Certificate in Computer Applications (CCA)

CCA-102: Data Communications

ASSIGNMENT

Q. 1. What are the different types of networks?

Ans: - 11 Types of Networks in Use Today –

1. Personal Area Network (PAN)

The smallest and most basic type of network, a PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building. These types of networks are typically found in small offices or residences, and are managed by one person or organization from a single device.

2. Local Area Network (LAN)

We're confident that you've heard of these types of networks before – LANs are the most frequently discussed networks, one of the most common, one of the most original and one of the simplest types of networks. LANs connect groups of computers and low-voltage devices together across short distances (within a building or between a group of two or three buildings in close proximity to each other) to share information and resources. Enterprises typically manage and maintain LANs.

Using routers, LANs can connect to wide area networks (WANs, explained below) to rapidly and safely transfer data.

3. Wireless Local Area Network (WLAN)

Functioning like a LAN, WLANs make use of wireless network technology, such as Wi-Fi. Typically seen in the same types of applications as LANs, these types of networks don't require that devices rely on physical cables to connect to the network.

4. Campus Area Network (CAN)

Larger than LANs, but smaller than metropolitan area networks (MANs, explained below), these types of networks are typically seen in universities, large K-12 school districts or small businesses. They can be spread across several buildings that are fairly close to each other so users can share resources.

5. Metropolitan Area Network (MAN)

These types of networks are larger than LANs but smaller than WANs – and incorporate elements from both types of networks. MANs span an entire geographic area (typically a town or city, but sometimes a campus). Ownership and maintenance is handled by either a single person or company (a local council, a large company, etc.).

6. Wide Area Network (WAN)

Slightly more complex than a LAN, a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when they're miles apart.

The Internet is the most basic example of a WAN, connecting all computers together around the world. Because of a WAN's vast reach, it is typically owned and maintained by multiple administrators or the public.

7. Storage-Area Network (SAN)

As a dedicated high-speed network that connects shared pools of storage devices to several servers, these types of networks don't rely on a LAN or WAN. Instead, they move storage resources away from the network and place them into their own high-performance network. SANs can be accessed in the same fashion as a drive attached to a server. Types of storage-area networks include converged, virtual and unified SANs.

8. System-Area Network (also known as SAN)

This term is fairly new within the past two decades. It is used to explain a relatively local network that is designed to provide high-speed connection in server-to-server applications (cluster environments), storage area networks (called "SANs" as well) and processor-to-processor applications. The computers connected on a SAN operate as a single system at very high speeds.

9. Passive Optical Local Area Network (POLAN)

As an alternative to traditional switch-based Ethernet LANs, POLAN technology can be integrated into structured cabling to overcome concerns about supporting traditional Ethernet protocols and network applications such as PoE (Power over Ethernet). A point-to-multipoint LAN architecture, POLAN uses optical splitters to split an optical signal from one strand of single mode optical fibre into multiple signals to serve users and devices.

10. Enterprise Private Network (EPN)

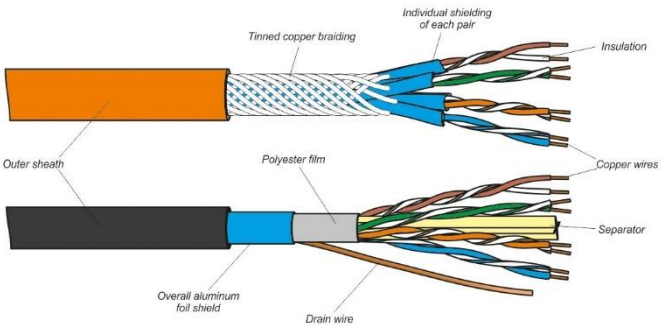
These types of networks are built and owned by businesses that want to securely connect its various locations to share computer resources.

11. Virtual Private Network (VPN)

By extending a private network across the Internet, a VPN lets its users send and receive data as if their devices were connected to the private network – even if they're not. Through a virtual point-to-point connection, users can access a private network remotely.

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

Ans – TWISTED PAIR (STP) –

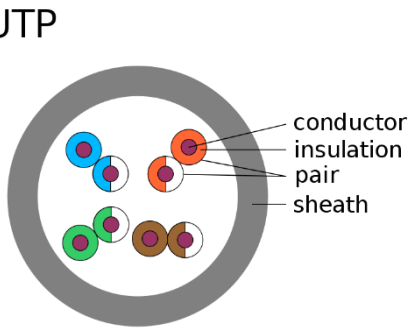


A twisted pair can be used as a balanced line, which as part of a balanced circuit can greatly reduce the effect of noise currents induced on the line by coupling of electric or magnetic fields. The idea is that the currents induced in each of the two wires are very nearly equal. The twisting ensures that the two wires are on average the same distance from the interfering source and are affected equally. The noise thus produces a common-mode signal which can be cancelled at the receiver by detecting the difference signal only, the latter being the wanted signal.

