CCA-102: Data Communications

ASSIGNMENT

1. What are the different types of networks?

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 singlemode optical fiber 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.

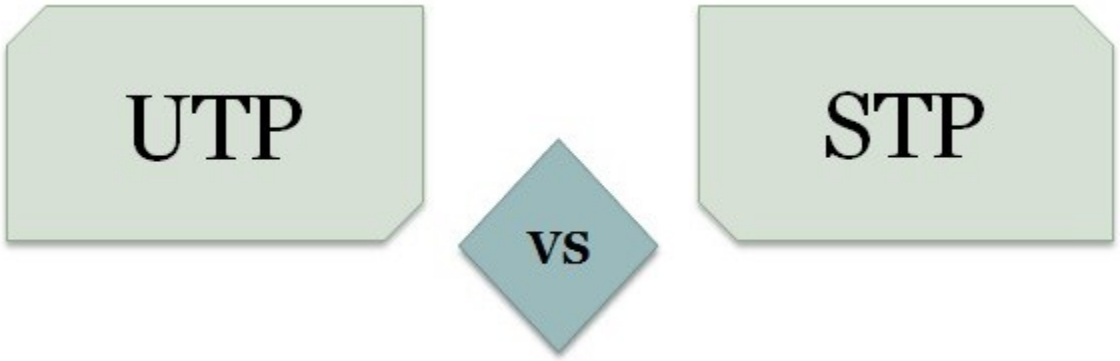
11. Virtual Private Network (VPN)

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.

If you have questions about which type of network is right for your organization, or want to learn more about Belden's network solutions that improve uptime, maintain security, and help improve user access, click here.

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

Difference Between UTP and STP Cables



UTP (Unshielded twisted pair) and STP (Shielded twisted pair) are the types of twisted pair cables which act as a transmission medium and imparts reliable connectivity of electronic equipment. Although the design and manufacture are different but both serve the same purpose.

The basic difference between UTP and STP is **UTP (Unshielded twisted pair)** is a cable with wires that are twisted together to reduce noise and crosstalk. On the contrary, **STP (Shielded twisted pair)** is a twisted pair cable confined in foil or mesh shield that guards the cable against electromagnetic interference.

Content: UTP Cable Vs STP Cable

Comparison Chart

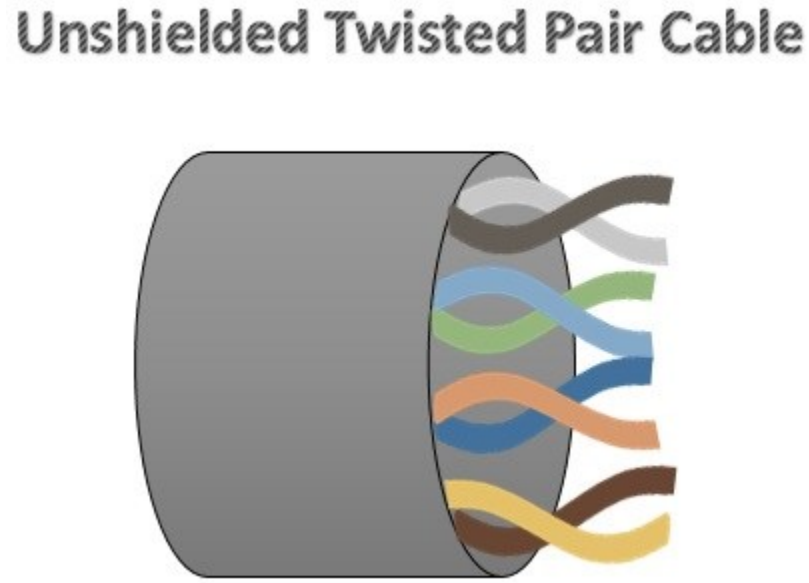
BASIS FOR COMPARISON	UTP	STP
Basic	UTP (Unshielded twisted pair) is a cable with wires that are twisted together.	STP (Shielded twisted pair) is a twisted pair cable enclosed in foil or mesh shield.
Noise and crosstalk generation	High comparatively.	Less susceptible to noise and crosstalk.
Grounding cable	Not required	Necessarily required
Ease of handling	Easily installed as cables are smaller, lighter, and flexible.	Installation of cables is difficult comparatively.
Cost	Cheaper and does not require much maintenance.	Moderately expensive.
Data Rates	Slow comparatively.	Provides high data rates

Definition of UTP Cable

Unshielded twisted-pair (UTP) cable is the most prevalent type of telecommunication medium in use today. Its frequency range is suitable for

transmitting both data and voice. Therefore, these are most commonly used in telephone systems.

A twisted pair consists of two insulated conductors (usually copper) in a twisted configuration. Color bands are used in plastic insulation for identification. In addition, colors also identify the specific conductors in a cable and to indicate which wires belong in pairs and how they relate to other pairs in a larger bundle.

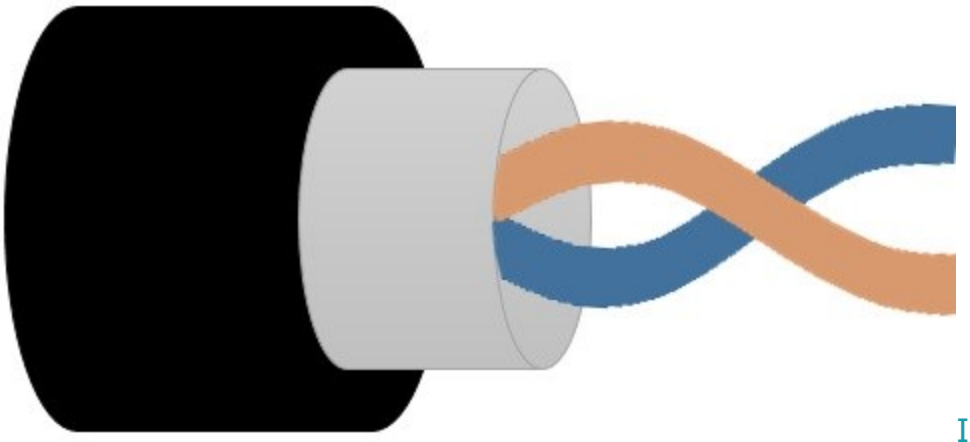


The two wires are twisted in the twisted pair cable which significantly reduces the noise generated by the external source. The **noise** here we are talking about is generated when two wires are parallel which causes an increase in voltage level in the wire closest to the source and also uneven load and damaged signal.

Definition of STP Cable

Shielded twisted-pair (STP) cable has an additional braided mesh coating or metal foil that wraps each set of insulated conductors. The metal casing intercepts the penetration of **electromagnetic noise**. It also can eradicate a phenomenon called crosstalk, which is the unwanted effect of one circuit (or channel) on another circuit (or channel).

Shielded Twisted Pair Cable



It occurs when one line (acting as a kind of receiving antenna) picks up some of the signals travelling down another line (acting as a kind of sending antenna). This effect can be experienced during telephone conversations when one can hear other conversations in the background. Shielding each pair of a twisted-pair cable can eliminate most crosstalk.

STP has the similar quality factor and uses the same connectors as UTP, but the shield must be connected to the **ground**.

Key Differences Between UTP and STP Cables

1. UTP and STP are the types of twisted pair cable where UTP is the unshielded type whereas STP is shielded, for doing so metal foil or braided mesh is used.
2. UTP reduces the crosstalk and noise as compared to the parallel arrangement of the wires but not at great extent. On the contrary, STP decreases the crosstalk, noise, and electromagnetic interference significantly.
3. UTP cables are easily installed while installation of STP cables is difficult are the cables are bigger, heavier and stiffer.
4. Grounding is not required in UTP cables. As against, STP cables requires grounding.
5. UTP cables are inexpensive whereas STP cables are costly comparatively due to additional material and manufacturing.
6. STP cables incorporate a conducting shield built of metallic foil enclosing the twisted wire pairs, which obstructs out electromagnetic interference, permitting it to carry data at an enhanced rate of speed. In contrast, UTP provides less speed of data transfer.

Conclusion

UTP and STP cables differ in the design and structure where STP cable has an additional metal foil wrapped in insulated conductors.

However, both STP and UTP cables have their respective merits and demerits, when it comes to proper installation and maintenance in a suitable situation for their use, both work finely.

3. What is difference between baseband and broadband transmission?

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?

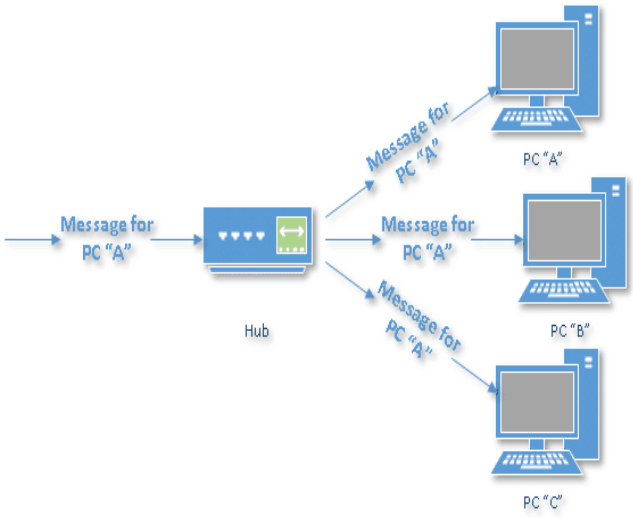
Hubs, switches, and routers are all devices that let you connect one or more computers to other computers, networked devices, or even other networks. Each has two or more connectors called ports, into which you plug the cables to make the connection.

Varying degrees of magic happen inside each device — and therein lies the difference.

