INDUSTRIAL TRAINING REPORT

‘CCNA Module – INTRODUCTION TO NETWORKS’

Submitted in partial fulfillment of requirement of the Degree

of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

SUBMITTED BY

Ayush Asati

EN20CS301107

SUBMITTED TO

Prof. Mrs. Sonali Potadar

Department of Computer Science & Engineering

Faculty of Engineering

MEDI-CAPS UNIVERSITY, INDORE- 453331

Aug-Dec 23

Report Approval

The Industrial Training Report entitled **"CCNA Module – INTODUCTION TO NETWORKS"** is hereby approved as a creditable study of an engineering subject carried out and presented in a manner satisfactory to warrant its acceptance as prerequisite for the Degree for which it has been submitted.

It is to be understood that by this approval the undersigned do not endorse or approved any statement made, opinion expressed, or conclusion drawn there in; but approve the "Industrial Training Report" only for the purpose for which it has been submitted.

Internal Examiner Name:
Designation:
Affiliation:

External Examiner Name:
Designation:
Affiliation:

Declaration

I hereby declare that the Industrial Training entitled **“CCNA Module – INTODUCTION TO NETWORKS”** submitted in partial fulfillment for the award of the degree of Bachelor of Technology in ‘Computer Science & Engineering’ completed under the supervision of Prof. **Dr. Kailash Bandhu**, Department of **Computer Science & Engineering,** Medi-Caps University, Indore from **June 12, 2023** to **July 7, 2023** . Further, I declare that the content of this Industrial Training, in full or in parts, have neither been taken from any other source nor have been submitted to any other Institute or University for the award of any degree or diploma.

Ayush Asati

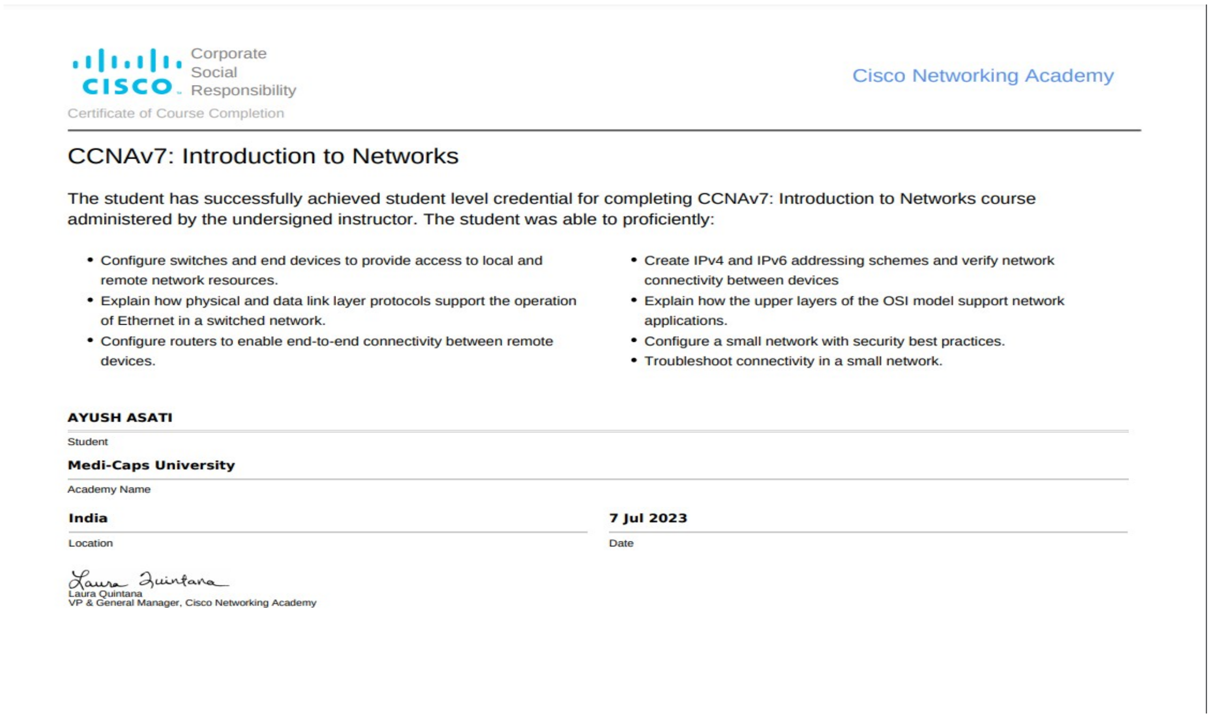
EN20CS301107

SIGNATURE

Certificate

This is to certify that Ayush Asati has completed Industrial Training during the period from June 12, 2023 to July 7, 2023 in our Organization as a Partial Fulfillment of Degree of Bachelor of Technology in Computer Science & Engineering. He was trained in the field of Computer Science.

Signature & Seal of Training Manager



CISCO Corporate Social Responsibility

Cisco Networking Academy

Certificate of Course Completion

CCNAv7: Introduction to Networks

The student has successfully achieved student level credential for completing CCNAv7: Introduction to Networks course administered by the undersigned instructor. The student was able to proficiently:

- Configure switches and end devices to provide access to local and remote network resources.
- Explain how physical and data link layer protocols support the operation of Ethernet in a switched network.
- Configure routers to enable end-to-end connectivity between remote devices.
- Create IPv4 and IPv6 addressing schemes and verify network connectivity between devices
- Explain how the upper layers of the OSI model support network applications.
- Configure a small network with security best practices.
- Troubleshoot connectivity in a small network.

AYUSH ASATI

Student

Medi-Caps University

Academy Name

India	**7 Jul 2023**
Location	Date

Laura Quintana

Laura Quintana
VP & General Manager, Cisco Networking Academy

Dr. Pramod S. Nair

Head of the Department

Computer Science & Engineering

Medi-Caps University, Indore

Acknowledgements

I would like to express my deepest gratitude to Honorable Chancellor, **Shri R C Mittal**, who has provided me with every facility to successfully carry out this Industrial Training, and my profound indebtedness to **Prof. (Dr.) Dilip Kumar Patnaik**, Vice Chancellor, Medi-Caps University, whose unfailing support, and enthusiasm has always boosted up my morale. I also thank **Prof. (Dr.) Pramod S. Nair**, Dean, Faculty of Engineering, Medi-Caps University, for giving me a chance to work on this Industrial Training. I would also like to thank my Head of the Department **Prof. (Dr.) Ratnesh Litoriya** for his continuous encouragement for betterment of the Industrial Training.

