# 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, click here.

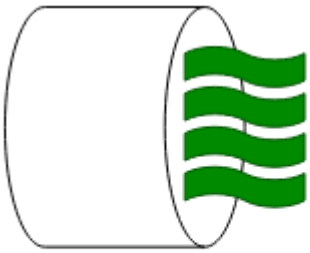
Previous Post*How Edge Data Centers Satisfy Data-Hungry Consumers*
Next Post*HPDs (Health Product Declarations) Explained*

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

Ans. # Difference between Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP) cables

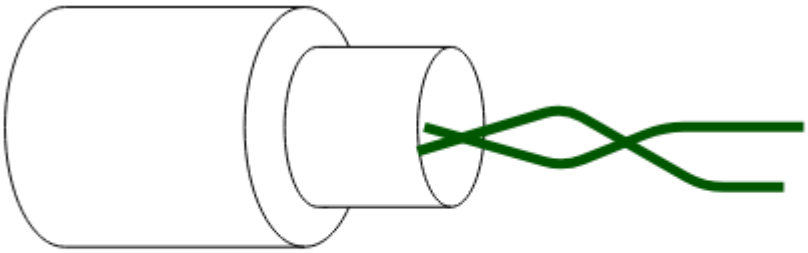
- Last Updated : 21 May, 2020

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



**Unshielded Twisted Pair**

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



Shielded Twisted Pair

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

| S.NO | UTP | STP |
|---|---|---|
| 1. | UTP stands for Unshielded twisted pair. | STP stands for Shielded twisted pair. |
| 2. | In UTP grounding cable is not necessary. | While in STP grounding cable is required. |
| 3. | Data rate in UTP is slow compared to STP. | Data rate in STP is high. |
| 4. | The cost of UTP is less. | While STP is costlier than UTP. |
| 5. | In UTP much more maintenance are not needed. | While in STP much more maintenance are needed. |
| 6. | In UTP noise is high compared to STP. | While in STP noise is less. |
| 7. | In UTP the generation of crosstalk is also high compared to STP. | While in STP generation of crosstalk is also less. |
| 8. | In UTP, attenuation is high in comparison to STP. | While in STP attenuation is low. |



3. 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.

**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. Do You Know the Difference Between Hub, Switch & Router?

*Orenda*

*Feb 15, 2017·3 min read*

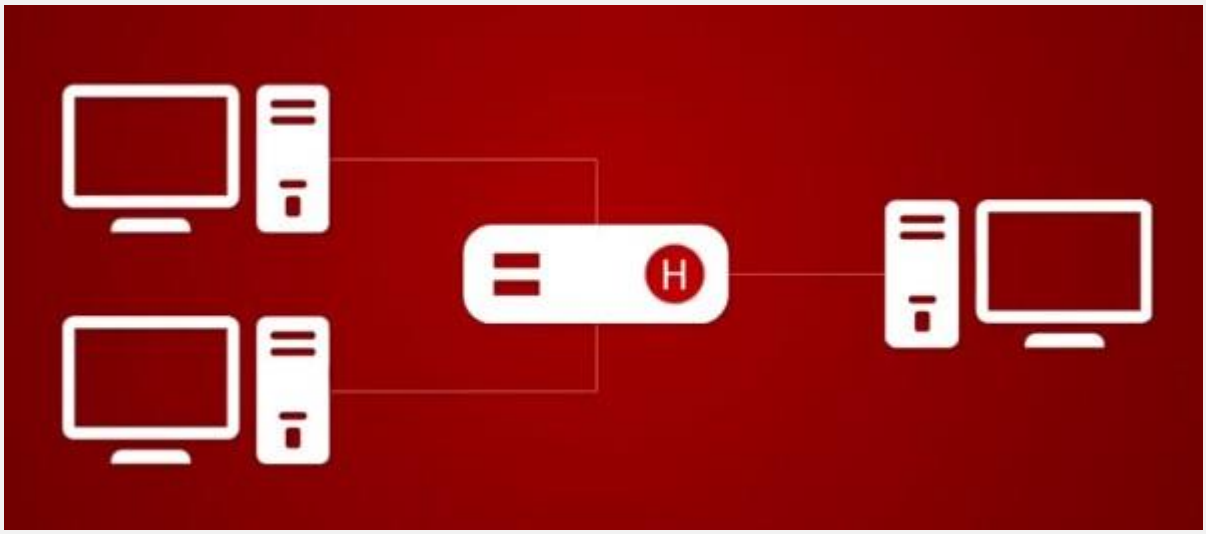
When computers, network devices or other networks are required to be connected, hubs, **switches** and routers are the bridges to link them together. All the three types of devices can perform the same function, and technicians sometimes may use the terms interchangeably. However, this will make people 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

