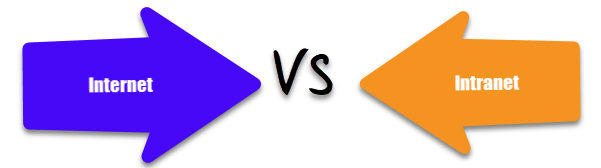
UNIT 1 WMC

Comparison between LAN, MAN, WANS.

| LAN | MAN | WAN |
| --- | --- | --- |
| LAN stands for local area network. | MAN stands for metropolitan area network. | WAN stands for wide area network. |
| LAN’s ownership is private. | MAN’s ownership can be private or public. | While WAN also might not be owned by one organization. |
| The transmission speed of a LAN is high. | While the transmission speed of a MAN is average. | Whereas the transmission speed of a WAN is low. |
| The propagation delay is short in a LAN. | There is a moderate propagation delay in a MAN. | Whereas, there is a long propagation delay in a WAN. |
| There is less congestion in LAN. | While there is more congestion in MAN. | Whereas there is more congestion than MAN in WAN. |
| LAN’s design and maintenance is easy. | While MAN’s design and maintenance is difficult than LAN. | Whereas WAN’s design and maintenance is also difficult than LAN as well MAN. |
| There is more fault tolerance in LAN. | While there is less fault tolerance. | In WAN, there is also less fault tolerance. |

………………………………………………………………………………………………………………………………………………………………

**Difference between Internet and Intranet**

[](https://cdn.guru99.com/images/1/020820_1146_InternetvsI1.png)

|  |  |
| --- | --- |
| **Internet** | **Intranet** |
| The Internet is a wide network of computers and is available to all. | Intranet is a network of computers designed for a certain group of users. |
| Internet contains a large number of intranets. | Intranet can be accessed from the Internet with specific restrictions. |
| Number of internet users are very high. | Number of users is limited. |
| Internet contains various source of information. | Intranet only contains group-specific information. |
| Anyone can access the internet | Accessible only by the organization employees or admin who have login details. |
| It is not as safe as compared to intranet | Safe and secure network. |
| It is a public network. | It is a private network. |

**Application of Internet**

Here, are important applications of Internet

* Download programs and files
* To send and receive E-Mails
* Voice and video Conferencing
* E-Commerce
* File sharing
* Browsing various types of Information
* Search the web addresses for access through the search engine and chatting

**Application of Intranet**

Here, are important applications of internet

* Sharing the detail of company rules/policies & regulations
* Access employee database
* Access product & customer data
* Sharing some common information
* Intranet also use for launching personal or department-specific home pages
* Submission of reports
* Corporate telephone directories

………………………………………………………………………………………………………………………………………………………………

**What are network devices?**

Network devices, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer network.

**Types of network devices**

Here is the common network device list:

* Hub
* Switch
* Router
* Bridge
* Gateway
* Modem
* Repeater
* Access Point

## Hub

Hubs connect multiple computer networking devices together. A hub also acts as a repeater in that it amplifies signals that deteriorate after traveling long distances over connecting cables. A hub is the simplest in the family of network connecting devices because it connects LAN components with identical protocols.

A hub can be used with both digital and analog data, provided its settings have been configured to prepare for the formatting of the incoming data. For example, if the incoming data is in digital format, the hub must pass it on as packets; however, if the incoming data is analog, then the hub passes it on in signal form.

Hubs do not perform packet filtering or addressing functions; they just send data packets to all connected devices. Hubs operate at the Physical layer of the Open Systems Interconnection (OSI) model. There are two types of hubs: simple and multiple port.

## Switch

Switches generally have a more intelligent role than hubs. A switch is a multiport device that improves network efficiency. The switch maintains limited routing information about nodes in the internal network, and it allows connections to systems like hubs or routers. Strands of LANs are usually connected using switches. Generally, switches can read the hardware addresses of incoming packets to transmit them to the appropriate destination.

Using switches improves network efficiency over hubs or routers because of the virtual circuit capability. Switches also improve network security because the virtual circuits are more difficult to examine with network monitors. You can think of a switch as a device that has some of the best capabilities of routers and hubs combined. A switch can work at either the Data Link layer or the Network layer of the OSI model. A multilayer switch is one that can operate at both layers, which means that it can operate as both a switch and a router. A multilayer switch is a high-performance device that supports the same routing protocols as routers.

Switches can be subject to distributed denial of service (DDoS) attacks; flood guards are used to prevent malicious traffic from bringing the switch to a halt. Switch port security is important so be sure to secure switches: Disable all unused ports and use DHCP snooping, ARP inspection and MAC address filtering.