Common-mode rejection starts to fail on untwisted wires when the noise source is close to the signal wires; the closer wire will couple with the noise more strongly and the receiver will be unable to eliminate it. This problem is especially apparent in telecommunication cables where pairs in the same cable lie next to each other for many miles. Twisting the pairs counters this effect as on each half twist the wire nearest to the noise-source is exchanged. Provided the interfering source remains uniform, or nearly so, over the distance of a single twist, the induced noise will remain common-mode.

The twist rate (also called pitch of the twist, usually defined in twists per metre) makes up part of the specification for a given type of cable. When nearby pairs have equal twist rates, the same conductors of the different pairs may repeatedly lie next to each other, partially undoing the benefits of twisting. For this reason, it is commonly specified that, at least for cables containing small numbers of pairs, the twist rates must differ.

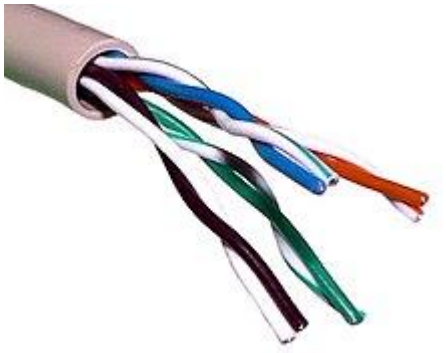
UNSHIELDED TWISTED PAIR (UTP) –



Unshielded twisted pair (UTP) cables are found in many Ethernet networks and telephone systems. For indoor telephone applications, UTP is often grouped into sets of 25 pairs according to a standard 25-pair colour code originally developed by AT&T Corporation. A typical subset of these colours (white/blue, blue/white, white/orange, orange/white) shows up in most UTP cables. The cables are typically made with copper wires measured at 22 or 24 American Wire Gauge (AWG),[5] with the coloured insulation typically made from an insulator such as polyethylene or FEP and the total package covered in a polyethylene jacket.

For urban outdoor telephone cables containing hundreds or thousands of pairs, the cable is divided into small but identical bundles. Each bundle consists of

twisted pairs that have different twist rates, as pairs having the same twist rate within the cable can still experience some degree of crosstalk. The bundles are in turn twisted together to make up the cable.



UTP is also the most common cable used in computer networking. Modern Ethernet, the most common data networking standard, can use UTP cables. Twisted-pair cabling is often used in data networks for short and medium-length connections because of its relatively lower costs compared to optical fibre and coaxial cable.

As UTP cable bandwidth has improved to match the baseband of television signals, UTP is now used in some video applications, primarily in security cameras.

Q. 3. What is difference between baseband and broadband transmission?

Ans – **Difference between baseband and broadband transmission –**

S.No.	Broadband Transmission	Baseband Transmission
1.	In broadband transmission, the type of signalling used is digital.	In baseband transmission, the type of signalling used is analog.
2.	Baseband Transmission is bidirectional in nature.	Baseband 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 broadband transmission, Manchester and Differential Manchester encoding are used.	Only PSK encoding is used.

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

Ans –

Device	What is does
Hubs:	Unlike switches, hubs broadcast data to all ports, which is inefficient, so hubs are basically a multiport repeater.
Modem:	Stands for "modulating-demodulating": modems are hardware devices that allow a computer or another device, such as a router or switch, to connect to the Internet. They convert or "modulate" an analogue signal from a telephone or cable wire to digital data (1s and 0s) that a computer can recognize. Simply send traffic from point A to point B without further manipulation.
Routers:	Are responsible for sending data from one network to another. Work at Layer 3 (Network) of the OSI model, which deals with IP addresses. Typically, routers today will perform the functionality of both a router and a switch - that is, the router will have multiple ethernet ports that devices can plug into.
Switches:	They use the MAC address of a device to send data only to the port the destination device is plugged into. Work at Layer 2 (Data Link) of the OSI model, which deals with MAC addresses.

Q. 5. When you move the NIC cards from one PC to another PC, does the MAC address gets transferred as well?

Ans – 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.

Q. 6. When troubleshooting computer network problems, what common hardware-related problems can occur?

Ans – 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 start-ups. Incorrect hardware configuration is also one of those culprits to look into.

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

Ans – The best solution is to install anti-virus on all the computers in the network. This will protect each device from the other in case some malicious user tries to insert a virus into the servers or legitimate users.

Q. 8. Define Static IP and Dynamic IP? Discuss the difference between IPV4 and IPV6.

Ans – When a device is assigned a static IP address, the address does not change. Most devices use dynamic IP addresses, which are assigned by the network when they connect and change over time.

Dynamic IP address –

Use advanced settings for your network to configure dynamic DNS. When your IP address changes, the DNS entry for your server is automatically updated with its new IP address, so outside users can use the same domain name. You can choose the Dynamic DNS provider and don't have to install additional software on your computer.

Static IP address –

Use advanced settings to reserve an IP address for a device on your local network. Your device keeps the same IP address until you cancel the reservation or remove the device from your network, even if the device is disconnected.

