Dr. D. Y. Patil Pratishthan's

Institute for Advanced Computing &Software Development

IACSD

Fundamental of Computer Networks

INDEX

Internetworking

Internetworking term in computer networking explains how computer networks connect with each other through Internetworking devices. Before we learn internetworking in details, let’s understand what computer network is first.

Computer networks are basically built from three components; End Devices, Networking Devices and Media.

End Devices: - End devices are used to access or transmit the data. Computer, laptop, data server and tablet are the example of end devices.

Networking Devices: - Networking devices are used to control the data flow. Switches, Routers, HUB, Bridges, firewalls and modems are the example of networking devices.

Media: - Media is used to transmit the data. Copper cables, fiber cable and wireless signals are the example of media.

In computer network:-

- Destination hostname must be converted with IP address before source can access it.
- Source PC uses DNS or ARP broadcast to resolve the hostname with IP address.

Every computer in network has a unique network address. This address represents its location in network. Computer address is built from two addresses IP address and MAC address.

- **IP Address**: - IP address is a software address. We need to configure it on each PC.
- **MAC Address**: - MAC address is a hardware address. It is assigned with Ethernet card from its manufacture company.
- Computers know their own address but they don't know others. To know others address they use two types of broadcast ARP and RARP.

- Network applications rely on broadcast messages to get the necessary information. Beside ARP and RARP there are lots of broadcast in the network that create serious performance issue. To deal with broadcast issue, a large network is divided in many small networks. Each small network has its own broadcast boundaries and known as broadcast domain.

Networking devices

In this section we will take five key networking devices those are used to connect multiple computers in single network and explain how they affect broadcast and collision.

Hub

If you have two devices, you can connect them directly with a cable. But if you have more than two devices, you need a center device that can connect them. HUB solves this issue. It has single purpose, connect multiple devices in single network.

Hub is a multi-port repeater. It cannot control collision and broadcast. HUB is the earliest device in computer network. Usually you will not see it in current network.

Bridge

Bridge connects devices more intelligently. It can remove collision from network.It keeps record of connected device and create separate route for each devices. Bridge have following limitations.

- They cannot control broadcast.
- Bridges manage collision by software that slows down overall network performance.
- Bridges have port limitation.
- Bridges are outdated now. They are hard to find in current time computer network. They are replaced by switches.

Switch

Switches have all goodies of bridges. They can control collision at hardware level that improves overall network performance.Switches create separate route for each connected device that eliminates CSMA/CD process completely.

Switch keeps route information in memory. We will explain this process in detail with example in our next article. For this article just make sure that you know switch maintain a table which is used to keep track of connected devices. It is known as CAM table and also used to remove the collision. Switches can control the collision but they cannot control the broadcast.

Router

A router is a device that analyzes the contents of data packets transmitted within a network or to another network. Routers determine whether the source and destination are on the same network or whether data must be transferred from one network type to another, which requires encapsulating the data packet with routing protocol header information for the new network type.

Routers have following drawback: -

- They are very expensive
- They have limited ports

Multilayer switches

Multilayer switches are the most expensive device among these. They can control both collision and broadcast.

Ethernet

Ethernet is a standard communication protocol embedded in software and hardware devices. It is used for building a local area network. The local area network is a computer network that interconnects a group of computers and shares the information through cables or wires.

Wired Ethernet Network

The Ethernet technology mainly works with the fiber optic cables that connect devices within a distance of 10 km. The Ethernet supports 10 Mbps.

Ethernet communication:A computer network interface card (NIC) is installed in each computer, and is assigned to a unique address. An Ethernet cable runs from each NIC to the central switch or hub. The switch and hub act as a relay though they have significant differences in the manner in which they handle network traffic – receiving and directing packets of data across the LAN. Thus, Ethernet networking creates a communications system that allows sharing of data and resources including printers, fax machines and scanners.

Wireless Ethernet

Ethernet networks can also be wireless. Rather than using Ethernet cable to connect the computers, wireless NICs use radio waves for two-way communication with a wireless switch or hub. It consists of Ethernet ports, wireless NICs, switches and hubs. Wireless network technology can be more flexible to use, but also require extra care in configuring security.

Types of Ethernet Networks

There are several types of Ethernet networks, such as Fast Ethernet, Gigabit Ethernet, and Switch Ethernet. A network is a group of two or more computer systems connected together.

1. Fast Ethernet

The fast Ethernet is a type of Ethernet network that can transfer data at a rate of 100 Mbps using a twisted-pair cable or a fiber-optic cable. The older 10 Mbps Ethernet is still used, but such networks do not provide necessary bandwidth for some network-based video applications.

2. Gigabit Ethernet

The Gigabit Ethernet is a type of Ethernet network capable of transferring data at a rate of 1000 Mbps based on a twisted-pair or fiber optic cable, and it is very popular. The type of twisted-pair cables that support Gigabit Ethernet is Cat 5e cable, where all the four pairs of twisted wires of the cable are used to achieve high data transfer rates. The 10 Gigabit Ethernet is a latest generation Ethernet capable of transferring data at a rate of 10 Gbps using twisted-pair or fiber optic cable.

3. Switch Ethernet

Multiple network devices in a LAN require network equipment’s such as a network switch or hub. When using a network switch, a regular network cable is used instead of a crossover cable. The crossover cable consists of a transmission pair at one end and a receiving pair at the other end.

Different Types of Ethernet Cables

Different type and diameter of the cables used as given below:

- 10Base2: The cable used is a thin coaxial cable: thin Ethernet.
- 10Base5: The cable used is a thick coaxial cable: thick Ethernet.
- 10Base-T: The cable used is a twisted-pair (T means twisted pair) and the speed achieved is around 10 Mbps.
- 100Base-FX: Makes it possible to achieve a speed of 100 Mbps by using multimode fiber optic (F stands for Fiber).
- 100Base-TX: Similar to 10Base-T, but with a speed 10 times greater (100 Mbps).
- 1000Base-T: Uses a double-twisted pair of category 5 cables and allows a speed up to one Gigabit per second.
- 1000Base-SX: Based on multimode fiber optic uses a short wavelength signal (S stands for short) of 850 nanometers (770 to 860 nm).
- 1000Base-LX: Based on multimode fiber optic uses a long wavelength signal (L stands for long) of 1350 nm (1270 to 1355 nm).

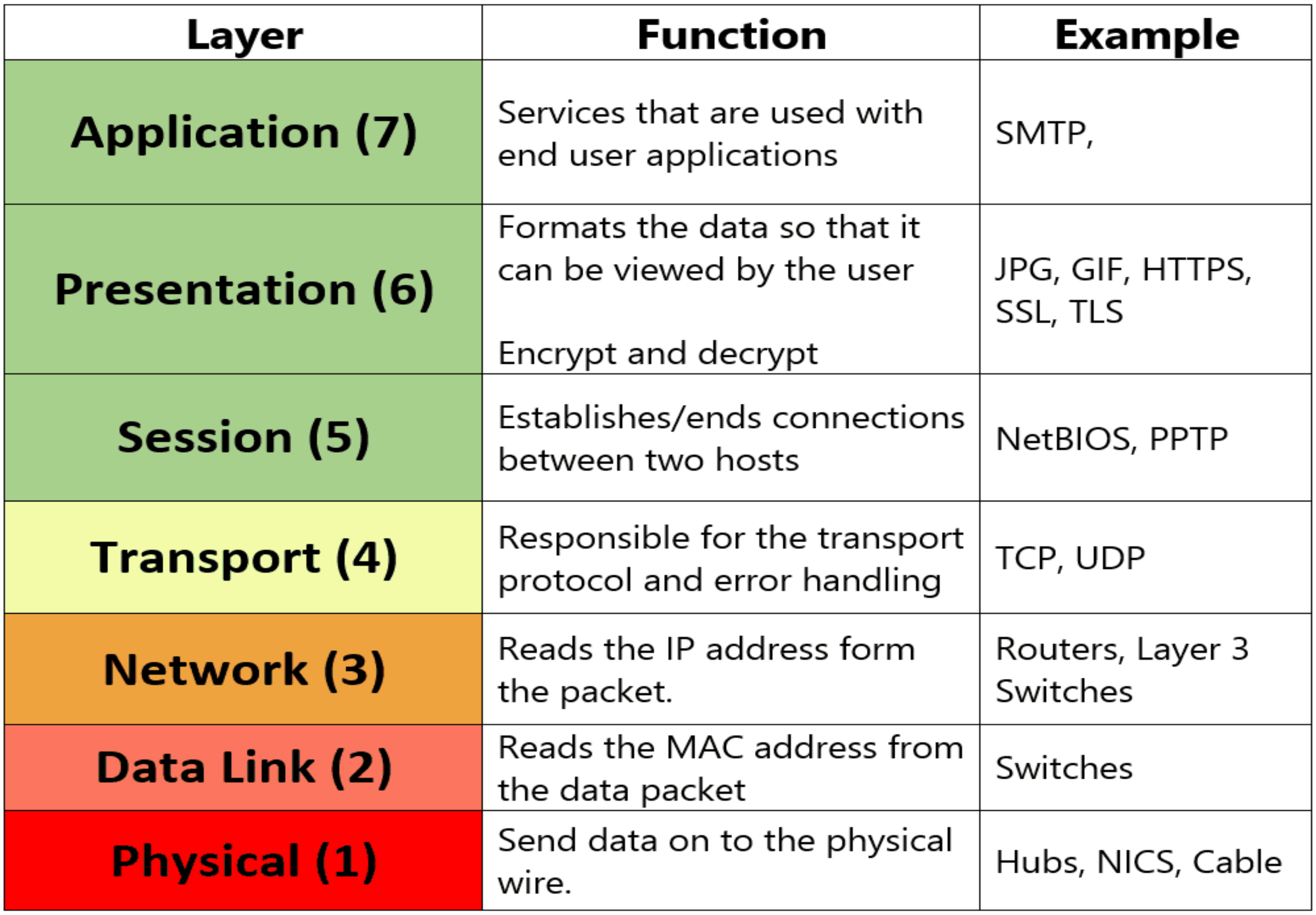
Wireless Networking

Wireless networks use radio waves to connect devices such as laptops to the Internet, the business network and applications. When laptops are connected to Wi-Fi hot spots in public places, the connection is established to that business's wireless network. There are four main types of wireless networks:

- Wireless Local Area Network (LAN): Links two or more devices using a wireless distribution method, providing a connection through access points to the wider Internet.
- Wireless Metropolitan Area Networks (MAN): Connects several wireless LANs.
- Wireless Wide Area Network (WAN): Covers large areas such as neighboring towns and cities.
- Wireless Personal Area Network (PAN): Interconnects devices in a short span, generally within a person's reach.

