

New Hires Topics for Cisco Account

Content

1. Section 1.....	2
1.1. Unit 1: Computer parts (Hard disk, cpu, memory).....	2
1.2. Unit 2: Computer devices (Input/output devices)	3
1.3. Unit 3: Operating system/communication language.....	5
1.4. Unit 4: Application programs (email, browser, instant message, etc).....	5
1.5. Unit 5: URL (Difference between folder path, e-mail, ip, url)	7
1.6. Unit 6: Client-Server (infrastructure).....	8
1.7. Unit 7: Network components (Physical media, DSL modem)	9
1.8. Unit 8: Units of measure for computer data (Bytes)	11
1.9. Unit 9: Network Tool: PING	12
2. Section 2.....	14
2.1. Unit 1: TCP/IP model (OSI model) and Protocols per layer.....	14
2.2. Unit 2: TCP vs UDP.....	18
2.3. Unit 3: IP addressing (IP config)	19
2.4. Unit 4: Subnetting (Subnet ID and broadcast)	23
2.5. Unit 5: MAC address (OUI), Switch LED status, Switch functionality (Flooding)	25
2.6. Unit 6: Vlan and Trunk (Native Vlan).....	29
2.7. Unit 7: ARP (Windows Commands)	32
2.8. Unit 8: InterVlan	34
2.9. Unit 9: Static Routing.....	35
3. Section 3.....	38
3.1. Unit 1: Dynamic Routing (Administrative Distance and metric).....	38
3.2. Unit 2: DHCP (DHCP relay, Renewal and rebinding, DORA process).....	42
3.3. Unit 3: ACL (Standard and Extended) (Statement order)	46
3.4. Unit 4: NAT (Static, Dynamic NAT, PAT, Overload).....	49

1. Section 1

1.1. Unit 1: Computer parts (Hard disk, cpu, memory)

What is a computer?

A computer is a machine that is made up of various parts or components which help it in carrying out instructions which are in the form of arithmetic commands or different algorithms for it to process.

Components of computer

All types of computers follow the same basic logical structure and perform the following seven basic operations for converting raw input data into information useful to their users.

Motherboard:

A motherboard is a circuit board through which all the different components of a computer communications and it keeps everything together. The input and output devices are plugged into the motherboard for function.

Input Unit:

This unit contains devices with the help of which we enter data into the computer. This unit creates a link between the user and the computer. The input devices translate the information into a form understandable by the computer. (Example: keyboard, joystick, etc.)

Output Unit:

The computer's response is relayed through output devices in the form of a visual response (monitor), sound (speakers), or media devices (CD or DVD drives). The function of these devices is to convert the machine's response into a format that the computer user can understand.

Central Processing Unit (CPU):

CPU is considered as the brain of the computer. CPU performs all types of data processing operations. It stores data, intermediate results, and instructions (program). It controls the operation of all parts of the computer.

CPU itself has the following three components –

- ALU (Arithmetic Logic Unit)
- Memory Unit
- Control Unit

Memory Unit

The information entered through the input devices is saved in the memory of the CPU and then passed on to the other parts. Similarly, when the output is ready it is saved in the memory before the result is given to the user.

Control Unit

This unit controls the functioning component of the computer. It collects the data entered, leads it on for processing after the processing is done, receives the output and provides it to the user. So, getting instructions, decoding it, signaling the execution, and receiving the output is done by the control center and hence it is called the center of all processing actions that happen in the computer.

Arithmetic and Logical Unit

This unit does mathematical calculations, arithmetic operations, comparison of data and decision making. It has circuits that are built for addition, subtraction, multiplication, division, and other calculations.

Graphics Processing Unit (GPU):

GPU is a specialized processor that is created to accelerate graphics processing. It can render many pieces of data making them ideal for machine learning, video editing and gaming.

Random Access Memory (RAM):

RAM is the most referred component in a computer. The RAM is also known as the volatile memory since it gets erased every time the computer restarts. It stores the data regarding the programs which are frequently accessed programs and processes. It helps programs to start up and close quickly.

Storage Unit:

The computers need to store all their data and they have either a Hard Disk Drive (HDD) or a Solid-State Drive (SSD) for this purpose. Hard disk drives are disks that store data, and this data is read by a mechanical arm. Solid-State drives are like SIM cards in mobile phones. They have no moving parts and are faster than hard drives. There is no need for a mechanical arm to find data on a physical location on the drive and therefore this takes no time at all.

1.2. Unit 2: Computer devices (Input/output devices)

The functioning of a computer system is based on the combined usage of both input and output devices. Using an input device, we can give instructions to the computer to perform an action and the device reverts to our action through an output device.

What is an Input Device?

A piece of equipment/hardware which helps us enter data into a computer is called an input device. For example, keyboard, mouse, etc.

Given below is the list of the most common input devices along with brief information about each of them.

Keyboard

A simple device comprising keys and each key denotes either an alphabet, number or number commands which can be given to a computer for various actions to be performed. The keyboard is

an essential input device and computer and laptops both use keyboards to give commands to the computer.

Mouse

It is also known as a pointing device. Using a mouse, we can directly click on the various icons present on the system and open various files and programs.

In case of laptops, the touchpad is given as a replacement of the mouse which helps in the movement of the mouse pointer.

Joystick

It is a device which comprises a stick which is attached at an angle to the base so that it can be moved and controlled. Mostly used to control the movement in video games.

Light Pen

It is a wand-like looking device which can directly be moved over the device's screen, it is light-sensitive.

Microphone

Using a microphone, sound can be stored in a device in its digital form, it converts sound into an electrical signal. To record or reproduce a sound created using a microphone, it needs to be connected to an amplifier.

Scanner

This device can scan images or text and convert it into a digital signal, when we place any piece of a document on a scanner, it converts it into a digital signal and displays it on the computer screen.

Barcode Reader

It is a kind of an optical scanner that can read bar codes. A source of light is passed through a bar code, and its aspects and details are displayed on the screen.

What is an Output Device?

A piece of equipment/hardware which gives out the result of the entered input, once it is processed (i.e., converts data from machine language to a human-understandable language), is called an output device. For example, printer, monitor, etc.

The commonly used output devices have been listed below with a summary of what their function is and how they can be used.

Monitor

The device which displays all the icons, text, images, etc. over a screen is called the Monitor, when we ask the computer to perform an action, the result of that action is displayed on the monitor.

Printer

A device which makes a copy of the pictorial or textual content, usually over a paper is called a printer.

Speakers

A device through which we can listen to a sound as an outcome of what we command a computer to do is called a speaker. Speakers are attached with a computer system and are a hardware device which can be attached separately.

With the advancement in technology, speakers are now available which are wireless and can be connected using Bluetooth or other applications.

Projector

An optical device which presents an image or moving images onto a projection screen is called a projector. Most commonly these projectors are used in auditoriums and movie theatres for the display of the videos or lighting.

Headphones

They perform the same function as a speaker, the only difference is the frequency of sound. Using speakers, the sound can be heard over a larger area and using headphones, the sound is only audible to the person using them. Also known as earphones or headset.

1.3. Unit 3: Operating system

What is an Operating System?

An operating system is a software which performs all the basic tasks that controls and manages the hardware and other software on a computer.

All computers and computer-like devices require operating systems, including your laptop, tablet, desktop, smartphone, smartwatch, and router.

Following are some of important functions of an operating System.

- Memory Management
- Processor Management
- Device Management
- File Management
- Security
- Control over system performance
- Job accounting
- Error detecting aids
- Coordination between other software and users

Operating System Examples

There are various examples of Operating System, which are given below.

- Microsoft Windows (Windows 10, 8.1, 7).
- Microsoft DOS (MS-DOS)
- Ubuntu OS
- Mac OS
- Apple IOS
- Linux OS
- UNIX OS
- Android OS
- Fedora OS

1.4. Unit 4: Application programs (email, browser, instant message, etc.)

What is an Application Program?

An application program is a comprehensive, self-contained program that performs a particular function directly for the user. Among many others, application programs include:

- Email:
Outlook, Gmail, Yahoo, etc.
- Web browsers
Google Chrome, Mozilla Firefox, Opera, Internet Explorer, Netscape Navigator, etc.
- Instant Message
Messenger, Facebook chat, Instagram chat, etc.
- Games
Halo, Call of Duty, Free Fire, etc.
- Word processors
Microsoft word, Google drive DOCs, etc.
- Accounting software
Siigo, Ziur, etc.
- Database management
- Enterprise software

Because every program has a particular application for the end user, the term "application" is used. For instance, a word processor can help the user create an article, whereas a game application can be used for entertainment.

An application program is also known as an application or application software.

1.5. Unit 5: URL (Difference between folder path, e-mail, ip, url)

Folder Path

This term is descriptive in that it represents a type of "road map" to a specific file or directory. (Alternate definition: A path is a list, beginning with a drive letter, that tells which folders to open so that you can find a file or another folder.)

If you opened a Windows Explorer folder window and wanted to get to example.docx that was saved in the Users directory, you would start at **Local Disk C**, then you would open the **Users** directory and find example.docx inside. The entire path to the file would be (shown on below Figure 1):

C:\Users\example.docx

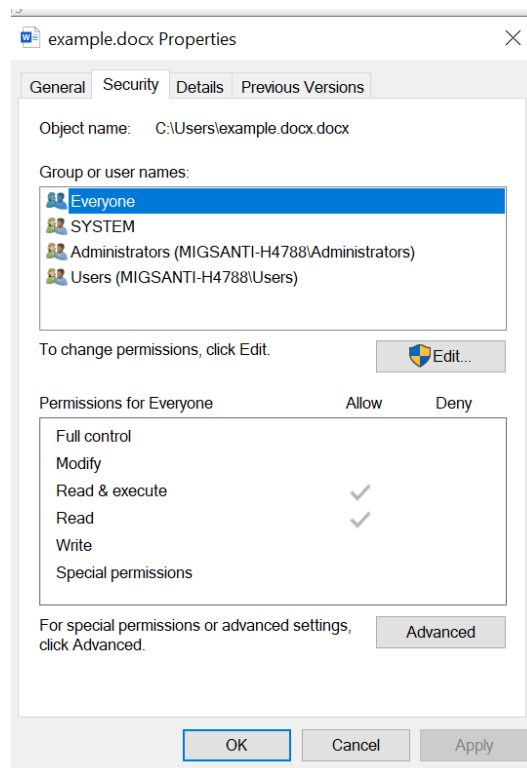


Figure 1. Folder Path

Email

An email address is a unique identifier for an email account. It is used to both send and receive email messages over the Internet. Like physical mail, an email message requires an address for both the sender and recipient to be sent successfully.

Every email address has two main parts: a username and domain name. The username comes first, followed by an at (@) symbol, followed by the domain name. In the example below, "mail" is the username and "colombia.com" is the domain name.

mail@colombia.com

IP address

An IP address (internet protocol address) is a numerical representation that uniquely identifies a specific interface on the network.

Addresses in IPv4 are 32-bits long. This allows for a maximum of 4,294,967,296 (2^{32}) unique addresses. Addresses in IPv6 are 128-bits, which allows for 3.4×10^{38} (2^{128}) unique addresses.

IP addresses are binary numbers but are typically expressed in decimal form (IPv4) or hexadecimal form (IPv6) to make reading and using them easier for humans.

An IPv4 address is, as such, generally shown as 4 octets (8 bits) of numbers from 0-255 represented in decimal form instead of binary form.

192.168.17.43 is an example of IPv4 address

URL

Also known as an internet address or web address, a URL (Uniform Resource Locator) is a URI and standardized naming convention for addressing documents accessible over the Internet and Intranet. The URL makes it possible for a computer to locate and open a web page on a different computer on the Internet. An example of a URL is **<https://www.cisco.com>**, the URL for the Cisco website.

A URL contains the following information:

- The protocol used to access the resource.
- The location of the server (whether by IP address or domain name).
- The port number on the server (optional).
- The location of the resource in the directory structure of the server.