- Hubs are "dumb" devices that pass on anything received on one connection to all other connections.
- Switches are semi-intelligent devices that learn which devices are on which connection.
- Routers are essentially small computers that perform a variety of intelligent tasks.

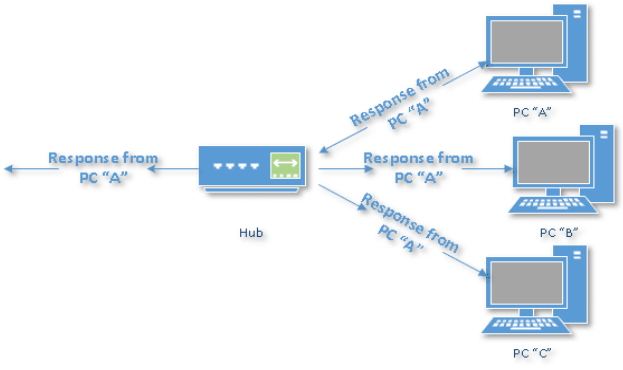
Hubs

A hub is the least expensive, least intelligent, and least complicated of the three. Its job is very simple: anything that comes in one port is sent out to the others. That's it.
If a message[1] comes in destined for computer "A", that message is sent out to all the other ports, regardless of which computer "A" is.



Incoming data passing through a hub.

When computer "A" responds, its response also goes out to every other port on the hub.



Returned response passing through a hub.

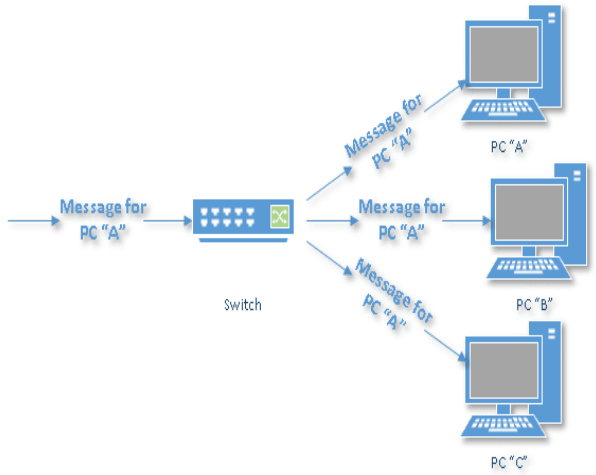
Every computer connected to the hub "sees" everything every other computer on the hub does. It's up to the computers themselves to decide if a message is for them and whether or not it should be paid attention to. The hub itself is blissfully ignorant of the data being transmitted.

For many years, hubs were quick and easy ways to connect computers in small networks. In recent years, hubs aren't as common, and switches have come into greater use.

Switches

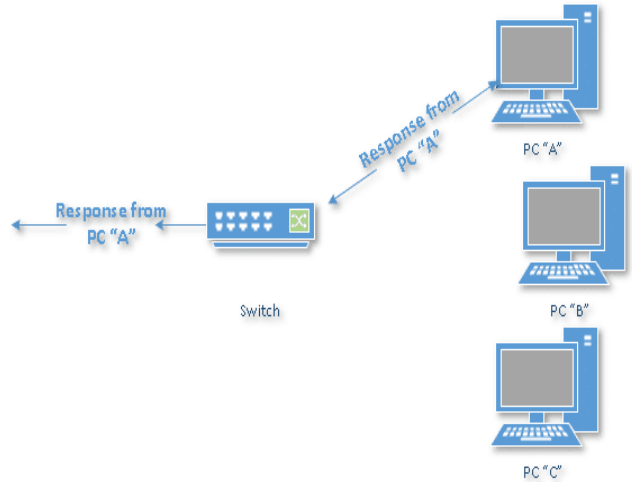
A switch does what a hub does, but more efficiently. By paying attention to the traffic that comes across it, it learns which computers are connected to which port.

Initially, a switch knows nothing, and simply sends on incoming messages to all ports.



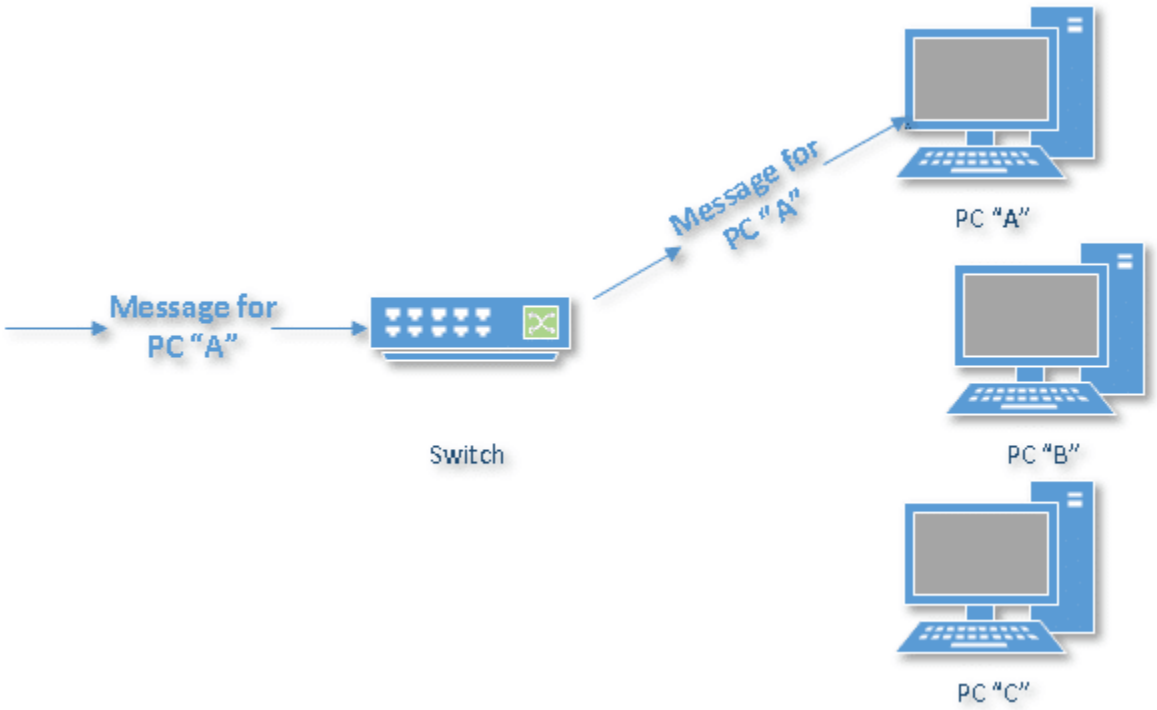
Incoming data passing through a switch.

Just by accepting that first message, however, the switch has learned something: it knows on which connection the *sender* of the message is located. Thus, when machine "A" responds to the message, the switch only needs to send that message out to the one connection.



Returned response passing through a switch.

By processing the response, the switch has learned something else: it now knows on which connection machine “A” is located. That means subsequent messages destined for machine “A” need only be sent to that one port.



Second incoming message passing through a switch.

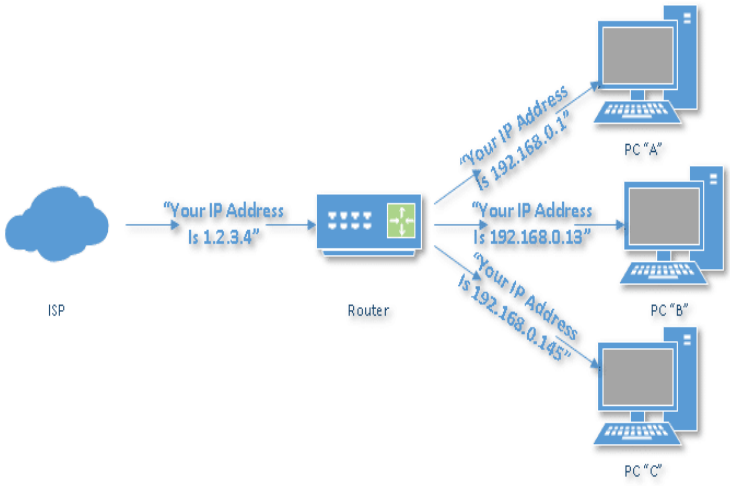
Switches learn the location of the devices they are connected to almost instantaneously. The result is, most network traffic only goes where it needs to, rather than to every port. On busy networks, this can make the network *significantly* faster.

Routers

A router is the smartest and most complicated of the three. Routers come in all shapes and sizes, from small, four-port broadband routers to large industrial-strength devices that drive the internet itself. One way to think of a router is as a computer[2] that can be programmed to understand, manipulate, and act on the data it handles.

A router operates as a switch for basic routing: it learns the location of the computers sending traffic, and routes information only to the necessary connections.

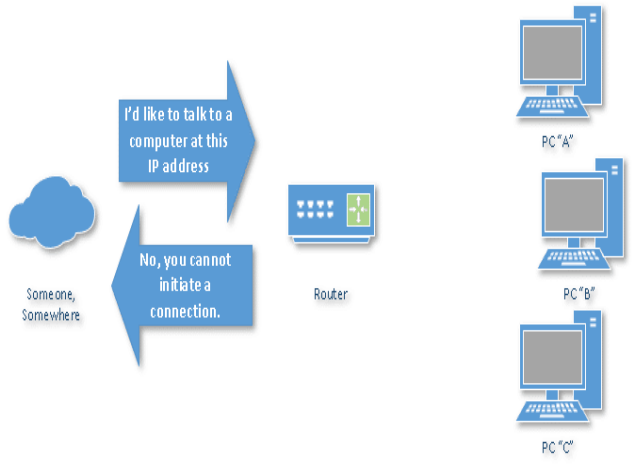
Consumer-grade routers perform (at minimum) two additional and important tasks: DHCP and NAT.
DHCP — Dynamic Host Configuration Protocol — is how dynamic IP addresses are assigned. When it first connects to the network, a device asks for an IP address to be assigned to it, and a DHCP server responds with an IP address assignment. A router connected to your ISP-provided internet connection will ask your ISP's server for an IP address; this will be your IP address on the internet. Your local computers, on the other hand, will ask the router for an IP address, and these addresses are local to your network.



