CCA-102: Data Communications

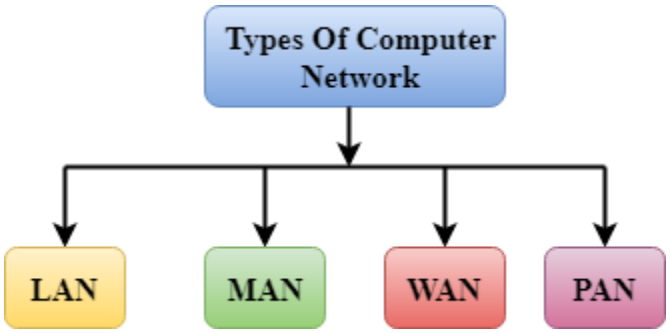
ASSIGNMENT

1. What are the different types of networks?

Ans Computer Network Types

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:



- LAN(Local Area Network)
- PAN(Personal Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

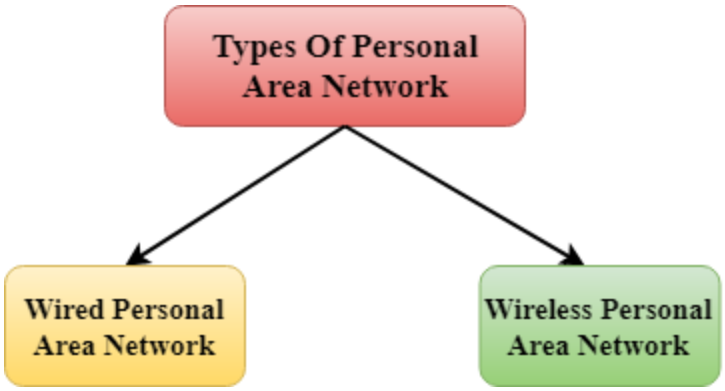
LAN(Local Area Network)

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

PAN(Personal Area Network)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of **30 feet**.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

There are two types of Personal Area Network:



- Wired Personal Area Network
- Wireless Personal Area Network

Wireless Personal Area Network: Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

Wired Personal Area Network: Wired Personal Area Network is created by using the USB.

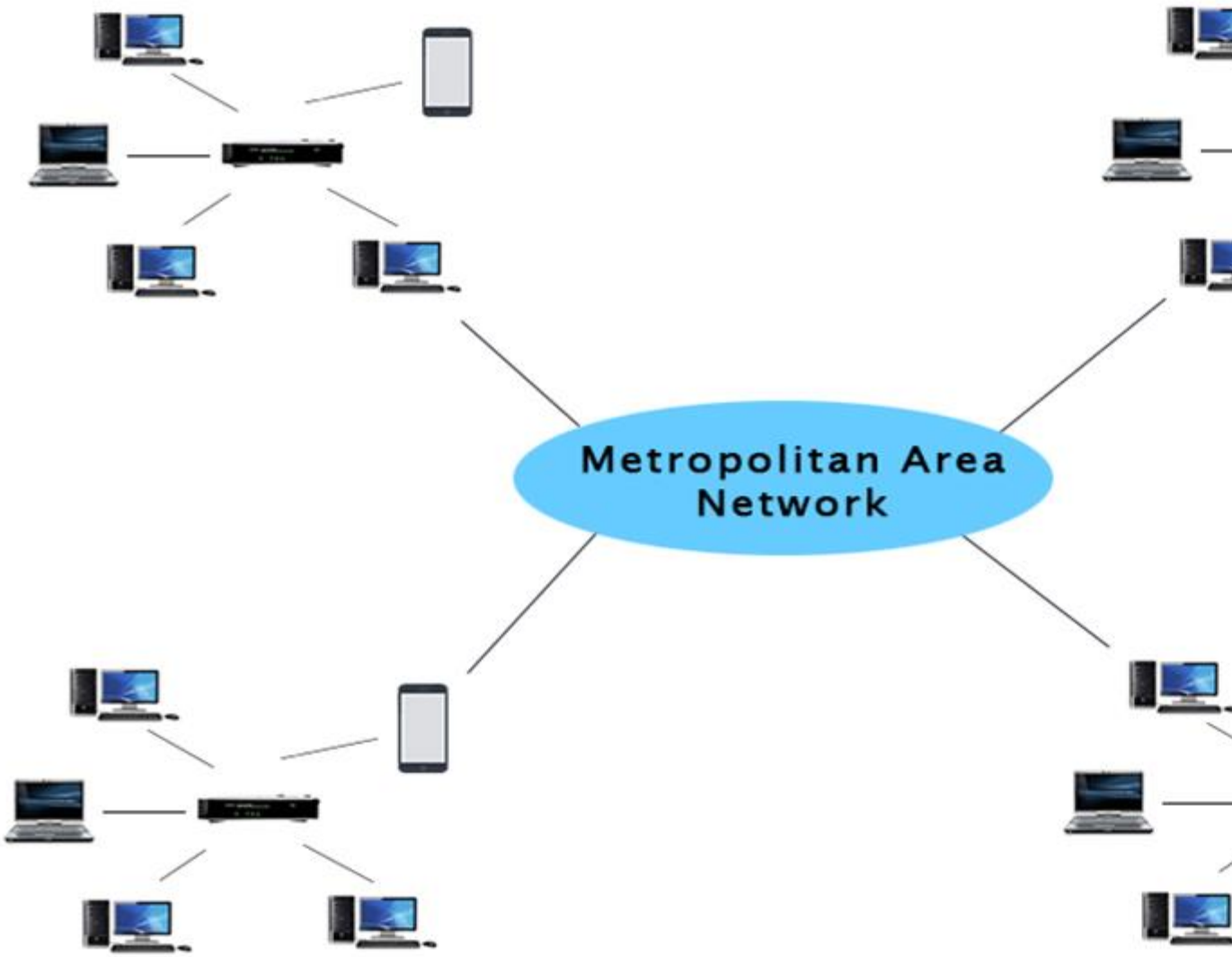
Examples Of Personal Area Network:

- **Body Area Network:** Body Area Network is a network that moves with a person. **For example**, a mobile network moves with a person. Suppose a person establishes a network connection and then creates a connection with another device to share the information.

- **Offline Network:** An offline network can be created inside the home, so it is also known as a **home network**. A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.
- **Small Home Office:** It is used to connect a variety of devices to the internet and to a corporate network using a VPN

MAN(Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).



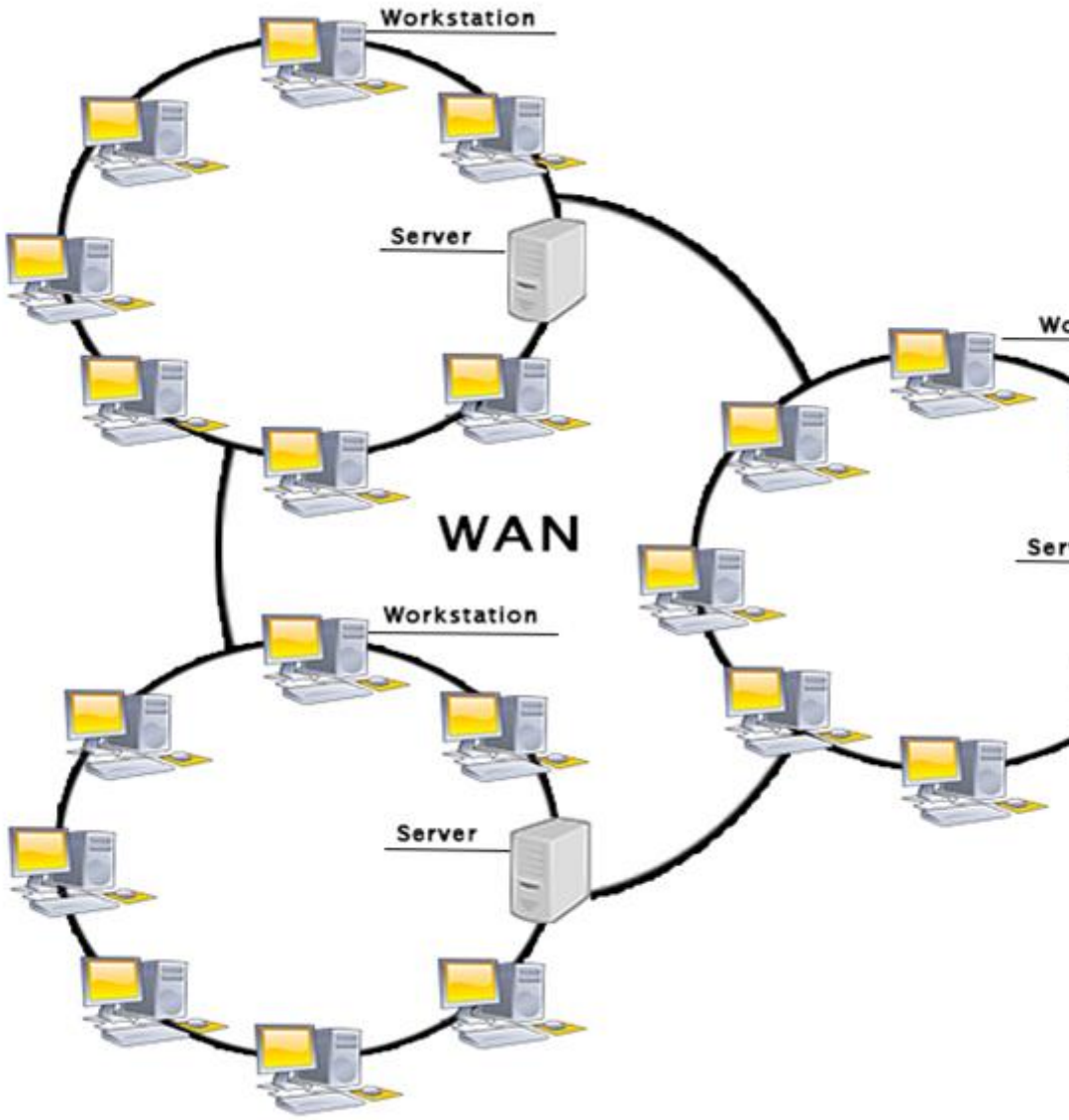
Uses Of Metropolitan Area Network:

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

WAN(Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.

- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.



Examples Of Wide Area Network:

- **Mobile Broadband:** A 4G network is widely used across a region or country.