## Router

Routers help transmit packets to their destinations by charting a path through the sea of interconnected networking devices using different network topologies. Routers are intelligent devices, and they store information about the networks they’re connected to. Most routers can be configured to operate as packet-filtering firewalls and use access control lists (ACLs). Routers, in conjunction with a channel service unit/data service unit (CSU/DSU), are also used to translate from LAN framing to WAN framing. This is needed because LANs and WANs use different network protocols. Such routers are known as border routers. They serve as the outside connection of a LAN to a WAN, and they operate at the border of your network.

Router are also used to divide internal networks into two or more subnetworks. Routers can also be connected internally to other routers, creating zones that operate independently. Routers establish communication by maintaining tables about destinations and local connections. A router contains information about the systems connected to it and where to send requests if the destination isn’t known. Routers usually communicate routing and other information using one of three standard protocols: Routing Information Protocol (RIP), Border Gateway Protocol (BGP) or Open Shortest Path First (OSPF).

Routers are your first line of defense, and they must be configured to pass only traffic that is authorized by network administrators. The routes themselves can be configured as static or dynamic. If they are static, they can only be configured manually and stay that way until changed. If they are dynamic, they learn of other routers around them and use information about those routers to build their routing tables.

Routers are general-purpose devices that interconnect two or more heterogeneous networks. They are usually dedicated to special-purpose computers, with separate input and output network interfaces for each connected network. Because routers and gateways are the backbone of large computer networks like the internet, they have special features that give them the flexibility and the ability to cope with varying network addressing schemes and frame sizes through segmentation of big packets into smaller sizes that fit the new network components. Each router interface has its own Address Resolution Protocol (ARP) module, its own LAN address (network card address) and its own Internet Protocol (IP) address. The router, with the help of a routing table, has knowledge of routes a packet could take from its source to its destination. The routing table, like in the bridge and switch, grows dynamically. Upon receipt of a packet, the router removes the packet headers and trailers and analyzes the IP header by determining the source and destination addresses and data type, and noting the arrival time. It also updates the router table with new addresses not already in the table. The IP header and arrival time information is entered in the routing table. Routers normally work at the Network layer of the OSI model.

## Bridge

Bridges are used to connect two or more hosts or network segments together. The basic role of bridges in network architecture is storing and forwarding frames between the different segments that the bridge connects. They use hardware Media Access Control (MAC) addresses for transferring frames. By looking at the MAC address of the devices connected to each segment, bridges can forward the data or block it from crossing. Bridges can also be used to connect two physical LANs into a larger logical LAN.

Bridges work only at the Physical and Data Link layers of the OSI model. Bridges are used to divide larger networks into smaller sections by sitting between two physical network segments and managing the flow of data between the two.

Bridges are like hubs in many respects, including the fact that they connect LAN components with identical protocols. However, bridges filter incoming data packets, known as frames, for addresses before they are forwarded. As it filters the data packets, the bridge makes no modifications to the format or content of the incoming data. The bridge filters and forwards frames on the network with the help of a dynamic bridge table. The bridge table, which is initially empty, maintains the LAN addresses for each computer in the LAN and the addresses of each bridge interface that connects the LAN to other LANs. Bridges, like hubs, can be either simple or multiple port.

Bridges have mostly fallen out of favor in recent years and have been replaced by switches, which offer more functionality. In fact, switches are sometimes referred to as “multiport bridges” because of how they operate.

## Gateway

Gateways normally work at the Transport and Session layers of the OSI model. At the Transport layer and above, there are numerous protocols and standards from different vendors; gateways are used to deal with them. Gateways provide translation between networking technologies such as Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP). Because of this, gateways connect two or more autonomous networks, each with its own routing algorithms, protocols, topology, domain name service, and network administration procedures and policies.

Gateways perform all of the functions of routers and more. In fact, a router with added translation functionality is a gateway. The function that does the translation between different network technologies is called a protocol converter.

## Modem

Modems (modulators-demodulators) are used to transmit digital signals over analog telephone lines. Thus, digital signals are converted by the modem into analog signals of different frequencies and transmitted to a modem at the receiving location. The receiving modem performs the reverse transformation and provides a digital output to a device connected to a modem, usually a computer. The digital data is usually transferred to or from the modem over a serial line through an industry standard interface, RS-232. Many telephone companies offer DSL services, and many cable operators  use modems as end terminals for identification and recognition of home and personal users. Modems work on both the Physical and Data Link layers.