I express my heartfelt gratitude to my **Instructor and Guide** Prof. **Dr. Kailash Bandhu**, Department of Computer Science & Engineering, Medi-Caps University, Indore, without whose continuous help and support, this Industrial Training would ever have reached to the completion.

It is their help and support, due to which we became able to complete the design and technical report.

Without their support this report would not have been possible.

Ayush Asati

EN20CS301107

B. Tech - IV Year

Department of Computer Science & Engineering

Faculty of Engineering

Medi-Caps University, Indore

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction About Industry

The whole training program is done under Cisco Networking Academy in Medi-Caps University. Cisco Networking Academy is an IT skills and career building program for learning institutions and individuals worldwide. More than 5.5 million people have joined the Networking Academy and become a force for change in the global economy since 1997.

From secondary schools to universities to community organizations, more than 9000 institutions in 170+ countries offer the Networking Academy curriculum. It is the flagship program of Cisco Corporate Social Responsibility (CSR) efforts. Together, they are building the workforce of tomorrow.

This academy provides the latest courses on the Networking domain to its students inside the campus to keep them updated about the latest advancements. The support provided by CISCO for the course includes:

- Establishment of Latest Technology Labs
- Train the Trainer Program
- Student Engagement

Chapter 2: Overview of Training

I have completed the Module – 'Introduction to Networks' in Cisco Networking Academy during summers.

Module gives the advanced and fundamental concepts of networking technology. It provides complete understanding of both the practical and conceptual skills that build the foundation for understanding basic networking. It consists following:

- Examine human versus network communication and see the parallels between them
- Be introduced to the two major models used to plan and implement networks: OSI and TCP/IP
- Gain an understanding of the "layered" approach to networks
- Examine the OSI and TCP/IP layers in detail to understand their functions and services
- Become familiar with the various network devices and network addressing schemes
- Discover the types of media used to carry data across the network

Tools and Technology Used

- Cisco Packet Tracer
- PUTTY

Work Done

A. To design and study various cables and devices.
B. To design a LAN & VLAN.
C. To design a WAN.
D. To program & configure a Switch.
E. To program & configure a Router.
F. To design a network.
G. To set & encrypt passwords for router and switches.

Chapter 3: Learning After Training

3.1 Different Network Devices & Cables

Hubs

Hubs function at the physical layer and provide a logical bus structure for Ethernet; devices connected to the hub have the illusion that they are all connected to the same physical piece of wire. Devices connected to a hub are in the same collision domain, since hubs are repeaters and they repeat any physical layer signal that they receive. Cisco has many hub products, including the following: 1500 Micro Hub; 1528 10/100 Micro Hub; 100, 200, 300, and 400 Fast Hubs.

Switches

They are normally used to solve bandwidth and collision problems. Cisco supports different switching products, including the following: 1548 Micro Switch 10/100, Catalyst 1900 and 2800, Catalyst 2950, Catalyst 3550, Catalyst 4000, Catalyst 6x00, and Catalyst 8500 switches. Most of these switches support only layer-2 functionality, like the Catalyst 1900, while others, such as the Catalyst 3550 switch, support bother layer-2 and layer-3.

Routers

As I mentioned in Chapter 2, routers are used to solve many problems, including the containment of broadcasts for home office solutions, Cisco recommends the following products: 800, 900, 1600, and 1700 series routers. For small office solutions, Cisco recommends the 1600, 1700, and 2500 series of routers. For branch office solutions, Cisco recommends the 2600, 3600, and 3700 series routers. For central site solutions, Cisco recommends the 3600, 3700, 7x00, and 12000

Connections

Cisco's networking products support two types of external connections: **ports (referred to as lines) and interfaces.** Physical ports are used for management purposes and provide an out-of-band method for managing your Cisco product. Out-of-band means that your management tasks do not affect traffic that is flowing through your Cisco product. Interfaces are used to connect different networking devices together, such as a switch to router or a hub to a PC. Interfaces are connected to the backplane of the switch. You can also use interfaces for management purposes, but doing so can affect the performance of your network device. These types of connections are called in-band connections.

Console Port

Almost every Cisco product has a console port. This port is used to establish an out of-band connection in order to access the CLI to manage Cisco device. Once ***Out-of-band management does not affect the bandwidth flowing through your network, while in-band management does.***

CERTIFICATION OBJECTIVE 4.03

Cabling

Ethernet Cabling

Ethernet has become the de facto standard for LAN implementations. At one time, there were three competing technologies: Ethernet, Token Ring, and FDDI. Because of the cost of FDDI, it was never really implemented on a wide scale but used only for backbone connections. Token Ring, however, was designed and heavily promoted by IBM. Therefore, most companies that used other LAN media types have converted to Ethernet.

Cabling Specifications

IEEE 802.3 specifies the following standards for 10 Mbps Ethernet: 10Base2, 10Base5, 10BaseT, and 10BaseFL. IEEE 802.3r specifies the following standards for 100 Mbps Ethernet, called Fast Ethernet: 100BaseFX and 100BaseTX.

Cabling Devices

With today’s implementation of Ethernet over copper, two components make up the connection: an RJ-45 connector and a Category-5 UTP cable. The cable has eight wires in it (4-pair of wires). There are two types of implementations for the pinouts of the two sides of the cable: straight-through and crossover. A straight-through cable has pin 1 on one side connected to pin 1 on the other side, pin 2 to pin 2, and so on. A straight-through cable is used for DTE-to-DCE connections. The terms DTE and DCE are typically used in WAN connections, where the DCE provides clocking. In LAN terms, a DTE is a router, PC, or file server and a DCE is a hub or a switch. Here is when you should use a straight-through cable: A crossover cable crosses over two sets of wires: pin 1 on one side is connected to pin 3 on the other and pin 2 is connected to pin 6. Crossover cables should be used when you connect a DTE to another DTE or a DCE to another DCE.

3.2 IP Addressing

Introduction

Ipv4 addresses are 32 bits in length. However, to make the addresses readable, they are broken into four bytes (called octets), with a period (decimal) between each byte. Let’s look at a simple example: 11111111111111111111111111111111, which is 32 1’s. This is broken up into four octets, like this: 11111111.11111111.11111111.1111111. Then each of these octets is converted into decimal, resulting in 255.255.255.255. The format of this address is commonly called *dotted decimal*.

