Cisco Certified Network Associate
CCNA

Lab Manual
Revision 2

Developed by

Muhammad Irfan Ghauri
Muhammad Rizwan

Etronics Solution Provider
F1, 8th floor, Flat # 132
Sunny Pride, Gulistan-e-Jauhar, Karachi.
Ph # 021-6034003

Table of Contents

Section-I Network Fundamentals

1- Ethernet Cables
- Cross Cable……..…… ……4
- Straight Cable…….....5
- Roll-Over Cable……..…….……6

2- How To Make A LAN
- Connecting Two PC's via Cross Cable..…….....….7
- Connecting Two PC's via Straight Cable……...……8

3- How To Make A Web & Ftp Server
- Web Server…….…….....14
- Ftp Server……..…….21

4- Open a Hyper Terminal Session…….……..……...28

Section-II Routing

5- Router Basic IOS
- Router Basic Commands…..…….…….....33
- Assign the IP address on the Ethernet Interface of Router…….....42
- Assign the IP address on the Serial interface of Router…….....45

6- Accessing Router Through A Telnet……...49

7- Static Routes…….…….....53

8- Dynamic Routes
- RIP Configuration……..……..…….....57
- IGRP Configuration……..……..….…….....61
- EIGRP Configuration……..……..….....66
- OSPF Configuration In A Single Area……..…….....71

Section-III IP Traffic Management

9- Access Control List
- Standard ACL……..…… ……..……77
- Extended ACL……..……82

10- Network Address Translation
Static NAT……..……...87
Dynamic NAT……..……..92
Overload NAT...…….…….……..97

Section-IV Switching

11- Switch Basic IOS……..…….……103
12- Spanning Tree Protocol…….……..……..….....117
13- VLAN & VLAN Trunking Protocol..…….……..……..….....125

Section-V WAN

14- Frame Relay…….……...137
15- ISDN……..……140

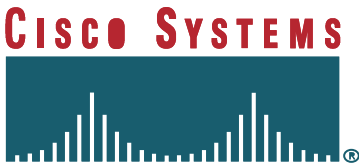
Section-VI Appendix

16- Password Recovery……148
17- Port Security. ……..……...….....151
18- TFTP Server
Uploading Configuration Through A TFTP Server……..….....154
Downloading Configuration Through A TFTP Server……...….....157

Section 1

Network Fundamentals

Etronics Solution Provider



By **M. Irfan Ghauri**
M. Rizwan

Lab # 1

Ethernet CABLES

Objective

This lab demonstrates how to make an Ethernet Cables.

The types of Ethernet cables are:

1) **Straight-through cable**
2) **Crossover cable**
3) **Rolled cable**

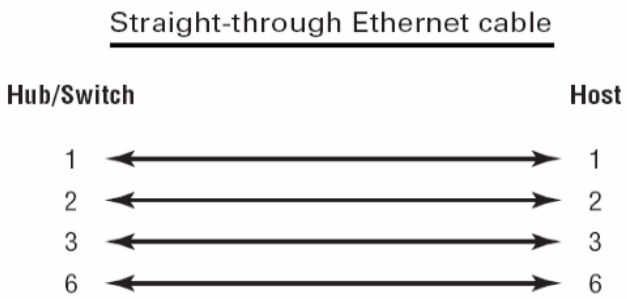
i. Straight-Through Cable

The straight-through cable is used to connect

1) **Host to switch or hub**
2) **Router to switch or hub**

Four wires are used in straight-through cable to connect Ethernet devices. It is relatively simple to create ; Figure shows the four wires used in a straight-through Ethernet cable.

Diagram



Notice that only pins 1, 2, 3, and 6 are used. Just connect 1 to 1, 2 to 2, 3 to 3, and 6 to 6. However, remember that this would be an Ethernet-only cable and wouldn't work with Voice, Token Ring, ISDN, etc.

ii. Crossover Cable Cable

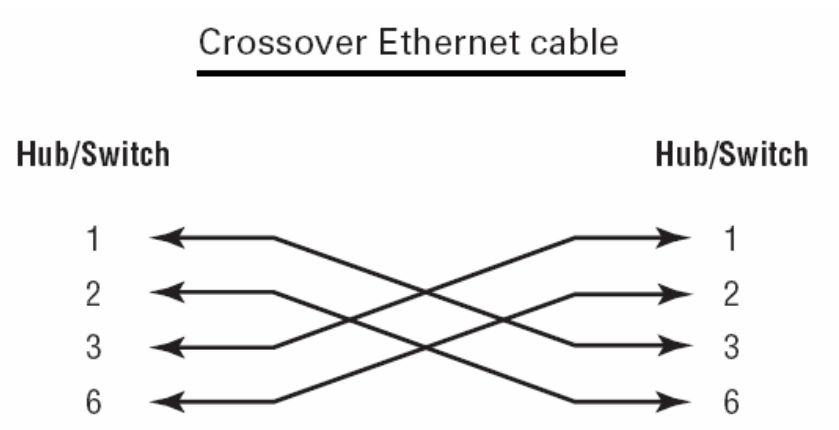
The crossover cable can be used to connect

1) **Switch to switch**
2) **Hub to hub**
3) **Host to host**
4) **Hub to switch**
5) **Router direct to host**

The same four wires are used in this cable as in the straight-through cable; we just connect different pins together. Figure shows how the four wires are used in a crossover Ethernet cable.

Notice that instead of connecting 1 to 1, etc., here we connect pins 1 to 3 and 2 to 6 on each side of the cable.

Diagram

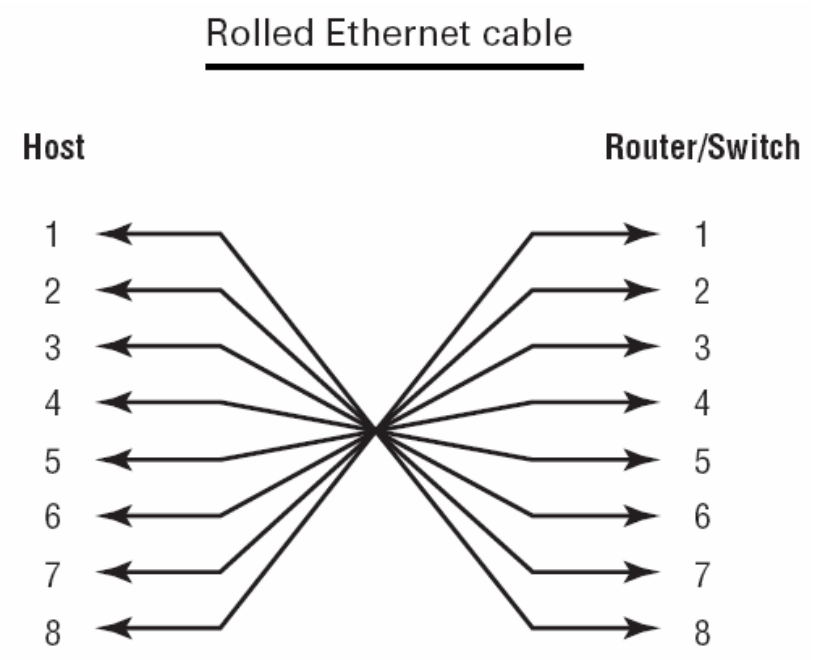


iii. Rolled Cable

Although rolled cable isn't used to connect any Ethernet connections together, you can use a rolled Ethernet cable to connect a host to a router console serial communication (com) port.

Eight wires are used in this cable to connect serial devices, although not all eight are used to send information, just as in Ethernet networks. Figure shows the eight wires used in a rolled cable.

Diagram



To make, just cut the one side like a straight-through cable and reverse the other end.

Once you connect the cable from your PC to the Cisco router or switch, you can start HyperTerminal to create a console connection and configure the device

Lab # 2

How to Create A LAN

Objective

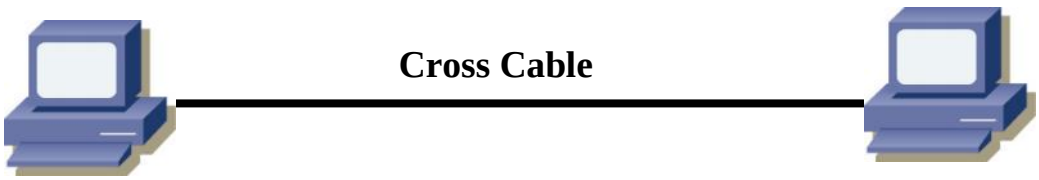
This lab demonstrates how to make a LAN Network.

The demonstration includes :

1. To connect 2 PC's with a cross cable.
2. To connect 2 PC's with a switch using a straight cable.

i. Connecting 2 PC's via Cross Cable

Diagram

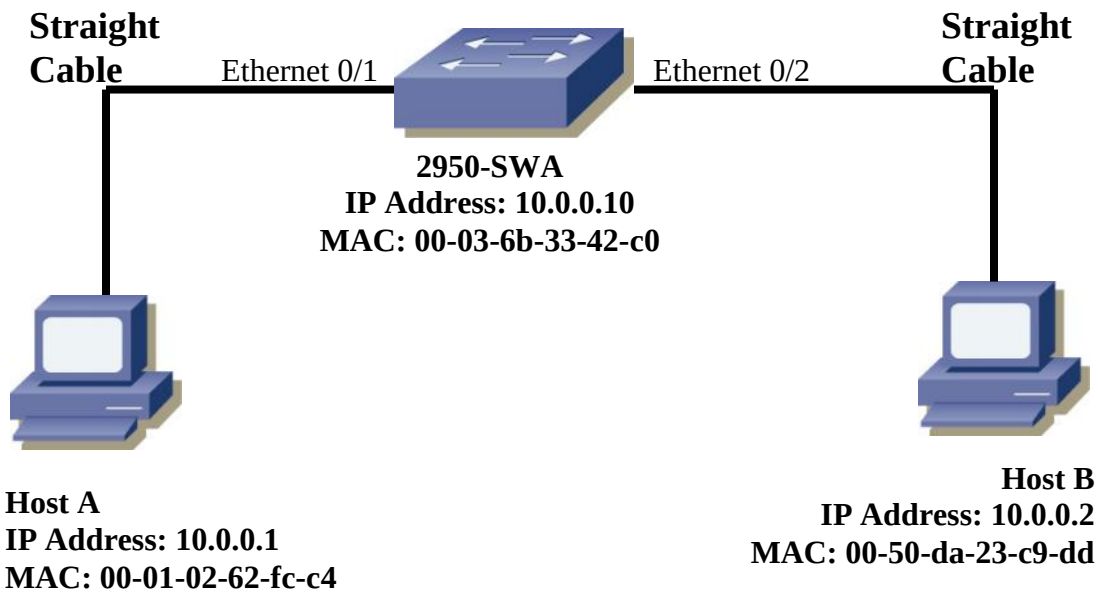


Host A
IP Address: 10.0.0.1
MAC: 00-01-02-62-fc-c4

Host B
IP Address: 10.0.0.2
MAC: 00-50-da-23-c9-dd

ii. Connecting 2 PC's via Straight Cable

Diagram



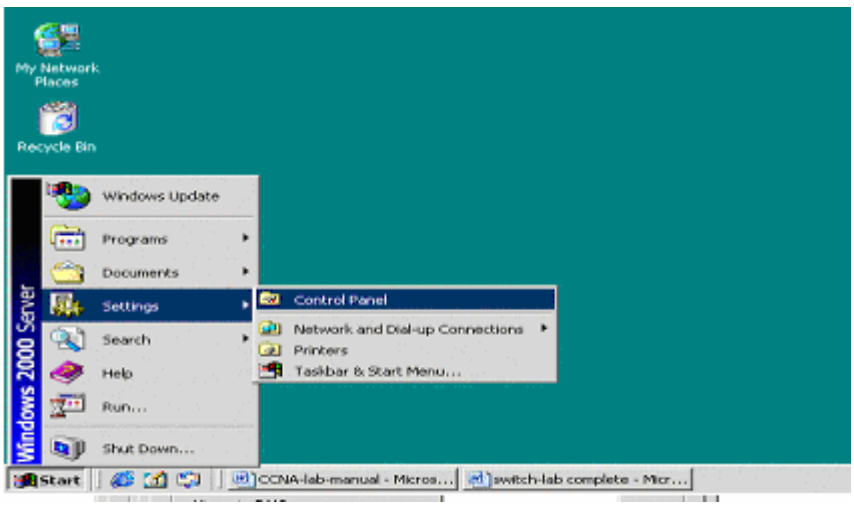
Procedure

1. Make sure that both NICs are installed onto your PC's.
2. Assign IP address to your LAN (NIC) card on both PC's.
3. Check their connectivity by **PING command & DATA sharing.**

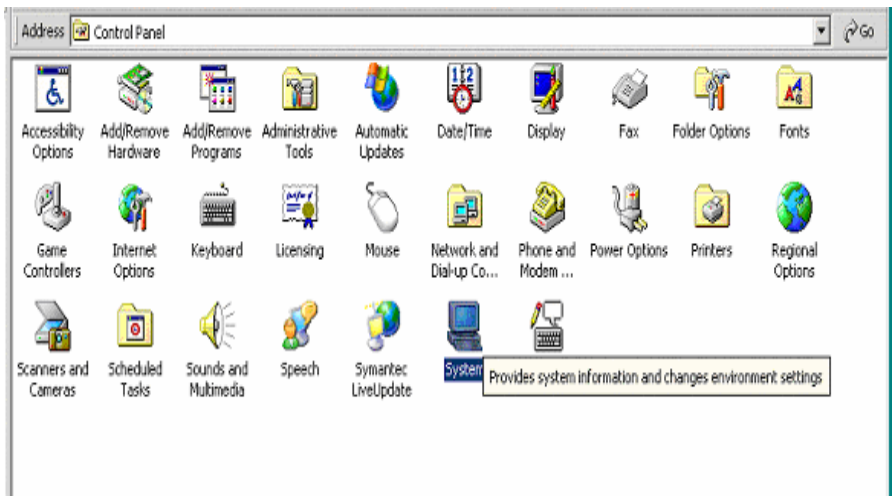
Configuration

Step 1: Make sure that both NICs are installed onto your PC's.

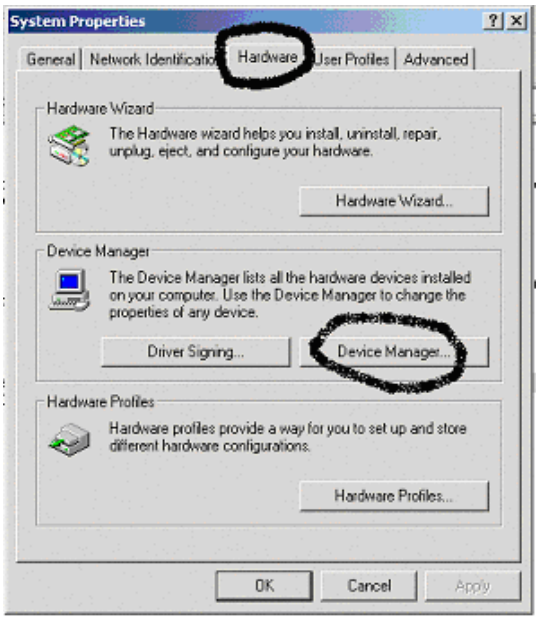
Go to **Windows Start Button** > **Settings** > **Control Panel**



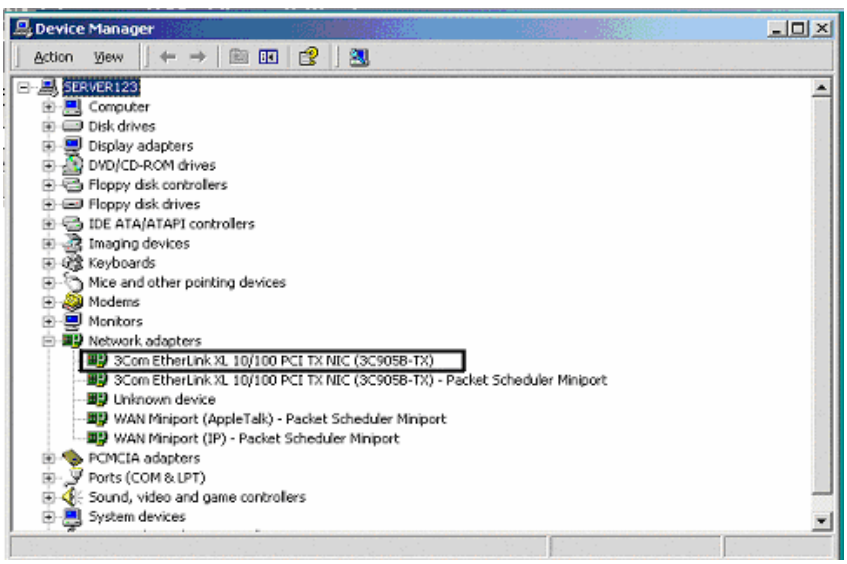
Then go to **System**



Then go to **Hardware** tab > **Device Manager**



Expand the **SERVER123 (Computer Name) tab > Network Adapters**

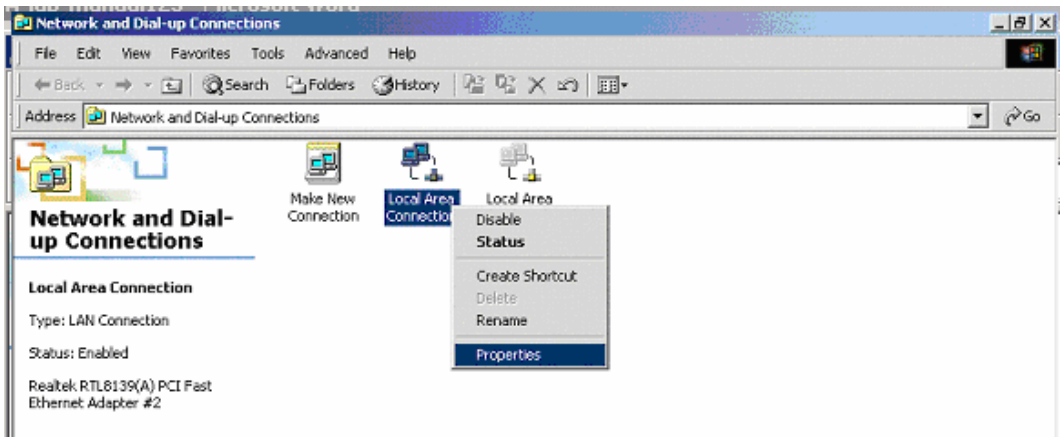


Note: - If LAN (NIC) card is not installed onto your PC then go to **Windows Start Button** > **Settings** > **Control Panel** > **Add/Remove Hardware.**

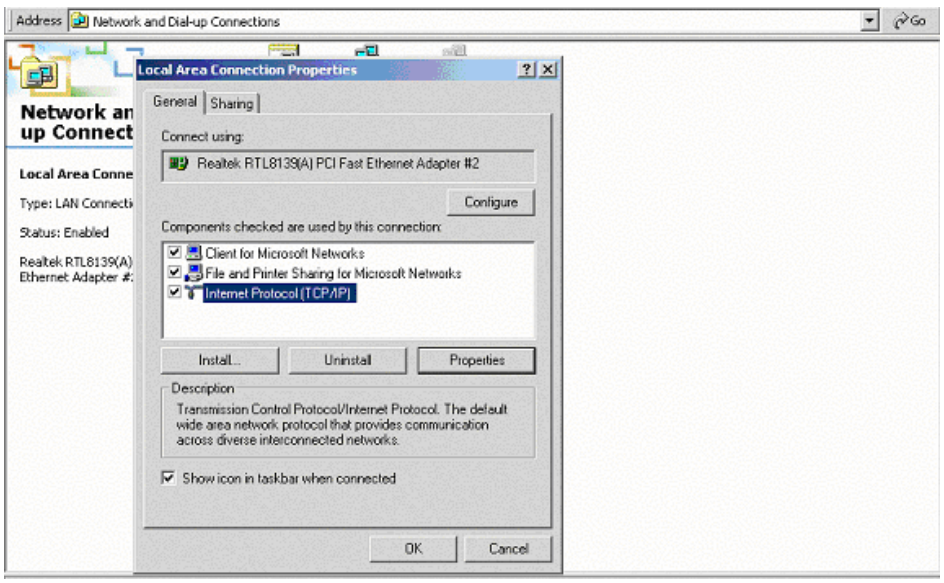
Step 2: Assign IP address to your LAN (NIC) card on both PC's.

