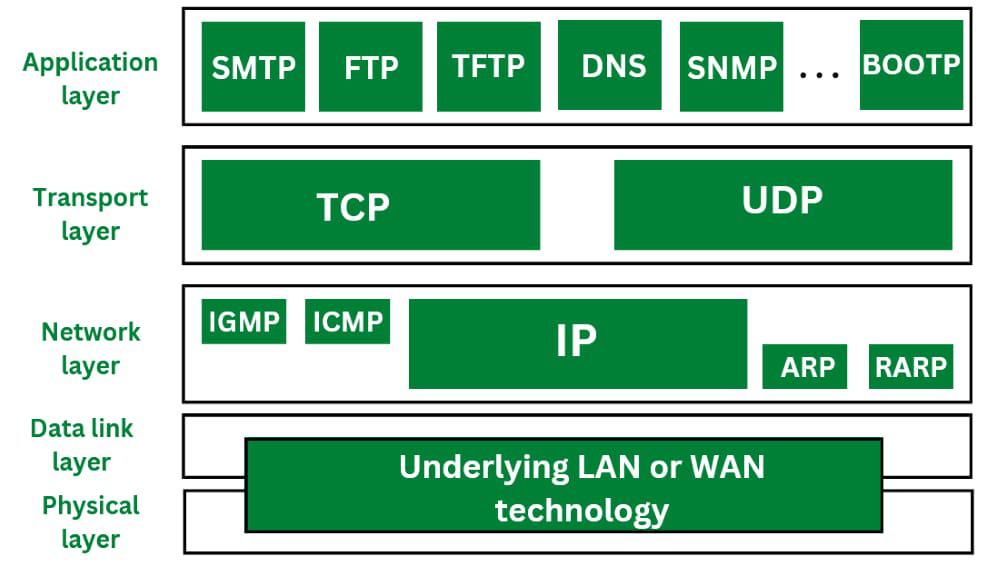
**Network Layer Protocols**

There are various protocols used in the network layer. Each protocol is used for a different task. Below are the protocols used in the network layer:



**1. IP (Internet Protocol)**

IP stands for Internet Protocol. Internet Protocol helps to uniquely identify each device on the network. Internet protocol is responsible for transferring the data from one node to another node in the network. Internet protocol is a connectionless protocol therefore it does not guarantee the delivery of data. For the successful delivery higher level protocols such as TCP are used to guarantee the data transmission. The Internet Protocol is divided in two types. They are:

* **IPv4:** IPv4 provides with the 32 bit address scheme. IPv4 addressing has four numeric fields and are separated by dot. IPv4 can be configured either using DHCP or manually. IPv4 does not provide with more security features as it does not support authentication or encryption techniques. IPv4 is further divided into five classes as Class A, Class B, Class C, Class D and Class E.
* **IPv6:** IPv6 is the most recent version of IP. If provided with a 128 bit addressing scheme. IP address has eight fields that are separated by colon, and these fields are alphanumeric. The IPv6 address is represented in hexadecimal. IPv6 provides with more security features such as authentication and encryption. IPv6 supports end-to-end connection integrity. IPv6 provides with more range of IP address as compared to IPv4.

**Difference Between IPv4 and IPv6**

Last Updated : 30 Aug, 2024

The address through which any computer communicates with our computer is simply called an Internet Protocol Address or IP address. For example, if we want to load a web page or download something, we require the address to deliver that particular file or webpage. That address is called an IP Address.

There are two versions of IP: IPv4 and IPv6. IPv4 is the older version, while IPv6 is the newer one. Both have their own features and functions, but they differ in many ways. Understanding these differences helps us see why we need IPv6 as the internet grows and evolves.

**What is IP?**

An IP, or Internet Protocol address, is a unique set of numbers assigned to each device connected to a network, like the Internet. It’s like an address for your computer, phone, or any other device, allowing them to communicate with each other. When you visit a website, your device uses the IP address to find and connect to the website’s server.

