot be changed.

Because there are millions of networkable devices in existence, and each device needs to have a unique MAC address, there must be a very wide range of possible addresses. For this reason, MAC addresses are made up of six two-digit hexadecimal numbers, separated by colons. For example, an Ethernet card may have a MAC address of 00:0d:83:b1:c0:8e. Fortunately, you do not need to know this address, since it is automatically recognized by most networks.

Reason to have both IP and MAC addresses.

Both MAC and IP addresses are operated on different layers of the internet protocol suite. The MAC address works on layer 2 and helps identify the devices within the same broadcast network (such as the router). On the other hand, the IP addresses are used on layer 3 and help identify the devices on different networks.

MAC vs IP Address

Both the MAC address and IP address are the way to identify the device on the network.

IP Address	MAC Address
stands for Internet Protocol.	stands for Media Access Control.
It is the logical address provided by the ISP or Internet Service Provider.	It is the unique address provided by the manufacturer.
It is the logical address that identifies a network or device on the internet.	It is the physical address of the device's NIC that is used to identify a device within a network.
It operates on a network Layer.	It operates on the data link layer.
It is of 4 bytes for IPv4 and 8 bytes for IPv6 addresses.	It is the 6 -bytes hexadecimal address.

MAC Address Format

We cannot assign the MAC address to the device's NIC; it is preconfigured by the manufacturers.

- It is 12 digits or 6-byte hexadecimal number, which is represented in colon-hexadecimal notation format. It is divided into six octets, and each octet contains 8 bits.
- The first three octets are used as the OUI or Organisationally Unique Identifier. These MAC prefixes are assigned to each organization or vendor by the IEEE Registration Authority Committee.

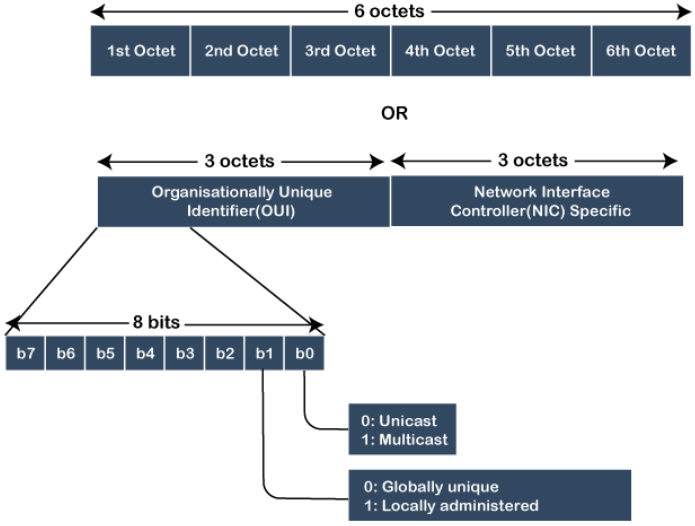


Figure 2. Mac Address Format

Why should the MAC address be unique in the LAN network?

If a LAN network has two or more devices with the same MAC address, that network will not work.

Suppose three devices A, B, and C are connected to a network through a switch. The MAC addresses of these devices are 11000ABB28FC, 00000ABB28FC, and 00000ABB28FC, respectively. The NIC of devices B and C have the same MAC address. If device A sends a data frame to the address 00000ABB28FC, the switch will fail to deliver this frame to the destination, as it has two recipients of this data frame.

What is a network switch?

A network switch connects devices within a network (often a local area network, or LAN*) and forwards data packets to and from those devices. Unlike a router, a switch only sends data to the single device it is intended for (which may be another switch, a router, or a user's computer), not to networks of multiple devices.

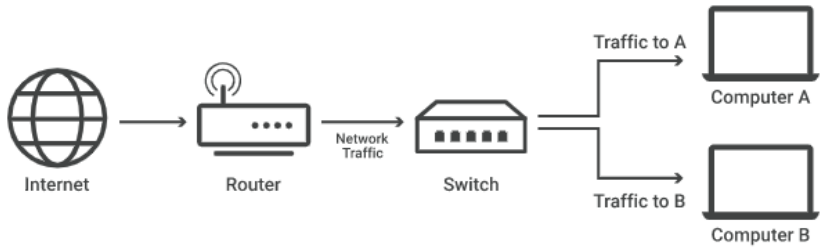


Fig 1. A local area network (LAN) is a group of connected devices within close physical proximity.