Go to **My Network Places,** Right Click & take the **Properties** & open the **Network & Dial-up Connections**

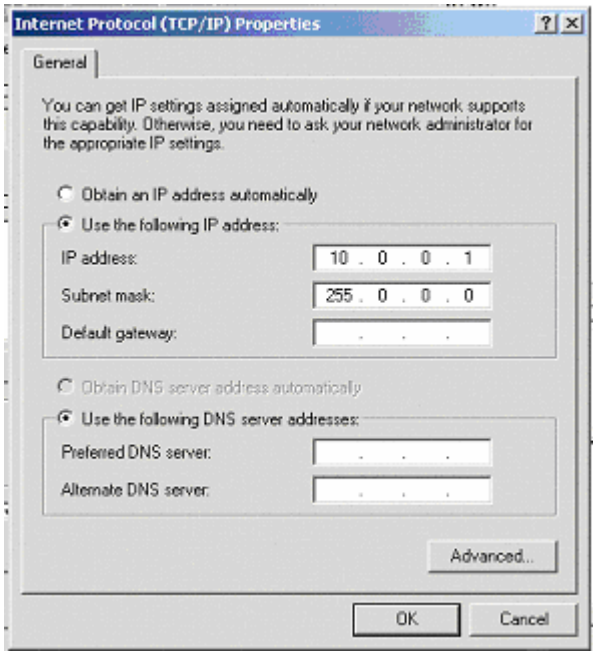
Choose your **LAN card**, & take the **Properties,**



Go to the **TCP/IP,** & take the **Properties**



Give the **IP Address,** & press **O.K.**



Check the **IP Address** on the **Command Prompt.**

D:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
IP Address . . . . . : 10.0.0.1
Subnet Mask . . . . . : 255.0.0.0
Default Gateway . . . . . :

Step 3(A): Check their connectivity by PING command.

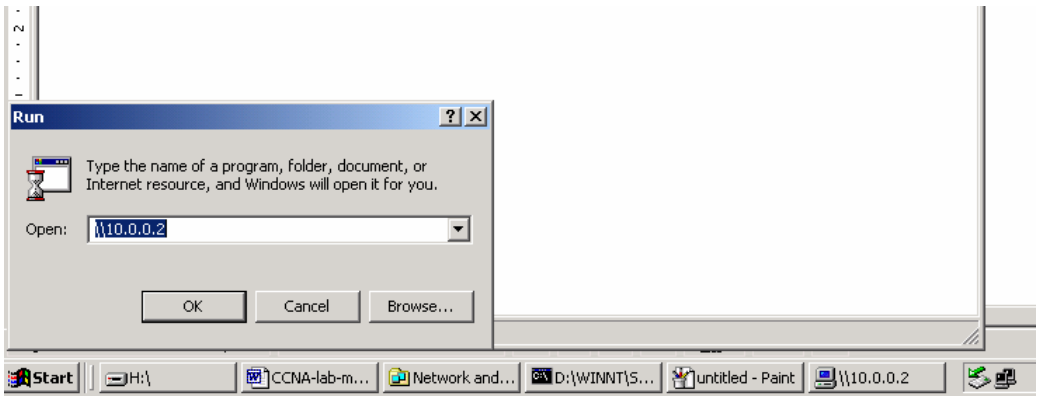
D:\>ping 10.0.0.2
Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<10ms TTL=128
Reply from 10.0.0.2: bytes=32 time<10ms TTL=128
Reply from 10.0.0.2: bytes=32 time<10ms TTL=128
Reply from 10.0.0.2: bytes=32 time<10ms TTL=128

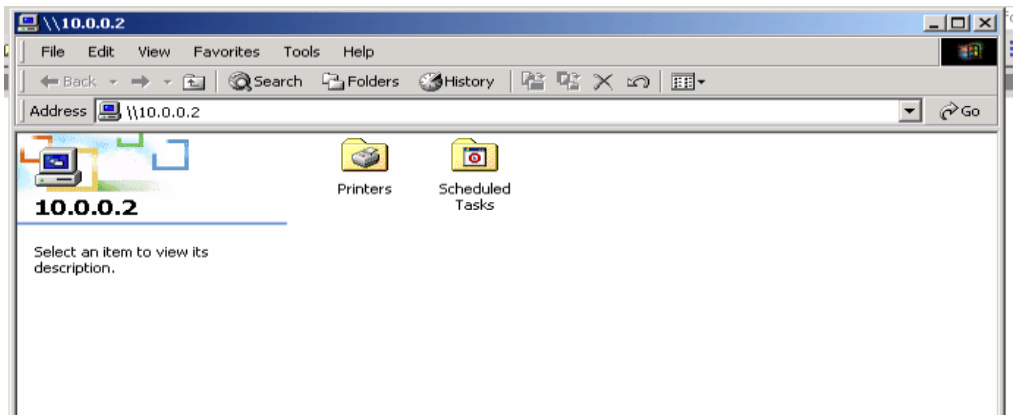
Ping statistics for 10.0.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

Step 3(B): Check their connectivity by Data Sharing.

Type on RUN as: **\\10.0.0.2**



The following screen will pop-up,



Lab # 3

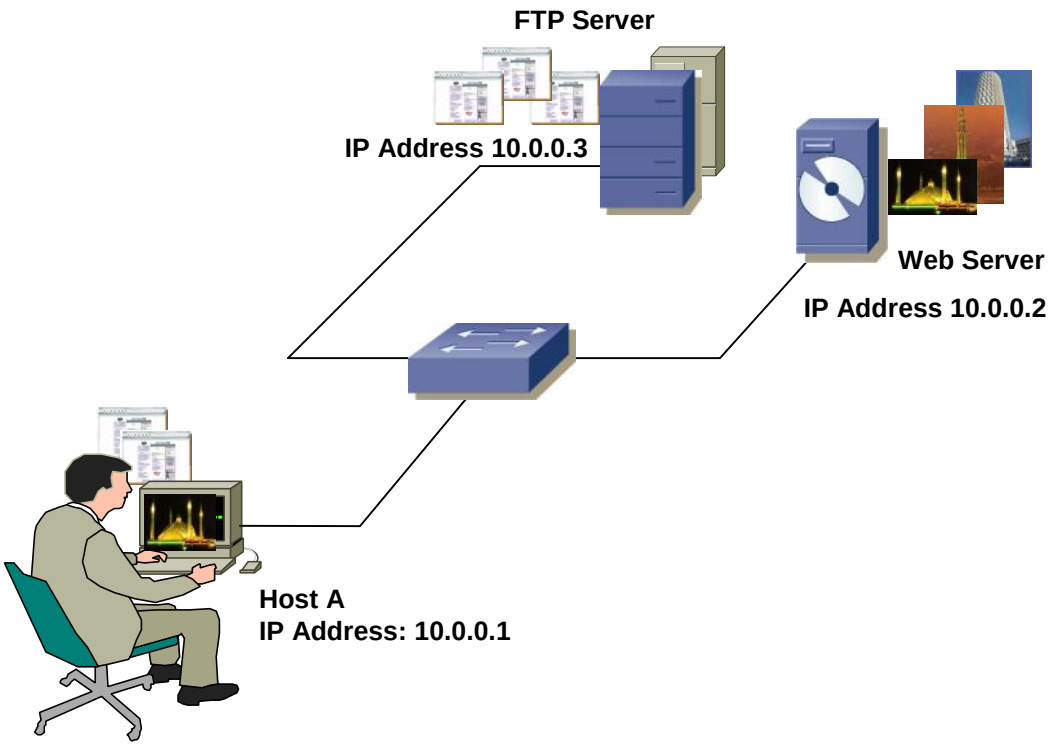
How to Make a Web & Ftp Server

Objective

This lab demonstrates how to make a Web & Ftp Server.
The demonstrations include:

1. Web Server.
2. Ftp Server.

Diagram



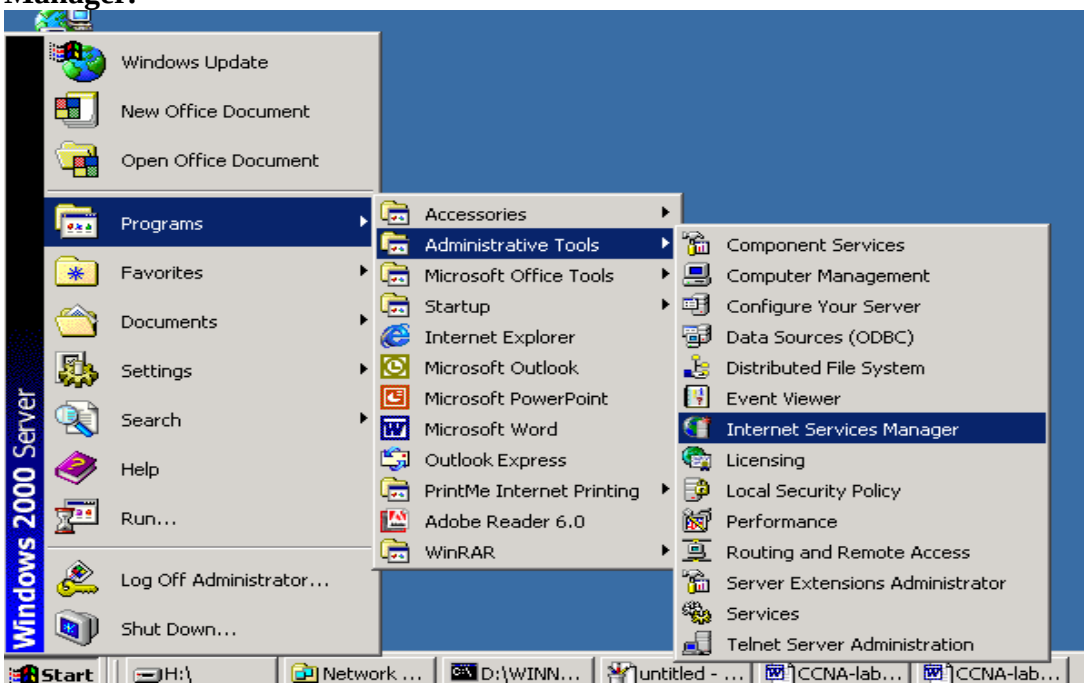
Procedure

1. Open an Internet Information Service (IIS) from an Administrative tools and Make a WEB Server.
2. Open an Internet Information Service (IIS) from an Administrative tools and Make a FTP Server.
3. Verifying the WEB & FTP Server from Host 'A'.

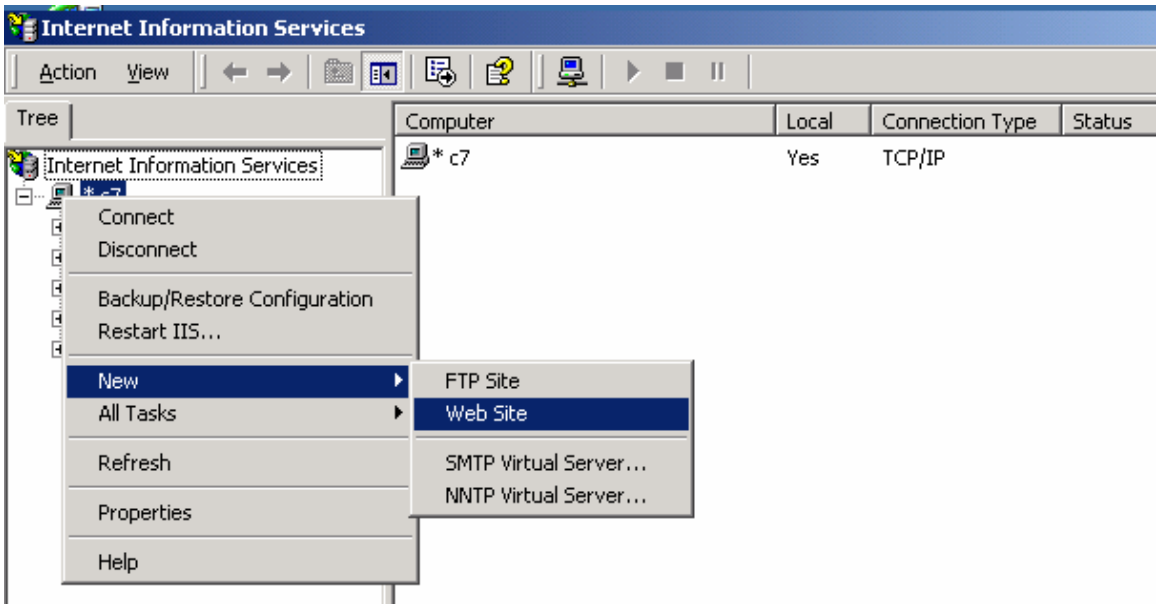
Configuration

Step 1: Open an Internet Information Service (IIS) from an Administrative tools & Make a WEB Server.

Go to **Windows Start Button** > **Programs** > **Administrative Tools** > **Internet Services Manager.**

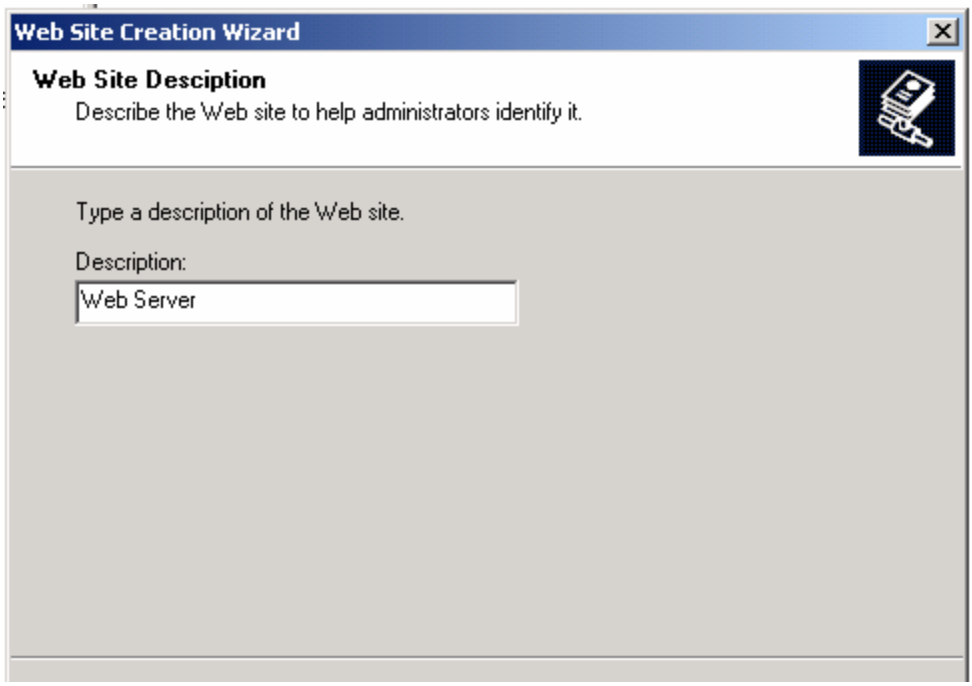


Then, Start **IIS** & Right Click on the **Computer Name** > **New** > **Web Site**

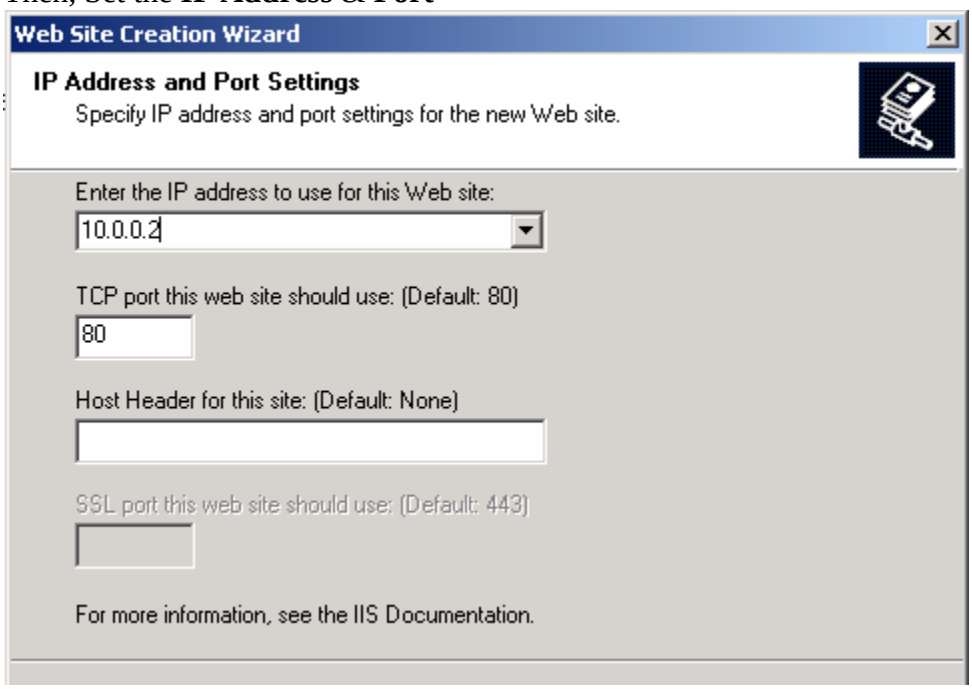


Then, Start **IIS** & Right Click on the **Computer Name** > **New** > **Web Site**

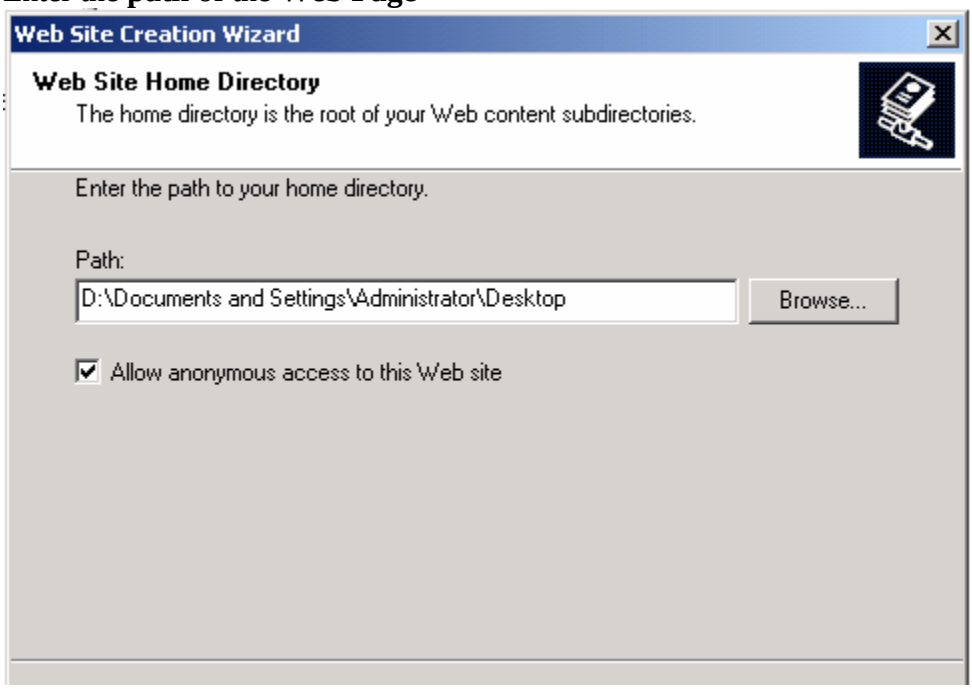
Then, Start **IIS** & Right Click on the **Computer Name** > **New** > **Web Site**



