CCA-102: Data Communications

ASSIGNMENT

1. What are the different types of networks?

Ans.

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,

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

Ans.

Difference Between UTP and STP Cables

August 21, 2017 8 Comments

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).
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

2. What is difference between baseband and broadband transmission?

Ans.

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.

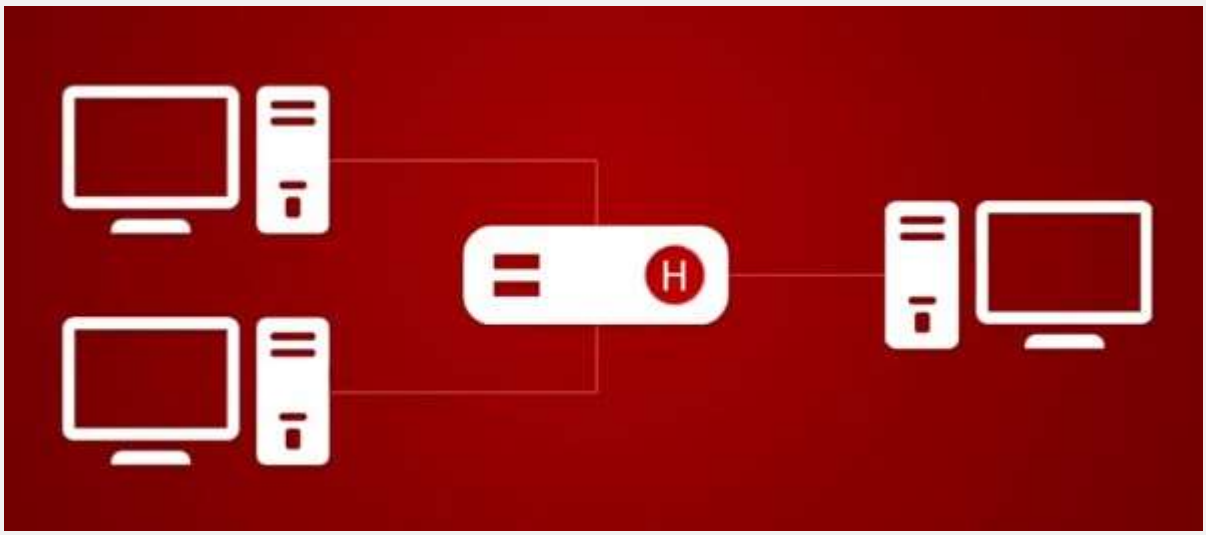
4. What is the difference between a hub, modem, router and a switch?

Ans. When computers, network devices or other networks are required to be connected, hubs, **switches** and routers are the bridges to link them together. All the three types of devices can perform the same function, and technicians sometimes may use the terms interchangeably. However, this will make people confuse whether they are the same thing or different from each other. This post is going to explore the actual meanings of hub, switch, router and what they are used for.

Overview of Hub, Switch & Router

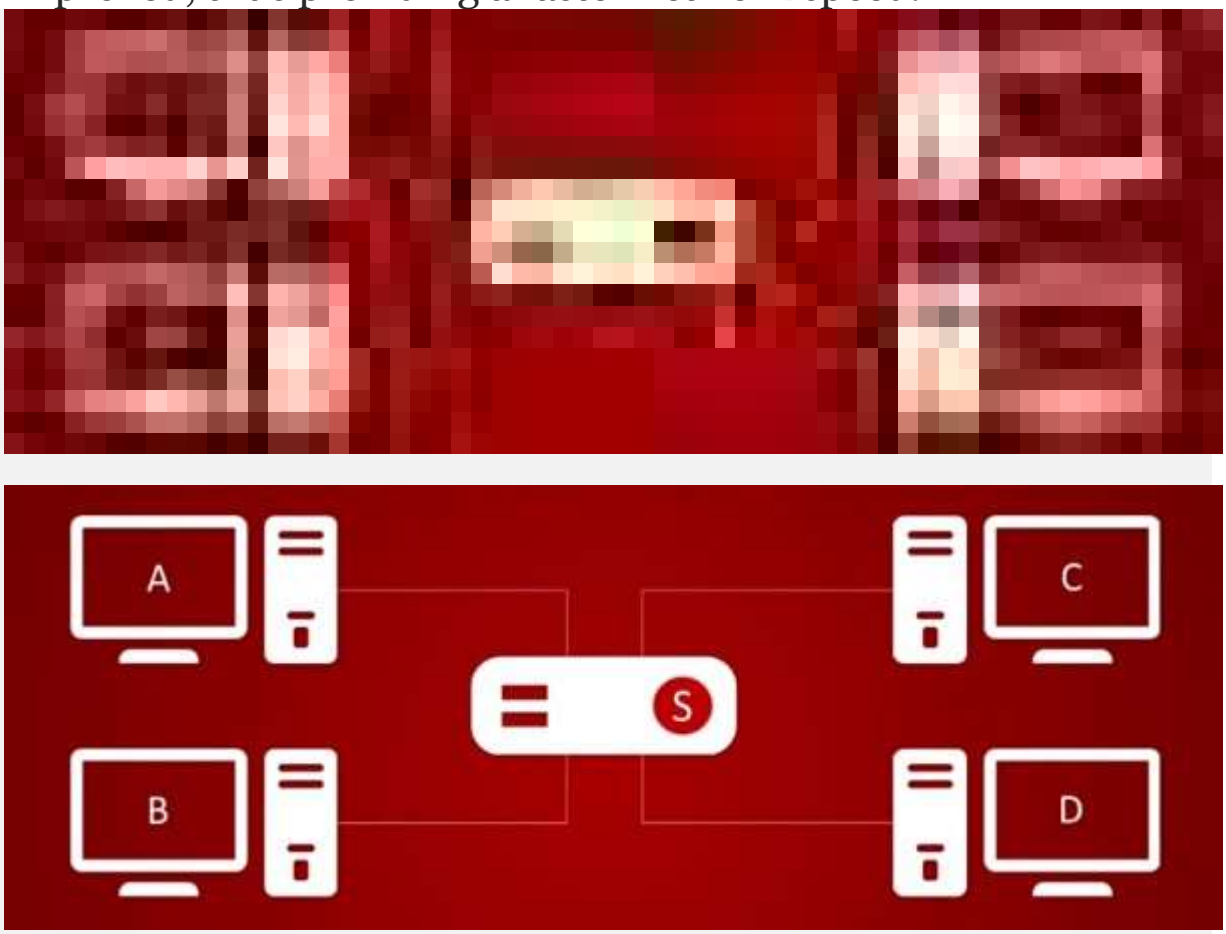
Hub

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

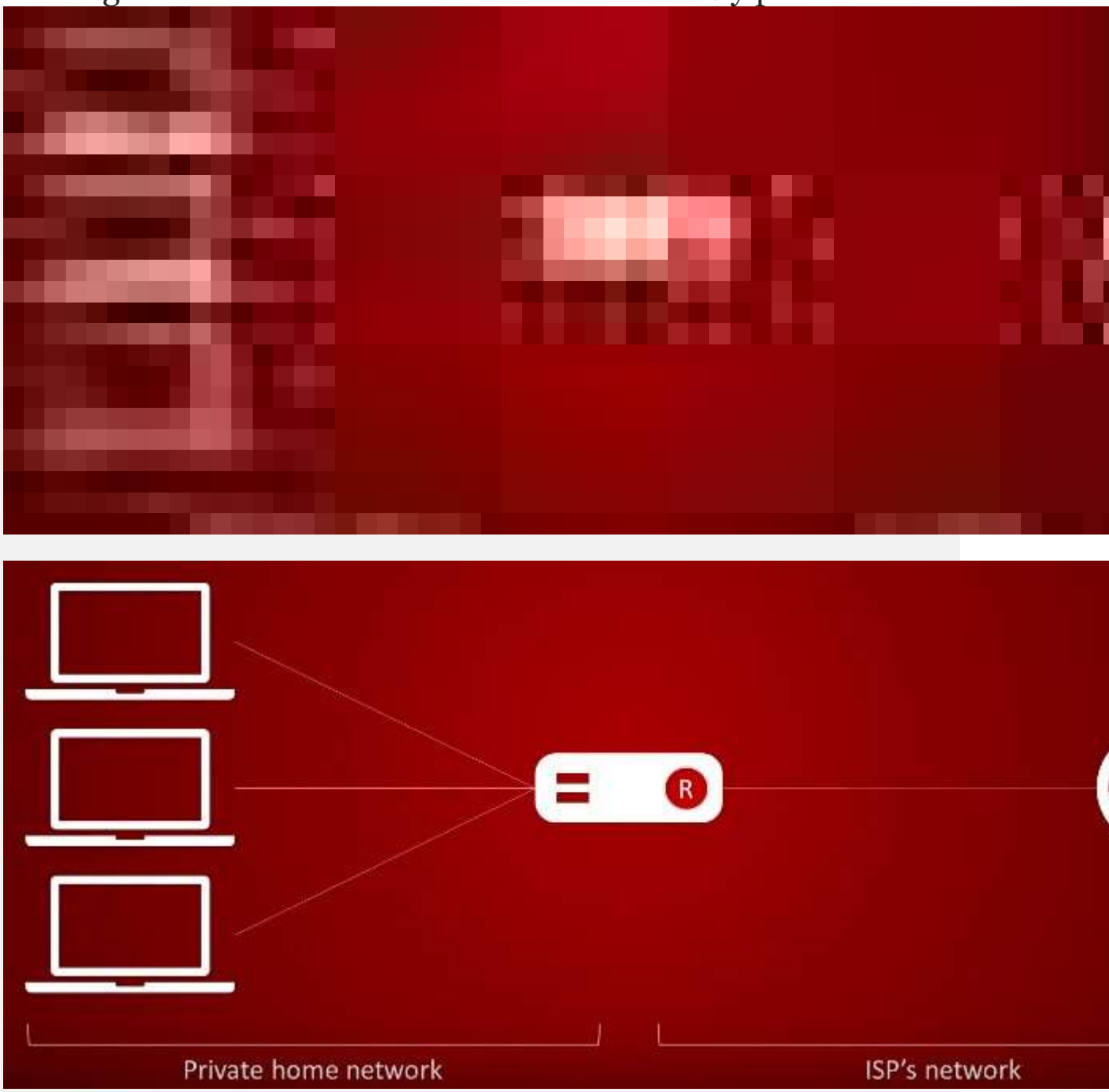
A switch is able to handle the data and knows the specific addresses to send the message. It can decide which computer is the message intended for and send the message directly to the right computer. The efficiency of switch has been greatly improved, thus providing a faster network speed.



