ANSWAR ; 1. What are the different types of network?

A computer network is a system in which multiple computers are connected to share information and resources. Computer network varies with each other based on their functionality, geography, ownership, and communication media used.

So, in this blog, we are going to learn about various types of computer networks based on geographical areas they cover, functionality, ownership, and communication media used.

A computer network can be divided into the following types, based on the geographical area that they cover, they are:

1. **LAN(Local Area Network)**
2. **MAN(Metropolitan Area Network)**
3. **WAN(Wide Area Network)**

Now, let us study these networks one by one:

LAN(Local Area Network)

A local area network is a network, which is designed to operate over a very small geographical or physical area such as an office, building, a group of buildings, etc.

Generally, it is used to connect two or more personal computers through a communication medium such as coaxial, twisted-pair cables, etc. A LAN can use either wired or wireless mode of communication. The LAN which entirely uses wireless media for communication can be termed as **WLAN(Wireless Local Area Network)**.

Local Area Networks came under existence in around 1970s. IEEE developed the specifications for LAN. The speed of this network varies from 10mbps(Ethernet network) to 1gbps(FDDI or Gigabit Ethernet).

In other words, a LAN connects a relatively small number of machines in a relatively close geographical area. Bus, Ring, and Star topology are generally used in a local area network. In LAN, one computer can become a server in a star topology, serving all other computers called clients. Two different buildings can be connected very easily in LAN using a 'Bridge'.

Ethernet LAN is the most commonly used LAN. The speed of a Local Area Network also depends on the topology used. ***For example,*** a LAN using bus topology has a speed of 10mbps to 100mbps, while in ring topology it is around 4mbps to 16mbps. LAN's are generally privately owned networks.

Following are the functionalities of a Local Area Network:

1. **File Serving:** In LAN, a large storage disk acts as a central storage repository.
2. **Print Serving:** Printers can be shared very easily in a LAN by various computers.

3. **Academic Support:** A LAN can be used in the classroom, labs, etc. for educational purposes.
4. **Manufacturing Support:** LAN can support the manufacturing and industrial environment.
5. **High Reliability:** Individual workstations might survive the network in case of failures.

Following are the advantages of a LAN:

1. File transfer and file access
2. Resource or peripherals sharing
3. Personal computing
4. Document distribution
5. Easy to design and troubleshoot
6. Minimum propagation delay
7. High data rate transfer
8. Low error rate
9. Easily scalable(devices can be added or removed very easily)

Following are the disadvantages of a LAN:

1. Equipment and support may be costly
2. Some hardware devices may not inter-operate properly

MAN(Metropolitan Area Network)

A Metropolitan Area Network is a bigger version of LAN that uses similar technology as LAN. It spans over a larger geographical area such as a town or an entire city.

It can be connected using an optical fiber cable as a communication medium. Two or more LAN's can also be connected using routers to create a MAN. When this type of network is created for a specific campus, then it is termed as CAN(Campus Area Network).

The MAN spans over a geographical area of about 50km. The best example of MAN is the cable television network that spans over the whole city.

A MAN can be either a public or privately owned network. Generally, a telephone exchange line is most commonly used as a communication medium in MAN. The protocols that are used in MAN are RS-232, Frame Relay, ISDN, etc.

Uses of MAN are as follows:

1. MAN can be used for connecting the various offices of the same organization, spread over the whole city.
2. It can be used for communication in various governmental departments.

Following are the advantages of using MAN:

1. Large geographical area cover as compared to LAN
2. High-speed data connectivity

3. The Propagation delay of MAN is moderate

Following are the disadvantages of MAN:

1. It is hard to design and maintain a MAN
2. MAN is less fault-tolerant
3. It is costlier to implement
4. Congestions are more in a MAN

WAN(Wide Area Network)

A Wide Area Network is the largest spread network. It spans over very large-distances such as a country, continent or even the whole globe. Two widely separated computers can be connected very easily using WAN. For Example, the Internet.

A WAN may include various Local and Metropolitan Area Network. The mode of communication in a WAN can either be wired or wireless. Telephone lines for wired and satellite links for wireless communication can be used in a wide area network.

In other words, WAN provides long distance transmission of data, voice, image, and video, over a large geographical area. A WAN may span beyond 100km range. It may be privately or publicly owned.

The protocols used in WAN are ISDN(Integrated Service Digital Network), SMDS(Switched Multi-Megabit Data Service), SONET(Synchronous Optical Network), HDLC(High Data Link Control), SDLC(Synchronous Data Link Control), etc.

The advantage of WAN is that it spans over a very large geographical area, and connects a huge mass of people.

Following are the disadvantages of WAN:

1. The propagation delay is more in a WAN
2. The data rate is low
3. The error rate is high
4. It is very complex to design a WAN

These are the types of network according to geographical area.

Following are the types of network, based on functionality:

- **Client-Server Network:** Client-Server network is a network in which a client runs the program and access data that are stored on the server. In this kind of network, one computer becomes the server, serving all other computers called clients.

- **Peer-to-Peer Network:** Peer-to-Peer network facilitates the flow of information from one peer to another without any central server. In other words, each node on a server acts as both client and server.

Following are the types of network, based on Ownership:

- **Private Network:** A private network is a network in which various restrictions are imposed to secure the network, to restrict unauthorized access. This type of network is privately owned by a single or group of people for their personal use. Local Area Network(LAN) can be used as a private network.
- **Public Network:** A public network is a network that has the least or no restrictions on it. It can be freely accessed by anyone, without any restrictions. This type of network is publicly owned by the government or NGOs. Metropolitan Area Network(MAN) and Wide Area Network(WAN) can be used as a public network.

Following are the types of network, based on Transmission Media:

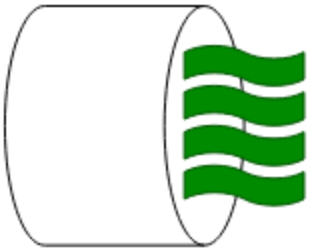
- **Bound/Guided Media Network:** Bounded/Guided media can also be referred to as wired media. This kind of networks provides a physical link between two nodes connected in a network. The physical links are directed towards a particular direction in the network. Co-axial, twisted pair, optical fiber cable, etc. can be used in such networks for connectivity. Local Area Network(LAN) and Metropolitan Area Network(MAN) can be used as a Bound/Guided media network.
- **Unbound/Unguided Media Network:** Unbounded/Unguided media can also be referred to as wireless media. This kind of network does not need any physical link for electromagnetic transmission. Radio waves, Microwaves, Infrared, etc. can be used in such networks for connectivity. Metropolitan Area Network(MAN) and Wide Area Network(WAN) can be used as an Unbound/Unguided media network.

ANSWAR;2. Difference between Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP) cables

- Last Updated : 02 Nov, 2021

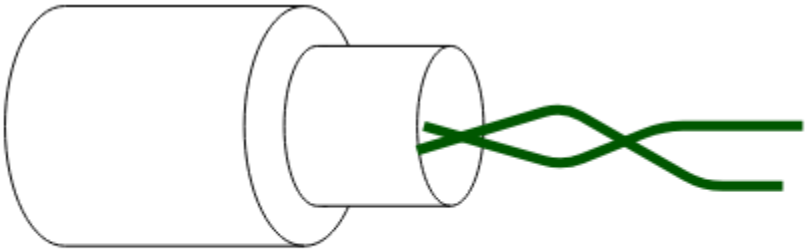
UTP:

UTP is the type of twisted pair cable. It stands for Unshielded twisted pair. Both Data and voice both are transmitted through UTP because its frequency range is suitable. In UTP grounding cable is not necessary also in UTP much more maintenance are not needed therefore it is cost effective.



Unshielded Twisted Pair

STP:
STP is also the type of twisted pair which stands for Shielded twisted pair. In STP grounding cable is required but in UTP grounding cable is not required. in Shielded Twisted Pair (STP) much more maintenance are needed therefore it is costlier than Unshielded Twisted Pair (UTP).



Shielded Twisted Pair

Difference between Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP) cables:

S.NO	UTP	STP
1.	UTP stands for Unshielded twisted pair.	STP stands for Shielded twisted pair.
2.	In UTP grounding cable is not necessary.	While in STP grounding cable is required.
3.	Data rate in UTP is slow compared to STP.	Data rate in STP is high.
4.	The cost of UTP is less.	While STP is costlier than UTP.
5.	In UTP much more maintenance are not needed.	While in STP much more maintenance are needed.

6.	In UTP noise is high compared to STP.	While in STP noise is less.
7.	In UTP the generation of crosstalk is also high compared to STP.	While in STP generation of crosstalk is also less.
8.	In UTP, attenuation is high in comparison to STP.	While in STP attenuation is low.
9.	In UTP, speed offered is about 10 to up to 1000 Mbps.	While in STP speed offered is about 10 to up to 100 Mbps.
10.	It is used for data transmission within short distance such as for home and office networks.	Generally used for connecting organizations over a long distance.

Answar;3. Difference between Broadband and Baseband Transmission

- Difficulty Level : Basic
- Last Updated : 28 Jan, 2022

Broadband system use modulation techniques to reduce the effect of noise in the environment. Broadband transmission employs multiple channel unidirectional transmission using combination of phase and amplitude modulation.

Baseband is a digital signal is transmitted on the medium using one of the signal codes like NRZ, RZ Manchester biphase-M code etc. is called baseband transmission.

These are following differences between Broadband and Baseband transmission.

Baseband transmission –

1. Digital signalling.
2. Frequency division multiplexing is not possible.
3. Baseband is bi-directional transmission.
4. Short distance signal travelling.
5. Entire bandwidth is for single signal transmission.
6. Example: Ethernet is using Basebands for LAN.

Broadband transmission –

1. Analog signalling.
2. Transmission of data is unidirectional.
3. Signal travelling distance is long.
4. Frequency division multiplexing possible.
5. Simultaneous transmission of multiple signals over different frequencies.
6. Example : Used to transmit cable TV to premises.

S.No	Baseband Transmission	Broadband Transmission
1.	In baseband transmission, the type of signalling used is digital.	In broadband transmission, the type of signalling used is analog.
2.	Baseband Transmission is bidirectional in nature.	Broadband Transmission is unidirectional in nature.
3.	Signals can only travel over short distances.	Signals can be travelled over long distances without being attenuated.
4.	It works well with bus topology.	It is used with a bus as well as tree topology.
5.	In baseband transmission, Manchester and Differential Manchester encoding are used.	Only PSK encoding is used.
6.	Baseband transmission have 50 ohm impedance.	Broadband transmission have 70 ohm impedance.
7.	Baseband transmission is easy to install and maintain.	Broadband transmission is difficult to install and maintain.
8.	This transmission is cheaper to design.	This transmission is expensive to design.

ANSWAR;4. Differences between a Hub, a Switch, and a Router

In networking, the terms `switches`, `hubs`, and `routers` are sometimes used interchangeably which is wrong.

Despite them being similar, there are differences in how they handle data. These three components may be integrated into a single device making it hard for a student to distinguish between them.

In this article, we are going to discuss each device and its functionalities in a network.

What is a Switch?

A switch is a multicast networking device that works under the Datalink layer of the OSI model and connects a bunch of computers or devices in a network. It's mainly used to send a private message and it does not waste data.

A switch can easily identify which device is connected to which port by using a MAC address giving it the ability to deliver the message to a particular machine.