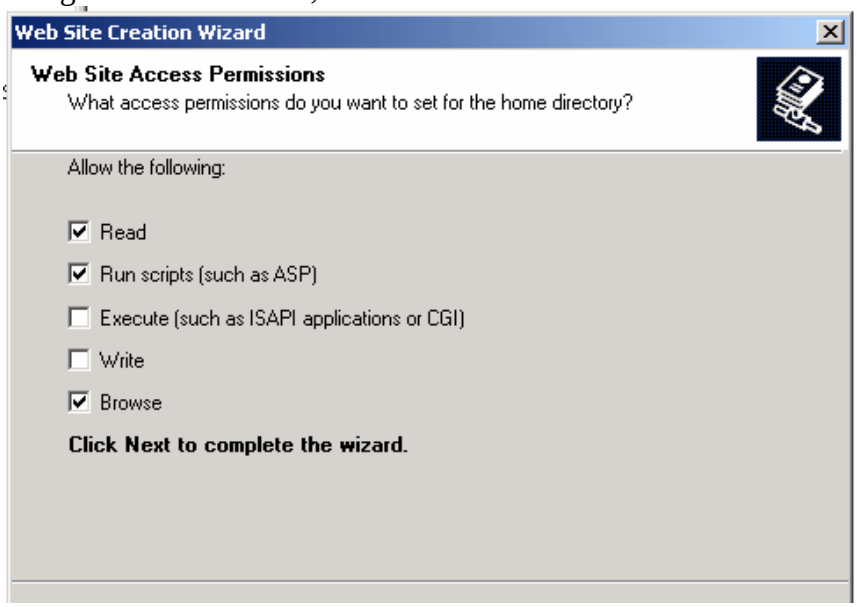
Then, Set the **IP Address** & **Port**



Enter the **path** of the **Web Page**

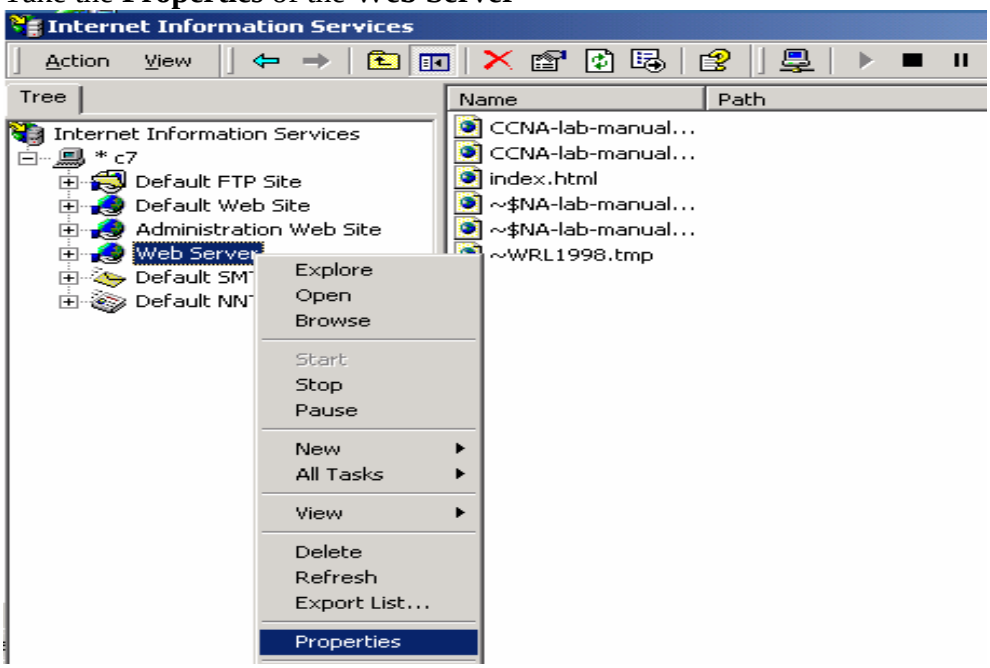


Assigns the **Permission**,

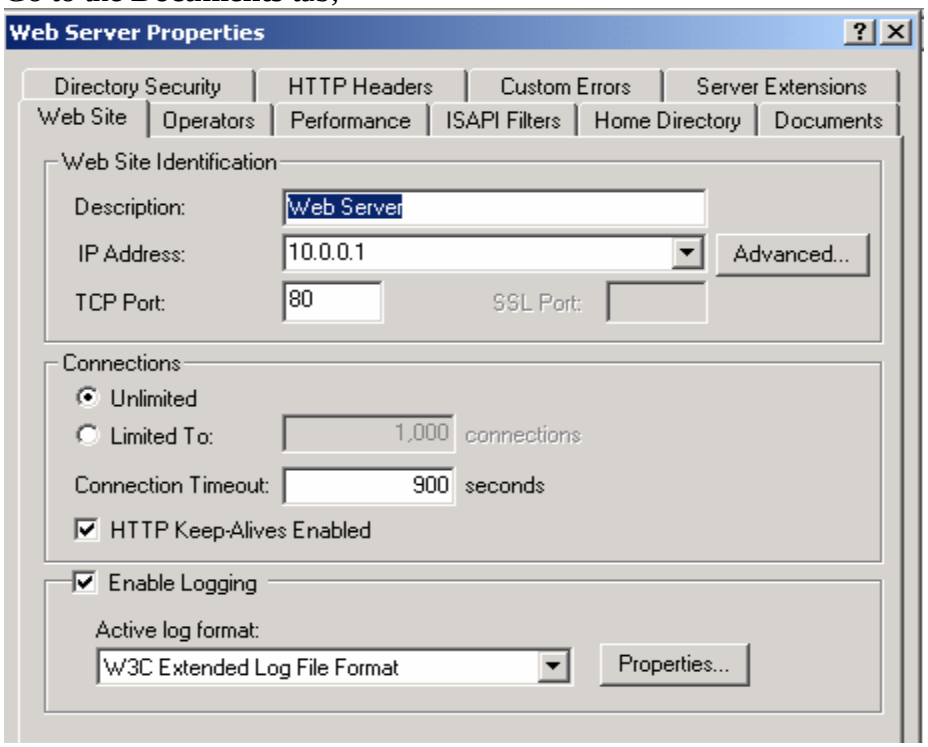


Wizard will finish now successfully.

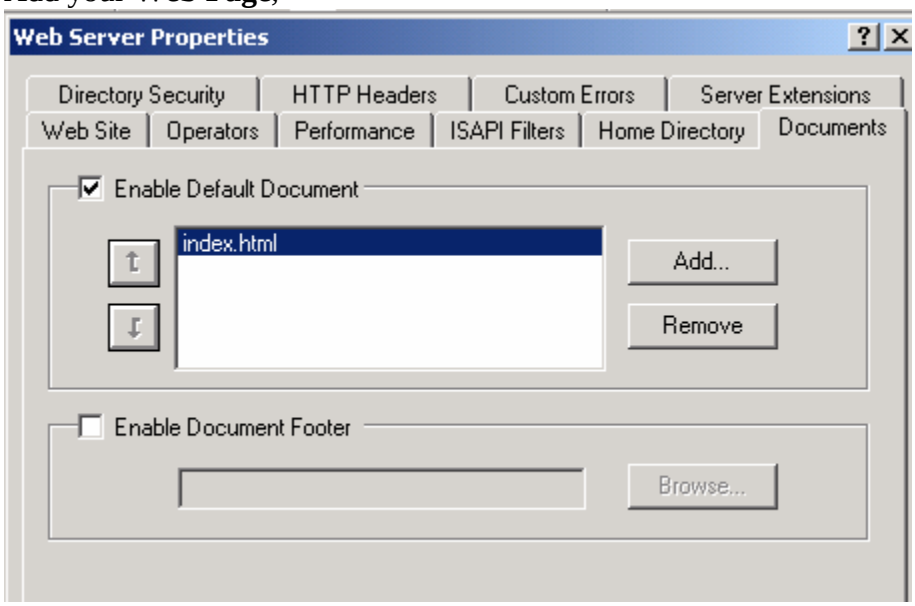
Take the **Properties** of the **Web Server**



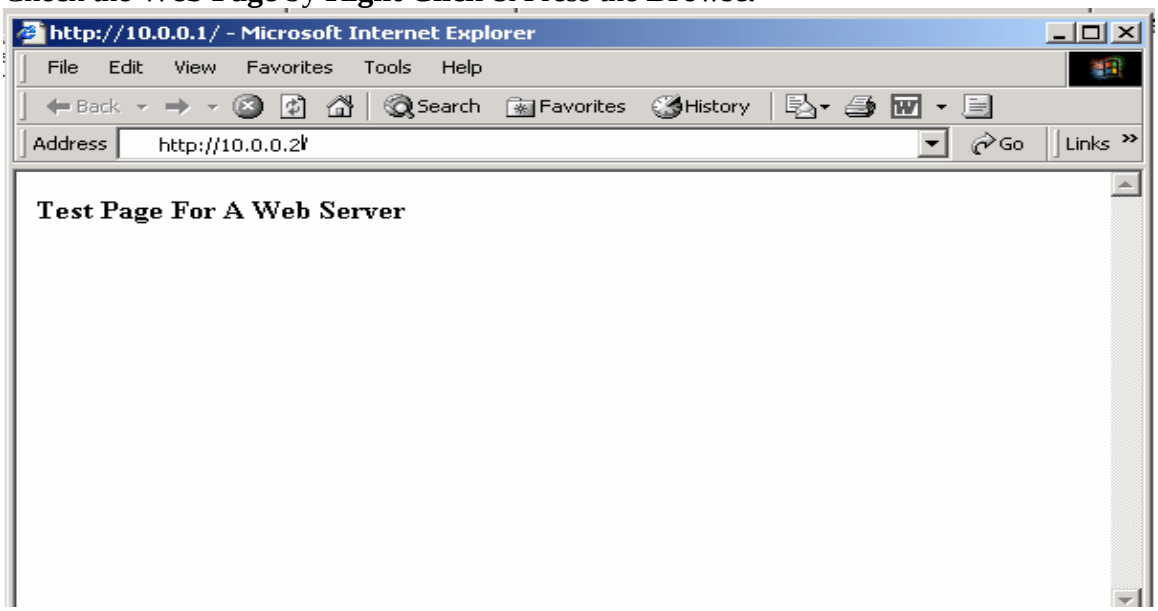
Go to the **Documents** tab,



Add your **Web Page**,

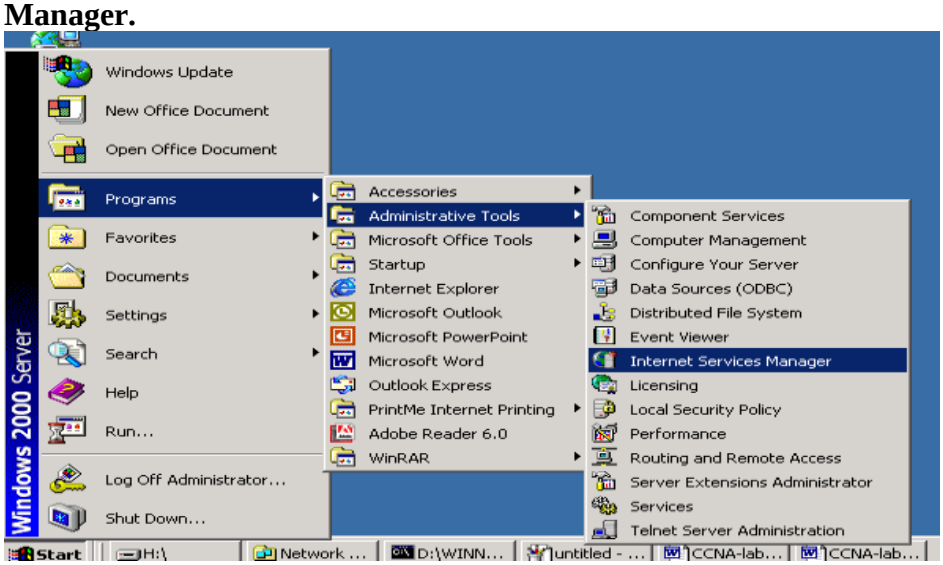


Check the **Web Page** by **Right Click** & Press the **Browse.**

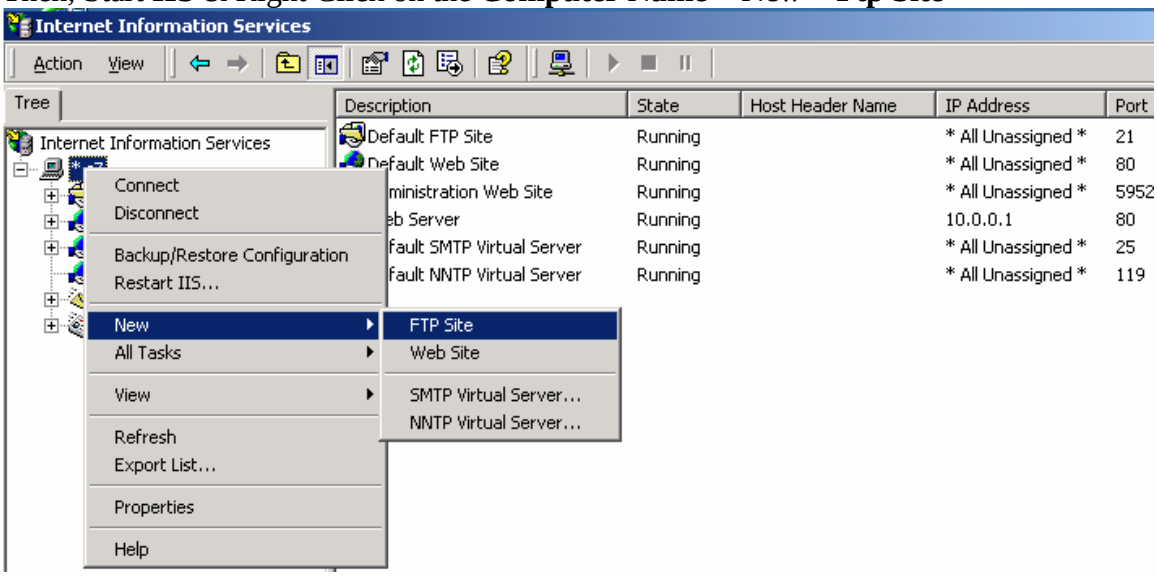


Step 2: Open an Internet Information Service (IIS) from an Administrative tools & Make a FTP Server.

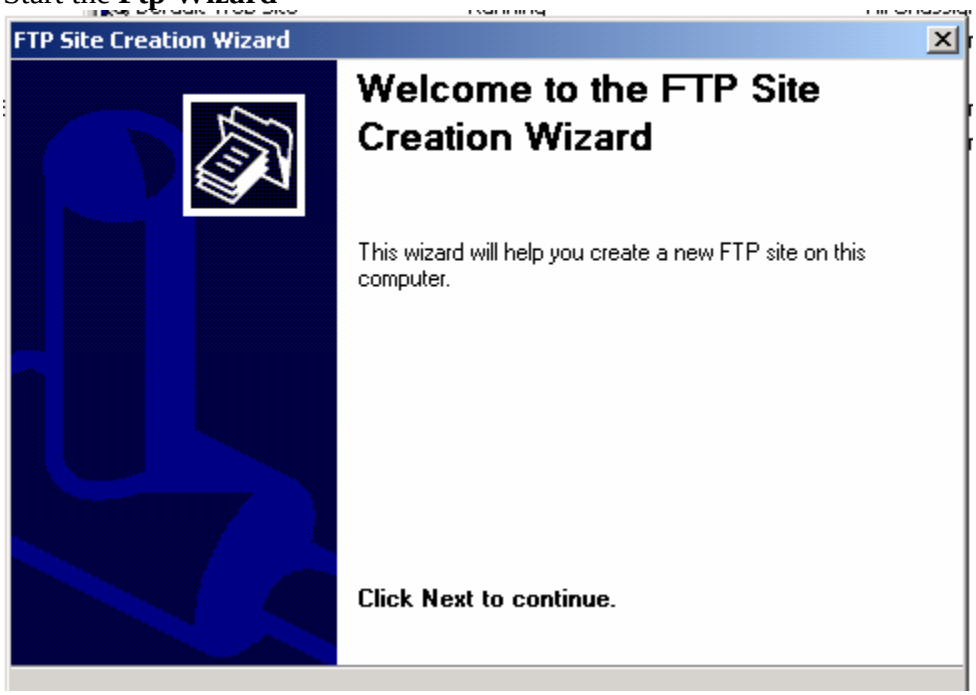
Go to **Windows Start Button** > **Programs** > **Administrative Tools** > **Internet Services Manager.**



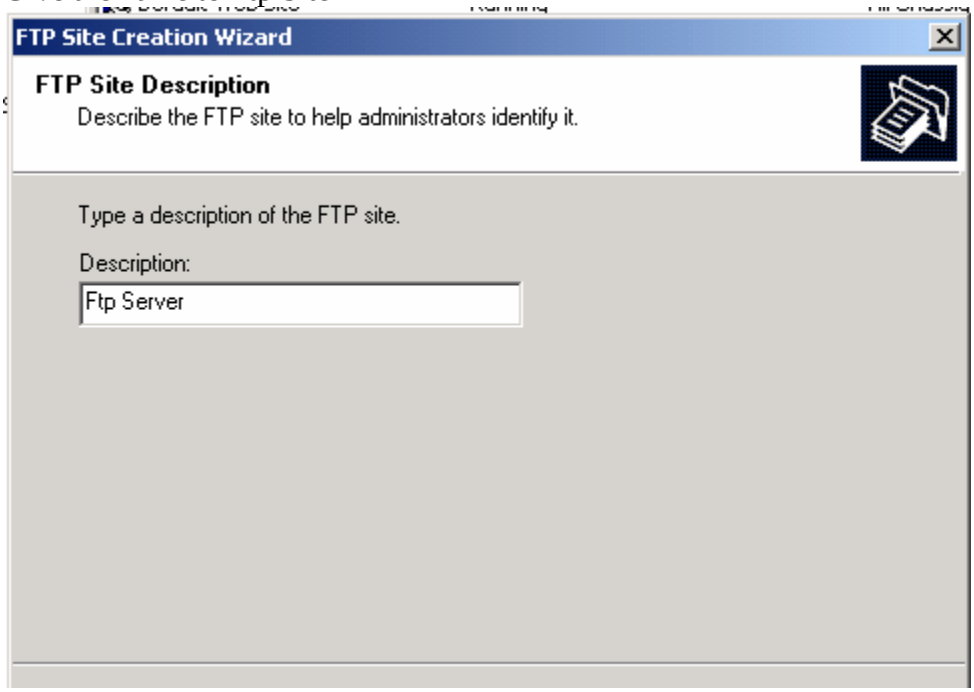
Then, Start **IIS** & Right Click on the **Computer Name** > **New** > **Ftp Site**



