# **How Internet works**

Internet is global communication system which includes two main components, hardware and protocols. Hardware includes everything from cables that carry information to computer that we use. All this hardware are capable of creating network only with the help of second component that is protocols. Protocols are set of rules that the computers connected with Internet must follow in order to have communications between them. These protocols provide method as well as common language for these computers to transmit data. So when we want any kind of information from web using Internet we follow protocols. In this case study we will be learning about how we are able to use Internet in home.

## **How my home network is connected to Internet**

We use end device such as laptop or mobile at home to use Internet. Let us suppose we are using laptop where we open the web browser to visit website gsmarena.com. When we do this our laptop sends an electronic request over internet connection to our **Internet Service Provider (ISP)**. When we connect to the Internet through an ISP, we are usually assigned a temporary **IP address** for the duration of dial-in session. Since Internet is global network of computers, each computer connected to the Internet has a unique address called IP address. IP address are the internet address in the form nnn.nnn.nnn.nnn where nnn must be a number from 0-255. Our laptop needs protocols to communicate on the Internet which is built into its OS. Here, to get the requested webpage.

The ISP routes the request to a server further up the chain on the Internet. This request is sent to **DNS** server. This server will look for a match for the domain name we typed in which is www.gsmarena.com. If it finds a match, it will direct our request to the proper server's **IP address**. If it doesn't find a match, it will send the request further up the chain to another DNS server that has more information.

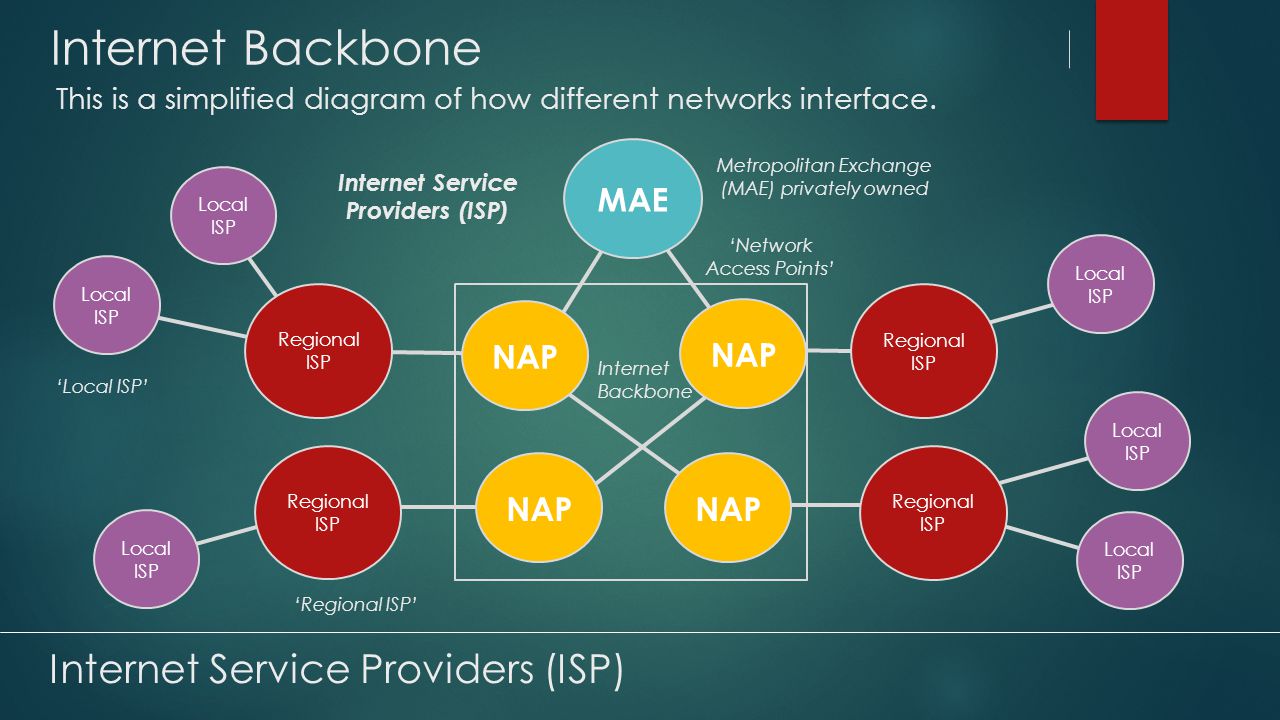
The request will eventually go to their Web server. The server will respond by sending the requested file in a series of packets. When the packets get to us, our device arranges them according to the rules of the protocols. The end result is that we see the required page that we requested.

The ISP maintains a pool of modems for their dial-in customers. This is managed by some form of computer that is usually a dedicated one which controls data flow from the modem pool to a backbone or dedicated line router. This setup may be refered to as a port server, as it serves access to the network. Billing and usage information is usually collected here as well.

After packets traverse the phone network and ISP's local equipment, they are routed onto the ISP's backbone or a backbone the ISP buys bandwidth from. From here the packets will usually journey through several routers and over several backbones, dedicated lines, and other networks until they find their destination.

The Internet backbone is made up of many large networks which interconnect with each other. These large networks are known as **Network Service Providers** or **NSP**s.