Advantages of using a Switch

- It's secure since it delivers data to the specified node.
- It lowers the chances of frame collisions domains.
- It increases the bandwidth in a network.
- It increases the number of ports needed to connect the nodes available in a network.
- It operates under full-duplex.

Disadvantages of using Switches

- They are more expensive compared to hubs and other devices used in a network.
- To deal with multicast parcels, proper planning is required.
- Problems may arise when broadcasting traffic.

What is a Hub?

A Hub is a simple and cheap networking device that works under the physical layer of the OSI model and connects a bunch of computers in a Local Area Network(LAN). It is considered less intelligent because it does not filter data and does not know where the data is to be sent.

All information sent to a hub is automatically sent to all ports of the devices connected to it. This leads to wastage of bandwidth.

Advantages of using hubs

- They have the ability to connect to the network using different physical media.
- They can be used to increase the network distance.
- Hubs are relatively cheap compared to switches and other devices in the network.

Disadvantages of using a hub

- It increases the chances of collision domains between packets when being transferred from one device to another.
- Hubs operate under half-duplex. Only one device can send or receive data at a time
- Hubs share data to all the devices in a network thus making the network insecure.
- Hubs waste lots of bandwidth when transmitting data.

Switch vs Hub

- A Hub is a broadcast device that sends data from one node to all nodes but a Switch is a multicast device that can send data to a particular node.
- A Hub supports half-duplex i.e., only one device can send or receive data at a time while a switch supports full-duplex i.e., both devices can send and receive data at the same time.

- A switch is located on the second layer of the OSI model while a Hub is located on the first layer.

What is a Router?

A Router is a networking device that operates under the network layer of the OSI model and is used to connect two or more networks. It is a device that establishes a common link between networks to enable data flow between them.

Advantages of Routers

- With the aid of dynamic routing algorithms, it can choose the best path in the internetwork.
- It creates collision domains to reduce network traffic.
- It provides connections between different network architectures.

Disadvantages of Routers

- They are expensive compared to hubs and switches.
- They need to analyze data. This makes them slower.
- They have low bandwidth because of their dynamic router communication.

Let's look at their differences on the OSI model.

The component's layer in the OSI model

The Open Systems Interconnection Model(OSI Model) is a 7 layer model that is used to describe, in a pictorial way, how computer systems communicate. A switch, a router, and a hub each operate on a different layer.

A switch is located on the OSI model's Data Link layer i.e., the second layer. The link layer is specific to the medium over which the packet is traveling. The Ethernet and Mac Address are part of this layer.

A router resides in the Network Layer of the OSI model i.e., the third layer.

A hub is located in the Physical Layer of the OSI model i.e., the first layer.

Functions of each device

Switch

- It allows various connections of many devices in the same network and the management of port and VLAN security settings.
- **Learning** - This is the process of collecting the MAC address of linked devices.
- **Forwarding** - This is the process of transferring network traffic from one device connected to one port of a network switch to another device connected to another port.

- **Preventing Layer 2 Switching Loops** - In a Local Area Network, redundant connections are built to prevent the entire network from failing if one link fails. Layer 2 switching loops and broadcast storms can be caused by redundant connections. A network switch's job is to prevent layer 2 switching loops and broadcast storms.

Router

- Its major purpose is to connect many types of networks at the same time using adaptive and non-adaptive routing.
- The router is connected to at least two networks and decides how to deliver each data packet depending on its current knowledge of the network status.
- If a packet is traveling to the LAN, the router bounces it back. The packet will be toured depending on the routing table if this is not the case.

Hub

- A hub is a simple and cheap networking device that allows a bunch of computers to be connected to a single network
- When a hub receives a data packet (an Ethernet frame) from a network device at one of its ports, it broadcasts (repeats) the packet to all of its ports,i.e, to all other network devices. A collision occurs when two network devices on the same network try to send packets at the same time.

Applications of each device

Switch

- It is commonly used in local area networks for connecting many nodes.
- **Forwards a message to a specific host** - On each port, a switch, like a bridge, employs the same forwarding or filtering logic. When a host or switch on the network transmits a message to another host or switches on the same network, the switch receives the frames and decodes them to read the physical (MAC) address component of the message.
- **Increase LAN bandwidth** - A switch divides a LAN into many collision domains, each with its broadband connection, considerably improving the LAN's bandwidth.

Router

- It is commonly used in Local Area Network and Metropolitan Area Network (MAN).
- **It manages traffic** by forwarding data packets to their proper IP addresses. Traffic between these networks may be managed.
- It determines the best path to send packets.

Hub

- It is similar to a switch because it is used in the Local Area Network (LAN).
- It is used for network monitoring.
- They are also used in organizations to provide connectivity.

- It can be used to create a device that is available throughout the network.

Modes of data transmission

They define the direction in which data flows between two communicating devices. There are three types of transmission modes:

1. **Simplex** - In this mode of transmission, data can only move to one direction i.e., a device can only send data but cannot receive and the receiver can only receive but cannot send the data.
2. **Half-Duplex** - In this mode, only one device can send or receive data at a time but not both at the same time.
3. **Full-Duplex** - In this mode, a device can send and receive data at the same time.

Read this documentation for more information on the different modes of data transmission.

Both **switches** and **routers** support full-duplex transmission. Thus, a bunch of computers can send data at the same time.

Hubs support half-duplex transmission. Thus, only one node can send data at a time.

In networking, the terms `switches`, `hubs`, and `routers` are sometimes used interchangeably which is wrong.

Despite them being similar, there are differences in how they handle data. These three components may be integrated into a single device making it hard for a student to distinguish between them.

In this article, we are going to discuss each device and its functionalities in a network.

Table of contents

- What is a Switch?
- What is a Hub?
- What is a Router?
- The component's layer in the OSI model
- Function of each device
- Application of each device
- Modes of data transmission
- Addresses used in each device
- Transmission of Data

What is a Switch?

A switch is a multicast networking device that works under the Datalink layer of the OSI model and connects a bunch of computers or devices in a network. It's mainly used to send a private message and it does not waste data.

A switch can easily identify which device is connected to which port by using a MAC address giving it the ability to deliver the message to a particular machine.

Advantages of using a Switch

- It's secure since it delivers data to the specified node.
- It lowers the chances of frame collisions domains.
- It increases the bandwidth in a network.
- It increases the number of ports needed to connect the nodes available in a network.
- It operates under full-duplex.

Disadvantages of using Switches

- They are more expensive compared to hubs and other devices used in a network.
- To deal with multicast parcels, proper planning is required.
- Problems may arise when broadcasting traffic.

What is a Hub?

A Hub is a simple and cheap networking device that works under the physical layer of the OSI model and connects a bunch of computers in a Local Area Network(LAN). It is considered less intelligent because it does not filter data and does not know where the data is to be sent.

All information sent to a hub is automatically sent to all ports of the devices connected to it. This leads to wastage of bandwidth.

Advantages of using hubs

- They have the ability to connect to the network using different physical media.
- They can be used to increase the network distance.
- Hubs are relatively cheap compared to switches and other devices in the network.

Disadvantages of using a hub

- It increases the chances of collision domains between packets when being transferred from one device to another.
- Hubs operate under half-duplex. Only one device can send or receive data at a time
- Hubs share data to all the devices in a network thus making the network insecure.
- Hubs waste lots of bandwidth when transmitting data.

Switch vs Hub

- A Hub is a broadcast device that sends data from one node to all nodes but a Switch is a multicast device that can send data to a particular node.
- A Hub supports half-duplex i.e., only one device can send or receive data at a time while a switch supports full-duplex i.e., both devices can send and receive data at the same time.

- A switch is located on the second layer of the OSI model while a Hub is located on the first layer.

What is a Router?

A Router is a networking device that operates under the network layer of the OSI model and is used to connect two or more networks. It is a device that establishes a common link between networks to enable data flow between them.

Advantages of Routers

- With the aid of dynamic routing algorithms, it can choose the best path in the internetwork.
- It creates collision domains to reduce network traffic.
- It provides connections between different network architectures.

Disadvantages of Routers

- They are expensive compared to hubs and switches.
- They need to analyze data. This makes them slower.
- They have low bandwidth because of their dynamic router communication.

Let's look at their differences on the OSI model.

The component's layer in the OSI model

The Open Systems Interconnection Model(OSI Model) is a 7 layer model that is used to describe, in a pictorial way, how computer systems communicate. A switch, a router, and a hub each operate on a different layer.

A switch is located on the OSI model's Data Link layer i.e., the second layer. The link layer is specific to the medium over which the packet is traveling. The Ethernet and Mac Address are part of this layer.

A router resides in the Network Layer of the OSI model i.e., the third layer.

A hub is located in the Physical Layer of the OSI model i.e., the first layer.

Functions of each device

Switch

- It allows various connections of many devices in the same network and the management of port and VLAN security settings.
- **Learning** - This is the process of collecting the MAC address of linked devices.
- **Forwarding** - This is the process of transferring network traffic from one device connected to one port of a network switch to another device connected to another port.

- **Preventing Layer 2 Switching Loops** - In a Local Area Network, redundant connections are built to prevent the entire network from failing if one link fails. Layer 2 switching loops and broadcast storms can be caused by redundant connections. A network switch's job is to prevent layer 2 switching loops and broadcast storms.

Router

- Its major purpose is to connect many types of networks at the same time using adaptive and non-adaptive routing.
- The router is connected to at least two networks and decides how to deliver each data packet depending on its current knowledge of the network status.
- If a packet is traveling to the LAN, the router bounces it back. The packet will be toured depending on the routing table if this is not the case.

Hub

- A hub is a simple and cheap networking device that allows a bunch of computers to be connected to a single network
- When a hub receives a data packet (an Ethernet frame) from a network device at one of its ports, it broadcasts (repeats) the packet to all of its ports,i.e, to all other network devices. A collision occurs when two network devices on the same network try to send packets at the same time.

Applications of each device

Switch

- It is commonly used in local area networks for connecting many nodes.
- **Forwards a message to a specific host** - On each port, a switch, like a bridge, employs the same forwarding or filtering logic. When a host or switch on the network transmits a message to another host or switches on the same network, the switch receives the frames and decodes them to read the physical (MAC) address component of the message.
- **Increase LAN bandwidth** - A switch divides a LAN into many collision domains, each with its broadband connection, considerably improving the LAN's bandwidth.

Router

- It is commonly used in Local Area Network and Metropolitan Area Network (MAN).
- **It manages traffic** by forwarding data packets to their proper IP addresses. Traffic between these networks may be managed.
- It determines the best path to send packets.

Hub

- It is similar to a switch because it is used in the Local Area Network (LAN).
- It is used for network monitoring.
- They are also used in organizations to provide connectivity.

- It can be used to create a device that is available throughout the network.

Modes of data transmission

They define the direction in which data flows between two communicating devices. There are three types of transmission modes:

1. **Simplex** - In this mode of transmission, data can only move to one direction i.e., a device can only send data but cannot receive and the receiver can only receive but cannot send the data.
2. **Half-Duplex** - In this mode, only one device can send or receive data at a time but not both at the same time.
3. **Full-Duplex** - In this mode, a device can send and receive data at the same time.

Read this documentation for more information on the different modes of data transmission.

Both **switches** and **routers** support full-duplex transmission. Thus, a bunch of computers can send data at the same time.