- **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Advantages Of Wide Area Network:

Following are the advantages of the Wide Area Network:

- **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business:** We can do the business over the internet globally.
- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall

needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.

- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

Internetwork

- An internetwork is defined as two or more computer network LANs or WAN or computer network segments are connected using devices, and they are configured by a local addressing scheme. This process is known as **internetworking**.
- An interconnection between public, private, commercial, industrial, or government computer networks can also be defined as **internetworking**.
- An internetworking uses the **internet protocol**.
- The reference model used for internetworking is **Open System Interconnection(OSI)**.

Types Of Internetwork:

1. **Extranet:** An extranet is a communication network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. It is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, atleast it must have one connection to the external network.

2. **Intranet:** An intranet is a private network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

Intranet advantages:

- **Communication:** It provides a cheap and easy communication. An employee of the organization can communicate with another employee through email, chat.

- **Time-saving:** Information on the intranet is shared in real time, so it is time-saving.
- **Collaboration:** Collaboration is one of the most important advantage of the intranet. The information is distributed among the employees of the organization and can only be accessed by the authorized user.
- **Platform independency:** It is a neutral architecture as the computer can be connected to another device with different architecture.

2. Explain the Shielded twisted pair (STP) and Unshielded twisted pair(UTP)

STP and UTP Cables

Shielded twisted pair cable (STP) has the individual pairs of wires wrapped in foil, which are then wrapped again for double protection. Unshielded twisted pair cable (UTP) has each pair of wires twisted together. Those wires are then wrapped in tubing without any other protection. UTP cables are less expensive, and a more popular type of cabling.

Why are Shielded Cables Necessary?

Knowing which cable to use for a specific application depends on the protection needed from power frequency and any electromagnetic interference (EMI). This is where shielded vs. unshielded cable becomes important.

Preventing Electromagnetic Interference (EMI)

Electromagnetic interference (EMI), or radio frequency interference (RFI) as it's also referred to, is an electronic disturbance generated by external electronic or electrical sources such as electrostatic coupling, electromagnetic radiation, or electrical circuit noise. The truth is, EMI/RFI is all around us. Just like the static you may hear during a phone call, the same is true for networking. If the EMI 'noise' is strong enough it may interfere with the actual data traffic and prevent computers from 'hearing' each other. When this happens, data is lost and the network has to resend the information a second time. The more often this process is repeated, the more often the network slows down. Thus, EMI disturbances can lower performance of a circuit or prevent it from functioning properly. Data paths can be interrupted ranging from an increase in error rate to a complete loss of information.

Different Types of Shielded Cable

Shielded twisted pair cabling (STP) reduces electromagnetic and radio frequency interference from other devices and electronic objects to ensure a steady signal. Cables consist of a bundle of wires divided into four pairs. Each pair is twisted together to reduce crosstalk interference from the other wire pairs in the bundle. There are 3 different shielding configurations, each with their own level of protection:

- **Braided** (90% EMI shielding)
- **Spiral** (98% EMI shielding)
- **Metal-coated Mylar or foil** (100% EMI shielding)

When to Use Shielded Cable

Shielded cables are useful in any environments where there is a high chance of electronic interference, such as radio stations (**telecom cable assemblies**) and airports (**aerospace cable assemblies**). STP cables are also used in security systems to provide protection from power frequency and radio frequency interference, or in **box builds** where there are multiple different components operating in close proximity. As well as being protected from external interference, the shielding also keeps noise from exiting the cable, minimizing the chance of causing interference in other devices.

When to Use Unshielded Cable

Unshielded cable (UTP) does not utilize shielding to reduce interference. UTP cables are designed to limit electromagnetic

interference by the way the pairs are twisted inside the cable. UTP cable is most suitable for office LANS and similar **network cabling systems**. While offering less protection from interference, unshielded cables are popular because they are

- Versatile
- Inexpensive
- Easy to install
- Lightweight
- Flexible

The main disadvantage of UTP cables is their susceptibility to electromagnetic interference and radio frequency interference. They also have a smaller bandwidth compared to coaxial cables or fiber optic cables.

3. What is difference between baseband and broadband transmission?

Ans

Network+ Exam Prep: Ethernet Networking Standards

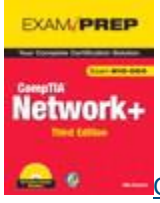
- By Mike Harwood
- Jul 28, 2009

Contents

- Print
- + Share This

This chapter is from the book

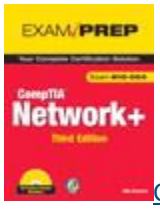
This chapter is from the book



CompTIA Network+ N10-004 Exam Prep, 3rd Edition

Learn More Buy

This chapter is from the book



CompTIA Network+ N10-004 Exam Prep, 3rd Edition

Learn More Buy

Differentiating Between Baseband and Broadband Signaling

Two types of signaling methods are used to transmit information over network media: baseband and broadband. Before we get any further into 802.3 standards we should clarify the difference between the two.

Exam Alert: Baseband and broadband

Be prepared to identify the characteristics of baseband and broadband for the Network+ exam.

Baseband

Baseband transmissions typically use digital signaling over a single wire; the transmissions themselves take the form of either electrical pulses or light. The digital signal used in baseband transmission occupies the entire bandwidth of the network media to transmit a single data signal. Baseband communication is bidirectional, allowing computers to both send and receive data using a single cable. However, the sending and receiving cannot occur on the same wire at the same time.

Note: Ethernet and baseband

Ethernet networks use baseband transmissions; notice the word "base"—for example, 10BaseT or 10BaseFL.

Using baseband transmissions, it is possible to transmit multiple signals on a single cable by using a process known as *multiplexing*. Baseband uses Time-Division Multiplexing (TDM), which divides a single channel into time slots. The key thing about TDM is that it doesn't change how baseband transmission works, only the way data is placed on the cable.

Broadband

Whereas baseband uses digital signaling, broadband uses analog signals in the form of optical or electromagnetic waves over multiple transmission frequencies. For signals to be both sent and received, the transmission media must be split into two channels. Alternatively, two cables can be used: one to send and one to receive transmissions.

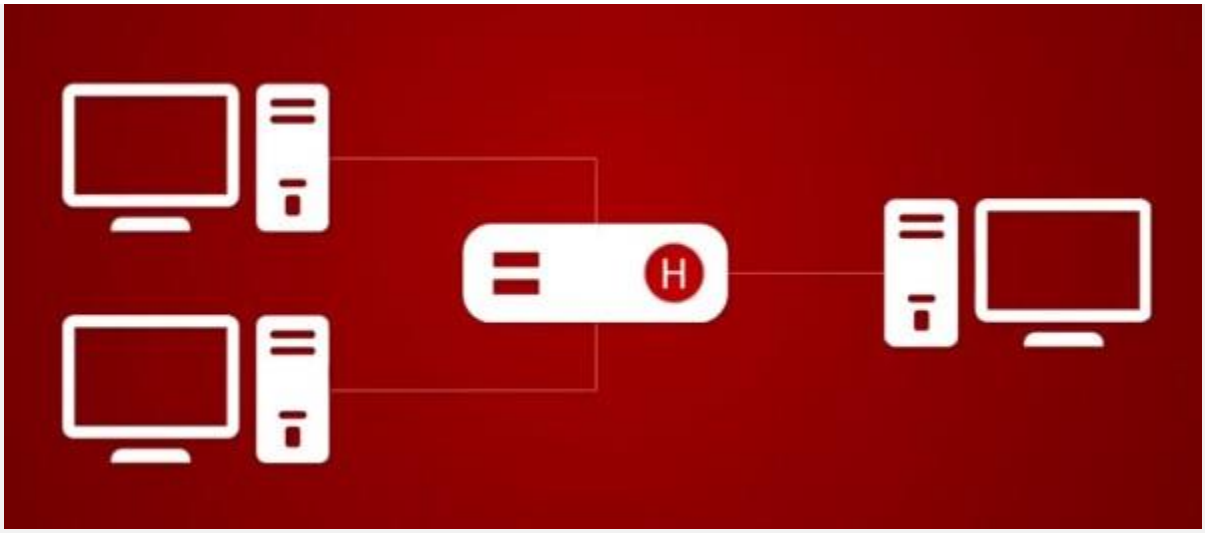
Multiple channels are created in a broadband system by using a multiplexing technique known as *Frequency-Division Multiplexing (FDM)*. FDM allows broadband media to accommodate traffic going in different directions on a single media at the same time.

4. **What is the difference between a hub, modem, router and a switch?**

Ans **Overview of Hub, Switch & Router**

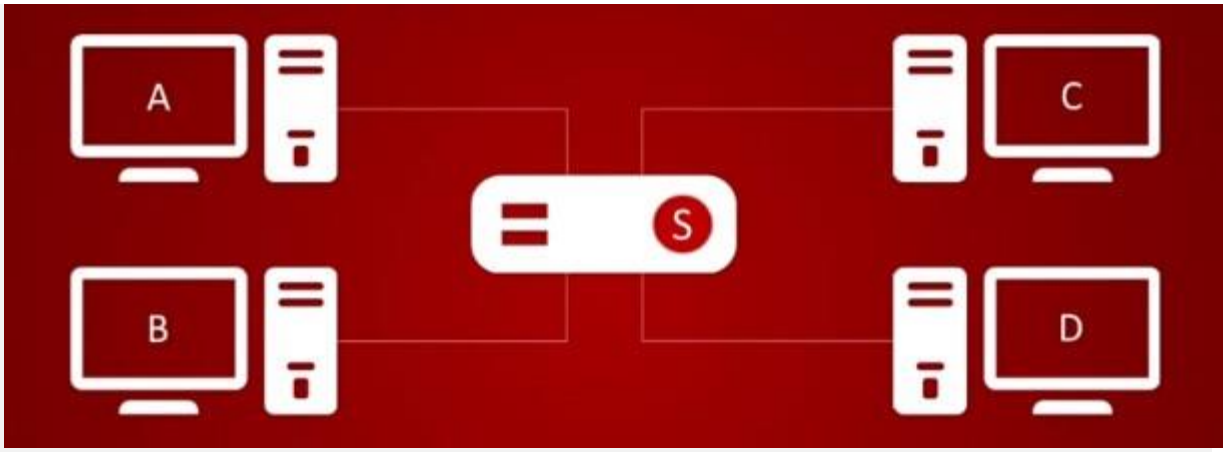
Hub

A hub is to sent out a message from one port to other ports. For example, if there are three computers of A, B, C, the message sent by a hub for computer A will also come to the other computers. But only computer A will respond and the response will also go out to every other port on the hub. Therefore, all the computers can receive the message and computers themselves need to decide whether to accept the message.