Classes of Addresses

Logical, or layer-3, addresses have two components: a network and host number. The network number uniquely identifies a segment in the network and a host number uniquely identifies a device on a segment. The combination of these two numbers must be unique throughout the entire network. Network numbers is divided into five classes: Class A, B, C, D, and E. Each of these classes has a predefined network and host boundary:

- With a Class A address, the first byte is a network number (8 bits) and the last 3 bytes are for host numbers (24 bits)
- With a Class B address, the first two bytes are a network number (16 bits) and the last 2 bytes are for host numbers (16 bits)
- With a Class C address, the first three bytes are a network number (24 bits) and the last 1 byte is for host numbers (8 bits)
- Class D addresses are used for multicasting and Class E addresses are reserved
- Class A addresses range from 1-126: 0 is reserved and represents all IP addresses; 127 is a reserved address and are used for testing, like a loop back on an interface: 00000001-01111111.
- Class B addresses range from 128-191: 10000000-10111111.
- Class C addresses range from 192-223: 11000000-11011111.
- Class D addresses range from 224-239: 11100000-11101111.
- Class E addresses range from 240-254: 255 is a reserved address and are used for broadcasting purposes.

When you are dealing with IP addresses, there are always two numbers reserved for a given network number: the first address in the network represents the network's address, and the last address in the network represents the broadcast address for this network, commonly called a *directed broadcast*. There are two IP addresses reserved: 0.0.0.0 (the very first address), which represents all IP addresses, and 255.255.255.255 (the very last address), which is the local broadcast address (all devices should process this datagram). Within this range of addresses for Class A, B, and C addresses, there are some reserved addresses, commonly called *Private Addresses*. All the other addresses in these classes are called public addresses.

Here is a list of private addresses, which are assigned in RFC 1918:

- Class A: 10.0.0.0-10.255.255.255 (1 Class A network)
- Class B: 172.16.0.0-172.31.255.255 (16 Class B networks)
- Class C: 192.168.0.0-192.168.255.255 (256 Class C networks)

IP Address Components

There are two components to addressing: network and host. The host portion is actually broken into three subcomponents: network address, host addresses, and directed broadcast address. The very first address in a network number is called the network address. This address is used to uniquely identify one segment from all of the other segments in the network. The last address in the network number is called the directed broadcast address, and is used to represent all hosts on this network segment. Middle addresses can be assigned to host devices on the segment, like PCs, servers, routers, and switches.

Host Addresses

Any number between the network address and the directed broadcast address is a host address. In An important item to point out about this process is that for any given network number, you *lose* two addresses. The first address in a network is reserved for the network itself and the last address is reserved for the directed broadcast address. There is a formula that defines the number of available host addresses, assuming that you know the number of bits that are reserved for host numbers: **2N – 2**.

So, as an example, a Class C network has a 24-bit network number component and an 8-bit host component. Therefore, for a Class C network, the lowest address in this fourth octet is 0 and the last address in this octet is 255 (all 8 bits are set to 1). All numbers between 1-254, are host addresses for the class C network. Using the addressing formula, it can be easily shown that Class C network has 254 host addresses.

Subnetting

To overcome the efficiency issue, subnetting was introduced. Subnetting allows you to take some of the higher-order ***host*** bits in a network number and use them to create more networks. In the process of creating more networks, each of these additional networks has a lesser number of hosts. These smaller networks are commonly called *subnets*. Let's look at an example. A Class C network has 8 host bits, giving you a total of 256 addresses. Of these 256 addresses, you can only use 254 for host devices, like PCs, routers, and servers. Let's assume that you use the highest-order bit to create more networks, leaving 7 bits for host addresses. With this example, you are creating two subnets: 21 = 2. In this formula, the 1 is the number of subnet bits. In each of these subnets you have 126 host addresses: 27 – 2 = 126.

In this example, there is smaller wastage of addresses.

Subnet Masks

When dealing with TCP/IP addresses, there are actually three components to the address: A network component, a host component, and a *subnet mask*. The function of the subnet mask is to differentiate between the network address, the host addresses, and the directed broadcast address. Subnetting is defined in RFC 950. Like an IP address, the subnet mask is 32 bits long. In binary, a 1 in a bit position in the subnet mask represents a network component and a 0 in a bit position represents a host component. One restriction of subnet masks is that all the network bits (1s) must be contiguous and all the host bits (0s) are contiguous. A subnet mask of 111111.11111111.11111111.11111000 (255.255.255.248), however, is valid.

There are actually four methods that you can use to represent a subnet mask.

Here is a list with a demonstration using a Class C network:

- Dotted-decimal: 192.168.1.0 255.255.255.0
- Number of networking bits: 192.168.1.0/24
- Hexadecimal: 192.168.1.0 0xFFFFFF00
- Binary: 192.168.1.0 11111111111111111111111100000000

Subnet Masks Values

Given the fact that subnet mask values must have all 1's contiguous and all 0's contiguous. For a Class A network, the default subnet mask is 255.0.0.0: the first octet is the network number and the last three octets are the host numbers. For a Class B network, the default subnet mask is 255.255.0.0: the first two octets are the network number and the last two octets are the host numbers. For a Class C network, the default subnet mask is 255.255.255.0: the first three octets are the network number and the last octet is the host numbers.

3.3 OSI Model

The OSI model is a layered model and a conceptual standard used for defining standards to promote multi-vendor integration as well as maintain constant interfaces and isolate changes of implementation to a single layer. It is NOT application or protocol specific. In order to pass any Cisco exam, you need to know the OSI model inside and out.

The OSI Model consists of 7 layers as follows:

Layer	Description	Device	Protocol
Application	Provides network access for applications, flow control and error recovery. Provides communications services to applications by identifying and establishing the availability of other computers as well as to determine if sufficient resources exist for communication purposes.	Gateway	NCP, SMB, SMTP, FTP, SNMP, Telnet, Appletalk
Presentation	Performs protocol conversion, encryption, and data compression	Gateway and redirectors	NCP, AFP, TDI
Session	Allows 2 applications to communicate over a network by opening a session and synchronizing the involved computers. Handles connection establishment, data transfer and connection release	Gateway	NetBios
Transport	Repackages messages into smaller formats, provides error free delivery and error handling functions	Gateway	NetBEUI, TCP, SPX, and NWLink
Network	Handles addressing, translates logical	Router and	IP, IPX,

	addresses and names to physical addresses, routing, and traffic management.	brouter	NWLink, NetBEUI
**Data Link	Packages raw bits into frames making it transmittable across a network link and includes a cyclical redundancy check (CRC). It consists of the LLC sublayer and the MAC sublayer. The MAC sublayer is important to remember, as it is responsible for appending the MAC address of the next hop to the frame header. On the contrary, LLC sublayer uses Destination Service Access Points and Source Service Access Points to create links for the MAC sublayers.	Switch, bridge and brouter	None
Physical	Physical layer works with the physical media for transmitting and receiving data bits via certain encoding schemes. It also includes specifications for certain mechanical connection features, such as the adaptor connector.	Multiplexer and repeater	None

Table – 1 OSI Model

Here is an easy way to memorize the order of the layers: **A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing. The first letter of each word corresponds to the first letter of one of the layers. It is a little corny, but it works.