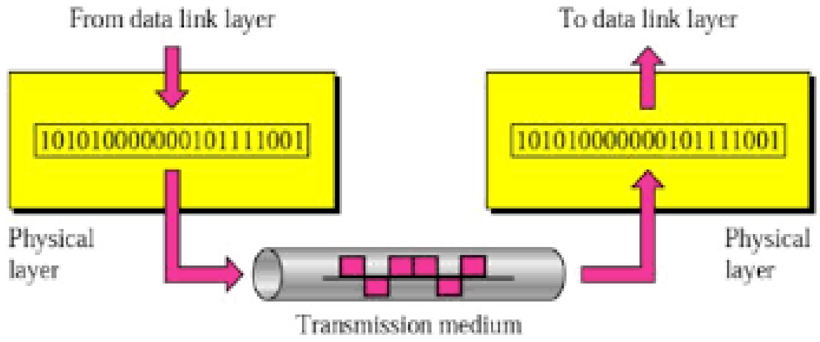
OSI MODEL

Layer architecture



Layer	Function	Example
Application (7)	Services that are used with end user applications	SMTP,
Presentation (6)	Formats the data so that it can be viewed by the user Encrypt and decrypt	JPG, GIF, HTTPS, SSL, TLS
Session (5)	Establishes/ends connections between two hosts	NetBIOS, PPTP
Transport (4)	Responsible for the transport protocol and error handling	TCP, UDP
Network (3)	Reads the IP address form the packet.	Routers, Layer 3 Switches
Data Link (2)	Reads the MAC address from the data packet	Switches
Physical (1)	Send data on to the physical wire.	Hubs, NICS, Cable

Layer 1: Physical Layer



The physical layer is responsible for the transmission and reception of unstructured raw data between a device and a physical transmission medium. It converts the digital bits into electrical, radio, or optical signals. The components of a physical layer can be described in terms of a network topology. Bluetooth, Ethernet, and USB all have specifications for a physical layer.

Functions of Physical Layer

Following are the various functions performed by the Physical layer of the OSI model.

1. **Representation of Bits:** Data in this layer consists of stream of bits. The bits must be encoded into signals for transmission. It defines the type of encoding i.e. how 0's and 1's are changed to signal.

2. **Data Rate:** This layer defines the rate of transmission which is the number of bits per second.

3. **Synchronization:** It deals with the synchronization of the transmitter and receiver. The sender and receiver are synchronized at bit level.

4. **Interface:** The physical layer defines the transmission interface between devices and transmission medium.

5. **Line Configuration:** This layer connects devices with the medium: Point to Point configuration and Multipoint configuration.

6. **Topologies:** Devices must be connected using the following topologies: Mesh, Star, Ring and Bus.

7. **Transmission Modes:** Physical Layer defines the direction of transmission between two devices: Simplex, Half Duplex, Full Duplex.

8. Deals with baseband and broadband transmission.

Layer 2: Data Link Layer

The data link layer provides node-to-node data transfer—a link between two directly connected nodes. It defines the protocol to establish and terminate a connection between two physically connected devices. It also defines the protocol for flow control between them.

IEEE 802 divides the data link layer into two sublayers

- Medium access control (MAC) layer – responsible for controlling how devices in a network gain access to a medium and permission to transmit data.
- Logical link control (LLC) layer – responsible for identifying and encapsulating network layer protocols, and controls error checking and frame synchronization.

Functions of Data Link Layer

1. **Framing:** Frames are the streams of bits received from the network layer into manageable data units. This division of stream of bits is done by Data Link Layer.
2. **Physical Addressing:** The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network.
3. **Flow Control:** A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side.
4. **Error Control:** Error control is achieved by adding a trailer at the end of the frame. Duplication of frames are also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames.
5. **Access Control:** Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.

Layer 3: Network Layer

The network layer provides the functional and procedural means of transferring variable length data sequences (called packets) from one node to another connected in "different networks". If the message is too large to be transmitted from one node to another on the data link layer between those nodes, the network may implement message delivery by splitting the message into several fragments at one node, sending the fragments independently, and reassembling the fragments at another node.

Message delivery at the network layer is not necessarily guaranteed to be reliable; a network layer protocol may provide reliable message delivery, but it need not do so.

Functions of Network Layer

1. It translates logical network address into physical address. Concerned with circuit, message or packet switching.
2. Routers and gateways operate in the network layer. Mechanism is provided by Network Layer for routing the packets to final destination.
3. Connection services are provided including network layer flow control, network layer error control and packet sequence control.
4. Breaks larger packets into small packets.

Layer 4: Transport Layer

The transport layer provides the functional and procedural means of transferring variable-length data sequences from a source to a destination host, while maintaining the quality of service functions.

The transport layer controls the reliability of a given link through flow control, and error control. Some protocols are state- and connection-oriented.

Functions of Transport Layer

1. **Service Point Addressing:** Transport Layer header includes service point address which is port address. This layer gets the message to the correct process on the computer unlike Network Layer, which gets each packet to the correct computer.

2. **Segmentation and Reassembling:** A message is divided into segments; each segment contains sequence number, which enables this layer in reassembling the message. Message is reassembled correctly upon arrival at the destination and replaces packets which were lost in transmission.

3. **Connection Control:** It includes 2 types:

   - Connectionless Transport Layer : Each segment is considered as an independent packet and delivered to the transport layer at the destination machine.

   - Connection Oriented Transport Layer : Before delivering packets, connection is made with transport layer at the destination machine.

4. **Flow Control:** In this layer, flow control is performed end to end.

5. **Error Control:** Error Control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error. Error Correction is done through retransmission.

TRANSMISSION CONTROL PROTOCOL (TCP)	USER DATAGRAM PROTOCOL (UDP)
TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Sequencing of data is a feature of Transmission Control Protocol (TCP). This means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP.If ordering is required, it has to be managed by the application layer.
TCP is comparatively slower than UDP.	UDP is faster, simpler, and efficient than TCP.
Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in User Datagram Protocol (UDP).
TCP has a (20-80) bytes variable length header.	UDP has an 8 bytes fixed length header.
TCP doesn’t supports Broadcasting.	UDP supports Broadcasting.

Layer 5: Session Layer

The session layer controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. In the OSI model, this layer is responsible for gracefully closing a session, which is handled in the Transmission Control Protocol at the transport layer in the Internet Protocol Suite. The session layer is commonly implemented explicitly in application environments that use remote procedure calls.

Functions of Session Layer

1. **Dialog Control :** This layer allows two systems to start communication with each other in half-duplex or full-duplex.
2. **Token Management:** This layer prevents two parties from attempting the same critical operation at the same time.
3. **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into stream of data. Example: If a system is sending a file of 800 pages, adding checkpoints after every 50 pages is recommended. This ensures that 50 page unit is successfully received and acknowledged. This is beneficial at the time of crash as if a crash happens at page number 110; there is no need to retransmit 1 to100 pages.

Layer 6: Presentation Layer

The presentation layer establishes context between application-layer entities, in which the application-layer entities may use different syntax and semantics if the presentation service provides a mapping between them. If a mapping is available, presentation protocol data units are encapsulated into session protocol data units and passed down the protocol stack.This layer provides independence from data representation by translating between application and network formats. The presentation layer transforms data into the form that the application accepts.

Functions of Presentation Layer

1. **Translation:** Before being transmitted, information in the form of characters and numbers should be changed to bit streams. The presentation layer is responsible for interoperability between encoding methods as different computers use different encoding methods. It translates data between the formats the network requires and the format the computer.

2. **Encryption:** It carries out encryption at the transmitter and decryption at the receiver.
3. **Compression:** It carries out data compression to reduce the bandwidth of the data to be transmitted. The primary role of Data compression is to reduce the number of bits to be 0transmitted. It is important in transmitting multimedia such as audio, video, text etc.

Layer 7: Application Layer

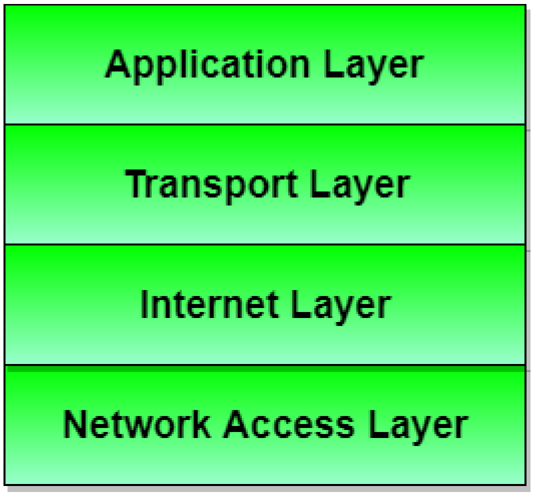
The application layer is the OSI layer closest to the end user, which means both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component. Application-layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication. Application protocols that are used are File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Simple Mail Transfer Protocol (SMTP), TELNET, Domain Name System(DNS) etc.