IP address assignments to and through a router.

NAT — Network Address Translation- – is the way the router *translates* the IP addresses of packets that cross the internet/local network boundary. When computer "A" sends a packet, the IP address that it's "from" is that of computer "A" — 192.168.0.1, in the example above. When the router passes that on to the internet, it replaces the local IP address with the internet IP address assigned by the ISP — 1.2.3.4, in the example. It also keeps track, so if there's a

response the router knows to do the translation in reverse, replacing the internet IP address with the local IP address for machine “A”, and then sending that response packet on to machine “A”.
A side effect of NAT is that machines on the internet cannot *initiate* communications to local machines; they can only respond to communications initiated by them. This means that the router also acts as an effective firewall.



Router acting as a firewa

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

The Media Access Control address (MAC address) for any network adapter is hard coded into the card itself. Each manufacturer of network adapters has a group of characters assigned that refer specifically to that company. I believe that is the first 1/2 of the MAC address which is 12 hexadecimal characters long. But the MAC address is part and parcel of the network adapter, just as your internal organs are part of you. When you move to a new house, you take your liver with you. In the same way, when you move a NIC to a different computer, it takes its MAC address with it.

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

Answer= VOTE 1

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

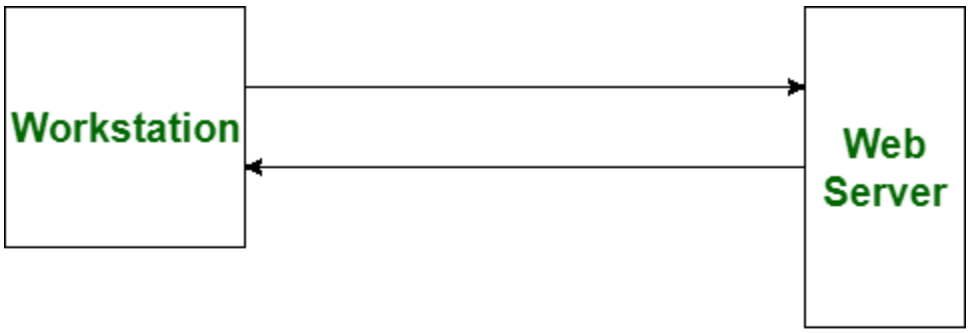
The best solution is to install anti-virus on all the computers in the network. This will protect each device from the other in case some malicious user tries to insert a virus into the servers or legitimate users.

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

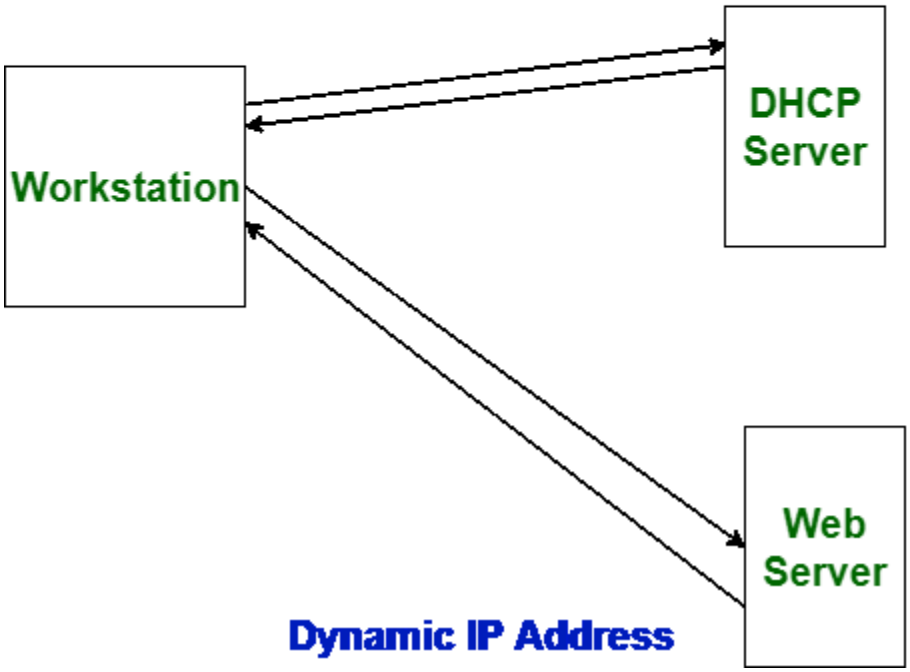
Difference between Static and Dynamic IP address

Last Updated: 15-06-2020

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.



Static IP Address



Dynamic IP Address

Difference between Static and 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).

S.NO	STATIC IP ADDRESS	DYNAMIC IP ADDRESS
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	While it is used where data is more confidential and needs more

S.NO	STATIC IP ADDRESS	DYNAMIC IP ADDRESS
	confidential.	security.

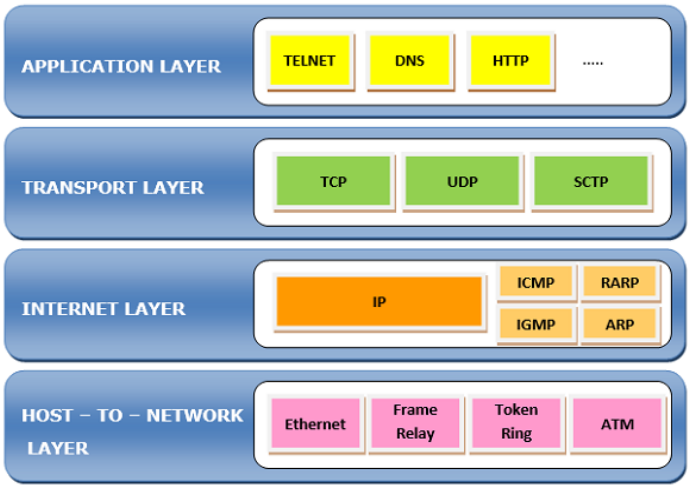
9. Discuss TCP/IP model in detail.

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 −



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

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

The primary function of a web browser is to render HTML, the code used to design or "mark up" webpages. Each time a browser loads a web page, it processes the HTML, which may include text, links, and references to images and other items, such as cascading style sheets and JavaScript functions. The browser processes these items, then renders them in the browser window.

Early web browsers, such as Mosaic and Netscape Navigator, were simple applications that rendered HTML, processed form input, and supported bookmarks. As websites have evolved, so have web browser requirements. Today's browsers are far more advanced, supporting multiple types of HTML (such as XHTML and HTML 5), dynamic JavaScript, and encryption used by secure websites.

The capabilities of modern web browsers allow web developers to create highly interactive websites. For example, Ajax enables a browser to dynamically update information on a webpage without the need to reload the page. Advances in CSS allow browsers to display a responsive website layouts and a wide array of visual effects. Cookies allow browsers to remember your settings for specific websites.

While web browser technology has come a long way since Netscape, browser compatibility issues remain a problem. Since browsers use different rendering engines, websites may not appear the same across multiple browsers. In some cases, a website may work fine in one browser, but not function properly in another. Therefore, it is smart to install multiple browsers on your computer so you can use an alternate browser if necessary.

Updated: February 28, 2014

Cite this definition:

APAMLAChicagoHTMLLink

TechTerms - The Tech Terms Computer Dictionary

This page contains a technical definition of Web Browser. It explains in computing terminology what Web Browser means and is one of many software terms in the TechTerms dictionary.

All definitions on the TechTerms website are written to be technically accurate but also easy to understand. If you find this Web Browser definition to be helpful, you can reference it using the citation links above. If you think a term should be updated or added to the TechTerms dictionary, please email TechTerms!

11. What is a search engine? Give example.

A search engine is a web-based tool that enables users to locate information on the World Wide Web. Popular examples of search engines are Google, Yahoo!, and MSN Search. Search engines utilize automated software applications (referred to as robots, bots, or spiders) that travel along the Web, following links from page to page, site to site. The information gathered by the spiders is used to create a searchable index of the Web.

How do search engines work?

Every search engine uses different complex mathematical formulas to generate search results. The results for a specific query are then displayed on the SERP. Search engine algorithms take the key elements of a web page, including the page title, content and keyword density, and come up with a ranking for where to place the results on the pages. Each search engine's algorithm is unique, so a top ranking on Yahoo! does not guarantee a prominent ranking on Google, and vice versa. To make things more complicated, the algorithms used by search engines are not only closely guarded secrets, they are also constantly undergoing modification and revision. This means that the criteria to best optimize a site with must be surmised through observation, as well as trial and error — and not just once, but continuously.

Gimmicks less reputable SEO firms tout as the answer to better site rankings may work at best for only a short period before the search engine's developers become wise to the tactics and change their algorithm. More likely, sites using these tricks will be labeled as spam by the search engines and their rankings will plummet.

Search engines only "see" the text on web pages, and use the underlying HTML structure to determine relevance. Large photos, or dynamic Flash animation mean nothing to search engines, but the actual text on your pages does. It is difficult to build a Flash site that is as

friendly to search engines; as a result, Flash sites will tend not to rank as high as sites developed with well coded HTML and CSS (Cascading Style Sheets — a complex mechanism for adding styles to website pages above and beyond regular HTML). If the terms you want to be found by do not appear in the text of your website, it will be very difficult for your website to yield high placement in the SERPs.