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.

Source:http://www.fiber-optic-cable-sale.com/know-difference-hub-switch-router.html

WRITTEN BY

Orenda

743
3

- Hub

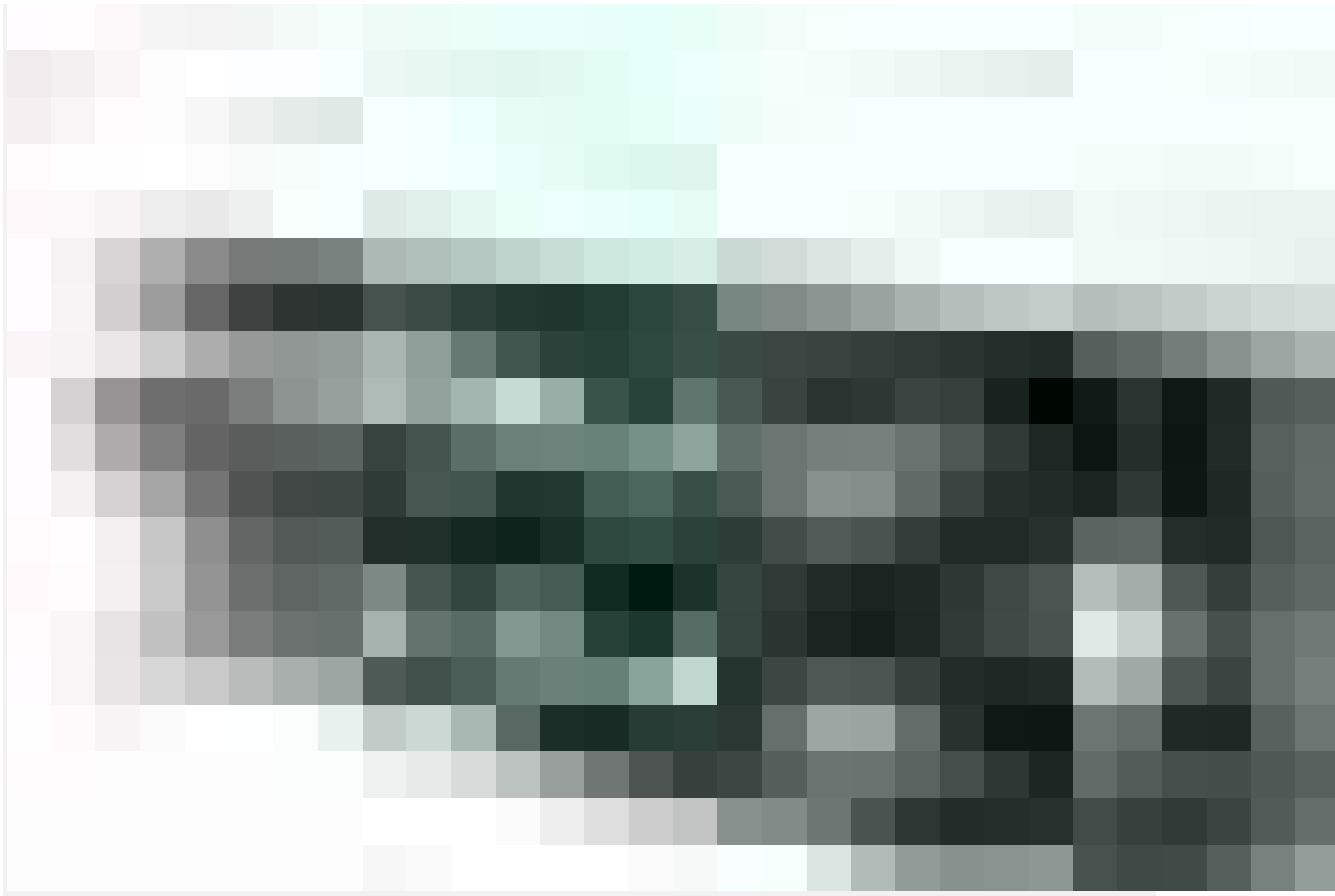
- Switch
- Router

More from Orenda
Follow

Feb 13, 2017

Different Ports on WDM Mux/Demux

In the WDM (wavelength-division multiplexing) system, CWDM (coarse wavelength-division multiplexing) and DWDM (dense wavelength-division multiplexing) Mux/Demux (multiplexer/demultiplexer) modules are often deployed to join multiple wavelengths onto a single fiber. Multiplexer is for combining signals together, while demultiplexer is for splitting signals apart. On a WDM Mux/Demux, there are many kinds of ports for different applications. This article will discuss the functions of these ports on WDM Mux/Demux.



Necessary Ports on WDM Mux/Demux

Channel port and line port are the necessary ports to support the basic function of WDM Mux/Demux to join or split signals in the data network.

Channel Port

A WDM Mux/Demux usually has several channel ports on different wavelengths. ...

Read more · 3 min read

Feb 9, 2017

How Will SDN Change the Future Network?

Traditional networks are usually built with tiers of Ethernet **switches** in a tree structure. However, the development of mobile devices, server virtualization and cloud computing service has driven the need for dynamic computing and storage in data centers. Thus, the concept of software-defined networking (SDN) was put forward to construct a more flexible and agile network. This technology has widely caught people's attention in the industry over the years. In this post, some basic knowledge about SDN will be introduced to help you have better understanding.

Definition of SDN Architecture

SDN is a developing network architecture that aims to directly program the network computing. Through the open interfaces and abstraction of lower-level functionality, this approach allows the network administrators to programmatically initialize, control, change and manage network behavior dynamically. SDN is different from the traditional network architecture whose network devices are based on both control plane and data plane. Instead, SDN puts the control plane on the SDN controller to communicate with a physical or virtual switch data plane through the OpenFlow protocol. ...

Read more · 3 min read

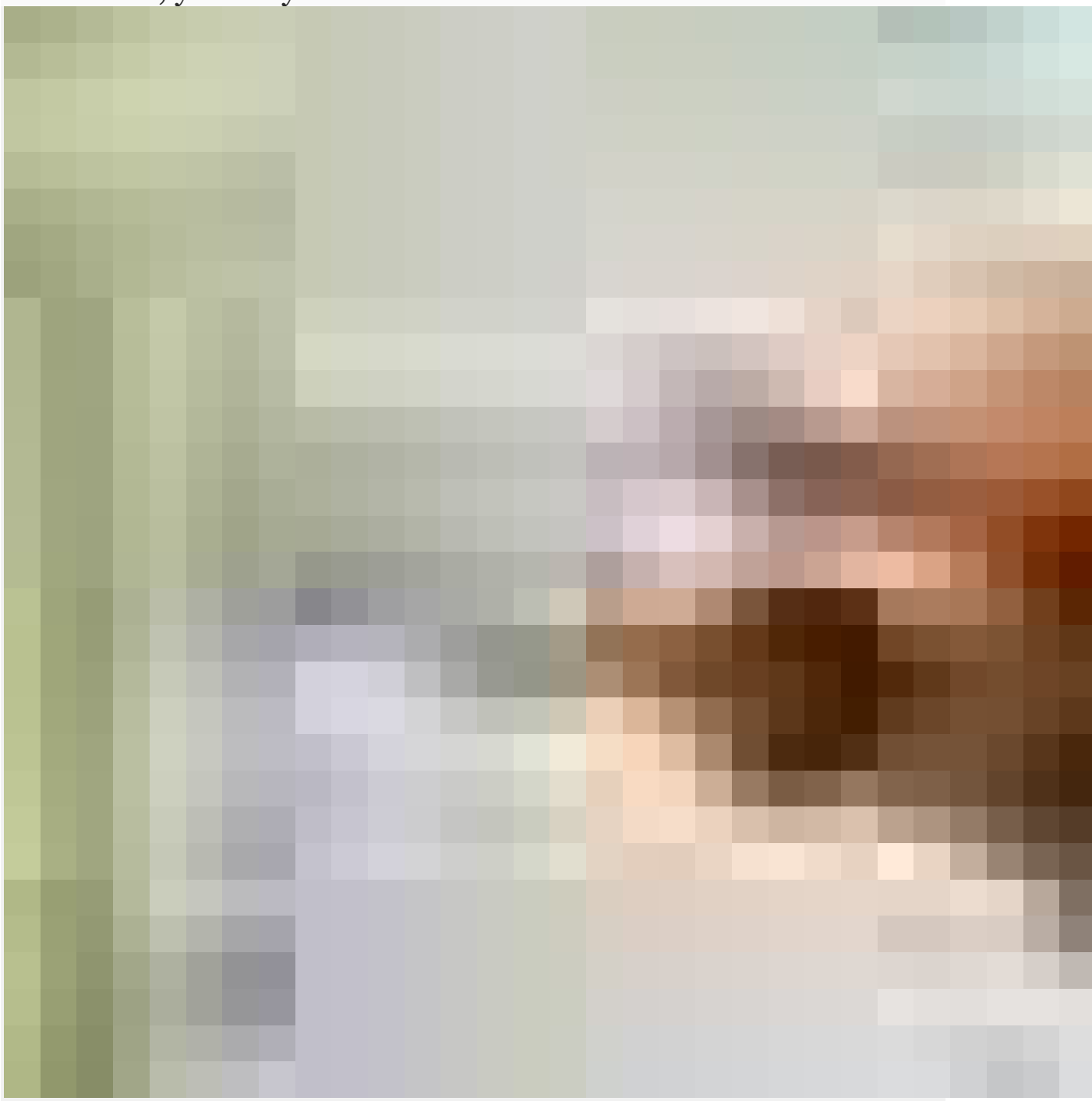
7

Jan 18, 2017

Have You Chosen the Right Power Cord?

Different cables have particular applications. Some are used for data transmission like fiber optic cable or copper cable, and some are used for the transmission of electrical power. **Power**

cord is the assembly widely used as the connection between main electricity supply and the device through a wall socket or extension cord. Power cord is adopted in almost every where when the alternating current power is required. However, have you chosen the right type of power cord for your device? From this article, you may find the answers.



Overview of Power Cord

A power cord set usually has connectors molded to the cord at each end, thus both ends can detach from the power supply and device. Specifically, power cord assembly consists of three major

parts. First is the cable plug, and it is also a male connector used for inserting into the AC outlet to provide power. Then is the receptacle on the other end. Receptacle part is also known as the female connector attached to equipment. Cord is the main section that contains the insulated wires with different lengths and thicknesses. ...