Functions of Application Layer

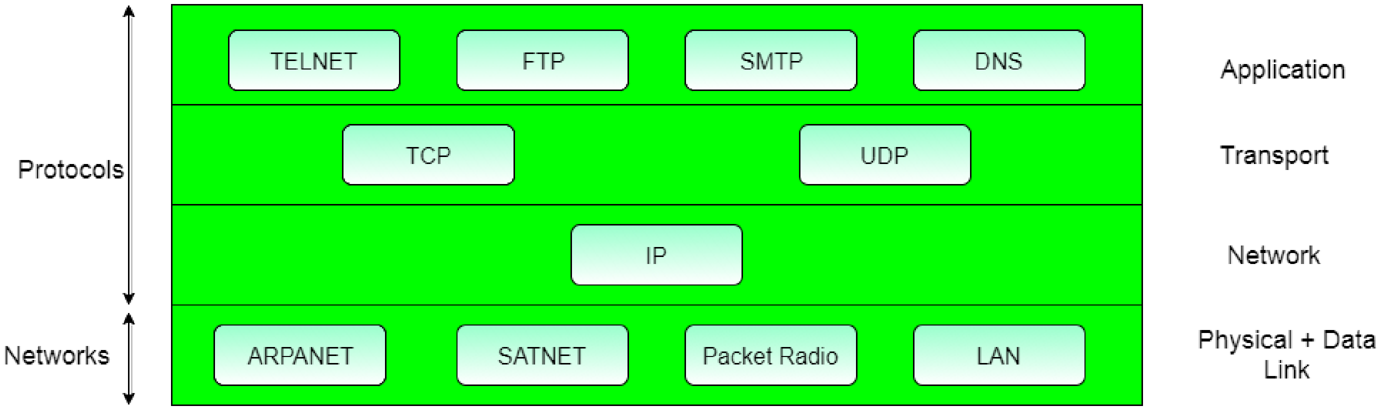
1. **Mail Services:** This layer provides the basis for E-mail forwarding and storage.
2. **Network Virtual Terminal:** It allows a user to log on to a remote host. The application creates software emulation of a terminal at the remote host. User's computer talks to the software terminal which in turn talks to the host and vice versa. Then the remote host believes it is communicating with one of its own terminals and allows user to log on.
3. **Directory Services:** This layer provides access for global information about various services.
4. **File Transfer, Access and Management (FTAM):** It is a standard mechanism to access files and manages it. Users can access files in a remote computer and manage it. They can also retrieve files from a remote computer.

TCP/IP(Transmission Control Protocol/ Internet Protocol)

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. **Protocols** are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. They also offer simple naming and addressing schemes.



Protocols and networks in the TCP/IP model:



Overview of TCP/IP reference model

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of **Defence's Project Research Agency** (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact untill the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

Different Layers of TCP/IP Reference Model

Below we have discussed the 4 layers that form the TCP/IP reference model:

Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.

3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.
6. The various functions performed by the Internet Layer are:
    - Delivering IP packets
    - Performing routing
    - Avoiding congestion

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. **TELNET** is a two-way communication protocol which allows connecting to a remote machine and run applications on it.

2. **FTP**(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. **SMTP**(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. **DNS**(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.
5. It allows peer entities to carry conversation.
6. It defines two end-to-end protocols: TCP and UDP
   - **TCP(Transmission Control Protocol):** It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.
   - **UDP(User-Datagram Protocol):** It is an unreliable connection-less protocol that do not want TCPs, sequencing and flow control. Eg: One-shot request-reply kind of service.

Merits of TCP/IP model

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers.

Demerits of TCP/IP

1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.

3. Replacing protocol is not easy.

4. It has not clearly separated its services, interfaces and protocols.

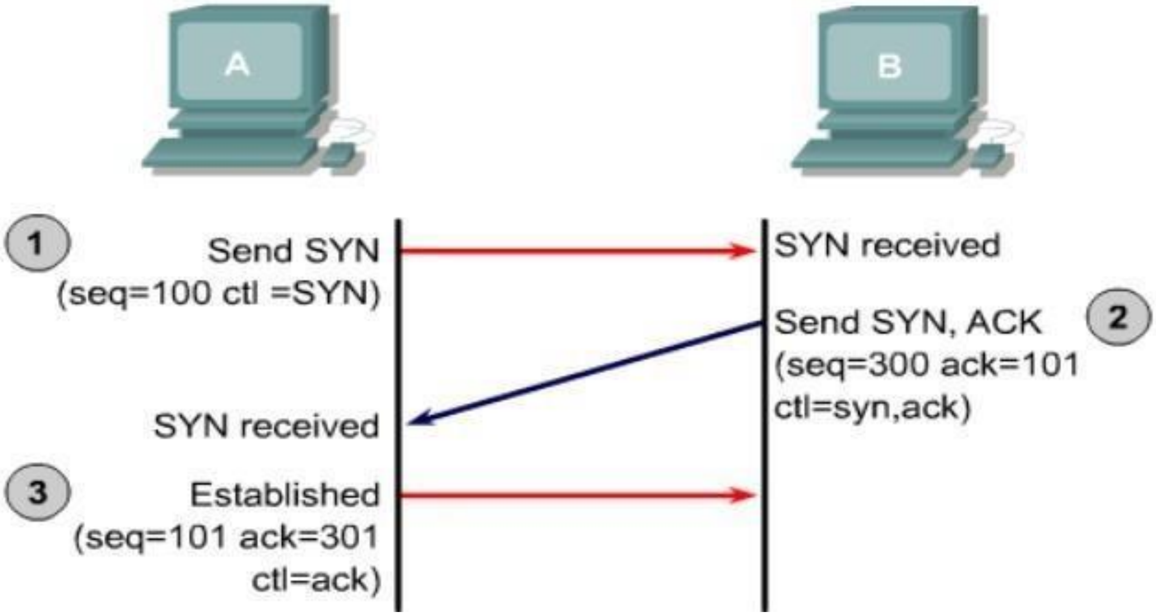
Comparison between OSI and TCP model

OSI(Open System Interconnection)	**TCP/IP(Transmission Control Protocol / Internet Protocol)**
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.

6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. Protocols are hidden in OSI model and are easily replaced as the technology changes.	9. In TCP/IP replacing protocol is not easy.
10. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	10. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
11. It has 7 layers	11. It has 4 layers

3-Way Handshake

TCP requires connection establishment before data transfer begins. For a connection to be established or initialized, the two hosts must synchronize their Initial Sequence Numbers (ISNs).



3 way handshaking technique is often referred to as "SYN-SYN-ACK" (or more accurately SYN, SYN-ACK, ACK) because there are **three** messages transmitted by TCP to negotiate and start a TCP session between two computers.

This is done by sending a **SYN** (synchronization) packet, as if to initiate a three-way handshake, to every port on the server. If the server responds with a **SYN/ACK** (synchronization acknowledged) packet from a particular port, it means the port is open.

IPv4 address and Subnetting

The IP hierarchy contains many classes of the IP addresses. Broadly, the IPv4 addressing system is divided into five classes of IP address. All the five classes are identified by the first octet of the IP address.

The Classes of IPv4 addresses

The different classes of the IPv4 address are the following:

1) Class A address

2) Class B address

3) Class C address

4) Class D address

5) Class E address

Class A Address

The first bit of the first octet is always set to zero. So that the first octet ranges from 1 – 127. The class A address only include IP starting from 1.x.x.x to 126.x.x.x. The IP range 127.x.x.x is reserved for loop back IP addresses. The default subnet mask for class A IP address is 255.0.0.0. This means it can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2). Class A IP address format is thus: **N**.H.H.H

Class B Address

Here the first two bits in the first two bits is set to zero. Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x. Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses. Class B IP address format is: **N.N**.H.H

Class C Address

The first octet of this class has its first 3 bits set to 110. Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x. Class C gives 2097152 (2^{21}) Network addresses and 254 (2^{8}-2) Host addresses. Class C IP address format is: **N.N.N**.H

Class D Address

The first four bits of the first octet in class D IP address are set to 1110. Class D has IP address rage from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not intended for a particular host, but multiple ones. That is why there is no need to extract host address from the class D IP addresses. The Class D does not have any subnet mask.

Class E Address

The class E IP addresses are reserved for experimental purpose only for R&D or study. IP addresses in the class E ranges from 240.0.0.0 to 255.255.255.254. This class too is not equipped with any subnet mask.

Subnetting

Each IP address consists of a subnet mask. All the class types, such as Class A, Class B and Class C include the subnet mask known as the default subnet mask. The subnet mask is intended for determining the type and number of IP addresses required for a given local network. The firewall or router is called the default gateway. The default subnet mask is as follows:

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

The subnetting process allows the administrator to divide a single Class A, Class B, or Class C network number into smaller portions. The subnets can be subnettedagain into sub-subnets.

Dividing the network into a number of subnets provides the following benefits:

- Reduces the network traffic by reducing the volume of broadcasts
- Helps to surpass the constraints in a local area network (LAN), for example, the maximum number of permitted hosts.
- Enables users to access a work network from their homes; there is no need to open the complete network.

Example using the **Class C** mask of 255.255.255.224

Subnet bits are used in this mask is 3 bits or 2^3-2=6 subnets

Host bits are available per subnet is 5 bits or 2^5-2=30 hosts per subnet

Subnet addresses are 256-224 =32, 64, 96, 128, 160 and 192 (Six subnets found by continuing to add 32 to itself.)

Broadcast address of each subnet is the broadcast address for the 32 subnet is 63. The broadcast address for the 64 subnet is 95. The broadcast address for the 96 subnet is 127. The broadcast address for the 160 subnet is 191. The broadcast address for the 192 subnet is 223 (since 224 is the mask).Valid host range of each subnet is valid hosts are the numbers in between the subnet and broadcast addresses.

Example using **class B**maskof 255.255.240.0

1. 2-2=14 subnets
2. 2-2=4094 hosts per subnet
3. 256-240=16.0, 32.0, 48.0, 64.0, etc.
4. Broadcast for the 16.0 subnet is 31.255. Broadcast for the 32.0 subnet is 47.255, etc.