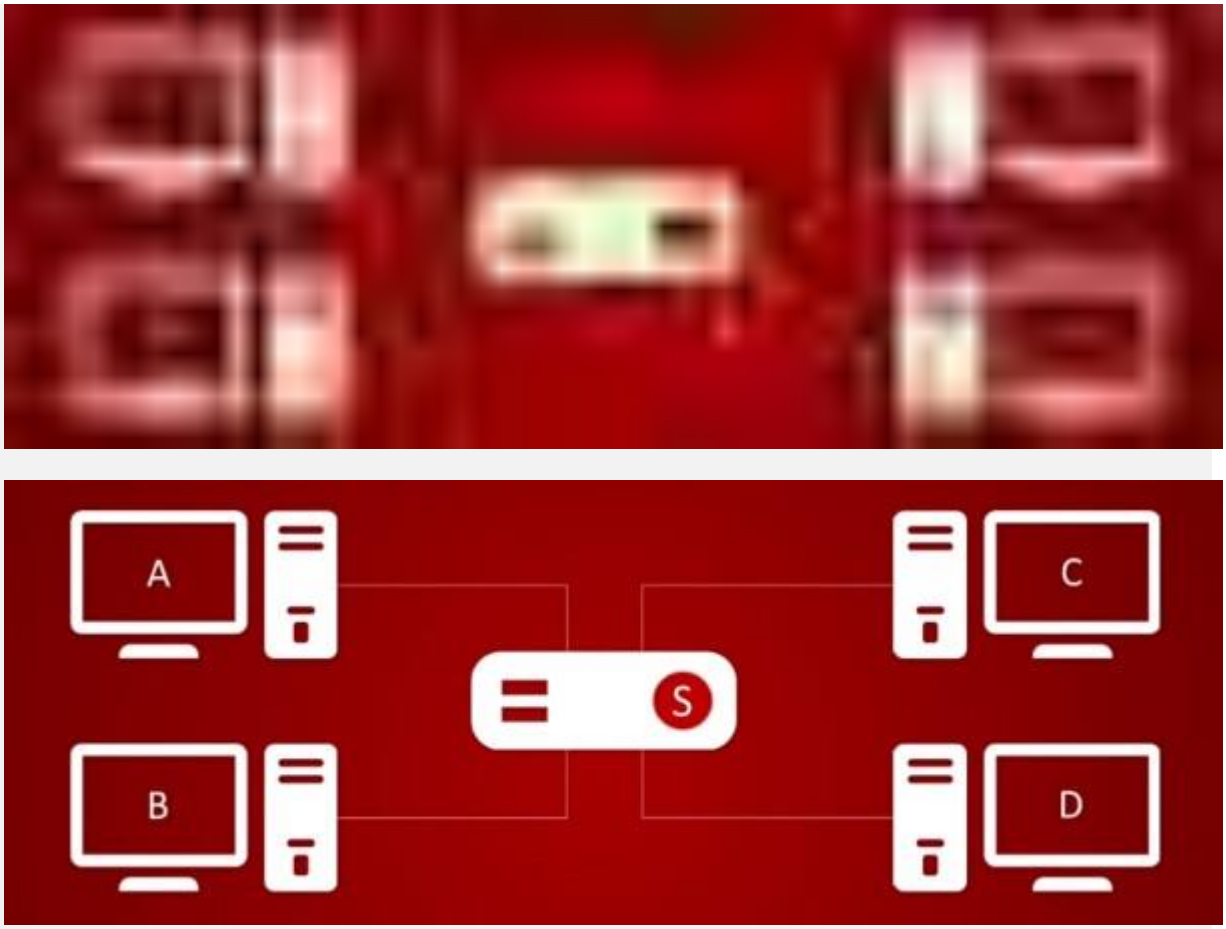
A hub is to sent out a message from one port to other ports. For example, if there are three computers of A, B, C, the message sent by a hub for computer A will also come to the other

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.



