Anjali Adhikari

Anjali.adhikari@ibm.com

Abstract

This document will give you a high level understanding of various network devices Switches, routers, and wireless access points which are the essential networking basics. Through them, devices connected to your network can communicate with one another and with other networks, like Internet

Networking Basics

Terminology and Network Layer Understanding

**Internetworking Devices used on a network**

For connecting internet, we require various internetworking devices. Some of the common devices used in building up Internet are.

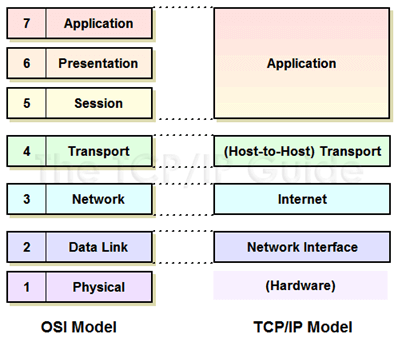
* **NIC:** Network Interface Card or NIC are printed circuit boards that are installed in workstations. It represents the physical connection between the workstation and network cable. Although NIC operates at the physical layer of the OSI model, it is also considered as a data link layer device. Part of the NIC's is to facilitate information between the workstation and the network. It also controls the transmission of data onto the wire
* **Hubs**: A hub helps to extend the length of a network cabling system by amplifying the signal and then re-transmitting it. They are basically multiport repeaters and not concerned about the data at all. The hub connects workstations and sends a transmission to all the connected workstations.
* **Bridges**: As network grow larger, they often get difficult to handle. To manage these growing network, they are often divided into smaller LANs. These smaller LANS are connected to each other through bridges. This helps not only to reduce traffic drain on the network but also monitors packets as they move between segments. It keeps the track of the MAC address that is associated with various ports.
* **Switches**: Switches are used in the option to bridges. It is becoming the more common way to connect network as they are simply faster and more intelligent than bridges. It is capable of transmitting information to specific workstations. Switches enable each workstation to transmit information over the network independent of the other workstations. It is like a modern phone line, where several private conversation takes place at one time.
* **Routers**: The aim of using a router is to direct data along the most efficient and economical route to the destination device. They operate at Network layer 3, which means they communicate through IP address and not physical (MAC) address. Routers connect two or more different networks together, such as an Internet Protocol network. Routers can link different network types such as Ethernet, FDDI, and Token Ring.
* **Brouters**: It is a combination of both routers and bridge. Brouter act as a filter that enables some data into the local network and redirects unknown data to the other network.
* **Modems**: It is a device that converts the computer-generated digital signals of a computer into analog signals, traveling via phone lines.

**Understanding TCP/ IP layers**

TCP/IP stands for Transmission Control Protocol/ Internet Protocol. It determines how a computer should be connected to the Internet and how data should be transmitted between them.

* **TCP:** It is responsible for breaking data down into small packets before they can be sent on the network. Also, for assembling the packets again when they arrive.
* **IP (Internet Protocol):**It is responsible for addressing, sending and receiving the data packets over the internet.

Below image shows [TCP/IP model](https://www.guru99.com/tcp-ip-model.html) connected to OSI Layers..

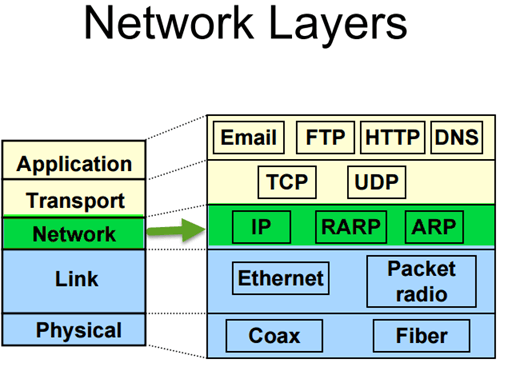
[](https://www.guru99.com/images/ccna/061516_1051_Introductio3.png)

**Understanding TCP/IP Internet Layer**

To understand TCP/IP internet layer we take a simple example. When we type something in an address bar, our request will be processed to the server. The server will respond back to us with the request. This communication on the internet is possible due to the TCP/IP protocol. The messages are sent and received in small packages.