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

Difference Between WWW and Internet

The terms World Wide Web (WWW) and the Internet are so often used interchangeably that the fundamental difference between the two is easily forgotten.

In simple words, WWW is just a common point of connectivity for information sharing that is facilitated by a global network of computers.

The internet, on the other hand, is a connection between computers and countless other devices that form a huge network of systems.

This article will further highlight the differences between WWW and the Internet within the context of the IAS Exam.

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	The internet is a public network of network with a maze of wired and wireless connections between separate groups of servers computers

common one.	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 Internters, 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

Both the World Wide Web and the Internet are concepts covered under the Science and Technology Segment of the UPSC IAS Exam. Aspirants can study this segment through the links given below

- Science and Technology Notes for UPSC
- How to Tackle Science and Technology for UPSC
- General Science Preparation for UPSC
- Science and Technology MCQs for UPSC
- Difference Between Hardware and Software

Aspirants can find more Difference Between Articles, by visiting the linked page

Difference Between WWW and Internet – Download PDF Here

Become familiar with the general pattern of the IAS Exam by visiting the IAS 2020 Syllabus page. For more exam-related preparation materials, refer to the links given in the table below:

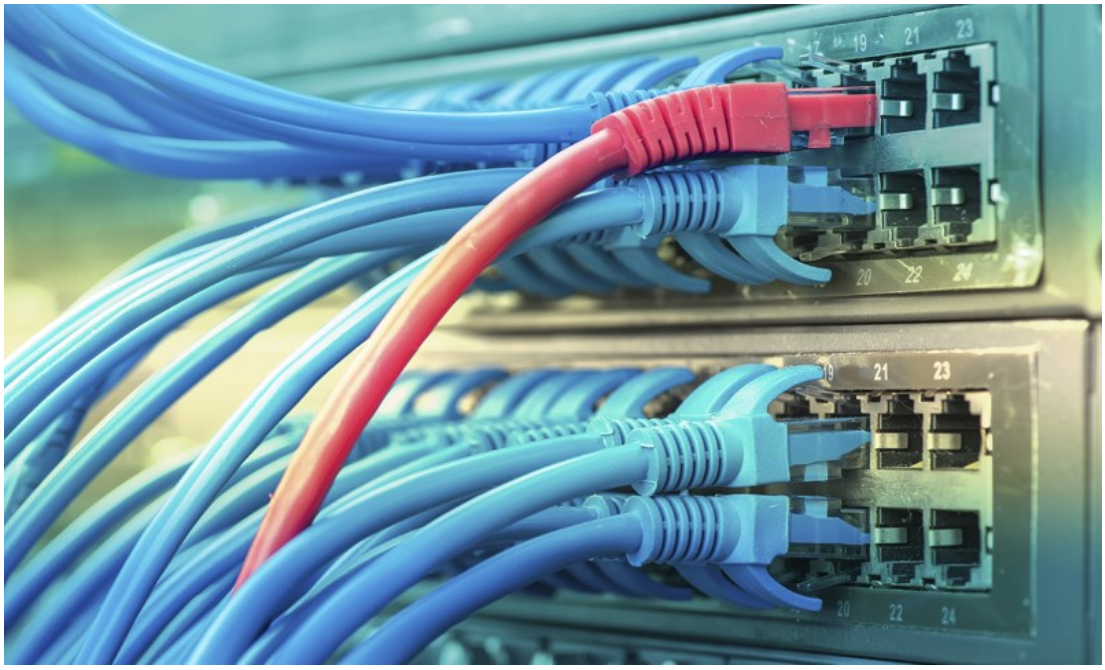
Based on a recent survey of Internet traffic, the 10 most popular uses of the Internet in descending order of use are:

1. **Electronic mail.** At least 85% of the inhabitants of cyberspace send and receive e-mail. Some 20 million e-mail messages cross the Internet every week.
2. **Research.**
3. **Downloading files.**
4. **Discussion groups.** These include public groups, such as those on Usenet, and the private mailing lists that ListServ manages.
5. **Interactive games.** Who hasn't tried to hunt down at least one game?
6. **Education and self-improvement.** On-line courses and workshops have found yet another outlet.
7. **Friendship and dating.** You may be surprised at the number of electronic "personals" that you can find on the World Wide Web.
8. **Electronic newspapers and magazines.** This category includes late-breaking news, weather, and sports. We're likely to see this category leap to the top five in the next several years.
9. **Job-hunting.** Classified ads are in abundance, but most are for technical positions.
10. **Shopping.** It's difficult to believe that this category even ranks. It appears that "cybermalls" are more for curious than serious shoppers.

The survey shows that individuals, corporations, business people, and groups use Internet primarily as a communications vehicle as these users reduce their use of fax machines, telephones, and the postal service. E-mail should remain at the top of the list. The Internet has continued and will continue to change how we view the world. — *by Diane Myers, Analyst Communications, End Use, In-Stat, Scottsdale, AZ. (602) 483-4442*

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

hat is an Internet Service Provider?



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

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

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

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

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

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

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

Types of ISPs

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

DSL and Cable.

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

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

Fiber Internet: On its way to you?

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

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

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

ISP stands for ‘internet server provide. Examplexs are – airtel; ect.

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

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:

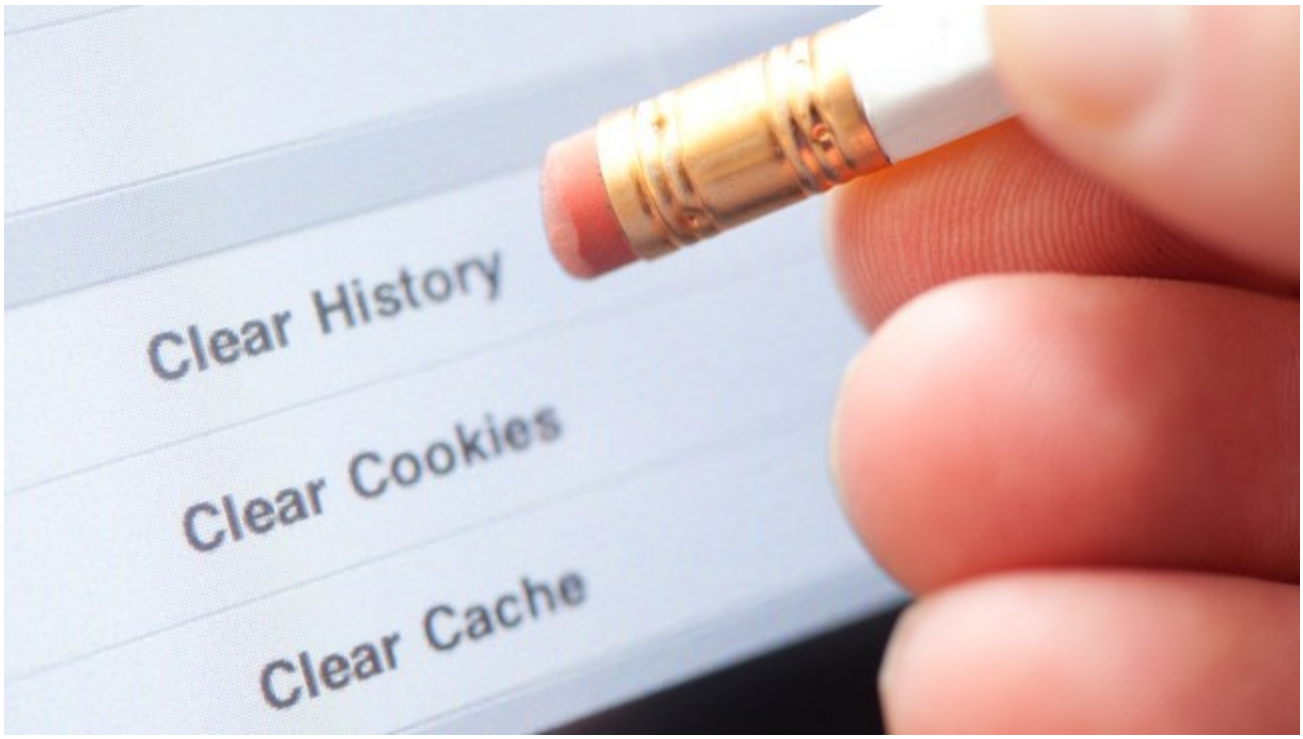
S.NO	MAC ADDRESS	IP ADDRESS
1.	MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.
2.	MAC Address is a six byte hexadecimal address.	IP Address is either four byte (IPv4) or six byte (IPv6) address.
3.	A device attached with MAC Address can retrieve by 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 found by third party.

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

Can’t find a webpage you were only looking at last week? It’s easy using your browser’s History feature - you just need to know where to look.