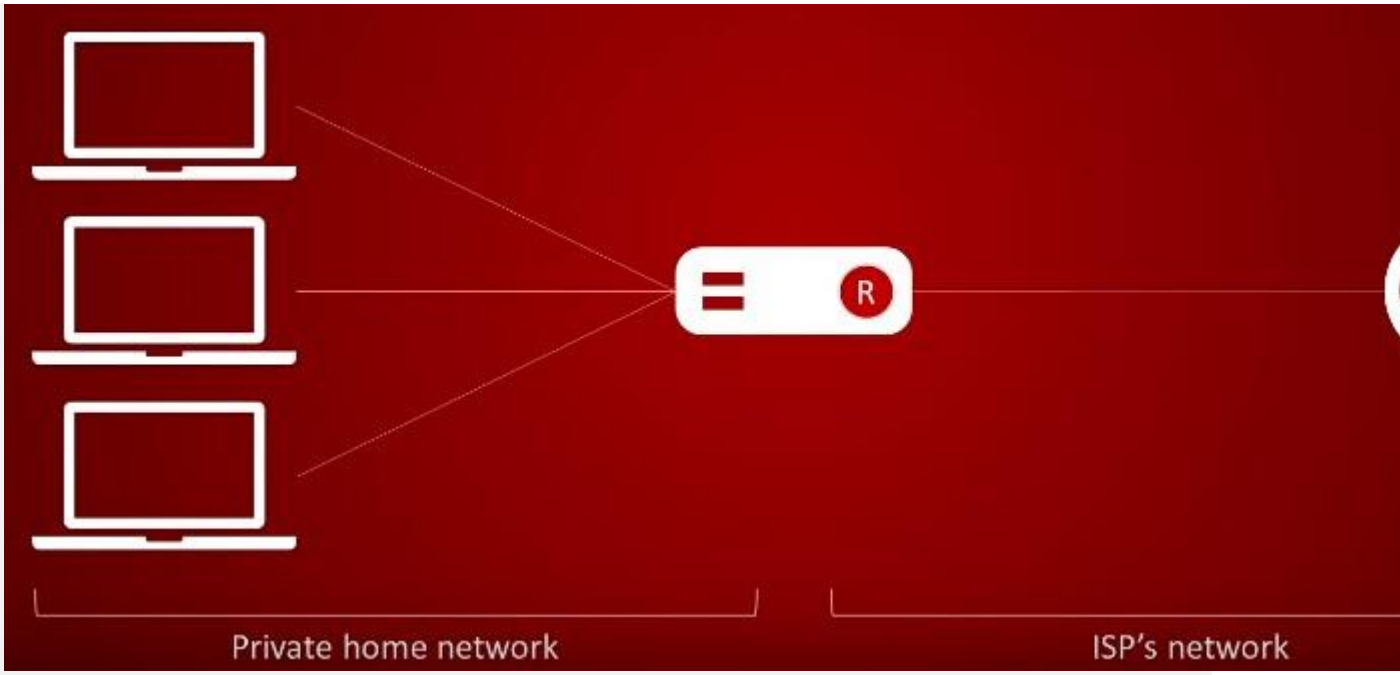
Switch

A switch is able to handle the data and knows the specific addresses to send the message. It can decide which computer is the message intended for and send the message directly to the right computer. The efficiency of switch has been greatly improved, thus providing a faster network speed.



Router

Router is actually a small computer that can be programmed to handle and route the network traffic. It usually connects at least two networks together, such as two LANs, two WANs or a LAN and its ISP network. Routers can calculate the best route for sending data and communicate with each other by protocols.



What Is the Difference?

Hub Vs. Switch

A hub works on the physical layer (Layer 1) of OSI model while Switch works on the data link layer (Layer 2). Switch is more efficient than the hub. A switch can join multiple computers within one LAN, and a hub just connects multiple Ethernet devices together as a single segment. Switch is smarter than hub to determine the target of the forwarding data. Since switch has a higher performance, its cost will also become more expensive.

Switch Vs. Router

In the OSI model, router is working on a higher level of network layer (Layer 3) than switch. Router is very different from the switch because it is for routing packet to other networks. It is

also more intelligent and sophisticated to serve as an intermediate destination to connect multiple area networks together. A switch is only used for wired network, yet a router can also link with the wireless network. With much more functions, a router definitely costs higher than a switch.

Hub Vs. Router

As mentioned above, a hub only contains the basic function of a switch. Hence, differences between hub and router are even bigger. For instance, hub is a passive device without software while router is a networking device, and data transmission form in hub is in electrical signal or bits while in router it is in form of packet.

Which One Should I Buy?

Whatever device you use for your network, you must make sure it can perform all the functions required by the network. As for performance, wireless router is recommended because it allows different devices to connect to the network. If you have a limited budget, switch is a good solution with relatively high performance and lower cost.

Conclusion

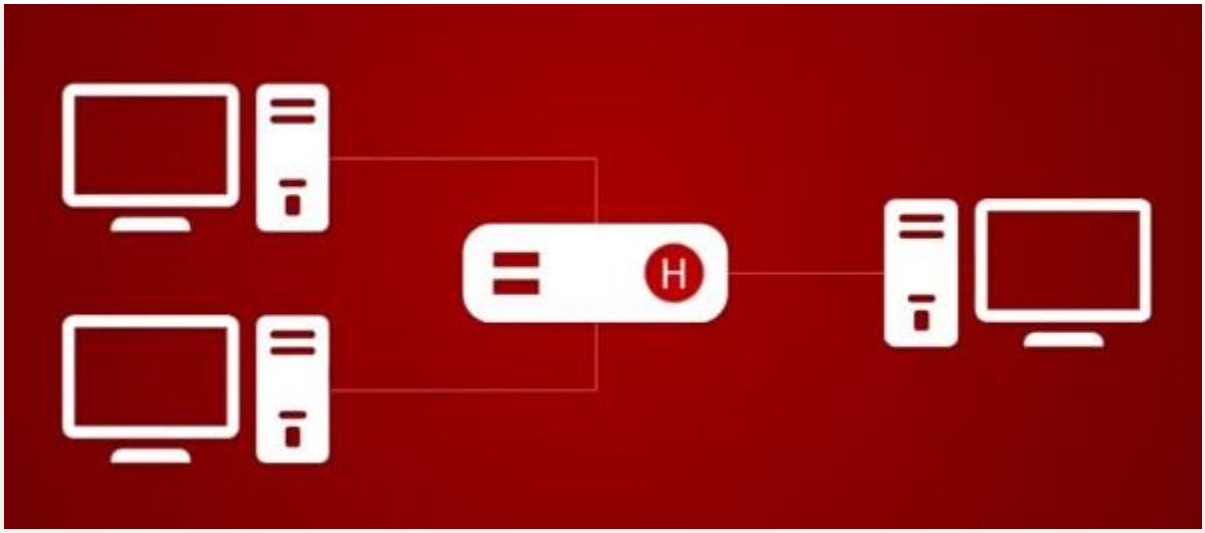
Although sometimes specialists alternatively use hub, switch or router to describe these devices, they still have their own

differences. Understanding their distinctions can be helpful to find the most appropriate device for your network.

Overview of Hub, Switch & Router

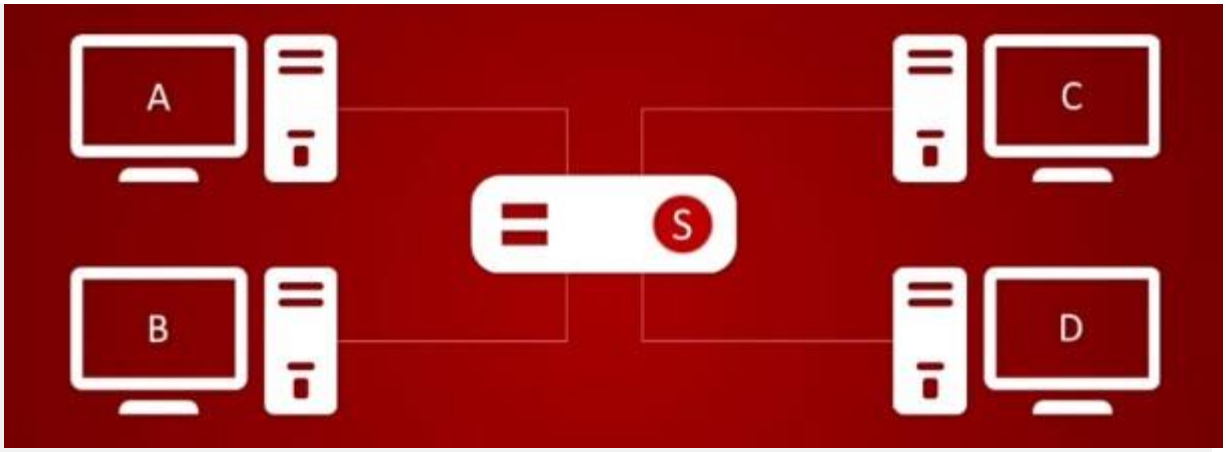
Hub

A hub is to sent out a message from one port to other ports. For example, if there are three computers of A, B, C, the message sent by a hub for computer A will also come to the other computers. But only computer A will respond and the response will also go out to every other port on the hub. Therefore, all the computers can receive the message and computers themselves need to decide whether to accept the message.