The table above mentions the term “MAC Address”. A MAC address is a 48 bit address for uniquely identifying devices on the network. Something likes 00-00-12-33-FA-BC, we call this way of presenting the address a 12 hexadecimal digits format. The first 6 digits specify the manufacture, while the remainders are for the host itself. The ARP Protocol is used to determine the IP to MAC mapping. And of course, MAC addresses cannot be duplicated in the network or problems will occur.

Data encapsulation takes place in the OSI model. It is the process in which the information in a protocol raped in the data “ection of a”other protocol. The process can be broken down into the following steps:

User information -> data -> segments -> packets/datagrams -> frames -> bits.

When discussing the OSI model it is important to keep in mind the differences between “Connection-oriented” and “Connectionless” communications. A connection-oriented communication has the following characteristics:

- A session is guaranteed.
- Acknowledgements are issued and received at the transport layer, meaning if the sender does not receive an acknowledgement before the timer expires, the packet is retransmitted.
- Phrases in a connection-oriented service involve Call Setup, Data transfer and Call termination.
- All traffic must travel along the same static path.
- A failure along the static communication path can fail the connection.
- A guaranteed rate of throughput occupies resources without the flexibility of dynamic allocation.
- Reliable = SLOW (this is always the case in networking).

In contrast, a connectionless communication has the following characteristics:

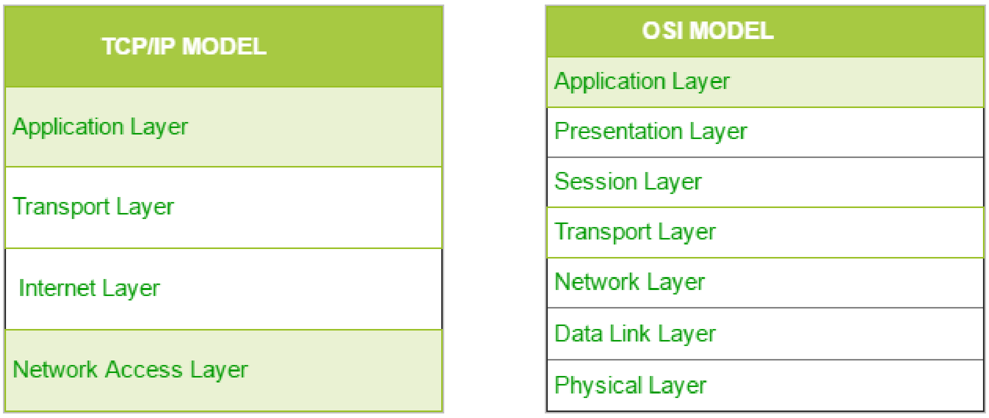
- Often used for voice and video applications.
- Neither guarantee nor acknowledgement.
- Dynamic path selection.
- Dynamic bandwidth allocation.
- Unreliable = FAST.

3.4 TCP/IP Model

The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

The diagrammatic comparison of the TCP/IP and OSI model is as follows :



TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer

OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Figure – 1

1.5 Network Access Layer –

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.
We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

1.6 Internet Layer –

This layer parallels the functions of OSI’s Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers.
2. IP has 2 versions: Ipv4 and Ipv6. Ipv4 is the one that most of the websites are using currently. But Ipv6 is growing as the number of Ipv4 addresses are limited in number when compared to the number of users.
3. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
4. **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

1.7 Host-to-Host Layer –

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

1. **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
2. **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

1.8 Application Layer –

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

2. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
3. **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
4. **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it’s out of sync.

3.5 Switch Configuration & VLAN

Basic switching concepts and the operation of Cisco switches

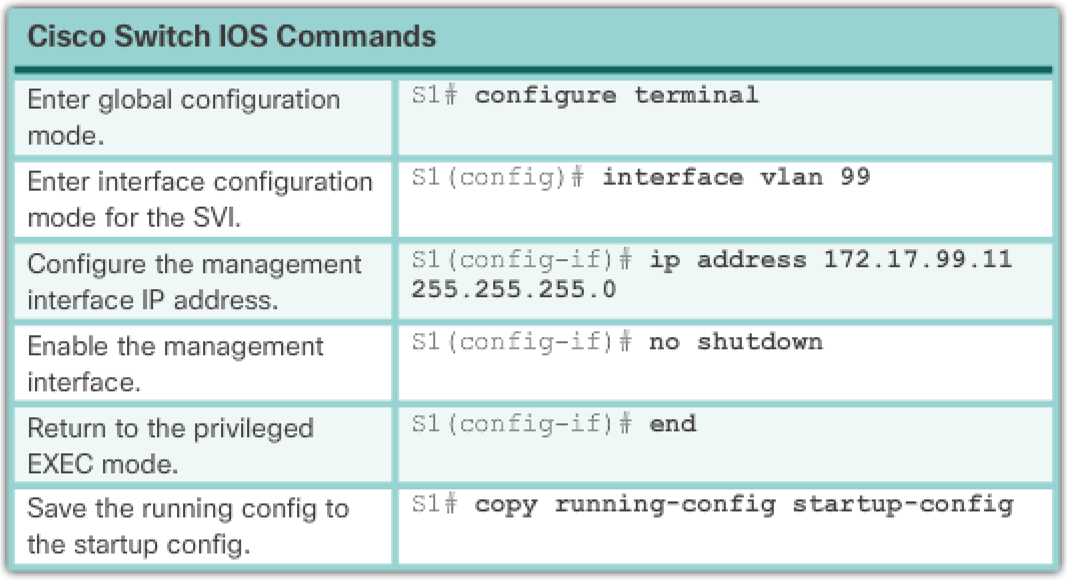
Switches are used to connect multiple devices together on the same network. In a properly designed network, LAN switches are responsible for directing and controlling the data flow at the access layer to networked resources.