**Types of IP Addresses**

* [IPv4 (Internet Protocol Version 4)](https://www.geeksforgeeks.org/what-is-ipv4/)
* [IPv6 (Internet Protocol Version 6)](https://www.geeksforgeeks.org/internet-protocol-version-6-ipv6/)

To deepen your understanding of networking concepts like IPv4 and IPv6, consider enrolling in the [**GATE CS Self-Paced course.**](https://gfgcdn.com/tu/R8X/) This course covers crucial topics needed for GATE preparation and provides a strong foundation in computer science, equipping you with the skills needed to excel in your studies and career.

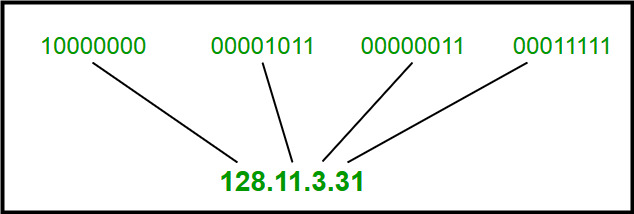
**What is IPv4?**

IPv4 addresses consist of two things: the network address and the host address. It stands for **Internet Protocol version four.** It was introduced in 1981 by DARPA  and was the first deployed version in 1982 for production on SATNET and on the ARPANET in January 1983.

IPv4 addresses are 32-bit integers that have to be expressed in Decimal Notation. It is represented by 4 numbers separated by dots in the range of 0-255, which have to be converted to 0 and 1, to be understood by Computers. For Example, An IPv4 Address can be written as **189.123.123.90.**

**IPv4 Address Format**

IPv4 Address Format is a 32-bit Address that comprises binary digits separated by a dot (.).



IPv4 Address Format

**Drawback of IPv4**

* **Limited Address Space** : IPv4 has a limited number of addresses, which is not enough for the growing number of devices connecting to the internet.
* **Complex Configuration** : IPv4 often requires manual configuration or DHCP to assign addresses, which can be time-consuming and prone to errors.
* **Less Efficient Routing** : The IPv4 header is more complex, which can slow down data processing and routing.
* **Security Issues** : IPv4 does not have built-in security features, making it more vulnerable to attacks unless extra security measures are added.
* **Limited Support for Quality of Service (QoS)** : IPv4 has limited capabilities for prioritizing certain types of data, which can affect the performance of real-time applications like video streaming and VoIP.
* **Fragmentation** : IPv4 allows routers to fragment packets, which can lead to inefficiencies and increased chances of data being lost or corrupted.
* **Broadcasting Overhead** : IPv4 uses broadcasting to communicate with multiple devices on a network, which can create unnecessary network traffic and reduce performance.

**What is IPv6?**

IPv6 is based on IPv4 and stands for Internet Protocol version 6. It was first introduced in December 1995 by Internet Engineering Task Force. IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. IPv6 is written as a group of 8 hexadecimal numbers separated by colon (:). It can be written as 128 bits of 0s and 1s.

**IPv6 Address Format**

IPv6 Address Format is a 128-bit IP Address, which is written in a group of 8 hexadecimal numbers separated by colon (:).



IPv6 Address Format

To switch from IPv4 to IPv6, there are several strategies:

* **Dual Stacking** : Devices can use both IPv4 and IPv6 at the same time. This way, they can talk to networks and devices using either version.
* **Tunneling** : This method allows IPv6 users to send data through an IPv4 network to reach other IPv6 users. Think of it as creating a “tunnel” for IPv6 traffic through the older IPv4 system.
* **Network Address Translation (NAT)** : NAT helps devices using different versions of IP addresses (IPv4 and IPv6) to communicate with each other by translating the addresses so they understand each other.