5. The valid hosts are:

Subnet	16.0	32.0	48.0	64.0
first host	16.1	32.1	48.1	64.1
last host	31.254	47.254	63.254	79.254
broadcast	31.255	47.255	63.255	79.255

Example using **Class A** mask 255.240.0.0 (/12)this mask provides you with only four subnet bits, or 16 subnets (14 if you're not using subnet zero) with 1,048,574 hosts each. The valid subnets are 256-240=16, 32, 48, 64, 80, etc., all the way to 224. The first subnet, assuming subnet zero, is:

- Subnet: 10.0.0.0
- Broadcast: 10.15.255.255
- Valid host range: 10.0.0.1 through 10.15.255.254

The last subnet, assuming subnet zero, is:

- Subnet: 10.240.0.0
- Broadcast: 10.255.255.255
- Valid host range: 10.240.0.1 through 10.255.255.254

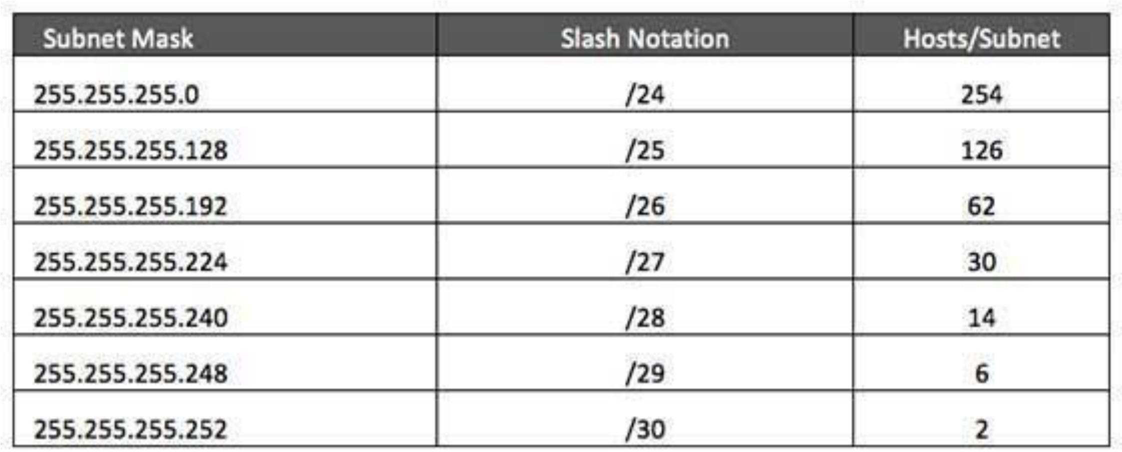
Variable Length Subnet Mask (VLSM)

A Variable Length Subnet Mask (VLSM) is a numerical masking sequence, or IP address subset, based on overall network requirements. A VLSM allows a network administrator to use long masks for networks with few hosts and short masks for networks with multiple hosts. A VLSM is used with a VLSM router and must have routing protocol support. A VLSM is also known as a classless Internet Protocol (IP) address.

For example, an administrator have 192.168.1.0/24 network. The suffix /24 tells the number of bits used for network address. In this example, the administrator has three different departments with different number of hosts. Sales department has 100 computers, Purchase department has 50 computers, Accounts has 25 computers and Management has 5 computers. In CIDR, the subnets are of fixed size. Using the same methodology the administrator cannot fulfill all the requirements of the network.

The following procedure shows how VLSM can be used in order to allocate department-wise IP addresses as mentioned in the example.

Step –1 Make a list of Subnets possible.



Subnet Mask	Slash Notation	Hosts/Subnet
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2

Step – 2 Sort the requirements of IPs in descending order (Highest to Lowest).

- Sales 100
- Purchase 50
- Accounts 25
- Management 5

Step –3 Allocate the highest range of IPs to the highest requirement, so let's assign 192.168.1.0 /25 (255.255.255.128) to the Sales department. This IP subnet with Network number 192.168.1.0 has 126 valid Host IP addresses which satisfy the requirement of the Sales department. The subnet mask used for this subnet has 10000000 as the last octet.

Step – 4 Allocate the next highest range, so let's assign 192.168.1.128 /26 (255.255.255.192) to the Purchase department. This IP subnet with Network number 192.168.1.128 has 62 valid Host IP Addresses which can be easily assigned to all the PCs of the Purchase department. The subnet mask used has 11000000 in the last octet.

Step –5 Allocate the next highest range, i.e. Accounts. The requirement of 25 IPs can be fulfilled with 192.168.1.192 /27 (255.255.255.224) IP subnet, which contains 30 valid host IPs. The network number of Accounts department will be 192.168.1.192. The last octet of subnet mask is 11100000.

Step –6 Allocate the next highest range to Management. The Management department contains only 5 computers. The subnet 192.168.1.224 /29 with the Mask 255.255.255.248 has exactly 6 valid host IP addresses. So this can be assigned to Management. The last octet of the subnet mask will contain 11111000.

By using VLSM, the administrator can subnet the IP subnet in such a way that least number of IP addresses are wasted. Even after assigning IPs to every department, the administrator, in this example, is still left with plenty of IP addresses which was not possible if he has used CIDR.

IPv6 address

An Internet Protocol Version 6 address (IPv6 address) is a numerical label that is used to identify a network interface of a computer or a network node participating in an IPv6 computer network.

An IPv6 address consists of 128 bits. An IP address serves the purpose of identifying an individual network interface of a host, locating it on the network, and thus permitting the routing of IP packets between hosts. For routing, IP addresses are present in fields of the packet header where they indicate the source and destination of the packet.

A **unicast** address identifies a single network interface. The Internet Protocol delivers packets sent to a unicast address to that specific interface.

An **anycast** address is assigned to a group of interfaces, usually belonging to different nodes. A packet sent to an anycast address is delivered to just one of the member interfaces, typically the nearest host, according to the routing protocol's definition of distance. Anycast addresses cannot be identified easily, they have the same format as unicast addresses, and differ only by their presence in the network at multiple points. Almost any unicast address can be employed as an anycast address.

A **multicast** address is also used by multiple hosts, which acquire the multicast address destination by participating in the multicast distribution protocol among the network routers. A packet that is sent to a multicast address is delivered to all interfaces that have joined the corresponding multicast group. IPv6 does not implement broadcast addressing. Broadcast's traditional role is subsumed by multicast addressing to the all-nodes link-local multicast group ff02::1. However, the use of the all-nodes group is not recommended, and most IPv6 protocols use a dedicated link-local multicast group to avoid disturbing every interface in the network.

Representation

An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets, a group sometimes also called a hextet. The groups are separated by colons (:). An example of an IPv6 address is:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

The hexadecimal digits are case-insensitive, but IETF recommendations suggest the use of lower case letters. The full representation of eight 4-digit groups may be simplified by several techniques, eliminating parts of the representation.

Leading zeroes in a group may be omitted, but each group must retain at least one hexadecimal digit. Thus, the example address may be written as:

2001:db8:85a3:0:0:8a2e:370:7334

One or more consecutive groups containing zeros only may be replaced with a single empty group, using two consecutive colons (::). The substitution may only be applied once in the address, however, because multiple occurrences would create an ambiguous representation. Thus, the example address can be further simplified:

2001:db8:85a3::8a2e:370:7334

The localhost (loopback) address, 0:0:0:0:0:0:0:1, and the IPv6 unspecified address, 0:0:0:0:0:0:0:0, are reduced to ::1 and ::, respectively.

Cisco IOS

Cisco technology is built around the Cisco Internetwork Operating System (IOS), which is the software that controls the routing and switching functions of internetworking devices. A solid understanding of the IOS is essential for a network administrator.

The Purpose of Cisco IOS: As with a computer, a router or switch cannot function without an operating system. Cisco calls its operating system the Cisco Internetwork Operating System or Cisco IOS. It is the embedded software architecture in all of the Cisco routers and is also the operating system of the Catalyst switches.

Without an operating system, the hardware does not have any capabilities. The Cisco IOS provides the following network services:

1. Basic routing and switching functions
2. Reliable and secure access to networked resources
3. Network scalability

Operation of Cisco IOS Software

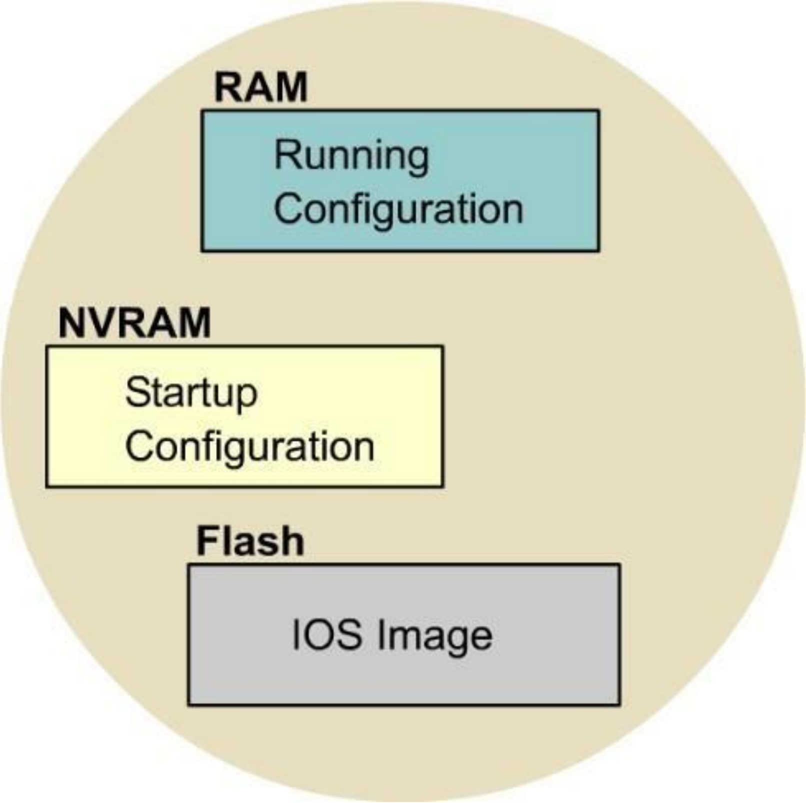
The Cisco IOS devices have three distinct operating environments ormodes:

1. ROM monitor
2. Boot ROM
3. Cisco IOS

The startup process of the router normally loads into RAM and executes one of these operating environments. The configuration register setting can be used by the system administrator to control the default start up mode for the router.

