NETWORKING

A.Andrew Bergeran M.Sc.,B.Ed.,M.B.A

andrewanbu17@gmail.com 9444473301

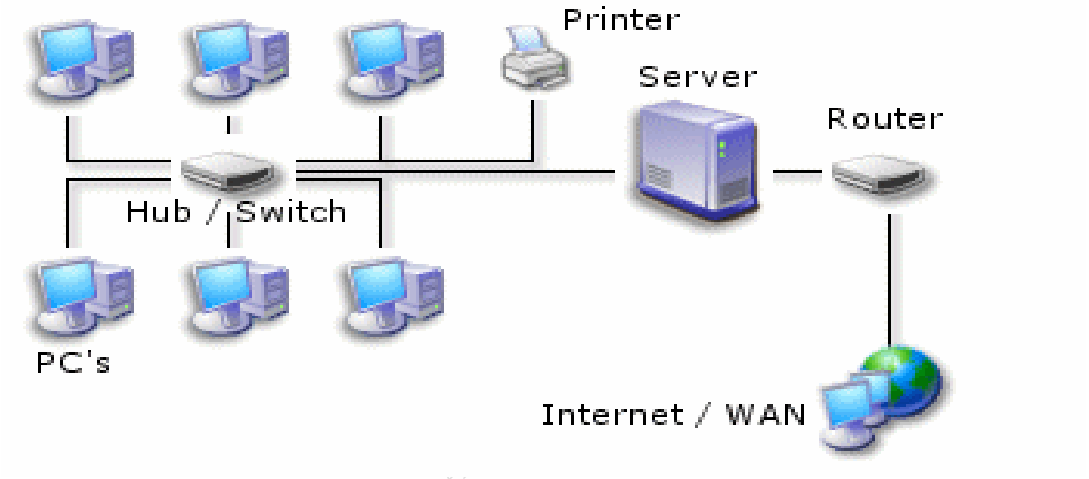
Chapter 1: Networking

A computer network is a system in which multiple computers are connected to each other to share information and resources.

Network: Network is a collection computers connected together.

Networking: It's a process of communication among the systems.

Use: Share the network resources Like Data and Hardware.



Components of Data Communication:

Message: It is the information to be delivered.

Sender: Sender is the person who is sending the message.

Receiver: Receiver is the person to him the message is to be delivered.

Medium: It is the medium through which message is to be sent.

Protocol: These are some set of rules which manage data communication.

Types of Communication Networks:

LAN: Systems connected to the same geographical area.

MAN: Systems connected to the same city.

WAN: Systems connected to same geographical area (or) different area depends on the telecommunications.

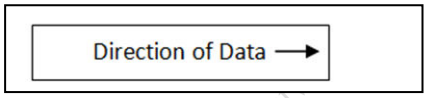
Data is transported over a network by three simple method

1. Unicast: one-to-one. From one source to one destination.
2. Broadcast: one-to-all. From one source to all possible destination.
3. Multicast: one-to-several. From one source to multiple destination.

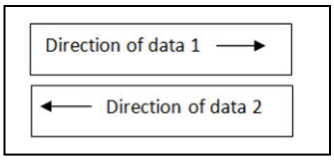
Transmission Modes in Computer Networks

Transmission mode means transferring of data between two devices. These modes direction of flow or information.

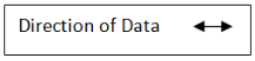
1. Simplex Mode: In this type of transmission mode data can be sent only through one direction i.e. communication is unidirectional. We cannot send a message back to the sender. Examples: loudspeaker, television broadcasting.



2. Half duplex Mode: In half duplex system we can send data in both directions but it is done one at a time that is when the sender is sending the data at that time we can't send the sender our message. Example: walkie- talkie in which message is sent one at a time and messages are sent in both the directions.



3. Full duplex Mode: In full duplex system we can send data in both directions as it is bidirectional. Data can be sent in both directions simultaneously. We can send as well as we receive the data. Example: Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.



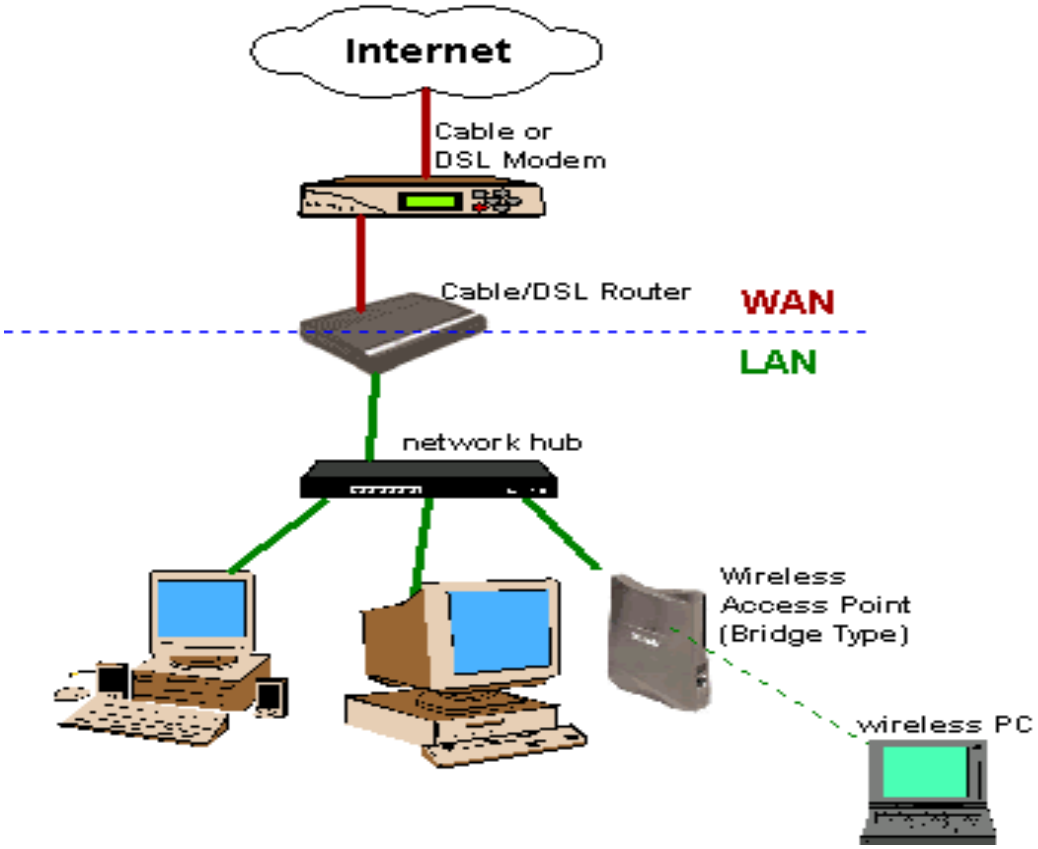
Network Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called Linear Bus topology.

Ring topology is a network in which every computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

Star topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

Network Structure



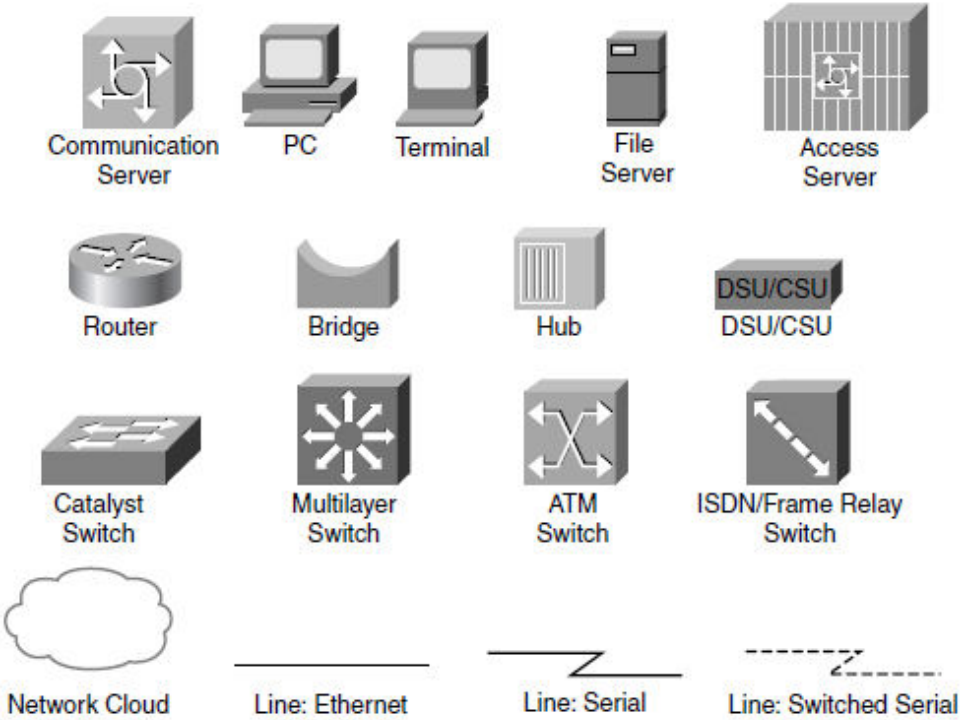
Network Devices

A computer network is basically a group of multiple networking devices connected together for data sharing. To achieve this goal every networking device has its own functionality.

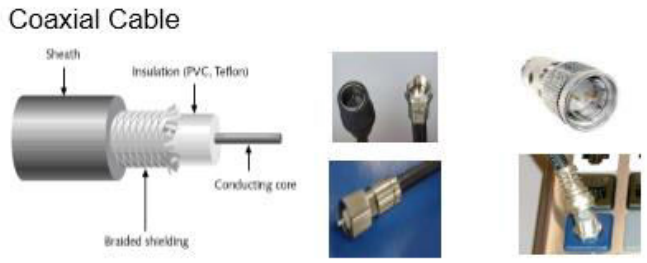
- Network Interface Card(NIC)

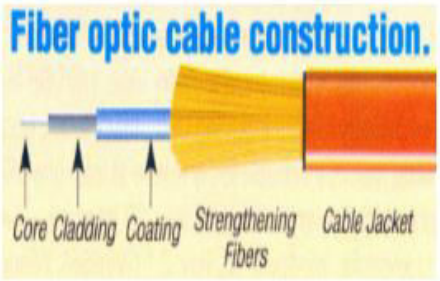
- Switch
- Router
- Modem

Hubs
Switches
Bridges
Routers
Gateways
NIC
Modems
Firewalls



Networking Cables and Connector





Interface Cable	Speed	Cable Length
Cat 5 Twisted Pair	100 Mbps	100m
Cat 5e Twisted Pair	100/1000 Mbps	100m
Cat 6 Twisted Pair	1000 Mbps	100m
Coaxial	100Mbps	185m/500m
Fiber Optic	100 Mbps/10Gbps	10Km

Determining which cable to use when wiring Device Together

Dissimilar Device (Straight Through) and **Similar Device (Cross Over)**

Straight Through

Switch / Hub - Computer NIC

Switch / Hub - Router Ethernet

Cross Over

Switch - Switch

Computer – Computer

Router Ethernet –R Ethernet

Computer NIC – R-Ethernet

Rollover

Computer COM port – Router CON port

DTE/DCE

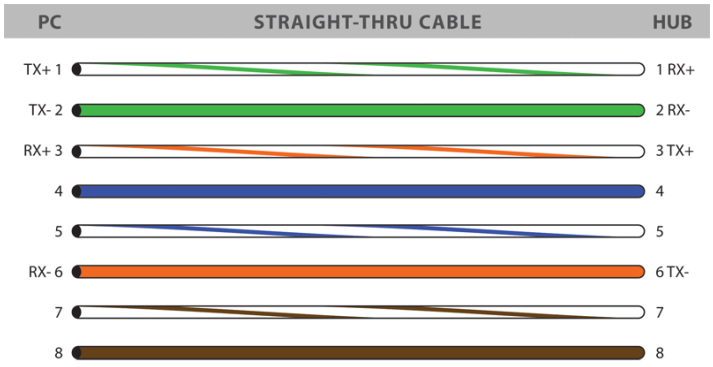
Router Serial port - Router Serial port

Twisted Pair Network

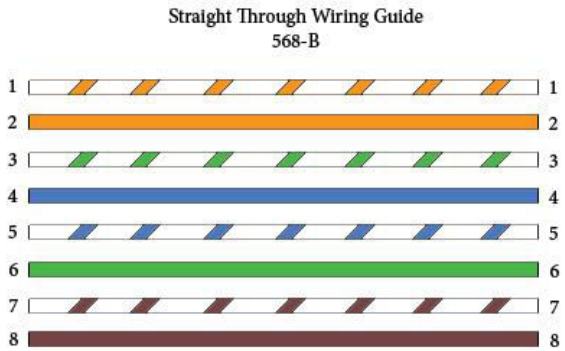
Cable Color Coding's

Straight through Cable: Wires on cable ends in the same order.

568A Standard	568A Standard
GreenWhite / Green	GreenWhite / Green
OrangeWhite / Blue	OrangeWhite / Blue
BlueWhite / Orange	BlueWhite / Orange
BrownWhite / Brown	BrownWhite / Brown

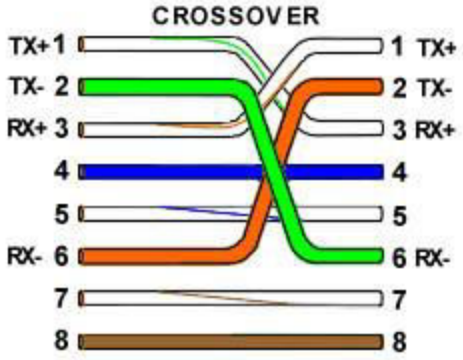


568B Standard	568B Standard
OrangeWhite / Orange	OrangeWhite / Orange
GreenWhite / Blue	GreenWhite / Blue
BlueWhite / Green	BlueWhite / Green
BrownWhite / Brown	BrownWhite / Brown

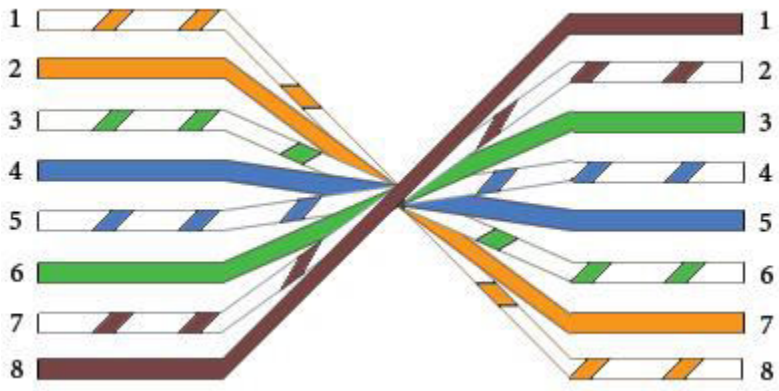


Cross Over Cable: Some wires on cable ends are crossed

568A Standard	568B Standard
GreenWhite / Green	OrangeWhite / Orange
OrangeWhite / Blue	GreenWhite / Blue
BlueWhite / Orange	BlueWhite / Green
BrownWhite / Brown	BrownWhite / Brown

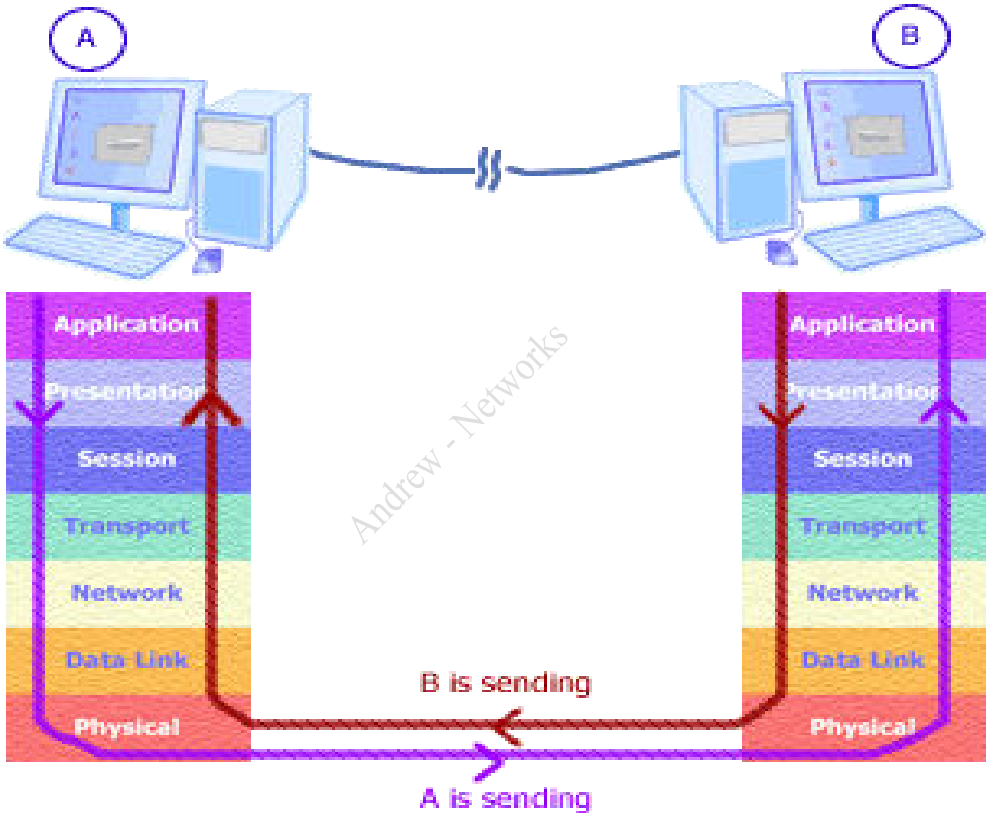


Rollover	
OrangeWhite / Orange	Brown / BrownWhite
GreenWhite / Blue	Green / BlueWhite
BlueWhite / Green	Blue / GreenWhite
BrownWhite / Brown	Orange / OrangeWhite



Chapter 2: OSI Layer (Open system Interconnection)

Different Hardware vendor or Different Operating System can communicate the network connection is called OSI layer. This model defines a networking framework to implement protocols in seven layers, with control passed from one layer to the next. Technically called Packet Structure. OSI layer is a Backbone of the Network. Standard architecture for building network systems.