**Difference Between IPv4 and IPv6**

|  |  |
| --- | --- |
| **IPv4** | **IPv6** |
| IPv4 has a 32-bit address length | IPv6 has a 128-bit address length |
| It Supports Manual and [DHCP](https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/) address configuration | It supports Auto and renumbering address configuration |
| In IPv4 end to end, connection integrity is Unachievable | In IPv6 end-to-end, connection integrity is Achievable |
| It can generate 4.29×10 9 address space | The address space of IPv6 is quite large it can produce 3.4×10 38 address space |
| The Security feature is dependent on the application | IPSEC is an inbuilt security feature in the IPv6 protocol |
| Address representation of IPv4 is in decimal | Address representation of IPv6 is in hexadecimal |
| [Fragmentation](https://www.geeksforgeeks.org/what-is-fragmentation-in-operating-system/) performed by Sender and forwarding routers | In IPv6 fragmentation is performed only by the sender |
| In IPv4 Packet flow identification is not available | In IPv6 packet flow identification are Available and uses the flow label field in the header |
| In IPv4 checksum field is available | In IPv6 [checksum](https://www.geeksforgeeks.org/difference-between-checksum-and-crc/) field is not available |
| It has a broadcast Message Transmission Scheme | In IPv6 multicast and any cast message transmission scheme is available |
| In IPv4 Encryption and Authentication facility not provided | In IPv6 [Encryption](https://www.geeksforgeeks.org/what-is-data-encryption/) and Authentication are provided |
| IPv4 has a header of 20-60 bytes. | IPv6 has a header of 40 bytes fixed |
| IPv4 can be converted to IPv6 | Not all IPv6 can be converted to IPv4 |
| IPv4 consists of 4 fields which are separated by addresses dot (.) | IPv6 consists of 8 fields, which are separated by a colon (:) |
| IPv4’s  IP addresses are divided into five different classes. Class A , Class B, Class C, Class D , Class E. | IPv6 does not have any classes of the IP address. |
| IPv4 supports VLSM( [Variable Length subnet mask](https://www.geeksforgeeks.org/introduction-of-variable-length-subnet-mask-vlsm/) ). | IPv6 does not support VLSM. |
| Example of IPv4:  66.94.29.13 | Example of IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB |

**Benefits of IPv6 over IPv4**

The recent Version of IP IPv6 has a greater advantage over IPv4. Here are some of the mentioned benefits:

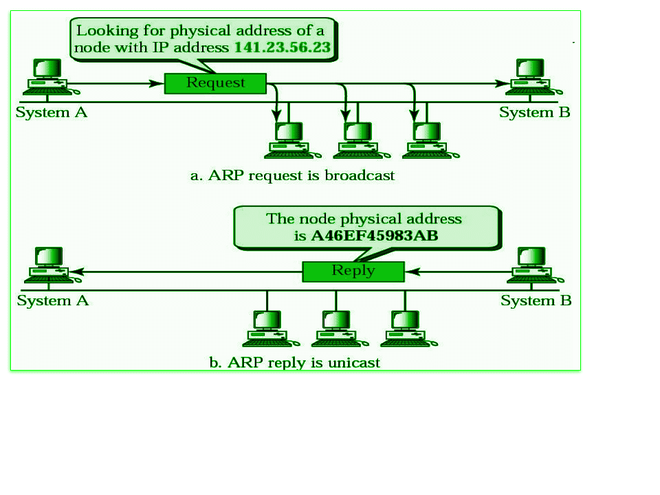
* **Larger Address Space:** IPv6 has a greater address space than IPv4, which is required for expanding the IP Connected Devices. IPv6 has 128 bit IP Address rather and IPv4 has a 32-bit Address.
* **Improved Security:** IPv6 has some improved security which is built in with it. IPv6 offers security like Data Authentication, Data Encryption, etc. Here, an Internet Connection is more Secure.
* **Simplified Header Format:** As compared to IPv4, IPv6 has a simpler and more effective header Structure, which is more cost-effective and also increases the speed of Internet Connection.
* **Prioritize:** IPv6 contains stronger and more reliable support for QoS features, which helps in increasing traffic over websites and increases audio and video quality on pages.
* **Improved Support for Mobile Devices:** IPv6 has increased and better support for Mobile Devices. It helps in making quick connections over other Mobile Devices and in a safer way than IPv4.