What is the difference between a switch and a router?

Routers select paths for data packets to cross networks and reach their destinations. In practice, what this means is that routers are necessary for an Internet connection, while switches are only used for interconnecting devices. Homes and small offices need routers for Internet access, but most do not need a network switch, unless they require a large amount of Ethernet* ports. However, large offices, networks, and data centers with dozens or hundreds of computers usually do require switches.

What is a layer 2 switch and layer 3 switch?

Network switches can operate at either OSI layer 2 (the data link layer) or layer 3 (the network layer). Layer 2 switches forward data based on the destination MAC address (see below for definition), while layer 3 switches forward data based on the destination IP address. Some switches can do both.

Most switches, however, are layer 2 switches. Layer 2 switches most often connect to the devices in their networks using Ethernet cables. Ethernet cables are physical cables that plug into devices via Ethernet ports.

What is an unmanaged switch? What is a managed switch?

An unmanaged switch simply creates more Ethernet ports on a LAN, so that more local devices can access the Internet. Unmanaged switches pass data back and forth based on device MAC addresses.

A managed switch fulfills the same function for much larger networks, and offers network administrators much more control over how traffic is prioritized. They also enable administrators to set up Virtual LANs (VLANs) to further subdivide a local network into smaller chunks.

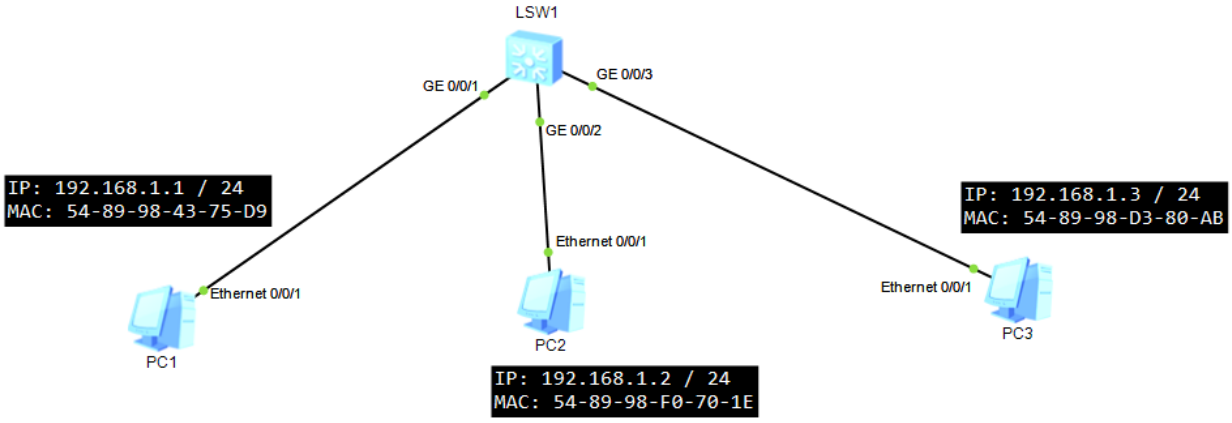
How do network switches know the MAC addresses of the devices in their network?

In layer 2, Network Switches maintains a MAC address table known as Content Addressable Memory (CAM) table that contains MAC Address and port number. Switches follow this simple algorithm:

1. When a frame is received, the switch compares the Source MAC address to the MAC address table. If the Source is unknown, the switch adds it to the table along with the port number the packet was received on. In this way, the switch learns the MAC address and port of every transmitting device.
2. The switch then compares the Destination MAC address with the table. If there is an entry, the switch forwards the frame out the associated port. If there is no entry, the switch sends the packet out all its ports, except the port that the frame was received on (Flooding).