Difference between IPV4 and IPV6 –

Basis for differences	IPv4	IPv6
Size of IP address	IPv4 is a 32-Bit IP Addres s.	IPv6 is 128 Bit IP Address.
Addressing method	IPv4 is a numeric address , and its binary bits are se parated by a dot (.)	IPv6 is an alphanumeric a ddress whose binary bits are separated by a colon (:). It also contains hexad ecimal.
Number of header fields	12	8
Length of header filed	20	40
Checksum	Has checksum fields	Does not have checksum fields
Example	12.244.233.165	2001:0db8:0000:0000:00 00:ff00:0042:7879
Type of Addresses	Unicast, broadcast, and multicast.	Unicast, multicast, and a nycast.
Number of classes	IPv4 offers five different classes of IP Address. Cla ss A to E.	lPv6 allows storing an unl imited number of IP Addr ess.
Configuration	You have to configure a n ewly installed system bef ore it can communicate with other systems.	In IPv6, the configuration is optional, depending up on on functions needed.
VLSM support	IPv4 support VLSM (Virtu al Length Subnet Mask).	IPv6 does not offer supp ort for VLSM.
Fragmentation	Fragmentation is done by sending and forwarding r outes.	Fragmentation is done by the sender.
Routing Information Pro tocol (RIP)	RIP is a routing protocol s upported by the routed d aemon.	RIP does not support IPv 6. It uses static routes.

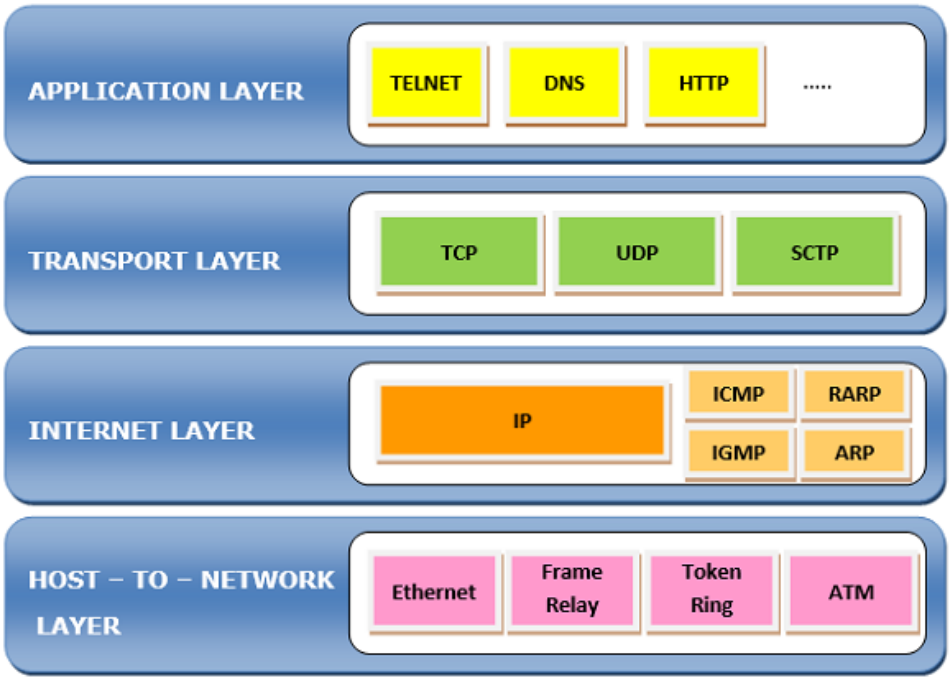
Q. 9. Discuss TCP/IP model in detail.

Ans – 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–



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

Ans – Web browser –

A web browser (commonly referred to as a browser) is a software application for accessing information on the World Wide Web. When a user requests a web page from a particular website, the web browser retrieves the necessary content from a web server and then displays the page on the user's device.

A web browser is not the same thing as a search engine, though the two are often confused. For a user, a search engine is just a website that provides links to other websites. However, to connect to a website's server and display its web pages, a user must have a web browser installed.

Web browsers are used on a range of devices, including desktops, laptops, tablets, and smartphones. In 2020, an estimated 4.9 billion people use a browser, with more than half of them in Asia. The most used browser is Google Chrome, with a 66% global market share on all devices, followed by Safari with 17%. Other notable browsers include Firefox and Microsoft Edge.

Web browsers –

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Internet Explorer
- Safari
- QQ browser
- Sogou Explorer
- Opera
- Yandex Browser
- UC Browser

Q.11. What is a search engine? Give example.

Ans – Search Engine –

A search engine is a software system that is designed to carry out web searches (Internet searches), which means to search the World Wide Web in a systematic way for particular information specified in a textual web search query. The search results are generally presented in a line of results, often referred to as search engine results pages (SERPs) The information may be a mix of links to web pages, images, videos, infographics, articles, research papers, and other types of files. Some search engines also mine data available in databases or open directories. Unlike web directories, which are maintained only by human editors, search engines also maintain real-time information by running an algorithm on a web crawler. Internet content that is not capable of being searched by a web search engine is generally described as the deep web.

