NETWORK
KINGS
CCNA VER0.3
WWW.NETWORKKINGS.ORG
WWW.NWKINGS.COM

CCNA :- Cisco Certified Network Associate

Congratulations! you've probably already decided to go for your Cisco certification. If you want to succeed as a technical person in the networking industry, you need to know Cisco. Cisco has a ridiculously high market share in the router and switch marketplace, with more than an 80 percent share in some markets. In many geographies and markets around the world, networking equals Cisco. If you want to be taken seriously as a network engineer, Cisco certification makes perfect sense

Cisco company name derived from SANFRANCISCO

Cisco Systems, Inc. is an American multinational corporation headquartered in San Jose, California, United States, that designs, manufactures, and sells networking equipment.

Important Websites:
Video Lessons : www.nwkings.com
Official Website: www.networkkings.org

Download packet tracer
Register in netcad account : https://goo.gl/pWbLFU

Gns3 (First make account and download)
https://www.gns3.com/software

Icons Used in This Book

Tips for Study :-

Basics of Networking

What is a network anyway?

A network is just a collection of devices and end systems connected to each other and able to communicate with each other. These could be computers, servers, smartphones, routers etc.

A network could be as large as the internet or as small as your two computers at home sharing files and a printer.

What is Networking ?

Whenthe devices which are connected together share data and resources is known as network.

Some of the components that make up a network:

Personal Computers (PC): These are the endpoint of your network, sending and
receiving data.

Interconnections: These are components that make sure data can travel from one
device to another, you need to think about:

Network Cards: they translate data from your computer in a readable format for the network.it is also known as NIC (Network interface card)

Media Cables and connectors : network cables, perhaps wireless,

Connectors: the plug you plug in your network card ,

RJ 45 is commond for ethernet cable , RJ 11 connector for landline telephones.

Routers: Routers interconnect networks and choose the best path to each network Destination, router makes its routing table for best path.

- It is an internetworking device used to connect two or more different networks
- It works on layer 3 i.e. network layer
- It Performs Routing

The Difference Between Unicast, Multicast and Broadcast Messages

Some Command Prompt for CCNA !

1. **ping** :- packet internet gopher
   it uses icmp (internet control message protocol) protocol
   For verification the other device is reachble to me or not ??
2. **ipconfig** :- to check the ip address of a computer
3. **ipconfig /all** :- to check the ip address + mac address
4. **getmac** :- to check the mac address of a computer
5. **netstat** :- to check the session's
6. **nslookup** :- to check the all servers of a website
7. **arp -a** :- to check arp table
8. **arp –d** :- to delete arp table (run as administrator)
9. **To check public ip**

Visit :- **www.whatismyipaddress.com** to check your public ip

How To assign address to your PC ?

1.windows button + R
2. type ncpa.cpl to go to your network connections
3.choose your lan adapter and go to properties and click on IPV4
4.Assign Ip address
Or visit :- http://www.wikihow.com/Configure-a-Static-Internet-Protocol-(IP)-Address-on-a-Computer

HUB	SWITCH
• **Known as Dummy Device.** • **ALWAYS do Broadcast** • **Layer 1 device** • **Shared bandwidth** • **Less no of ports** • **Doesn't learn mac address**	• which connects two or more computers together • Many no of ports • Learn mac address • Two types of switch :- ➢ Manageble switch ➢ unmanageable switch • Its is a Layer 2 Device

MAC Address vs. IP Address

- 48-bit MAC address
  - Layer 2
  - Used to get packet from one interface to another within the same LAN/subnet (Ethernet, token ring...)
  - Flat
  - Unique
  - No change when moving
- 32-bit IP address
  - Network layer
  - Used to get packet to destination IP subnet
  - Hierarchical
  - Change when moving
    - Depending on IP subnet to which node is attached

IP networks require two types of addresses. **MAC and IP**. Each station stores it's MAC address and IP address in it's own IP stack. It stores MAC and IP addresses of other stations on it's LAN or subnet in the ARP cache.

- When the packet is being sent out to a station that is on the same network LAN segment, only the MAC address is needed.
- When the packet goes beyond, to different networks and travels through routers, the MAC address is still contained in the packet, but only the IP address is used by the routers.

Figure 2-15 *Structure of Unicast Ethernet Addresses*

Ethernet Frame Form

Figure 2-14 *Commonly Used Ethernet Frame Format*

Field	Bytes	Description
Preamble	7	Synchronization.
Start Frame Delimiter (SFD)	1	Signifies that the next byte begins the Destination MAC Address field.
Destination MAC Address	6	Identifies the intended recipient of this frame.
Source MAC Address	6	Identifies the sender of this frame.
Type	2	Defines the type of protocol listed inside the frame; today, most likely identifies IP version 4 (IPv4) or IP version 6 (IPv6).
Data and Pad*	46–1500	Holds data from a higher layer, typically an L3PDU (usually an IPv4 or IPv6 packet). The sender adds padding to meet the minimum length requirement for this field (46 bytes).
Frame Check Sequence (FCS)	4	Provides a method for the receiving NIC to determine whether the frame experienced transmission errors.

IPv4 Addressing

- IP Address is Logical Address.It is a Network Layer address (Layer 3), IPv4 addresses are 32-bit numbers that are typically displayed in dotted decimal notation. A 32-bit address contains two primary parts: the network prefix and the host number.

- All hosts within a single network share the same network address. Each host also has an address that uniquely identifies it. Depending on the scope of the network and the type of device, the address is either globally or locally unique

- IP addresses are assigned by a central numbering authority called the Internet Assigned Numbers Authority (IANA).

Two Versions of IP:

IP version 4 is a 32 bit address

IP version 6 is a 128 bit address

IP Addresses are divided into 5 Classes, These are divided by IANA :- Internet Assigned Number authority.

Figure 4-6 *Division of the Entire IPv4 Address Space by Class*

Figure 4-7 *Size of Network and Host Parts of Class A, B, and C Addresses*

Network & Broadcast Address

- The network address is represented with all bits as ZERO in the host portion of the address
- The broadcast address is represented with all bits as ONES in the host portion of the address
- Valid IP Addresses lie between the Network Address and the Broadcast Address.
- Only Valid IP Addresses are assigned to hosts/clients

Private IP Address

There are certain addresses in each class of IP address that are reserved for Private Networks. These addresses are called private addresses.

Class A 10.0.0.0 to 10.255.255.255
Class B 172.16.0.0 to 172.31.255.255
Class C 192.168.0.0 to 192.168.255.255

PRIVATE IP	PUBLIC IP
• Used with the LAN or within the organization	• Used on public network (INTERNET)
• Not recognized on internet	• Recognized on internet
• Given by the administrator	• Given by the service provider (from IANA)
• Unique within the network or organization	• Globally unique
• Free	• Pay to service provider (or IANA)
• Unregistered IP	•
	• Registered

Subnet Mask

Subnet Mask:-Its an address used to identify the network and host portion of the ip address

Class A	**N.H.H.H**	**255.0.0.0**
Class B	**N.N.H.H**	**255.255.0.0**
Class C	**N.N.N.H**	**255.255.255.0**

Note:- "255" represents the network and "0" represents host.

Network:- collection / group hosts
Host:- Single PC/ computer.

Default Gateway:- Its an entry and exit point of the network.
ex:- The ip address of the router ethernet address.

Subnetting

- **Problem**: Organizations have multiple groups/entities within their organization which are independently managed. Each would prefer to manage their own IT facilities, i.e., own network
  - **Solution 1:** Allocate to each entity their own IP network/domain
    - Organization must own multiple IP address domains
    - Expensive (each IP domain costs money) and cumbersome to manage
  - **Solution 2:** Add another level of hierarchy to the existing IP addressing structure → **Subnetting**

It is the process of Dividing a Single Network into Multiple Networks.
Converting Host bits into Network Bits i.e. Converting 0's into 1's

Subnetting can be perform in two ways.

1. FLSM (Fixed Length Subnet Mask)
2. VLSM (Variable Length subnet mask)

Subnetting can be done based on requirement .

Requirement of Hosts ? **2^h - 2 >= requirement**
Requirement of Networks ? **2^n >= requirement**

What is Supernetting or CIDR?

Classless Inter-Domain Routing (CIDR) merges or combine network addresses of same class into one single address to reduce the size of the routing table.
It is done on core router to reduce the size of routing table.
It is implemented by ISP (internet service providers).

2^1 = 2	**2^{10} = 1024**
2^2 = 4	**2^{11} = 2048**
2^3 = 8	**2^{12} = 4096**
2^4 = 16	**2^{13} = 8192**
2^5 = 32	**2^{14} = 16384**
2^6 = 64	**2^{15} = 32768**
2^7 = 128	**2^{16} = 65536**
2^8 = 256	**2^{17} = 131072**

2^9 = 512	

FLSM : Example-- 1

Req = 40 hosts using C-class address network 192.168.1.0/24

1. 2^h - 2 >= req
   2^6 – 2 >= 40
   64 – 2 >= 40
   62 >= 40

Host bits required **(h) = 6**

2.Converted network Bits (n) = Total. H. Bits -- req. H. Bits
= 8 --- 6 **= 2 (n)**

4.Total . Network Bits =total network bits + converted bits = 24 + 2 = /26
subnet mask = (/26)= 255.255.255.192

5.Blocksize = 2^h = 2^6 = 64

6.Subnets = 2^n = 2^2 = 4 Subnets

7.Range :

Network ID --- Broadcast ID
192.168.1.0/26 ----- 192.168.1.63/26
192.168.1.64/26 ----- 192.168.1.127/26
192.168.1.128/26 ----- 192.168.1.191/26
192.168.1.192/26 ----- 192.168.1.255/26

FLSM : Example-- 2

1.Req = 500 hosts using B-class address network 172.16.0.0/16

2^h - 2 >= req

2^9 – 2 >= 500

512 – 2 >= 500

510 >= 500

2.Host bits required **(h)= 9**

3. **Converted network Bits** (n) = Total. H. Bits -- req. H. Bits

= 16 --- 9 = **7 (n)**

3. Total . Network Bits = total network bits + converted bits = 16 + 7 = /23

subnet mask = (/23)= 255.255.254.0

6. **Blocksize** = = 2^h = 2^9 = 512

7.**Subnets** = 2^n = 2^7 = 128 Subnets

Range

Network ID --- Broadcast ID

172.16.0.0/23 ---- 172.16.1.255/23

172.16.2.0/23 ---- 172.16.3.255/23

172.16.4.0/23 ---- 172.16.5.255/23

172.16.6.0/23 ---- 172.16.7.255/23

FLSM : Example-- 3

1.Req = 2000 hosts using A-class address network 10.0.0.0/8

2^h - 2 >= req

2^{11} – 2 >= 2000

2048 – 2 >= 2000

2046 >= 2000

2.Host bits required (h)= 11

3.Converted network Bits (n) = Total. H. Bits -- req. H. Bits
= 24 --- 11 = **13 (n)**
4. Converted network Bits (n)= 13

5.Total . N. Bits = 8+ 13 = /21
subnet mask = (/21) = 255.255.248.0

6.blocksize = $2^h = 2^{11}$ = **2048**
7.Subnets = 2n = 2^{13} = 8192 Subnets

8.Range:
Network ID --- Broadcast ID
10.0.0.0/21 … 10.0.7.255/21
10.0.8.0/21 … 10.0.15.255/21
10.0.16.0/21 … 10.0.23.255/21
…
…
10.0.248.0/21 … 10.0.255.255/21
10.1.0.0/21 --- 10.1.7.255/21
10.1.8.0/21 --- 10.1.15.255/21
10.1.16.0/21 --- 10.1.23.255/21
….
10.1.248.0/21 … 10.1.255.255/21
10.2.0.0/21 --- 10.2.7.255/21

10.2.8.0/21 --- 10.2.15.255/21
10.2.16.0/21 --- 10.2.23.255/21
…
…
10.2.248.0/21 … 10.2.255.255/21
….
…
….