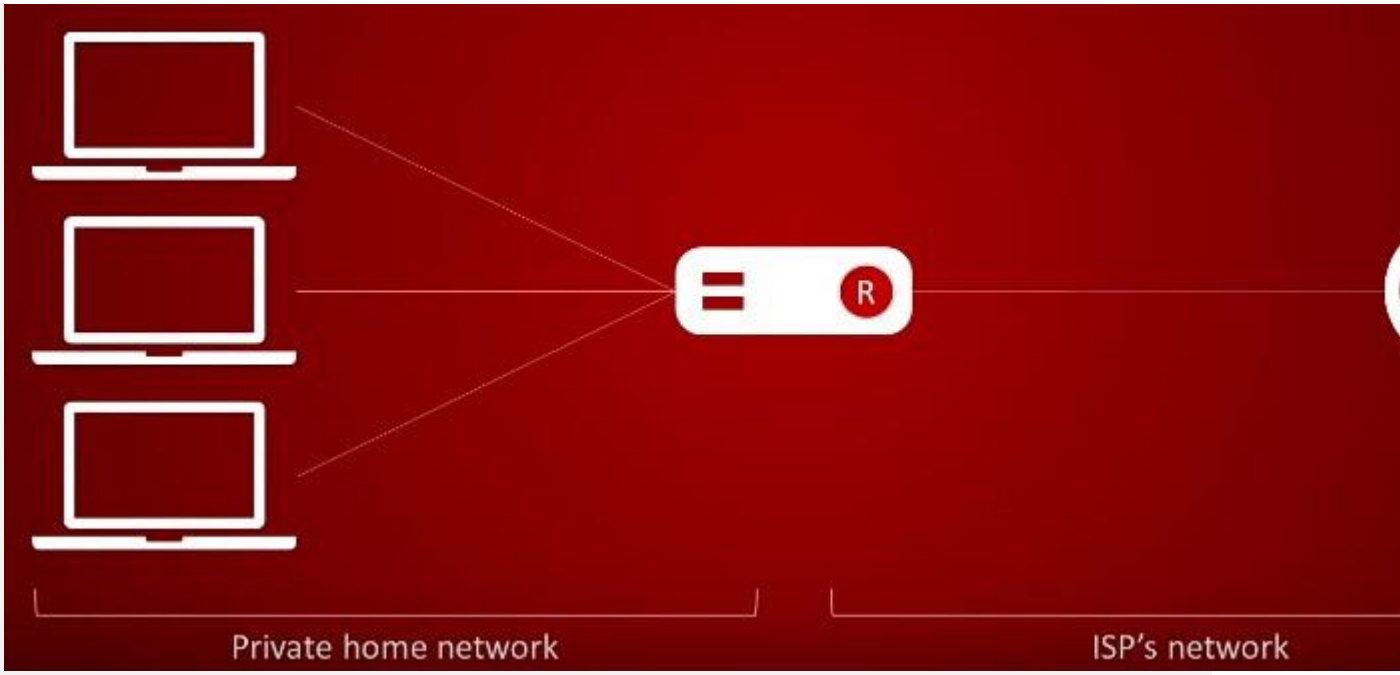
Switch

A switch is able to handle the data and knows the specific addresses to send the message. It can decide which computer is the message intended for and send the message directly to the right computer. The efficiency of switch has been greatly improved, thus providing a faster network speed.



Router

Router is actually a small computer that can be programmed to handle and route the network traffic. It usually connects at least two networks together, such as two LANs, two WANs or a LAN and its ISP network. Routers can calculate the best route for sending data and communicate with each other by protocols.



What Is the Difference?

Hub Vs. Switch

A hub works on the physical layer (Layer 1) of OSI model while Switch works on the data link layer (Layer 2). Switch is more efficient than the hub. A switch can join multiple computers within one LAN, and a hub just connects multiple Ethernet devices together as a single segment. Switch is smarter than hub to determine the target of the forwarding data. Since switch has a higher performance, its cost will also become more expensive.

Switch Vs. Router

In the OSI model, router is working on a higher level of network layer (Layer 3) than switch. Router is very different from the switch because it is for routing packet to other networks. It is

also more intelligent and sophisticated to serve as an intermediate destination to connect multiple area networks together. A switch is only used for wired network, yet a router can also link with the wireless network. With much more functions, a router definitely costs higher than a switch.

Hub Vs. Router

As mentioned above, a hub only contains the basic function of a switch. Hence, differences between hub and router are even bigger. For instance, hub is a passive device without software while router is a networking device, and data transmission form in hub is in electrical signal or bits while in router it is in form of packet.

Which One Should I Buy?

Whatever device you use for your network, you must make sure it can perform all the functions required by the network. As for performance, wireless router is recommended because it allows different devices to connect to the network. If you have a limited budget, switch is a good solution with relatively high performance and lower cost.

Conclusion

Although sometimes specialists alternatively use hub, switch or router to describe these devices, they still have their own

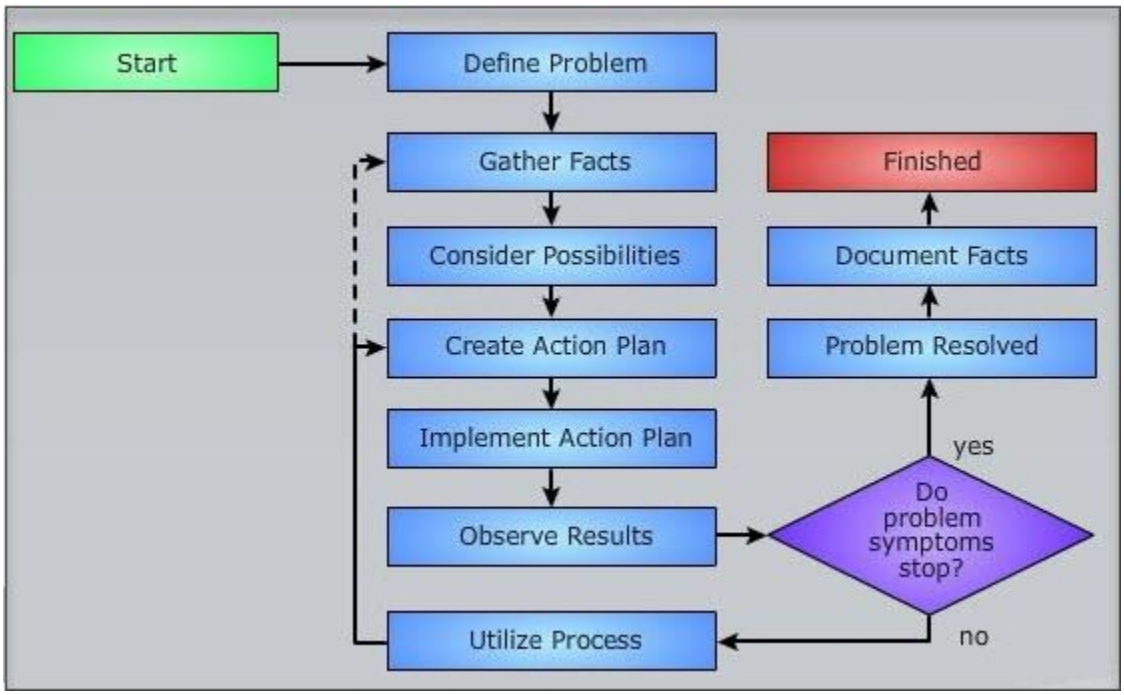
differences. Understanding their distinctions can be helpful to find the most appropriate device for your network.

5. When you move the NIC cards from one PC to another PC, does the MAC address getstransferred as well?
   Ans
6. When troubleshooting computer network problems, what common hardware-relatedproblems can occur?

Ans Basic Network Problems

- **Cable Problem**: The cable which is used to connect two devices can get faulty, shortened or can be physically damaged.
- **Connectivity Problem**: The port or interface on which the device is connected or configured can be physically down or faulty due to which the source host will not be able to communicate with the destination host.
- **Configuration Issue**: Due to a wrong configuration, looping the IP, routing problem and other configuration issues, network fault may arise and the services will get affected.
- **Software Issue**: Owing to software compatibility issues and version mismatch, the transmission of IP data packets between the source and destination is interrupted.
- **Traffic overload:** If the link is over utilized then the capacity or traffic on a device is more than the carrying capacity of it and due to overload condition the device will start behaving abnormally.
- **Network IP issue:** Due to improper configuration of IP addresses and subnet mask and routing IP to the next hop, the source will not be able to reach the destination IP through the network.

Network Troubleshooting Flowchart



[image source]

Network Troubleshooting Tools

There are various tools that are used for checking the IP reachability issues and to locate where the packet is lost while communicating with the destination host. These tools make troubleshooting easier and minimize the time for restoration.

Some of the popular tools are mentioned below:

#1) SolarWinds Engineer's Toolset

SolarWinds provides a network software, Engineer's Toolset that contains over 60 tools.

With the help of these tools, you will be able to automate network discovery. For automated network discovery, it has a set of tools like Port Scanner, Switch Port Mapper, SNMP sweep, IP Network Browser, etc.

This software has powerful diagnostic capabilities. It will perform real-time monitoring and alerting. It provides the features of IP address & DHCP scope monitoring, Configuration & log management, and enhanced network security.

Engineer's Toolset can be integrated with SolarWinds Network Performance Monitor. The tool will help you to perform network stress tests with WAN Killer. According to your specifications, it will generate random traffic and will allow you to adjust packet size, bandwidth, and percentage of bandwidth.

SolarWinds offers a fully functional free trial for 14 days. Per seat license of Engineer's Toolset will cost you $1495.

=> Download SolarWinds Engineer's Toolset For Free

#2) Obkio

Obkio is a simple network performance monitoring solution that provides real-time, end-to-end performance monitoring to help you assess the health of network and core business applications to quickly identify intermittent network problems within minutes! Obkio's software application is designed for monitoring network performance and web applications and identifies the causes of common network problems like VoIP, video, and application slowdown.

Deploy Network performance monitoring Agents at strategic locations in your company's offices or network destinations to easily identify the source of a system failure so you can quickly apply the corrective measures.

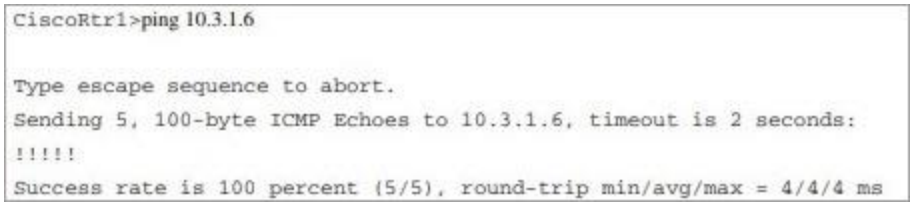
Obkio alerts you as soon as a problem occurs or even if there are signs that a failure is about to happen. Not only does it alert you and pinpoint the source of the issue, but it also allows you to go back in time to complete a diagnosis.

=> Try Obkio's End-to-end Performance Monitoring Solution For FREE!

#3) Ping

By using IP ICMP echo request and echo reply messages, the PING tool verifies the reachability to the destination host at the remote end.

It contains two messages, first is, if the data packet is competent to send and receive the messages from the destination IP address and the second is the RTT time for the process (RTT means round trip time and is calculated in milliseconds).