- Ask.com
- Baidu
- Dogpile
- DuckDuckGo
- Ecosia
- Exalead
- Excite
- Gigablast
- Google Search
- HotBot
- Lycos
- MetaCrawler
- Microsoft Bing
- Mojeek
- Qwant
- Searx
- Sogou
- Soso
- Startpage.com
- Swisscows
- WebCrawler
- Yahoo! Search

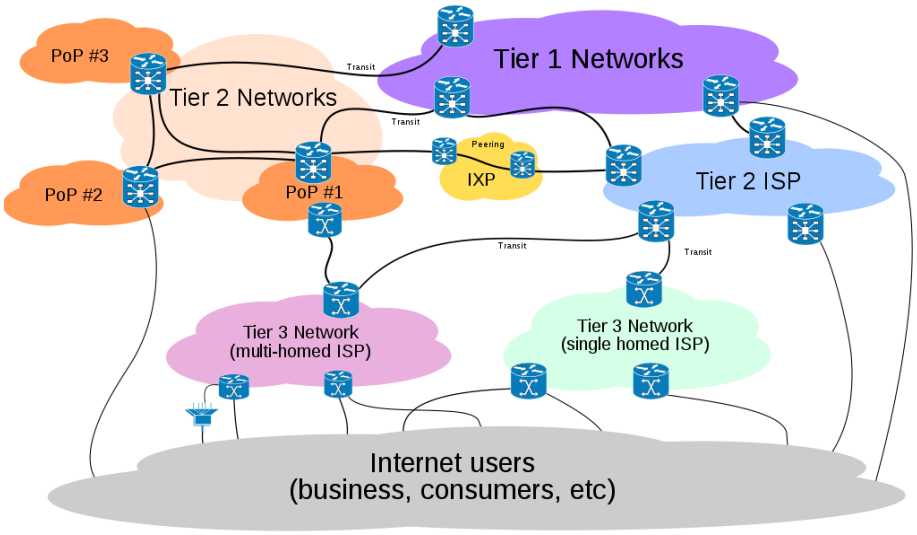
Q. 12. What is the Internet & WWW? What are the uses of internet in our daily life?

Ans – Differences between WWW and Internet –

WWW (World Wide Web)	Internet
The World Wide Web is the common system for navigating the internet. It is not the only system that can be used for such access, but it is by far the most common one.	The internet is a public network of network with a maze of wired and wireless connections between separate groups of servers' computers and countless devices from around the world
The World Wide Web is distinguished from other systems through its use of HTTP (Hypertext Transfer Protocol). It can be safely said that the HTTP is the language of the World Wide Web	Along with Internets, there also exist the Intranets, which is the same type of information network but more privatized in order to control access.
WWW is more software-oriented as compared to the Internet	Internet is primarily hardware-based.
The HTTP along with being the language of the World Wide Web also governs it by dealing with linking of files, documents and other resources	The internet is governed by a set of rules and regulations collectively known as Internet Protocol (IP). The IP deals with data transmitted through the internet.
The invention of the World Wide Web can be credited to Sir Tim Berners Lee. During his work at the European Organization for Nuclear Research in 1989, he had developed the basic idea of the WWW to merge the evolving technologies of computers, data networks and hypertext into a powerful and easy to use global information system.	The first workable prototype of the Internet was the ARPANET (Advanced Research Project Agency Network) in the late 1960s. After its adoption on January 1st 1983, researchers began to develop a "network of networks" which evolved into the modern form of the Internet

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

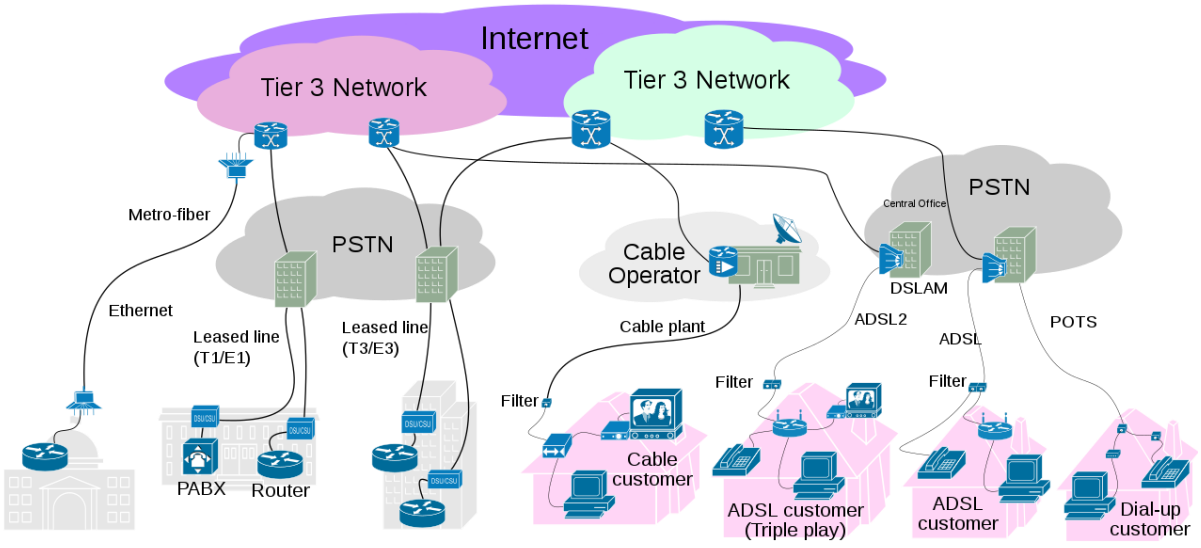
Ans – Internet Service Provider (ISP) –



An **Internet service provider (ISP)** 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.