10.255.0.0/21 --- 10.0.7.255/21
10.255.8.0/21 --- 10.0.15.255/21
10.255.16.0/21 --- 10.0.23.255/21
….
…
10.255.248.0/21 … 10.255.255.255/21

OSI Reference Model

- OSI was developed by the International Organization for Standardization (ISO) and introduced in 1984.
- It is a layered architecture (consists of seven layers).
- Each layer defines a set of functions in data communication.

All People Seem To Need Data Processing

Physical Layer: This layer describes stuff like voltage levels, timing, physical data rates, physical connectors and so on. Everything you can "touch" since it‟s physical.

Data Link: This layer makes sure data is formatted the correct way, takes care of error detection and makes sure data is delivered reliably. This might sound a bit vague now, for now try to remember this is where "Ethernet" lives. MAC Addresses and Ethernet frames are on the Data Link layer.

Network: This layer takes care of connectivity and path selection (routing). This is where IPv4 and IPv6 live. Every network device needs a unique address on the network.

Transport: The transport layer takes care of transport, when you downloaded this book from the Internet the file was sent in segments and transported to your computer.

- TCP lives here; it‟s a protocol which send data in a reliable way.
- UDP lives here; it‟s a protocol which sends data in an unreliable way.
- ICMP lives here; when you send a ping you are using ICMP.

Session: The session layer takes care of establishing, managing and termination of sessions between two hosts. When you are browsing a website on the internet you
are probably not the only user of the webserver hosting that website. This webserver
needs to keep track of all the different "sessions".

Presentation: This one will make sure that information is readable for the application layer by formatting and structuring the data. Most computers use the
ASCII table for characters. If another computer would use another character like
EBCDIC than the presentation layer needs to "reformat" the data so both computers
agree on the same characters.

Application: Here are your applications. E-mail, browsing the web (HTTP), FTP and
many more.

Port Numbers

TCP/UDP :- Both have 65535 ports

1- 1023 well known
1024 - 49151 registered ports

49152 - 65535 dynamic ports (generated by host)

Port Number	Protocol	Application
20	TCP	FTP data
21	TCP	FTP control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP, TCP[1]	DNS
67	UDP	DHCP Server
68	UDP	DHCP Client
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL
514	UDP	Syslog

[1] DNS uses both UDP and TCP in different instances. It uses port 53 for both TCP and UDP.

The major functions described at the Transport Layer are..

- Identifying Service
- Multiplexing & De-multiplexing
- Segmentation
- Sequencing & Reassembling
- Error Correction
- Flow Control

Identifying a Service : Services are identified at this layer with the help of Port No's. The major protocols which takes care of Data Transportation at Transport layer are…TCP,UDP

Transmission Control Protocol	User Datagram Protocol
• Connection Oriented • Reliable communication(with Ack's) • Slower data Transportation • Protocol No is 6 • Eg: HTTP, FTP, SMTP	• Connection Less • Unreliable communication (no Ack's) • Faster data Transportation • Protocol No is 17 • Eg: DNS, DHCP, TFTP

Network Layer

It is responsible for end-to end Transportation of data across multiple networks.
Logical addressing & Path determination (Routing) are described at this layer.
The protocols works at Network layer are

Routed Protocols:

Routed protocols acts as data carriers and defines logical addressing.
IP,IPX, AppleTalk.. Etc

Routing Protocols:

Routing protocols performs Path determination (Routing).
RIP, IGRP, EIGRP, OSPF.. Etc

Devices works at Network Layer are Router, Multilayer switch etc..

Data-link Layer

It is responsible for end-to-end delivery of data between the devices on a Network segment. Data link layer comprises of two sub-layers.

1) MAC (Media Access Control)

It deals with hardware addresses (MAC addresses).

MAC addresses are 12 digit Hexa-decimal identifiers used to identify the devices uniquely on the network segment.

It also provides ERROR DETECTION using CRC (Cyclic Redundancy Check) and FRAMING (Encapsulation).

Ex: Ethernet, Token ring…etc

2) LLC (Logical Link Control)

It deals with Layer 3 (Network layer)

Devices works at Data link layer are Switch, Bridge, NIC card.

Physical Layer

- It deals with physical transmission of Binary data on the given media (copper, Fiber, wireless..).
- It also deals with electrical, Mechanical and functional specifications of the devices, media.. etc
- The major functions described at this layer are..

Encoding/decoding: It is the process of converting the binary data into signals based on the type of the media.

Copper media :	Electrical signals of different voltages
Fiber media :	Light pulses of different wavelengths
Wireless media:	Radio frequency waves

Mode of transmision of signals: Signal Communication happens in three different modes Simplex, Half-duplex, Full-duplex

Devices works at physical layer are Hub, Modems, Repeater, Transmission Media

The Cisco Three-Layer Hierarchical Model:

1- Core Layer: Uses multi-layer switches.
Functions: Switches traffic as fast as possible using high speed technology (i.e. FDDI, Fast-Ethernet/Gigabit-Ethernet, ATM).

2- Distribution Layer: (also called *Workgroup layer.*) Uses routers.
Functions: Routes between LANs and VLANs. Provides Security (i.e. *Access List, Packet Filtering, Queuing, Route Redistribution*) and broadcasts control.

3- Access Layer: (also called *Desktop Layer.*) Uses switches.
Functions: Provides access to the network. Breaks collision domains.

INTRODUCTION TO ROUTERS

Wht is a Router ?

- Router is a device which makes communication possible between two or more different networks present in different geographical locations.

  - It is an internetworking device used to connect two or more different networks
  - It works on layer 3 i.e. network layer.

- It does two basic things:-
  - Select the best path from the routing table.
  - Forward the packet on that path

Which Routers to buy ?

Many companies are manufacturing Router :

- Cisco
- Juniper
- huawei

But Cisco is having Monopoly in the market of Routers

Router Classification

FIXED ROUTER	MODULAR ROUTER
• Fixed router (Non Upgradable cannot add and remove the Ethernet or serial interfaces) • Access Layer Routers are example of Fixed Router except 1600 and 1700 series	• Modular router (Upgradable can add and remove interfaces as per the requirement) • Distribution and Core Layer Routers example of Modular Router

Branch

Gain highly secure connectivity, machine learning, and cloud-managed security.

ISR 4000 Series (updated)

ISR 1000 Series (updated)

ISR 900 Series (new)

ISR 800 Series

Meraki MX

WAN aggregation

Get performance and security for WAN, Internet, and machine-to-machine (M2M) interconnectivity.

NCS 5000 Series

NCS 5500 Series

ASR 1000 Series

Edge

Grow density and resiliency with programmability for a scalable network edge.

ASR 9000 Series

ASR 1000 Series

Service provider core

Address today's needs and scale for future ones with strong ROI.

NCS 6000 Series

NCS 5500 Series

ASR 9000 Series

Industrial

Deliver enterprise-class features in rugged and harsh environments.

900 Series Industrial (new)

800 Series Industrial ISR

2000 Series Connected Grid Routers

1000 Series Connected Grid

Virtual

Get multitenant network services for public, private, or provider-hosted clouds.

IOS XRv 9000

CSR 1000v

Meraki vMX100

Small Business Routers

Get advanced capabilities and security features at an affordable price.

ISR 4221

ISR 1000 Series

ISR 900 Series (new)

Example Modular Router

Attachment Unit Interface

- AUI pin configuration is 15 pin female.
- It is known as Ethernet Port or LAN port or Default Gateway.
- It is used for connecting LAN to the Router.
- **Transceiver** is used for converting 8 wires to 15 wires. i.e. RJ45 to 15 pin converter.

Serial Port

- Serial pin configuration is 60 pin configuration female (i.e. 15 pins and 4 rows) and Smart Serial pin configuration is 26 pin configuration female.
- It is known as WAN Port
- It is used for connecting to Remote Locations
- V.35 cable is having 60 pin configuration male at one end and on the other end 18 pin configuration male.

Console Port

- It is known as Local Administrative Port
- It is generally used for Initial Configuration, Password Recovery and Local Administration of the Router. It is RJ45 Port
- **IMP :** It is the most delicate port on the Router. So make less use of the Console Port.

Console Connectivity

- Connect a rollover cable to the router console port (RJ-45 connector).
- Connect the other end of the rollover cable to the RJ-45 to DB-9 converter
- Attach the female DB-9 converter to a PC Serial Port.
- Open Emulation Software

Auxiliary Port

- It is known as Remote Administrative Port.
- Used for remote administration
- Its an RJ-45 port
- A console or a rollover cable is to be used.