By **Julian Prokaza**
Last updated: 24 September 2018 - 11.25am



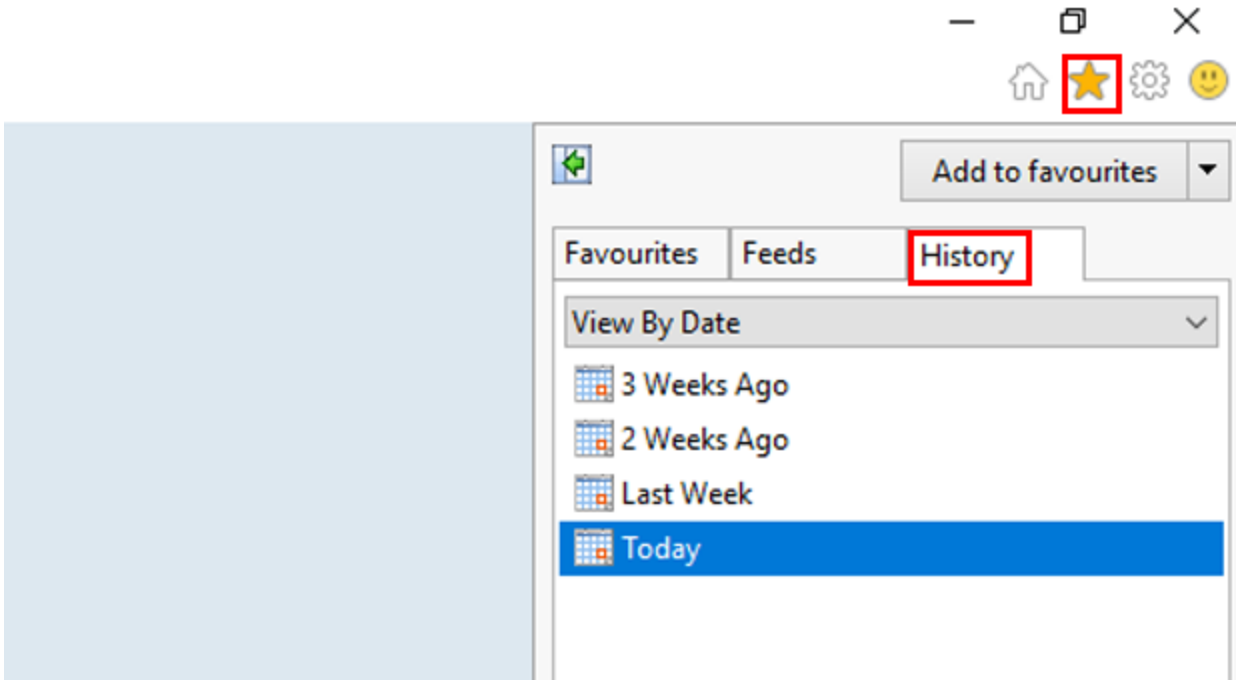
Finding a particular web page long after you last visited it can be a tricky business unless you bookmarked it or can track it down with a search engine.

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.

[Read more: How to check your child’s online web browser history]

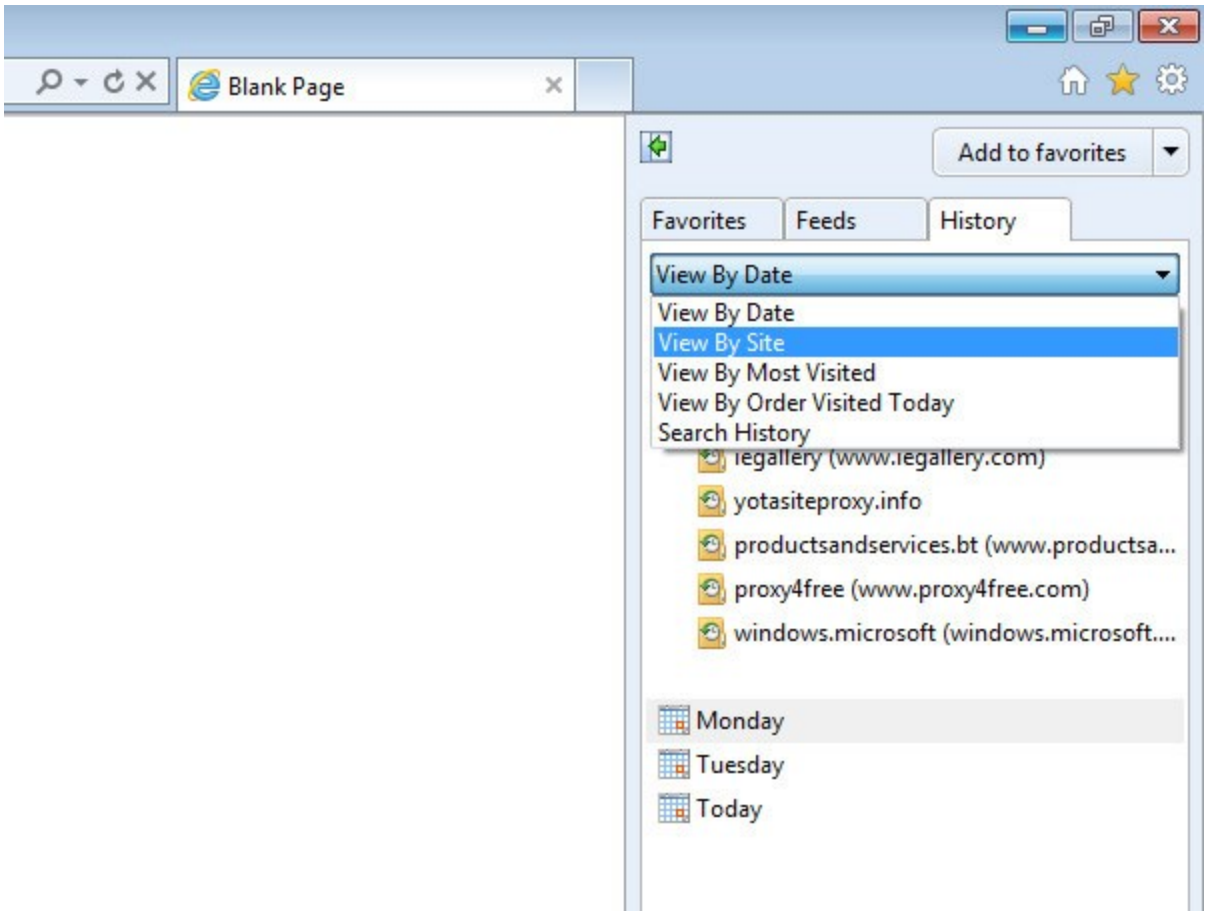
View and delete in Internet Explorer

Step 1: Open the History menu



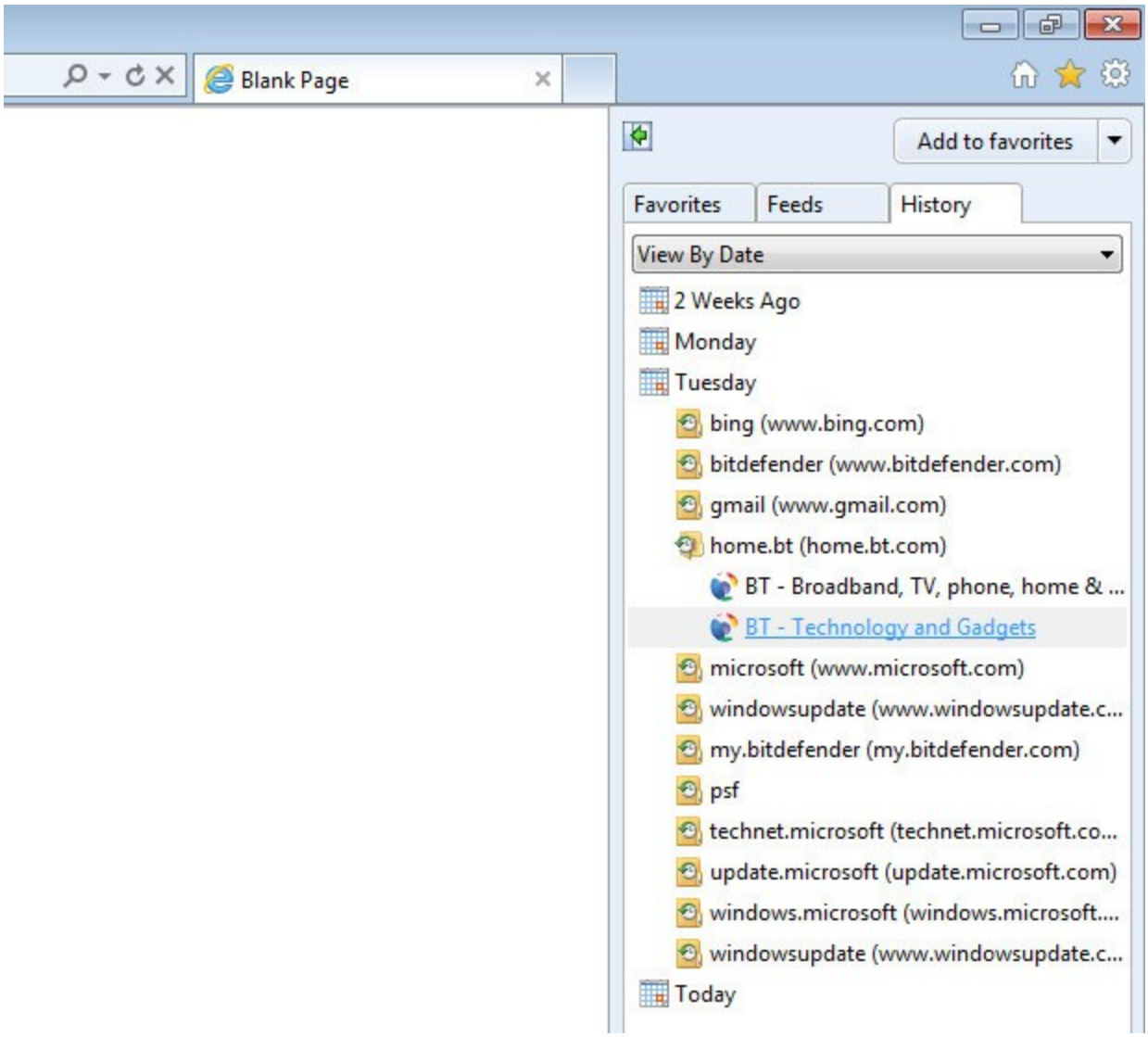
In Internet Explorer 11, click the **star** icon at the top-right of the window.