1.6. Unit 6: Client-Server (infrastructure)

Client-server architecture

Client-server architecture (shown on below Figure 2), architecture of a computer network in which many clients (remote processors) request and receive service from a centralized server (host computer). Client computers provide an interface to allow a computer user to request services of the server and to display the results the server returns. Servers wait for requests to arrive from clients and then respond to them. Ideally, a server provides a standardized transparent interface to clients so that clients need not be aware of the specifics of the system (i.e., the hardware and software) that is providing the service. Clients are often situated at workstations or on personal computers, while servers are located elsewhere on the network, usually on more powerful machines.

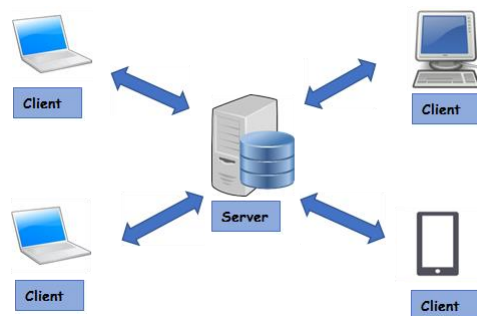


Figure 2. Client-Server Infrastructure

1.7. Unit 7: Network components (Physical media, DSL modem)

Computer Network Components

Computer networks share common devices and features, including **NIC (Network Interface Card)**, **transmission media (Physical media as cable)**, **Hub**, **Switch**, **Router**, and **modem**.

Network Interface Card.

NIC mainly provide the physical interface between computer and cabling. NIC prepares data, sends the data, and controls the flow of data. It can also receive and translate the data into bytes for the CPU to understand.

There are two types of NIC:

- 1) Wired NIC
- 2) Wireless NIC

Transmission Media.

Transmission media are the facilities used to interconnect computers in a network, such as twisted-pair wire, coaxial cable, and optical fiber cable. Transmission media are sometimes called transmission medium channels, links, or lines.

There are three types of cables used in transmission:

- Twisted pair cable
- Coaxial cable
- Fiber-optic cable

Hub.

Hub acts as a device that connects all the computer in a network to each other. Any request that comes from a client computer first received by Hub and then hub transmit this request over a network so that the correct server receives and respond to it.

- A network hub is basically a centralized distribution point for all the data transmission in a network.
- Hub is a passive device.
- The hub receives the data and then rebroadcasts the data to other computers that are connected to it. Hub mainly does not know the destination of a received data packet. Thus, it is required to send copies of data packets to all the hub connections.
- Also, Hubs consumes more bandwidth on the network and thus limits the amount of communication.
- One disadvantage of using hubs is that they do not have the intelligence to find out the best path for the data packets which then leads to inefficiencies and wastage.

Switch.

A switch is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub. The Switch contains the updated table that decides where the data is transmitted or not. Switch delivers the message to the correct destination based on the physical address present in the incoming message. A Switch does not broadcast the message to the entire network like the Hub.

- The switch is a network component and is mainly used to connect the segments of the network.
- The switch is more intelligent than the network hub.
- Mainly Switches can inspect the data packets as soon as they are received, then determine the source and destination of that packet, and then forward it appropriately.
- Switch differs from the hub as it also contains ports of different speeds.
- Before forwarding the data to the ports switch performs the error checking and this feature makes the switch efficient.
- As the switch delivers the message to the connected device it was intended for, thus it conserves the bandwidth of the network and offers better performance than the hub.
- The most important feature of the switch is that it supports unicast (one to one), multicast (one to many), and broadcast (one to all) communications.
- The switch makes use of MAC address to send data packets to the selected destination ports.

Router.

When we talk about computer network components, the other device that used to connect a LAN with an internet connection is called Router. When you have two distinct networks (LANs) or want to share a single internet connection to multiple computers, we use a Router.

- A router works in a Layer 3 (Network layer) of the OSI Reference model.
- A router forwards the packet based on the information available in the routing table.
- It determines the best path from the available paths for the transmission of the packet.

Modem (DSL).

The modem is basically a hardware component that mainly allows a computer or any other device like a router, switch to connect to the Internet. A modem is basically a shorthand form of Modulator-Demodulator.

- A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
- A modem is not integrated with the motherboard rather than it is installed on the PCI slot found on the motherboard.
- It stands for Modulator/Demodulator. It converts the digital data into an analog signal over the telephone lines.

1.8. Unit 8: Units of measure for computer data (Bytes)

What is a Byte?

A byte is a storage unit capable of representing a single character, such as a letter, number, or symbol. Technically speaking, a byte is a sequence of binary bits in a serialized data stream in data transmission systems. In most computers, one byte is equated to eight smaller units called bits, although the size of a byte has always been dependent on hardware. On table 1, we have some conversion for bytes units

Memory capacity hierarchy and conversion chart		
UNIT	ABBREVIATION	APPROXIMATE SIZE
bit	b	Binary digit, single 1 or 0
nibble	—	4 bits
byte/octet	B	8 bits
kilobyte	KB	1,024 bytes or 10^3 bytes
megabyte	MB	1,024 KB or 10^6 bytes
gigabyte	GB	1,024 MB or 10^9 bytes
terabyte	TB	1,024 GB or 10^{12} bytes
petabyte	PB	1,024 TB or 10^{15} bytes
exabyte	EB	1,024 PB or 10^{18} bytes
zettabyte	ZB	1,024 EB or 10^{21} bytes
yottabyte	YB	1,024 ZB or 10^{24} bytes

Table 1. Bytes conversion

Example:

1 GB = 1024 MB

1 MB = 1024 KB

1 KB = 1024 B

1 B = 8 bits

1.9. Unit 9: Network Tool: PING

Accessing the Windows Command Prompt

To run any of the network tools or utilities described in this article, you need to first open a Windows Command Prompt. To open a command prompt on Windows 8 or Windows 10, proceed as follows.

1. Right-click on the **Start** button in the lower-left corner of the screen and, from the menu, select **Command Prompt** (or **Command Prompt (Admin)** if the task requires Admin rights).

On Figure 3, we can see how the CMD (Command Prompt) looks on Windows machine.

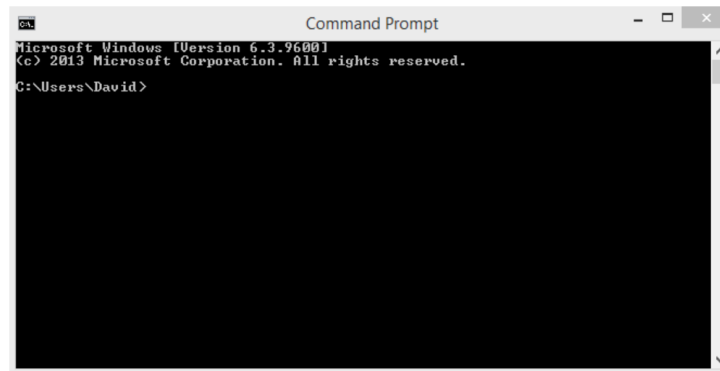


Figure 3. Command Prompt Interface

What is ping?

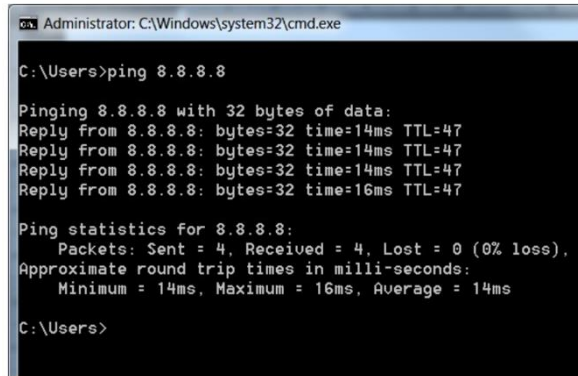
Ping is a Terminal / Shell command utility used as a simple way to verify that a machine has internet access and can communicate with other computers or network devices.

Some of the functions of the ping command are:

- Test network connectivity: local network, internet
- Troubleshoot network interface card
- Test DNS name resolution issues

To ping a device, proceed as follows.

1. Open a Windows Command Prompt window.
2. At the command prompt, type, ping <IP address>, as shown below on Figure 4.

A screenshot of a Windows Command Prompt window. The title bar reads "Administrator: C:\Windows\system32\cmd.exe". The command prompt shows the user typing "C:\Users>ping 8.8.8.8". The output displays four successful replies from 8.8.8.8, each with 32 bytes of data, a time of 14ms or 16ms, and a TTL of 47. It also shows ping statistics for 8.8.8.8: 4 packets sent, 4 received, 0% loss, with round trip times of 14ms minimum, 16ms maximum, and 14ms average. The prompt ends with "C:\Users>".

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=14ms TTL=47
Reply from 8.8.8.8: bytes=32 time=14ms TTL=47
Reply from 8.8.8.8: bytes=32 time=14ms TTL=47
Reply from 8.8.8.8: bytes=32 time=16ms TTL=47