## Repeater

A repeater is an electronic device that amplifies the signal it receives. You can think of repeater as a device which receives a signal and retransmits it at a higher level or higher power so that the signal can cover longer distances, more than 100 meters for standard LAN cables. Repeaters work on the Physical layer.

## Access Point

While an access point (AP) can technically involve either a wired or wireless connection, it commonly means a wireless device. An AP works at the second OSI layer, the Data Link layer, and it can operate either as a bridge connecting a standard wired network to wireless devices or as a router passing data transmissions from one access point to another.

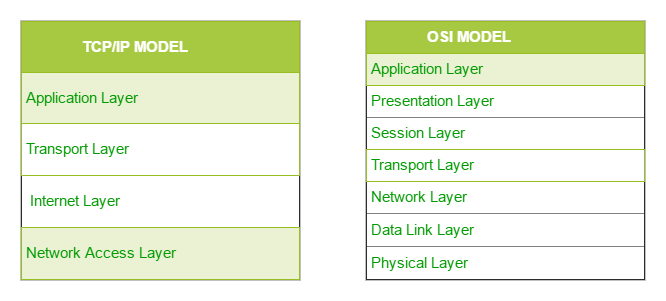
……………………………………………………………………………………………………………………………

# TCP/IP Model

The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

The diagrammatic comparison of the TCP/IP and OSI model is as follows :



Difference between TCP/IP and OSI Model:

|  |  |
| --- | --- |
| TCP/IP | OSI |
| TCP refers to Transmission Control Protocol. | OSI refers to Open Systems Interconnection. |
| TCP/IP has 4 layers. | OSI has 7 layers. |
| TCP/IP is more reliable | OSI is less reliable |
| TCP/IP does not have very strict boundaries. | OSI has strict boundaries |
| TCP/IP follow a horizontal approach. | OSI follows a vertical approach. |
| TCP/IP uses both session and presentation layer in the application layer itself. | OSI uses different session and presentation layers. |
| TCP/IP developed protocols then model. | OSI developed model then protocol. |
| Transport layer in TCP/IP does not provide assurance delivery of packets. | In OSI model, transport layer provides assurance delivery of packets. |
| TCP/IP model network layer only provides connection less services. | Connection less and connection oriented both services are provided by network layer in OSI model. |
| Protocols cannot be replaced easily in TCP/IP model. | While in OSI model, Protocols are better covered and is easy to replace with the change in technology. |

### 1. Network Access Layer –

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.  
We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

### 2. Internet Layer –

This layer parallels the functions of OSI’s Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are:

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:  
   IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses is limited in number when compared to the number of users.
2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagram and is responsible for providing hosts with information about network problems.
3. **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

### 3. Host-to-Host Layer –

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

1. **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
2. **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

### 4. Application Layer –

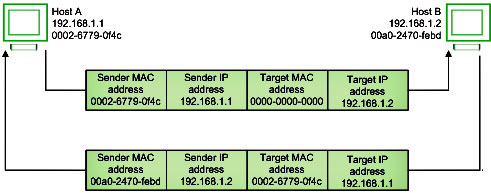
This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

* + 1. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL (Secure Socket Layer). It is efficient in cases where the browser needs to fill out forms, sign in, authenticate, and carry out bank transactions.
    2. **SSH –** SSH stands for Secure Shell. It is a terminal emulations software like Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
    3. **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it’s out of sync.

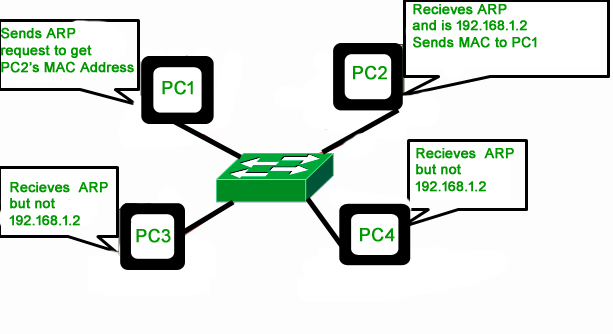
………………………………………………………………………………………………………………………………

### 1. Address Resolution Protocol (ARP) –

Address Resolution Protocol is a communication protocol used for discovering physical address associated with given network address. Typically, ARP is a network layer to data link layer mapping process, which is used to discover MAC address for given Internet Protocol Address.  
In order to send the data to destination, having IP address is necessary but not sufficient; we also need the physical address of the destination machine. ARP is used to get the physical address (MAC address) of destination machine.