To see the IOS image and version that is running, use the show versioncommand, which also indicates the configuration register setting.

IOS File System Overview



Initial Startup of Cisco Routers

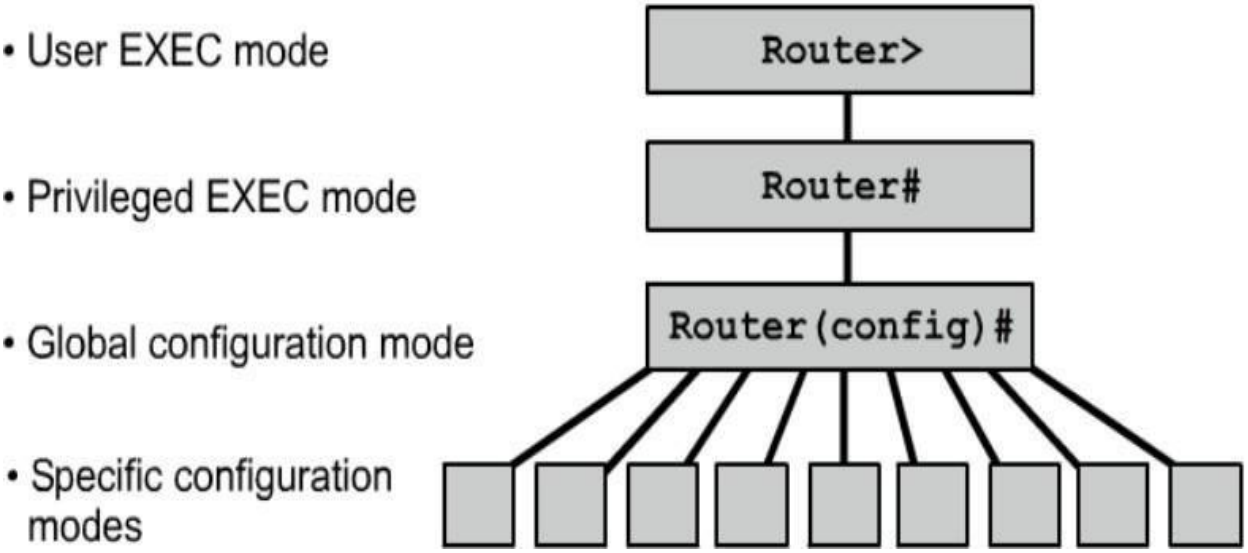
A router initializes by loading the bootstrap, the operating system, and aconfiguration file.If the router cannot find a configuration file, it enters setup mode.Upon completion of the setup mode a backup copy of the configuration filemay be saved to nonvolatile RAM (NVRAM).The goal of the startup routines for Cisco IOS software is to start the routeroperations. To do this, the startup routines must accomplish the following:

- Make sure that the router hardware is tested and functional.
- Find and load the Cisco IOS software.
- Find and apply the startup configuration file or enter the setupmode.

When a Cisco router powers up, it performs a power-on self-test (POST).During this self-test, the router executes diagnostics from ROM on allhardware modules.

Router User Interface Modes

The Cisco command-line interface (CLI) uses a hierarchical structure. Thisstructure requires entry into different modes to accomplish particular tasks.Each configuration mode is indicated with a distinctive prompt and allowsonly commands that are appropriate for that mode.As a security feature the Cisco IOS software separates sessions into twoaccess levels, user EXEC mode and privileged EXEC mode. The privileged EXEC mode is also known as enable mode.



Routing protocols

Routing Protocolsprocess for sharingroute information allows routers tocommunicate with other routers to updateand maintain therouting tables.Examples of routingprotocols that supportthe IP routed protocol are:

RIP, IGRP,EIGRP, OSPF, AND BGP.

Protocols used at the network layer that transfer data from one host to another acrossa router are called routed or routable protocols. The Internet Protocol (IP) and Novell'sInternetwork Packet Exchange (IPX) are examples of routed protocols. Routers userouting protocols to exchange routing tables and share routing information.

Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance vector routing protocol which has AD value 120 and works on the application layer of OSI model. RIP uses port number 520.

Hop Count:

Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hopes allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and hop count of 16 is considered as network unreachable.

Features of RIP:

1. Updates of the network are exchanged periodically.
2. Updates (routing information) are always broadcast.
3. Full routing tables are sent in updates.
4. Routers always trust on routing information received from neighbor routers. Thisis also known as routing on rumors.

RIP versions:

There are three versions of routing information protocol – **RIP Version1**, **RIP version2** and **RIPng**.

RIP V1	RIP V2	RIPng
Sends update as broadcast	Sends update as multicast	Sends update as multicast
Broadcast at 255.255.255.255	Multicast at 224.0.0.9	Multicast at FF02::9 (RIPng can only run on IPv6 networks)
Doesn't support authentication of update messages	Supports authentication of RIPv2 update messages	–
Classful routing protocol	Classless protocol, supports classful	Classless updates are sent

RIP v1 is known as Classful Routing Protocol because it doesn't send information of subnet mask in its routing update.
RIP v2 is known as Classless Routing Protocol because it sends information of subnet mask in its routing update.

Interior Gateway Routing Protocol (IGRP)

Cisco created Interior Gateway Routing Protocol (IGRP) in response to the limitations in Routing Information Protocol (RIP), which handles a maximum hop count of 15. IGRP supports a maximum hop count of up to 255. The primary two purposes of IGRP are to:

- Communicate routing information to all connected routers within its boundary or autonomous system
- Continue updating whenever there is a topological, network or path change that occurs

IGRP sends a notification of any new changes, and information about its status, to its neighbors every 90 seconds.IGRP manages a routing table with the most optimal path to respective nodes and to networks within the parent network. Because it is a distance vector protocol, IGRP uses several parameters to calculate the metric for the best path to a specific destination. These parameters include delay, bandwidth, reliability, load and maximum transmission unit (MTU).

Some features of Interior Gateway Routing Protocol (IGRP) are

- IGRP uses a sophisticated metric based on bandwidth and delay.

- IGRP uses triggered updates to speed-up convergence.

- IGRP supports unequal-cost load balancing to a single destination.

Distance vector routing is based on distance. A distance vector table is built by each router that contains two primary entries: a vector (destination) and a distance (cost).

EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP (Enhanced Interior Gateway Routing Protocol) is an advanced distance vector routing protocol. This protocol is an evolution of an earlier Cisco protocol called IGRP, which is now considered obsolete. EIGRP supports classless routing and VLSM, route summarization, incremental updates, load balancing and many other useful features. It is a Cisco proprietary protocol, so all routers in a network that is running EIGRP must be Cisco routers.

Routers running EIGRP must become neighbors before exchanging routing information. To dynamically discover neighbors, EIGRP routers use the multicast address of 224.0.0.10.

Each EIGRP router stores routing and topology information in three tables:

- **Neighbor table** – stores information about EIGRP neighbors
- **Topology table –** stores routing information learned from neighboring routers
- **Routing table** – stores the best routes

Administrative distance of EIGRP is 90, which is less than both the administrative distance of RIP and the administrative distance of OSPF, so EIGRP routes will be preferred over these routes. EIGRP uses Reliable Transport Protocol (RTP) for sending messages.

EIGRP calculates it's metric by using bandwidth, delay, reliability and load. By default, only bandwidth and delay are used when calculating metric, while reliability and load are set to zero.

EIGPR uses the concept of autonomous systems. An autonomous system is a set of EIGRP enabled routers that should become EIGRP neighbors. Each router inside an autonomous system must have the same autonomous system number configured, otherwise routers will not become neighbors.

EIGRP Neighbors

EIGRP must establish neighbor relationships with other EIGRP neighboring routers before exchanging routing information. To establish a neighbor relationships, routers send hello packets every couple of seconds. Hello packets are sent to the multicast address of 224.0.0.10.

Open Shortest Path First (OSPF) protocol

Open Shortest Path First (OSPF) is a link-state routing protocol which is used to find the best path between the source and the destination router using its own Shortest Path First).

It is a network layer protocol which works on the protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router (DR)/Backup Designated Router (BDR).

OSPF will listen to neighbors and gather all link state data available to build a topology map of all available paths in its network and then save the information in its topology database, also known as it's **Link-State Database** (**LSDB**).

Using the information from its topology database. From the information gathered, it will calculate the best shortest path to each reachable subnet/network using an algorithm called **Shortest Path First** (**SFP**).

OSPF will then construct **three tables** to store the following information:

- **Neighbor Table:** Contains all discovered OSPF neighbors with whom routing information will be interchanged
- **Topology Table:** Contains the entire road map of the network with all available OSPF routers and calculated best and alternative paths.
- **Routing Table:** Contain the current working best paths that will be used to forward data traffic between neighbors.

Understanding OSPF Areas

OSPF offers a very distinguishable feature named: **Routing Areas**. It means dividing routers inside a single autonomous system running OSPF, into areas where each area consists of a group of connected routers.

The idea of dividing the OSPF network into areas is to simplify administration and optimize available resources. Resource optimization is especially important for large enterprise networks with a plethora of network and links. Having many routers exchange the link state database could flood the network and reduce its efficiency – this was the need that led to the creation of concept Areas.

Areas are a logical collection of routers that carry the same **Area ID** or number inside of an OSPF network, the OSPF network itself can contain multiple areas, the first and main Area is called the backbone area **"Area 0"**,all other areas must connect to **Area0**

OSPF terms –

1. **Router I'd –** It is the highest active IP address present on the router. First, highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.

2. **Router priority –** It is a 8 bit value assigned to a router operating OSPF, used to elect DR and BDR in a broadcast network.

3. **Designated Router (DR) –** It is elected to minimize the number of adjacency formed. DR distributes the LSAs to all the other routers. DR is elected in a broadcast network to which all the other routers shares their DBD. In a broadcast network, router requests for an update to DR and DR will respond to that request with an update.

4. **Backup Designated Router (BDR) –** BDR is backup to DR in a broadcast network. When DR goes down, BDR becomes DR and performs its functions.