Hubs support half-duplex transmission. Thus, only one node can send data at a time.

In networking, the terms `switches`, `hubs`, and `routers` are sometimes used interchangeably which is wrong.

Despite them being similar, there are differences in how they handle data. These three components may be integrated into a single device making it hard for a student to distinguish between them.

In this article, we are going to discuss each device and its functionalities in a network.

Table of contents

- What is a Switch?
- What is a Hub?
- What is a Router?
- The component's layer in the OSI model
- Function of each device
- Application of each device
- Modes of data transmission
- Addresses used in each device
- Transmission of Data

What is a Switch?

A switch is a multicast networking device that works under the Datalink layer of the OSI model and connects a bunch of computers or devices in a network. It's mainly used to send a private message and it does not waste data.

A switch can easily identify which device is connected to which port by using a MAC address giving it the ability to deliver the message to a particular machine.

Advantages of using a Switch

- It's secure since it delivers data to the specified node.
- It lowers the chances of frame collisions domains.
- It increases the bandwidth in a network.
- It increases the number of ports needed to connect the nodes available in a network.
- It operates under full-duplex.

Disadvantages of using Switches

- They are more expensive compared to hubs and other devices used in a network.
- To deal with multicast parcels, proper planning is required.
- Problems may arise when broadcasting traffic.

What is a Hub?

A Hub is a simple and cheap networking device that works under the physical layer of the OSI model and connects a bunch of computers in a Local Area Network(LAN). It is considered less intelligent because it does not filter data and does not know where the data is to be sent.

All information sent to a hub is automatically sent to all ports of the devices connected to it. This leads to wastage of bandwidth.

Advantages of using hubs

- They have the ability to connect to the network using different physical media.
- They can be used to increase the network distance.
- Hubs are relatively cheap compared to switches and other devices in the network.

Disadvantages of using a hub

- It increases the chances of collision domains between packets when being transferred from one device to another.
- Hubs operate under half-duplex. Only one device can send or receive data at a time
- Hubs share data to all the devices in a network thus making the network insecure.
- Hubs waste lots of bandwidth when transmitting data.

Switch vs Hub

- A Hub is a broadcast device that sends data from one node to all nodes but a Switch is a multicast device that can send data to a particular node.
- A Hub supports half-duplex i.e., only one device can send or receive data at a time while a switch supports full-duplex i.e., both devices can send and receive data at the same time.

- A switch is located on the second layer of the OSI model while a Hub is located on the first layer.

What is a Router?

A Router is a networking device that operates under the network layer of the OSI model and is used to connect two or more networks. It is a device that establishes a common link between networks to enable data flow between them.

Advantages of Routers

- With the aid of dynamic routing algorithms, it can choose the best path in the internetwork.
- It creates collision domains to reduce network traffic.
- It provides connections between different network architectures.

Disadvantages of Routers

- They are expensive compared to hubs and switches.
- They need to analyze data. This makes them slower.
- They have low bandwidth because of their dynamic router communication.

Let's look at their differences on the OSI model.

The component's layer in the OSI model

The Open Systems Interconnection Model(OSI Model) is a 7 layer model that is used to describe, in a pictorial way, how computer systems communicate. A switch, a router, and a hub each operate on a different layer.

A switch is located on the OSI model's Data Link layer i.e., the second layer. The link layer is specific to the medium over which the packet is traveling. The Ethernet and Mac Address are part of this layer.

A router resides in the Network Layer of the OSI model i.e., the third layer.

A hub is located in the Physical Layer of the OSI model i.e., the first layer.

Functions of each device

Switch

- It allows various connections of many devices in the same network and the management of port and VLAN security settings.
- **Learning** - This is the process of collecting the MAC address of linked devices.
- **Forwarding** - This is the process of transferring network traffic from one device connected to one port of a network switch to another device connected to another port.

- **Preventing Layer 2 Switching Loops** - In a Local Area Network, redundant connections are built to prevent the entire network from failing if one link fails. Layer 2 switching loops and broadcast storms can be caused by redundant connections. A network switch's job is to prevent layer 2 switching loops and broadcast storms.

Router

- Its major purpose is to connect many types of networks at the same time using adaptive and non-adaptive routing.
- The router is connected to at least two networks and decides how to deliver each data packet depending on its current knowledge of the network status.
- If a packet is traveling to the LAN, the router bounces it back. The packet will be toured depending on the routing table if this is not the case.

Hub

- A hub is a simple and cheap networking device that allows a bunch of computers to be connected to a single network
- When a hub receives a data packet (an Ethernet frame) from a network device at one of its ports, it broadcasts (repeats) the packet to all of its ports,i.e, to all other network devices. A collision occurs when two network devices on the same network try to send packets at the same time.

Applications of each device

Switch

- It is commonly used in local area networks for connecting many nodes.
- **Forwards a message to a specific host** - On each port, a switch, like a bridge, employs the same forwarding or filtering logic. When a host or switch on the network transmits a message to another host or switches on the same network, the switch receives the frames and decodes them to read the physical (MAC) address component of the message.
- **Increase LAN bandwidth** - A switch divides a LAN into many collision domains, each with its broadband connection, considerably improving the LAN's bandwidth.

Router

- It is commonly used in Local Area Network and Metropolitan Area Network (MAN).
- **It manages traffic** by forwarding data packets to their proper IP addresses. Traffic between these networks may be managed.
- It determines the best path to send packets.

Hub

- It is similar to a switch because it is used in the Local Area Network (LAN).
- It is used for network monitoring.
- They are also used in organizations to provide connectivity.

- It can be used to create a device that is available throughout the network.

Modes of data transmission

They define the direction in which data flows between two communicating devices. There are three types of transmission modes:

1. **Simplex** - In this mode of transmission, data can only move to one direction i.e., a device can only send data but cannot receive and the receiver can only receive but cannot send the data.
2. **Half-Duplex** - In this mode, only one device can send or receive data at a time but not both at the same time.
3. **Full-Duplex** - In this mode, a device can send and receive data at the same time.

Read this documentation for more information on the different modes of data transmission.

Both **switches** and **routers** support full-duplex transmission. Thus, a bunch of computers can send data at the same time.

Hubs support half-duplex transmission. Thus, only one node can send data at a time.

Addresses used in each device

A **switch** stores and uses the MAC address of a device to transfer data while a **router** uses the IP address of the device to transfer data between networks.

A **hub** on the other hand does not store any MAC/IP address to transfer data.

Transmission of data

A **switch** transmits data from one device to another in form of frames while a **router** transmits data from one network to another in form of packets.

A **hub** transmits data from one device to another in form of binary bits.

ANSWAR;5. 74) When you move the NIC cards from one PC to another PC, does the MAC address gets transferred as well? **Yes, that's because MAC addresses are hard-wired into the NIC circuitry, not the PC**. This also means that a PC can have a different MAC address when another one replaced the NIC card

ust like each house has it's own postal address, every device connected on a network has a Media Access Control (MAC) address, that uniquely identifies it. **The MAC address is tied to the Network Interface Controller (NIC), a subcomponent of the larger device**.

ANSWAR;6. 88) When troubleshooting computer network problems, what common hardware-related problems can occur? A large percentage of a network is made up of hardware. Problems in these areas can range from **malfunctioning hard drives, broken NICs, and even hardware startups**

ANSWAR;7. In a network that contains two servers and twenty workstations, where is the best place to install an anti-virus program? When troubleshooting computer network problems, what common hardware-related problems can occur?

IT Director at Quakertown Christan School (2011-present)

Updated 3 years ago · Author has 938 answers and 870.8K answer views

You need AT LEAST three levels of security.

1. A good firewall. This can stop intrusions, malware, unauthorized access, etc. before they reach the workstations.
2. Antivirus software on the servers and at the endpoint workstations. This software should be centrally managed to keep end users updated constantly and to minimize user meddling with the settings. Good antivirus will also protect email clients.
3. Educated and aware users who: do not casually install downloaded programs; don't click on unknown links; don't fall for phishing emails, etc. Establish a strong password policy for all users. You shoul

Related questions

What are the basic network troubleshooting tools for finding errors and problems in the network?

When troubleshooting computer network problems, what common hardware-related problems can occur?

How can I troubleshoot network problems?

What commands are useful for troubleshooting network connection issues?

After troubleshooting my network, I get these two errors."Windows can’t communicate with the device or resource (primary DNS server)", and "security or firewall settings might be blocking the connection". How do I solve this issue?

Adrian Hum

, ERP Consultant and Software Developer

Answered 1 year ago · Author has 4K answers and 3M answer views

Anti-virus? Everywhere…

Network topology such as WIFI is subject to hot and cold spots especially if a mesh is in use.

The hardware of course can fail. You need to probably have some HDD recovery tools.

Matthew Hunt

, Cisco, HPE, PKI, 800-171, AD/GPOs, CLI

Answered 3 years ago · Author has 353 answers and 184.5K answer views

Anti-virus on all devices, servers and workstati oins!

Troubleshooting…is the network cable plugged in? That's usually the first thing to check. Replace the client-end of the cabling (wall to desktop). Beyond that, ipconfig is your friend.

Hitesh Hambarde

, Head - Technical (2007-present)

Answered 3 years ago · Author has 289 answers and 350.8K answer views

Antivirus should be on each computer, if you implement server and node base antivirus that will be best for controlling.

There are no special problems just because you are two server and 20 computer. Every general issue will come along with critical. It will be same as any other computer setup issue.

Frionx Calamari

Answered 1 year ago

Related

A completed computer is connected to the Internet. If you have a firewall on your computer, do you still need antivirus software? Why or why not?

Yes, a firewall protects from incoming connections to the computer and outbound connections that the user doesn't give permission for.

On the other hand,
If you know and are smart on the internet (not running random apps, etc), you mostlikely won't need a antivirus and if you are on windows, could use the built in windows defender. Just never, never turn it off.

Gaurav Singh

, Technical Head

Answered 1 year ago · Author has 102 answers and 161.5K answer views

Related

Can I install an antivirus if I have a virus?

Yes, you can install antivirus software if your PC is already infected with viruses.

But some viruses prevent to install an Antivirus program then you can scan your PC via a bootable antivirus program.

So make a bootable CD/DVD/USB and scan your PC and after completing the scan process restarts your PC and again try to install antivirus software.

Yaro Kasear

, Programmer, Linux Enthusiast

Answered Apr 9, 2022 · Author has 4.3K answers and 3.5M answer views

Related

A user calls & reports that their PC keeps getting disconnected from the network. The internet and their mapped network drives are not accessible when the disconnect occurs. What info do you need & what steps would you perform to isolate the problem?

Look in your network documentation under the header, “Do your own fucking homework.”

Laurence Perkins

, studied at Gonzaga University

Answered 2 years ago · Author has 232 answers and 288.9K answer views

Related

Will wiping a computer remove viruses?

Usually…

So, in order to infect a computer, a virus or other malicious program has to be stored somewhere that the computer will run it. If you've got a virus that stores itself on the computer's hard drive and nowhere else, then erasing all the data off that disk removes the virus.