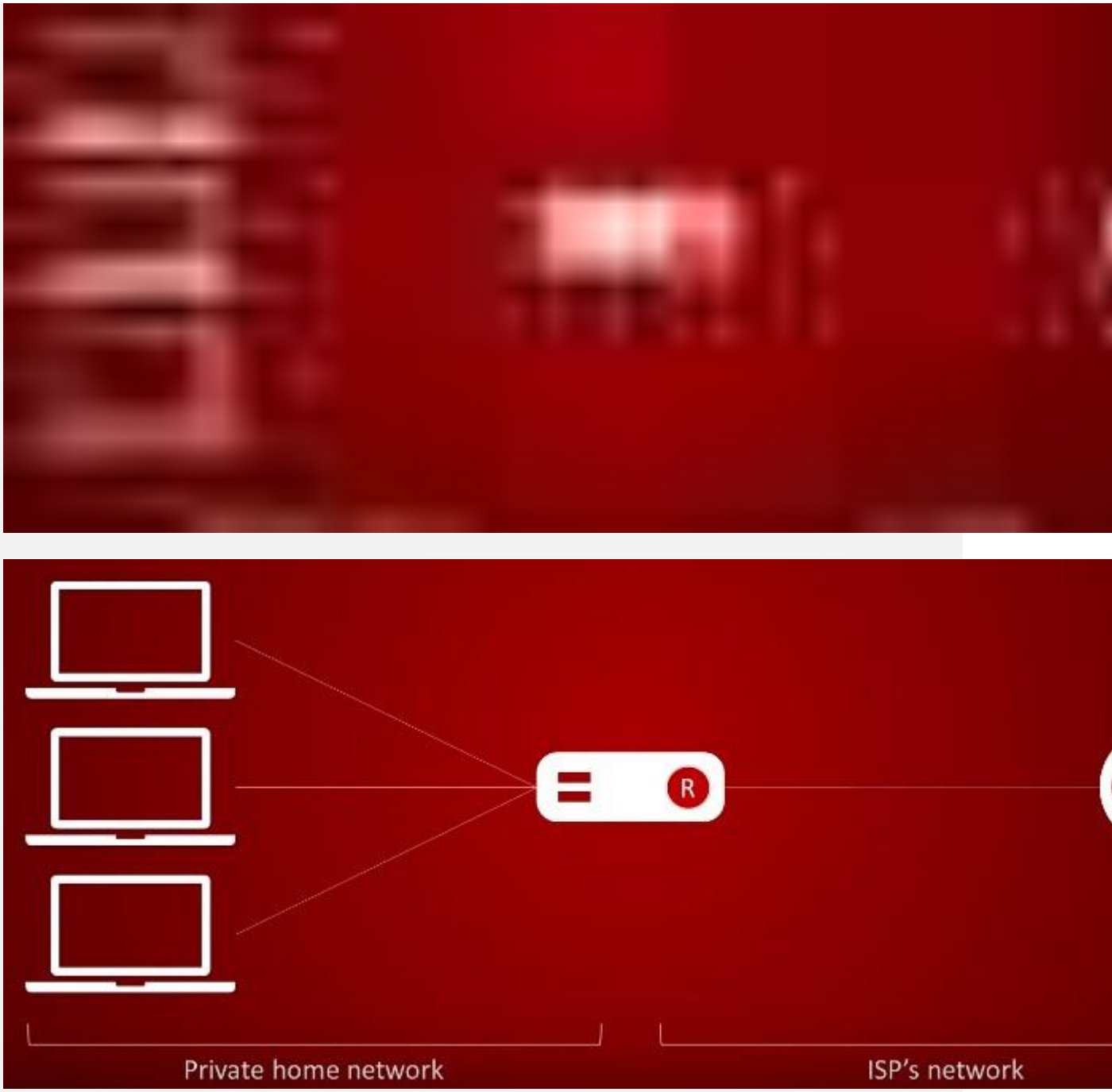

**Switch**

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.

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

Ans. Yes, that's because MAC addresses are hard-wired into the NIC circuitry, not the PC. This also means that a PC can have a different MAC address when the NIC card was replace by another one

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

Ans. A large percentage of a network is made up of hardware. Problems in these areas can range from malfunctioning hard drives, broken NICs and even hardware startups. Incorrectly hardware configuration is also one of those culprits to look into

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

Ans. An anti-virus program must be installed on all servers and workstations to ensure protection.
That's because individual users can access any workstation and introduce a computer virus when plugging in their removable hard drives or flash drives.

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

## Ans. IPv4 Definition

IP addresses operate in the same way as street addresses laid out on a map. They direct packets to their intended destinations.

IP controls all internet traffic. Data packets with the IP information of their points of origin and their destinations travel on the internet, with routers helping to direct them down the correct path.

IP is the other half of TCP/IP, or the so-called Internet Protocol Suite. TCP, Transmission Control Protocol, governs the transport layer while IP is concerned with the network layer. TCP/IP was developed by the Defense Advanced Research Projects Agency (DARPA), a US federal agency under the Department of Defense. It became the computer networking standard for the US military in 1982. Soon after, it became the primary standard for packet-switching networks like the internet.

IPv4 is a connectionless protocol operating on a best-effort delivery model, which means it does not guarantee delivery nor can it avoid duplicates. TCP sits atop IP and addresses these shortcomings through mechanisms such as data integrity checking.