2601 Model Router

Networking Software Systems

IOS

- Integrates technology, business services, and hardware support
- Reduces operational spending
- Optimizes return on investment
- Improves business productivity

IOS XE

- Supports next-generation platforms
- Runs as a single daemon within a modern Linux operating system
- Separates the data plane and control plane
- Improved services integration

IOS XR

- Focuses on the needs of service providers
- Designed for the dynamic network usage requirements of services
- Flexible programmability for dynamic reconfiguration

NX-OS

- Open, modular and programmable for an agile data center infrastructure
- Optimized for both physical and virtual data center deployments
- Highly reliable continuous system operation, optimizing uptime

Internal Components

- **ROM**
  A bootstrap program is located here. It is same as the BIOS of the PC. Bootstrap program current version is 11.0
- **Flash**
  Internetwork Operating System (IOS) developed by Cisco is stored here. IOS is Command line interface.

- **NVRAM**
  Non volatile RAM, similar to Hard Disk It is also known as Permanent Storage or Startup Configuration. Generally size of NVRAM is 32 KB.

- **RAM**

It is also known as Temporary Storage or running Configuration. Minimum size of RAM is 2MB. The size of RAM is greater than NVRAM in the Router.

- **Processor**
  Motorola Processor 70 Mhz, RISC based processor (Reduced Instruction Set Computer)

Router Start-up Sequence

- Bootstrap program loaded from ROM
- Bootstrap runs the POST
- Bootstrap locates IOS in Flash
- IOS is expanded and then loaded into RAM
- Once IOS is loaded into RAM, it looks for startup-config in NVRAM
- If found, the configuration is loaded into RAM

MODES OF A ROUTER:-

- **User Mode:-** Only some basic monitoring
- **Privileged Mode:-** monitoring and some troubleshooting
- **Global Configuration mode:-** All Configurations that effect the router globally
- **Interface mode:-** Configurations done on the specific interface
- **Rommon Mode:-** Reverting Password

Configuration Mode	Prompt
Interface	Router(config-if)#
Subinterface	Router(config-subif)#
Controller	Router(config-controller)#
Map-list	Router(config-map-list)#
Map-class	Router(config-map-class)#
Line	Router(config-line)#
Router	Router(config-router)#
IPX-router	Router(config-ipx-router)#
Route-map	Router(config-route-map)#

Console Connectivity

- Connect a rollover cable to the router console port (RJ-45 connector).
- Connect the other end of the rollover cable to the RJ-45 to DB-9 converter
- Attach the female DB-9 converter to a PC Serial Port.
- Open emulation software on the PC.

Exercise- 1
BASIC COMMANDS

User mode:
Router >
Router > enable

Privilege mode:
Router # show running-config
Router # show startup-config
Router # show flash
Router # show version
Router #show ip interface brief

Router # configure terminal (to enter in Global configurarion mode)

Global configuration mode:

Router(config) #

Assigning ip address to Ethernet interface:

Router(config) # interface <interface type> <interface no>
Router(config-if) # ip address <ip address> <subnet mask> (Interface Mode)
Router(config-if) # no shut

Assigning Telnet password:

Router(config) # line vty 0 4
Router(config-line) #login (line mode)
Router(config-line) #password <password>

Router(config-line) #exit
Router(config) #exit

Assigning console password:

Router(config) # line con 0
Router(config-line) # login (line mode)
Router(config-line) # password <password>
Router(config-line) # exit
Router(config) # exit

Assigning enable password:

Router(config) # enable secret <password> (To encrypt the password)
Router(config) # enable password <password>

Show commands:

Router # show running-config
Router # show startup-config
Router # show version
Router # show flash

Commands to save the configuration:

Router # copy running-config startup-config
(OR)
Router # write memory
(OR)
Router # write

Basic Show Commands

Router#show running-config

Router#show flash

Router#show ip protocols

Use this command to view the status of the current layer 3 routed protocols running on your router

Router#show version

This command will give you critical information, such as: router platform type, operating system revision, operating system last boot time and file location, amount of memory, number of interfaces, and configuration register

Router#show clock

***1:46:13.169 UTC Mon Nov 1 2009**

Will show you Routers clock

Router#show hosts

will display a cached list of hosts and all of their interfaces IP addresses

Router#show users

Will show a list of all users who are connected to the router

Router#show interfaces

will give you detailed information about each interface

Router#show protocols

will show the global and interface-specific status of any layer 3 protocols

Router#show ip interface brief

This command will show brief descriptions about interface. This command mostly used in troubleshooting.

There may be three possible conditions of status.

UP: - interface is up and operational

DOWN: - physical link is detected but there is some problem in configurations.

Administratively down: - port is disable by shutdown command (Default mode of any port on router.)

R1#show ip route

This command will give a detail about known route. Router will not forward packet if route is not shown here for that packet. Router's routing decision is made by this routing table.

R1#show controllers serial 0/0/0

Most common use of this command is to find out whether the port is DCE end or DTE. If the port is DCE end then clock rate and bandwidth command will require. As you can see in output that port is DCE.

R1#show ip protocols

Use this command to know about running routing protocols.

How to configure a new router or a switch.

Show ip int brief : Ip address, Interface is up or down

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

Show version: Hardware & software information.

Show flash : To check the **IOS** File in flash memory.

```
Router#show flash:

System flash directory:
File  Length   Name/status
  3   33591768 c1900-universalk9-mz.SPA.151-4.M4.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
```

To change the **hostname**:

Router>enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#**hostname Delhi-Gw1**
Delhi-Gw1(config)#

To check the current configuration:

Delhi-Gw1#**show running-config** (Ram)

To check the Startup configuration:

Delhi-Gw1#**show startup-config** (NVRAM)

To save the configuration:

Delhi-Gw1#**write**
Building configuration...
[OK]

To reload the Router:

Delhi -Gw1#**reload**
Proceed with reload? [confirm]

To check the routing table:

Delhi -Gw1#**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, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
       ia - IS-IS inter area, * - candidate default, U - per-user static ro
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
C       10.1.3.0/24 is directly connected, FastEthernet0/1
S       10.1.0.0/16 [1/0] via 10.1.3.1
C       10.1.4.0/24 is directly connected, FastEthernet0/0
S       10.200.1.1/32 [1/0] via 10.1.3.1
S       10.200.1.4/32 [1/0] via 10.1.4.1
```

Note: To select the best path, router makes a routing table.

To Check the interfaces/ports status and Ip address.

```
Pune-Gw1#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES NVRAM  administratively down down
GigabitEthernet0/1     unassigned      YES NVRAM  administratively down down
Vlan1                  unassigned      YES NVRAM  administratively down down
Pune-Gw1#
```

Router has two ports Gig0/0 and Gig0/1

LAB#1 : Connect two different Networks.

1) **All The Lan Should Be In Diffrenet Networks (Should Not Repeat The Same Net)**

2) **Router Ethernet And The Pc's --> Same Networks**

3) **Routers Ports Facing Each Other --> Same Networks**

4) **All The Interfaces Of The Router --> Different Network**

Router>enable
Router#configure terminal

Router(config)#**interface fastEthernet 0/1**
Router(config-if)#**ip address 172.16.0.2 255.255.0.0**
Router(config-if)#**no shutdown**
Router(config-if)#**end**

Show ip interface brief: Interface IP address and status
Show ip route : Its shows the routing table.

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        172.16.0.1      YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#
Router#
Router#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

C    172.16.0.0/16 is directly connected, FastEthernet0/1
```

Error : IF you will try to assign the same network on another interface.
Router(config)#interface fa0/0
Router(config-if)#ip address 172.16.0.1 255.255.0.0
% 172.16.0.0 overlaps with FastEthernet0/1

Assign always a different network on different interface.
Router(config)#interface fa0/0
Router(config-if)#ip address 172.17.0.1 255.255.0.0
Router(config-if)#no shutdown

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        172.17.0.1      YES manual up                    up
FastEthernet0/1        172.16.0.1      YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#
Router#
Router#
Router#
Router#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

C    172.16.0.0/16 is directly connected, FastEthernet0/1
C    172.17.0.0/16 is directly connected, FastEthernet0/0
```

In short, router has learned both the networks from both the interfaces.

Now, both the routers can communicate between each other.

Assign IP in all the computers.

Router Gateway and Lan Network Should be in same network.

Ping Results,

ROUTING

Routing

- Forwarding of packets from one network to another network choosing the best path from the routing table.
- Routing table consist of only the best routes for every destinations.

Types of Routing

1. Static Routing

2. Default Routing

3. Dynamic Routing

Static Routing

- It is configured by Administrator manually.
- Mandatory need of Destination Network ID
- It is Secure & fast
- Used for Small organizations with a network of 10-15 Routers.

Disadvantages :-

- Used for small network.
- Everything to manually
- Network change effect complete n/W

Configuring Static Route

```
Router(config)# ip route <Destination Network ID>
                         <Destination Subnet Mask>
                         <Next-hop IP address >
```

Or