DR and BDR election –

DR and BDR election takes place in broadcast network or multi access network. Here is the criteria for the election:

1. Router having the highest router priority will be declared as DR.
2. If there is a tie in router priority then highest router I'd will be considered. First, highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.

Switching

Switching is a technology that decreases congestion in Ethernet, TokenRing, and FDDI LANs. Switching accomplishes this by reducing traffic andincreasing bandwidth. LAN switches are often used to replace shared hubsand are designed to work with existing cable infrastructures.

Switching equipment performs the following two basic operations:

- Switching data frames
- Maintaining switching operations

Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes.

At broad level, switching can be divided into two major categories:

- **Connectionless:** The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
- **Connection Oriented:** Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

Switching Methods

1. Store-and-Forward

The entire frame is received before any forwarding takes place. Filters areapplied before the frame is forwarded. Most reliable and also most latencyespecially when frames are large.

2. Cut-Through

The frame is forwarded through the switch before the entire frame isreceived. At a minimum the frame destination address must be read beforethe frame can be forwarded. This mode decreases the latency of thetransmission, but also reduces error detection.

3. Fragment-Free

Fragment-free switching filters out collision fragments before forwarding begins.Collision fragments are the majority of packet errors. In a properlyfunctioning network, collision fragments must be smaller than 64 bytes.Anything > 64 bytes is a valid packet and is usually received without error.

Switch Command Modes

Switches have several command modes. The default mode is User EXEC mode, which ends in agreater-than character (>).The commands available in User EXEC mode are limited tothose that change terminal settings, perform basic tests, and display system information.

The enable command is used to change from User EXECmode to Privileged EXEC mode, which ends in a pound-signcharacter (#).The configure command allows other command modes to beaccessed.

Spanning-Tree Protocol

Redundancy in a network is extremely important becauseredundancy allows networks to be fault tolerant.Redundant topologies based on switches and bridges aresusceptible to broadcast storms, multiple frametransmissions, and MAC address database instability. Therefore network redundancy requires careful planningand monitoring to function properly.

The Spanning-Tree Protocol is used in switched networksto create a loop free logical topology from a physicaltopology that has loops.The Spanning-Tree Protocolestablishes a root node, called theroot bridge/switch.

The Spanning-Tree Protocolconstructs a topology that has onepath for reaching every networknode. The resulting tree originatesfrom the root bridge/switch.The Spanning-Tree Protocol requiresnetwork devices to exchangemessages to detect bridging loops.Links that will cause a loop are putinto a blocking state.The message that a switch sends,allowing the formation of a loop freelogical topology, is called a BridgeProtocol Data Unit (BPDU).

Selecting the Root Bridge

The first decision that all switches in the network make, is to identifythe root bridge. The position of the root bridge in a network will affectthe traffic flow.When a switch is turned on, the spanning-tree algorithm is used toidentify the root bridge. BPDUs are sent out with the Bridge ID (BID).The BID consists of a bridge priority that defaults to 32768 and theswitch base MAC address.

When a switch first starts up, it assumes it is the root switch andsends BPDUs. These BPDUs contain the switch MAC address in boththe root and sender BID. As a switch receives a BPDU with a lowerroot BID it replaces that in the BPDUs that are sent out. All bridgessee these and decide that the bridge with the smallest BID value willbe the root bridge.A network administrator may want to influence the decision by settingthe switch priority to a smaller value than the default.

Bridge Protocol Data Unit (BPDU)

BPDUs contain enough information so that all switches can dothe following:

Select a single switch that will act as the root of thespanning treeCalculate the shortest path from itself to the root switchDesignate one of the switches as the closest one to theroot, for each LAN segment. This bridge is called the“designated switch”. The designated switch handles allcommunication from that LAN towards the root bridge.

Each non-root switch choose one of its ports as its rootport, this is the interface that gives the best path to theroot switch.Select ports that are part of the spanning tree, thedesignated ports. Non-designated ports are blocked.

Spanning Tree Operation

When the network has stabilized, it has converged and there is one spanningtree per network. As a result, for every switched network the followingelements exist:

One root bridge per networkone root port per non root bridgeone designated port per segmentUnused, non-designated portsRoot ports and designated ports are used for forwarding (F) data traffic.

Non-designated ports discard data traffic.Non-designated ports are called blocking (B) or discarding ports.

VLAN

VLAN is a logical grouping of networking devices. When we create VLAN, we actually break large broadcast domain in smaller broadcast domains. Consider VLAN as a subnet. Same as two different subnets cannot communicate with each other without router, different VLANs also requires router to communicate.

Advantage of VLAN

VLAN provides following advantages:-

- Solve broadcast problem
- Reduce the size of broadcast domains
- Allow us to add additional layer of security
- Make device management easier
- Allow us to implement the logical grouping of devices by function instead of location

VLAN Connections

During the configuration of VLAN on port, we need to know what type of connection it has.Switch supports two types of VLAN connection

- Access link
- Trunk link

Access link

Access link connection is the connection where switch port is connected with a device that has a standardized Ethernet NIC. Standard NIC only understand IEEE 802.3 or Ethernet II frames. Access link connection can only be assigned with single VLAN. That means all devices connected to this port will be in same broadcast domain.

For example twenty users are connected to a hub, and we connect that hub with an access link port on switch, then all of these users belong to same VLAN. If we want to keep ten users in another VLAN, then we have to purchase another hub. We need to plug in those ten users in that hub and then connect it with another access link port on switch.

Trunk link

Trunk link connection is the connection where switch port is connected with a device that is capable to understand multiple VLANs. Usually trunk link connection is used to connect two switches or switch to router. Remember earlier in this article I said that VLAN can span anywhere in network, that is happen due to trunk link connection. Trunking allows us to send or receive VLAN information across the network. To support trunking, original Ethernet frame is modified to carry VLAN information.

Trunk Tagging

In trunking a separate logical connection is created for each VLAN instead of a single physical connection. In tagging switch adds the source port's VLAN identifier to the frame so that other end device can understands what VLAN originated this frame. Based on this information destination switch can make intelligent forwarding decisions on not just the destination MAC address, but also the source VLAN identifier.

Since original Ethernet frame is modified to add information, standard NICs will not understand this information and will typically drop the frame. Therefore, we need to ensure that when we set up a trunk connection on a switch's port, the device at the other end also supports the same trunking protocol and has it configured. If the device at the other end doesn't understand these modified frames it will drop them. The modification of these frames, commonly called tagging. Tagging is done in hardware by application-specific integrated circuits (ASICs).

Switch supports two types of Ethernet trunking methods:

- **ISL [Inter Switch Link, Cisco's proprietary protocol for Ethernet]**
- **Dot1q [IEEE's 802.1Q, protocol for Ethernet]**

Router-on-a-stick

Router on a stick is a network configuration used to allow the routing of traffic between different VLANs.

Almost all enterprise networks use VLANs which stands for Virtual Local Area Network. Each VLAN is a separate subnet and in order to route IP packets in and out of those VLANs – or more accurately, the subnets that sit on each of those VLANs – some router needs to have an IP address in each subnet and have a connected route for each of those subnets. The hosts inside each subnet can then use the router IP addresses as their default gateways, respectively.

There are three options available for connecting a router to each subnet on a VLAN:

1. Use a router, with one router LAN interface and cable connected to the switch for each and every VLAN (typically not used).
2. Use a router with a VLAN trunk connected to a LAN switch
3. Use a Layer 3 switch

Router on a Stick Configuration

- Use the **interface** type number.subint command in global configuration mode to create a unique sub interface for each VLAN to be routed.
- Use the **encapsulation** dot1q vlan_id command to enable 802.1Q trunking and associate each VLAN with the sub interface.
- Use the **ip address** address mask command to configure the IP settings.

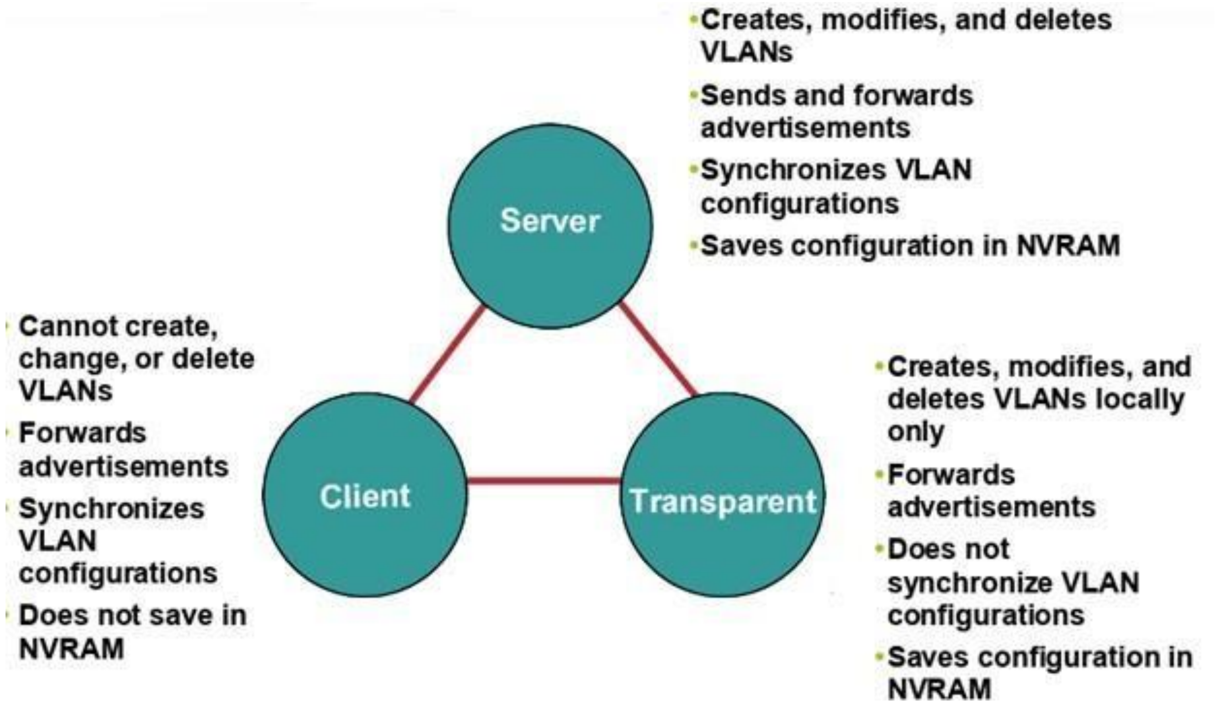
VTP Protocol

VLAN Trunk Protocol (VTP) reduces administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere. VTP is a Cisco-proprietary protocol that is available on most of the Cisco Catalyst series products.