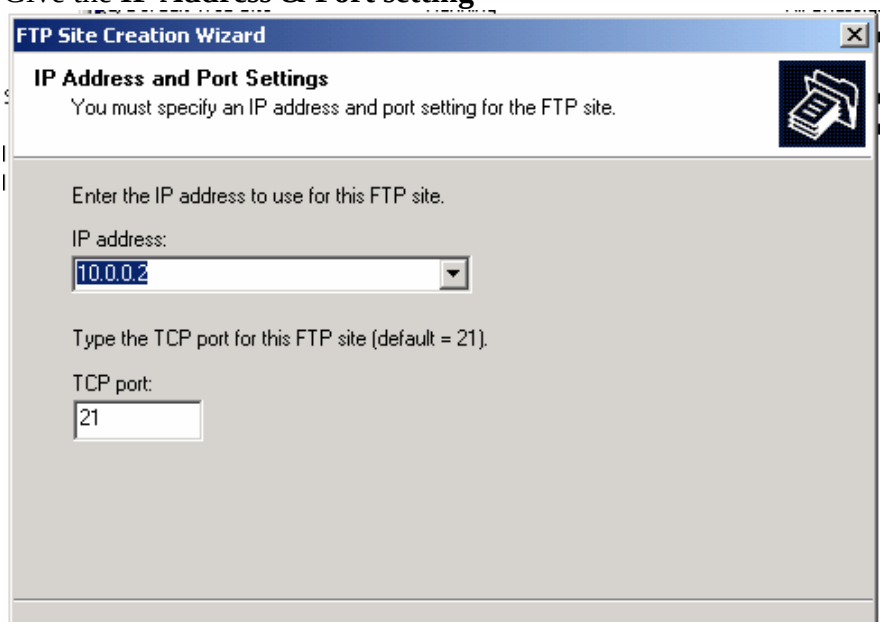
Start the **Ftp Wizard**



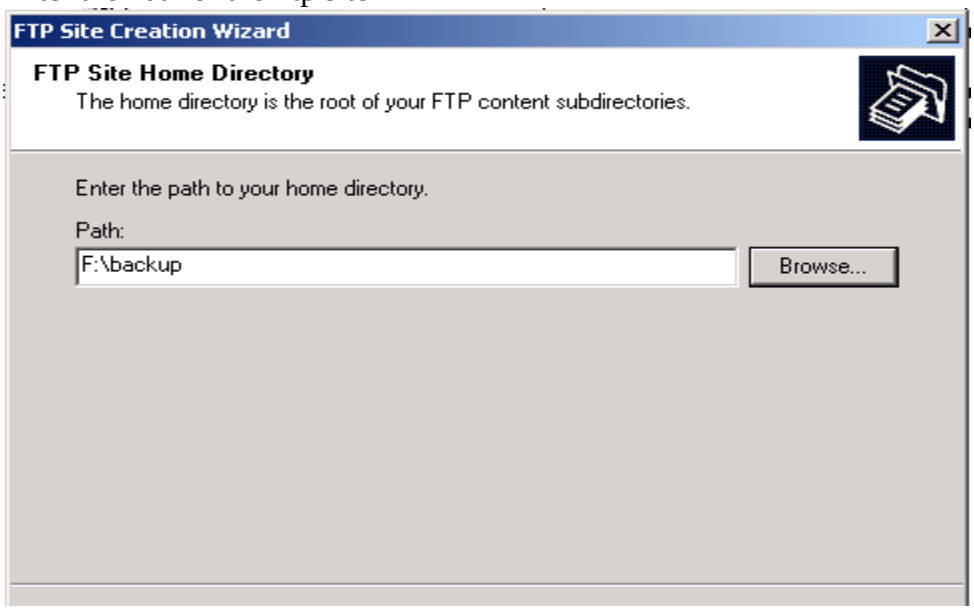
Give the name to Ftp Site



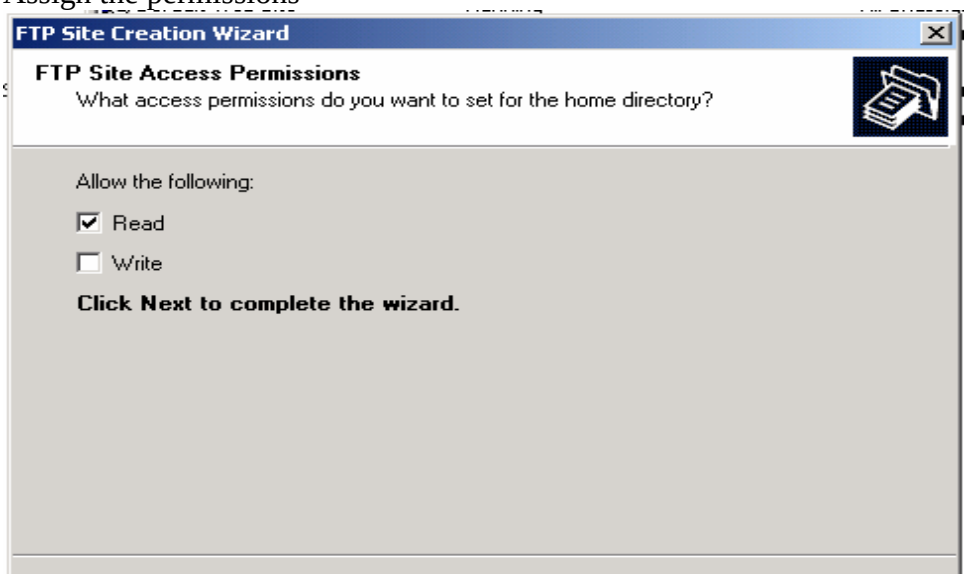
Give the **IP Address & Port setting**



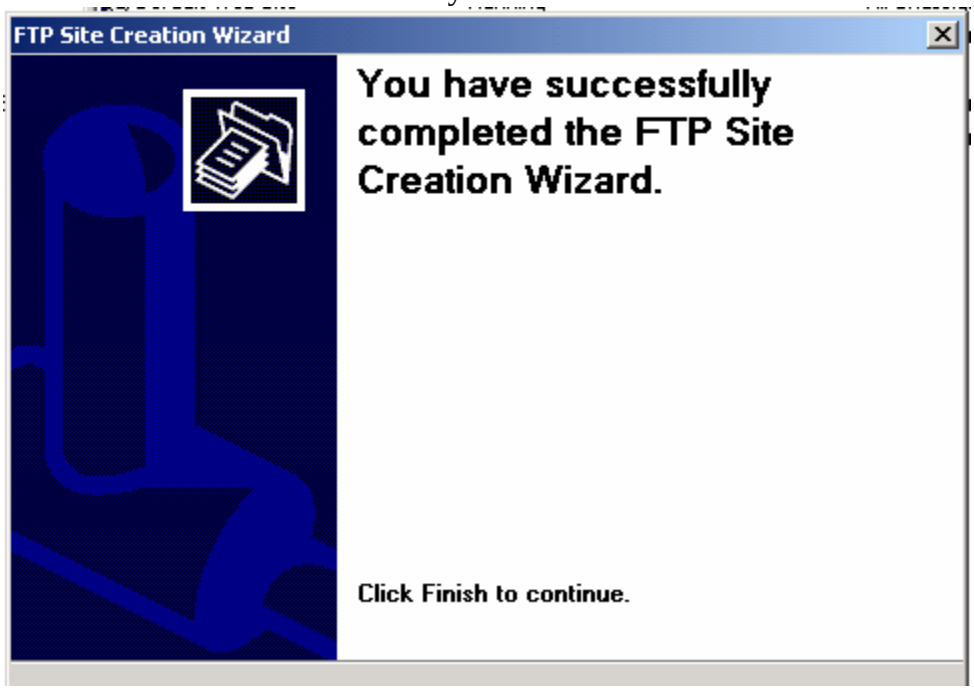
Enter the Path of the Ftp site



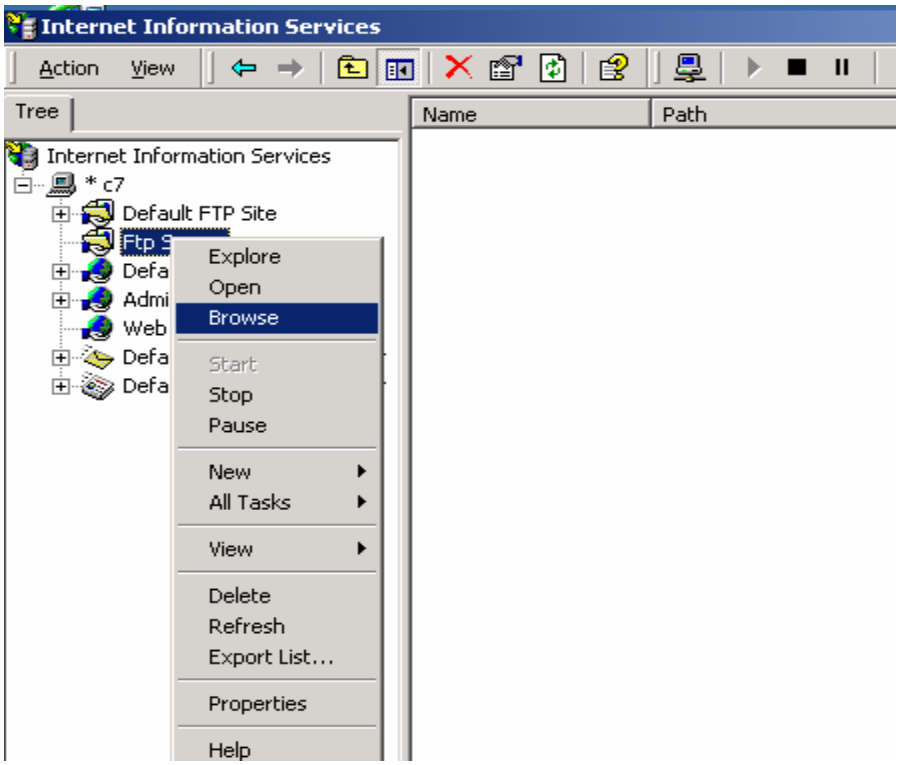
Assign the permissions



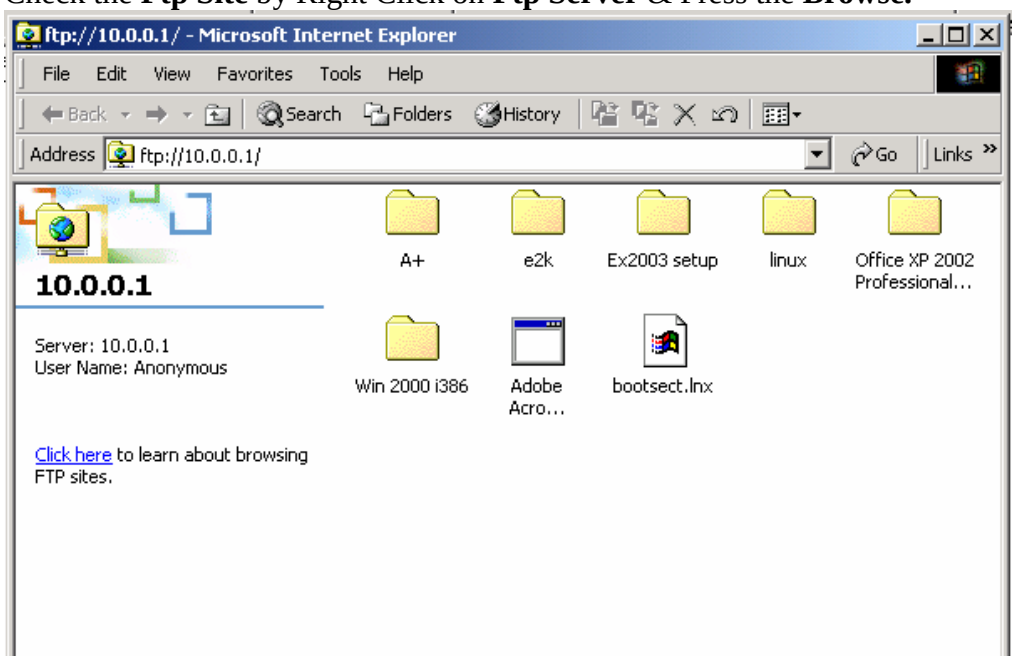
Wizard will finish now successfully.



Check the **Ftp Site** by Right Click on **Ftp Server** & Press the **Browse.**

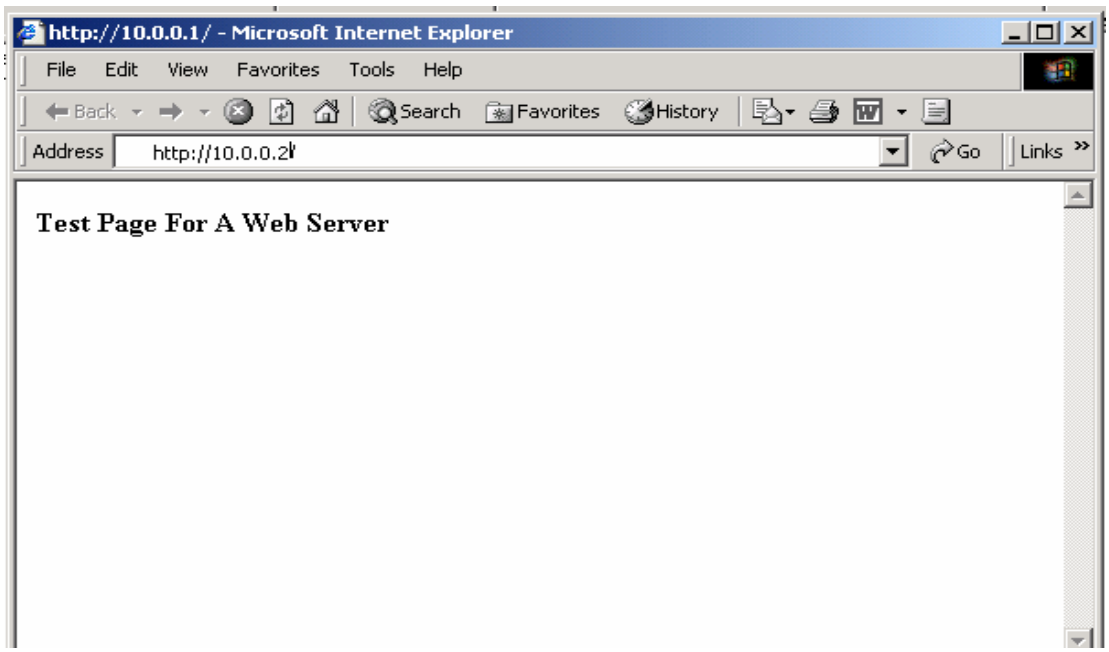


Check the **Ftp Site** by Right Click on **Ftp Server** & Press the **Browse.**

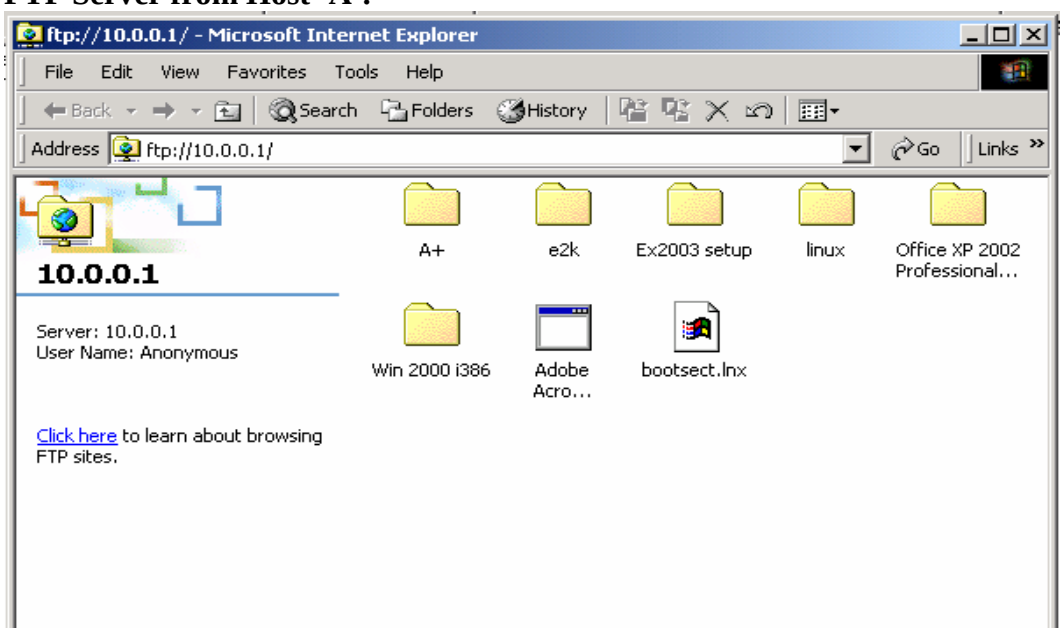


Step 3: Verifying the WEB & FTP Server from Host 'A'.

WEB Server from Host 'A'.



FTP Server from Host 'A'.



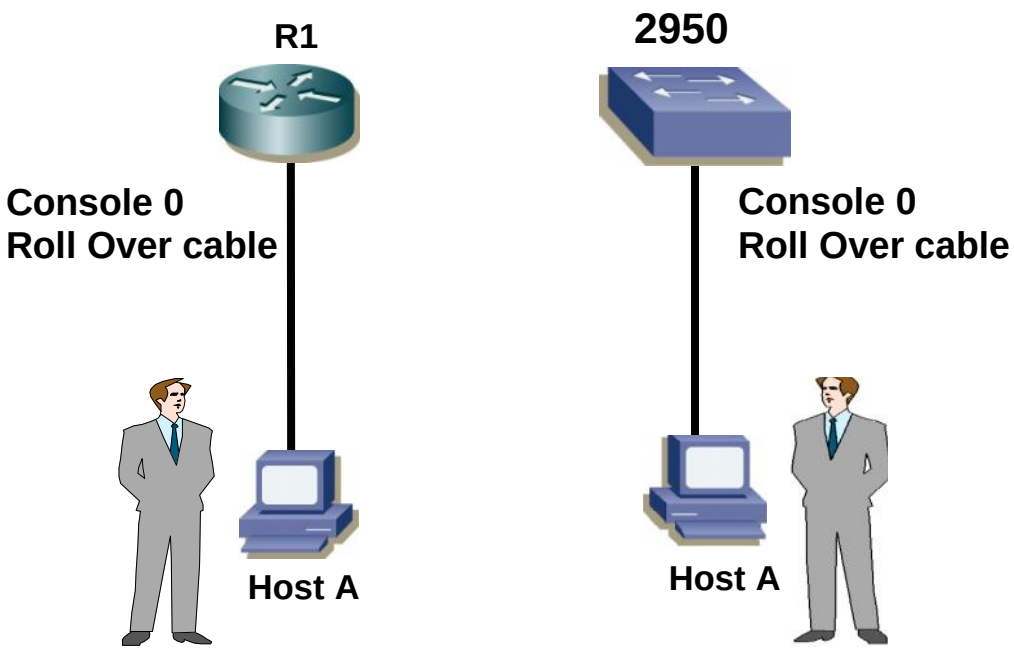
Lab # 4

Open A Hyper Terminal Session

Objective

This lab demonstrates how to open a Hyper Terminal session.

Diagram



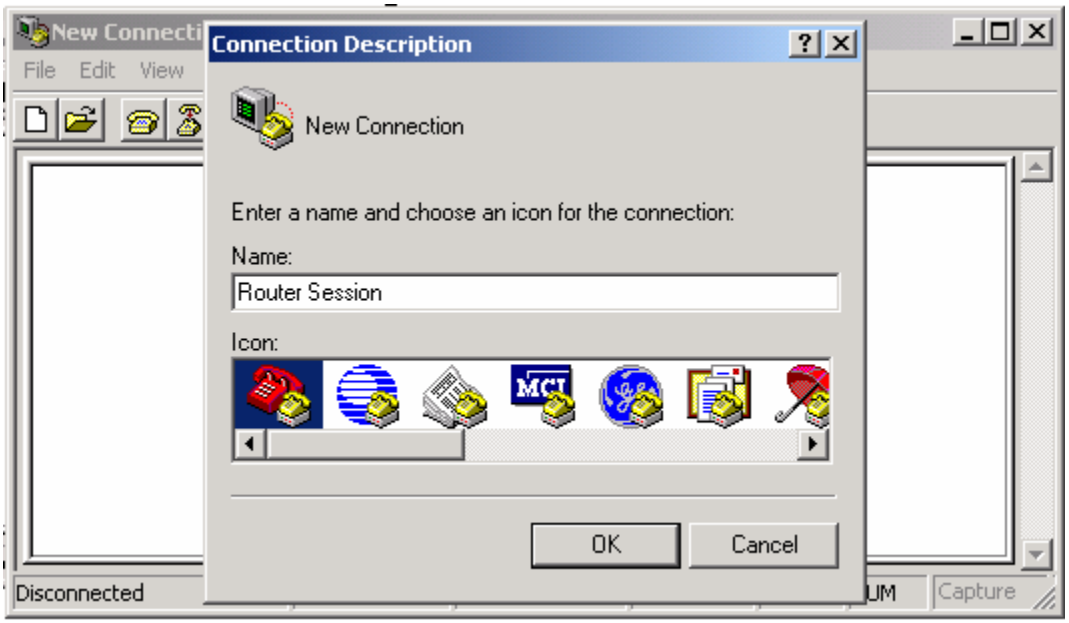
Procedure

1. Open the Hyper Terminal Session From **RUN** by giving the command '**hypertrm**' or from **STRART Button -> Programs -> Accessories -> Communications -> Hyper Terminal**.
2. Give the Session name.
3. Define the connection type i-e., **COM1**.

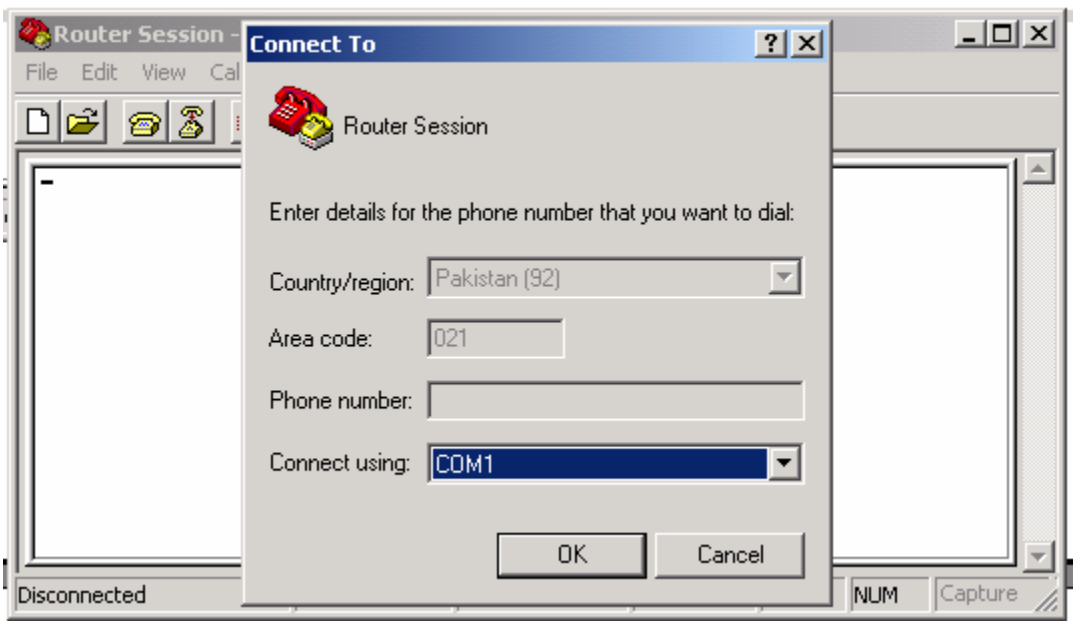
Configuration

Step 1: Open the Hyper Terminal Session From RUN by giving the command 'hypertrm' or from START Button -> Programs -> Accessories -> Communications -> Hyper Terminal.