Step 2: Search and sort Internet Explorer History



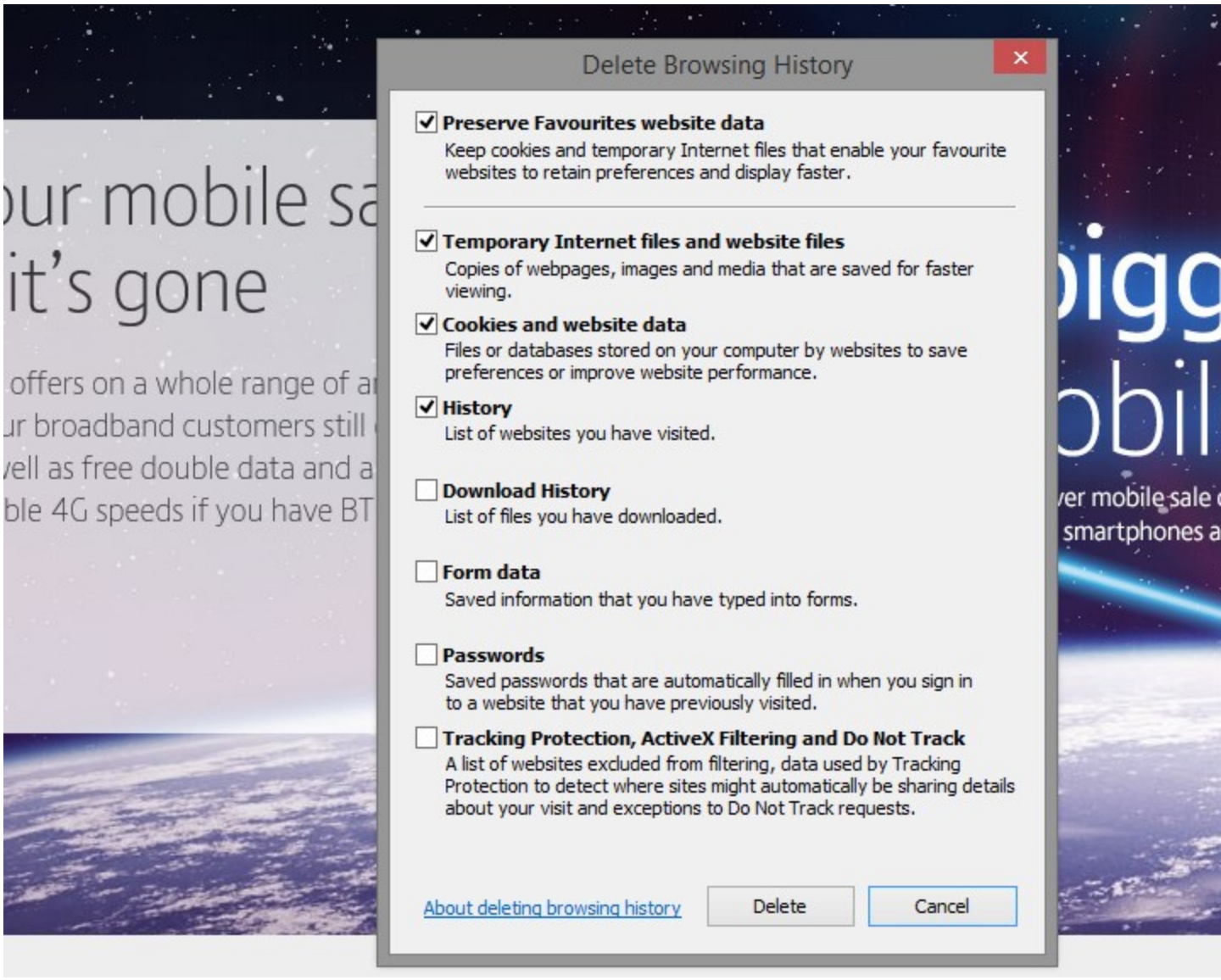
When the dialog box opens, click the **History** tab to view the web pages you've visited previously, ordered by date. There's also a drop-down list so you can view the pages by **Site, Name, Most Visited** and **Order Visited Today**, plus a **Search History** option for when it's quicker to find a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

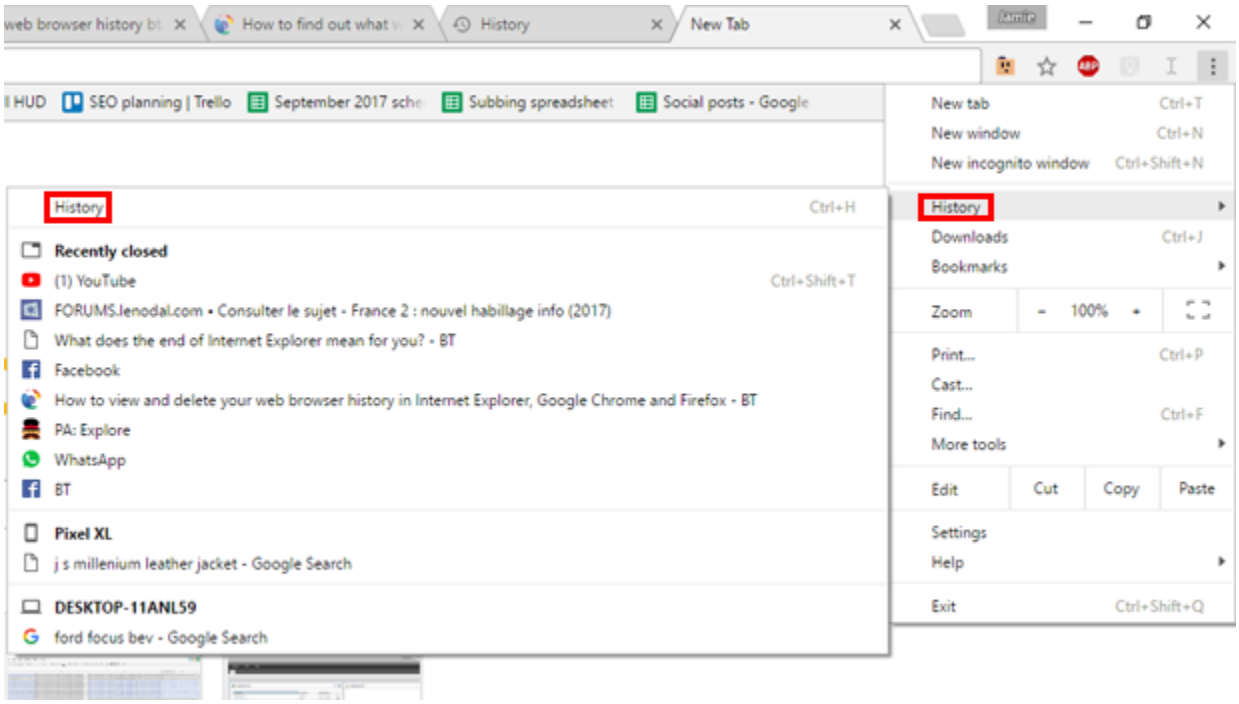
Alternatively, from the **cog**, click on **Safety**, then **Delete Browsing History**, or press **Ctrl+Shift+Delete** on your keyboard.

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.

Remember, Internet Explorer is being phased out in favour of Microsoft's new web browser Edge. **Find out what it means for your PC.**

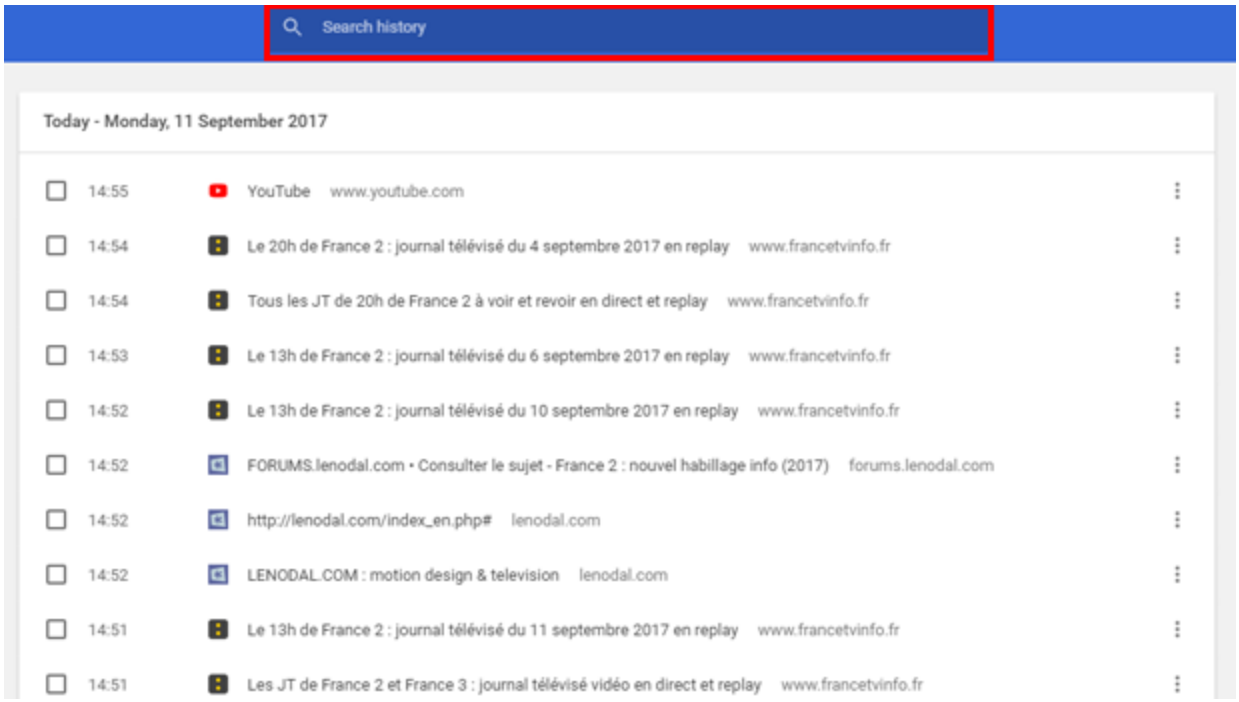
View and delete browsing history in Google Chrome