The exclamation shows that ping is successful. If the ping returns saying the destination is unreachable then there are many reasons for this. To find out the cause, we will go for the next tool.

#4) Trace Route

It sends the ICMP echo request messages with a step by step increase in the IP TTL (time to live) values.

The starting value is 1. It sends the data packet in a forward direction and each hop decreases the TTL value by 1 while routing the data and rejects the packet whose TTL value is zero by responding that the message ICMP time has exceeded.

Now again the source host sends the data packet, but this time with a TTL value of 2. In this way, the process will keep going until the packet has arrived at the destination and then the destination host reverts with ICMP echo reply messages.

With the help of traceroute, the router will keep a record of which route is followed by the packets to reach the destination and calculates the latency and other parameters as well.

#5) Protocol Analyzer

It is an advanced tool for finding out the network issues.

It is the software that intercepts and records the data packet flow between the source and the destination. Like, if the system is running slow then it can check for the latency issues and other networking problems which will help in diagnosing the root cause.

Steps Involved In Network Diagnostics

Here steps to troubleshoot and diagnose various network problems like IP, connectivity, wireless connection, etc.

Troubleshooting IP Problems

In the TCP/IP protocol suite, if we are not able to reach at the destination IP address and not able to find the route to reach the next hop at any point in the network, then we will use PING and TRACEROUTE tools for troubleshooting the cause and location of the issue.

The generic steps to troubleshoot the IP related issues in the network include:

- Firstly locate the pair of devices between the source and the destination host between which the connectivity issue has occurred.
- Once you locate the devices using the tools, the fault can be due to a physical connectivity issue. Thus check the physical connections all over the path.
- There can be a fault in the LAN connectivity as well if you are working in a LAN network. So check the LAN connections. The local port can be faulty or down due to which the source cannot be able to reach the destination IP.
- One of the reasons of the fault can be the router connectivity issue while traveling through various paths to reach the destination. Hence check that if the router is defined properly at each of the intermediate hops.

- Check the configuration settings.

Troubleshooting Local Connectivity Issues

Once on the broad level, if you find that there is an issue in the LAN connectivity, then in order to locate the root cause and to resolve it, you should follow the below steps:

- If the destination and the source are of the identical subnet mask, then try to ping the destination IP.
- Else, if the destination is of some other subnet mask then try to ping the gateway IP address of the router.
- Now, if both the ping fails, then first check that in the configuration settings, if both the subnet mask and route to be followed to reach the destination are defined properly in the routing table or not?
- Once you are done with the configuration part and found everything OK, then check if your source host is able to ping some another hop in the LAN network other than the destination host or route to that?
- If you are not able to ping to another device then there can be many reasons for this. It may even be a configuration issue, a physical connectivity issue, and repetitive IP address entry issue.

Correcting the Repetitive IP address Entry Issue

For rectifying the duplicate entry of an IP issue, disconnect the doubtful device from the LAN and also make the interface on which the device was connected shut down.

Now ping the device from some another device of the same subnet or LAN network. If the ping is OK, then it indicates that the IP is being used by some other device as well on the network. From the ARP table of the device, find out its MAC address and modify the IP address according to planning.

But if the problem persists still, then there will be a physical connectivity or configuration issue in it.

Troubleshooting Physical Connectivity Issues

The list of faults that come under this category are:

1. Improper connection of cables
2. Router, switch or hub port is faulty or down[].

7. In a network that contains two servers and twenty workstations, where is the best placeto install an Anti-virus program?

Ans

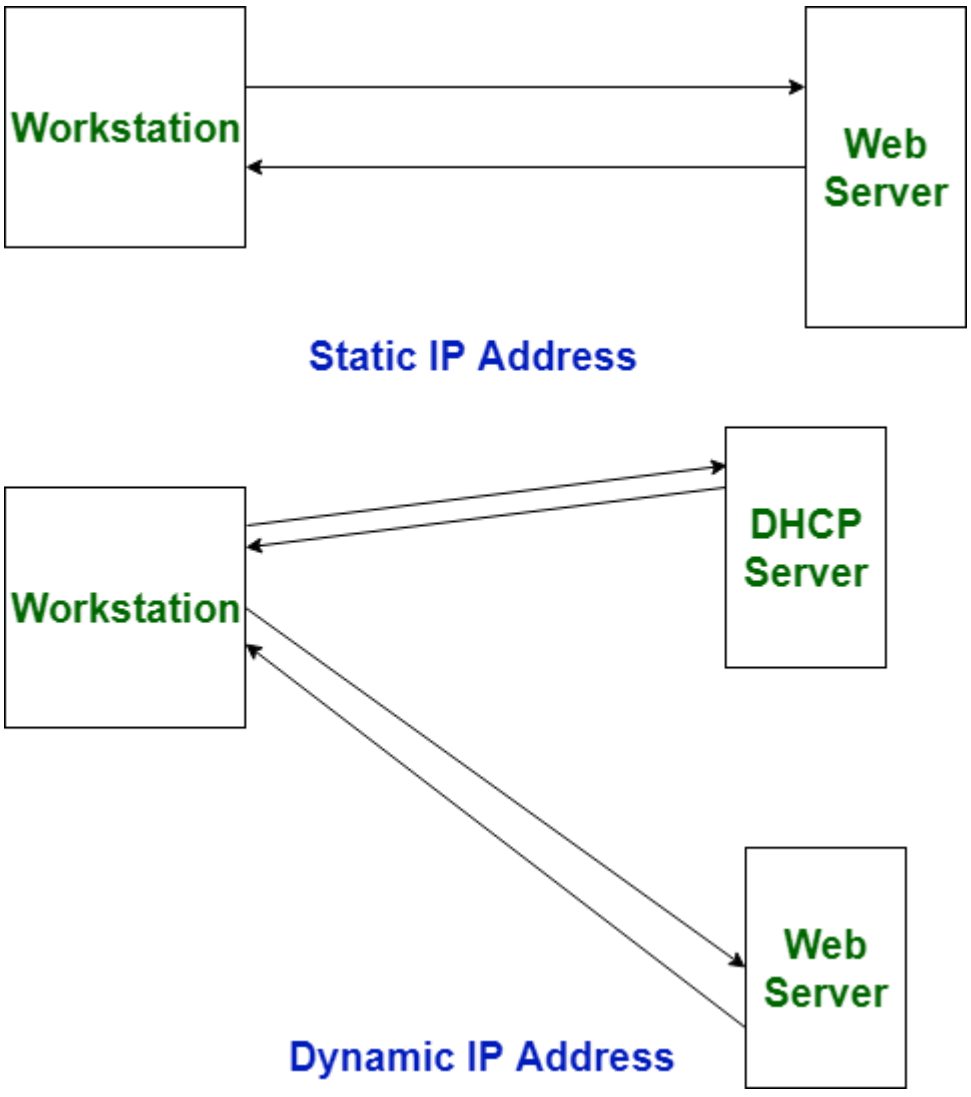
Q8 .Define Static IP and Dynamic IP? Discuss the difference between IPV4 and IPV6.

Ans

Difference between Static and Dynamic IP address

- Last Updated : 15 Jun, 2020

IP stands for **Internet Protocol**. IP address may be a distinctive numerical symbol allotted to every device on a network to spot each affiliation unambiguously.
The distinction between Static and Dynamic IP address lies inside the length of allotted scientific discipline address. The static scientific discipline address is fastened scientific discipline address that is manually allotted to a tool for a protracted amount of your time. On the opposite hand, the Dynamic scientific discipline address oft changes whenever user boots his/her machine, and it's mechanically allotted.



Difference between Static and Dynamic IP address:

S.NO	Static IP Address	Dynamic IP address

S.NO	Static IP Address	Dynamic IP address
1.	It is provided by ISP(Internet Service Provider).	While it is provided by DHCP (Dynamic Host Configuration Protocol).
2.	Static ip address does not change any time, it means if a static ip address is provided then it can't be changed or modified.	While dynamic ip address change any time.
3.	Static ip address is less secure.	While in dynamic ip address, there is low amount of risk than static ip address's risk.
4.	Static ip address is difficult to designate.	While dynamic ip address is easy to designate.
5.	The device designed by static ip address can be trace.	But the device designed by dynamic ip address can't be trace.
6.	Static ip address is more stable than dynamic ip address.	While dynamic ip address is less stable than static ip address.
7.	The cost to maintain the static ip address is higher than dynamic ip address.	While the maintaining cost of dynamic ip address is less than static ip address.
8.	It is used where computational data is less confidential.	While it is used where data is more confidential and needs more securit

9. Discuss TCP/IP model in detail.

Ans Introduction to the TCP/IP Model

The TCP/IP model is a part of the Internet Protocol Suite. This model acts as a communication protocol for computer networks and connects hosts on the Internet. It is a concise version of the OSI Model and comprises four layers in its structure.

This concept of TCP/IP is not just important for people in the computer or IT fields but also is an essential part of the Computer Knowledge syllabus, included in major competitive exams.

Before, diving deep into the different aspects of the structure, refer to the table below and know about some basic and introductory features of the model:

Basics of TCP/IP Model	
Full-Form	Transmission Control Protocol/ Internet Protocol
Developed By	Department of Defence (DoD), United States
Developed in	During the 1970s
Year for acknowledgement as a standard protocol by ARPANET	1983
Function of TCP	Collecting and Reassembling Data Packets
Function of IP	Sending the Data Packets to the correct destination
Number of Layers in TCP/IP Model	4 layers

In this article, we shall discuss in detail the different layers of the TCP/IP model along with their functions. Also, a few sample questions based on this topic have been given further below for the reference of Government exam aspirants.

To study in detail about what is a Computer Network and its different types, candidates can visit the linked article.

Interested in learning more about Computer-related terms, applications, and software??
Strengthen your Computer Awareness with the help of links given below:

- **Microsoft Windows**
- **High Level Computer Languages**
- **Input and Output Devices**
- **Web Browsers**
- **Database Management System (DBMS)**
- **Introduction to Operating System**

TCP/IP Notes PDF:-Download PDF Here

History and Development of TCP/IP Model

This protocol is a result of the research and development by the Defense Advanced Research Projects Agency (DARPA) during the 1960s. Given below are a few points which had played an important role in the advancement of the TCP/IP model:

- A two-network TCP/IP communications test was conducted between Stanford and University College London in 1975
- An important thing which resulted in promoting this model was when the US Department of Defense declared TCP/IP as the standard for all military computer networking. This was In March 1982
- In 1983, this structured protocol was adopted by ARPANET as a standard protocol
- Later on other Computer and IT companies including IBM, DEC, etc. had also adapted the TCP/IP model as their standard communication protocol
- In 1989, the University of California has accepted the TCP/IP code for public domain

Gradually, this Internet protocol suite or the TCP/IP model was accepted across the globe as a comprehensive framework for computer networking and Internet communication.