Lab Task (Lab # 03):

Create the following scenario in eNSP with the mentioned IP addresses. Please note the MAC address may vary system to system, mention your MAC addresses. Ping PC3 from PC1 and explain how the ARP table would be maintained and what would be the role of PC2 in this process. Also explain the difference between the static and dynamic ARP entries.



Lab # 04

Objective

Understand Virtual Local Area Network (VLAN).

Theory

VLAN

VLANs (Virtual LANs) are logical grouping of devices in the same broadcast domain. VLANs are usually configured on switches by placing some interfaces into one broadcast domain and some interfaces into another. Each VLAN acts as a subgroup of the switch ports in an Ethernet LAN.

VLANs can spread across multiple switches, with each VLAN being treated as its own subnet or broadcast domain. This means that frames broadcasted onto the network will be switched only between the ports within the same VLAN.

A VLAN acts like a physical LAN, but it allows hosts to be grouped together in the same broadcast domain even if they are not connected to the same switch.

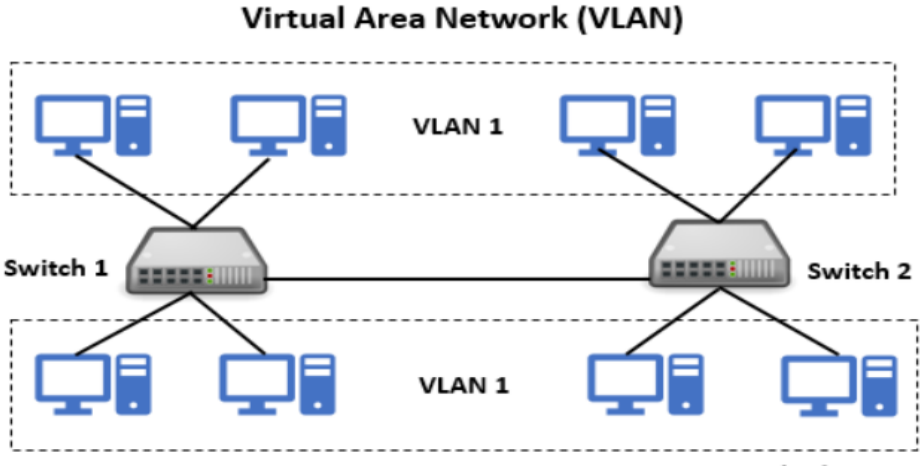


Figure 1. VLAN

Function of VLAN

The function is to separate layer 2 traffic. When the host in one VLAN is unable to communicate data between the host in another VLAN, a router is placed to pass the data between these two. We can connect all the hosts in one switch to connect each group, but the cost is prohibitive, so it is preferred for VLANs to broadcast the data. Also, the other best reason is for the secure data transfer between two hosts. The only members in the VLANs can access the network and data.

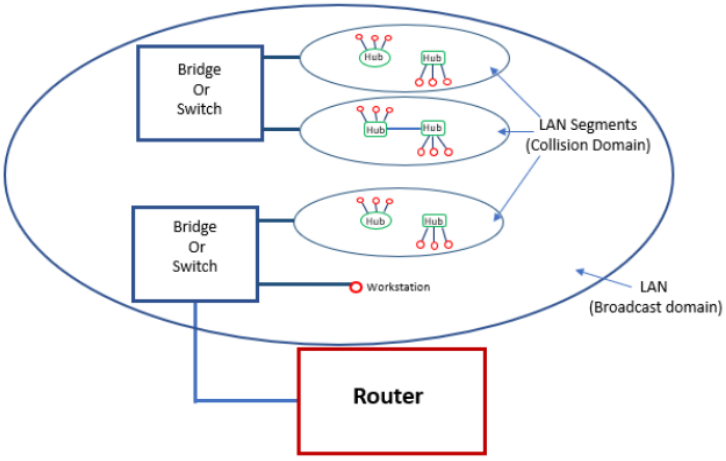


Figure 2. Function of VLAN

How VLAN works

Here is step by step details of how VLAN works:

- VLANs in networking are identified by a number.
- A Valid range is 1-4094. On a VLAN switch, you assign ports with the proper VLAN number.
- The switch then allows data which needs to be sent between various ports having the same VLAN.
- Since almost all networks are larger than a single switch, there should be a way to send traffic between two switches.
- One simple and easy way to do this is to assign a port on each network switch with a VLAN and run a cable between them.