L7. Application Layer - User Applications
L6. Presentation Layer - Encrypt and Decrypt
L5. Session Layer - Perform Security
L4. Transport Layer - UDP DNS Query, TCP Data, Message
L3. Network Layer - Router
L2. Data Link Layer - Switch
L1. Physical Layer - Hub, Wire Cable, Wireless

TCP / IP	Data	Layers	Protocols
Application Layer	Data	**L7. Application** Network Process to Application	HTTP,HTTPS, FTP,TELNET, DNS, DHCP, LDAP, SSH, RDP, SMTP,IMAP, POP3
	Data	**L6. Presentation** Data Representation and Encryption	JPEG, GIF, MPEG,SSL, TLS,ASCII,EBCDIC
	Data	**L5. Session** Establish, Terminate, Authentication	NetBIOS, PPTP, NFS, RPC
Transport Layer	Segments	**L4. Transport** End to End connection , Reliability	TCP,UDP
Internet Layer	Packets	**L3. Network** Route Data Packets, IP Logical Addressing, Path Determination	ICMP, IPv4, IPv6, IPsec, Routing Protocols (RIP,IGRP, EIGRP, OSPF, BGP)
Link Layer	Frames	**L2. Data Link** Physical Address, Error Detection	MAC, ARP, Ethernet, VLAN, PPP, L2TP, Frame Relay, Token Ring, HDLC, ATM, CDP, FDDI
	Bits	**L1. Physical** Wired and Wireless connection, Media, Signal, Binary Transmission	Twisted Pair, Coaxial, Optical Fiber, Wireless

L1. Physical Layer

It converts the digital/analog bits into electrical signal or optical signal. This Physical Link layer with wired Connection and wireless Connection

Wire (Copper –Electrical signals)

Twisted pair, Coaxial, Optical Fiber (Light Signal)

Wireless (Air Waves) – Electromagnetic Spectrum

Transmitter-Receiver Communication, Radio Frequency, Microwave, Satellite, Wireless ATM (Asynchronous Transfer Mode) Wi-Fi Router, Cell phone, Bluetooth, Access Point, Satellite

L2. Data Link Layer

Transmitting and receiving data frames sequentially managed by this layer. Source and Designation Identification.

Data Link Frames. MAC (Identification) and (NIC card physical Address) 48bit hexadecimal value, it's a Unique Address. CRC Cyclic Redundancy Check. ARP – IP to Physical address Mapping, **Commands**: getmac , arp -a

L3. Network Layer

The Network Layer is responsible for routing packets. Routing is a process of communication between two different Networks or same network

Gateway: router access to the another network

L3 Protocols: IP, Route, ICMP (internet Control Message Protocol)

IP address is a logical address. It's a location attribute.

ICMP Echo Request / Echo Reply

Routing Protocols: RIP, BGP, OSPF, IGRP, EIGRP

Commands: ipconfig /all, route print, ping

4. Transport Layer

Transport Layer provides end-to-end communication services for applications

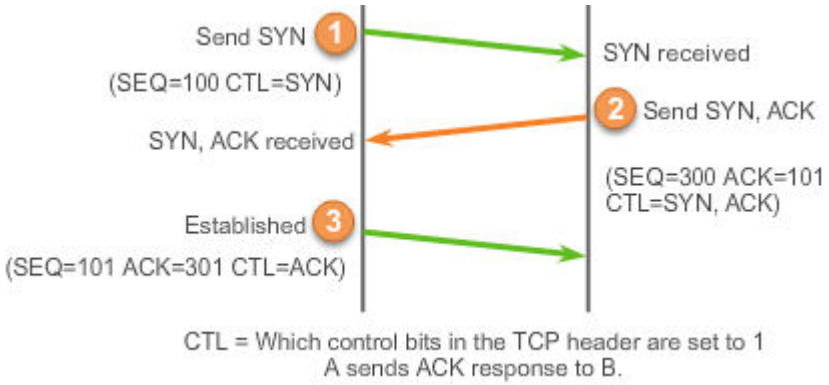
There are two Major Protocols: TCP /UDP.

TCP streaming of bytes the data one system to another (DATA PACKET)

Source port /Designation Port. Example: http protocol 80

Request / Response services like port no, Segmentation, Sync, Sequence, acknowledgement 3 way hand shake

TCP= Connection oriented, reliable, state full



UDP computer applications can send messages, in this case referred to as datagram. http:\\www.google.com (or) \\sys2

Process: Push the data

DNS query: 1) DNS name resolution, 2) NetBIOS name resolution.

UDP= Connection less, non-reliable, stateless.

Example:

Client request: http://www.yahoo.com

ftp://www.yahoo.com

Telnet 192.168.20.251

If the services are available client will get the data. Server Response to the client. In this services are located in: Http (webserver) ftp (file server)

Application Protocols and its Port Numbers

20, 21 FTP (data 20) (control 21)

23 TELNET

25 SMTP

53 DNS

80 HTTP

110 pop3, 143 IMAP, 220 IMAP3, 161 SNMP

389 LDAP

443 HTTPS Total no. of ports 65,535. Familiar: 1023

5. Session Layer

Creates a session between the source and the destination nodes and Connection time and State management, Connection Establish / Termination, Authentication and permission

6. Presentation Layer

Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data. It converts data formats into a format readable by the application layer. It performs Data compression, Data encryption, Data conversion etc... Compression: Zip, ASCII, Encode / Decode and Encryption

7. Application Layer

Application Program is an effective communication with another application program in a network. This Application layer supplies network services to end-user applications. It's a service layer that provides communication services.

HTTP, HTTPS, FTP, TELNET, DNS, DHCP, LDAP, SSH, RDP, SMTP, IMAP, POP3

Chapter 3: IP Address Classification

Internet Protocol address is an identifier assigned to each computer and other device. Such as printer, router, mobile device connected to a TCP/IP network that is used to locate and identify the node in communications with other nodes on the network.

Function: host address, id, Location

IANA has designed IPv4 4.2billions of IP, (2^{32})

IETF has designed IPv6 (2^{128})

Internet Protocol hierarchy contains IPv4 Addressing system is divided into five classes of IP Addresses

IPv4 is a 32 bit Dotted Decimal System. IP address classified in first octet referred here is the left most of all.

11111111 . 11111111 . 11111111 . 11111111
8 bit 8 bit 8 bit 8 bit = 32 bit

Class	Octet	Starting Bits	Ending Bits	IP Range
A	0	00000001	01111111	1 -127
B	10	10000000	10111111	128 -191
C	110	11000000	11011111	192 -223
D	1110	11100000	11101111	224 -239
E	1111	11110000	11111111	240 – 255

Class A : octet bit 0

Value	0	0	0	0	0	0	0	1	0	64	32	16	8	4	2	1
Bits	0	0	0	0	0	0	0	1	0	1	1	1	1	1	1	1
Base^{exp}	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

IP Address Range **1 - 127**

Address Format: **0NNNNNNN**.HHHHHHHH.HHHHHHHH.HHHHHHHH

	N	.	**H**	.	**H**	.	**H**
Subnet Mask:	**255**	.	0	.	0	.	0

No of Network/Host Bit: **2^7** **2^{24}**

Class B : octet bit 10

Value	128	0	0	0	0	0	0	0	128	0	32	16	8	4	2	1
Bits	1	0	0	0	0	0	0	0	1	0	1	1	1	1	1	1
Base^{exp}	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

IP Address Range: **128 - 191**

Address Format: **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH

	N	.	**N**	.	**H**	.	**H**
Subnet Mask:	**255**	.	**255**	.	0	.	0

No of Network/Host Bit: **2^{14}** **2^{16}**

Class C : octet bit 110

Value	128,64	0	0	0	0	0	0	128,64	0	16	8	4	2	1
Bits	1	1	0	0	0	0	0	0	1	1	0	1	1	1	1	1
Base^{exp}	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

IP Address Range: **192 - 223**

Address Format : **110NNNNN.NNNNNNNN.NNNNNNNN**.HHHHHHHH

	N	.	**N**	.	**N**	.	**H**
Subnet Mask:	**255**	.	**255**	.	**255**	.	0

No of Network/Host Bit: **2^{21}** **2^{8}`**

Class	**IP Range**	**NW/H**	**No.of.NW**	**No.of.Host**	**Subnet mask**
A	1-127	N.H.H.H	2^7-2	2^{24}-2	255.0.0.0
B	128-191	N.N.H.H	2^{14}-2	2^{16}-2	255.255.0.0
C	192-223	N.N.N.H	2^{21}-2	2^8-2	255.255.255.0
D	224-239	Reserved for Multicasting			
E	240-255	Reserved for future use / Testing or R&D Purpose			

Subnet Mask is used for determine the Network ID portion and Host ID portion

Class A: 10.0.0.1 Class B: 172.16.0.10 Class C: 192.168.1.10

255.0.0.0 255.255.0.0 255.255.255.0

11111111 = 255

8 bit

All 1 s in host portion = Broadcast address

00000000 = 0

All 0 s in host portion = network address

Reserved IP Address

127.0.0.1 - 127.255.255.254 loopback – self test

255.255.255.255 Broadcast Address

169.254.0.0 - 169.254.255.254 APIPA

APIPA (Automatic Private IP Assigning) it resolve DHCP failover

Private IP using the LAN Networks

Class	Private IP Range
A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.255.255
C	192.168.0.0 - 192.168.255.255

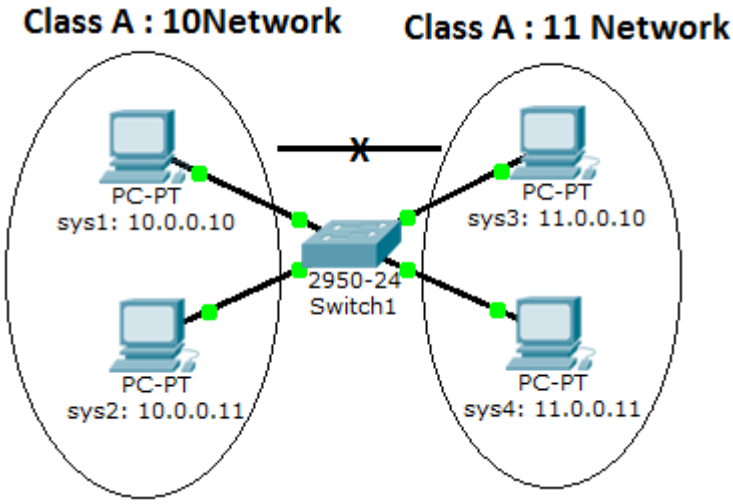
Public IP using WAN Networks

Class	Public IP Range
A	1.0.0.0 - 9.255.255.255 11.0.0.0 - 126.255.255.255
B	128.0.0.0 - 172.15.255.255 172.32.0.0 - 191.255.255.255
C	192.0.0.0 - 192.167.255.255 192.169.0.0 - 233.255.255.255

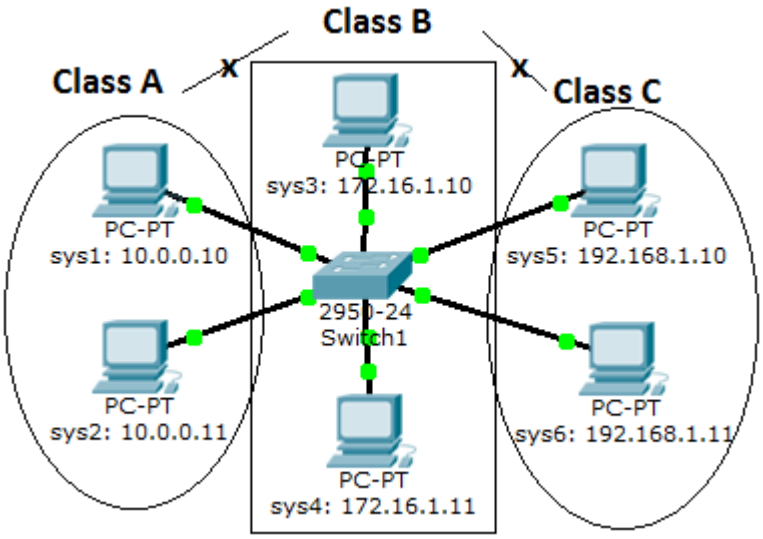
Same IP series and Different IP series

Class A	Class B	Class C
Same Series/Network		
10.0.0.10	172.16.1.10	192.168.1.10
10.0.0.11	172.16.1.11	192.168.1.11
Different Series/Network		
11.0.0.10	172.32.1.10	192.169.1.10
11.0.0.11	172.32.1.11	192.169.1.11

Class A 10 series and 11 series are different IP Series.



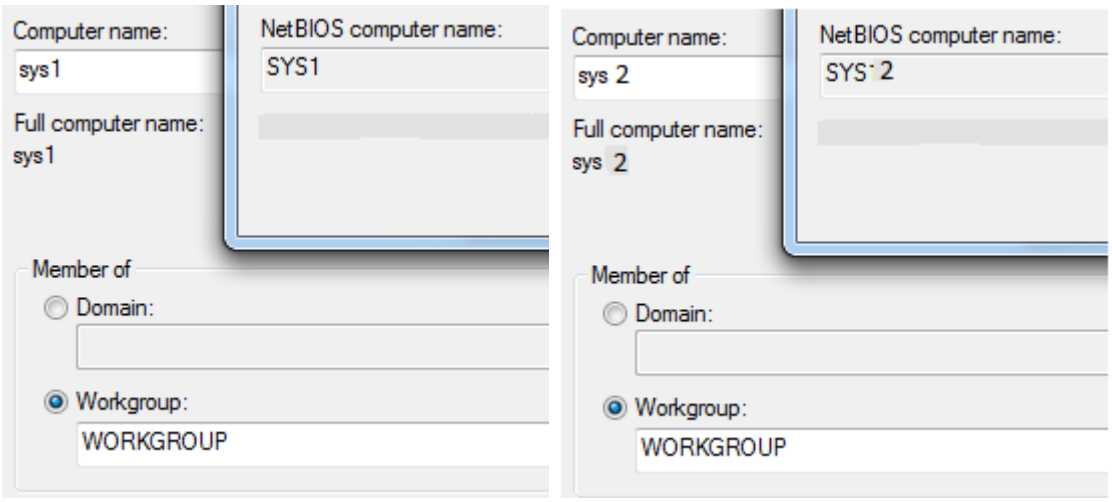
Class A, B , C IP address are different Network IP Series.



NetBIOS Name Resolution

We don't want to need IP Address can communicate one to another in Lan.

Computer name SYS1 and SYS2 communicate via NetBIOS Protocol



C:\Users\Andrew>hostname

SYS1

C:\Users\Andrew>getmac

Physical Address

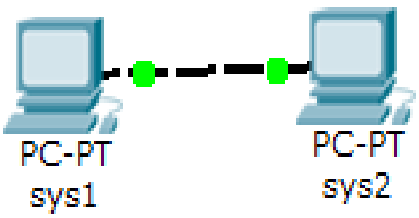
94-DE-80-5A-FD-90

C:\Users\Andrew>nbtstat –c

Local Area Connection:

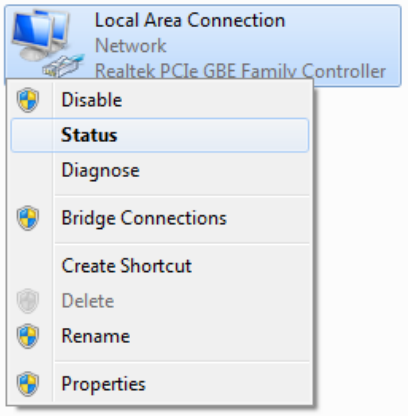
NetBIOS Remote Cache Name Table

Name	Type	Host Address	Life [sec]
SYS2	<00> UNIQUE	10.18.229.162	592

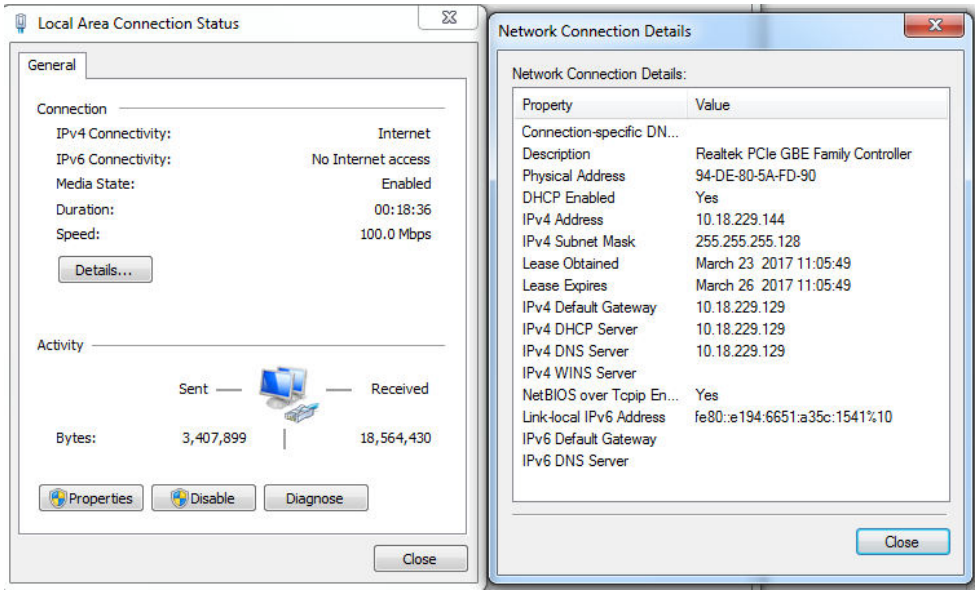


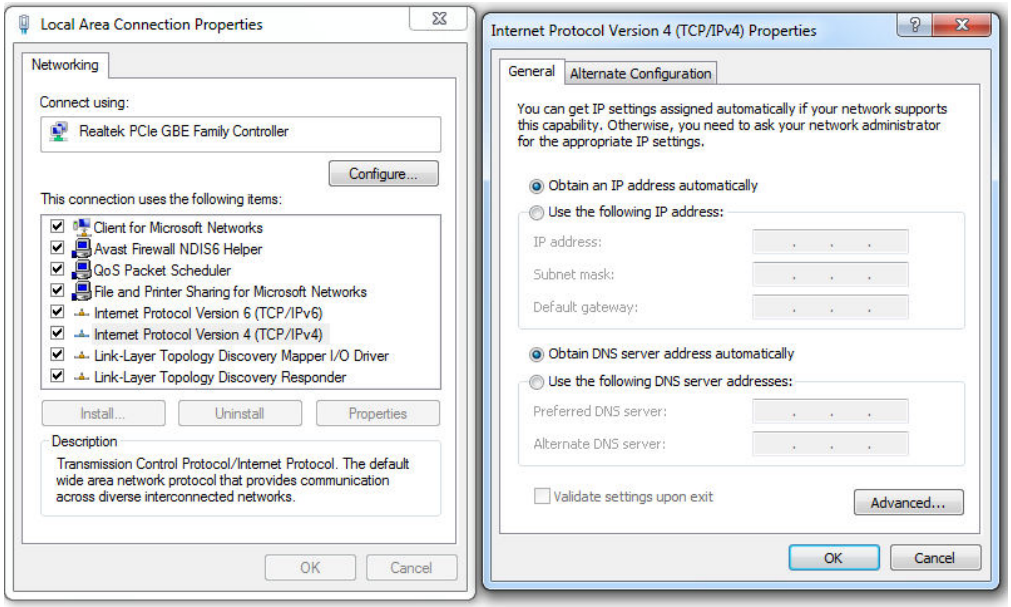
Computer IP Address

Network Connections: Go to Run, type (ncpa.cpl)



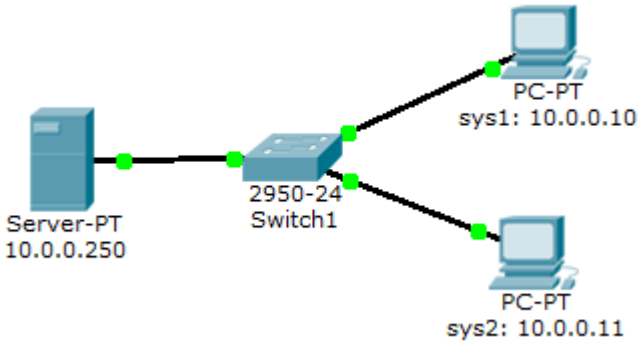
IP Address	: 192.168.1.10
Subnet Mask	: 255.255.255.0
Default Gateway	: 192.168.1.1
Preferred DNS Server	: 218.248.245.10
Alternate DNS Server	: 218245.255.140





Client – Server Configuration

Server Services
HTTP
FTP
DHCP
DNS
Email



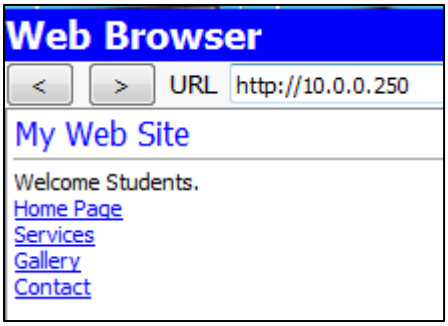
Client Request

HTTP: http://10.0.0.250

DNS: http://myweb.com

FTP: ftp://10.0.0.250 or ftp://myweb.com or cmd>ftp 10.0.0.250

Server Response



PC>ftp 10.0.0.0250 or ftp myweb.com

Trying to connect...

Username: Andrew

Password: ******

ftp>dir

Listing /ftp directory from myweb.com:

0 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768

1 : c1841-ipbase-mz.123-14.T7.bin 13832032

Basic Network Commands

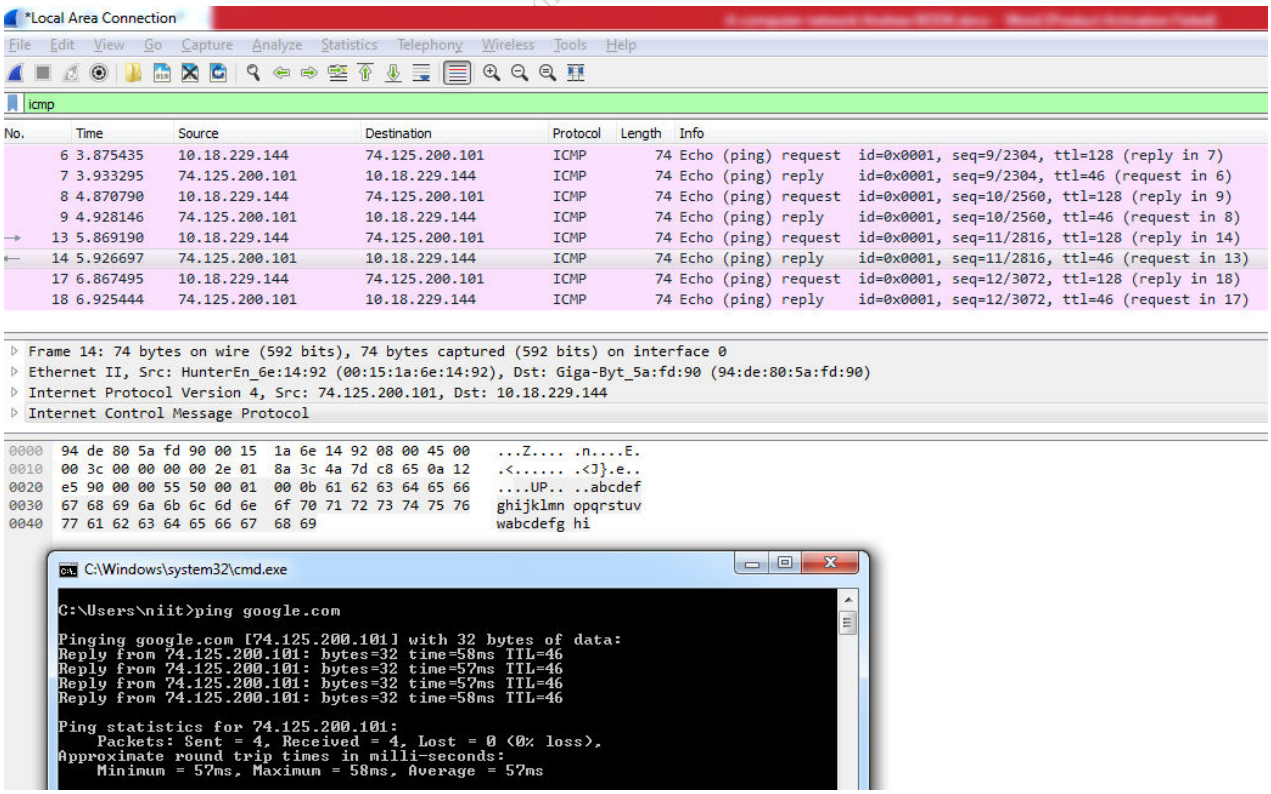
1. Ping www.google.com , ping 192.168.1.1
2. Pathping www.google.com , ping 192.168.1.251
3. Tracert www.google.com , ping 192.168.1.251
4. Nslookup www.google.com, ping 192.168.1.251
5. Ipconfig /all (Identify your computer IP address & Name)
6. Arp –a (Address resolution protocol cache the ip
7. Netstat –a (open the network port numbers)
8. Nbtstat –c (netbios cache the ip computers)
9. \\computername\sharename

   UNC (universal Naming Conventional)

Network Monitoring Tool

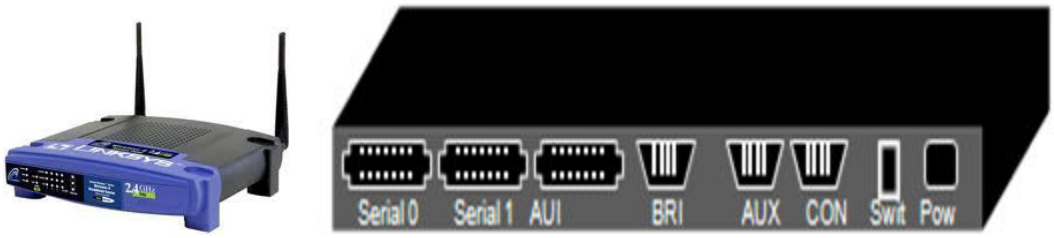
Microsoft Network Monitoring Tool

Wireshark



Chapter 4: Router Configuration

Router is a networking Layer3 device that forwards data packets between computer networks. It is a process of communication between two different Networks or same network. The Network Layer is responsible for routing packets. Router act as a gateway and Maintain Routing Table.



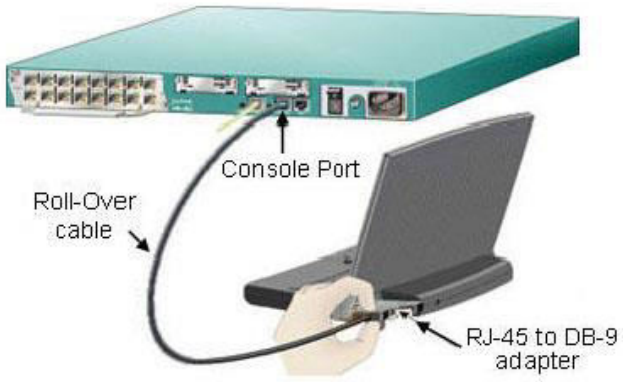
Serial0 and Serial1 : Router to Router Connection

AUI (Attachment Unit Interface) : Router to Lan and Ethernet Connection

BRI (Basic Rate Interface) : ISDN BRI Voice Interface Card

AUX (Auxiliary port) : Router to Modem Connection

CON(Console Port):Router to Computer com port/RJ-45 to DB-9 Adapter



Router Models: 2501, 2514, 2610, 2611, 2620, 2621, 2801, 2811, 1721, 1760, 1841

Router Modes:

	Mode	Prompt
1	**User Execution Mode** Entry Level , EXEC Commands	**Router> enable** Router>?
2	**Privileged Mode** show command and ping, debug	**Router# configure terminal** Router# show interface
3	**Global Configuration Mode** enable password, host name enter interface mode enter a number of protocol mode ip host Andrew 10.0.0.10	**Router(config)# hostname RA** **RA(config)# interface ethernet 0** RA(config-if)# **RA(config)# Router RIP** Router(config-router)#
4	**Specific Configuration Mode**	
4.1	Interface Mode Interface configuration mode	**Router(config-if)#** IP address 10.0.0.1 255.0.0.0 No shutdown
4.2	Router Protocol Mode Routing protocols configuration	**Router(config-router)#** Network 10.0.0.0
4.3	Sub Interface Mode Virtual interface configuration	Router(config-subif)# Interface serial 2/0.1
4.4	Line Mode Virtual terminal line configuration	Router(config-line)# Line vty 01

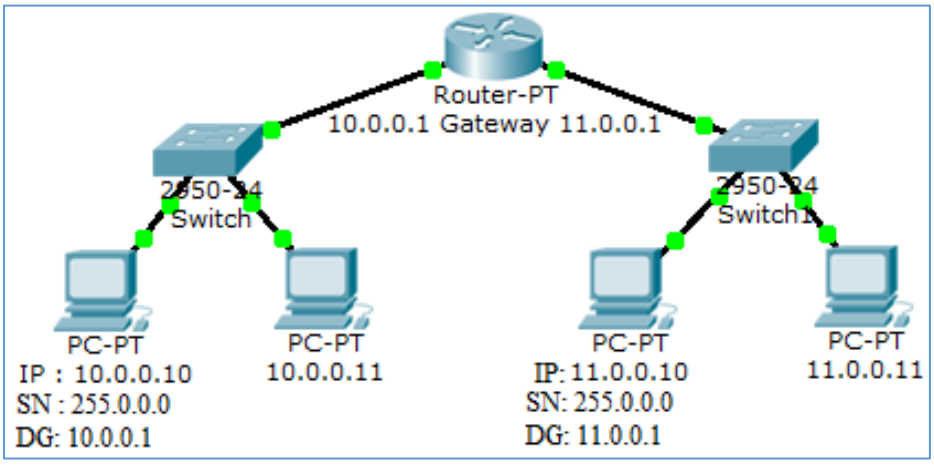
Simple Steps:

1) Router>enable
2) Router#configure Terminal
3) Router(config)#interface serial 0 or(config)# interface fastEthernet 0/0
4) Router(Config-if)#ip address 10.0.0.1 255.0.0.0 / no ip address
5) Router(config-if)#no shutdown (up) / shutdown(down)
6) Router(config-if)#exit
7) Router(config)#router rip / no router rip (remove rip)
8) Router(config-router)#network 10.0.0.0 / no network (remove)

Show Commands

Router> enable Router#disable, Router#logout, Router#exit

Router# show ?	Lists all show commands available.
Router# show interfaces	Displays statistics for all interfaces.
Router#show interface serial0	Displays statistics for specific interfaces
Router#**show ip interface brief**	Displays a summary of all interfaces
Router#**show ip route**	Displays IP routing Tables
Router#show hosts	Displays a localhost to ip address cache
Router#show users	Displays all users connected to device
Router#show history	Displays history of commands
Router#show flash	Displays information about Flash memory
Router#show version	Displays information about current IOS
Router#show arp	Displays the ARP table
Router#**show protocols**	Displays layer 3 protocols
Router#show startup-config	Displays configuration saved in NVRAM
Router#show running-config	Displays configuration currently running
Router#copy run start	Saves the running-config to local NVRAM
Router#erase start	Delete the startup-config file from nvram



Simple Routing Configuration

Router>enable

Router#configure Terminal

Router(config)#interface serial 0 or(config)# interface **fastEthernet 0/0**

Router(Config-if)#ip address 10.0.0.1 255.0.0.0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface serial 1 or(config)# interface **fastEthernet 0/1**

Router(Config-if)#ip address 11.0.0.1 255.0.0.0

Router(config-if)#no shutdown

Router(config-if)#exit

Try:

10.0.0.0/8 Network and 192.168.1.0/24 Network

172.16.0.0/14 Network and 172.31.0.0 Network

192.168.1.0/24 Network and 192.168.2.0/24 Network

IP Address : 192.168.1.10 (**Recall)**

Subnet mask: 255.255.255.0

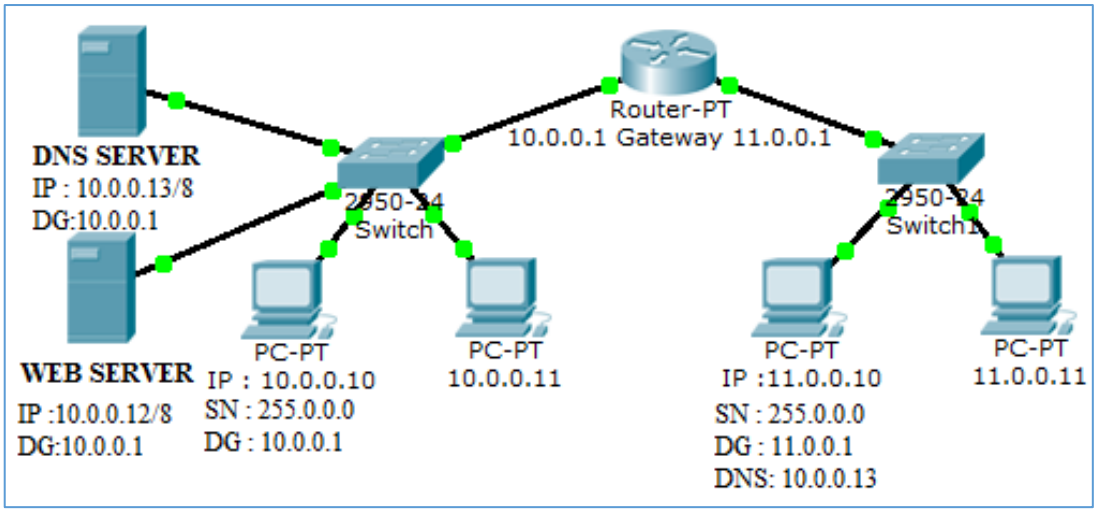
Network address is 192.168.1 and host address is 10

Binary Format

IP address 11000000.10101000.00000001.00001010

Subnet mask 1111111.11111111.11111111.00000000

DNS Server address and Webserver Configuration



Password Management

Enable Password : Router(config)# enable password 123

Secret Password : Router(config)# enable secret admin

Console Password: Router(config)# line console 0

Router(config-line)# password console

Router(config-line)# login

Virtual Terminal Password: Router(config)# line vty 04

Router(config-line)# password AAA

Router(config-line)# login

Auxiliary Password : Router(config)# line aux 0

Router(config-line)# password AAB

Router(config-line)# login

Encryption Password : Router(config)#service password-encryption

Router(config)#enable password 123

Show Routing Table in Computer Systems

C:\users\Andrew>route print

```
C:\Documents and Settings\admin>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 16 76 8e 3a 2b ...... Realtek RTL8139 Family PCI Fast Ethernet NIC -
eefer2 Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.12.1    192.168.20.2      20
        127.0.0.0        255.0.0.0      127.0.0.1      127.0.0.1       1
      192.168.0.0      255.255.0.0    192.168.20.2    192.168.20.2      20
     192.168.20.2  255.255.255.255      127.0.0.1      127.0.0.1      20
   192.168.20.255  255.255.255.255    192.168.20.2    192.168.20.2      20
        224.0.0.0        240.0.0.0    192.168.20.2    192.168.20.2      20
  255.255.255.255  255.255.255.255    192.168.20.2    192.168.20.2       1
Default Gateway:      192.168.12.1
===========================================================================
Persistent Routes:
  None
```

Chapter 5: Static Routing & Dynamic Routing

Static Route:

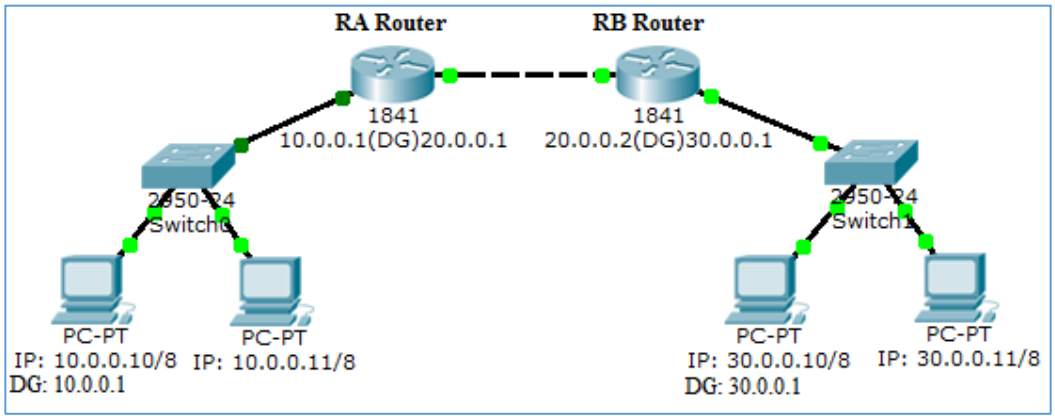
Use a route that a network administrator enters into the router manually.

Dynamic Route:

Use a route that a network routing protocol adjusts automatically for topology or traffic changes.

* RIPv1 uses classful routing protocol; RIPv2 uses classless routing protocol

- **Router(config)#router rip**
- **Router(config-router)# version 2**



RA Router : assign IP address

```
Router> enable
Router# configure terminal
Router(config)#interface fastEthernet 0/0
Router(config-if)# ip address 10.0.0.1  255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)#
Router(config)#interface fastEthernet 0/1
Router(config-if)# ip address 20.0.0.1  255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)#exit
Router#
```

RB Router : assign IP address

```
Router> enable
Router# configure terminal
Router(config)#interface fastEthernet 0/0
Router(config-if)# ip address 30.0.0.1  255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)#
```

Router(config)#interface fastEthernet 0/1

Router(config-if)# ip address 20.0.0.2 255.0.0.0

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)#

RA Router : assign Static Route

Router> enable

Router# configure terminal

Router(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.2

(Destination Network: 30.0.0.0, mask 255.0.0.0 via 20.0.0.2)

RB Router : assign Static Route

Router> enable

Router# configure terminal

Router(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1

(Destination Network: 10.0.0.0, mask 255.0.0.0 via 20.0.0.1)

Verify Commands

Roure# show ip protocols

Roure# show ip interface brief

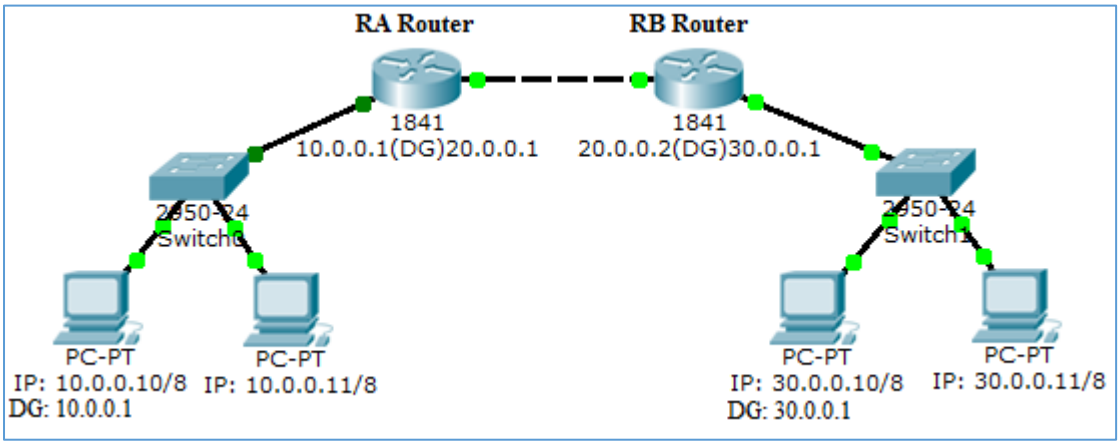
Router#ping 30.0.0.1

Router#show ip route

Router#show interfaces

Router#show interface fastEthernet 0/1

Dynamic Route – RIP Protocol



RA Router

Router> enable

Router# configure terminal

Router(config)#router rip

Router(config-router)# network 10.0.0.0

Router(config-router)# network 20.0.0.0

RB Router

Router> enable

Router# configure terminal

Router(config)#router rip

Router(config-router)# network 20.0.0.0

Router(config-router)# network 30.0.0.0

Verify Commands

Router#show ip rip database

Router#show ip route

Router#show ip protocols

Chapter 6: SUBNET

Subnetting is a process of dividing large network into the smaller networks and Sub divided group of networks. Subnet mask value is changed into **Netmask.**

As IP addresses are limited, so it reduces the IP wastage, a large network can be divided into various small networks using subnetting. It involves conversion of host bits into network bits. Usage: Fast, Security, Avoid Data traffic/ same bandwidth/same broadcast.

FLSM Fixed-Length subnet masking is a sequence of numbers unchanging length that streamlines and it is dividing IP into subnet with same range. All subnets have the same number of hosts, this is known as FLSM.

VLSM Variable-Length Subnet Masking is dividing IP into subnet with different sizes. VLSM is a process of dividing an IP network into the subnets of different sizes without wasting IP addresses.

It is the ability to specify a different subnet mask for the same network number on different subnets. It can helps to optimize a available address space. When calculating the subnets manually, you should allocate addresses to the largest subnets first. This results in the most efficient use of addresses.

WAN links require only two IP addresses. This results in the smallest subnet possible. As a result, WAN link subnets are best allocated at the end of the address space

Classless Inter Domain Routing (CIDR) provides the flexibility of borrowing bits in the Host part of the IP address and using them as Network in Network, called Subnet.

Class C - Network ID: 192.168.1.0 / 24

NID	**192**	**.**	**168**	**.**	**1**	**.**	**0**
SM	**255**		**255**		**255**		**0**

Q: Need 8 Sub Network? / Borrow 3 Bits? / Need 30 host per subnet?

IP	192	.	168	.	1	.	**0**
SM	255		255		255		**111 00000**
	N		N		N		**SSS hhhhh**

Subnet Bitmap

110NNNNN	.	NNNNNNNN	.	NNNNNNNN	.	**SSS hhhhh**

No.of.Host	128	64	**32**	0	0	0	0	0	32-2=**30 host**
No.of.Subnet	2	4	**8**	16	32	64	128	256	
Subnet Bits	**1**	**1**	**1**	0	0	0	0	0	
Base^{exponent}	2^7	2^6	$\mathbf{2^5}$	2^4	2^3	2^2	2^1	2^0	$\mathbf{2^5}$

No.of Subnet Bits / Borrow Bits =**3**

No.of Subnet = **8**

No.of Host bits = **5** No.of Host per Subnet = 2^5-2=**30**

No.of Mask Bits = **27**

Subnet Bits / Borrow bits: **1 1 1 0 0 0 0 0**

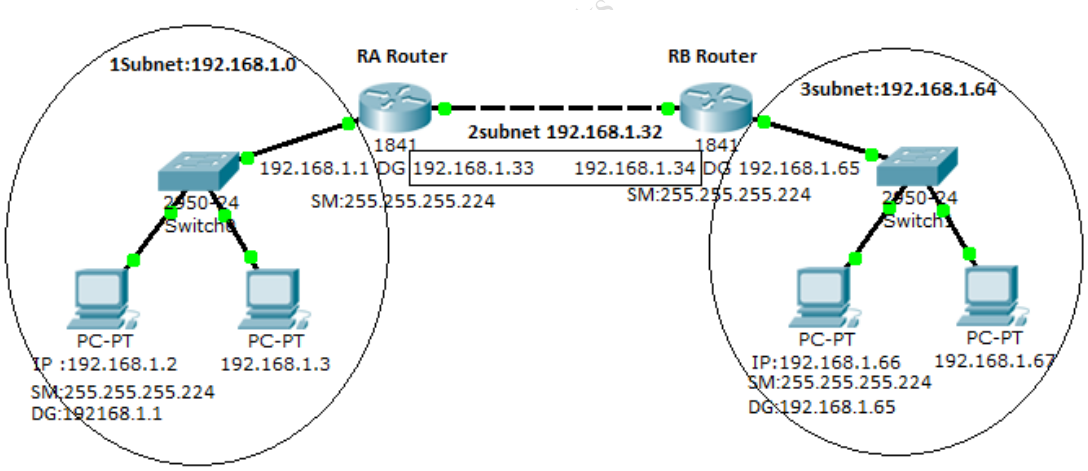
Mask Value: 128+64+32 = **224**

New Subnet Mask (**NSM**): 255.255.255**.224**

Subnet Table

	Subnet NID	FHID	LHID	BID
1	**192.168.1.0**	192.168.1.**1**	192.168.1.**30**	192.168.1.**31**
2	**192.168.1.32**	192.168.1.**33**	192.168.1.**62**	192.168.1.**63**
3	**192.168.1.64**	192.168.1.**65**	192.168.1.**94**	192.168.1.**95**
4	**192.168.1.96**	192.168.1.**97**	192.168.1.**126**	192.168.1.**127**
5	**192.168.1.128**	192.168.1.**129**	192.168.1.**158**	192.168.1.**159**
6	**192.168.1.160**	192.168.1.**161**	192.168.1.**190**	192.168.1.**191**
7	**192.168.1.192**	192.168.1.**193**	192.168.1.**222**	192.168.1.**223**
8	**192.168.1.224**	192.168.1.**225**	192.168.1.**254**	192.168.1.**255**
	192.168.1.256 x			

NID = Network Id, FHID = First host, LHID= Last host, BID=Broadcast



Static Route

RA(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.34

RB(config)#ip route 192.168.1.0 255.255.255.224 192.168.1.33

Dynamic Routing

RA(config)#router RIP

RA(config-router)#version 2

RA(config-router)#network 192.168.1.0

RA(config-router)#network 192.168.1.32

RB(config-router)#network 192.168.1.32

RB(config-router)#network 192.168.1.64

Class B - Network ID: 172.16.0.0 / 16

Q: Need 8 Sub Network? / Borrow 3 Bits? / Need 8000 host per subnet?

NID	**172**	**.**	**16**	**.**	**0**	**.**	**0**
SM	**255**		**255**		**0**		**0**

IP	172	.	16	.	0	.	0
SM	255		255		**111** 00000		00000000
	N		**N**		**SSS** hhhhh		Hhhhhhhh

Subnet Bitmap

10NNNNNN	.	NNNNNNNN	.	**SSS hhhhh**	.	**hhhhhhhh**

Host	**8192**, 0, 0, 0, 0, 0	8192-2=8190 **host**
Subnet	2 4 **8** 16 32 64 128 256	
Borrow Bits	**1 1 1** 0 0 0 0 0	
Base^{exponent}	2^{15} 2^{14} $\mathbf{2^{13}}$ 2^{12} 2^{11} 2^{10} 2^{9} 2^{8}	$\mathbf{2^{13}}$

No.of Subnet Bits / Borrow Bits =**3**

No.of Subnet = **8**

No.of Host bits = **13** No.of Host per Subnet = 2^{13}-2=**8190**

No.of Mask Bits = **19**

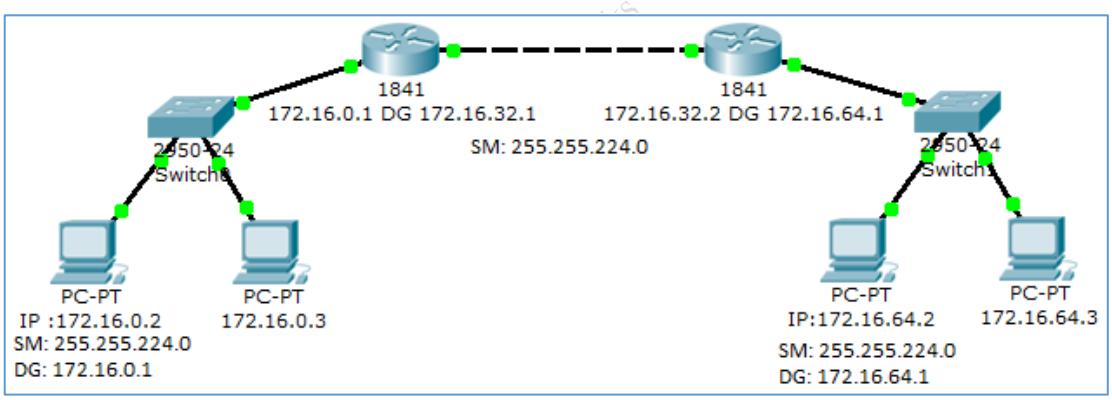
Borrow Bits: **1 1 1 0 0 0 0 0**

Mask Value: 128+64+32 = **224**

New Subnet Mask (**NSM**): 255.255.**224.0**

Subnet Table

	Subnet NID	FHID	LHID	BID
1	**172.16.0.0**	172.16.**0.1**	172.16.**31.254**	172.16.**31.255**
2	**172.16.32.0**	172.16.**32.1**	172.16.**63.254**	172.16.**63.255**
3	**172.16.64.0**	172.16.**64.1**	172.16.**95.254**	172.16.**95.255**
4	**172.16.96.0**	172.16.**96.1**	172.16.**127.254**	172.16.**127.255**
5	**172.16.128.0**	172.16.**128.1**	172.16.**159.254**	172.16.**159.255**
6	**172.16.160.0**	172.16.**160.1**	172.16.**191.254**	172.16.**191.255**
7	**172.16.192.0**	172.16.**192.1**	172.16.**233.254**	172.16.**223.255**
8	**172.16.224.0**	172.16.**224.1**	172.16.**255.254**	172.16.**255.255**
	172.16.256.0 x			



RA(config)#ip route 172.16.64.0 255.255.224.0 172.16.32.2

RB(config)#ip route 172.16.0.0 255.255.224.0 172.16.32.1

Class A - Network ID: 10.0.0.0 / 8

NID	**10**	**.**	**0**	**.**	**0**	**.**	**0**
SM	**255**		**0**		**0**		**0**

Q: Need 8 Sub Network? / Borrow 3 Bits? / Need 8000 host per subnet?

IP	10	.	0	.	0	.	0
SM	255		**111** 00000		00000000		00000000
	N		**SSS** hhhhh		hhhhhhhh		hhhhhhhh

Subnet Bitmap

0NNNNNNN	.	**SSS hhhhh**	.	**hhhhhhhh**	.	**hhhhhhhh**

Host	**2097152**, 0, 0, 0,0, 0	2097152-2=2097150 **host**
Subnet	2 4 **8** 16 32 64 128 256	
Borrow Bits	**1 1 1** 0 0 0 0 0	
Base^{exponent}	2^{23} 2^{22} $\mathbf{2^{21}}$ 2^{20} 2^{19} 2^{18} 2^{17} 2^{16}	$\mathbf{2^{21}}$

No.of Subnet Bits / Borrow Bits =**3**

No.of Subnet = **8**

No.of Host bits = **21** No.of Host per Subnet = 2^{21}-2=**2097150**

No.of Mask Bits = **11**

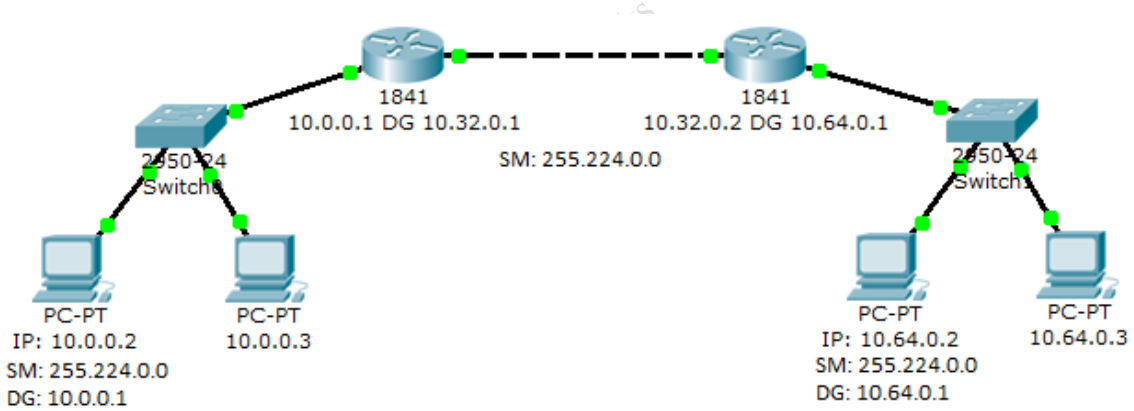
Borrow Bits: **1 1 1 0 0 0 0 0**

Mask Value: 128+64+32 = **224**

New Subnet Mask (**NSM**): 255.**224.0.0**

Subnet Table

	Subnet NID	FHID	LHID	BID
1	**10.0.0.0**	10.0.0.**1**	10.**31.255.254**	10.**31.255.255**
2	**10.32.0.0**	10.32.0.1	10.63.255.254	10.63.255.255
3	**10.64.0.0**	10.64.0.1	10.95.255.254	10.95.255.255
4	**10.96.0.0**	10.96.0.1	10.127.255.254	10.127.255.255
5	**10.128.0.0**	10.128.0.1	10.159.255.254	10.159.255.255
6	**10.160.0.0**	10.160.0.1	10.191.255.254	10.191.255.255
7	**10.192.0.0**	10.192.0.1	10.223.255.254	10.223.255.255
8	**10.**224.0.0	10.224.0.1	10.255.255.254	10.255.255.255
	10.256.0.0 x			



RA(config)#ip route 10.64.0.0 255.224.0.0 10.32.0.2

RB(config)# ip route 10.0.0.0 255.224.0.0 10.32.0.1

Reference Website Address

http://www.subnet-calculator.com/

VLSM

http://subnettingpractice.com/vlsm.html/

Class C - Network ID: 192.168.1.0 / 24

NID	**192**	**.**	**168**	**.**	**1**	**.**	**0**
SM	**255**		**255**		**255**		**0**
	N		**N**		**N**		**H**

Subnet Name Number of Hosts

Lab1 50

Router IP 2

Lab2 30

Lab1: 50 hosts

Host	128	**64**	32	16	8	4	2	1	64-2=**62 host**
	2^7	**2^6**	2^5	2^4	2^3	2^2	2^1	2^0	

IP	192	.	168	.	1	.	**11** 000000
SM	255		255		255		**SS** hhhhhh

Subnet Bitmap

110NNNNN	.	NNNNNNNN	.	NNNNNNNN	.	**SS hhhhhh**

Host	128	**64**	0	0	0	0	0	0	64-2=**62 host**
Borrow Bits	**1**	**1**	0	0	0	0	0	0	
Base^{exponent}	2^7	**2^6**	2^5	2^4	2^3	2^2	2^1	2^0	**2^6**

No.of Host bits = **6** No.of Host per Subnet = 2^6-2=**62**

No.of Subnet Bits / Borrow Bits =**2**

No.of Mask Bits = **26**

Borrow bits: **1 1 0 0 0 0 0 0**

Mask Value: 128+64 = 192

New Subnet Mask (**NSM**): 255.255.255**.192**

Lab2: 30 hosts

Host	128 64 **32** 16 8 4 2 1	32-2=**30 hosts**
Base^{exponent}	2^7 2^6 $\mathbf{2^5}$ 2^4 2^3 2^2 2^1 2^0	

IP	192	.	168	.	1	.	**111** 00000
SM	255		255		255		**SSS** hhhhh

Subnet Bitmap

110NNNNN	.	NNNNNNNN	.	NNNNNNNN	.	**SSS hhhhh**

Host	128 64 **32** 16 8 4 2 1	32-2=30 **host**
Borrow Bits	**1** 1 **1** 0 0 0 0 0	
Base^{exponent}	2^7 2^6 $\mathbf{2^5}$ 2^4 2^3 2^2 2^1 2^0	$\mathbf{2^5}$

No.of Host bits = **5** No.of Host per Subnet = 2^5-2=**30**

No.of Subnet Bits / Borrow Bits =**3**

No.of Mask Bits = **27**

Borrow bits: **1 1 1 0 0 0 0 0**

Mask Value: 128+64+32 = 224

New Subnet Mask (**NSM**): 255.255.255**.224**

Router IP: 2 hosts

Host	128	64	32	16	8	**4**	2	1	4-2=**2 hosts**
Base^{exponent}	2^7	2^6	2^5	2^4	2^3	$\mathbf{2^2}$	2^1	2^0	

IP	192	.	168	.	1	.	**111111** 00
SM	255		255		255		**SSSSSS** hh

Subnet Bitmap

110NNNNN	.	NNNNNNNN	.	NNNNNNNN	.	**SSSSSS hh**

Host	128	64	32	16	8	**4**	2	1	4-2=2 **host**
Borrow Bits	**1**	**1**	**1**	**1**	**1**	**1**	0	0	
Base^{exponent}	2^7	2^6	2^5	2^4	2^3	$\mathbf{2^2}$	2^1	2^0	$\mathbf{2^2}$

No.of Host bits = 2 No.of Host per Subnet = 2^2-2=2

No.of Subnet Bits / Borrow Bits =6

No.of Mask Bits = **30**

Borrow bits: **1 1 1 1 1 1 0 0**

Mask Value: 128+64+32+16+8+4 = 252

New Subnet Mask (**NSM**): 255.255.255**.252**

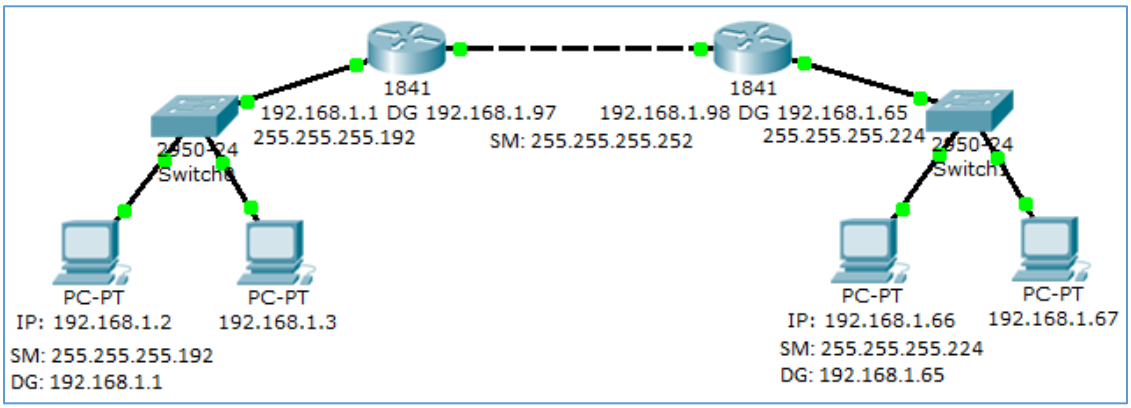
VLSM Subnet Table:

	Subnet NID	**FHID**	**LHID**	**BID/ wildcard**
A	**192.168.1.0**	192.168.1.**1**	192.168.1.**62**	192.168.1.**63 /63**
C	**192.168.1.64**	192.168.1.**65**	192.168.1.**94**	192.168.1.**95/31**
B	**192.168.1.96**	192.168.1.**97**	192.168.1.**98**	192.168.1.**99/3**
	192.168.1.100 x			

A: 192.168.1.1/26 or IP: 192.168.1.1 mask: 255.255.255.192

B: 192.168.1.97/30 or IP: 192.168.1.97 mask: 255.255.255.252

C: 192.168.1.65/27 or IP: 192.168.1.65 mask: 255.255.255.224



Static Route

RA(config)# ip route 192.168.1.64 255.255.255.224 192.168.1.98

RB(config)# ip route 192.168.1.0 255.255.255.192 192.168.1.97

RIP

RA(config)#router rip

RA(config-router)#version 2

RA(config-router)#network 192.168.1.0

RA(config-router)#network 192.168.1.96

RB(config-router)#network 192.168.1.64

RB(config-router)#network 192.168.1.96

Verify Command

Router#show ip rip database

Subnet bit & Values	Net mask value	No.of subnet	No.of Host
1000 0000 = 128	255.255.255.128	2	2^7-2 = 126
1100 0000 = 192	255.255.255.192	4	2^6-2 = 62
1110 0000 = 224	255.255.255.224	8	2^5-2 = 30
1111 0000 = 240	255.255.255.240	16	2^4-2= 14
1111 1000 = 248	255.255.255.248	32	2^3-2 = 6
1111 1100 = 252	255.255.255.252	64	2^2-2 = 2
1111 1110 = 254	255.255.255.254	128	2^1-2 = 0
1111 1111 = 255	255.255.255.255	Broadcast	

Administrative Distance

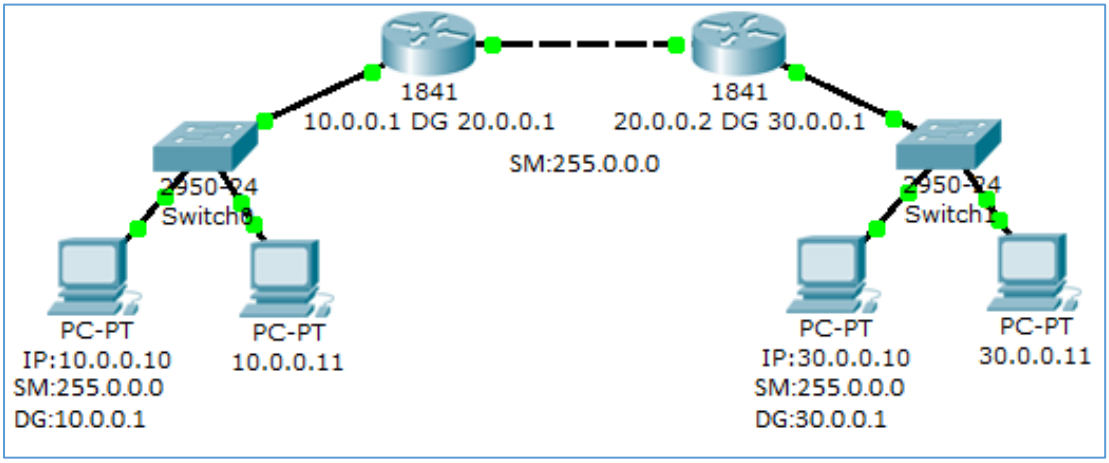
Administrative distance rates the "trustworthiness" of a route. AD is a number from 0- 255, where 0 is absolutely trusted and 0 is assigned directly to connected route. A static route is assigned an administrative distance (AD) of 1. AD of 1 is an extremely reliable rating.

Route Type	**Administrative Distance**
Connected	0
Static	1
EIGRP Summary Route	5
EBGP	20
EIGRP internal	90
IGRP	100
OSPF	110
RIP	120

Chapter 7: EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced Distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration.100% loop-free classless routing. Easy configuration and Flexible network design.

Router eigrp 100 is the autonomous system (AS) number.
Range (1-65535) all routers in the same AS must use the same AS number. Turns off the Auto-Summarization feature.



RA(config)# router eigrp 100

RA(config-router)#network 10.0.0.0

RA(config-router)#network 20.0.0.0

IP-EIGRP 100: neighbor 20.0.0.2 is up. New Adjacency

RA(config-router)#no auto-summary

RB(config)# router eigrp 100

RB(config-router)#network 20.0.0.0

RB(config-router)#network 30.0.0.0

IP-EIGRP 100: neighbor 20.0.0.1 is up. New Adjacency

Verifying Eigrp

RB#show ip eigrp interfaces

RB#show ip eigrp neighbours

RB#show ip protocols

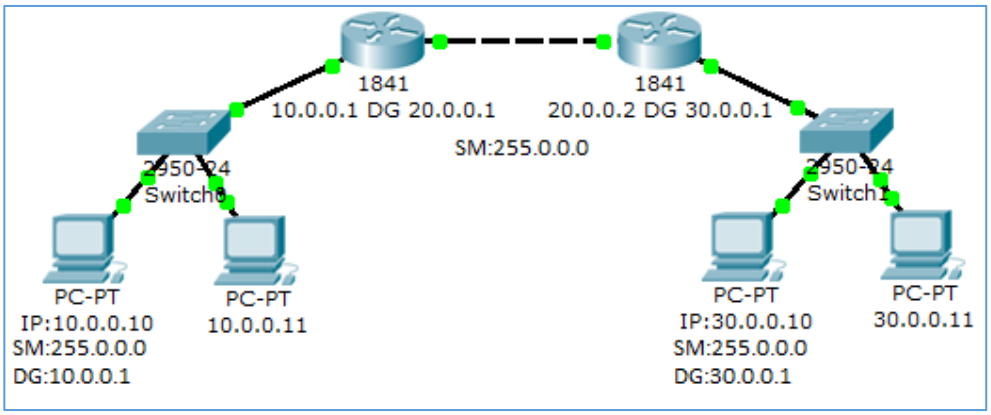
OSPF

Single-Area OSPF (Open Shortest Path First)

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) standardized by the Internet Engineering Task Force (IETF) and commonly used in large Enterprise networks. OSPF is a link-state routing protocol providing fast convergence and excellent scalability. Like all link-state protocols, OSPF is very efficient in its use of network bandwidth.

It supports both IPv4 and IPv6 routed protocols. It supports load balancing with equal cost routes for same destination. Since it is based on **open standards**, it will run on most routers.

Link state advertisement (LSA) is data packet. It contains link-state and routing information. OSPF uses it to share and learn network information.



RA Router:

Router(config)#no ip domain-lookup

(Turns off DNS Queries so that spelling mistakes will not show you down)

Router(config)#router ospf 1

Router(config-router)#network 10.0.0.0 0.0.0.255 area 0

Router(config-router)#network 20.0.0.0 0.0.0.255 area 0

(OSPF advertise interfaces, not networks. uses the wildcard mask to determine which interface to advertise. Any interface with an address of 10.x.x.x area 0)

RB Router:

Router(config)#no ip domain-lookup

Router(config)#router ospf 2

Router(config-router)#network 20.0.0.0 0.0.0.255 area 0

OSPF-5-ADJCHG: Process 2, Nbr 20.0.0.1 on FastEthernet0/1 from LOADING to FULL, Loading Done

Router(config-router)#network 30.0.0.0 0.0.0.255 area 0

Verifying OSPF

Router#show ip protocols

Router#show ip route

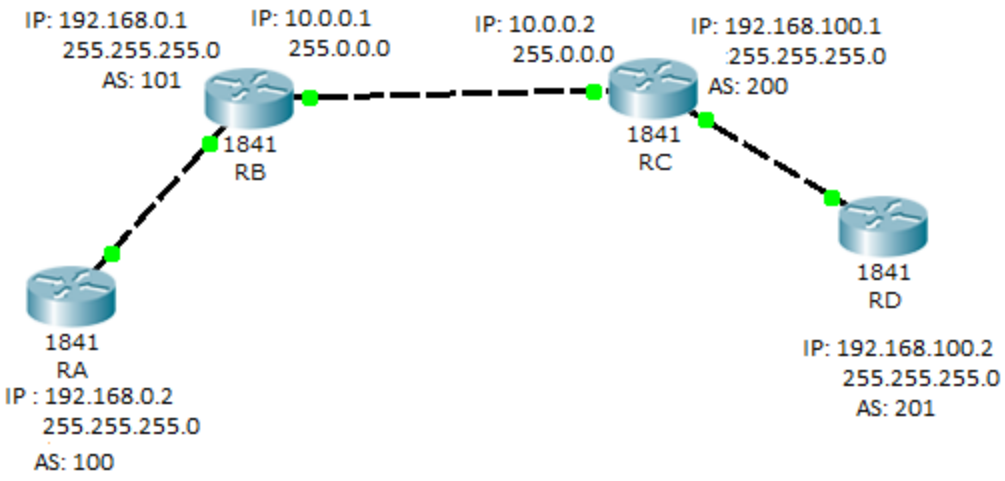
Router#show ip ospf

Router#show ip ospf neighbor

Router#show ip ospf neighbor detail

BGP

Border Gateway Protocol (**BGP**) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous system (AS) on the Internet. The protocol is often classified as a path vector protocol . Sometimes it will classed as a distance-vector routing protocol. BGP is the routing protocol of the global Internet, as well as for Service Provider private networks.



RA(config)#router bgp 100

RA(config-router)#neighbor 192.168.0.1 remote-as 101

RA(config-router)#network 192.168.0.0 mask 255.255.255.0

RB(config)#router bgp 101

RB(config-router)#neighbor 192.168.0.2 remote-as 100

RB(config-router)#neighbor 10.0.0.2 remote-as 200

RB(config-router)#network 192.168.0.0 mask 255.255.255.0

RB(config-router)#network 10.0.0.0 mask 255.0.0.0

RC(config)#router bgp 200

RC(config-router)#neighbor 192.168.100.2 remote-as 201

RC(config-router)#neighbor 10.0.0.1 remote-as 101

RC(config-router)#network 192.168.100.0 mask 255.255.255.0

RC(config-router)#network 10.0.0.0 mask 255.0.0.0

RD(config)#router bgp 201

RD(config-router)#neighbor 192.168.100.1 remote-as 200

RD(config-router)#network 192.168.100.0 mask 255.255.255.0

Verifying BGP

RA# show ip protocols

RA#show ip bgp neighbors

RA#show ip bgp summary

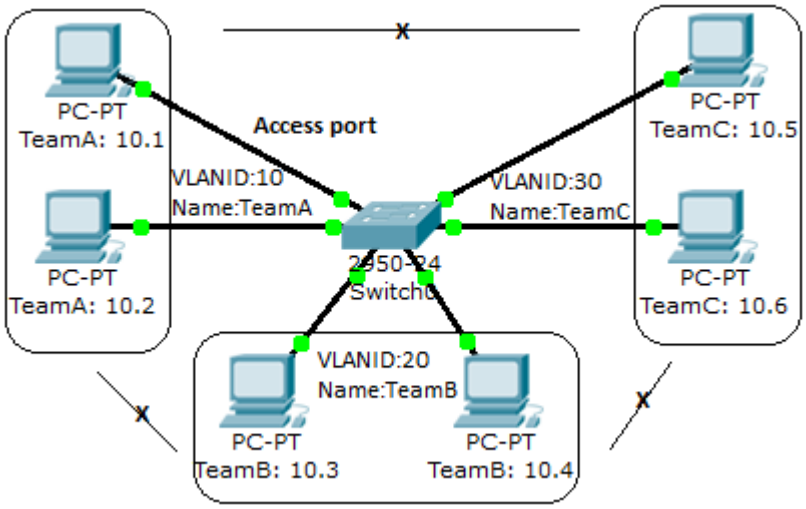
RA#show ip route

RA#show ip route bgp

Chapter 8: VLAN –Virtual LAN

A VLAN might comprise a subset of the ports on a single switch or subsets of ports on multiple switches. Systems on one VLAN don't see the traffic associated with systems on other VLANs on the same network.

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



10.1 means IP: 10.0.0.1, Similar this other IP address. 10.2 IP: 10.0.0.2

TeamA connect vlan id 10 networks only.

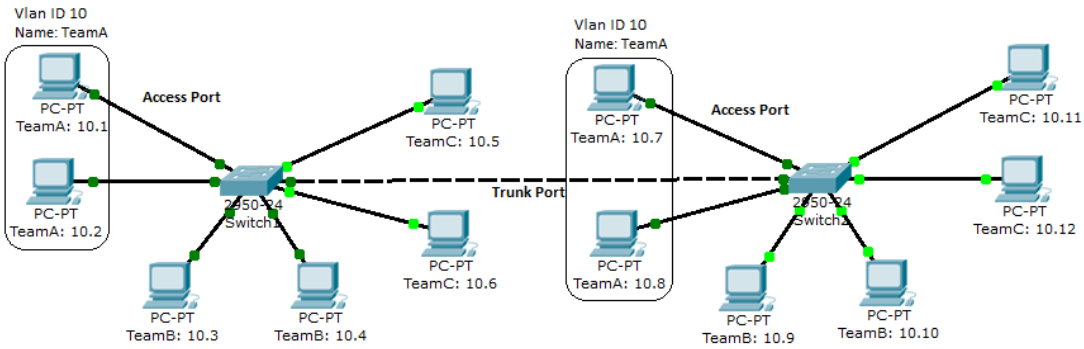
TeamB connect vlan id 20 networks only.

TeamA can’t connect to other VLAN ID like TeamB, TeamC,

Switch>
Switch>enable
Switch#configure terminal

```
Switch(config)#vlan 10
Switch(config-vlan)#name TeamA
Switch(config-vlan)#exit

Switch(config)#vlan 20
Switch(config-vlan)#name TeamB
Switch(config-vlan)#exit

Switch(config)#vlan 30
Switch(config-vlan)#name TeamC
Switch(config-vlan)#exit

Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit

Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit

Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit

Switch(config)#interface FastEthernet0/4
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit

Switch(config)#interface FastEthernet0/5
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit

Switch(config)#interface FastEthernet0/6
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
```


Switch# show vlan brief



Switch A

Switch>enable

Switch#configure terminal

Switch(config)#interface FastEthernet0/7

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan add 10

Switch(config-if)#switchport trunk allowed vlan add 20

Switch(config-if)#switchport trunk allowed vlan add 30

Switch B

Switch>enable

Switch#configure terminal

Switch(config)#interface FastEthernet0/7

Switch(config-if)#switchport mode trunk

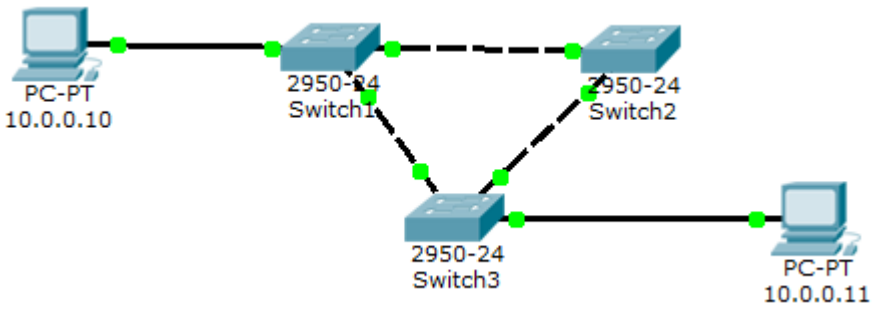
Switch(config-if)#switchport trunk allowed vlan add 10

Switch(config-if)#switchport trunk allowed vlan add 20

Switch(config-if)#switchport trunk allowed vlan add 30

STP (Spanning Tree Protocol)

The Spanning Tree Protocol (STP) is a network protocol that builds a logical loop-free topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails.



Switch1(config)#no spanning-tree vlan 1

Switch2(config)#no spanning-tree vlan 1

Switch3(config)#no spanning-tree vlan 1

Switch1(config)# spanning-tree vlan 1 root primary

Switch1(config)#vlan 10

Switch1(config-vlan)#name vlan10

Switch1(config-vlan)#exit

Switch1(config)# spanning-tree vlan 10 root primary

Switch1#show spanning-tree vlan 10

Switch2(config)#vlan 20

Switch2(config-vlan)#name vlan20

Switch2(config-vlan)#exit

Switch2(config)# spanning-tree vlan 20 root primary

Switch2#show spanning-tree vlan 20

Switch3(config)#vlan 30

Switch3(config-vlan)#name vlan30

Switch3(config-vlan)#exit

Switch3(config)# spanning-tree vlan 30 root primary

Switch3#show spanning-tree vlan 20

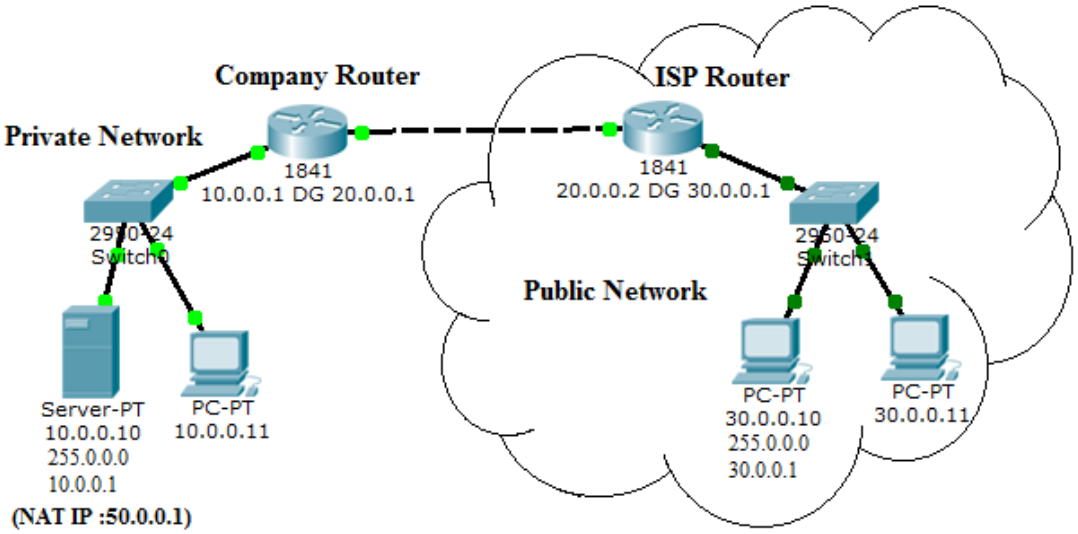
Chapter 9: NAT

NAT - Network Address Translation

Public IP to Private IP translation
Private IP to Public IP translation

Network address translation (NAT) is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.

NAT is a method that is used to translate Private IP addresses to Public IP addresses.



Company Router Configuration

Router(config)#

Router(config)#interface FastEthernet0/0

Router(config-if)#ip nat inside

Router(config-if)#exit

Router(config)#interface FastEthernet0/1

Router(config-if)#ip nat outside

Router(config-if)#exit

Router(config)#ip nat inside source static 10.0.0.10 50.0.0.1

Static Route

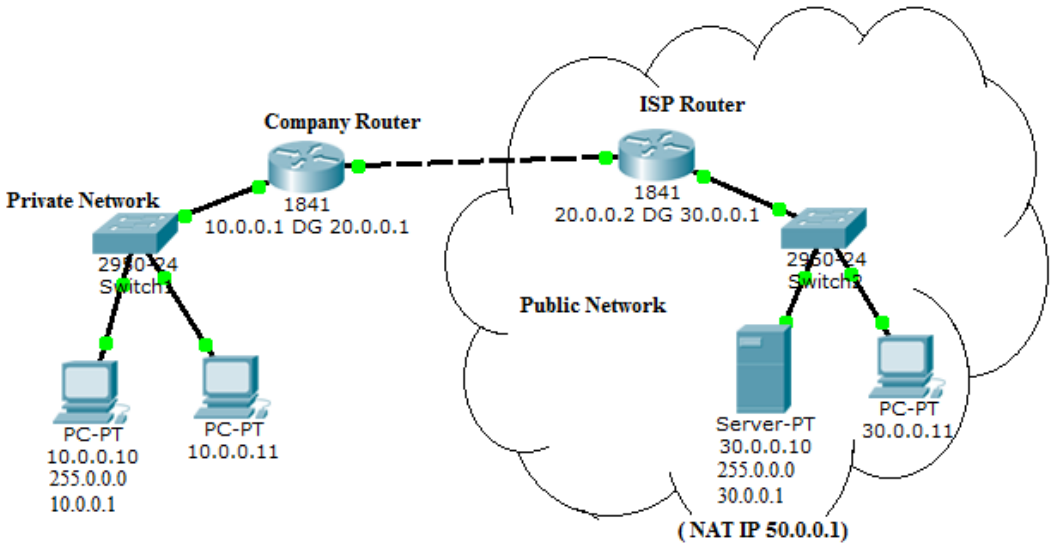
Company Router(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.2

ISP Router(config)#ip route 50.0.0.0 255.0.0.0 20.0.0.1

Verifying Command

Router#show ip nat translations

Inside global	Inside local	Outside local	Outside global
50.0.0.1	10.0.0.10	---	---



ISP Router

Router(config)#interface FastEthernet0/0

Router(config-if)#ip nat inside

Router(config-if)#exit

Router(config)#interface FastEthernet0/1

Router(config-if)#ip nat outside

Router(config-if)#exit

Router(config)#ip nat inside source static 30.0.0.10 50.0.0.1

Static Route

ISP Router(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1

Company Router(config)# ip route 50.0.0.0 255.0.0.0 20.0.0.2

DHCP

DHCP - Dynamic Host Configuration protocol

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

DHCP **server** is a Centralized IP Management. Automatically Assign IP Address, to the client request.

The DHCP **Client** enable DHCP an obtain IP from the server

DHCP is built on a client-server model.

DHCP server hosts allocate network addresses and deliver configuration parameters.

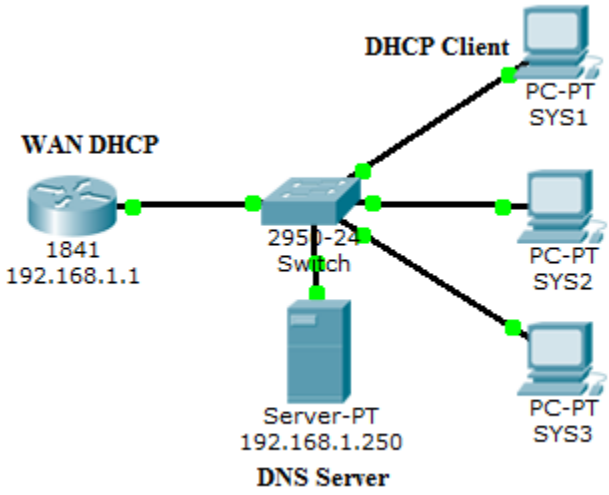
DORA Process

Discover -broadcast

Offer-unicast

Request- broadcast

Acknowledgement-unicast



Router(config)#ip dhcp pool AnyName

Router(dhcp-config)#network 192.168.1.0 255.255.255.0

Router(dhcp-config)#default-router 192.168.1.1

Router(dhcp-config)#dns-server 192.168.1.250

Router(config)#ip dhcp excluded-address 192.168.1.240 192.168.1.249

Router(config)#no ip domain-lookup

Verifying Command

Router# show ip dhcp binding

Router# show ip dhcp server statistics

Router# show ip dhcp events

VPN

VPN – Virtual Private Network

Private data is tunneled and send to the designation. To protect the private data over internet. Using public network for access the private data that via is called VPN. Virtual: Information within a private network is transported over a public network.

Private: The traffic is encrypted to keep the data confidential.

IPsec Security Services

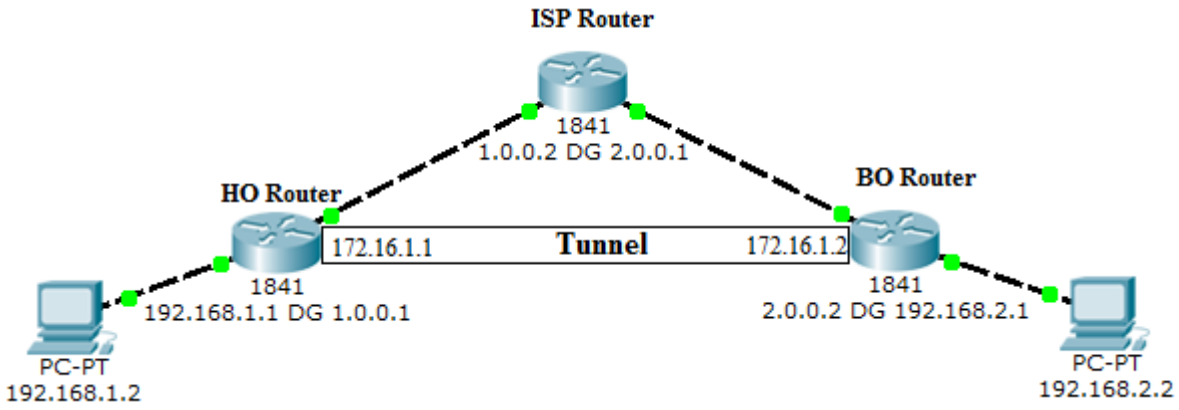
Encryption algorithms: AES, DES, RSA

Data Integrity: MD5 (message Digest 5 Algorithm 112bits)

SHA (Scope Hash Algorithm 118 bits)

Authentication: Digital Signature, certificate authority

Kerberos Authentication : Pre-shot key (PSK), RSA signature



HO Static Route:

Router(config)#ip route 0.0.0.0 0.0.0.0 1.0.0.2

BO Static Route:

Router(config)#ip route 0.0.0.0 0.0.0.0 2.0.0.1

Tunnel HO:

Router(config)#interface tunnel 10

Router(config-if)#ip address 172.16.1.1 255.255.255.0

Router(config-if)#tunnel source fastEthernet 0/1

Router(config-if)#tunnel destination 2.0.0.2

Tunnel BO:

Router(config)#interface tunnel 100

Router(config-if)#ip address 172.16.1.2 255.255.0.0

Router(config-if)# tunnel source fastEthernet 0/1

Router(config-if)#tunnel destination 1.0.0.1

HO Static Route:

Router(config)#ip route 192.168.2.0 255.255.255.0 172.16.1.2

BO Static Route:

Router(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.1

Router>show ip interface tunnel 10

```
PC>tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.1.1
  2    0 ms      0 ms      0 ms      172.16.1.2
  3    0 ms      0 ms      0 ms      192.168.2.2

Trace complete.
```

Chapter 10: Frame Relay

Frame Relay is a standardized wide area network technology that specifies the physical and data link layers of digital telecommunications channels using a packet switching methodology.

Frame Relay is an industry-standard, switched data link layer protocol that handles multiple virtual circuits using High-Level Data Link Control (HDLC) encapsulation between connected devices. In many cases, Frame Relay is more efficient than X.25. Connections made by virtual circuits. Connection-oriented service

Frame Relay PVC(permanent Virtual Circuit) are identified with DLCIs, and the status of the PVCs are reported via the LMI protocol.

A data link connection identifier (DLCI) is a Frame Relay 10 bit wide link-local virtual circuit identifier. Local Management Interface (LMI) is a term for some signaling standards used in networks

Cisco supports three LMI standards:

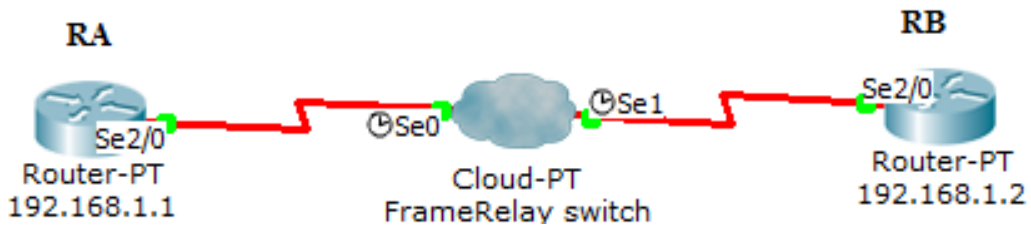
Cisco, ANSI T1.617 Annex D , ITU-T Q.933 Annex A

Point-to-point

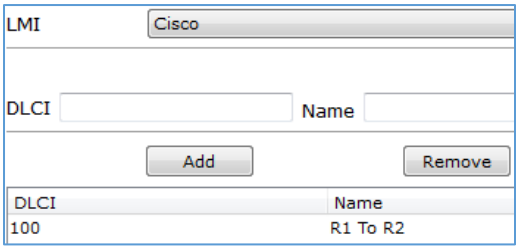
Subinterfaces act like leased lines.

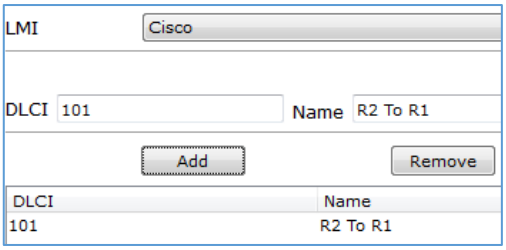
Each point-to-point subinterface requires its own subnet.

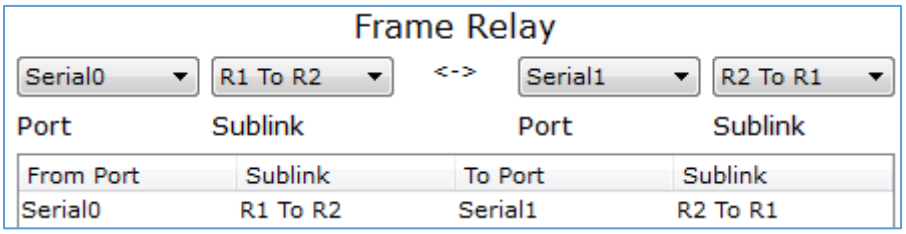
Point-to-point is applicable to hub-and-spoke topologies.



Frame Relay: Serial 0 Serial 1







RA Router

Router(config)#interface serial 2/0

Router(config-if)#encapsulation frame-relay

Router(config-if)#frame-relay interface-dlci 100

Router(config-if)#frame-relay lmi-type cisco

Router(config-if)#no shutdown

RB Router

Router(config)#interface serial 2/0

Router(config-if)#encapsulation frame-relay

Router(config-if)#frame-relay interface-dlci 101

Router(config-if)#no shutdown

Verify Frame Relay

Router#show frame-relay pvc

Router#show frame-relay lmi Router#show frame-relay map

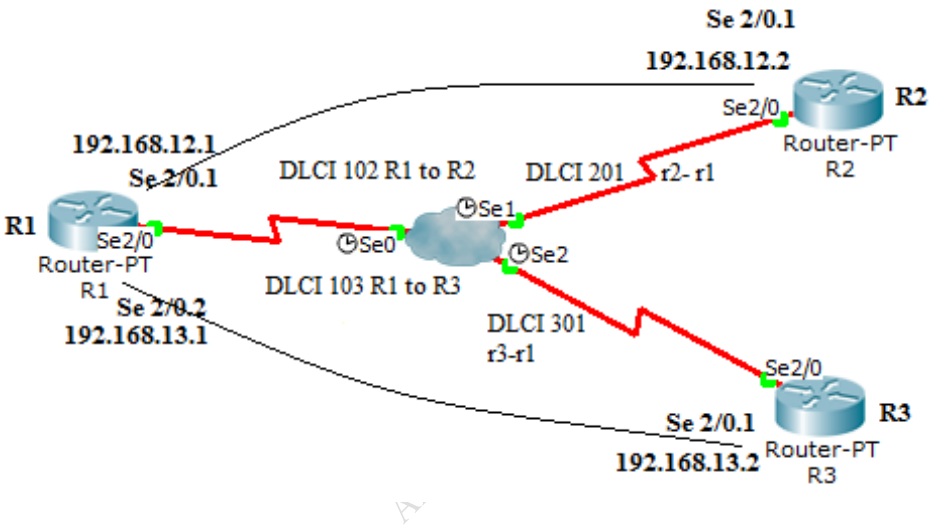
Frame-Relay Point to Point

Multipoint.

Subinterfaces act like NBMA networks, so they do not resolve the split-horizon issues.

Multipoint can save address space because it uses a single subnet.

Multipoint is applicable to partial-mesh and full-mesh topologies.



Serial 0

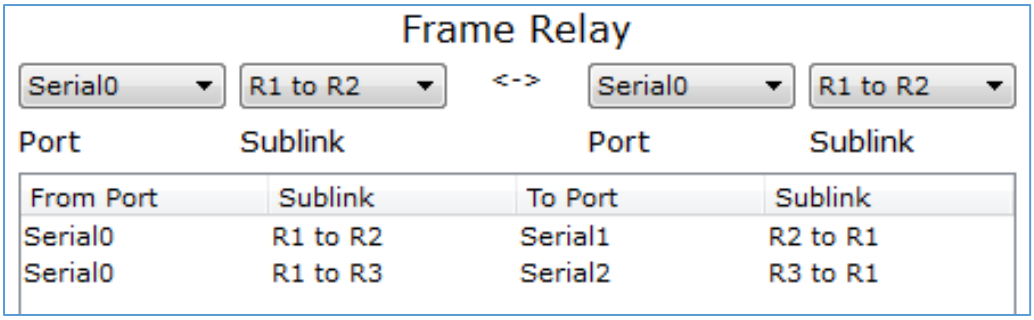
DLCI	Name
102	R1 to R2
103	R1 to R3

Serial 1

DLCI	Name
201	R2 to R1

Serial 2

DLCI	Name
301	R3 to R1



R1 Router

Router(config)#interface serial 2/0

Router(config-if)#encapsulation frame-relay

Router(config-if)#exit

Router(config)#interface serial 2/0.1 point-to-point

Router(config-subif)#ip address 192.168.12.1 255.255.255.0

Router(config-subif)#frame-relay interface-dlci 102

Router(config-subif)#exit

Router(config)#interface serial 2/0.2 point-to-point

Router(config-subif)#ip address 192.168.13.1 255.255.255.0

Router(config-subif)#frame-relay interface-dlci 103

Router(config)#interface Serial2/0

Router(config-if)#no shutdown

R2 Router

Router(config)#interface s2/0

Router(config-if)#encapsulation frame-relay

Router(config-if)#exit

Router(config)#

Router(config)#interface serial 2/0.1 point-to-point

Router(config-subif)#ip address 192.168.12.2 255.255.255.0

Router(config-subif)#frame-relay interface-dlci 201

Router(config-subif)#

Router(config)#interface Serial2/0

Router(config-if)#no shutdown

R3 Router

Router(config)#interface serial 2/0

Router(config-if)#encapsulation frame-relay

Router(config-if)#exit

Router(config)#interface serial 2/0.1 point-to-point

Router(config-if)#ip address 192.168.13.2 255.255.255.0

Router(config-if)#frame-relay interface-dlci 301

ACL - Access Control List

Access control lists (ACLs) provide means to filter packets by allowing a user to permit or deny IP packets from crossing specified interface.

Access lists filter network traffic by controlling whether packets are forwarded or blocked at the router's interfaces based on the criteria you specified within the access list. There are 3 popular types of ACL: Standard, Extended and Named ACLs.

Access List Type	**Range**
Standard	1-99, 1300-1999
Extended	100-199, 2000-2699
Named	

Standard IP lists

Configuration Syntax
Access-list access-list-number {permit | deny} source {source-mask}

Router(config)#access-list 1 permit 10.0.0.0 0.255.255.255
Router(config)#access-list 1 permit any

Apply ACL to an interface

ip access-group access-lit-number {in |out}

Router(config)#interface Fa0/1

Router(config-if)#ip access-group 1 in

Extended IP Access List

Extended IP lists (100-199) check both source and destination addresses, specific UDP/TCP/IP protocols, and destination ports.

Configuration Syntax
Access-list access-list-number {permit |deny} protocol source {source-mask} destination{destination-mask} [eq destination-port]

Router(config)#access-list 101 deny tcp 10.0.0.0 0.255.255.255 187.100.1.6 0.0.0.0 eq 21

Router(config)#access-list 101 deny tcp 10.0.0.0 0.255.255.255 187.100.1.6 0.0.0.0 eq 20

Router(config)#access-list 101 permit ip any any

Router(config)#interface Fa0/1

Router(config-if)#ip access-group 101 in

Named IP Access List

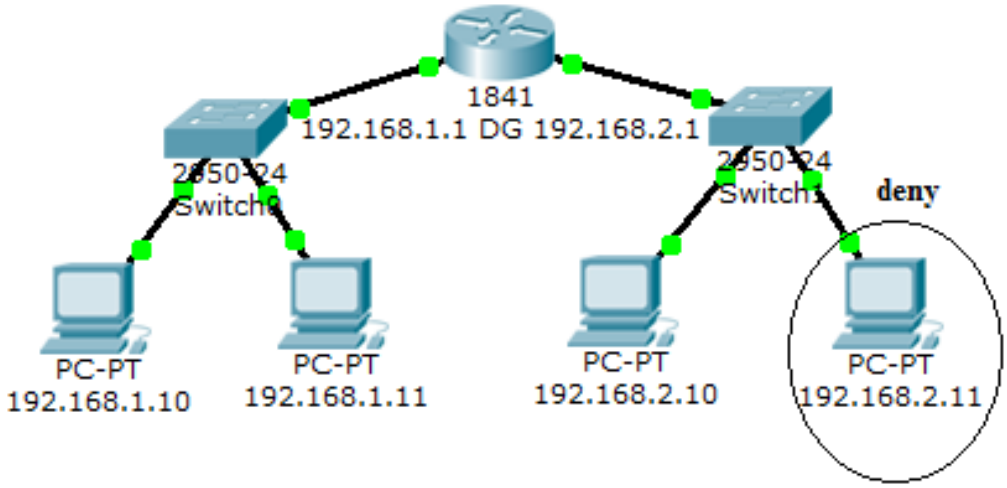
This allows standard and extended ACLs to be given names instead of numbers

Named IP Access List Configuration Syntax
ip access-list {standard | extended} {name | number}

Router(config)#ip access-list extended in_to_out permit tcp host 10.0.0.1 host 187.100.1.6 eq telnet

Router(config)#interface Fa0/1

Router(config-if)#ip access-group in_to_out in



Router(config)#access-list 1 deny host 192.168.2.11

Router(config)#access-list 1 permit any

Router(config)#access-list 1 deny ?

A.B.C.D	Address to match
any	Any source host
host	A single host address

Router(config)#interface fastEthernet 0/1

Router(config-if)#ip access-group 1 in

Router#show access-lists 1

Standard IP access list 1

deny host 192.168.2.11 (6 match(es))

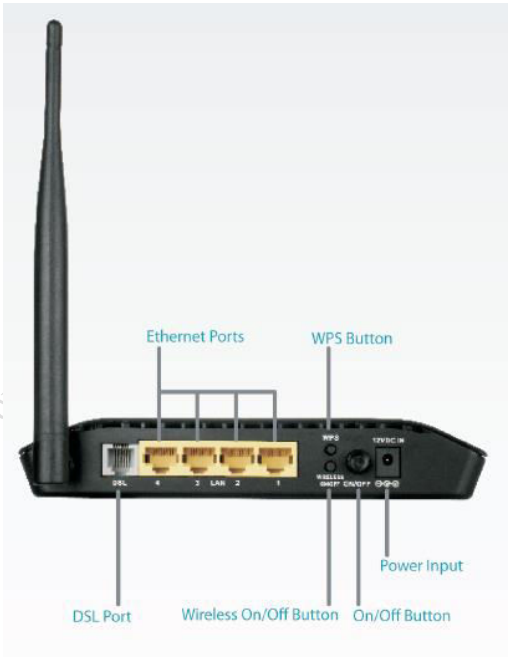
permit any (22 match(es))

Router#show access-lists

Router(config)#no access-list 1

Modem Configuration

Modem (modulator-demodulator) is a network hardware device that modulates one or more carrier wave signals to encode digital information for transmission and demodulates signals to decode the transmitted information.

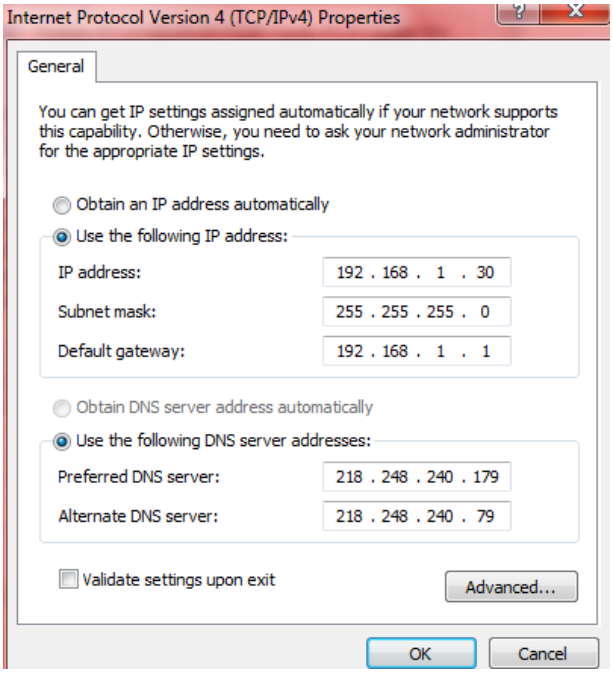


LAN Configuration in LAN Computer:

Put the IP address in Local Area Connection as IP Add: 192.168.1.30 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.1

Configuring lan setting go to run, type ncpa.cpl

Modem/Router : DSL or ADSL



In the Internet Explorer, type 192.168.1.1 and press enter.

User Name: admin and Password: *****

1. Device Info / Basic Info
2. Advanced setup

    Connection Type => Encapsulation Mode LLC/SNAP-BRIDGING

    Protocol => PPP over Enthernet

Ethernet (PPPoE) =>username/password/service name/authentication

    Enable NAT and WAN Service, Summary.

3. Wireless Basic

    Enable Wireless, SSID=Andrew

4. Wireless Security

    Select SSID, Network Authentication: WPA2-PSK

    WPA pre-Shared Key: ****** WPA Encryption: TKIP /AES

5. LAN interface - IP: 192.168.1.1 DHCP: Enabled
6. Click Save/ Apply
7. Click Save/ Reboot

Windows Operating System Versions

Client OS:

XP, Vista, Win 7, Win 8, win10

Server OS:

Win 2003 server, Win 2008 server, Win2012 Server, win2016 Server

Linux Operating System Versions

Client OS:

Red hat 6.2, Red hat 7.2, Red hat 9, Debian, Ubuntu, Centos, Fedora

Server OS:

RHEL 2.1, RHEL 3.4, RHEL 5, RHEL 6, RHEL 7

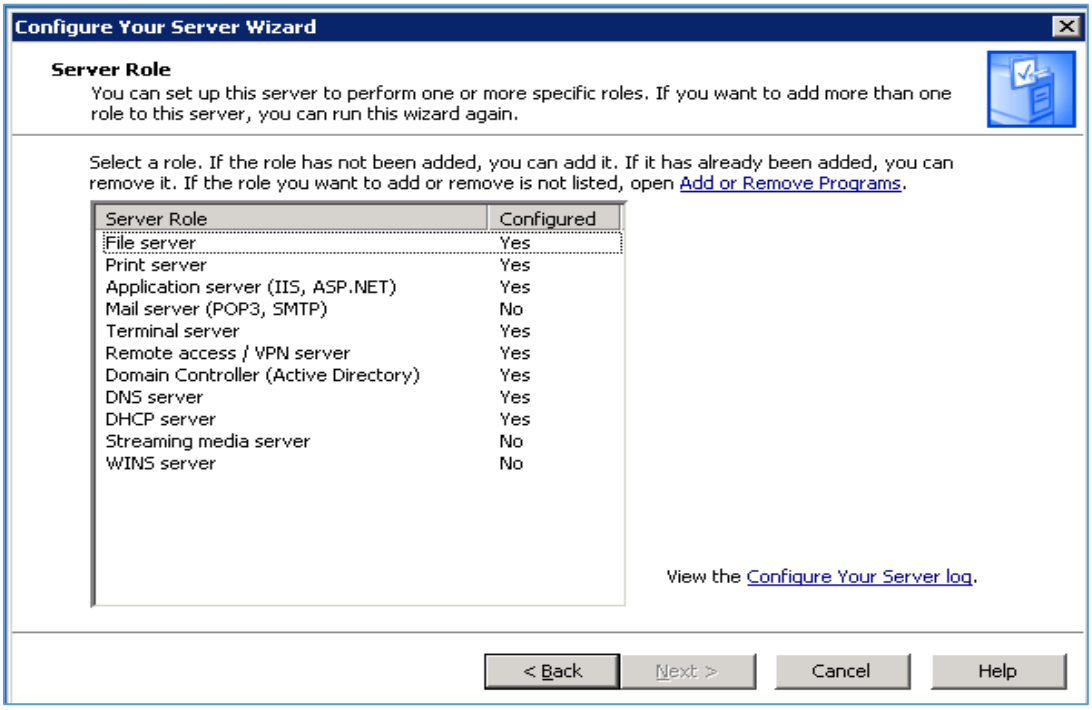
Dos Commands

Cd\ (Root directory)
Date (system date)
Time (system time)
Ver (os Version)
Cls (clear screen)
Dir (view directory)
Dir/p/w (view pagewise)
Dir/ah – (view hidden files)

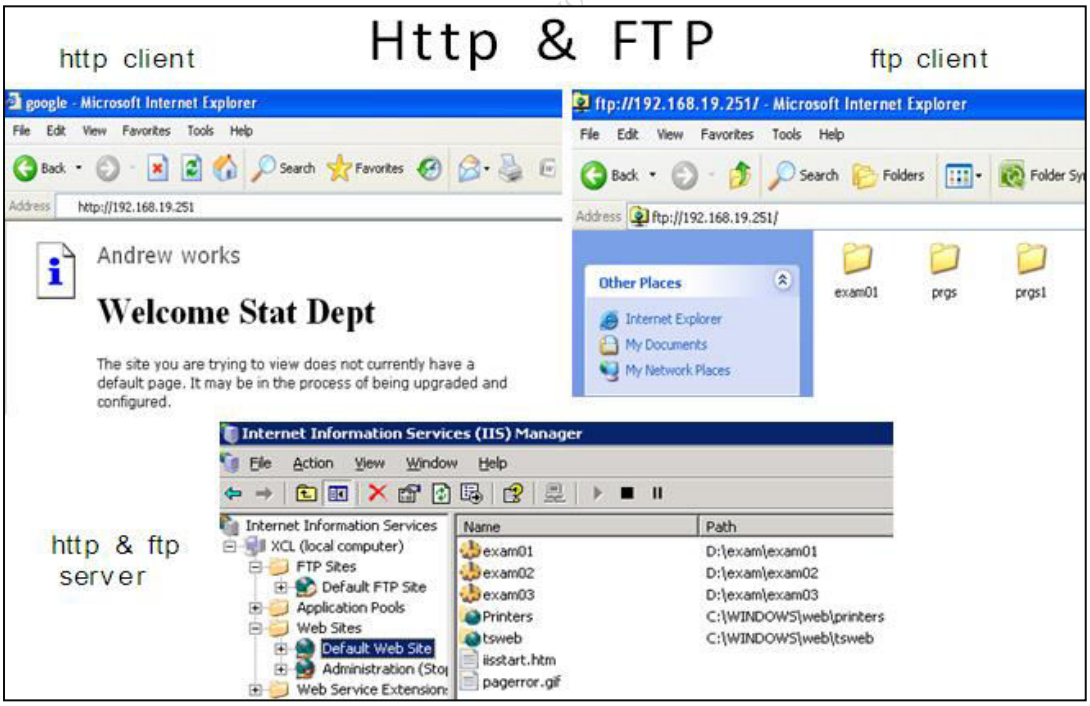
Md test1 (make Directory)
Rd test1 (Remove Directory)
Cd test1 (Change Directory)
Copy con f1.txt (create the file)
Ctrl+z (save file)
Type f1.txt (view the file)
Edit f1.txt (edit the file)
Copy f1.txt d:\ (copy the file)
Del f1.txt (delete the file)
Dir /ah (View hidden Files)
Dir –s –h dir or file (un hidden))

Dxdiag* this command using identify your system configuration

Chapter 11: Server Administration – LAN Infrastructure



Http (web server), FTP, DHCP, DNS Server, Print Server, Domain

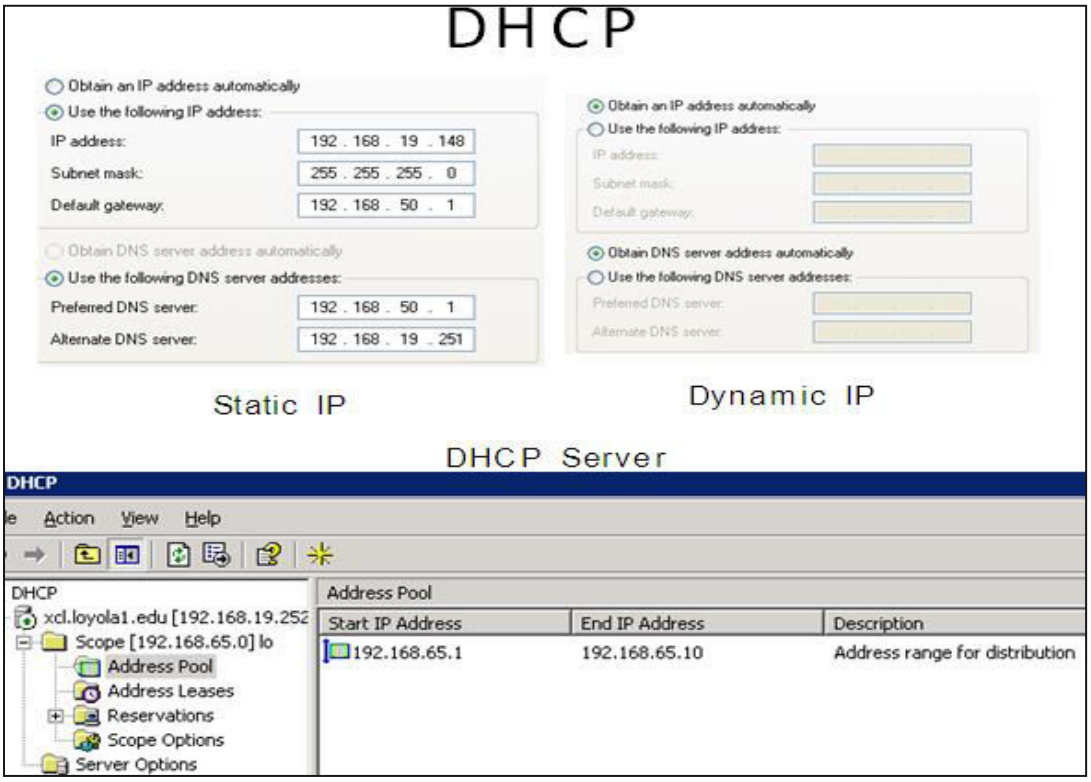


DHCP

Dynamic Host Configuration protocol

DHCP **server** Centralized IP Management

Automatically Assign IP Address, to the client request



DNS Domain Name System

Name Resolution: Host name to IP, IP to Host name and Hierarchical Name space like naming system for computers, services, or other resources

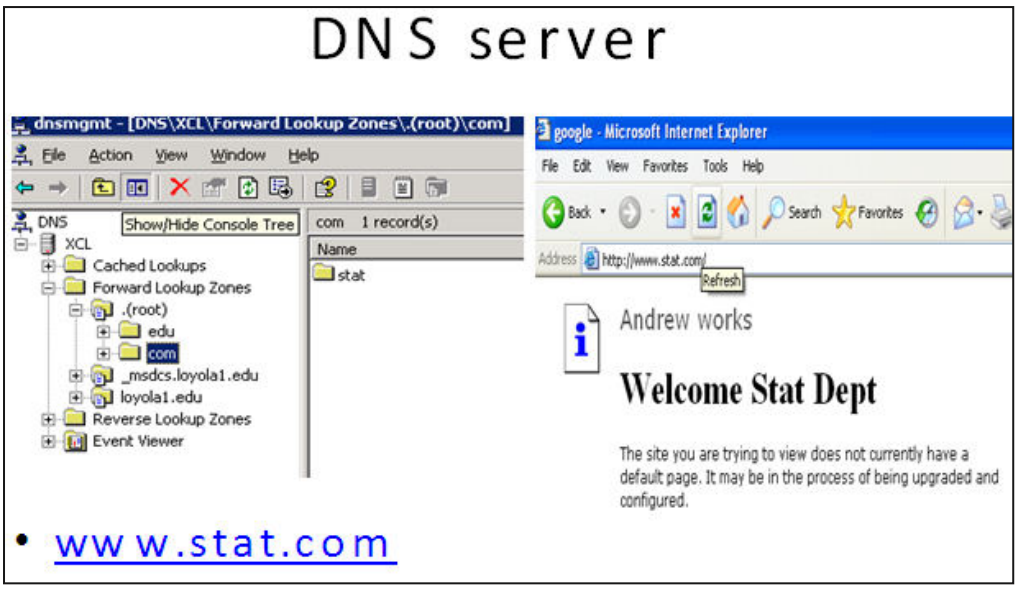
EX: www.google.com

DNS **Root** server→ .com .edu .org .gov

DNS com **Web** server →google.com, yahoo.com

DNS Web Server → www.google.com

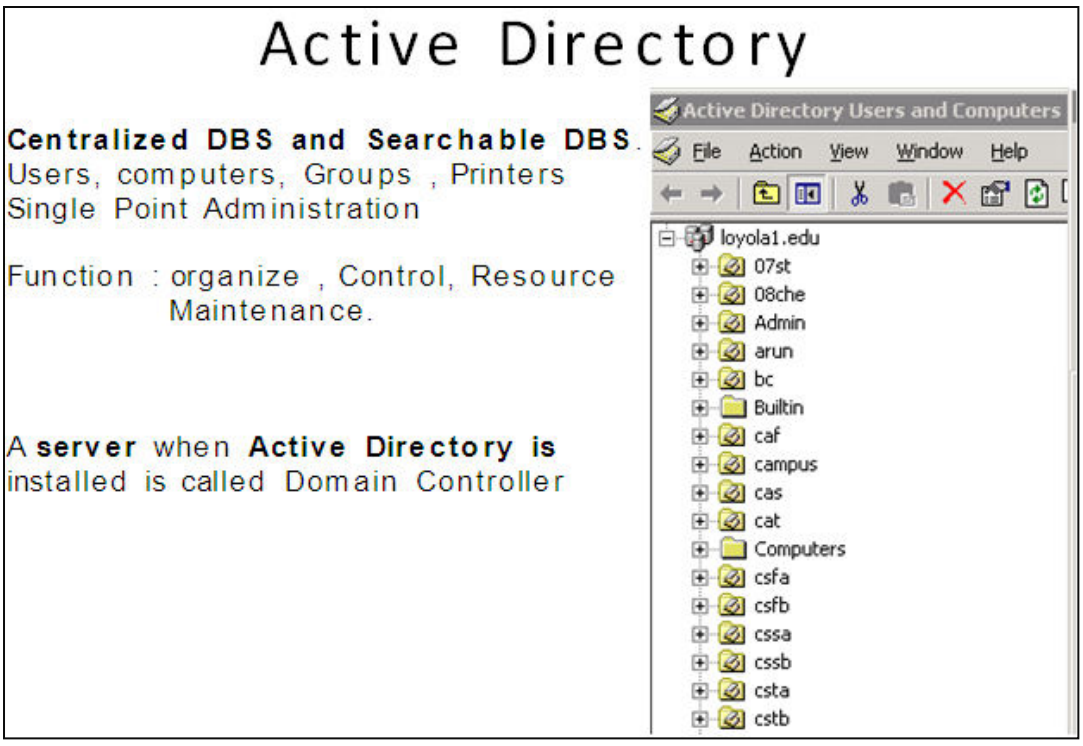
The Domain Name System (DNS) is a technology standard for managing names of public Web sites and other Internet domains



Domain Controller Server

A domain controller (DC) is a server that responds to security authentication requests within a Windows Server domain. Server computer that responds to security authentication requests within a Windows domain.

Domain: Client / Server. Centralized Administration and server that respond to secure authentication.



Chapter 12: Trouble Shooting

Network troubleshooting means recognizing, diagnosing and isolating the problems in a computer network. It's the primary responsibility of the network administrators to maintain the computer network, fault management, network security, monitoring, resources allocation and maintaining the performance.

Ping
pathping
Tracert / Traceroute
Ipconfig, ipconfig/all ,ifconfig
Nslookup
Netstat -ao
Check Physical connection
Check LAN cable and IP address.
Check WAN and LAN connections
Verify TCP/IP settings
Network Services (services.msc) start / stop
Ipconfig /flushdns
Check the IP, Default Gateway, DNS IP

Router# Show interfaces
Router# Show ip interface
Router# Show ip route
Router# Show running-config
Router# Show startup-config

IPv6

Internet Protocol version 6 (IPv6) is the latest revision of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion

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

IPv4 2^5=32 bit 2^{32} = 4294967296 (4.2 billion IP)

32 bits divided into four 8-bits blocks

11111111 . 11111111 . 11111111 . 11111111

IPv6 2^7=128 bit 2^{128} =3.40282366920938463463374607431768e+38

128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbols

0010000000000001 0000000000000000 0011001000111000 1101111111100001

0000000001100011 0000000000000000 0000000000000000 1111111011111011

Each block is then converted into Hexadecimal

2001:0000:3238:DFE1:0063:0000:0000:FEFB

Even after converting into Hexadecimal format, IPv6 address remains long. IPv6 provides some rules to shorten the address. The rules are as follows:

Rule.1: Discard leading Zero:

In Block 5, 0063, the leading two 0s can be omitted, such as (5th block):

2001:0000:3238:DFE1:63:0000:0000:FEFB

Rule.2: If two or more blocks contain consecutive zeroes, omit all of and replace with double colon sign**::** such as (6th and 7th block):

2001:0000:3238:DFE1:63::FEFB

Consecutive blocks of zeroes can be replaced only once by :: so if there are still blocks of zeroes in the address, they can be shrunk down to a single zero, such as (2nd block):

2001:0:3238:DFE1:63:FEFB

Another Example:

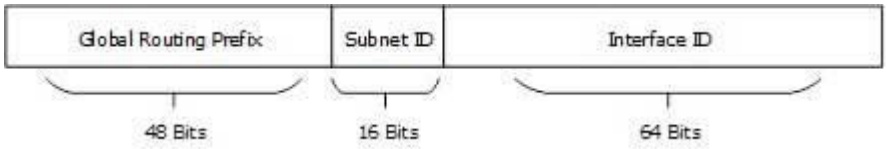
0010000000000001 0000000000000000 0000000000001010 0000000000000000

0000000000000000 0000000000000000 0000000000000000 0000000000000001

2001:0:A::1

Global Unicast Address

This address type is equivalent to IPv4 public address. Global Unicast addresses in IPv6 are globally identifiable and uniquely addressable.



Global Routing Prefix: The most significant 48-bits are designated as Global Routing Prefix which is assigned to specific autonomous system. The three most significant bits of Global Routing Prefix is always set to 001.

Link-Local Address

Auto-configured IPv6 address is known as Link-Local address.

FE80 1111 1110 **1000** 0000

FE90 1111 1110 **1001** 0000

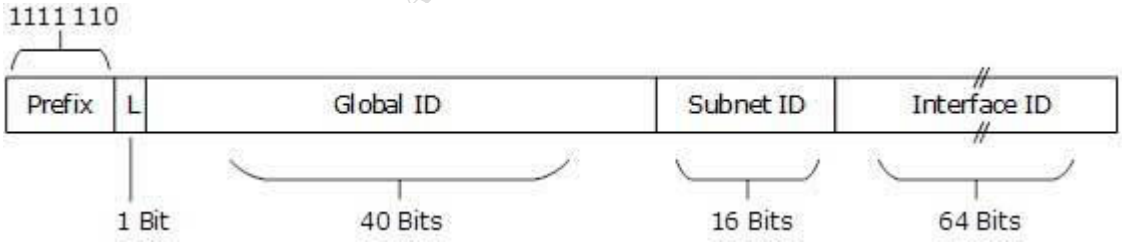
FEA0 1111 1110 **1010** 0000

FEB0 1111 1110 **1011** 0000

Link-local addresses are used for communication among IPv6 hosts on a link (broadcast segment) only. These addresses are not routable, so a Router never forwards these addresses outside the link.

Unique-Local Address

This type of IPv6 address is globally unique, but it should be used in local communication. The second half of this address contain Interface ID and the first half is divided among Prefix, Local Bit, Global ID and Subnet ID.



FEC0	1111	1110	**1100**	0000
FED0	1111	1110	**1101**	0000
FEE0	1111	1110	**1110**	0000
FEF0	1111	1110	**1111**	0000

Scope of IPv6 Unicast Addresses:

The scope of Link-local address is limited to the segment. Unique Local Address are locally global, but are not routed over the Internet, limiting their scope to an organization's boundary. Global Unicast addresses are globally unique and recognizable. They shall make the essence of Internet v2 addressing.

Reserved Multicast Address for Routing Protocols

IPv6 Address	**Routing Protocol**
FF02::5	OSPFv3
FF02::6	OSPFv3 Designated Routers
FF02::9	RIP
FF02::A	EIGRP

The above table shows the reserved multicast addresses used by interior routing protocol.

Reserved Multicast Address for Routers/Node

IPv6 Address	**Scope**
FF01::1	All Nodes in interface-local
FF01::2	All Routers in interface local
FF02::1	All nodes in link-local
FF02::2	All Routers in link-local
FF05::2	All Routers in site-local

Unicast:

Address is for a single interface. IPv6 has several types (for example, global, reserved, link-local, and site-local)

Multicast:

One-to-many. Enables more efficient use of the network uses a larger address range

Anycast:

One-to-nearest (allocated from unicast address space).Multiple devices share the same address. All anycast nodes should provide uniform service. Source devices send packets to anycast address Routers decide on closest device to reach that destination.Suitable for load balancing and content delivery services

Types of IPv6 unicast addresses:

Global: Starts with 2000::/3 and assigned by IANA

Reserved: Used by the IETF

Private: Link local (starts with FE80::/10)

Loopback (::1)

Unspecified (::)

A single interface may be assigned multiple IPv6 addresses of any type: unicast, anycast, or multicast. IPv6 addressing rules are covered by multiple RFCs.Architecture defined by RFC 4291

Glossary

CIDR—Classless Inter-Domain Routing

DHCP—Dynamic Host Configuration Protocol

DSL/ADSL Digital Subscriber Line/ Asymmetric Digital Subscriber Line

FQDN—Fully Qualified Domain Name

IOS—Internet Operating System

IPsec—IP security

ISDN—Integrated Services Digital Network

KDC—Key Distribution Center. Kerberos Authentication

LDAP—Lightweight Directory Access Protocol. Active Directory

NAS—Network Access Server

NAT—Network Address Translation

NIC—Network Interface Card

NTP—Network Time Protocol

NVRAM—Non-Volatile Random Access Memory

PCI—Peripheral Component Interconnect

PKI—Public Key Infrastructure

PPP—Point-to-Point Protocol

PPTP—Point-to-Point Tunneling Protocol

PSK – Pre Shared Key

QoS—Quality of Service

RAS/RRAS—Remote Access Service, Routing & Remote Access Service

RDP—Remote Desktop Protocol

SSH—Secure Shell

SSID – Service set Identifier

SSL/TLS—Secure Sockets Layer/Transport Layer Security

Static IP- Permanent IP

SYN/ACK—Synchronization/Acknowledgement

TTL—Time To Live

VLAN—Virtual LAN

VoIP—Voice over IP

WAP—Wireless Access Point

WEP—Wired Equivalent Privacy (or Wireless Encryption Protocol)

WPA – Wifi Protected Access