VTP Protocol Features

- Advertises VLAN configuration information
- Maintains VLAN configuration consistency throughout a common administrative domain
- Sends advertisements on trunk ports only

VTP Modes


Creates, modifies, and deletes VLANs
Sends and forwards advertisements
Synchronizes VLAN configurations
Saves configuration in NVRAM
Server
Cannot create, change, or delete VLANs
Forwards advertisements
Synchronizes VLAN configurations
Does not save in NVRAM
Client
Transparent
Creates, modifies, and deletes VLANs locally only
Forwards advertisements
Does not synchronize VLAN configurations
Saves configuration in NVRAM

VTP Operation

- VTP advertisements are sent as multicast frames
- VTP servers and clients are synchronized to the latest update identifiedrevision number.
- VTP advertisements are sent every 5 minutes or when there is a change.

VTP Configuration Guidelines

Configure the following:

- VTP domain name
- VTP mode (server mode is the default)
- VTP pruning
- VTP password

Be cautious when adding a new switch into an existingdomain.Add a new switch in a Client mode to get the lastup-to-date information from the network then convert it toServer mode.Add all new configurations to switch in transparent modeand check your configuration well then convert it toServer mode to prevent the switch from propagatingincorrect VLAN information.

ACL (Access Control Lists)

ACLs are lists of conditions that are applied to traffic travelingacross a router's interface. These lists tell the router what typesof packets to accept or deny. Acceptance and denial can bebased on specified conditions.

ACLs can be created for all routed network protocols, such asInternet Protocol (IP) and Internetwork Packet Exchange (IPX).ACLs can be configured at the router to control access to anetwork or subnet.

Some ACL decision points are source and destination addresses,protocols, and upper-layer port numbers.ACLs must be defined on a per-protocol, per direction, or per portbasis.

The following are some of the primary reasons to create ACLs:

- Limit network traffic and increase network performance.
- Provide traffic flow control.
- Provide a basic level of security for network access.

Decide which types of traffic are forwarded or blocked atthe router interfaces. For example: Permit e-mail traffic tobe routed, but block all telnet traffic.Allow an administrator to control what areas a client can accesson a network.

If ACLs are not configured on the router, all packets passingthrough the router will be allowed onto all parts of the network.

Basic Rules for ACLs

These basic rules should be followed when creating and applying access lists:

- One access list per protocol per direction. Standard IP access lists should be applied closest to the destination.
- Extended IP access lists should be applied closest to the source. Use the inbound or outbound interface reference as if looking at the portfrom inside the router.

- Statements are processed sequentially from the top of list to the bottomuntil amatch is found, if no match is found then the packet is denied.
- There is an implicit deny at the end of all access lists. This will not appearinthe configuration listing.
- Access list entries should filter in the order from specific to general.Specifichosts should be denied first, and groups or general filters shouldcome last.Never work with an access list that is actively applied.
- New lines are always added to the end of the access list.A no access-list x command will remove the whole list.
- It is not possibletoselectively add and remove lines with numbered ACLs.
- Outbound filters do not affect traffic originating from the local router.

Standard ACLs

Standard ACLs check the source address of IP packets that are routed.The comparison will result in either permit or deny access for an entire protocolsuite, based on the network, subnet, and host addresses.

The standard version of the access-list global configuration command is used todefine a standard ACL with a number in the range of 1 to 99 (also from 1300 to 1999 in recent IOS).

If there is no wildcard mask. The default mask is used, which is 0.0.0.0.(This only works with Standard ACLs and is the same thing as using host.)

The full syntax of the standard ACL command is:

Router(config)#access-list access-list-number {deny | permit} source [source-wildcard] [log]

The no form of this command is used to remove a standard ACL. This is the syntax:

Router(config)#no access-list access-list-number

Extended ACLs

Extended ACLs are used more often than standard ACLs because they provide a greater range of control. Extended ACLs check the source and destination packetaddresses as well as being able to check for protocols and port numbers.

The syntax for the extended ACL statement can get very long and often will wrap inthe terminal window.The wildcards also have the option of using the host or any keywords in thecommand.

At the end of the extended ACL statement, additional precision is gained from a fieldthat specifies the optional Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port number.

Logical operations may be specified such as, equal (eq), not equal (neq), greaterthan (gt), and less than (lt), that the extended ACL will perform on specific protocols.Extended ACLs use an access-list-number in the range 100 to 199 (also from 2000to 2699 in recent IOS).

Named ACLs

IP named ACLs were introduced in Cisco IOS Software,allowing standard and extended ACLs to be given names instead ofnumbers.The advantages that a named access list provides are:

- Intuitively identify an ACL using an alphanumeric name.
- Eliminate the limit of 798 simple and 799 extended ACLs Named ACLs provide the ability to modify ACLs without deleting them completely and then reconfiguring them.
- Named ACLs are not compatible with Cisco IOS releases prior to Release 11.2.

The same name may not be used for multiple ACLs.

Point-to-Point Protocol (PPP)

PPP is a standard encapsulation protocol for thetransport of different Network Layer protocols(including, but not limited to, IP).It has the following main functional components

- Link Control Protocol (LCP) that establishes, authenticates, and tests the data link connection.
- Network Control Protocols (NCPs) that establishes and configure different network layer protocols.

PPP discards frames that do not pass the error check.PPP is a standard protocol, and so it canbe used with all types of routers (not CiscoProprietary).

PPP Session Establishment:

Establishing a PPP session is a two stage process comprising:

1. Link establishment and configuration negotiation—before PPP exchanges any network layer datagrams (for example, IP), the LCP must first open the connection and negotiate configuration options. This phase is complete when the receiving router sends a configuration-acknowledgment frame back to the router initiating the connection.

2. Network layer protocol configuration negotiation—after the LCP has finished the link quality determination phase, the appropriate NCP can separately configure the Network layer protocols, and bring them up. If the LCP closes the link, it informs the network layer protocols so that they can take appropriate action.

PPP LCP Features

1. Authentication
2. Compression
3. Multilink PPP
4. Error Detection
5. Looped Link Detection

Authentication

PPP can be authenticated by either:

- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication

Protocol)PAP (Password Authentication Protocol)

PAP provides a simple method for a remote node to establish its identity using a two-way handshake. PAP is not interactive. When the ppp authentication pap command is used, the username and password are sent as one LCP data package, rather than the server CHAP (Challenge Handshake Authentication Protocol) **|** Page 13 Point-to-Point Protocol (PPP) sending a login prompt and waiting for a response. After PPP completes the link establishment phase, the remote node repeatedly sends a username-password pair across the link until the sending node acknowledges it or terminates the connection. At the receiving node, the username-password is checked by an authentication server that either allows or denies the connection. An accept or reject message is returned to the requester. PAP is not a strong authentication protocol. Using PAP, you send passwords across the link in clear text and there is no protection from playback or repeated trial-and-error attacks.

CHAP (Challenge Handshake Authentication Protocol)

CHAP provides protection against playback attack by using a variable challenge value that is unique and unpredictable. Because the challenge is unique and random, the resulting hash value is also unique and random.

If an incoming CHAP request requires no authentication, then CHAP progresses to the next stage. If an incoming PPP request requires authentication, then it can be authenticated against the local user database. Successful authentication progresses to the next stage, while an authentication failure will disconnect and drop the incoming PPP request. The PPP interface of the router being authenticated will be configured to provide a secret password to the authenticator.

The Authenticator will be configured to compare the received secret password against a user data base.

Compression

Compression enables higher data throughputacross the link.Different compression schemes are available:

Predictor: checks if the data was already compressed.

Stacker: it looks at the data stream and only sendseach type of data once with information about wherethe type occurs and then the receiving side uses thisinformation to reassemble the data stream.

MPPC (Microsoft Point-to-Point Compression):allows Cisco routers to compress data with Microsoftclients.

PPP Multilink

PPP Multilink provides load balancing overdialer interfaces-including ISDN,synchronous, and asynchronousinterfaces.This can improve throughput and reducelatency between systems by splittingpackets and sending fragments overparallel circuits.

Error Detection

PPP can take down a link based on thevalue of what is called LQM (Link QualityMonitor) as it gets the ratio of corruptedpackets to the total number of sentpackets, and according to a predeterminedvalue, the link can be brought down if it isthought that its performance is beyondlimits accepted.

Looped Link Detection

PPP can detect looped links (that aresometimes done by Teleco companies)using what is called Magic Number.Every router will have a magic number,and if packets were received having thesame router’s magic number, then the linkis looped.

Network Address Translation (NAT)

Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.

NAT Addressing Terms

- **Inside Local:** The term “inside” refers to an address used for a host inside an enterprise. It is the actual IP address assigned to a host in the private enterprise network.
- **Inside Global:** NAT uses an inside global address to represent the inside host as the packet is sent through the outside network, typically the Internet. A NAT router changes the source IP address of a packet sent by an inside host from an inside local. Address to an inside global address as the packet goes from the inside to the outside network.
- **Outside Global:** The term “outside” refers to an address used for a host outside an enterprise, the Internet. An outside global is the actual IP address assigned toa host that resides in the outside network, typically theInternet.
- **Outside Local:**NAT uses an outside local address to represent theoutside host as the packet is sent through the privateenterprise network.A NAT router changes a packet’s destination IPaddress, sent from an outside global address to aninside host, as the packet goes from the outside to theinside network.