 **2. ARP (Address Resolution Protocol)**

ARP stands for Address Resolution Protocol. ARP is used to convert the logical address ie. IP address into physical address ie. MAC address. While communicating with other nodes, it is necessary to know the MAC address or physical address of the destination node. If any of the node in a network wants to know the physical address of another node in the same network, the host then sends an ARP query packet. This ARP query packet consists of IP address and MAC address of source host and only the IP address of destination host. This ARP packet is then received to every node present in the network. The node with its own IP address recognises it and sends it MAC address to the requesting node. But sending and receiving such packets to know the MAC address of destination node it increases the traffic load. Therefore in order to reduce this traffic and improve the performance, the systems that makes use of ARP maintain a cache of recently acquired IP into MAC address bindings.

**How Does ARP Work?**

* The host broadcasts an ARP inquiry packet containing the IP address over the network in order to find out the physical address of another computer on its network.
* The [ARP](https://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works/) packet is received and processed by all hosts on the network; however, only the intended recipient can identify the IP address and reply with the physical address.
* After adding the physical address to the datagram header and cache memory, the host storing the datagram transmits it back to the sender.



**Types of ARP Entries**

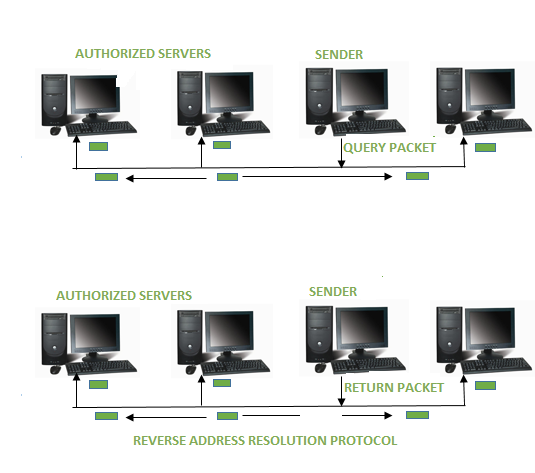
* **Static Entry:** This type of entry is created when a user uses the ARP command utility to manually enter the IP to MAC address association.
* **Dynamic Entry:** A dynamic entry is one that is automatically formed when a sender broadcasts their message to the whole network. Dynamic entries are periodically removed and are not permanent.

**3. RARP**

RARP stands for Reverse Address Resolution Protocol. RARP works opposite of ARP. Reverse Address Resolution Protocol is used to convert MAC address ie. physical address into IP address ie. logical address. RARP provides with a feature for the systems and applications to get their own IP address from a DNS( Domain Name System) or router. This type of resolution is required for various tasks such as executing reverse DNS lookup. As Reverse Address Resolution Protocol works at low level it requires direct network addresses. The reply from the server mostly carries a small information but the 32 bit internet address is used and it does not exploit the full potential of a network such as ethernet.

**How Does RARP Work?**

* Data is sent between two places in a network using the RARP, which is on the Network Access Layer.
* Every user on the network has two distinct addresses: their MAC (physical) address and their IP (logical) address.
* Software assigns the IP address, and the hardware then builds the MAC address into the device.
* Any regular computer connected to the network can function as the RARP server, answering to RARP queries. It must, however, store all of the MAC addresses’ associated IP addresses. Only these RARP servers are able to respond to RARP requests that are received by the network. The information package must be transmitted over the network’s lowest tiers.
* Using both its physical address and Ethernet broadcast address, the client transmits a [RARP](https://www.geeksforgeeks.org/what-is-rarp/) request. In response, the server gives the client its IP address.