Step 1: Open the History menu



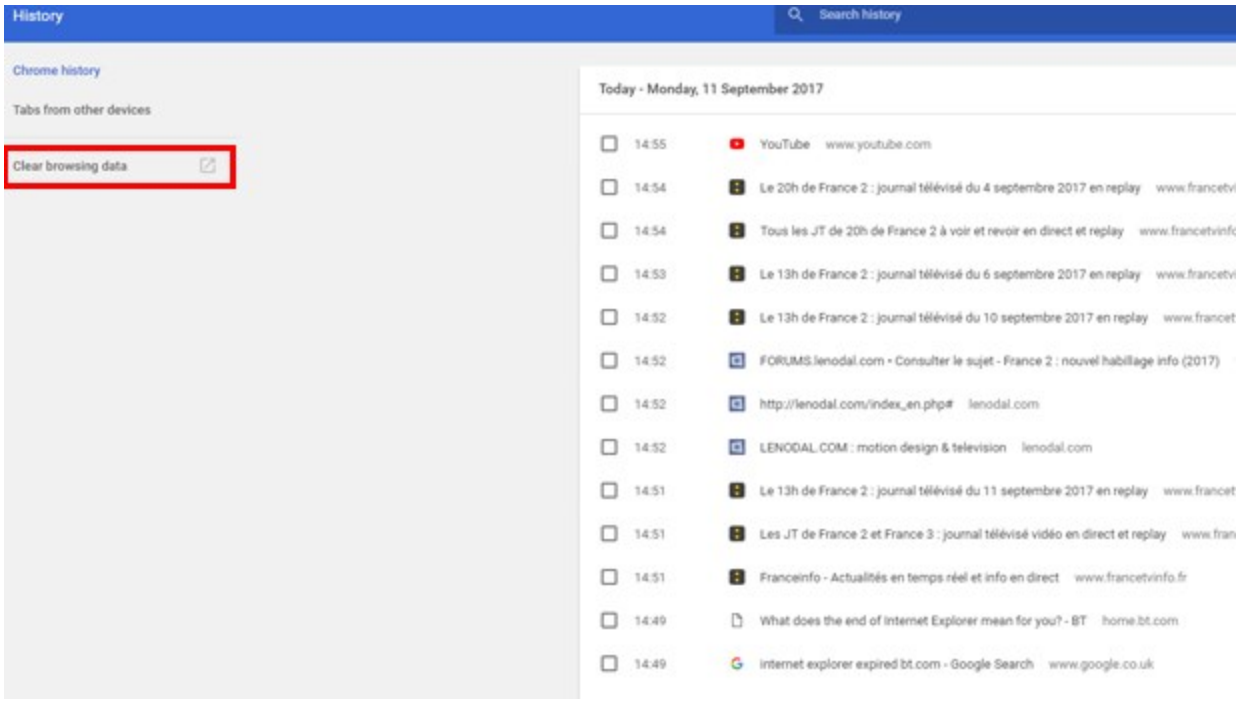
To view the web history in Google Chrome, click to open the menu ⋮ at the top-right of its window and select **History**, then click **History** a second time. Or press **Ctrl+H** on your keyboard.

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



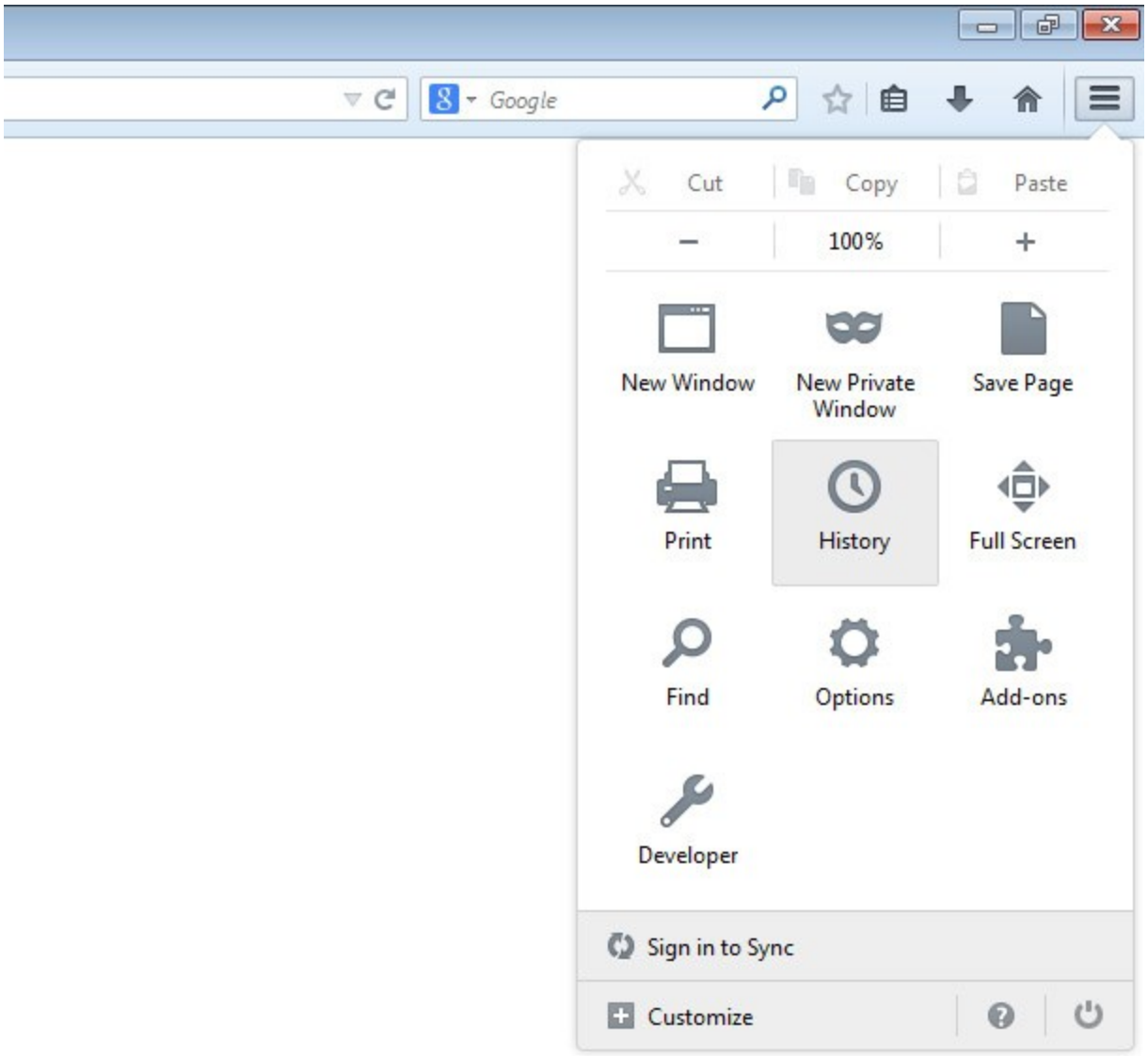
To clear the browsing history, click the **Clear browsing data** button to the left.

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.

[Read more: How to speed up Google Chrome]

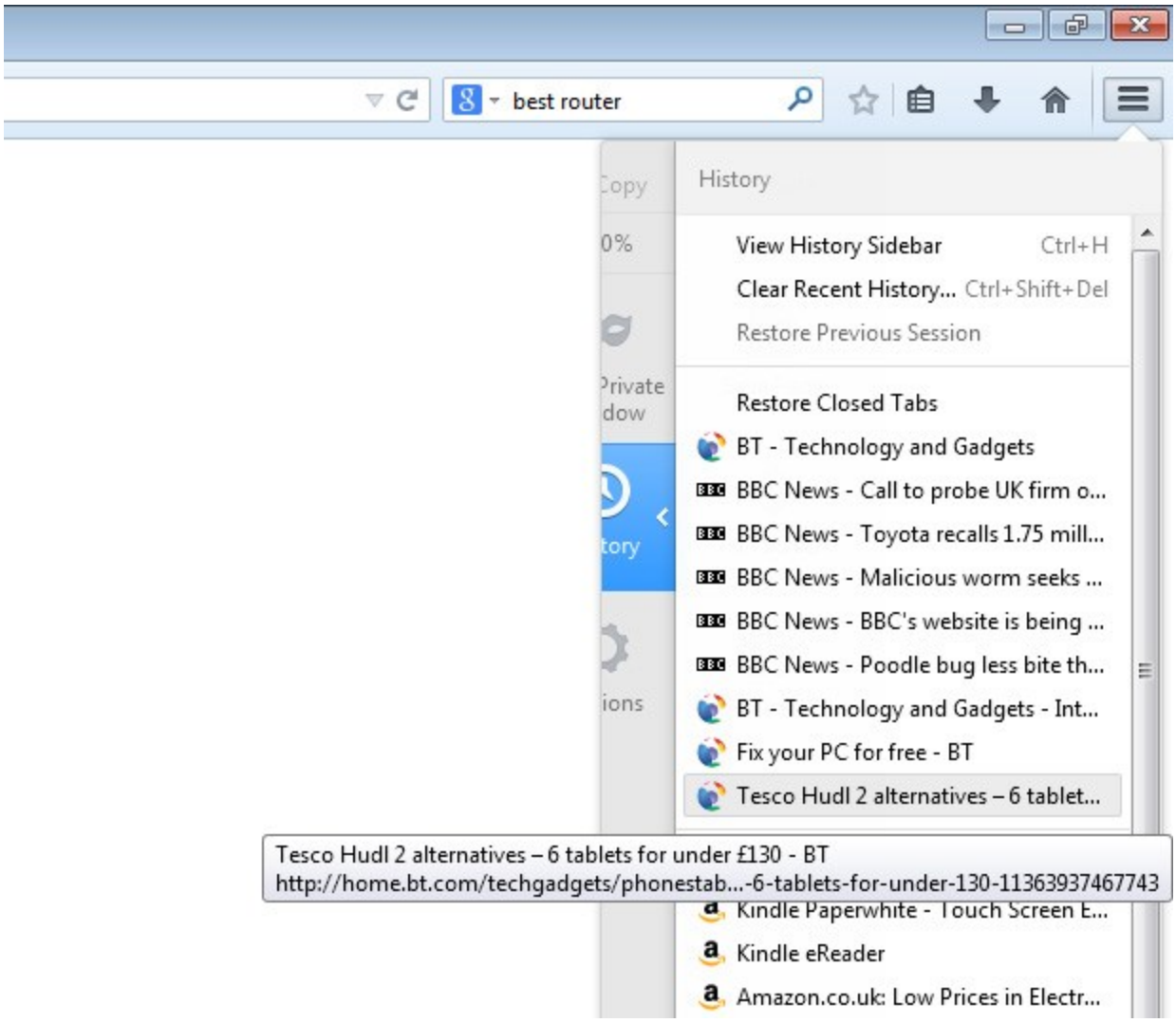
View and delete browsing history in Mozilla Firefox