Read more · 3 min read

Jan 16, 2017

Basic Knowledge of Wireless Access Point

With the rapid development of Ethernet network, cables are widely adopted for wired network connectivity. However, this may also lead to the problem of cable mess when large quantities of cables are deployed. In order to solve this issue, wireless network is now accepted by most network users to reduce the employment of cables. **Wireless access point** is an important device for connecting the wired network with wireless

network. This article will talk about the fundamental knowledge about wireless access point.

What Is Wireless Access Point?

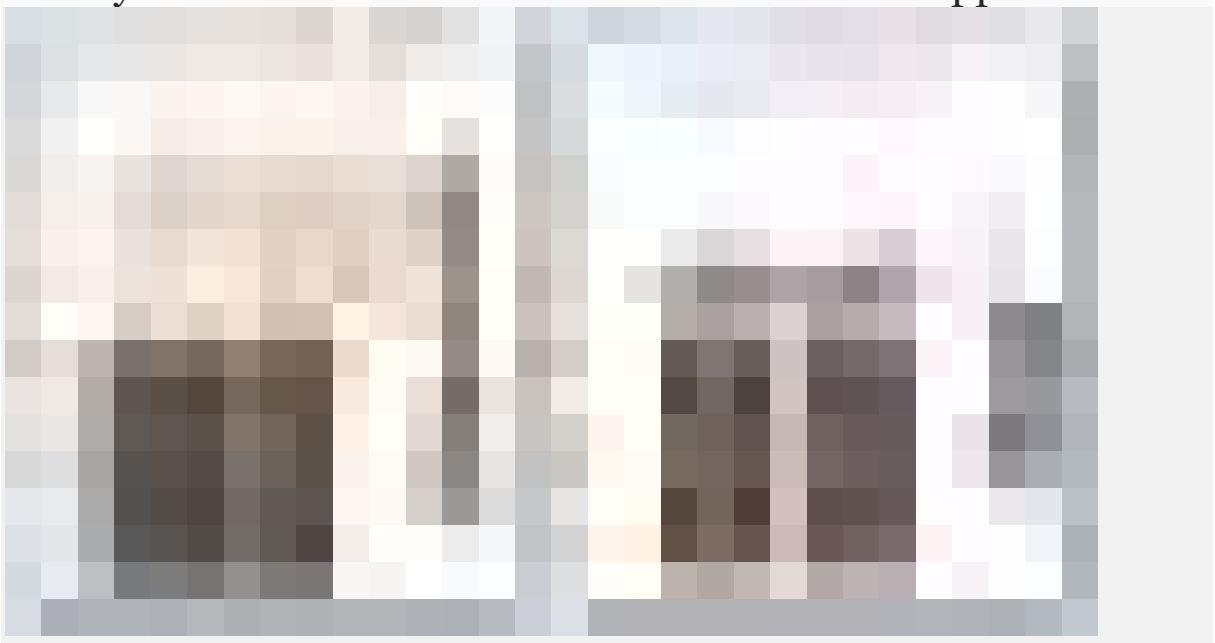
Wireless access point (WAP) is also known as access point (AP). It is a hardware device used in a wireless local area network (WLAN) for data transmitting and receiving. An access point connects users to other users within the network and also serves as the point of interconnection between the WLAN and a fixed wire network. Basically, the working principle of wireless access point is to broadcast a wireless signal that computers can detect, then computers can link to the network without using any wires. ...

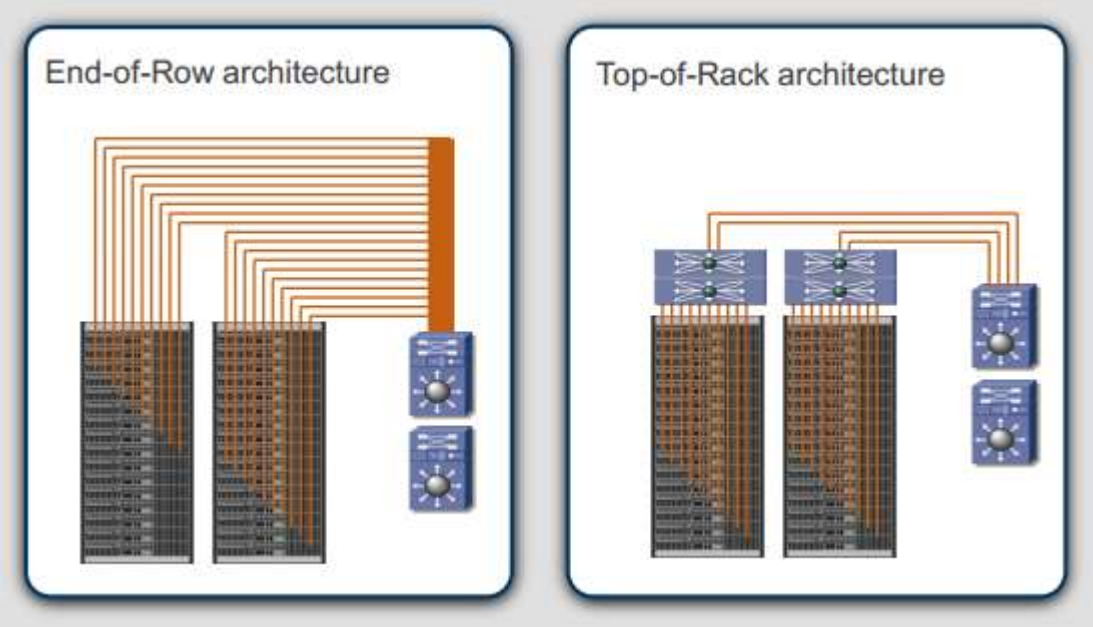
Read more · 3 min read

Jan 12, 2017

Data Center Architecture Designs Comparison: ToR Vs. EoR

The interconnection of switches and warranty of data communication are the basic aspects to consider when designing a data center architecture. Today's data centers have been shifted into 1RU and 2RU appliances, thus setting the 1RU and 2RU **switches** into the same-sized **racks** can greatly save space and reduce cabling demands. Typically, Top of Rack (ToR) and End of Row (EoR) are now the common infrastructure designs for data centers. In this article, we will mainly discuss the differences between these two approaches.





Overview of ToR & EoR

What Is ToR?

ToR approach refers to the physical placement of network access switch in the top of a server rack. Servers are directly linked to the access switch in this method. Each server rack usually has one or two access switches. Then all the access switches are connected with the aggregation switch located in the rack. Only a small amount of cables are needed to run from server rack to aggregation rack. ...

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

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

Ans. 0

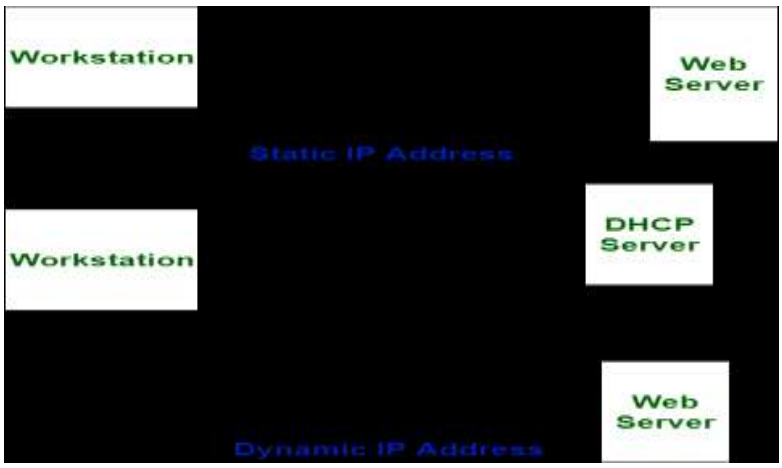
7. In a network that contains two servers and twenty workstations, where is the best place to install an Anti-virus program?

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.

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

Ans. **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
1.	It is provided by ISP(Internet Service	While it is provided by DHCP (Dynamic Host Configuration

S.NO	STATIC IP ADDRESS	DYNAMIC IP ADDRESS
	Provider).	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.

S.NO	STATIC IP ADDRESS	DYNAMIC IP ADDRESS
8.	It is used where computational data is less confidential.	While it is used where data is more confidential and needs more security.

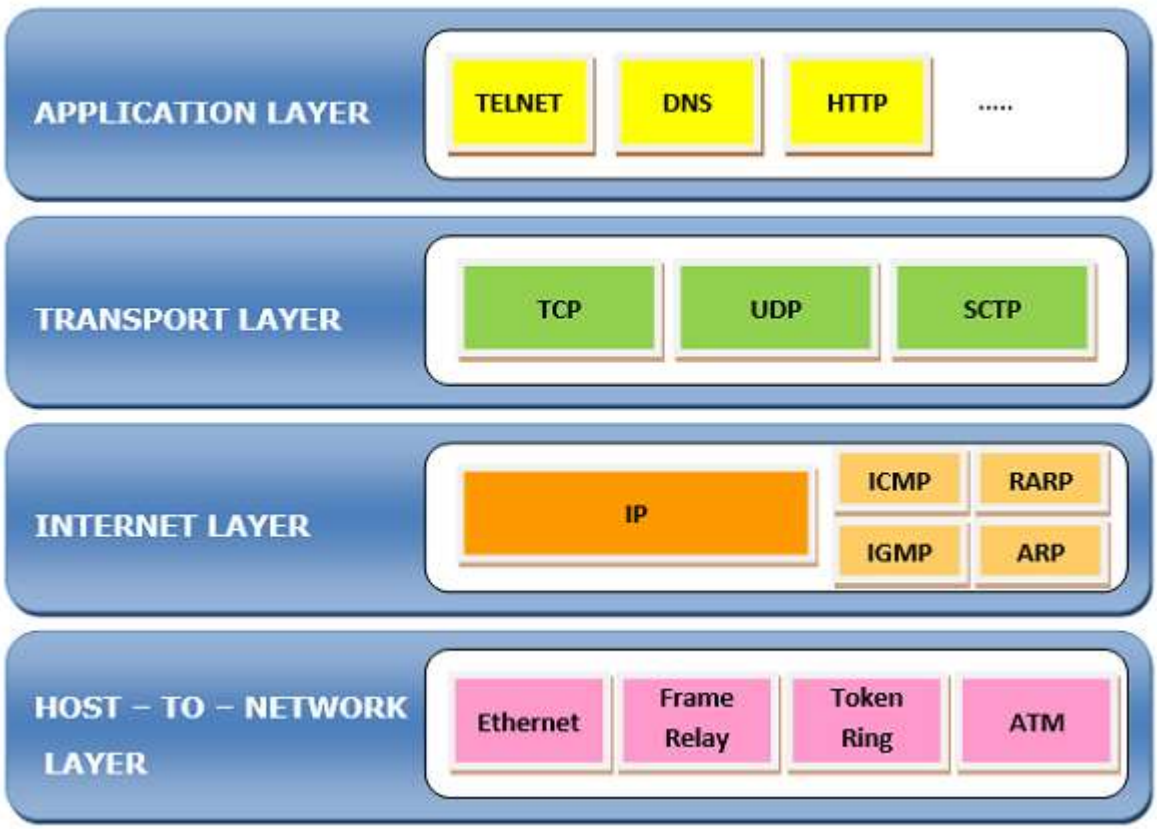
1. Discuss TCP/IP model in detail.