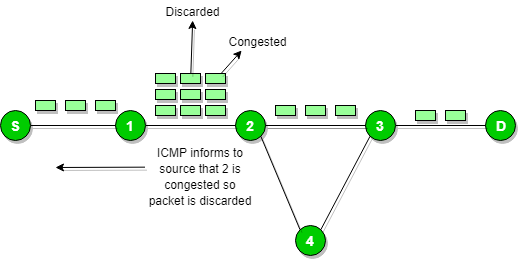
**4. ICMP**

ICMP stands for Internet Control Message Protocol. ICMP is a part of IP protocol suite. ICMP is an error reporting and network diagnostic protocol. Feedback in the network is reported to the designated host. Meanwhile, if any kind of error occur it is then reported to ICMP. ICMP protocol consists of many error reporting and diagnostic messages. ICMP protocol handles various kinds of errors such as time exceeded, redirection, source quench, destination unreachable, parameter problems etc. The messages in ICMP are divided into two types. They are given below:

* Error Message: Error message states about the issues or problems that are faced by the host or routers during processing of IP packet.
* Query Message: Query messages are used by the host in order to get information from a router or another host.

**How Does ICMP Work?**

* The main and most significant protocol in the IP suite is called ICMP. However, unlike TCP and UDP, ICMP is a connectionless protocol, meaning it doesn’t require a connection to be established with the target device in order to transmit a message.
* TCP and [ICMP](https://www.geeksforgeeks.org/internet-control-message-protocol-icmp/) operate differently from one another; TCP is a connection-oriented protocol, while ICMP operates without a connection. Every time a connection is made prior to a message being sent, a TCP Handshake is required of both devices.
* Datagrams including an IP header containing ICMP data are used to transmit ICMP packets. An independent data item like a packet is comparable to an ICMP datagram.



**5. IGMP**

IGMP stands for Internet Group Message Protocol. IGMP is a multicasting communication protocol. It utilizes the resources efficiently while broadcasting the messages and data packets. IGMP is also a protocol used by TCP/IP. Other hosts connected in the network and routers makes use of IGMP for multicasting communication that have IP networks. In many networks multicast routers are used in order to transmit the messages to all the nodes. Multicast routers therefore receives large number of packets that needs to be sent. But to broadcast this packets is difficult as it would increase the overall network load. Therefore IGMP helps the multicast routers by addressing them while broadcasting. As multicast communication consists of more than one senders and receivers the Internet Group Message Protocol is majorly used in various applications such as streaming media, web conference tools, games, etc.

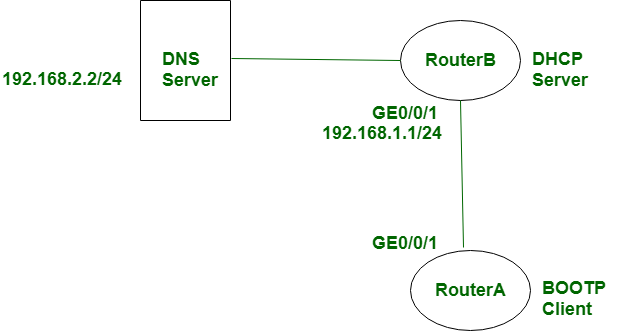
**How Does IGMP Work?**

* Devices that can support dynamic multicasting and multicast groups can use IGMP.
* The host has the ability to join or exit the multicast group using these devices. It is also possible to add and remove customers from the group using these devices.
* The host and local multicast router use this communication protocol. Upon creation of a multicast group, the packet’s destination IP address is changed to the multicast group address, which falls inside the class D IP address range.

**Difference between BOOTP and DHCP**

Last Updated : 25 Aug, 2024

**BOOTP** stands for **Bootstrap Protocol** and **DHCP** stands for **Dynamic Host Configuration Protocol**. These protocols square measure used for getting the information science address of the host alongside the bootstrap info. The operation of each protocol is totally different in some manner. Dynamic host configuration protocol is also the extended version of the Bootstrap Protocol.