These networks **peer** with each other to exchange packet traffic. Each NSP is required to connect to three **Network Access Points** or **NAP**s. At the NAPs, packet traffic may jump from one NSP's backbone to another NSP's backbone. NSPs also interconnect at **Metropolitan Area Exchanges** or **MAE**s. MAEs serve the same purpose as the NAPs but are privately owned. NAPs were the original Internet interconnect points. Both NAPs and MAEs are referred to as Internet Exchange Points or **IX**s. NSPs also sell bandwidth to smaller networks, such as ISPs and smaller bandwidth providers. Below is a picture showing this hierarchical infrastructure.



Laptop does not know where servers are, and packets do not get sent to every computer. The information used to get packets to their destinations are contained in routing tables kept by each router connected to the Internet.

Routers are packet switches**.** A router is usually connected between networks to route packets between them. Each router knows about its sub-networks and which IP addresses they use. The router usually doesn't know what IP addresses are 'above' it. When a packet arrives at a router, the router examines the IP address put there by the IP protocol layer on the originating computer. The router checks its routing table. If the network containing the IP address is found, the packet is sent to that network. If the network containing the IP address is not found, then the router sends the packet on a default route, usually up the backbone hierarchy to the next router. Hopefully the next router will know where to send the packet. If it does not, again the packet is routed upwards until it reaches a NSP backbone. The routers connected to the NSP backbones hold the largest routing tables and here the packet will be routed to the correct backbone, where it will begin its journey 'downward' through smaller and smaller networks until it finds its destination.

The protocol stack used on the Internet is referred to as the TCP/IP protocol stack because of the two major communication protocols used. The TCP/IP stack looks like this: 

|  |  |
| --- | --- |
| **Protocol Layer** | **Comments** |
| Application Protocols Layer | Protocols specific to applications such as WWW, e-mail, FTP, etc. |
| Transmission Control Protocol Layer | TCP directs packets to a specific application on a computer using a port number. |
| Internet Protocol Layer | IP directs packets to a specific computer using an IP address. |
| Hardware Layer | Converts binary packet data to network signals and back. (E.g. ethernet network card, modem for phone lines, etc.) |

* Whenever we type any address i.e. [www.gsmarena.com](http://www.gsmarena.com) in address bar of browser, processing gets started. Web browser uses [Hypertext Transfer Protocol](http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol) which is an Application layer protocol. Web browser is programmed in such a way that it extracts [IP address](http://en.wikipedia.org/wiki/IP_address) of the URL you typed using [Domain Name System](http://en.wikipedia.org/wiki/Domain_Name_System). DNS is also an Application layer protocol. Once DNS look up is done, browser gets IP address of the website’s primary server. Browser now creates a HTTP packet having request details of [gsmarena.com](http://www.gsmarena.com). The packet is still in our Laptop. Now browser connects to the lower layer. Every layer have some interface exposed to above and below layers so that these layers can communicate with each other. So the browser gives the HTTP packet to TCP process ([Transmission Control Protocol](http://en.wikipedia.org/wiki/Transmission_Control_Protocol)) which is a Transport Layer protocol. TCP’s main function is to split request into multiple packets. These packets are having packet level identity. TCP controls the reliability of message transmissions through handshakes and acknowledgements. TCP creates a pipe between source and destinations so that system can transfer the data. This pipe called as TCP connection. TCP now put own info on top of these packets. System needs this information to maintain the session/connection.
* The packet is still in our Laptop. TCP now handovers these packets to next layer through its provided interface i.e. IP process ([Internet Protocol](http://en.wikipedia.org/wiki/Internet_Protocol)) which is an Internet Layer protocol.
* The main job of IP layer is addressing and routing. This layer puts source, destination IP addresses and routing information in packets so that packets can be route to the correct location.  IP now put its own info on top of TCP packet. System needs this information for routing in the internet. The packet is still in our PC. IP now handovers the packet to network access/network interface layer. Network access layer defines the protocols and hardware required to deliver data across some physical network. Here Ethernet or Wifi. Our laptop now encapsulates Ethernet header and Ethernet trailer with the IP packet, creates an Ethernet frame. Ethernet contains [MAC address](http://en.wikipedia.org/wiki/MAC_address) which is used to send frame locally. Now laptop physically transmits the bits of this Ethernet frame, using electricity signals over the Ethernet cabling.
* The packet is now out of laptop. It reaches web server. Note that all packets are not transmitted using same route. These may go through different routes using the most efficient routing.
* The web server physically receives the electrical signal over a cable, and re-creates the same bits by interpreting the meaning of the electrical signals.
* Web server now de-encapsulates the IP packets from the Ethernet frame by removing and discarding the Ethernet header and trailer. After this it hands over to Internet protocol layer.
* Internet protocol layer then verifies source and destination info and then hands over to TCP layer.
* TCP layer reads the TCP information. It merges all incoming packets and create HTTP packet which source created originally.
* This layer provide acknowledgement about each packet so that if any packet is missing or corrupt then source can transmit that again. This confirms the reliability of the message.
* And finally TCP hands it over to HTTP process which understands the HTTP get request.
* Web server now process the request through running web process hence generates the response.
* Server sends this response in the same way to the intended device which initiated the request.
* Finally information reaches to device’s application layer then browser displays this as web page.

So this is how all the layers are in action when we request a webpage.