```
Router(config)# ip route <Destination Network ID>
                         <Destination Subnet Mask>
                   <Exit interface type><interface number>
```

Lab 2 # Configuring Static Route

Delhi 192.168.1.0 - Nwid 192.168.1.127 - Broadcast Id	Mumbai 192.168.1.128 - Nwid 192.168.1.255 - Broadcast Id
Delhi conf t hostname delhi int fa0/0 ip address 192.168.1.1 255.255.255.128 no shutdown int fa4/0 ip address 205.1.1.1 255.255.255.0 no shutdown	Mumbai conf t hostname Mumbai int fa0/0 ip address 192.168.1.200 255.255.255.128 no shutdown int fa4/0 ip address 205.1.1.2 255.255.255.0 no shutdown

ip route 192.168.1.128 255.255.255.128 205.1.1.2	**ip route 192.168.1.0 255.255.255.128 205.1.1.1**

Loopback Interfaces

- Loopback interfaces are internal interfaces and treated like other interfaces
  - Loopback interfaces are never shutdown
- Loopback interfaces are useful when you need an interface that will never go down

Default Routes

- Manually adding the single route for all the destination. Default route is used when destination is unknown
- Last preferred route in the routing table
- When there is no entry for the destination network in a routing table, the router will forward the packet to its default router.
- Default routes help in reducing the size of your routing table.

Configuring Default Route

Router(config)# ip route <Destination Network ID> <Destination Subnet Mask>
<Next-hop IP address >

Or

Router(config)# ip route <Destination Network ID> <Destination Subnet Mask>
<Exit interface type><interface number>

Lab 3 # Default Routing

A loopback interface is a **logical**, **virtual** interface in a Cisco Router. A loopback interface is not a physical interface like Fast Ethernet interface or Gigabit Ethernet interface. A loopback interface has many uses.

To make a LAB Internet Router – we make loopbacks on router

You can make as many loopbacks :

The **Loopback Range :**
Router(config)#interface loopback ?
<0-2147483647> Loopback interface number

Jio conf terminal int fa4/0	Dell-delhi-gw1 conf terminal hostname dell-delhi-gw1

ip address 203.1.1.1 255.255.255.0 no shutdown **int loopback 0** ip address **172.217.166.14** 255.255.255.0 description google.com **int loopback 1** ip address **31.13.79.35** 255.0.0.0 description facebook.com **int loopback 2** ip address **104.244.42.193** 255.0.0.0 description twitter.com int loopback 3 ip address 13.13.13.13 255.0.0.0 description nwkings.com **Static Route for Dell company** Jio(config)#ip route 192.168.1.0 255.255.255.0 203.1.1.2	int fa4/0 ip address 203.1.1.2 255.255.255.0 no shutdown int fa0/0 ip address 192.168.1.1 255.255.255.0 no shutdown **Default route** dell-delhi-gw1(config)#ip route 0.0.0.0 0.0.0.0 203.1.1.1

dell-delhi-gw1
203.1.1.2
192.168.1.1
Fa0
192.168.1.2
Ping statistics for 13.13.13.13:
Packets: Sent = 4, Received = 4, Lost = 0 (0%
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
C:\>
C:\>
Ping Successfull
C:\>ping 172.217.166.14
Pinging 172.217.166.14 with 32 bytes of data:
Reply from 172.217.166.14: bytes=32 time=1ms TTL=25
Reply from 172.217.166.14: bytes=32 time<1ms TTL=25
Reply from 172.217.166.14: bytes=32 time<1ms TTL=25
Reply from 172.217.166.14: bytes=32 time=1ms TTL=25
Ping statistics for 172.217.166.14:
Packets: Sent = 4, Received = 4, Lost = 0 (0%
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>

Troubleshooting commands:

Router # show ip interface Brief

1) Serial is up , line protocol is up (connectivity is fine)

2) Serial is administratively down, line protocol is down
(No Shutdown has to be given on the local router serial interface)

3) Serial is up, line protocol is down
(Encapsulation mismatch or clock rate has to be given on dce)

4) Serial is down, line protocol is down
(Serial interface on the remote router has to be configured)

Dynamic Routing

Advantages of Dynamic over static :

- There is no need to know the destination networks.
- Need to advertise the directly connected networks.
- Updates the topology changes dynamically.
- Administrative work is reduced
- Used for large organizations.
- Neighbor routers exchange routing information and build the routing table automatically.

Types of Dynamic Routing Protocols

Routing Protocol Classification

IGP	EGP
• Interior Gateway Protocol • Routing protocols used within an autonomous system • All routers will be routing within the same Autonomous boundary • RIP, IGRP, EIGRP, OSPF, IS-IS	• Exterior Gateway Protocol • Routing protocol used between different autonomous systems • Routers in different AS need an EGP • Border Gateway Protocol is extensively used as EGP

- IGPs operate within an autonomous system

– EGPs connect different autonomous systems

- Distance Vector Protocol
- Link State Protocol
- Hybrid Protocol

Distance Vector Protocol	Link State Protocol	Hybrid Protocol
• Works with Bellman Ford algorithm • Periodic updates • Classful routing protocol • Full Routing tables are exchanged • Updates are through broadcast • Example: RIP 1, RIP 2,	• Works with Dijkstra algorithm • Link state updates • Classless routing protocol • Missing routes are exchanged • Updates are through multicast • Example : OSPF, IS-IS	• Also called as Advance Distance vector Protocol • Works with DUAL algorithm • Link state updates • Classless routing protocol • Missing routes are exchanged • Updates are through

IGRP		multicast • Example : EIGRP

Administrative Distance

- Rating of the Trustworthiness of a routing information source.
- The Number is between 0 and 255
- The higher the value, the lower the trust.
- Default administrative distances are as follows :
    - Directly Connected = 0
    - Static Route = 1
    - IGRP = 100
    - OSPF = 110
    - RIP = 120
    - EIGRP = 90/170

Routing Information Protocol v1

- Open Standard Protocol
- Classful routing protocol
- Updates are broadcasted via 255.255.255.255
- Administrative distance is 120
- Metric : Hop count
  Max Hop counts : 15 Max routers : 16
- Load Balancing of 4 equal paths
- Used for small organizations
- Exchange entire routing table for every 30 seconds

Rip Timers

- Update timer : 30 sec

  - Time between consecutive updates
- Invalid timer : 180 sec
  - Time a router waits to hear updates
  - The route is marked unreachable if there is no update during this interval.
- Flush timer : 240 sec
  - Time before the invalid route is purged from the routing table

RIP Version 2

- Classless routing protocol
- Supports VLSM
- Auto summary can be done on every router
- Supports authentication
- Trigger updates
- Uses multicast address 224.0.0.9.

Advantages of RIP

  - Easy to configure
  - No design constraints
  - No complexity
  - Less overhead

Disadvantage of RIP

  - Bandwidth utilization is very high as broadcast for every 30 second
  - Works only on hop count
  - Not scalable as hop count is only 15
  - Slow convergence

Configuring RIP 1

```
Router(config)# router rip
Router(config-router)# network <Network ID>
```

Configuring RIP 2

Router(config)# router rip
Router(config-router)# network <Network ID>
Router(config-router)# version 2

LAB Practical RIP

conf t	conf t	conf t	conf t

hostname R1 int f0/0 ip address 192.168.12.1 255.255.255.0 no shutdown int f0/1 ip address 192.168.13.1 255.255.255.0 no shutdown int loopback 0 ip address 1.1.1.1 255.255.255.255 int loopback 1 ip address 4.1.1.1 255.255.255.255 **Router rip** **version 2** **no auto-summary** **network 192.168.12.0** **network 192.168.13.0** **network 1.1.1.1**	hostname R2 int f0/0 ip address 192.168.12.2 255.255.255.0 no shutdown int f0/1 ip address 192.168.24.2 255.255.255.0 no shutdown int loopback 0 ip address 2.2.2.2 255.255.255.255 **Router rip** **version 2** **no auto-summary** **network 192.168.12.0** **network 192.168.24.0** **network 2.2.2.2**	hostname R3 int f0/0 ip address 192.168.34.3 255.255.255.0 no shutdown int f0/1 ip address 192.168.13.3 255.255.255.0 no shutdown int loopback 0 ip address 3.3.3.3 255.255.255.255 **Router rip** **version 2** **no auto-summary** **network 192.168.34.0** **network 192.168.13.0** **network 3.3.3.3**	hostname R4 int f0/0 ip address 192.168.34.4 255.255.255.0 no shutdown int f0/1 ip address 192.168.24.4 255.255.255.0 no shutdown int loopback 0 ip address 4.4.4.4 255.255.255.255 **Router rip** **version 2** **no auto-summary** **network 192.168.34.0** **network 192.168.24.0** **network 4.4.4.4**

Autonomous System Number

- A unique number identifying the Routing domain of the routers.
- An autonomous system is a collection of networks under a common administrative domain
- Ranges from 1- 65535
- Public – 1 – 64512 Private – 64513 – 65535

EIGRP - Enhanced Interior Gateway Routing Protocol

- Cisco proprietary protocol
- Classless routing protocol
- Includes all features of IGRP
- Metric (32 bit) : Composite Metric (BW + Delay + load + MTU + reliability)
- Administrative distance is 90
- Updates are through Multicast (224.0.0.10)
- Max Hop count is 255 (100 by default)
- Supports IP, IPX and Apple Talk protocols
- Hello packets are sent every 5 seconds
- Convergence rate is fast
- First released in 1994 with IOS version 9.21.
- Support VLSM and CIDR
- It uses DUAL (diffusion update algorithm)
- Summarization can be done on every router
- Supports equal and unequal cost load balancing

- It maintains three tables
  - Neighbor table
  - Topology table
  - Routing table

Disadvantages of EIGRP

- Works only on Cisco Routers

Configuring EIGRP

```
Router(config)# router eigrp <as no>
Router(config-router)# network <Network ID>
```

OSPF - Open Shortest path first

- OSPF stand for Open Shortest path first
- Standard protocol
- It's a link state protocol
- It uses SPF (shortest path first) or dijkistra algorithm
- Unlimited hop count
- Metric is cost (cost=10 ^8/B.W.)
- Administrative distance is 110
- It is a classless routing protocol
- It supports VLSM and CIDR
- It supports only equal cost load balancing
- Introduces the concept of Area's to ease management and control traffic

- Provides hierarchical network design with multiple different areas
- Must have one area called as area 0
- All the areas must connect to area 0
- Scales better than Distance Vector Routing protocols.
- Supports Authentication
- Updates are sent through multicast address 224.0.0.5
- Faster convergence.
- Sends Hello packet every 10 seconds
- Trigger/Incremental updates
- Router's send only changes in updates and not the entire routing tables in periodic updates

OSPF PACKET ENCAPSULATION

- **VERSION**: OSPF VERSION
- **TYPE**: TYPE 1/TYPE 2/TYPE 3/TYPE 4/TYPE 5
- **PACKET LENGTH**: LENGTH OF PROTOCOL IN BYTES
- ROUTER ID: ROUTER IDENTIFIER IN OSPF
- AREA ID : REPRESENTS THE AREA OF INTERFACE OPERATION
- CHECKSUM : USED TO CHECK THE PACKET INTEGRITY
- AuTYPE: TYPE OF OSPF PACKET AUTHENTICATION: 0/1/2
- AUTHENTICATION: USED FOR AUTHENTICATION

OSPF PACKET TYPES

- TYPE 1: HELLO PACKETS : USED TO DISCOVER NEIGHBORS
- TYPE 2: DATABASE DESCRIPTION : SYNCHRONIZATION BETWEEN ROUTERS
- TYPE 3: LINK STATE REQUEST :LIST OF ALL MISSING LSAs
- TYPE 4: LINK STATE UPDATE: RESPONSE TO LSR
- TYPE 5: LINK STATE ACKNOWLEDGEMENT: ACKNOWLEDGES THE RECEIPT OF LSAs

1. Hello
2. Database Description (DBD)
3. Link-State Request (LSR)
4. Link-State Update (LSU)
5. Link-State Acknowledgment (LSAck)

Router ID

The highest IP address of the active physical interface of the router is Router ID.
If logical interface is configured, the highest IP address of the logical interface is Router ID

Router Types

In OSPF depending upon the network design and configuration we have different types of routers.

Internal Routers are routers whose interfaces all belong to the same area. These routers have a single Link State Database.

Area Border Routers (ABR) It connects one or more areas to the backbone area and has at least one interface that belongs to the backbone, Backbone Router Area 0 routers

Autonomous System Boundary Router (ASBR) Router participating in OSPF and other protocols (like RIP, EIGRP and BGP)

OSPF maintains three tables :

1) Neighbor Table Neighbor table contains information about the directly connected ospf neighbors forming adjacency.

2) Database table Database table contains information about the entire view of the topology with respect to each router.

3) Routing information Table Routing table contains information about the best path calculated by the shortest path first algorithm in the database table.

Advantages of OSPF

- Open standard
- No hop count limitations
- Loop free
- Faster convergence

Disadvantages

- Consume more CPU resources
- Support only equal cost balancing
- Support only IP protocol don't work on IPX and APPLE Talk
- Summarization only on ASBR and ABR

Wild Card Mask

- Tells the router which addressing bits must match in the address of the ACL statement.
- It's the inverse of the subnet mask, hence is also called as Inverse mask.
- A bit value of 0 indicates MUST MATCH (Check Bits)
- A bit value of 1 indicates IGNORE (Ignore Bits)
- Wild Card Mask for a Host will be always 0.0.0.0
- A wild card mask can be calculated using the formula :

Global Subnet Mask

– **Customized Subnet Mask**

Wild Card Mask

E.g.