Cisco switches are self-configuring and no additional configurations are necessary for them to function out of the box. However, Cisco switches run Cisco IOS, and can be manually configured to better meet the needs of the network. This includes adjusting port speed, bandwidth, and security requirements. Additionally, Cisco switches can be managed both locally and remotely. To remotely manage a switch, it needs to have an IP address and default gateway configured.

The beauty of Cisco switches is that we can remotely access and manages switches whichh removes the overhead of manual configuration of network administrator. So, to gain remote access of switch we need to do following steps:

Table – 2

Configure Switch Management Interface



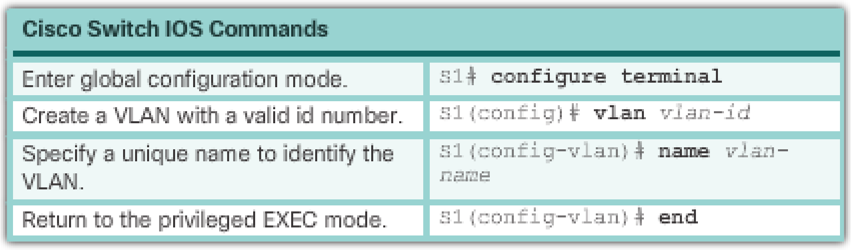
Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode for the SVI.	`S1(config)# interface vlan 99`
Configure the management interface IP address.	`S1(config-if)# ip address 172.17.99.11 255.255.255.0`
Enable the management interface.	`S1(config-if)# no shutdown`
Return to the privileged EXEC mode.	`S1(config-if)# end`
Save the running config to the startup config.	`S1# copy running-config startup-config`

VLAN Switching Technology

Within a switched internetwork, VLANs provide segmentation and organizational flexibility. VLANs provide a way to group devices within a LAN. A group of devices within a VLAN communicate as if they were attached to the same wire. VLANs are based on logical connections, instead of physical connections.

VLANs allow an administrator to segment networks based on factors such as function, project team, or application, without regard for the physical location of the user or device.

Create a VLAN

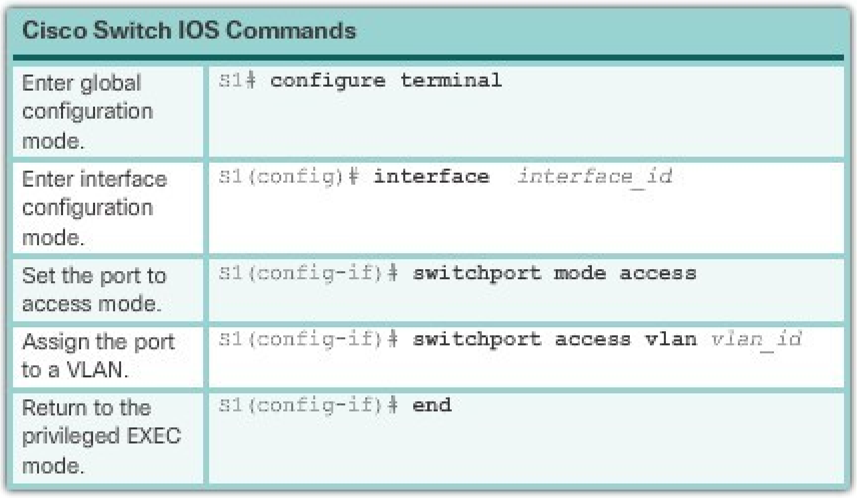


Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Create a VLAN with a valid id number.	S1(config)# **vlan** *vlan-id*
Specify a unique name to identify the VLAN.	S1(config-vlan)# **name** *vlan-name*
Return to the privileged EXEC mode.	S1(config-vlan)# **end**

Table – 3

After creating a VLAN, the next step is to assign ports to the VLAN. An access port can belong to only one VLAN at a time.

Assign Ports to VLANs



Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface** *interface_id*
Set the port to access mode.	S1(config-if)# **switchport mode access**
Assign the port to a VLAN.	S1(config-if)# **switchport access vlan** *vlan_id*
Return to the privileged EXEC mode.	S1(config-if)# **end**

Table – 4

Now for verifying VLAN Information **show vlan** command is used in privileged mode.

3.6 Router & Routing

Bringing Up a Router

When you first bring up a Cisco router, it will run a power-on self-test (POST). If it passes, it will then look for and load the Cisco IOS from flash memory—if an IOS file is present. In case you don't know, flash memory is an electronically erasable programmable read-only memory—an EEPROM. The IOS then proceeds to load and looks for a valid configuration—the startup config— that is stored by default in nonvolatile RAM, or NVRAM.

Once the IOS is loaded, and up and running, a valid configuration will be loaded from NVRAM. If there isn't a configuration in NVRAM, the router will go into *setup mode* —a step-by-step process to help you configure the router. You can also enter setup mode at any time from the command line by typing the command **setup**
from something called privileged mode, which I'll get to in a minute. Setup mode only covers some very global commands, but it can be helpful.

Logging into the Router

After the interface status messages appear and you press Enter, the Router> prompt will appear. This is called *user exec mode* (user mode) and is mostly used to view statistics, but it's also a stepping-stone to logging into privileged mode. You can only view and change the configuration of a Cisco router in *privileged exec mode* (privileged mode), which you get into with the enable command. Here is how you would do that:

```
Router>
Router>enable
Router#
```

You now end up with a Router# prompt, which indicates you're in *privileged mode*, where you can both view and change the router's configuration. You can go back from privileged mode into user mode by using the disable command, as seen here:

```
Router#disable
Router>
```

At this point, you can type **logout** to exit the console:

```
Router>logout
```

Overview of Router Modes

To configure from a CLI, you can make global changes to the router by typing configure terminal (or **config t** for short), which puts you in global configuration mode and changes what's known as the running-config. A global command (a command run from global config) is one that is set once and affects the entire router.

```
Router#config
```

Gathering Basic Routing Information

The show version command will provide basic configuration for the system hardware as well as the software version, the names and sources of configuration files, and the boot images. Here is an example:

```
Router#sh version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-BIN-M), Version 12.2(13)T1,RELEASE SOFTWARE(fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Sat 04-Jan-03 05:58 by ccai
Image text-base: 0x80008098, data-base: 0x80C4AD94
```