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 −



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

Ans. 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.[1][2] 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.[3]

Web browsers are used on a range of devices, including desktops, laptops, tablets, and smartphones. In 2019, an estimated 4.3 billion people used a browser.[4] The most used browser is Google Chrome, with a 64% global market share on all devices, followed by Safari with 18%.[5] Other notable browsers include Firefox and Microsoft Edge.

Contents

History[edit]

Main article: History of the web browser

The first web browser, called WorldWideWeb, was created in 1990 by Sir Tim Berners-Lee.[6] He then recruited Nicola Pellow to write the Line Mode Browser, which displayed web pages on dumb terminals; it was released in 1991.[7]

Nicola Pellow and Tim Berners-Lee in their office at CERN.

Marc Andreessen, lead developer of Mosaic and Navigator

1993 was a landmark year with the release of Mosaic, credited as "the world's first popular browser".[8] Its innovative graphical interface made the World Wide Web system easy to use and thus more accessible to the average person. This, in turn, sparked the Internet boom of the 1990s, when the Web grew at a very rapid rate.[8] Marc Andreessen, the leader of the Mosaic team, soon started his own company, Netscape, which released the Mosaic-influenced Netscape Navigator in 1994. Navigator quickly became the most popular browser.[9]

Microsoft debuted Internet Explorer in 1995, leading to a browser war with Netscape. Microsoft was able to gain a dominant position for two reasons: it bundled Internet Explorer with its popular Microsoft Windows operating system and did so as freeware with no restrictions on usage. Eventually the market share of Internet Explorer peaked at over 95% in 2002.[10]

WorldWideWeb was the first web browser.

[11]

In 1998, Netscape launched what would become the Mozilla Foundation to create a new browser using the open source software model. This work evolved into Firefox, first released by Mozilla in 2004. Firefox reached a 28% market share in 2011.[12] Apple released its Safari browser in 2003. It remains the dominant browser on Apple platforms, though it did not become popular elsewhere.[12]

Google debuted its Chrome browser in 2008, which steadily took market share from Internet Explorer and became the most popular browser in 2012.[13][14] Chrome has remained dominant ever since.

In 2011, the first version of HTTPS Everywhere was launched, while NoScript got its main awards and Mozilla launched the stable version of Tor Firefox browser, the free add-on to navigate the dark web.[15][16]

Microsoft released its Edge browser in 2015 as part of the Windows 10 release, and rebuilt it as a Chromium-based browser in 2019. (Internet Explorer is still used on older versions of Windows.)

In terms of technology, browsers have greatly expanded their HTML, CSS, JavaScript, and multimedia capabilities since the 1990s. One reason has been to enable more sophisticated websites, such as web applications. Another factor is the significant increase of broadband connectivity, which enables people to access data-intensive web content, such as YouTube streaming, that was not possible during the era of dial-up modems.

Function[edit]

The purpose of a web browser is to fetch information resources from the Web and display them on a user's device.

This process begins when the user inputs a Uniform Resource Locator (URL), such as `https://en.wikipedia.org/`, into the browser. Virtually all URLs on the Web start with either `http:` or `https:` which means the browser will retrieve them with the Hypertext Transfer Protocol (HTTP). In the case of `https:`, the communication between the browser and the web server is encrypted for the purposes of security and privacy.

Once a web page has been retrieved, the browser's rendering engine displays it on the user's device. This includes image and video formats supported by the browser.

Web pages usually contain hyperlinks to other pages and resources. Each link contains a URL, and when it is clicked or tapped, the browser navigates to the new resource. Thus the process of bringing content to the user begins again.

Most browsers use an internal cache of web page resources to improve loading times for subsequent visits to the same page. The cache can store many items, such as large images, so they do not need to be downloaded from the server again.[17] Cached items are usually only stored for as long as the web server stipulates in its HTTP response messages.[18]

Settings[edit]

Web browsers can typically be configured with a built-in menu. Depending on the browser, the menu may be named *Settings*, *Options*, or *Preferences*.

The menu has different types of settings. For example, users can change their home page and default search engine. They also can change default web page colors and fonts. Various network connectivity and privacy settings are also usually available.

Privacy[edit]

During the course of browsing, cookies received from various websites are stored by the browser. Some of them contain login credentials or site preferences.[19] However, others are used for tracking user behavior over long periods of time, so browsers typically provide settings for removing cookies when exiting the browser.[19] Finer-grained management of cookies usually requires a browser extension.[20]

Features[edit]

The most popular browsers have a number of features in common. They allow users to set bookmarks and browse in a private mode. They also can be customized with extensions, and some of them provide a sync service.

Most browsers have these user interface features:

- Allow the user to open multiple pages at the same time, either in different browser windows or in different tabs of the same window.
- *Back* and *forward* buttons to go back to the previous page visited or forward to the next one.
- A *refresh* or *reload* button to reload the current page.
- A *stop* button to cancel loading the page. (In some browsers, the stop button is merged with the reload button.)
- A *home* button to return to the user's home page.
- An address bar to input the URL of a page and display it.
- A search bar to input terms into a search engine. (In some browsers, the search bar is merged with the address bar.)

There are also niche browsers with distinct features. One example is text-only browsers that can benefit people with slow Internet connections or those with visual impairments.

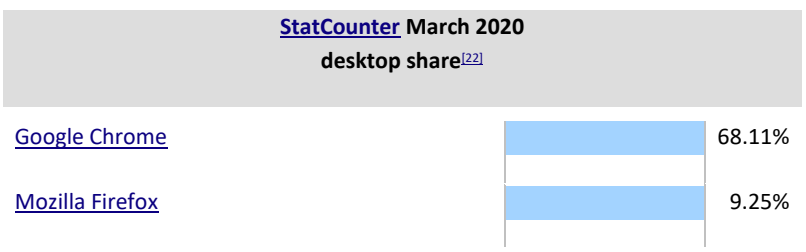
Security[edit]

Main article: Browser security

Web browsers are popular targets for hackers, who exploit security holes to steal information, destroy files, and other malicious activities. Browser vendors regularly patch these security holes, so users are strongly encouraged to keep their browser software updated. Other protection measures are antivirus software and avoiding known-malicious websites.[21]

Market share[edit]

Main article: Usage share of web browsers



Safari	8.93%
Microsoft Edge	5.13%
Internet Explorer	3.77%
Opera	2.37%
360 Secure Browser	0.62%
Yandex Browser	0.46%
Cốc Cốc	0.25%
UC Browser	0.21%
Mozilla Suite	0.20%
QQ browser	0.17%
Chromium	0.14%
Sogou Explorer	0.12%
Naver Whale	0.08%
Maxthon	0.08%
Vivaldi	0.02%
Pale Moon	0.02%
Waterfox	0.01%
Other	0.04%

See also[edit]

- ***Internet portal***

- Mobile browser
- List of web browsers
- Comparison of web browsers

References[edit]

1. ^ *"What is a Browser?". Google (on YouTube). 30 April 2009. Less than 8% of people who were interviewed on this day knew what a browser was.*
2. ^ *"No-Judgment Digital Definitions: Internet, Search Engine, Browser". Mozilla. 11 October 2017. Let's start by breaking down the differences between internet, search engine, and browser. Lots of us get these three things confused with each other.*
3. ^ *"Difference Between Search Engine and Browser".*

4. ^ *"World Internet Users Statistics and 2019 World Population Stats"*. *www.internetworldstats.com. Retrieved 21 April 2019.*
5. ^ *"StatCounter Global Stats"*. *StatCounter. Retrieved 14 June 2020.*
6. ^ *"Tim Berners-Lee: WorldWideWeb, the first Web client"*. *W3.org. Retrieved 7 December2011.*
7. ^ *Gillies, James; Cailliau, R. (2000). How the Web was Born: The Story of the World Wide Web. Oxford University Press. pp. 6. ISBN 0192862073.*
8. ^ Jump up to:[a] [b] *"Bloomberg Game Changers: Marc Andreessen"*. *Bloomberg. 17 March 2011. Retrieved 7 December 2011.*
9. ^ *Enzer, Larry (31 August 2018). "The Evolution of the Web Browsers". Monmouth Web Developers. Retrieved 31 August 2018.*
10. ^ *"Mozilla Firefox Internet Browser Market Share Gains to 7.4%"*. *Search Engine Journal. 24 November 2004. Retrieved 7 December 2011.*
11. ^ *Stewart, William. "Web Browser History". Retrieved 5 May 2009.*
12. ^ Jump up to:[a] [b] *"StatCounter Global Stats – Browser, OS, Search Engine including Mobile Usage Share". Retrieved 2 May 2015.*
13. ^ *"Internet Explorer usage to plummet below 50 percent by mid-2012". 3 September 2011. Retrieved 4 September 2011.*
14. ^ *"StatCounter Global Stats – Browser, OS, Search Engine including Mobile Usage Share". Retrieved 2 May 2015.*
15. ^ *Alan Pearce (24 December 2014). The dark web. Youtube. Brighton: TEDx. Retrieved 23 September 2020.*
16. ^ *Sudhanshu Chauhan; Nutan Kumar Panda (2015). Online Anonymity. Hacking Web Intelligence. doi:10.1016/B978-0-12-801867-5.00008-2.*
17. ^ *"Definition of browser cache". PCmag. Retrieved 19 February 2020.*
18. ^ *Fountis, Yorgos. "How does the browser cache work?". Retrieved 19 February 2020.*
19. ^ Jump up to:[a] [b] *"Tracking Cookies: What They Are, and How They Threaten Your Privacy". Tom's Guide. Retrieved 11 March 2019.*
20. ^ *"Alternatives to Cookie AutoDelete extension". AlternativeTo. Retrieved 11 March 2019.*
21. ^ *"Securing Your Web Browser". www.us-cert.gov. Retrieved 21 April 2019.*
22. ^ *"Desktop Browser Market Share Worldwide". StatCounter.*

11. What is a search engine? Give example.

Ans. 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?