IPv4 became the main protocol governing data packet transmissions in 1981. During the definition of the standard, the version numbers progressed rapidly, starting with version 1 until IPv4 became the one that was utilized in ARPANET, the forerunner of the internet, in 1983.

Originally, IP addresses were designed to support only a low number of networks. By the time IPv4 was rolled out in 1981, it had been divided into address classes in a classful network addressing architecture to cope with this limitation. This architecture was superseded in 1993 when Classless Inter-Domain Routing (CIDR) was introduced to slow both IPv4 address exhaustion and the rapid growth of routing tables across the internet.

IPv4 addresses are numeric and formatted using dotted decimal notation, or four decimal octets separated by dots, e.g., 172.217.31.238. Since an octet is eight bits in length, with the four octets, each IPv4 address is 32-bits, or four bytes, long.

At 232 IP addresses, the number of IPv4 addresses total almost 4.3 billion. The number goes down to around four billion if some 300 million addresses reserved for multicast and private networks are excluded. Network address translation (NAT) is used to allow IP addresses reserved for private networks to communicate over the internet.

It was originally thought that IPv4 could provide IP addresses for all devices on the internet but it soon became apparent that a more robust alternative was needed to meet future demand, even if IPv4 addresses could be reused. With the number of devices accessing the internet already numbering in the billions, especially since smartphones and the Internet of Things (IoT) have become ubiquitous, almost all IPv4 addresses have been assigned—enter IPv6.

# IPv6 Definition

As internet use took off in the 1990s, the Internet Engineering Task Force (IETF), the open standards body in charge of defining technical internet protocols, became aware of a potential problem in IPv4: The number of available IP addresses it can

generate is limited and will not be enough to assign to devices accessing the internet in the foreseeable future.

The IETF decided that a better standard for future-proof IP addressing was needed. By 1998, it had come up with a draft standard for the better and improved IPv6, which was intended to supersede IPv4 eventually.

IPv6 provides for a 128-bit IP address. This means that it allows the generation of 2^128 or approximately 3.4 × 10^38 addresses. In layman's terms, the number of IPv6 addresses can be trillions of trillions.

Since IPv6 also reserves blocks of numbers for special use or excludes some numbers from use altogether, the actual number of IPv6 addresses should be slightly less, just like in IPv4. Still, the number of IPv6 addresses is virtually limitless and should be enough to meet future demand.

While IPv6 conforms to the same design principles as IPv4, IPv6 addresses come in eight groups of four hexadecimal digits, with each separated by colons such as fe80:0000:0000:0350:9804:1781:4371:2d03. The majority of IPv6 addresses don't occupy all their 128 bits, leading to fields that contain only zeros or gets padded with zeros.

With IPv6 addressing architecture, you can use the two-colons (::)to represent a contiguous 16-bit field of zeros. For example, you can collapse fe80:0000:0000:0350:9804:1781:4371:2d03 into fe80::0350:9804:1781:4371:2d03 to make it more readable.

# IPv4 and IPv6 Differences

| **Feature** | **IPv4** |
|---|---|
| Size of the address | 32 bits |
| Addressing method | IPv4 is a numeric address. It uses a dotted notation to separate the binary octets. |
| Number of classes | There are five classes, A to E. |
| Type of addresses | Unicast, multicast, broadcast |
| Number of header fields | 12 |

| | |
|---|---|
| Length of header filed | 20 |
| Checksum fields | Has checksum fields |
| Packet size | The minimum packet size for an IPv4 is 576 bytes. |
| Mapping | IPv4 uses the address resolution protocol (ARP) to map ar IP address to the media access control (MAC) address. |
| Dynamic host configuration server (DHCS) | Clients request the DHCSs' for IP addresses before connecting to the network. |
| Simple network management protocol (SNMP) | IPv4 uses SNMP for system management. |
| Compatibility with mobile devices | IPv4 uses a dot-decimal notation, which is not appropriate for mobile networks. |
| Local subnet group management | IPv4 uses the internet group management protocol (GMP) |
| Interoperability and mobility | It limits network topologies, therefore, hindering interoperability and mobility. |
| Subnet mask | The designated network uses the subnet mask from the ho portion. |
| Routing information protocol (RIP) | IPv4 supports RIP |
| Address features | IPv4 uses the network address translation (NAT) that allow a single address to mask multiple non-routable addresses. |
| Security | Security depends on the applications. |

| Optional fields | Has optional fields |
| --- | --- |

The most significant difference between IPv4 and IPv6 is the virtually limitless number of IP addresses allowed in the latter. When IPv4 came out, mobile devices were not yet common. Thus, IPv4 was built without mobile networks and IoT-enabled devices in mind. When these devices go online and connect to the internet, they go through indirectly, via NAT. This process can sometimes pose problems for IPv4 devices.