The TCP/IP model is considered to be similar to the Open Systems Interconnection Model. However, the framework and the structuring of the two was completely different and Transmission Control Protocol/ Internet Protocol was released prior to the OSI Model. For a detailed difference between the two, candidates can visit the Difference Between TCP/IP and OSI Model page.

Links to a few other fundamental topics and concepts have been given below for people to learn and understand one of the most complex, yet essential devices, which is the Computer:

Computer Abbreviations	Components of Computer
Computer Virus	Important Computer-related Terms
Microsoft Windows	Microsoft Office

Layers of the TCP/IP Model

Unlike the OSI model which comprises seven layers, the TCP/IP model is structured with four different layers. These four layers are:

1. Network Access Layer
2. Internet Layer
3. Host to Host Layer
4. Application Layer

Now, let us discuss each of these four layers in detail along with their functions as a part of the protocol architecture.

1. Network Access Layer

- This is the bottom-most layer of the TCP/IP model architecture
- It is a combination of the Data Link and Physical Layer of the OSI model

- The physical transmission of data takes place at this layer
- Once the frames are transmitted by a network, encapsulating the IP datagram into these frames is done in this layer
- Also, the mapping of IP address into physical address is done here
- Mainly, the function of this layer is to transmit the data between two devices, connected in a network

2. Internet Layer

- It is the second layer of the TCP/IP model and this layer is parallel to the Network Layer of the OSI Model, in terms of the structure
- Sending the data packets to their destination network is the main function of the Internet layer
- The logical transmission of data takes place at this level

10. What is a Web Browser (Browser)? Give some example of browsers.

Ans **Google Chrome**

Chrome, created by internet giant Google, is the most popular browser in the USA, perceived by its computer and smartphone users as fast, secure, and reliable. There are also many options for customization in the shape of useful extensions and apps that can be downloaded for free from the Chrome Store. Chrome also allows easy integration with other Google services, such as Gmail. Due to the success of the "Chrome" brand name, Google has now extended it to other products, for example, Chromebook, Chromebox, Chromecast, and Chrome OS.

2. Apple Safari

Safari is the default on Apple computers and phones, as well as other Apple devices. It's generally considered to be an efficient browser, its slick design being in keeping with the ethos of Apple. Originally developed for Macs, Safari has become a significant force in the mobile market due to the domination of iPhones and iPads. Unlike some of the other browsers listed, Safari is exclusive to Apple, it doesn't run on Android devices, and the Windows version of Safari is no longer supported by important security updates from Apple.

3. Microsoft Internet Explorer and Edge

Although it has been discontinued, Internet Explorer is worthy of mention as it was the go-to browser in the early days of the internet revolution, with usage share rising to 95% in 2003. However, its relatively slow start-up speed meant that many users turned to Chrome and Firefox in the years that followed. In 2015, Microsoft announced that Microsoft Edge would replace Internet Explorer as the default

browser on Windows 10, making Internet Explorer 11 the final version to be released. At the time of writing, the market share of Microsoft Edge remains lower than Internet Explorer, which is still used by many people around the world.

4. Mozilla Firefox

Unlike Chrome, Safari, Internet Explorer, and Microsoft Edge, Firefox is an open-source browser, created by community members of the Mozilla Foundation. It is perhaps the most customizable of the main browsers, with many add-ons and extensions to choose from. In late 2003, it had a usage share of 32.21% before gradually losing out to competition from Google Chrome. It currently remains a strong competitor in the "desktop" field but has a lower market share in the mobile arena, where Google Chrome and Apple Safari tend to dominate.

5. Opera

Another web browser worthy of mention is Opera, which is designed for Microsoft Windows, Android, iOS, macOS, and Linux operating systems. It has some interesting features and is generally considered to be a reliable option by many users. Many of its earlier features have gone on to be incorporated into rival browsers. It also has a distinct user interface. At the time of writing, Opera has a usage of just 2.28% but remains influential, albeit from the fringes.

Which Browser Am I Using Right Now?

If you don't know or are unsure which browser or version that you are using to view this article right now, there are a number of ways to find out.

Probably the easiest way is to use a website which tells you. I've listed examples of three below (click on a link to find out):

- What's My Browser
- WhatIsMyBrowser.com
- thismachine.info

  Another way to find out which browser you are using is through the browser itself. Browsers vary in their setup and layout, so it's impossible to give advice that works in every case. However, if you click on the browser's drop-down menu, usually found in the top right-hand corner of the page, then click on "help" and then "about," it will tell you which browser and version you are using in most cases.

This content is accurate and true to the best of the author’s knowledge and is not m

11. What is a search engine? Give example.

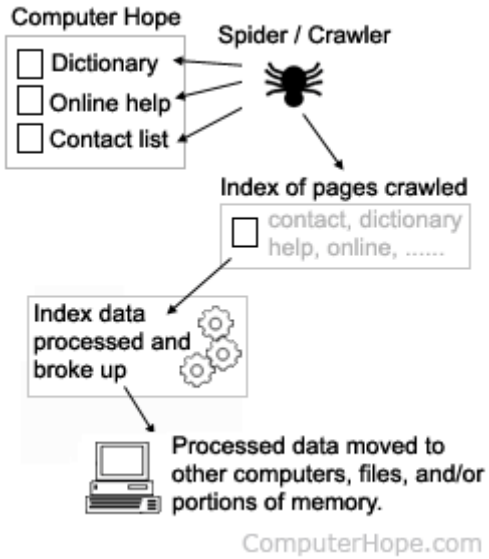
Ans **How to access a search engine**

For users, a search engine is accessed through a browser on their computer, smartphone, tablet, or another device. Today, most new browsers use an omnibox, which is a text box at the top of the browser. The omnibox allows users to type in a URL or a search query. You can also visit one of the major search engines' home page to perform a search.

- How to find information on the Internet.

How a search engine works

Because large search engines contain millions and sometimes billions of pages, many search engines display the results depending on their importance. This importance is commonly determined by using various algorithms.



As illustrated, the source of all search engine data is collected using a spider or crawler that visits each page on the Internet and collects its information.

Once a page is crawled, the data contained in the page is processed and indexed. Often, this can involve the steps below.

- Strip out stop words.
- Record the remaining words on the page and the frequency they occur.
- Record links to other pages.
- Record information about any images, audio, and embedded media on the page.

The data collected is used to rank each page. These rankings then determine which pages to show in the search results and in what order.

Finally, once the data is processed, it's broken up into files, inserted into a database, or loaded into memory where it's accessed when a search is performed.

Do all search engines give the same results?

Not necessarily. Search engines use proprietary algorithms to index and correlate data, so every search engine has

its own approach to finding what you're trying to find. Its results may be based on where you're located, what else you've searched for, and what results were preferred by other users searching for the same thing. Each search engine uniquely weights these and offers you different results.

What is the best search engine?

There isn't one search engine that is better than all the others. Many people could argue that Google's search engine is the best, and it is the most popular and well-known. It's so popular that people often use it as a verb when telling someone to search for their question.

Microsoft's Bing search engine is also popular and used by many people. Bing does an excellent job of finding information and answering questions. Bing is also what powers the search in Windows 10 and the Yahoo search engine.

Users concerned with privacy, enjoy using Duck Duck Go. This search engine makes its users anonymous and is an excellent solution for users concerned with how much information Google and Bing collect on its users.

12. What is the Internet & WWW? What are the uses of internet in our daily life?

Ans 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. 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.

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.

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

13. What is an Internet Service Provider? Give some example of ISP in India.

Ans **Mailbox providers**[edit]

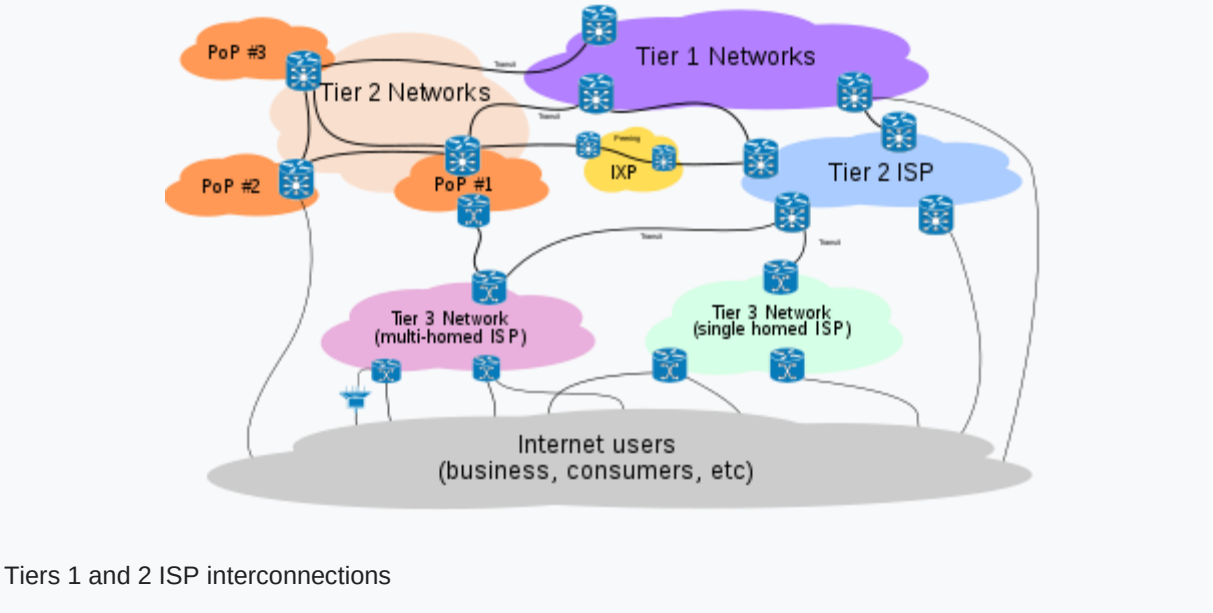
A mailbox provider is an organization that provides services for hosting electronic mail domains with access to storage for mail boxes. It provides email servers to send, receive, accept, and store email for end users or other organizations.