Ans. . 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 be hard to imagine a world without the internet.

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

Ans. List of internet service providers in India

From Wikipedia, the free encyclopedia

Jump to navigationJump to search

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.[1]

Contents

By subscribers[edit]

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.[2]

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	MTNL	170,697	855,744	1,026,441
7	Hathway	0	969,157	969,157
8	Your Broadband	14,660	778,584	793,244
9	GTPL Broadband	0	359,347	359,347

Rank	ISP	Narrowband	Broadband	Total
10	Excitel	0	350,783	350,783

Note:

1. On 28 February 2018 Aircel filed for bankruptcy at NCLT and a substantial number of customers have migrated to other services due to closing down of most of the consumer services.[3][4]
2. The services of Telenor India has been merged with Airtel on 14 May 2018.[5]
3. On 31 August 2018, Vodafone India has been merged with Idea Cellular and renamed as Vodafone Idea Limited.[6]

Other notable ISPs[edit]

ISP	Coverage area
RailTel Corporation of India	State-owned ISP with pan-India optic fiber network along Railway track

Enterprise/wholesale only[edit]

- CtrlS Datacenters Ltd
- GAILTEL
- National Knowledge Network for educational institutions in India
- Tulip Telecom
- PowerGrid
- ERNET

See also[edit]

- List of telecom companies in India
- Internet in India

References[edit]

1. ^ *"The Indian Telecom Services Performance Indicators October — December, 2019" (PDF). TRAI. Retrieved 6 June 2019.*
2. ^ *"The Indian Telecom Services Performance Indicators January – March, 2020" (PDF). Telecom Regulatory Authority of India. 17 September 2020.*
3. ^ *Sengupta, Devina (28 February 2018). "Aircel, country's last small mobile phone operator, files for bankruptcy". The Economic Times. Retrieved 28 February 2018.*
4. ^ *"Aircel's bankruptcy note on Facebook".*
5. ^ *Gulveen Aulakh. "DoT approves Bharti Airtel and Telenor India merger". The Economic Times.*
6. ^ *Parbat, Kalyan (31 August 2018). "NCLT gives go-ahead to Idea-Vodafone merger". The Economic Times.*

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

Ans. Both MAC Address and IP Address are used to uniquely identify a machine on the internet. MAC address is provided by the chip maker while IP Address is provided by the Internet Service Provider.

Following are the important differences between MAC Address and IP Address.

Sr. No.	Key	MAC Address	IP Address
1	Definition	MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.
2	Usage	MAC Address ensure that physical address of the computer is unique.	IP Address is a logical address of the computer and is used to uniquely locate computer connected via a network.
3	Format	MAC Address is of six byte hexadecimal address.	IP Address is of 4 bytes or of 16 bytes.
4	Access Protocol	MAC Address can be retrieved using ARP protocol.	IP Address can be retrieved using RARP protocol.
5	Provider	Chip maker manufacturer provides the MAC Address.	Internet Service Provider, ISP provides the IP Address.

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

Ans.

How to find your web history and how to delete it

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

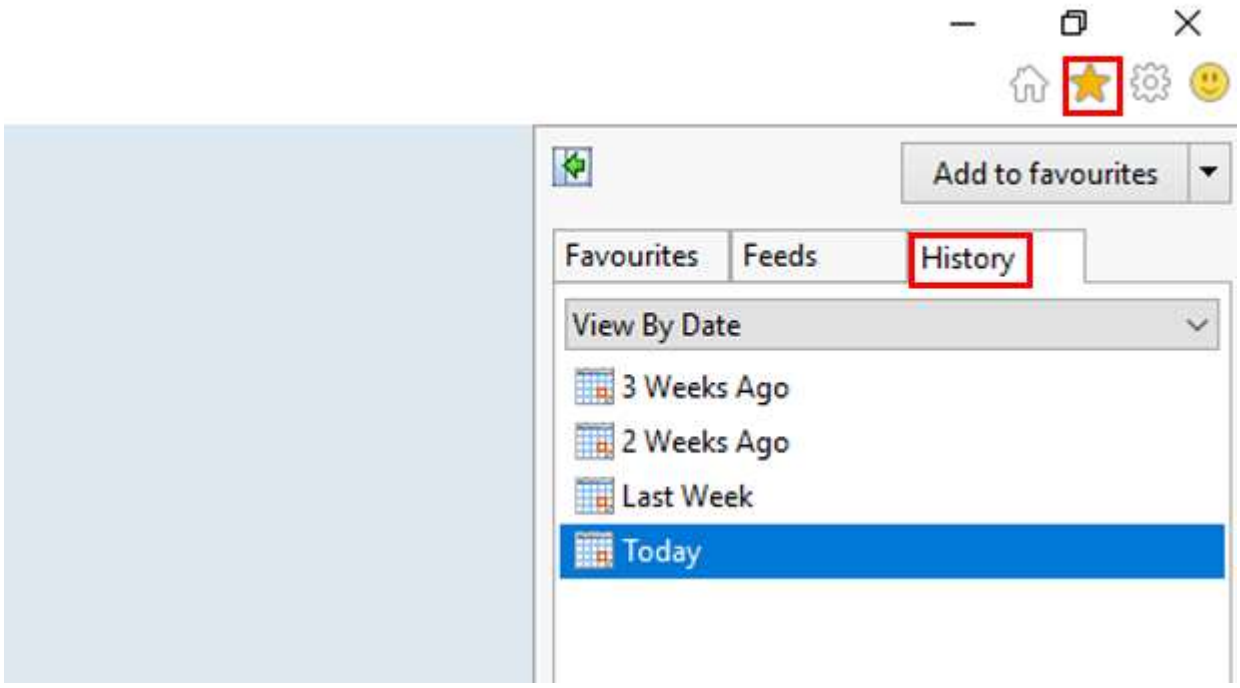
Finding a particular web page long after you last visited it can be a tricky business unless you bookmarked it or can track it down with a search engine.

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]