Internet services typically provided by ISPs can include Internet access, Internet transit, domain name registration, web hosting, Usenet service, and colocation.

An ISP typically serves as the access point or the gateway that provides a user, access to everything available on the Internet.



List of internet service providers in India –

This is a list of **internet service providers in India.** There were 358 Internet Service Providers (ISPs) offering broadband and narrow band internet services in India as of 31 December 2019.

By subscribers –

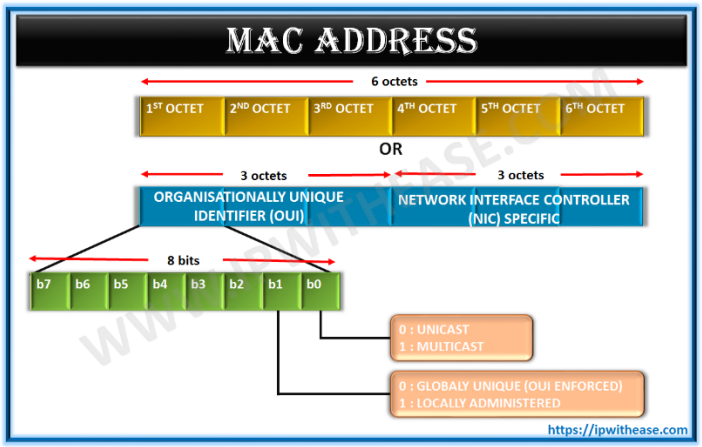
The following table shows the top 10 ISPs in India by total subscriber base as of 31 March 2020. Broadband is defined as "an always-on Internet connection with download speed of 512 kbit/s or above." The number of internet users is 743.19 million, out of which 55.75 million are narrow band subscribers and 687.44 million are broadband subscribers.

Rank	ISP	Narrowband	Broadband	Total
1	Reliance Jio	0	388,390,116	388,390,116
2	Airtel	27,111,012	148,569,937	175,680,949
3	Vodafone Idea	22,019,406	117,451,416	139,470,822
4	BSNL	6,400,380	24,507,496	30,907,876
5	ACT Fibernet	0	1,607,015	1,607,015
6	APSFL	0	970,270	970,270
7	MTNL	170,697	855,744	1,026,441
8	Hathway	0	969,157	969,157
9	You Broadband	14,660	778,584	793,244
10	GTPL Broadband	0	359,347	359,347
11	Excitel	0	350,783	350,783

Q. 14. Discuss the difference between MAC address, IP address and Port address.

Ans – MAC (Media Access Control) Address –

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. MAC address is a unique identifier that is assigned to a NIC (Network Interface Controller/ Card). It consists of a 48 bit or 64-bit address, which is associated with the network adapter. MAC address can be in hexadecimal format. The full form of MAC address is Media Access Control address. A MAC address is generally in six sets of two-digits/characters that are separated by colons.



IP (Internet Protocol) Address –

An IP address is used for communication within the local area network and for communication between networks (usually through the Internet). An IP address is an address that helps you to identify a network connection. It is termed as the 'Logical Address,' which is provided to a connection in a network.

IP address helps you to control how devices on the Internet communicate and defines the behavior of internet routers.

IP controls how devices on the internet communicate and defines the behavior of internet routers. It corresponds to Layer 3, the network layer, of the OSI reference model. The internet was initially built around IP version 4 (IPv4) and is in transition to IPv6.

An IP address identifies a device on the global internet. An IPv4 address consists of 32 bits, usually written as four decimal numbers, or a dotted quad. Possible values range from 000.000.000.000 through 255.255.255.255, although many possible addresses are disallowed or reserved for specific purposes.

IP address classes (pre 1993 mindset)

Class A	1.0.0.1 to 126.255.255.254	16M hosts 127 networks
Class B	128.1.0.1 to 191.255.255.254	64K hosts 16K networks
Class C	192.0.1.1 to 223.255.254.254	254 hosts 2M networks
Class D	224.0.0.0 to 239.255.255.255	Multicast
Class E	240.0.0.0 to 254.255.255.254	R&D == wasted

Port Numbers –

Port numbers are used as part of IP communications to determine which program the communication is to or from. Ports are represented by 16-bit numbers. Hence ports range from 0-65,525. The port numbers from 0 -1023 are restricted because they are reserved for the use of well-known protocol services such as HTTP and FTP. In a network, the endpoint, which two hosts communicate with each other are identified as ports.