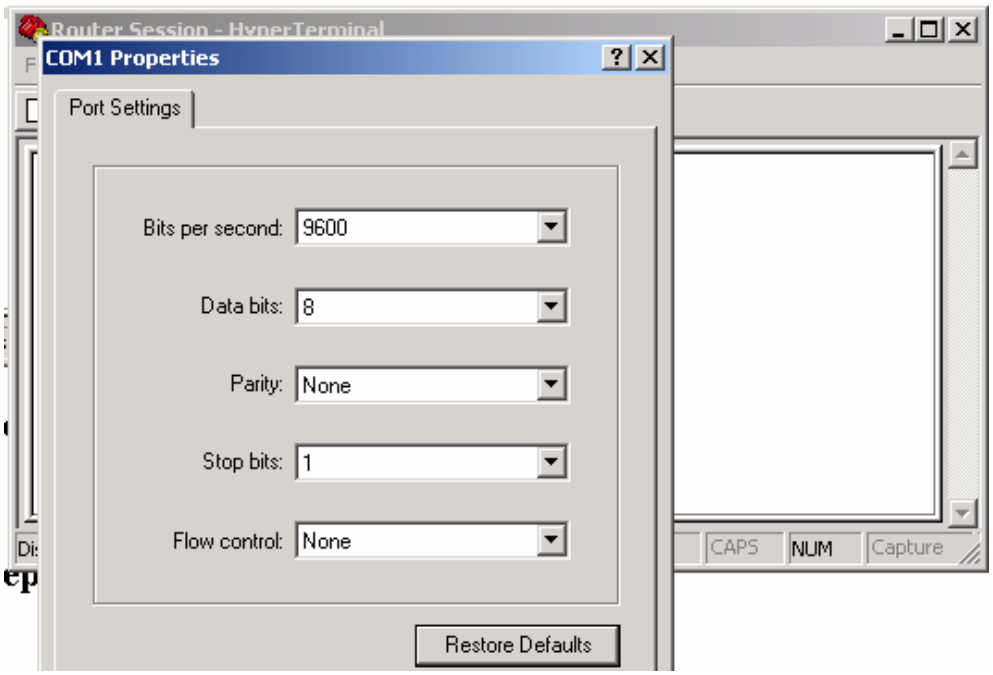
Step 2: Give the Session name.



Step 3: Define the Connection Type i-e., COM1.

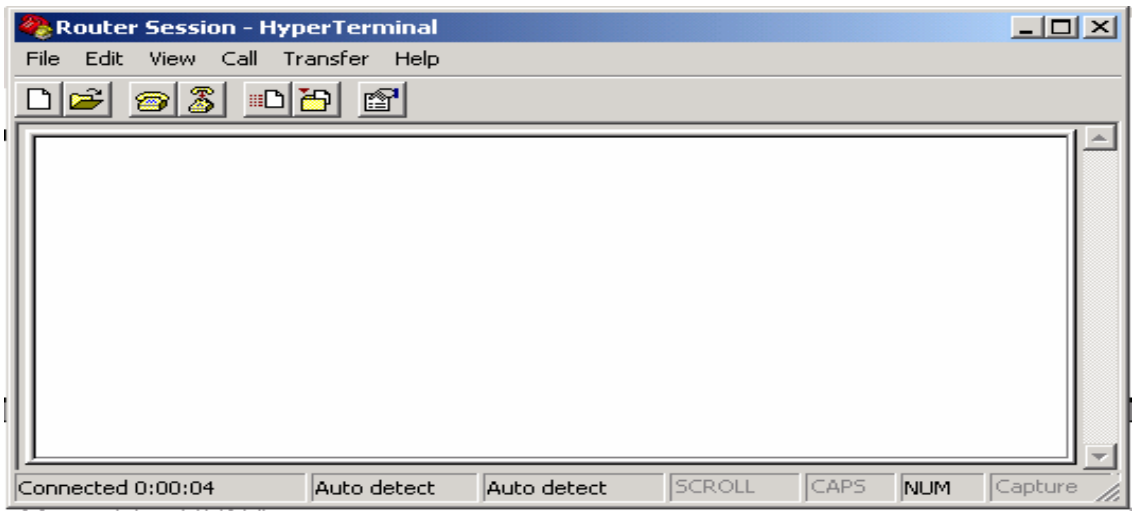


Step 4: Define the Port Settings of COM Port.



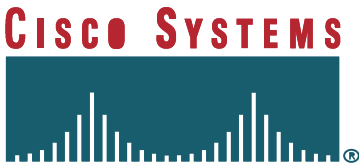
Note: Press Restore Defaults Button

Step 5: Start the Hyper Terminal Session.



Section 2

Routing



By **M. Irfan Ghauri**
M. Rizwan

Lab # 5

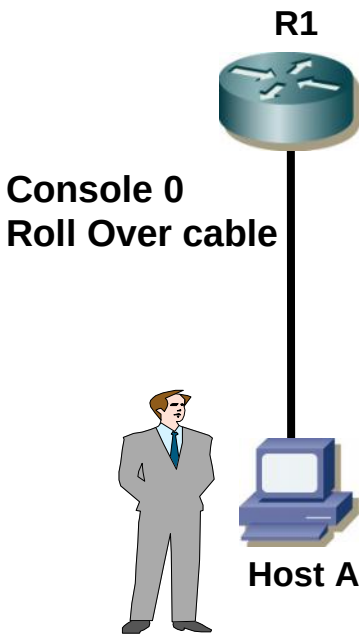
Router Basic IOS

Objective

This lab includes basic commands of Router IOS on 2500 Series.

i. Router Basic Commands.

Diagram



Configuration

Step 1: After connecting your PC to the Console Port.

Router con0 is now available

Press RETURN to get started.
Router>

Step 2: To Enter Into Privilege mode/Executive Mode From User Mode & Vice-Versa.

Router>enable
Router#
Router#disable
Router>

Step 3: To Enter Into Global Configuration Mode.

Router#configure terminal
Router(config)#

Step 4: To change the Host Name of Router.

Router(config)#hostname R1
R1(config)#

Step 5(A): Set the System Clock, Date & Time on the Router

R1#clock set ?

hh:mm:ss Current Time

R1#clock set 6:30:45 ?

<1-31> Day of the month
MONTH Month of the year

R1#clock set 6:30:45 1 JAN ?

<1993-2035> Year

R1#clock set 6:30:45 1 JAN 2005

Step 5(B): Verify the System Clock, Date & Time on the Router

R1#show clock

06:32:33.527 UTC Sat Jan 1 2005

Step 6(A): Set the Message of the Day Banner on the Router.

R1(config)#banner motd # HELLO & WELCOME TO CISCO WORLD #

Step 6(B): Verify the Message of the Day Banner on the Router.

R1 con0 is now available

Press RETURN to get started.

HELLO & WELCOME TO CISCO WORLD

R1>

Step 7: Display the Version Information of the Router.

R1#show version

Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-I-L), Version 12.0(7)T, RELEASE SOFTWARE (fc2)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Mon 06-Dec-99 14:50 by phanguye
Image text-base: 0x0303C728, data-base: 0x00001000

ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a), RELEASE SOFTWARE (fc1)
R1 uptime is 1 minute
System returned to ROM by reload
System image file is "flash:c2500-i-l[1].120-7.T.bin"

cisco 2500 (68030) processor (revision F) with 16384K/2048K bytes of memory.
Processor board ID 04851445, with hardware revision 00000000
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2102

Step 8: Display the Flash Information.

R1#dir

OR

R1#show flash:

System flash directory:
File Length Name/status
1 7432656 c2500-i-l[1].120-7.T.bin
[7432720 bytes used, 955888 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)

Step 9: Show contents of Current Configuration (RAM).

R1#show running-config

Step 10: Show contents of Startup Configuration (NVRAM).

R1#show startup-config

Step 11(A): Set the Line Console Password on the Router.

R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login

Step 11(B): Verification Line Console Password on the switch.

R1 con0 is now available

Press RETURN to get started.

User Access Verification

Password:
R1>

Step 12(A): Set the privileged mode password in clear text.

R1(config)#enable password cisco

Step 12(B): Verifying the privileged mode password in clear text.

R1#disable
R1>enable
Password:
R1#

Step 13(A): Set the Privileged Mode password in encrypted form.

R1(config)#enable secret cisco

The enable secret you have chosen is the same as your enable password.
This is not recommended. **Re-enter the enable secret**.

R1(config)#enable secret cisco1

Step 13(B): Verifying the Privileged Mode password in encrypted form.

R1#disable
R1>enable
Password: (Enter Clear Text Password)
Password: (Enter Encrypted Password)
R1#

Step 14: Set the Line VTY Password on the Router.

R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login

Step 15: Set the Line Auxiliary Password on the Router.

R1(config)#line aux 0
R1(config-line)#password cisco
R1(config-line)#login

Step 16: Remove the Privileged Mode Password (Level 15) in clear form.

R1(config)#no enable password cisco

Step 17: Remove the Privileged Mode Secret Password (Level 15) in encrypted form.

R1(config)#no enable secret cisco1

Step 18: To enter in the Setup Mode (Initial Configuration Dialog) of Router.

Router#setup

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: y

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: y

Configuring global parameters:
Enter host name [Router]: R1

The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
Enter enable secret: cisco1

The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password: cisco

The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: cisco

Configure SNMP Network Management? [no]:

Current interface summary

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	**unassigned**	**YES**	**NVRAM**	**administratively down**	**down**
Serial0	**unassigned**	**YES**	**NVRAM**	**administratively down**	**down**
Serial1	**unassigned**	**YES**	**NVRAM**	**administratively down**	**down**

Enter interface name used to connect to the
management network from the above interface summary: **Ethernet0**

Configuring interface Ethernet0:
Configure IP on this interface? [no]: yes
IP address for this inerface: 10.0.0.20
Subnet mask for this interface [255.0.0.0] : 255.0.0.0
Class A network is 10.0.0.0, 8 subnet bits; mask is /8

The following configuration command script was created:

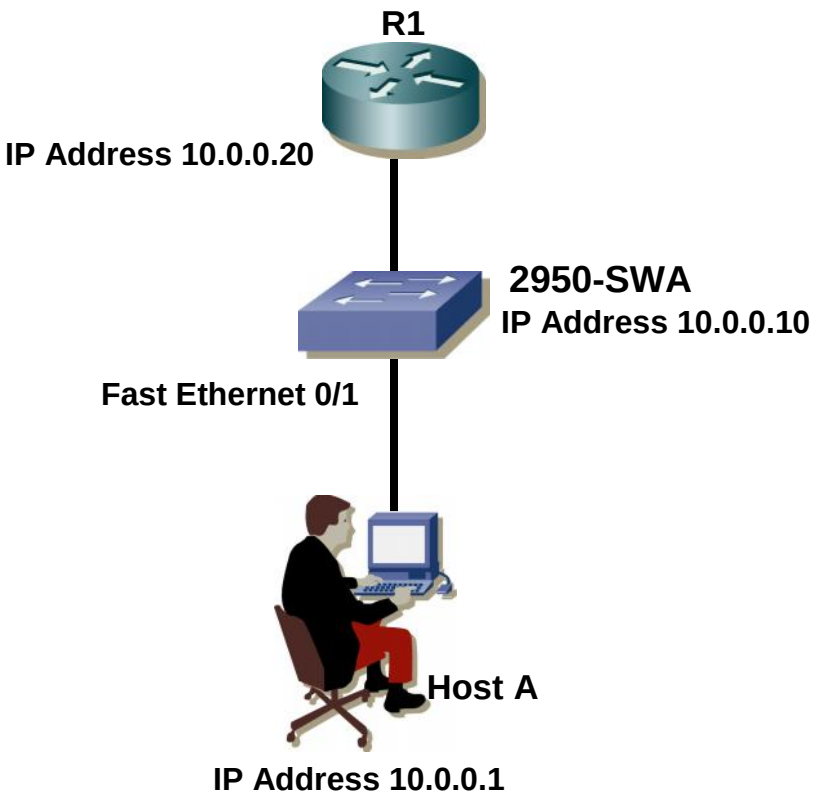
hostname R1
enable secret 5 1ZFA2$ZR288i7VkOufhqSdIyiOs.
enable password cisco
line vty 0 4
password cisco
no snmp-server
!
no ip routing
!
interface Ethernet0
no shutdown
ip address 10.0.0.20 255.0.0.0
!
interface Serial0
shutdown
no ip address
!
!
interface Serial1
shutdown

no ip address
!
end
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 0
% You can enter the setup, by typing setup at IOS command prompt
Router#

ii. Assign the IP Address on the Ethernet Interface of the Router.

Diagram



Procedure

1. Check for the interfaces summary of the Router.
2. Assign the IP Address on the Ethernet Interface of the Router.
3. Display the interface information of the Ethernet interface of the router.
4. Verify the connectivity of the Router with the switch & PC.

Configuration

Step 1: Check for the Interfaces summary of the Router.

R1#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	**unassigned**	**YES**	**NVRAM**	**administratively down**	**down**
Serial0	**unassigned**	**YES**	**NVRAM**	**administratively down**	**down**
Serial1	**unassigned**	**YES**	**NVRAM**	**administratively down**	**down**

Step 2: Assign the IP Address on the Ethernet Interface of the Router.

R1(config)#interface ethernet 0
R1(config-if)#no ip address
R1(config-if)#ip address 10.0.0.20 255.0.0.0
R1(config-if)#no shutdown

Step 3: Display the interface information of the Ethernet interface of the Router.

R1#show interfaces ethernet 0

Ethernet0 is up, line protocol is up
Hardware is Lance, address is 0000.0c3e.93e1 (bia 0000.0c3e.93e1)
Internet address is 10.0.0.20/8
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never

Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
<Output Omitted>

Step 4(A): Check for the Interfaces summary of the Router.

R1#show ip interface brief

Interface	IP-Address	OK? Method	Status	Protocol
Ethernet0	**10.0.0.20**	**YES manual**	**up**	**up**
Serial0	unassigned	YES NVRAM	administratively down	down
Serial1	unassigned	YES NVRAM	administratively down	down

Step 4(B): Verify the connectivity of the Router with the Switch.

R1#ping 10.0.0.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

Step 4(C): Verify the connectivity of the Router with the PC.

R1#ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

iii. Assign the IP Address on the Serial Interfaces of the Router.

Diagram

Procedure

1) Check for the interfaces summary of the Router R1 & R2
2) Check for the DCE & DTE interfaces of the Router R1 & R2
3) Assign the IP Address on the Serial Interfaces of the Router R1 & R2.
4) Display the interface information of the Serial interface of the Router R1 & R2.
5) Verify the connectivity of the Router R1 & R2.

Configuration

Step 1: Check for the Interfaces summary of the Routers.

R1#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	**unassigned**	**YES**	**NVRAM**	**administratively down**	**down**
Serial0	**unassigned**	**YES**	**NVRAM**	**administratively down**	**down**
Serial1	**unassigned**	**YES**	**NVRAM**	**administratively down**	**down**

Step 2(A): Check for the DCE cable of the Router R1.

R1#show controllers serial 0

HD unit 0, idb = 0x10DB04, driver structure at 0x1139D8
buffer size 1524 HD unit 0, **RS-232 DCE cable**
cpb = 0x22, eda = 0x4140, cda = 0x4000
<Output Omitted>
0 missed datagrams, 0 overruns
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns
0 residual bit errors

Step 2(B): Check for the DTE cable of the Router R2.

R2#show controllers serial 0

HD unit 0, idb = 0x160118, driver structure at 0x165478
buffer size 1524 HD unit 0, **RS-232 DTE cable**
cpb = 0x22, eda = 0x412C, cda = 0x4140
<Output Omitted>
0 missed datagrams, 0 overruns
0 bad datagram encapsulations, 0 memory errors

0 transmitter underruns
0 residual bit errors

Step 3(A): Assign the IP Address on the Serial Interface of the Router R1.

R1(config)#interface serial 0
R1(config-if)#ip address 15.0.0.1 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#clock rate 64000 (Clock Rate will set only DCE Interface)
R1(config-if)#end

Step 3(A): Assign the IP Address on the Serial Interface of the Router R2.

R2(config)#interface serial 0
R2(config-if)#ip address 15.0.0.2 255.0.0.0
R2(config-if)#no shutdown
R2(config-if)#end

Step 4: Display the interface information of the Serial interface of the Router.

R1#show interfaces serial 0

Serial0 is up, line protocol is up
Hardware is HD64570
Internet address is 15.0.0.1/8
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input 00:00:04, output 00:00:00, output hang never
Last clearing of "show interface" counters 01:48:12
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
<Output Omitted>

Step 5(A): Check for the Interfaces summary of the Router R1.

R1#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	unassigned	YES	unset	administratively down	down
Serial0	**15.0.0.1**	**YES**	**manual**	**up**	**up**
Serial1	unassigned	YES	NVRAM	administratively down	down

Step 5(B): Verify the connectivity of the Router R1 & R2.

R1#ping 15.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 15.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms

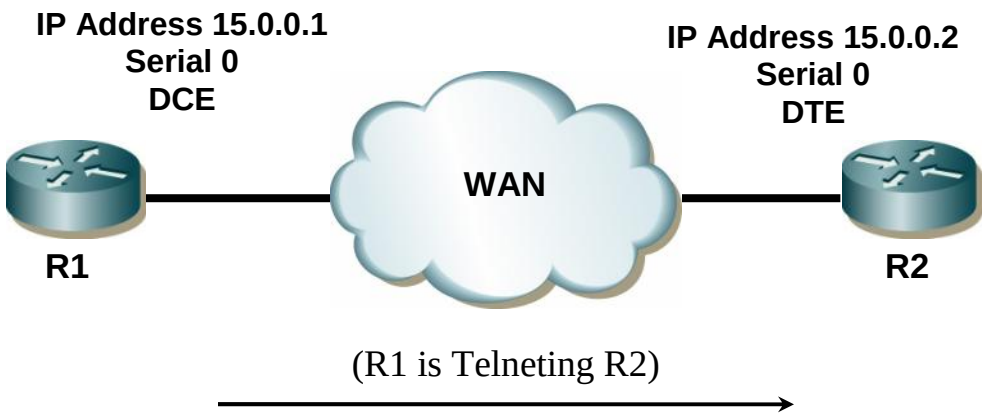
Lab # 6

Accessing Router through Telnet
(Telnet between 2 Routers)

Objective

Understanding the telnet operations. In this lab Router R1 is going to be telnet to Router R2.

Diagram



Procedure

1) Check the Connectivity between 2 routers.
2) Set the **Privilege mode password** on Router R2.
3) Set the **TELNET** (**line VTY) password** on Router R2.
4) Verify the telnet Session from Router R1 to Router R2.
5) Disconnect the telnet Session.

Configuration

Step 1: Check the Connectivity between 2 routers.

R1#ping 15.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 15.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms

Step 2: Set the Telnet (Line VTY)password on Router R2.

R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login

Step 3: Set the Privilege mode password on Router R2.

R2(config)#enable password cisco

Step 4: Verify the telnet Session from Router R1 to Router R2.

R1#telnet 15.0.0.2
Trying 15.0.0.2 ... Open

User Access Verification

Password:
R2>enable
Password:
R2#

Step 5(A): Verify the telnet line on Router R2.

R2#show line

	Tty	Typ	Tx/Rx	A	Modem	Roty	AccO	AccI	Uses	Noise	Overruns
	0	CTY		-	-	-	-	-	0	1	0/0
	1	AUX	9600/9600	-	-	-	-	-	0	0	0/0
*	**2**	**VTY**		**-**	**-**	**-**	**-**	**-**	**5**	**0**	**0/0**
	3	VTY		-	-	-	-	-	0	0	0/0
	4	VTY		-	-	-	-	-	0	0	0/0
	5	VTY		-	-	-	-	-	0	0	0/0
	6	VTY		-	-	-	-	-	0	0	0/0

Step 5(B): Verify the telnet User on Router R2.

R2#show users

	Line	User	Host(s)	Idle	Location
*	**2 vty 0**		**idle**	**00:00:00**	**15.0.0.1**

Step 5(C): Verify the telnet sessions from Router R1.

R1#sh sessions

Conn	Host	Address	Byte	Idle	Conn Name
*	**1 15.0.0.2**	**15.0.0.2**	**0**	**0**	**15.0.0.2**

Step 6: Switch the telnet session from Router R2 to Router R1.

R2#
Press **[Ctrl+Shift+6 and then 'x']**
R1#

(Note: And then Resume connection by just Enter Key.)

Step 7(A): Disconnect the telnet session from Router R1 *(Gracefully).*

R1#disconnect
Closing connection to 15.0.0.2 [confirm]
R1#

Step 7(B): Disconnect the telnet session from Router R2 *(Disgracefully).*

R2#Clear line 2
[Connection to 15.0.0.2 closed by foreign host]
R1#

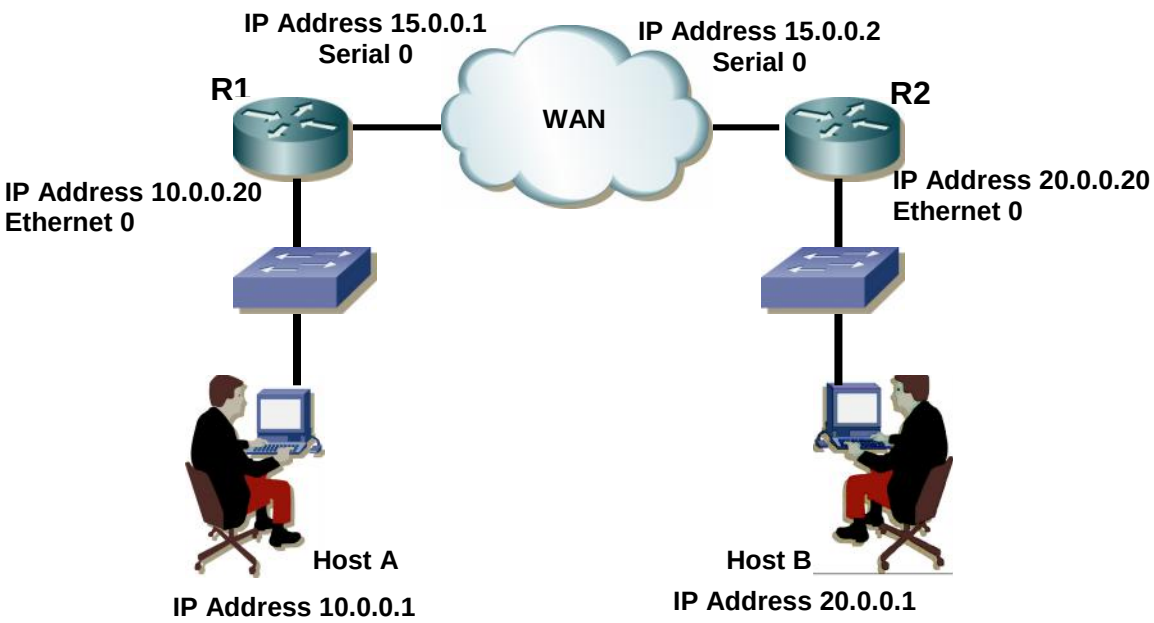
Lab # 7

STATIC Routes

Objective

Understanding the Operation of Static Routes. Static Routes are administratively defined routes that specify the address or interface of the next hop in the path that packets must take while moving between a source & destination.

Diagram



Procedure

1. Configuring & Assigning the IP addresses on the routers R1 & R2.
2. Check the routing table on both the routers.
3. Administratively define the Static Routes on both routers so that hosts on the both routers can communicate with each other.
4. Check the routing table on both the routers after defining the Static Routes on both sides.
5. Verifying the connection of both hosts.

Configuration

Step 1(A): Assigning the IP addresses on the Router R1.

R1(config)#interface serial 0
R1(config-if)#ip address 15.0.0.1 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#clock rate 64000 (Clock Rate will set only DCE Interface)

R1(config)#interface ethernet 0
R1(config-if)#ip address 10.0.0.20 255.0.0.0
R1(config-if)#no shutdown

Step 1(B): Assigning the IP addresses on the Router R2.

R2(config)#interface serial 0
R2(config-if)#ip address 15.0.0.2 255.0.0.0
R2(config-if)#no shutdown

R2(config)#interface ethernet 0
R2(config-if)#ip address 20.0.0.2 255.0.0.0
R2(config-if)#no shutdown

Step 2(A): Check the Routing table of the Router R1.

R1#sh ip route

C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 2(B): Check the Routing table of the Router R2.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 3(A): Administratively define the Static Route on the Router R1.

R1(config)#ip route 20.0.0.0 255.0.0.0 15.0.0.2 (Desired destination networks)

Step 3(B): Administratively define the Static Route on the Router R2.

R2(config)#ip route 10.0.0.0 255.0.0.0 15.0.0.1 (Desired destination networks)

Step 4(A): Check the Routing table of the Router R1 after enabling RIP.

R1#sh ip route

S 20.0.0.0/8 [1/0] via 15.0.0.2
C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 4(B): Check the Routing table of the Router R2 after enabling RIP.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
S 10.0.0.0/8 [1/0] via 15.0.0.1
C 15.0.0.0/8 is directly connected, Serial0

Step 5: Verifying the connection of Host 'A' & Host 'B'.

C:\>ping 20.0.0.1

Pinging 20.0.0.1 with 32 bytes of data:
Reply from 20.0.0.1: bytes=32 time=20ms TTL=254
Reply from 20.0.0.1: bytes=32 time=20ms TTL=254
Reply from 20.0.0.1: bytes=32 time=10ms TTL=254
Reply from 20.0.0.1: bytes=32 time=10ms TTL=254

Ping statistics for 20.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 10ms, Maximum = 20ms, Average = 15ms

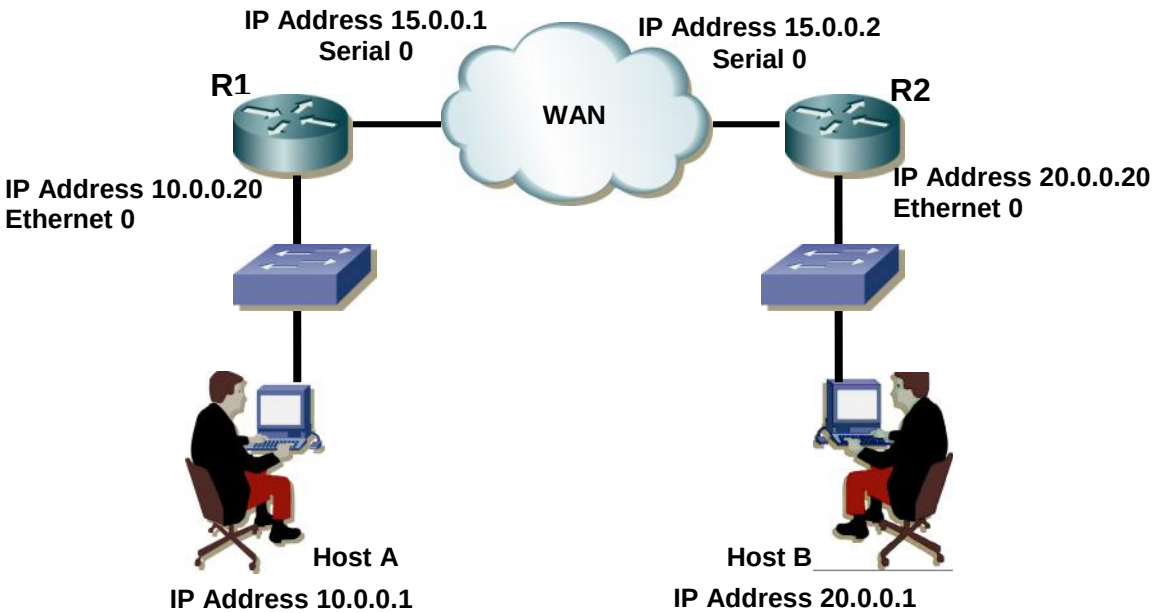
Lab # 8 (i)

Routing Protocols
(RIP Configuration)

Objective

Understanding the Dynamic Routing table Updates using the Routing Protocol (RIP).

Diagram



Procedure

1. Configuring & Assigning the IP addresses on the routers R1 & R2.
2. Check the routing table on both the routers.
3. Enable the RIP protocol on both routers so that hosts on the both routers can communicate with each other.
4. Verifying the Routing protocols on the Router.
5. Check the routing table on both the routers after enabling the RIP on both sides.
6. Verifying the connection of both hosts.

Configuration

Step 1(A): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R1 as shown in figure.

Step 1(B): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R2 as shown in figure.

Step 2(A): Check the Routing table of the Router R1.

R1#sh ip route

C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 2(B): Check the Routing table of the Router R2.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 3(A): Enable the RIP protocol on the Router R1.

R1(config)#router rip
R1(config-router)#network 10.0.0.0 *(Network to be advertised which is Directly Connected)*
R1(config-router)#network 15.0.0.0 *(Network to be advertised which is Directly Connected)*

Step 3(B): Enable the RIP protocol on the Router R2.

R2(config)#router rip
R2(config-router)#network 20.0.0.0 *(Network to be advertised which is Directly Connected)*
R2(config-router)#network 15.0.0.0 *(Network to be advertised which is Directly Connected)*

Step 4(A): Check the Routing Protocol on the Router R1.

R1#show ip protocols

Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 3 seconds
Invalid after 180 seconds, hold down 180, flushed after 240

Routing for Networks:
10.0.0.0
15.0.0.0
Routing Information Sources:
Gateway Distance Last Update
15.0.0.2 120 00:00:26
Distance: (default is 120)

Step 4(B): Check the Routing Protocol on the Router R2.

R2#show ip protocols

Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 5 seconds
Invalid after 180 seconds, hold down 180, flushed after 240

Routing for Networks:
15.0.0.0

20.0.0.0

Routing Information Sources:

Gateway	Distance	Last Update
15.0.0.1	120	00:00:18

Distance: (default is 120)

Step 5(A): Check the Routing table of the Router R1 after enabling RIP.

R1#sh ip route

R 20.0.0.0/8 [120/1] via 15.0.0.2, 00:00:19, Serial0
C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 5(B): Check the Routing table of the Router R2 after enabling RIP.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
R 10.0.0.0/8 [120/1] via 15.0.0.1, 00:00:22, Serial0
C 15.0.0.0/8 is directly connected, Serial0

Step 6: Verifying the connection of Host 'A' & Host 'B'.

C:\>ping 20.0.0.1

Pinging 20.0.0.1 with 32 bytes of data:

Reply from 20.0.0.1: bytes=32 time=20ms TTL=254
Reply from 20.0.0.1: bytes=32 time=20ms TTL=254
Reply from 20.0.0.1: bytes=32 time=10ms TTL=254
Reply from 20.0.0.1: bytes=32 time=10ms TTL=254

Ping statistics for 20.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 10ms, Maximum = 20ms, Average = 15ms

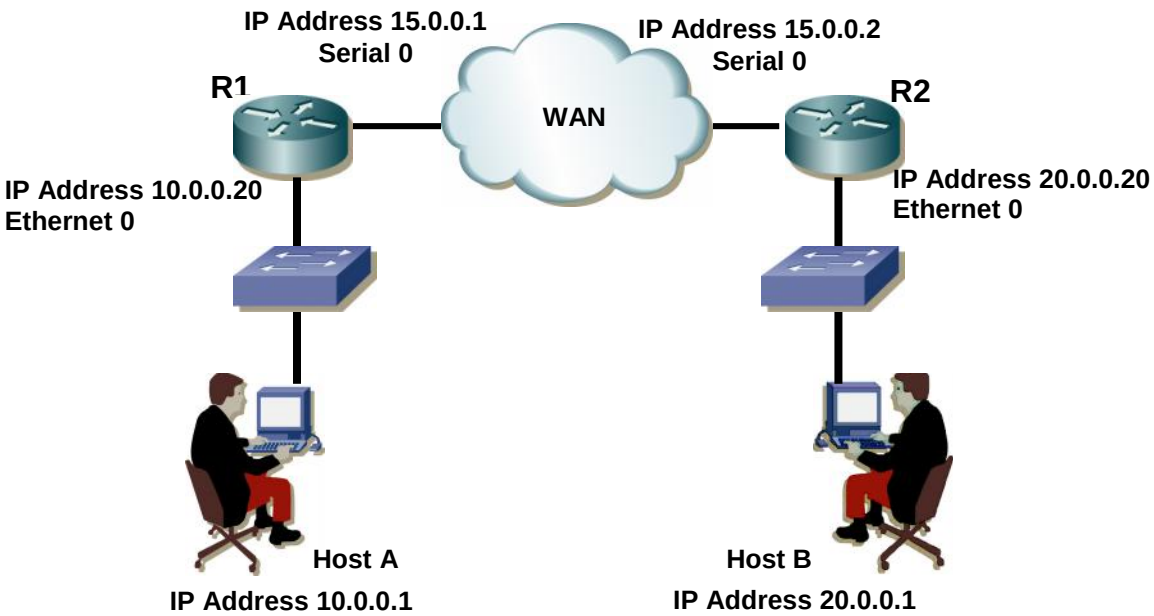
Lab # 8 (ii)

Routing Protocols
(IGRP Configuration)

Objective

Understanding the dynamic Routing table updates using the Interior Gateway Routing Protocol (IGRP).

Diagram



Procedure

1. Configuring & Assigning the IP addresses on the routers R1 & R2.
2. Check the routing table on both the routers.
3. Enable the IGRP protocol on both routers so that hosts on the both routers can communicate with each other.
4. Verifying the Routing protocols on the Router.
5. Check the routing table on both the routers after enabling the IGRP on both sides.
6. Verifying the connection of both hosts.

Configuration

Step 1(A): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R1 as shown in figure.

Step 1(B): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R2 as shown in figure.

Step 2(A): Check the Routing table of the Router R1.

R1#sh ip route

C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 2(B): Check the Routing table of the Router R2.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 3(A): Enable the IGRP protocol on the Router R1.

R1(config)#router igrp 10
R1(config-router)#network 10.0.0.0 *(Network to be advertised which is Directly Connected)*
R1(config-router)#network 15.0.0.0 *(Network to be advertised which is Directly Connected)*

Step 3(B): Enable the IGRP protocol on the Router R2.

R2(config)#router igrp 10
R2(config-router)#network 20.0.0.0 *(Network to be advertised which is Directly Connected)*
R2(config-router)#network 15.0.0.0 *(Network to be advertised which is Directly Connected)*

Step 4(A): Check the Routing Protocol on the Router R1.

R1#show ip protocols

Routing Protocol is "igrp 10"
Sending updates every 90 seconds, next due in 38 seconds
Invalid after 270 seconds, hold down 280, flushed after 630

IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0

IGRP maximum hopcount 100

IGRP maximum metric variance 1

Redistributing: igrp 10
Routing for Networks:
10.0.0.0
15.0.0.0

Routing Information Sources:

Gateway	Distance	Last Update
15.0.0.2	100	00:00:13

Distance: (default is 100)

Step 4(B): Check the Routing Protocol on the Router R2.

R2#show ip protocols

Routing Protocol is "igrp 10"
Sending updates every 90 seconds, next due in 4 seconds
Invalid after 270 seconds, hold down 280, flushed after 630

IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0

IGRP maximum hop count 100

IGRP maximum metric variance 1

Redistributing: igrp 10

Routing for Networks:
15.0.0.0
20.0.0.0

Routing Information Sources:

Gateway	Distance	Last Update
15.0.0.1	100	00:00:32

Distance: (default is 100)

Step 5(A): Check the Routing table of the Router R1 after enabling IGRP.

R1#sh ip route

I 20.0.0.0/8 [100/8576] via 15.0.0.2, 00:01:09, Serial0
C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 5(B): Check the Routing table of the Router R2 after enabling IGRP.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
I 10.0.0.0/8 [100/8576] via 15.0.0.1, 00:01:00, Serial0
C 15.0.0.0/8 is directly connected, Serial0

Step 6: Verifying the connection of Host 'A' & Host 'B'.

C:\>ping 20.0.0.1

Pinging 20.0.0.1 with 32 bytes of data:

Reply from 20.0.0.1: bytes=32 time=20ms TTL=254
Reply from 20.0.0.1: bytes=32 time=20ms TTL=254
Reply from 20.0.0.1: bytes=32 time=10ms TTL=254
Reply from 20.0.0.1: bytes=32 time=10ms TTL=254

Ping statistics for 20.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 10ms, Maximum = 20ms, Average = 15ms

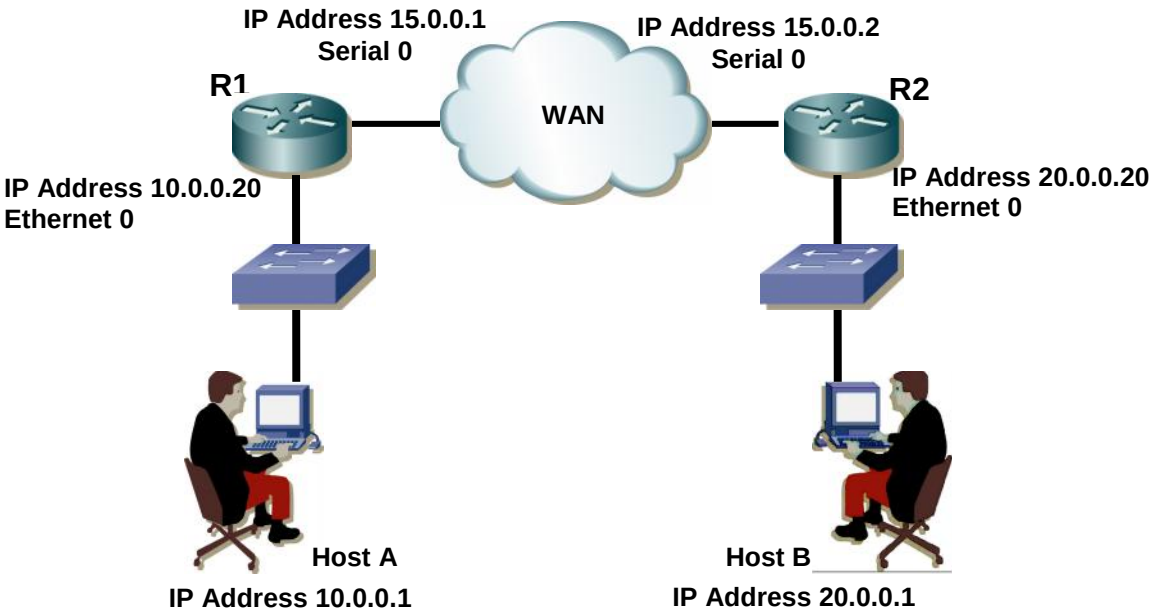
Lab # 8 (iii)

Routing Protocols
(EIGRP Configuration)

Objective

Understanding the Routing Updates processs using Enhanced Interior Gateway Routing Protocol (EIGRP).

Diagram



Procedure

1. Configuring & Assigning the IP addresses on the routers R1 & R2.
2. Check the routing table on both the routers.
3. Enable the EIGRP protocol on both routers so that hosts on the both routers can communicate with each other.
4. Verifying the Routing protocols on the Router.
5. Check the routing table on both the routers after enabling the EIGRP on both sides.
6. Verifying the connection of both hosts.

Configuration

Step 1(A): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R1 as shown in figure.

Step 1(B): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R2 as shown in figure.

Step 2(A): Check the Routing table of the Router R1.

R1#sh ip route

C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 2(B): Check the Routing table of the Router R2.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 3(A): Enable the EIGRP protocol on the Router R1.

R1(config)#router eigrp 10
R1(config-router)#network 10.0.0.0 *(Network to be advertised which is Directly Connected)*
R1(config-router)#network 15.0.0.0 *(Network to be advertised which is Directly Connected)*

Step 3(B): Enable the EIGRP protocol on the Router R2.

R2(config)#router eigrp 10
R2(config-router)#network 20.0.0.0 *(Network to be advertised which is Directly Connected)*
R2(config-router)#network 15.0.0.0 *(Network to be advertised which is Directly Connected)*

Step 4(A): Check the Routing Protocol on the Router R1.

R1#show ip protocols

Routing Protocol is "eigrp 10"

EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0

EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
Redistributing: eigrp 10

Automatic network summarization is in effect
Automatic address summarization:
15.0.0.0/8 for Ethernet0

Routing for Networks:
10.0.0.0
15.0.0.0

Routing Information Sources:

Gateway	Distance	Last Update
15.0.0.2	90	00:01:06

Distance: internal 90 external 170

Step 4(B): Check the Routing Protocol on the Router R2.

R2#show ip protocols

Routing Protocol is "eigrp 10"

EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0

EIGRP maximum hopcount 100

EIGRP maximum metric variance 1

Redistributing: eigrp 10

Automatic network summarization is in effect

Automatic address summarization:
15.0.0.0/8 for Ethernet0
20.0.0.0/8 for Serial0
Routing for Networks:
15.0.0.0
20.0.0.0
Routing Information Sources:

Gateway	Distance	Last Update
15.0.0.1	90	00:02:47

Distance: internal 90 external 170

Step 5(A): Check the Routing table of the Router R1 after enabling EIGRP.

R1#sh ip route

D 20.0.0.0/8 [90/2195456] via 15.0.0.2, 00:04:42, Serial0
C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 5(B): Check the Routing table of the Router R2 after enabling EIGRP.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
D 10.0.0.0/8 [90/2195456] via 15.0.0.1, 00:01:12, Serial0
C 15.0.0.0/8 is directly connected, Serial0

Step 6: Verifying the connection of Host 'A' & Host 'B'.