```
          255.255.255.255
     –    255.255.255.240
  ---------------------
          0.  0.   0.  15
```

Configuring OSPF

Router(config)# router ospf <pid>

Router(config-router)# network <Network ID> <wildcard mask> area <area id>

OSPF STATES

DR/BDR

- DR : DESIGNATED ROUTER BDR: BACKUP DESIGNATED ROUTER
- DR SERVE AS COLLECTION POINTS OF LINK STATE ADVERTISEMENTS
- BDR BACKS UP THE DR
- GREATLY REDUCES OSPF TRAFFIC

- DR/BDR Selection
- First Router to Initialize
- Router with Highest Priority ID
- Router with Highest Router ID
- Set the Highest Router ID
- Highest Loopback Interface IP Address
- Highest Interface IP Address

Designated Router Operation

- Designated Router (DR)
  - Listens for LSAs on all designated routers multicast address of 224.0.0.6
  - Transmits network LSA to other routers on 224.0.0.5
  - Ensures that all routers on that network have the same synchronized LSBD
- Backup Designated Router (BDR)
  - Listens for LSAs via all designated routers multicast address of 224.0.0.6
  - Listens for network LSAs on 224.0.0.5
  - Ensures quick failover if the designated router is no longer reachable
- Other OSPF routers
  - Transmits LSAs to DR and BDR using 224.0.0.6
  - Listens for network LSAs on 224.0.0.5

Access Control List

- ACL is a set of rules which will allow or deny the specific traffic moving through the router
- It is a Layer 3 security which controls the flow of traffic from one router to another.
- It is also called as Packet Filtering Firewall.

Standard Access List	Extended Access List
• The access-list number range is 1 – 99 • Can block a Network, Host and Subnet • Two way communication is stopped • All services are blocked. • Implemented closest to the destination. • Filtering is done based on only source IP address	• The access-list number range is 100 – 199 • Can block a Network, Host, Subnet and Service • One way communication is stopped • Selected services can be blocked. • Implemented closest to the source. • Checks source, destination, protocol, port

	no

Terminology

- **Deny :** Blocking a Network/Host/Subnet/Service
- **Permit :** Allowing a Network/Host/Subnet/Service
- **Source Address :** The address of the PC from where the request starts.
- **Destination address :** The address of the PC where the request ends.
- **Inbound :** Traffic coming into the interface
- **Outbound** : Traffic going out of the interface

Rules of Access List

- All deny statements have to be given First
- There should be at least one Permit statement
- An implicit deny blocks all traffic by default when there is no match (an invisible statement).
- Can have one access-list per interface per direction. (i.e.) Two access-list per interface, one in inbound direction and one in outbound direction.
- Works in Sequential order
- Editing of access-lists is not possible (i.e) Selectively adding or removing access-list statements is not possible.

Creation of Standard Access List

```
Router(config)# access-list  <acl no>  <permit/deny>  <source address>
                             <source WCM>
```

Implementation of Standard Access List

Router(config)# interface <interface type> <interface no>

Router(config-if)# ip access-group <number> <out/in>

To Verify :

Router# show access-list
Router# show access-list <no>

Creation of Extended Access List

Router(config)# access-list <acl no> <permit/deny> <protocol>
<source address> <source wildcard mask>
<destination address> < destination wildcard mask> <operator> <service>

Implementation of Extended Access List

Router(config)#interface <interface type> <interface no>
Router(config-if)#ip access-group <number> <out/in>

LAB Standard ACL

r1	r2
conf t int fa0/1 ip address 192.168.1.1 255.255.255.0 no shutdown int fa0/0 ip address 1.0.0.1 255.255.255.252 no shutdown router eigrp 1 network 192.168.1.0 network 1.0.0.0 no auto-summary	conf t int fa0/1 ip address 172.16.1.1 255.255.0.0 no shutdown int fa0/0 ip address 1.0.0.2 255.255.255.252 no shutdown router eigrp 1 network 172.16.1.0 network 1.0.0.0 no auto-summary

Standard ACL Objective:
Block **PC 192.168.1.2** to reach **Server 172.16.1.2**
Block PC **192.168.1.3** to reach whole network **172.16.0.0**

Make access list
R2(config)#access-list 1 deny host 192.168.1.2
R2(config)#access-list 1 deny host 192.168.1.3
R2(config)#access-list 1 permit any

Block 192.168.1.2
Block 192.168.1.3
Permit any – **Very important**
Explict deny

Apply access list
R2(config)#int fa0/1
R2(config-if)#ip access-group 1 out

```
R2#show access-lists
Standard IP access list 1
    10 deny host 192.168.1.2 (256 match(es))
    20 deny host 192.168.1.3
    30 permit any (5 match(es))
```

Hence, traffic is blocked.

Block Telnet Access for all networks on R1 except **192.168.1.0**

Configure telnet on R1

```
line vty 0 4
password cisco
login
exit
enable password cisco
```

Make ACL

R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255

Permit 192.168.1.0 Explict deny

Apply Inside Line vty – always apply inbound

R1(config)#line vty 0 4
R1(config-line)#access-class 1 in

Operators : eq (equal to)
neq (not equal to)
lt (less than)
gt (greater than)

Named Access List

- Access-lists are identified using Names rather than Numbers.
- Names are Case-Sensitive
- No limitation of Numbers here.
- One Main Advantage is Editing of ACL is Possible (i.e) Removing a specific statement from the ACL is possible.

(IOS version 11.2 or later allows Named ACL)

Creation of Standard Named Access List

```
Router(config)# ip access-list standard <name>
Router(config-std-nacl)# <permit/deny> <source address> <source wildcard mask>
```

Implementation of Standard Named Access List

```
Router(config)#interface <interface type><interface no>
Router(config-if)#ip access-group <name> <out/in>
```

Creation of Extended Named Access List

```
Router(config)# ip access-list extended <name>
Router(config-ext-nacl)# <permit/deny> <protocol>  <source address>
                         <source wildcard mask> <destination address>
                         < destination wildcard mask> <operator> <service>
```

LAB Extended ACL

Objective :

Block HTTP - 80 **PC 192.168.1.2 > Nwkings 192.168.2.2** **PC 192.168.1.3 > Cisco 192.168.2.3**
R1(config)#access-list 100 deny tcp host 192.168.1.2 host 192.168.2.2 eq 80 R1(config)#access-list 100 deny tcp host 192.168.1.3 host 192.168.2.3 eq 80

Block FTP - 21 Network 192.168.1.0 > Nwkings 192.168.2.2
R1(config)#access-list 100 deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 21

Block ICMP Network 192.168.1.0 > Cisco 192.168.2.3
R1(config)#access-list 100 deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.3 echo R1(config)#access-list 100 deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.3 echo-reply **Rest Permit all** R1(config)#access-list 100 permit IP any any

Apply to interface inbound
R1(config)#int fa0/1n
R1(config-if)#ip access-group 100 in

Named ACL – You can edit Named ACL
R1(config)#ip access-list extended ABC
R1(config-ext-nacl)#deny tcp host 192.168.1.2 host 192.168.2.2 eq 80
R1(config-ext-nacl)#deny tcp host 192.168.1.3 host 192.168.2.3 eq 80
R1(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 21
R1(config-ext-nacl)#deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.3 echo
R1(config-ext-nacl)#deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.3 echo-reply
R1(config-ext-nacl)#permit IP any any
R1(config-ext-nacl)#end

R1(config)#int fa0/1
R1(config-if)#ip access-group ABC in

R1#show access-lists
Extended IP access list ABC
10 deny tcp host 192.168.1.2 host 192.168.2.2 eq www
20 deny tcp host 192.168.1.3 host 192.168.2.3 eq www
30 deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq ftp
40 deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.3 echo
50 deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.3 echo-reply

60 permit ip any any

If you want to remove 50 sequence number - echo reply statement

```
R1(config)#ip access-list extended ABC
R1(config-ext-nacl)#no 50 deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.3 echo-repl
R1#show access-lists
Extended IP access list ABC
    10 deny tcp host 192.168.1.2 host 192.168.2.2 eq www
    20 deny tcp host 192.168.1.3 host 192.168.2.3 eq www
    30 deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq ftp
    40 deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.3 echo
    60 permit ip any any
```

Router Password Breaking

1. console connnection
2. open hypertrm
3. power on the device

4. press CTRL+SHIFT+BREAK to enter in to rommon mode

5. on modular routers

```
Rommon1> confreg 0x2142
Rommon1> reset
```

OR

on fixed routers

```
>o/r 0x2142
>i
```

6. now the router boots without asking passwords

```
>enable
#copy start run
```

7. change the passwords

8. (config)#config-register 0x2102
(config)#exit