With mobile device internet access now the standard, shifting to IPv6 is imperative, as it allows for more streamlined communications between devices. It is not surprising that mobile networks lead in the adoption of IPv6, given the advantages it offers them. IPv6 allows a single device to have multiple IP addresses depending on how that device is used. Instead of going through NAT, each device connects directly to the internet using its own assigned IP address.

When IPv4 came out, network security was not yet anyone's foremost concern. However, IPv4's updates allow it to be configured with the same IP security standards as IPv6. Although IPv6 is designed to be more secure with its built-in encryption capabilities and packet integrity checking, IPv4 can also be made more secure so there is essentially no difference between them when it comes to Internet Protocol security (IPsec).

However, IPv4 requires Address Resolution Protocol (ARP) to map to a device's physical, or media access control (MAC), address. ARP is prone to spoofing and can be a vector for man-in-the-middle or denial-of-service attacks on a network. Although this risk can be mitigated by using software designed to prevent such attacks, it nevertheless poses a problem.

To map to a device's MAC address, IPv6 uses the more robust Neighbor Discovery Protocol (NDP) and its related extensions, including Secure Neighbor Discovery Protocol (SEND), a security extension that provides cryptographic addresses and a public key infrastructure (PKI) separate from the IPsec inherent in IPv6. Thus, despite IP security presence in IPv4, there remains a difference between IPv4 and IPv6, security-wise.

As for device configuration, IPv4 may either require extensive manual configuration or assisted configuration using Dynamic Host Configuration Protocol (DHCP). In contrast, autoconfiguration is available for each device with an IPv6 address. Again, IPv6 wins hands down when it comes to device configuration.

Since it has matured and improved through the years, IPv4 performs at speeds up to par with IPv6, which is theoretically faster since it does not require NAT. However, IPv6 network performance should surpass IPv4 networks soon, as network administrators become more adept in optimizing them like they have learned to tune IPv4 networks.

# IPv6 Pros and Cons

The danger of eventually running out of IP addresses has passed because of IPv6. However, the larger number of addresses in IPv6 is not the only advantage it has over IPv4.

For one, hierarchical address allocation in IPv6 addresses the increasingly complex routing tables in IPv4, an issue that had been addressed previously through CIDR. IPv6 addressing is straightforward and does not pose a problem for routers. With IPv6, CIDR is no longer essential, though you can still use it for router configuration.

Moreover, IPv6 has a new packet format that is designed to undergo minimal router processing. Thus, IPv6 should make for easier network management, more efficient routing and better device mobility. However, since the packet format for IPv6 is different from that of IPv4, the two IP standards are not interoperable. The IETF has tried to mitigate the potential issues arising from this non-interoperability; so far, these measures have proven successful in ensuring that both standards can operate together without any major issues.

Another area where IPv6 holds an edge is multicast addressing, which allows devices to send bandwidth-intensive packets such as multimedia streams to multiple destinations simultaneously.

IPv6 also provides for easier configuration. It allows simultaneous connections to multiple networks, which is not possible with IPv4. While IPv6 can still use static IP addresses or DHCP, it can utilize stateless automatic configuration. This allows seamless integration with prefixes and routers on the network and at the same time gives IPv6 devices the capability to assign addresses automatically to themselves using a unique 64-bit identifier. This auto-configuration capability is why IPv6 is ideal for use in IoT-enabled devices.

Other benefits of IPv6 include better security out of the box. With IPv6, ping scans are no longer needed, taking away a potential vector for worms to spread across your network. On the minus side, this leaves DNS servers as potential targets for attackers.

Other cons of IPv6 include the need to upgrade networking devices that are not designed for IPv6.

It may also prove difficult to type and remember overly long IPv6 addresses composed of letters and numbers and fit them in network topology diagrams. Although this sounds trivial, it may prove to be difficult and bothersome if you are administering large networks. You also must remember to enable IPv6 routing and disable IPv4 routing at the same time when you start moving to IPv6.

Migration from IPv4 to IPv6 may prove complicated, given that the two protocols are not backward compatible. This may mean assigning new IP addresses manually at the start. This process should become less problematic as networks eventually transition to IPv6.

To minimize costs when moving to IPv6, companies can adopt a strategy that would allow them to leverage their current IPv4 infrastructure while taking advantage of the benefits offered by IPv6. Instead of totally replacing IPv4 with IPv6, you can opt to have a dual-stack network where your hardware runs on both protocols, using IPv6 when possible. This approach is feasible since it is supported by major vendors.