The Internet layer in the TCP/IP reference model is responsible for transferring data between the source and destination computers. This layer includes two activities

* Transmitting data to the Network Interface layers
* Routing the data to the correct destinations

[](https://www.guru99.com/images/ccna/061516_1051_Introductio4.png)

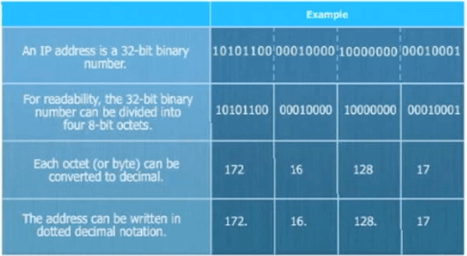
So how this happen?

Internet layer packs data into data packets referred as IP datagrams. It consists of source and destination IP address. Beside this, IP datagram header field consists of information like version, header length, type of service, datagram length, time to live, and so on.

In network layer, you can observe network protocols like ARP, IP, ICMP, IGMP, etc. The datagram are transported through network using these protocols. They each resemble some function like.

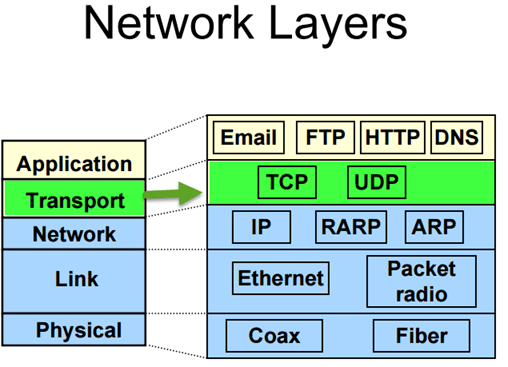
* The Internet Protocol (IP) is responsible for IP addressing, routing, the fragmentation and reassembly of packets. It determines how to route message on the network.
* Likewise, you will have ICMP protocol. It is responsible for diagnostic functions and reporting errors due to the unsuccessful delivery of IP packets.
* For the management of IP multicast groups, IGMP protocol is responsible.
* The ARP or Address Resolution Protocol is responsible for the resolution of the Internet layer address to the Network Interface layer address such as a hardware address.
* RARP is used for disk less computers to determine their IP address using the network.

The image below shows the format of an IP address.

[](https://www.guru99.com/images/ccna/061516_1051_Introductio5.png)

**Understanding TCP/IP Transport Layer**

The transport layer also referred as Host-to-Host Transport layer. It is responsible for providing the Application layer with session and datagram communication services.

[](https://www.guru99.com/images/ccna/061516_1051_Introductio6.png)

The main protocols of the Transport layer are User Datagram Protocol (UDP) and the Transmission Control Protocol (TCP).

* TCP is responsible for the sequencing, and acknowledgment of a packet sent. It also does the recovery of packet lost during transmission. Packet delivery through TCP is more safe and guaranteed. Other protocols that falls in the same category are FTP, HTTP, SMTP, POP, IMAP, etc.
* UDP is used when the amount of data to be transferred is small. It does not guarantee packet delivery. UDP is used in VoIP, Videoconferencing, Pings, etc.

**Network Segmentation**

Network segmentation implicates splitting the network into smaller networks. It helps to split the traffic loads and improve the speed of the Internet.

Network Segmentation can be achieved by following ways,

* By implementing DMZ (demilitarised zones) and gateways between networks or system with different security requirements.
* By implementing server and domain isolation using Internet Protocol Security (IPsec).
* By implementing storage based segmentation and filtering using techniques like LUN (Logical Unit Number) masking and Encryption.
* By implementing DSD evaluated cross-domain solutions where necessary

**Why Network Segmentation is important**

Network Segmentation is important for following reasons,

* **Improve Security**- To protect against malicious cyber attacks that can compromise your network usability. To detect and respond to an unknown intrusion in the network
* **Isolate network problem**- Provide a quick way to isolate a compromised device from the rest of your network in case of intrusion.
* **Reduce Congestion**- By segmenting the LAN, the number of hosts per network can be reduced
* **Extended Network**- Routers can be added to extend the network, allowing additional hosts onto the LAN.

**VLAN Segmentation**

VLANs enables an administrator to segment networks. Segmentation is done based on the factors such as project team, function or application, irrespective of the physical location of the user or device. A group of devices connected in a VLAN act as if they are on their own independent network, even if they share a common infrastructure with other VLANs. VLAN is used for data-link or internet layer while subnet is used for Network/IP layer. Devices within a VLAN can talk to each other without a Layer-3 switch or router.

The popular device used for segmenting are a switch, router, bridge, etc.