```
# write
# reload
```

Dhcp :- automatically assign the ip addresss to host

```
router(config)# ip dhcp excluded-address 192.168.1.50   (if you  don't want  to assign ip's range )
router(config-dhcp)#  ip dhcp pool cisco
router(config-dhcp)# network 192.168.1.0 255.255.255.0
router(config-dgcp)# default-router 192.168.1.1
router(config-dgcp)#exit
```

APIPA:-

Short for **A**utomatic **P**rivate **IP A**ddressing, a feature of later Windows operating systems. With APIPA, DHCP clients can automatically self-configure an IP address and subnet mask when a DHCP server isn't available. When a DHCP client boots up, it first looks for a DHCP server in order to obtain an IP address and subnet mask. If the client is unable to find the information, it uses APIPA to automatically configure itself with an IP address from a range that has been reserved especially for Microsoft. The IP address range is 169.254.0.1 through 169.254.255.254. The client also configures itself with a default class B subnet mask of 255.255.0.0. A client uses the self-configured IP address until a DHCP server becomes available.

The APIPA service also checks regularly for the presence of a DHCP server (every five minutes, according to Microsoft). If it detects a DHCP server on the network, APIPA stops, and the DHCP server replaces the APIPA networking addresses with dynamically assigned addresses.
APIPA is meant for nonrouted small business environments, usually less than 25 clients.

NAT :- NETWORK ADDRESS TRANSLATION

Natting means "Translation of private IP address into public IP address ".
In order to communicate with internet we must have public IP address.

Address translation was originally developed to solve two problems:

1. to handle a shortage of IPv4 addresses
2. hide network addressing schemes.

Small companies typically get their public IP addresses directly from their ISPs, which have a limited number.
Large companies can sometimes get their public IP addresses from a registration authority, such as the Internet Assigned Numbers Authority (IANA).

Common devices that can perform address translation include firewalls, routers, and servers. Typically address translation is done at the perimeter of the network by either a firewall (more commonly) or a router.

There are certain addresses in each class of IP address that are reserved for Private Networks. These addresses are called private addresses.

Class A 10.0.0.0 to 10.255.255.255
Class B 172.16.0.0 to 172.31.255.255
Class C 192.168.0.0 to 192.168.255.255

- **Inside Local Addresses –** An IP address assigned to a host inside a network. This address is likely to be a RFC 1918 private address

- **Inside Global Address –** A legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP address to the outside world.

- **Outside Local Address -** The IP address of an outside host as it known to the hosts in the inside network.

- **Outside Global Address -** The IP address assigned to a host on the outside network. The owner of the host assigns this address.

Types of NAT:-

1. Dynamic NAT
2. Static NAT
3. PAT

Static NAT

- This type of NAT is designed to allow one-to-one mapping between local and global addresses.
- Keep in mind that the static version requires you to have one real Internet IP address for every host on your network..

Syntax:

(Config)# IP nat inside source static <private IP> <public IP>

Implementation :

(Config) # interface s0
(Config-if)# ip nat outside

(Config)# interface e0
(Config-if)# ip nat inside

Dynamic NAT

- This version gives you the ability to map an unregistered IP address to a registered IP address from out of a pool of registered IP addresses.
- You don't have to statically configure your router to map an inside to an outside address as you would using static NAT, but you do have to have enough real IP addresses for everyone who's going to be sending packets to and receiving them from the Internet.

Syntax :

(Config)# access-list < NO> permit <net.ID> <WCM>

(Config)#ip nat inside pool <name> <starting Pub IP><end Pub IP>
<netmask < mask>

(Config)# ip nat inside source list <Aclno> pool <name>

Implementation :

(Config) # interface s0
(Config-if)# ip nat outside

(Config)# interface e0
(Config-if)# ip nat inside

Dynamic NAT Overload (PAT)

- This is the most popular type of NAT configuration. Understand that overloading really is a form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address—many-to-one—by using different ports.

- It is also known as Port Address Translation (PAT), and by using PAT (NAT Overload), you get to have thousands of users connect to the Internet using only one real global IP address.

- NAT Overload is the real reason we haven't run out of valid IP address on the Internet

Syntax :

(Config)# access-list < NO> permit <net.ID> <WCM>

(Config)#ip nat inside pool <name> <starting Pub IP><end Pub IP> netmask
< mask>

(Config)# ip nat inside source list <Aclno> pool <name> **overload**

Implementation :

(Config) # interface s0
(Config-if)# ip nat outside
(Config)# interface e0

```
(Config-if)# ip nat inside
```

BASIC SWITCHING

Hub

- It is a Physical layer device (Layer 1)
- It is Dummy Device
- It works with 0's and 1's (Bits)
- It works with broadcasting
- It works with shared bandwidth
- It is has 1 Broadcast Domain and 1 Collision Domain
- Collisions are identified using Access Methods called CSMA/CD and CSMA/CA

Switch

- It is Datalink layer device (Layer 2)
- Its is An Intelligent device
- It works with Physical addresses (i.e. MAC addresses)
- It works with fixed bandwidth
- It works with Flooding and Unicast
- It has 1 Broadcast domain and Number of Collision domains depends upon the number of ports.
- It maintains a MAC address table

Broadcast Domain & Collision Domain

- **Broadcast Domain**
  Set of all devices that receive broadcast frames originating from any device within the set.
- **Collision domain**
  In Ethernet, the network area within which frames that have collided are propagated is called a collision domain.
- A collision domain is a network segment with two or more devices sharing the same bandwidth.

Broadcast Domains **Collision Domains**

Types of Switches

- **Manageable switches**
  On a Manageable switch, an IP address can be assigned and configurations can be made. It has a console port .

- **Unmanageable switches**
  On an Unmanageable switch, configurations cannot be made, an IP address cannot be assigned as there is no console port.

Cisco's Hierarchical Design Model

Cisco divided the Switches into 3 Layers

1. **Access Layer Switches**
   Switches Series : 1900 & 2900

2. **Distribution Layer Switches**
   Switches Series : 3000 & 5000

3. **Core Layer Switches**
   Switches Series : 7000, 8000 & 10,000

Access Layer Switch

Catalyst 1900

Catalyst 2900

Distribution Layer Switch

3550 switch

Core Layer Switches

Switching Mode

Three types of Switching Mode **:**

- **Store & Forward**
  - A Default switching method for distribution layer switches.
  - Latency : High
  - Error Checking : Yes
- **Fragment Free**
  - It is also referred to as Modified Cut-Through
  - A Default Switching method for access layer switches.
  - Latency : Medium
  - Error Checking : On 64 bytes of Frame
- **Cut through**
  - A Default switching method for the core layer switches
  - Latency : Low
  - Error Checking : No

Latency is the total time taken for a Frame to pass through the Switch. Latency depends on the switching mode and the hardware capabilities of the Switch.

Console Connectivity

- Connect a rollover cable to the Switch console port (RJ-45 connector).
- Connect the other end of the rollover cable to the RJ-45 to DB-9 adapter
- Attach the female DB-9 adapter to a PC Serial Port.
- Open emulation software on the PC.

Emulation Software

IN WINDOWS

- Start ⍰ Programs ⍰ Accessories ⍰ Communications ⍰ HyperTerminal ⍰ HyperTerminal.
- Give the Connection Name & Select Any Icon
- Select Serial (Com) Port where Switch is Connected.
- In Port Settings ⍰ Click on Restore Defaults

IN LINUX

- # minicom -s

INITIAL CONFIGURATION OF A SWITCH:

Connect one end of console cable to console port of switch and other end of cable to your computer's com port.
Now open Hyper terminal and power on the switch.

Would you like to enter into initial configuration dialog (yes/no): no

2950>en
2950#config terminal

TO assign telnet Password

2950(config) # line vty 0 4
2950(config-line) # login
2950(config-line) # password <password>

TO assign Console Password

2950(config) # line con 0
2950(config-line) # login
2950(config-line) # password <password>

TO assign Enable Password

2950(config) #enable secret < password>
2950(config) #enable password < password>
2950(config) #exit

switch# Show mac-address-table (to see the entries of the MAC table)
switch# Show interface status

To assign IP to a Switch

switch(config)# Interface Vlan 1
switch(config-if)# ip address <ip> <mask>
switch(config-if)# no shutdown

To assign Default Gateway to a Switch

switch(config)#ip default-gateway 192.168.20.1

ADVANCE SWTCHING

Spanning Tree Protocol

- Spanning Tree Protocol (STP) uses Spanning Tree Algorithm to avoid the Switching loops in layer-2 devices (bridges or switches).
- STP works when multiple switches are used with redundant links avoiding Broadcast Storms, Multiple Frame Copies & Database instability.
- First Developed By DEC
- STP is a open standard (IEEE 802.1D)
- STP is enabled by default on all Cisco Catalyst switches

STP Terminology

- **BPDU**
  - All switches exchange information through what is called as Bridge Protocol Data Units (BPDUs**)**
  - BPDUs contain a lot of information to help the switches determine the topology and any loops that result from that topology.
  - BPDUs are sent every 2 sec

- **Bridge ID**
  - Each switch has a unique identifier called a Bridge ID or Switch ID
  - Bridge ID = Priority + MAC address of the switch
  - When a switch advertises a BPDU , they place their switch id in these BPDUs**.**

- **Root Bridge**
  - The bridge with the Best (Lowest) ID.
  - Out of all the switches in the network , one is elected as a root bridge that becomes the focal point in the network.

- **Non-Root bridge**
  - All Switches other than the Root Bridge are Non-Root Bridges

- **Designated port**
  - Either a port On a root bridge or a port that has been determined as having the best (lower) cost.
  - A designated port will always in Forward Mode
- **Root port**
  - The link directly connected to the root bridge, or the shortest path to the root bridge.
  - Priority and Alternatives if Config occurred.
    - Root port with the least cost (Speed) connecting to the root bridge.
    - The bridge with the Best (Lowest) Switch ID.
    - Lowest Physical Port Number.
  - Only One root port will Be in Bridge or switch.
- **Non Designated port**
  - All the Port or ports which are blocked by STP to avoid switching loop.
  - A Non Designated port Will Always in Blocked Mode.

STP port states

- Blocking - 20 Sec Or No Limits.
- Listening - 15 Sec.
- Learning - 15 Sec.
- Forwarding - No Limits.
- Disable - No Limits.

Switch - Port States

- **Blocking :** Won't forward frames; listens to BPDUs. All ports are in blocking state by default when the switch is powered up.
- **Listening** : Listens to BPDUs to make sure no loops occur on the network before passing data frames.
- **Learning** : Learns MAC addresses and builds a filter table but does not forward frames**.**
- **Forwarding** : Sends and receives all data on the bridged port.

Typical Costs of Different Ethernet Networks

Speed New	IEEE Cost	Original IEEE Cost
10Gbps	2	1
1Gbps	4	1
100Mbps	19	10
10Mbps	100	100

Virtual LAN

- A Layer 2 Security
- Divides a Single Broadcast domain into Multiple Broadcast domains.
- By default all ports of the switch are in VLAN1 . This VLAN1 is known as Administrative VLAN or Management VLAN

- VLAN can be created from 2 – 1001
- Can be Configured on a Manageable switch only
- 2 Types of VLAN Configuration
  - Static VLAN
  - Dynamic VLAN

- By default, routers allow broadcasts only within the originating network, but switches forward broadcasts to all segments.
- The reason it's called a flat network is because it's one Broadcast domain , not because its design is physically flat. (Flat Network Structure)

- Network adds, moves, and changes are achieved by configuring a port into the appropriate VLAN.
- A group of users needing high security can be put into a VLAN so that no users outside of the VLAN can communicate with them.
- As a logical grouping of users by function, VLANs can be considered independent from their physical or geographic locations.
- VLANs can enhance network security.
- VLANs increase the number of broadcast domains while decreasing their size.

Static VLAN

- Static VLAN's are based on port numbers
- Need to manually assign a port on a switch to a VLAN
- Also called Port-Based VLANs
- It can be a member of single VLAN and not multiple VLAN's

Static VLAN On 2900 series Switch

- **Creation of VLAN:-**