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 16ms, Average = 14ms

C:\Users>
```

Figure 4. Command Prompt Interface: Ping results

Understanding Ping results

Ping operates by sending ICMP Echo Request packets to the target device and waiting for an ICMP Echo Reply. The program reports errors, packet loss, and a statistical summary of the results.

2. Section 2

2.1. Unit 1: TCP/IP model (OSI model) and Protocols per layer

OSI Model

This model is a reference model since it is not used, it was not ever user, but it will help to understand how the networking world works. On Figure 5, we can see each layer for the OSI Model

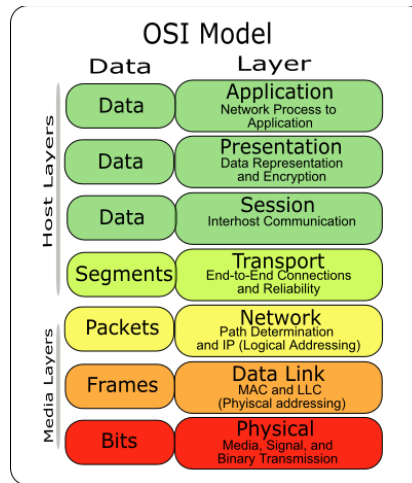


Figure 5. OSI Model Layers

Below Figure 6, you can find a table showing the most common protocols used in each layer. Notice that for Physical layer it is shown physical medias.

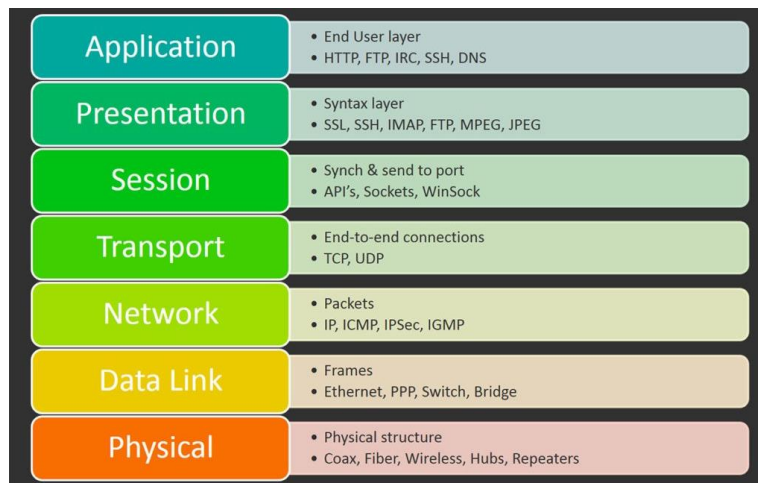


Figure 6. Common Protocols.

Data Encapsulation

Process that performs the sender. It adds headers when moving from upper layers to lower layers. (Shown on below Figure 7).

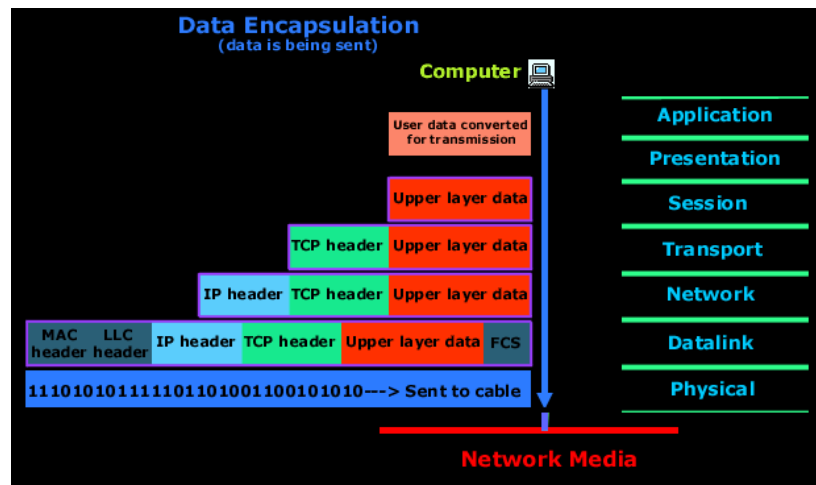


Figure 7. Encapsulation process.

Data Decapsulation

In the opposite direction the receiver performs the other way around. It removes headers when moving from lower layers to upper layers. (Shown on below Figure 8).

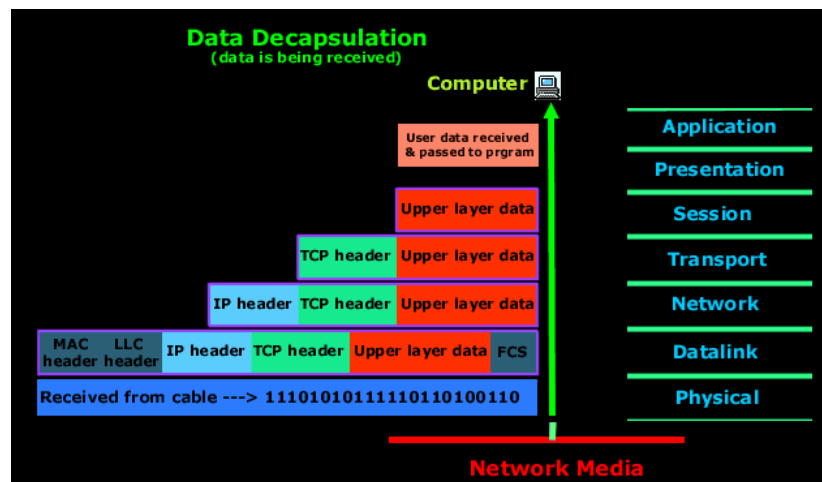


Figure 8. Common Protocols.

See below a brief explanation of each layer.

Application Layer

The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

Presentation Layer

The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

Session Layer

The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.

Transport Layer

The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

Network Layer

The network layer has two main functions. One is breaking up segments into network packets and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.

Data Link Layer

The data link layer establishes and terminates a connection between two physically connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking, and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

Physical Layer

The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.

Now the OSI model is already discussed, let us talk about the model that is used now a days: the TCP/IP model, it basically does the same thing, but the structure is different.

What is the difference between TCP and IP?

TCP and IP are **separate computer network protocols**. The difference between TCP (Transmission Control Protocol) and IP (Internet Protocol) is their role in the data transmission process. IP obtains the address where data is sent (your computer has an IP address). TCP ensures accurate data delivery once that IP address has been found. Together, the two form the TCP/IP protocol suite.

This is how the OSI, and TCP/IP models are related, see below Figure 9.

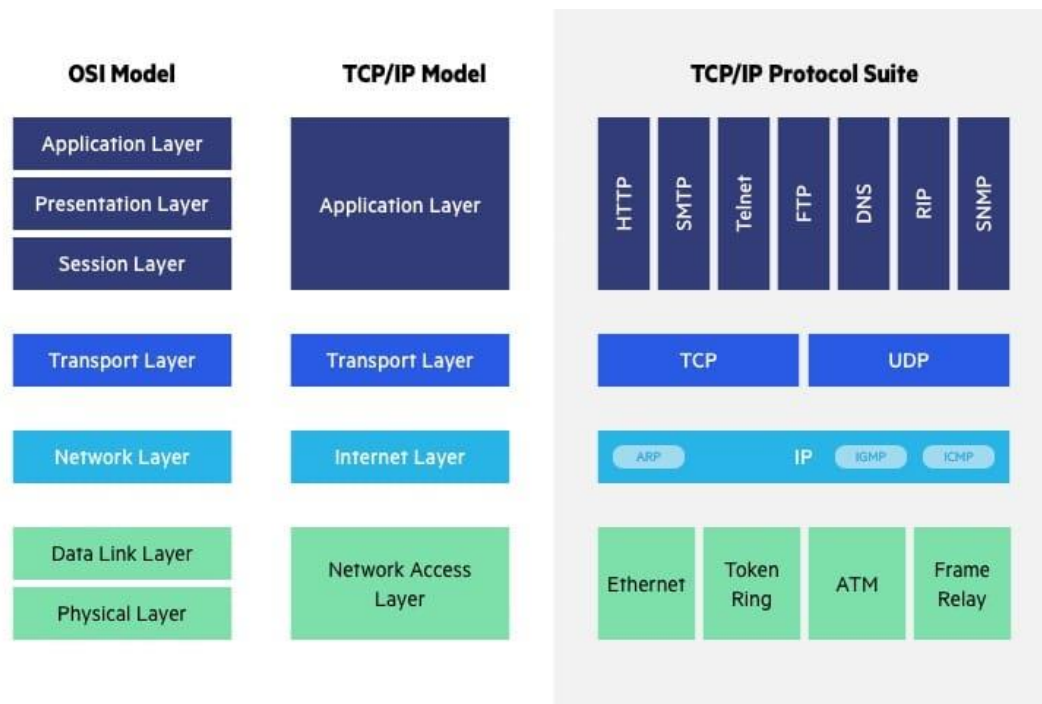


Figure 9. OSI and TCP/IP Model.

2.2. Unit 2: TCP vs UDP

On the following table 2, we can check the main difference between TCP and UDP.

Basis	Transmission control protocol (TCP)	User datagram protocol (UDP)
Type of Service	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 types of network transmission.
Reliability	TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
Error checking mechanism	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.
Acknowledgment	An acknowledgment segment is present.	No acknowledgment segment.
Sequence	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 the order is required, it must be managed by the application layer.
Speed	TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.
Retransmission	Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP).
Header Length	TCP has a (20-60) bytes variable length header.	UDP has an 8 bytes fixed-length header.
Handshaking Techniques	Uses handshakes such as SYN, ACK, SYN-ACK	It is a connectionless protocol i.e. No handshake
Protocols	TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet.	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.
Stream Type	The TCP connection is a byte stream.	UDP connection is message stream.

Table 2. TCP vs UDP

2.3. Unit 3: IP addressing (IP config)

These definitions are helpful to you, use these vocabulary terms to get you started:

- **Address** - The unique number ID assigned to one host or interface in a network.
- **Subnet** - A portion of a network that shares a particular subnet address.
- **Subnet mask** - A 32-bit combination used to describe which portion of an address refers to the subnet and which part refers to the host.
- **Interface** - A network connection.

Understand IP Addresses

An IP address is an address used to uniquely identify a device on an IP network. The address is made up of 32 binary bits, which can be divisible into a **network portion** and **host portion** with the help of a subnet mask. The 32 binary bits are broken into four octets (1 octet = 8 bits). Each octet is converted to decimal and separated by a period (dot). For this reason, an IP address is said to be expressed in dotted decimal format (for example, 172.16.81.100). The value in each octet ranges from 0 to 255 decimal, or 00000000 - 11111111 binary.

Here is how binary octets convert to decimal: The right most bit, or least significant bit, of an octet holds a value of 2^0 (two to the power of zero). The bit just to the left of that holds a value of 2^1 (Two to the power of one) This continues until the left-most bit, or most significant bit, which holds a value of 2^7 (Two to the power of seven) So if all binary bits are a one, the decimal equivalent would be 255 as shown here:

1 1 1 1 1 1 1 1

128 64 32 16 8 4 2 1 (128+64+32+16+8+4+2+1=255)

Here is a sample octet conversion when not all the bits are set to 1.

0 1 0 0 0 0 0 1

0 64 0 0 0 0 0 1 (0+64+0+0+0+0+0+1=65)

And this sample shows an IP address represented in both binary and decimal.

10. 1. 23. 19 (decimal)

00001010.00000001.00010111.00010011 (binary)

Network Masks

A network mask helps you know which portion of the address identifies the network and which portion of the address identifies the node. Class A, B, and C networks have default masks, also known as natural masks, as shown here:

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

Also, you need to know the following are the IP address classes from A to E in IPv4 (Shown on below Figure 10).

Five Different Classes of IPv4 Addresses						
Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID	# of networks
Class A	0 – 127	0XXXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24} - 2$	2^7
Class B	128 – 191	10XXXXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16} - 2$	2^{14}
Class C	192 – 223	110XXXXXX	192.0.0.0-223.255.255.255	255.255.255.0	$2^8 - 2$	2^{21}
Class D (Multicast)	224 – 239	1110XXXXX	224.0.0.0-239.255.255.255			
Class E (Experimental)	240 – 255	1111XXXXX	240.0.0.0-255.255.255.255			

Figure 10. IP addresses class Range

Notice that the values corresponding to X can change in the first octet, which delimits the ranges expressed in the table. Additionally note, that for IPv4 addresses (class A, B and C specifically) has something that the others do not have: The Subnet mask. Basically, this is the parameter that let you know which part of the IP address (how many bits) belongs to the Network Portion, and what part of the IP address (how many bits) belongs to the Host portion (Shown on below Figure 11).

	8 bits	8 bits	8 bits	8 bits
Class A:	Network	Host	Host	Host
Class B:	Network	Network	Host	Host
Class C:	Network	Network	Network	Host
Class D:	Multicast			
Class E:	Research			

Figure 11. Network Portion and Host Portion

Class A has 8 bits for the Network Portion and 24 bits for the Host portion,