**BOOTP (Bootstrap Protocol)**

BOOTP is a network protocol for assigning an [IP address](https://www.geeksforgeeks.org/what-is-an-ip-address/) to every piece of networking equipment and providing all the major configuration information, such as the [default gateway](https://www.geeksforgeeks.org/default-gateway-in-networking/) and the [subnet mask](https://www.geeksforgeeks.org/role-of-subnet-mask/). It was previously invented for the diskless workstations that needed to download their operating systems from a network server.

**Advantages of BOOTP**

* **Automatic IP Addressing:** BOOTP allows devices to automatically obtain an IP address and other pertinent network configurations without administrative intervention.
* **Central Management:** A network administrator can manage the assignment of IP addresses and their configurations from one central server, thereby making the management of a network easier.
* **Stable IP Addresses:** Most BOOTP implementations allot the same IP address for any given machine whenever it boots, which provides the same configuration for the network.
* **Legacy Support:** BOOTP is backward compatible; that is, it functions with older network devices and systems that may not support more modern protocols, such as DHCP.

**Disadvantages of BOOTP**

* **No Flexibility:** BOOTP does not provide any dynamic IP address leasing, hence is inefficient for IP address allocation in environments where devices are changing often.
* **Static Configuration:** BOOTP configurations are static and need to be updated manually on the server in case of any changes in the network settings; hence, it is not much adapted to dynamic network settings.
* **Slower Initialization:** BOOTP requires a more complex setup process compared to DHCP that can slow down the initialization of devices on a network.
* **Obsolescence:** BOOTP has been overridden by DHCP, which is much more functional and better suited to modern network configurations.

**DHCP – Dynamic Host Configuration Protocol**

DHCP refers to Dynamic Host Configuration Protocol. This is a network protocol used for automating the process of assigning IP addresses and other network configurations to devices on a network. Devices request and obtain an IP address and configuration information from the DHCP server; hence, in this case, managing the network becomes easy and efficient.

**Advantages of DHCP**

* **Auto-IP Assignment:** DHCP clients reserve or get auto-assignment of the IP address to a system, which decreases the manual configuration of the IP address and avoids address conflicts.
* **Centralized Management:** Network settings and IP address assignments are configured on a central DHCP server managed by the network administrators.
* **Dynamic IP Allocation:** DHCP can dynamically allocate and reclaim IP addresses depending on demand, optimizing IP address usage and accommodates devices which frequently join and leave the network.
* **Configuration Flexibility:** It configures various options on the network; DHCP supports a whole series of configuration options for the network, for example, subnet masks, default gateways, [DNS](https://www.geeksforgeeks.org/domain-name-system-dns-in-application-layer/) servers, many more. Hence, the protocol is adaptable to different network configurations.

**Disadvantages of DHCP**

* **Dependency Upon the DHCP Server:** If the [DHCP server](https://www.geeksforgeeks.org/dhcp-server-configuration-in-cisco/) goes down or is unavailable, the devices might not obtain the IP addresses, hence not connecting over the network.
* **Security Issues:** The DHCP, when not configured and secured properly, is prone to attacks, like DHCP [spoofing](https://www.geeksforgeeks.org/what-is-mac-spoofing-attack/). Here, unauthorized servers start issuing incorrect configuration information.
* **Leasing of IP Address:** IP addresses provided by DHCP are leased for some time. This may result in temporary shortages or inefficiency of address allocation, especially when devices are frequently added and removed from the network.
* **Complexity in Large Networks:** In large networks, handling a large number of DHCP servers or complex configuration takes a lot of time and needs a good planning and monitoring process.