Before sending the IP packet, the MAC address of destination must be known. If not so, then sender broadcasts the ARP-discovery packet requesting the MAC address of intended destination. Since ARP-discovery is broadcast, every host inside that network will get this message but the packet will be discarded by everyone except that intended receiver host whose IP is associated. Now, this receiver will send a unicast packet with its MAC address (ARP-reply) to the sender of ARP-discovery packet. After the original sender receives the ARP-reply, it updates ARP-cache and start sending unicast message to the destination.



### 2. Reverse Address Resolution Protocol (RARP) –

Reverse ARP is a networking protocol used by a client machine in a local area network to request its Internet Protocol address (IPv4) from the gateway-router’s ARP table. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.

When a new machine is setup or any machine which don’t have memory to store IP address, needs an IP address for its own use. So the machine sends a RARP broadcast packet which contains its own MAC address in both sender and receiver hardware address field.

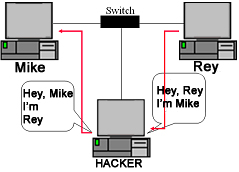


A special host configured inside the local area network, called as RARP-server is responsible to reply for these kind of broadcast packets. Now the RARP server attempt to find out the entry in IP to MAC address mapping table. If any entry matches in table, RARP server send the response packet to the requesting device along with IP address.

* LAN technologies like Ethernet, Ethernet II, Token Ring and Fiber Distributed Data Interface (FDDI) support the Address Resolution Protocol.
* RARP is not being used in today’s networks. Because we have much great featured protocols like BOOTP (Bootstrap Protocol) and DHCP (Dynamic Host Configuration Protocol).

### What is ARP poisoning (ARP spoofing) –

ARP spoofing is a type of network attack in which the attacker sends the falsified ARP request over the LAN (say to the default gateway), which results connecting attacker’s MAC address to the legitimate server on that victim network. Now, the attacker will start receiving the data which was intended for that IP address. With the help of ARP Poisoning (or ARP Spoofing) attacker is able to intercept data frames, modify traffic or even stop data in-transit.



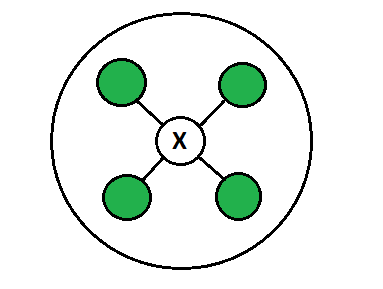
ARP poisoning can act as the opening for other major attacks, such as Man in the middle, denial of service, or session hijacking attacks.

………………………………………………………………………………………

# Routing Tables in Computer Network

Routers**:**

A Router is a networking device that forwards data packets between computer networks. This device is usually connected to two or more different networks. When a data packet comes to a router port, the router reads address information in packet to determine out which port the packet will be sent. For example, a router provides you with the internet access by connecting your LAN with the Internet.



When a packet arrives at a Router, it examines destination IP address of a received packet and make routing decisions accordingly. Routers use *Routing Tables* to determine out which interface the packet will be sent. A routing table lists all networks for which routes are known. Each router’s routing table is unique and stored in the RAM of the device.

**Routing Table:**

A routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables. See below a Routing Table:

**Destination** **Subnet mask** **Interface**

128.75.43.0 255.255.255.0 Eth0

128.75.43.0 255.255.255.128 Eth1

192.12.17.5 255.255.255.255 Eth3

default Eth2

The entry corresponding to the *default* gateway configuration is a network destination of 0.0.0.0 with a network mask (netmask) of 0.0.0.0. The Subnet Mask of default route is always 255.255.255.255 .

**Entries of an IP Routing Table:**

A routing table contains the information necessary to forward a packet along the best path toward its destination. Each packet contains information about its origin and destination. Routing Table provides the device with instructions for sending the packet to the next hop on its route across the network.

Each entry in the routing table consists of the following entries:

1. **Network ID:**

The network ID or destination corresponding to the route.

1. **Subnet Mask:**

The mask that is used to match a destination IP address to the network ID.

1. **Next Hop:**

The IP address to which the packet is forwarded

1. **Outgoing Interface:**

Outgoing interface the packet should go out to reach the destination network.

1. **Metric:**  
   A common use of the metric is to indicate the *minimum number of hops* (routers crossed) to the network ID.

Routing table entries can be used to store the following types of routes:

* Directly Attached Network IDs
* Remote Network IDs
* Host Routes
* Default Route
* Destination

……………………………………………………………………………………………………………………………………

## What is the Internet Control Message Protocol (ICMP)?

The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether data is reaching its intended destination in a timely manner. Commonly, the ICMP protocol is used on network devices, such as routers. ICMP is crucial for error reporting and testing, but it can also be used in distributed denial-of-service (DDoS) attacks.