# IPv6 Adoption

While IPv4 and IPv6 coexist right now, they are not designed to be interoperable. The IETF has several strategies in place to ensure that both protocols can exist together while preparing for the transition to IPv6. These allow IPv4 and IPv6 hosts to communicate with each other. Eventually, IPv6 addresses will become the norm, but that may still take a few more years.

While the anticipated total shift to IPv6 has yet to occur, internet registries around the world are already running out of IPv4 addresses. The biggest factor behind the slow adoption of IPv6 is the NAT, which allows the relatively narrow range of private IPv4 addresses to be used over the public internet. With NAT providing a workaround for the limited number of IPv4 addresses, corporate networks have not moved hastily towards IPv6.

Thus, the transition towards IPv6 has been slow. Although deployment of IPv6 started in 2006, IPv6 itself only became an official internet standard in 2017.

With internet registries sounding the alarm, IPv6 is now poised to take center stage in the IP-addressing space. Although it had more than two decades to mature, it has gained widespread traction in recent years.

Mobile networks, followed closely by internet service providers (ISPs), lead adoption of IPv6. Major websites have started transitioning to IPv6 as well. Trailing at the back are enterprises, hampered by their existing investments in IPv4 networks.

Problems encountered when migrating to IPv6 make matters worse for IPv6 adoption. For example, a Windows 10 bug related to IPv6 delayed Microsoft's efforts to transition to IPv6 at its Seattle headquarters in 2017.

IPv4 will probably linger around for a few more years, or even another decade, as IPv4 equipment is expensive to replace. That is not to say that you should not adopt IPv6. Your organization should start moving towards IPv6 adoption to avoid any major issues later.

# Parallels RAS is IPv6 Compliant

Parallels® Remote Application Server (RAS) is IPv6-compliant and maintains backward compatibility with IPv4. It supports various deployment models, from on-premises to public cloud to a mix of the two and even hyper-converged deployment.

Parallels RAS allows quick creation of a virtual desktop infrastructure (VDI) with improved security and centralized desktop management capabilities. It offers support

for various hypervisors and can facilitate automatic deployment of VDI desktops on-demand through custom guest virtual machine (VM) templates.

Parallels RAS supports a multi-tenant architecture through its own Tenant Broker, allowing different tenants to share Parallels Secure Client Gateways and High Availability Load Balancers while maintaining security and usage efficiency and lowering ownership costs.

Parallels RAS also provides Security Assertion Markup Language single sign-on (SAML SSO) integration, allowing centralized access to hosted resources. It even supports third-party load balancers such as Amazon Web Services Elastic Load Balancing services.

From the Parallels RAS Console, your administrators can configure a Parallels RAS farm, deploy servers, publish applications and desktops, monitor resources, manage connected devices and define security policies using a single pane of glass. These capabilities are also available on a web-based console, which can be served from any HTML5-compliant web browser. Get started with an IPv6-compliant VDI by downloading the Parallels RAS trial.

Get started with an IPv6-compliant VDI by downloading the Parallels RAS trial.

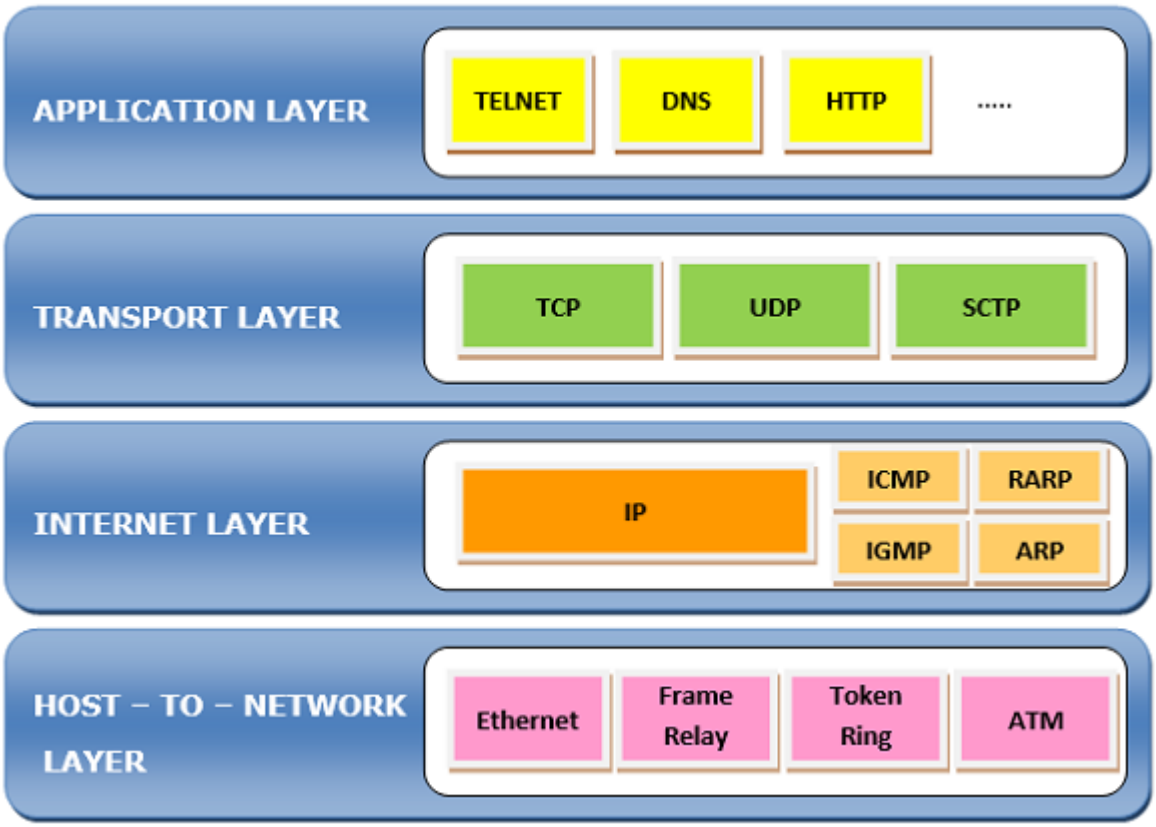
## 9. Discuss TCP/IP model in detail.