Many mailbox providers are also access providers,[44] while others are not (e.g., Gmail, Yahoo! Mail, Outlook.com, AOL Mail, Po box). The definition given in RFC 6650 covers email hosting services, as well as the relevant department of companies, universities, organizations, groups, and individuals that manage their mail servers themselves. The task is typically accomplished by implementing Simple Mail Transfer Protocol (SMTP) and possibly providing access to messages through Internet Message Access Protocol (IMAP), the Post Office Protocol, Webmail, or a proprietary protocol.[45]

Hosting ISPs[edit]

Internet hosting services provide email, web-hosting, or online storage services. Other services include virtual server, cloud services, or physical server operation.[46]

Transit ISPs[edit]



Tiers 1 and 2 ISP interconnections

Just as their customers pay them for Internet access, ISPs themselves pay upstream ISPs for Internet access. An upstream ISP usually has a larger network than the contracting ISP or is able to provide the contracting ISP with access to parts of the Internet the contracting ISP by itself has no access to.[47]

In the simplest case, a single connection is established to an upstream ISP and is used to transmit data to or from areas of the Internet beyond the home network; this mode of interconnection is often cascaded multiple times until reaching a tier 1 carrier. In reality, the situation is often more complex. ISPs with more than one point of presence (PoP) may have separate connections to an upstream ISP at multiple PoPs, or they may be customers of multiple upstream ISPs and may have connections to each one of them at one or more point of presence.[47] Transit ISPs provide large amounts of bandwidth for connecting hosting ISPs and access ISPs.[48]

Virtual ISPs[edit]

A virtual ISP (VISP) is an operation that purchases services from another ISP, sometimes called a *wholesale ISP* in this context,[49] which allow the VISP's customers to access the Internet using services and infrastructure owned and operated by the wholesale ISP. VISPs resemble mobile virtual network operators and competitive local exchange carriers for voice communications.

Free ISPs[edit]

Free ISPs are Internet service providers that provide service free of charge. Many free ISPs display advertisements while the user is connected; like commercial television, in a sense they are selling the user's attention to the advertiser. Other free ISPs, sometimes called freenets, are run on a nonprofit basis, usually with volunteer staff.[50]

Wireless ISP[edit]

A wireless Internet service provider (WISP) is an Internet service provider with a network based on wireless networking. Technology may include commonplace Wi-Fi wireless mesh networking, or proprietary equipment designed to operate over open 900 MHz, 2.4 GHz, 4.9, 5.2, 5.4, 5.7, and 5.8 GHz bands or licensed frequencies such as 2.5 GHz (EBS/BRS), 3.65 GHz (NN) and in the UHF band (including the MMDS frequency band) and LMDS.[51]

Peering[edit]

ISPs may engage in peering, where multiple ISPs interconnect at peering points or Internet exchange points (IXPs), allowing routing of data between each network, without charging one

another for the data transmitted—data that would otherwise have passed through a third upstream ISP, incurring charges from the upstream ISP.[47]

ISPs requiring no upstream and having only customers (end customers or peer ISPs) are called Tier 1 ISPs.

Network hardware, software and specifications, as well as the expertise of network management personnel are important in ensuring that data follows the most efficient route, and upstream connections work reliably. A tradeoff between cost a

14. Discuss the difference between MAC Ans Address

- Difficulty Level : Easy
- Last Updated : 23 Dec, 2020

Both MAC Address and IP Address are used to uniquely defines a device on the internet. NIC Card's Manufacturer provides the MAC Address, on the other hand Internet Service Provider provides IP Address.
The main difference between MAC and IP address is that, MAC Address is used to ensure the physical address of computer. It uniquely identifies the devices on a network. While IP address are used to uniquely identifies the connection of network with that device take part in a network.

Let's see the difference between MAC Address and IP Address:

S.NO	MAC Address	IP Address
1.	MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.
2.	MAC Address is a six byte hexadecimal address.	IP Address is either four byte (IPv4) or eight byte (IPv6) address.
3.	A device attached with MAC Address can retrieve by ARP protocol.	A device attached with IP Address can retrieve by RARP protocol.
4.	NIC Card's Manufacturer provides the MAC Address.	Internet Service Provider provides IP Address.
5.	MAC Address is used to ensure the physical address of computer.	IP Address is the logical address of the computer.
6.	MAC Address operates in the data link layer.	IP Address operates in the network layer.

7.	MAC Address helps in simply identifying the device.	IP Address identifies the connection of the device on the network.
8.	MAC Address of computer cannot be changed with time and environment.	IP Address modifies with the time and environment.
9.	MAC Address can't be found easily by third party.	IP Address can be foun

15. How do we view my Internet browser's history?

Ans

BrowsingHistoryView v2.46 - View browsing history of your Web browsers
Copyright (c) 2012 - 2021 Nir Sofer

1.7K

See Also

- ChromeCacheView - Cache viewer for Google Chrome Web browser

Description

BrowsingHistoryView is a utility that reads the history data of different Web browsers (Mozilla Firefox, Google Chrome, Internet Explorer, Microsoft Edge, Opera) and displays the browsing history of all these Web browsers in one table. The browsing history table includes the following information: Visited URL, Title, Visit Time, Visit Count, Web browser and User Profile. BrowsingHistoryView allows you to watch the browsing history of all user profiles in a running system, as well as to get the browsing history from external hard drive.
You can also export the browsing history into csv/tab-delimited/html/xml file from the user interface, or from command-line, without displaying any user interface.

Versions History

- Version 2.46:
  - Added support for Brave Web browser.
- Version 2.45:
  - Added 'Display QR Code' option (Under the View menu): When it's turned on, QR Code of the selected URL is displayed in the lower pane, and you can use QR Code Reader app on your Smartphone to instantly open the URL in the Web browser of your Smartphone.
- Version 2.41:
  - Fixed the /cfg command-line option to load the .cfg file from the current directory if full path is not specified.
- Version 2.40:
  - Added new date/time filter: 'Load history items from the following time range and date range (separately)'. For example... You can search browsing history items that their modified date is between 01/01/2019 - 01/01/2020 and their modified time is between 02:00 - 04:00.
- Version 2.36:
  - Added button on the toolbar to delete Chrome / Firefox history records.
- Version 2.35:
  - Added 'Delete Selected History Records' option (Ctrl+Delete), which allows you to delete individual history records of Chrome and Firefox Web browsers (Including Web browsers that use the same history database of Chrome/Firefox, like Waterfox, SeaMonkey, Vivaldi, and so on...)
  - Other Web browsers are not suported.
- Version 2.30:
  - Added new columns: 'History File' and 'Record ID'.
- Version 2.26:
  - Added 'Double-Click Action' option, which allows you to choose what to do when you double-click on history item - Open properties window or open the URL in Web browser.
- Version 2.25:
  - Added support for Waterfox Web browser.
- Version 2.21:
  - Added option to specify the time range in local time (Instead of GMT).
- Version 2.20:
  - BrowsingHistoryView now automatically detects the Chromium-based Edge Web browser.
- Version 2.17:
  - You can now specify environment variables in the history files of the 'Load history from the specified history files' option.
- Version 2.16:
  - Fixed to work with Firefox 61.0
- Version 2.15:

    - Added support for Pale Moon Web browser.
- Version 2.12:
    - Added new options to the 'Quick Filter' feature.
- Version 2.11:
    - The remote computer name ('Load history from remote computer' option) is now saved in the .cfg file. Also, you can set the remote computer from command-line with /ComputerName command-line option.
- Version 2.10:
    - Added new option: 'Automatically stop the cache task of IE10/IE11/Edge for unlocking the database file.' If this option is turned on - BrowsingHistoryView automatically stops the 'CacheTask' Scheduled task to unlock the database file of IE10/IE11/Edge (WebCacheV01.dat).
    - When you use the 'Load history from remote computer' option, BrowsingHistoryView will stop the 'CacheTask' Scheduled task on the remote computer, so you'll be able to view the history of IE10/IE11/Edge remotely.
- Version 2.05:
    - Added 'Load history from remote computer' option in 'Advanced Options' window. Be aware that this option works only when you have full admin access to the remote computer. Also, the history of IE10/IE11 is only available before the user logged-on to the system, because after the log-on the history database of IE10/IE11 is locked.
    - Fixed bug: 'Copy Selected Items' worked improperly when setting the 'Unicode/Ascii Save Mode' to 'Always UTF-8'.
- Version 2.00:
    - Added 'Visit Type' column for Chrome and Firefox Web browsers. (Link, Typed URL, Bookmark, and so on)
- Version 1.95:
    - Added 'Quick Filter' feature (View -> Use Quick Filter or Ctrl+Q). When it's turned on, you can type a string in the text-box added under the toolbar and BrowsingHistoryView will instantly filter the history table, showing only lines that contain the string you typed.
- Version 1.91:
    - Fix bug: When using /SaveDirect command-line option, the file was always saved according to the default encoding, instead of using the selected encoding in Options -> Save File Encoding.
- Version 1.90:
    - Added support for Vivaldi Web browser.
    - When 'Load history from the specified profiles folder' option is selected, the folders combo-box is filled with the profiles folders stored in shadow copies of your hard drive. When loading history from shadow copies, you may find history items older than what you can find in

your current system.