Class B has 16 (8+8) bits for the network portion and 16 bits for the Host portion, and

Class C has 24 (8+8+8) bits for the Network portion and 8 bits for the Host portion.

Network portion is always the same for the same network. Only network portion is variable in the subnet.

Important: The first IP address on a network and the last IP address on a network are reserved for the network ID and the broadcast IP address, respectively. For example:

For network: **192.168.1.0** **255.255.255.0**

The subnet mask indicates that the first three octets belong to the network portion, and the last octet can vary, this way we get:

Subnet Range: 192.168.1.0 until 192.168.1.255 (256 IP addresses)

Network ID: 192.168.1.1

Broadcast IP: 192.168.1.255

It means that we have only available 254 IP address to assign, so:

Available/assignable IP range: 192.168.1.1 until 192.168.1.254

Notations for subnet masks:

For subnet 192.168.1.0 using 24 bits for Network portion:

Decimal notation:

192.168.1.0 255. 255. 255. 0

Binary notation:

192.168.1.0 11111111.11111111.11111111.00000000

Prefix notation:

192.168.1.0 /24

IP addresses ranges: These are defined in the below Table 3.

IP address classes

Class	1st Octet Decimal Range	1st Octet High Order Bits	Network/Host ID (N=Network, H=Host)	Default Subnet Mask	Number of Networks	Hosts per Network (Usable Addresses)
A	1 – 126*	0	N.H.H.H	255.0.0.0	126 ($2^7 - 2$)	16,777,214 ($2^{24} - 2$)
B	128 – 191	10	N.N.H.H	255.255.0.0	16,382 ($2^{14} - 2$)	65,534 ($2^{16} - 2$)
C	192 – 223	110	N.N.N.H	255.255.255.0	2,097,150 ($2^{21} - 2$)	254 ($2^8 - 2$)
D	224 – 239	1110	Reserved for Multicasting			
E	240 – 254	1111	Experimental; used for research			

Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback and diagnostic functions.

www.certiology.com

Table 3. IP address Range

Not all of them can transit over the internet network, these are the private IP address range which is listed below Table 4.

Private IP Addresses

Class	Private Networks	Subnet Mask	Address Range
A	10.0.0.0	255.0.0.0	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.0.0	255.240.0.0	172.16.0.0 - 172.31.255.255
C	192.168.0.0	255.255.0.0	192.168.0.0 - 192.168.255.255

Table 4. Private IP address Range

The IP addresses outside of this range is consider a Public IP address, which can flow/transit on the internet network.

2.4. Unit 4: Subnetting (Subnet ID and broadcast)

What is subnetting?

Subnetting is the practice of dividing a network into two or more smaller networks. It increases routing efficiency, enhances the security of the network, and reduces the size of the broadcast domain.

CIDR (Classless inter-domain routing)

CIDR (Classless inter-domain routing) is a method of public IP address assignment. It was introduced with the following goals:

- to deal with the IPv4 address exhaustion problem
- to slow down the growth of routing tables on Internet routers

Before CIDR, public IP addresses were assigned based on the class boundaries:

- **Class A** – the classful subnet mask is /8. The number of possible IP addresses is 16,777,216 (2 to the power of 24).
- **Class B** – the classful subnet mask is /16. The number of addresses is 65,536
- **Class C** – the classful subnet mask is /24. Only 256 addresses available.

To combat this, the classful network scheme of allocating the IP address was abandoned. The new system was classless – a classful network was split into multiple smaller networks. For example, if a company needs 12 public IP addresses, it will get something like this: **192.50.4.16/28**.

The number of usable IP addresses can be calculated with the following formula:

2 to the power of host bits – 2

Subnets

There are a couple of ways to create subnets.

Before we start subnetting, we must ask ourselves these two questions:

1. How many subnets do we need?

2^x = number of subnets. x is the number of 1s in the subnet mask. With 1 subnet bit, we can have 2 or 4 subnets. With 2 bits, 4 or 8 subnets, with 3 bits, 8 or 16 subnets, etc.

2. How many hosts per subnet do we need?

$2^y - 2$ = number of hosts per subnet. y is the number of 0s in the subnet mask.

Subnet ID and Broadcast ID

The Network ID is its beginning number, and it is always an even number. It designates a particular subnet to give it an identity on the network. When a subnet is referred to, the Network ID and the subnet's subnet mask is used. The Broadcast ID is always an odd number and is the subnet's ending number.

Subnet ID and Broadcast ID IP addresses can not be assigned on a network, so when we do the calculation for hosts requirement, we need to decrease the number of the available IP address by 2

VLSM

Each network has a different requirement (number of hosts). With the previous subnetting, we will guarantee the same number of hosts for all subnets. Since our private IP addresses are limited, we need to do a better distribution of the networks (To prevent wasting IP addresses). To efficiently use subnetting, we can use Variable-Length Subnet Mask (VLSM)

Steps to implement VLSM

Step 1. Identify the host requirement. We need to know how many hosts or IP addresses are needed by the subnet. We must arrange from the highest number of hosts to lowest.

Step 2. Determine the subnet mask of IP subnet. We need to determine what the appropriate subnet mask is based on our number of hosts requirement.

Step 3. Identify the hosts bits for every subnet. We will use the power 2 table for this calculation and take in consider the formula $2^y - 2$ which y is the number of 0s in the subnet mask.

Note: If we identify the subnet mask, we can do the hosts bits calculation with $y = 32 - \text{Subnet mask}$

Step 4. Get the increment. For determining the increment, we use 2^y , in that case, we will know all the IP addresses over one network (Including subnet ID and broadcast ID)

Step 5. Determine the network address, broadcast address and IP address range. From the base IP address, we will use the increment value

Subnet ID:

We will use the subnet mask, if the subnet mask value is equal to 255, we will use the same octet value for the subnet ID address.

If the subnet mask value is equal to 0, we will use 0 for this octet.

If the subnet mask is different than 0 or 255, we will use the increment value for getting the multiples (Increment * 0, Increment * 1, Increment * 2, etc.). Then, we will use the closest multiple to the original octet value without overpassing the original value.

Broadcast ID:

We will use the subnet mask, if the subnet mask value is equal to 255, we will use the same octet value for the subnet ID address.

If the subnet mask value is equal to 0, we will use 255 for this octet.

If the subnet mask is different than 0 or 255, we will use the increment value. We will use the subnet ID octet + increment - 1.

Next Subnet ID:

We use the previous subnet ID + Increment and we will get the next Subnet ID IP address.

2.5. Unit 5: MAC address (OUI), Switch LED status, Switch functionality (Flooding)

MAC Addressing.

- MAC address is the physical address, which uniquely identifies each device on a given network. To make communication between two networked devices, we need two addresses: **IP address and MAC address**. It is assigned to the NIC (Network Interface card) of each device that can be connected to the internet.
- It stands for **Media Access Control**, and also known as **Physical address, hardware address, or BIA (Burned In Address)**.
- It is globally unique; it means two devices cannot have the same MAC address. It is represented in a hexadecimal format on each device, such as **00:0a:95:9d:67:16**.
- It is 12-digit, and 48 bits long, out of which the first *24 bits are used for OUI (Organization Unique Identifier)*, and *24 bits are for NIC/vendor-specific*.
- It works on the data link layer of the OSI model.