Setting Passwords

There are five passwords used to secure your Cisco routers: console, auxiliary, telnet (VTY), enable password, and enable secret.. This will prompt a user for a password when the enable command is used. The other three are used to configure a password when user mode is accessed either through the console port, the auxiliary port, or via Telnet

Enable Passwords

You set the enable passwords from global configuration mode like this:

```
Router(config)#enable ?
last-resort Define enable action if no TACACS servers
respond
password Assign the privileged level password
secret Assign the privileged level secret
use-tacacs Use TACACS to check enable passwords
```

Auxiliary Password

To configure the auxiliary password, go into global configuration mode and type **line aux ?**. You can see that you only get a choice of 0–0 (that’s because there’s only one port):

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line aux ?
```

Console Password

To set the console password, use the line console 0 command. But look at what happened when I tried to type line console 0? From the aux line configuration—I received an error. You can still type line console 0 and it will accept it, but the help screens just don't work from that prompt. Type **exit** to get back one level and you'll find that your help screens now work. This is a "feature." Really.

Here's the example:

```
Router(config-line)#line console ?
% Unrecognized command
Router(config-line)#exit
Router(config)#line console ?
<0-0> First Line number
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password todd1
```

Telnet Password

To set the user-mode password for Telnet access into the router, use the line vty command. Routers that aren't running the Enterprise edition of the Cisco IOS default to five VTY lines, through 4.

```
Router(config-line)#line vty 0 ?
<1-4> Last Line Number
<cr>
Router(config-line)#line vty 0 4
Router(config-line)#login
Router(config-line)#password todd2
```

Encrypting Your Passwords

Because only the enable secret password is encrypted by default, you'll need to manually configure
the user-mode and enable passwords for encryption.

```
Router#sh running-config
[output cut]
!
enable secret 5 $1$rFbM$8.aXocHg6yHrM/zzeNkAT.
```

```
Enable password todd1
!
[output cut]
line con 0
password todd1
login
line aux 0
password todd
login
line vty 0 4
password todd2
login
!
end
Router#
```

Router Interfaces

Different routers use different methods to choose the interfaces used on them. For instance, the following command shows a Cisco 2522 router with 10 serial interfaces, labeled 0 through 9:

```
Router(config)#int serial ?
<0-9> Serial interface number
```

The 2522 router has one Ethernet 10BaseT port, and typing **interface ethernet 0** can configure that interface, as seen here:

```
Router(config)#int ethernet ?
<0-0> Ethernet interface number
Router(config)#int ethernet 0
Router(config-if)#
```

interface *type slot/port*, as seen here:

```
Router(config)#int fastethernet ?
<0-1> FastEthernet interface number
Router(config)#int fastethernet 0
% Incomplete command.
Router(config)#int fastethernet 0?
```

```
/
Router(config)#int fastethernet 0/?
<0-1> FastEthernet interface number
```

You can bring up the interface with the no shutdown command (no shut for short):

```
Router#config t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#int ethernet0
Router(config-if)#no shutdown
Router(config-if)#^Z
```

Configuring an IP Address on an Interface

Even though you don’t have to use IP on your routers, it’s most often what people use. To configure
IP addresses on an interface use the ip address command from interface configuration mode:

```
Router(config)#int e0
Router(config-if)#ip address 172.16.10.2 255.255.255.0
Router(config-if)#no shut
```

You can verify that both addresses are configured on the interface with the show runningconfig
command (sh run for short):