Step 1: Open the History menu

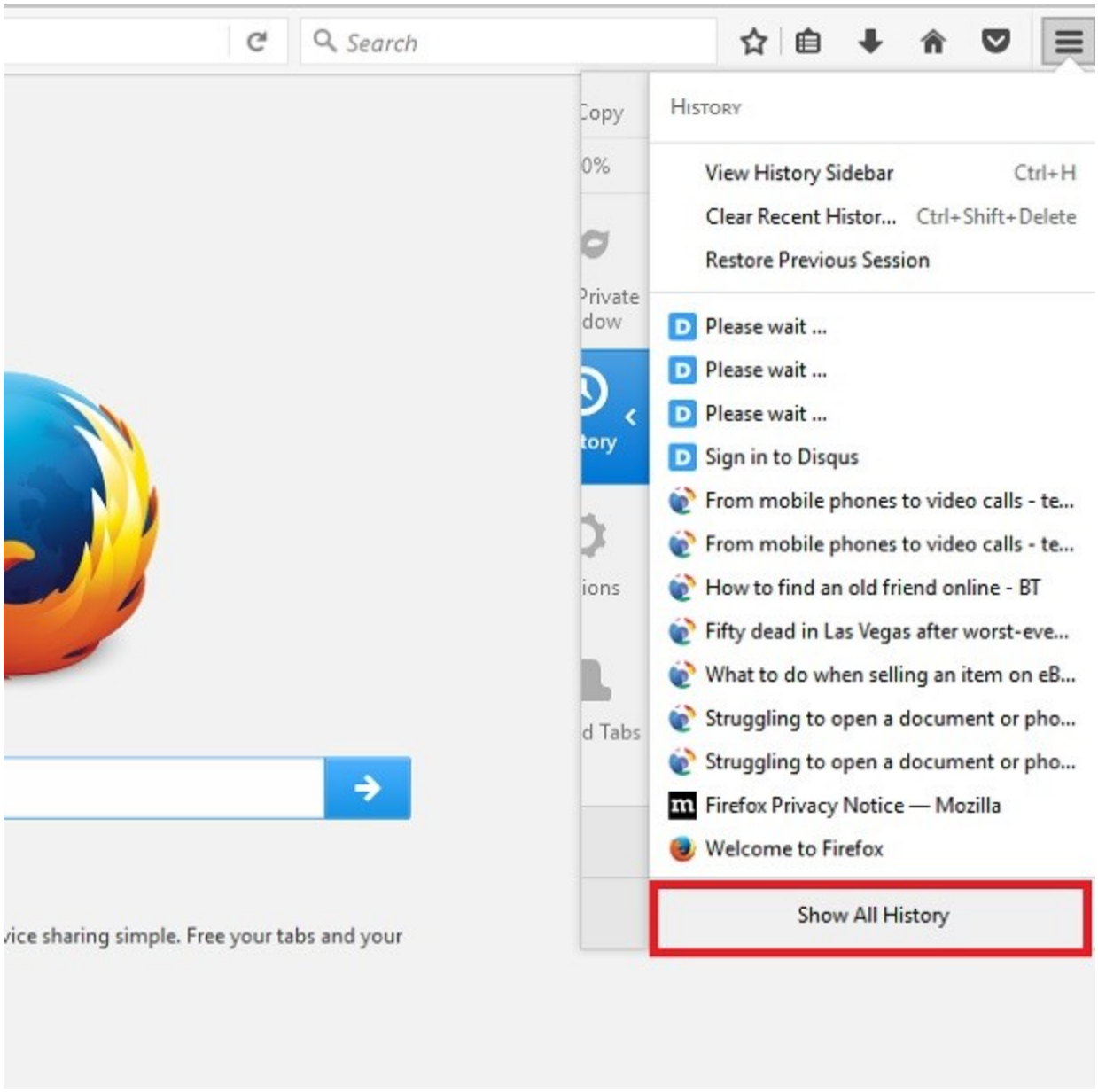


In Mozilla Firefox, you view the web history by clicking the **Menu** button at the top-right of its window and selecting **History.**

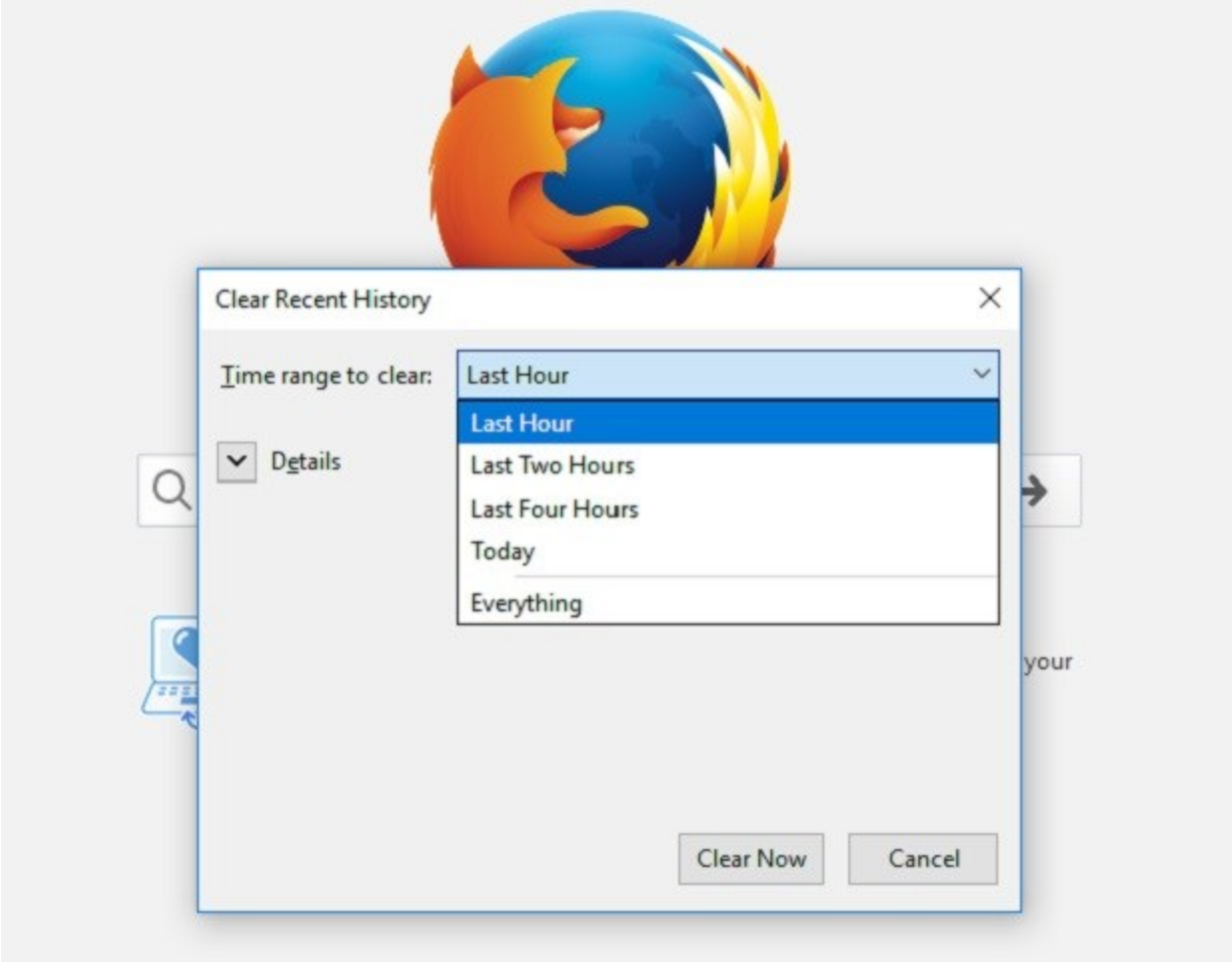
Step 2: Search your History



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**.

View and delete web history in Microsoft Edge

To find out how to view and delete your web history from Microsoft Edge, **read our separate guide**.