- It is provided by the device's vendor at the time of manufacturing and embedded in its NIC, which is ideally cannot be changed.
- The **ARP protocol** is used to associate a logical address with a physical or MAC address.

Switch LED statuses:

On below Figure 12, we can check the LED status

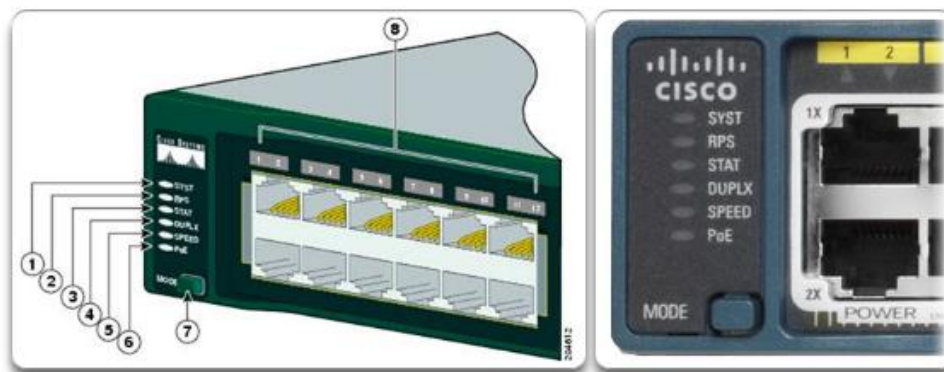


Figure 12. Switch LED

1. System LED
2. RPS LED
3. Port LED Status
4. Port Duplex Mode LED
5. Port Speed LED
6. Ethernet Power Status LED
7. Mode Button
8. Port LED

Port LED status

On below Table 5, we have some port status.

Port Mode	Port LED Color	Meaning
STAT (port status)	Off	No link, or port was administratively shut down.
	Green	Link present, no activity.
	Blinking green	Activity. Port is sending or receiving data.
	Alternating green-amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication.
	Amber	Port is blocked by Spanning Tree Protocol (STP) and is not forwarding data. After a port is reconfigured, the port LED can be amber for up to 30 seconds as STP checks the switch for possible loops.

Table 5. Port Status

Switch Default behavior

A layer 2 switch, or a switch is a device capable of forwarding data frames from one host to another host, this is when the data frames enter in one port and the switch sends the traffic throughout another port, this process is called Switching. Now, this forwarding information is made via the MAC address table that contains in which direction (which port) we can find the MAC address of the host under concern.

The MAC address table has some parameters such as the VLAN ID, the MAC address, the associated switch port to that MAC address

Find below a brief of the behaviors a Cisco switch has when fulfilling the MAC address table and performing the forwarding decision.

1. When the frame arrives to a switch port, the switch checks the ethernet header of the frame looking for the **Source** MAC address, and it adds this MAC address to the MAC address table on the corresponding entering port.
This is the MAC Learning process of the switch. (Shown on Figure 13)

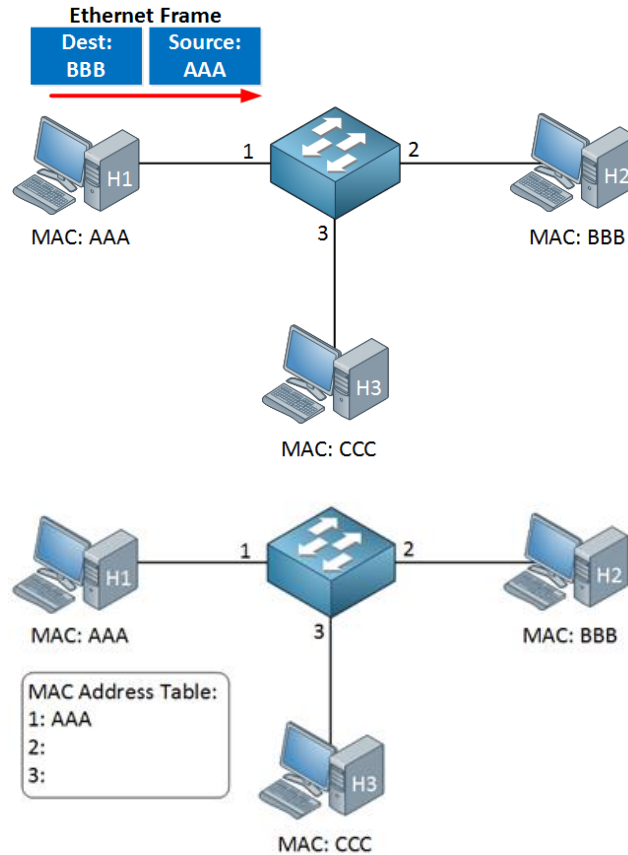
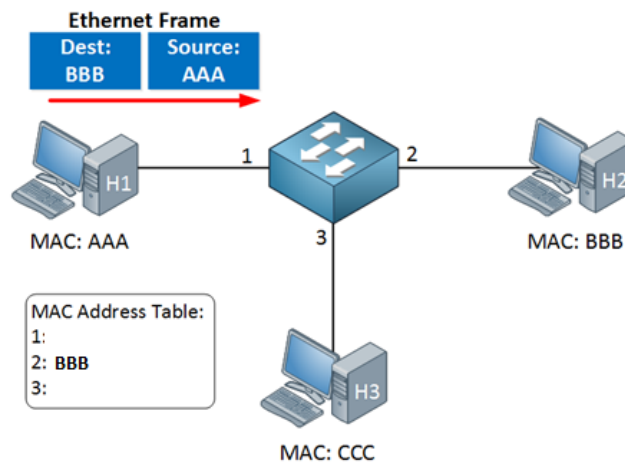


Figure 13. Switch behavior step 1.

2. Once above is done, the switch is ready to forward the traffic, in every case, the switch is going to look up the **Destination** MAC address in the data frame and decide; it can happen one of the following scenarios:
 - 2.1. The switch already knows in which direction that MAC address is, it is the MAC address previously learned in one of the ports in the same VLANID. Then, the switch will forward a **unicast** frame to the destination (no other copies are created). (Shown on Figure 14)



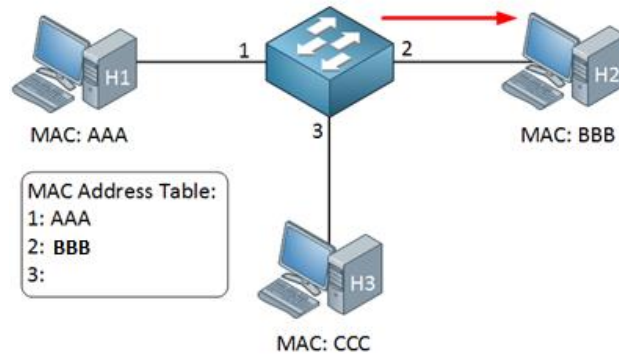


Figure 14. Switch behavior step 2.

- 2.2. The switch does not know in which direction that MAC address is, it means the switch has not learned the MAC address yet in the VLAN ID. Then the switch will create copies of the data frame and will forward a copy of that to every port assigned to the same VLAN ID, except to the one the data frame was received in the first place. (Show on Figure 15).

This whole is called **unknown unicast flooding**.

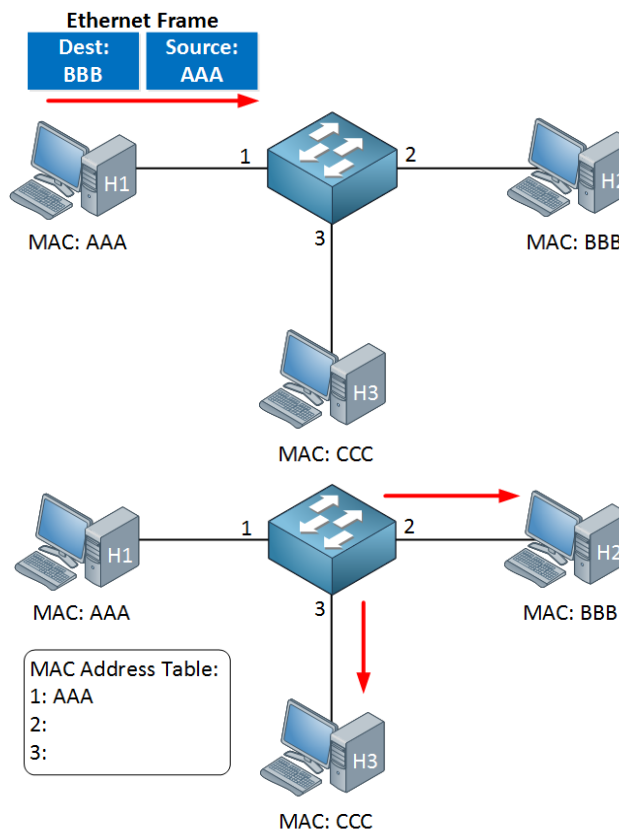


Figure 15. Switch behavior step 3.

- 2.3. Or, if the data frame is a broadcast frame, it means the destination MAC address has all its bits as F's (example: FF:FF:FF:FF:FF:FF), then the switch will create copies of the data frame and will forward a copy of that to every port assigned to the same

VLAN ID, except to the one the data frame was received in the first place. (Show on Figure 16).

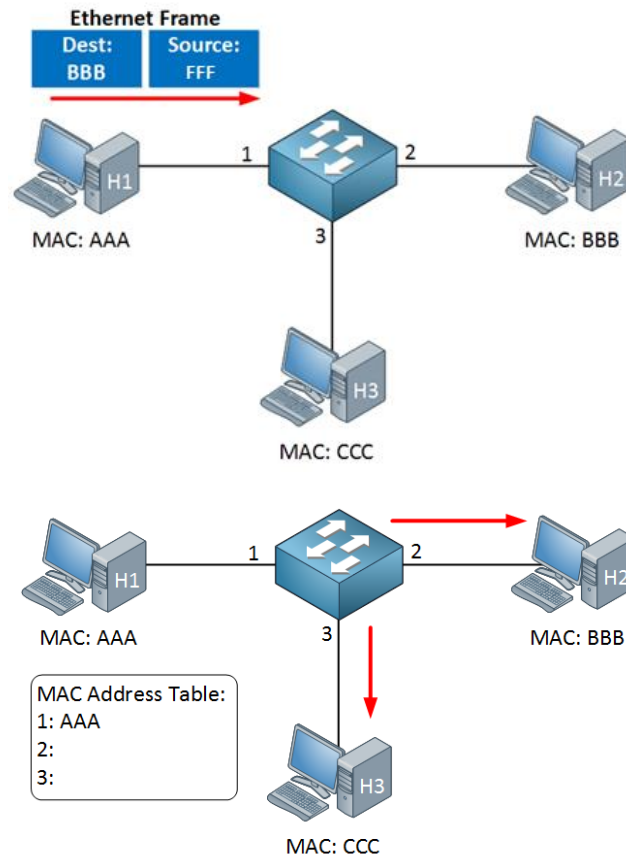


Figure 16. Switch behavior step 1.

This whole is called **Broadcast**.

2.6. Unit 6: VLAN and Trunk (Native VLAN)

What is a VLAN?

VLAN is a logical grouping of networking devices. When we create VLAN, we 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.

Benefits of using VLANs

Using VLANs not only improves the scaling of the campus LAN. It has many more advantages such as:

- **It improves the security** by reducing the number of end-stations that receive copies of BUM traffic.

- **It creates smaller fault domains** by isolating different groups of devices in separate broadcast domains.
- **It reduces the CPU overhead** on each device in the LAN by limiting the number of broadcast frames received.
- **It improves network performance** and speed of failure recovering.

VLAN ID

VLAN ID is a number that identifies the VLAN on the switch. It will be unique per subnet that it is configured on the device.

We have normal range (1-1005) or extended range (1006 – 4094). When the device is turn on, it is created automatically VLAN 1, 1002 to 1005. These VLANs can not be removed. All the information about the VLANs is stored in the vlan.dat file in flash memory.

Types of VLANs

Types of VLANs include Protocol based, static and dynamic VLANs.

- **A Protocol VLAN-** which has traffic handled based on its protocol. A switch will segregate or forward traffic based on the traffics protocol.
- **Static VLAN-** also referred to as port-based VLAN, needs a network administrator to assign the ports on a network switch to a virtual network.
- **Dynamic VLAN-** allows a network administrator just to define network membership based on device characteristics, as opposed to switch port 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 port is the connection between a switch port and end user device (Computer/Server). Each port can belong only to a single VLAN. That means all devices connected to this port will be in same broadcast domain. We can associate one port to single VLAN.

Trunk Link

Trunk link connection is the link between two devices that can understand multiple VLANs. It is common to use it between two switches or switch to router. Trunk link allows us to send or receive information from multiple VLANs on a single link. The standard for trunk protocol is 802.1Q. To support trunking, original ethernet frame is modified to carry VLAN information (VLAN ID) like the Figure 17.

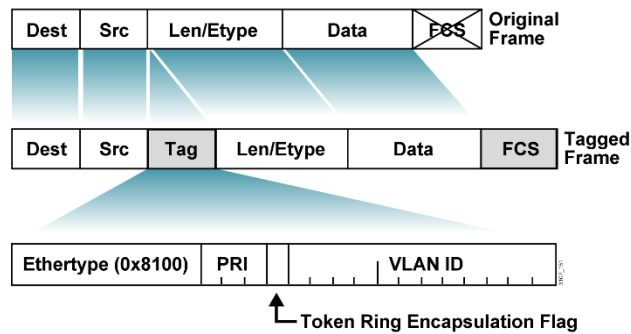


Figure 17. Tag Frame

Without trunk, we will have a similar situation like the Figure 18. On here, we have a one physical link per VLAN (which it is an expensive configuration).

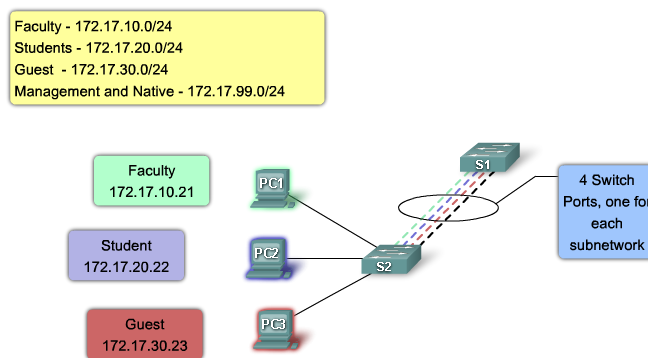


Figure 18. Link without trunk protocol

On Figure 19, we have the correct configuration as we used one physical link for multiple VLANs by using Trunk link.

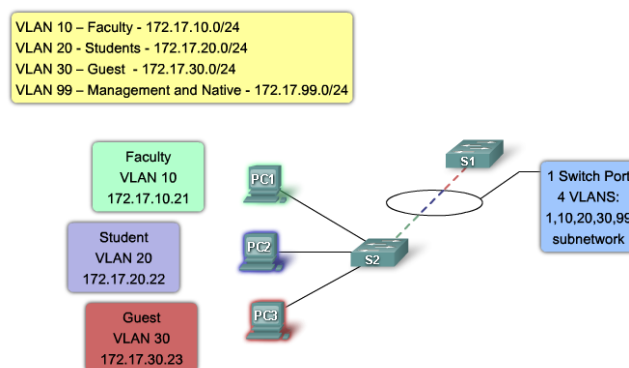


Figure 19. Link trunk protocol

Native VLAN

A **native VLAN** is a special VLAN whose traffic traverses on the 802.1Q trunk without any VLAN tag. A native VLAN is defined in 802.1Q (it supports untagged traffic while inter-switch link doesn't support

untagged traffic.) trunk port standard which supports traffic coming from several VLANs as well as the traffic that doesn't come from a VLAN. The native VLAN is per trunk per switch configuration. The 802.1Q trunk port assigns untagged traffic on a native VLAN. Native VLAN needs to be the same between each port connected on the same link

2.7. Unit 7: ARP (Windows Commands)

What is ARP?

The **Address Resolution Protocol (ARP)** is a communication protocol that maps the **Internet Protocol (IP) address** to the **Media Access Control (MAC)** address. This protocol facilitates the communication of the devices connected to the network.

Applications and software connected to the internet use IP addresses to send information. Meanwhile, the communication between systems happens through hardware addresses, also known as MAC or physical addresses. Without ARP, software and devices would not be able to send data to each other.