VLAN Tag

Vlan Tags help identify the VLAN to which a received frame belongs. IEEE 802.1Q defines a 4-byte VLAN tag for Ethernet frames, enabling switches to identify the VLANs to which received frames belong.

Figure 3. Untagged Frame

Figure 4. Tagged Frame

Components of VLAN Tag

- Tag protocol identifier (TPID): identifies the type of a frame. The value 0x8100 indicates an IEEE 802.1Q frame.

- PRI: identifies the priority of a frame, which is mainly used for QoS.
- Canonical format indicator (CFI): indicates whether a MAC address is in the canonical format. For Ethernet frames, the value of this field is 0.
- VLAN ID: identifies the VLAN to which a frame belongs.

Figure 5. Vlan Tag Components

Types of VLANs

Here are the important types of VLANs

- Post-Based VLAN
- Protocol-Based VLAN
- MAC-Based VLAN

Port-Based VLAN

Port-based VLANs group virtual local area networks by port. In this type of virtual LAN, a switch port can be configured manually to a member of VLAN.

Devices that are connected to this port will belong to the same broadcast domain that is because all other ports are configured with a similar VLAN number.

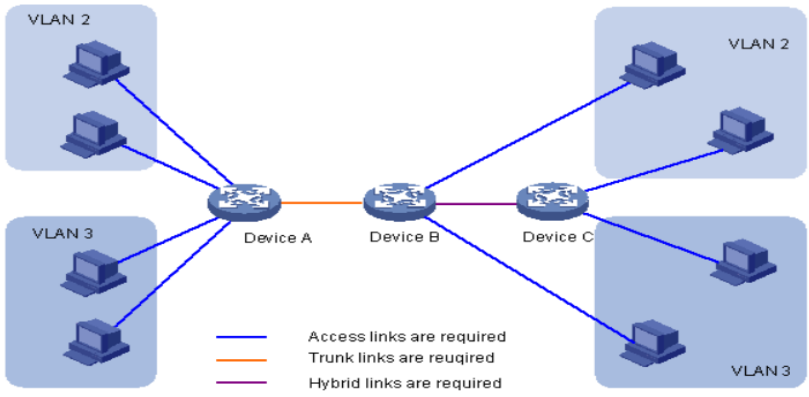


Figure 6. Port-Based VLAN

Protocol Based VLAN

This type of VLAN processes traffic based on a protocol that can be used to define filtering criteria for tags, which are untagged packets.

In this VLAN, the layer-3 protocol is carried by the frame to determine VLAN membership. It works in multi-protocol environments. This method is not practical in a predominately IP based network.