```
Switch # vlan database
Switch(vlan)# vlan <vlan id> name <vlan name>
Switch(vlan)# exit
```

- **Assigning port in VLAN:-**

```
Switch#config t
Switch(config)# int fastethernet <int no>
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan <vlan id>
```

- **Verify using**

  Switch # show vlan

VLAN Creation – 1900 Series

Switch(config)# vlan <no>
Switch(config-Vlan)# name <name>
Switch(config-Vlan)# Exit

Assigning ports in Vlan

Switch(config)# interface <interface type> <interface no.>
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access Vlan <no>

The range command (Assigning multiple ports at same time)

The range command, you can use on switches to help you configure multiple ports at the same time

Switch(config)# int range fastEthernet 0/1 - 12

Dynamic VLAN

- Dynamic VLAN's are based on the MAC address of a PC
- Switch automatically assigns the port to a VLAN
- Each port can be a member of multiple VLAN's
- For Dynamic VLAN configuration, a software called VMPS(VLAN Membership Policy Server) is needed

Types of links/ports

- **Access links**
  - This type of link is only part of one VLAN, and it's referred to as the native VLAN of the port.

- Any device attached to an access link is unaware of a VLAN membership—the device just assumes it's part of a broadcast domain, but it has no understanding of the physical network.
- Switches remove any VLAN information from the frame before it's sent to an accesslink device.

- **Trunk links**
  - Trunks can carry multiple VLANs.
  - A trunk link is a 100- or 1000Mbps point-to-point link between two switches, between a switch and router, or between a switch and server. These carry the traffic of multiple VLANs—from1 to 1005 at a time.
  - Trunking allows you to make a single port part of multiple VLANs at the same time.

VLAN Identification Methods (Frame Tagging)

- VLAN identification is what switches use to keep track of all those frames
- It's how switches identify which frames belong to which VLANs, and there's more than one trunking method :
  - **Inter-Switch Link (ISL)**

– **IEEE 802.1Q**

ISL	IEEE 802.1Q
• It's a Cisco proprietary • It adds 30 bytes to the header • All VLAN traffic is tagged • It works with Ethernet, Token ring, FDDI • Frame is not modified	• Created by the IEEE as a standard method or frame tagging. • Open standard, we can use on different vendors switches. • It works only on Ethernet • Unlike ISL , 802.1q does not encapsulate the frame . It modifies the existing Ethernet frame to include the VLAN ID • Only 4 Byte tag will add to original frame.

Trunking Configuration – 2900 Series

```
Switch(config)#  interface <interface type> <interface no.>
Switch(config-if)#  switchport trunk allowed vlan {<vlan no.>|all}
Switch(config-if)#  switchport trunk encapsulation dot1q/ISL
```

VTP - Virtual LAN Trunking Protocol

- VTP is a CISCO proprietary protocol
- used to share the VLAN configurations with multiple switches and to maintain consistency throughout that network.
- Information will be passed only if switches connected with FastEthernet or higher ports.
- VTP allows an administrator to add, delete, and rename VLANs-information that is then propagated to all other switches in the VTP domain.
- **Note:** Switches Should be configure with same Domain. Domain are not Case sensitive.

VTP Modes

VTP Mode are of three types :

- **Server Mode**
  - A Switch configured in Server mode can Add , Modify and Delete VLAN's
  - A Default VTP mode for all switches

- **Client Mode**
  - A switch configured in Client mode cannot Add , Modify and Delete its VLAN configurations
  - Doesn't store its VLAN configuration information in the NVRAM. Instead , learns it from the server every time it boots up

- **Transparent Mode**
  - A switch configured in a Transparent Mode can Add , Modify and Delete VLAN configurations.
  - Changes in one transparent switch will not affect any other switch.

Benefits of VLAN Trunking Protocol (VTP)

- Consistent VLAN configuration across all switches in the network
- Accurate tracking and monitoring of VLANs
- Dynamic reporting of added VLANs to all switches in the VTP domain
- Plug-and-Play VLAN adding

VTP Pruning

- Preserves bandwidth by configuring it to reduce the amount of broadcasts, multicasts, and unicast packets.
- VTP pruning only sends broadcasts to trunk links that truly must have the information.
- Enabling pruning on a VTP server, enables it for the entire domain.
- By default, VLANs 2 through 1005 are pruning-eligible, but VLAN 1 can never prune because it's an administrative VLAN.

VTP Configuration – 2950 Series

```
Switch(config)# VTP Domain <Name>
Switch(config)# VTP Password <password>
Switch(config)# VTP Mode <server/client/transparent>
Switch(config)# VTP pruning
```

VTP Configuration – 1900 Series

```
Switch#VLAN Database
Switch(VLAN)# VTP Domain <Name>
Switch(VLAN)# VTP Password <password>
Switch(VLAN)# VTP Mode <server/client/transparent>
Switch(VLAN)# VTP pruning
```

SSH :- To remotely access the device , it creates encrypted session

Step 1. As a requirement to generate an RSA general-usage key you'll need to change the hostname to a hostname other then the default "Router" hostname. In this case, you can use R1 as shown below;

Router>enable
Password:
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1

R1(config)#ip domain-name ccies.in

R1(config)#crypto key generate rsa modulus 2048

R1(config)#
. Configure the transport input protocol on the VTY lines to accept only SSH by executing the transport input ssh under the vty line configuration mode as shown below;

R1(config)#line vty 0 4
R1(config-line)#transport input ssh

Step 6. Verify your SSH configuration by using the Cisco IOS SSH client and SSH to the routers loopback interface 10.1.1.1

R1(config-line)#end
R1#ssh -l john 10.1.1.1

Password:

R1#ssh -l john 10.1.1.1

Password:

R1#show ssh

```
Connection Version Mode Encryption  Hmac        State              Username
0          1.99    IN   aes128-cbc  hmac-sha1    Session started      john
0          1.99    OUT  aes128-cbc  hmac-sha1    Session started      john
%No SSHv1 server connections running.
```

IPv6

IPv6 has 128 bit addresses and has a much larger address space than 32-bit IPv4 which offered us a bit more than 4 billion addresses. Keep in mind every additional bit doubles the number of IP addresses…so we go from 4 billion to 8 billion, 16,32,64, etc. Keep doubling until you reach 128 bit. With 128 bits this is the largest value you can create:

340,282,366,920,938,463,463,374,607,431,768,211,456

The main reason to start using IPv6 is that we need more addresses but it also offers some new features:

- **No Broadcast traffic**: No broadcasts anymore. We use multicast in IPV6. It means protocols like ARP are replaced with other solutions.
- **Stateless Autoconfiguration:** Its like a "mini DHCP server". Routers running IPv6 are able to advertise the IPv6 prefix and gateway address to hosts so that they can automatically configure themselves and get access outside of their own network.
- **Address Renumbering**: Renumbering static IPv4 addresses on your network is a pain. If you use stateless autoconfiguration for IPv6 then you can easily swap the current prefix with another one.
- **Mobility**: IPv6 has built-in support for mobile devices. Hosts will be able to move from one network to another and keep their current IPv6 address.
- **No NAT / PAT**: we have so much IPv6 addresses that we don't need NAT or PAT anymore, every device in your network can have a public IPv6 address.

- **IPsec**: IPv6 has native support for IPsec, you don't have to use it but it's built-in the protocol.
- **Improved header**: the IPv6 header is simpler and doesn't require checksums. It also has a flow label that is used to quickly see if certain packets belong to the same flow or not.
- **Migration Tools**: IPv4 and IPv6 are **not compatible** so we need migration tools. There are multiple tunneling techniques that we can use to transport IPv6 over IPv4 networks (or the other way around). Running IPv4 and IPv6 simultaneously is called "dual stack".

IPv6 Header

Bit 0 4 8 12 16 20 24 28
0
64
128
192
256
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address
Ethernet Header
IPv6 Header
TCP Header
Application data
Ethernet Trailer
Ethernet frame

IPv6 looks different than IPv4 but there are some similarities.
For example we have unicast addresses and we still have a "public" and "private" range. We use different names for these but the idea is the same. One of the differences is that IPv6 has some additional unicast address types.

- **IPV4 released in 1980 , 32 bit** therefore support 2^{32} (4,294,967,296) addresses
- **IPV6 released in 1999 , 128 bit** (approximately 340 undecillion or 3.4×10^{38}) addresses

Unicast

Unicast IPv6 addresses are similar to unicast IPv4 addresses. These are meant to configure on one interface so that you can send and receive IPv6 packets. There are a number of different unicast address types that we'll discuss here.

Global Unicast

The global unicast IPv6 addresses are similar to IPv4 public addresses. These addresses can be used on the Internet. The big difference with IPv4 is that we have so much address space that we can use global unicast addresses on any device in the network.

Unique Local

Unique local addresses work like the IPv4 private addresses. You can use these addresses on your own network if you don't intend to connect to the Internet or if you plan to use IPv6 NAT. The advantage of unique local addresses is that you don't need to register at an authority to get some address space. The FC00::/7 prefix is reserved for unique local addresses

Shortening IPv6 Addresses

2001:0000:0000:0012:0000:0000:1234:56ab

2001:0db8:3c4d:0012:**0000**:**0000**:1234:56ab **8 groups Each Group = 16 bit or 4 hexadecimal**

Not easy to remember:- we have 2 rules

1. Eliminate the consecutive zero's:- represent with double :: (colon's)

2001:0db8:3c4d:0012:**0000**:**0000**:1234:56ab

2001:0db8:3c4d:0012::1234:56ab _____ also _____2001::

We can remove the one or more blocks of zeros by replacing them with double colons, But you can only replace one contiguous block of zeros in an address

2001:0000:0000:0012:**0000**:**0000**:1234:56ab
2001:0000:0000:0012::1234:56ab
2001:0:0:12::1234:56ab

2 Eliminate the Leading zeros

2001:db8:3c4d:12::1234:56ab _____ remove the starting zero's
2001:0000:0000:0012:**0000**:**0000**:1234:56ab
2001:0000:0000:0012::1234:56ab
2001:0:0:12::1234:56ab

If address has four blocks of zeros .
Example:

2001:0000:0000:0012:0000:0000:1234:56ab

2001:0:0:12:**0 : 0**:1234:56ab

- 2001**:: 12 :: 1234: 56ab (wrong)**
- 2001**::**12**:0:0**:1234:56ab (correct)

ADDRESS TYPES:

1) **UNICAST**	**2) Multicast**
1) **Global unicast** : public , routable2001:: 2001:1234:12:121:fe12::1/64 2) **Site local** : private routable FC, FD FC00:1234:12:121:fe12::1/ FD00:1234:12:121:fe12::1/ **3) Link local :`** address which the device assings automatically (nonroutable) **FE80::45E:34:fc::0**	Just like class D **FF**

To summarize these rules:

- An entire string of zeros can be removed, you can only do this once.
- 4 zeros can be removed, leaving only a single zero.
- Leading zeros can be removed.

How to find IPv6 Prefix

What part from this IPv6 address is the prefix and what part identifies the host?

Since we use a /64 it means that the first 64 bits are the prefix. Each hexadecimal character represents 4 binary bits so that means that this part is the prefix:

2001:1234:5678:1234:0000:0000:0000:0000/64 is a valid prefix but we can shorten it :- **2001:1234:5678:1234::/64**

2001:1234:abcd:5678:9877:3322:5541:aabb/53

IPv6 EUI-64 explained

EUI-64 (Extended Unique Identifier) is a method we can use to automatically configure IPv6 host addresses. An IPv6 device will use the MAC address of its interface to generate a unique 64-bit interface ID. However, a MAC address is 48 bit and the interface ID is 64 bit. What are we going to do with the missing bits?

1. We take the MAC address and split it into two pieces.

2. We insert "FFFE" in between the two pieces so that we have a 64 bit value.

3. We invert the 7th bit of the interface ID.

Static Routing IPV6

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ipv6 enable
```