- Version 1.87:
  - Added secondary sorting support: You can now get a secondary sorting, by holding down the shift key while clicking the column header. Be aware that you only have to hold down the shift key when clicking the second/third/fourth column. To sort the first column you should not hold down the Shift key.
  - Fixed bug: BrowsingHistoryView crashed when using the find option while the last item was selected.
- Version 1.86:
  - You can now choose the desired encoding (ANSI, UTF-8, UTF-16) to save the csv/xml/text/html files. (Under the Options menu)
- Version 1.85:
  - Added new option to the 'Advanced Options' window: Load only URLs contain one of the specified strings (comma-delimited list).
  - Added new option to the 'Advanced Options' window: Don't load URLs that contain one of the specified strings (comma-delimited list).
- Version 1.81:
  - The 'Web Browser' column now displays 'Internet Explorer 10/11 / Edge' for items of IE10/IE11/Edge (In previous versions it displayed 'Internet Explorer 10')
- Version 1.80:
  - Added support for Yandex Web browser.
- Version 1.77:
  - The properties window is now larger and resizable.
- Version 1.76:
  - Added option to skip duplicate URLs that their visit time difference is less than xx seconds. (In 'Advanced Options' window) Sometimes, A web browser may record a Web page visit multiple times with a difference of a few seconds, even when the Web page was visited only once. This option allows you to hide these duplicate history records.
- Version 1.75:
  - Added support for Microsoft Edge/Project Spartan (On Windows 10).
  - Fixed issue: When Internet Explorer 10/11 was opened by multiple users, BrowsingHistoryView displayed all history records of IE 10/11 multiple times.
- Version 1.71:
  - Fixed issue: When loading large amount of history items, some actions, like selecting items and copying selected items to the clipboard were very slow.
- Version 1.70:
  - Added 'Typed Count' column (Only relevant to Chrome Web browser).
- Version 1.69:

    - Fixed issue: On some systems, BrowsingHistoryView failed to read the history of IE10/IE11 from WebCacheV01.dat
- Version 1.68:
    - BrowsingHistoryView now detects the portable version of Firefox if it's running in the background.
- Version 1.67:
    - Added 'URL Length' column.
- Version 1.66:
    - Added 'Load history items from the last xx minutes' to the 'Advanced Options' window.
    - Fixed bug: BrowsingHistoryView failed to remember the last size/position of the main window if it was not located in the primary monitor.
- Version 1.65:
    - Added support for Opera (Version 15 or later).
- Version 1.60:
    - Added 'Browser Profile' column, which displays the folder name of the Web browser profile (For Firefox and Chrome Web browsers).
- Version 1.55:
    - Added 'Save Configuration To File' and 'Load Configuration From File' options.
- Version 1.52:
    - Fixed bug: When getting history information from a remote computer and both local computer and remote computer have IE10 or IE11, BrowsingHistoryView displayed the IE10/IE11 history of the local computer... (Be aware that BrowsingHistoryView cannot display the IE10/IE11 history of a remote computer while the WebCacheV01.dat file on the remote computer is locked)
- Version 1.51:
    - Fixed to find the correct item when typing the string you want to search into the main List View.
- Version 1.50:
    - Added 'Load history from the specified history files' option in the 'Advanced Options' window.
- Version 1.44:
    - Fixed bug from v1.43: BrowsingHistoryView stopped working on Windows 2000.
- Version 1.43:
    - Fixed to display date/time values according to daylight saving time settings.
- Version 1.42:
    - Added /cfg command-line option, which instructs BrowsingHistoryView to use a config file in another location instead if the default config file, for example: BrowsingHistoryView.exe /cfg "%AppData%\BrowsingHistoryView.cfg"
- Version 1.41

    - Fixed a bug with displaying IDN URLs (URLs containing non-English characters) from Firefox history.
- Version 1.40
    - Added new data source in the 'Advanced Options' window: Load history from the specified custom folders. In this option, you can select the correct AppData folder, Local AppData folder, and the History folder of the profile you want to inspect.
- Version 1.36
    - Fixed the problem with the 'Advanced Options' window on Windows 2000.
- Version 1.35
    - Added 'Show Advanced Options On Start' option. You can turn off this option if you don't want that the 'Advanced Options' window will appear on every time that you run BrowsingHistoryView.
- Version 1.33
    - Improved the detection of AppData and Local AppData folders when reading the history from external drive.
- Version 1.32
    - Added secondary sorting: When clicking the 'Web Browser' column header, the list is sorted by the 'Web Browser' column, and then by the 'Visit Time' column.
- Version 1.31
    - Added option to get the history from Internet Explorer API, instead of reading the file directly. (Available only when loading the history of the current user).
- Version 1.30
    - Added improved support for Internet Explorer 10, which works smoothly and doesn't require to run BrowsingHistoryView as administrator. There is no need to execute BrowsingHistoryView with any additinal command-line option in order to read the locked file of IE10 (WebCacheV24.dat or WebCacheV01.dat), and the /UseVolumeShadowCopy command-line option added on v1.15 was removed from this version.
      Be aware that during browsing on IE10, you may get corrupted history result, because the database is not fully flushed to the disk.
      Also, be aware that BrowsingHistoryView cannot read a locked IE10 file on a remote network system.
- Version 1.27
    - Fixed bug: BrowsingHistoryView failed to load Firefox profile located on a drive letter which is different from the drive letter where the Windows profiles (c:\users ...) are located.
    - Fixed the flickering appeared while scrolling the history items.
- Version 1.26
    - Fixed bug: When exporting browser history data with /SaveDirect command-line option, BrowsingHistoryView

added byte order mark of Unicode, while the file was saved as Ascii.

- Version 1.25
  - BrowsingHistoryView now reads the history of all profiles from Chrome and Chrome Canary Web browsers.
- Version 1.21
  - Fixed bug: BrowsingHistoryView displayed corrupted URLs from partially deleted records of Internet Explorer history file.
- Version 1.20
  - Added support for Chrome Canary and SeaMonkey Web browsers.
  - Added 'Mark Odd/Even Rows' option, under the View menu. When it's turned on, the odd and even rows are displayed in different color, to make it easier to read a single line.
- Version 1.16
  - Fixed bug: BrowsingHistoryView failed to read some of the history items of Internet Explorer 10.
- Version 1.15
  - Added support for Internet Explorer 10 (WebCacheV24.dat or WebCacheV01.dat). There are some limitations and problems with this version of Internet Explorer. See the 'Internet Explorer 10 Support' section for more information.
- Version 1.10
  - Added 'Visited From' column (Only for Firefox and Chrome), which displays the URL that the user has visited prior to the Web page specified under the URL column.
- Version 1.06
  - Fixed BrowsingHistoryView to display the Web page title for Internet Explorer Web browser.
- Version 1.05
  - Added 'Copy URLs' option (Ctrl+U)
  - Added 'Open URL In Web Browser' option.
- Version 1.01
  - BrowsingHistoryView now reads the profiles.ini file of Firefox to get the correct profile folders.
- Version 1.00 - First release.

System Requirements

This utility works on any version of Windows, starting from Windows 2000, and up to Windows 10. Both 32-bit and x64 systems are supported.

The following Web browsers are supported:

- Internet Explorer (Version 4.00 and greater)
- Mozilla Firefox (Version 3.00 and greater)

- Microsoft Edge
- Google Chrome
- Safari
- Opera (Version 15 or later, which is based on Chrome Web browser)

Known Limitations and Problems

- 'Visit Count' on Internet Explorer Web browser: The 'Visit Count' column is taken "as is" from the history file of Internet Explorer. Unfortunately, Internet Explorer tend to extremely bloat the 'Visit Count' number, which means that you cannot assume that the 'Visit Count' number represents the actual number of times that the user visited the specified Web site. This remark is only relevant for Internet Explorer. Other Web browsers count the number of visits properly, as far as I know.
- Limitations and problems with reading the history of IE10, IE11 and Microsoft Edge: Version 10 and 11 of Internet Explorer stores the history data inside WebCacheV01.dat, and this file is locked by the operating system most of the time, even when IE is closed.
  In order to unlock the history database file, you should turn on the 'Automatically stop the cache task of IE10/IE11/Edge' option. If you use the 'Load history from remote computer' option - BrowsingHistoryView will stop the cache task of IE10/IE11/Edge on the specified remote system, so you'll be able to see the history of IE10/IE11/Edge remotely.

Start Using BrowsingHistoryView

BrowsingHistoryView doesn't require any installation process or additional dll files. In order to start using it, simply run the executable file - BrowsingHistoryView.exe

After you run BrowsingHistoryView, the 'Advanced Options' window is displayed. By default, BrowsingHistoryView offers you to load the history of all Web browsers and all user profiles in the last 10 days, but you can change the options according to your needs.

After pressing 'Ok' in the 'Advanced Options' window, BrowsingHistoryView loads and displays the browsing history according to the options you chose.

The 'Advanced Options' Window

- **Filter by visit date/time:** Allows you to load the history from the last number of days/hours, or from specific date/time range.
- **Web Browsers:** BrowsingHistoryView will load the history only from the selected Web browsers. For example, if you want to

only get the browsing history of Internet Explorer, then you need to select the 'Internet Explorer' check-box and deselect all others.

- **Load history from:** Allows you to choose the data source of the browsing history:
    - **Load history from the current running system (All users):** If you choose this option, BrowsingHistoryView scans all the user profiles on your system (C:\Documents and Settings or C:\Users) and loads the history data from them.
      Be aware that the Registry file of every user profile (NTUSER.DAT) should be readable, because BrowsingHistoryView uses the Registry file to locate the correct history file/folder of every Web browser. If BrowsingHistoryView cannot read NTUSER.DAT, it'll try to locate the correct folders in other less reliable ways.
    - **Load history from the current running system (Only current user):** If you choose this option, BrowsingHistoryView loads only the browsing history of the current logged-on user.
    - **Load history from the specified profiles folder:** If you choose this option, BrowsingHistoryView scans all the user profiles under the specified folder. The specified folder should be something like H:\Documents and Settings (On Windows XP) or H:\Users (On Windows 7/2008/Vista/8).
      Be aware that the Registry file of every user profile (NTUSER.DAT) should be readable, because BrowsingHistoryView uses the Registry file to locate the correct history file/folder of every Web browser. If BrowsingHistoryView cannot read NTUSER.DAT, it'll try to locate the correct folders in other less reliable ways.
    - **Load history from the specified profile:** If you choose this option, BrowsingHistoryView loads the history from the specified profile folder. The specified profile folder should be something like H:\Documents and Settings\Administrator (On Windows XP) or H:\Users\Administrator (On Windows 7/2008/Vista/8).
    - **Load history from the specified custom folders:** If you choose this option, you should specify the following folders of the user profile you want to load: History (e.g: C:\Users\user01\AppData\Local\Microsoft\Windows\History), App Data (e.g: C:\Users\user01\AppData\Roaming), Local App Data (e.g: C:\Users\user01\AppData\Local)
    - **Load history from the specified history files:** If you choose this option, you have to specify the history file of every Web browser that you want to load.

- **Load history from remote computer:** Allows you to load the browsing history from remote computer on your network. Be aware that this option works only when you have full admin access to the remote computer. If you want to view the history of IE10/IE11/Edge Web browser, you have to turn on the following option: 'Automatically stop the cache task of IE10/IE11/Edge for unlocking the database file.'

Reading Older History From Shadow Copies

If your hard drive has one or more shadow copies, you can view the history stored inside these shadow copies by selecting the 'Load history from the specified profiles folder' option in the 'Advanced Options' window and then choosing the desired shadow copy path (I'll be something like '\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\users') from the path combo-box.