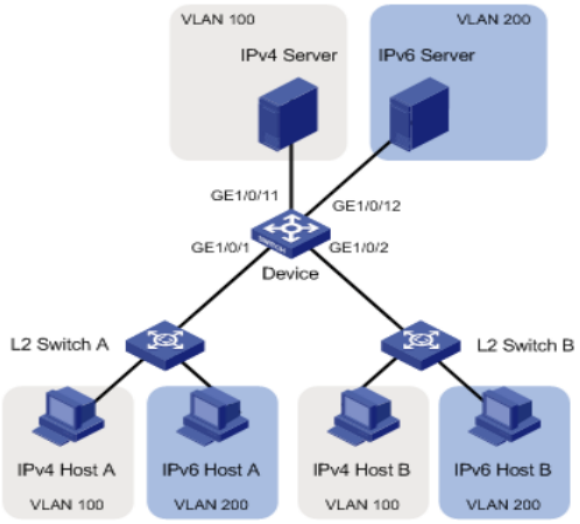


Figure 7. Protocol-Based VLAN

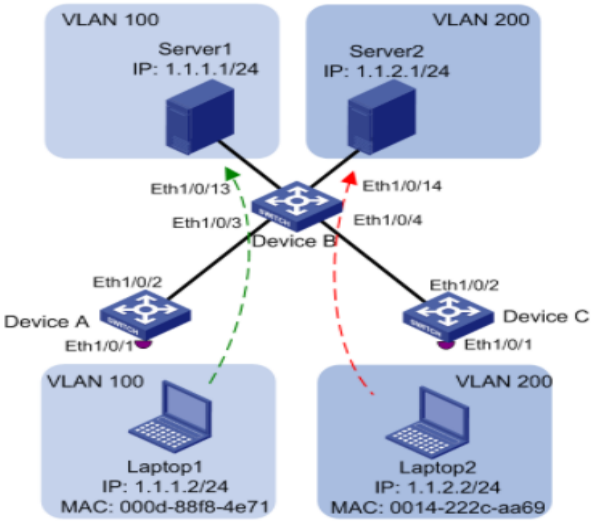


Figure 8. MAC-Based VLAN

MAC Based VLAN

MAC Based VLAN allows incoming untagged packets to be assigned virtual LAN and, thereby, classify traffic depending on the packet source address. You define a Mac address to VLAN mapping by configuring mapping the entry in MAC to the VLAN table.

This entry is specified using the source Mac address proper VLAN ID. The configurations of tables are shared among all device ports.

VLAN Ranges

Here are the important ranges of VLAN:

Range	Description
VLAN 0-4095	Reserved VLAN, which cannot be seen or used.
VLAN 1:	This is a default VLAN of switches. You cannot delete or edit this VLAN, but it can be used.
VLAN 2-1001:	It is a normal VLAN range. You can create, edit, and delete it.
VLAN 1002-1005:	These ranges are CISCO defaults for token rings and FDDI. You cannot delete this VLAN.
VLAN 1006-4094:	It is an extended range of VLANs.

Example of VLAN

In the below example, there are 6 hosts on 6 switches having different VLANs. You need 6 ports to connect switches together. It means, if you have 24 various VLANs, you will have only 24 hosts on 45 port switches.

Figure 9. Example of VLAN

Application/Purpose of VLAN

Here are the important uses of VLAN:

- VLAN is used when you have 200+ devices on your LAN.
- It is helpful when you have a lot of traffic on a LAN.
- VLAN is ideal when a group of users need more security or are being slowed down by many broadcasts.
- It is used when users are not on one broadcast domain.
- Make a single switch into multiple switches.

Basic Configuration Commands

Command	Description
	VLAN (To be used in system view)
vlan *vlan-id*	This command creates a VLAN and displays the VLAN view. If the VLAN to be created already exists, this command directly displays the VLAN view (value of vlan-id is an integer that ranges from 1 - 4096)
vlan *batch* {*vlan-id1* [to *vlan-id2*]}	This command creates VLAN in a batch. In this command. • "batch" creates VLANs in a batch • "vlan-id1" specifies a start VLAN ID. • "vlan-id2" specifies an end VLAN ID.

	Access Interface (To be used in interface view)
port link-type access	In the interface view, set the link type of the interface to access.
port default vlan *vlan-id*	In the interface view, configure a default VLAN for the interface and add the interface to the VLAN. • "vlan-id" specifies an ID for the default VLAN (value of vlan-id is an integer that ranges from 1 - 4096)
	Trunk Interface (To be used in interface view)
port link-type trunk	Set the link type of the interface to trunk.
port trunk allow-pass vlan { { *vlan-id1* [to *vlan-id2*] } | all }	Add the trunk interface to specified VLANs.
port trunk pvid vlan vlan-id	In the interface view, configure a default VLAN for the trunk interface.
	Hybrid Interface (To be used in interface view)
port link-type hybrid	Set the link type of the interface to hybrid.
port hybrid untagged vlan { { *vlan-id1* [to *vlan-id2*] } | all }	Add the hybrid interface to specified VLANs in untagged mode.
port hybrid tagged vlan { { *vlan-id1* [to *vlan-id2*] } | all }	Add the hybrid interface to specified VLANs in tagged mode.
port hybrid pvid vlan vlan-id	Configure a default VLAN for the hybrid interface.

Lab Task (Lab # 04):

Implement the following VLAN scenario in eNSP simulator: