RS-100

CCNA

CISCO CERTIFIED NETWORK ASSOCIATE

NAGABABU

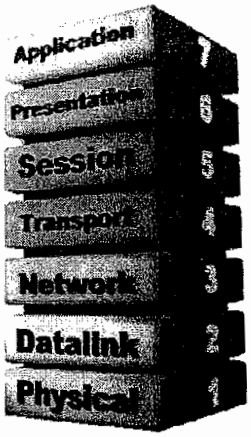
STUDENTNAME

BASIC

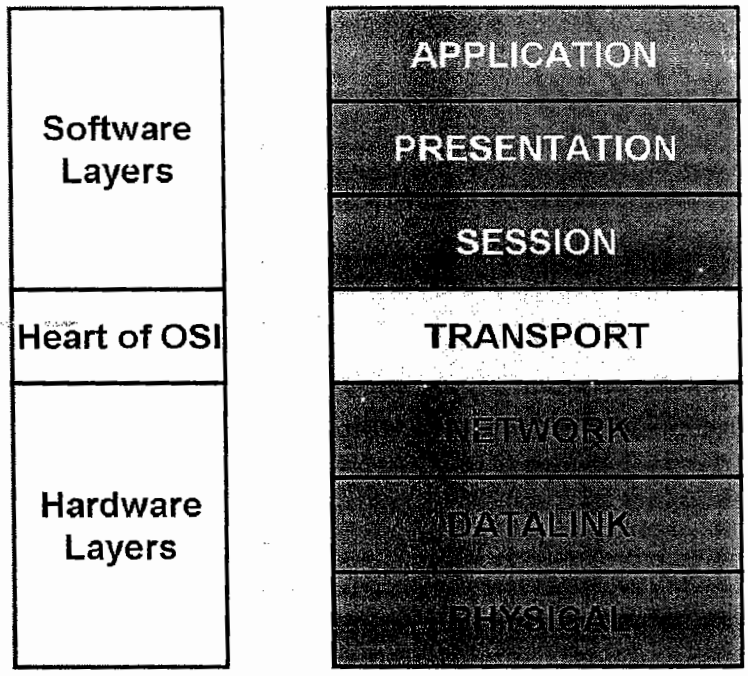
NETWORKING

OSI Layers

- OSI Layers explain the complete network communication process
- It explains how the systems interact with each other
- OSI Layered architecture was designed by ISO & ITU-T
  - ISO - International standards Organization
  - ITU-T - International Telecommunication Union - Telecom standard sector



NAGABABU



Application, Presentation, Session Layers are called **Software Layers**
Transport Layer is called **Heart of OSI**
Network, Data link, Physical layers are called **Hardware Layers**

7. Application Layer

Functions:

- It provides user interface
- It gives network services to the user
- Identification of port No depends on service

Protocols:

DNS, DHCP, HTTP, FTP, SMTP, Telnet

6. Presentation Layer

Functions:

- It converts data from standard format to machine format
- Encryption and decryption
- Compression and decompression

Protocols:

ASCII, EBCDIC,
GIF, TIFF, BMP, JPEG
MPEG, AVI, WAV

- ASCII - American standard code for Information Interchange
- EBCDIC - Extended binary coded decimal interchange code
- JPEG - Joint picture expert group
- TIFF - Tagged Image file format
- GIF - Graphical Image Format
- BMP - Bitmap Image
- MPEG - Motion Picture expert group
- AVI - Audio video Interleave
- WAV - Windows audio video

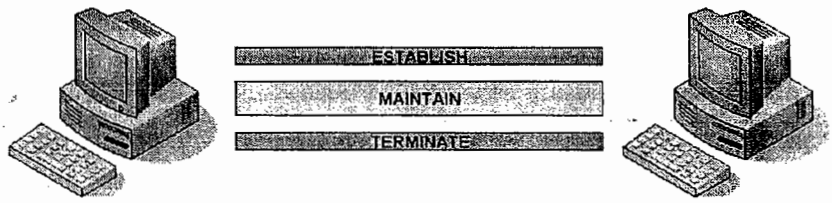
5. Session Layer

Functions:

- It establish, maintains and terminates a logical session

Protocols:

NFS - Network file system
RPC - Remote Procedure call



CISCO

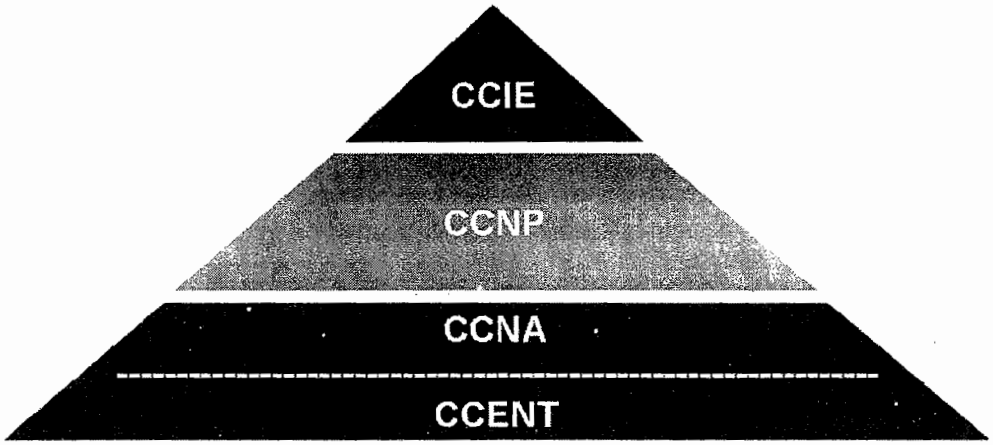
- Network devices manufacturing company
- Started in 1984
- Leader in network devices production
- Started by a couple came from Sanfran**cisco**

Cisco Network Academy Program

3 Levels are there in Cisco Network Academy Program

- Associate Level - CCNA, CCDA
- Professional Level - CCNP, CCDP, CCSP, CCVP
- Expert Level - CCIE

Cisco Certifications Path

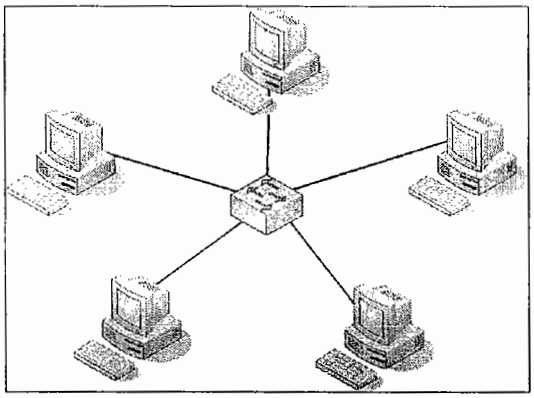


What is the role of CCNA ?

- LAN Management
  - Local Area Network management
- WAN Management
  - Wide Area Network management

What is a Network?

Group of two or more computers/devices connected together.



What is the purpose of Network?

To share the resources like printers, servers, folders etc

What is the advantage of Network?

Easy access to resources. Time save & Security

What are the requirements of Network?

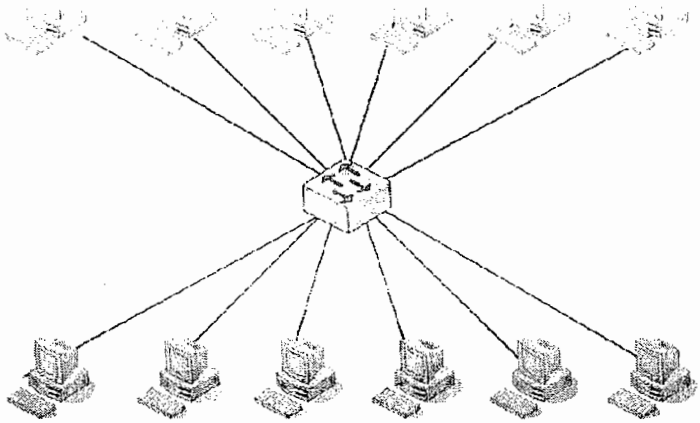
- Computers with Operating system
- NIC(Network interface card for every computer)
- Cables and RJ-45 connectors
- Centralized device (Hub/Switch)
- IP Address for every computer(Internet Protocol Address)

Types of Networks

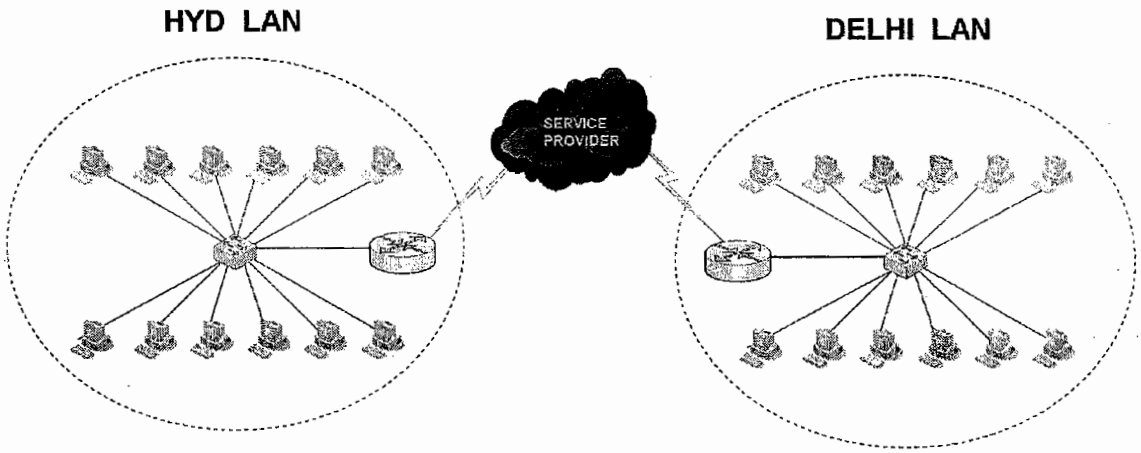
LAN & WAN

- LAN
  - Local Area Network
  - Network devices connected in a limited geographical area
  - Within room, within building, within campus
  - No service provide existence
  - Computers are connected to switches
- WAN
  - Wide Area Network
  - Network devices are in distant areas
  - In different cities, countries
  - Service provider existence
  - Networks are connected with the help of routers

LAN



WAN



What is Network topology?

It is layout of a network
It defines the physical structure of a network

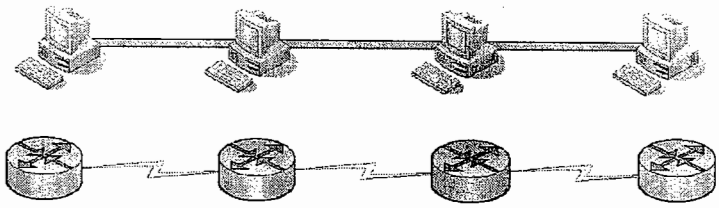
- Physical topology
  - Physical structure of a network
- Logical topology
  - Logical behavior of a network

NAGABABU

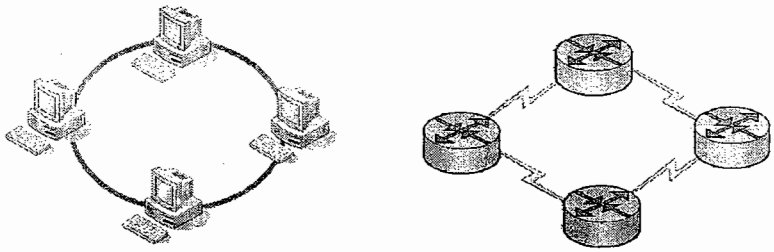
Topology types

- Bus topology
- Ring topology
- Mesh topology
- Star topology
- Extended star/tree topology

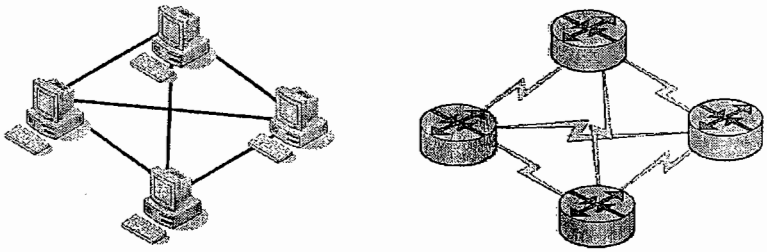
Bus Topology



Ring Topology

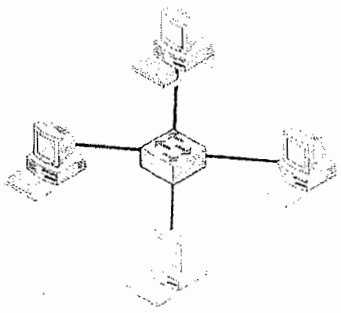


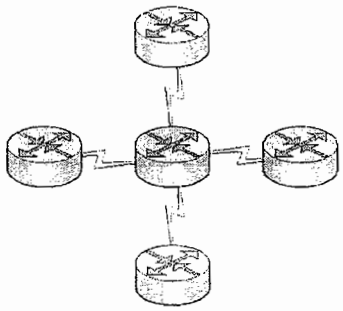
Mesh Topology



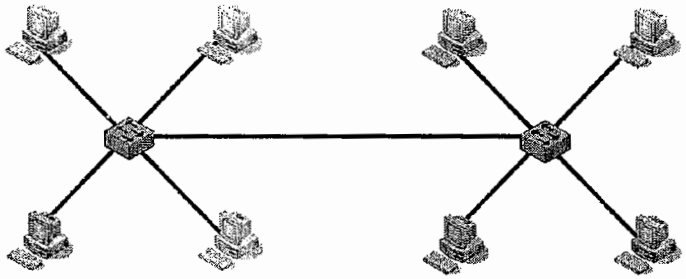
NAGABABU

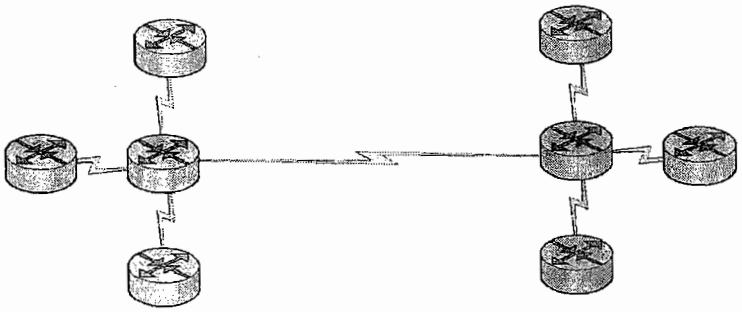
Star Topology





Extended Star Topology





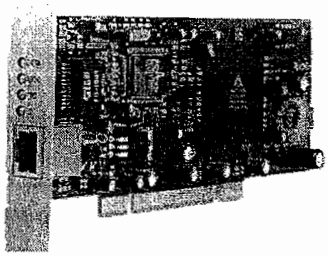
NAGABABU

NETWORK DEVICES

NIC
Hub
Switch
Router

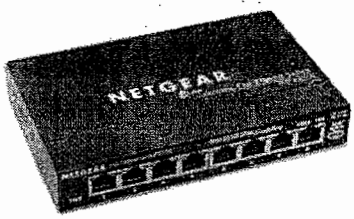
NIC:

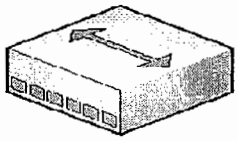
Network interface card - Gives the network services to the computer. Every computer must have NIC to communicate with other computers.



Hub:

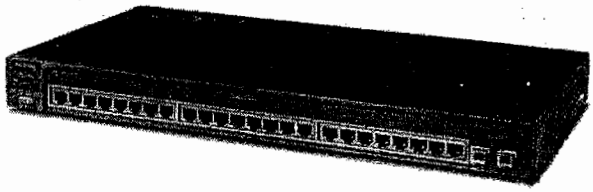
Used to group the devices (Regenerates the signal). called as Multi port repeater

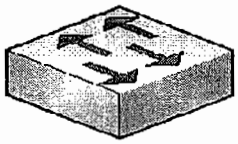




Switch:

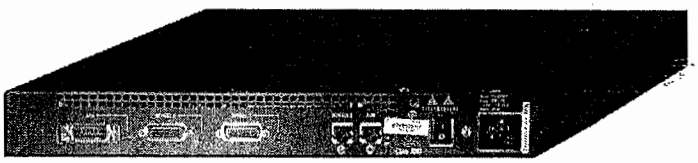
Used to group the devices (Forwards data). Faster than Hub

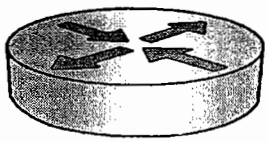




Router:

Used to communicate between different networks





NUMBERING SYSTEMS

1. Binary Numbering System
2. Octal Numbering System
3. Decimal Numbering System
4. Hexadecimal Numbering System

1. Binary Numbering System: Base 2
   Digits: **0 1**
2. Octal Numbering System: Base 8
   Digits: **0 1 2 3 4 5 6 7**
3. Decimal Numbering System: Base 10
   Digits: **0 1 2 3 4 5 6 7 8 9**
4. Hexadecimal Numbering System: Base 16
   Digits: **0 1 2 3 4 5 6 7 8 9 A B C D E F**

CONVERSIONS

Decimal to Binary:

2 | 78	
2 | 39	- 0
2 | 19	- 1
2 | 9	- 1
2 | 4	- 1
2 | 2	- 0
	1 - 0

78 = 1001110

Binary to Decimal:

$2^6\,2^5\,2^4\,2^3\,2^2\,2^1\,2^0$

1101011

$2^6+2^5+0+2^3+0+2^1+2^0$

$= 64+32+8+2+1$

$= 107$

2 power chart:

$2^0=1$
$2^1=2$
$2^2=4$
$2^3=8$
$2^4=16$
$2^5=32$
$2^6=64$
$2^7=128$
$2^8=256$

$2^9=512$
$2^{10}=1024$
$2^{11}=2048$
$2^{12}=4096$
$2^{13}=8192$
$2^{14}=16384$
$2^{15}=32768$
$2^{16}=65536$
$2^{32}=4294967296$

Hexadecimal-decimal-binary equivalents:

HEXADECIMAL	DECIMAL	BINARY
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

Binary - Decimal equivalents:

BINARY	DECIMAL
00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

NIC - Addresses

Two addresses are associated with NIC
Physical Address
Logical Address

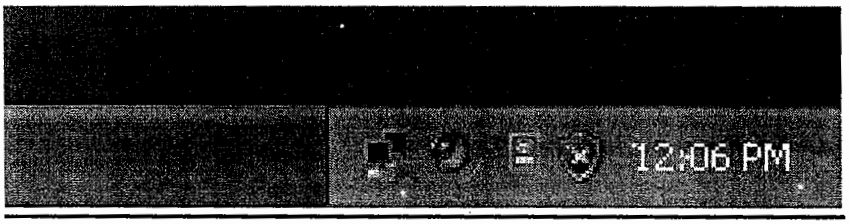
Physical Address	Logical Address
MAC-media access control	IP- Internet Protocol
L2 Address	L3 Address
Permanent-BIA	Logical (Can be changed)
48 Bit	32 Bit
Hexadecimal notation	Dotted decimal Notation
Example: 01-5C-D9-6B-03-2E	Example: 192.168.6.1

MAC address:

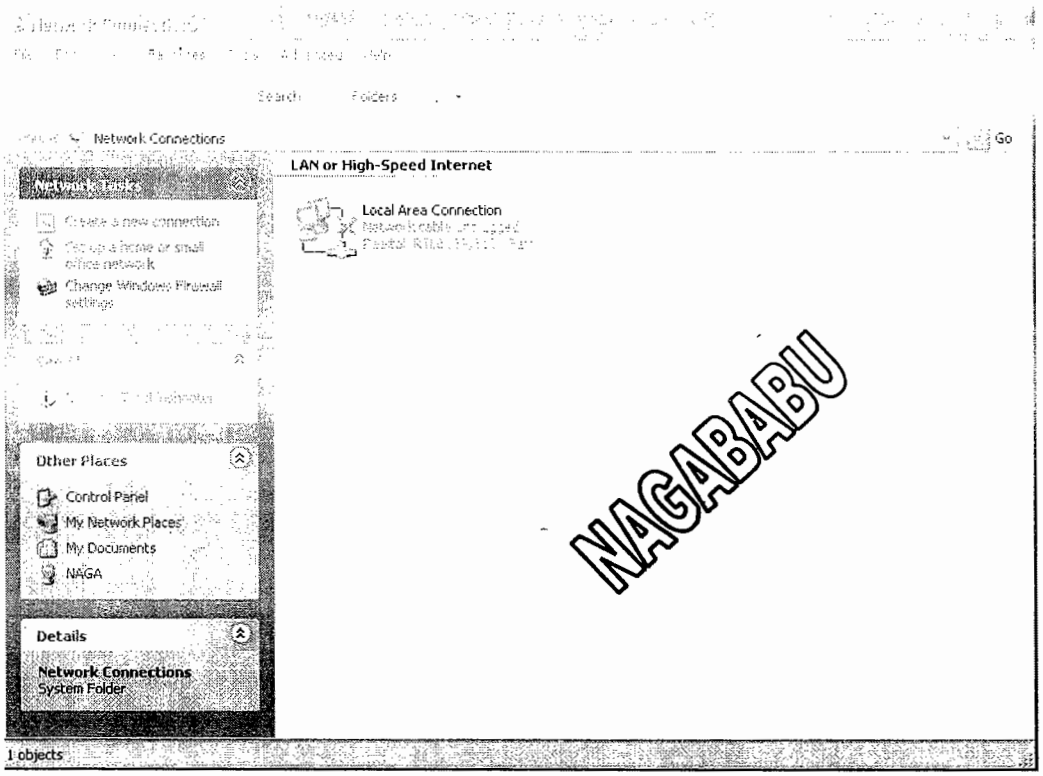
01-5E-7F-20-3A-9D
00000001 01011111 01111111 00100000 00111010 10011101

The first 24 Bits group in the MAC address is called **OUI** - Organizationally Unique Identifier
OUI is manufacturer identification

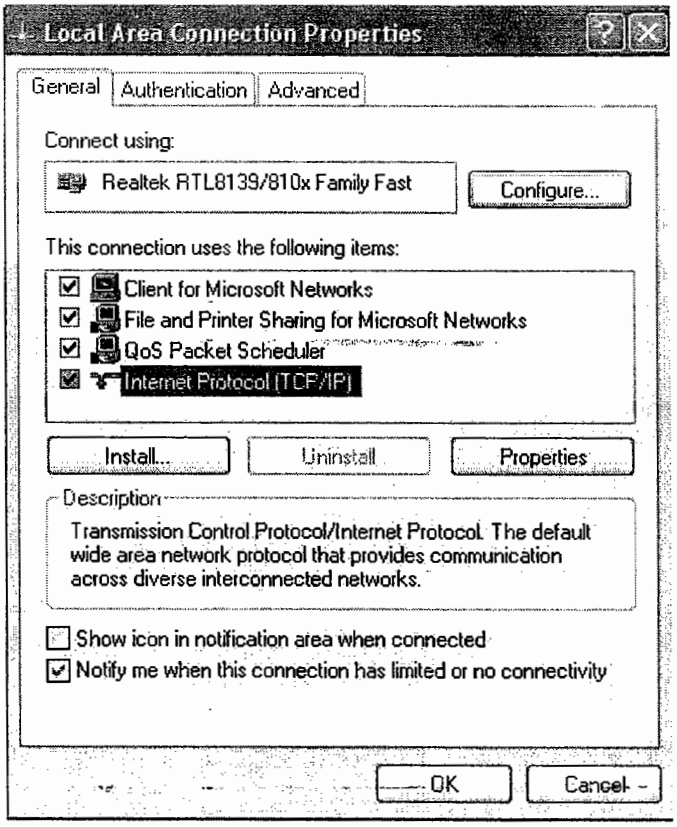
How to assign IP address



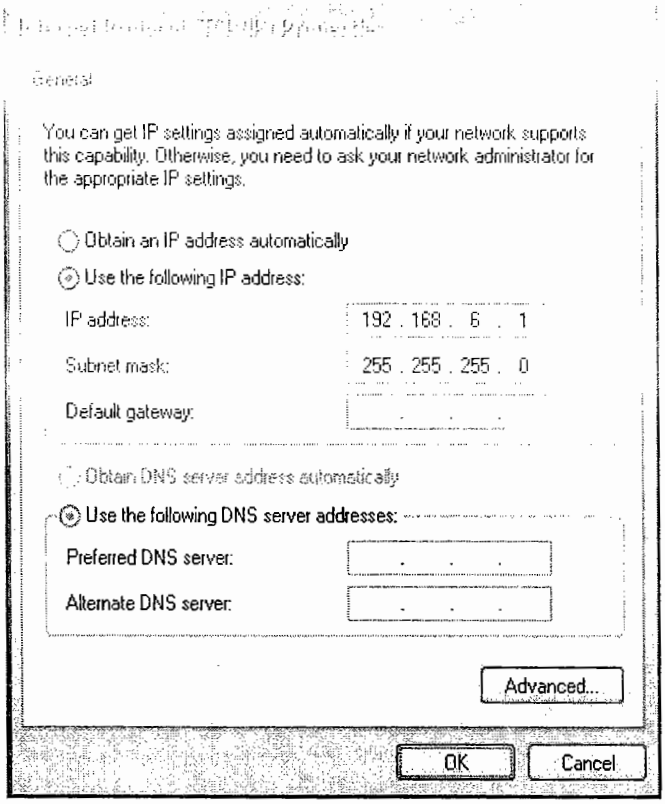
Double click on the Network icon and follow the steps below



Double click on Local Area connection



Select Internet Protocol (TCP/IP), then properties tab



Enter IP address, Subnet Mask. Click OK

How to check assigned IP address

Open Command prompt (Start+ Run + cmd). Use the following commands.

ipconfig - To check the IP address
ipconfig /all - To check complete IP information
getmac - To check MAC address
systeminfo - To check complete system information
ping 192.168.6.1 - To check the connectivity

CABLES

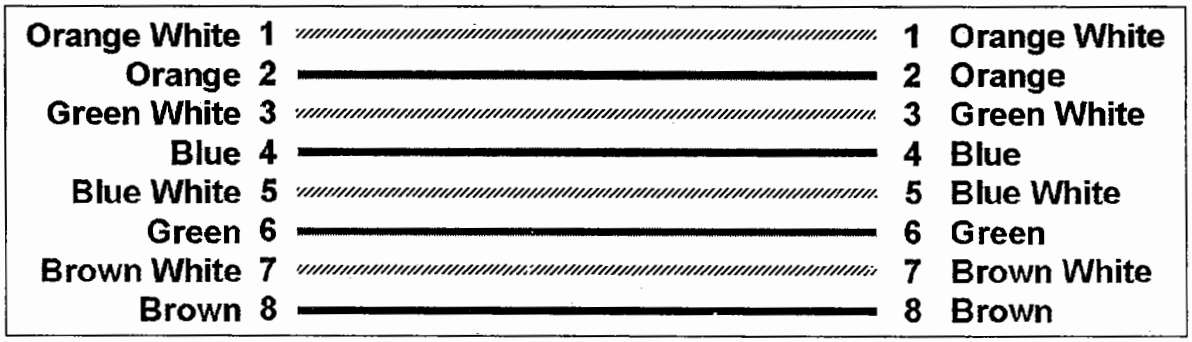
3 Types of Ethernet cable are used in Networking

- Straight through Cable
- Cross Over Cable
- Roll over cable

Straight through cable, Cross over Cables are used for data transfer
Rollover cable is used to configure routers / switches / network devices

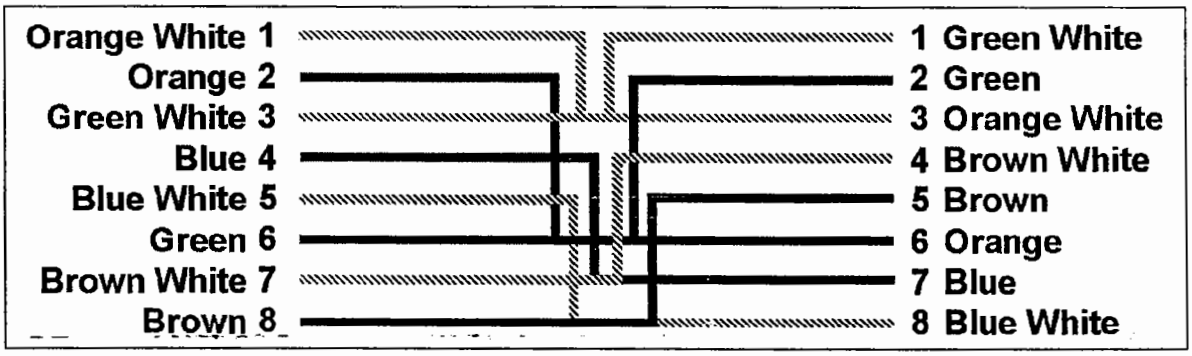
Straight through Cable:

- Straight cable is used to connect dissimilar devices
- switch - router, switch - pc , hub - pc



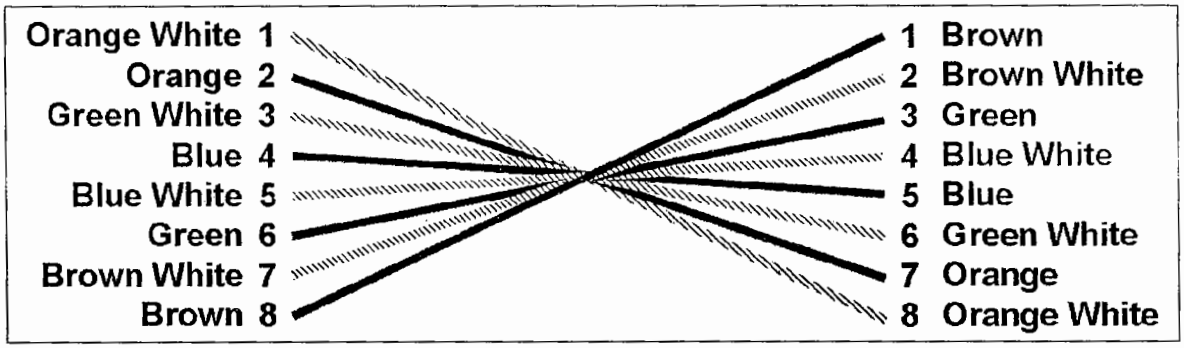
Cross Over Cable:

- Cross over cable is used to connect similar devices
- switch - switch, router - pc , switch - hub , pc - pc

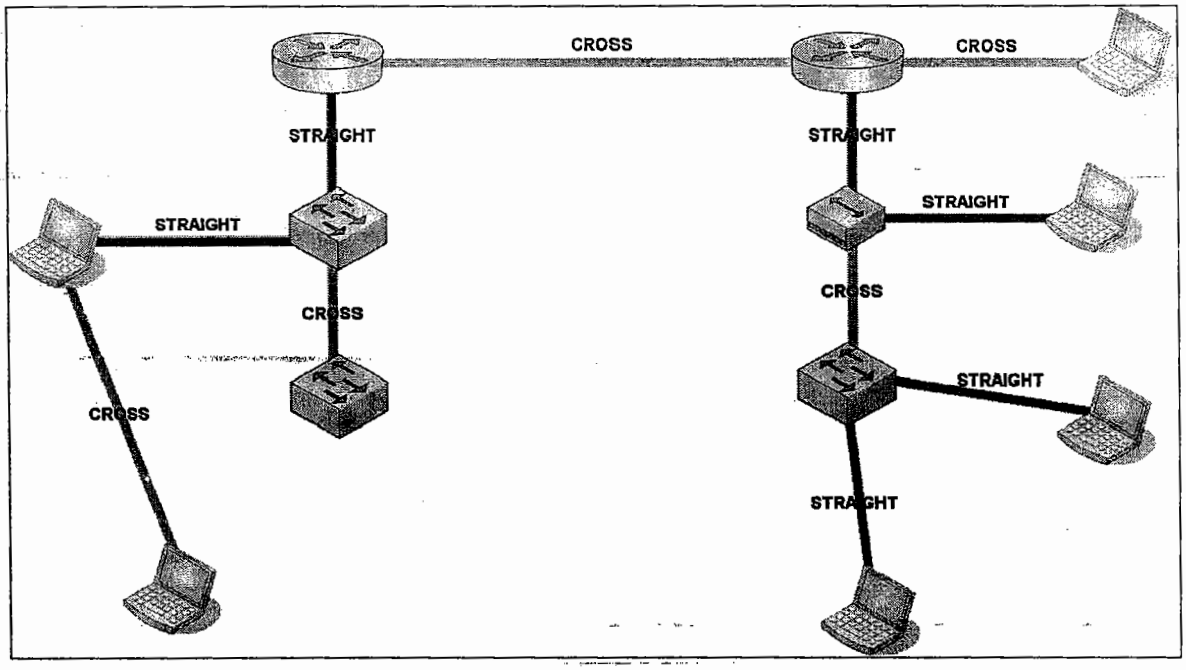


Roll Over Cable:

- Rollover cable is used to configure router/switch/Network devices
- Switch / router console connectivity



Ethernet Cable connections



NAGABABU

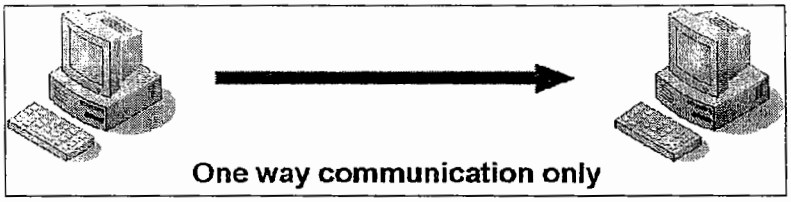
System communication

System communications are basically 3 types

- Simplex
- Half duplex
- Full duplex

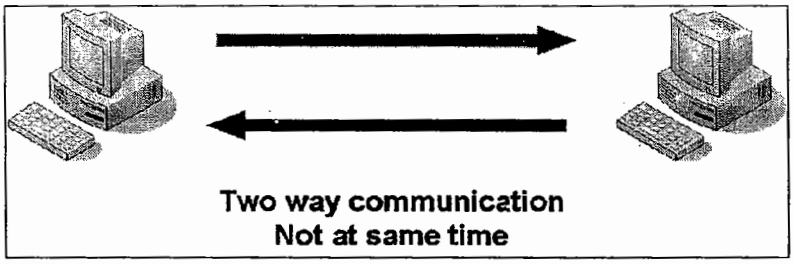
Simplex:

- Only one device can send the data. Other device can receive the data
- Pager communication



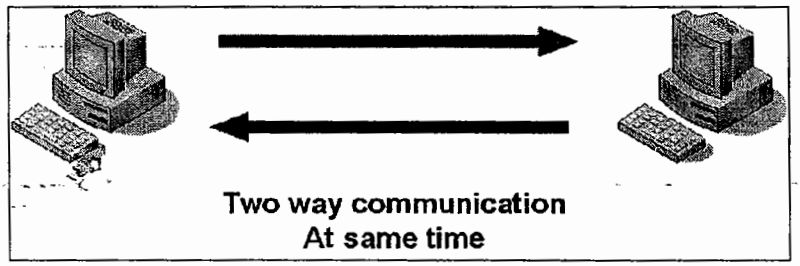
Half Duplex:

- Two way communication is possible, but not at same time
- At one time only one device can send the data or receive the data
- Communication with Hub (Hub supports only Half duplex)
- Collisions happen in half duplex communication



Full Duplex:

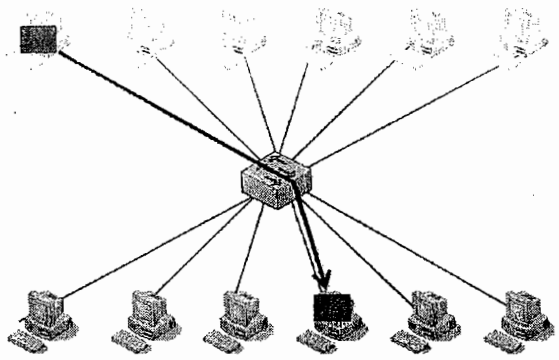
- Two way communication is possible, at same time
- Both devices can send and receive data at one time
- Communication with Switch (Switch supports Half duplex & Full duplex)
- Collisions do not happen in full duplex communication



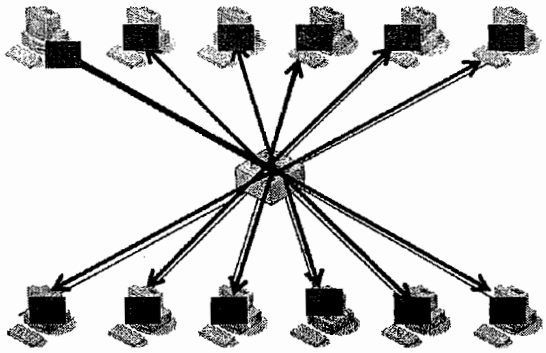
Systems communication

- UNICAST: One device - One device
- BROADCAST: One device - All devices
- MULTICAST: One device - Group of devices

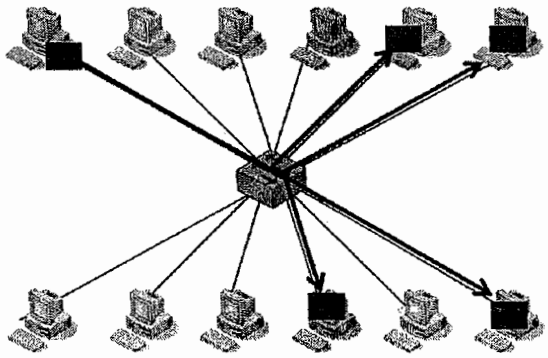
Unicast:



Broadcast:



Multicast:



Systems Communication

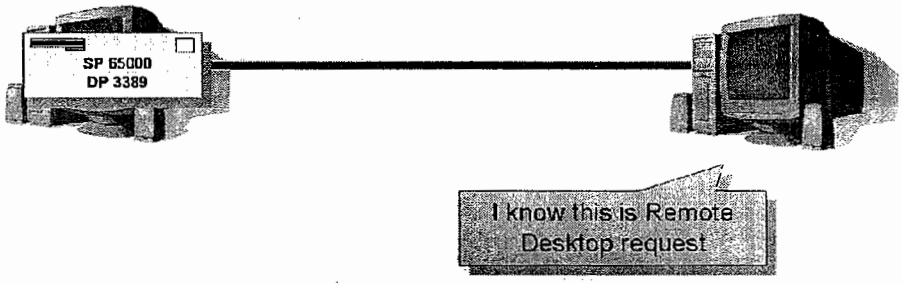
System Architecture: **Hardware & Software** is called Architecture
Systems with different architectures can communicate because they have same protocols

What is Protocol?

- Protocol is a standard set of rules
- Operation sequence to carryout a specific task
- Example: DNS, DHCP, HTTP

What is Port No?

- Port No is a channel of communication
- A system can initiate multiple sessions with destination computer, Unique number is required to identify that session. This Number is port No.
- Port No is 16 bit value
- Range is 0 to 65535



Well Known	Registered	Dynamically Assigned
0 - 1023	1024 - 49151	49152 - 65535

- System uses two port numbers to identify a session
- They are called source port No and destination port no.
- Source Port is selected by system randomly. Typically it is a value between 49152&65535
- Destination Port is used to identify the service of the session at destination computer

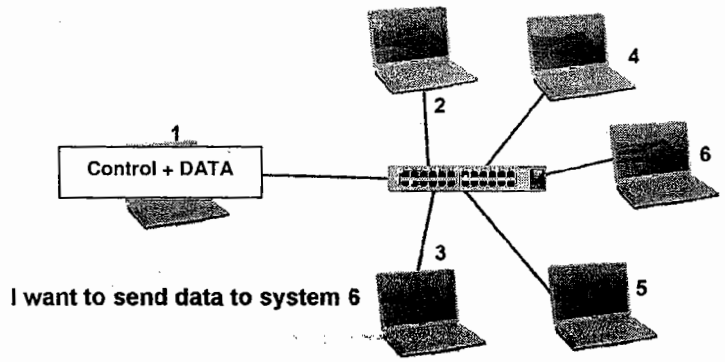
NAGABABU

Important Port Numbers

Protocol	Expansion	Port No
FTP	File Transfer Protocol	20/21
SSH	Secure Shell	22
TELNET	Terminal Network	23
SMTP	Simple Mail Transfer Protocol	25
DNS	Domain Naming System	53
DHCP	Dynamic Host Configuration Protocol	67
TFTP	Trivial File Transfer Protocol	69
HTTP	Hyper Text Transfer Protocol	80
POP3	Post Office Protocol	110
SNMP	Simple Network Management Protocol	161
HTTPS	HTTP Secure	443

Systems Communication

System sends some control information along with the data.
This is the reason; data is directly forwarded to the correct destination.
This control information is called **header** information



- System uses application to send the data
- System converts standard format of data to machine format
- System maintains sessions with destination systems
- System makes the data into small segments
- System adds Source port & Destination port
- System adds Source IP & Destination IP
- System adds Source MAC & Destination MAC
- System sends the data through the Cable

This complex process can be explained by OSI layers

NAGABABU

OSI LAYERS

4. Transport Layer

Functions:

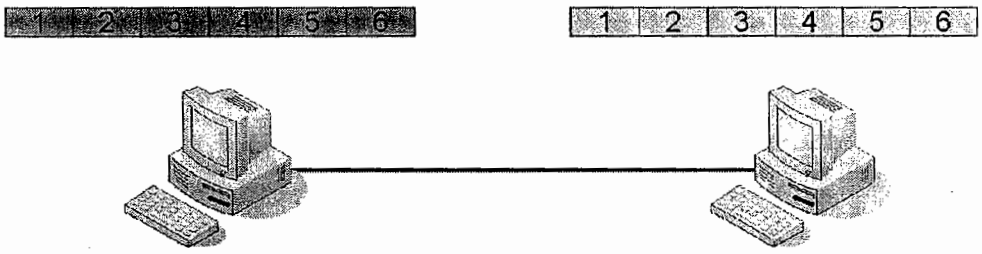
- Segmentation
- Adding TCP/UDP header
- Sequencing & Reassembling
- Multiplexing & Demultiplexing
- Error correction
- Flow control

Protocols:

TCP- Transmission Control Protocol
UDP- User datagram Protocol

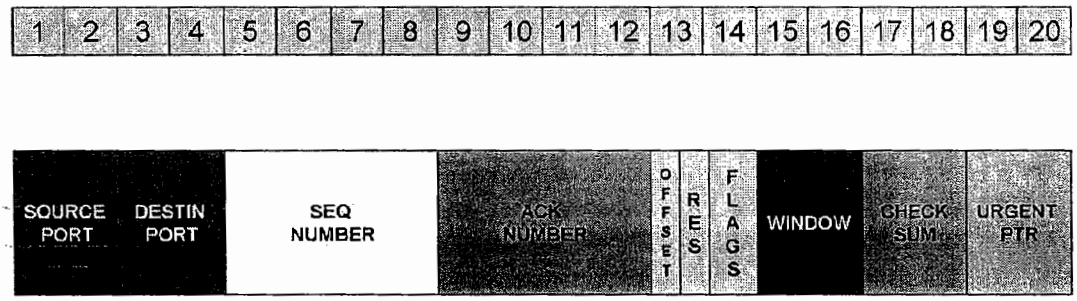
Segmentation:

- It is not possible to handle whole data as a Unit
- TCP typically handles 64KB of data as payload
- The data is divided into smaller segments.
- No of Segments = Total size / 64KB
- Example: 1MB of data is made into 16 segments



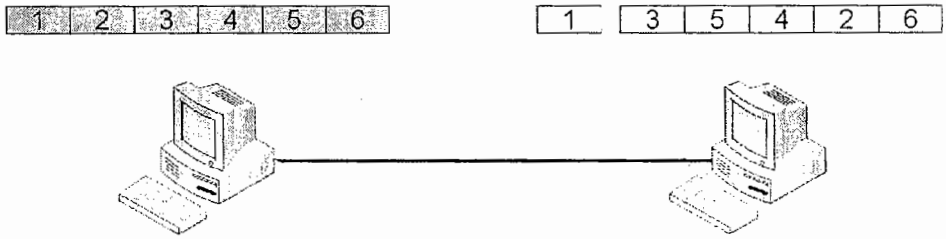
Adding TCP/UDP Header:

- TCP/UDP Header is added to the data fragment
- TCP Header size is 20 Bytes



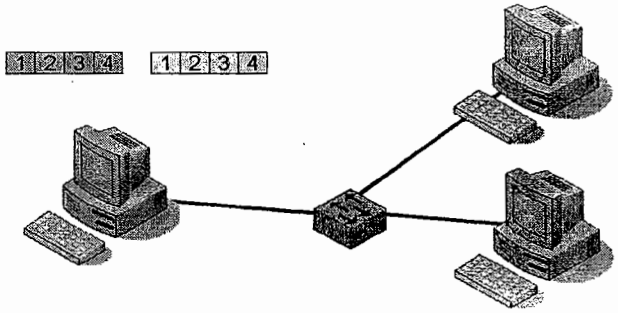
Sequencing & Reassembling:

- Segments will be rearranged if they arrive in different order
- This can be done with the help of sequence number in TCP Header



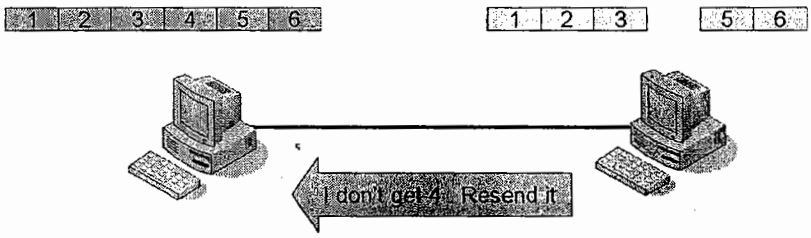
Multiplexing & Demultiplexing:

- When a system communicates with multiple systems, it sends segments to all systems simultaneously



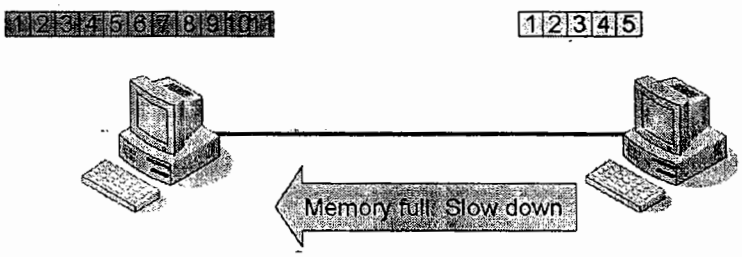
Error Correction:

- Destination system queries the source for missing segments. Source needs to resend them



Flow Control:

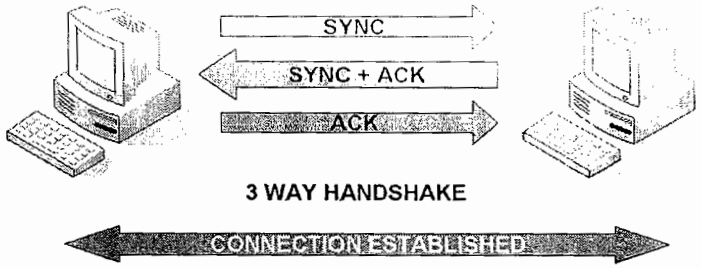
- Speed is adjusted automatically between source and destination computers, if one of the computers is slower



TCP & UDP Differences

TCP	UDP
Transmission control protocol	User datagram protocol
Connection oriented	Connection less
Reliable and slow	Unreliable and fast
Eg. Telnet, FTP, HTTP, SMTP	Eg. SNMP, TFTP, DHCP

TCP:



3. Network Layer

Functions:

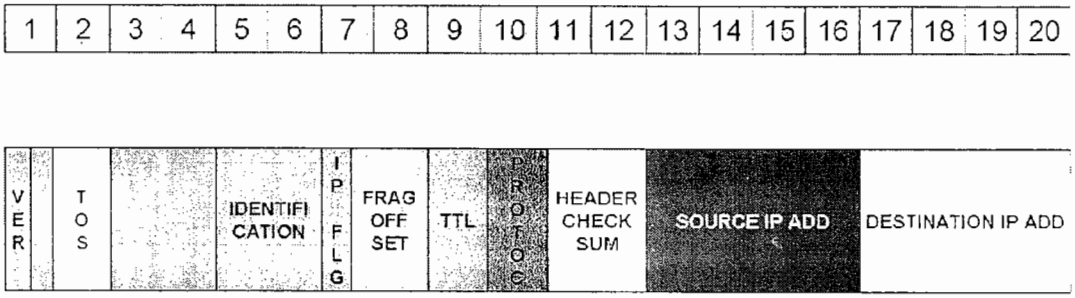
- It provides logical IP Addressing Scheme
- IP Header is added at Network layer
- It chooses best path to destination
- Carries the data in the chosen path

Protocols:

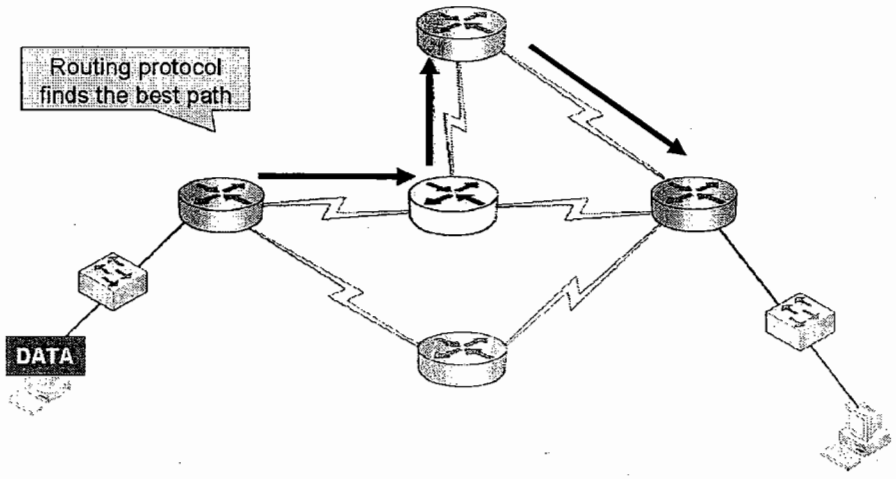
- **Routing Protocols:** Finds all possible paths and chooses the best path
  - RIP - Routing information Protocol
  - IGRP - Interior Gateway Routing Protocol
  - EIGRP - Enhanced IGRP
  - OSPF - Open Shortest Path First
  - ISIS - Intermediate system to Intermediate System
- **Routed Protocols:** Carries the data in the chosen path
  - IP - Internet Protocol
  - IPX - Internet Packet exchange
  - Apple talk

Adding IP Header:

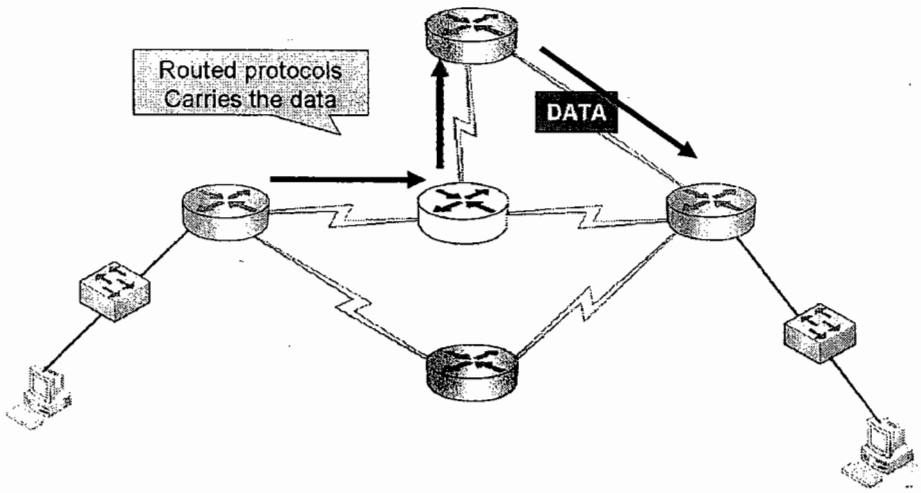
20Byte IP Header is added to the segment



Routing Protocols:



Routed Protocols:



NAGABABU

2. Data Link Layer

Functions:

- It gives network services to the computer
- It does error detection (No correction) -FCS
- Data link Header and Tailor are added to the packet

Protocols/sub layers:

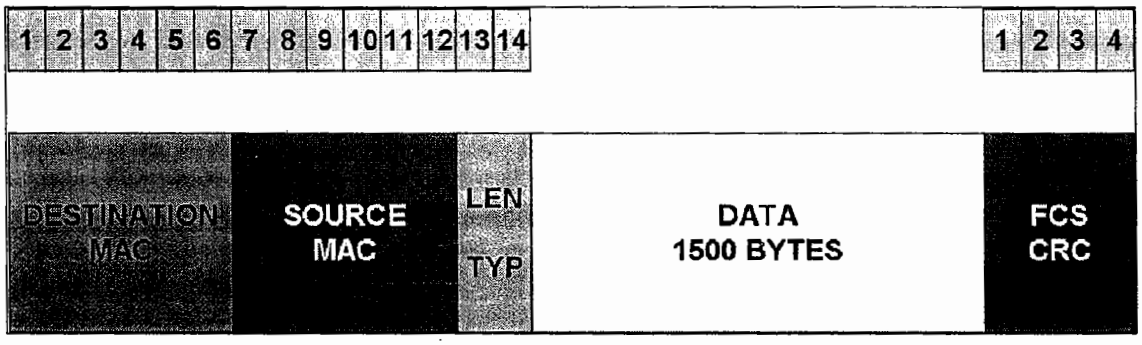
- **MAC Sub Layer** : Media Access Control
  - LAN protocols (LAN connectivity)
  - FDDI, token ring, Ethernet
    - FDDI - Fiber Distributed Data Interface
- **LLC Sub Layer** : Logical Link Control
  - WAN protocols (WAN connectivity)
  - HDLC, PPP, Frame-relay, X.25

Differences between HDLC and PPP:

HDLC	PPP
High level Data link control	Point to Point Protocol
Cisco proprietary	Open Standard
No compression	Supports compression
Doesn't support Authentication	Supports authentication PAP- Password Authentication protocol CHAP - Challenge handshake Authentication protocol

Adding Data link Header and Tailor:

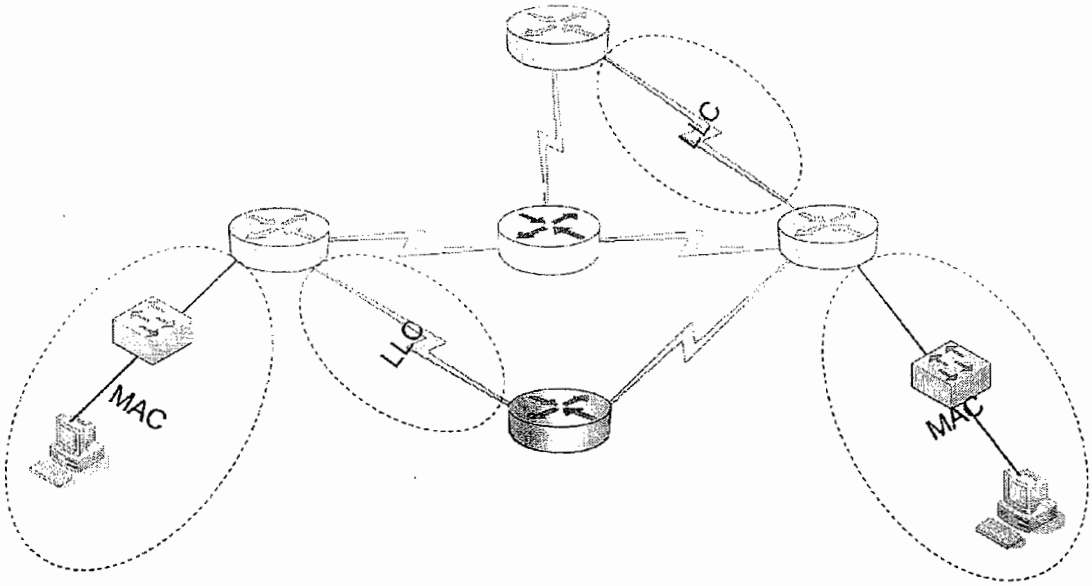
14 Byte Data link Header is added to the packet at beginning
4 Byte Data link Tailor is added to the packet at ending (FCS/CRC)



Data link tailor is used for error checking

Source computer generates one value by running CRC algorithm on the data and sends that value in the tailor. Destination computer also runs CRC and compares that value with original. Destination system accepts the data if it matches.

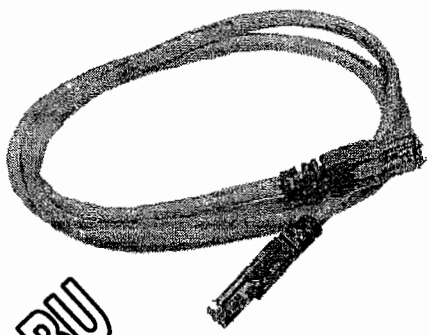
Data link Layer Sub Layers:

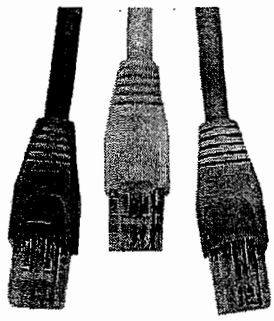


1. Physical Layer

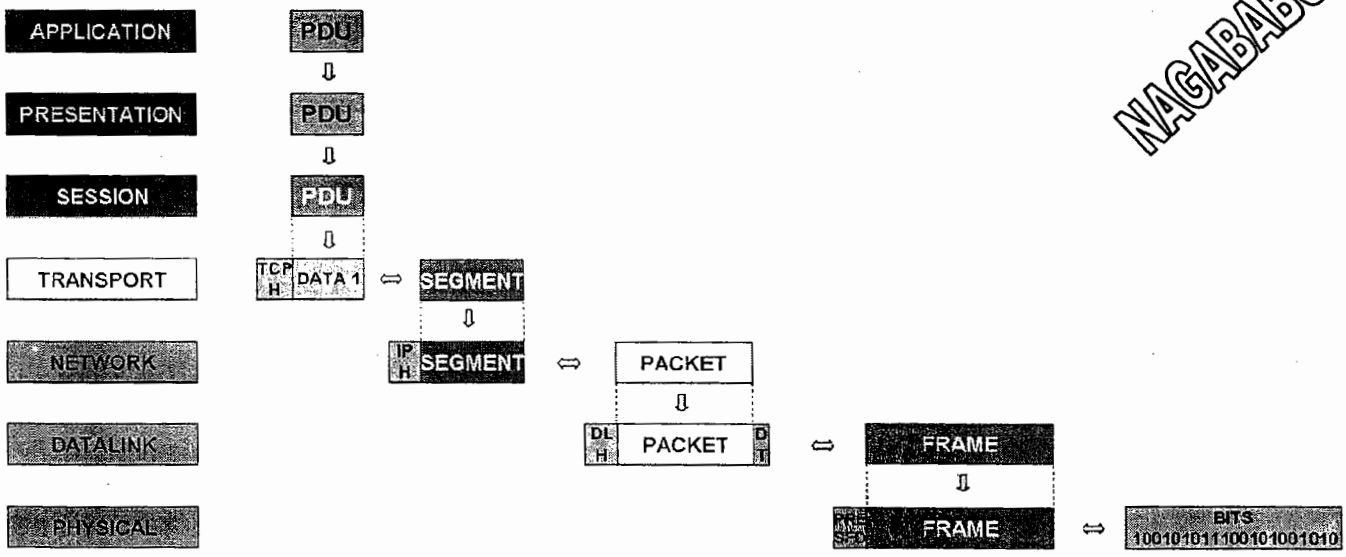
Functions:

- It deals with electrical and mechanical properties
- Cables, connectors, voltage levels
- Eg. Rj-45, Rj-11 connectors, Transceiver, V.35 cables





OSI LAYERS - DATA TYPES



OSI LAYERS

NAGABABU

Layer No	Layer	Data Type	Layer Type	Devices	Protocols
7	Application	PDU	Upper Layers Software layers	Application	HTTP, SMTP, TFTP, FTP, Telnet, DHCP
6	Presentation	PDU			ASCII, EBCDIC, JPEG, BMP, MPEG
5	Session	PDU			RPC, NFS
4	Transport	Segment	Heart of OSI		TCP, UDP
3	Network	Packet / Datagram	Lower Layers Hardware layers	Router MLS	RIP, IGRP, EIGRP, OSPF, ISIS IP, IPX, Apple talk, IGMP,ICMP,ARP,RARP
2	Data link	Frame		Switch NIC	FDDI, Token ring, Ethernet HDLC, LLC, X.25, Frame-relay
1	Physical	Bits		Hub cables	Cables, Connectors

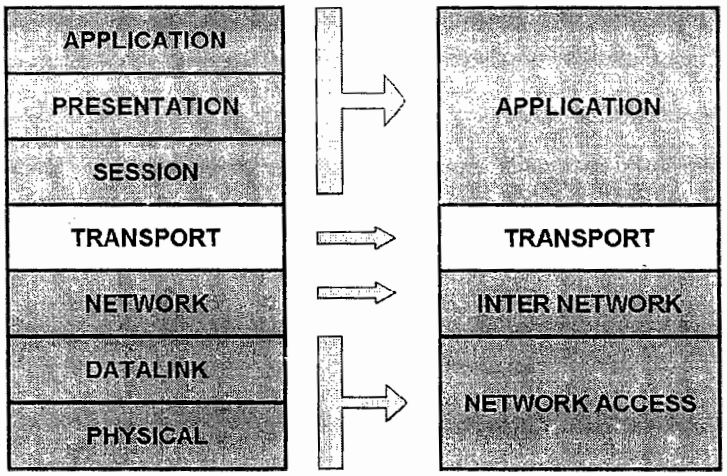
TCP/IP REFERENCE MODEL

NAGABABU

TCP/IP Model is also called as DOD model
Before 1980 ARPANet was used by US Department of defense (DOD)
After 1980 ARPANet eventually turned to Internet

TCP/IP reference model explains protocols related to TCP/IP protocol suite
OSI reference model explains all protocols

OSI REFERENCE MODEL **TCP/IP REFERENCE MODEL**

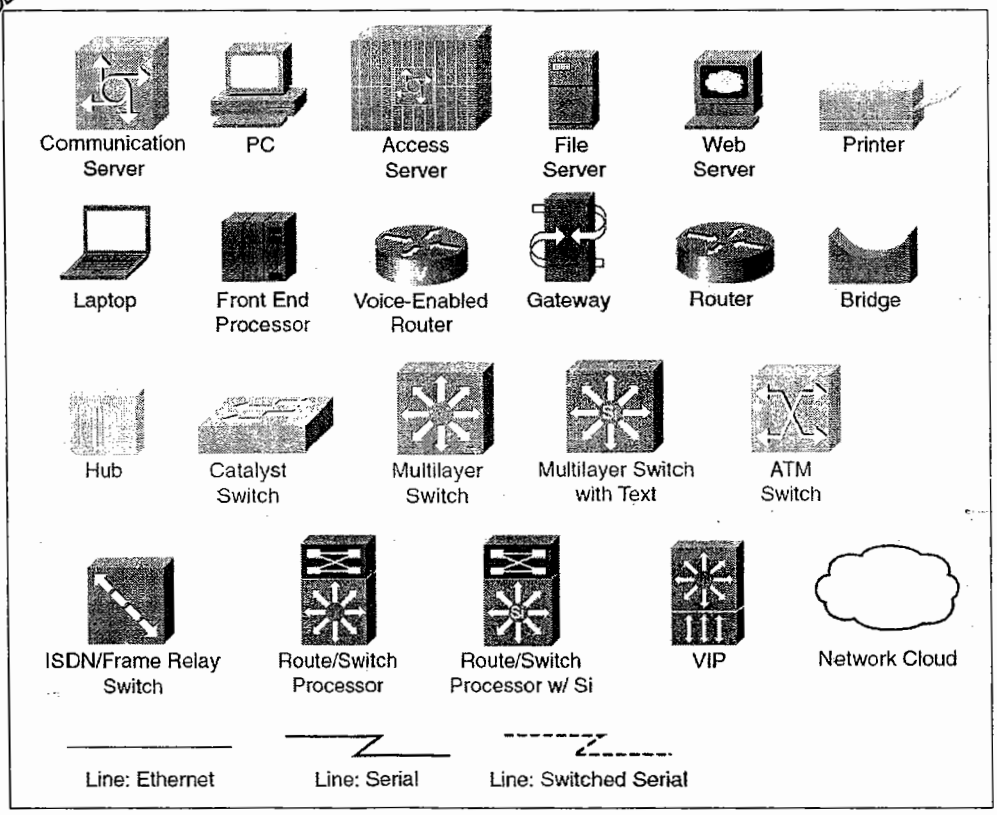


Network devices

Network device	Function	Operates at OSI
Repeater	Regenerates the weekend signal	Layer 1
HUB	Regenerates the signal, flooding (Multi port repeater)	Layer 1
Bridge	Filters and forwards the data	Layer 2
Switch	Filters and forwards the data (Multi port Bridge)	Layer 2
NIC	Gives network services to the system	Layer 2
Router	Communicates between different Networks	Layer 3
Brouter	Bridge with Layer 3 function	Layer 3
Multilayer Switch	Switch with Layer 3 function (L3 switch/MLS)	Layer 3
PIX	Firewall (Filters the unwanted traffic)	Layer 3

NAGABABU

Network devices



IP ADDRESSING

SUBNETTING

IP Addressing

IP Address is a 32 Bit Value

00000000.00000000.00000000.00000000
0 . 0 . 0 . 0
First IP Address

11111111.11111111.11111111.11111111
255 . 255 . 255 . 255
Last IP Address

IP Address order:

0.0.0.0	0.0.0.251	0.0.1.251	0.0.255.250	255.255.255.245
0.0.0.1	0.0.0.252	0.0.1.252	0.0.255.251	255.255.255.246
0.0.0.2	0.0.0.253	0.0.1.253	0.0.255.252	255.255.255.247
0.0.0.3	0.0.0.254	0.0.1.254	0.0.255.253	255.255.255.248
0.0.0.4	0.0.0.255	0.0.1.255	0.0.255.254	255.255.255.249
0.0.0.5	0.0.1.0	0.0.2.0	0.0.255.255	255.255.255.250
0.0.0.6	0.0.1.1	0.0.2.1	0.1.0.0	255.255.255.251
0.0.0.7	0.0.1.2	0.0.2.2	0.1.0.1	255.255.255.252
0.0.0.8	0.0.1.3	0.0.2.3	0.1.0.2	255.255.255.253
0.0.0.9	0.0.1.4	0.0.2.4	0.1.0.3	255.255.255.254
0.0.0.10	0.0.1.5	0.0.2.5	0.1.0.4	255.255.255.255
0.0.0.11	0.0.1.6	0.0.2.6	0.1.0.5	
0.0.0.12	0.0.1.7	0.0.2.7	0.1.0.6	
0.0.0.13	0.0.1.8	0.0.2.8	0.1.0.7	
0.0.0.14		0.0.2.9	0.1.0.8	
0.0.0.15	--------	0.0.2.10		
---------	--------	--------	---------	
---------	--------	--------	---------	

NAGABABU

IP addresses from 0.0.0.0 to 255.255.255.255 are classified into 5 classes based on First octet value

- Class A 0-127
- Class B 128-191
- Class C 192-223
- Class D 224-239
- Class E 240-255

Class A:

Parity Bit - 0
00000000 = 0
01111111 = 127

Class B:

Parity Bit - 10
10000000 = 128
10111111 = 191

Class C:

Parity Bit - 110
11000000 = 192
11011111 = 223

Class D:

Parity Bit - 1110
11100000 = 224
11101111 = 239

Class E:

Parity Bit - 1111
11110000 = 240
11111111 = 255

IP Address has four octets. Every octet contains 8 bits

octet1 octet2 octet3 octet4

192. 168. 6. 1

11000000.10101000.00000110.00000001

Subnet Mask Value

- Subnet mask value defines properties of IP Address to which it can communicate and to which it can not
- Subnet mask value defines Network component and host component of an IP address
- IP address uses subnet mask to find out boundaries of network.
- Subnet mask value is a driver of IP Address

- Network Bits are always represented with 1
- Host Bits are always represented with 0

Subnet Mask Structures:

CLASS A Subnet Mask Structure

N.H.H.H

11111111.00000000.00000000.00000000

255.0.0.0

CLASS B Subnet Mask Structure

N.N.H.H

11111111.11111111.00000000.00000000

255.255.0.0

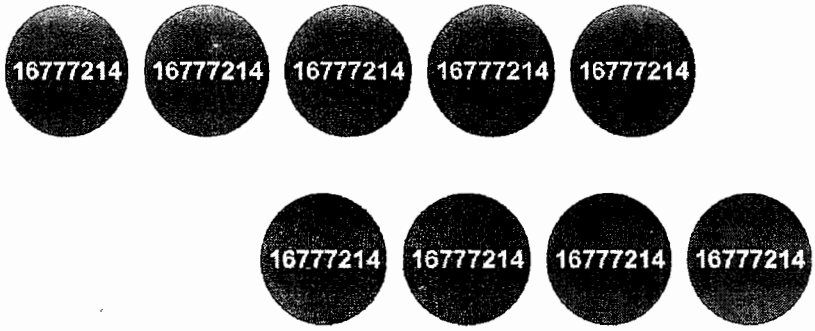
CLASS C Subnet Mask Structure

N.N.N.H

11111111.11111111.11111111.00000000

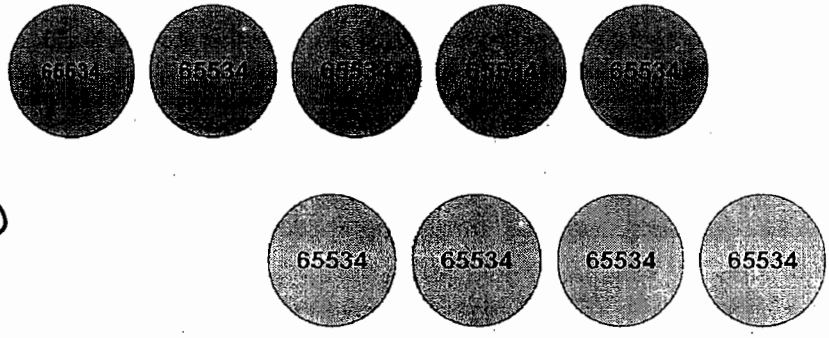
255.255.255.0

Class A Networks:



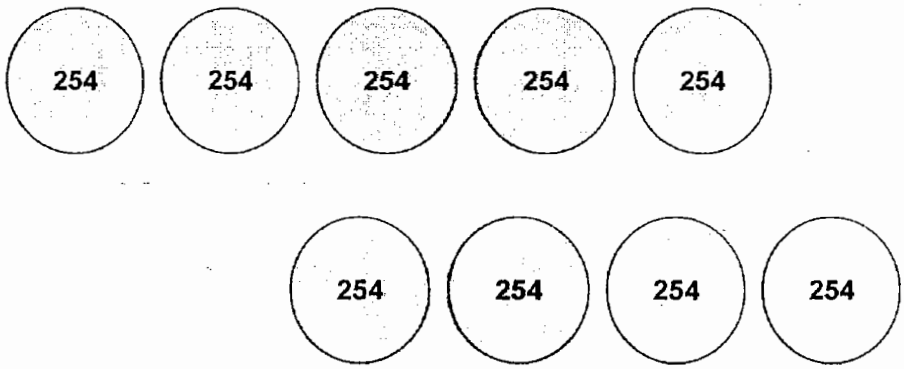
Number of Networks : **126**
Number of Hosts per Network : 2 power 24 = **16777216**

Class B Networks:



Number of Networks : **16384**
Number of Hosts per Network : 2 power 16 = **65536**

Class C Networks:



Number of Networks : **2097152**
Number of Hosts per Network : 2 power 8 = **256**

What is Network Address?

- Network Address is the identification address for all the systems in the network
- The systems with same network address can communicate with each other
- Systems with different network addresses can not communicate generally

What is Broadcast Address?

- Broadcast Address is used to deliver a broadcast message to all the computers in the network
- The systems with same network address can have same broadcast address
- All the systems in between Network address and broadcast address form a logical network to communicate with each other

Network Address and Broadcast Address are the boundaries of a network
They can't be assigned to computers

How to find out Network Address?

- Identify class of IP Address and Subnet mask Structure.
  Replace Host portion with 0 (or)
- Perform a logical AND operation between IP Address and subnet mask value

How to find out Broadcast Address?

- Identify class of IP Address and Subnet mask Structure
  Replace Host portion with 255 (or)
- Perform a logical OR operation between IP Address and inverse subnetmask value

10.185.223.19

N . H . H . H

Network Address = 10.0.0.0
Broadcast Address = 10.255.255.255

172.20.18.96

N . N . H . H

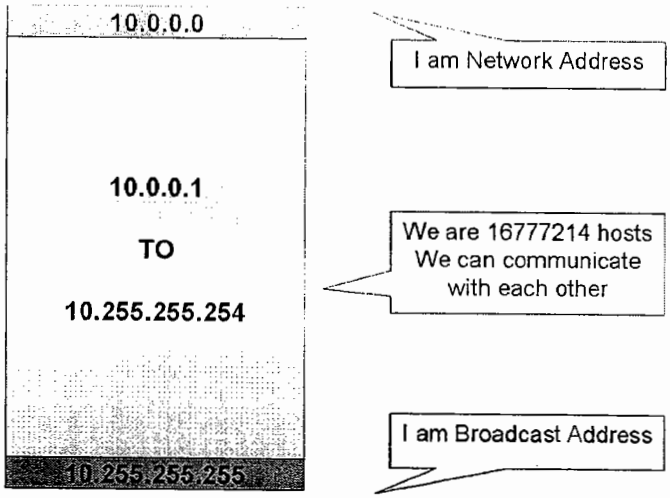
Network Address = 172.20.0.0
Broadcast Address = 172.20.255.255

192.168.6.145

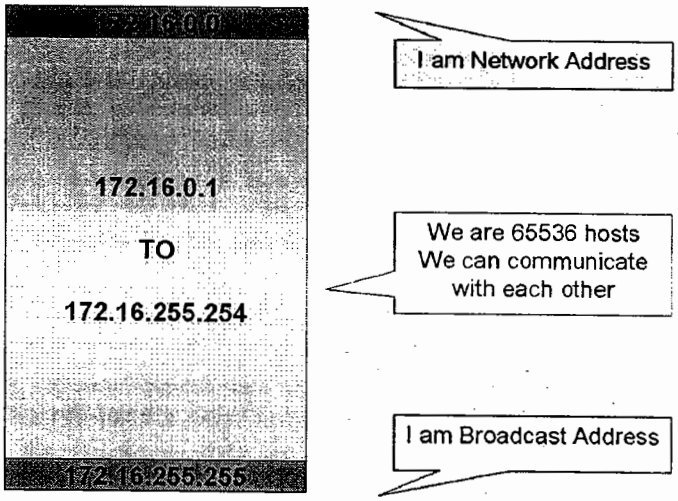
N . N . N . H

Network Address = 192.168.6.0
Broadcast Address = 192.168.6.255

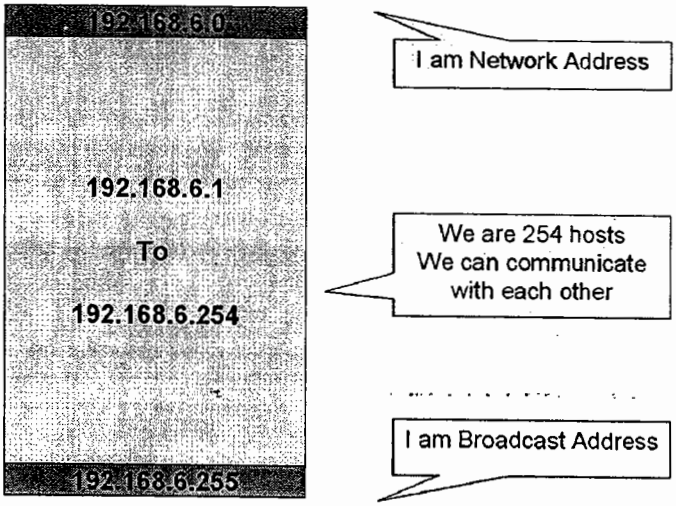
Class A Networks:



Class B Networks:



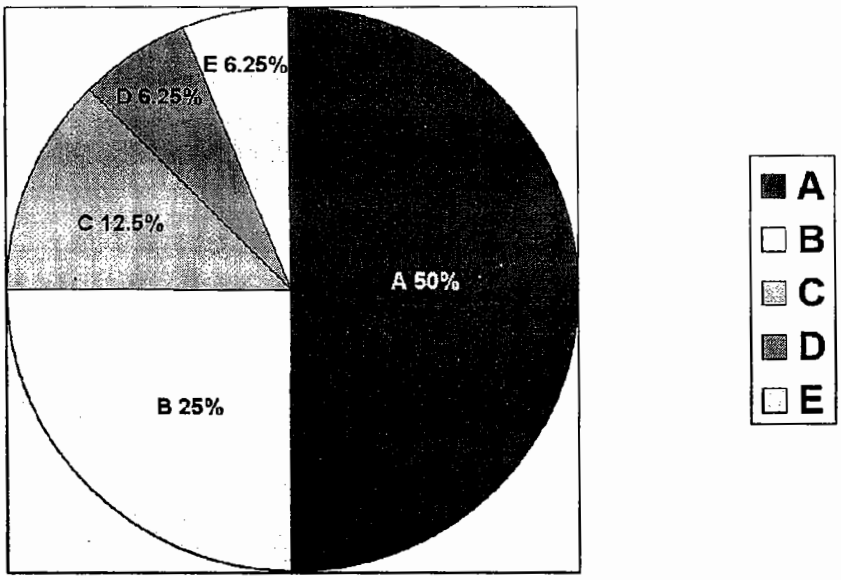
Class C Networks:



IP ADDRESSING

Class	Parity	Range	Subnet Mask Structure	Subnet Mask Value	Networks	Hosts per Network
A	0	0-127	N.H.H.H	255.0.0.0	126	16777214
B	10	128-191	N.N.H.H	255.255.0.0	16384	65534
C	110	192-223	N.N.N.H	255.255.255.0	2097152	254
D	1110	224-239	Multicasting -- Video Conference			
E	1111	240-255	Reserved by IETF – for R&D			

IP Address Percentage:



IP Address Related Organizations:

IANA - Internet Assigned Numbers Authority
ICANN - Internet Corporation for Assigned Numbers and Names

Private IP Addresses:

- The IP addresses not routable in public network
- Used to communicate within private network
- Internet access is not possible with private IP address
- Defined in RFC 1918

CLASS A	10.0.0.0 /8	10.0.0.0 - 10.255.255.255
CLASS B	172.16.0.0 /12	172.16.0.0 - 172.31.255.255
CLASS C	192.168.0.0 /16	192.168.0.0 - 192.168.255.255

Special IP Addresses:

- 0.0.0.0 Network is reserved for default routing. Can't be assigned to systems
- 127.0.0.0 Network is reserved for loop back purpose (NIC diagnosis)
- Class D Networks are reserved for multicasting. Not for systems
- Class E Networks are reserved for Research and Development. Not for systems

SUBNETTING

What is Subnetting?

Logically breaking the major network into smaller networks - **Subnets**

Advantage of Subnetting

- Reduce wastage of IP Addresses

(Once the network is used, it can't be used again in the same organization)

Subnetting Procedure

Increase network bits in the subnet mask value from left to right

192.168.6.0 Subnetting

256
11111111.11111111.11111111.00000000 255.255.255.0

128	128
11111111.11111111.11111111.10000000 255.255.255.128	

64	64	64	64
11111111.11111111.11111111.11000000 255.255.255.192			

32	32	32	32	32	32	32	32
11111111.11111111.11111111.11100000 255.255.255.224							

Subnetting Formulae:

No of Networks = 2^N
N= increased Network bits

No of Hosts per Network = $2^H - 2$
H= remaining Host bits

Example to understand Formulae:

192.168.6.0 Subnetting : 3 Network bits increased

32	32	32	32	32	32	32	32

11111111.11111111.11111111.**11**100000

255.255.255.224

N=3
No of Networks = $2^N = 2^3 = 8$

H=5
No of Hosts per Network = $2^H - 2 = 2^5 - 2 = 32 - 2 = 30$

Subnetting methods

Subnetting can be done in two ways

- Based on No of Networks
- Based on No of Hosts

SUBNETTING Calculations

Based on No of Networks:

- Identify required No of subnets
- Refer 2 power chart

- Identify N value
- Increase the bits in the subnetmask value
- **Identify H value**

- Find out new subnet mask value
- Find out No of subnets and No of hosts

- Subtract new subnet mask value from 255.255.255.255
- Find out network address & Broadcast address of all subnets

Based on No of Hosts:

- Identify required No of Hosts per subnet
- Refer 2 power chart

- **Identify H value**
- Increase the bits in the subnetmask value
- **Identify N value**

- Find out new subnet mask value
- Find out No of subnets and No of hosts

- Subtract new subnet mask value from 255.255.255.255
- Find out network address & Broadcast address of all subnets

Based on No of Networks

Q1. Divide 192.168.6.0 into 4 subnets

➢Divide 192.168.6.0 into 4 Subnets

$2^0=1$
$2^1=2$
$2^2=4$
$2^3=8$
$2^4=16$
$2^5=32$
$2^6=64$
$2^7=128$
$2^8=256$
$2^9=512$
$2^{10}=1024$
$2^{11}=2048$
$2^{12}=4096$
$2^{13}=8192$
$2^{14}=16384$
$2^{15}=32768$

255.255.255.0

11111111.11111111.11111111.11000000

255.255.255.192

N=2 H=6

No of Networks = $2^N = 4$

No of Hosts per Network = $2^H - 2 = 62$

00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

255.255.255.255

255.255.255.192

0 . 0 . 0 . 63

	Network Address	Broadcast Address
Subnet 1	192.168.6.0	192.168.6.63
Subnet 2	192.168.6.64	192.168.6.127
Subnet 3	192.168.6.128	192.168.6.191
Subnet 4	192.168.6.192	192.168.6.255

NAGABABU

Based on No of Networks

Q2. Divide 10.0.0.0 into 100 subnets

➢Divide 10.0.0.0 into 100 Subnets

$2^0=1$
$2^1=2$
$2^2=4$
$2^3=8$
$2^4=16$
$2^5=32$
$2^6=64$
$2^7=128$
$2^8=256$
$2^9=512$
$2^{10}=1024$
$2^{11}=2048$
$2^{12}=4096$
$2^{13}=8192$
$2^{14}=16384$
$2^{15}=32768$

255.0.0.0

11111111.11111110.00000000.00000000

255.254.0.0

N=7 H=17

No of Networks = 2^N = **128 (use 100)**

No of Hosts per Network = $2^H - 2$ = **131070**

00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

255.255.255.255

255.254. 0 . 0

0 . 1 .255. 255

	Network Address	Broadcast Address
Subnet 1	10.0.0.0	10.1.255.255
Subnet 2	10.2..0.0	10.3.255.255
Subnet 3	10.4.0.0	10.5.255.255
---------	--------	---------
Subnet 127	10.252.0.0	10.253.255.255
Subnet 128	10.254.0.0	10.255.255.255

NAGABABU

Based on No of Networks

Q3. Divide 172.16.0.0 into 64 subnets

➢Divide 172.16.0.0 into 64 Subnets

$2^0=1$
$2^1=2$
$2^2=4$
$2^3=8$
$2^4=16$
$2^5=32$
$2^6=64$
$2^7=128$
$2^8=256$
$2^9=512$
$2^{10}=1024$
$2^{11}=2048$
$2^{12}=4096$
$2^{13}=8192$
$2^{14}=16384$
$2^{15}=32768$

255.255.0.0

11111111.11111111.**11111100.00000000**

255.255.252.0

N=6 H=10

No of Networks = 2^N = **64**

No of Hosts per Network = $2^H - 2$ = **1022**

00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

255.255.255.255

255.255.252. 0

0 . 0 . 3 . 255

	Network Address	Broadcast Address
Subnet 1	**172.16.0.0**	**172.16.3.255**
Subnet 2	172.16.4.0	172.16.7.255
Subnet 3	172.16.8.0	172.16.11.255
--------	-------	-------
Subnet 127	172.16.248.0	172.16.251.255
Subnet 128	172.16.252.0	172.16.255.255

Based on No of Hosts

Q1. Divide 192.168.6.0 into subnets with 28 hosts

➢Divide 192.168.6.0 into Subnets with 28 hosts

$2^0=1$
$2^1=2$
$2^2=4$
$2^3=8$
$2^4=16$
$2^5=32$
$2^6=64$
$2^7=128$
$2^8=256$
$2^9=512$
$2^{10}=1024$
$2^{11}=2048$
$2^{12}=4096$
$2^{13}=8192$
$2^{14}=16384$
$2^{15}=32768$

255.255.255.0

11111111.11111111.11111111.11100000

255.255.255.224

N=3 H=5

No of Networks = 2^N = **8**

No of Hosts per Network = $2^H - 2$ = **30**

00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

255.255.255.255

255.255.255.224

0 . 0 . 0 . 31

	Network Address	Broadcast Address
Subnet 1	192.168.6.0	192.168.6.31
Subnet 2	192.168.6.32	192.168.6.63
Subnet 3	192.168.6.64	192.168.6.95
Subnet 4	192.168.6.96	192.168.6.127
Subnet 5	192.168.6.128	192.168.6.159
Subnet 6	192.168.6.160	192.168.6.191
Subnet 7	192.168.6.192	192.168.6.223
Subnet 8	192.168.6.224	192.168.6.255

NAGABABU

Based on No of Hosts

Q2. Divide 10.0.0.0 into subnets with 4000 hosts

➢Divide 10.0.0.0 into Subnets with 4000 hosts

$2^0=1$
$2^1=2$
$2^2=4$
$2^3=8$
$2^4=16$
$2^5=32$
$2^6=64$
$2^7=128$
$2^8=256$
$2^9=512$
$2^{10}=1024$
$2^{11}=2048$
$2^{12}=4096$
$2^{13}=8192$
$2^{14}=16384$
$2^{15}=32768$

255.0.0.0

11111111.11111111.11110000.00000000

255.255.240.0

N=12 H=12

No of Networks = 2^N = **4096**

No of Hosts per Network = $2^H - 2$ = **4094**

00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

255.255.255.255

255.255.240. 0

0 . 0 . 15 . 255

	Network Address	Broadcast Address
Subnet 1	10.0.0.0	10.0.15.255
Subnet 2	10.0.16.0	10.0.31.255
Subnet 3	10.0.32.0	10.0.47.255
Subnet 4	10.0.48.0	10.0.63.255
-------	----------	--------
Subnet 4094	10.255.208.0	10.255.223.255
Subnet 4095	10.255.224.0	10.255.239.255
Subnet 4096	10.255.240.0	10.255.255.255

NAGABABU

Based on No of Hosts

Q3. Divide 172.16.0.0 into subnets with 500 hosts

➢Divide 172.16.0.0 into Subnets with 500 hosts

$2^0=1$
$2^1=2$
$2^2=4$
$2^3=8$
$2^4=16$
$2^5=32$
$2^6=64$
$2^7=128$
$2^8=256$
$2^9=512$
$2^{10}=1024$
$2^{11}=2048$
$2^{12}=4096$
$2^{13}=8192$
$2^{14}=16384$
$2^{15}=32768$

255.255.0.0

11111111.11111111.**11111110.00000000**

255.255.254.0

N=7 H=9

No of Networks = 2^N = **128**

No of Hosts per Network = $2^H - 2$ = **512 (use 500)**

00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

255.255.255.255

255.255.254. 0

0 . 0 . 1 .255

	Network Address	Broadcast Address
Subnet 1	**172.16.0.0**	**172.16.1.255**
Subnet 2	172.16.2.0	172.16.3.255
Subnet 3	172.16.4.0	172.16.5.255
Subnet 4	172.16.6.0	172.16.7.255
-------	-------	--------
Subnet 126	172.16.250.0	172.16.251.255
Subnet 127	172.16.252.0	172.16.253.255
Subnet 128	172.16.254.0	172.16.255.255

NAGABABU

Subnet Mask Values

/0	00000000.00000000.00000000.00000000	0.0.0.0
/1	10000000.00000000.00000000.00000000	128.0.0.0
/2	11000000.00000000.00000000.00000000	192.0.0.0
/3	11100000.00000000.00000000.00000000	224.0.0.0
/4	11110000.00000000.00000000.00000000	240.0.0.0
/5	11111000.00000000.00000000.00000000	248.0.0.0
/6	11111100.00000000.00000000.00000000	252.0.0.0
/7	11111110.00000000.00000000.00000000	254.0.0.0
/8	11111111.00000000.00000000.00000000	255.0.0.0
/9	11111111.10000000.00000000.00000000	255.128.0.0
/10	11111111.11000000.00000000.00000000	255.192.0.0
/11	11111111.11100000.00000000.00000000	255.224.0.0
/12	11111111.11110000.00000000.00000000	255.240.0.0
/13	11111111.11111000.00000000.00000000	255.248.0.0
/14	11111111.11111100.00000000.00000000	255.252.0.0
/15	11111111.11111110.00000000.00000000	255.254.0.0
/16	11111111.11111111.00000000.00000000	255.255.0.0
/17	11111111.11111111.10000000.00000000	255.255.128.0
/18	11111111.11111111.11000000.00000000	255.255.192.0
/19	11111111.11111111.11100000.00000000	255.255.224.0
/20	11111111.11111111.11110000.00000000	255.255.240.0
/21	11111111.11111111.11111000.00000000	255.255.248.0
/22	11111111.11111111.11111100.00000000	255.255.252.0
/23	11111111.11111111.11111110.00000000	255.255.254.0
/24	11111111.11111111.11111111.00000000	255.255.255.0
/25	11111111.11111111.11111111.10000000	255.255.255.128
/26	11111111.11111111.11111111.11000000	255.255.255.192
/27	11111111.11111111.11111111.11100000	255.255.255.224
/28	11111111.11111111.11111111.11110000	255.255.255.240
/29	11111111.11111111.11111111.11111000	255.255.255.248
/30	11111111.11111111.11111111.11111100	255.255.255.252
/31	11111111.11111111.11111111.11111110	255.255.255.254
/32	11111111.11111111.11111111.11111111	255.255.255.255

VLSM

What is VLSM?

- Variable Length Subnet Mask
- Also called as Subnetting of Subnetting
- Subnetting is used to break the network equally
- If these networks are subnetted again, different subnets may have different subnet mask values, also called as Variable length subnet masks
- With VLSM, IP addressing scheme is used more efficiently without wastage

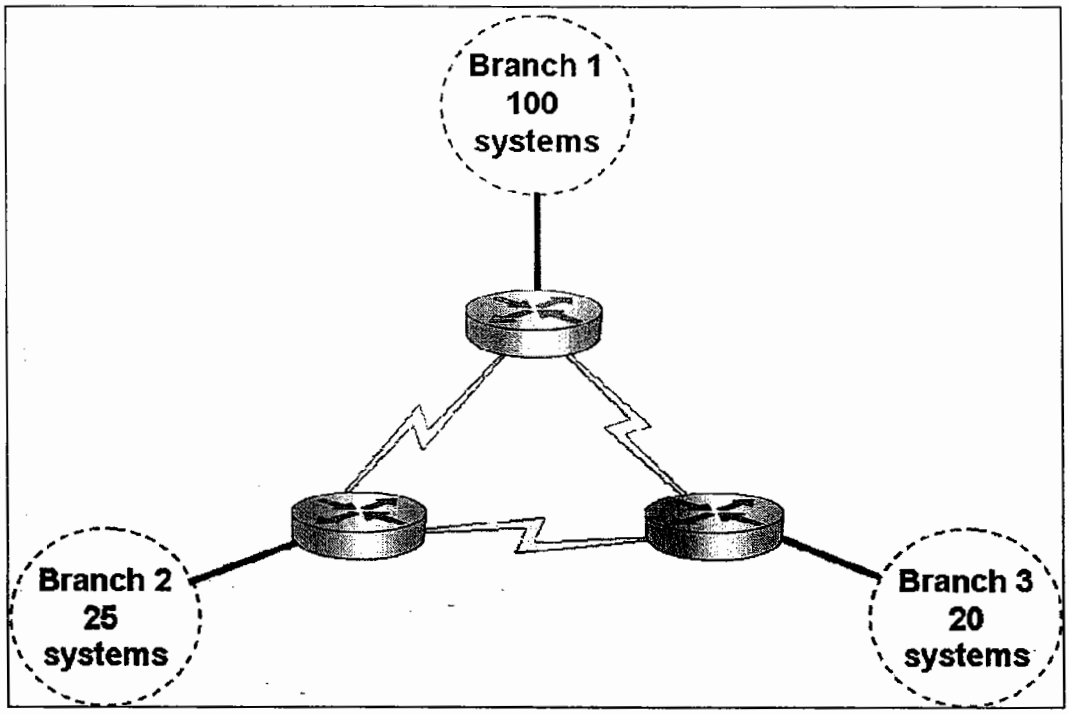
192.168.6.0 SUBNETTING			
64	64	64	64
255.255.255.192	255.255.255.192	255.255.255.192	255.255.255.192

192.168.6.0 VLSM												
64	8	8	8	8	8	8	8	8	64	16	16	16	16
255.255.255.192	255.255.255.248								255.255.255.192	255.255.255.240		

Subnetting & VLSM comparisons:

Subnetting	VLSM
Breaking network equally	Breaking network unequally
Sub-netting	Subnetting of Subnetting
Has same subnet mask value	Has different subnet mask values
Reduce IP wastage	Reduce IP wastage more effectively

Design IP Addressing scheme for this network with 192.168.6.0



Required networks = 6

Branch1	101 hosts
Branch2	26 hosts
Branch3	21 hosts
Branch 1-2 wan link	2 hosts
Branch 2-3 wan link	2 hosts
Branch 3-1 wan link	2 hosts

Branch 1 requires 101 hosts. Divide 192.168.6.0 into subnets based on No of Hosts

Subnet 1	192.168.6.0 - 192.168.6.127	/25	Assigned to Branch 1
Subnet 2	192.168.6.128 - 192.168.6.255	/25	Further division

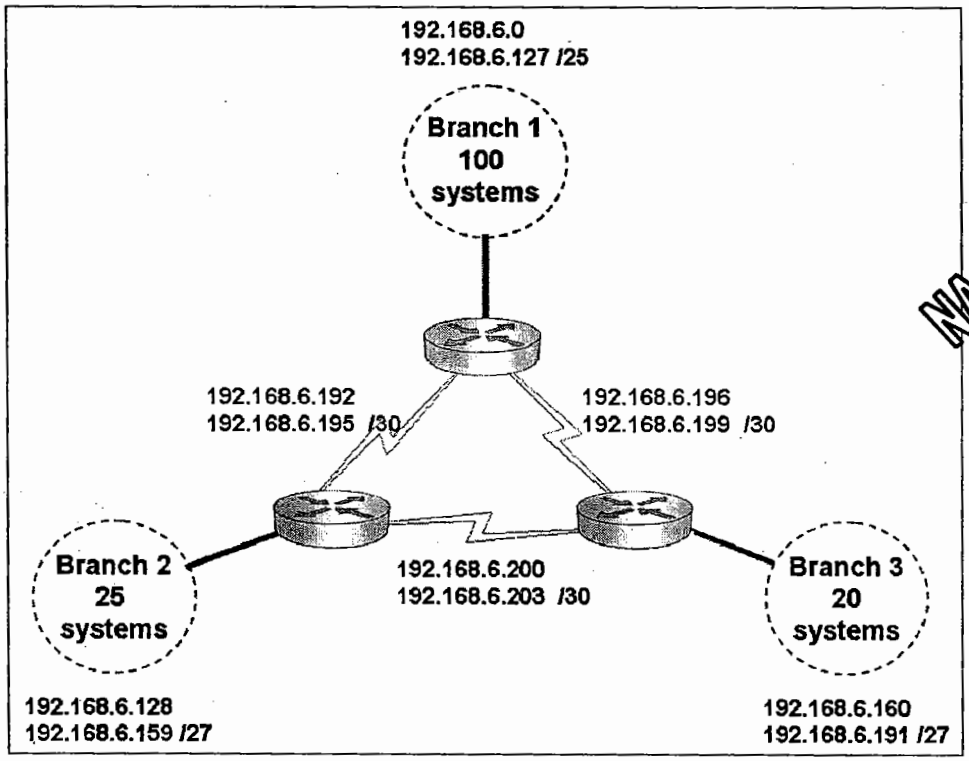
Branch 2 requires 26 hosts, Branch 3 requires 21 hosts. Divide the subnet again

Subnet 1	192.168.6.128 - 192.168.6.159	/27	Assigned to Branch 2
Subnet 2	192.168.6.160 - 192.168.6.191	/27	Assigned to Branch 3
Subnet 3	192.168.6.192 - 192.168.6.223	/27	Further division
Subnet 4	192.168.6.224 - 192.168.6.255	/27	Future use

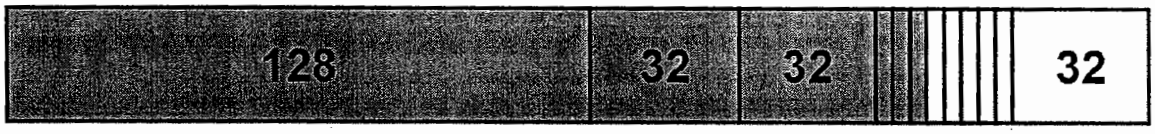
Point to Point links require 2 hosts. Divide the subnet again

Subnet 1	192.168.6.192 - 192.168.6.195	/30	Branch 1-2 wan link
Subnet 2	192.168.6.196 - 192.168.6.199	/30	Branch 2-3 wan link
Subnet 3	192.168.6.200 - 192.168.6.203	/30	Branch 3-1 wan link
Subnet 4	192.168.6.204 - 192.168.6.207	/30	Future use
Subnet 5	192.168.6.208 - 192.168.6.211	/30	Future use
Subnet 6	192.168.6.212 - 192.168.6.215	/30	Future use
Subnet 7	192.168.6.216 - 192.168.6.219	/30	Future use
Subnet 8	192.168.6.220 - 192.168.6.223	/30	Future use

Network Solution



NAGABABU

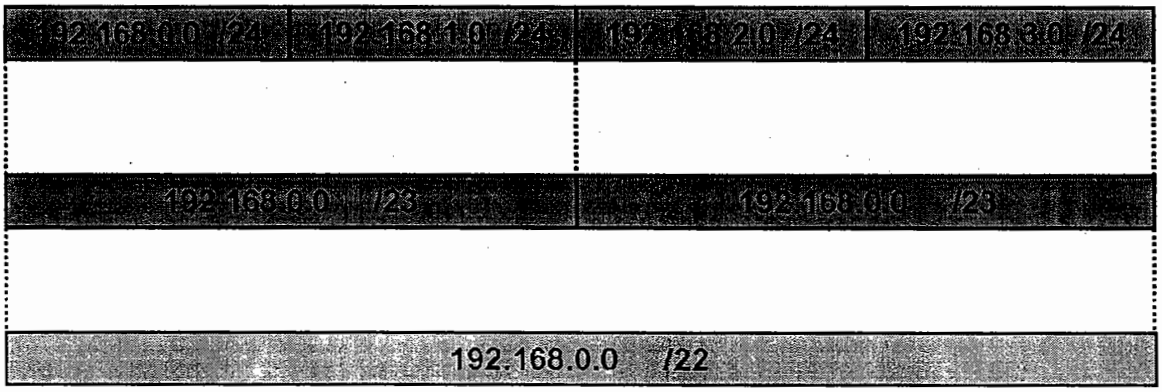


Supernetting

What is Supernetting?

- This is reverse procedure of Subnetting
- It is used to combine the networks / subnetworks
- To combine the networks decrease the network bits from right to left

- Generally Supernetting concept is used in router advertisements, called as route summarization
- Supernetting calculations are similar to Subnetting calculations



ROUTERS

What is Router?

- Communicates between different networks
- It provides WAN connectivity
- It does routing (Selects best paths)
- It works at Layer 3
- It can read IP Header
- It maintains IP routing table which contains best paths to destination networks

Types of Routers

- **Software Routers**
  - Dual home system with routing enabled
  - Windows 2003 server, Linux Server
- **Hardware Routers**
  - Hardware device - Dedicated routing
  - Cisco router

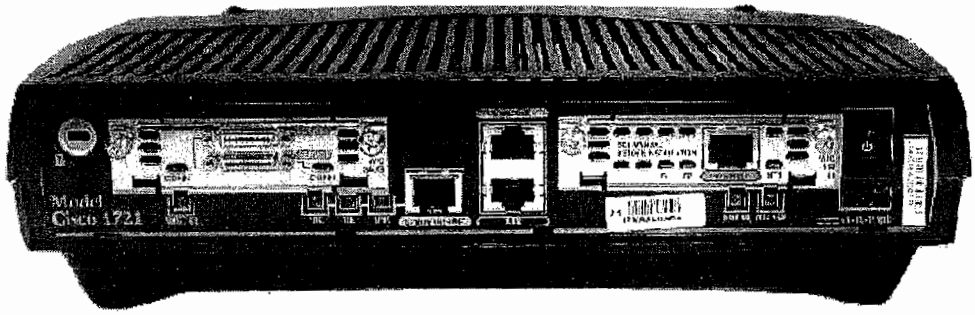
Router manufacturers

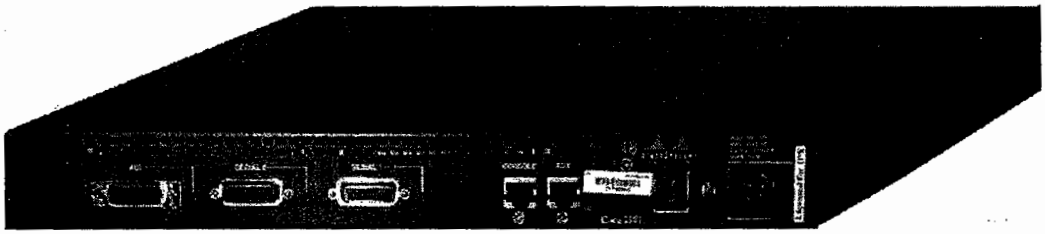
- CISCO
- DAX
- JUNIPER
- LINKSYS
- NOKIA
- D-LINK
- ZYXEL
- 3COM

Types of Cisco Routers:

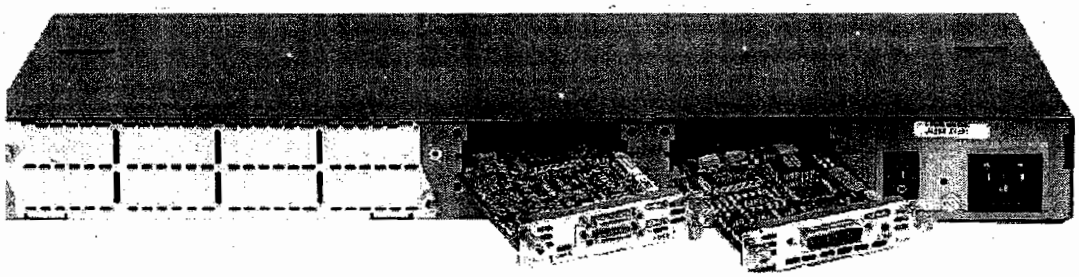
- **Fixed Routers**
  - Fixed No of interfaces
  - No hardware upgrade
  - Cheaper
- **Modular Routers**
  - No of interfaces can be increased
  - Hardware upgrade is possible
  - Costlier

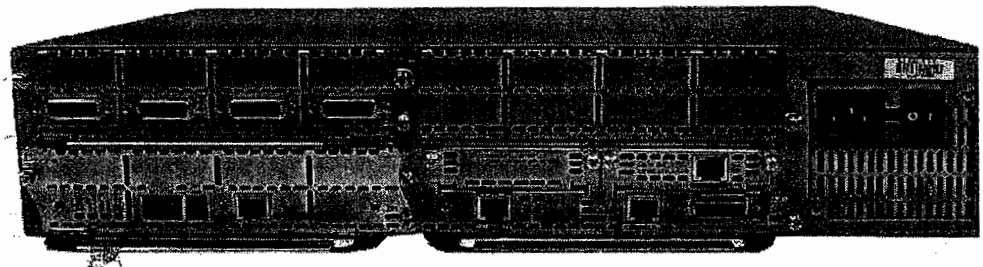
Fixed Routers





Modular Routers



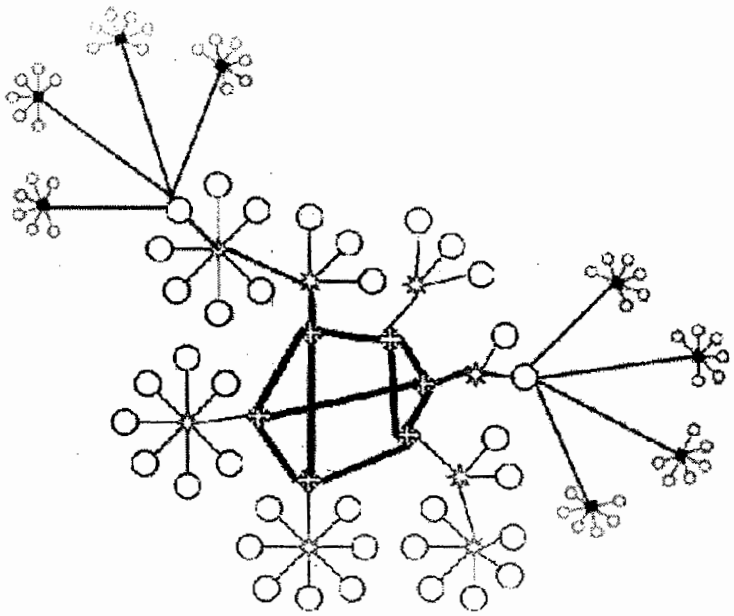


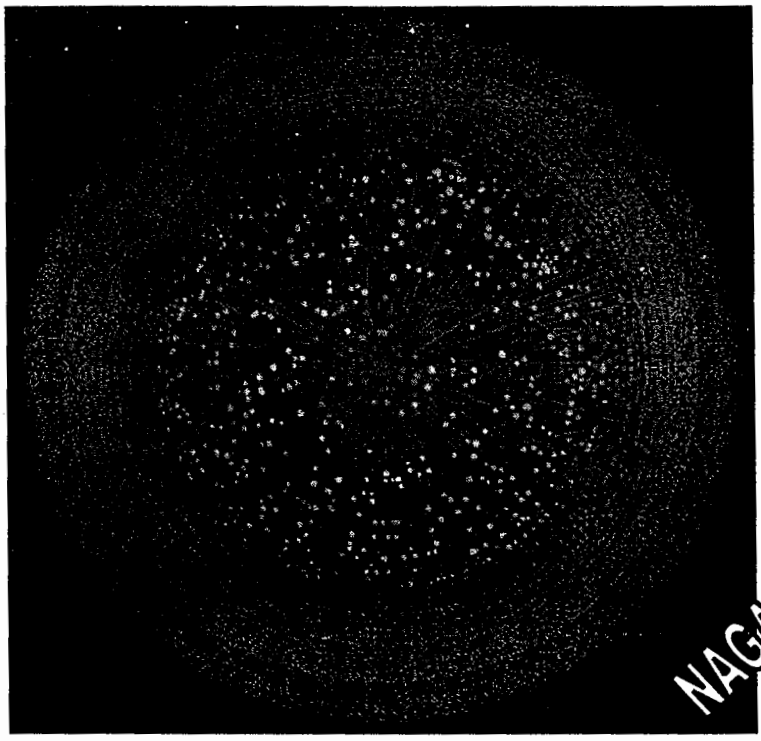
NAGABABU

Internet Structure:

Internet centers, companies are connected to local ISPs (Internet Service Provider)
Local ISPs are connected to Regional ISPs
Regional ISPs are connected to National ISPs
National ISPs are connected to Global ISPs

Data flow rate is low at Local ISPs and gradually increases till Global ISPs
The devices at Global ISPs must be high end devices

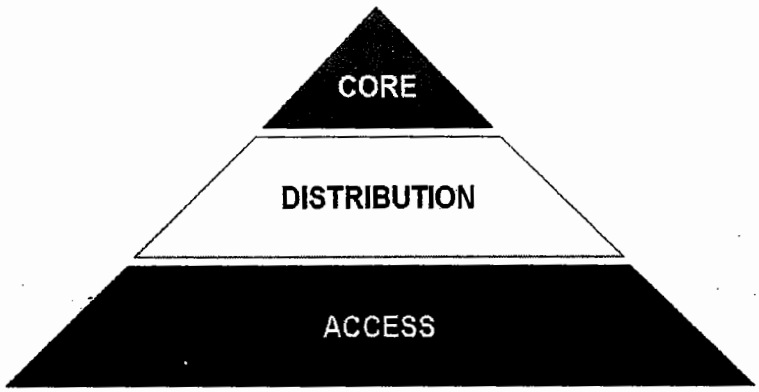




Cisco 3-Layer hierarchy

Cisco routers are divided into 3 categories based on hardware capabilities

- Access Layer
- Distribution Layer
- Core Layer



Access Layer:

- Used for small Organizations
- Data transfer speed is low
- Local ISPs
- 1600, 1700, 2500 series routers
- Fixed Routers

Distribution Layer:

- Used for medium level Organizations
- Data transfer speed is medium
- Regional ISPs, National ISPs
- 2600, 2800, 3600 series routers
- Modular Routers

Core Layer:

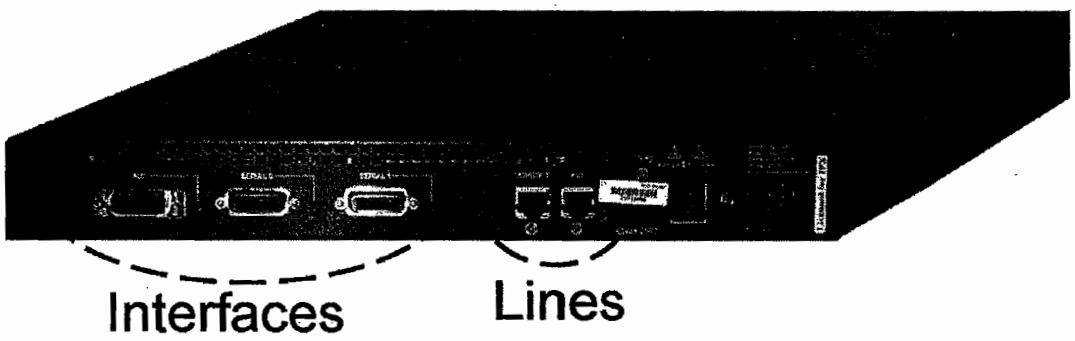
- Used for medium level Organizations
- Data transfer speed is high
- National ISPs , Global ISPs
- 6000, 7000, 10000, 12000 series routers
- Modular Routers

Router Model Numbers:

2500 series has following models

- 2501
- 2503
- 2509
- 2511
- 2520

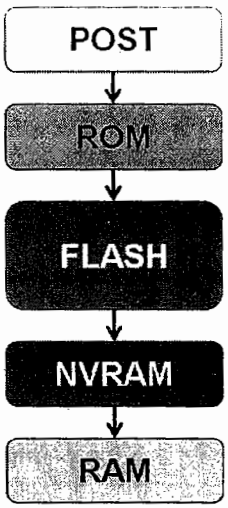
Router Physical Structure - External Components - Cisco 2501



Router Ports:

- **Interfaces: For data transfer**
  - LAN interfaces: For LAN connectivity
    - e 0, e 1, e 2 , fa 0/0, fa 0/1
  - WAN interfaces: For WAN connectivity
    - s 0, s1, s2, s3 , s 0/0, s 0/1
- **Lines: For Router management**
  - Physical lines: Exist on router
    - Console 0 (local), aux 0 (remote)
  - Logical lines: Not exist on router
    - Vty 0 4 (also called as telnet)

Router internal Components - Boot sequence



POST:

- Power On Self Test
- Hardware Checkup
- RAM, CPU, Interfaces diagnosis

ROM:

- Read only Memory
- Bootstrap loader / Mini IOS
- Finds the location of complete IOS

FLASH:

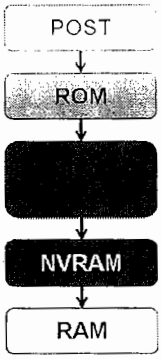
- Complete IOS Image
- May have multiple IOS Images
- Router operates with single IOS
- Eg: c2500-d-l.120-7.bin

NVRAM:

- Non Volatile Random Access Memory
- Permanent configuration
- File name : Startup-config
- Router always uses nvram configuration when booting
- Router copies NVRAM into RAM

RAM:

- Random Access Memory
- Temporary configuration
- File name : Running-config
- Router copies NVRAM into RAM
- Router always works with RAM configuration only



If there is no valid IOS, router uses bootstrap loader

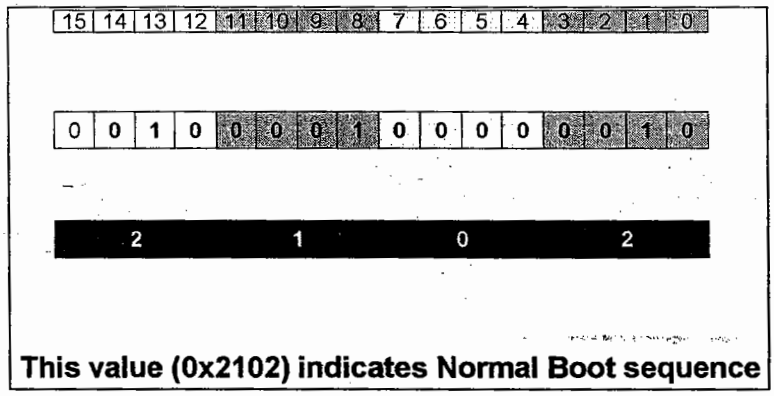
The prompt would be **Router (boot)>** or **Rommon>**

Router Boot Sequence:

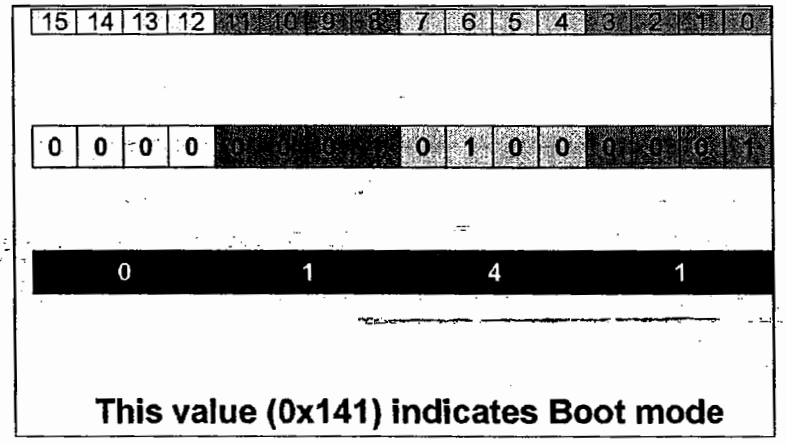
- Router boot sequence depends on Configuration Register Value
- This value decides the router to use IOS or Bootstrap loader
- This value decides the router to use NVRAM or not
- Configuration Register value is 16 Bit value

What is Configuration Register?

- 16 Bit register which is used to define the boot sequence
- Every bit in the register has specific purpose



This value (0x2102) indicates Normal Boot sequence



This value (0x141) indicates Boot mode

What is the Operating System in Router?

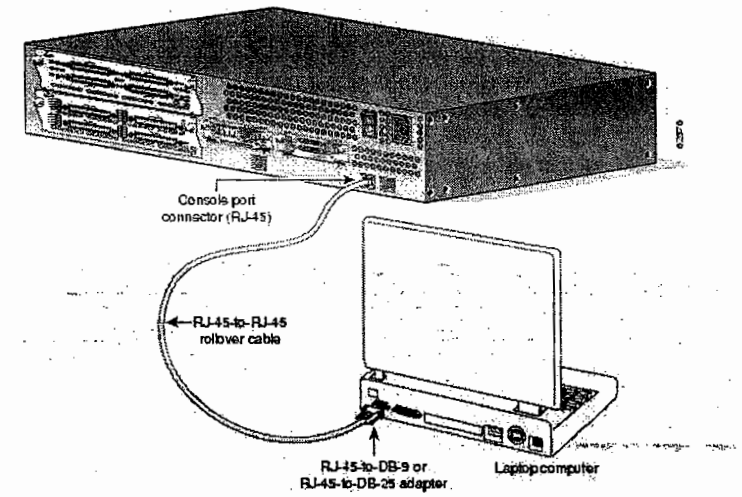
- Router works on IOS
- **IOS - Internetwork Operating System**
- Router works on singe IOS Image File

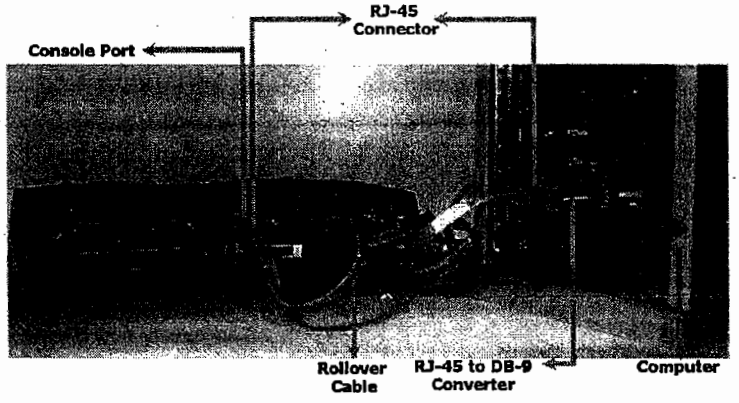
Router Configuration is Mandatory?

- Configuration is mandatory
- Router works if it is configured properly
- Don't connect the router without configuration
- Router is not a zero touch configuration device

How to configure the router?

- Use console 0 to configure the router for the first time
- Connect roll over cable between **console 0** on router & **COM1 port** on the computer/laptop





Emulation Software:

➢ One application is required on the laptop/system to access IOS and

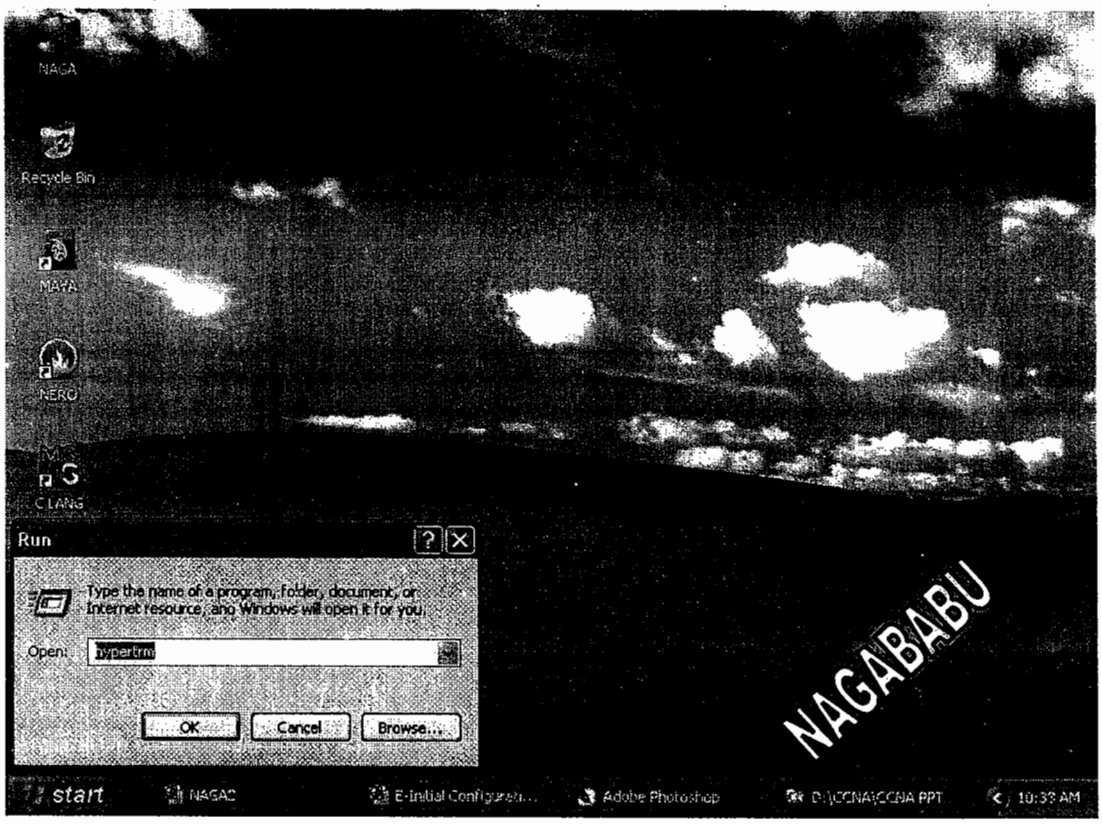
to configure the router. This software is called emulation software

Eg: hyper terminal, Putty

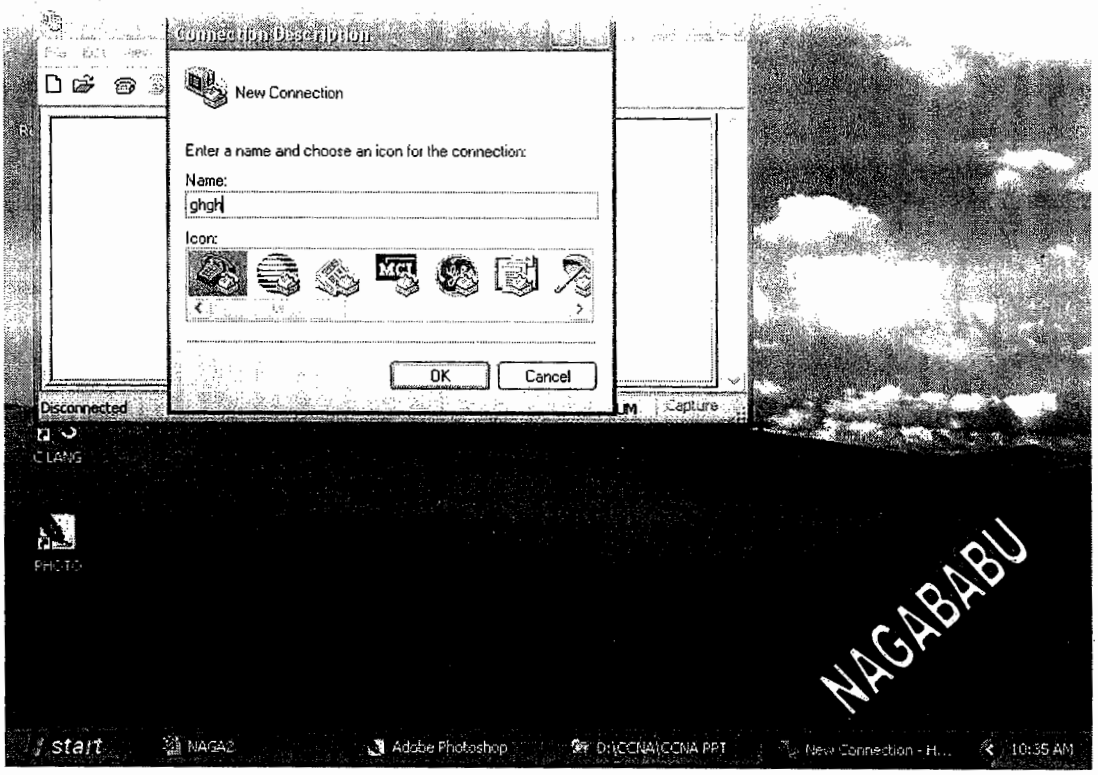
Hyper terminal is the default program in Windows XP

How to access Hyper terminal:

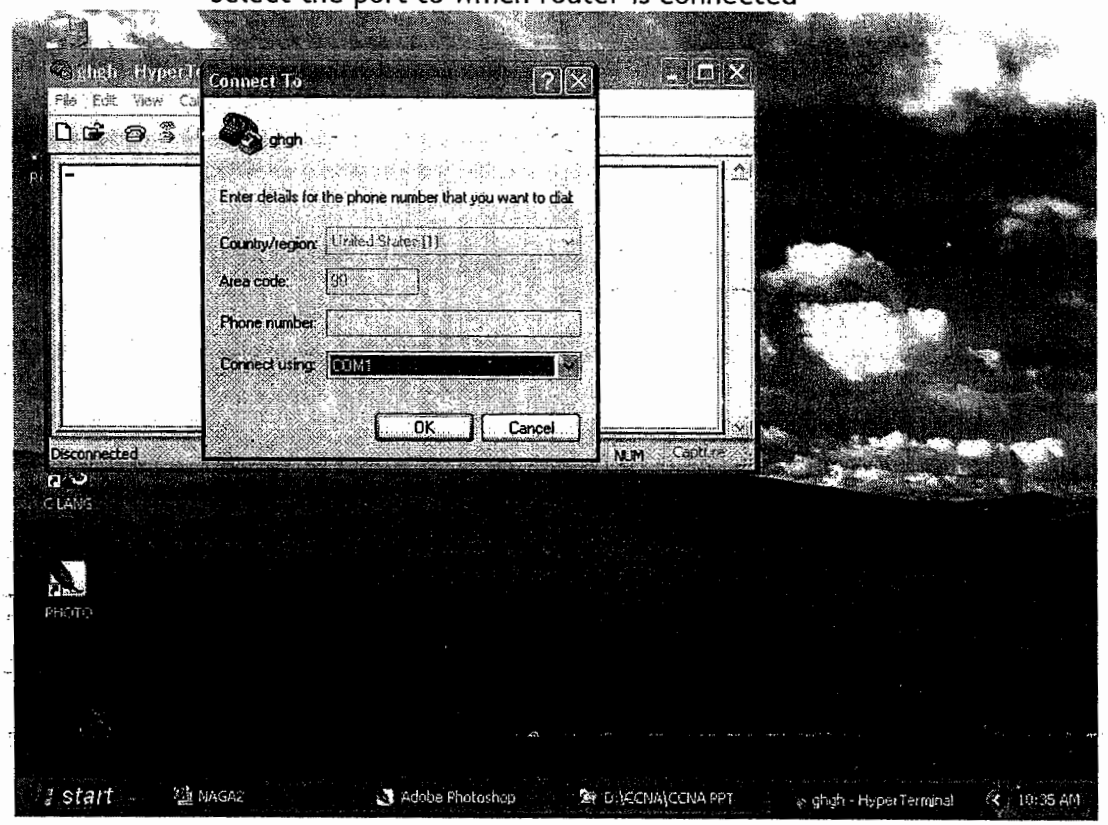
- ➢ Start -> Programs -> Accessories -> communications -> hyper terminal (or)
- ➢ Type **hypertrm** at run prompt



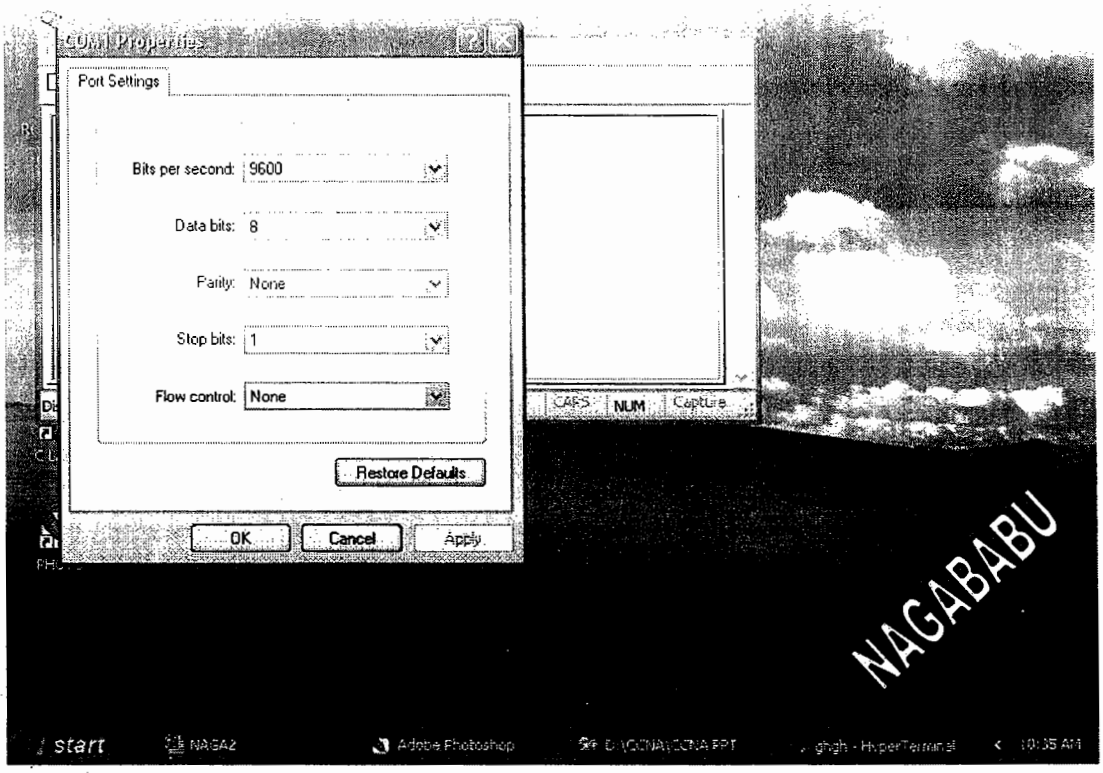
Type a name for the session



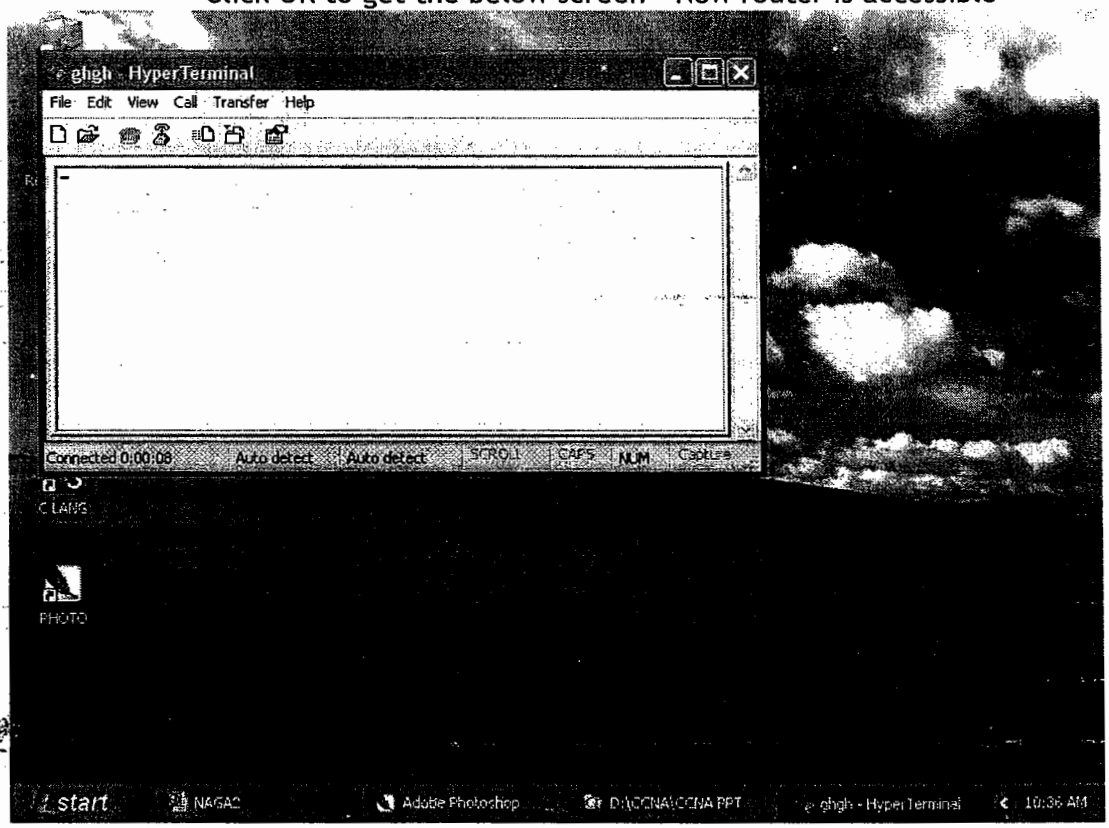
Select the port to which router is connected



Select Restore defaults (Cisco router accepts default settings)



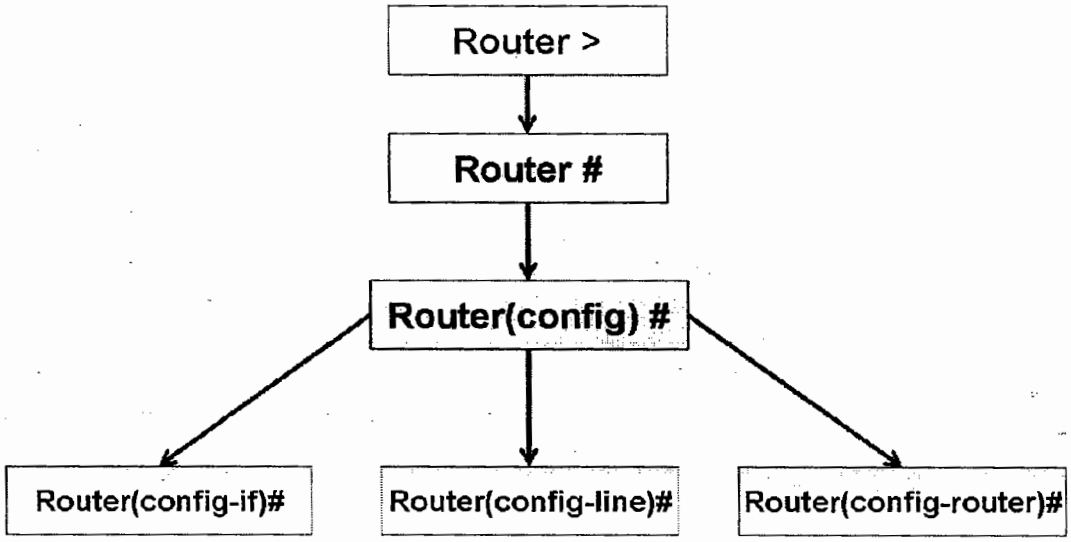
Click OK to get the below screen - Now router is accessible



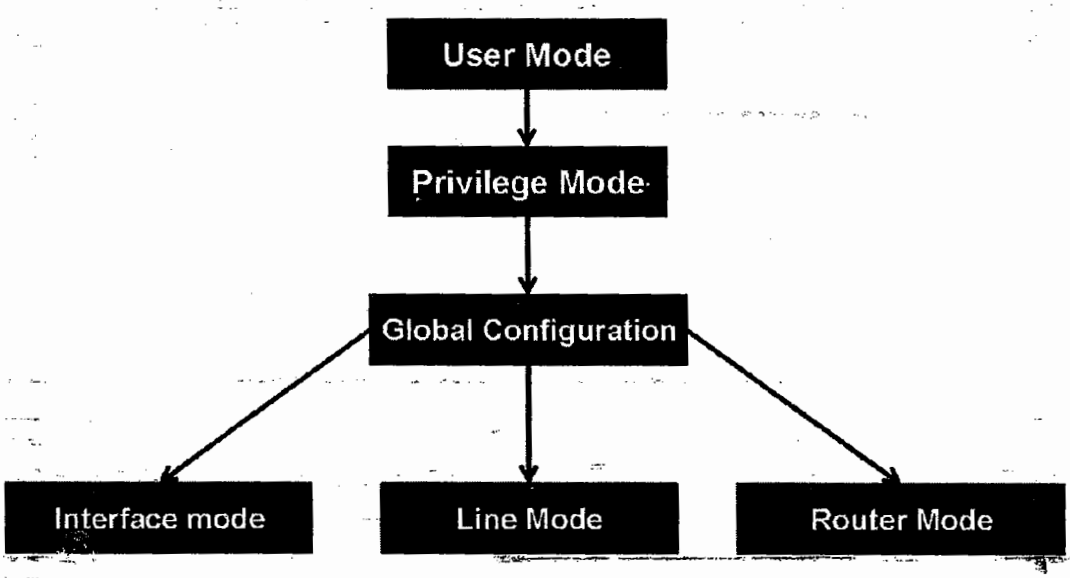
Router Modes

- Cisco IOS has different modes
- Every mode has its own functionalities
- Cisco IOS is CLI (command line interface) based
- Commands are mode specific

Router Modes - Prompts:



Router Modes - Names:

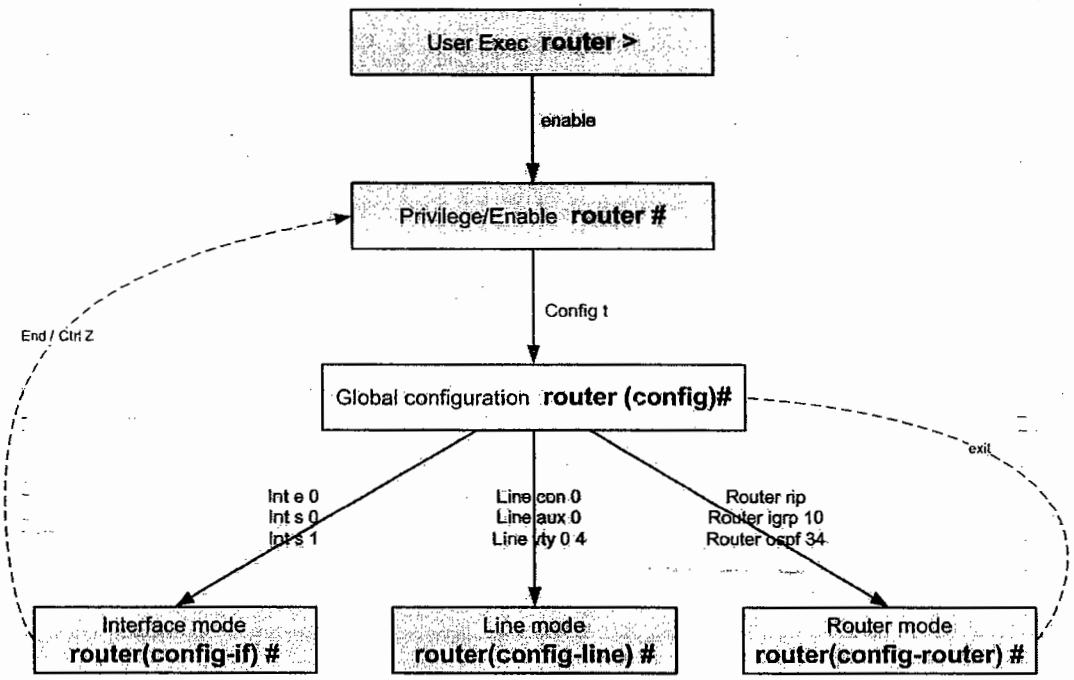


NAGABABU

Router Modes - Navigation

ROUTER MODES

NAGABABU



Router Modes - Functionalities - Commands

1. User mode: Router>

Functions:

- To check the Connectivity
- It has limited functionality

Commands:

Command	Function
telnet ip	to telnet into a device
Ping ip	to check connectivity
Traceroute ip	to trace the path
Enable	to enter privilege mode

2. Privilege mode: Router#

Functions:

- View Entire configuration
- Backup & Recovery

Commands:

Command	Function
Show run	to see temporary configuration
Show start	to see permanent configuration
Show int s 0	displays info about interface s 0
Show ip route	displays routing table
Show version	displays version, config register value
Show flash	displays flash contents /ios image
Show ip protocols	displays configured routing protocols
Show ip int brief	displays interface ip information
Show controllers serial 0	displays hardware info of s0 -DCE/DTE
Reload	restarts the router
Config t	enters into global configuration mode
Copy run start / Write	save RAM contents to NVRAM

3. Global configuration mode: Router (config)#

Functions:

- To do entire configuration of router (globally)

Commands:

Command	Function
No logging console	turns off logging (logging messages)
Hostname *hostname*	changes the hostname
Enable password *cisco*	set privilege mode password
Enable secret *cisco*	set secret password for privilege mode
Ip routing	Enables routing table
No ip routing	Disables routing table
Config-register 0x2102	Sets the config register value to 2102
Ip route	To configure static route
Int s 0	to interface mode
Int s 1	
Int e 0	
Line con 0	to line mode
Line aux 0	
Line vty 0 4	
Router rip	to router mode
Router eigrp 23	
Router ospf 56	

4. Interface mode: Router (config-if)#

Functions:

- Configuration of interfaces

Commands:

Command	Function
ip address <*ip*><*subnetmask*>	to configure ip address for interface
no shutdown	activate the interface
encapsulation *hdlc*	set L2 encapsulation for wan ports
clock rate *64000*	set clock rate (DCE interfaces)
bandwidth *64*	set interface bandwidth

5. Line mode: Router(config-line)#

Functions:

- Authentication of lines
- Configuring console 0, aux 0, vty 0 4

Commands:

Command	Function
Password <password>	To configure password for line
login	To set login type

6. Router mode: Router (config-router)#

Functions:

- **To configure dynamic routing protocols**

Commands:

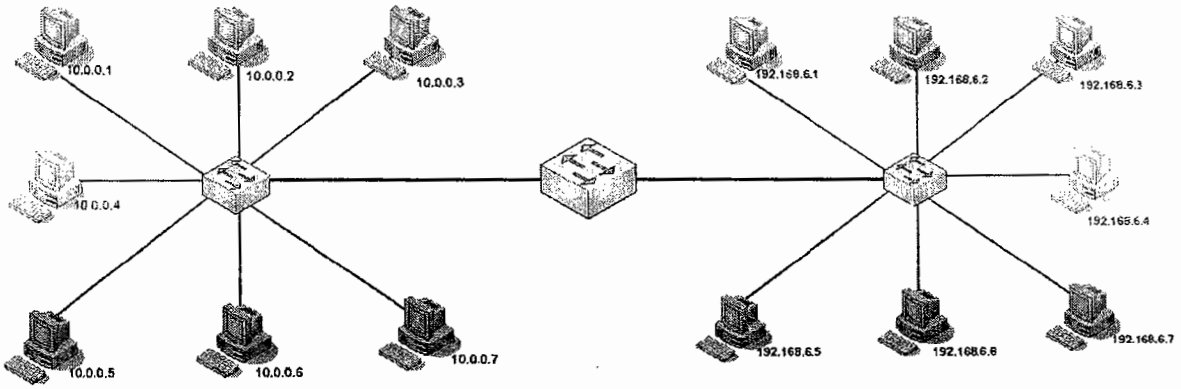
Command	Function
Network <network address>	To advertise networks in routing
Auto-summary	Auto summarize networks

Tips in IOS usage:

- Use "?" to get the help
- Use "tab" to get the complete command after entering unique characters of a command
- Use "no" keyword along with the command for reverse results
- Use "q" or "Ctrl+C" to terminate output

Router & Switch properties

Switch in LAN:



We can't talk to Second group

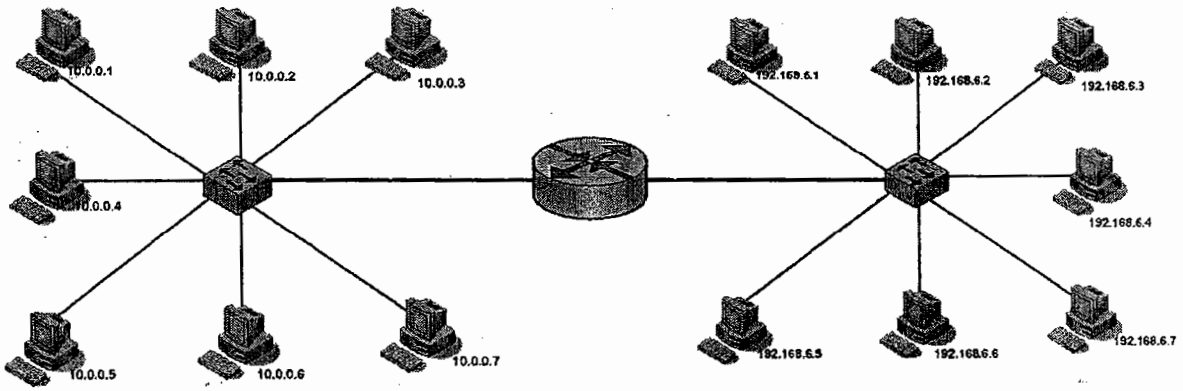
Connected to switch

We can't talk to first group

Connected to switch

NAGABABU

Router in LAN:



Now we can talk to each other

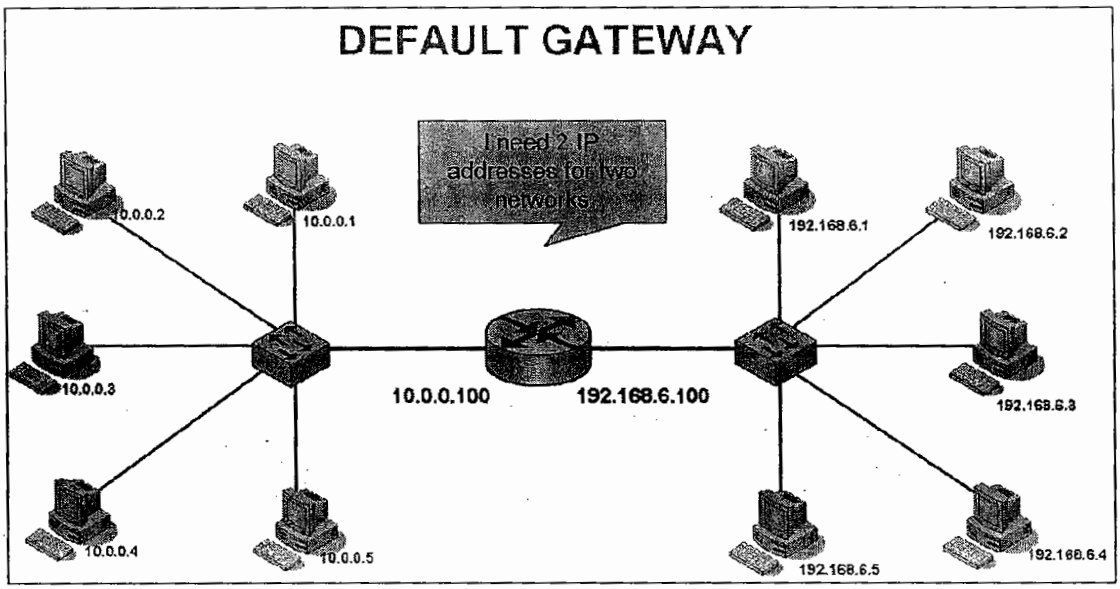
Connected to router

Now we can talk to each other

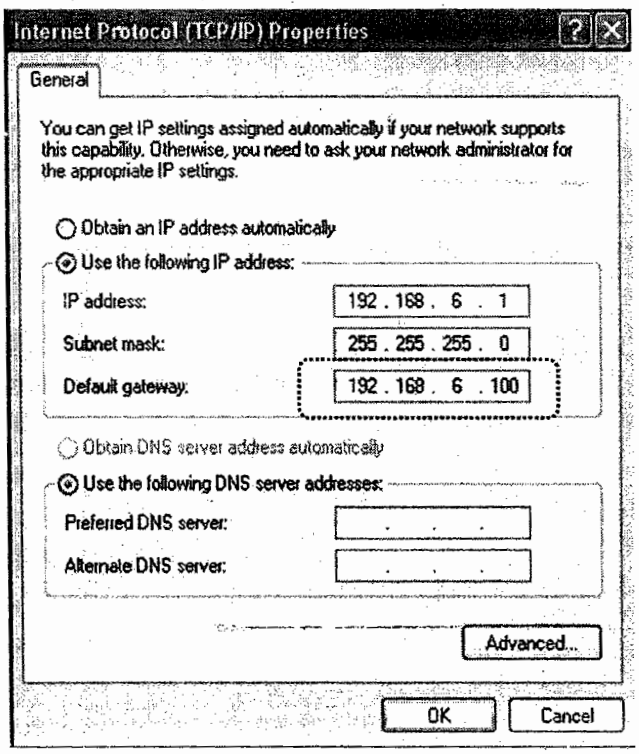
Connected to router

What is Default Gateway?

- Entry or Exit point of a network
- This is the IP address used to communicate with different networks
- Default gateway is typically the ip address of router
- Default gateway is not required within the network
- Default gateway must be configured in every computer to communicate with different networks



How to assign the Default Gateway?



NAGABABU

What is Routing Table?

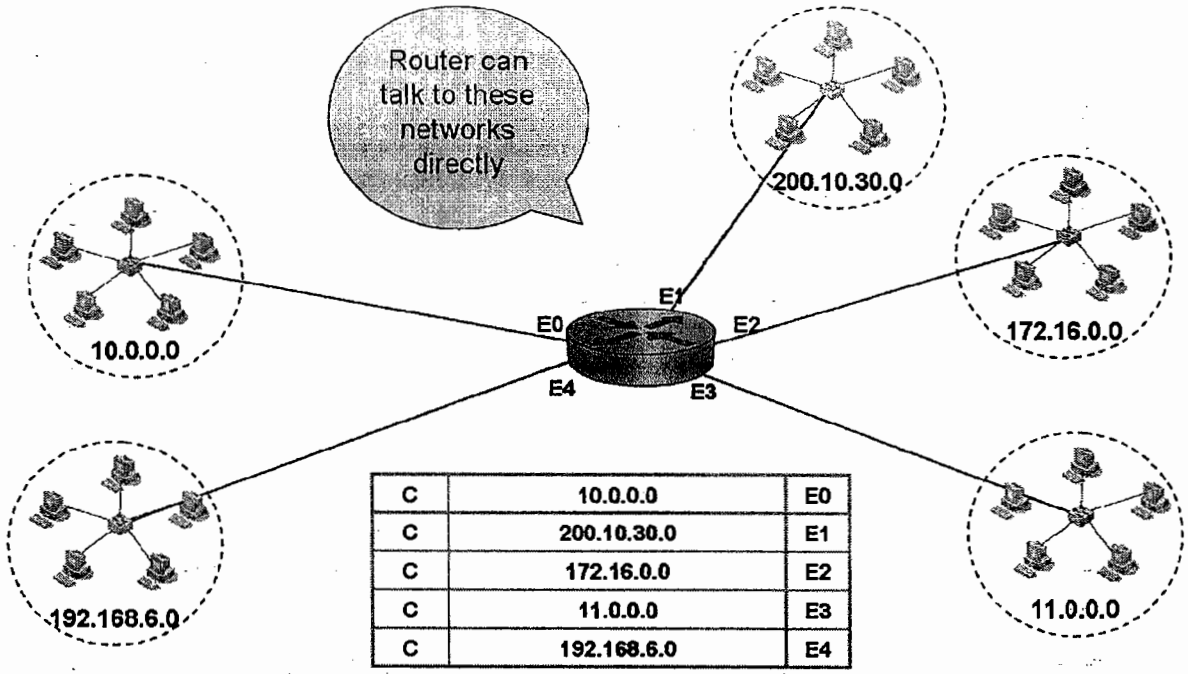
- The list of networks that router knows
- Router can reach only those networks which are presented in its routing table
- Routing table contains only the best paths to reach networks
- Routing table includes network address, exit interface, metric

This is my routing table, so I can reach these networks

C	172.17.0.0	E0
C	12.0.0.0	S0
C	11.0.0.0	S1
S	192.168.6.0	S1
S	192.168.5.0	S0

NAGABABU

By default routing table contains directly connected networks information

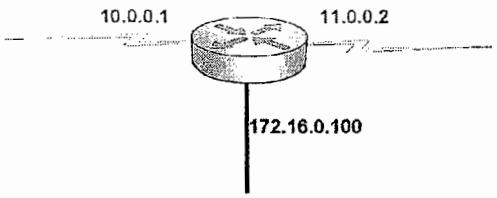


C	10.0.0.0	E0
C	200.10.30.0	E1
C	172.16.0.0	E2
C	11.0.0.0	E3
C	192.168.6.0	E4

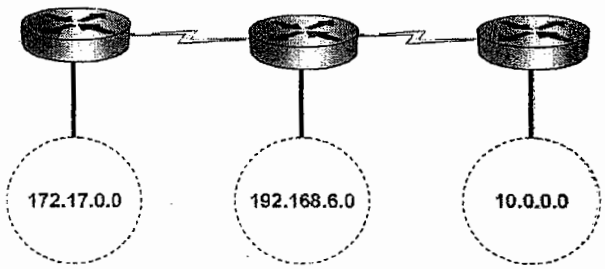
Network design Rules

- All the connected interfaces must be different networks
- All the LANs must be different networks
- LAN and default gateway must be in same network
- Two directly connected interfaces must be same network

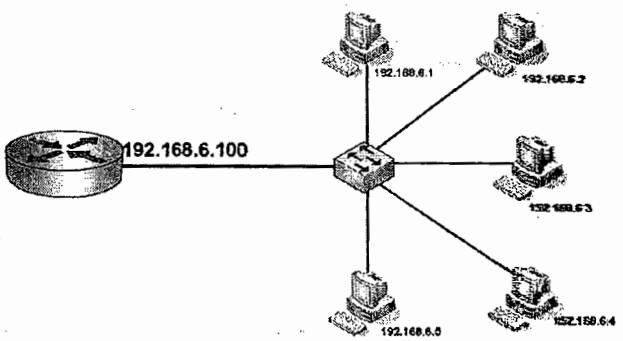
All the connected interfaces must be different networks



All the LANs must be Different Networks



LAN and default gateway must be in same network

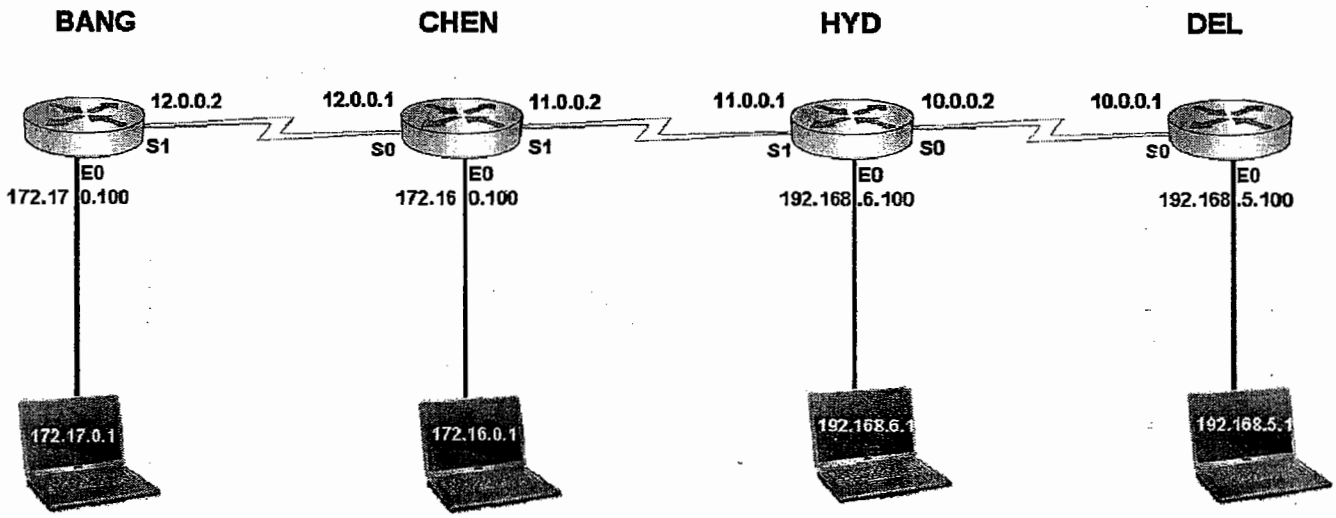


NAGABABU

Two directly connected interfaces must be same network

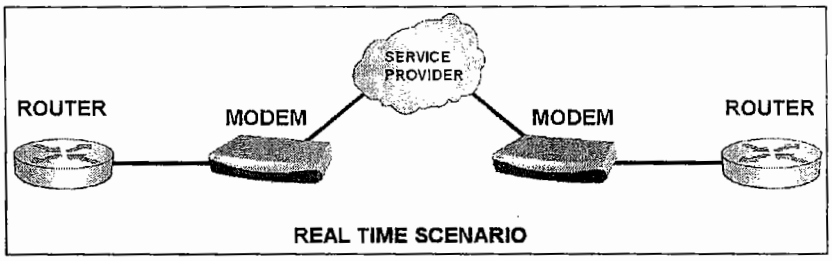
NAGABABU

LAB NETWORK

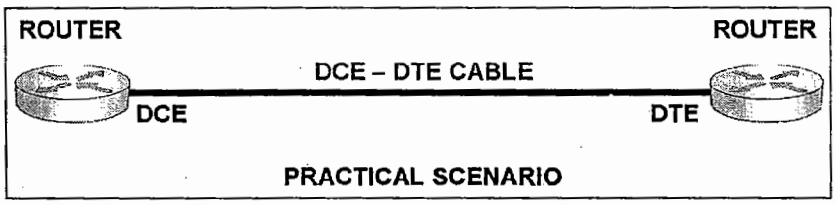


DCE - DTE

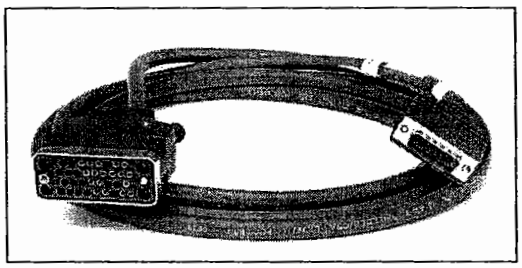
- Data synchronization is required on WAN links (on serial interfaces)
- In real time scenarios this synchronization is provided by modems connected to serial interfaces
- Modems generate clock rate to synchronize the data between WAN ports

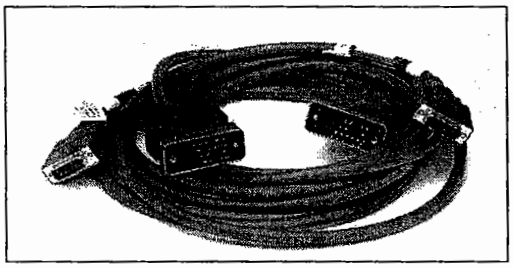


- Because of no modems in practical scenarios, this clock rate need to be generated by one of the router in the point to point connectivity
- **DCE-DTE** cable is used in practical scenarios between routers
- If one router is connected to DCE end, the second router will be connected to DTE end (In point to point connectivity, if one end is DCE, other end is DTE



DCE- DTE cables:





DCE- DTE differences:

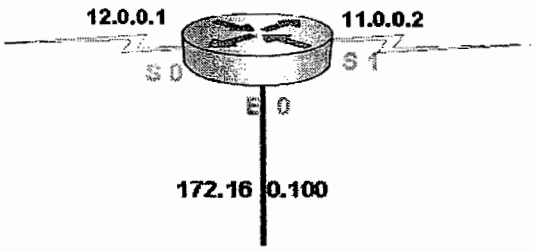
DCE	DTE
Data communication Equipment	Data terminating equipment
Master	SLAVE
Generates clock rate (64000 Hz)	Accepts clock rate
Dial up, leased line modems CSU/DSU	PC, Router

Router Initial Configuration

- Router is not a zero-touch configuration device
- It must be configured with proper IP Addresses. If not, it won't work

Router Configuration includes 4 steps

1. Hostname change
2. Secure router
3. Configure interfaces
4. View and Save



1. Hostname Change:

```
Router> enable
Router# config t
Router(config)# hostname CHEN
```

2. Secure Router:

```
CHEN(config)# enable password cisco
CHEN(config)# enable secret ccna

CHEN(config)# line con 0
CHEN(config-line)# password cisco
CHEN(config-line)# login
CHEN(config-line)# exit

CHEN(config)# line aux 0
CHEN(config-line)# password cisco
CHEN(config-line)# login
CHEN(config-line)# exit

CHEN(config)# line vty 0 5
CHEN(config-line)# password cisco
CHEN(config-line)# login
CHEN(config-line)# exit
CHEN(config)# service password-encryption
CHEN(config)# exit
```

NAGABABU

3. Configure interfaces:

```
CHEN(config)# interface s 1
CHEN(config-if)# ip address 11.0.0.2  255.0.0.0
CHEN(config-if)# no shutdown
CHEN(config-if)# bandwidth 64
CHEN(config-if)# clock rate 64000
CHEN(config-if)# encapsulation hdlc

CHEN(config)# interface s 0
CHEN(config-if)# ip address 12.0.0.1  255.0.0.0
CHEN(config-if)# no shutdown
CHEN(config-if)# bandwidth 64
CHEN(config-if)# clock rate 64000
CHEN(config-if)# encapsulation ppp

CHEN(config)# interface e 0
CHEN(config-if)# ip address 172.16.0.100  255.255.0.0
CHEN(config-if)# no shutdown
CHEN(config-if)# exit
CHEN(config)# exit
```

4. View & Save:

```
CHEN# show ip int brief
CHEN# show run
CHEN# show ip route
CHEN# show interfaces

CHEN# copy run start
CHEN# write
```

Routing

What is Routing?

- **Communication between two different networks**

- Router can communicate with those networks presented in its Routing Table
- By default Routing table maintains connected networks Information
- If there is no information in the routing table about a destination network router drops all the packets for that destination
- So Destination networks must be added to the routing table
- **This process is called ROUTING**

Router(Config)# no ip routing	**- To disable routing process**
Router(Config)# ip routing	**- To enable routing process**
Router# show ip route	**- To view routing table**

Routing can be done in two ways

- Static Routing
- Dynamic Routing

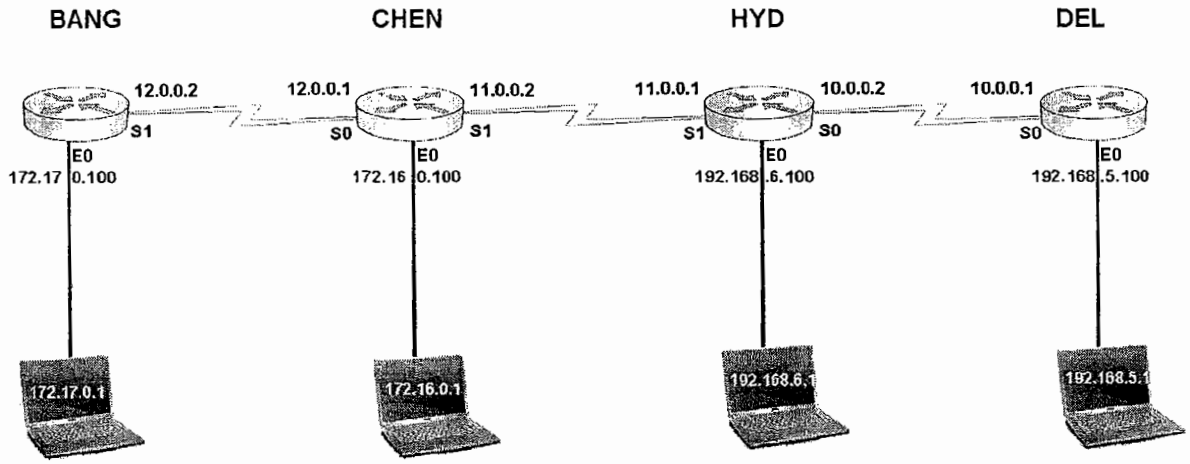
Static Routing:

- Manual Routing
- Administrative work is more
- It is suitable for small networks
- Suitable for Fixed networks
- Administrative distance is **1**
- Single change may effect all the router configuration

Dynamic Routing:

- Routing happens dynamically (auto) by using routing protocols
- Administrative work is less
- It is suitable for large networks
- Suitable for Scalable networks
- Administrative distance depends on routing protocol
- Single change will not effect the remaining routers configuration
- Destination network information is obtained and updated Automatically

Static Routing



Syntax:

Router(Config)# ip route <network> <subnetmask> <exit int>

(Or)

Syntax:

Router(Config)# ip route <network> <subnetmask> <nexthop>

Exit Interface:

Interface on the home router which forwards the data to the next router

Next hop IP address:

Interface IP Address of next immediate router towards the destination

NAGABABU

Static Routing configuration

Bang:

```
Bang> enable
Bang# show ip route
Bang# config t
Bang(config)# no ip routing
Bang(config)# ip routing
Bang(config)# ip route 172.16.0.0 255.255.0.0 s 1
Bang(config)# ip route 192.168.6.0 255.255.255.0 s 1
Bang(config)# ip route 192.168.5.0 255.255.255.0 s 1
Bang(config)# exit
Bang # show ip route
```

Chen:

```
Chen> enable
Chen# show ip route
Chen# config t
Chen(config)# no ip routing
Chen(config)# ip routing
Chen(config)# ip route 172.17.0.0 255.255.0.0 s 0
Chen(config)# ip route 192.168.6.0 255.255.255.0 s 1
Chen(config)# ip route 192.168.5.0 255.255.255.0 s 1
Chen(config)# exit
Chen # show ip route
```

Hyd:

```
Hyd> enable
Hyd# show ip route
Hyd# config t
Hyd(config)# no ip routing
Hyd(config)# ip routing
Hyd(config)# ip route 172.17.0.0 255.255.0.0 s 1
Hyd(config)# ip route 172.16.0.0 255.255.0.0 s 1
Hyd(config)# ip route 192.168.5.0 255.255.255.0 s 0
Hyd(config)# exit
Hyd # show ip route
```

Del:

```
Del> enable
Del# show ip route
Del# config t
Del(config)# no ip routing
Del(config)# ip routing
Del(config)# ip route 172.17.0.0 255.255.0.0 s 0
Del(config)# ip route 172.16.0.0 255.255.0.0 s 0
Del(config)# ip route 192.168.6.0 255.255.255.0 s 0
Del(config)# exit
Del # show ip route
```

Static default Routing configuration

- It is a form of static routing
- Used when destination information is not available
- Used as the last option
- Configured at "End points" /stub network (with one exit interface)
- In default routing destination network address is 0.0.0.0
- Used in Internet configuration

Syntax:

Router(Config)# ip route 0.0.0.0 0.0.0.0 <exit int>

0.0.0.0 Network with 0.0.0.0 subnet mask value represents all ip addresses from 0.0.0.0 to 255.255.255.255

Bang, Del routers are the end points/stub routers in the LAB network

Bang:

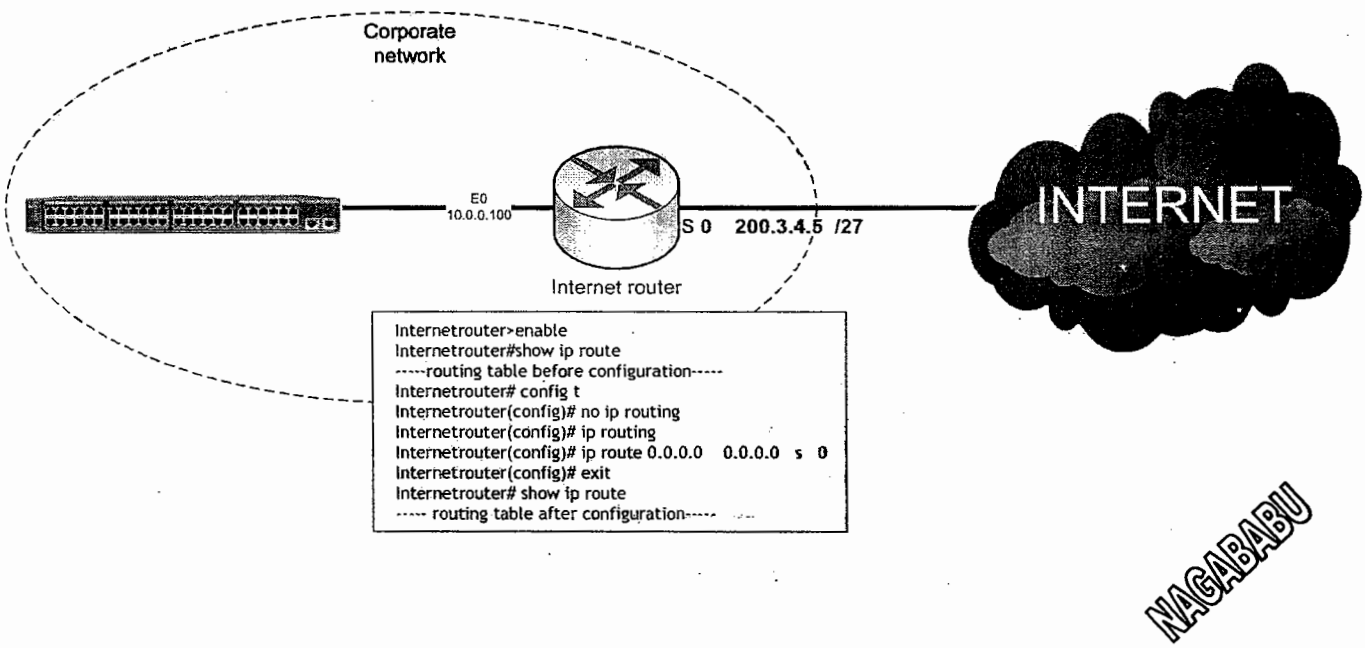
```
Bang> enable
Bang# show ip route
Bang# config t
Bang(config)# no ip routing
Bang(config)# ip routing
Bang(config)# ip route 0.0.0.0  0.0.0.0 s 1
Bang(config)# exit
Bang # show ip route
```

Del:

```
Del> enable
Del# show ip route
Del# config t
Del(config)# no ip routing
Del(config)# ip routing
Del(config)# ip route  0.0.0.0  0.0.0.0 s 0
Del(config)# exit
Del # show ip route
```

NAGABABU

Internet Router Configuration (Static default Routing)




```
Internetrouter>enable
Internetrouter#show ip route
-----routing table before configuration-----
Internetrouter# config t
Internetrouter(config)# no ip routing
Internetrouter(config)# ip routing
Internetrouter(config)# ip route 0.0.0.0    0.0.0.0  s  0
Internetrouter(config)# exit
Internetrouter# show ip route
----- routing table after configuration-----
```

NAGABABU

Dynamic Routing

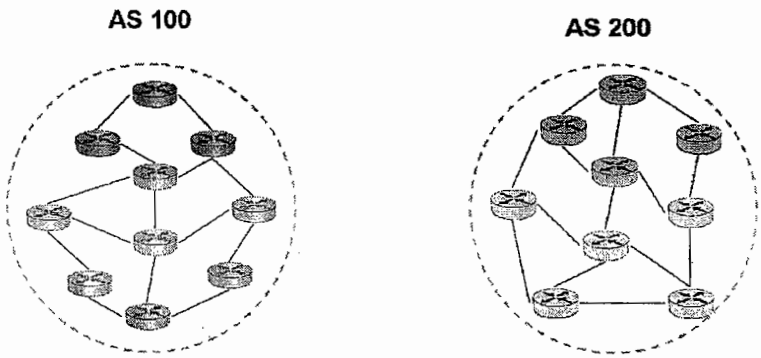
- Dynamic routing can be done through dynamic Routing Protocols

- Dynamic routing protocols choose the best path. Do not carry data
- Routed protocols carry the data in the chosen path
- Dynamic routing protocols are divided into two categories

  - IGP
  - EGP

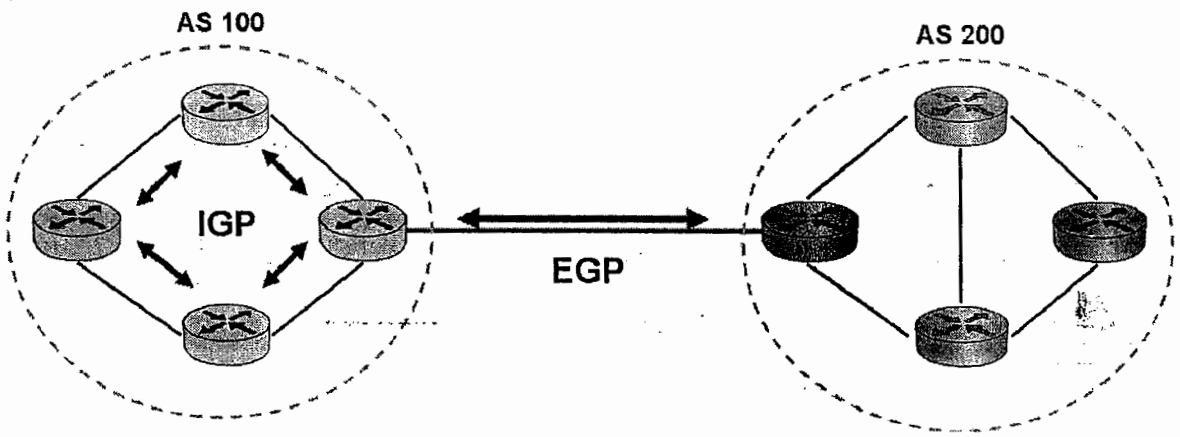
What is Autonomous System (AS)?

- Autonomous system is the collection of networks with single Administration
- Collection of networks with common routing policies
- Autonomous system is 16 bit value
- Range is 1-65535



IGP & EGP protocols:

- IGP category protocols work within AS
- EGP category protocols work between AS



Intra domain routing:

- Routing within AS
- Possible with IGP protocols

Inter domain routing:

- Routing between AS
- Possible with EGP protocols

Routing Protocols

IGP		EGP	
Distance vector	RIP	Path vector	BGP
	IGRP		
Link state	OSPF		
	ISIS		
Hybrid	RIPv2		
	EIGRP		

IGP Routing Protocols:

- IGP protocols are used to communicate with AS
- IGP protocols are divided into 3 categories
  - **Distance Vector**
    - RIP, IGRP
  - **Link State**
    - OSPF, ISIS
  - **Advanced Distance vector/ Hybrid**
    - Ripv2, EIGRP

- The goal of every routing protocols is same
- That is to select the best path
- But the selection criteria is different
- Every protocol has distinct characteristics in finding best paths

Category	Protocol	Expansion
Distance vector	**RIP**	Routing Information protocol
	IGRP	Interior Gateway Routing Protocol
Link state	**OSPF**	Open Shortest Path First
	ISIS	Intermediate system to Intermediate system
Hybrid	**EIGRP**	Enhanced IGRP
	RIPv2	RIP version 2

What is Administrative Distance (AD)?

- It is trustworthiness of a protocol
- It is a value given by cisco that indicates reliability
- It is 8 Bit value : Range 0 -255
- Lesser the AD better the routing protocol

Protocol	A.D.
Connected	0
Static route	1
RIP	120
IGRP	100
EIGRP	90
OSPF	110
ISIS	115
RIPV2	120
Eigrp summary	5
External BGP	20
EGP	140
ODR	160
External Eigrp	170
Internal BGP	200
Unknown	255

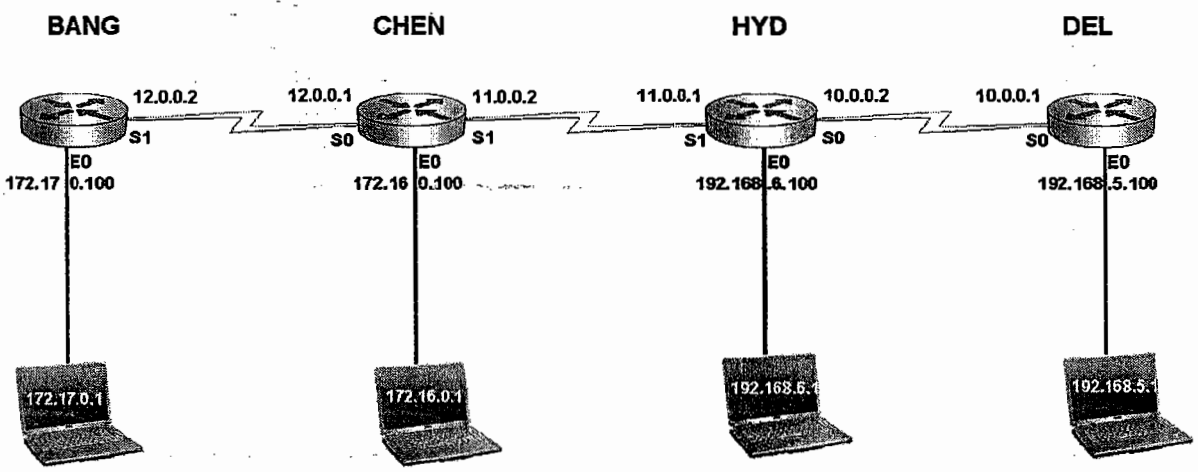
RIPv1

Routing Information Protocol (v1)

- AD=120 (Administrative distance)
- Metric=hop count (15=max, 16=invalid)
- Algorithm= bellman ford
- Update timer =30 sec
- Invalid timer =180 sec
- Hold down timer =180 sec
- Flush timer =240 sec
- Load balancing =6 equal paths
- Classful routing (subneting "not"supported)
- Open Standard

Syntax:

Router(config)# router rip
Router(config-router)# network <network Address>



NAGABABU

RIPv1 configuration

Bang:

```
Bang> enable
Bang# config t
Bang(config)# no ip routing
Bang(config)# ip routing
Bang(config)# router rip
Bang(config-router)# version 1
Bang(config-router)# network 172.17.0.0
Bang(config-router)# network 12.0.0.0
Bang(config-router)# end
Bang # show ip route
```

Chen:

```
Chen> enable
Chen# config t
Chen(config)# no ip routing
Chen(config)# ip routing
Chen(config)# router rip
Chen(config-router)# version 1
Chen(config-router)# network 172.16.0.0
Chen(config-router)# network 12.0.0.0
Chen(config-router)# network 11.0.0.0
Chen(config-router)# end
Chen # show ip route
```


Hyd:

```
Hyd> enable
Hyd# config t
Hyd(config)# no ip routing
Hyd(config)# ip routing
Hyd(config)# router rip
Hyd(config-router)# version 1
Hyd(config-router)# network 192.168.6.0
Hyd(config-router)# network 11.0.0.0
Hyd(config-router)# network 10.0.0.0
Hyd(config-router)# end
Hyd # show ip route
```

Del:

```
Del> enable
Del# config t
Del(config)# no ip routing
Del(config)# ip routing
Del(config)# router rip
Del(config-router)# version 1
Del(config-router)# network 192.168.5.0
Del(config-router)# network 10.0.0.0
Del(config-router)# end
Del # show ip route
```

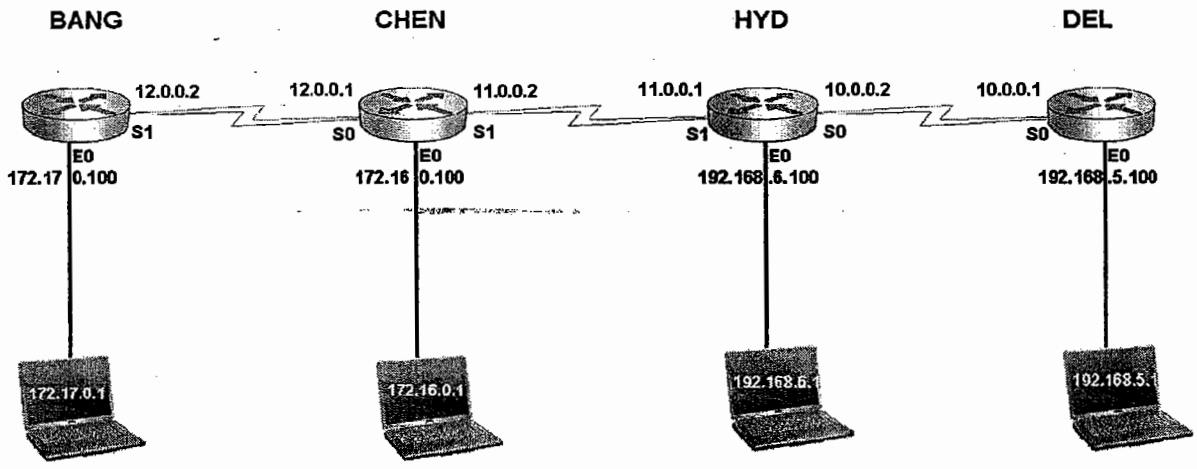
RIPv2

Routing Information Protocol (v2)

- AD=120 (Administrative distance)
- Metric=hop count (15=max, 16=invalid)
- Algorithm= bellman ford
- Triggered updates
- Multicast updates on 224.0.0.9
- Load balancing =6 equal paths
- Classless routing (subnetting supported)
- Open Standard

Syntax:

```
Router(config)#  router  rip
Router(config-router)# version 2
Router(config-router)# network  <network Address>
```



RIPv2 configuration

Bang:

```
Bang> enable
Bang# config t
Bang(config)# no ip routing
Bang(config)# ip routing
Bang(config)# router rip
Bang(config-router)# version 2
Bang(config-router)# network 172.17.0.0
Bang(config-router)# network 12.0.0.0
Bang(config-router)# end
Bang # show ip route
```

Chen:

```
Chen> enable
Chen# config t
Chen(config)# no ip routing
Chen(config)# ip routing
Chen(config)# router rip
Chen(config-router)# version 2
Chen(config-router)# network 172.16.0.0
Chen(config-router)# network 12.0.0.0
Chen(config-router)# network 11.0.0.0
Chen(config-router)# end
Chen # show ip route
```

Hyd:

```
Hyd> enable
Hyd# config t
Hyd(config)# no ip routing
Hyd(config)# ip routing
Hyd(config)# router rip
Hyd(config-router)# version 2
Hyd(config-router)# network 192.168.6.0
Hyd(config-router)# network 11.0.0.0
Hyd(config-router)# network 10.0.0.0
Hyd(config-router)# end
Hyd # show ip route
```


Del:

```
Del> enable
Del# config t
Del(config)# no ip routing
Del(config)# ip routing
Del(config)# router rip
Del(config-router)# version 2
Del(config-router)# network 192.168.5.0
Del(config-router)# network 10.0.0.0
Del(config-router)# end
Del # show ip route
```

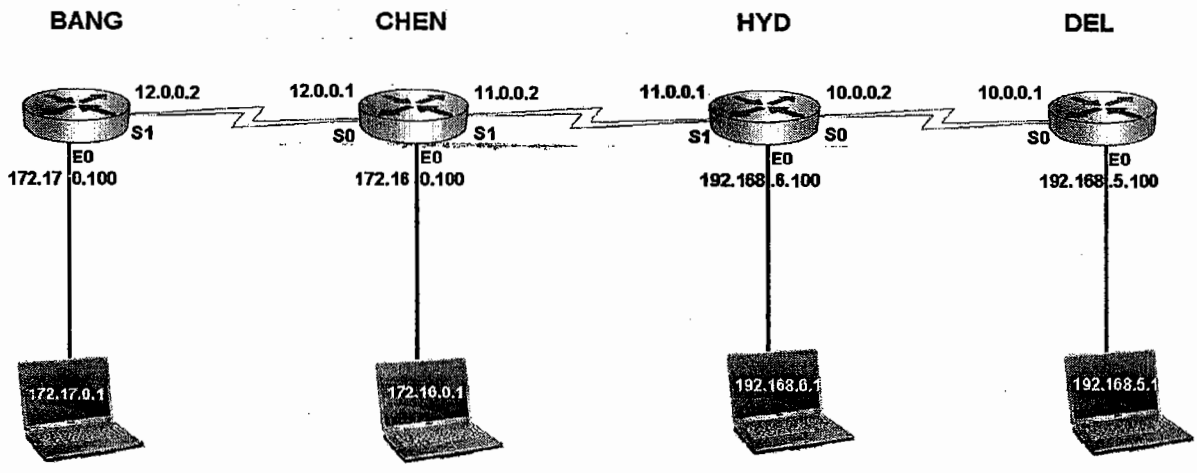
IGRP

Interior Gateway Routing Protocol

- AD=100
- Metric = 24 Bit Composite
  (Bandwidth+Delay+Load+Reliablity+MTU)
- Algorithm = Bellman Ford
- Update timer = 90 Sec
- Invalid timer = 270 Sec
- Hold On timer = 280 Sec
- Flush timer = 630 Sec
- Load balancing = 4-6 equal /unequal paths
- Classful routing (subnetting "not" supported)
- Cisco proprietary

Syntax:

Router(config)# router igrp <AS No>
Router(config-router)# network <network Address>



NAGABABU

IGRP configuration

Configure all routers in the same Autonomous system

IGRP communicates within AS only

Bang:

```
Bang> enable
Bang# config t
Bang(config)# no ip routing
Bang(config)# ip routing
Bang(config)# router igrp 87
Bang(config-router)# network 172.17.0.0
Bang(config-router)# network 12.0.0.0
Bang(config-router)# end
Bang # show ip route
```

Chen:

```
Chen> enable
Chen# config t
Chen(config)# no ip routing
Chen(config)# ip routing
Chen(config)# router igrp 87
Chen(config-router)# network 172.16.0.0
Chen(config-router)# network 12.0.0.0
Chen(config-router)# network 11.0.0.0
Chen(config-router)# end
Chen # show ip route
```


Hyd:

```
Hyd> enable
Hyd# config t
Hyd(config)# no ip routing
Hyd(config)# ip routing
Hyd(config)# router igrp 87
Hyd(config-router)# network 192.168.6.0
Hyd(config-router)# network 11.0.0.0
Hyd(config-router)# network 10.0.0.0
Hyd(config-router)# end
Hyd # show ip route
```

Del:

```
Del> enable
Del# config t
Del(config)# no ip routing
Del(config)# ip routing
Del(config)# router igrp 87
Del(config-router)# network 192.168.5.0
Del(config-router)# network 10.0.0.0
Del(config-router)# end
Del # show ip route
```

EIGRP

Enhanced Interior Gateway Routing Protocol

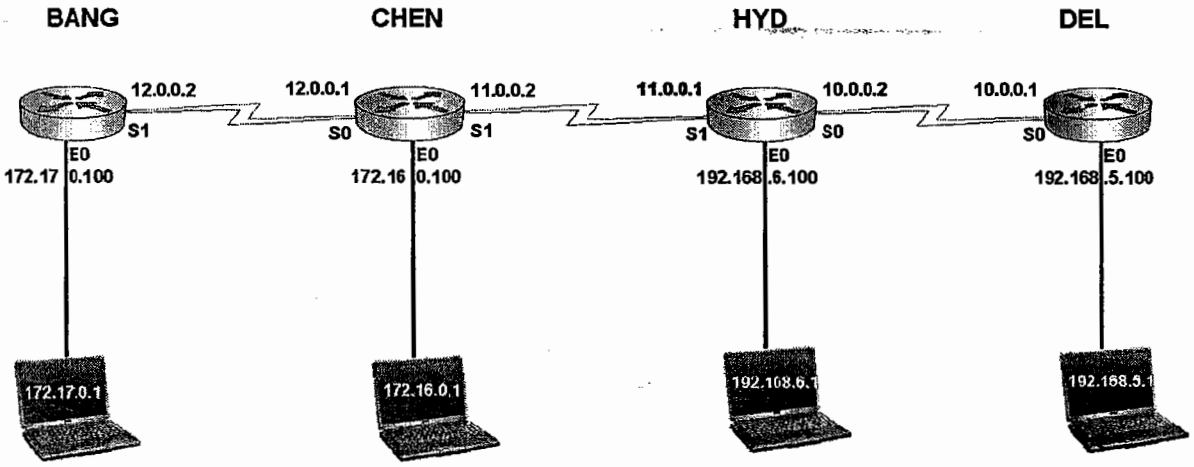
- AD=90
- Metric = 32 Bit Composite
  (Bandwidth+Delay+Load+Reliablity+MTU)
- Algorithm = DUAL (Diffused update algorithm)
- Hello timer = 5 sec
- It sends incremental, triggered updates
- Multicast updates on 224.0.0.10
- Load balancing = 4-6 equal /unequal paths
- It is Classless (Subnetting supported)
- Cisco proprietary

Syntax:

Router(config)# router eigrp <AS No>
Router(config-router)# network <network Address> <WCM>

What is WCM?

- Wild Card Mask
- Inverse of Subnet Mask Value
- Class A WCM : 0.255.255.255
- Class B WCM : 0.0.255.255
- Class C WCM : 0.0.0.255



EIGRP configuration

Configure all routers in the same Autonomous system

EIGRP communicates within AS only
Some older IOS versions may not support WCM for EIGRP

Bang:

```
Bang> enable
Bang# config t
Bang(config)# no ip routing
Bang(config)# ip routing
Bang(config)# router eigrp 145
Bang(config-router)# network 172.17.0.0  0.0.255.255
Bang(config-router)# network 12.0.0.0  0.255.255.255
Bang(config-router)# end
Bang # show ip route
```

Chen:

```
Chen> enable
Chen# config t
Chen(config)# no ip routing
Chen(config)# ip routing
Chen(config)# router eigrp 145
Chen(config-router)# network 172.16.0.0  0.0.255.255
Chen(config-router)# network 12.0.0.0   0.255.255.255
Chen(config-router)# network 11.0.0.0   0.255.255.255
Chen(config-router)# end
Chen # show ip route
```


Hyd:

```
Hyd> enable
Hyd# config t
Hyd(config)# no ip routing
Hyd(config)# ip routing
Hyd(config)# router eigrp 145
Hyd(config-router)# network 192.168.6.0  0.0.0.255
Hyd(config-router)# network 11.0.0.0   0.255.255.255
Hyd(config-router)# network 10.0.0.0   0.255.255.255
Hyd(config-router)# end
Hyd # show ip route
```

Del:

```
Del> enable
Del# config t
Del(config)# no ip routing
Del(config)# ip routing
Del(config)# router eigrp 145
Del(config-router)# network 192.168.5.0  0.0.0.255
Del(config-router)# network 10.0.0.0    0.255.255.255
Del(config-router)# end
Del # show ip route
```

OSPF

Open Shortest Path First

- AD=110
- Metric = cost (10^8/bandwidth in bps)
- Algorithm = DIJKSTRA or SPF
- Hello timer = 10 sec
- Dead timer = 40 sec
- Flush timer = 30 min
- Multicast updates on 224.0.0.5, 224.0.0.6
- It is Classless (Subnetting supported)
- Open Standard

Syntax:

Router(config)# router ospf <Process id No>
Router(config-router)# network <network> <WCM> area <area id>

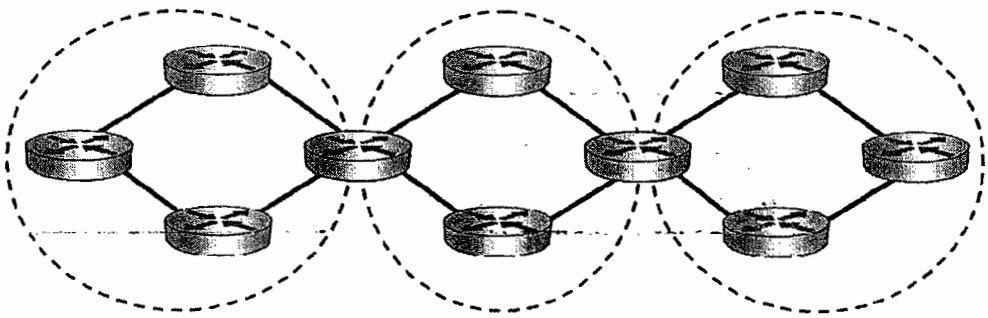
What is WCM?

- Wild Card Mask
- Inverse of Subnet Mask Value
- Class A WCM : 0.255.255.255
- Class B WCM : 0.0.255.255
- Class C WCM : 0.0.0.255

What is Area?

- Ospf maintains Link state information of every router to run SPF algorithm
- Router consumes more resources if more routers present in the network
- Areas are used to limit the link state database handled by router

- Area is a logical boundary for OSPF routers
- OSPF routers handle the link state information of all routers belong to same area
- Area Border Routers(ABR) route the data between different areas



What is Process id?

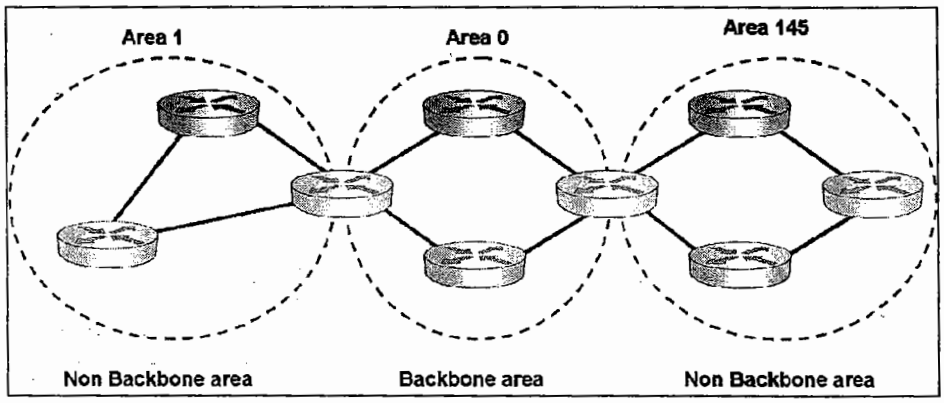
- OSPF can be configured as multiple instances on the same router
- Process id is used to identify the instance of OSPF
- It need not be the same on all routers
- Process id is 16 bit value
- Range : 1- 65535

OSPF areas:

- OSPF areas are basically two types

  - **Backbone area**
    - Area 0 is called as backbone area
    - Transit area between different areas

  - **Non Backbone area**
    - Areas other than Backbone area
    - All non backbone areas must be directly connected to area 0



OSPF Router Types:

- **Backbone routers**
- **Internal routers**
- **ABR**
- **ASBR**

Backbone routers

Routers in Back bone area (area 0).

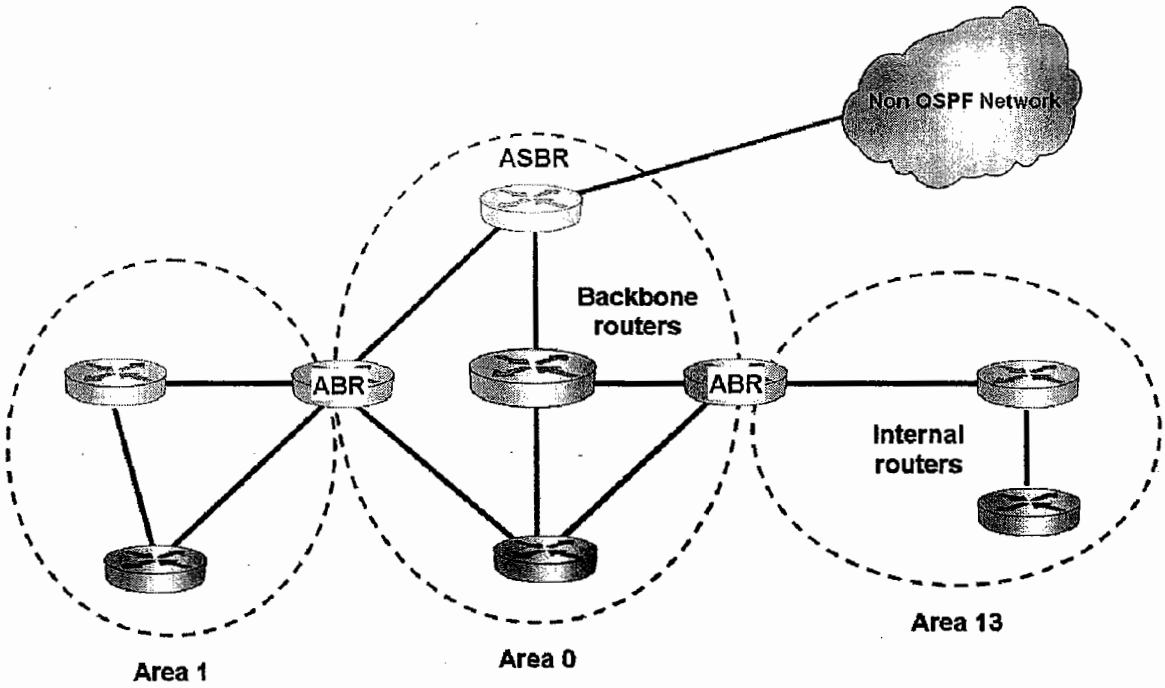
Internal routers

Routers belong to same area (backbone or non back bone).
Back bone routers are internal routers

ABR - Area Border Router

Router belongs to multiple areas.
For ABR, at least one interface must be in Back bone area

ASBR - Autonomous system boundary router
OSPF router that is connected to non OSPF network
ASBR is generally placed in area 0



OSPF area Types:

- Backbone area
- Stub Area
- Totally stub area
- NSSA (Not so stubby area)

LSA Types:

- LSA - Link state Advertisement
- It contains Link state information and networks available on that link

LSA Types	Name
1	Router LSA
2	Network LSA
3	Summary LSA
4	ASBR summary
5	AS external LSA
6	Multicast OSPF
7	NSSA LSA

OSPF configuration

Configure all routers in single area (Area 0)

Process id can be different from router to router

Bang:

```
Bang> enable
Bang# config t
Bang(config)# no ip routing
Bang(config)# ip routing
Bang(config)# router ospf 14
Bang(config-router)# network 172.17.0.0  0.0.255.255  area 0
Bang(config-router)# network 12.0.0.0  0.255.255.255  area 0
Bang(config-router)# end
Bang # show ip route
```

Chen:

```
Chen> enable
Chen# config t
Chen(config)# no ip routing
Chen(config)# ip routing
Chen(config)# router ospf 1456
Chen(config-router)# network 172.16.0.0  0.0.255.255  area 0
Chen(config-router)# network 12.0.0.0   0.255.255.255  area 0
Chen(config-router)# network 11.0.0.0   0.255.255.255  are 0
Chen(config-router)# end
Chen # show ip route
```


Hyd:

```
Hyd> enable
Hyd# config t
Hyd(config)# no ip routing
Hyd(config)# ip routing
Hyd(config)# router ospf 258
Hyd(config-router)# network 192.168.6.0  0.0.0.255  area 0
Hyd(config-router)# network 11.0.0.0   0.255.255.255  area 0
Hyd(config-router)# network 10.0.0.0   0.255.255.255  area 0
Hyd(config-router)# end
Hyd # show ip route
```

Del:

```
Del> enable
Del# config t
Del(config)# no ip routing
Del(config)# ip routing
Del(config)# router ospf 25696
Del(config-router)# network 192.168.5.0  0.0.0.255  area 0
Del(config-router)# network 10.0.0.0    0.255.255.255  area 0
Del(config-router)# end
Del # show ip route
```

Routing Protocols

Property	RIPv2	EIGRP	OSPF
Expansion	Routing information protocol	Enhanced interior gateway routing protocol	Open shortest path first
Category	Distance vector	Advanced distance vector	Link state
AD	120	90	110
IGP/EGP	IGP	IGP	IGP
Standard/proprietary	Open standard	Cisco	Open standard
Hop count	15 maximum	224=default : 255=maximum	255=maximum
Metric	Hop count	32-bit composite metric Bandwidth:Delay:realibility:load:MTU Bandwidth +Delay (default) [K1*bw]+[K2*bw/256-load]+[K3*delay] Multiplied by [K5/realibility+K4]	Cost = 10^8/bandwidth (bps)
Algorithm	Bellman ford	DUAL - diffused update algorithm	Dijikstra or SPF
Classful/classless	Classless	Classless	Classless
VLSM/Subnetting	Yes	Yes	Yes
Casting	Multicast	Multicast	Multicast
Multicast address	224.0.0.9	224.0.0.10	224.0.0.5 & 224.0.0.6
Packet types	Routing updates	Hello Update Query Reply Ack	Hello DBD Link state Request Link state Update Link state Ack
Updates	Triggered updates	Triggered and incremental updates	Incremental updates(Link state)
Tables	Routing table	Neighbor table (neighbors list) Topology table (topology info) Routing table (best routes)	Adjacency table (neighbors list) Database table (LS database/topology) Routing table (best routes)
Routed protocols	IP, IPX	IP, IPX, Appletalk	IP
Routing loops	Yes	Less chances	No
Fast convergence	No	Yes	Yes
Load balancing	Equal paths	Equal/unequal paths	Equal paths
IPv6 support	RIPng -RIP next generation	EIGRP for ipv6	OSPFv3
Routing table flag	R	D	O
Protocol No	520	88	89

NAGABABU

Router Backup & Recovery

- It is always better to take back up of router **startup-configuration** and **IOS Image** periodically

- If something happens to router/configuration, or if the router is replaced with a new one, it won't take much time to bring the router online (if backup is already taken)

Requirements for Backup & Recovery:

- TFTP server is required for backup & Recovery operations
- TFTP (Trivial FTP) is used to transfer the files
  - from router to system(Backup)
  - from system to router (Recovery)
- TFTP server is a small free software
- Install TFTP server program in the computer/laptop
- Always ensure TFTP server has connectivity with router while performing backup and recovery operations

How to take Backup?

Startup-configuration Backup:

```
Router# copy   startup-config   tftp
```


Running-configuration Backup:

```
Router# copy   running-config   tftp
```

IOS image /Flash Backup:

```
Router# copy   flash   tftp
```

How to Recovery?

Startup-configuration recovery:

```
Router# copy   tftp   startup-config
```

Flash recovery (or) IOS Image upgrade:

```
Router# copy   tftp   flash
```

```
Router(boot)# copy   tftp   flash
```

For backup and recovery operations router requires some information such as IOS image name, startup-config name, address of tftp server etc.
Enter the required information correctly

Router Password Recovery (2500 series)

Restart the router (power cycling / force restart)

Press ctrl+Break within one minute

```
> o/r   0x141          - setting config register value to 0x141
> i                    - Initialize
```

--- Router restarts---

```
Router(boot)> enable
Router(boot)# copy start run

Router(boot)# config t

Router(boot)(config)# no enable secret
Router(boot)(config)# no enable password

Router(boot)(config)# line con 0
Router(boot)(config-line)# no password
Router(boot)(config-line)# login
Router(boot)(config-line)# exit

Router(boot)(config)# config-register 0x2102
Router(boot)(config)# exit

Router(boot)# write
Router(boot)# reload
```


------ Router restarts------

```
Router>enable
Router#
```

Some routers display **Rommon>** prompt instead of **>**. Then use these commands

```
Rommon> confreg  0x141      (similar to  > o/r  0x141)
Rommon> reset               (similar to  > i)
```

Config - register values:

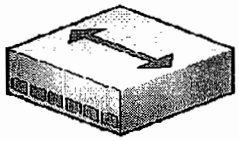
Config-register value	Purpose
0x2102	normal boot sequence
0x141	bootstrap loader/ boot mode

SWITCHES

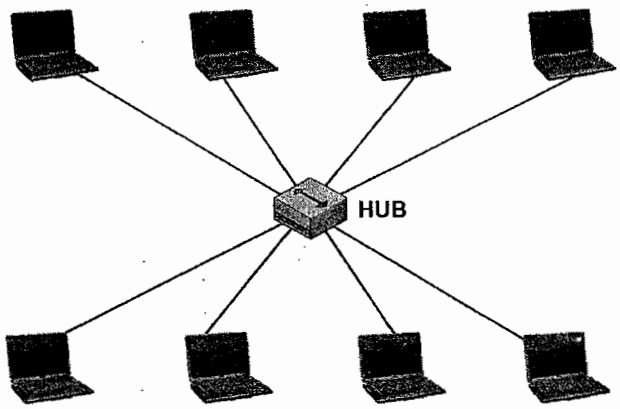
STUDENTNAME 105 NAGABABU

What is Hub?

- layer 1 device
- Dummy device (unintelligent)
- No technology to handle MAC information
- No memory
- It always broadcasts the data
- It gets the data from one port, regenerates the data and sends the data to all ports
- Also called as multi port repeater



How does Hub forward the data?



- It gets the data from one port
- It regenerates the same data and floods the data to all ports
- All systems receive the same data; but only one system accepts it

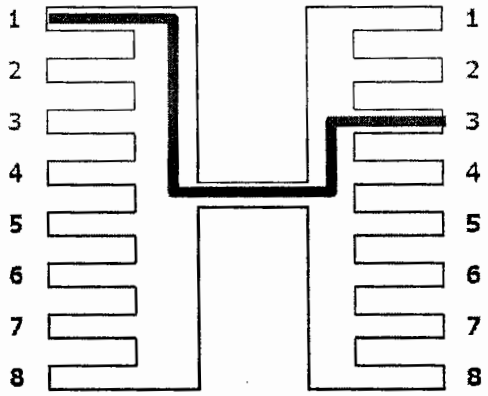
- Hub is shared media
- Hub supports only half duplex communication
- Hub cannot read **L2** header, **L3** header, **L4** Header

L2 Header contains source MAC, destination MAC information
L3 Header contains source IP, destination IP information
L4 Header contains source Port, destination Port information

What is CSMA ?

Carrier sense multiple Access

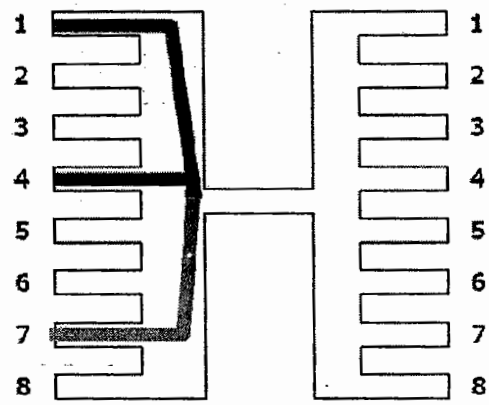
- First system looks for the carrier whether it is free or not
- If carrier is free it sends the data. If not it waits for some time
- Multiple systems can access single carrier with CSMA mechanism



What is collision ?

- Multiple ports may sense the free carrier and try to send the data exactly at same time
- If two ports want to send the data at same time the voltage levels from one port mix up with other ports. Finally data is collided.

- Collision is a situation where the data from one port collide with the data from other ports

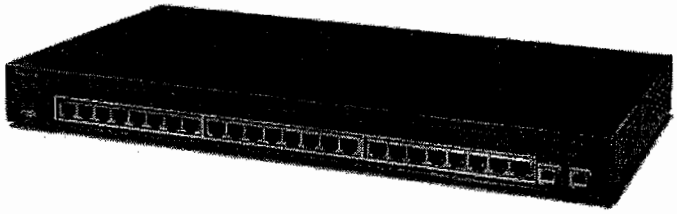


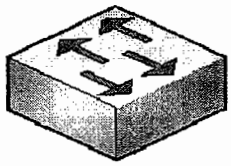
- CSMA/CD
  - Carrier sense multiple access - Collision detection
  - The mechanism used to detect collision

- CSMA/CA
  - Carrier sense multiple access - Collision avoid
  - The mechanism to avoid the collisions (by setting random timer)

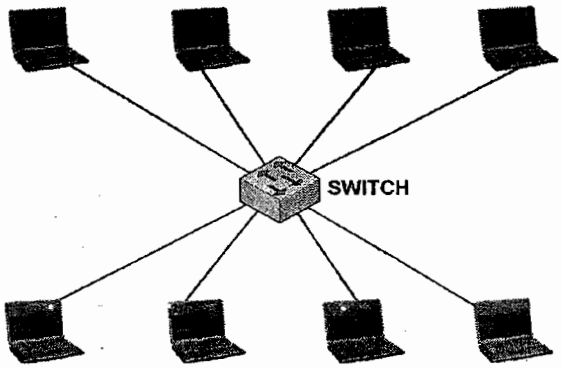
What is Switch?

- layer 2 device
- Intelligent device
- It has RAM to handle MAC information
- It maintains MAT (MAC Address Table) in RAM
- It forwards the with the help of MAT
- This is Hardware based device
- It has specialized hardware called ASICS
- Also called as multi port bridge (Bridge is software based device)





How does switch forward the data?



- It gets the data from one port
- It reads source MAC and destination MAC from L2 Header
- Looks into MAT, finds the outgoing port information
- Then unicasts the data to outgoing port
- If there is no outgoing port information then broadcasts the data

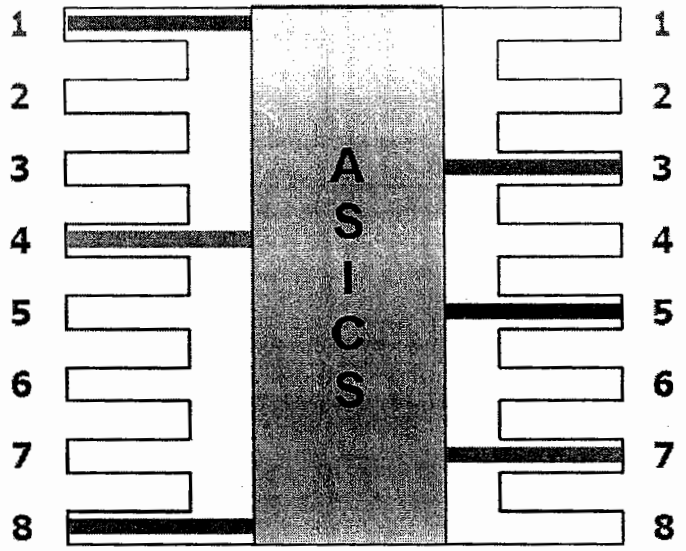
- It enters source MAC, incoming port information in MAT
- If MAT already has that entry refreshes it
- Switch can work at full duplex or half duplex
- Switch has dedicated circuits between ports (Every port has dedicated bandwidth)

- Switch can read L2 header. It can't read L3 header, L4 Header

L2 Header contains source MAC, destination MAC information L3 Header contains source IP, destination IP information L4 Header contains source Port, destination Port information

What is ASICS?

- Application Specific Integrated Circuits
- ASICS is specialized hardware designed for faster switching
- Switch has dedicated circuits between ports
- Every port has dedicated bandwidth
- Multiple ports can communicate at same time
- This hardware design is called **micro segmentation**



What is MAT?

- MAC Address Table
- MAT contains port information, associated MAC information, entry type, vlan membership
- Switch maintains MAT in CAM (content addressable Memory)
- CAM is a part of Switch RAM
- If the switch is rebooted, MAT becomes blank
- Switch automatically builds MAT
- MAT entry expires dynamically, if that port is idle for 5 minutes

Vlan	Type	MAC ADDRESS	PORT
1	Dynamic	128c.34ba.92de	Fa 0/1
1	Dynamic	Ae6c.78b3.9a08	Fa 0/2
1	Dynamic	bc56.78f5.780a	Fa 0/4
10	Dynamic	1e5c.9005.89ae	Fa 0/15
10	Dynamic	45ab.fb70.8903	Fa 0/9
46	Dynamic	Bd6c.89ac.6709	Fa 0/6
95	Dynamic	1cc0.458f.f9b1	Fa 0/3
95	Dynamic	780b.89ef.9012	Fa 0/18

What is collision domain?

- Collision domain is the bounded area of a collision
- It defines the area that a collision can span

What is broadcast domain?

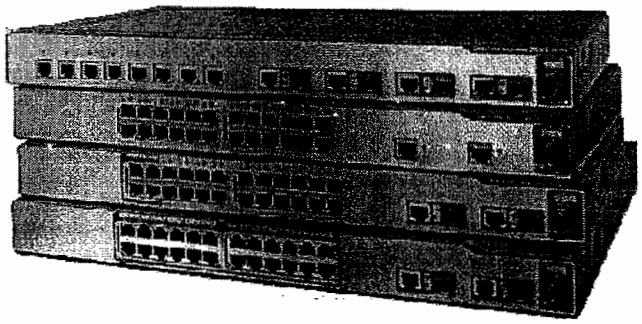
- Broadcast domain is the bounded area of a broadcast
- It defines the area that a broadcast can span

Device	Collision domain	Broadcast domain
Hub	1	1
Switch	No of Ports	1 (No of vlans)
Router	No of ports	No of ports

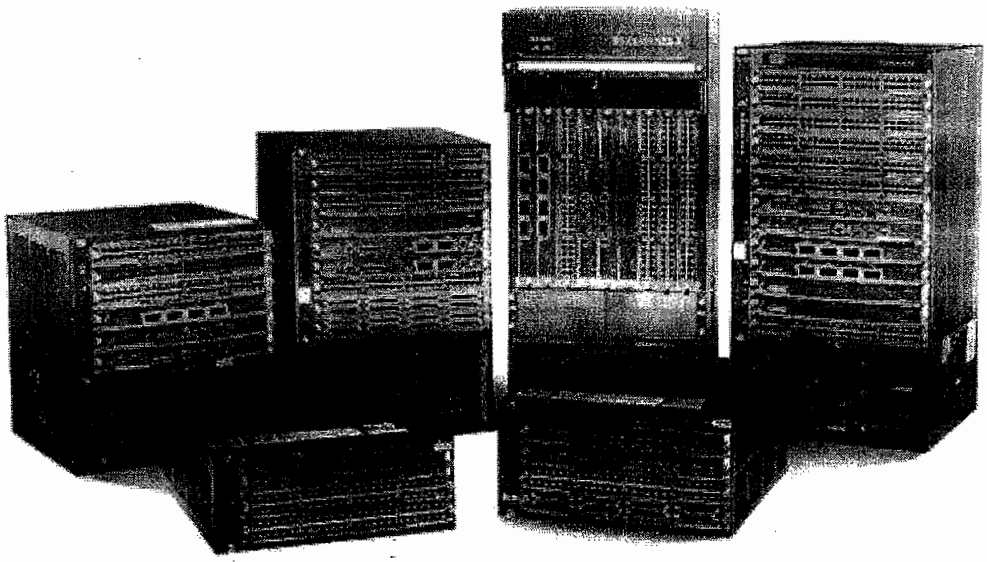
Types of Cisco Switches:

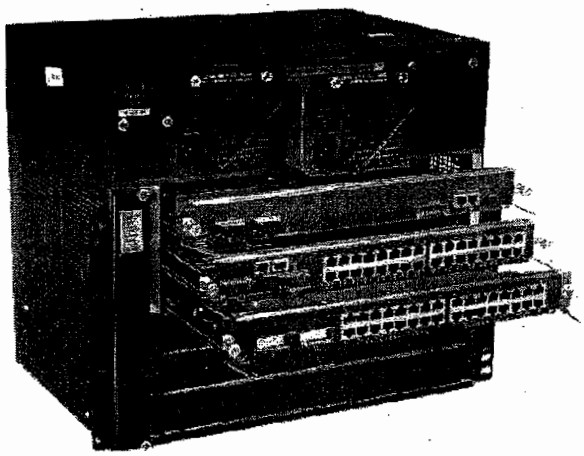
- **Fixed Switches**
  - Fixed No of interfaces
  - No hardware upgrade
  - Cheaper
- **Modular Switches**
  - No of interfaces/modules can be increased
  - Hardware upgrade is possible
  - Costlier

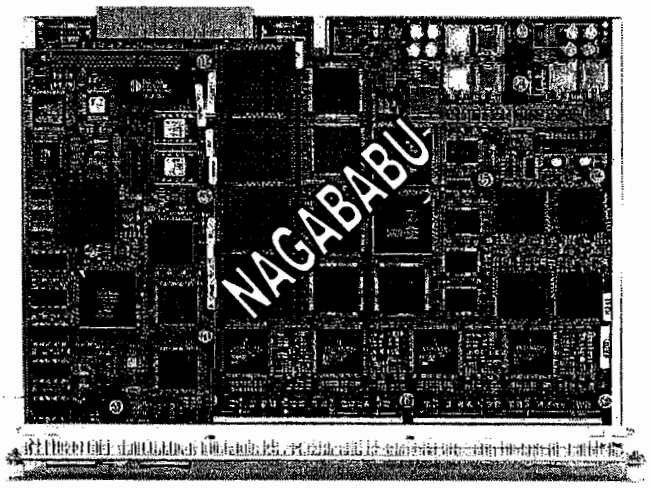
Fixed Switches:



Modular Switches:



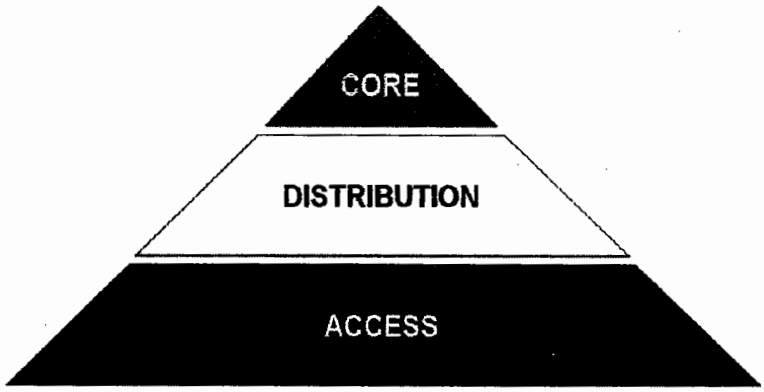




Cisco 3-Layer hierarchy:

Cisco switches are divided into 3 categories based on hardware capabilities

- Access Layer
- Distribution Layer
- Core Layer



Access Layer:

- Used for small Organizations
- Data transfer speed is low
- Local ISPs
- 1900, 2900 series switches
- Fixed switches

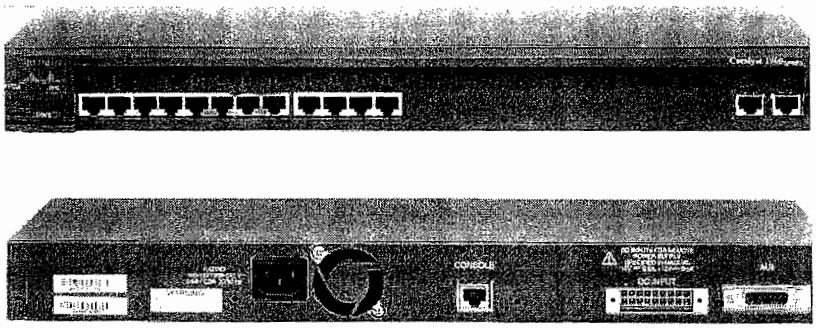
Distribution Layer:

- Used for medium level Organizations
- Data transfer speed is medium
- Regional ISPs, National ISPs
- 3500, 3700, 4500, 5000, 6000 series switches
- Modular switches

Core Layer:

- Used for medium level Organizations
- Data transfer speed is high
- National ISPs , Global ISPs
- 6500, 7000, 10000 series switches
- Modular switches

Switch Front and Rear Panels



Switch - Ports:

- **Interfaces: For data transfer**
  - In switches all the ports are called interfaces
    - fa 0/1, fa 0/2, fa 0/3, fa 0/4 and so on
- **Lines: For Switch management**
  - Physical lines: Exist on router
    - Console 0
  - Logical lines: Not exist on router
    - Vty 0 15 (also called as telnet)

Port Speeds:

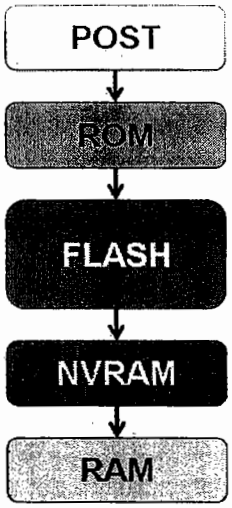
Port	Representation	Speed
e 0	Ethernet	10 Mbps
Fa 0/1	Fast Ethernet	100 Mbps
Gig 0/1	Gigabit Ethernet	1 Gbps
10Gig 0/1	10Gigabit Ethernet	10 Gbps

Port Representation:

Fixed switches have single module, indicated with 0
Modular switches have multiple modules start from 1, 2, 3 and so on

Fa 0/13 -	Fast Ethernet Module 0 Port No - 13	Gig 2/48 -	Gigabit Ethernet Module 2 Port No - 48

Switch internal Components - Boot sequence



POST:

- Power On Self Test
- Hardware Checkup
- RAM, CPU, Interfaces diagnosis

ROM:

- Read only Memory
- Bootstrap loader / Mini IOS
- Finds the location of complete IOS

FLASH:

- Complete IOS Image
- May have multiple IOS Images
- Switch operates with single IOS
- Eg: C2950-lanbase-mz.122-25.SEE2
- Switch maintains vlan information in a separate file called vlan.dat
- Vlan.dat resides in Flash memory

NVRAM:

- Non Volatile Random Access Memory
- Permanent configuration
- File name : Startup-config
- Switch always uses nvram configuration when booting
- Switch copies NVRAM into RAM

RAM:

- Random Access Memory
- Temporary configuration
- File name : Running-config
- Switch copies NVRAM into RAM
- Switch always works with RAM configuration only

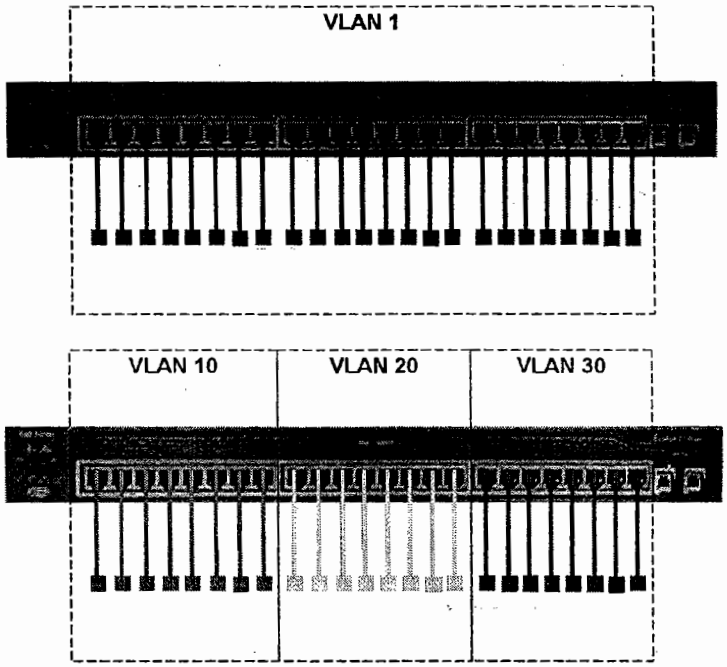
VLANs

What is VLAN?

- Virtual Local Area Network
- It is a logical boundary on the switch
- All the ports in a vlan can communicate with each other
- The ports in different vlans can not communicate in L2 switch
- Inter vlan communication is possible in L3 switch

- The ports with same vlan id can communicate even though they belong to different switches

- Vlan Range is 1-1005
- Vlan breaks the broadcast domain in the switch



What is Default VLAN?

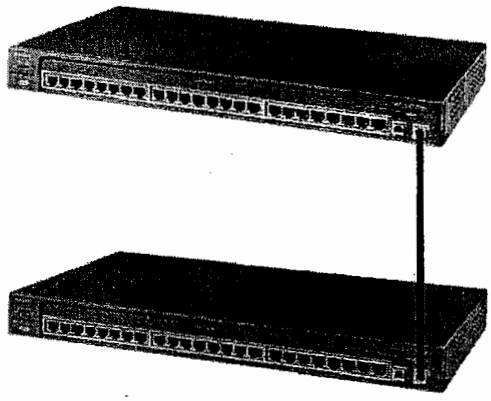
- By default a vlan exist on the switch with vlan id 1
- This vlan 1 is called as default vlan or management vlan
- By default all the ports belong to vlan 1 in the switch
- Vlan 1 can't be created or deleted
- Generally Vlan 1 carries management information like cdp, vtp

What is management VLAN?

- The active vlan to which ip address is assigned and operational
- Management vlan carries switch management information
- By default vlan 1 is management vlan

What is Trunking?

- The link between different switches that can carry the data from various vlans



Switch Port Types:

- **Access Port**
  - **Used to connect a computer**
  - **Access port can understand normal Ethernet frame**
  - **Access port belongs to only one vlan**

- **Trunk Port**
  - Used to connect a switch
  - Trunk port can understand tagged Ethernet frames
  - Trunk port can be a member of multiple vlans
  - Trunk port minimum speed is 100Mbps

What is Frame Tagging?

- Trunk port inserts Vlan id information within the frame before sending it through trunk link

- Trunk port removes Vlan id information from the frame before sending it to system

Tagging vlan id information to the original Ethernet frame is called frame tagging or frame encapsulation

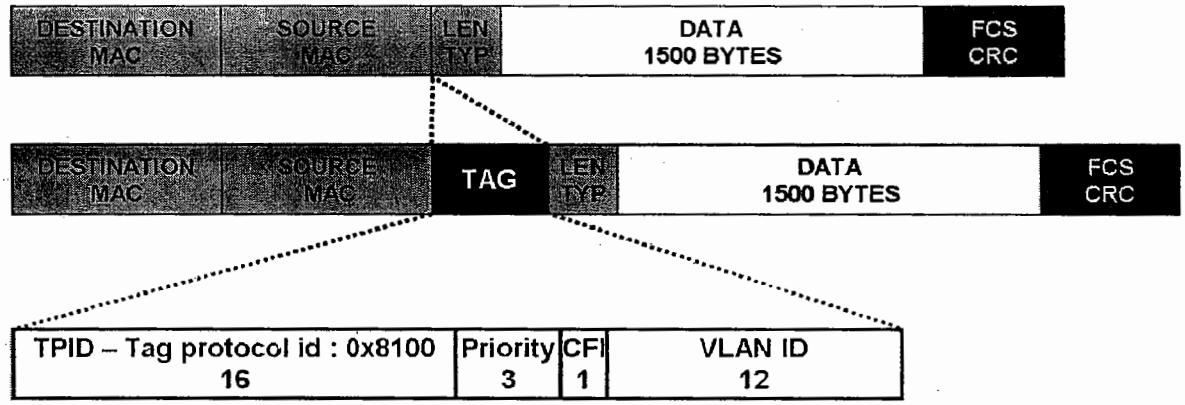
Frame Tagging methods:

- **Dot1q**
- **ISL**

Differences between dot1q and ISL

Dot1q	ISL
IEEE 802.1q encapsulation	Inter Switch Link
Open standard	Cisco proprietary
Inserts vlan id within the frame	Encapsulates Ethernet frame with new header & tailor
Inserts 4 bytes	Header is 26 bytes, Tailor is 4 bytes
Original frame size is 1518 Bytes New frame size is 1522 Bytes	Original frame size is 1518 Bytes New frame size is 1548 Bytes

Dot1q frame tagging:



What is Native VLAN?

- The vlan from which frames are not tagged
- By default vlan 1 is native vlan
- Native vlans must match at both ends of trunk link

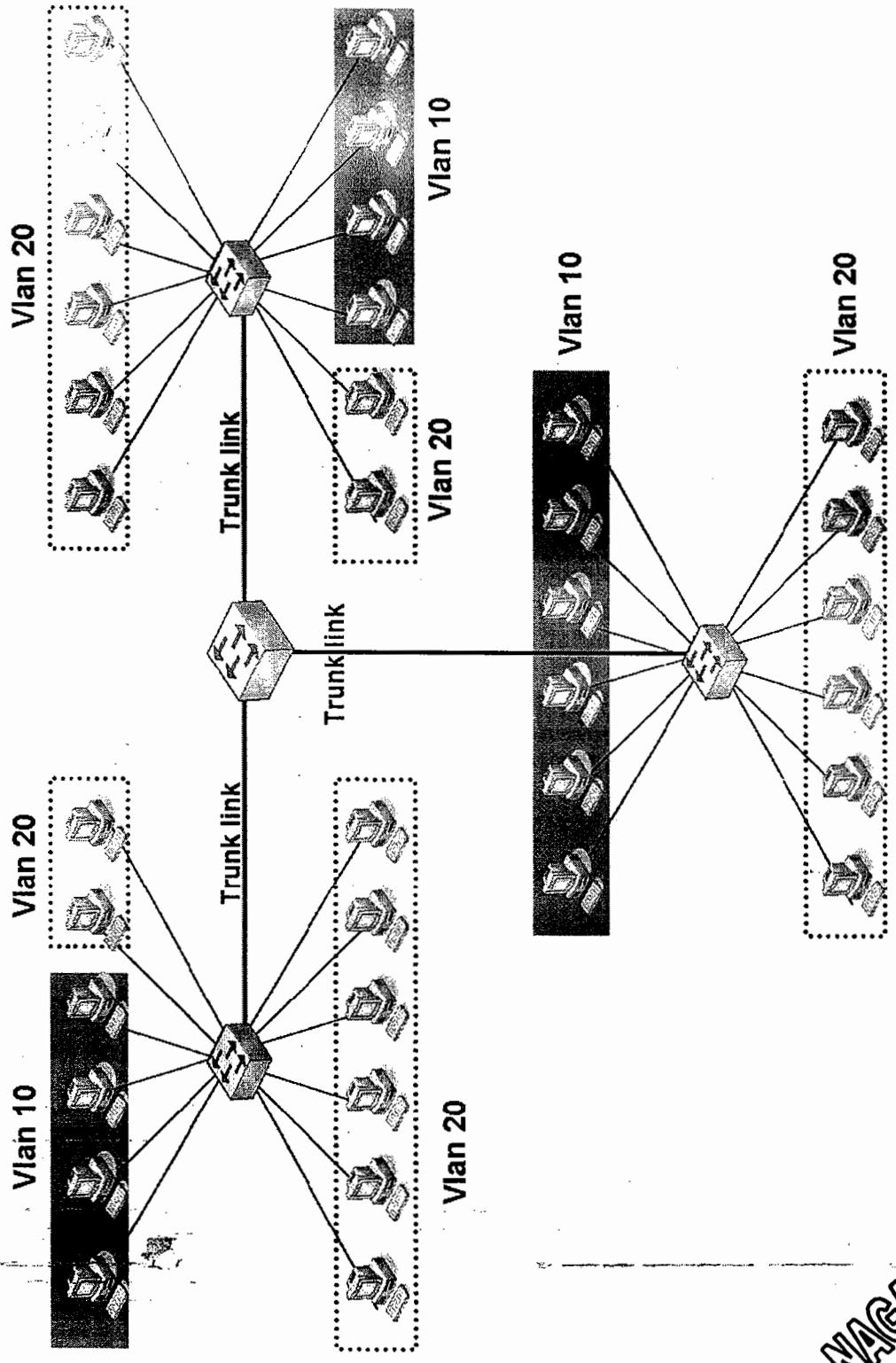
Servers at trunk ports:

- The ports from different vlans may need to access common servers
- Servers with trunk NIC can be connected at trunk ports
- Trunk NIC can understand tagged frames

NAGABABU

Vlan Communication

All the systems in vlan 10 communicate with each other
All the systems in vlan 20 communicate with each other



NAGABABU

What is the Operating System in Switches?

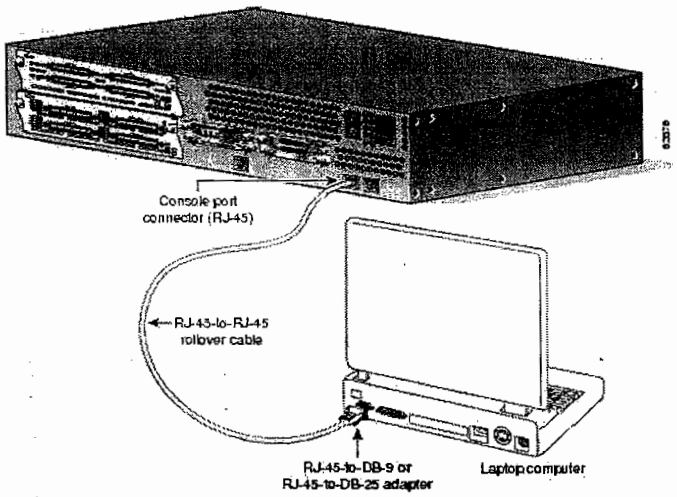
- Switch works on IOS
- **IOS - Internetwork Operating System**
- Switch works on singe IOS Image File

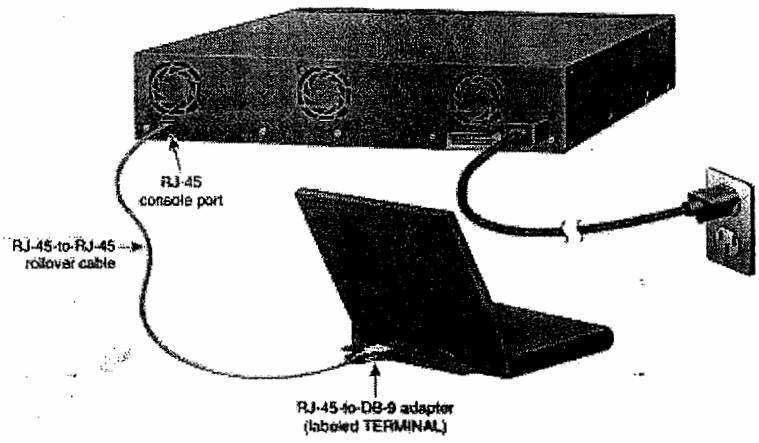
Switch Configuration is Mandatory?

- Configuration is not mandatory
- Switch is a zero touch configuration device
- However switch can be configured to create vlans, security

How to configure the switch?

- Use console 0 to configure the switch for the first time
- Connect roll over cable between **console 0** on switch & **COM1** port on the computer/laptop





NAGABABU

Emulation Software:

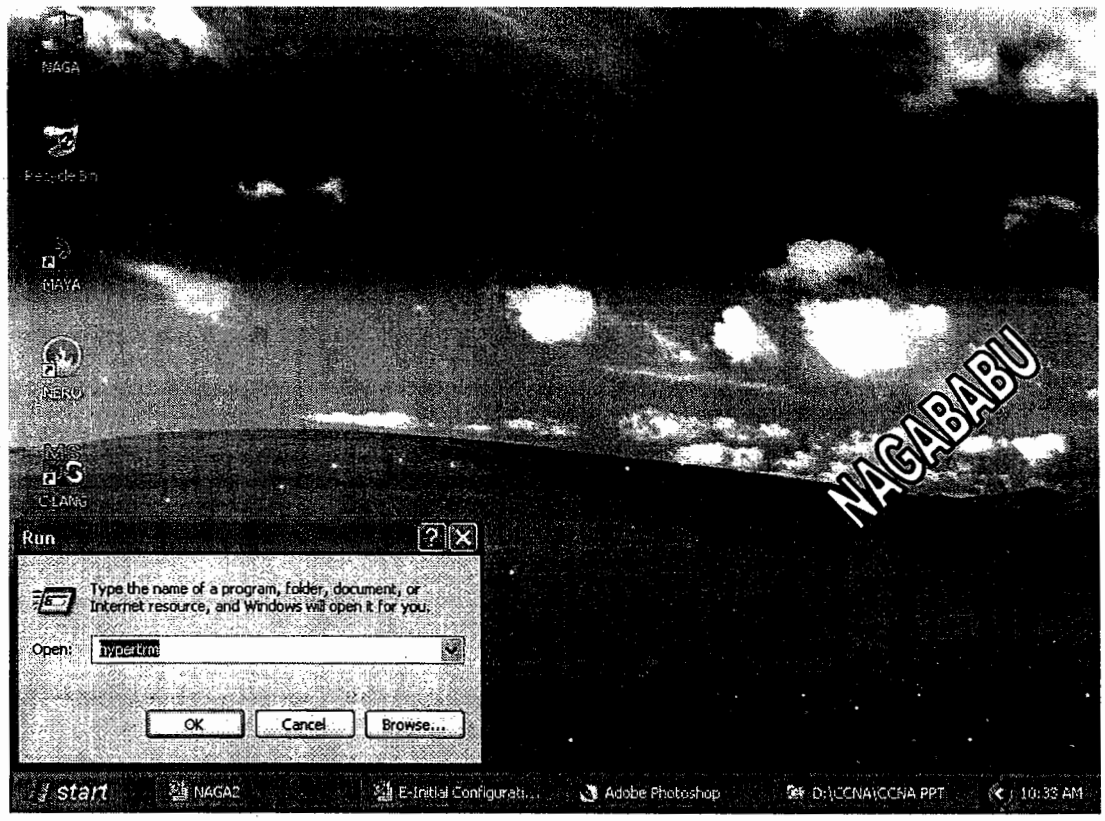
- One application is required on the laptop/system to access IOS and to configure the switch. This software is called emulation software

  Eg: hyper terminal, Putty

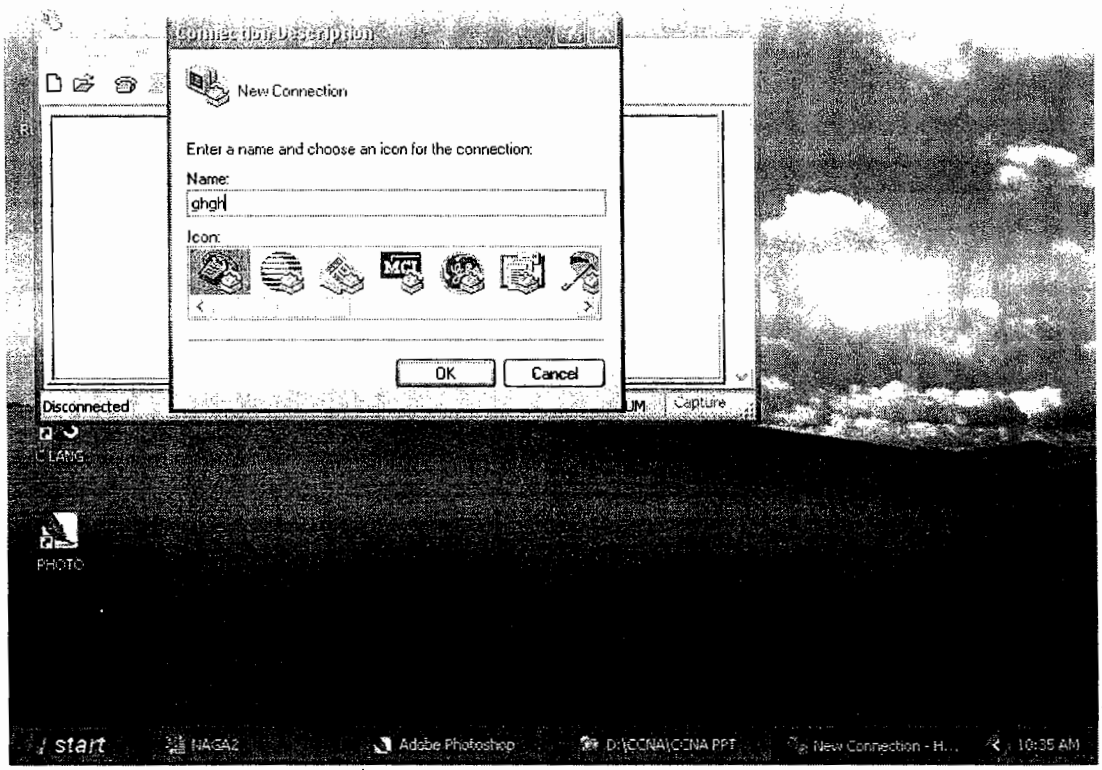
  Hyper terminal is the default program in Windows XP

How to access Hyper terminal:

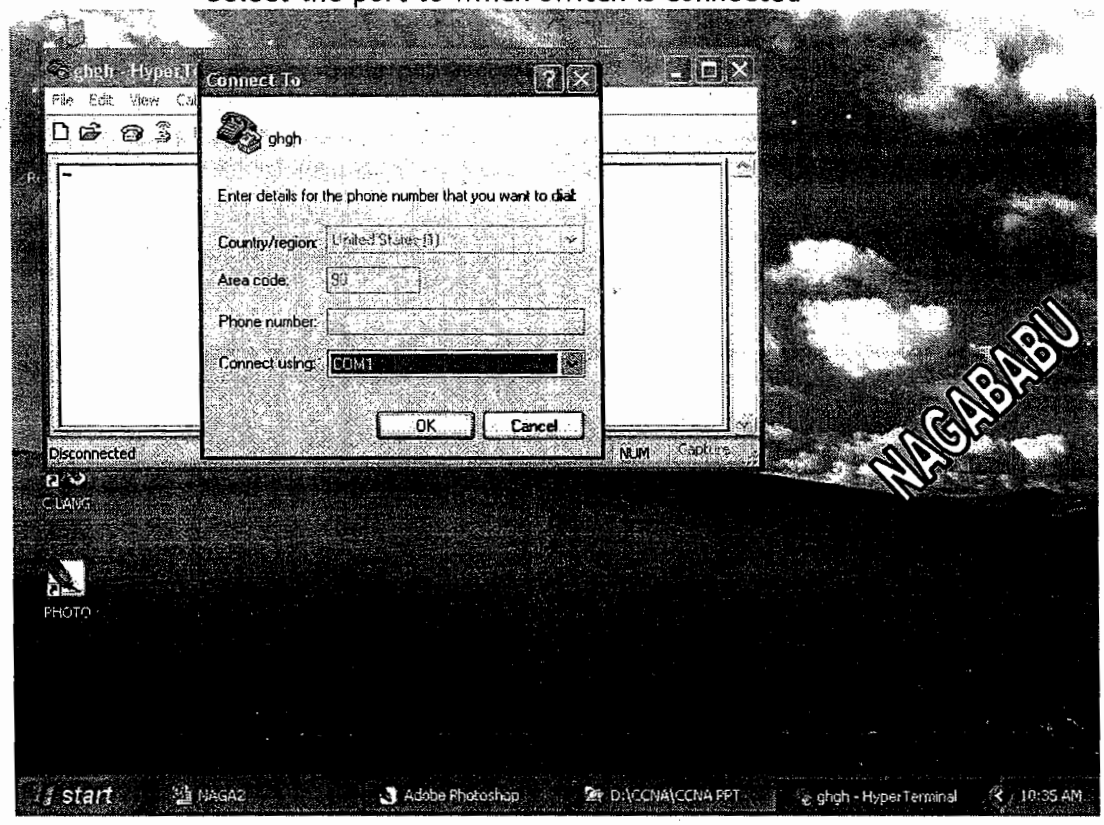
- Start -> Programs -> Accessories -> communications -> hyper terminal (or)
- Type **hypertrm** at run prompt



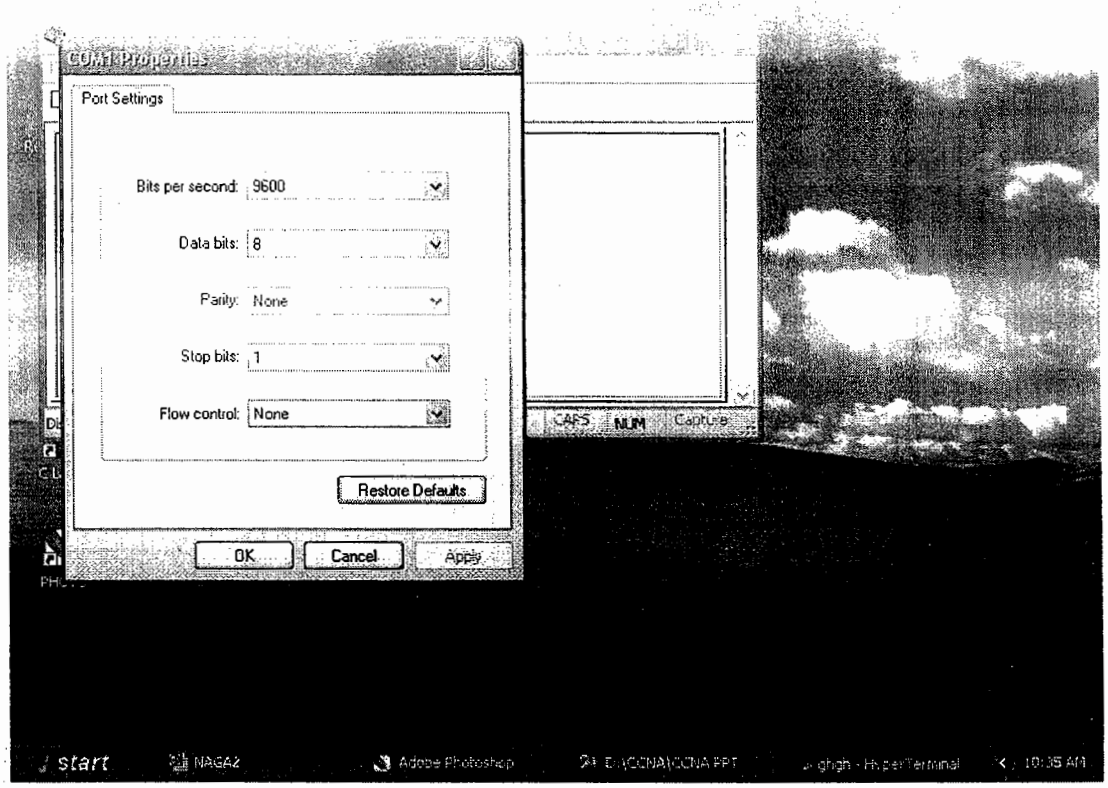
Type a name for the session



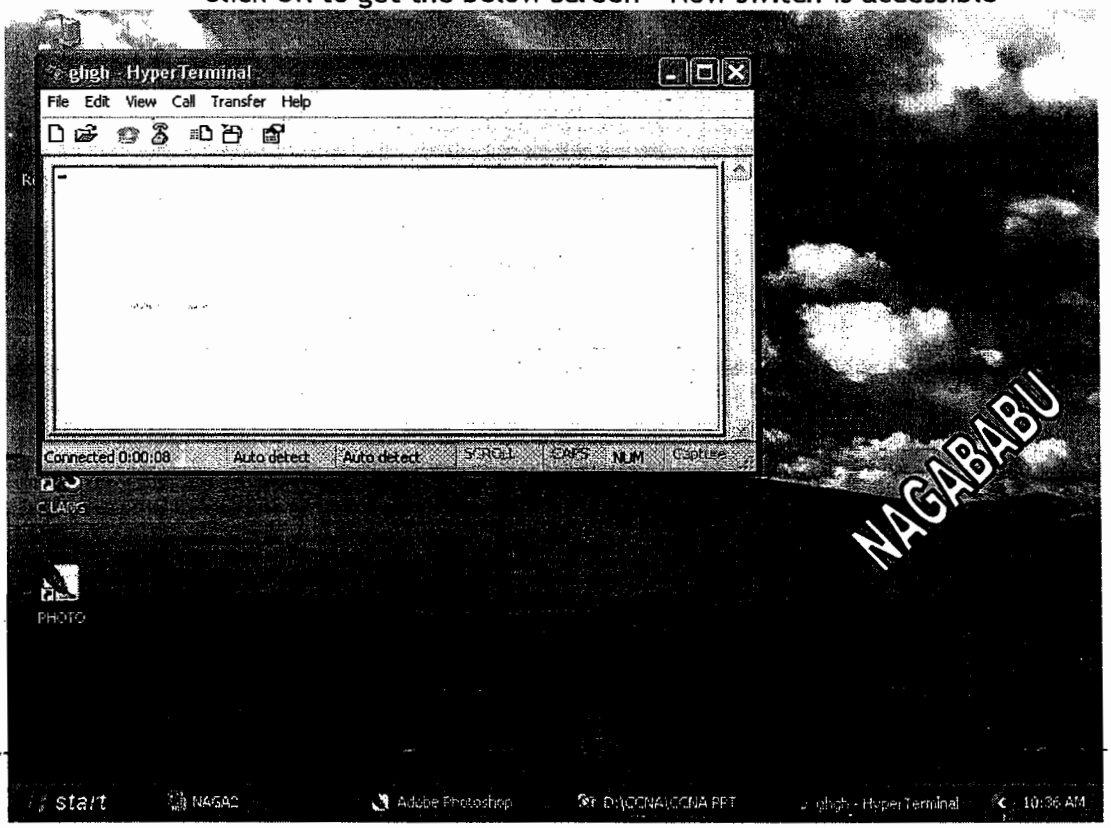
Select the port to which switch is connected



Select Restore defaults (Cisco switch accepts default settings)



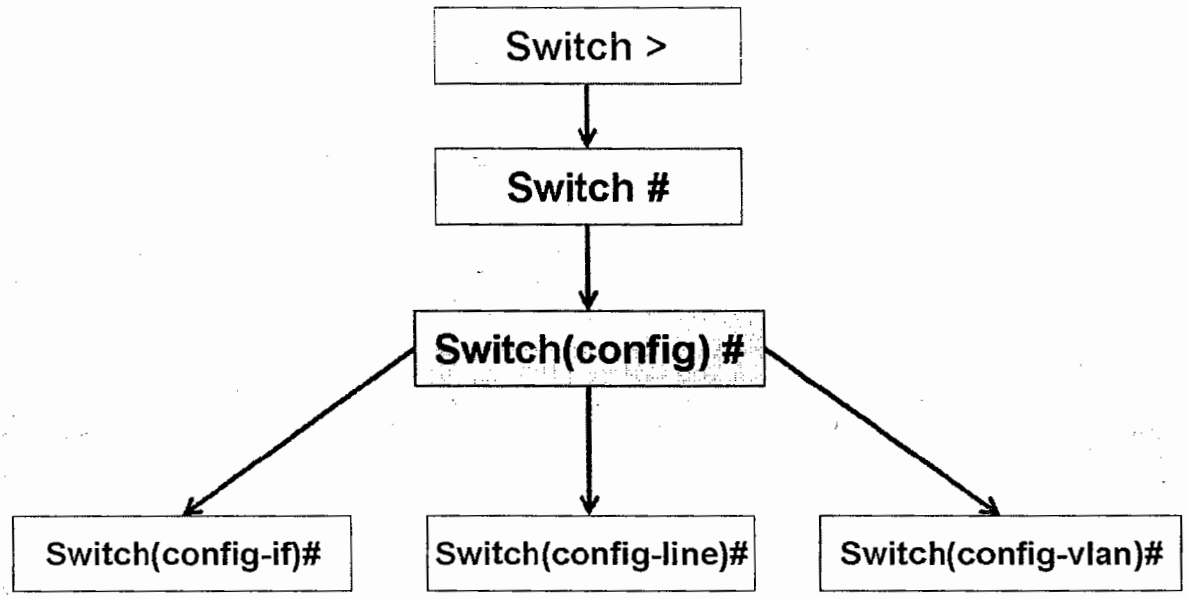
Click OK to get the below screen - Now switch is accessible



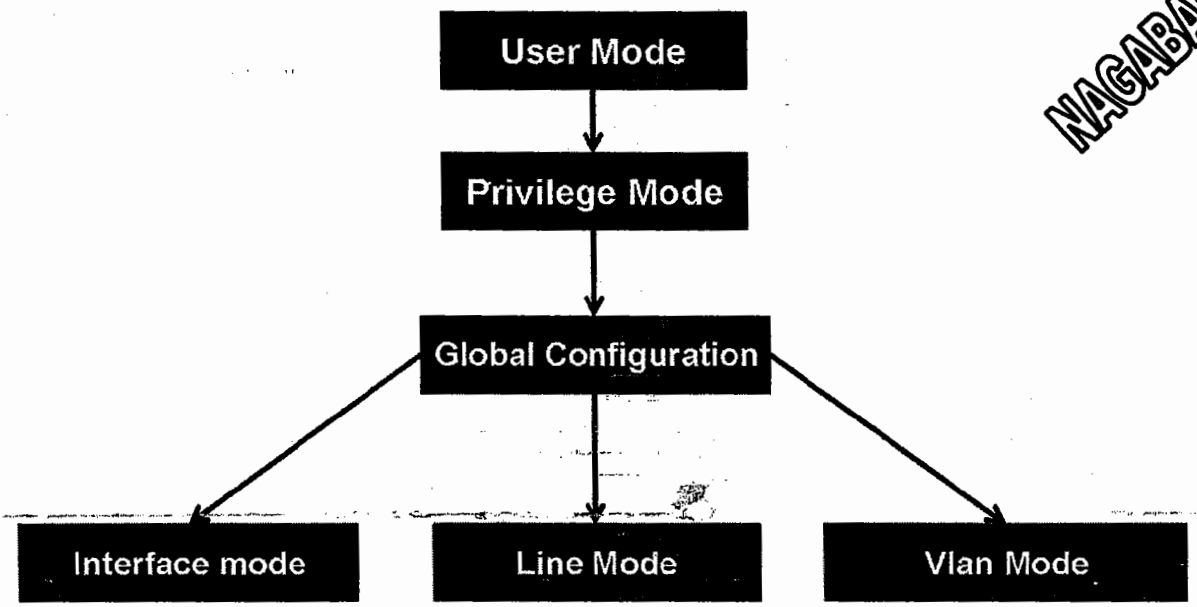
Switch Modes

- Cisco IOS has different modes
- Every mode has its own functionalities
- Cisco IOS is CLI (command line interface) based
- Commands are mode specific

Switch Modes - Prompts:



Switch Modes - Names:



NAGABABU

Switch Modes - Functionalities - Commands

1. User mode: Switch>

Functions:

- To check the Connectivity
- It has limited functionality

Commands:

Command	Function
telnet ip	to telnet into a device
Ping ip	to check connectivity
Traceroute ip	to trace the path
Enable	to enter privilege mode

2. Privilege mode: Switch#

Functions:

- View Entire configuration
- Backup & Recovery

Commands:

Command	Function
Show run	to see temporary configuration
Show start	to see permanent configuration
Show int fa 0/1	displays info about interface fa 0/1
Show version	displays version
Show flash	displays flash contents /ios image
Show ip int brief	displays interface ip information
Reload	restarts the Switch
Config t	enters into global configuration mode
Copy run start / Write	save RAM contents to NVRAM
Show mac-address-table	Displays MAC address Table
Show vlan	Displays Vlan Information
Show int trunk	Displays active trunk ports
Show interface	Displays all interface information
Show vtp status	Displays vtp information

3. Global configuration mode: Switch (config)#

Functions:

- To do entire configuration of Switch (globally)

Commands:

Command	Function
No logging console	turns off logging (logging messages)
Hostname *hostname*	changes the hostname
Enable password *cisco*	set privilege mode password
Enable secret *cisco*	set secret password for privilege mode
Int fa0/1	to interface mode
Int fa 0/2	
Int range fa 0/5 -8	
Line con 0	to line mode
Line vty 0 15	
Vlan 40	to vlan mode (creates a vlan)
Vtp mode server	Set vtp mode to server
Vtp password <naga>	Set vtp password
Vtp domain <cisco>	Set vtp domain name
Spanning-tree mode pvst	To set spanning-tree mode

4. Interface mode: Switch (config-if)#

Functions:

- Configuration of interfaces (ports)

Commands:

Command	Function
ip address <*ip*><*subnetmask*>	configure ip address for vlan interface
no shutdown	activate the interface
Speed 100	Sets speed to 100Mbps
Duplex full	Sets duplex to full
bandwidth *80*	Sets bandwidth/port speed
Switchport mode access	configure switchport as access port
Switchport mode trunk	configure switchport as trunk port
Switchport access vlan 34	Moves the port to specified vlan
Switchport trunk allowed vlan all	Configure trunk port as a member of all vlans
Switchport trunk enca dot1q	Sets dot1q encapsulation on trunk port
Spanning-tree portfast	Enables portfast feature on the port

5. Line mode: Switch(config-line)#

Functions:

- Authentication of lines
- Configuring console 0, vty 0 15

Commands:

Command	Function
Password <password>	To configure password for line
login	To set login type

6. Vlan mode: Switch (config-vlan)#

Functions:

- To configure vlans

Commands:

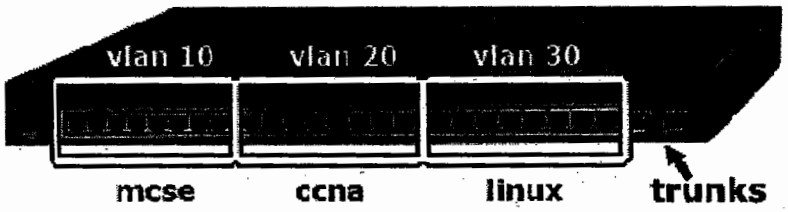
Command	Function
Vlan 40	Creates a vlan with id 40
Name mcse	To assign a name to vlan
State active	Activate vlan

Switch Initial Configuration

- Switch is a zero-touch configuration device
- However, it can be configured to implement vlans, security, IP address

Switch Configuration includes 5 steps

1. Hostname change
2. Secure switch
3. Configure vlans
4. Configure interfaces
5. View and Save



1. Hostname Change:

```
Switch> enable
Switch# config t
Switch(config)# hostname 2950
```

2. Secure Switch:

```
2950(config)# enable password cisco
2950(config)# enable secret ccna

2950(config)# line con 0
2950(config-line)# password cisco
2950(config-line)# login
2950(config-line)# exit

2950(config)# line vty 0 15
2950(config-line)# password cisco
2950(config-line)# login
2950(config-line)# exit

2950(config)# service password-encryption
2950(config)# exit
```

3. Configure vlans:

```
2950(config)# vlan 10
2950(config-vlan)# name mcse
2950(config-vlan)# state active
2950(config-vlan)# exit

2950(config)# vlan 20
2950(config-vlan)# name ccna
2950(config-vlan)# state active
2950(config-vlan)# exit

2950(config)# vlan 30
2950(config-vlan)# name linux
2950(config-vlan)# state active
2950(config-vlan)# exit
```

4. Configure interfaces:

Access Ports

```
2950(config)# interface range fa 0/1 - 8
2950(config-if-range)# switchport mode access
2950(config-if-range)# switchport access vlan 10
2950(config-if-range)# no shutdown
2950(config-if-range)# exit

2950(config)# interface range fa 0/9 - 16
2950(config-if-range)# switchport mode access
2950(config-if-range)# switchport access vlan 20
2950(config-if-range)# no shutdown
2950(config-if-range)# exit

2950(config)# interface range fa 0/17 - 24
2950(config-if-range)# switchport mode access
2950(config-if-range)# switchport access vlan 30
2950(config-if-range)# no shutdown
2950(config-if-range)# exit
```

Trunk Ports

```
2950(config)# interface gig 0/1
2950(config-if)# switchport mode trunk
2950(config-if)# switchport trunk allowed vlan all
2950(config-if)# switchport trunk encapsulation dot1q
2950(config-if)# no shutdown
2950(config-if)# exit

2950(config)# interface gig 0/2
2950(config-if)# switchport mode trunk
2950(config-if)# switchport trunk allowed vlan all
2950(config-if)# switchport trunk encapsulation dot1q
2950(config-if)# no shutdown
2950(config-if)# exit
```

Assigning IP address

```
2950(config)# interface vlan 1
2950(config-if)# ip address   192.168.6.20    255.255.255.0
2950(config-if)# no shutdown
2950(config-if)# exit
2950(config)# exit
```

5. View & Save:

```
2950# show ip int brief
2950# show run
2950# show interface
2950# show vlan
2950# show vlan brief
2950# show mac-address-table
2950# show interface trunk

2950# copy run start
2950# write
```

VTP

What is VTP?

- Vlan Trunking Protocol
- In corporate networks, adding a single vlan in all switches consumes time
- VTP carries vlan information from one switch to another switch
- Vlans replicate automatically between switches with VTP
- Vlan replication is bounded by vtp domain

- All the switches belong to same vtp domain synchronize vlan information

VTP Modes:

- Server Mode
- Client Mode
- Transparent Mode

Change the switch to one of these vtp modes as per requirement. Server is default.

VTP Modes comparison

Server Mode	Client Mode	Transparent Mode
Vlan configuration is possible	Vlan configuration is not possible	Vlan configuration is possible
Server is master	Client follows server	Transparent does not follow server
Vlan replication	Vlan replication	No vlan replication

VTP Modes configuration

Set VTP Domain:

2950(config)# vtp domain <cisco>

Set VTP Mode:

2950(config)# vtp mode <server/client/transparent>

Set VTP Password:

2950(config)# vtp password <ccna>

Check VTP information:

2950 # show vtp status

Switch Functions

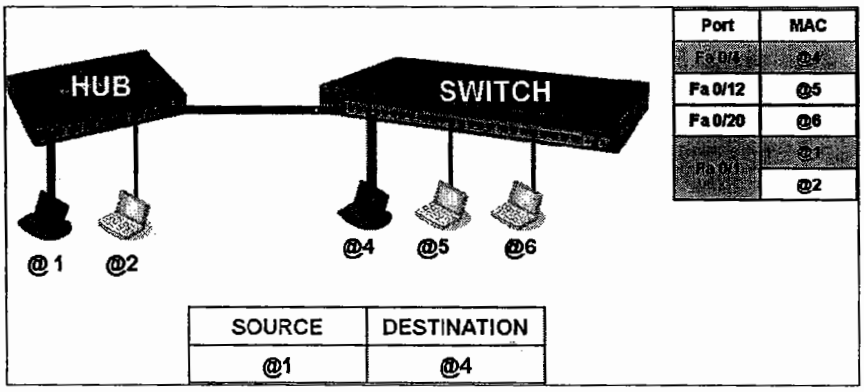
1. Builds MAT
2. Forwarding
3. Filtering
4. Loop Avoidance

1. Builds MAT:

Switch builds MAC address table based on L2 Header information.
Switch enters source MAC, sending port details in the MAT

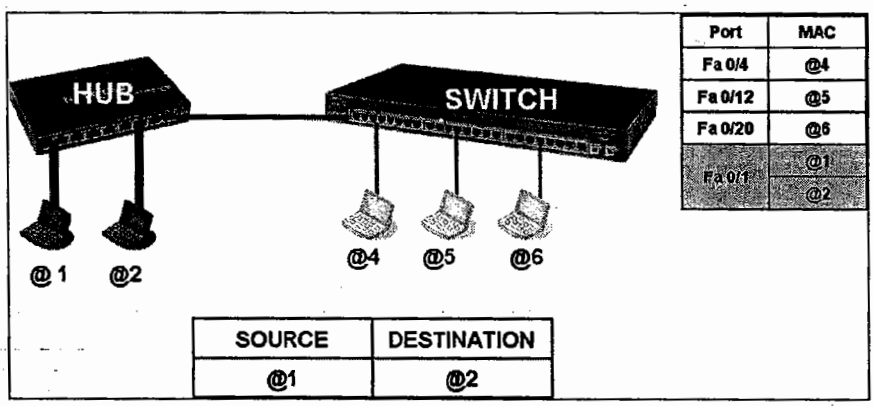
2. Forwarding:

Switch forwards the data if source MAC and destination MAC appear at different ports in MAC address table



3. Filtering:

Switch filters the data if source MAC and destination MAC appear at same port in MAC address table



4. Loop Avoidance:

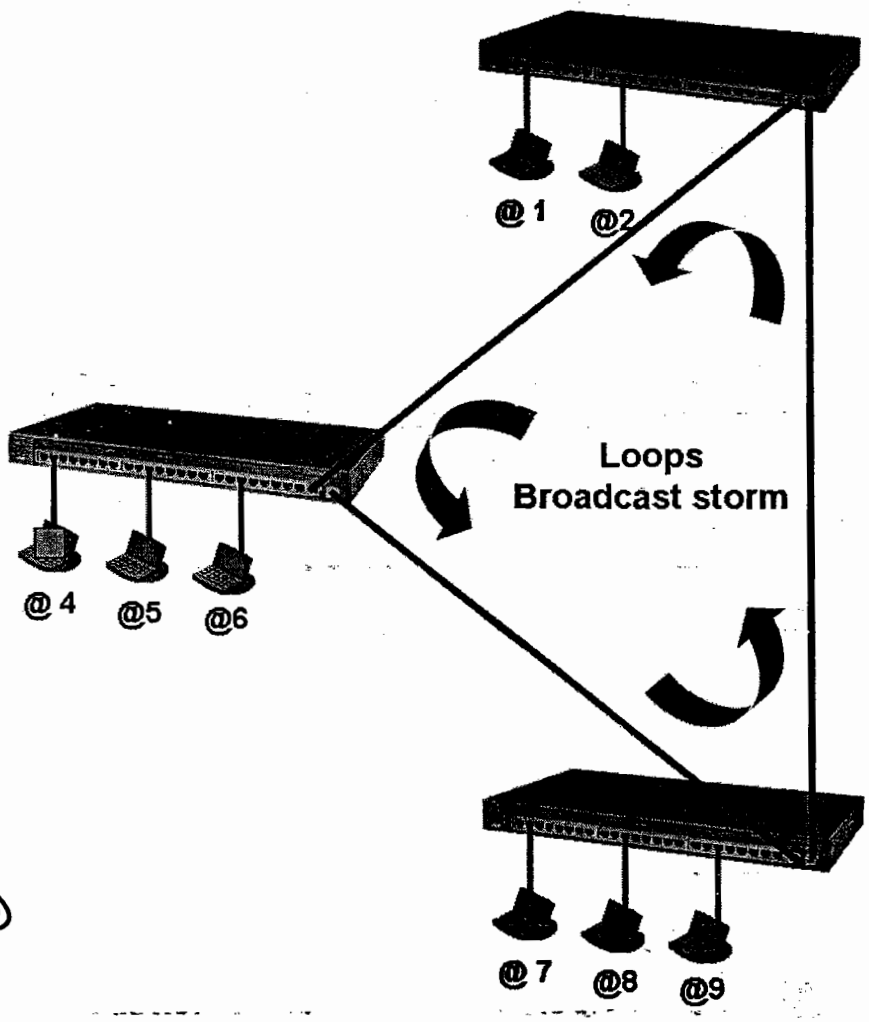
Switch avoids L2 loops with the help of STP (Spanning tree protocol)

What is Loop in Switches?

- Loops occur if a switch has multiple paths to another switch
- This the situation where a single frame propagates between switches multiple times, in various paths

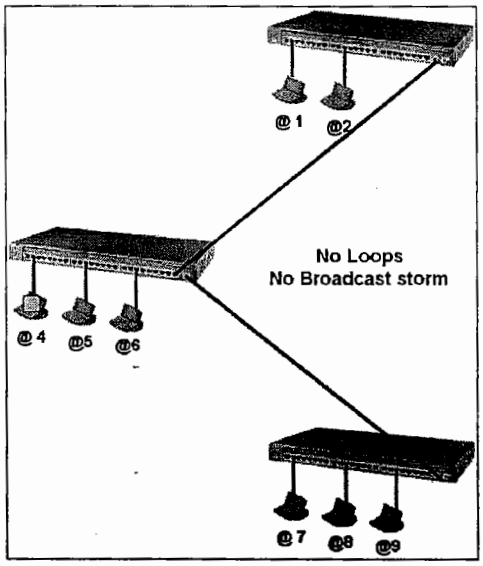
What is Broad cast Storm?

- If a system broadcasts the data in the loop network, a single frame goes to all the systems as multiple copies in various paths
- It consumes switch processing cycles and memory
- Finally Network performance comes down
- This situation is called broadcast storm



How to avoid loops ?

- Ensure the switches have only one path to reach other switch

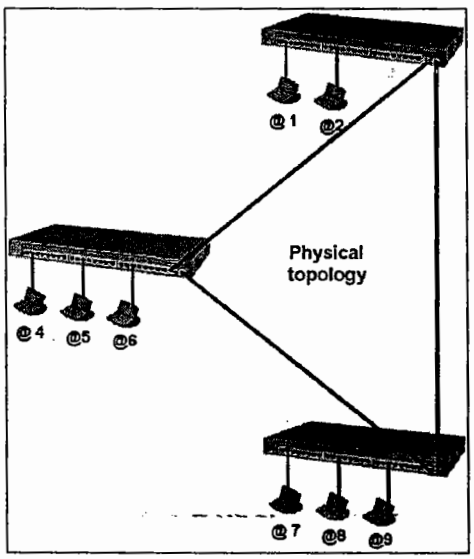


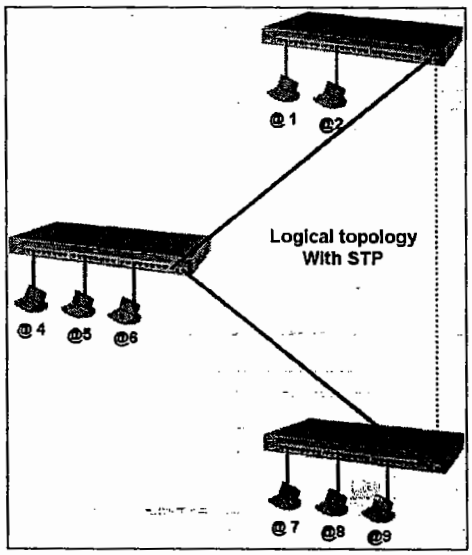
Why the switches need multiple paths ?

- Redundancy is required between switches to avoid network outages

How to avoid loops with redundancy ?

- Backup paths are required to achieve 100% network uptime
- At the same time loops must be avoided
- This can be done spanning tree protocol (STP) dynamically
- STP blocks some ports automatically which are causing loops





SPANNING TREE PROTOCOL - STP

What is STP?

- Spanning Tree protocol
- It is used to prevent loops in Layer 2 Networks
- It identifies the ports which are causing loops and blocks them
- STP builds new logical topology by blocking some ports
- If there is a problem with operational link, STP unblocks the blocked ports to provide redundant paths
- If the link comes up, STP runs again to prevent loops

What is STA ?

- Spanning Tree Algorithm
- Operations sequence in building new STP logical topology

STP Port states:

Disabled	Shutdown	
Blocked	Send/receive BPDU - No data	20 sec
Listening	Send/receive BPDU - Analyze data	15 sec
Learning	Send/receive BPDU - Learn MAC -Build MAT	15 sec
Forwarding	Send/receive BPDU - Forward Data	

STP Port Cost:

Port Speed	STP cost
10 Gbps	2
1 Gbps	4
100 Mbps	19
10 Mbps	100

STP terminology:

BPDU	Bridge Protocol data Unit	Message contains priority, switch MAC
RB	Root Bridge	Switch with best BPDU
NRB	Non Root Bridge	Switches other than RB
RP	Root Port	Port on NRB that has best path to RB
DP	Designated Port	Port in forwarding state
NDP	Non Designated Port	Port in Blocking state (BLK)

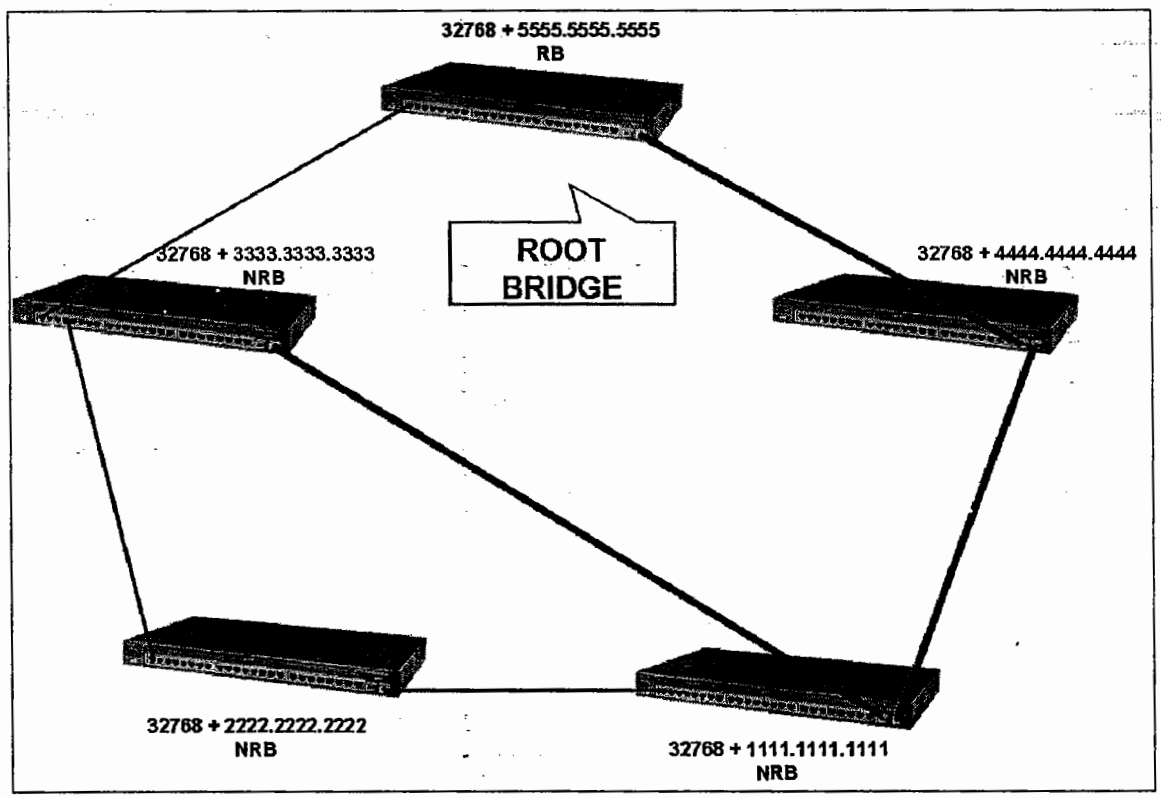
SPANNING TREE Algorithm

1. Electing **Root Bridge**
2. Electing **Root port** per switch
3. Electing **Designated port** per segment (Switch to switch)
4. Electing **Non designated ports**

1. Electing Root Bridge:

- All ports on all switches are in blocked state initially
- Every switch treats itself as Root Bridge
- Every switch sends BPDU to the remaining switches
- Every switch compares received BPDU with its own BPDU
- Finally only one switch will be elected as Root Bridge

- **BPDU** contains Switch Priority and Switch MAC address
- Default Priority is 32768
- The switch with Highest Priority becomes the Root Bridge
- If Priority is same, the switch with Highest MAC becomes Root Bridge

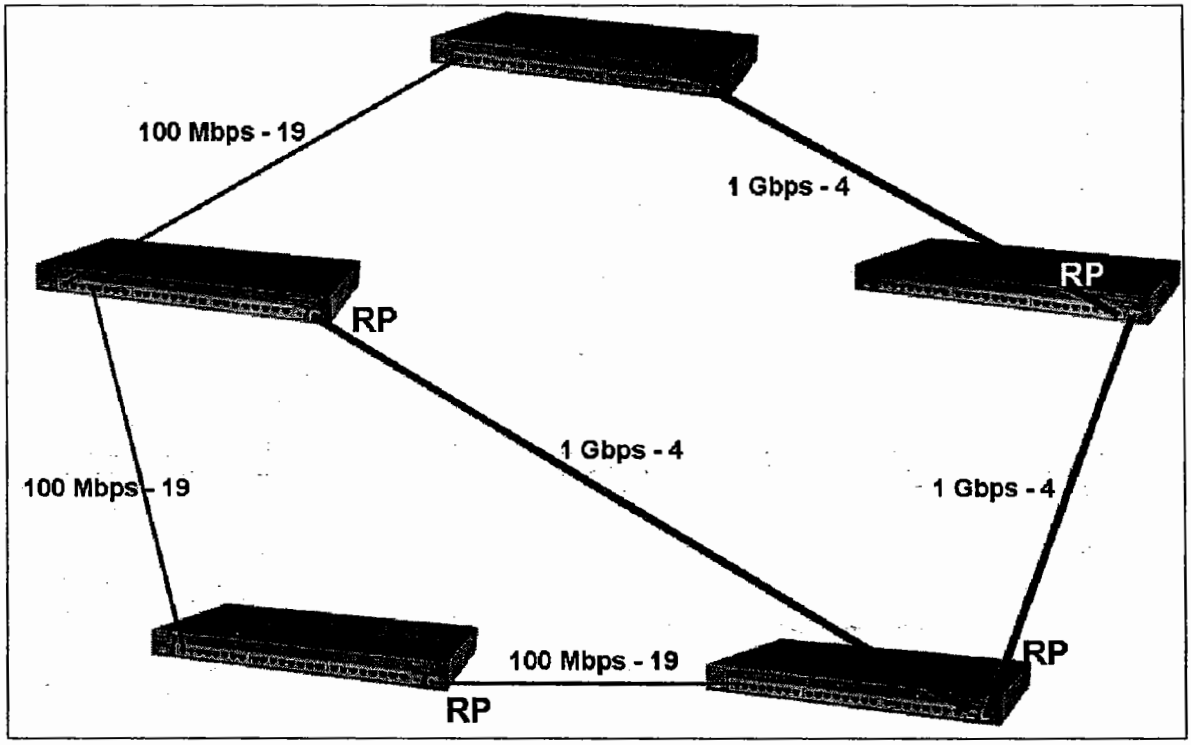


NAGABABU

2. Electing Root Port:

- Switch may have multiple paths to reach root bridge
- The port with best cost path to RB is elected as Root Port
- High speed ports have best cost paths
- Cost is inversely proportional to speed
- Only one Root Port exists per switch
- Root Port goes to forwarding state

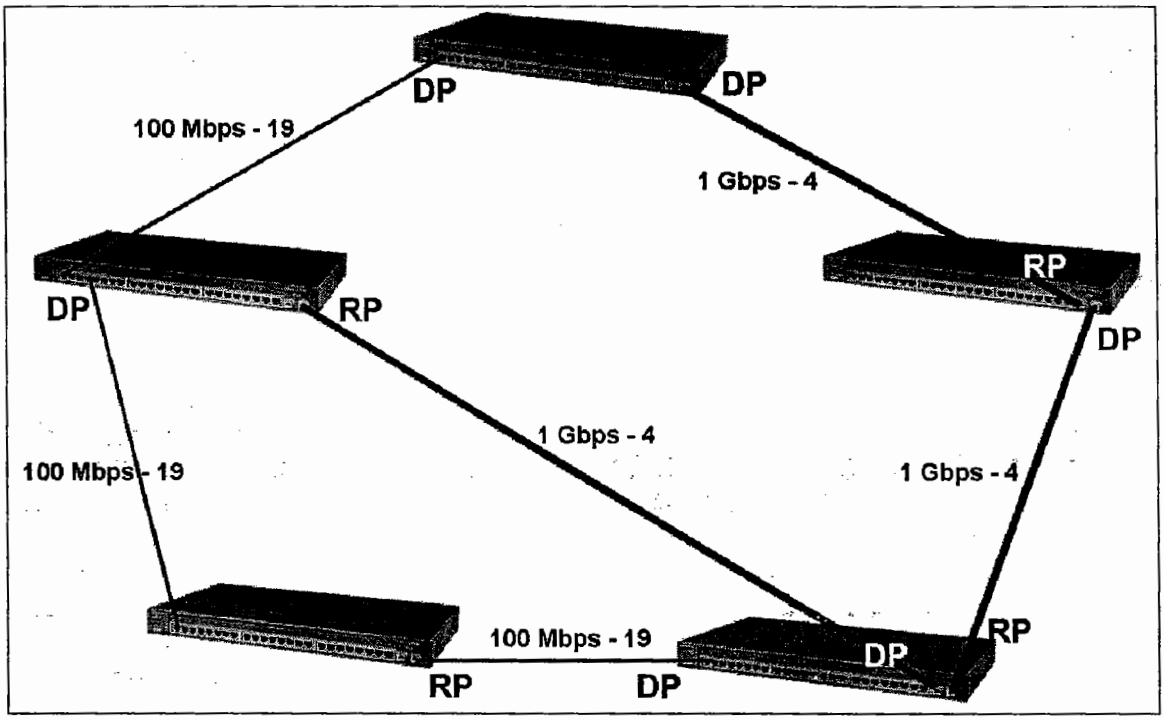
- If there is a tie in selecting Root Port, It prefers the link from the switch with best BPDU
- Still there is a tie, then looks at Port ID, the port with least port id is preferred



3. Electing Designated Ports:

- The port on the segment that has best cost path to RB is elected as designated Port (DP)
- Only one DP exists per segment (switch to switch link)
- DP goes to forwarding state
- All the ports on Root Bridge are Designated Ports

- If there is a tie in selecting Designated Port, It prefers the link from the switch with best BPDU
- Still there is a tie, then looks at Port ID, the port with least port id is preferred

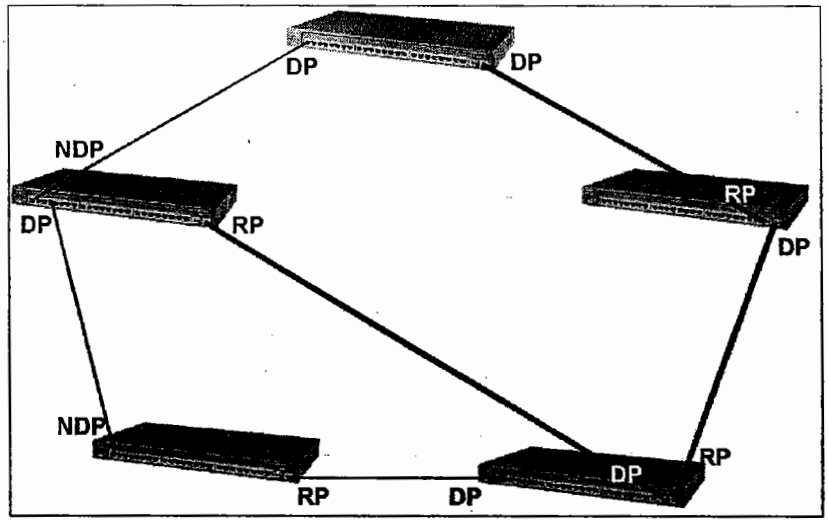


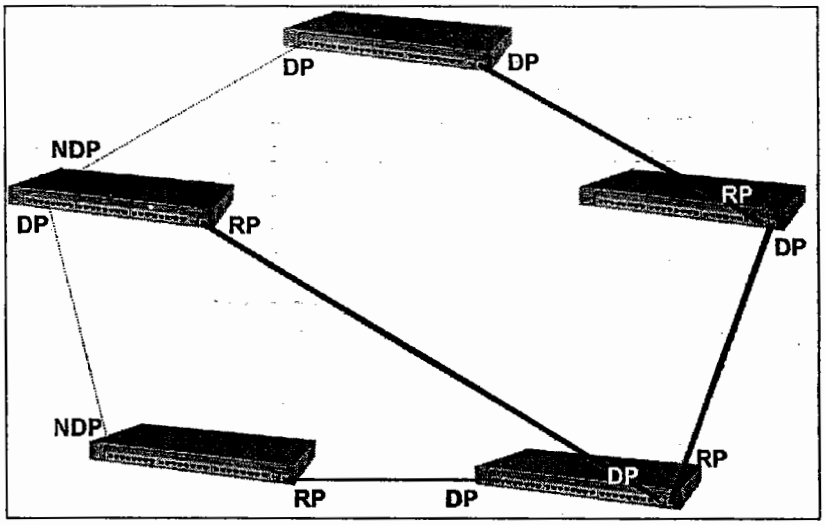
NAGABABU

4. Electing Non Designated Ports:

- The port neither RP nor DP becomes Non designated port
- Non designated port goes to blocking state
- NDP is also called as Blocked port (BLK)

- These ports have the chances to become active if operational link fails
- STP rebuilds the topology if something goes wrong with active links
- STP rebuilds the new topology by activating blocked ports





STP Types

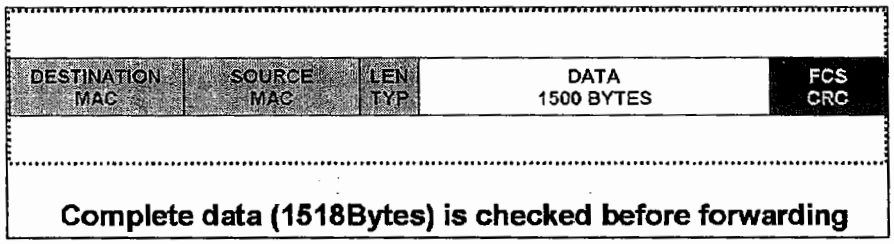
STP Type	Expansion	Standard	Description
STP	Spanning Tree	802.1d	Common Spanning Tree (CST)
RSTP	Rapid Spanning Tree	802.1w	For fast convergence
MSTP	Multiple Spanning Tree	802.1s	Multiple STP instances
PVST+	Per Vlan STP	Cisco proprietary	One STP instance per vlan

Switch - Operating Modes

1. Store & Forward
2. Cut through
3. Fragment Free (or) Modified cut through

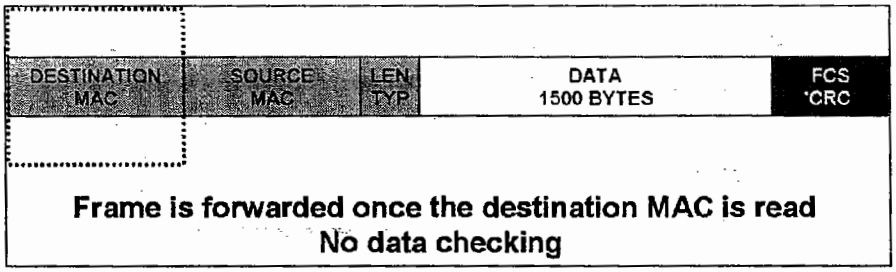
1. Store and Forward:

- The entire frame is buffered
- Runs CRC on complete frame before forwarding
- Latency is high
- Reliability is high



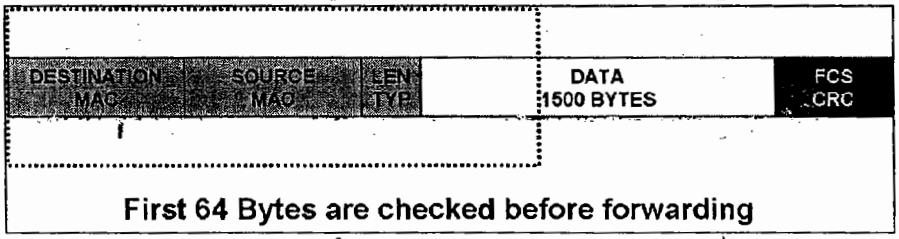
2. Cut through:

- The frame is forwarded once the destination MAC address (first 6 bytes) are arrived
- No CRC on the frame
- Latency is low
- Reliability is low



3. Fragment Free(Modified cut through):

- The frame is forwarded once the first 64 Bytes are arrived
- CRC runs on the first 64 Bytes
- Ethernet collisions do not occur usually after the first 64 Bytes
- Latency is medium
- Reliability is medium



Differences between Switch and Bridge

Bridge	Switch
Software Based	Hardware Based (ASICS)
Relatively Slow	Comparatively fast
No vlans	Vlans exist
One STP per Bridge	Many STPs possible
Typically up to 16 ports	Possibly hundreds of ports
Out dated device	Widely used device

Switch Password Breaking

- Power off the switch
- Power on the switch by pressing mode button
- Type **flash_init** (Initializes the flash)
- Type **load_helper**
- Type **dir flash:** (displays contents of flash)
- Type **rename flash:/config.text flash:/config.old** (renaming file)
- Type **boot** (to restart the switch)

- Switch is being restarted
- **Switch>** will appear

ARP & RARP

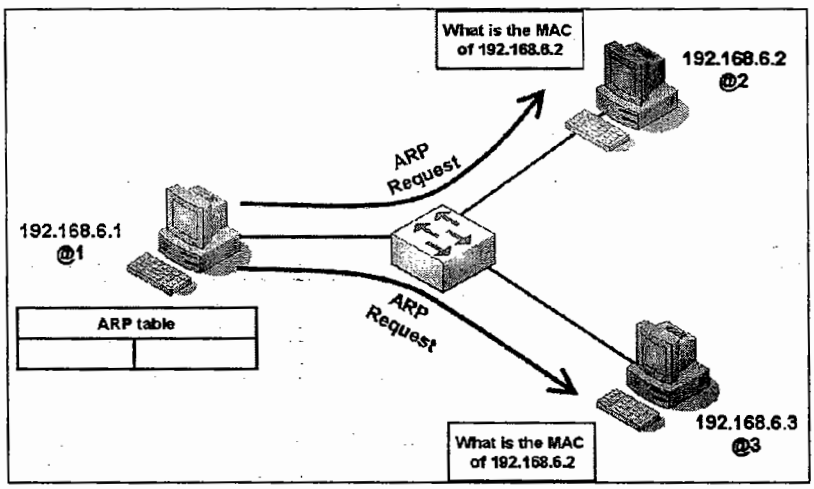
ARP- Address Resolution Protocol
RARP- Reverse Address Resolution Protocol

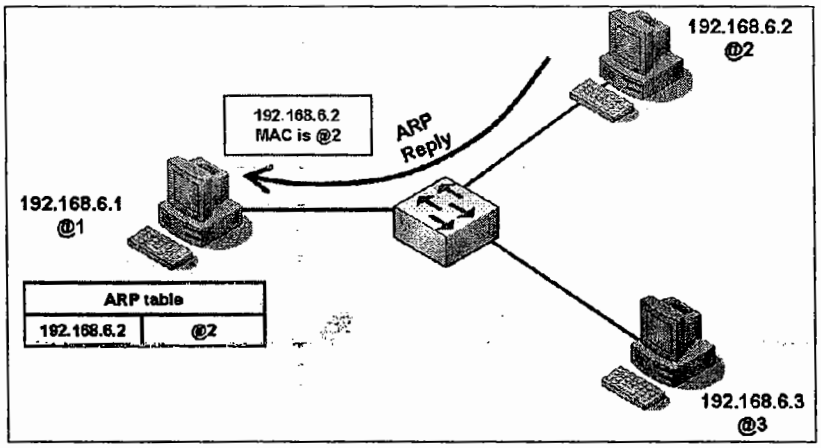
Systems communicate with the help of MAC address and IP Address

Source computer needs destination computer MAC address to send the data.
So source computer broadcasts a request to all computers to know destination MAC address. Only one computer will respond and send the reply

Source computer maintains destination IP, MAC information in ARP table locally
System uses ARP table contents to communicate with destinations
ARP table entry expires if the communication is idle for a long time

- **ARP - Address Resolution Protocol**
  Used to find MAC address for a known IP address
- **RARP - Reverse Address Resolution Protocol**
  Used to find IP for a known MAC
- ARP, RARP requests are Broadcast messages
- ARP, RARP replies are unicast messages





CDP

CDP - Cisco Discovery Protocol:

- CDP is Cisco proprietary data link layer protocol
- CDP discovers directly connected neighbor cisco devices
- CDP is enabled on cisco devices by default
- Cisco devices exchange CDP messages to discover neighbors dynamically
- CDP can obtain the following information of a neighbor
  - Name of the device
  - IOS software version
  - Hardware capabilities such as routing, switching
  - Hardware platform, such as 2800 or 2960
  - Layer 3 address of a device
  - The interface on which the CDP update was generated

CDP - commands:

Enabling CDP:	
IOS(config)#cdp run	Enable CDP globally
IOS(config)#no cdp run	Disable CDP globally
IOS(config-if)# cdp enable	Enable CDP on the interface
CDP status:	
IOS# show cdp	Status of CDP
IOS# show cdp interface	Show CDP on interface basis
CDP Neighbors:	
IOS# show cdp neighbors	Summary of all cisco neighbors
IOS# show cdp neighbors detail	Complete details of all cisco neighbors
IOS# show cdp entry <neighborname>	Details of a specified neighbor
IOS# show cdp traffic	Displays CDP traffic details

These commands are common for switches and routers

ACL

STUDENTNAME 143 NAGABABU

ACL (Access Control List)

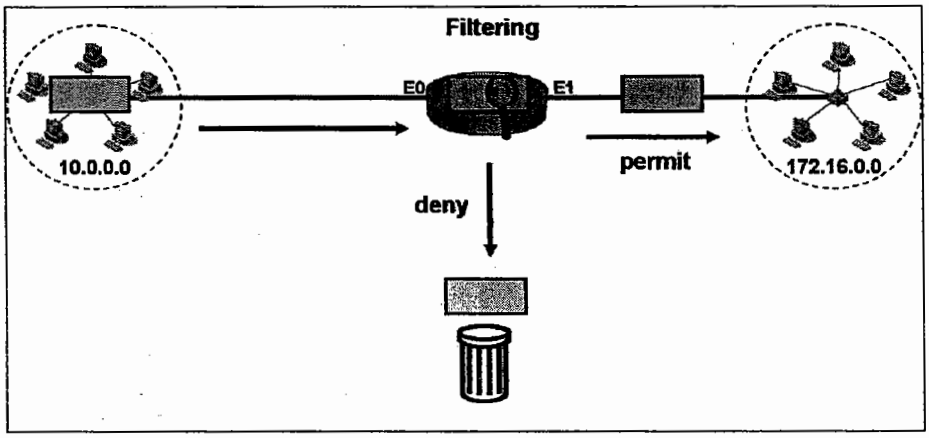
What is ACL ?

- Access Control List
- Security implementation feature
- It is used to **filter the network** traffic that crosses routers
- ACL is the list of statements that allows or denies the predefined traffic
- With ACL, router works as **packet filtering** firewall

- Router takes filtering decisions based on **L3 Header** and **L4 Header**

  L3 Header contains Source IP, destination IP, Protocol Number
  L4 Header contains Source Port, destination Port numbers

ACL Basic idea:



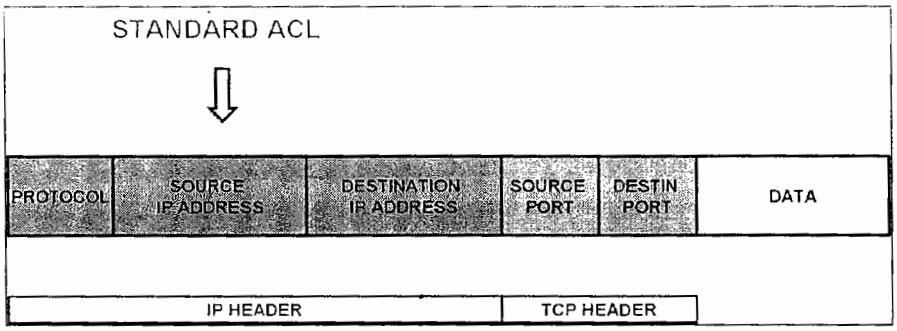
ACL Types:

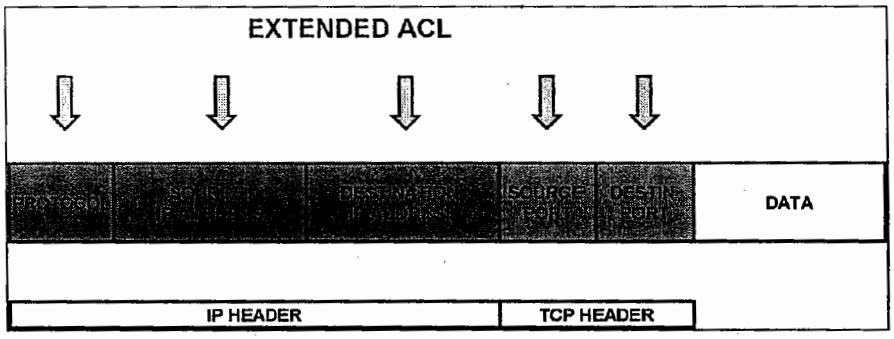
Basically ACL's are two types

- Standard ACL
- Extended ACL

Standard - Extended ACL differences:

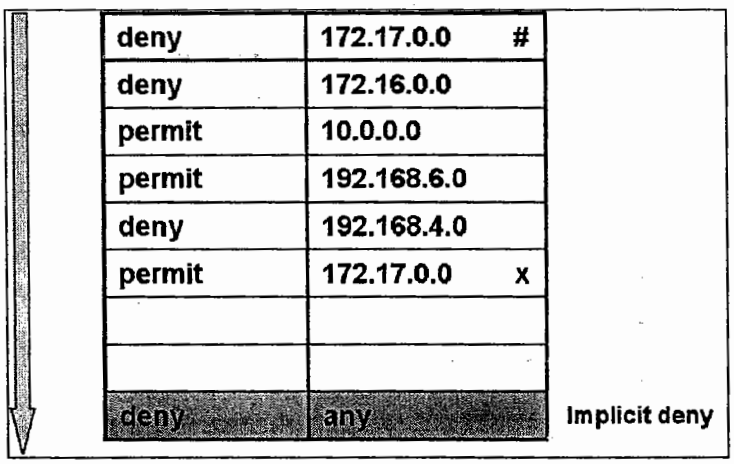
Standard ACL	Extended ACL
It takes decisions based on Source IP	It can take decisions based on Source IP - Destination IP Protocol Source Port - Destination Port
Implemented close to destination	Implemented close to source
ACL creation Number: **1-99**	ACL creation Number: **100-199**
Works on both direction	Works on single direction
Works on all services	Can work on single service





ACL statements order:

- Router checks ACL statements from top to bottom to find a match
- If a match is found, router will not check further statements
- "deny any" statement presents as a last statement in the ACL list, which is called **implicit deny.** So by default router blocks everything with ACL
- Implicit deny can be overridden by "permit any" statement



deny	172.17.0.0
deny	172.16.0.0
permit	10.0.0.0
permit	192.168.6.0
deny	192.168.4.0
permit	172.17.0.0
permit	any
deny	any

Over riding Implicit deny

What is Match?

- Match is 32 bit value that defines the scope of IP address
- It is similar to Wild card Mask value
- 0 is must match: 1 is ignore
- It indicates on what range IP addresses action should be taken

Examples:

IP Address	Match	Action taken on
172.16.5.145	0.0.0.0	172.16.5.145
172.16.5.145	0.0.0.255	172.16.5.0 to 172.16.5.255
172.16.5.145	0.0.255.255	172.16.0.0 to 172.16.255.255
172.16.5.145	0.255.255.255	172.0.0.0 to 172.255.255.255
172.16.5.145	255.255.255.255	All ip addresses
10.0.0.123	255.255.255.255	All ip addresses
10.156.128.73	0.255.255.255	10.0.0.0 to 10.255.255.255
10.156.128.73	0.0.0.4	10.156.128.73 & 10.156.128.77

IP Address	**10.156.128.73**	**00001010.10011100.10000000.01001001**
Match	**0.0.0.4**	**00000000.00000000.00000000.00000100**
Result	**10.156.128.73** **10.156.128.77**	**00001010.10011100.10000000.01001001** **00001010.10011100.10000000.01001101**

In the Match 3rd Bit indicates ignore. So 0 or 1 can be taken in the ip address 3rd bit That results two IP addresses

IP addressing, Binary operations knowledge is required to understand this concept

ACL implementation

- First understand the requirement
- Identify source ip, destination ip, protocol, source port, destination port
- Select the type of ACL (Standard / Extended) to implement
- Identify the traffic flow (in bound, out bound)
- Select the router as a filtering point
- Create ACL on the router and implement ACL on appropriate interface

First understand the requirement:

- First understand need to implement ACL
- Which traffic should be denied and which traffic should be allowed

Identify source ip, destination ip, protocol, source port, destination port:

- Identify IP addresses from which to which the traffic should be filtered
- Identify IP protocol to filter the traffic
  - TCP
  - UDP
  - IP
  - Eigrp
  - Icmp
  - ospf
- Identify TCP/UDP ports that should be filtered
  - http
  - ftp
  - dns
  - smtp
  - telnet

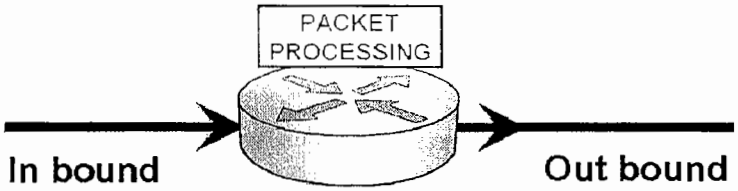
Select the type of ACL (Standard / Extended) to implement:

- Select Standard or Extended ACL which is best suitable for the task
- Standard ACL is a subset of Extended ACL
- Extended ACL can be implemented for all types of scenarios

Identify traffic flow (in bound, out bound):

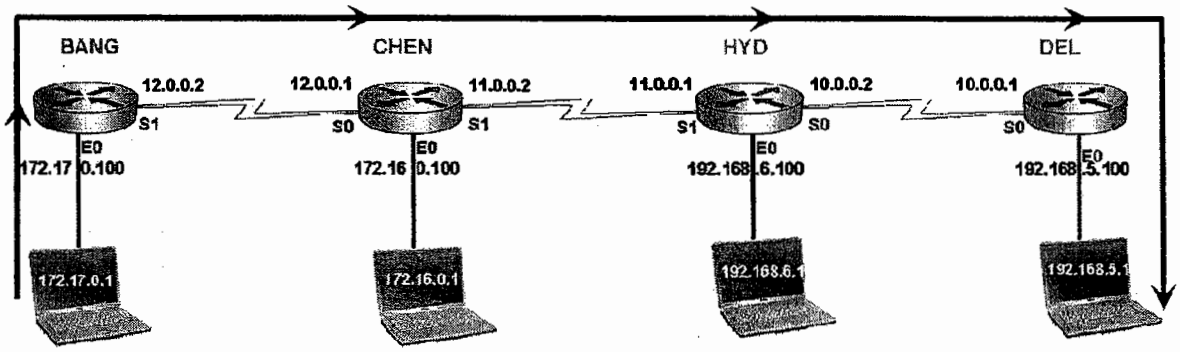
- **In bound :** The traffic entering in to the router
  It filters the traffic before the packet is processed, does not consume router resources

- **Out bound :** The traffic leaving from router
  It filters traffic after the packet is processed, consumes router resources



Select a router as a filtering point:

- There may be number of routers appear in the traffic flow
- Select one of the router as a best filtering point
- Generally ACL is configured nearer to source or destination



Create ACL on the router and implement ACL on appropriate interface :

- Create ACL in global configuration mode
- Implement ACL on one of the interface, in interface mode

- Maximum two ACL's can be applied on one interface
  - One as inbound
  - Second as outbound

NAGABABU

ACL Syntax

Standard ACL

Creation:

Router(config)# access-list <1-99> <permit/deny> <sourceip> <match>
Router(config)# access-list <1-99> <permit/deny> <sourceip> <match>

Router(config)# access-list <1-99> <deny/permit> any

Implementation:

Router(config)# interface <s0/e0/s1>
Router(config-if)# ip access-group <1-99> <in/out>

Extended ACL

Creation:

Router(config)# access-list <100-199> <permit/deny> <protocol> <sourceip> <match> <destination ip> <match> <eq> <port>
Router(config)# access-list <100-199> <permit/deny> <protocol> <sourceip> <match> <destination ip> <match> <eq> <port>

Router(config)# access-list <100-199> <deny/permit> <protocol> any any

Implementation:

Router(config)# interface <s0/e0/s1>
Router(config-if)# ip access-group <100-199> <in/out>

Checking ACL:

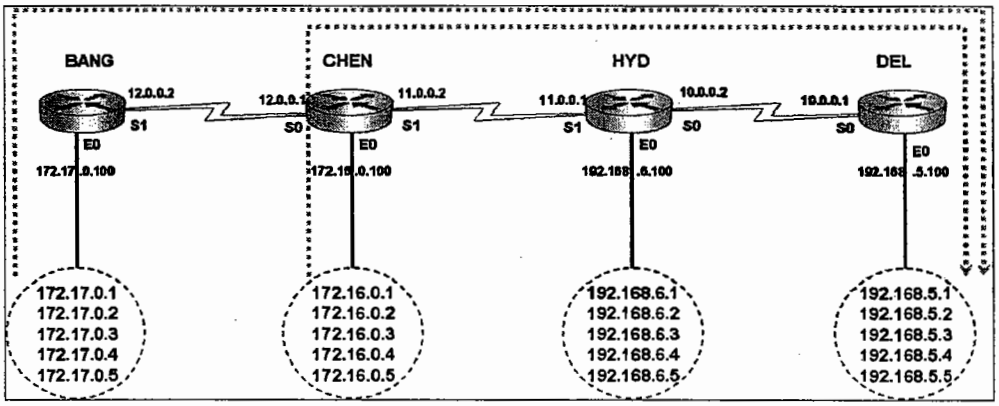
Router # show access-list

Deleting ACL:

Router(config)# no access-list <ACL No>

Standard ACL Examples

1. Don't allow 172.17.0.1 and 172.16.0.5 to access Delhi network



Source ip = 172.17.0.1 and 172.16.0.5
Destination ip = 192.168.5.0 network
Standard ACL implementation
Delhi router -- e 0 interface

Creation:

```
Delhi(config)# access-list    35    deny      172.17.0.1   0.0.0.0
Delhi(config)# access-list    35    deny      172.16.0.5   0.0.0.0
Delhi(config)# access-list    35    permit    any
```

Implementation:

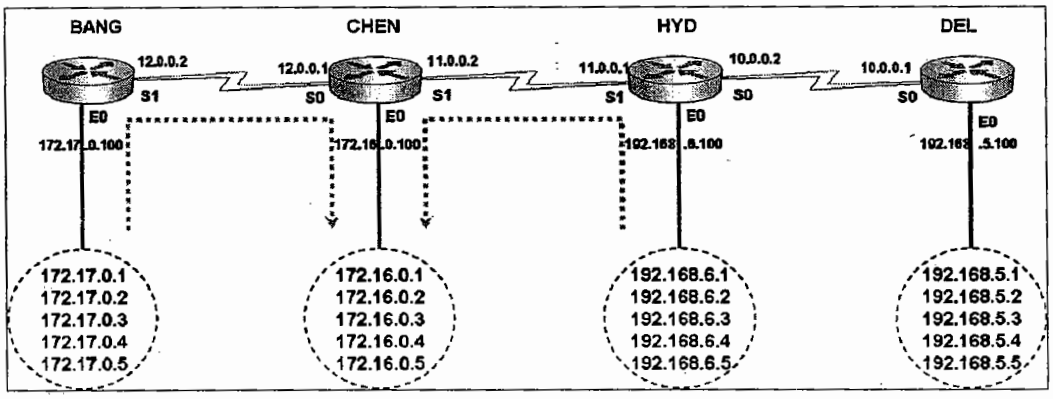
```
Delhi(config)# interface    e 0
Delhi(config-if)# ip access-group   35    out
```

```
Delhi# show access-list 35
```

NAGABABU

Standard ACL Examples

2. Don't allow 192.168.6.1, 192.168.6.2, 172.17.0.3 to access Chennai network



Source ip = 192.168.6.1, 192.168.6.2 and 172.17.0.3

Destination ip = 172.16.0.0 network

Standard ACL implementation

Chennai router – e 0 interface

Creation:

```
Chen(config)# access-list    89    deny      192.168.6.1  0.0.0.0
Chen(config)# access-list    89    deny      192.168.6.2  0.0.0.0
Chen(config)# access-list    89    deny      172.17.0.3   0.0.0.0
Chen(config)# access-list    89    permit    any
```

Implementation:

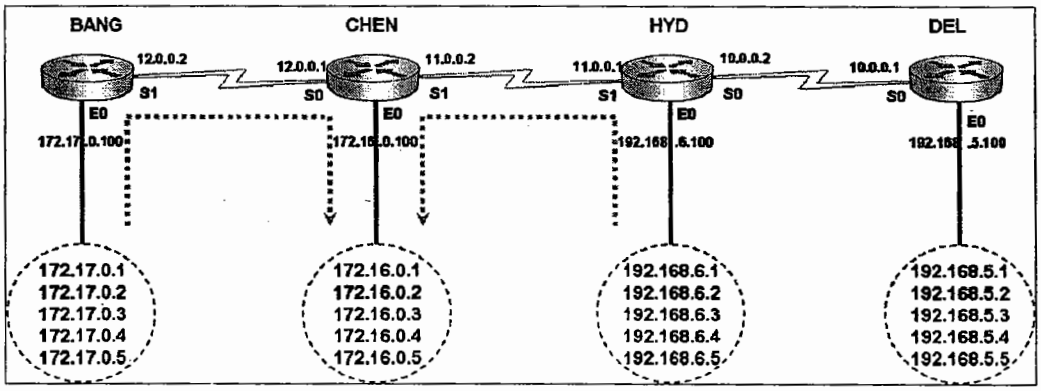
```
Chen(config)# interface    e 0
Chen(config-if)# ip access-group  89   out

Chen# show access-list  89
```

NAGABABU

Extended ACL Examples

1. Don't allow 192.168.6.4, 172.17.0.2, 172.17.0.3 to access 172.16.0.5



Source ip = 192.168.6.4, 172.17.0.2 172.17.0.3

Destination ip = 172.16.0.5

Extended ACL implementation

Chennai router – e 0 interface

Creation:

```
Chen(config)# access-list    167  deny    ip  192.168.6.4  0.0.0.0  172.16.0.5  0.0.0.0
Chen(config)# access-list    167  deny    ip  172.17.0.2   0.0.0.0  172.16.0.5  0.0.0.0
Chen(config)# access-list    167  deny    ip  172.17.0.3   0.0.0.0  172.16.0.5  0.0.0.0
Chen(config)# access-list    167  permit  ip        any              172.16.0.5  0.0.0.0
```

Implementation:

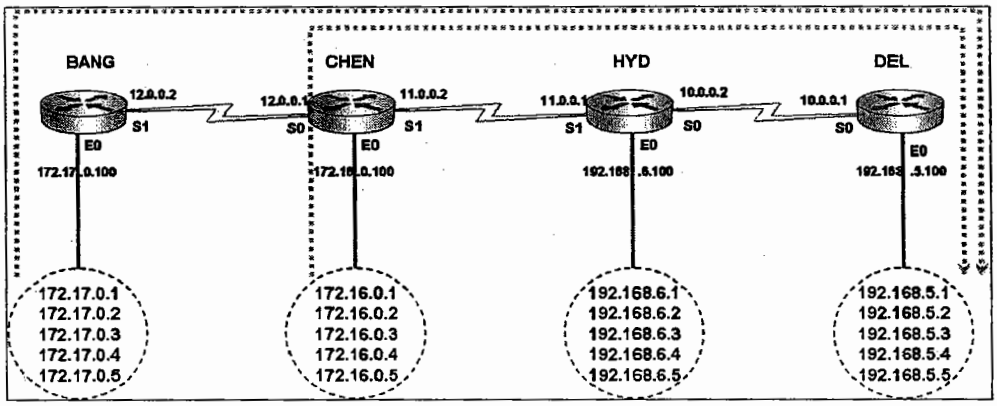
```
Chen(config)# interface     e 0
Chen(config-if)# ip access-group  167   out

Chen# show access-list  167
```

NAGABABU

Extended ACL Examples

2. Permit 172.17.0.1, 172.17.0.5, 172.16.0.3 to access web services on 192.168.5.4



Source ip = 172.17.0.1,172.17.0.5 and 172.16.0.3

Destination ip = 192.168.5.4 : 80

Extended ACL implementation

Delhi router – e 0 interface

Creation:

```
Delhi(config)# access-list   153   permit   tcp   172.17.0.1   0.0.0.0   192.168.5.4   0.0.0.0   eq   80
Delhi(config)# access-list   153   permit   tcp   172.17.0.5   0.0.0.0   192.168.5.4   0.0.0.0   eq   80
Delhi(config)# access-list   153   permit   tcp   172.16.0.3   0.0.0.0   192.168.5.4   0.0.0.0   eq   80
Delhi(config)# access-list   153   deny     tcp         any             192.168.5.4   0.0.0.0   eq   80
Delhi(config)# access-list   153   permit   ip          any                   any
```

Implementation:

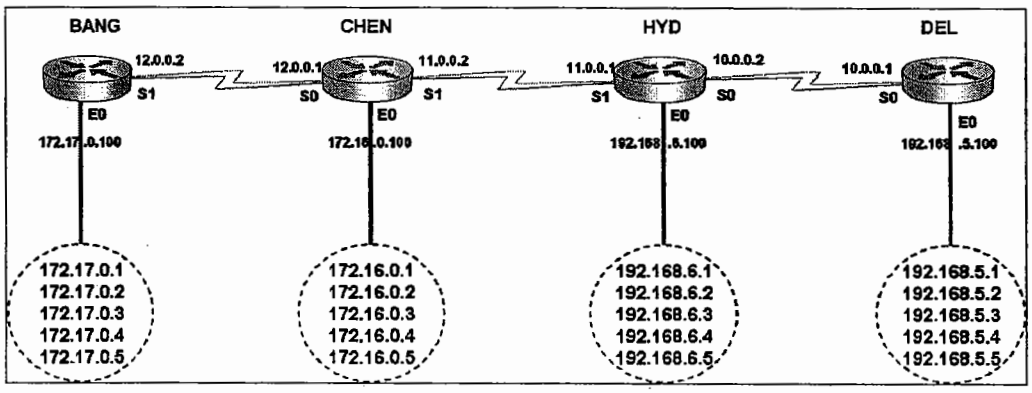
```
Delhi(config)# interface    e 0
Delhi(config-if)# ip access-group   153   out
Delhi# show access-list   153
```

NAGABABU

STUDENTNAME **153** **NAGABABU**

Controlling Telnet Access with ACL

Permit 192.168.5.1, 192.168.5.2 to telnet into Delhi router



Source ip = 192.168.5.1, 192.168.5.2
Destination = Del vty 0 4
Standard ACL implementation
Delhi router – line vty 0 4

Creation:

```
Delhi(config)# access-list      67   permit    192.168.5.1   0.0.0.0
Delhi(config)# access-list      67   permit    192.168.5.2   0.0.0.0
Delhi(config)# access-list      67   deny      any
```

Implementation:

```
Delhi(config)# line vty 0 4
Delhi(config-line)# access-class  67   in
```

```
Delhi# show access-list 67
```

NAGABABU

Numbered ACL limitations:

- Numbered ACL can't be modified once created
- Numbered ACL's have limited number range to create ACL
- To overcome these limitations, Named ACL is introduced

Named ACL

- Named ACLs overcome the limitations with Numbered ACL
- Named ACLs can be modified (ACL statements order can be changed)
- Named ACLs have no limitation (as alphanumerical names are unlimited)
- Named ACLs are case sensitive

Named ACL Types:

Named ACLs are also two types.

- Standard ACL
- Extended ACL

Named standard ACL has same properties of **Numbered standard ACL**
Named extended ACL has same properties of **Numbered extended ACL**

Differences between Numbered & Named ACL

Numbered ACL	Named ACL
Numbers are used Standard : 1-99 Extended : 100-199	Alphanumeric Names are used Standard : ccna Extended : Ccnp23 Names are unique and case sensitive
Can't be modified	Can be modified
Statement order cant be changed	Statement orders can be changed
Limited features	Enhanced features
Types: Standard Extended	Types: Standard Extended

Named ACL Syntax

Standard Named ACL

Creation:

```
Router(config)# ip access-list  standard  <name>
Router(config-std-nacl)# <permit/deny>   <sourceip>   <match>
Router(config-std-nacl)# <permit/deny>   <sourceip>   <match>

Router(config-std-nacl)# <deny/permit>   any
```

Implementation:

```
Router(config)# interface <s0/e0/s1>
Router(config-if)# ip  access-group   <name>   <in/out>
```

Extended Named ACL

Creation:

```
Router(config)# ip access-list  extended  <name>
Router(config-ext-nacl)# <permit/deny>   <protocol >   <sourceip>  <match>   <destinationip>  <match>   <eq>   <port>
Router(config-ext-nacl)# <permit/deny>   <protocol >   <sourceip>  <match>   <destinationip>  <match>   <eq>   <port>

Router(config-ext-nacl)# <deny/permit>   <protocol>          any                  any
```

Implementation:

```
Router(config)# interface <s0/e0/s1>
Router(config-if)# ip  access-group   <name>   <in/out>
```

Checking ACL:

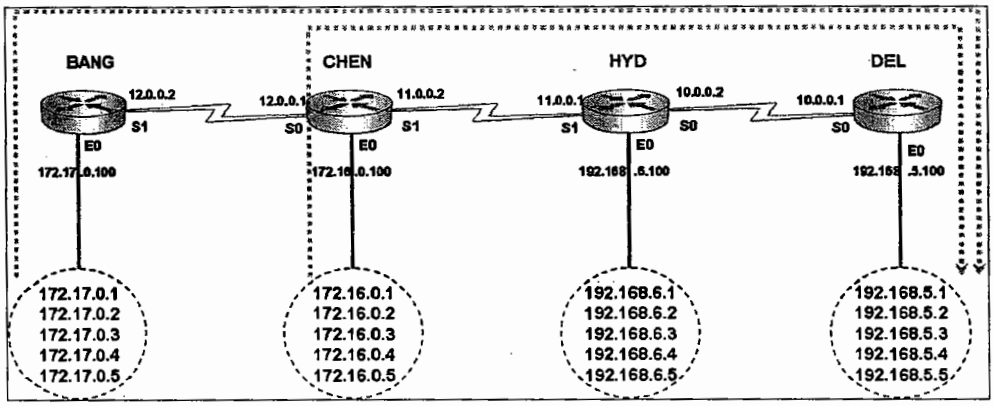
```
Router # show ip access-list
```

Deleting ACL:

```
Router(config)# no ip access-list <standard/extended>  <name>
```

Standard Named ACL Examples

1. Don't allow 172.17.0.1 and 172.16.0.5 to access Delhi network



Source ip = 172.17.0.1 and 172.16.0.5
Destination ip = 192.168.5.0 network
Standard ACL implementation
Delhi router – e 0 interface

Creation:

```
Del(config)# ip access-list  standard  naga
Del(config-std-nacl)# deny   172.17.0.1   0.0.0.0
Del(config-std-nacl)# deny   172.16.0.5   0.0.0.0
Del(config-std-nacl)# permit              any
```

Implementation:

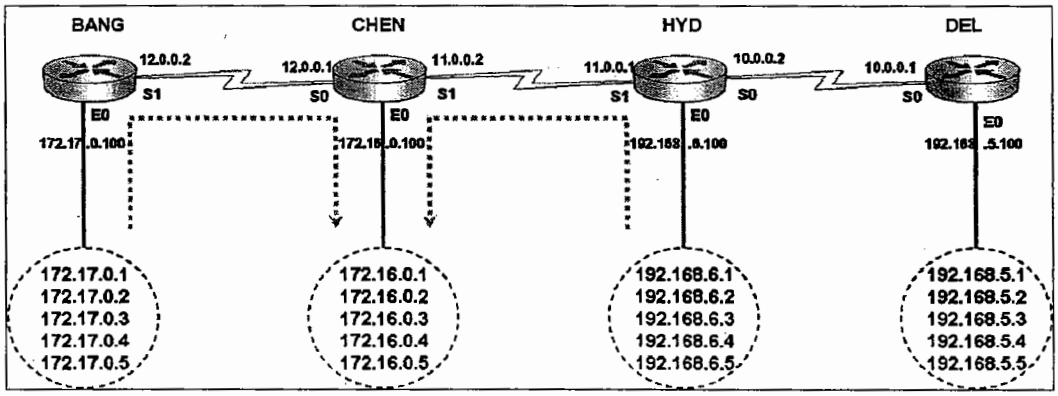
```
Del(config)# interface e 0
Del(config-if)# ip  access-group   naga    out

Delhi# show ip access-list
```

NAGABABU

Standard Named ACL Examples

2. Don't allow 192.168.6.1, 192.168.6.2, 172.17.0.3 to access Chennai network



Source ip = 192.168.6.1, 192.168.6.2 and 172.17.0.3

Destination ip = 172.16.0.0 network

Standard ACL implementation

Chennai router – e 0 interface

Creation:

```
Chen(config)# ip access-list  standard  naga
Chen(config-std-nacl)# deny    192.168.6.1   0.0.0.0
Chen(config-std-nacl)# deny    192.168.6.2   0.0.0.0
Chen(config-std-nacl)# deny    172.17.0.3   0.0.0.0
Chen(config-std-nacl)# permit              any
```

Implementation:

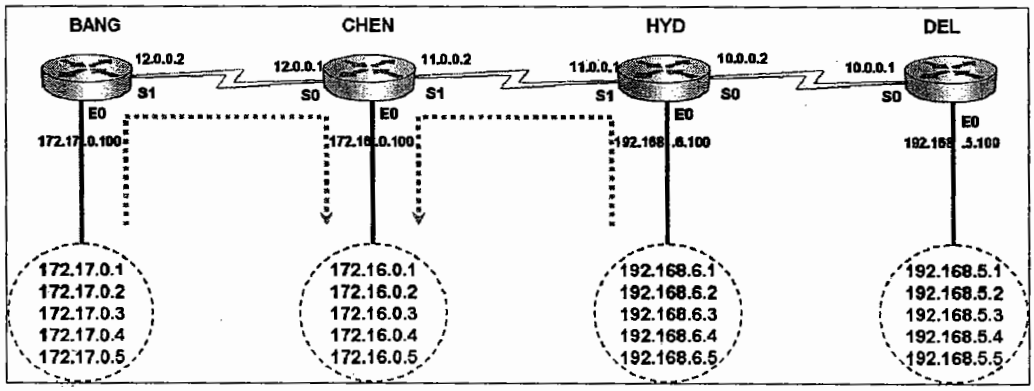
```
Chen(config)# interface e 0
Chen(config-if)# ip  access-group   naga    out

Chen# show ip access-list
```

NAGABABU

Extended Named ACL Examples

1. Don't allow 192.168.6.4, 172.17.0.2, 172.17.0.3 to access 172.16.0.5



Source ip = 192.168.6.4, 172.17.0.2
172.17.0.3

Destination ip = 172.16.0.5

Extended ACL implementation

Chennai router – e 0 interface

Creation:

```
Chen(config)# ip      access-list   extended     naga
Chen(config-ext-nacl)# deny              ip     192.168.6.4   0.0.0.0      172.16.0.5   0.0.0.0
Chen(config-ext-nacl)# deny              ip     172.17.0.2    0.0.0.0      172.16.0.5   0.0.0.0
Chen(config-ext-nacl)# deny              ip     172.17.0.3    0.0.0.0      172.16.0.5   0.0.0.0
Chen(config-ext-nacl)# permit            ip           any                       any
```

Implementation:

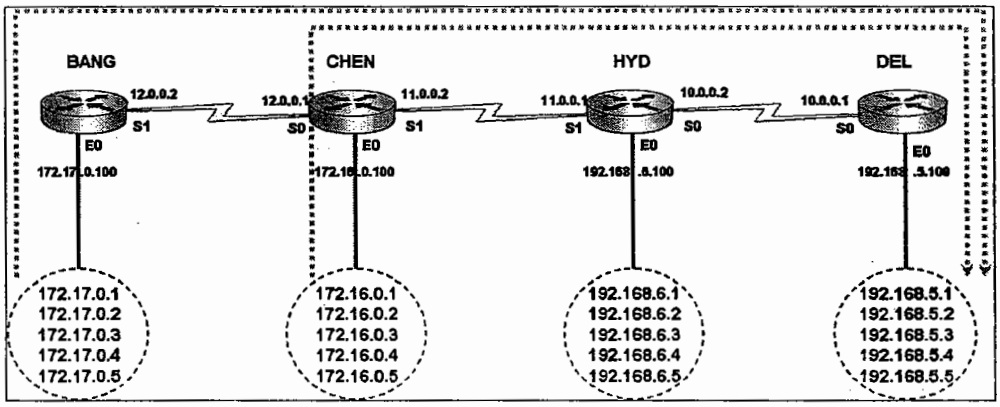
```
Chen(config)# interface    e 0
Chen(config-if)# ip access-group   naga    out

Chen# show  ip  access-list
```

NAGABABU

Extended Named ACL Examples

2. Permit 172.17.0.1, 172.17.0.5, 172.16.0.3 to access web services on 192.168.5.4



Source ip = 172.17.0.1,172.17.0.5 and 172.16.0.3

Destination ip = 192.168.5.4 : 80

Extended ACL implementation

Delhi router – e 0 interface

Creation:

```
Delhi(config)# ip    access-list   extended    naga
Delhi(config-ext-nacl)# permit   tcp   172.17.0.1   0.0.0.0    192.168.5.4  0.0.0.0   eq   80
Delhi(config-ext-nacl)# permit   tcp   172.17.0.5   0.0.0.0    192.168.5.4  0.0.0.0   eq   80
Delhi(config-ext-nacl)# permit   tcp   172.16.0.3   0.0.0.0    192.168.5.4  0.0.0.0   eq   80
Delhi(config-ext-nacl)# deny     tcp         any              192.168.5.4  0.0.0.0   eq   80
Delhi(config-ext-nacl)# permit   ip          any                    any
```

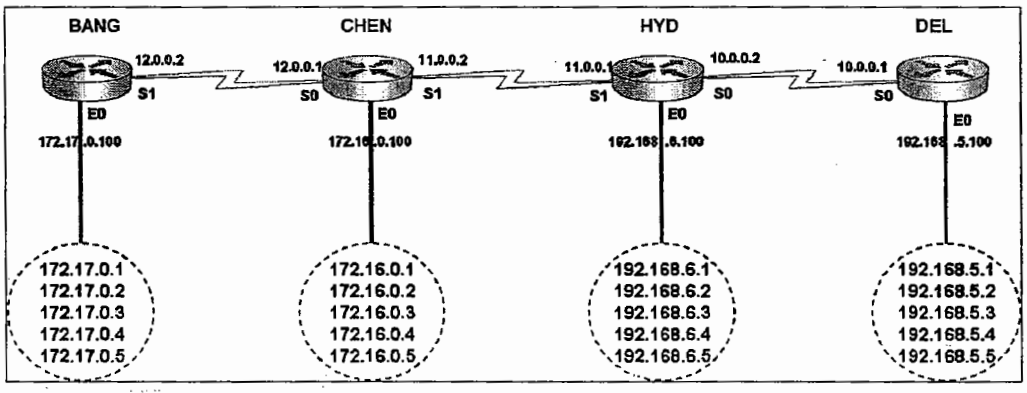
Implementation:

```
Delhi(config)# interface    e 0
Delhi(config-if)# ip access-group   naga    out
Delhi# show  ip  access-list
```

NAGABABU

Controlling Telnet Access with Named ACL

Permit 192.168.5.1, 192.168.5.2 to telnet into Delhi router



Source ip = 192.168.5.1, 192.168.5.2
Destination = Del vty 0 4
Standard ACL implementation
Delhi router – line vty 0 4

Creation:

```
Delhi(config)# ip access-list standard  naga
Delhi(config-std-nacl)# permit    192.168.5.1    0.0.0.0
Delhi(config-std-nacl)# permit    192.168.5.2    0.0.0.0
Delhi(config-std-nacl)# deny              any
```

Implementation:

```
Delhi(config)#  line  vty  0  4
Delhi(config-line)# access-class   naga   in

Delhi# show  ip  access-list
```

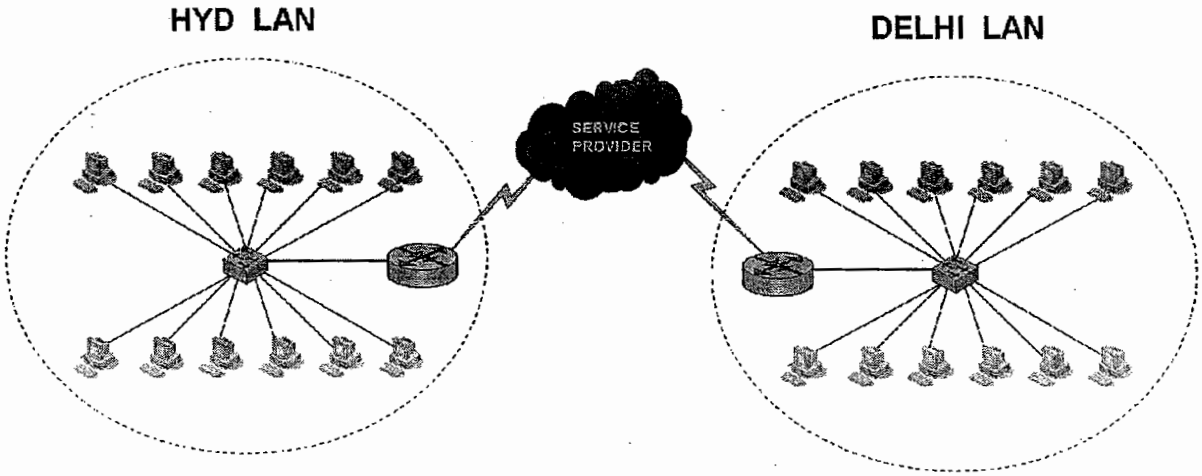
NAGABABU

WAN TECHNOLOGIES

WAN Technologoies

What is WAN?

- Wide Area Network
- Communication between LANs which are in distant areas
  Like different cities, different countries
- Service provider network is the transit area in WAN
- Customer need to pay money to the service provider
- Amount depends on speed of the WAN link



WAN Technologies - Types

- Leased lines
- Circuit Switching
- Packet Switching

NAGABABU

Leased lines

- A pre-established, private connection from one site to another through a provider's network
- Also called a dedicated circuit or a dedicated connection
- Always a **point-to-point** connection between two end points
- Used when there is a constant flow of data, or when a dedicated amount of bandwidth is required
- Leased line is reliable, secured, always up, dedicated connection
- Billing is done on 24/7 basis
- One router interface is connected to one destination site
- PPP and HDLC are used as WAN protocols

TELCO:

- Telecommunication Company. Service provider network

CPE:

- Customer premises Equipment
- Network devices physically located at customer site
- Customer is typically required to maintain the equipment
- Equipment include router, CSU/DSU modems

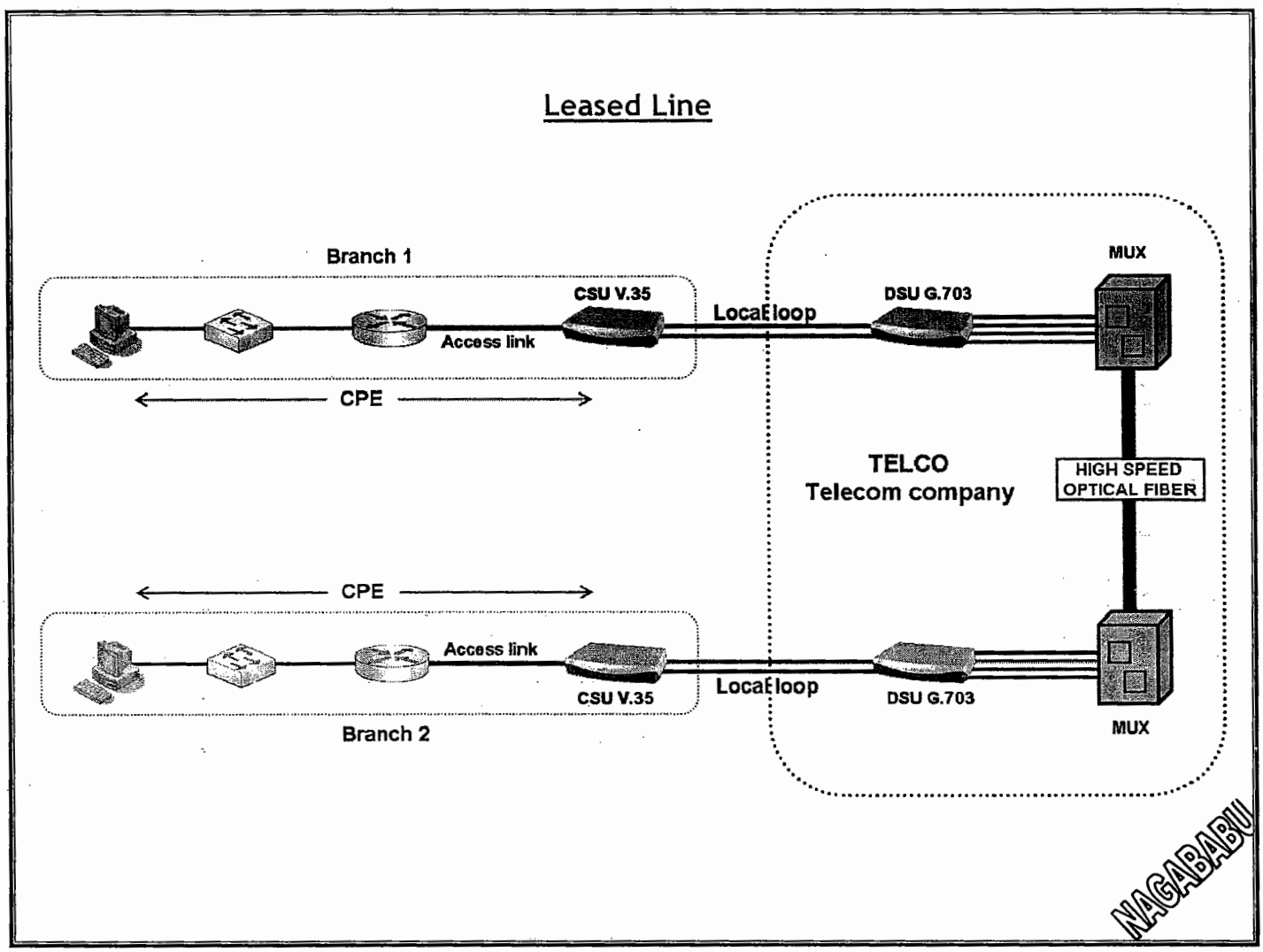
Local Loop:

- The link from the Telco to the customer location
- Also called as "last mile"
- Normally distance is 5 -10 kilometers

Demarcation Point :

- The line between customer site and provide network
- Inside the Demarc is CPE
- Outside the Demarc is the local loop

NAGABABU


Leased Line
Branch 1
CSU V.35
Access link
Local loop
DSU G.703
MUX
CPE
TELCO
Telecom company
HIGH SPEED
OPTICAL FIBER
CPE
Access link
CSU V.35
Local loop
DSU G.703
MUX
Branch 2
NAGABABU

HDLC & PPP

HDLC and PPP are WAN link encapsulation protocols (LLC)

HDLC:

- High level data link control
- Cisco proprietary Protocol
- Doesn't support authentication
- No data compression

HDLC configuration:

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

PPP:

- Point to Point Protocol
- Open standard
- Supports authentication
- Data compression
- PPP has three main components
  - Frame format (encapsulation)
  - Link control Protocol (LCP)
  - Network control Protocol (NCP)
- LCP and NCP are responsible for establishing, configuring, authenticating and testing PPP connection

PPP configuration:

```
Router (config)#  interface  s 0
Router (config-if)# encapsulation ppp
```

PPP Authentication

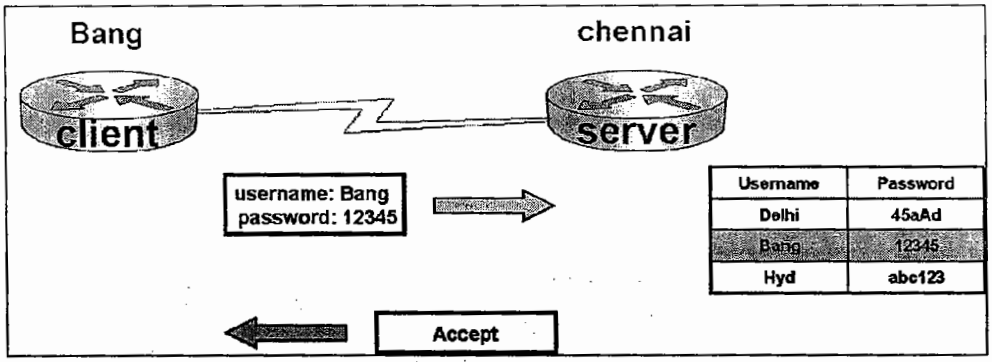
PPP uses two methods to support authentication : PAP and CHAP

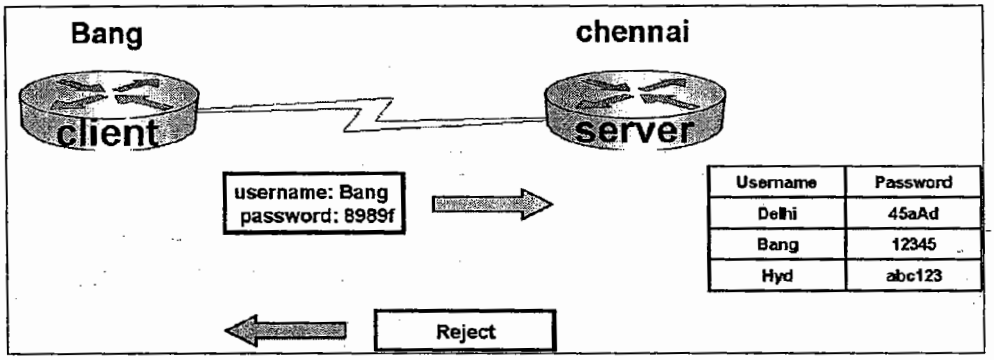
PAP - Password Authentication Protocol

CHAP - Challenge Handshake Authentication Protocol

PAP

- Password Authentication Protocol
- Simplest but less secure
- Two way hand shake process
- Source sends its username and password in clear text to destination
- Destination compares username and password with its database
- If it is correct then sends accept message otherwise sends reject message





PAP server configuration:

```
Chennai (config)#  username <bang> password <12345>
Chennai (config)#  int s 0
Chennai (config-if)# encapsulation ppp
Chennai (config-if)# ppp authentication pap
```

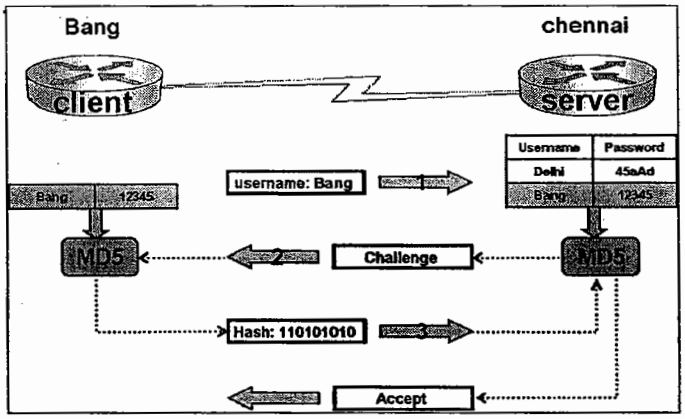
NAGABABU

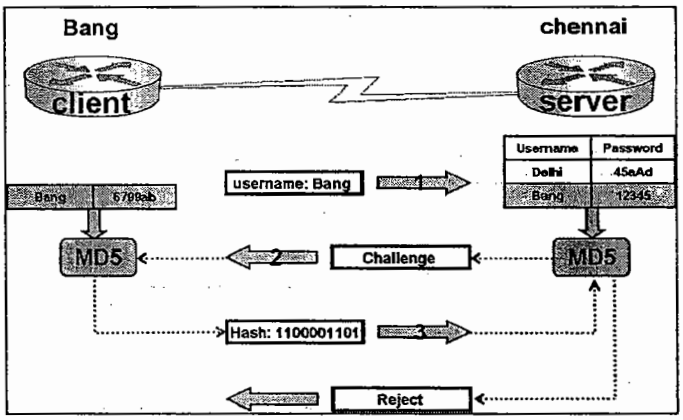
PAP client configuration:

```
Bang (config)# interface s 1
Bang (config-if)# encapsulation ppp
Bang (config-if)# ppp pap sent-username <bang> password <12345>
```

CHAP

- Challenge Handshake Authentication Protocol
- Three way hand shake process & secured than PAP
- Source sends its username to destination.
- Destination looks at username/password in its database and generates a challenge value using md5 and sends that value to source
- Source uses that challenge and generates a hash value and sends it to destination
- Destination verify that hash value and sends accept or reject message
- Password is never sent on the link to provide security





CHAP server configuration:

```
Chennai (config)#  username <bang> password <12345>
Chennai (config)#  int s 0
Chennai (config-if)# encapsulation ppp
Chennai (config-if)# ppp authentication chap
```

CHAP client configuration:

```
Bang (config)# interface s 1
Bang (config-if)# encapsulation ppp
Bang (config-if)# ppp-authentication chap

Bang# debug ppp authentication
```

Circuit Switching

- A dial-up connection through a provider's voice-grade network
- Either uses an analog modem or an ISDN connection
- Used when only a slow-speed connection is needed, or when there is not much of a need to transfer a lot of data
- One call establishes a circuit to one destination site
- Establishes logical circuits between source and destination (circuit switching)
- PPP, HDLC, SLIP are the protocols used in circuit switching

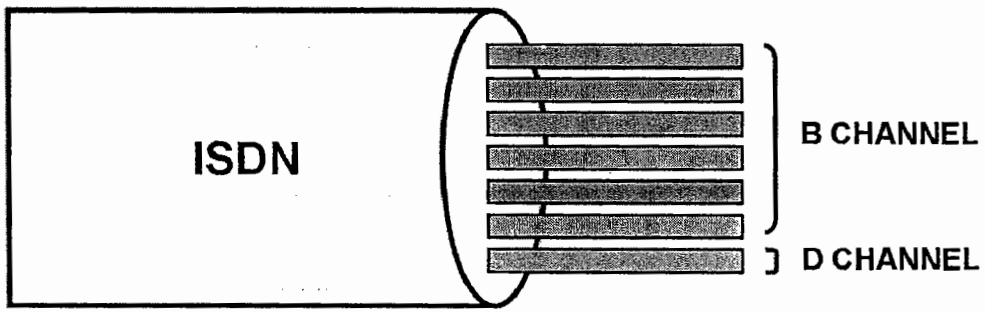
ISDN

- Integrated services digital Network
- Guaranteed Bandwidth
- Digital Network (Error prune)
- Faster connectivity (2sec)
- Multiple services are processed simultaneously
- Economical
- Suitable for networks that require slow-speed connection
- Billing is done based on usage

ISDN channels:

ISDN contains two channels

- B-Channel - Bearer channel : carries the data
- D-Channel - Control channel : carries control information/signaling



ISDN Interface Types

- BRI - Basic Rate Interface
- PRI - Primary Rate Interface

BRI - PRI Bandwidths

BRI Bandwidth:

B-channel = 64 kbps
D-channel = 16 kbps

Bandwidth = 2B+1D = 128 +16 = **144kbps**

PRI Bandwidths:

B-channel = **64** kbps
D-channel = **64** kbps

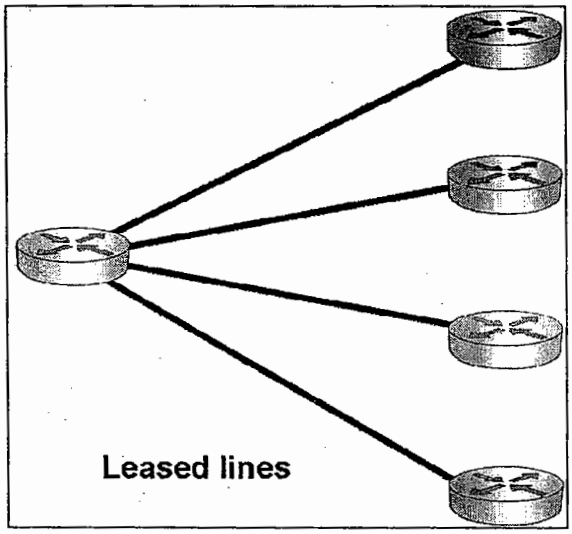
PRI has two standards globally

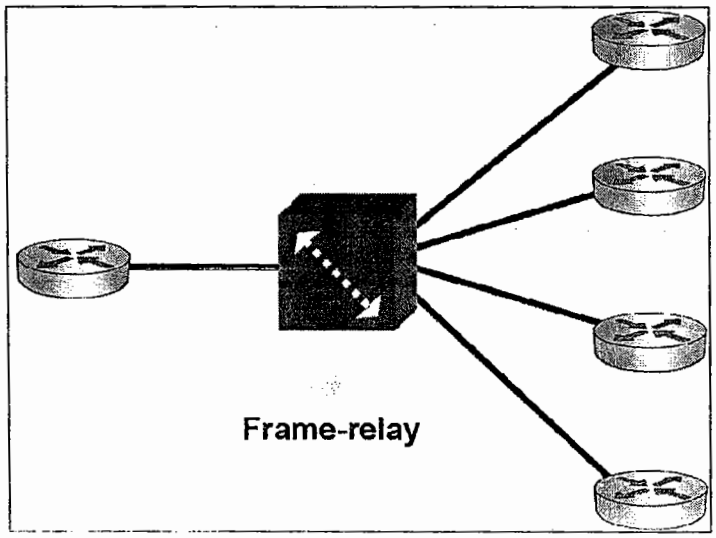
North American standard	European standard
23B + 1D 23 x 64 + 64 kbps **1.544 Mbps**	30B + 1D 30 x 64 + 64 kbps **2.048 Mbps**
Called as **T1** link	Called as **E1** link
U.S. follows this standard	India follows this standard

Packet Switching

Frame-relay

- Contains all features of leased line and ISDN
- VCs reduce required No of leased lines significantly
- PVC & SVC offers flexibility
- Very economical
- Billing can be done on any basis
- Bandwidth may boost (Free)
- Suitable for all scenarios
- Availability is an issue
- No frame-relay technology in India





NAGABABU

Frame-relay terminology

FRS	Frame relay switch
VC	Virtual Circuit (A logical circuit established between FRS)
PVC	Permanent Virtual Circuit
SVC	Switched/semi Virtual Circuit
DLCI	Data link connection identifier (tag attached to VC for identification)
CIR	Committed information rate (bandwidth committed by service provider)
LMI	Local Management interface (keep alive messages)
FECN	Forward Explicit congestion notification
BECN	Backward Explicit congestion notification
BE	Burst Excessive (boosting bandwidth)

FRS:

The switch used at service provider end in frame-relay network

VC:

Logical connection between two Frame relay switches

Permanent Virtual Circuit (PVC):

The VC that is always available. Similar to dedicated line

Switched Virtual Circuit (SVC):

The VC that is established when needed. Similar to ISDN

DLCI:

It is Identification for VC. Range is 16-1007.
It is Local reference to one end of VC.
The DLCI numbers are assigned by the frame relay service providers.

CIR:

The bandwidth committed by service provider
The maximum allowed bandwidth through the PVC from one end to the other.
Each PVC can have a unique CIR.

LMI:

Signal checks the keep alive status: DTE to DCE
Signaling between router and the frame relay switch.
LMI does not travel across the entire PVC from one end to the other.
LMI types: q933a, cisco, ansi

FECN:

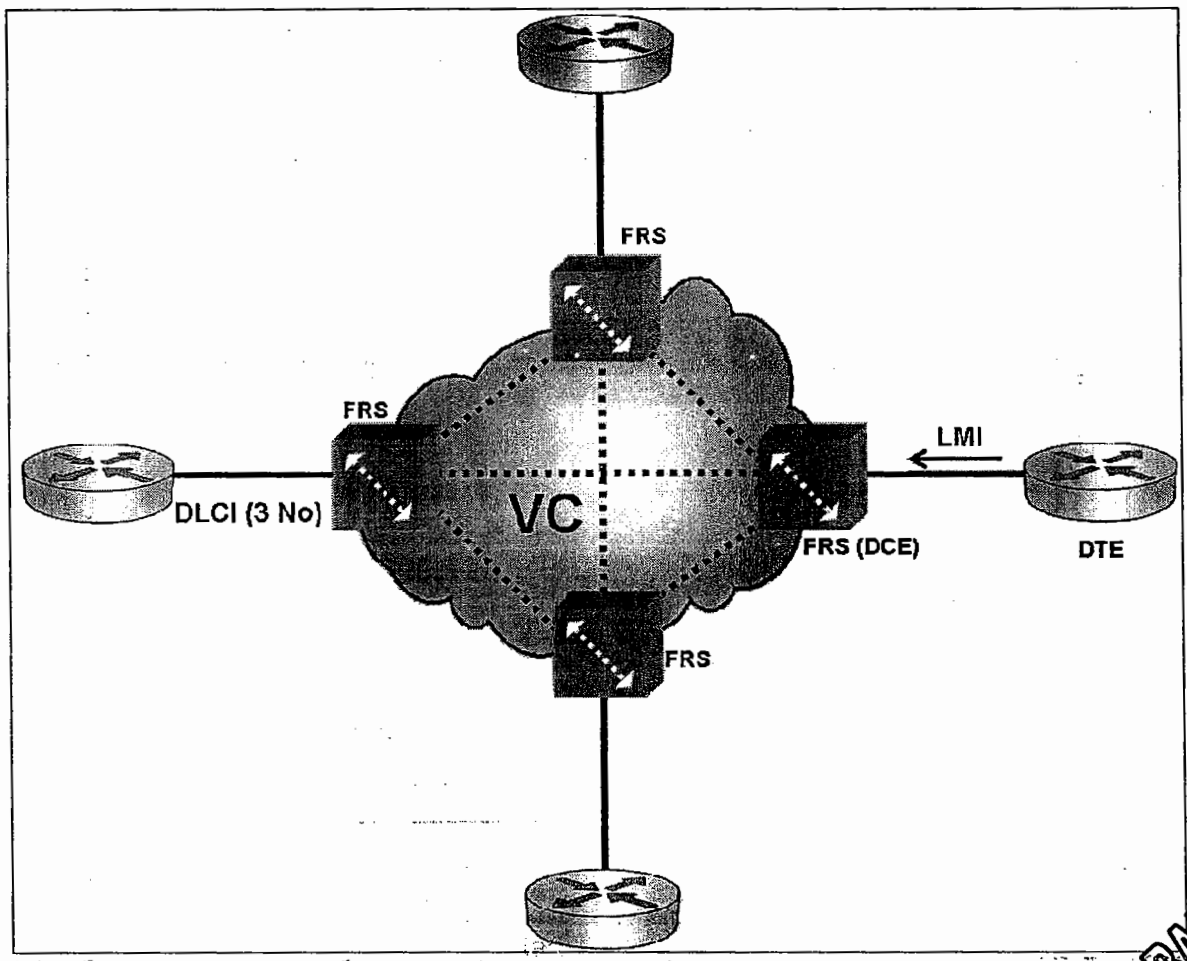
Forward explicit congestion notification
Message from FRS to source if congestion occurs between FRS and destination

BECN:

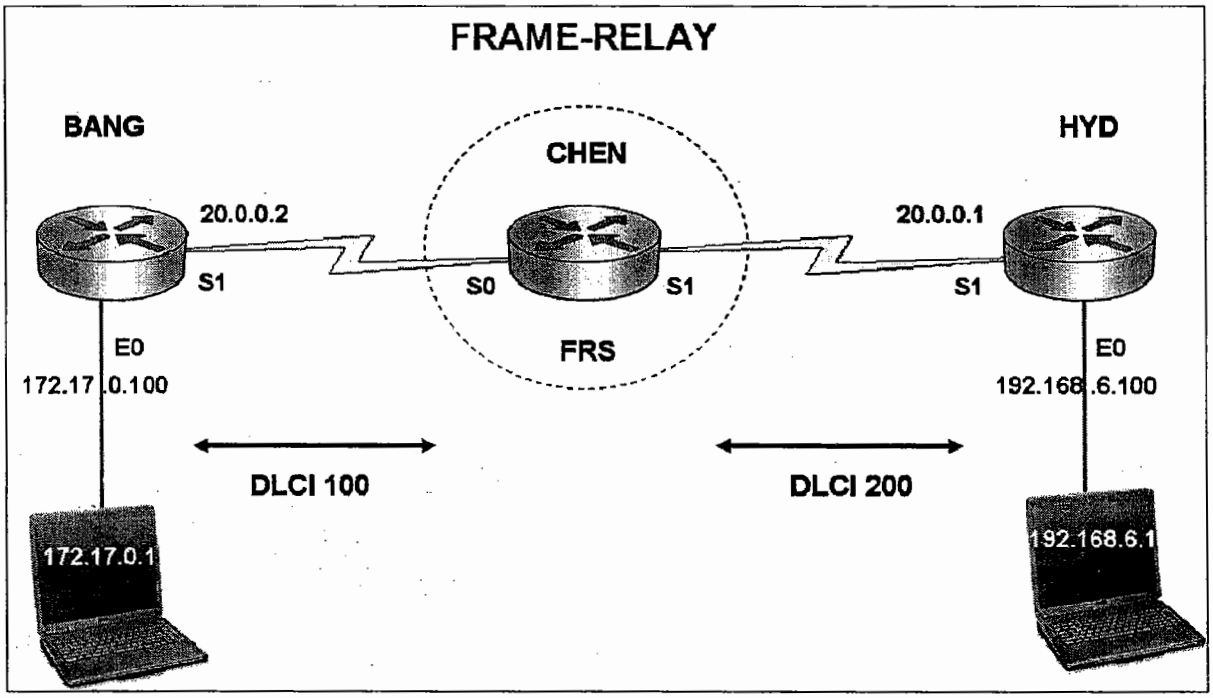
Backward explicit congestion notification
Message from FRS to destination, if congestion occurs between FRS and source

BE:

Frame-relay boosts the bandwidth of VC if network is free.



Frame-relay configuration (FRS)



Frame-relay configuration (FRS)

End point 1 configuration:

```
Bang(config)# int s 1
Bang(config-if)# ip address 20.0.0.2 255.0.0.0
Bang(config-if)# no shutdown

Bang(config-if)# encapsulation frame-relay

Bang(config-if)# frame-relay interface-dlci 100
Bang(config-if)# frame-relay lmi-type cisco
Bang(config-if)# exit

Bang(config)# router eigrp 10
Bang(config-router)# network 20.0.0.0
Bang(config-router)# network 172.17.0.0
Bang(config-router)# end
```

End point 2 configuration:

```
Hyd(config)# int s 1
Hyd(config-if)# ip address 20.0.0.1 255.0.0.0
Hyd(config-if)# no shutdown

Hyd(config-if)# encapsulation frame-relay

Hyd(config-if)# frame-relay interface-dlci 200
Hyd(config-if)# frame-relay lmi-type cisco
Hyd(config-if)# exit

Hyd(config)# router eigrp 10
Hyd(config-router)# network 20.0.0.0
Hyd(config-router)# network 192.168.6.0
Hyd(config-router)# end
```

FRS configuration:

```
Chen(config)# frame-relay switching

Chen(config)# int s 0
Chen(config-if)# no ip address
Chen(config-if)# no shutdown

Chen(config-if)# encapsulation frame-relay

Chen(config-if)# clockrate 64000
Chen(config-if)# bandwidth 64

Chen(config-if)# frame-relay intf-type dce
Chen(config-if)# frame-relay route 100 interface  serial    1     200
Chen(config-if)# exit

Chen(config)# int s 1
Chen(config-if)# no ip address
Chen(config-if)# no shutdown

Chen(config-if)# encapsulation frame-relay

Chen(config-if)# clock rate 64000
Chen(config-if)# bandwidth 64

Chen(config-if)# frame-relay intf-type dce
Chen(config-if)# frame-relay route 200 interface    serial    0     100
Chen(config-if)# exit
```

For practice, Router is configured as FRS.
In real time scenario FRS is different.

NAT

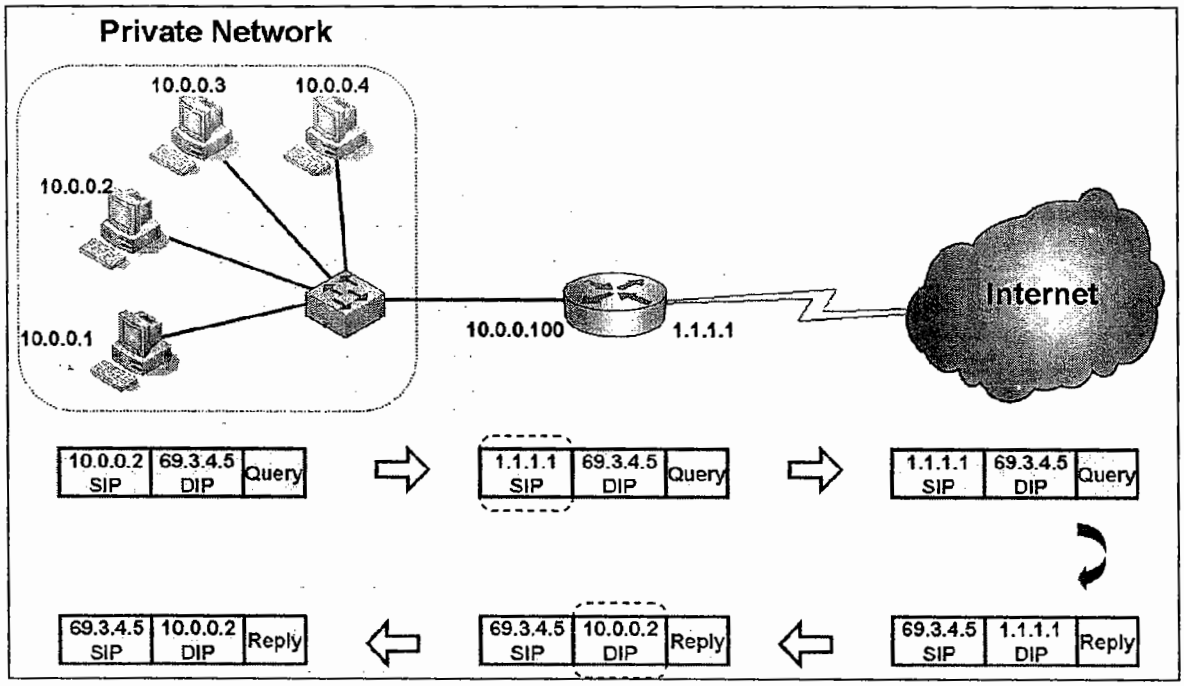
What is NAT?

- Network Address Translation
- All the Local Area Networks use private IP addressing scheme
- Private IP addresses are not routable in public network
- To access public Network public IP address is required

- Systems within the LAN communicate with private IP addresses
  These private IP addresses need to be translated into public IP addresses while accessing public network (internet)
- When reply comes back, Public IP addresses are translated back to private IP addresses before forwarding data to system

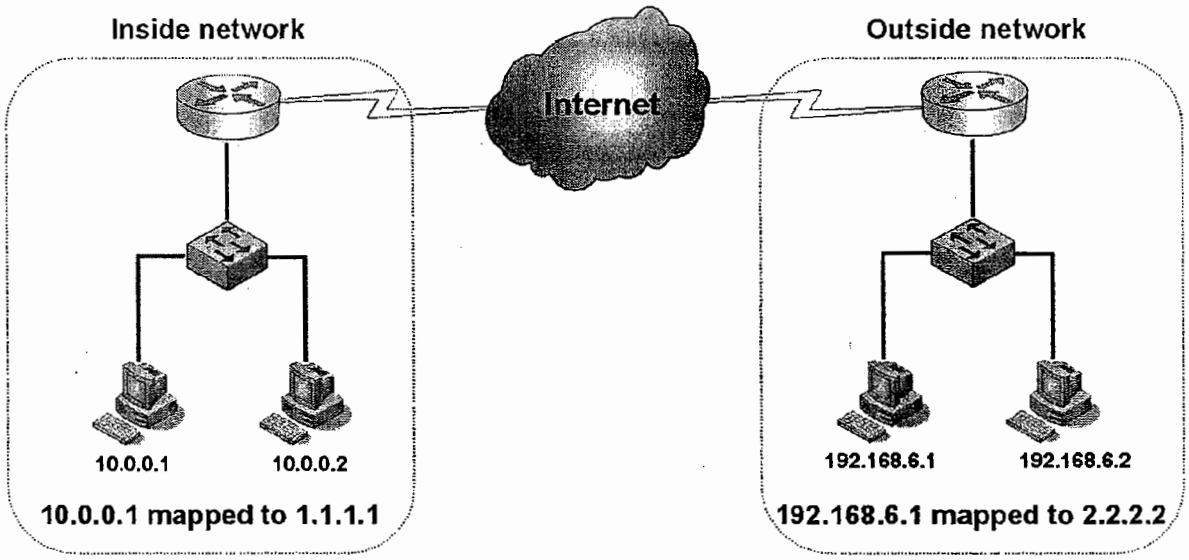
- **Private to Public** and **Public to Private IP** translation is called NAT
- Generally NAT operations are taken care by router

NAT Operations:



NAT terms:

Inside local	An inside device with an assigned private IP address
Inside global	An inside device with a mapped public IP address
Outside local	An outside device with an assigned private IP address
Outside global	An outside device with a mapped public IP address



Inside local	10.0.0.1
Inside global	1.1.1.1
Outside local	192.168.6.1
Outside global	2.2.2.2

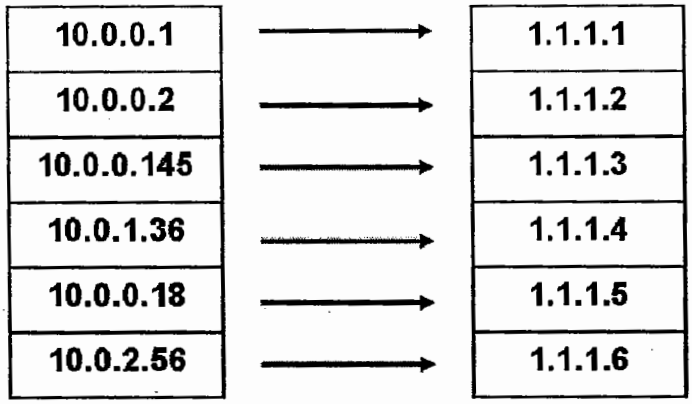
Types of NAT:

- NAT is basically two types
  - Static NAT
  - Dynamic NAT

Static NAT:

- In static NAT one private IP address is mapped to one Public IP
- Also called as 1 to 1 NAT
- It is not possible to map every private IP to a public IP
- Generally static NAT is used for public servers

STATIC NAT

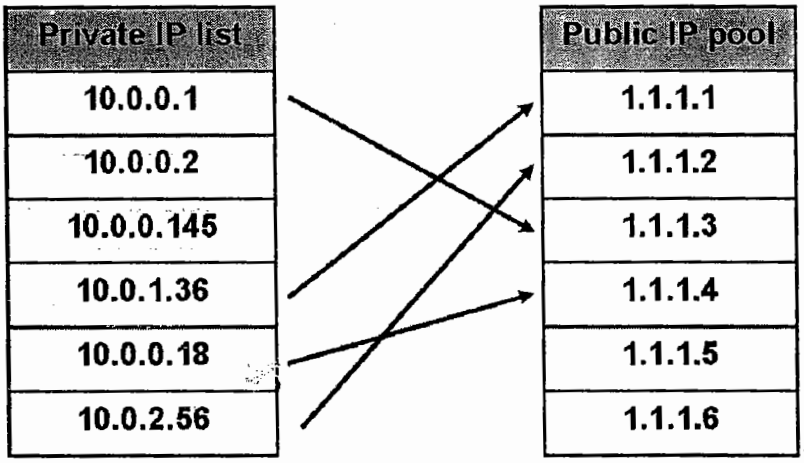


Dynamic NAT:

- In dynamic NAT a group of private ip addresses are mapped to a pool of public IP addresses
- NAT happens dynamically on First come First serve basis

- Access-list is created to specify a group of private ip addresses
- A pool is created with public IP addresses
- Access-list is mapped with the pool

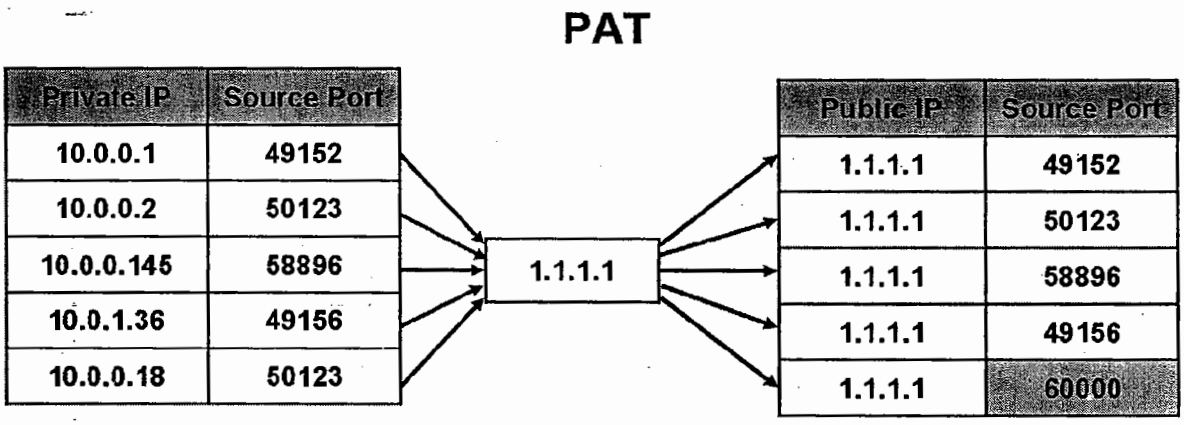
DYNAMIC NAT



What is PAT?

- Port Address Translation
- Overloading of NAT is called PAT
- In PAT all the private ip addresses are translated to a single Public IP address
- Router uses source port number as a reference to avoid ambiguity in translations
- If source port is also same, translates that port to a random value and memorize them in cache
- When the reply comes back, Public IP address is translated to private IP addresses with source port reference
- Translated port numbers are changed to original value

With PAT multiple systems can access public network with a single Public IP Address



Static NAT configuration

Syntax:

IP address Mapping:

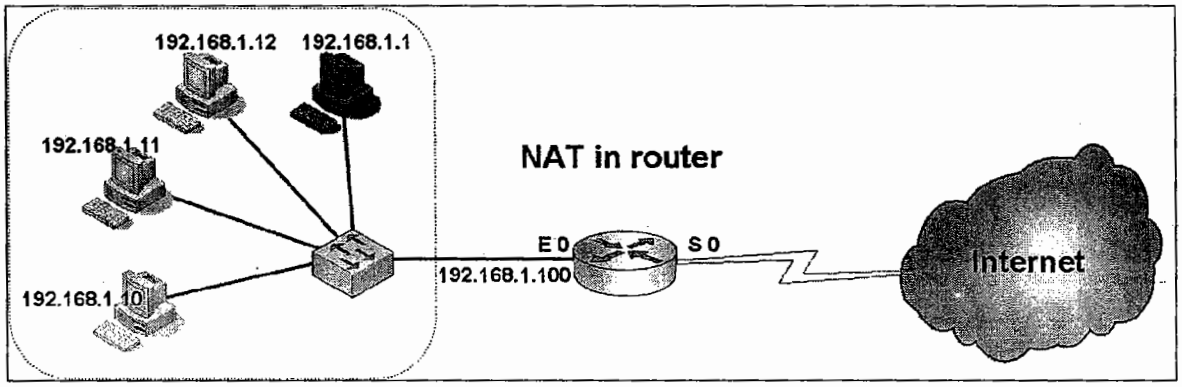
Router(config)# ip nat inside source static <inside local> <inside global>

Apply NAT on the interface:

Router(config)# interface <s0/e0/s1>
Router(config-if)# ip nat inside | outside

Example:

NAT 192.168.1.1 to 200.200.200.1



Configuration:

IP address Mapping:

Router(config)# ip nat inside source static 192.168.1.1 200.200.200.1

Apply NAT on the interface:

Router(config)# interface e 0
Router(config-if)# ip nat inside

Router(config)# interface s 0
Router(config-if)# ip nat outside

Checking NAT results:

Router# show ip nat translations
Router# show ip nat statistics

Dynamic NAT configuration

Syntax:

Create ACL:

Router(config)# access-list <1-99> permit <sourceip> <match>

Create NAT Pool:

Router(config)# ip nat pool <poolname> <starting ip> <ending ip> netmask <mask>

Map ACL to NAT Pool:

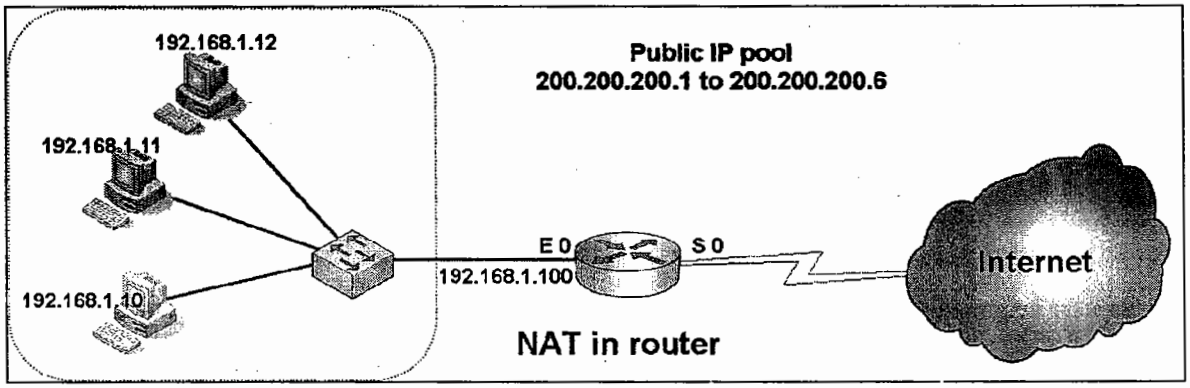
Router(config)# ip nat inside source list <1-99> pool <poolname>

Apply NAT on the interface:

Router(config)# interface <s0/e0/s1>
Router(config-if)# ip nat inside | outside

Example:

NAT 192.168.1.10, 192.168.1.11, 192.168.1.12 to public IP pool dynamically



Configuration:

Create ACL:

Router(config)# access-list 73 permit 192.168.1.10 0.0.0.0
Router(config)# access-list 73 permit 192.168.1.11 0.0.0.0
Router(config)# access-list 73 permit 192.168.1.12 0.0.0.0

Create NAT Pool:

Router(config)# ip nat pool naga 200.200.200.1 200.200.200.6 netmask 255.255.255.240

Map ACL to NAT Pool:

Router(config)# ip nat inside source list 73 pool naga

Apply NAT on the interface:

Router(config)# interface e 0
Router(config-if)# ip nat inside

Router(config)# interface s 0
Router(config-if)# ip nat outside

NAGABABU

PAT configuration

PAT is Dynamic NAT with single public IP in the pool

Syntax:

Create ACL:

Router(config)# access-list <1-99> permit <sourceip> <match>

Create NAT Pool:

Router(config)# ip nat pool <poolname> <public ip> <public ip> netmask <mask>

Map ACL to NAT Pool:

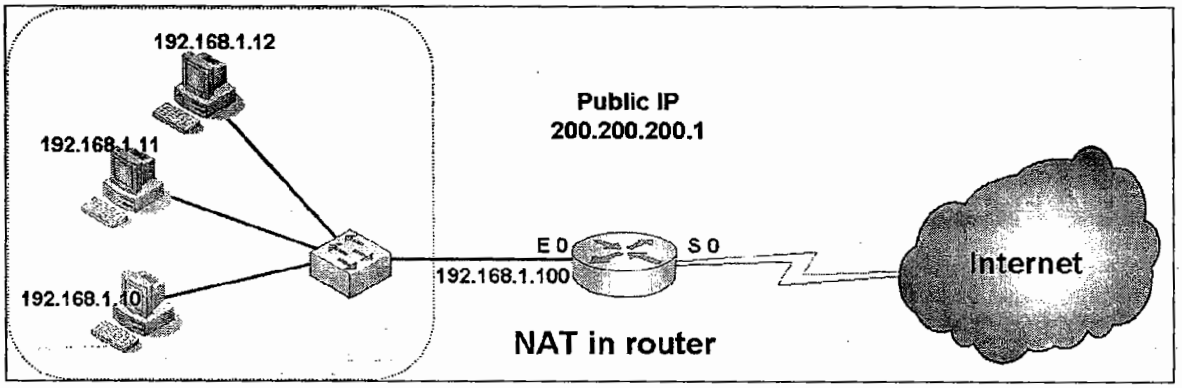
Router(config)# ip nat inside source list <1-99> pool <poolname> overload

Apply NAT on the interface:

Router(config)# interface <s0/e0/s1>
Router(config-if)# ip nat inside | outside

Example:

PAT 192.168.1.10, 192.168.1.11, 192.168.1.12 to public IP 200.200.200.1



Configuration:

Create ACL:

Router(config)# access-list 19 permit 192.168.1.10 0.0.0.0
Router(config)# access-list 19 permit 192.168.1.11 0.0.0.0
Router(config)# access-list 19 permit 192.168.1.12 0.0.0.0

Create NAT Pool:

Router(config)# ip nat pool naga 200.200.200.1 200.200.200.1 netmask 255.255.255.252

Map ACL to NAT Pool:

Router(config)# ip nat inside source list 19 pool naga overload

Apply NAT on the interface:

Router(config)# interface e 0
Router(config-if)# ip nat inside

Router(config)# interface s 0
Router(config-if)# ip nat outside

NAGABABU

SDM (Security Device Manager)

What is SDM?

- Generally CLI is used to manage IOS devices
- Cisco also supports GUI as an alternative management method
- SDM- Security device manager is one GUI product to manage IOS devices

- SDM is a web-based application, implemented with Java
- SDM can manage the basic administration and security features

- SDM is installed in the router's flash memory and is remotely accessed from an administrator's desktop using web browser with Java & SSL(secure socket layer)
- Cisco started supporting SDM in the routers released after June 2003
- Routers manufactured before June 2003 do not support SDM

PC requirements to use SDM:

- Microsoft XP / Vista / 2003 / 2000 professional
- Fire fox 1.0.6 and later / Internet Explorer 5.5 and later / Netscape 7.1, 7.2, 9.0
- JRE(Java Run time Environment) 1.4.2 (08) (minimum)
- Screen Resolution 1024 x 768 as a minimum

SDM files in Router Flash:

- SDM is not supported on all IOS routers
- IOS router that supports SDM includes following files in Flash memory
  - Common.tar
  - Es.tar
  - Home.shtml
  - Home.tar
  - Sdmconfig-xxxx.cfg
  - Sdm.tar
  - Xxxx.sdf
  - Securedesktop-ios-xxx-k9.pkg
  - Sslclient-win-xxxx.pkg
  - Wlanui.tar

(Use show flash or dir commands in privilege mode to view these files)

Necessary router configuration to access SDM:

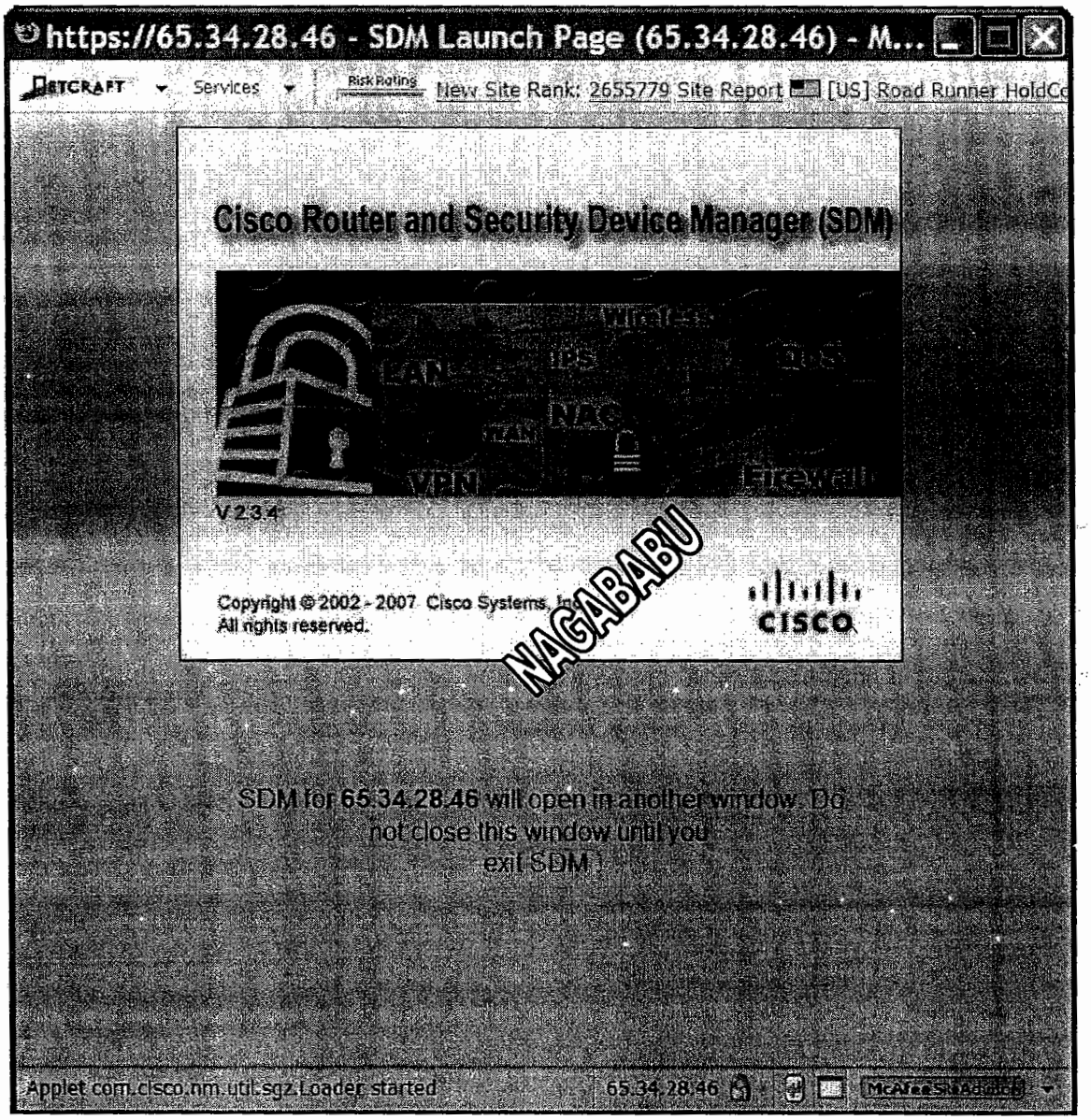
```
Router(config)# hostname <routername>
Router(config)# ip domain-name <domainname>
Router(config)# ip http server
Router(config)# ip http secure-server
Router(config)# ip http authentication local
Router(config)# username <username> privilege 15 secret <password>
Router(config)# ip http timeout-policy idle <seconds> life <seconds>
Router(config)#line vty 0 15
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input ssh
```

Accessing SDM

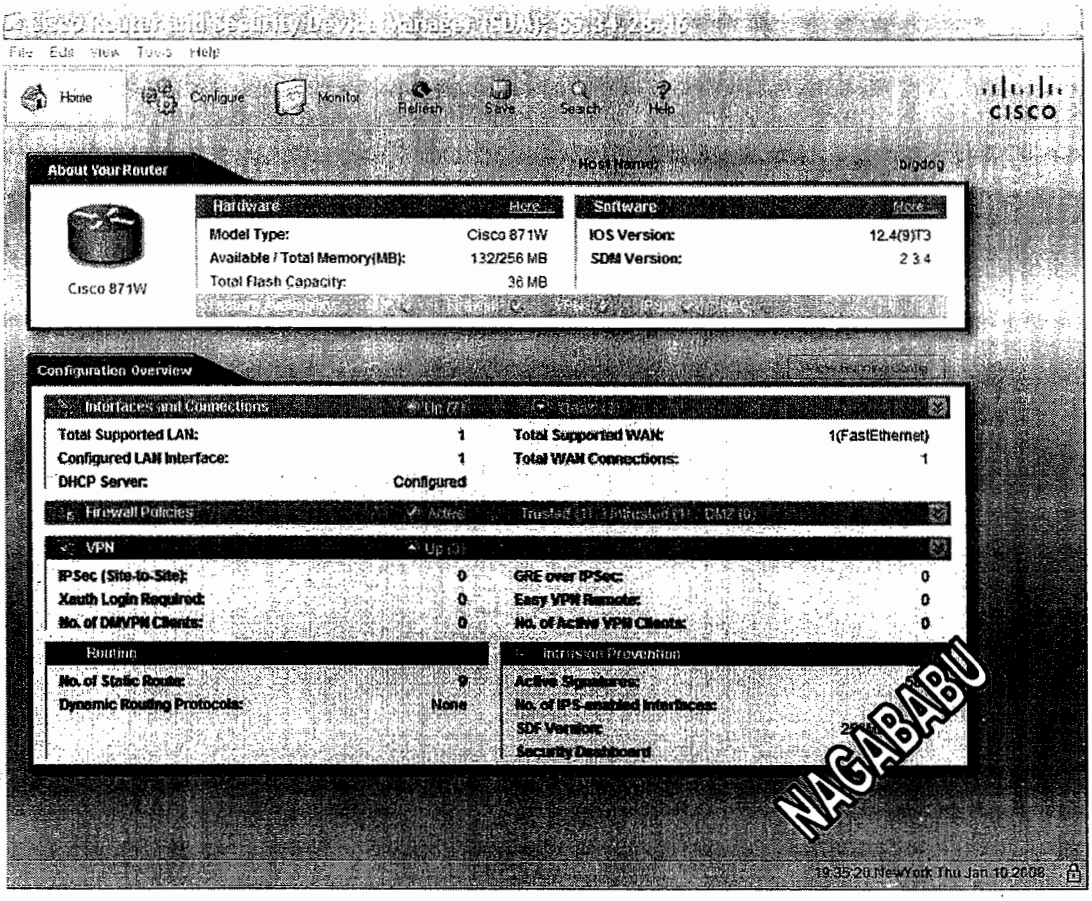
Type https:// <router-ip address> in web browser to access SDM

- 10.10.10.1 is the default ip (https://10.10.10.1)

Startup Wizard (SSL interface):



SDM Home Screen:



SDM Home Screen contains the following tabs:

Home:
Displays home page - summary of router configuration

Configure:
To change the configuration of the router

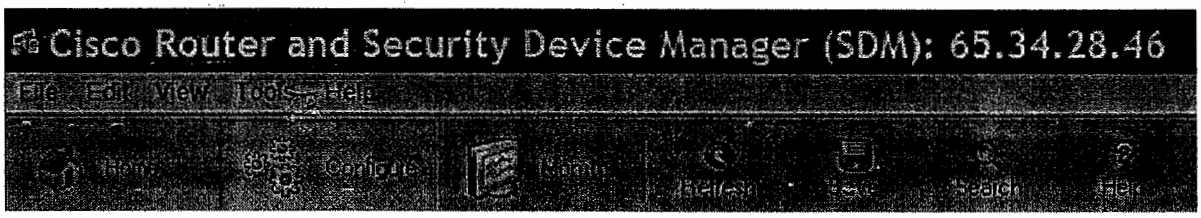
Monitor
Information of the router such as logging and interface statistics

Refresh:
Refresh configuration (pulls running configuration into SDM)

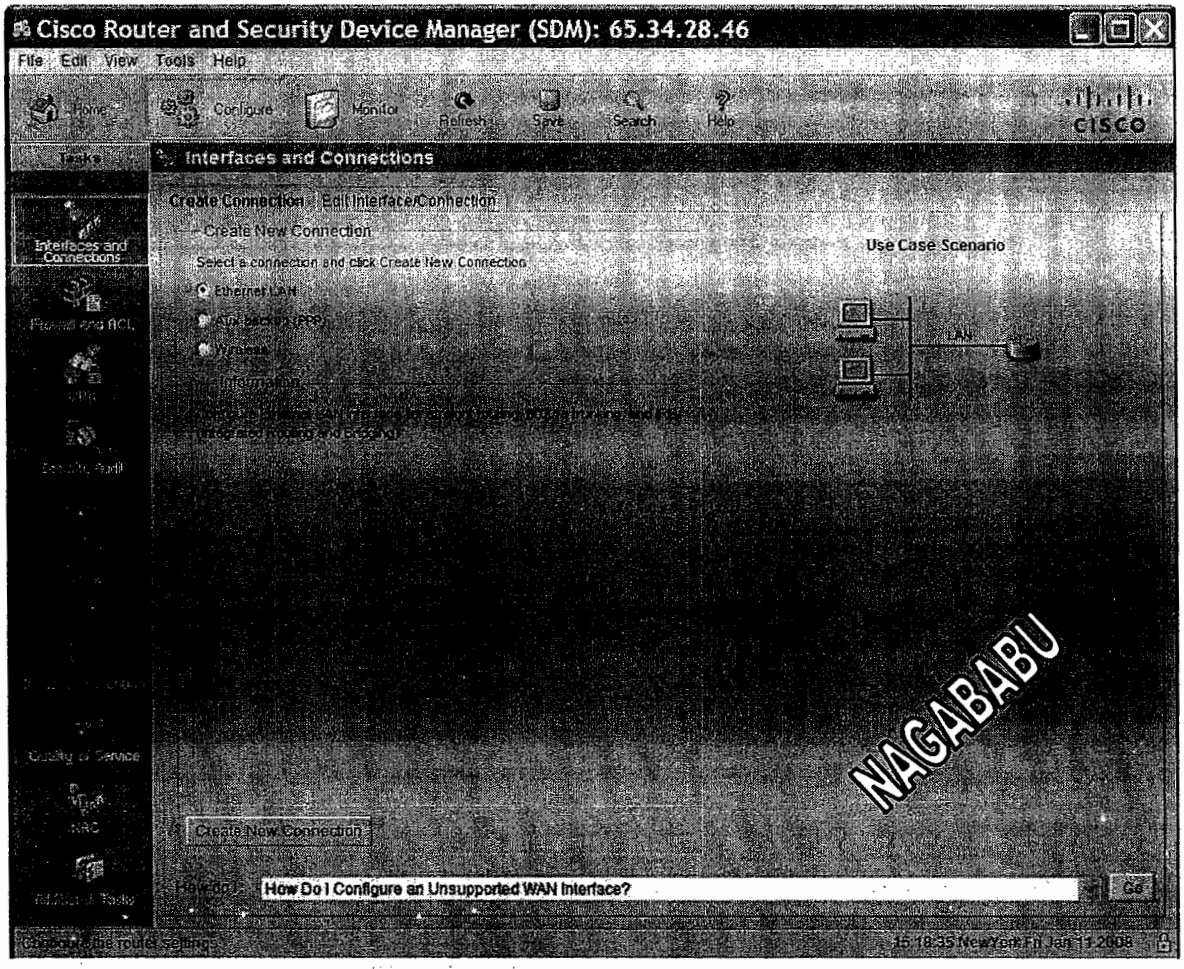
Save:
Saves configuration into NVRAM

Search:
Quick search to find a screen. Displays hyperlinks for the results.

Help:
Help on how to use SDM to configure the router



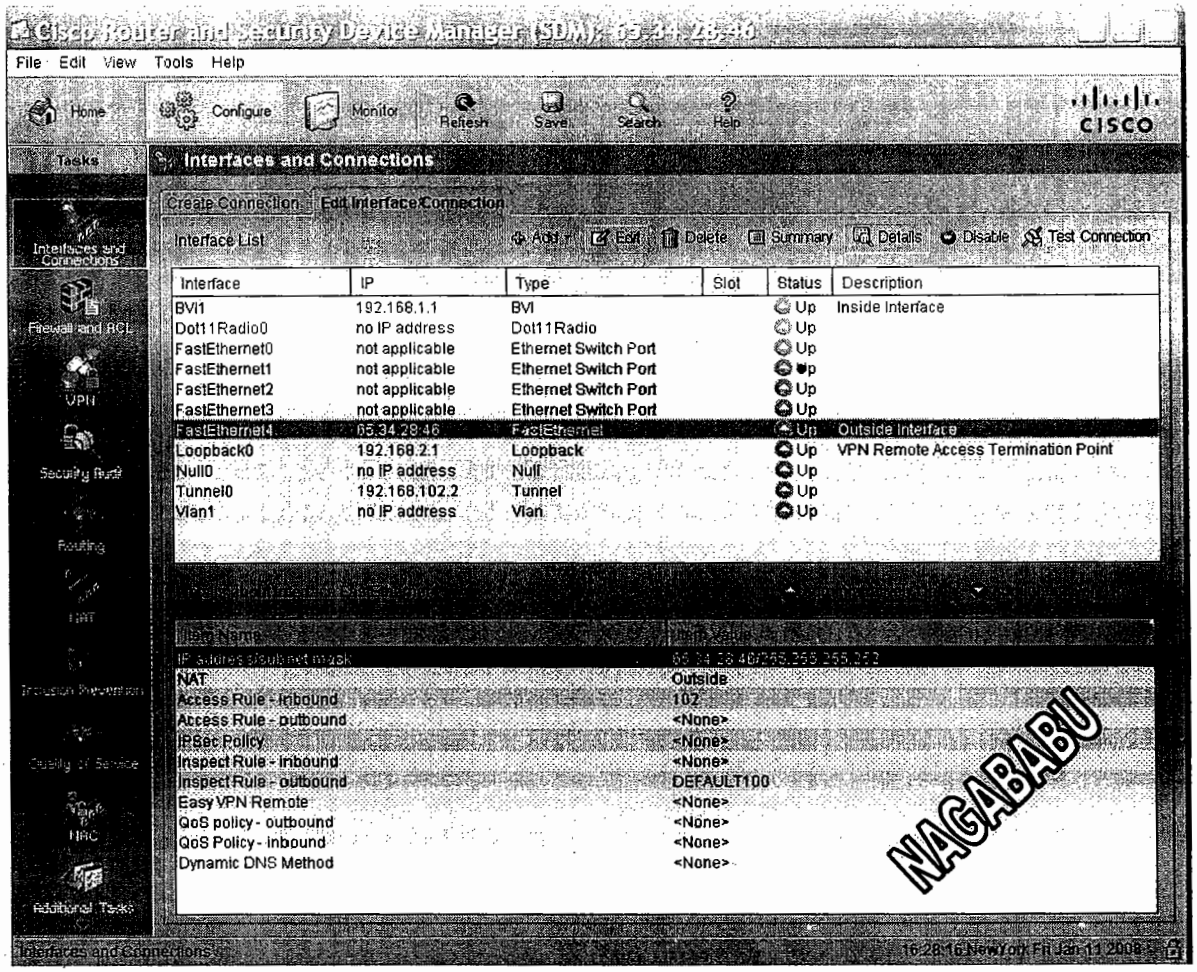
Basic Router configuration using SDM:

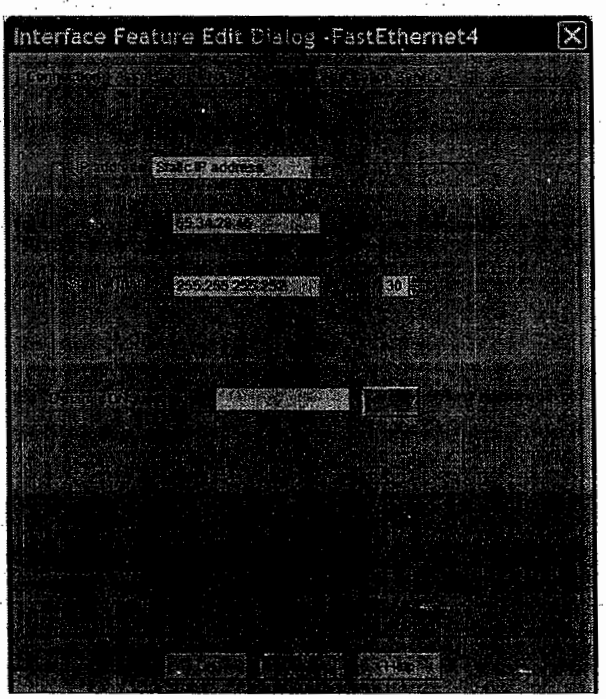


SDM configure Screen contains the following tasks at left side of the window:

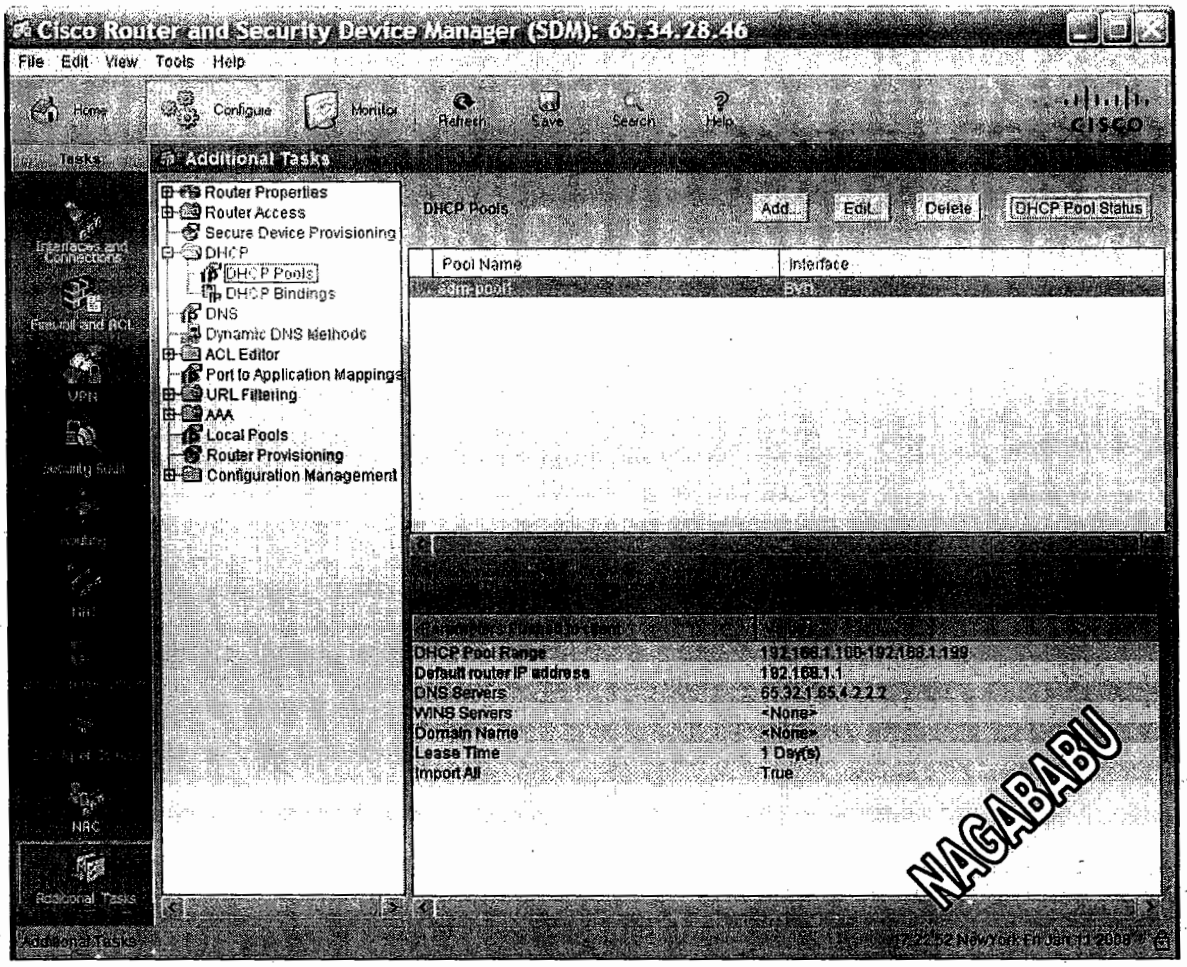
Task	Purpose
Interfaces and connections	Configuration of interfaces, their status
Firewall and ACL	Configure firewall policies and Access control list
VPN	Virtual Private Network configuration. Create, edit, view IPsec site-site, remote access and SSL VPN
Security Audit	Router Security auditing. Recommendation of security features what should be enabled and disabled.
Routing	Static, dynamic routing configuration
NAT	Configure Network Address Translations
Intrusion Prevention	Configure policies to look for network and host attacks
Quality of Service	Configure Qos prioritize the important traffic
NAC	Defining Network Access control server
Additional Tasks	DHCP settings, user accounts management, telnet access control, setting up SSH and other management functions

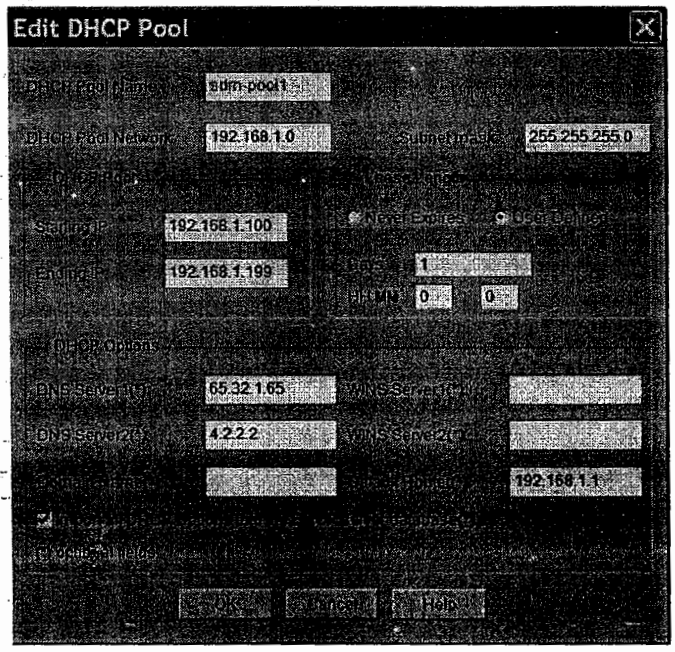
SDM configure Screen - Interfaces and connections task:



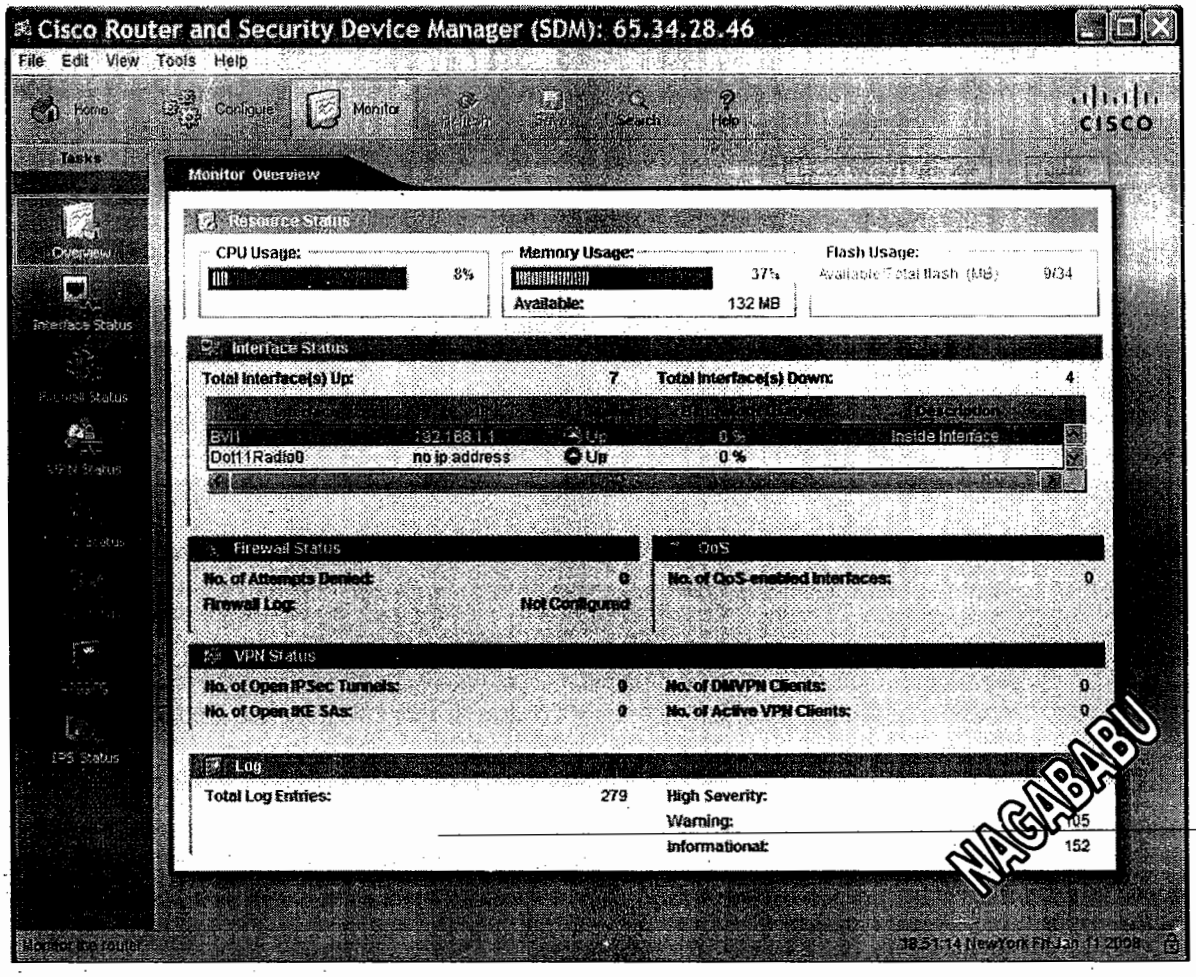


SDM configure Screen - Additional Tasks - DHCP settings:





Basic Router Monitoring using SDM:



SDM Monitor Screen contains the following information:

Status	Purpose
Overview	Displays overview of the operation of the router
Interface status	Displays interface status with real time graphs such as bandwidth
Firewall status	Displays log messages of matches on ACL statements
VPN status	Displays status of VPN tunnels terminated on the router
Traffic status	Displays traffic statistics if NBAR is enabled NBAR - Network Based application recognition
NAC status	Displays information about the interaction with NAC policy server
Logging	Displays log messages stored in the router's RAM
IPS status	Displays the IPS alerts from attacks

IPv6

What is IPv6?

- Internet Protocol version 6 (Also called as IPng - IP next generation)

- IPv4 addressing scheme has 4294967296 IP addresses
- IPv4 addresses are not enough in future with Internet evolution
- IPv6 is introduced as IPv4 addresses are being saturated
- IPv6 is 128 bit, Hexadecimal notation

Differences between IPv4 and IPv6

IPv4	IPv6
Internet Protocol version 4	Internet Protocol version 6
32 bit value	128 bit value
4294967296 ip addresses	3.4×10^{38} ip addresses
Dotted decimal notation	Hexadecimal notation (string notation)
192.168.6.1	2000:58ab:0000:0000:12cd:0011:8901:13fd
Uses unicast, multicast, broadcast	Uses unicast, multicast, any cast
Classified into A B C D E classes	No classification

IPv6 Features:

Very large Address space:

IPv6 has 3.4×10^{38} IP addresses.
With IPv6 every device in every house can have IP address

Security:

IPSec is in built into IPv6. Two devices can dynamically negotiate security parameters and build a secure tunnel between them with no user intervention

Mobility:

With the growth of mobile devices, such as PDAs and smart phones, devices can roam between wireless networks without breaking their connectivity

Streamlined encapsulation:

IPv6 encapsulation is simpler than IPv4, providing faster forwarding rates by routers and better routing efficiency. No checksum is included in IPv6 header

Transition capabilities:

Various solutions exist to allow IPv4 and IPv6 to successfully coexist when migrating between the two.

IPv6 addressing scheme:

First IPv6 Address:

0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

0000:0000:0000:0000:0000:0000:0000:0000

Last IPv6 Address:

1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111

FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

IPv6 addressing scheme - simplification:

A leading zero in a set of numbers can be omitted.

1200:5600:0028:afcd:0004:0589:0009:ca39 1200:5600:28:afcd:4:589:9:ca39

Successive fields of zeroes are replaced with :: but only once
If :: is used more than once, it leads to confusion to identify set of zeroes

2000:0001:0000:0000:0000:000c:00ea:0000 2000:1:0:0:0:c:ea:0 2000:1::c:ea:0

An unspecified address is represented with :: since it contains all zeroes

0000:0000:0000:0000:0000:0000:0000:0000 ::

Types of IPv6 Addresses

- Unicast
  - One to one interface (same as IPv4)
- Multicast
  - One to a group of devices (same as IPv4)
- Anycast
  - One to nearest interface, where many interfaces can share the same address

No Broadcast exists in IPv6

:: is unspecified address that is 0000:0000:0000:0000:0000:0000:0000:0000 :: 1 is loop back address that is 0000:0000:0000:0000:0000:0000:0000:0001

Unicast:

- One to one interface communication

Private IPv6 addresses: (FE80::/10)
IP addresses are used for devices that don't need to access a public network

Two kinds of private addresses:
- Site-local FEC:: through FEF:: (locally specific in the LAN)
- Link-local FE8:: through FEB:: (locally specific on the link)

Global/Public IPv6 addresses: (2000::/3)
IP addresses are used for devices that need to access a public network

IANA has currently assigned only **2000::/3** addresses to the global pool, which is about $1/6^{th}$ of the available IPv6 addresses

Multicast:

- One to group of devices communication

FF::/8 is the address range

First 8 bits are set to FF
Next 4 bits are the lifetime of the address: 0 is permanent and 1 is temporary
Next 4 bits indicate scope of the multicast address (Eg: 1 is for a node, 2 is for a link, 5 is for the site, 8 is for the organization, and E is global, the internet)

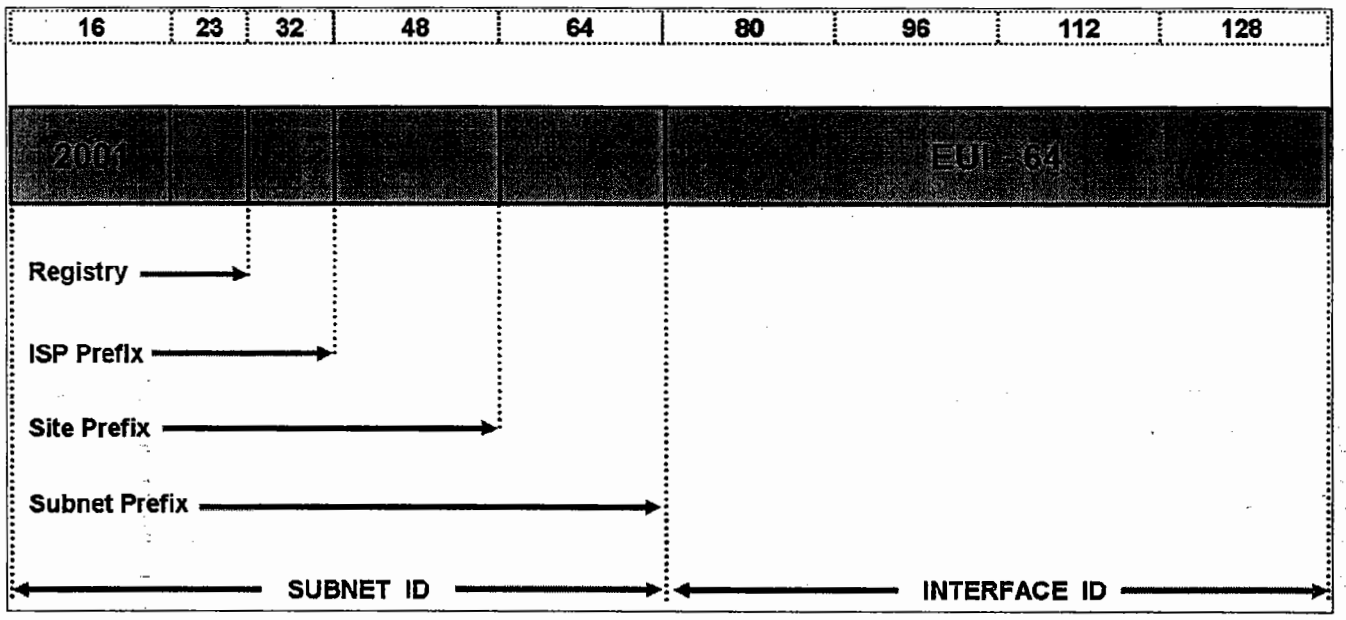
For example FF02::/16 is a permanent link address
FF15::/16 is a temporary address for a site

Anycast:

- One to nearest interface
- Anycast address identifies one or more interfaces
- Anycast is a hybrid of unicast and multicast address
- A packet is sent to any one member of a group of devices that are configured with the anycast address
- By default packets sent to an anycast addresses are forwarded to the closest interface
- Anycast address is also known as one-to-the-nearest address

- Anycast addresses are allocated from the global pool of unicast addresses in IPv6
- It is difficult to distinguish between unicast and anycast as they use common address space
- Don't assign anycast addresses to hosts
- Anycast addresses can be assigned to routers
- Don't put anycast address in the source of a packet - only the destination
- Anycast addresses and their uses are still in their infancy and some known problems can occur when using them

IPv6 Address Structure



IPv6 Address structure - Assignment

IANA has assigned only 2000::/3 addresses to the global pool.
Of these addresses, only 2001::/16 are assigned to various Internet address registries

Global Unicast addresses are made up of two components

- Subnet ID (64 bits)
- Interface ID(EUI -64 bits)

Subnet ID contains:

The Registry	(which is responsible for assigning it, such as IANA)
The ISP prefix	(Which ISP is associated with the address)
The site prefix	(Which company is associated with the address)
The subnet prefix	(subnets within the site)

Interface ID is EUI-64:

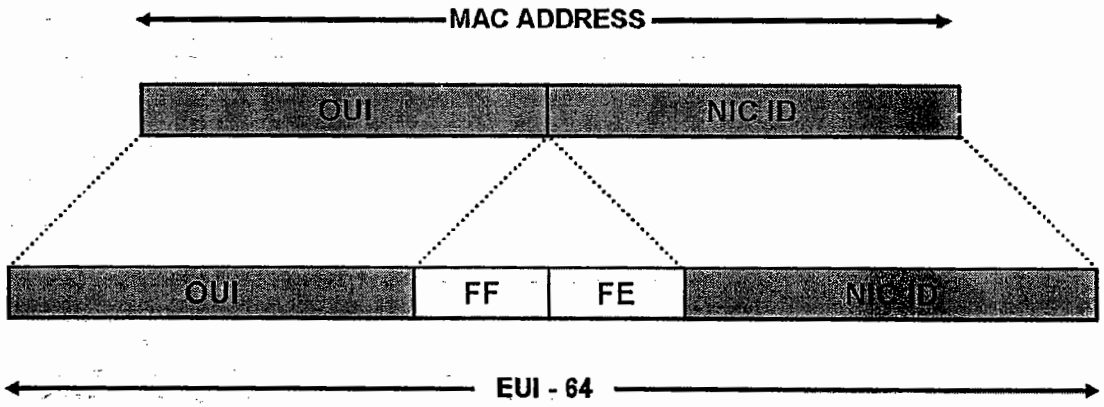
EUI -64 Extended unique identifier 64 (EUI-64)

❖ **IPv6 address can be assigned in three ways**

- Static IP (specify all 128-bits manually)
- Dynamic IP (through DHCP server)
- EUI- 64 (stateless auto configuration)

IPv6 is auto configurable with EUI-64 as interface ID

EUI-64 is obtained by inserting FF FE in between MAC address of the system to fulfill 64 bits



Routers with IPv6

Enable IPv6 routing:

```
Router(config)# ipv6 unicast-routing
```

Assigning IPv6 address to interface:

```
Router(config)# interface fa 0/1
Router(config-if)# ipv6  address  2001:1cc1:dddd:2::/64   eui-64
```

Routing protocols for IPv4 and IPv6:

IPv4 Routing Protocols	IPv6 Routing Protocols
RIP	RIPng (RIP new generation)
OSPFv2	OSPFv3
EIGRP	EIGRP for ipv6

IPv4 to IPv6 transition options:

- Dual stacking
- Manual IPv6-over-IPv4 (6to4) tunneling
- Dynamic 6to 4 tunneling
- Intra-site-Automatic tunnel addressing protocol tunneling (ISATAP)
- Teredo tunneling
- NAT Proxying and Translation (NAT-PT)

WIRELESS

What is Wireless Network?

Network that uses RF (Radio frequency) technology to communicate between systems, air as media

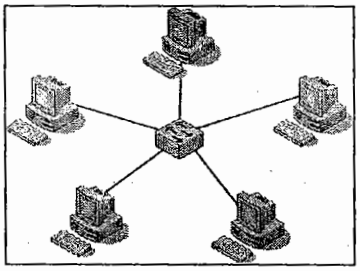
What are the advantages with wireless?

- No cables are required (or) little cabling
- Mobility is possible within specified area

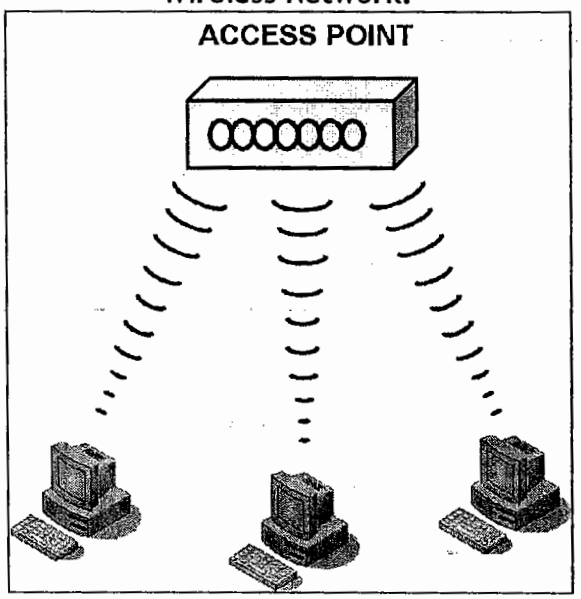
Differences between Wired and Wireless Networks

Wired Networks	Wireless Networks
Cables are required	Cables are not required
Copper/ fiber as the media	Air as the media
Electrical signal transmission	Radio Wave transmission
No user mobility	User Mobility
Full/ Half duplex	Half duplex
Switch is the centralized device	Access Point (AP) is the centralized device
IEEE 802.2, 802.3 standards	IEEE 802.11, 802.16 standards
Secured networks	Comparatively low security
Signal distortions are low	Signal distortions are high

Wired Network:



Wireless Network:



NAGABABU

Wireless Technologies:

Basically Wireless Technologies are 3 types

1. **Narrow band**
    - **Used in WLAN**
    - Limited to a small area, such as a small campus
    - Typically require license and operate at low data rate
    - Only one frequency is used for transmission
      900MHz, 2.4GHz or 5GHz
2. **Broad band**
    - For broader coverage
    - Typically National wide coverage (Wireless WAN - Vsat)
    - Provide lower data rates than narrowband solutions
    - Personal communication services (PCS)
3. **Circuit and Packet data solutions**
    - Based on cellular technologies
    - Provide low data rate than narrowband and broadband
    - Cellular phone, 3G implementation

Narrow band Wireless technology is used in Wireless LAN

What is Access Point?

- Access Point is centralized device
- It is responsible to maintain WLAN (Wireless LAN)
- If two systems want to communicate, they must exchange the data through Access point
- Access point is analogous to hub (serves function similar to hub)

SSID:

- Service Set Identifier
- Generally SSID the MAC address of AP's wireless card
- SSID is set in Access Point & AP allows only the clients configured with same SSID
- SSID is used to group the devices
- Systems that share same SSID form a group and communicate with each other
- SSID is similar to Vlan in switching
- AP periodically broadcast signals, announcing its SSID to allow new clients

WLAN operations:

- Every client must have Wireless NIC. Client can detect nearest AP dynamically
- Clients may need to be authenticated to join the wireless network
- Access point can transmit or receive data from only one client at a time
- Half duplex communication
- WLAN uses CSMA/CA mechanism to avoid collisions
  - CSMA/CA - carrier sense multiple access - collision avoidance
  - Device uses **RTS** (ready to send) and **CTS** (clear to send) signals to avoid collisions
- Security is low. Anybody with a compatible device can sniff the airwaves and may disturb the communication

Factors that influence WLAN transmission:

- **Absorption**
  - Walls, ceilings, floors absorb RF waves causing signal loss
- **Scattering**
  - Rough plaster on walls, carpet on the floor disperse the RF waves causing signal loss
- **Reflection**
  - Metal, glass objects reflect RF waves causing signal loss

WLAN Standards

Standards organizations are primarily responsible for implementing WLANs

- IEEE - Institute of Electrical and Electronic Engineers
- Wi-Fi alliance

WLAN uses IEEE 802.11 standards

IEEE 802.11 standard uses unlicensed frequencies 2.4GHz, 5GHz
4 basic standards are currently in use: 802.11a, 802.11b, 802.11g, and 802.11n

IEEE 802.11 standards:

	802.11a	802.11b	802.11g	802.11n
Data Rate	54Mbps	11Mbps	54Mbps	248Mbps
Throughput	23Mbps	4.3Mbps	19Mbps	74Mbps
Frequency	5GHz	2.4GHz	2.4GHz	2.4and/or 5GHz
Compatibility	None	With 802.11g	With 802.11b	802.11a,b,g
Range (meters)	35-120	38-140	38-140	70-250
No.of channels	3	Up to 23	3	14
Transmission	OFDM	DSSS	DSSS/OFDM	MIMO

OFDM - Orthogonal Frequency Division multiplexing
DSSS - Direct sequence spread spectrum
MIMO - Multiple Input Multiple Output

WLAN Authentication

IEEE 802.11 defines only two authentication methods for AP to authenticate clients

- **Open Authentication (No security)**
  - Exchanging four hello packets that contains no verification
- **Shared key Authentication**
  - A static encryption key is used with the Wireless Encryption Protocol

WLAN Security Solutions

WAN security solution should provide Encryption, Authentication, intrusion prevention

WLAN security solution	Description
WEP	Wired Equivalent Privacy Wireless Encryption Protocol
802.1x EAP	Extensible Authentication protocol LEAP - Light weight EAP PEAP - Protected EAP
WPA	Wi-Fi Protected Access 802.1x with EAP authentication and WEP/TKIP for encryption
WPA2 / 802.11i	Wi-Fi Protected Access 802.1x with EAP authentication and AES encryption

WLAN security solutions- comparison

	WEP	802.1X EAP	WPA	WPA2 (802.11i)
Introduced in	1997	2001	2003	2004
Encryption	Static keys, breakable	Dynamic keys	Dynamic keys, Per packet	Dynamic keys, Per packet, most secure
User authentication	None	Usernames Passwords certificates Pre-shared keys	User names Passwords, Certificates Pre-shared keys	Usernames Password Certificates Pre-shared keys

WLAN Implementation

Two IEEE 802.11 access modes can be used in a WLAN

- Ad hoc mode
  - It is based on the Independent Basic Service Set (IBSS)
  - Client can set up connections directly to other systems without AP
  - Peer to Peer connectivity

- Infrastructure mode
  - It is based on BSS (Basic service set) and ESS (Extended service set)
  - Client can set up connections to other systems with intermediate AP
  - WLAN connectivity (security, scalability)

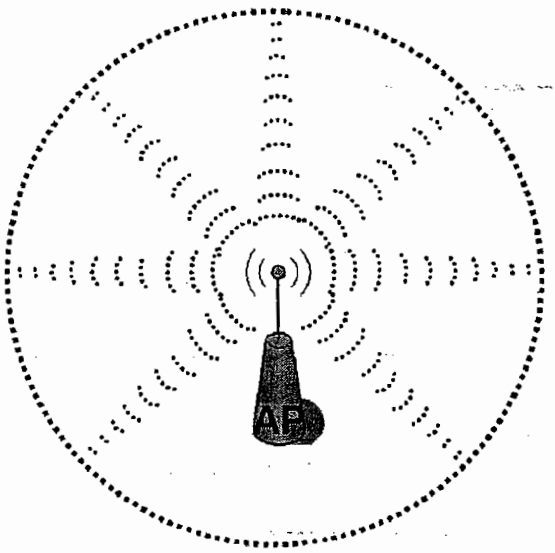
BSS - systems in WLAN connected to AP (Limited coverage)
ESS - two or more BSS are interconnected (wide coverage)

WLAN Coverage Areas

Cell:

- The coverage area of Access point
- Access point can cover only a limited area. The cell range depends on AP's transmitting power
- The radiating power decreases while moving away from access point
- The client nearer to AP can access network resources efficiently
- To cover more number of clients, WLAN requires multiple APs

CELL

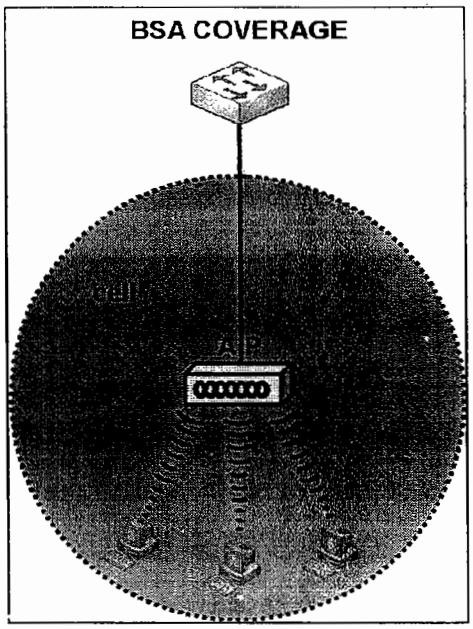


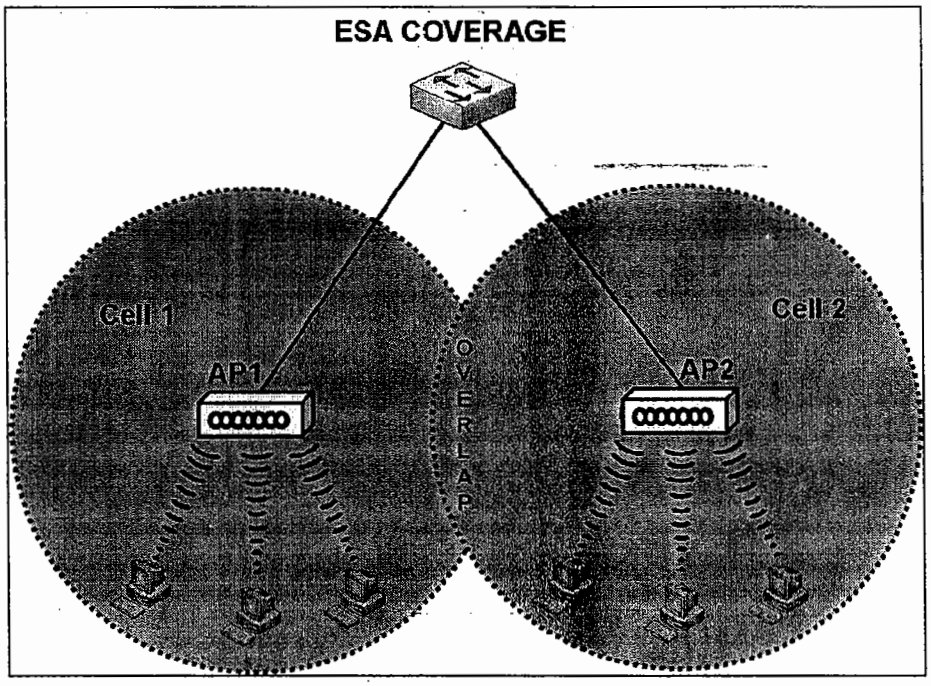
NAGABABU

Two types of coverage areas exist in WLAN

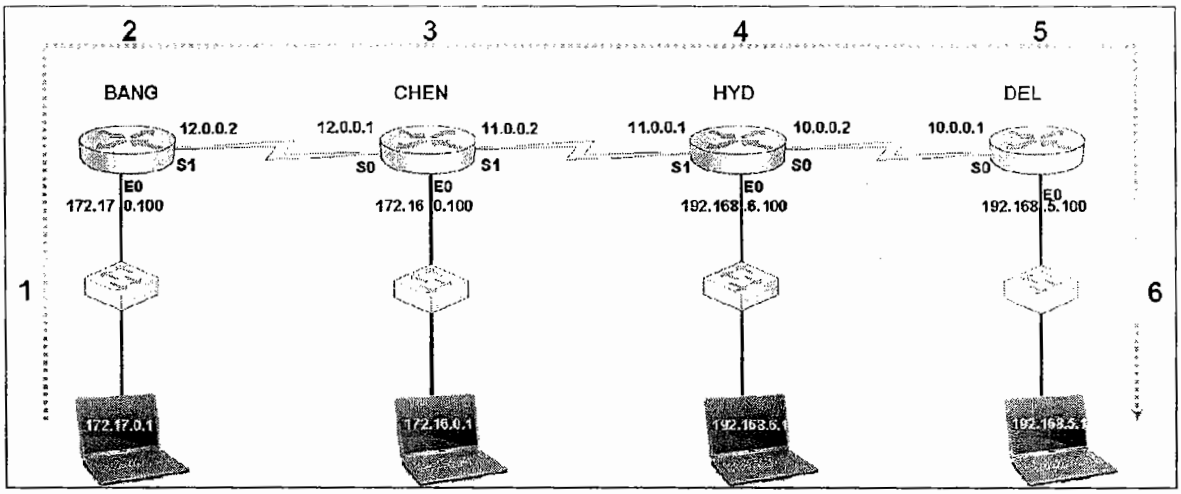
- BSA - Basic Service Area
  - A single cell
  - Only one AP exists to serve the clients

- **ESA - Extended Service Area**
  - Multiple BSA
  - Multiple APs exist to serve the clients





Troubleshooting WAN



Troubleshooting Bang to Delhi Network communication

From Bangalore host ping all the nodes one by one in the path till Delhi host
Use **ping** and **traceroute** as basic troubleshooting commands

1. If there is no response from Bangalore switch
- Check the physical connectivity to switch
- Switch configuration, mac-address-table, vlan configuration

2. If there is no response from Bangalore router
- Check the physical connectivity to Bangalore router LAN interface
- Router configuration, routing protocols, IP addresses, encapsulation etc

3. If there is no response from Chennai router
- Check the physical WAN connectivity between Bangalore and Chennai routers
- Router configuration, routing protocols, IP addresses, encapsulation etc

4. If there is no response from Hyderabad router
- Check the physical WAN connectivity between Chennai and Hyd routers
- Router configuration, routing protocols, IP addresses, encapsulation etc

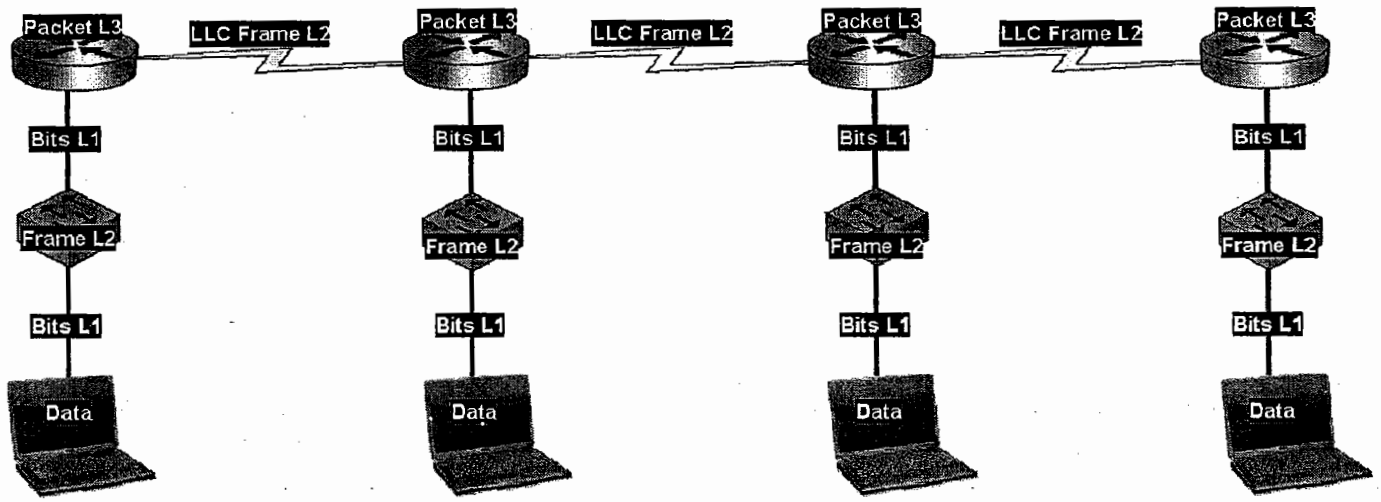
5. If there is no response from Delhi router
- Check the physical WAN connectivity between Hyd and Delhi routers
- Router configuration, routing protocols, IP addresses, encapsulation etc

6. If there is no response from Delhi switch
- Check the physical connectivity to switch
- Switch configuration, mac-address-table, vlan configuration

In real time scenario check modems status in wan connectivity
Contact service provider in case of wan link outages

NAGABABU

Trouble shooting - Devices- Data types



NAGABABU

STUDENTNAME NAGABABU 204

ROUTER IOS commands (additional)

NAGABABU

Creating Users:	
Router(config)#username <name> secret <password>	Creating a user
Router(config-line)# login local	To login into router with local users
Setting Banner:	
Router(config)#banner motd # <banner> #	Setting Banner of the router
Boot System:	
Router(config)#boot system flash <filename>	Boot using a different IOS in flash
Router(config)#boot system tftp <ip address>	Boot from TFTP server
Router(config)# boot system rom	Boot from rom
Config register values:	
Router(config)#config-register 0x2102	Normal boot sequence
Router(config)#config-register 0x141	Boot mode/Rommon mode
Router# show version	Check config register value
Erase configuration:	
Router# write erase	Erasing nvram / startup-config
Router# erase startup-config	Erasing nvram / startup-config
Router# delete flash:<filename>	Deletes specified file in flash memory
Clock settings:	
Router# clock set <time> <day> <month> <year>	Setting clock
Router# show clock	Displays clock
Command history:	
Router# show history	Displays command history buffer
Router# terminal history size <linecount>	Set the length of the history buffer
Setup:	
Router# setup	Using setup utility (alternative configuration way)
Router# auto secure	Auto secure the router(security auditing & configuration)
Interfaces:	
Router(config)#interface loop back <number>	Creating a loop back interface (logical interface)
Router(config)#interface s0.1	Creating a sub interface (logical interface in physical)

Miscellaneous:	
Router(config-line)# exec-timeout <minutes> <seconds>	Setting logout time for a line in idle state
Router(config)# ip subnet-zero	Using subnet-zero also (enabled by default)
Router(config)# ip host <hostname> <hostipaddress>	Creating a name for an ip address (static host)
Router# show hosts	Displays static hosts
Router(config)# ip name-server <dnsserveripaddress>	Setting dns server information
Router(config)# no ip domain-lookup	Disable DNS lookups
Router# show ip arp	To see arp table
Router# cd flash:	Change directory to flash
Router# dir	Displays directories and files
Router# no debug all	To disable all debugging
Router# undebug all	To disable all debugging
Router(config)# service password-encryption	Convert all passwords into secret passwords
Lines:	
Router# show users	To see the line users accessing this router
Router# clear line <linenumber>	To clear a line user
Telnet sessions:	
Router# show sessions	To see initiated telnet sessions from the router
Router# resume <connectionnumber>	To resume a session
Router# disconnect <connectionnumber>	To disconnect a session
RIP:	
Router(config)#router rip	Enabling rip as routing protocol
Router(config-router)# network <network address>	Advertising network
Router(config-router)# version <1/2>	Setting
Router(config-router)# ip rip send <version1/version2>	Setting version to send updates
Router(config-router)# ip rip receive <version1/version2>	Setting version to receive updates
Router# clear ip route *	Clears ip routing table and rebuilds it
Router# debug ip rip	Turn on debug for rip (rip background process messages)
EIGRP:	
Router(config)#router eigrp <AS>	Enabling eigrp as routing protocol
Router(config-router)# network <network address> <wcm>	Advertising network
Router(config-router)# variance <multiplier>	Unequal load balancing

Router(config-router)# traffic-share balanced	Load balancing the traffic according to bandwidth
Router(config-router)# traffic-share min across-interfaces	backup paths in the routing table for faster convergence
Router(config-router)# no auto-summary	Turn off router summarization
Router# show ip eigrp neighbors	Display neighbors list
Router# show ip eigrp topology	List of successors and feasible successors (active&backup)
Router# show ip eigrp interfaces	Displays eigrp enabled interface information
Router# show ip eigrp traffic	Traffic statistics information of eigrp
Router# debug ip eigrp	Turn on eigrp events debugging
Router# debug ip eigrp packets	Turn on eigrp packets debugging (Hello,update,query etc)
EIGRP neighbor authentication:	
Router(config)# key chain <keychainame>	Creating a keychain
Router(config-keychain)# key <keyno>	Creating a key no in the keychain
Router(config-keychain-key)# key-string <keyvalue>	Associate key value with a key number
Router(config-if)# ip authentication mode eigrp <AS> md5	enabling eigrp authentication mode on the interface
Router(config-if)# ip authentication key-chain eigrp <AS> <keychainname>	Applying keychain on the interface
OSPF:	
Router(config-router)#default-information originate	Making perimeter router as ASBR
Router(config-router)#maximum-paths <paths>	Customize load balancing paths (equal cost paths, max 16)
Router(config-if)# ip ospf cost <costvalue>	Customizing ospf cost
Router# show ip ospf	Overview of ospf configuration
Router# show ip ospf interface	Ospf configuration on interface basis
Router# show ip ospf neighbor	Ospf neighbors list
Router# debug ip ospf adj	Debugging ospf adjacency process
Router# debug ip ospf events	Debugging ospf events on the router
Router# debug ip ospf packets	Debugging ospf packets on the router (contents of LSA)
OSPF authentication:	
Router(config-if)#ip ospf authentication-key <password>	Enabling neighbor authentication
Router(config-if)#ip ospf authentication message-digest	Set type of authentication (cleartext/md5)
Router(config-router)#area <areaid> authentication message-digest	Set authentication for area

NAGABABU

SWITCH IOS commands (additional)

Creating Users:	
Switch(config)#username <name> secret <password>	Creating a user
Switch(config-line)# login local	To login into Switch with local users
Setting Banner:	
Switch(config)#banner motd # <banner> #	Setting Banner of the Switch
Boot system:	
Switch(config)#boot system flash <filename>	Boot using a different IOS in flash
Switch(config)#boot system tftp <ip address>	Boot from TFTP server
Switch(config)# boot system rom	Boot from rom
Erase configuration:	
Switch# write erase	Erasing nvram / startup-config
Switch# erase startup-config	Erasing nvram / startup-config
Switch# delete flash:<filename>	Deletes specified file in flash memory
Clock settings:	
Switch# clock set <time> <day> <month> <year>	Setting clock
Switch# show clock	Displays clock
Command history:	
Switch# show history	Displays command history buffer
Switch# terminal history size <linecount>	Set the length of the history buffer
Setup:	
Switch# setup	Using setup utility (alternative configuration way)
Miscellaneous:	
Switch(config-line)# exec-timeout <minutes> <seconds>	Setting logout time for a line in idle state
Switch(config)# ip host <hostname> <hostipaddress>	Creating a name for an ip address (static host)
Switch# show hosts	Displays static hosts
Switch(config)# ip name-server <dnsserveripaddress>	Setting dns server information
Switch(config)# ip default-gateway <ipaddress>	Set default gateway for the switch
Switch# show ip arp	To see arp table
Switch# cd flash:	Change directory to flash

Switch# dir	Displays directories and files
Switch(config)# service password-encryption	Convert all passwords into secret passwords
Lines:	
Switch# show users	To see the line users accessing this Switch
Switch# clear line <linenumber>	To clear a line user
Telnet sessions:	
Switch# show sessions	To see initiated telnet sessions from the Switch
Switch# resume <connectionnumber>	To resume a session
Switch# disconnect <connectionnumber>	To disconnect a session
Switch(config)# mac-address-table static <12bc.4567.be3f> vlan <1> interface <fa 0/32>	Associate mac address with a port in the vlan (Static mac binding)
Switch# show mac-address-table	To check the mac address table
Switch# clear mac-address-table dynamic	Clear mac-address-table (dynamic contents)
Port security:	
Switch(config-if)# switchport port-security	Enable port-security on the switch
Switch(config-if)# switchport port-security maximum <value>	Maximum no of devices that can be associated with a port
Switch(config-if)# switchport port-security violation <protect/restrict/shutdown>	Action to be taken if security is violated
Switch(config-if)# switchport port-security mac-address <macaddres>	Enter the mac address that has to be associated
Switch(config-if)# switchport port-security mac-address sticky	Sticky the mac address of connected system
Switch# show interface status err-disable	Check the ports that violated security
Switch# show port-security	Check the port security features on all interfaces
Switch# show port-security interface fa 0/2	Check the port-security features of a port
Spanning-tree:	
Switch(config)# spanning-tree portfast default	Enables portfast feature on all non-trunking ports
Switch(config-if)# spanning-tree portfast trunk	Enable portfast feature on trunk ports (systems connected to trunk ports with trunk NIC)
Switch(config)# spanning-tree mode rapid-pvst	To enable per vlan rapid spanning tree protocol
Switch# show spanning-tree vlan <10>	To view spanning-tree features of the specified vlan

Ether Channels:	
Switch(config-if)# channel-group <groupno> mode <mode>	configure an interface into a channel-group
Switch(config)# port-channel load-balance <methods>	Load balancing method for the port channel Src-ip, dst-ip, src-dst-ip, src-mac, dst-mac, src-dst-mac
Switch# show port-channel	Displays port channel information

DHCP configuration: (Router & Switch)	
IOS(config)# service dhcp	Enable dhcp feature
IOS(config)# ip dhcp pool <poolname>	Creating a dhcp pool
IOS(config-dhcp)# network <networkaddress> <subnetmask>	Specifying network for the dhcp pool
IOS(config-dhcp)# domain-name <domainname>	Setting domain name
IOS(config-dhcp)# dns-server <ipaddress1> <ipaddress2>	Setting dns server
IOS(config-dhcp)# default-router <ipaddress>	Setting default gateway for the systems
IOS(config-dhcp)# lease <days> <hours> <minutes>	Setting lease period for dhcp
IOS(config)# ip dhcp excluded-address <beginip> <endingip>	Excluding specified ip addresses from the pool
IOS# show ip dhcp binding	View dhcp bindings
IOS# clear ip dhcp binding *	Clear all dhcp bindings
IOS# show ip dhcp conflict	Displays ip confliction with static IP addresses (if any)

Important Port Numbers (L4)

Protocol	Expansion	Port No
FTP	File Transfer Protocol	20/21
SSH	Secure Shell	22
TELNET	Terminal Network	23
SMTP	Simple Mail Transfer Protocol	25
DNS	Domain Naming System	53
DHCP	Dynamic Host Configuration Protocol	67
TFTP	Trivial File Transfer Protocol	69
HTTP	Hyper Text Transfer Protocol	80
POP3	Post Office Protocol	110
NTP	Network Time protocol	123
IMAP	Internet message access protocol	143
SNMP	Simple Network Management Protocol	161
HTTPS	HTTP Secure	443
SysLog	System log	514

Important Protocol Numbers (L3)

Protocol	Expansion	Protocol No
IP	Internet Protocol	0
ICMP	Internet control message protocol	1
TCP	Transmission control protocol	6
UDP	User datagram protocol	11/17
RIP	Routing information protocol	520
EIGRP	Enhanced IGRP	88
OSPF	Open shortest path first	89

IMPORTANT TERMS

AAA	Authentication, authorization, accounting
ACK	Acknowledgement
ACL	Access control list
AP	Access point
AES	Advanced encryption standard
AH	Authentication header
ANSI	American national standards institute
ARP	Address resolution protocol
AS	Autonomous system
ASBR	Autonomous system boundary router
ASCII	American standard code for information interchange
ASICS	Application specific integrated circuits
ATM	Asynchronous transfer mode
BDR	Backup designated router
BGP	Border gateway protocol
BIA	Burnt in address
BPDU	Bridge protocol data unit
BRI	Basic rate interface
BSA	Basic service area
BSS	Basic service set
CAM	Content address memory
CBAC	Context based access control
CCK	Complementary code keying (wlan)
CCO	Cisco connection online
CDP	Cisco discovery protocol
CEF	Cisco express forwarding
CHAP	Challenge handshake authentication protocol
CIDR	Classless inter domain routing
CLI	Command line interface
COM	Communication port
CRC	Cyclic redundancy check
CSI	Computer security institute
CSMA/CA	Carrier sense multiple access / collision avoidance
CSMA/CD	Carrier sense multiple access / collision detection
CST	Common spanning tree
CSU/DSU	Channel service unit/ data service unit
CTS	Clear to send
DARPA	Defense advanced research project agency
DB	Data bus
DCE	Data communication equipment
DDR	Dial on demand routing
DES	Data encryption standard
DH	Diffie-hellman protocol
DHCP	Dynamic host configuration protocol
DNS	Domain naming system
DSL	Digital subscriber line
DSSS	Direct sequence spread spectrum

DTE	Data communication equipment
DTP	Dynamic trunking protocol
DUAL	Diffused update algorithm
DWDM	Dense mode Wave division multiplexing
EAP	Extensible authentication protocol
EBCDIC	Extended binary coded decimal interchange code
EGP	Exterior gateway protocol
EIGRP	Enhanced interior gateway routing protocol
EMI	Electro magnetic interference
ESA	Extended service area
ESP	Encapsulation security protocol
ESS	Extended service set
ETSI	European telecommunication standards institute
EUI	Extended unique identifier
FCC	Federal communications commission
FCS	Frame check sequence
FDDI	Fiber distributed data interface
FTP	File transfer protocol
GBIC	Gigabit interface card
HDLC	High level data link control
HMAC	Hashed message authentication protocol
HSSI	High speed serial interfaces
HTTP	Hypertext transfer protocol
IANA	Internet assigned numbers authority
IBSS	Independent basic service set
ICMP	Internet control message protocol
IDS/IPS	Intrusion detection system / intrusion prevention system
IEEE	Institute of electrical and electronic engineers
IETF	Internet engineering task force
IFS	IOS file system
IGP	Interior gateway protocol
IGRP	Interior gateway routing protocol
IKE	Internet key exchange
IMAP4	Internet message access protocol
IOS	Internetwork operating system
IPSEC	Internet protocol security
IPV4	Internet protocol version 4
IPV6	Internet Protocol version 6
IPX	Internet Packet exchange
IRQ	Interrupt request line
IS-IS	Intermediate system to intermediate system
ISAKMP	Internet security association key management protocol
ISDN	Integrated services digital network
ISL	Inter switch link
ISO	International standards organization
ITU-T	International telecom union - telecom standards sector
L2TP	Layer 2 tunneling protocol
LACP	Link aggregation control protocol
LAN	Local area network

LCP	Link control protocol
LEAP	Lightweight extensible authentication protocol
LED	Light emitting diode
LLC	Logical link control
LSA	Link state advertisement
MAC	Media access control
MD5	Message digest 5
MMF	Multimode fiber
MTU	Maximum transmission unit
NAC	Network access control
NAT-PT	Network address translation - protocol translation
NAT	Network address translation
NBMA	Non broadcast multi access
NCP	Network control protocol
NIC	Network interface card
NT1	Network termination 1
NT2	Network termination 2
NFS	Network file system
NTP	Network time protocol
OFDM	Orthogonal frequency division multiplexing
OSPF	Open shortest path first
OSI	Open system interconnection
OUI	Organizationally unique identifier
OTP	One time password
PAP	Password authentication protocol
PAR	Port address redirection
PAT	Port address translation
PCS	Personal communication service
PDU	Protocol data unit
PEAP	Protected extensible authentication protocol
POP3	Post office protocol
POST	Power on self test
POTS	Plain old telephone system
PPP	Point to point protocol
PPTP	Point to point tunneling protocol
PSK	Pre shared key
PVC	Permanent virtual circuit
PVRST	Per vlan rapid spanning tree protocol
QOS	Quality of service
RADIUS	Remote access dial in user service
RAM	Random access memory
RARP	Reverse address resolution protocol
RTS	Ready to send
RF	Radio frequency
RIP	Routing information protocol
RIPng	Rip next generation
RJ-45	Registered jack 45
ROM	Read only memory
ROMMON	Rom monitor

PC	Personal computer
RSA	Rivest - Shamir -adelman
RSTP	Rapid spanning tree protocol
RTS	Ready to send
SAP	Service access point
SDH	Synchronous digital hierarchy
SDM	Security device manager
SHA	Secure hashing algorithm
SMDS	Switched multi-megabit data services
SMF	Single mode fiber
SMTP	Simple mail transfer protocol
SNAP	Sub network access protocol
SNMP	Simple network management protocol
SOH	Section over head
SOHO	Small office home office
SONET	Synchronous Optical network
SPAN	Switch Port analyzer
SPF	Shortest path first
SSH	Secure shell
SSID	Service set identifier
SSL	Secure socket layer
STP	Spanning tree protocol
STP	Shielded twisted pair
SYN	Synchronize
TAC	Technical assistant centre
TCP/IP	Transmission control protocol / internet protocol
TKIP	Temporal Key Integrity protocol
UDP	User datagram protocol
UPS	Uninterrupted power supply
UTP	Unshielded twisted pair
VLSM	Variable length subnet mask value
VC	Virtual circuit
VLAN	Virtual local area network
VMPS	Vlan management policy server
VOIP	Voice over Internet protocol
VPN	Virtual private network
VTP	Vlan trunking protocol
VTY	Virtual type terminal
WAN	Wide area network
WEP	Wired equivalent Privacy (Wireless Encryption Protocol)
WLAN	Wireless LAN
WPA	Wi-Fi Protected Access
WZC	Wireless Zero configuration

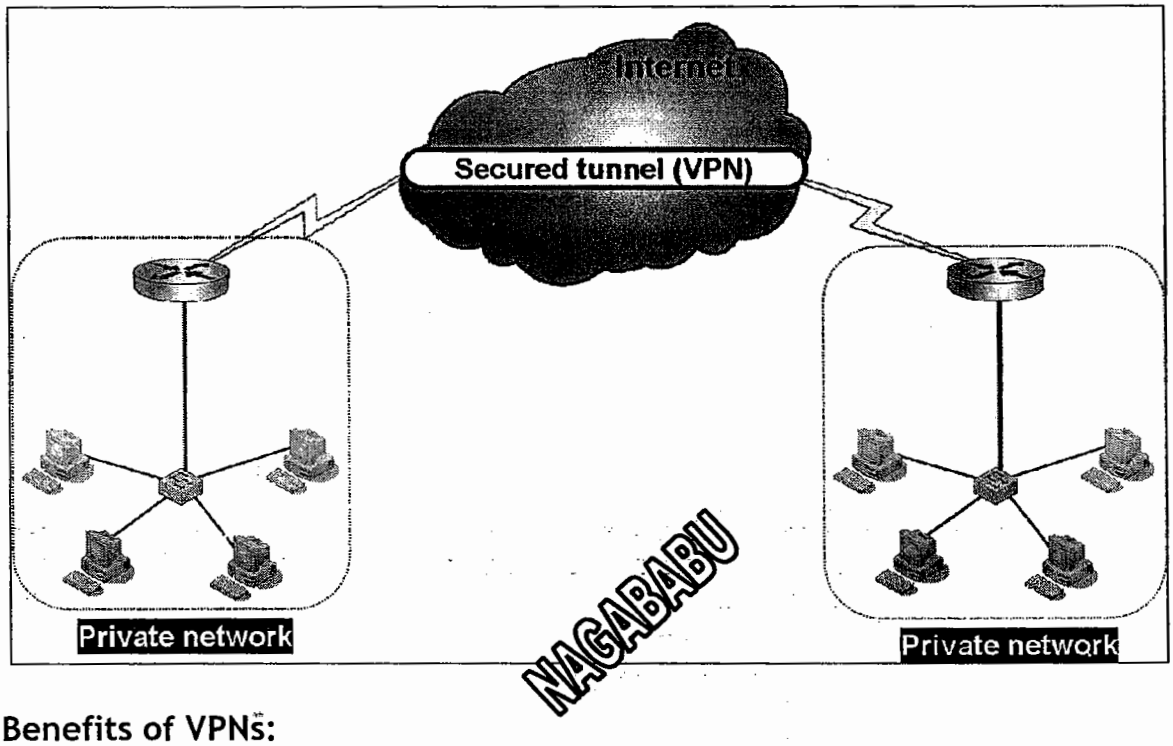
VPN Basics

What is VPN?

Virtual Private Network
It is a logical secured tunnel established between networks in unsecured network

Public network is unsecured network.
The secured networks can communicate via internet with security using VPN
The end network devices take care of encapsulation/encryption of packets

With VPN, networks can have security equal to private network security



Benefits of VPNs:

- **Security**
  - Security is provided through data encryption to protect confidentiality
- **Cost**
  - VPN reduce WAN infrastructure cost of a company
- **Bandwidth**
  - Inexpensive high bandwidth connections, such as DSL can be used to interconnect offices to allow fast and secure access to corporate offices
- **Scalability**
  - Companies can easily add large number of users and offices without building significant WAN structure

VPN Types

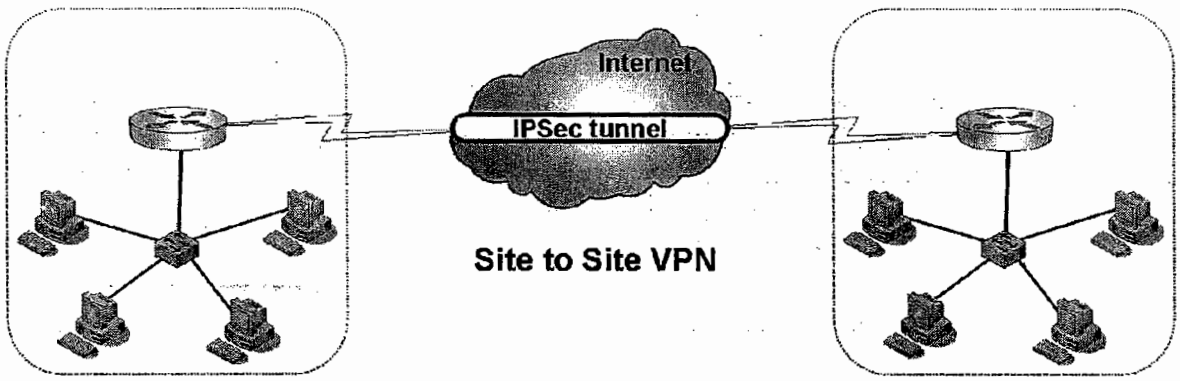
VPNs fall under two implementation types

- **Site to site VPN**
- **Remote Access VPN**

Site to Site VPN:

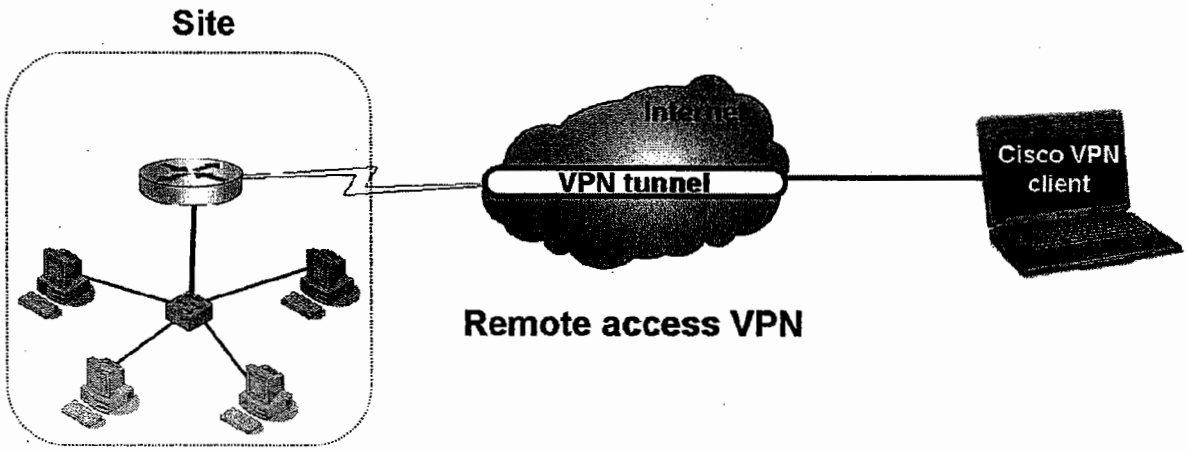
- Site to site VPNs, sometimes called as LAN-to-LAN or L2L VPNs
- Connect two locations or sites together (similar to P2P Wan connectivity)
- Two intermediate devices(VPN gateways) protect the traffic between two LANs
- The original IP packet from one LAN is encrypted by one gateway, forwarded to destination gateway and then decrypted and forwarded to the local LAN
- Traffic is protected by **IPSec** protocol

- Site to site VPNs are two types
  - **Intranet:** VPN between sites belong to same company
  - **Extranet:** VPN between sites belong to different companies



Remote Access VPN:

- VPN connectivity between a site and remote user
- Remote access VPN is used by mobile users to have the connectivity with site
- The can have access to resources as they are in site
- VPN software is required in the PC to access site (cisco VPN client)
- Traffic is protected by protocols like IPSec, SSL, PPTP, L2TP
- Remote Access VPN has two implementations
    - Easy VPN
    - Web VPN



Remote access VPN

IPSec

NAGABABU

IPSec:

- IPSec - IP security
- It is open standard protocol
- IPSec is actually a group of standards, protocols and technologies that work together to build a secure session, commonly called a tunnel, to a remote peer
- It works at Network layer and protects IP packets
- It can be used for Site-Site VPN and remote access VPN

IPSec Services:

IPsec provides four main services

1. Authentication
   - Verifying the identify of remote peers
   - Digital signatures are used to provide identity verification via pre-shared keys or digital certificates
2. Confidentiality
   - Guaranteeing that no intermediate device can decipher the contents of the payload in a packet
   - Encryption is used to hide the real data
3. Integrity
   - Guaranteeing that the contents of a packet have not been changed by an intermediate device
   - HMAC functions are used to verify the source of every packet as well as checking if it was tampered (changed) or not
4. Anti-replay protection
   - Verifying that each packet is unique and not duplicated
   - Ensuring that copies of a valid packet are not used to create a denial of service attacks
   - Protected sequence numbers are used to detect duplicate packets and drop them

IPSec Protocols:

- IPsec is actually a group of standards, protocols that work together to build a secure session
- An IPSec tunnel comprises three connections
  one management connection and two unidirectional data connections
- Tunnel is built across two phases
- The management connection is built during Phase 1and is used to share IPSec-related information between the two peers
- The two data connections are built during Phase 2 and are used to transmit user traffic
- All three connections are protected

- **ISAKMP** - Internet security association and key management protocol, used to build and maintain the tunnel. It defines the format of the management payload
- **IKE** - Internet key exchange protocol is responsible for generating and managing keys used for encryption algorithms and HMAC functions
- **DH** - Diffie-Hellman process is used to securely exchange the encryption and HMAC keys that will be used to secure the management and data connections
- **AH** - Authentication header protocol is used only to validate the origination and validity of data packets(on the data connections) received from a peer
- **ESP** - Encapsulation security payload protocol is used to provide packet confidentiality and authentication. It provides confidentiality through encryption and packet authentication through an HMAC function

International Organizations (Technical standards)

IANA	Internet Assigned Numbers authority
ICANN	Internet corporation for assigned names and numbers
IEEE	Institute of electrical and electronics engineers
IETF	Internet engineering task force
EIA/TIA	Electronic industry association /telecom industry association
ISO	International standard organization
ITU-T	International telecommunications union-telecom standards sector
FCC	Federal communications commission
ETSI	European Telecommunications standards institute
ANSI	American national standards institute

Prepared By

NAGABABU POLISETTI

Network Engineer

nagacisco@gmail.com
9701265230
9000235254