However…

In modern computers there are other places where data is stored. There are viruses which are capable of injecting themselves into motherboard or hard drive firmware. Such viruses are much less common because they rely on particular combinations of hardware and software being present at the same time in order

Keith Winstein

, Former Wall Street Journal reporter

Updated 8 years ago · Upvoted by

Shakthi SG

, M.S Electrical and Computer Engineering & Computer Networking, California State University, Los Angeles (2016… and

Greg Skinner

, 25+ years of software engineering, mostly in C and Perl, mostly in the BSD networking stack and Unix utilitie… · Author has 392 answers and 1.6M answer views

Related

Is computer networks a boring area? If you look at computer networks questions on Quora, they are sparse and just not exciting compared to other fields.

Originally Answered: Is Computer Networks a boring area?

I can't agree at all!! Computer networks and communications have much to arouse the passions. But the important question is what gets you going.

Here are a few recent innovations in the field that you may have heard of. All of this stuff would be in-scope (indeed, has been in-scope and published about) at the major academic conferences, e.g. ACM SIGCOMM, Usenix NSDI, IMC, MobiCom, MobiSys, CoNEXT, ANCS, INFOCOM, etc.:

- the Internet
- the World Wide Web
- Wi-Fi

- LTE / cellular packet networking
- NFC / RFID / low-power and no-power communications
- Skype / Facetime / Google Hangout / YouTube / Netflix

- Pee

When a network connection is not function as it should it is in need of some troubleshooting. Troubleshooting is the methodological “step-by-step” process of singling out the cause of the problem and rectifying it.

Take the following everyday example: I realize my car’s right headlight is not working. What’s my first step? Check the light bulb to see if it is fused, right? The most probable cause first. Once checked and its perhaps not the bulb then you check if maybe there is a loose wire and then the battery etc. Logic. One would not rip out all the wires before checking the bulb or take the

Related

How can I troubleshoot network problems?

Originally Answered: What are the steps in troubleshooting a computer network?

There are several approaches:

- Top-down (start with application level, e.g. web browser, then go to lower levels)
- Bottom-up (start with physical level, e.g. check cables and lights, then go to upper levels)
- Divide and conquer (start in the middle level)
- Follow the path (check network devices in turn on the path of network packets)
- Spot the difference (compare to a similar working setup)
- Move the problem (swap a potentially faulty component, see if the problem moves too)
- Shoot from the hill (spot a common problem from a past experience).

See Troubleshooting Methods for Cisco IP Networks

. These methods a

Suhas Dhole

, Computer Engineer

Answered Dec 15, 2021 · Author has 117 answers and 328K answer views

Related

How can I protect my computer with antivirus software?

U can protect without antivirus too. But u need to take care about few things,

Don't surfe unauthorised sights. Always check sight start with https: that mean it's a secure site. And see a lock icons near it. If u see open lock and red color or http then don't use that sites.

Do not click on any ads u see on unauthorised websites

Always turn on firewall

Do not download files, if u get any random popups that tell to download this software of important update and all

Check cracked softwares and games before using it.

If you want to protect with antivirus

Then just turn on all security features that

, studied Computer Science & Computer Security at Books (2017)

Answered 1 year ago · Author has 1.3K answers and 952.4K answer views

Related

How do I avoid antivirus firewall blocking?

this depends on how the firewall is blocking traffic.

If the firewall is blocking a specific port, change the port you're using.

If the firewall is blocking all ports with the exception of a hand full of them, use one of the whitelisted ports.

If the firewall is blocking traffic that displays malicious patterns; obfuscate the traffic.

Ajay Sehrawat

, studied GND Polytechnic

Answered 1 year ago · Author has 377 answers and 100.4K answer views

Related

What are the top network security and antivirus software?

Rank 1 is the best, rank 2 is the second best and so on.

If you use these antivirus software one by one for one month free each, you can have a great protection for 17 month

Use one and only one antivirus at any one time.

If you can not find any one software, you can always use the free version. This happen for case rank 2

Top ten list of antivirus software is given below:-

1 Kaspersky internet security or bitdefender total security antivirus

2 Avast ultimate software or AVG ultimate software

3 ESET NOD32 total security antivirus

4 Trendmicro total security or Bullguard total security antivirus

5 F-SEC

Ahmed Minegames

, Professional Malware Coder and Reverse Engineer

Answered 8 months ago · Author has 103 answers and 19.3K answer views

Related

How does antivirus work, and what does it lack?

How Does Antivirus Works?
antivirus works by checking a code from known malicious files and looks for bad (blacklisted) functions that can be used possibly by malware, for example RtlSetProcessIsCritical function

which are a blacklisted function that makes the process critical in windows to prevent termination, they can also check for blacklisted memory maps inside the file, and there's antiviruses which are signature based (gets signature about known malicious files from the cloud) but these kind of antiviruses that are based on signatures won't protect you from zero-day malware, they can als

Jonathan Thompson

, Escalation Engineer (Developer Support) at Microsoft (2014-present)

Answered Mar 9, 2022 · Author has 333 answers and 62K answer views

Related

Who undertakes troubleshooting computer hardware and software-related problems?

Tony Li

, Internet construction crew

Answered 3 years ago · Author has 13.8K answers and 46.7M answer views

Related

What is the channel allocation problem in a computer network?

That's an obsolete issue from back when we used Time-division Multiplexing (TDM) media and didn't have effective Reconfigurable optical add-drop multiplexers (ROADM)

. Once those existed, it was easy to remap channels at various multiplexing points, so channel allocation was greatly simplified.

Today, it's just not a problem. We now do Frequency Division Multiplexing (FDM) and channels are all translated back to native frequencies before interconnection.
I work on several security sites, mostly on http://www.2-viruses.com providing removal instructions for paras…

Answered 1 year ago · Author has 1.6K answers and 1.4M answer views

Related

Are there really new computer virus threats every day? My anti-virus program updates its virus list every day. Are there really that many new threats?

There are a lot of new viruses released each day, but even more malware is updated daily (sometimes automatically) so antiviruses would have problems in detecting them,

Alex Rounds

, Educator, Writer, Culinarian, Wisenheimer

Answered 1 year ago · Author has 2K answers and 380.3K answer views

Related

How can a computer virus spread in the local network? How do you prevent it?

A computer virus spreads by infecting every outgoing message - tweets, FB, email, etc.

You prevent it by acquiring a working antivirus program. Best to have one you pay for, but there are free ones by the same companies - such as Avast, Symantec, McAfee, and so on.

In my workplace, my computer is under attack on a regular basis. I keep my security software up to date to avoid getting an infection. You can do the same. It used to be said that there are no virus threats for Apple and Linux computers. This is naive - the computers that attack my Windows machine are all Apples. They are certainly in

Thomas Moser

, Runs a PC consulting business where 40% of my business is Malware removal.

Answered 3 years ago · Author has 4.7K answers and 3.5M answer views

Related

Which is the best free anti-malware software?

Originally Answered: What is the best free Malware protection for your computer?

A2A: A good AV (Avast, Avira, Bitdefender, Webroot, etc. — NOT Windows Defender) plus Malwarebytes (free, rootkit scan enabled, autostart disabled) once a month.

Leif Erickson

, former PC Technician for About 25 Years

Answered 4 years ago · Author has 2.1K answers and 1.3M answer views

Related

Where might I find a computer network?

Virtually everywhere. Most private homes have an uplink to the internet, so nearly every home has a computer that's on a network. If you mean a Local Area Network, most of those homes which have more than one computer have one, because all of the computers that can connect to the internet are also on a LAN inside the home.

The same is true of business and many organizations. If there's one computer, it's probably on the internet, and if there are multiple computers, they're probably on one or more LANs, and maybe even a WAN or VPN with other locations of the same company.

Rahul Chatterjee

, Bachelor of Science from University of Calcutta (2019)

Answered 4 years ago · Author has 447 answers and 2.9M answer views

Related

How do I know if my computer has been compromised despite having a good antivirus?

Originally Answered: how do I know if my computer has been compromised despite having a good antivirus?

I personally believe that privacy and security depends upon the respective user who is the administrator of that particular device, just a great antivirus cannot protect us from A to Z thoroughly with 100% assurance if the administrator is so casual enough, nowadays

Your Question does not have any specific answer, it depends upon perspectives, so if I slightly modify your Question to What should I do to protect my privacy and security despite having a good antivirus? I am stating the answer

1. Always it is recommended to use only one paid antivirus software (With a good rating of its own segment),

Allen Walker

, works at Microsoft (2009-present)

Answered Nov 30, 2021 · Author has 655 answers and 249.6K answer views

Related

How do you clean a virus using ESET Nod32?

In the main program window, click Computer scan.

Click Scan your computer to begin scanning your system.

After the scan has finished, review the log with the number of scanned, infected and cleaned files.

If you wish to only scan a certain part of your disk, click Custom scan and select targets to be scanned for viruses.

https://help.eset.com/eav/13/en-US/how_to_clean_pc_from_virus.html

Tony Li

, Ph.D. Computer Science, University of Southern California (1990)

Answered 3 years ago · Author has 13.8K answers and 46.7M answer views

Related

Why network computers?

Because data must MOVE. Data in the wrong place, on the wrong computer, is worthless. And data on the right computer, at the right time, is priceless.

The spice must flow.

Manish Riuga

, Software Developer at Oracle

Answered 3 years ago

Related

How do antivirus software work?

For starters most AV run on some kind of pattern matching algorithms.

The AV keeps scanning all the directories you have in you storage.

This scan checks the filename, file extension, file's hex data does the hex match the given extension in display, if not then flag it, then it also checks entire file for malware signatures already known to the AV.

Once it finds any file with the malware signature it will flag that file and share that details with you.

But most of the AV do not understand the intent of the file which is why there are a lot of false positives even today.

Modern day AV now try to em

Suresh Devrari

, Certified Ethical Hacker from Computer Security

Answered 2 years ago · Author has 304 answers and 900.3K answer views

Related

Is computer networking related to hacking?

Yes, Obviously Networking is a very important subject in Hacking as well. It helps a Hacker to understand how data is transmitted in the wires and signals.

Some of topics which commonly used in Hacking:-

- IP Address
- DNS
- Subnet
- Proxy
- OSI Model
- TCP/IP Model
- Network Configurations
- Ports
- Network Services
- Traffic Monitoring
- Packet Analysis

Talvinder Singh

, loves ML, experience in RNN.

Answered 5 years ago · Author has 237 answers and 1.3M answer views

Related

Is tracert a feature of common network troubleshooting used in networking?

Originally Answered: is tracert a feature of common network troubleshooting used in networking?

tracert utility helps to up to which hop the data packets can reach. Internet is made up of numerous devices interconnect in a way. So, when a packet leaves your system, it hits your router, then next router, then next and finally hits the destination or your desired server. this route is traceable through tracert. A very simple tool but very effective.

Deval

, B. Tech Computer Science Engineering, Institute Of Technology, Nirma University (2021)

Answered 3 years ago · Author has 118 answers and 203.8K answer views

Related

How does one install an antivirus?

Read the manual given with product. Or read instructions from their website.

There are different steps and ways to install for different antivirus.

Sam Orton

, Trucker, former stagehand, former electonics tech

Answered 3 years ago · Author has 328 answers and 202.5K answer views

Related

How do I clean a virus?

Personally I'm fond of the Kaspersky Virus Removal Tool. It's a free download. Please note that it is NOT an antivirus, it doesn't run in the background and it won't *prevent* a virus from getting on your machine. But on the other hand, I've seen it find and kill things that Windows Defender and Norton Antivirus missed.

And just for the record, I've been using it since long before all the fearmongering about "Russian trolls" started.