## What is ICMP used for?

The primary purpose of ICMP is for error reporting. When two devices connect over the Internet, the ICMP generates errors to share with the sending device in the event that any of the data did not get to its intended destination. For example, if a packet of data is too large for a router, the router will drop the packet and send an ICMP message back to the original source for the data.

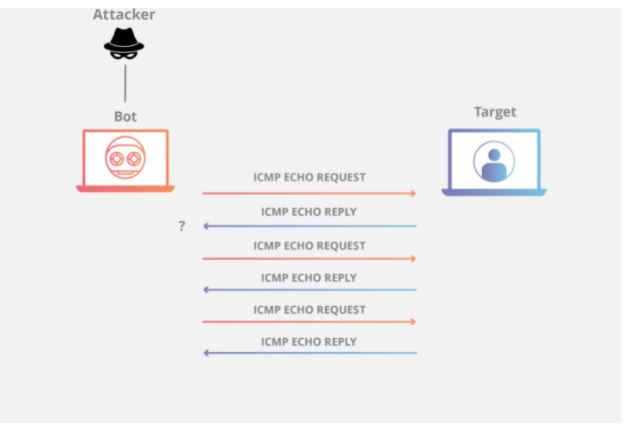
A secondary use of ICMP protocol is to perform network diagnostics; the commonly used terminal utilities traceroute and ping both operate using ICMP. The traceroute utility is used to display the routing path between two Internet devices. The routing path is the actual physical path of connected routers that a request must pass through before it reaches its destination. The journey between one router and another is known as a ‘hop,’ and a traceroute also reports the time required for each hop along the way. This can be useful for determining sources of network delay.

The ping utility is a simplified version of traceroute. A ping will test the speed of the connection between two devices and report exactly how long it takes a packet of data to reach its destination and come back to the sender’s device. Although ping does not provide data about routing or hops, it is still a very useful metric for gauging the latency between two devices. The ICMP echo-request and echo-reply messages are commonly used for the purpose of performing a ping.

Unfortunately network attacks can exploit this process, creating means of disruption such as the ICMP flood attack and the ping of death attack.

**ICMP flood attack**

A ping flood or ICMP flood is when the attacker attempts to overwhelm a targeted device with ICMP echo-request packets. The target has to process and respond to each packet, consuming its computing resources until legitimate users cannot receive service.



**Ping of death attack**

A ping of death attack is when the attacker sends a ping larger than the maximum allowable size for a packet to a targeted machine, causing the machine to freeze or crash. The packet gets fragmented on the way to its target, but when the target reassembles the packet into its original maximum-exceeding size, the size of the packet causes a buffer overflow.

…………………………………………………………………………………………………………………………………..

# Supernetting in Network Layer

**Supernetting** is the opposite of Subnetting. In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.

Supernetting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks. This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols.

More specifically,

* When multiple networks are combined to form a bigger network, it is termed as super-netting
* Super netting is used in route aggregation to reduce the size of routing tables and routing table updates

There are some points which should be kept in mind while supernetting:

1. All the Networks should be contiguous.
2. The block size of every networks should be equal and must be in form of 2n.
3. First Network id should be exactly divisible by whole size of supernet.

**Example –** Suppose 4 small networks of class C:

200.1.0.0,

200.1.1.0,

200.1.2.0,

200.1.3.0

Build a bigger network which have a single Network Id.

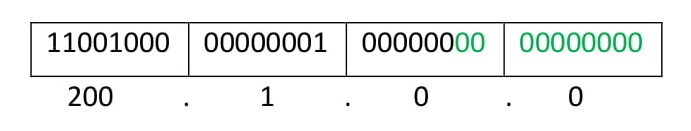
**Explanation –** Before Supernetting routing table will be look like as:

| Network Id | Subnet Mask | Interface |
| --- | --- | --- |
| 200.1.0.0 | 255.255.255.0 | A |
| 200.1.1.0 | 255.255.255.0 | B |
| 200.1.2.0 | 255.255.255.0 | C |
| 200.1.3.0 | 255.255.255.0 | D |

First, lets check whether three condition are satisfied or not:

1. **Contiguous:** You can easily see that all network are contiguous all having size 256 hosts.  
   Range of first Network from 200.1.0.0 to 200.1.0.255. If you add 1 in last IP address of first network that is 200.1.0.255 + 0.0.0.1, you will get the next network id that is 200.1.1.0. Similarly, check that all network are contiguous.
2. **Equal size of all network:** As all networks are of class C, so all of the have a size of 256 which in turn equal to 28.
3. **First IP address exactly divisible by total size:** When a binary number is divided by 2n then last n bits are the remainder. Hence in order to prove that first IP address is exactly divisible by while size of Supernet Network. You can check that if last n v=bits are 0 or not.