**Difference Between BOOTP and DHCP**

|  |  |
| --- | --- |
| **BOOTP** | **DHCP** |
| [BOOTP](https://www.geeksforgeeks.org/bootstrap-protocol-bootp/) stands for Bootstrap Protocol. | While [DHCP](https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/) stands for Dynamic host configuration protocol. |
| BOOTP does not provide temporary IP addressing. | While DHCP provides temporary IP addressing for only limited amount of time. |
| BOOTP does not support DHCP clients. | While it support BOOTP clients. |
| In BOOTP, manual-configuration takes place. | While in DHCP, auto-configuration takes place. |
| BOOTP does not support mobile machines. | Whereas DHCP supports mobile machines. |
| BOOTP can have errors due to manual-configuration. | Whereas in DHCP errors do not occur mostly due to auto-configuration. |

**Conclusion**

BOOTP are two types that refer to the protocol in integrating the automation of assigning the IP address and the configuration of the network. BOOTP represents an older protocol, which provides static configuration; as in, every time this device connects, it is assigned the same IP address. DHCP, on the other hand, represents a modern protocol of dynamic allocation of IP addresses and appends several more features to its features list, which makes it really flexible and efficient in the management of large and dynamic networks.

**Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Brouters)**

**Network Devices:** Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, Brouter, and NIC, etc.

**1. Repeater** – A repeater operates at the physical layer. Its job is to amplifies (i.e., regenerates) the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

**2. Hub** –  A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices.  In other words, the [collision domain](https://en.wikipedia.org/wiki/Collision_domain) of all hosts connected through Hub remains one.  Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

**Types of Hub**

* **Active Hub:-** These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
* **Passive Hub:-** These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend the distance between nodes.
* **Intelligent Hub:-** It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

**3. Bridge** – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

**Types of Bridges**

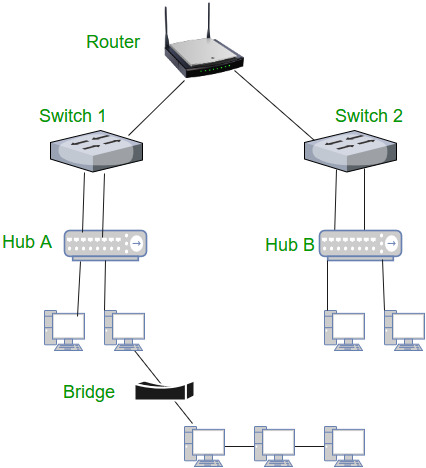
* **Transparent Bridges:-** These are the bridge in which the stations are completely unaware of the bridge’s existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
* **Source Routing Bridges:-** In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

**4. Switch** – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.  In other words, the switch divides the collision domain of hosts, but the [broadcast domain](https://en.wikipedia.org/wiki/Broadcast_domain) remains the same.

**Types of  Switch**

1. Unmanaged switches: These switches have a simple plug-and-play design and do not offer advanced configuration options. They are suitable for small networks or for use as an expansion to a larger network.
2. Managed switches: These switches offer advanced configuration options such as VLANs, QoS, and link aggregation. They are suitable for larger, more complex networks and allow for centralized management.
3. Smart switches: These switches have features similar to managed switches but are typically easier to set up and manage. They are suitable for small- to medium-sized networks.
4. Layer 2 switches: These switches operate at the Data Link layer of the OSI model and are responsible for forwarding data between devices on the same network segment.
5. Layer 3 switches: These switches operate at the Network layer of the OSI model and can route data between different network segments. They are more advanced than Layer 2 switches and are often used in larger, more complex networks.
6. PoE switches: These switches have Power over Ethernet capabilities, which allows them to supply power to network devices over the same cable that carries data.
7. Gigabit switches: These switches support Gigabit Ethernet speeds, which are faster than traditional Ethernet speeds.
8. Rack-mounted switches: These switches are designed to be mounted in a server rack and are suitable for use in data centers or other large networks.
9. Desktop switches: These switches are designed for use on a desktop or in a small office environment and are typically smaller in size than rack-mounted switches.
10. Modular switches: These switches have modular design, which allows for easy expansion or customization. They are suitable for large networks and data centers.

**5. Routers** – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.



**6. Gateway** – A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers.

**7. Brouter** – It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks and working as the bridge, it is capable of filtering local area network traffic.

**8. NIC** – NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN.  It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.