Glyn Davies

, B.Eng from Adelaide University (1980)

Answered 4 years ago · Author has 1K answers and 7.2M answer views

Related

What is computer hardware and networking?

hmmm,

computer hardware is ANY and ALL of the equipment you use for computing.

So it includes the computer, your printer, modem, routers, switches, power supplies,cables etc.

It also includes all of the bits that make up a computer like the CPU, motherboard, memory, hard disk etc.

networking refers to the hardware (physical bits and pieces) and software (the instructions for that hardware) which enables computers to transfer information from one computer to another

via either a local area network (LAN) which normally connects multiple computers in the same building or via the internet which connec

Andrei Vida-Rațiu

, IT System Administrator at Altran (2019-present)

Answered 3 years ago · Author has 3.5K answers and 2.6M answer views

Related

Which anti-virus software do you recommend to use for network computers of 500+ computers?

Depends on the OS. If it is Windows 10, use the built-in antivirus and lock down the workstations using GPO. You will be 99% safe.

I do this for around 200 computers and had 0 issues so far.

Jesse Pollard

, programmer/analyst/administrator from way back

Answered 3 years ago · Author has 18.6K answers and 7.6M answer views

Related

How is parallel computing used in solving network problems?

How is parallel computing used in solving network problems?

That depends on which problems you are referring to.

In some (such as load balancing), updating loading tables for different routes while still processing routing….

Running diagnostics to identify loads or failures (collecting statistics for load balancing) to avoid/reduce congestion.

But there are other kinds of "network problems" where multiple hosts pass data for application analysis. In some cases, two nodes that happen to be very far apart (network hops) might cause one or the other processes (or both) on those nodes to migrate to ot

Martin Aston

Answered 3 years ago · Author has 151 answers and 53.8K answer views

Related

Does having two anti-virus cause problem?

Yes, it may cause problems if both are running in realtime. Additionally, it would use extra system resources for absolutely no security gain.

Joseph o'Loughlin

, BA Hons Human Relations, National College of Ireland (2011)

Answered 2 years ago · Author has 6.9K answers and 1.8M answer views

Related

How do you update anti-virus software as a network manager?

Most corporate or enterprise antivirus products provide management software, typically installed on the AV deployment server, but sometimes cloud-managed, allowing you to see the state of the AV programs on each client (and servers where the AV is installed).

Kevin Thompson

, Founder (2010-present)

Answered 1 year ago · Author has 2.8K answers and 5.2M answer views

Related

How is the virus spread in computer networking?

Originally Answered: How does a computer virus spread? Explain briefly.

A PC VIRUS needs a host like a bio virus and it comes via EXE files in most cases that may be embedded into OTHER ITEMS.

FOR THIS REASON, WHEN YOU DOWNLOAD ANYTHING….

It is best to have a download location OUTSIDE OF C: DRIVE WHERE WINDOWS IS.

Then it can be wise to RIGHT CLICK ON THAT DOWNLOAD ITEM and select a AV scan to be run just on that item.

A virus activates when the file/folder/download is ACTIVATED and you may have a legit item as far as a downloaded app that a VIRUS HAS PIGGYBACKED ONTO and when this happens the virus hopefully gets detected by your AV.

At any rate the virus will activat

Alexander Lehmann

, Web security experience since 1998

Answered 2 years ago · Author has 51.9K answers and 14M answer views

Related

What happens when your computer gets a virus, and how do antivirus softwares help prevent them?

When your computer gets malware, different things can happen, the malware could collect all your typed text, steal your accounts, send spam mails, encrypt everything, ask for money, just delete your whole computer, in a tame version it will just display ads instead of your regular pages.

Antivirus will detect the software that contains the malware before it is run so that it does not get active on your computer at all (hopefully, there may be malware that gets past the antivirus if it is very new).

Lets say you have receivied a mail with a shipping confirmation for Fedex that contains an attachm

Shahid Sharif

, Experience in information security, manged switches, routers, firewalls, IDS/IPS

Answered 3 years ago · Author has 93 answers and 163.2K answer views

Related

If you install a network-based firewall on your home network & you want to configure the firewall to pass the traffic to and from Internet websites, which firewall ports should you open?

The standard ports that website content is delivered on are TCP/80(HTTP) and (HTTPS)TCP/443, hence you should open these two ports outbound.

ANSWAR;8. Difference between Static IP Address and Dynamic IP Address

---

Static IP Address and Dynamic IP Address, both are used to identify a computer on a network or on internet. Static IP address is provided by Internet Service Provider and remains fixed till the system is connected to the network. Dynamic IP address is provided by DHCP, generally a company gets a single static IP address and then generates the dynamic IP address for its computers within the organization's network.

Following are some of the important differences between Static IP Address and Dynamic IP Address.

Sr. No.	Key	Static IP Address	Dynamic IP Address
1	Provider	Internet Service Provider, ISP provides the static IP Address.	DHCP (Dynamic Host Configuration Protocol) is used to generate dynamic IP Address.
2	Changes	Static IP address does not get changed with time.	Dynamic IP address can be changed any time.
3	Security	Static IP Address is less secured.	Dynamic IP address being volatile in nature is less risky.
4	Designation	Static IP address is difficult to assign or reassign.	Dynamic IP address is easy to assign and reassign.
5	Device tracking	Device using static IP address can be traced easily.	Device using dynamic IP address is difficult to trace.
6	Stability	Static IP address is highly stable.	Dynamic IP address is less stable than static IP address.
7	Cost	Static IP address is costly to	Dynamic IP address is cheaper to use and

Sr. No.	Key	Static IP Address	Dynamic IP Address
		maintain.	maintain than static IP address.

- Related Questions & Answers
- Difference between MAC Address and IP Address
- Difference between IP Address and MAC Address
- Alias/Secondary IP Address
- Validate IP Address in C#
- Validate IP Address in C++
- Validate IP Address in Python
- Defanging an IP Address in Python
- C# program to Display Hostname and IP address
- Python program to Display Hostname and IP address?
- C Program to display hostname and IP address
- Program to display hostname and IP address C
- Java program to display Hostname and IP address
- C Program to validate an IP address
- JavaScript program to retrieve clients IP address
- Determining the User IP Address in Node

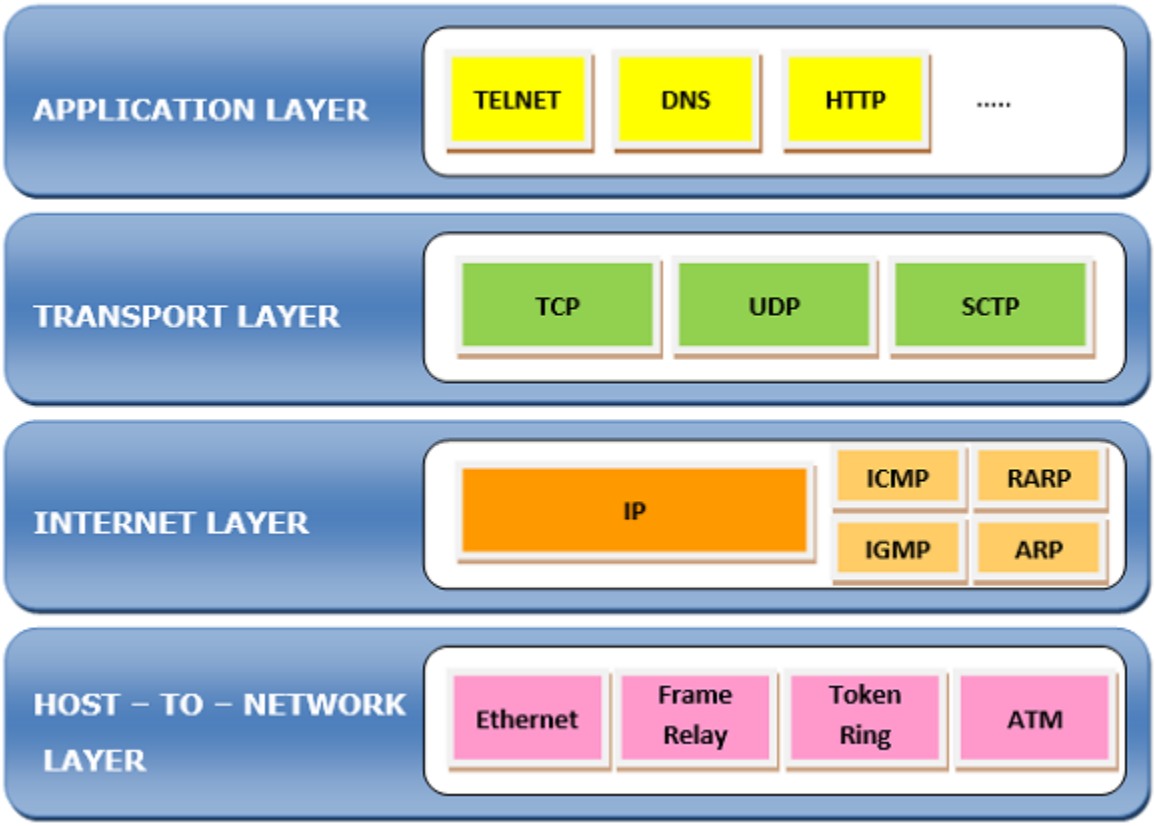
ANSWAR; 9. The TCP/IP Reference Model

TCP/IP Reference Model is a four-layered suite of communication protocols. It was developed by the DoD (Department of Defence) in the 1960s. It is named after the two main protocols that are used in the model, namely, TCP and IP. TCP stands for Transmission Control Protocol and IP stands for Internet Protocol.

The four layers in the TCP/IP protocol suite are −

- **Host-to- Network Layer** −It is the lowest layer that is concerned with the physical transmission of data. TCP/IP does not specifically define any protocol here but supports all the standard protocols.
- **Internet Layer** −It defines the protocols for logical transmission of data over the network. The main protocol in this layer is Internet Protocol (IP) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.
- **Transport Layer** − It is responsible for error-free end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- **Application Layer** − This is the topmost layer and defines the interface of host programs with the transport layer services. This layer includes all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc.

The following diagram shows the layers and the protocols in each of the layers −



ANSWAR;10. Web Browser - What is a Web/Internet Browser?

Definition of a "web browser" and links to support websites for further information and help.

"A web browser, or simply 'browser,' is an application used to access and view websites. Common web browsers include Microsoft Edge, Internet Explorer, Google Chrome, Mozilla Firefox, and Apple Safari.

The primary function of a web browser is to render HTML, the code used to design or 'mark up' webpages" (TechTerms, 2014).