Port Number(s)	Protocol	Application	access-list Command Keyword
20	TCP	FTP data	ftp-data
21	TCP	FTP control	ftp
22	TCP	SSH	—
23	TCP	Telnet	telnet
25	TCP	SMTP	smtp
53	UDP, TCP	DNS	domain
67, 68	UDP	DHCP	nameserver
69	UDP	TFTP	tftp
80	TCP	HTTP (WWW)	www
110	TCP	POP3	pop3
161	UDP	SNMP	snmp
443	TCP	SSL	—
16,384 – 32,767	UDP	RTP-based voice (VoIP) and video	—

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

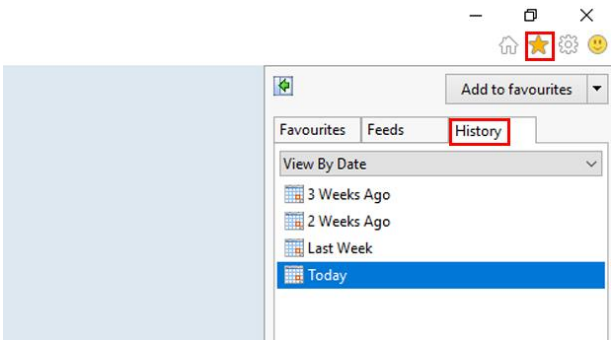
Ans – How to find your web history –

Finding a particular web page long after you last visited it can be a tricky business unless you bookmarked it or can track it down with a search engine.

Fortunately, all web browsers keep a record of every page you visit in their 'web history' - all you need to know is how to access it. We'll show you where to look on Google Chrome, Internet Explorer, Firefox and Microsoft Edge. Sometimes it's not so fortunate, so we'll show you how to delete it, too.

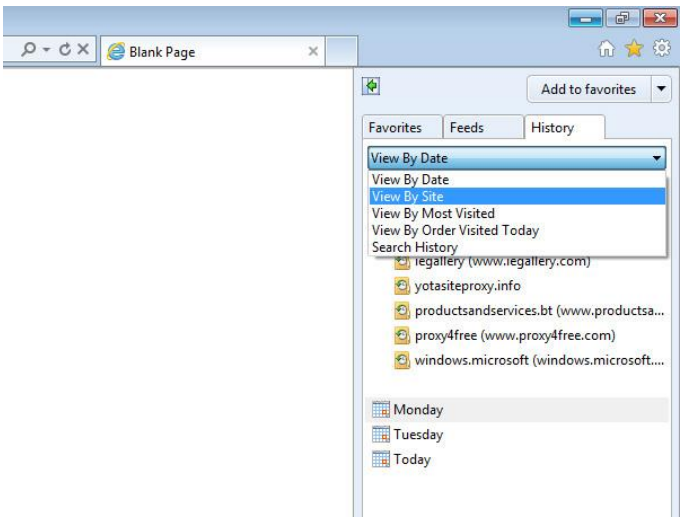
<u>View and delete in Internet Explorer –</u>

Step 1: Open the History menu



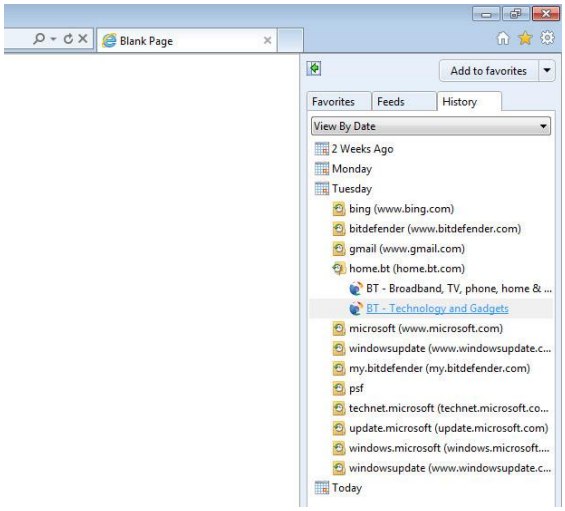
In Internet Explorer 11, click the **star** icon at the top-right of the window.

Step 2: Search and sort Internet Explorer History



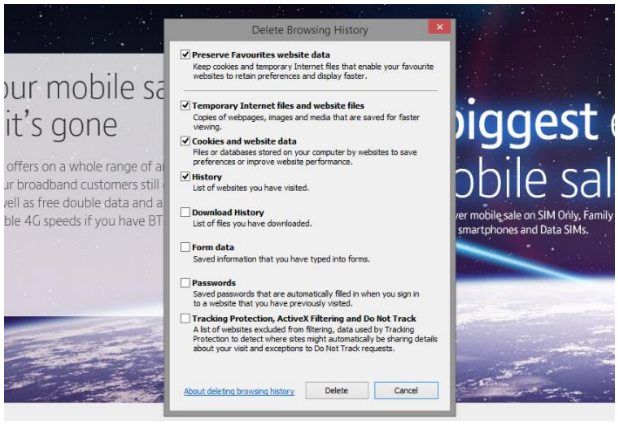
When the dialog box opens, click the **History** tab to view the web pages you've visited previously, ordered by date. There's also a drop-down list so you can view the pages by **Site, Name, Most Visited** and **Order Visited Today**, plus a **Search History** option for when it's quicker to find a page by name.

Step 3: Open a page



Clicking a day or a site in the list expands it and then you can click an individual page to open it in the current tab.