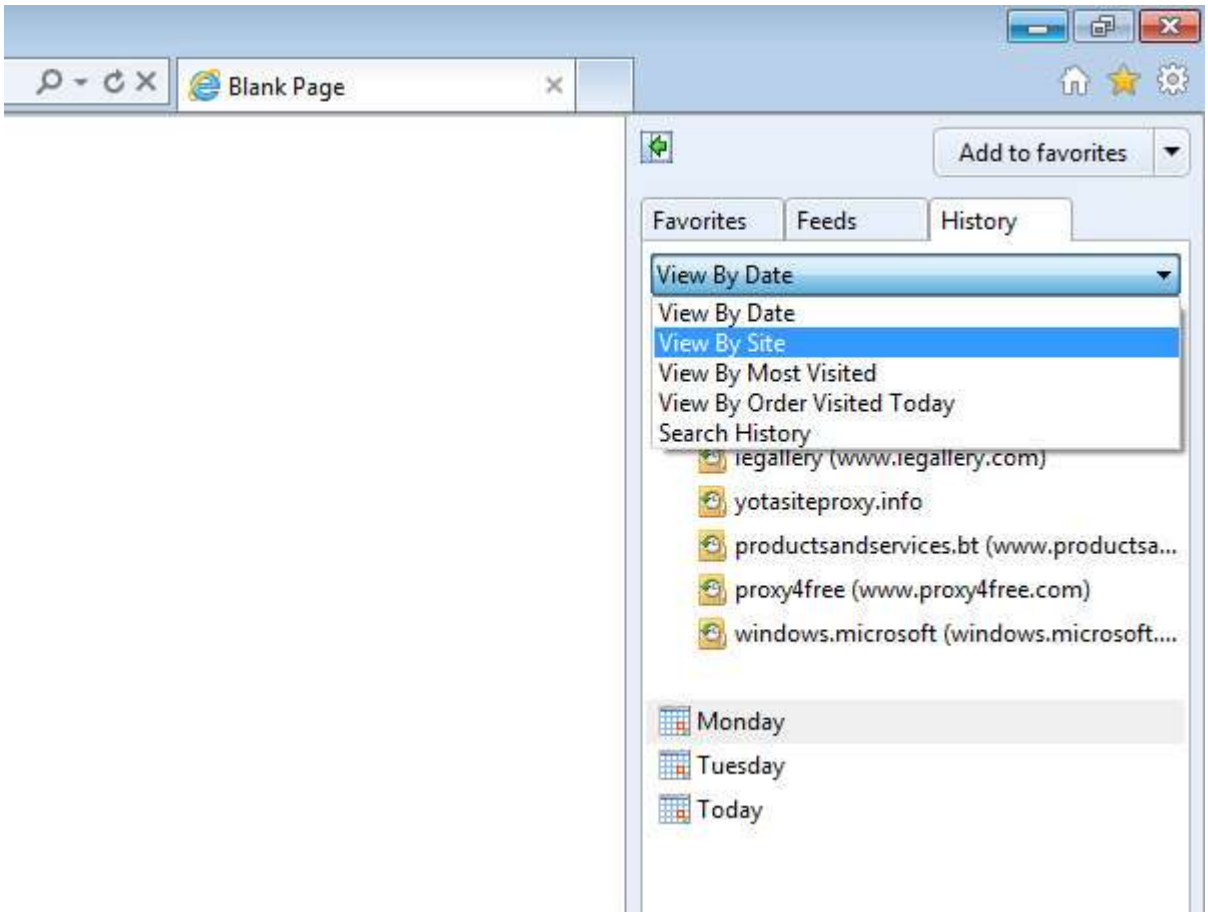
View and delete in Internet Explorer

Step 1: Open the History menu



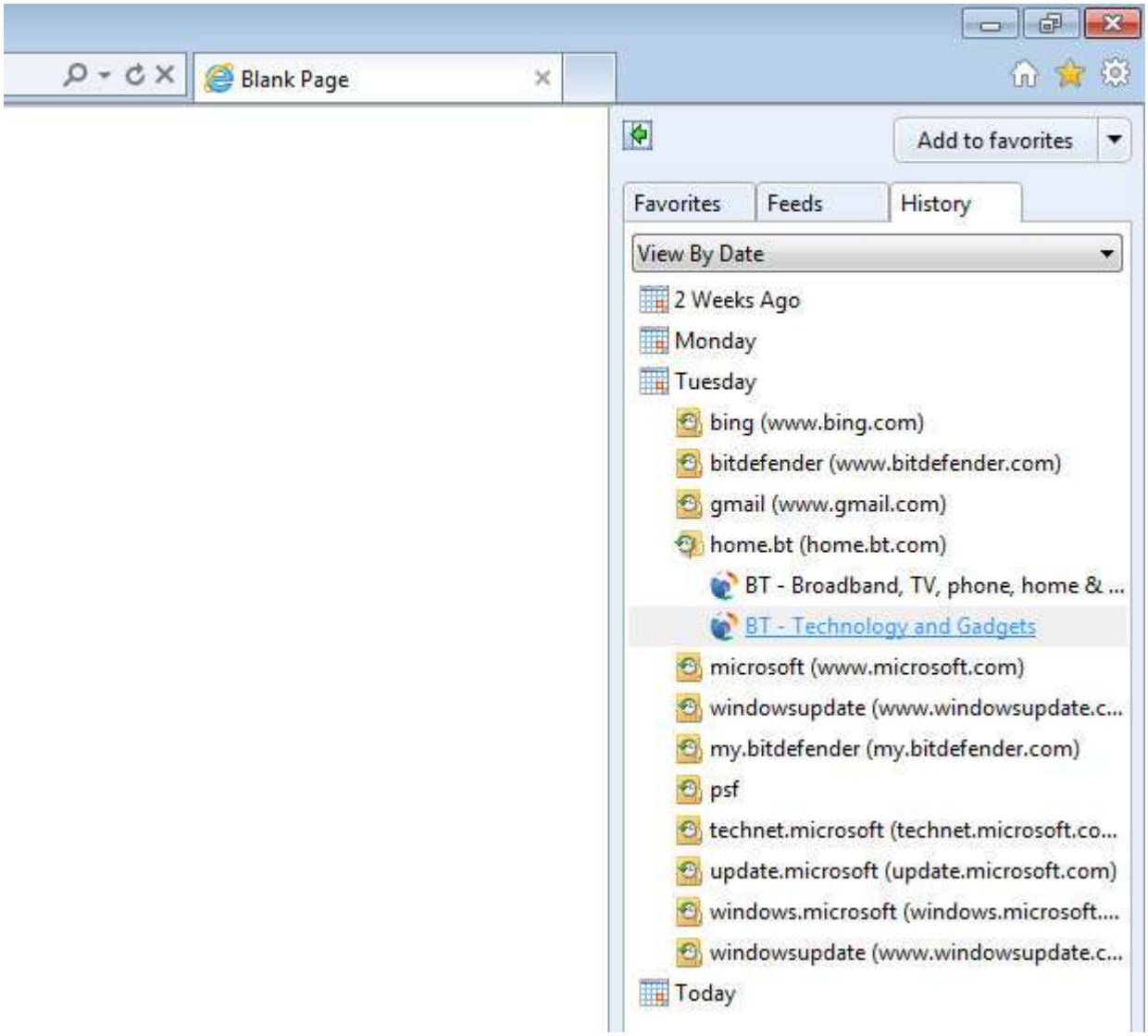
In Internet Explorer 11, click the **star** icon at the top-right of the window.

Step 2: Search and sort Internet Explorer History



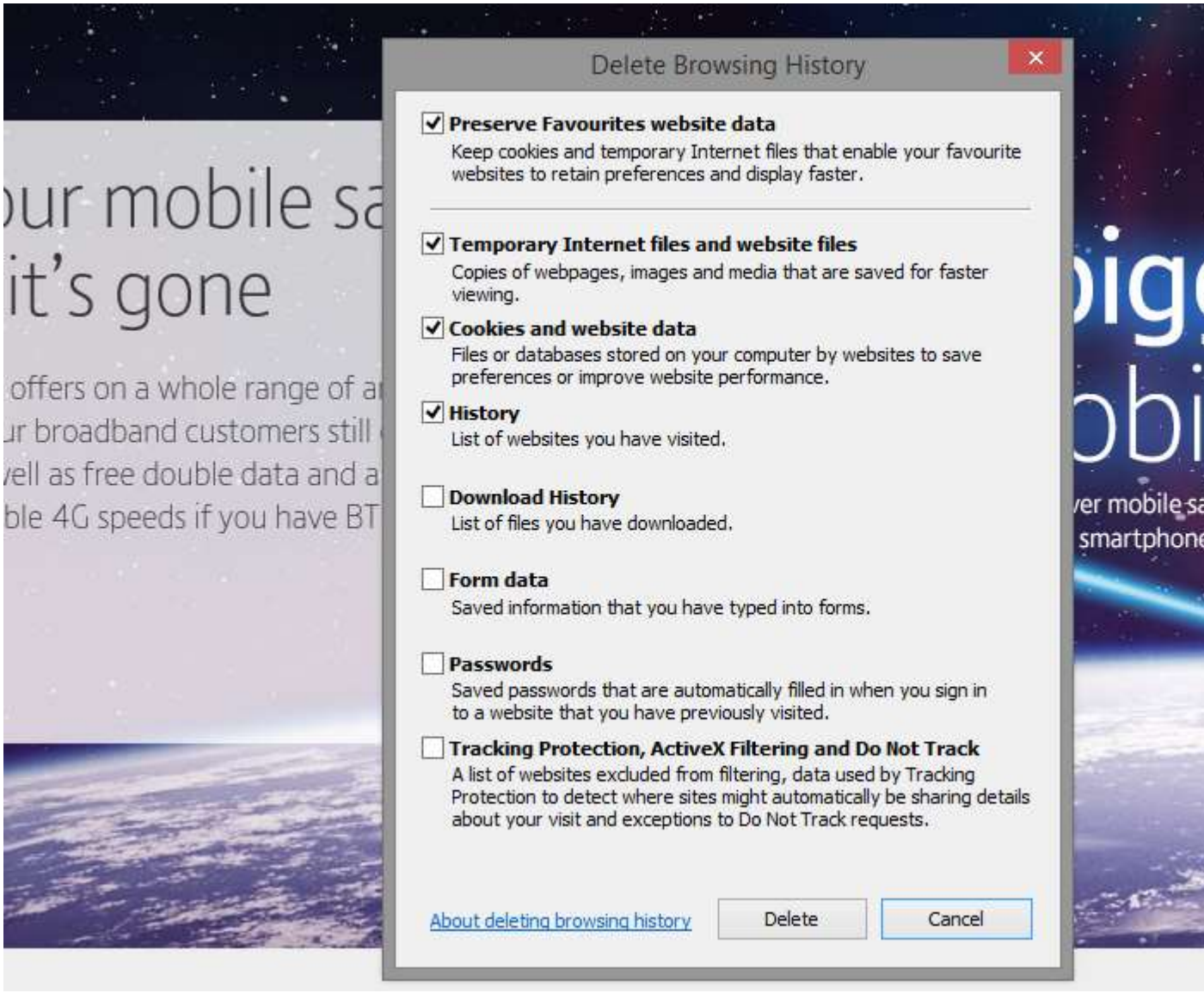
When the dialog box opens, click the **History** tab to view the web pages you've visited previously, ordered by date. There's also a drop-down list so you can view the pages by **Site, Name, Most Visited** and **Order Visited Today**, plus a **Search History** option for when it's quicker to find a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

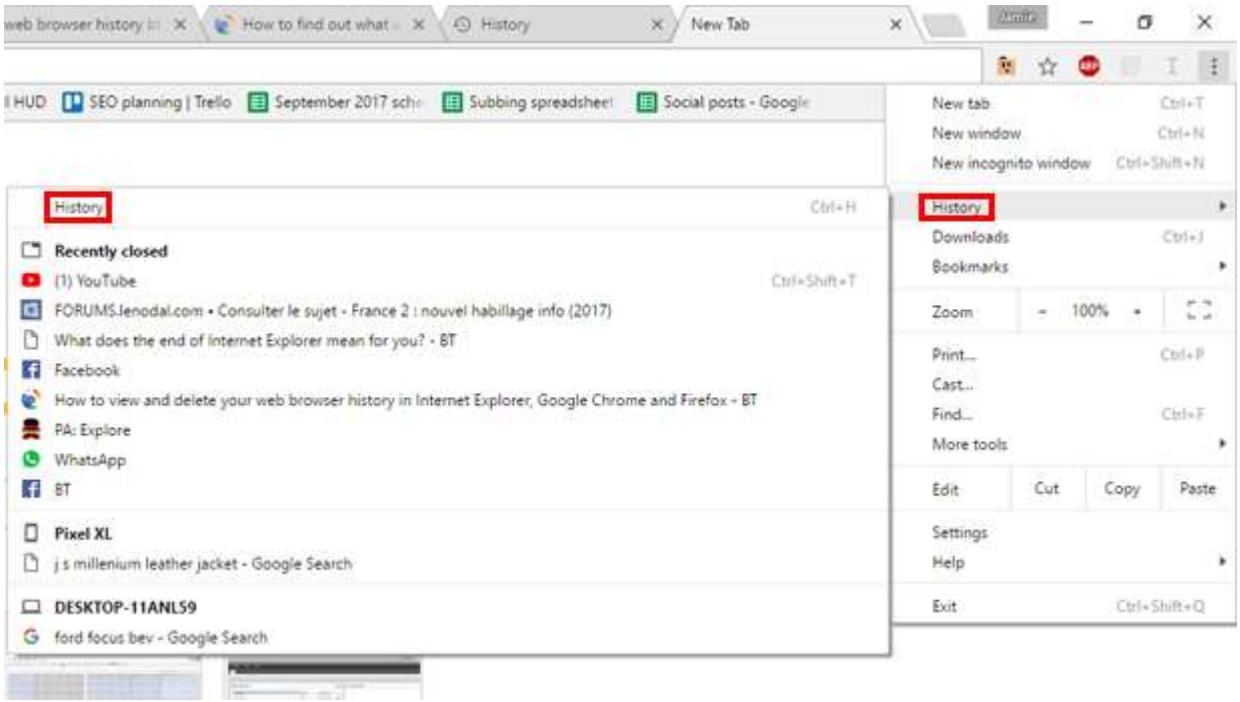
Alternatively, from the **cog**, click on **Safety**, then **Delete Browsing History**, or press **Ctrl+Shift+Delete** on your keyboard.