Choose your web browser:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Internet Explorer
- Safari

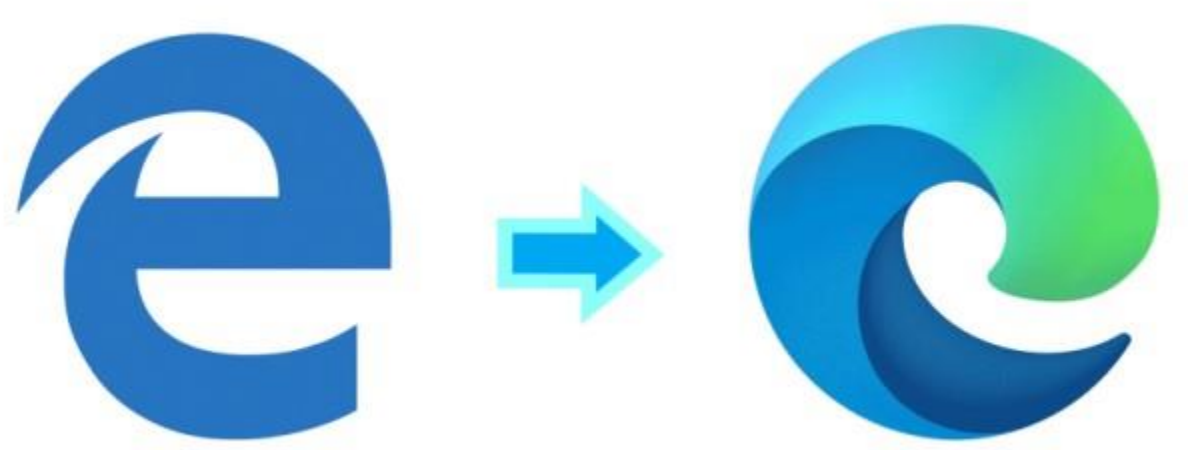
Google Chrome

- Information and Support: https://support.google.com/chrome

Mozilla Firefox

- Information and Support: https://support.mozilla.org/en-US/
- ***Note**: The newest version of Firefox (the icon on the right) has a different look.

Microsoft Edge



- Information and Support: https://support.microsoft.com/en-us/hub/4337664/microsoft-edge-help
- ***Note:** The newest version of Edge (the icon on the right) has a different look.

Internet Explorer

- Information and Support: https://support.microsoft.com/en-us/hub/4230784/internet-explorer-help

Safari

- Information and Support: https://support.apple.com/safari

To the top

See Also:

- Web Browser - Clearing Cache, Cookies, Browsing History
- Web Browser - How to Browse in Private
- Web Browser - Block or Allow Pop-ups
- Web Browser - How to Update
- Web Browser - Google Chrome - Remove Extensions

Keywords:	web, internet, browser, Mozilla Firefox, Internet Explorer, Google Chrome, Safari, Microsoft Edge, support Suggest keywords	**Doc ID:**	89012
Owner:	Erin B.	**Group:**	UW-La Crosse
Created:	2019-01-11 09:41 CDT	**Updated:**	2021-02-25 17:06 CDT
Sites:	UW-La Crosse		
Feedback:			

ANSWAR;11. What Is a Search Engine? Definition Plus 10 Examples

Paul's passion for technology and digital media goes back over 30 years. Born in the UK, he now lives in the US.

Public domain image via Pixabay

What Is a Search Engine?

Also known as a web search engine and an internet search engine, a search engine is a (usually web-based) computer program that collects and organizes content from all over the internet.

The user enters a query composed of keywords or phrases, and the search engine responds by providing a list of results that best match the user's query. The results can take the form of links to websites, images, videos, or other online data.

How Do Search Engines Work?

The work of a search engine can be broken down into three stages. Firstly, there is the process of discovering the information. Secondly, there is the organization of the information so that it can be effectively accessed and presented when users search for something. Thirdly, the information must be assessed to present search engine users with relevant answers to their queries.

These three stages are usually called crawling, indexing, and ranking.

Crawling

Search engines use pieces of software called web crawlers to locate publicly available information from the internet, which is why this process is known as crawling. Web crawlers can also sometimes be referred to as search engine spiders. The process is complicated, but essentially the crawlers/spiders find the webservers (also known as just servers for short) which host the websites and then proceed to investigate them.

A list of all the servers is created, and it is established how many websites are hosted on each server. The number of pages each website has, as well as the nature of the content, for example, text, images, audio, video, is also ascertained. The crawlers also follow any links that the website has, whether internal ones that point to pages within the site, or external ones that point to other websites and use them to discover more pages.

Indexing

Information found by the crawlers is organized, sorted, and stored so that it can later be processed by the algorithms for presentation to the search engine user. This is known as indexing. Not all the page information is stored by the search engine, instead, it's just the essential information needed by the algorithms to assess the relevance of the page for ranking purposes.

Ranking

When a query is entered into a search engine, the index is scoured for relevant information and then sorted into a hierarchical order by an algorithm. This ordering of the search engine results pages (SERPS) is known as ranking.

Different search engines use different algorithms, and so give different results. Over the years, algorithms have become more and more complex as they attempt to present more relevant and accurate answers in response to the queries of search engine users.

10 Examples of Search Engines

1. Google

Google is the biggest search engine in the world by far. It handles over 5 billion searches each day and has a market share of over 90% at the time of writing (August 2019). Developed originally by Larry Page and Sergey Brin in 1997, Google has become so successful that it has become synonymous with search engine services, even entering the dictionary as a verb, with people using expressions such as: "I googled it" when they've searched for something online.

2. Bing

The origins of Microsoft's Bing can be found in the technology company's earlier search engines, MSN Search, Windows Live Search, and Live Search. Bing was launched in 2009 with high hopes that it could usurp its rival Google, but despite attracting many fans, things haven't quite worked out that way. Even so, Bing is the third largest search engine worldwide after Google and Baidu. It is available in 40 different languages.

3. Yahoo!

Yahoo! Search is another big player in the search engine world. However, for much of its history it has supplied the user interface, but relied on others to power the searchable index and web crawling. From 2001 to 2004, it was powered by Inktomi and then Google. From 2004, Yahoo! Search was independent until a deal was struck with Microsoft in 2009 whereby Bing would power the index and crawling.

4. Ask.com

Originally known as Ask Jeeves, Ask.com is a little different from Google and Bing, as it uses a question and answer format. For a number of years, Ask.com was focused on becoming a direct rival to the big search engines, but nowadays, answers are supplied from its vast archive and users contributions, along with the help of an unnamed and outsourced third-party search provider.

5. Baidu

Founded in the year 2000 by Robin Li and Eric Xu, Baidu is the most popular search engine in China, and the fourth most visited website in the world, according to Alexa rankings. Baidu has its origins in RankDex, a search engine previously developed by Robin Li in 1996. As well as its Chinese search engine, Baidu also offers a mapping service called Baidu Maps and more than 55 other internet-related services.

6. AOL.com

AOL, now styled as Aol. and originally known as America Online, was a big player in the early days of the internet revolution, providing a dial-up service for millions of Americans in the late 1990's. Despite AOL's decline as broadband gradually replaced dial-up, the AOL search engine is still used by a significant minority of searchers. On June 23, 2015, AOL was acquired by Verizon Communications.

7. DuckDuckGo

DuckDuckGo (DDG) has a number of features that distinguish it from its main competitors. It has a strong focus on protecting searchers' privacy, so rather than profiling users and presenting them with personalized results, it provides the same search results for any given search term. There's also an emphasis on providing quality rather than quantity when it comes to search results. DDG's interface is very clean and not overladen with adverts.

8. WolframAlpha

WolframAlpha markets itself as a computational knowledge engine. Instead of answering the queries of searchers with a list of links, it responds with mathematical and scientific answers for their questions, using externally sourced "curated data". WolframAlpha was launched in 2009 and has become a valuable tool for academics and researchers.

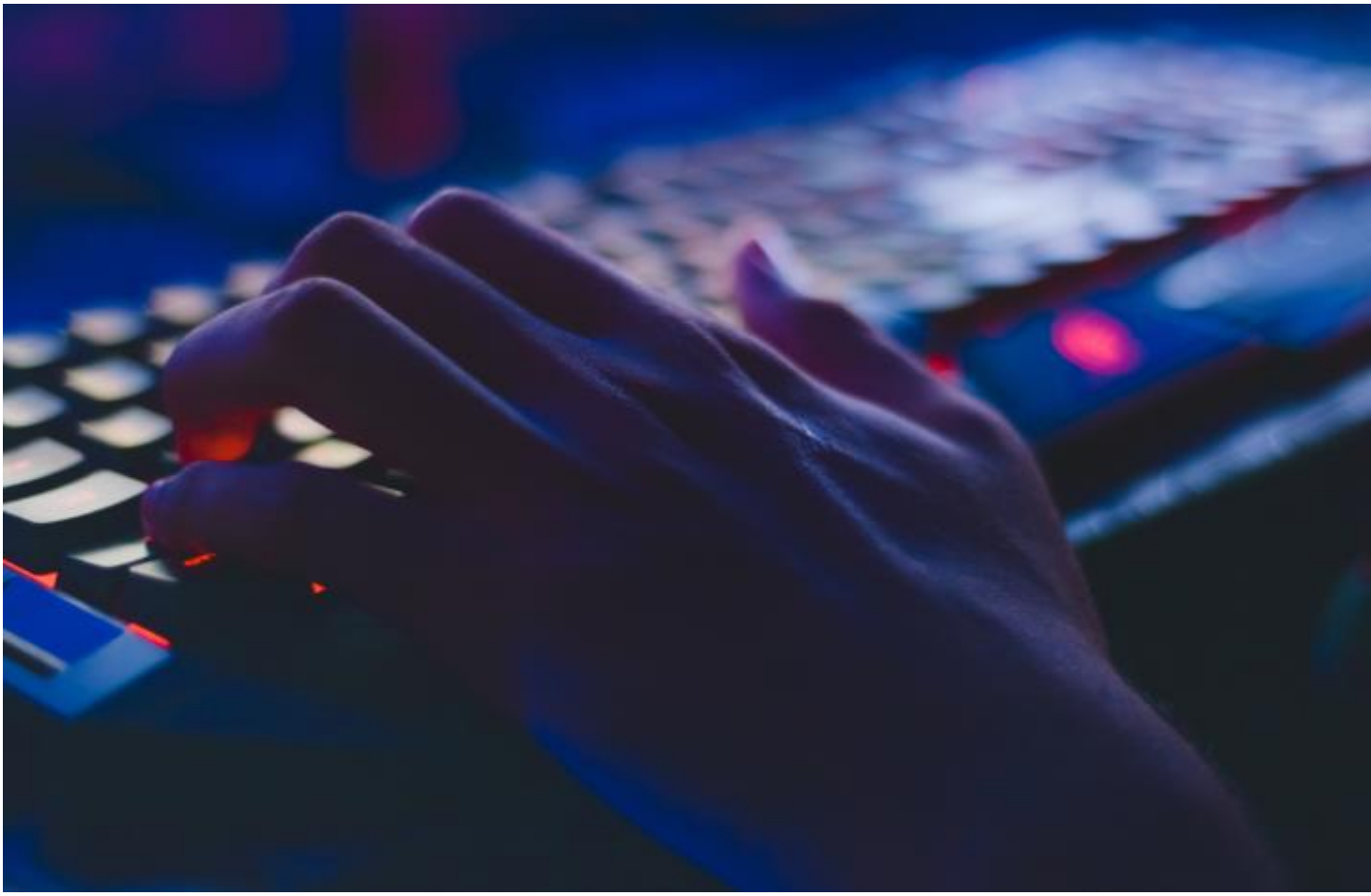
9. Yandex

Launched in 1997, Yandex is Russia's largest search engine, and the country's fourth most popular website. Outside of Russia, the search engine also has a major presence in Ukraine, Belarus, Kazakhstan, and other countries of the Commonwealth of Independent States. As well as search, Yandex offers many other internet-related products and services, including maps and navigation, music, eCommerce, mobile applications, and online advertising.