Types Of NAT

There are different types of NAT that can be used, which are

- Static NAT
- Dynamic NAT
- Overloading NAT with PAT (NAPT)

Static NAT

Static NAT defines a one-to-one mapping from one IP subnet to another IP subnet. The mapping includes destination IP address translation in one direction and source IP address translation in the reverse direction. From the NAT device, the original destination address is the virtual host IP address while the mapped-to address is the real host IP address.

Static NAT allows connections to be originated from either side of the network, but translation is limited to one-to-one or between blocks of addresses of the same size. For each private address, a public address must be allocated. No address pools are necessary.

Dynamic NAT

Like static NAT, the NAT router creates aone-to-one mapping between an insidelocal and inside global address andchanges the IP addresses in packets asthey exit and enter the inside network.However, the mapping of an inside localaddress to an inside global addresshappens dynamically.

Dynamic NAT sets up a pool of possibleinside global addresses and definescriteria for the set of inside local IPaddresses whose traffic should betranslated with NAT.Thedynamic entry in the NAT table staysin there as long as traffic flowsoccasionally.

Overloading NAT with PAT

NAT Overloading or Port Address Translation (PAT) is a modified form of dynamic NAT where the number of inside local addresses is greater than the number of inside global addresses. Mostly, there is just a single inside global IP address providing Internet access to all inside hosts. NAT Overloading is the only flavor of NAT that actually conserves IP addresses and it is also the most popular form of NAT as well.

TACACS+ and RADIUS

To provide a centralized management system for the authentication, authorization and accounting (AAA framework), Access Control Server (ACS) is used. For the communication between the client and the ACS server, two protocols are used namely TACACS+ and RADIUS.

TACACS+

Terminal Access Controller Access Control System (TACACS+) is Cisco proprietary protocol which is used for the communication of the Cisco client and Cisco ACS server. It uses TCP port number 49 which makes it reliable.

RADIUS

Remote Access Dial In User Service (RADIUS) is an open standard protocol used for the communication between any vendor AAA client and ACS server. If one of the client or server is from any other vendor (other than Cisco) then we have to use RADIUS. It uses port number 1812 for authentication and authorization and 1813 for accounting.

Similarities

The process is start by Network Access Device (NAD – client of TACACS+ or RADIUS). NAD contact the TACACS+ or RADIUS server and transmit the request for authentication (username and password) to the server. First, NAD obtain username prompt and transmit the username to the server and then again the server is contact by NAD to obtain password prompt and then the password is send to the server.
The server replies with access-accept message if the credentials are valid otherwise send an access-reject message to the client. Further authorization and accounting is different in both protocols as authentication and authorization is combined in RADIUS

Differences –

TACACS+	RADIUS
Cisco proprietary protocol	open standard protocol
It uses TCP as transmission protocol	It uses UDP as transmission protocol
It uses TCP port number 49.	It uses UDP port number 1812 for authentication and authorization and 1813 for accounting.
Authentication, Authorization and Accounting is separated in TACACS+.	Authentication and Authorization is combined in RADIUS.
All the AAA packets are encrypted.	Only the password are encrypted while the other information such as username, accounting information etc. are not encrypted.
Preferably used for ACS.	used when ISE is used
It provides more granular control i.e. can specify the particular command for authorization.	No external authorization of commands supported.
TACACS+ offers multiprotocol support	No multiprotocol support.
Used for device administration.	used for network access

Advantages (TACACS+ over RADIUS) –

1. As TACACS+ uses TCP therefore more reliable than RADIUS.
2. TACACS+ provides more control over the authorization of commands while in RADIUS, no external authorization of commands is supported.
3. All the AAA packets are encrypted in TACACS+ while only the passwords are encrypted in RADIUS i.e. more secure.

Advantage (RADIUS over TACACS+) –

1. As it is open standard therefore RADIUS can be used with other vendors device while because TACACS+ is Cisco proprietary, it can be used with Cisco devices only.
2. It has more extensive accounting support than TACACS+.

Software-defined networking (SDN)

Software-defined networking (SDN) is an architecture that aims to make networks agile and flexible. The goal of SDN is to improve network control by enabling enterprises and service providers to respond quickly to changing business requirements.

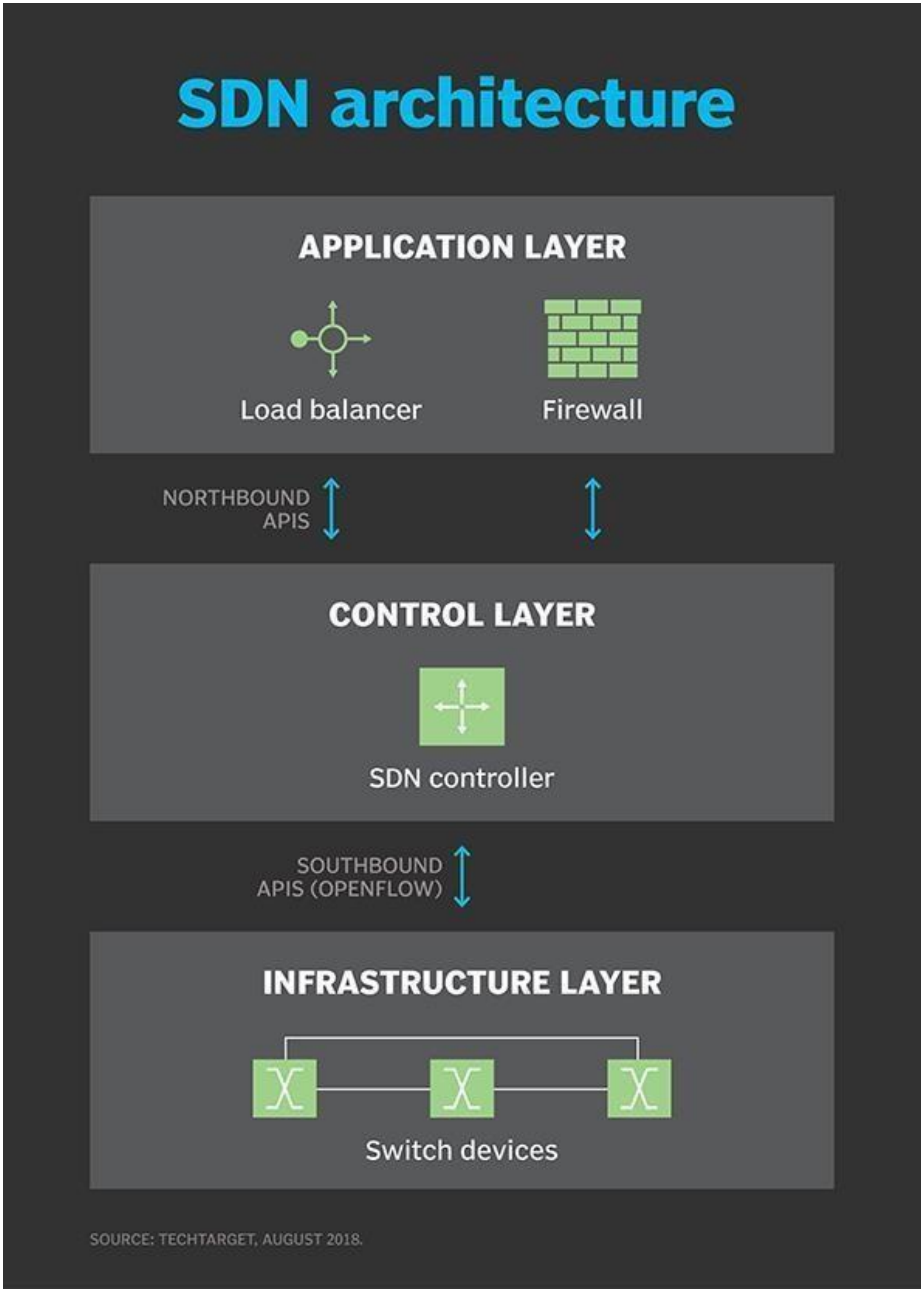
In a software-defined network, a network engineer or administrator can shape traffic from a centralized control console without having to touch individual switches in the network. The centralized SDN controller directs the switches to deliver network services wherever they're needed, regardless of the specific connections between a server and devices.

This process is a move away from traditional network architecture, in which individual network devices make traffic decisions based on their configured routing tables.

SDN architecture

A typical representation of SDN architecture comprises three layers: the application layer, the control layer and the infrastructure layer.

The application layer, not surprisingly, contains the typical network applications or functions organizations use, which can include intrusion detection systems, load balancing or firewalls. Where a traditional network would use a specialized appliance, such as a firewall or load balancer, a software-defined network replaces the appliance with an application that uses the controller to manage data plane behavior.



SOURCE: TECHTARGET, AUGUST 2018.

SDN architecture separates the network into three distinguishable layers, connected through northbound and southbound APIs.

The control layer represents the centralized SDN controller software that acts as the brain of the software-defined network. This controller resides on a server and manages policies and the flow of traffic throughout the network.

The infrastructure layer is made up of the physical switches in the network.These three layers communicate using respective northbound and southbound application programming interfaces (APIs). For example, applications talk to the controller through its northbound interface, while the controller and switches communicate using southbound interfaces, such as OpenFlow -although other protocols exist.

There is currently no formal standard for the controller's northbound API to match OpenFlow as a general southbound interface. It is likely the Open Daylight controller's northbound API may emerge as a de facto standard over time, given its broad vendor support.

Southbound interfaces define the way the SDN controller should interact with the data plane (aka forwarding plane) to make adjustments to the network, so it can better adapt to changing requirements. OpenFlow is a well-known southbound interface. With OpenFlow, entries can be added and removed to the internal flow-table of switches and potentially routers to make the network more responsive to real-time traffic demands.

Northbound interfaces define the way the SDN controller should interact with the application plane. Applications and services are things like load-balancers, firewalls, security services and cloud resources. The idea is to abstract the inner-workings of the network, so that application developers can ‘hook’ into the network and make changes to accommodate the needs of the application without having to understand exactly what that means for the network.