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

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

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

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




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

Ans. 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.

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.

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

Ans. Today, the internet has become unavoidable in our daily life. Appropriate use of the internet makes our life easy, fast and simple. The internet helps us with facts and figures, information and knowledge for personal, social and economic development.

There are many uses of the internet, however, the use of the internet in our daily life depends on individual requirements and goals.

**1. Uses of the Internet in Education**

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

**2. Internet Use to Speed Up Daily Tasks**

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

**3. Use of the Internet for Shopping**

With the help of the internet, anybody can order products online. The increase in online shopping has also resulted in companies offering a huge discount for their customers.

**4. Internet for Research & Development**

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

**5.Business Promotion and Innovation**

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

**6.Communication**

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

**7. Digital Transactions**

The internet facilitates internet banking, mobile banking, and e-wallets. Since all digital transactions are stored in a database, it helps the government to track income tax details or income reports in the ITR.

**8. Money Management**

The internet can also be used to manage money. Now, there are many websites, applications, and other tools that help us in daily transactions, transfers, management, budget, etc.

**9. Tour & Travel**

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 |

| Rank | ISP | Narrowband | Broadband | Total |
|---|---|---|---|---|
| 4 | BSNL | 6,400,380 | 24,507,496 | 30,907,876 |
| 5 | ACT Fibernet | 0 | 1,607,015 | 1,607,015 |
| 6 | APSFL | 0 | 970,270 | 970,270 |
| 7 | MTNL | 170,697 | 855,744 | 1,026,441 |
| 8 | Hathway | 0 | 969,157 | 969,157 |
| 9 | You Broadband | 14,660 | 778,584 | 793,244 |
| 10 | GTPL Broadband | 0 | 359,347 | 359,347 |
| 11 | Excitel | 0 | 350,783 | 350,783 |

**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.*


# 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 | APSFL | 0 | 970,270 | 970,270 |
| 7 | MTNL | 170,697 | 855,744 | 1,026,441 |
| 8 | Hathway | 0 | 969,157 | 969,157 |
| 9 | You Broadband | 14,660 | 778,584 | 793,244 |
| 10 | GTPL Broadband | 0 | 359,347 | 359,347 |
| 11 | Excitel | 0 | 350,783 | 350,783 |

**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. |

| Sr. No. | Key | MAC Address | IP 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 do I view my Internet browser's history?

Updated: 11/13/2018 by Computer Hope

Today, all major browsers have functionality that allows you to quickly and easily view your Internet browser's history. However, as multiple devices contain browser history, there are multiple ways to view as well. To proceed, choose your devices from the section below and follow the instructions.

- Desktop or laptop computer.
- Android phone or tablet running Google Chrome.
- iPhone or iPad running Safari.