10. Internet Archive

The Internet Archive provides free public access to a wide range of digital materials. A nonprofit digital library based in San Francisco, it's a great tool for tracing the history domains and seeing how they have evolved over the years. Besides websites, you can also find software applications and games, movies/videos, music, moving images, and a huge collection of public-domain books. The Internet Archive also campaigns for a free and open internet.

ANSWAR;12. Importance Of Internet Technology For Easy Life



Today, the internet has become unavoidable in our daily life. Appropriate use of the internet makes our life easy, fast and simple. The internet helps us with facts and figures, information and knowledge for personal, social and economic development. There are many uses of the internet, however, the use of the internet in our daily life depends on individual requirements and goals. That is why we have internet plans that suit those needs, whether that be Xfinity internet plans for the home or business internet, each one has a part to play.

1. Uses of the Internet in Education

The Internet is a great platform for students to learn throughout their lifetime. They can use the internet to learn new things and even acquire degrees through online education programs. Teachers can also use the internet to teach students around the world.

2. Internet Use to Speed Up Daily Tasks

The Internet is very much useful in our daily routine tasks. For example, it helps us to see our notifications and emails. Apart from this, people can use the internet for money transfers, shopping order online food, etc.

3. Use of the Internet for Shopping

With the help of the internet, anybody can order products online. With multiple choices ranging from online home décor stores to buying coats and jackets from Gym King or similar companies, the options are endless. Moreover, the increase in online shopping has also resulted in companies offering a huge discount for their customers.

4. Internet for Research & Development

The Internet plays a pivotal role in research and development as it is propelled through internet research. The benefit of the internet is enjoyed by small businessmen to big universities.

5.Business Promotion and Innovation

The Internet is also used to sell products by using various e-Commerce solutions. The result is new services and businesses starting every day thereby creating job opportunities and reducing unemployment.

6.Communication

Without a doubt, the internet is the most powerful medium of communication at present. It connects people across different parts of the world free and fast.

7. Digital Transactions

The internet facilitates internet banking, mobile banking, and e-wallets. Since all digital transactions are stored in a database, it helps the government to track income tax details or income reports in the ITR. It is also great for small businesses who are potentially looking at florida business banking services, or ones closer depending on the location of their business, so they can do everything remotely that can help them with keeping it running.

8. Money Management

The internet can also be used to manage money. Now there are many websites, applications, and other tools that help us in daily transactions, transfers, management, budget, etc. With the growing popularity of digital currency, it could be said that the internet is the necessity of this century. Cryptocurrency is one of the major platforms for trading digital assets or digital money through blockchain technology. If you want to learn more about how to invest in crypto, you can check out Bitcoin Prime review or other similar blogs.

9. Tour & Travel

During tour and travel, the use of the internet is highly effective as it serves as a guide. People browse the internet before they start visiting the places. Tour bookings can also be done using the internet.

The influence of the internet in our daily life is huge. It has opened us a magical world of information and we would have never seen the world as it is without the internet. Considering its scope and importance, it would be hard to imagine a world without the internet.

ANSWAR;13. Give some example of Internet Service providers.

Examples of ISP (Internet Service providers) are: Airtel, Jio, ACT

Explanation

- An Internet Service Provider (ISP) is the industry term for the company that is able to provide you with access to the Internet, typically from a computer.
- The examples of some internet service providers are Hathway, BSNL, Tata teleservices, Verizon, Reliance Jio, ACT Fibernet and many more working in India as well as worldwide.
- Internet service providers or ISPs are responsible for providing services for using the Internet. The several services provided by them are Internet transit and access, domain name registration, web hosting, and colocation.

An Internet Service Provider (ISP) is acompany such as AT&T, Verizon,Comcast, or BrightHouse that provides Internet access to companies, families, and even mobile users. ISPs use fiber-optics, satellite, copper wire, and other forms to provide Internet access to its customers

An Internet Service Provider (ISP) is the industry term for the company that is able to provide you with access to the Internet, typically from a computer. If you hear someone talking about the Internet and they mention their "provider," they're usually talking about their ISP.

Your ISP makes the Internet a possibility. In other words, you can have shiny computer with a built-in modem and could have a router for networking, but without a subscription with an ISP, you won't have a connection to the Internet.

For the typical homeowner or apartment dweller, the ISP is usually a "cable company" that, in addition or offering a TV subscription, also offers an Internet subscription. You don't get both for the price of one, however. You can get just cable TV or just high-speed Internet, or both.

An ISP is your gateway to the Internet and everything else you can do online. The second your connection is activated and set up, you'll be able to send emails, go shopping, do research and more. The ISP is the link or conduit between your computer and all the other "servers" on the Internet. You may feel like you're talking to your mom directly through email, but in reality it's

more "indirectly." Your email goes from your computer, to the ISP computers/servers, where it's sent along to its destination through other servers on the network.

Of course, that's its "electronic" path: the transmission is still virtually instantaneous.

Every home or organization with Internet access has an ISP. The good news is, we don't all have to have the same provider to communicate with each other and we don't have to pay anything extra to communicate with someone who has a different ISP.

Whereas just about anyone can have a website, not everyone can be an ISP. It takes money, infrastructure and a lot of very smart technicians. Your ISP maintains miles of cabling, employs hundreds of technicians and maintains network services for its hundreds of thousands of subscribers. Depending on where you live, you typically have a choice of ISPs.

Types of ISPs

In the 1990s, there were three types of ISPs: dial-up services, high-speed Internet (also referred to as "broadband") offered by cable companies, and DSL (Digital Line Subscribers) offered by phone companies. By 2013, dial-up services were rare (even though they were cheap), because they were very slow...and the other ISP options were typically readily available and much, much faster.

DSL and Cable.

Two of the leading DSL ISPs have been Verizon and AT&T. But in the last few years (from 2013), DSL has been on the decline, while cable-based ISPs, like Comcast and Time Warner, have been growing. Why the change? It's because the phone companies have been getting more into the lucrative smartphone business, and selling annual contracts for cellular service along with...smartphone Internet capabilities.

That's left a lot of the broadband business for the cable companies.

Fiber Internet: On its way to you?

With DSL dropping out of the picture, there's room for a new technology and it's already here in some areas: it's called fiber, or fiber optical, broadband. Supposedly, fiber is hundreds times FASTER than cable or DSL. That's especially exciting news (if it's true and available) to companies, and gamers and households with a lot of simultaneous wireless usage going on.

Verizon (yes, they are downplaying DSL) now offers FiOS in select areas (put an "f" before "eye" and the "os"-sound in "most"). FiOS stands for fiber optic services, and it claims to have superfast Internet connection speeds.

And for all of us not in the Kansas area, Google launched Google Fiber in 2013, which offers incredibly ultra-fast Internet speed. Other companies (and communities) are teaming up to bring the next generation of broadband to

An Internet Service Provider (ISP) is a company such as AT&T, Verizon, Comcast, or Spectrum that provides Internet access to companies, families, and even mobile users. ISPs use fiber-optics, satellite, copper wire, and other forms to provide Internet access to its customers. **An Internet Service Provider (ISP) is a company such as AT&T, Verizon, Comcast, or Spectrum that provides Internet access to companies, families, and even mobile users. ISPs use fiber-optics, satellite, copper wire, and other forms to provide Internet access to its customers. An Internet service provider is an organization that provides a myriad of services for accessing, using, or participating in the Internet. Internet service providers can be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned**
An Internet Service Provider (ISP) is a company such as AT&T, Verizon, Comcast, or BrightHouse that provides Internet access to companies, families, and even mobile users. ISPs use fiber-optics, satellite, copper wire, and other forms to provide Internet access to its customers.

ANSWAR;14.What is the difference between an IP address, a MAC address, and a port address? In which cases are these addresses used?

former Telecommunications Technician (1979-1990)

Answered 4 years ago · Author has 662 answers and 265.2K answer views

A MAC address is assigned to the network interface card by the manufacturer and is used for communication within the local area network. It is a globally unique address.

An IP address is used for communication within the local area network and for communication between networks (usually through the Internet).

Port numbers are used as part of IP communications to determine which program the communication is to or from.

This may be clearer if I relate it to the OSI (Open Systems Interconnect) model. This specifies 7 layers of communication. The left column is a memory key, read it from the bottom t

Ross Boulet

, IT Consultant at Boulet and Associates (1985-present)

Answered 4 years ago · Author has 152 answers and 69.8K answer views

There is a great technical explanation answer already, but for those that would like a more generic explanation:

Think of the IP address like a mailing address. The address can be divided in to parts, and some of those parts can be broken down further. Part of the IP address is like the zip code which gets mail to the right area (think network). The rest of the IP address is like the street address that identifies a specific building (think computer or server). But the local mail carrier delivers mail based on a physical address that the builder engraved on the buildings (think MAC address) bef

Ashish Singh

, studied Computer Science and Engineering at Amity University (2017)

Answered 3 years ago

Related

What is an IP address?

Let me tell you things that you better know about IP Address, Probably you know some of them already.

- **We need Them… Period.!!**
  yes I said it. we need them for connecting different systems/devices on network in order to communicate with each-other/Internet.
- **IP Addresses are Logical Address:**
  An IP address is not a physical address that means *IP Address* of a device may change. The current *IP address* of your device on which you are reading this answer may change. once you go to Starbucks you connect your device to their *wi-fi route*r more likely you will get a completely different *IP Address*. This hap

Pankaj Kedia

, studied at Malaviya National Institute of Technology, Jaipur

Answered 7 years ago · Upvoted by

Anushka Gurjar

, MSc. Computer Science, University of Delhi - Department of Computer Science (2021) and

Shivam Shrivastava

, M.S. Computer Science, University of California, Irvine (2018)

Related

When a MAC address itself is unique, why do we still need an IP address to uniquely identify a system on a network?

I will try to explain this in an easy way using an analogy. So here it goes -

Let's say your name is 'A'. Obviously some other people in the world might also have the same name 'A'. This is not unique. Now let's add your father's name (say father's name is 'B') along with your name, it becomes 'B.A'. Now people with this same name will be in less number as compared to your earlier original name 'A'. But still it is not unique. Let's say we keep on adding the names of your forefathers to your name – 'A', 'B.A', 'C.B.A', 'D.C.B.A', 'E.D.C.B.A', 'F.E.D.C.B.A', …… a time will come when the n

Ajitabh Gupta

, BING!

Answered 6 years ago · Author has 62 answers and 156.1K answer views

Related

Computer Networking: What exactly happens from the moment we type www.facebook.com till we log in?

Originally Answered: What exactly happens from the moment we type www.facebook.com till we log in?

Okay so let me answer this question at the socket level, which is quite interesting:

0) So at a very basic level, each new request to a server (www.facebook.com

) from a client (your browser), initiates a TCP connection. This connection is between two endpoints, called sockets. Now each socket is nothing but a IP and Port combo. As for the server it is listening on a fixed IP and Port (by default HTTP uses port 80). The client now needs to create a new socket to initiate a connection and this is delegated to the underlying OS.

1) The first thing that happens is a socket is created by the Sockets

OKportal Technology

, studied Computer Networking & Wireless Technology at MikroTik

Answered 2 years ago · Author has 862 answers and 10.5M answer views

Related

How is the IP address distributed based on the countries?