```
Router#sh run
Building configuration…
```

Classless Interdomain Routing

Classless Interdomain Routing (CIDR), specified in RFC 2050, is an extension to VLSM and route summarization. With VLSM, you can summarize subnets back to the Class A, B, or C network boundary. For example, if you have a Class C network 192.168.1.0/24 and subnet it with a 26-bit mask, you have created four subnets. Using VLSM and summarization, you can summarize these four subnets back to 192.168.1.0/24. CIDR takes this one step further and allows you to summarize a block of contiguous class A, B, and C network numbers. This practice is commonly referred to as *supernetting.* Figure 2 shows an example of CIDR. In this example, a router is connected to four networks: 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24. The router is summarizing these routes into a single entry: 192.168.0.0/22.

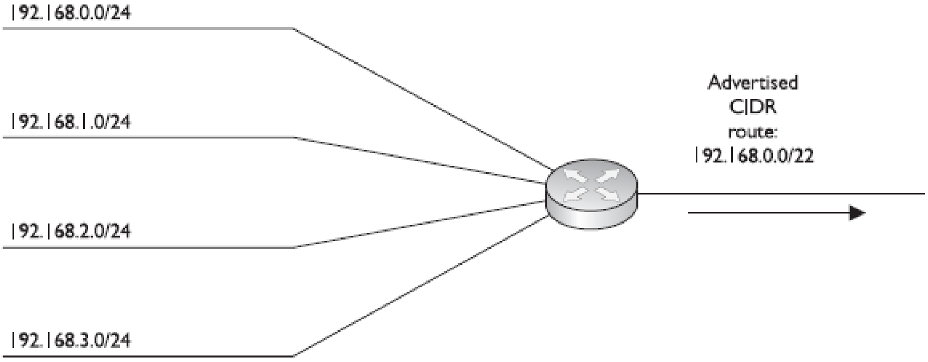


Figure -2

Routing and Subnet Masks

As mentioned in the preceding section, the routing protocol must carry the subnet mask with the corresponding network entries if you want to take advantage of route summarization. Otherwise, if you had more than one subnet mask applied to a class network number, the router wouldn't know which mask to use when routing a packet to a destination. A good example of this problem is apparent in classful protocols, such as RIPv1 and IGRP, and how you lay out your IP addresses in your network. With classful protocols, routing updates are sent out with only network entries: no subnet masks are included. The assumption is that the routers on other segments are connected to the same class network and thus know about the subnet mask. If a network number crosses boundaries from one class network to another, the classful protocol will *automatically* summarize it to the class address network number (A, B, or C), as is shown in the top part of Figure 3. As you can see, the classful protocol advertises just the network number (172.16.0.0) without any subnet mask. Plus, since the network number crosses a class boundary (172.16.0.0 to 192.168.1.0), the subnet (172.16.1.0) is not advertised, but instead the class address (172.16.0.0) is. Given the routing behavior of classful routing protocols, certain addressing designs will create problems. Let's use the network shown in the top part of Figure 4. With a classful protocol, like RIPv1, the routers, when advertising networks across a class boundary, summarize them back to their class boundary. In this example, both RouterA and RouterB advertise 172.16.0.0—they don't advertise their specific subnets for 172.16.0.0. This creates a problem with RouterC, which receives two routes for 172.16.0.0. If RouterC wanted to reach 172.16.1.0/24, it really wouldn't know which router (RouterA or RouterB) to send its packets to. This network design is referred to as a *discontiguous* subnet design—not all of the subnets are connected together. In this network, 172.16.1.0/24 and 172.16.2.0/24 are not connected via another 172.16.0.0 subnet number. This creates routing problems for other routers not connected to the 172.16.0.0 network, and therefore, discontiguous subnet designs are not recommended with classful protocols.

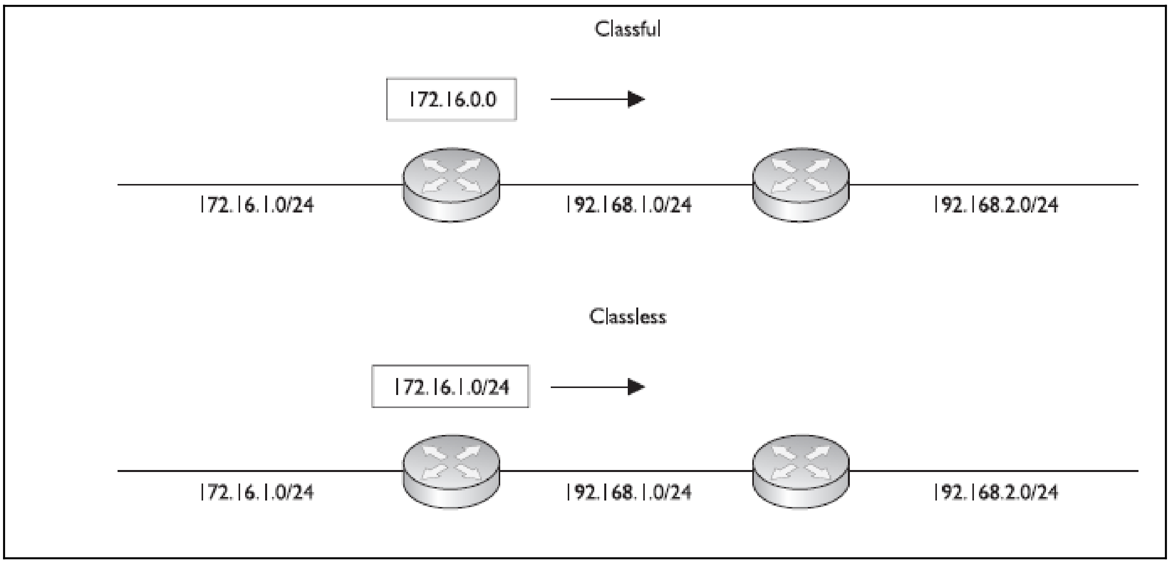


Figure – 3

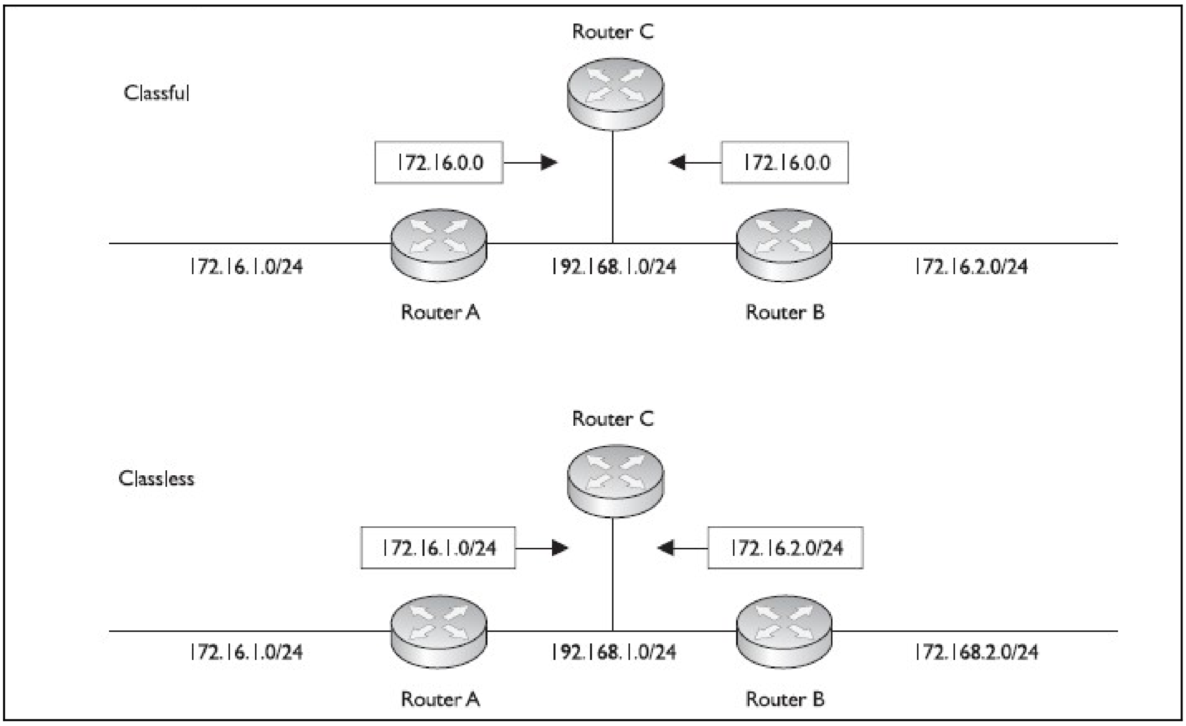


Figure – 4

The Routing Table

When implementing route summarization, another thing you'll need to consider is that routing decisions, by a router, must be made on the entire destination IP address in the IP packet header. The router always uses the longest matching prefix in the routing table to perform its routing decision. Let's use the following simplified routing table to illustrate the router's decision-making process:

1. 172.16.17.66/32
2. 172.16.17.64/27
3. 172.16.17.0/24
4. 172.16.0.0/16
5. 0.0.0.0/0

A router receives an inbound packet on one of its interfaces and examines the destination IP address in the packet header: 172.16.17.65. The router then needs to examine its routing table and find the best match for this packet and then route the packet out the corresponding interface to reach the destination. The router will basically sort the entries in the routing table from the most bits in a mask to the least
number of bits.

3.7 NAT – Network Address Translation

NAT is the virtualization of Internet Protocol (IP) addresses. NAT helps improve security and decrease the number of IP addresses an organization needs.

The main advantage of NAT (Network Address Translation) is that it can prevent the depletion of Ipv4 addresses: -

- NAT (Network Address Translation) can provide an additional layer of security by making the original source and destination addresses hidden.
- NAT (Network Address Translation) provides increased flexibility when connecting to the public Internet.
- NAT (Network Address Translation) allows to use your own private Ipv4 addressing system and prevent the internal address changes if you change the service provider.

Types of NAT: -

Static NAT (Network Address Translation) – Static NAT (Network Address

Translation) is one-to-one mapping of a private IP address to a public IP address. Static NAT (Network Address Translation) is useful when a network device inside a private network needs to be accessible from internet.

Dynamic NAT (Network Address Translation) – Dynamic NAT can be defined as mapping of a private IP address to a public IP address from a group of public IP addresses called as NAT pool. Dynamic NAT establishes a one-to-one mapping between a private IP address to a public IP address. Here the public IP address is taken from the pool of IP addresses configured on the end NAT router. The public to private mapping may vary based on the available public IP address in NAT pool.

PAT (Port Address Translation) – Port Address Translation (PAT) is another type of dynamic NAT which can map multiple private IP addresses to a single public IP address by using a technology known as Port Address Translation.