C:\>ping 20.0.0.1

Pinging 20.0.0.1 with 32 bytes of data:

Reply from 20.0.0.1: bytes=32 time=20ms TTL=254
Reply from 20.0.0.1: bytes=32 time=20ms TTL=254
Reply from 20.0.0.1: bytes=32 time=10ms TTL=254
Reply from 20.0.0.1: bytes=32 time=10ms TTL=254

Ping statistics for 20.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 10ms, Maximum = 20ms, Average = 15ms

Lab # 8 (iv)

Routing Protocols

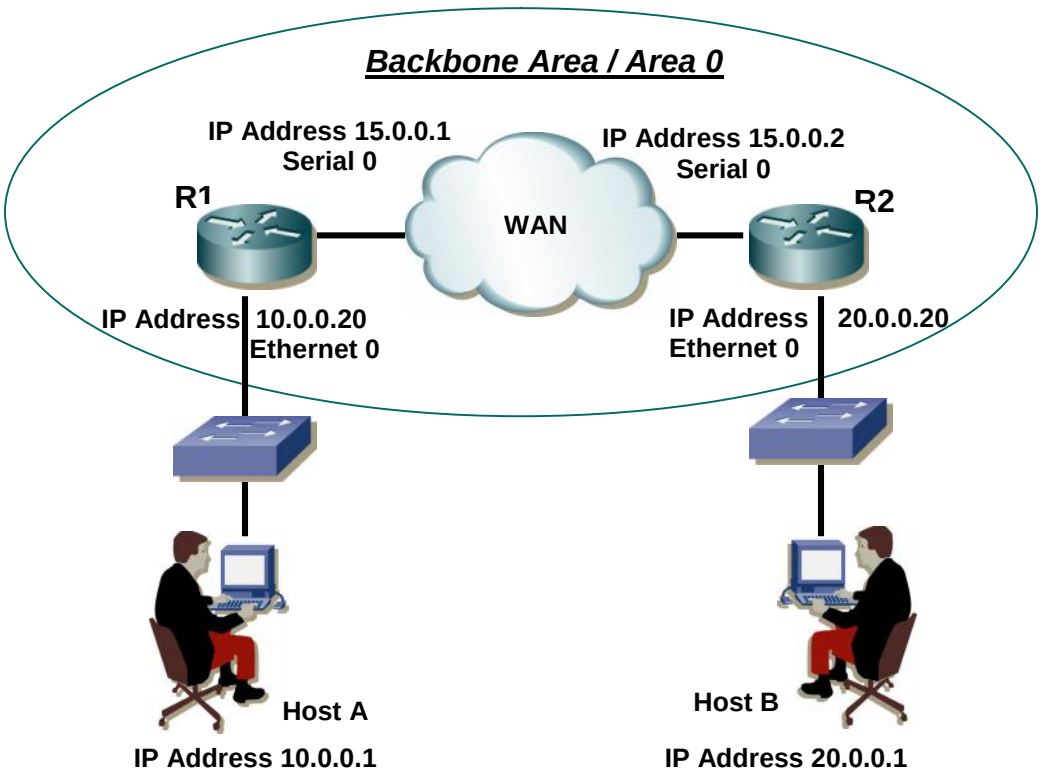
(OSPF)

Single Area Configuration

Objective

Understanding the Routing Updates process using the Open Shortest Path First (OSPF) in a single area.

Diagram



Procedure

1. Configuring & Assigning the IP addresses on the routers R1 & R2.
2. Check the routing table on both the routers.
3. Enable the OSPF protocol on both routers so that hosts on the both routers can communicate with each other.
4. Verifying the Routing protocols on the Router.
5. Check the routing table on both the routers after enabling the OSPF on both sides.
6. Verifying the OSPF neighbors on the routers.
7. Verifying the OSPF interfaces on the routers.
8. Verifying the OSPF database on the routers.
9. Verifying the connection of both hosts.

Configuration

Step 1(A): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R1 as shown in figure.

Step 1(B): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R2 as shown in figure.

Step 2(A): Check the Routing table of the Router R1.

R1#sh ip route

C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 2(B): Check the Routing table of the Router R2.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 3(A): Enable the OSPF protocol on the Router R1.

R1(config)#router ospf 64
R1(config-router)#network 10.0.0.0 0.255.255.255 area 0
(Directly Connected Network, its Wild card mask, & area ID)
R1(config-router)#network 15.0.0.0 0.255.255.255 area 0
(Directly Connected Network, its Wild card mask, & area ID)

Step 3(B): Enable the OSPF protocol on the Router R2.

R2(config)#router ospf 65
R2(config-router)#network 15.0.0.0 0.255.255.255 area 0
(Directly Connected Network, its Wild card mask, & area ID)

R2(config-router)#network 20.0.0.0 0.255.255.255 area 0
(Directly Connected Network, its Wild card mask, & area ID)

Step 4(A): Check the Routing Protocol on the Router R1.

R1#show ip protocols

Routing Protocol is "ospf 64"
Redistributing: ospf 64
Routing for Networks:
10.0.0.0
15.0.0.0
Routing Information Sources:
Gateway Distance Last Update
20.0.0.20 110 00:10:52
Distance: (default is 110)

Step 4(B): Check the Routing Protocol on the Router R2.

R2#show ip protocols

Routing Protocol is "ospf 65"
Redistributing: ospf 64
Routing for Networks:

15.0.0.0
20.0.0.0
Routing Information Sources:
Gateway Distance Last Update
15.0.0.1 110 00:12:17
Distance: (default is 110)

Step 5(A): Check the Routing table of the Router R1 after enabling OSPF.

R1#sh ip route

O 20.0.0.0/8 [110/74] via 15.0.0.2, 00:22:17, Serial0
C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 5(B): Check the Routing table of the Router R2 after enabling OSPF.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
O 10.0.0.0/8 [110/74] via 15.0.0.1, 00:20:57, Serial0
C 15.0.0.0/8 is directly connected, Serial0

Step 6: Verifying the OSPF neighbors on the Router

R#show ip ospf neighbor

Step 7: Verifying the OSPF interfaces on the Router

R#show ip ospf interface

Step 8: Verifying the OSPF database on the Router

R1#show ip ospf database

Step 9: Verifying the connection of Host 'A' & Host 'B'.

C:\>ping 20.0.0.1

Pinging 20.0.0.1 with 32 bytes of data:

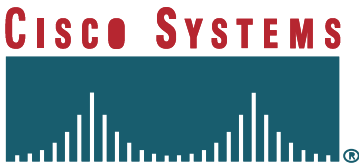
Reply from 20.0.0.1: bytes=32 time=20ms TTL=254
Reply from 20.0.0.1: bytes=32 time=20ms TTL=254
Reply from 20.0.0.1: bytes=32 time=10ms TTL=254
Reply from 20.0.0.1: bytes=32 time=10ms TTL=254

Ping statistics for 20.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 10ms, Maximum = 20ms, Average = 15ms

Section 3

IP Traffic Management

Etronics Solution Provider



By **M. Irfan Ghauri**
M. Rizwan

Lab # 9

Access Control List

Objective

Understanding the Packet Filtering capabilities of Router. Router can pass or filter the ip traffic as per required.

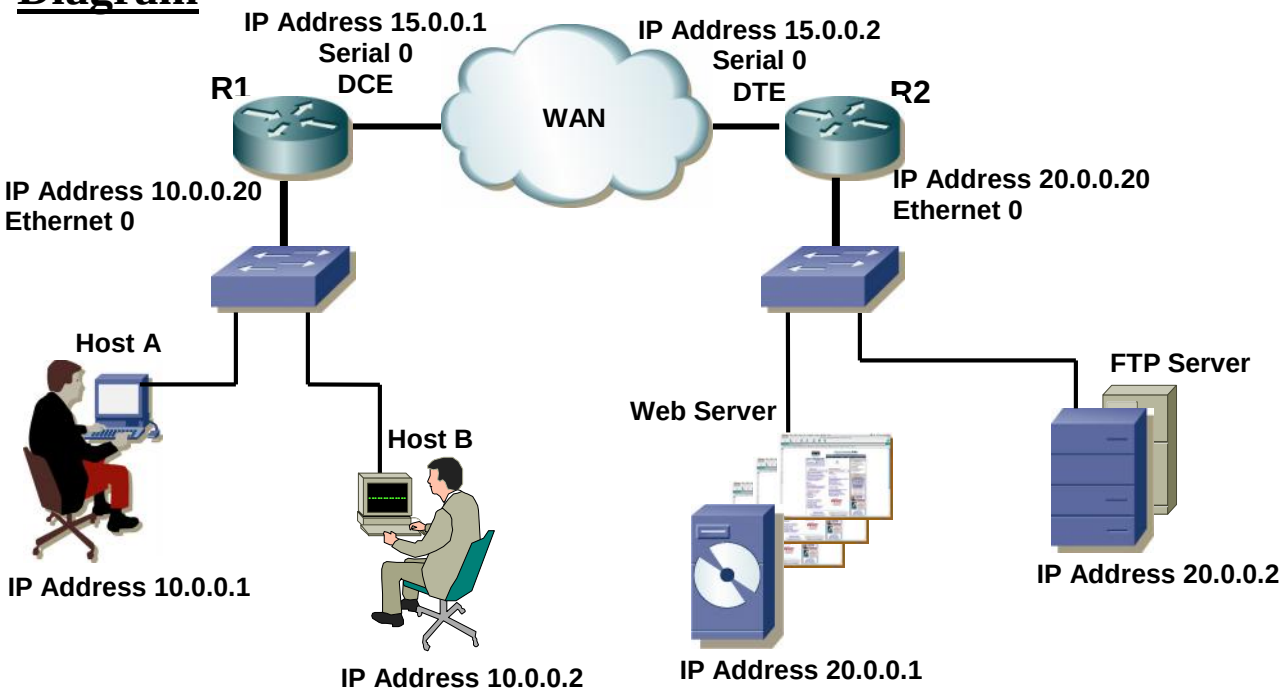
The demonstrations include:

1. Standard Access List (1-99).
2. Extended Access List (100-199).

i. STANDARD ACL

- Standard IP lists (1-99) test conditions of all IP packets from source addresses.
- In this lab scenario, initially both the Hosts 'A' & 'B' are accessing the Web & Ftp services but then apply the Standard ACL so that the Host 'A' could not access the Web & Ftp Services.
- It is recommended that place the Standard ACL near the destination.

Diagram



Procedure

1. Configuring & Assigning the IP addresses on the routers R1 & R2.
2. Check the routing table on both the routers.
3. Enable the routing protocol on both routers so that hosts on the both routers can communicate with each other.
4. Check the routing table on both the routers after enabling the routing protocol on both sides.
5. Make a web server & ftp server.
6. Verifying the access of web server & ftp server by the hosts A & B respectively.
7. Apply the Standard ACL on the router R1, so that Host A can not access these services.
8. Verifying the Standard ACL by accessing the web & ftp server from Host A.

Configuration

Step 1(A): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R1 as shown in figure.

Step 1(B): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R2 as shown in figure.

Step 2(A): Check the Routing table of the Router R1.

R1#sh ip route

C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 2(B): Check the Routing table of the Router R2.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 3(A): Enable the RIP protocol on the Router R1.

R1(config)#router rip
R1(config-router)#network 10.0.0.0 *(Network to be advertised which is Directly Connected)*
R1(config-router)#network 15.0.0.0 *(Network to be advertised which is Directly Connected)*

Step 3(B): Enable the RIP protocol on the Router R2.

R2(config)#router rip
R2(config-router)#network 20.0.0.0 *(Network to be advertised which is Directly Connected)*
R2(config-router)#network 15.0.0.0 *(Network to be advertised which is Directly Connected)*

Step 4(A): Check the Routing table of the Router R1 after enabling RIP.

R1#sh ip route

R 20.0.0.0/8 [120/1] via 15.0.0.2, 00:04:42, Serial0
C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 4(B): Check the Routing table of the Router R2 after enabling RIP.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
R 10.0.0.0/8 [120/1] via 15.0.0.1, 00:01:12, Serial0
C 15.0.0.0/8 is directly connected, Serial0

Step 5(A): Make a Web Server.

1. Make a Web Page & Save it on Desktop.
2. Go to Start Button > All Programs > Administrative Tool > Internet Service Manager
3. Right Click on the Computer name & goes to New tab > Web Site.
4. Follow the wizard and make the Web Server.

Step 5(B): Make a Ftp Server.

1. Make a Web Page & Save it on Desktop.
2. Go to Start Button > All Programs > Administrative Tool > Internet Service Manager
3. Right Click on the Computer name & goes to New tab > FTP Site.
4. Follow the wizard and make the FTP Server.

Step 6(A): Verifying the Access of Web Server on Host 'A' by giving (http://20.0.0.1) in the Address bar of Internet explorer.

(Host A will be accessing Web Server)

Step 6(B): **Verifying the Access of Ftp Server by the Host 'A' by giving (ftp://20.0.0.1) in the Address bar of Internet explorer.**

(Host A will be accessing FTP Server)

Step 6(C): **Verifying the Access of Web Server on Host 'B' by giving (http://20.0.0.1) in the Address bar of Internet explorer.**

(Host B will be accessing Web Server)

Step 6(D): **Verifying the Access of Ftp Server by the Host 'B' by giving (ftp://20.0.0.1) in the Address bar of Internet explorer.**

(Host B will be accessing FTP Server)

Step 7(A): **Make the Standard ACL on the Router R1 so that Host A can not accesses the Web & Ftp Server.**

```
R1(config)#access-list 10 deny host 10.0.0.1
R1(config)#access-list 10 permit any
```

Step 7(B): **Apply the Standard ACL on the Router (R1) Serial Interface.**

```
R1(config)#interface serial 0
R1(config-if)#ip access-group 10 out
```

Step 8(A): **Verifying the Standard ACL from Host 'A' by accessing Web Server.**

(Host A won't be accessing Web Server)

Step 8(B): **Verifying the Standard ACL from Host 'A' by accessing FTP Server.**

(Host A won't be accessing FTP Server)

Step 8(C): **Verifying the Standard ACL from Host 'B' by accessing Web Server.**

(Host B will be accessing Web Server)

Step 8(D): Verifying the Standard ACL from Host 'B' by accessing FTP Server.

(Host B will be accessing FTP Server)

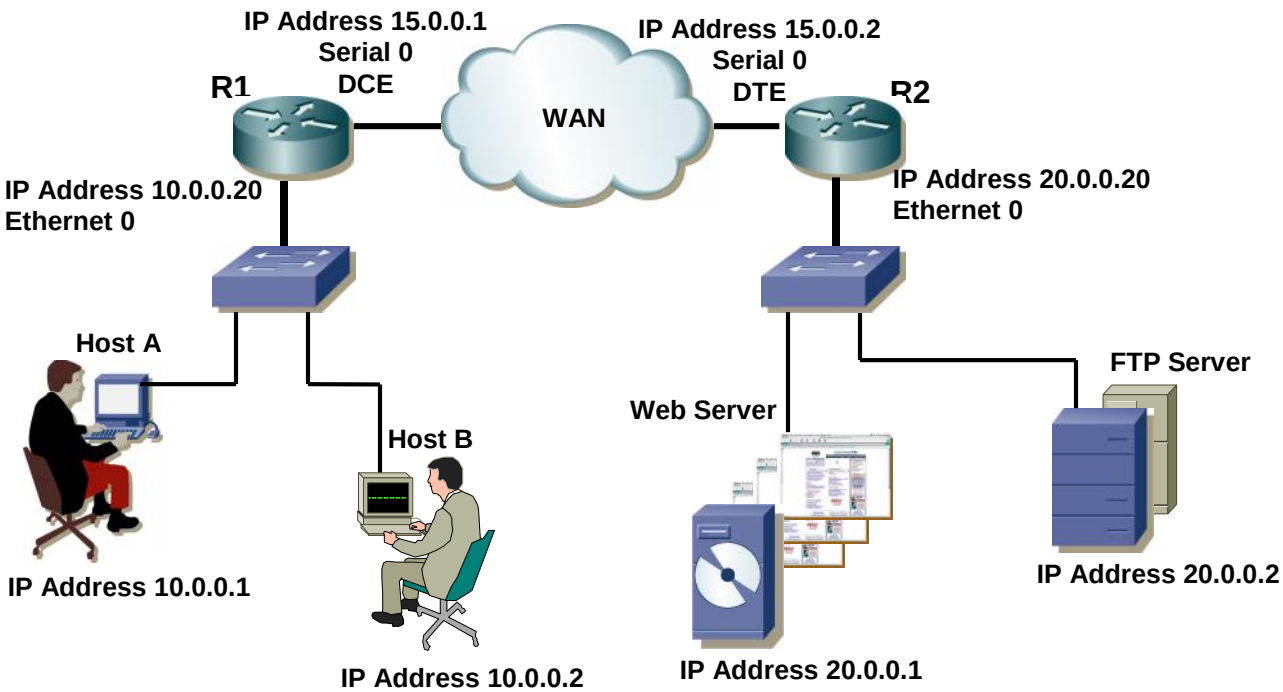
ii. EXTENDED ACL

Extended IP lists (100-199) test conditions of source and destination addresses, specific TCP/IP protocols, and destination ports.

In this lab scenario, initially both the Hosts 'A' & 'B' are accessing the Web & Ftp services but then apply the Extended ACL in such a way that Host 'A' can be access only the web services & and Host 'B' could be access the Ftp Services only.

It is recommended that place the Extended ACL near the source.

Diagram



Procedure

1. Configuring & Assigning the IP addresses on the routers R1 & R2.
2. Check the routing table on both the routers.
3. Enable the routing protocol on both routers so that hosts on the both routers can communicate with each other.
4. Check the routing table on both the routers after enabling the routing protocol on both sides.
5. Make a web server & ftp server.
6. Verifying the access of web server & ftp server by the hosts A & B respectively.
7. Make & Apply the Extended ACL on the router R1, so that Host 'A' can not access the Web services & Host 'B' can not access the Ftp services.
8. Verifying the ACL by accessing the Web & Ftp services from Host A & Host 'B'.

Configuration

Step 1(A): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R1 as shown in figure.

Step 1(B): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R2 as shown in figure.

Step 2(A): Check the Routing table of the Router R1.

R1#sh ip route

C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 2(B): Check the Routing table of the Router R2.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 3(A): Enable the RIP protocol on the Router R1.

R1(config)#router rip
R1(config-router)#network 10.0.0.0 *(Network to be advertised which is Directly Connected)*
R1(config-router)#network 15.0.0.0 *(Network to be advertised which is Directly Connected)*

Step 3(B): Enable the RIP protocol on the Router R2.

R2(config)#router rip
R2(config-router)#network 20.0.0.0 *(Network to be advertised which is Directly Connected)*
R2(config-router)#network 15.0.0.0 *(Network to be advertised which is Directly Connected)*

Step 4(A): Check the Routing table of the Router R1 after enabling RIP.

R1#sh ip route

R 20.0.0.0/8 [120/1] via 15.0.0.2, 00:04:42, Serial0
C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 4(B): Check the Routing table of the Router R2 after enabling RIP.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
R 10.0.0.0/8 [120/1] via 15.0.0.1, 00:01:12, Serial0
C 15.0.0.0/8 is directly connected, Serial0

Step 5(A): Make a Web Server.

5. Make a Web Page & Save it on Desktop.
6. Go to Start Button > All Programs > Administrative Tool > Internet Service Manager
7. Right Click on the Computer name & goes to New tab > Web Site.
8. Follow the wizard and make the Web Server.

Step 5(B): Make a Ftp Server.

5. Make a Web Page & Save it on Desktop.
6. Go to Start Button > All Programs > Administrative Tool > Internet Service Manager
7. Right Click on the Computer name & goes to New tab > FTP Site.
8. Follow the wizard and make the FTP Server.

Step 6(A): Verifying the Access of Web Server on Host 'A' by giving (http://20.0.0.1) in the Address bar of Internet explorer.

(Host A will be accessing Web Server)

Step 6(B): Verifying the Access of Ftp Server by the Host 'A' by giving (ftp://20.0.0.1) in the Address bar of Internet explorer.

(Host A will be accessing FTP Server)

Step 6(C): Verifying the Access of Web Server on Host 'B' by giving (http://20.0.0.1) in the Address bar of Internet explorer.

(Host B will be accessing Web Server)

Step 6(D): Verifying the Access of Ftp Server by the Host 'B' by giving (ftp://20.0.0.1) in the Address bar of Internet explorer.

(Host B will be accessing FTP Server)

Step 7(A): Make the Extended ACL on the Router R1 so that Host A can not access the Web Server & Host 'B' can not access the Ftp Server.

```
R1(config)#access-list 110 deny tcp host 10.0.0.1 host 20.0.0.1 eq www
R1(config)#access-list 110 deny tcp host 10.0.0.2 host 20.0.0.2 eq ftp
R1(config)#access-list 110 permit ip any any
```

Step 7(B): Apply the Extended ACL on the Router (R1) Ethernet Interface.

```
R1(config)#interface Ethernet 0
R1(config-if)#ip access-group 110 in
```

Step 8(A): Verifying the Extended ACL from Host 'A' by accessing Web Server.