In given example first IP is 200.1.0.0 and whole size of supernet is 4\*28 = 210. If last 10 bits of first IP address are zero then IP will be divisible.



Last 10 bits of first IP address are zero (highlighted by green color). So 3rd condition is also satisfied.

Therefore, you can join all these 4 networks and can make a Supernet. New Supernet Id will be 200.1.0.0.

**Advantages of Supernetting –**

* 1. Control and reduce network traffic
  2. Helpful to solve the problem of lacking IP addresses
  3. Minimizes the routing table

**Disadvantages of Supernetting –**

* + - It cannot cover different area of network when combined
    - All the networks should be in same class and all IP should be contiguous

# Supernetting in Network Layer

**Supernetting** is the opposite of [Subnetting](https://www.geeksforgeeks.org/ip-addressing-classless-addressing/). In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.

Supernetting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks. This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols.

More specifically,

* When multiple networks are combined to form a bigger network, it is termed as super-netting
* Super netting is used in route aggregation to reduce the size of routing tables and routing table updates

There are some points which should be kept in mind while supernetting:

1. All the Networks should be contiguous.
2. The block size of every networks should be equal and must be in form of 2n.
3. First Network id should be exactly divisible by whole size of supernet.

**Example –** Suppose 4 small networks of class C:

200.1.0.0,

200.1.1.0,

200.1.2.0,

200.1.3.0

Build a bigger network which has a single Network Id.

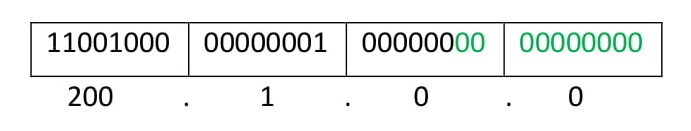
**Explanation –** Before Supernetting routing table will be look like as:

| Network Id | Subnet Mask | Interface |
| --- | --- | --- |
| 200.1.0.0 | 255.255.255.0 | A |
| 200.1.1.0 | 255.255.255.0 | B |
| 200.1.2.0 | 255.255.255.0 | C |
| 200.1.3.0 | 255.255.255.0 | D |

First, lets check whether three condition are satisfied or not:

1. **Contiguous:** You can easily see that all network are contiguous all having size 256 hosts.  
   Range of first Network from 200.1.0.0 to 200.1.0.255. If you add 1 in last IP address of first network that is 200.1.0.255 + 0.0.0.1, you will get the next network id that is 200.1.1.0. Similarly, check that all network are contiguous.
2. **Equal size of all network:** As all networks are of class C, so all of the have a size of 256 which in turn equal to 28.
3. **First IP address exactly divisible by total size:** When a binary number is divided by 2n then last n bits are the remainder. Hence in order to prove that first IP address is exactly divisible by while size of Supernet Network. You can check that if last n v=bits are 0 or not.

In given example first IP is 200.1.0.0 and whole size of supernet is 4\*28 = 210. If last 10 bits of first IP address are zero then IP will be divisible.



Last 10 bits of first IP address are zero (highlighted by green color). So 3rd condition is also satisfied.

Therefore, you can join all these 4 networks and can make a Supernet. New Supernet Id will be 200.1.0.0.

**Advantages of Supernetting –**

* 1. Control and reduce network traffic
  2. Helpful to solve the problem of lacking IP addresses
  3. Minimizes the routing table

**Disadvantages of Supernetting –**

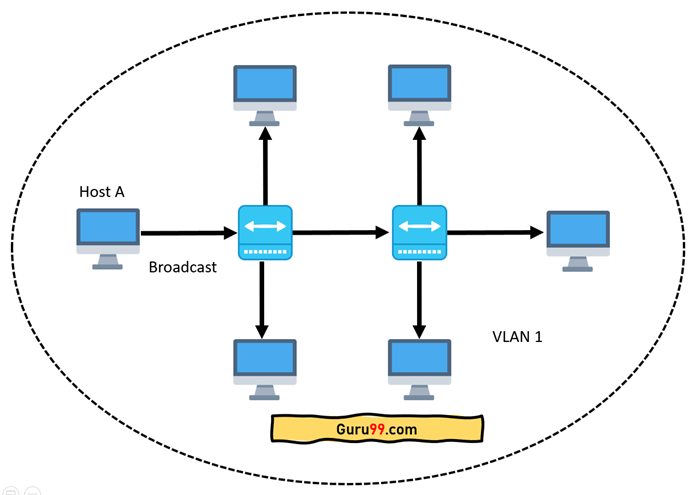
* + - It cannot cover different area of network when combined
    - All the networks should be in same class and all IP should be contiguous

…………………………………………………………………………………………………………………………………...