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.**

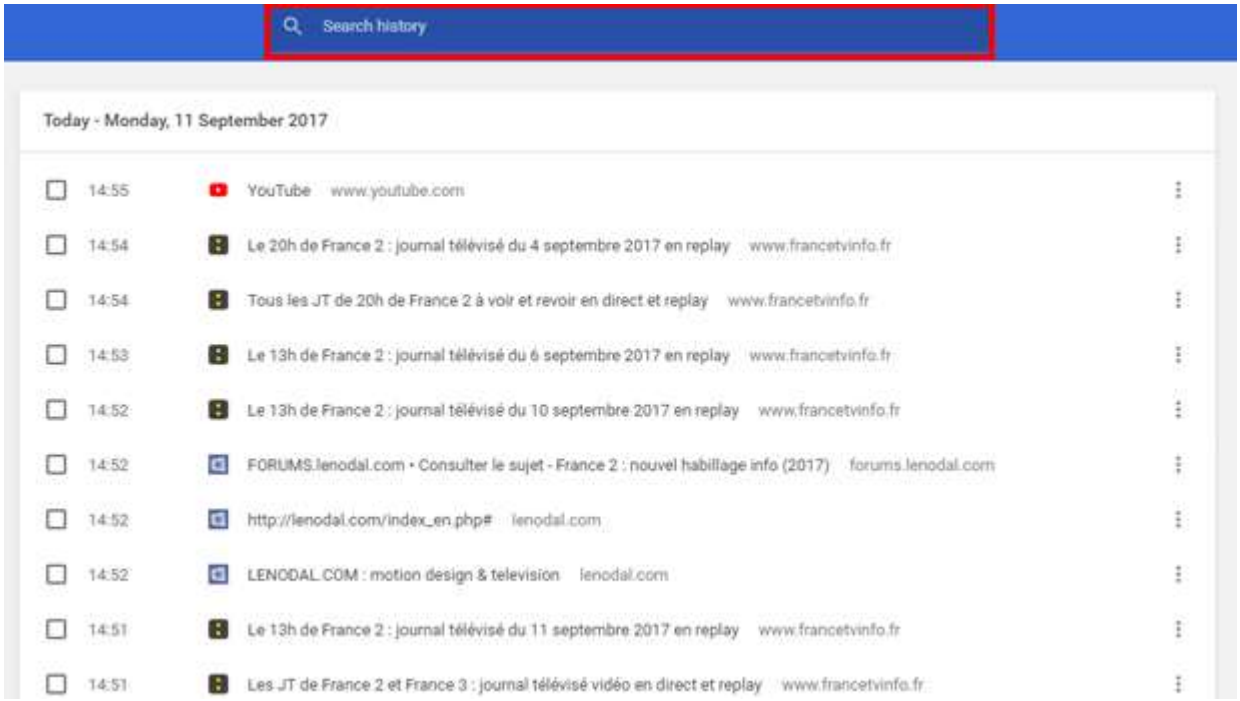
View and delete browsing history in Google Chrome

Step 1: Open the History menu



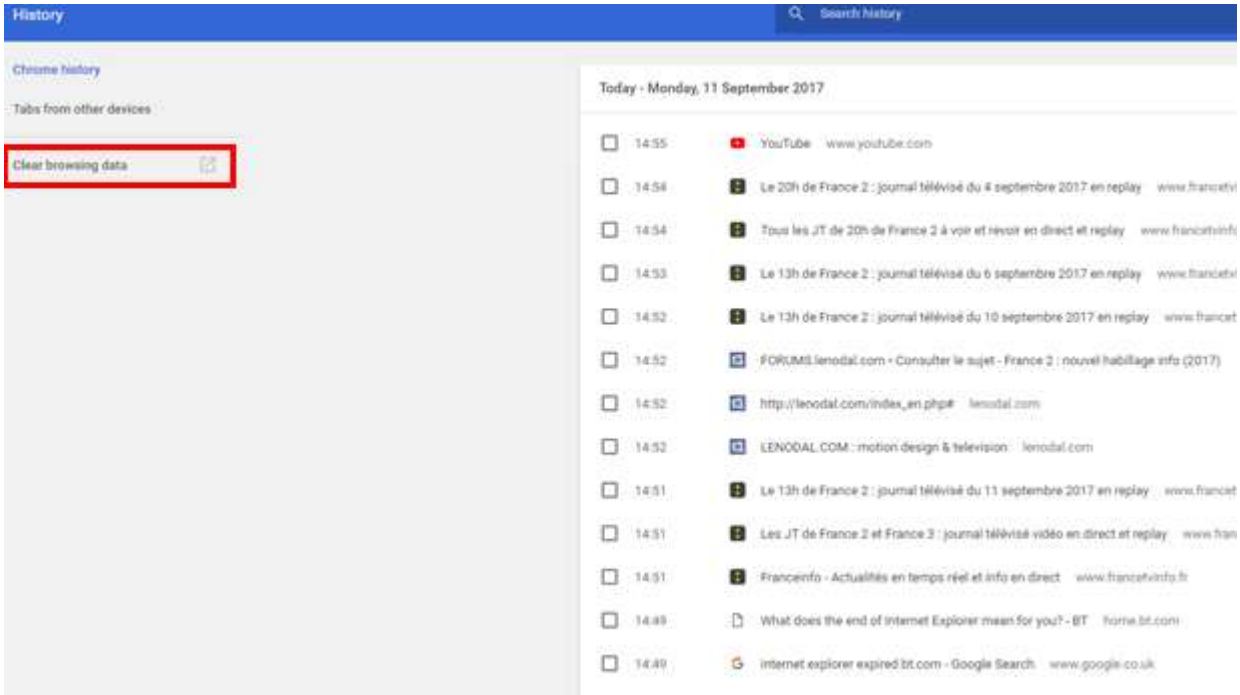
To view the web history in Google Chrome, click to open the menu ⋮ at the top-right of its window and select **History**, then click **History** a second time. Or press **Ctrl+H** on your keyboard.

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



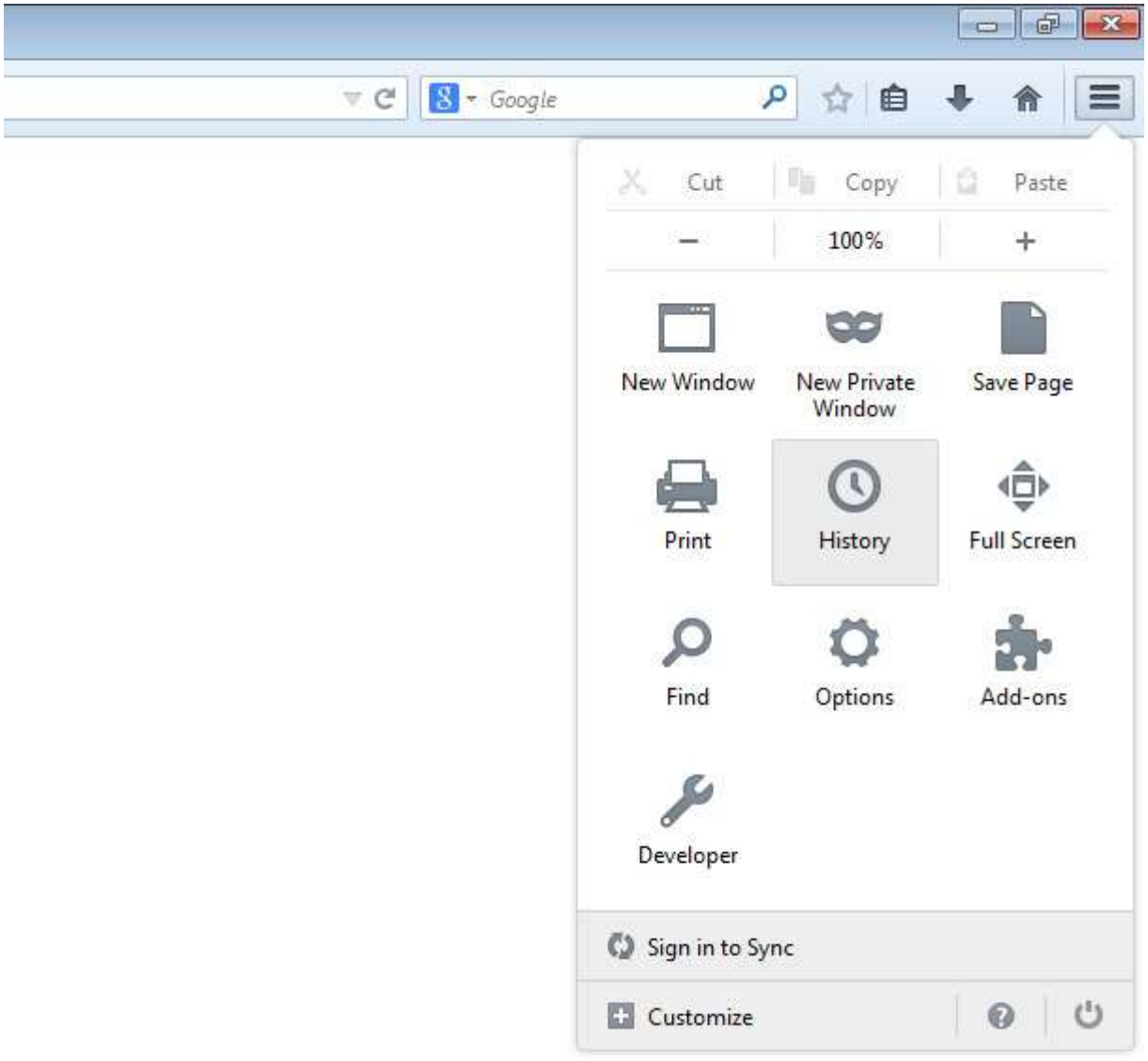
To clear the browsing history, click the **Clear browsing data** button to the left.