ARP translates the **software address** (IP address) to the **physical address** (MAC address) of the host connected to the network. ARP exists as the link layer protocol in the Open System Interconnection (OSI) model.

Destination decisions cannot be based on IP addresses. On the same network, an IP address maps the data link layer address of another computer.

Here's where ARP comes into play. Since IP version 4 (IPv4) addresses have different lengths (32-bit) than MAC addresses (48-bit), ARP translates these addresses to facilitate the information exchange. (Figure 20 for reference).

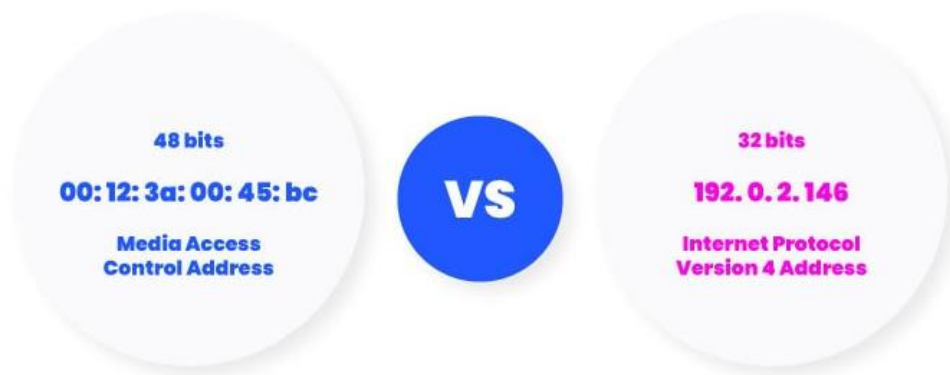


Figure 20. MAC and IP addresses

How does ARP work?

When a source device wants to send an IPv4 packet to another device, ARP performs two important tasks. First, the ARP program checks the **ARP cache table**, which consists of **IPv4 address to MAC address** mappings.

The second task starts if the ARP cache lookup does not provide a matching MAC address. In this case, the source server forms an **ARP message**, which is broadcast on the local area network (LAN).

ARP request

An ARP request establishes communication between devices on the network. It is enabled after a source device fails to retrieve necessary data from an **ARP cache table**.

The ARP table holds records of the IP address and MAC address of the devices connected to the same network. IT administrators do not maintain this table. Instead, the ARP protocol creates additions when it receives an **ARP response** (which is an interaction of ARP request and ARP response). All operating systems in a network keep **ARP caches**. ARP process is showed on Figure 21.

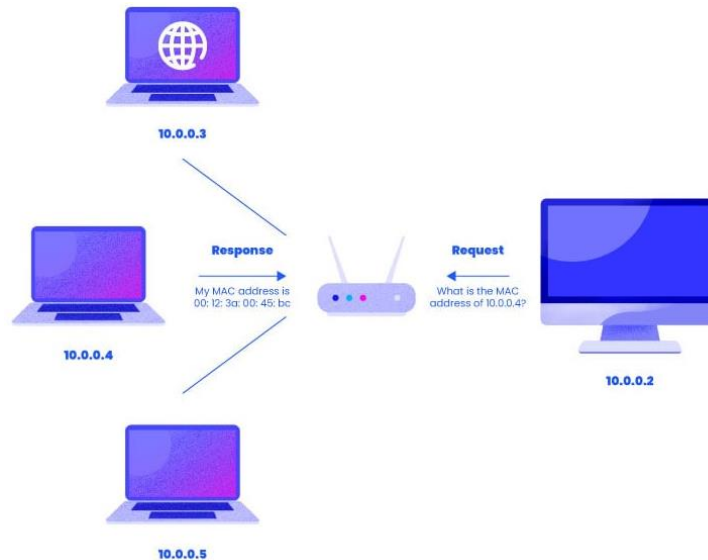


Figure 21. ARP process.

Once the ARP process is completed, then the communication can happen, since the entry already exists in the ARP cache table, so when it retrieves this information, it creates the packet information just fine.

ARP request: It is a L2 (layer 2) broadcast frame.

ARP response: It is also a L2 frame responding to the ARP request, but it's unicast.

You can see the ARP cache table on windows OS with the following command.

C> arp -a

In Cisco routers use the following command.

Router# show ip arp or Router# show arp

2.8. Unit 8: InterVlan

What is Inter-VLAN Routing?

VLANs are used to segment switched Layer 2 networks for a variety of reasons. Regardless of the reason, hosts in one VLAN cannot communicate with hosts in another VLAN unless there is a router or a Layer 3 switch to provide routing services.

Router-Based Inter-VLAN routing is a process for forwarding network traffic from one VLAN to another VLAN using a Layer 3 devices (Router or Layer 3 Switch).

There are three inter-VLAN routing options:

- Legacy inter-VLAN routing.
- Router-on-a-stick
- Layer 3 switch using switched virtual interfaces (SVIs)

Legacy inter-VLAN routing.

The first inter-VLAN routing solution is using a router with multiple physical interfaces. With the traditional method, we will need a dedicated link on the router per VLAN to communicate VLANs like the Figure 22 where we have a dedicated interface per VLAN (gig0/1 for VLAN 10 and gig0/2 for VLAN 20).

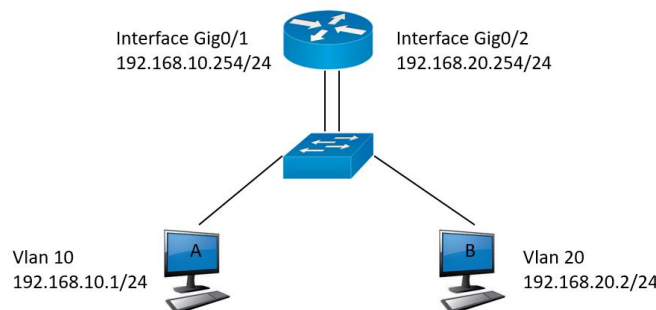


Figure 22. Legacy inter-VLAN routing

This solution has an important limitation. It is not scalable since routers have a limited number of physical interfaces. If we need to configure 100 VLANs, we will need 100 ports on the routers (routers usually have around 4 ports). This method is not using anymore, it is included only for explanation.

Router-on-a-stick Inter-VLAN routing.

This solution is handled the limitation with the legacy inter-VLAN routing. It requires only one physical interface to route traffic between multiple VLANs.

On Cisco IOS router interface will be configured as a trunk and connected to a trunk port on a Layer 2 Switch. More exactly, router interface is configured using subinterfaces to identity each VLAN.

Subinterfaces are virtual interfaces on the Router. We can configure each subinterface with a different subnet that correspond to their VLAN assignment. In addition, subinterfaces is handled by physical interface (If the physical interface is disabled, subinterfaces will be disabled).

Additionally, each subinterface needs to be configured for supporting encapsulation 802.1Q, since the data received will use 802.1Q Frame.

Figure 23 shows an example of router-on-a-stick. PC1 on VLAN 10 is communicating with PC3 on VLAN 30 through R1 using a single, physical interface. PC1 is using the corresponding subinterface and it is doing the process for passing the traffic from one subinterface to the other one.

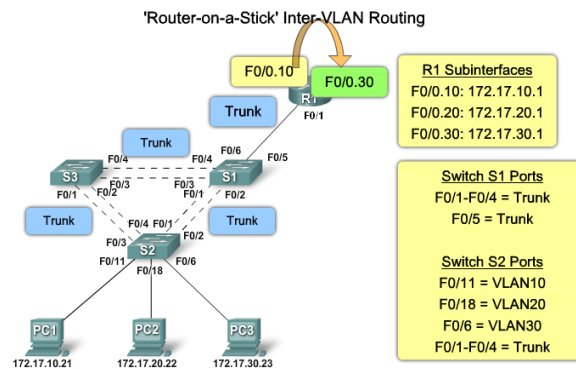


Figure 23. Router-on-a-stick inter-vlan routing

The router-on-a-stick method of inter-VLAN routing does not scale beyond 50 VLANs.

Inter-VLAN routing on a Layer 3 Switch

Similar process as subinterface on router-on-stick configuration, we will create a virtual interface called "interface VLAN" for helping us with the routing. Specifically, it provides layer 3 processing for packets that are sent to or from all switch ports associated with that VLAN.

The following are advantages of using Layer 3 switches for inter-VLAN routing:

- They are much faster than router-on-a-stick because everything is hardware switched and routed.
- There is no need for external links from the switch to the router for routing.

We will create a multiple interface VLAN per VLAN that we want to communicate. (Before creating VLAN interface, we need to create the VLAN)

2.9. Unit 9: Static Routing

What is Static Routing?

Routers forward packets using either route information from route table entries that you manually configure or the route information that is calculated using dynamic routing algorithms.

Static routes, which define explicit paths between two routers, cannot be automatically updated; you must manually reconfigure static routes when network changes occur. Static routes use less bandwidth than dynamic routes. No CPU cycles are used to calculate and analyze routing updates.

Static routes make use of an administrative distance which is the metric used by routers to choose the best path when there are two or more routes to the same destination from two different routing protocols. However, when talking about static routing, the administrative distance can be modified for different purposes:

[+] Path manipulation.

[+] Backup routes or floating routes.

Load balancing is the default behavior when the router has multiple routes for the one single destination, it happens because the default administrative distance of the static route if not configured is 1 (one).

Syntax in Cisco routers:

Ip route X.X.X.X Y.Y.Y.Y Z.Z.Z.Z [AD]

X.X.X.X is the destination network or host

Y.Y.Y.Y is the prefix length

Z.Z.Z.Z is the next hop IP address

[AD] (optional) is the administrative distance value, if not configured there is an implicit 1

Notes: prefix length of 255.255.255.255 is like defining a single host.

A static route of “**ip route 0.0.0.0 0.0.0.0 Z.Z.Z.Z [AD]**” is defined as a **Default route**, which is a match for all the traffic that does not match on any more specific static route.

Example:

Ip route 192.168.10.0 255.255.255.0 172.16.1.2 15

It means, there is a static route that will send to the next hop IP address 172.16.1.2 all the traffic that is destined to the network 192.168.10.0/24, and the configured administrative distance is 15.

Consider the following topology on Figure 24 and let us suppose that PC0 (10.0.0.1) is communicating with PC1 (5.0.0.2) and is sending a data stream of 4 packets.

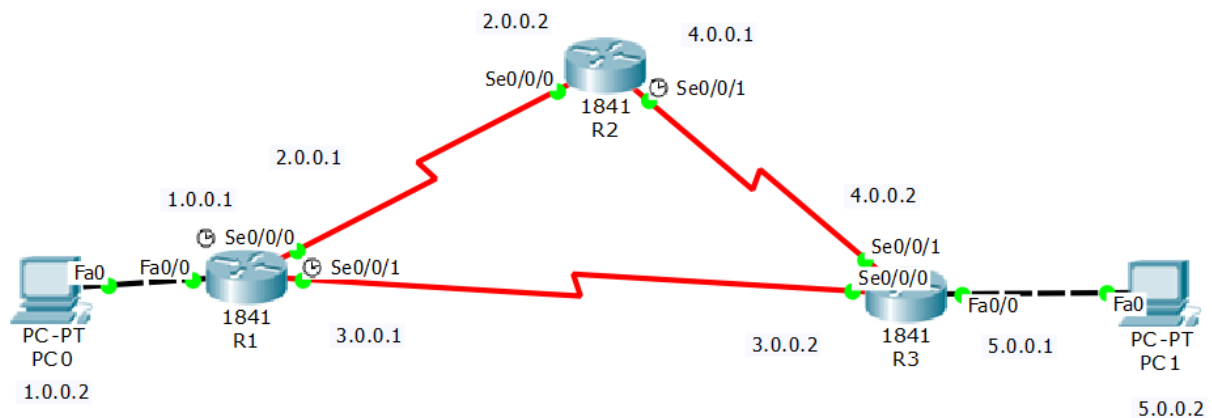


Figure 24. Static Routing Topology.

On this case, let us get focused on R1 which will be handling the static routing.

[+] For Load balancing:

```
ip route 5.0.0.2 255.255.255.255 2.0.0.2
ip route 5.0.0.2 255.255.255.255 3.0.0.2
```

or

```
ip route 5.0.0.2 255.255.255.255 2.0.0.2 30
ip route 5.0.0.2 255.255.255.255 3.0.0.2 30
```

Since both static routes have the same destination network, same prefix length and same administrative distance, so the first packet will be sent to R2 via IP address 2.0.0.2 from interface Se0/0/0 of R1, then the second packet will be sent to R2 via IP address 3.0.0.2 from interface Se0/0/1 of R2, then the sequence will be repeated. This is called load balancing.

[+] For backup route or path manipulation:

```
ip route 5.0.0.2 255.255.255.255 2.0.0.2
ip route 5.0.0.2 255.255.255.255 3.0.0.2 15
```

Since both static routes have the same destination network, same prefix length but different administrative distance, so the entire stream of 4 packets will be sent to R2 via ip address 2.0.0.2 from interface Se0/0/0 of R1, because the other route has an administrative distance of 15, which is less preferred, this last one route is called the backup route. This way we have manipulated the traffic to always be sent this way, but the second route will be present in case the main path fails due to any failure in the link of interface Se0/0/0.

3. Section 3

3.1. Unit 1: Dynamic Routing (Administrative Distance and metric)

Functions of Dynamic Routing Protocols

Routing protocols are used to facilitate the exchange of routing information between routers. A routing protocol is a set of processes, algorithms, and messages that are used to exchange routing information and populate the routing table with the routing protocol's choice of best paths. The purpose of dynamic routing protocols includes:

- Discovery of remote networks
- Maintaining up-to-date routing information
- Choosing the best path to destination networks
- Ability to find a best new path if the current path is no longer available

Components of a routing protocol

Routing protocols determine the best path, or route, to each network. That route is then added to the routing table. A primary benefit of dynamic routing protocols is that routers exchange routing information when there is a topology change. This exchange allows routers to automatically learn about new networks and to find alternate paths when there is a link failure to a current network.

In the case of a routing protocol algorithms are used for facilitating routing information and best path determination. These are messages for discovering neighbors and exchange of routing information like on the Figure 25.

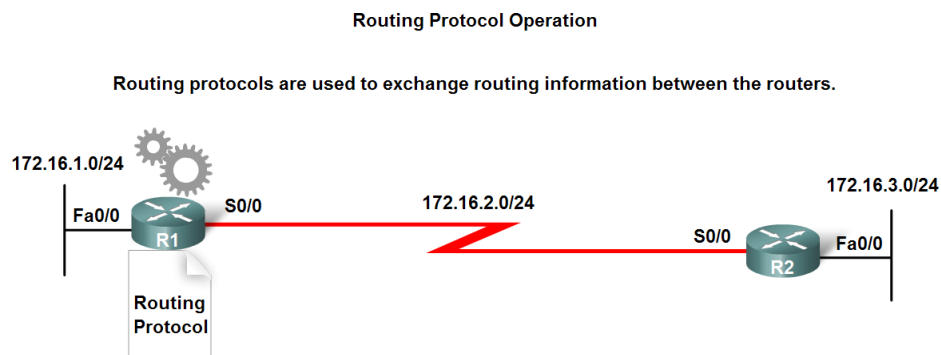


Figure 25. Routing protocol operation

Dynamic routing protocols are grouped according to characteristics. Examples include:

- RIP
- IGRP
- EIGRP
- OSPF
- IS-IS
- BGP

Autonomous System is a group of routers under the control of a single authority.

Types of routing protocols:

-Interior Gateway Protocols (IGP)

An interior gateway protocol (IGP) is a dynamic route update protocol used between routers that run on TCP/IP hosts within a single autonomous system. The routers use this protocol to exchange information about IP routes.

-Exterior Gateway Protocols (EGP)

An exterior gateway protocol is a routing protocol used to exchange routing information between autonomous systems. This exchange is crucial for communications across the Internet. Notable exterior gateway protocols include **Exterior Gateway Protocol (EGP)**, now obsolete, and **Border Gateway Protocol (BGP)**. On Figure 26 we can see the IGP vs EGP.

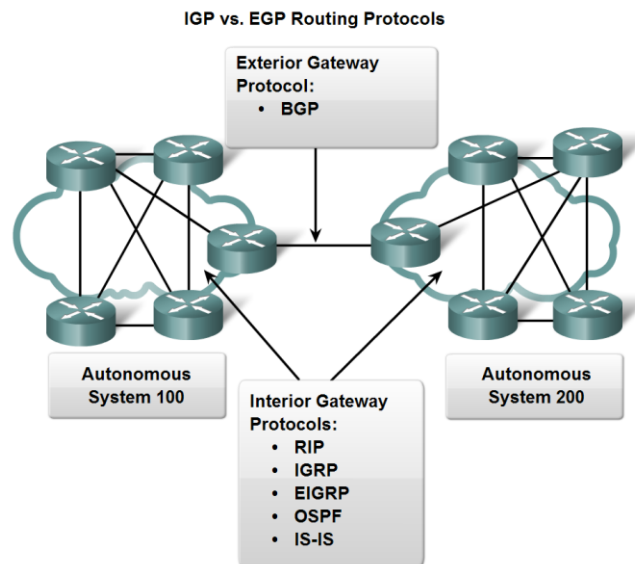


Figure 26. IGP vs EGP routing protocols

Dynamic Routing Protocol Operation

All routing protocols are designed to learn about remote networks and to quickly adapt whenever there is a change in the topology. The method that a routing protocol uses to accomplish this depends upon the algorithm it uses and the operational characteristics of that protocol.

In general, the operations of a dynamic routing protocol can be described as follows:

1. The router sends and receives routing messages on its interfaces.
2. The router shares routing messages and routing information with other routers that are using the same routing protocol.
3. Routers exchange routing information to learn about remote networks.
4. When a router detects a topology change, the routing protocol can advertise this change to other routers.

Classifying Routing Protocols

Distance Vector

Distance vector means that routes are advertised by providing two characteristics:

- **Distance:** Identifies how far it is to the destination network and is based on a metric such as the hop count, cost, bandwidth, delay, and more
- **Vector:** Specifies the direction of the next-hop router or exit interface to reach the destination

RIPv1: First generation legacy protocol

RIPv2: Simple distance vector routing protocol

IGRP: First generation Cisco proprietary protocol (obsolete and replaced by EIGRP)

EIGRP: Advanced version of distance vector routing

Link-State

In contrast to distance vector routing protocol operation, a router configured with a **link-state routing protocol** can create a complete view or topology of the network by gathering information from all the other routers.

To continue our analogy of signposts, using a link-state routing protocol is like having a complete map of the network topology. RIP-enabled routers send periodic updates of their routing information to their neighbors. Link-state routing protocols do not use periodic updates. After the network has converged, a link-state update is only sent when there is a change in the topology.

Link-state protocols work best in situations where:

- The network design is hierarchical, usually occurring in large networks
- Fast convergence of the network is crucial
- The administrators have good knowledge of the implemented link-state routing protocol

There are two link-state IPv4 IGPs:

- **OSPF:** Popular standards-based routing protocol
- **IS-IS:** Popular in provider networks

Classful routing protocols

Do not send subnet mask in routing updates

Classless routing protocols

Do send subnet mask in routing updates.

In addition, we have the term “**Convergence**” which it is defined as when all routers’ routing tables are at a state of consistency. When the dynamic routing protocol is doing changes on the routing table, it will take some time for updating it.

Administrative distance.

It is a numeric value that specifies the preference of a particular route. It is the first number in the brackets in the routing table like Figure 27.

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    192.168.1.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial0/0/1
R    192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
D    192.168.6.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
R    192.168.7.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
R    192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:08, Serial0/0/1
```

Figure 27. Routing table with administrative distance highlighted

Each route (routing protocol) on the routing table has a default administrative distance (and it is different between them) like it is described on the Figure 28.

Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

Figure 28. Administrative distance per protocol

Metric

A value used by a routing protocol to determine which routes are better than others.

Each dynamic routing protocol has owned Metric and it is calculated on a different way based on some information on your network.

-RIP - **hop count**

-IGRP & EIGRP - **Bandwidth** (used by default), **Delay** (used by default), **Load**, **Reliability**

-IS-IS & OSPF – **Cost, Bandwidth** (Cisco's implementation)

The metric is the second number which appears between brackets on the routing table (reference Figure 29).

```
R2#show ip route
<output omitted>

Gateway of last resort is not set

R    192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:24, Serial0/0
C    192.168.2.0/24 is directly connected, Serial0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial0/1
R    192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:26, Serial0/1
R    192.168.6.0/24 [120/1] via 192.168.2.1, 00:00:24, Serial0/0
      [120/1] via 192.168.4.1, 00:00:26, Serial0/1
R    192.168.7.0/24 [120/1] via 192.168.4.1, 00:00:26, Serial0/1
R    192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:26, Serial0/1
```

Figure 29. Metric on routing table

Routing Decision

For sending some packets, we will use the destination IP address and we have some criteria:

1. Prefix length (Subnet mask) (long prefix).
2. Administrative distance (Lower AD).
3. Metric (Lower).

3.2. Unit 2: DHCP (DHCP relay, Renewal and rebinding, DORA process)

What is DHCP?

The Dynamic Host Configuration Protocol (DHCP) is based on the Bootstrap Protocol (BOOTP), which provides the framework for passing configuration information to hosts on a TCP/IP network. DHCP adds the capability to automatically allocate reusable network addresses and configuration options to Internet hosts. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocating network addresses to hosts. DHCP is built on a client/server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts.

It uses 4 messages to complete the autoconfiguration of a host, this process is denominated as DORA (this is due to the initials of the 4 messages: Discover, Offer, Request and Ack). On below Figure 30, we can see the DORA process.

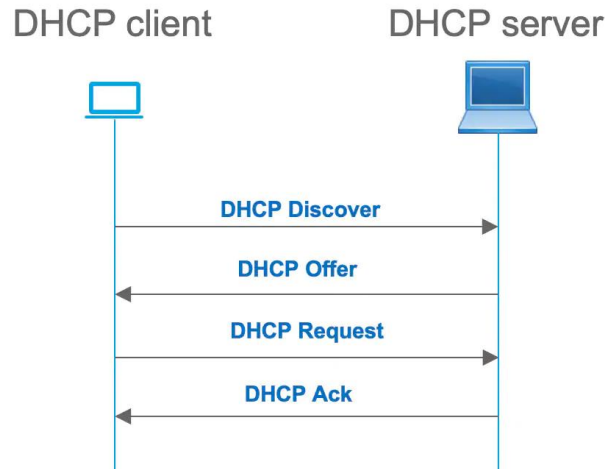


Figure 30. DORA Process.

When the DHCP server is in the same broadcast domain, then:

All communications from the client to the server during the DORA process are the broadcast type in the same broadcast domain, and the communication uses the UDP port 68.

All communications from the server to the client during the DORA process are the broadcast type in the same broadcast domain, and the communication uses the UDP port 67.

Now, when the DHCP server is in a different network than the client, then:

We need to make use of the DHCP Relay agent, which is a layer 3 device (usually a router) that has an active interface in the same broadcast domain than the client, and this router must have communication to the actual server via unicast, so this relay agent will continue the communication in behalf the client (which at this point is still unconfigured with IP parameters). On Figure 31, we can see the DHCP Relay process.

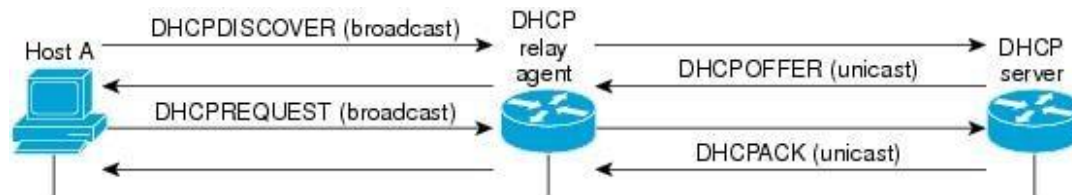


Figure 31. DHCP Relay

Notice that between the client and the DHCP relay agent device the communication is the same way than in local networks, but things change next:

All communications from the DHCP relay agent to the server during the DORA process are the unicast type in the network form that point, and the communication uses the UDP port 67.

All communications from the server to the DHCP relay agent during the DORA process are the unicast type in the network form that point, and the communication uses the UDP port 67.

After this whole process happens, the client (Host A from the image) will be configured with ip configuration.

Notice:

The relay agent is configured as below in the closet interface to the host A.

Ip helper-address X.X.X.X where X.X.X.X is the ip of the actual DHCP server

Also, notice the DHCP server can be any DHCP server, but it can also be a Cisco device such a router, see below how to configure the DHCP server on a router.

Ip dhcp pool <DHCP-pool-name>

Network X.X.X.X Z.Z.Z.Z X.X.X.X is the network id, Z.Z.Z.Z is the subnet mask

Default-router X.X.X.X X.X.X.X is the ip to be configured as de default router

Dns-server X.X.X.X X.X.X.X is the ip to be configured as de DNS router

Domain-name [LINE] [LINE] is a text will define as the system domain name

Notice, the **bolded** parameters are must, the rest of them are optional.