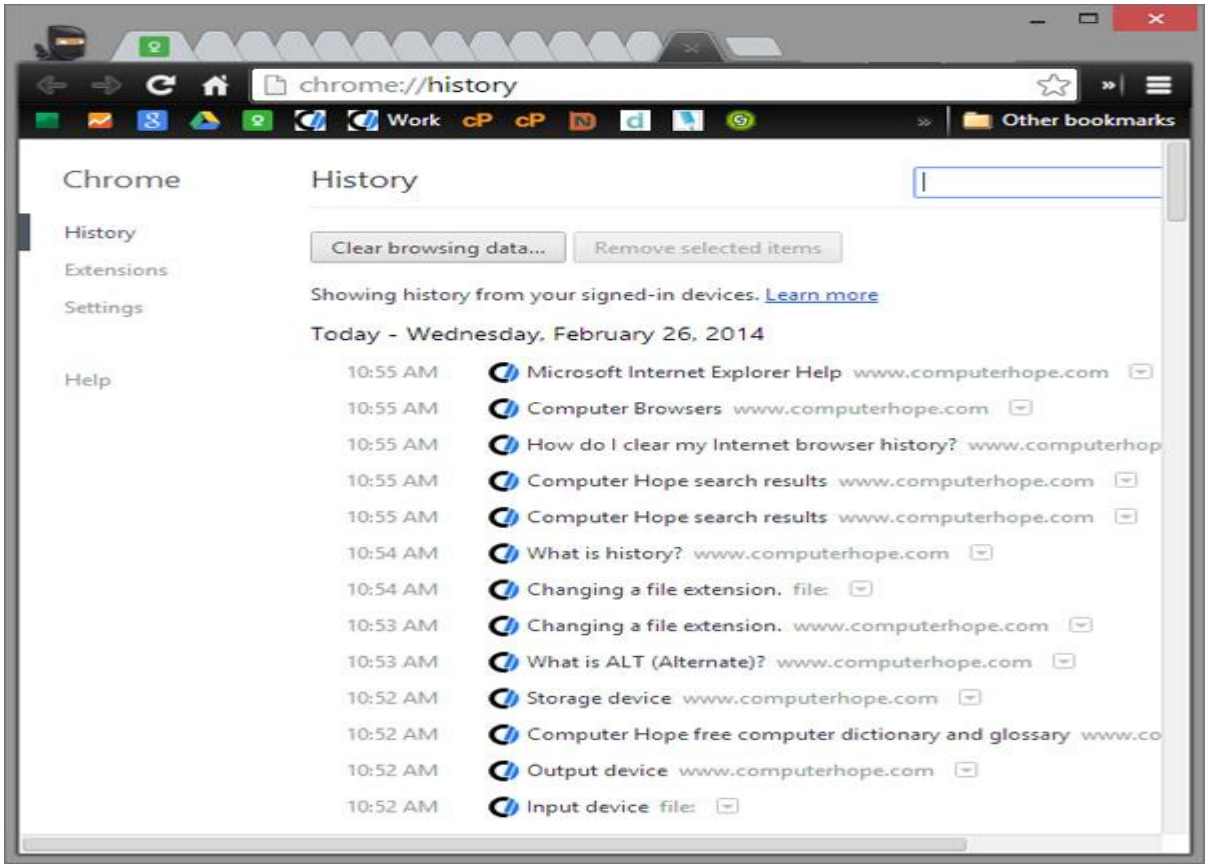
## Desktop or laptop computer

If you are using Windows, Linux, or macOS, there are quick shortcut key combinations that allow you to view your history.

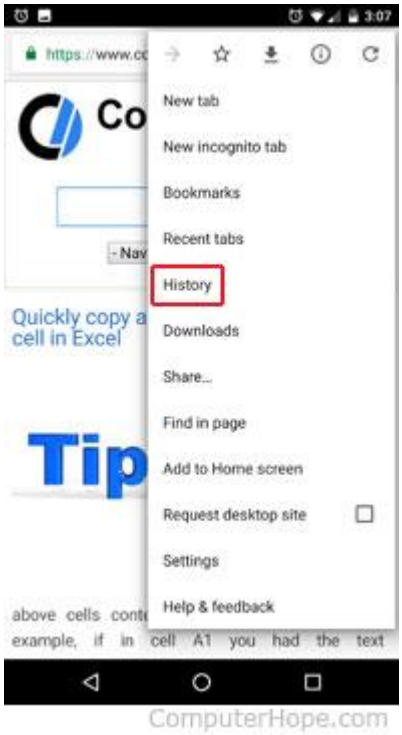
**Windows and Linux users:** Ctrl+H

**Apple users:** Command + Shift + H

Once one of the above shortcut keys is pressed, a history section similar to the example below should appear. In the following screenshot, browsing history is being viewed in Google Chrome.



# Android phone or tablet running Google Chrome




Users who are running Google Chrome on their Android phone or tablet can view their history with the following steps.

1. Open the Google Chrome Internet browser.
2. In the upper-right corner of the screen **tap the**  **icon**.
3. In the drop-down menu that appears, select **history** and shown in the image.
4. The following page contains your device's history