Step 4: Delete your History



To clear the browser history in Internet Explorer, click the **cog** icon at the top-right of the Internet Explorer window and select **Internet Options.**

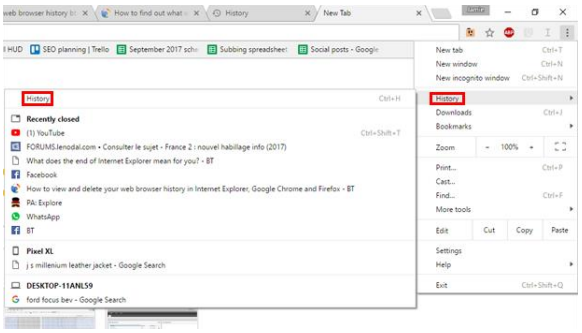
When the **Internet Options** dialog box opens, click the **Delete** button under **Browsing history** on the **General** tab.

Alternatively, from the **cog**, click on **Safety**, then **Delete Browsing History**, or press **Ctrl+Shift+Delete** on your keyboard.

Then click the **Delete** button on the dialog box that opens. If you want IE to retain your passwords make sure this option is unticked.

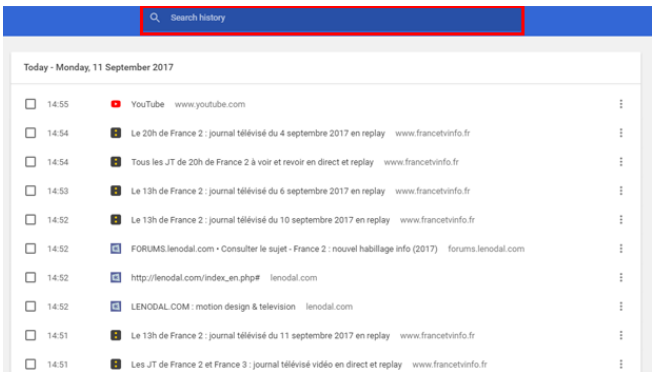
View and delete browsing history in Google Chrome –

Step 1: Open the History menu



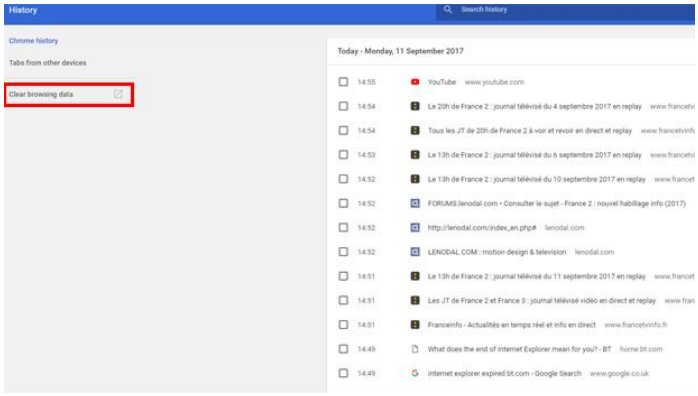
To view the web history in Google Chrome, click to open the menu ⋮ at the top-right of its window and select **History**, then click **History** a second time. Or press **Ctrl+H** on your keyboard.

Step 2: Searching History



This shows the web history as a list of pages, organised by time and date, in the current tab. You can search the web history using the **Search history** box at the top of the page. If you click the menu dots ⋮ to the right of any entry in the list, there's an option to show all pages in the web history for that site.

Step 3: Clear your Google Chrome History

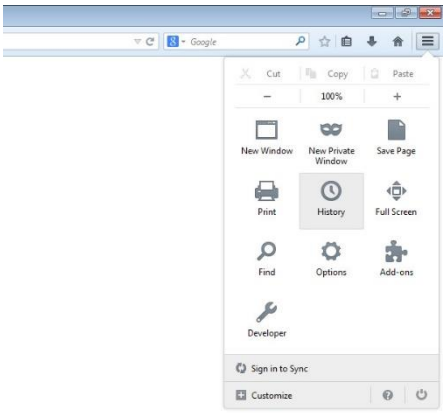


To clear the browsing history, click the **Clear browsing data** button to the left.

When the dialog box opens, choose how far back to clear using the drop-down list and click the **Clear browsing data** button. Select **Browsing History** to clear your visited websites and untick **Passwords** and **Cookies** to sign in quickly next time.