Credit image: Index

For technical reasons, the allocation of IP addresses has to follow the topology of the network and not geography or national borders (country) so in order to answer your question correctly, **we cannot judge the location (country) the IP address from, as it was never assigned based on nations but on topology.**

An IP address is managed by IANA (Internet Assigned Numbers Authority), a non-profit U.S. corporation, with the help of RIRs (Regional Internet Registries) who manage, distribute, and publicly register IP addresses and related Internet number resources from IP address poo

Pujan Vakharia

, Student at Surat, Gujarat, India

Answered 6 years ago

Related

Do IP addresses change?

Originally Answered: Why do IP addresses change?

Let me put in a very simple manner.

What is IP address? (Laying off the technical definition...)
- When you connect your computer to any network , your computer is assigned (automatically or manually by user) an IP address. Consider this analogy. You have parked your car in a parking lot. When you want to go back to your car , you need to remember where you parked it. Suppose you remember this , 'beside the elevators in the third row'. When you have parked your car in a parking lot , you have assigned an address to it. Anyone wants to reach your car-*machine* , one can go to the parking lot -*your*

network engineer, protocol designer; networking since 1981

Updated 10 months ago · Upvoted by

Martin Visser

, 25 years of experience in enterprise networking and

Andrew Lemke

, Managing Security Consultant at IBM · Author has 7.8K answers and 11.9M answer views

Related

What is the difference between IP address and MAC address, and how they are used?

Originally Answered: Why couldn't MAC addresses be used instead of IPv4|6 for networking?

Large, flat address spaces don't scale up for routing in computer networking; it makes both routing table lookup slow, and routing table maintenance unwieldy. Ethernet (or Wi-Fi) MAC Addresses are a large, flat address space with no routing hierarchy.

Every large scale address system has hierarchy and information hiding to make routing tractable.

For example, postal addresses: what does a postman in The United Kingdom need to know about zip codes, or States and Territories of the USA, so long as the envelope says "United States of America" on it? All he has to do is forward the letter to the USA

Mike Lieberman

, 38+ years working with IP (WAN) networks, NOCs and ran ISPs.

Answered 7 months ago · Author has 341 answers and 1M answer views

Related

Why do we have private IP addresses when we could just use MAC addresses?

MAC addresses do not survive the first hop. They are designed to tell any device connected to the same *segment* of local area network, *it's me!* But if you have a LAN with more than one switch the next switch will not see the address of the '*it's me* device. Rather, it sees the MAC address of a port on the switch *it's me* is connected to. And so you might see a few dozen devices with different IP addresses all advertised via the same MAC address; one which belongs to none of them but rather the switch they are connected to.

MAC addresses function at level 2 of the OSI and IP at level 3. They perfor

Dani Richard

, B.S. Information and Computer Science & Systems Programming, Georgia Institute of Technology

Answered 2 years ago · Upvoted by

Ed Bell

, 25+ yrs prof experience supporting networked computers. · Author has 4.6K answers and 6.3M answer views

Related

What exactly does an IP address tell about us and what does IP stand for?

“Internet Protocol”

Depend if it is an IPv4 or IPv6 address.

IPv4 address gets quickly complicated.

Originally IPv4 address was broken in to A, B, and C class addresses. Each class had a different demarcation between the number of sub-nets and number of host.

Later the “address mask” was added to facilitate additional sub-netting within an address class.

Also some address within each class were “not routable” outside a Local Area Network. So those addresses are “translated” by NAT (Network Address Translation) at the “edge router” that connects between the LAN to the “WAN” (Wide Area Network).

Each

Pranav Bharti

Answered 3 years ago

Related

Which port is used for ping?

ICMP(Internet Control Message Protocol)

Siddhant Dash

, Thinker and Doer

Answered 4 years ago · Author has 504 answers and 782.6K answer views

Related

What is meant by an IP address and a Mac address?

Originally Answered: What is meant by IP address and a Mac addresss?

MAC :

A MAC (or Machine Access Control) address is best thought of as kind of serial number assigned to every network adapter

. No two anywhere *should* have the same MAC address.

Each network adapter on your computer, including wired and wireless interfaces, has one.

MAC addresses are typically used only to direct packets from one device to the next as data travels on a network.

That means that your computer's network adapter's MAC address travels the network only until the next device along the way. If you have a router

, then your machine's MAC address will go no further than that. The MAC address

BTECH Electronics and Communication Engineering & Computer Networking, Adams Enginnering College (2014)

Answered 4 years ago · Author has 64 answers and 277.1K answer views

Related

What is the difference between telnet IP-address and telnet IP-address source IP-address?

When using telnet from an end user to remote network or device, we use Telnet Ip Address. Which helps us to connect to that device and perform desired actions.

Telnet Ip address Source Ip Address is used to connect a device from one location to device in other location. In this case what happens is we will be having more than one Ip address per device as Interface Ip,loopback Ip, management Ip.

In the above case we will use source Ip to say that to have a remote access to destination network using source Ip from my device.

Example: when we use Telnet from a router from Hyderabad to a router in De

Hashin Jithu

, Engineer, student of History, Philosophy and Anthropology.

Updated 7 years ago · Upvoted by

Ed Bell

, 25+ yrs prof experience supporting networked computers. · Author has 508 answers and 1.3M answer views

Related

What is the need of an IP address versus a MAC address?

Originally Answered: What is the need of an IP address over a Mac address?

MAC address is an address that is assigned to your hardware that is used as a signature to make it stand out from the network hardware used by the rest of world. It is a 48 bit address and is fixed for your device.

Since it is device specific, it doesn`t represent any qualities of the network you are connected with. For instance, it carry no useful information about your geographical area, nearest node, etc.

A real life analogy will be like giving your house name to a foreigner and asking him to find your home. We can be almost certain that he will never find your house. This is because any fea

Andrew McGregor

, IETF member since 2000

Answered 1 year ago · Author has 11.5K answers and 57.3M answer views

Related

Does a VPN hide your IP address?

Originally Answered: Can a VPN really hide your IP address?

Yes, to an extent. It makes it look like you're in the data center where your VPN endpoint is.

But it is also true that you don't care about people knowing your IP address most of the time.

Lars Poulsen

, I am the IT department at my workplace.

Answered 4 years ago · Author has 1.2K answers and 1.2M answer views

Related

What is the disadvantage of associating each registered MAC address with a predetermined IP address?

How good are your system management skills?

The default these days is that every device is set up to get its IP address "from the network", i.e. from a DHCP (Dynamic Host Configuration Protocol) server. This means that you don't need to go into the settings on your mobile phone when you move it from your home to your office or the local coffee shop. As soon as you are connected, you have an IP address that is compatible with the local network.

But it is possible to set up a DHCP server so that it has a list of known MAC addresses and issues the same IP address every time the device with that MAC

Rafael Dellà

, Network Technical Assistant (2012-present)

Answered 3 years ago · Author has 53 answers and 121.7K answer views

Related

What makes a MAC address different from an IP address and a port address?

The MAC address is a **fixed number** in any network interface **and unique**. There is **no math involved**. It's just a number to identity the device by the "layer 2" devices (switchs, hubs, bridges, etc) to exchange data with.

IP address is a **non-fixed** number (meaning, can change up to your choice or ISP's) It has some kind of math (with the mask number) used by routers (Layer 3 devices) to know where in the whole network you are.

Port number (not address) is an **arbitrary number** that **identifies services** runing in servers. There are many "well known" of this: like FTP (port 21) HTTP (80) HTTPS (443) etc…

Anwar Ahmed

Answered Mar 26, 2022

Related

What is the difference between a MAC address and an IP address? Which address can you assign to a computer?

Both are used to identify a device on the network, the Mac address is the physical unique address of a device given by the manufacturer, it allows communication between devices on the same network and it's a layer2 address, while IP address is a logical L3 address that allows communication between different network hosts, it's assigned by your ISP and there are two types private and public.

Internet needs both.

Ricardo Mendes

, Consultant, entrepreneur, so much more! 10+ on the Mac.

Answered 3 years ago · Author has 201 answers and 210.3K answer views

Related

Why do we use mac addresses if ip addresses are unique? why don't we just use ip adresses to forward the packets?

Thanks for the A2A.

You are starting with a wrong statement. Private network IP's aren't unique - only to that organization)

The public IP address pool is, so to say, unique, as one address can only be assigned to one interface faced to the public network.

The thing here is, there are far more devices (and interfaces) than there are IP addresses.

IPv4 which is 32 bit and allows for 4,294,967,296 different unique addresses. From these, 592,708,864 (RFC 6598) are reserved, so that leaves you 3,702,258,432 addresses.

MAC address is 48-bit and allow for 281,474,976,710,656 unique addresses.

The IPv6 is

ANSWAR;15. View & delete your Chrome browsing history

You can view your browsing history in Chrome. On a desktop or laptop computer, you can use the Journeys view of history to continue browsing that you've already started and find related searches.

If you don't want a record of pages you visited in Chrome, you can delete all or some of your browsing history. If you delete your browsing history, it takes effect on all devices where you turned sync on and signed in to Chrome. You can also disable the Journeys view of history if you'd like.

Separately, you can also delete your Google search history from your account.

Learn more about how to turn sync on or off in Chrome.

Android ComputeriPhone & iPad

See your history

On your Android phone or tablet, open the Chrome app .

1. At the top right, tap More > **History**.
    - If your address bar is at the bottom, swipe up on the address bar. Tap History .
2. To visit a site, tap the entry.
    - To open the site in a new tab, touch and hold the entry. At the top right, tap More > **Open in new tab**.
    - To copy the site, touch and hold the entry. At the top right, tap More > **Copy link**.

Clear your history

1. On your Android phone or tablet, open the Chrome app .
2. At the top right, tap More > **History**.
    - If your address bar is at the bottom, swipe up on the address bar. Tap History .
3. Tap **Clear browsing data**.
4. Next to "Time range:"

    - To clear a portion of your history, select the dates.
    - To clear everything, tap **All time**.
5. Check the box next to "Browsing history."
6. Uncheck any other data you don't want to delete.
7. Tap **Clear data**.

Tip: In My Activity, you can delete your search history.

Delete an item from your history

You can delete certain parts of your history. To search for something specific, at the top right, tap Search .

1. On your Android phone or tablet, open the Chrome app.
2. At the top right, tap More > **History**.
    - If your address bar is at the bottom, swipe up on the address bar before you tap History.
3. Find the entry you want to delete.
4. To the right, tap Remove.

To delete multiple items:

1. Touch and hold an entry.
2. Select other entries you want to delete.
3. At the top right, tap Remove.

Tip: You can remove an item from a specific site's history while on that site:

- Tap Lock > Last visited > Remove.

Remove an image from New Tab page

To see the sites you visit most, open a new tab. To remove an image, touch and hold it. Then, select **Remove**.

What your history page shows

Your History page shows the webpages you've visited on Chrome in the last 90 days. It doesn't store Chrome pages you've visited like chrome://settings, pages you've visited in Incognito mode, or pages you've already deleted from your browsing history.

If you're signed in to Chrome and syncing your history, then your History page shows webpages you've visited across all your synced devices for much longer. If you're signed out of Chrome, your History page won't show webpages across your other devices.

Browse privately

If you don’t want Chrome to save your browsing history at all, you can browse in private with Incognito mode.

Using a Chromebook at work or school? Your network administrator can turn off browsing history. If history is off, your History page won't list webpages you've visited. Learn about using a managed Chrome device.

Related resources

- Search the web on Chrome
- Set your default search engine