Here when a client from inside network communicate to a host in the internet, the router changes the source port (TCP or UDP) number with another port number. These port mappings are kept in a table. When the router receive from internet, it will refer the table which keep the port mappings and forward the data packet to the original sender.

3.8 Email Protocols

Email protocols are a collection of protocols that are used to send and receive emails properly. The email protocols provide the ability for the client to transmit the mail to or from the intended mail server. Email protocols are a set of commands for sharing mails between two computers. Email protocols establish communication between the sender and receiver for the transmission of email. Email forwarding includes components like two computers sending and receiving emails and the mail server. There are three basic types of email protocols.

Three basic types of email protocols involved for sending and receiving mails are:

- SMTP
- POP3
- IMAP

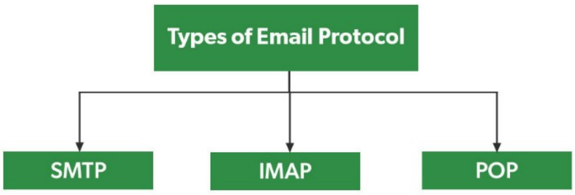


Figure – 5

SMTP (Simple Mail Transfer Protocol)

Simple Mail Transfer Protocol is used to send mails over the internet. SMTP is an application layer and connection-oriented protocol. SMTP is efficient and reliable for sending emails. SMTP uses TCP as the transport layer protocol. It handles the sending and receiving of messages between email servers over a TCP/IP network. This protocol along with sending emails also provides the feature of notification for incoming mails. When a sender sends an email then the sender's mail client sends it to the sender's mail server and then it is sent to the receiver mail server through SMTP. SMTP commands are used to identify the sender and receiver email addresses along with the message to be sent.

Some of the SMTP commands are HELLO, MAIL FROM, RCPT TO, DATA, QUIT, VERIFY, SIZE, etc. SMTP sends an error message if the mail is not delivered to the receiver hence, reliable protocol.

POP (Post Office Protocol)

Post Office Protocol is used to retrieve email for a single client. POP3 version is the current version of POP used. It is an application layer protocol. It allows to access mail offline and thus, needs less internet time. To access the message it has to be downloaded. POP allows only a single mailbox to be created on the mail server. POP does not allow search facilities Some of the POP commands are LOG IN, STAT, LIST, RETR, DELE, RSET, and QUIT.

IMAP (Internet Message Access Protocol

Internet Message Access Protocol is used to retrieve mails for multiple clients. There are several IMAP versions: IMAP, IMAP2, IMAP3, IMAP4, etc. IMAP is an application layer protocol. IMAP allows to access email without downloading them and also supports email download. The emails are maintained by the remote server. It enables all email operations such as creating, manipulating, delete the email without reading it. IMAP allows you to search emails. It allows multiple mailboxes to be created on multiple mail servers and allows concurrent access. Some of the IMAP commands are: IMAP_LOGIN, CREATE, DELETE, RENAME, SELECT, EXAMINE, and LOGOUT.

Chapter 4: Discussion

After the training, following were the key findings & learning.

1. OSI Model is the conceptual model giving basis for new research and development of models whereas TCP/IP model is the practical model used.
2. With the exhaustion of IPv4 addressed, NAT principle was used which adds complexity to the network systems and hence we are moving to IPv6 addresses. But it will take few more years to completely shift to a completely new architecture to support it.
3. Presently, we are using a hybrid version of IPv4 and IPv6 addressing along with Port Address Translation (PAT).
4. Further research is going on with more advanced versions of IP as well as to develop the robust and network architecture for future use.

Chapter 5: Conclusion

Among all the essentials for human existence, the need to interact with others ranks just below our need to sustain life. Communication is almost as important to us as our reliance on air, water, food, and shelter.

In today’s world, through the use of networks, we are connected like never before. People with ideas can communicate instantly with others to make those ideas a reality. News events and discoveries are known worldwide in seconds. Individuals can even connect and play games with friends separated by oceans and continents. We listen to recording artists, preview, or view motion pictures, read entire books, and download material for future offline access. Live sporting events and concerts can be experienced as they are happening, or recorded and viewed on demand.

Networks enable the creation of new forms of entertainment, such as online games. Players participate in any kind of online competition that game designers can imagine. We compete with friends and foes around the world as if we were all in the same room.

Even offline activities are enhanced using network collaboration services. Global communities of interest have grown rapidly. We share common experiences and hobbies well beyond our local neighborhood, city, or region. Sports fans share opinions and facts about their favorite teams. Collectors display prized collections and get expert feedback about them. Whatever form of recreation we enjoy; networks are improving our experience.

Modern networks continue to evolve to keep pace with the changing way organizations carry out their daily business. Users now expect instant access to company resources from anywhere and at any time. These resources not only include traditional data but also video and voice. There is also an increasing need for collaboration technologies that allow real-time sharing of resources between multiple remote individuals as though they were at the same physical location. All advanced services depend on the availability of a robust routing and switching infrastructure on which they can build. This infrastructure must be carefully designed, deployed, and managed to provide a necessary stable platform.

References

1. Cisco – CCNA Module 1
2. www.netacad.com
3. www.gfg.com
4. www.google.com