**What is VLAN?**

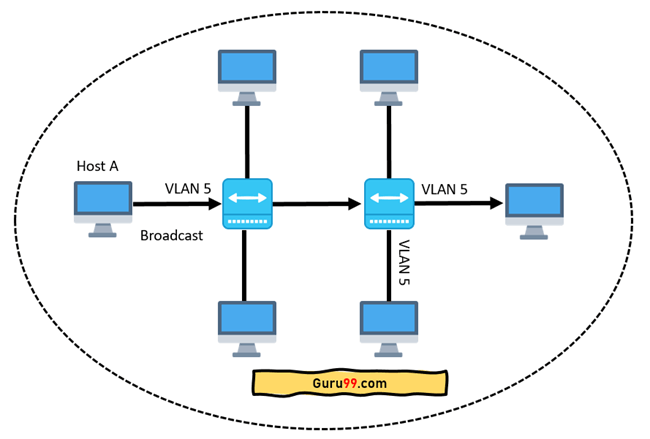
**VLAN** is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN. The full form of VLAN is defined as Virtual Local Area Network.

The below topology depicts a network having all hosts inside the same virtual LAN:

[](https://cdn.guru99.com/images/2/100720_0948_WhatisVLANT1.png)network having all hosts inside the same VLAN

Without VLANs, a broadcast sent from a host can easily reach all network devices. Each and every device will process broadcast received frames. It can increase the CPU overhead on each device and reduce the overall network security.

In case if you place interfaces on both switches into separate VLAN, a broadcast from host A can reach only devices available inside the same VLAN. Hosts of VLANs will not even be aware that the communication took place. This is shown in the below picture:

[](https://cdn.guru99.com/images/2/100720_0948_WhatisVLANT2.png)Host A can reach only devices available inside the same VLAN

VLAN in networking is a virtual extension of LAN. A 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 applications.

## 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 Ranges

Here are the important ranges of VLAN:

|  |  |
| --- | --- |
| **Range** | **Description** |
| VLAN 0 and 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. |

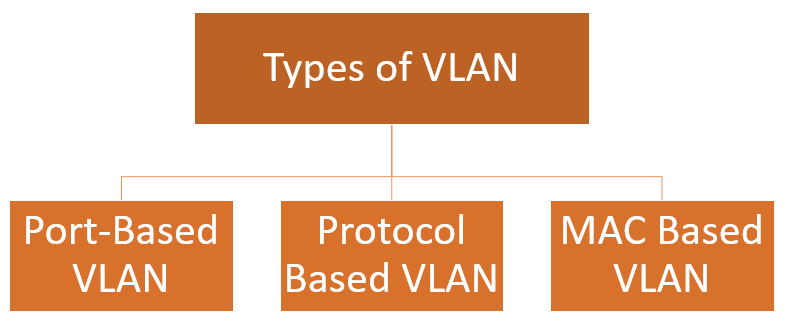
## Characteristics of VLAN

Here are the important characteristics of VLAN:

* Virtual LANs offer structure for making groups of devices, even if their networks are different.
* It increases the broadcast domains possible in a LAN.
* Implementing VLANs reduces the security risks as the number of hosts which are connected to the broadcast domain decreases.
* This is performed by configuring a separate virtual LAN for only the hosts having sensitive information.
* It has a flexible networking model that groups users depending on their departments instead of network location.
* Changing hosts/users on a VLAN is relatively easy. It just needs a new port-level configuration.
* It can reduce congestion by sharing traffic as individual VLAN works as a separate LAN.
* A workstation can be used with full bandwidth at each port.
* Terminal reallocations become easy.
* A VLAN can span multiple switches.
* The link of the trunk can carry traffic for multiple LANs.

## Types of VLANs

Here are the important types of VLANs

[](https://cdn.guru99.com/images/2/100720_0948_WhatisVLANT4.png)Types of VLAN

### Port-Based VLAN

Port-based VLANs groups virtual local area network 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.