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]

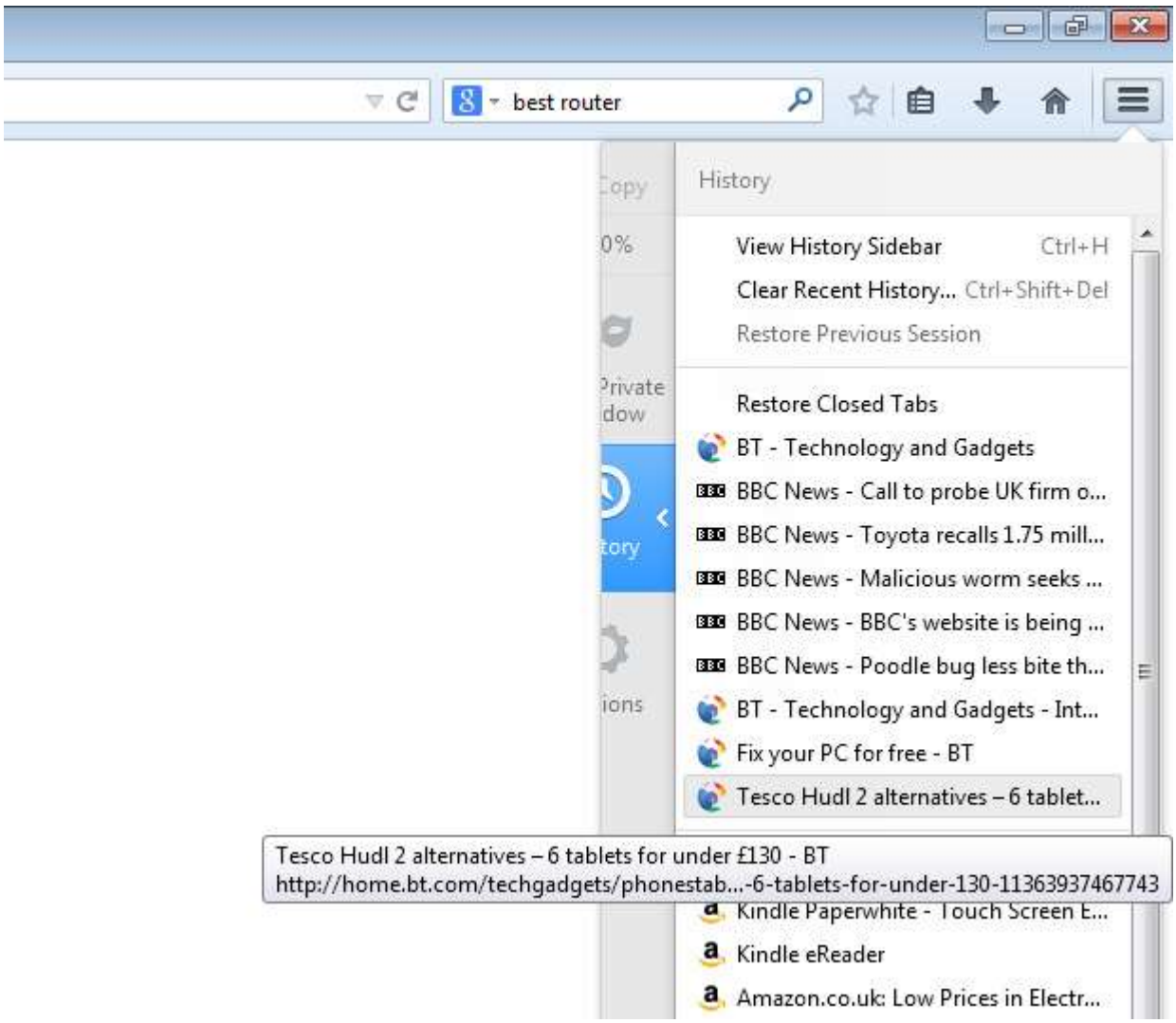
View and delete browsing history in Mozilla Firefox

Step 1: Open the History menu

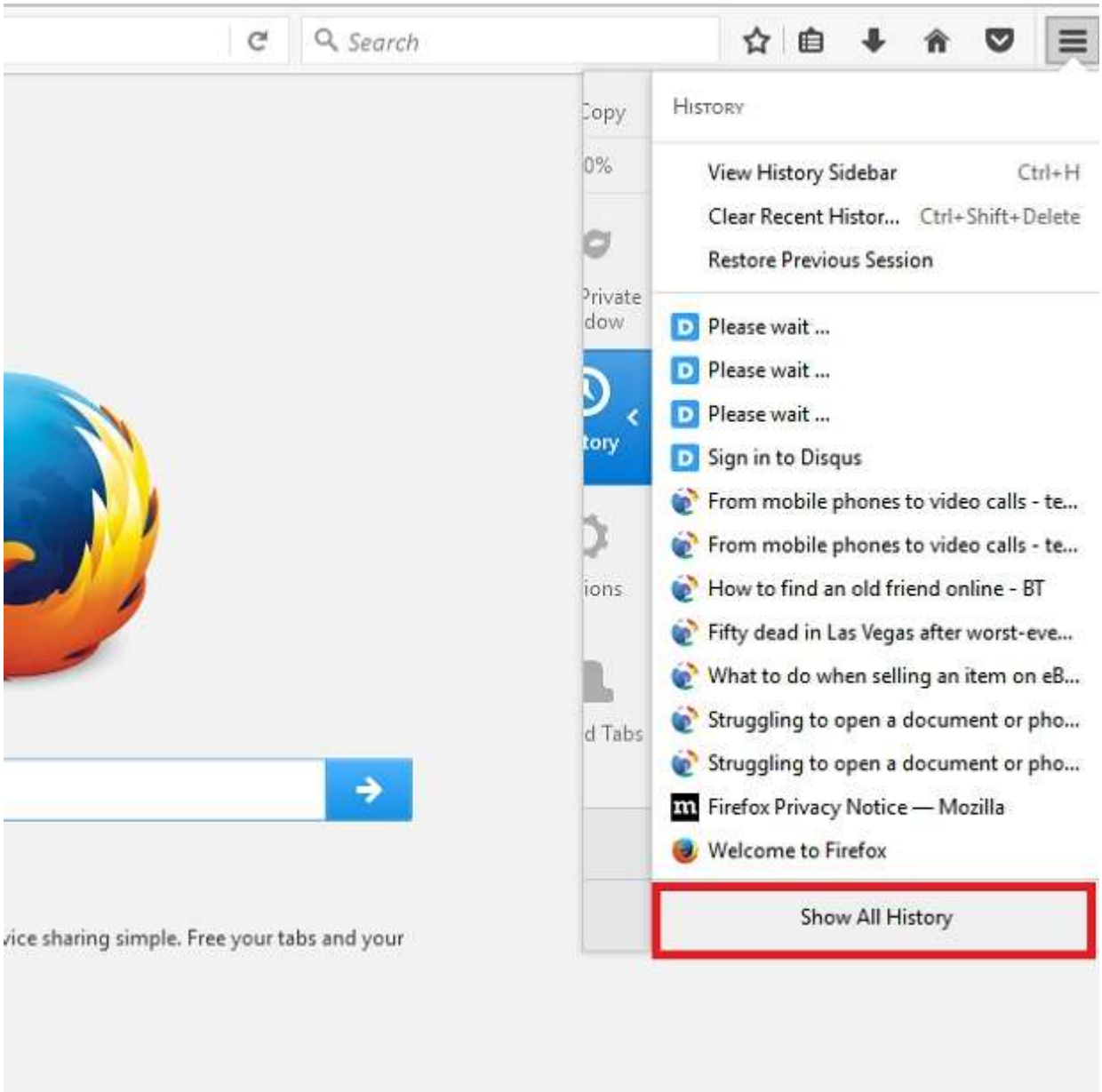


In Mozilla Firefox, you view the web history by clicking the **Menu** button at the top-right of its window and selecting **History.**

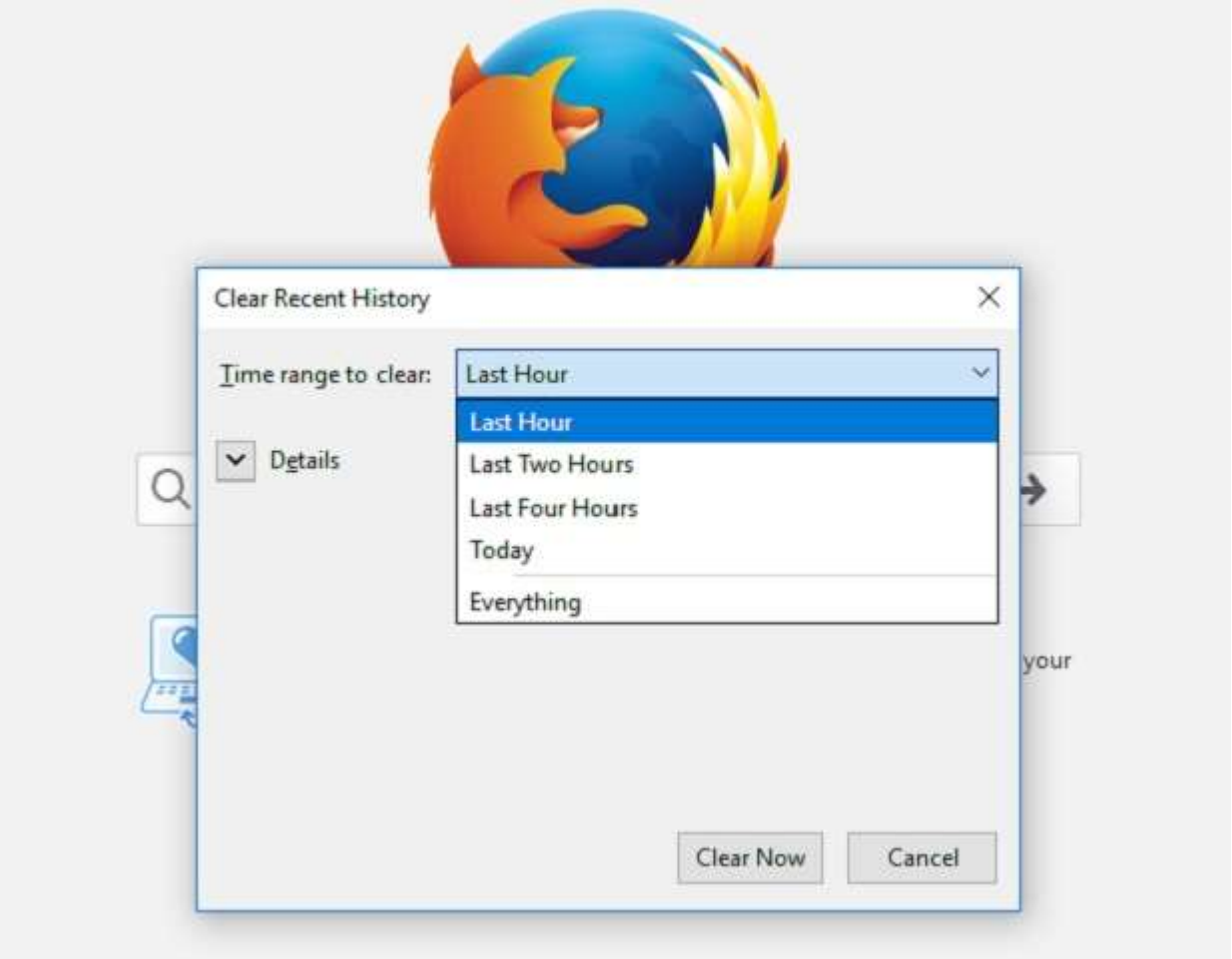
Step 2: Search your History



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**.