Now, there are other type of DHCP messages, but let us discuss that when talking about the renewing and rebinding processes.

Renewal Timer (*T1*) Expires

The renewal timer, *T1*, is set by default to 50% of the length of the lease. When the timer goes off, the client transitions from the *BOUND* state to the *RENEWING* state.

Note that a client *may* initiate lease renewal prior to *T1* timer expiration if it desires.

Client Sends *DHCPREQUEST* Renewal Message

The client creates a *DHCPREQUEST* message that identifies itself and its lease. It then transmits the message directly to the server that initially granted the lease, unicast. Note that this is different from the *DHCPREQUEST* messages used in the allocation/reallocation processes, where the *DHCPREQUEST* is broadcast. The client may request a particular new lease length, just as it may request a lease length in its requests during allocation, but as always, the server makes the final call on lease length.

Server Receives and Processes *DHCPREQUEST* Message and Creates Reply

Assuming the server is reachable, it will receive and process the client's renewal request. There are two possible responses:

Server Agrees to Renew Client Lease: The server decides that the client's lease can be renewed. It prepares to send to the client a *DHCPACK* message to confirm the lease's renewal, indicating the new lease length and any parameters that may have changed since the lease was created or last renewed.

Server Refuses to Renew Client Lease: The server decides for whatever reason not to renew the client's lease. It will create a *DHCPNAK* message.

Server Sends Reply

The server sends the *DHCPACK* or *DHCPNAK* message back to the client.

Client Receives and Processes Server Reply

The client takes the appropriate action in response to the server's reply:

Positive Acknowledgment: The client receives a *DHCPACK* message, renewing the lease. The client makes note of the new lease expiration time and any changed parameters sent by the server, resets the *T1* and *T2* timers, and transitions back to the *BOUND* state. Note that the client does *not* need to do an ARP IP address check when it is renewing.

Negative Acknowledgment: The message is a *DHCPNAK*, which tells the client that its lease renewal request has been denied. The client will immediately transition to the *INIT* state to get a new lease—step #1 in the allocation process.

Rebinding Timer (*T2*) Expires

If the client receives no reply from the server, it will remain in the *RENEWING* state, and will regularly retransmit the unicast *DHCPREQUEST* to the server. During this period of time, the client is still operating normally, from the perspective of its user. If no response from the server is received, eventually the rebinding timer (*T2*) expires. This will cause the client to transition to the *REBINDING* state. Recall that by default, the *T2* timer is set to 87.5% (7/8ths) of the length of the lease.

Client Sends *DHCPREQUEST* Rebinding Message

Having received no response from the server that initially granted the lease, the client “gives up” on that server and tries to contact any server that may be able to extend its existing lease. It creates a *DHCPREQUEST* message and puts its IP address in the *CIAddr* field, indicating clearly that it presently owns that address. It then broadcasts the request on the local network.

Servers Receives and Processes *DHCPREQUEST* Message and Send Reply

Each server receives the request, and responds according to the information it has for the client (a server that has no information about the lease or may have outdated information does not respond):

Server Agrees to Rebind Client Lease: A server has information about the client's lease and agrees to extend it. It prepares for the client a *DHCPACK* message to confirm the lease's renewal, indicating any parameters that may have changed since the lease was created or last renewed.

Server Decides Client Cannot Extend Its Current Lease: A server determines that for whatever reason, this client's lease should not be extended. It gets ready to send back to the client a *DHCPNAK* message.

Server Sends Reply

Each server that is responding to the client sends its *DHCPACK* or *DHCPNAK* message.

Client Receives Server Reply

The client takes the appropriate action in response to the two possibilities in the preceding step:

Positive Acknowledgment: The client receives a *DHCPACK* message, rebinding the lease. The client makes note of the server that is now in charge of this lease, the new lease expiration time, and any changed parameters sent by the server. It resets the *T1* and *T2* timers, and transitions back to the *BOUND* state. (It may also probe the new address as it does during regular lease allocation.)

Negative Acknowledgment: The message is a *DHCPNAK*, which tells the client that some server has determined that the lease should not be extended. The client immediately transitions to the *INIT* state to get a new lease—step #1 in the allocation process.

Lease Expires

If the client receives no response to its broadcast rebinding request, it will, as in the *RENEWING* state, retransmit the request regularly. If no response is received by the time the lease expires, it transitions to the *INIT* state to get a new lease.

3.3. Unit 3: ACL (Standard and Extended) (Statement order)

What is ACL?

An Access Control List (ACL) is a sequential list of permit or deny statements that apply to IP addresses or upper-layer protocols

ACLs enable you to control traffic into and out of your network.

- Can be as simple as permitting or denying network hosts or addresses.
- Or to control network traffic based on the TCP port being used.

Using ACLs to Secure Networks.

The ACL can extract the following information from the packet header, test it against its rules and make permit or deny decisions based on:

- Source IP address.
- Destination IP address.
and....
- TCP/UDP source port.
- TCP/UDP destination port

As each packet comes through an interface with an associated ACL:

- The ACL is checked from top to bottom.
 - One line at a time.

Matches the pattern defined in the ACL statement to the specified area of the incoming packet.

Stops checking when it finds a matching statement.

- Takes the defined action (permit or deny).

If no match is present, the default is to deny the packet.

Advantages of Access Lists.

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 at the router interfaces.

Allow an administrator to control what areas a client can access on a network. On Figure 32, we can see some ACL configuration on network topology.

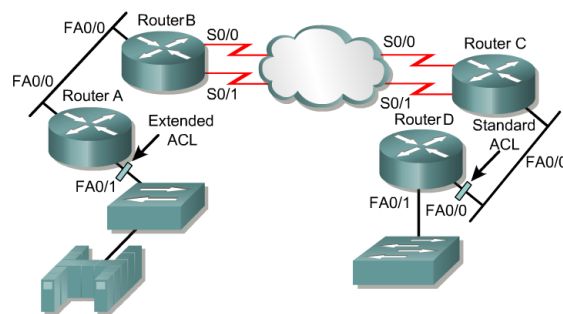


Figure 32. ACL configuration on Topology

The Three P's

- **One ACL per protocol.**
Defined for each protocol.
- **One ACL per direction.**
One direction at a time (in or out).
- **One ACL per interface.**
Control traffic an interface.

How ACLs work

Access-list needs to be attached on an interface (if the access-list is created but it is not assigned on interface {physical or virtual} it is not doing any traffic control).

The ACL consists of a sequential list of rules that apply to either incoming or outgoing packets. One rule may allow entry to the interface when it sees incoming packets from a field office's internet address. A second rule would block any other incoming packets from the public internet.

Depending on the type of ACL, control lists let an organization:

- Limit the people and devices allowed in from the internet.
- Limit the people and devices allowed to communicate to the internet.
- Limit access to internal networks or resources.
- Limit access between internal networks or resources.
- Reduce the risk of spoofing and denial of service attacks.

Types of ACL

Standard ACLs

Standard access control lists use the packet's source address as the filter. The source can be as specific or as general as needed. For example, rules may be set to accept traffic from a remote office's internet address but deny access to all other internet traffic. They do not distinguish between the IP traffic such as TCP, UDP, HTTPS, etc.

Extended ACLs

Extended access control lists are more flexible. These ACLs can filter packets based on their source, destination, port, or protocol. An extended ACL can have incoming rules that block all UDP traffic while accepting TCP packets.

In addition, the ACLs can be created by number or name.

Numbered ACLs

You assign a number based on which protocol you want filtered:

(1 to 99) and (1300 to 1999): Standard IP ACL

(100 to 199) and (2000 to 2699): Extended IP ACL

Named ACLs

You assign a name by providing the name of the ACL:

Names can contain alphanumeric characters.

It is suggested that the name be written in CAPITAL LETTERS.

Names cannot contain spaces or punctuation and must begin with a letter.

You can add or delete entries within the ACL.

Rules for ACL

- 1) The standard Access-list is generally applied close to the destination (but not always).
- 2) The extended Access-list is generally applied close to the source (but not always).
- 3) We can assign only one ACL per interface per protocol per direction, i.e., only one inbound and outbound ACL is permitted per interface.
- 4) We cannot remove a rule from an Access-list if we are using numbered Access-list. If we try to remove a rule, then the whole ACL will be removed. If we are using named access lists, then we can delete a specific rule.
- 5) Every new rule which is added to the access list will be placed at the bottom of the access list therefore before implementing the access lists, analyses the whole scenario carefully.
- 6) As there is an implicit deny at the end of every access list, we should have at least a permit statement in our Access-list otherwise all traffic will be denied.
- 7) Standard access lists and extended access lists cannot have the same name.

3.4. Unit 4: NAT (Static, Dynamic NAT, PAT, Overload)

What is NAT (Network Address Translation)?

There are several situations where we need address translation such as, a network which do not have sufficient public IP addresses want to connect with the Internet, two networks which have same IP addresses want to merge or due to security reason a network want to hide its internal IP structure from the external world. NAT (Network Address Translation) is the process which translates IP address. NAT can be performed at firewall, server, and router.

See below terms and their definitions, as it will help to understand how NAT works. On Table 6, we can see some NAT terminology.

Term	Description
Inside Local IP Address	Before translation source IP address located inside the local network.
Inside Global IP Address	After translation source IP address located outside the local network.
Outside Global IP Address	Before translation destination IP address located outside the remote network.
Outside Local IP Address	After translation destination IP address located inside the remote network.

Table 6. NAT definition

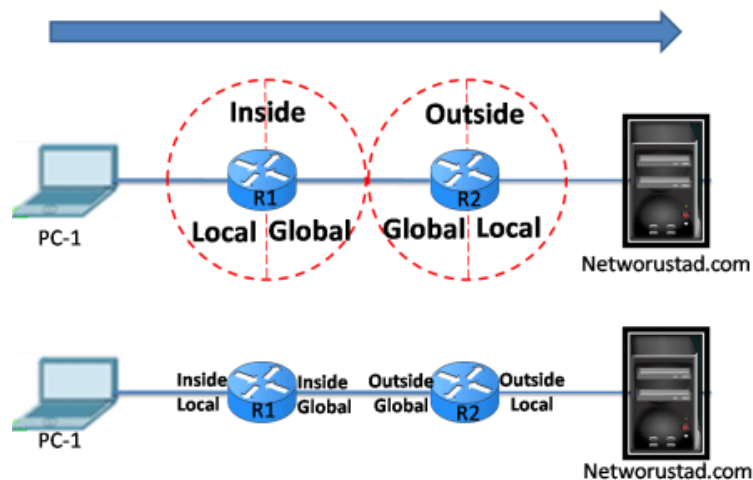


Figure 33. NAT flow.

Above Figure 33 refers to the R1 perspective.

Now, there are different NAT types (Static NAT, Dynamic NAT, NAT Overload & PAT), let us discuss all of them.

Types of NAT

There are three types of NAT: Static NAT, Dynamic NAT and PAT. These types define how inside local IP address will be mapped with inside global IP address.

Static NAT

In this type we manually map each inside local IP address with inside global IP address. Since this type uses one to one mapping, we need exactly same number of IP address on both sides.

Dynamic NAT

In this type we create a pool of inside global IP addresses and let the NAT device to map inside local IP address with the available outside global IP address from the pool automatically.

PAT

In this type a single inside global IP address is mapped with multiple inside local IP addresses using the source port address. This is also known as PAT (Port Address Translation) or NAT overload.

Advantages and disadvantages of NAT

Nat provides following advantages: -

- NAT solves IP overlapping issue.
- NAT hides internal IP structure from external world.
- NAT allows us to connect with any network without changing IP address.
- NAT allows us to connect multiple computers with internet through the single the public IP address.

NAT has following disadvantages: -

- NAT adds additional delay in network.
- Several applications are not compatible with NAT.
- End to end IP traceability will not work with NAT.
- NAT hides actual end device.