The challenge of this type of network is to know which ports are appropriate to each VLAN. The VLAN membership can't be known just by looking at the physical port of a switch. You can determine it by checking the configuration information.

### 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 Virtual Local Area Network, 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.

### 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.

……………………………………………………………………………………………………………………………………………..

# CIDR (Classless Inter-Domain Routing or supernetting)

CIDR (Classless Inter-Domain Routing) -- also known as supernetting -- is a method of assigning Internet Protocol ([IP](https://searchunifiedcommunications.techtarget.com/definition/Internet-Protocol)) addresses that improves the efficiency of address distribution and replaces the previous system based on Class A, Class B and Class C networks. The initial goal of CIDR was to slow the increase of [routing tables](https://searchnetworking.techtarget.com/definition/routing-table) on routers across the internet and decrease the rapid exhaustion of [IPv4 addresses](https://whatis.techtarget.com/definition/IPv4-address-class). As a result, the number of available internet addresses has greatly increased.

The original classful network design of the internet included inefficiencies that drained the pool of unassigned IPv4 addresses faster than necessary. The classful design included the following:

* Class A, with over 16 million identifiers
* Class B, with 65,535 identifiers
* Class C, with 254 host identifiers

If an organization needed more than 254 host machines, it would be switched into Class B. However, this could potentially waste over 60,000 hosts if the business didn't need to use them, thus unnecessarily decreasing the availability of IPv4 addresses. CIDR was introduced by the Internet Engineering Task Force (IETF) in 1993 to fix this problem.

CIDR is based on variable-length subnet masking ([VLSM](https://searchnetworking.techtarget.com/definition/variable-length-subnet-mask)), which enables network engineers to divide an IP address space into a hierarchy of subnets of different sizes, making it possible to create [subnetworks](https://searchnetworking.techtarget.com/definition/subnet) with different host counts without wasting large numbers of addresses.

CIDR addresses are made up of two sets of numbers: a prefix, which is the [binary](https://whatis.techtarget.com/definition/binary) representation of the network address -- similar to what would be seen in a normal IP address -- and a suffix, which declares the total number of bits in the entire address. For example, CIDR notation may look like: 192.168.129.23/17 -- with 17 being the number of bits in the address. IPv4 addresses allow a maximum of 32 bits.

..................................................................................................................................

## What is DNS?

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to [IP addresses](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/) so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

## How does DNS work?

The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device - like a street address is used to find a particular home. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (example.com) and the machine-friendly address necessary to locate the example.com webpage.

..................................................................................................................................

# Network Address Translation (NAT)

To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required.

**Network Address Translation (NAT):-**  is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

**Network Address Translation (NAT) working –**

Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

If NAT runs out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

……………………………………………………………………………………………………………………………………….

# Introduction to IPv6 Addresses

IPv6 uses a 128-bit addressing model compared with the 32-bit addresses used for IPv4. In addition to being larger, IPv6 addresses differ from IPv4 addresses in several ways:

* Notation
* Prefixes
* Address types

These differences give IPv6 addressing greater simplicity and scalability than IPv4 addressing gives.

IPv6 Notation

IPv6 addresses are 128 bits long (expressed as 32 hexadecimal numbers) and consist of eight colon-delimited sections. Each section contains 2 bytes, and each byte is expressed as a hexadecimal number from 0 through FF.

An IPv6 address looks like this:

2001:0db8:0000:0000:0000:0800:200c:7334

By omitting the leading zeroes from each section or substituting contiguous sections that contain zeroes with a double colon, you can write the example address as:

2001:db8:0:0:0:800:200c:7334 or 2001:db8::800:200c:7334

You can use the double-colon delimiter only once within a single IPv6 address.

For example, you cannot express the IPv6 address 2001:db8:0000:0000:ea34:0000:71ff:fe01 as 2001:db8::ea34::71ff:fe0.

IPv6 Prefixes

An IPv6 address prefix represents a block of address space or a network. The prefix is a combination of an IPv6 prefix (address) and a prefix length. It takes the form ipv6-prefix/prefix-length.

IPv6 addresses can be broken into prefixes of varying length. The prefix length is a decimal value that specifies the number of the leftmost bits in the address that make up the prefix. The prefix length follows a forward slash and, in most cases, identifies the portion of the address owned by an organization. All remaining bits (up to the right-most bit) represent individual nodes or interfaces.

For example, 2001:db8:0000:0000:250:af:34ff:fe26/64 has a prefix length of 64.

The first 64 bits of this address (2001:db8:0000:0000) are the prefix. The rest (250:af:34ff:fe26) identify the interface.

…………………………………………………………………………………………………………………………….