Static Route

```
(config)#ipv6 route 2001::2/128 fastEthernet 0/0 FE80::CE0A:22FF:FED5:0
```

```
R2(config)#interface fastEthernet 0/0
R2(config-if)#ipv6 enable
R2(config-if)#exit

R2(config)#interface loopback 0
R2(config-if)#ipv6 address 2001::2/128
```

RIPNG

R1(config)#**ipv6 unicast-routing** R1(config)#interface loopback 0 R1(config-if)#ipv6 address 2001::1/128 R1(config)#interface fastEthernet 0/0 R1(config-if)#ipv6 enable **R1#show ipv6 interface brief** FastEthernet0/0 [up/up] FE80::CE09:18FF:FE0E:0 Loopback0 [up/up] FE80::CE09:18FF:FE0E:0 2001::1 R1(config)#**ipv6 router rip RIPNGTEST** R1(config-rtr)#exit R1(config)#interface fastEthernet 0/0 R1(config-if)#ipv6 rip RIPNGTEST enable R1(config-if)#exit R1(config)#interface loopback 0 R1(config-if)#ipv6 rip RIPNGTEST enable	R2(config)#**ipv6 unicast-routing** R2(config)#interface loopback 0 R2(config-if)#ipv6 address 2001::2/128 R2(config)#interface fastEthernet 0/0 R2(config-if)#ipv6 enable **R2#show ipv6 interface brief** FastEthernet0/0 [up/up] FE80::CE0A:18FF:FE0E:0 Loopback0 [up/up] FE80::CE0A:18FF:FE0E:0 2001::2 R2(config)#**ipv6 router rip RIPNGTEST** R2(config-rtr)#exit R2(config)#interface fastEthernet 0/0 R2(config-if)#ipv6 rip RIPNGTEST enable R2(config-if)#exit R2(config)#interface loopback 0 R2(config-if)#ipv6 rip RIPNGTEST enable
EIGRP	

R1(config)#ipv6 router eigrp 1 R1(config-rtr)#router-id 1.1.1.1 R1(config-rtr)#no shutdown R1(config)#interface GigabitEthernet 0/1 R1(config-if)#ipv6 eigrp 1 R1(config)#interface loopback 0 R1(config-if)#ipv6 eigrp 1	R2(config)#ipv6 router eigrp 1 R2(config-rtr)#router-id 2.2.2.2 R2(config-rtr)#no shutdown R2(config)#interface GigabitEthernet 0/1 R2(config-if)#ipv6 eigrp 1 R2(config)#interface loopback 0 R2(config-if)#ipv6 eigrp 1

Wi-Fi

Wi-Fi: - wireless fidelity

1. Half duplex, connectivity issues (not reliable)
2. Shared signal
3. CSMA/CA

1. **AD-HOC**: - pc to pc also known as ibss (independent basic service set)
2. **BSS**: - basic service set: - one access point
3 **ESS**:-extended service set more than one access point

802.11a:- 25 mbps, can reach up to 54 mbps, indoor range is 100 feet , 5ghz frequency
802.11b:- 6.5 mbps, can reach up to 11 mbps, indoor range is 100 feet, 2.4 ghz frequency

802.11g: - 25 mbps, can reach up to 54 mbps, indoor range is 100 feet, 2.4 ghz
802.11n:- 200 mbps, can reach up to 540 mbps , indoor range is 160 feet , work on both 2.4 ghz frequency and 5 ghz

SSID: - service set identifier (name of your wlan) case sensitive 32 characters

Authentication

Wep:-wired equivalent privacy
1. clear text , easy to guess, one way authentication

Wap: - Wi-Fi protected access
Two way authentication
Strong encryption (tkip :- temporal key integrity protocol)

WAN :- wide area network

A WAN is a data communications network that operates beyond the geographic scope of a LAN.

1. Wireless
2. Satellite
3. Cables: - 1. Leased lines ---- dedicated lines

   2. Circuit switching

   3 . Packet switching

Option	Description	Advantages	Disadvantages	Sample protocols used
Leased line	Point-to-Point connection between two computers or Local Area Networks (LANs).	Most secure	Expensive	PPP, HDLC, SDLC, HNAS
Circuit switching	A dedicated circuit path is created between endpoints. Best example is dialup connections.	Less expensive	Call setup	PPP, ISDN
Packet switching	Devices transport packets via a shared single point-to-point or point-to-multipoint link across a carrier interwork. Variable length packets are transmitted over permanent virtual circuits (PVCs) or switched virtual		Shared media across link	X.25, Frame Relay

WAN Protocols

Leased Lines uses two types of WAN encapsulation protocols:

1) High Data Link Protocol (HDLC)
2) Point to Point Protocol (PPP)

HDLC	PPP
• Higher level data link Control protocol	• Point to Point Protocol

• Cisco Proprietary Layer 2 WAN Protocol • Doesn't support Authentication • Doesn't support Compression and error correction	• Standard Layer 2 WAN Protocol • Supports Authentication • Support error correction

PPP supports two authentication protocols:

1) PAP (Password Authentication Protocol)
2) CHAP (Challenge Handshake Authentication Protocol)

PAP (Password Authentication Protocol)

- PAP provides a simple method for a remote node to establish its identity using a two-way handshake.
- PAP is done only upon initial link establishment
- PAP is not a strong authentication protocol.
- Passwords are sent across the link in clear text.

CHAP (Challenge Handshake Authentication Protocol)

- After the PPP link establishment phase is complete, the local router sends a unique “challenge” message to the remote node.
- The remote node responds with a value (MD5)
- The local router checks the response against its own calculation of the expected hash value.
- If the values match, the authentication is acknowledged. Otherwise, the connection is terminated immediately.

Configuration of HDLC:-

```
Router(config)# interface serial 0/0
Router(config-if)# encapsulation hdlc
```

Configuration of PPP:

```
Router# configure terminal
Router(config)# interface serial 0/0
Router(config-if)# encapsulation ppp
```

Enable CHAP Authentication

```
Router(config)#   interface serial 0/0
Router(config-if)#  encapsulation ppp
Router(config-if)#  ppp authentication chap
```

Enable PAP Authentication:-

```
Router(config)#  interface serial 0/0
Router(config-if)#  encapsulation ppp
Router(config-if)#  ppp authentication pap
```

DCE	DTE
• Data Communication Equipment • Generate clocking (i.e. Speed). • Example of DCE device in Leased line setup : V.35 & G.703 Modem & Exchange (Modem & MUX) • Example of DCE device in Dial up setup : Dialup Modem	• Data Termination Equipment • Accept clocking (i.e. Speed). • Example of DTE device in Leased line setup : Router • Example of DTE device in Dial up setup : Computer

Router # show controllers (s0/0 or s0/1)
(To know whether the cable connected to the serial interface is DCE or DTE)

V.35 Modem
E0
10.1.1.1/8
V.35
Cable
V.35
Cable
E0
20.1.1.1/8
2 pair of
Copper Wire
LAN – 10.0.0.0/8
HYDERABAD
OFFICE
LAN – 20.0.0.0/8
KSA
OFFICE
EXCHANGE
G.703
Modem
G.703
Modem
HYDERABAD
MUX
KSA
MUX
Fiber Optic Cable

V.35 Back to Back Cable

Frame relay:-

* Cost effective
* shared bandwidth
* **NBMA** :-NOn broadcast multi acess-- which not broadcast neither multicast

CIR :- commited information rate :- guraanted bandwith given by isp
PVC :- permanent virtual circuit :- billing upon rent

DLCI :- data link connection indentifier
    * they are locally significant

(inverse arp) which converts DLCI TO IP

LMI:- local managment interface
* the language speaks between router and us
* signalling protocol
* Quality of transmission

VPN: - Virtual Private Network

* Cheaper connections
* Available anywhere where internet is available
* Heavily encrypted and secure
* HIGH OVERHEAD (disadvantage)