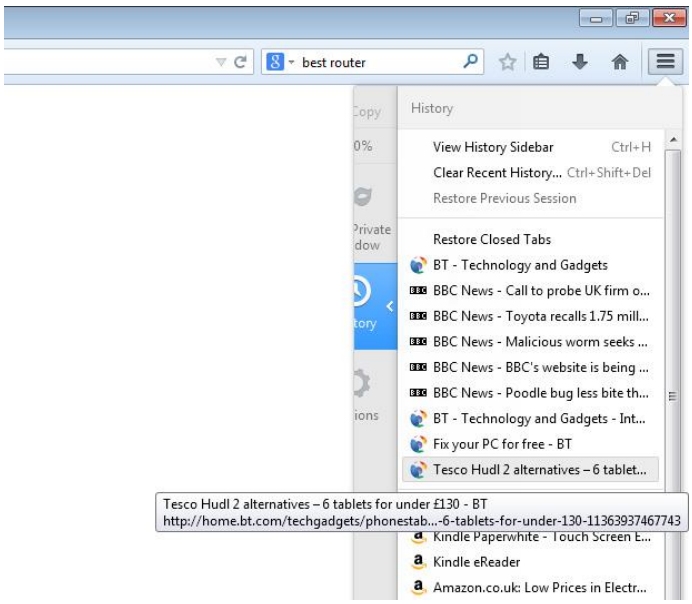
View and delete browsing history in Mozilla Firefox –

Step 1: Open the History menu

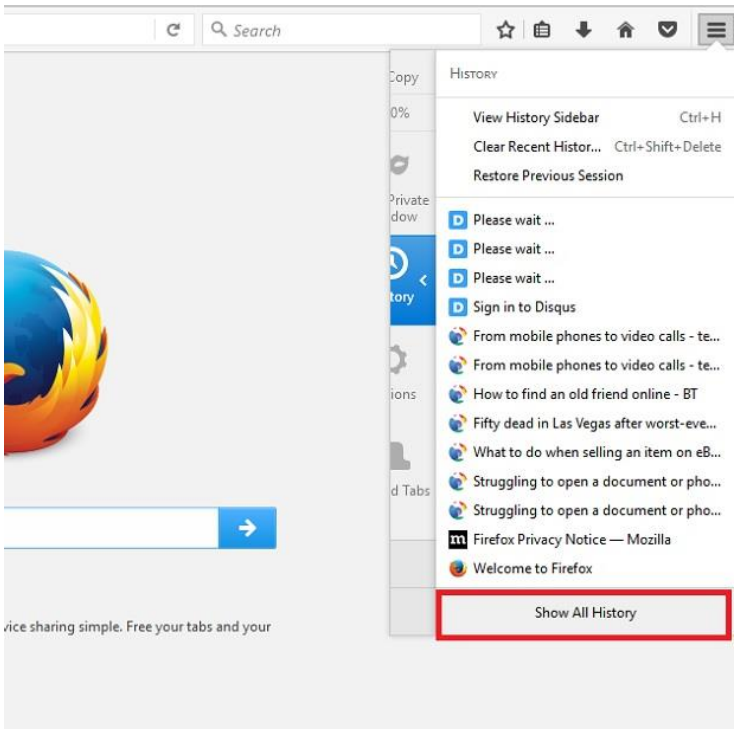


In Mozilla Firefox, you view the web history by clicking the **Menu** button at the top-right of its window and selecting **History.**

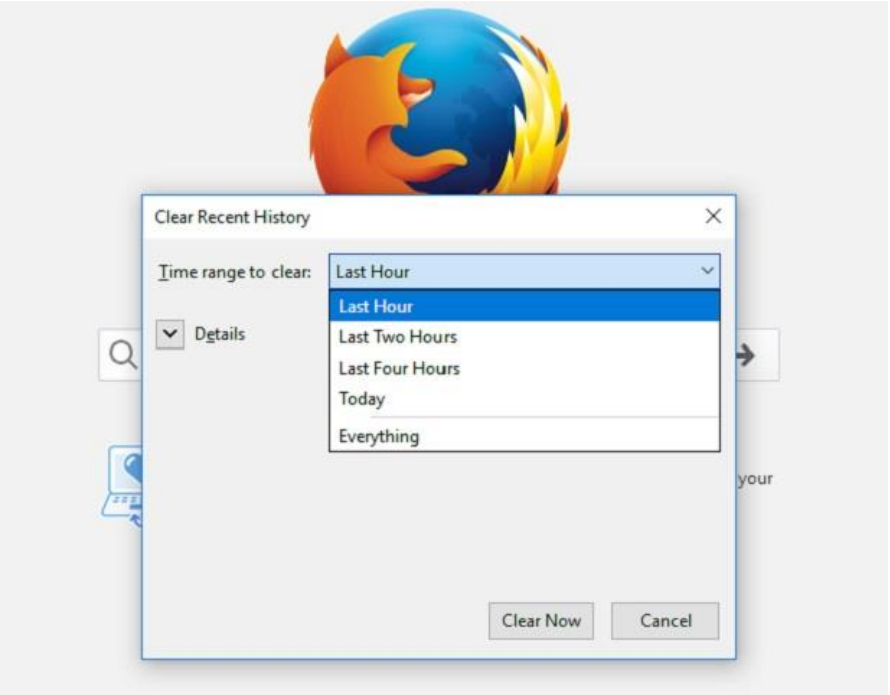
Step 2: Search your History



This shows the most recently opened web pages as a list, but you can also click the **Show All History** option at the bottom of the list to see the full history in a new window, complete with a search option.



Step 3: Clear your History



To clear the web history, select **History** from the menu again and click **Clear Recent History.** When the dialog box opens, use the drop-down list to choose how far back to clear and click the **Clear Now** button. Click **Details** to avoid deleting passwords - look for **Active Logins**.