(Host A won't be accessing Web Server)

Step 8(B): Verifying the Extended ACL from Host 'A' by accessing FTP Server.

(Host A will be accessing FTP Server)

Step 8(C): Verifying the Extended ACL from Host 'B' by accessing Web Server.

(Host B will be accessing Web Server)

Step 8(D): Verifying the Extended ACL from Host 'B' by accessing FTP Server.

(Host B won't be accessing FTP Server)

Lab # 10 (i)

Network Address Translation

(NAT)

Objective

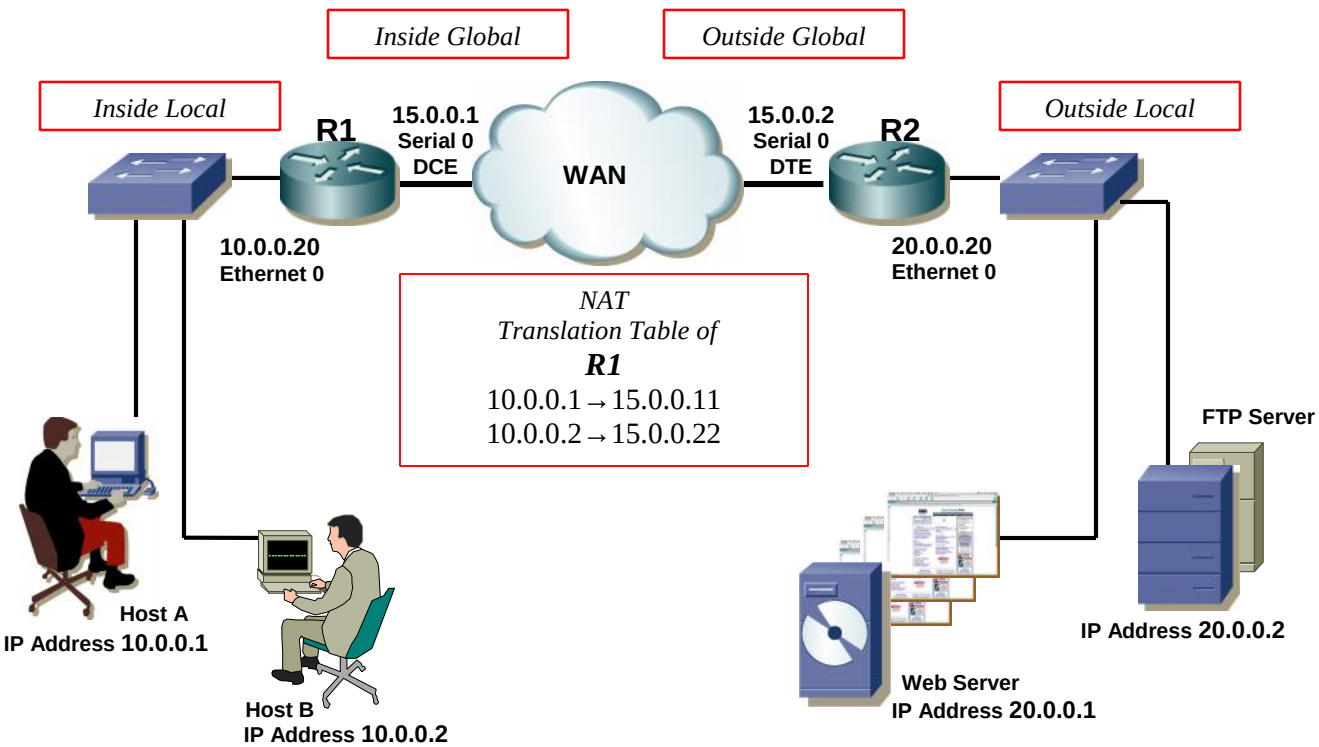
Understanding the operation of Network Address Translation.

1. Static NAT. 2. Dynamic NAT. 3.Overload NAT (PAT)

i. STATIC NAT

In the Static NAT, we map the 1 Private IP Address to 1 reserved Public IP Address.

Diagram



By **M. Irfan Ghauri**
M. Rizwan

Procedure

1. Configuring & Assigning the IP addresses on the routers R1 & R2.
2. Check the routing table on both the routers.
3. Enable the routing protocol on both routers so that hosts on the both routers can communicate with each other.
4. Check the routing table on both the routers after enabling the routing protocol on both sides.
5. Make web & FTP servers.
6. Establishes Static NAT Translation between an inside local address and an inside global address.
7. Marks the interface as connected to the inside & outside networks.
8. Verifying the Standard Static NAT Translation by commands.

Configuration

Step 1(A): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R1 as shown in figure.

Step 1(B): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R2 as shown in figure.

Step 2(A): Check the Routing table of the Router R1.

R1#sh ip route

C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 2(B): Check the Routing table of the Router R2.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 3(A): Enable the RIP protocol on the Router R1.

R1(config)#router rip
R1(config-router)#network 10.0.0.0 *(Network to be advertised which is Directly Connected)*
R1(config-router)#network 15.0.0.0 *(Network to be advertised which is Directly Connected)*

Step 3(B): Enable the RIP protocol on the Router R2.

R2(config)#router rip
R2(config-router)#network 20.0.0.0 *(Network to be advertised which is Directly Connected)*
R2(config-router)#network 15.0.0.0 *(Network to be advertised which is Directly Connected)*

Step 4(A): Check the Routing table of the Router R1 after enabling RIP.

R1#sh ip route

R 20.0.0.0/8 [120/1] via 15.0.0.2, 00:04:42, Serial0
C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 4(B): Check the Routing table of the Router R2 after enabling RIP.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
R 10.0.0.0/8 [120/1] via 15.0.0.1, 00:01:12, Serial0
C 15.0.0.0/8 is directly connected, Serial0

Step 5(A): Make a Web Server.

1. Make a Web Page & Save it on Desktop.
2. Go to Start Button > All Programs > Administrative Tool > Internet Service Manager
3. Right Click on the Computer name & go to New tab > Web Site.
4. Follow the wizard and make the Web Server.

Step 5(B): Make a Ftp Server.

1. Make a Web Page & Save it on Desktop.
2. Go to Start Button > All Programs > Administrative Tool > Internet Service Manager
3. Right Click on the Computer name & go to New tab > FTP Site.
4. Follow the wizard and make the FTP Server.

Step 6: Establishes Static NAT Translation between an inside local address and an inside global address.

R1(config)#ip nat inside source static 10.0.0.1 15.0.0.11
R1(config)#ip nat inside source static 10.0.0.2 15.0.0.22

Step 7(A): Marks the interface as connected to the Inside Network.

R1(config)#int Ethernet 0
R1(config-if)#ip nat inside

Step 7(B): Marks the interface as connected to the Outside Network.

R1(config)#int serial 0
R1(config-if)#ip nat outside

Step 8(A): Verifying the Static NAT Translation on Router R1 by translation table command.

R1#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	**15.0.0.11**	**10.0.0.1**	---	---
---	**15.0.0.22**	**10.0.0.2**	---	---

Step 8(B): Verifying the Static NAT Translation on Router R1 by debug.

R1#debug ip nat
IP NAT debugging is on

When Host 'A' pings to web server:

00:19:01: NAT: s=10.0.0.1->15.0.0.11, d=20.0.0.1 [34]
00:19:01: NAT*: s=20.0.0.1, d=15.0.0.11->10.0.0.1 [34]

00:19:01: NAT: s=10.0.0.1->15.0.0.11, d=20.0.0.1 [35]
00:19:01: NAT*: s=20.0.0.1, d=15.0.0.11->10.0.0.1 [35]

00:19:01: NAT: s=10.0.0.1->15.0.0.11, d=20.0.0.1 [36]
00:19:01: NAT*: s=20.0.0.1, d=15.0.0.11->10.0.0.1 [36]

When Host 'B' pings to web server:

00:19:01: NAT: s=10.0.0.2->15.0.0.22, d=20.0.0.1 [37]
00:19:01: NAT*: s=20.0.0.1, d=15.0.0.22->10.0.0.2 [37]

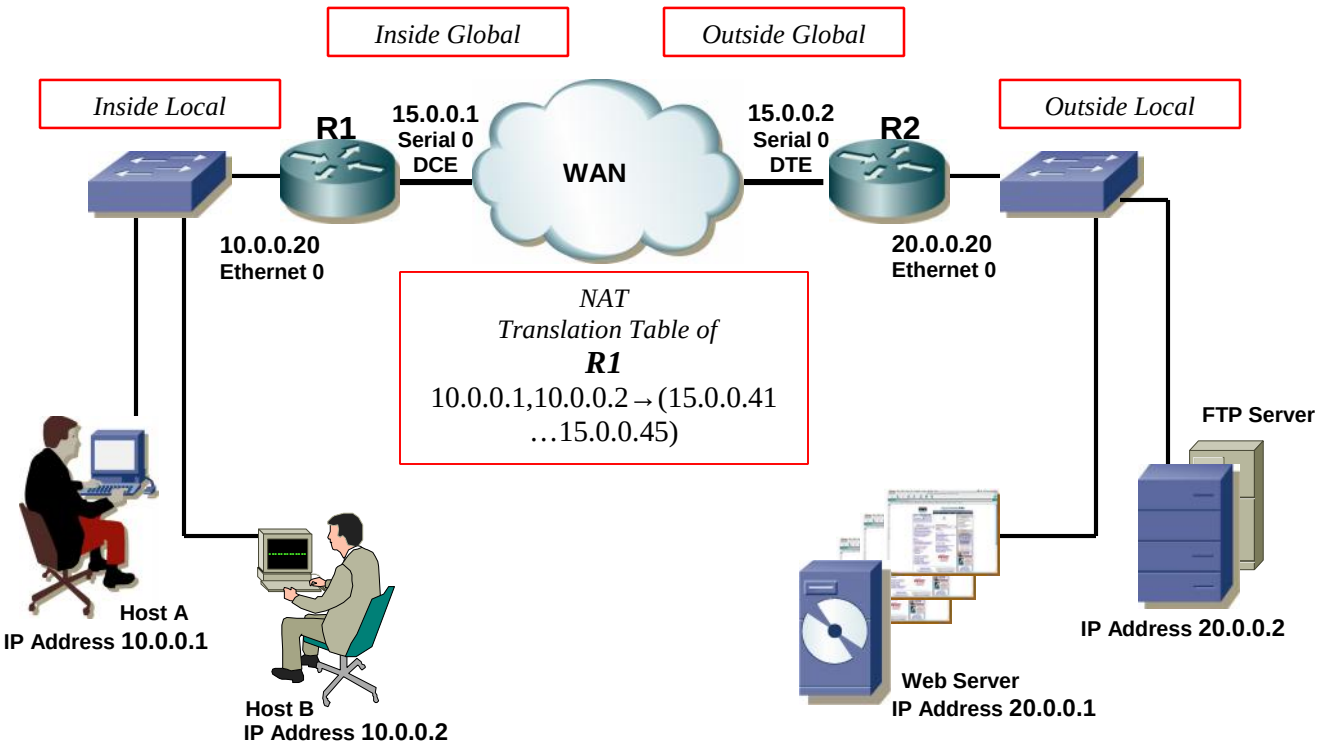
00:19:01: NAT: s=10.0.0.2->15.0.0.22, d=20.0.0.1 [38]
00:19:01: NAT*: s=20.0.0.1, d=15.0.0.22->10.0.0.2 [38]

00:19:01: NAT: s=10.0.0.2->15.0.0.22, d=20.0.0.1 [39]
00:19:01: NAT*: s=20.0.0.1, d=15.0.0.22->10.0.0.2 [39]

ii. Dynamic NAT

In the Dynamic NAT, we map the many Private IP Addresses to many Public IP Address.

Diagram



Procedure

1. Configuring & Assigning the IP addresses on the routers R1 & R2.
2. Check the routing table on both the routers.
3. Enable the routing protocol on both routers so that hosts on the both routers can communicate with each other.

4. Check the routing table on both the routers after enabling the routing protocol on both sides.
5. Make web & FTP servers.
6. Defines a pool of global addresses to be allocated as needed.
7. Defines a standard IP access list permitting those inside local addresses that are to be translated.
8. Establishes dynamic source translation, specifying the access list defined in the prior step.
9. Marks the interface as connected to the inside & outside networks.
10. Verifying the Standard Dynamic translation by commands.

Configuration

Step 1(A): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R1 as shown in figure.

Step 1(B): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R2 as shown in figure.

Step 2(A): Check the Routing table of the Router R1.

R1#sh ip route

C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 2(B): Check the Routing table of the Router R2.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 3(A): Enable the RIP protocol on the Router R1.

R1(config)#router rip
R1(config-router)#network 10.0.0.0 *(Network to be advertised which is Directly Connected)*
R1(config-router)#network 15.0.0.0 *(Network to be advertised which is Directly Connected)*

Step 3(B): Enable the RIP protocol on the Router R2.

R2(config)#router rip
R2(config-router)#network 20.0.0.0 *(Network to be advertised which is Directly Connected)*
R2(config-router)#network 15.0.0.0 *(Network to be advertised which is Directly Connected)*

Step 4(A): Check the Routing table of the Router R1 after enabling RIP.

R1#sh ip route

R 20.0.0.0/8 [120/1] via 15.0.0.2, 00:04:42, Serial0
C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 4(B): Check the Routing table of the Router R2 after enabling RIP.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
R 10.0.0.0/8 [120/1] via 15.0.0.1, 00:01:12, Serial0
C 15.0.0.0/8 is directly connected, Serial0

Step 5(A): Make a Web Server.

1. Make a Web Page & Save it on Desktop.
2. Go to Start Button > All Programs > Administrative Tool > Internet Service Manager
3. Right Click on the Computer name & goes to New tab > Web Site.
4. Follow the wizard and make the Web Server.

Step 5(B): Make a Ftp Server.

1. Make a Web Page & Save it on Desktop.
2. Go to Start Button > All Programs > Administrative Tool > Internet Service Manager
3. Right Click on the Computer name & go to New tab > FTP Site.
4. Follow the wizard and make the FTP Server.

Step 6: Defines a pool of global addresses to be allocated as needed.

R1(config)#ip nat pool abc 15.0.0.41 15.0.0.45 netmask 255.0.0.0

Step 7: Defines a standard IP access list permitting those inside local addresses that are to be translated.

R1(config)#access-list 1 permit 10.0.0.0 0.255.255.255

Step 8: Establishes dynamic source translation, specifying the access list defined in the prior step.

R1(config)#ip nat inside source list 1 pool abc

Step 9(A): Marks the interface as connected to the Inside Network.

R1(config)#int Ethernet 0
R1(config-if)#ip nat inside

Step 9(B): Marks the interface as connected to the Outside Network.

R1(config)#int serial 0
R1(config-if)#ip nat outside

Step 10(A): Verifying the Dynamic NAT Translation on Router R1 by debugging command.

R1#debug ip nat
IP NAT debugging is on

When Host 'A' pings to web server:

00:19:01: NAT: s=10.0.0.1->15.0.0.41, d=20.0.0.1 [34]
00:19:01: NAT*: s=20.0.0.1, d=15.0.0.41->10.0.0.1 [34]

00:19:01: NAT: s=10.0.0.1->15.0.0.41, d=20.0.0.1 [35]
00:19:01: NAT*: s=20.0.0.1, d=15.0.0.41->10.0.0.1 [35]

00:19:01: NAT: s=10.0.0.1->15.0.0.41, d=20.0.0.1 [36]
00:19:01: NAT*: s=20.0.0.1, d=15.0.0.41->10.0.0.1 [36]

When Host 'B' pings to web server:

00:19:01: NAT: s=10.0.0.2->15.0.0.42, d=20.0.0.1 [37]
00:19:01: NAT*: s=20.0.0.1, d=15.0.0.42->10.0.0.2 [37]

00:19:01: NAT: s=10.0.0.2->15.0.0.42, d=20.0.0.1 [38]
00:19:01: NAT*: s=20.0.0.1, d=15.0.0.42->10.0.0.2 [38]

00:19:01: NAT: s=10.0.0.2->15.0.0.42, d=20.0.0.1 [39]
00:19:01: NAT*: s=20.0.0.1, d=15.0.0.42->10.0.0.2 [39]

Step 10(B): Verifying the Dynamic NAT Translation on Router R1 by translation table.

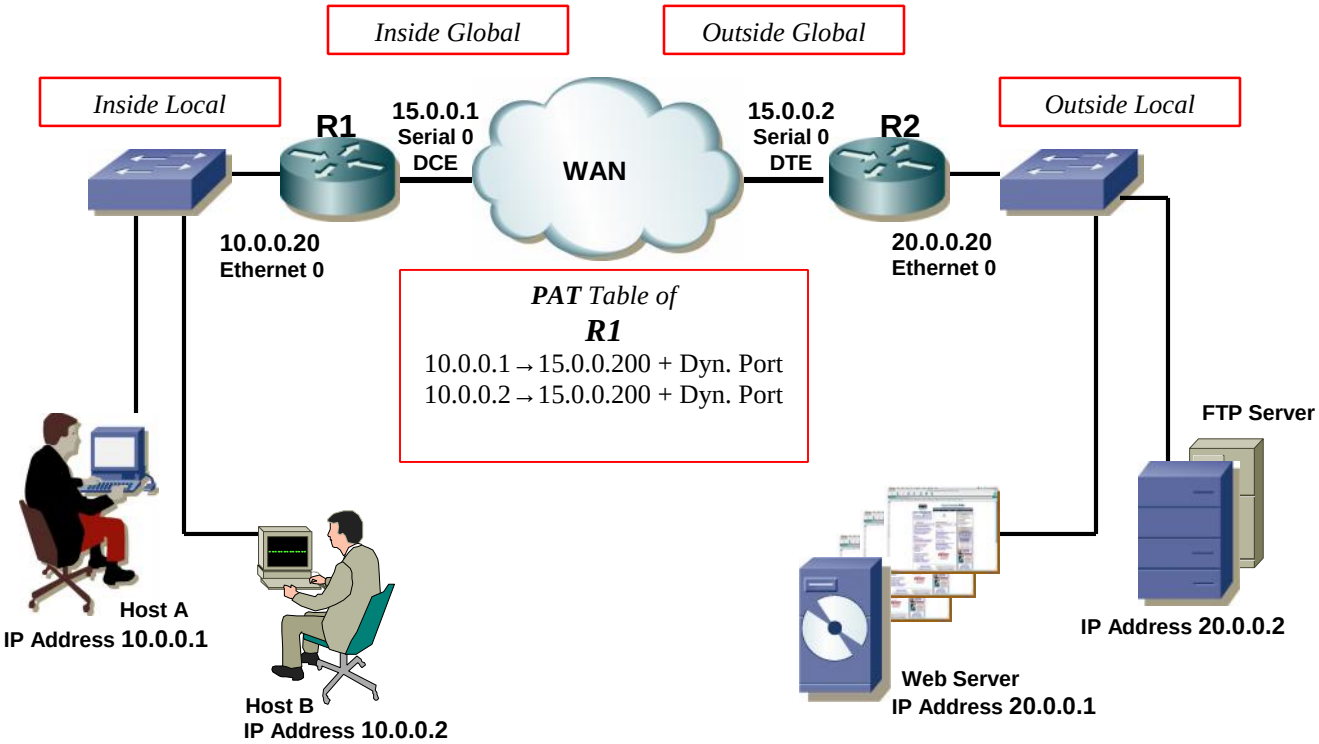
R1#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	**15.0.0.41**	**10.0.0.1**	---	---
---	**15.0.0.42**	**10.0.0.2**	---	---

iii. Overload NAT (PAT)

In the Overload NAT, we map the many Private IP Addresses to 1 Public IP Address.

Diagram



Procedure

1. Configuring & Assigning the IP addresses on the routers R1 & R2.
2. Check the routing table on both the routers.
3. Enable the routing protocol on both routers so that hosts on the both routers can communicate with each other.

4. Check the routing table on both the routers after enabling the routing protocol on both sides.
5. Make web & FTP servers.
6. Defines a pool of global addresses to be allocated as needed.
7. Defines a standard IP access list permitting those inside local addresses that are to be translated.
8. Establishes dynamic source translation, specifying the access list defined in the prior step along with the keyword ***"overload"***.
9. Marks the interface as connected to the inside & outside networks.
10. Verifying the Standard Dynamic translation by commands.

Configuration

Step 1(A): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R1 as shown in figure.

Step 1(B): Assigning the IP addresses on the Ethernet & Serial Interfaces of Router R2 as shown in figure.

Step 2(A): Check the Routing table of the Router R1.

R1#sh ip route

C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 2(B): Check the Routing table of the Router R2.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 3(A): Enable the RIP protocol on the Router R1.

R1(config)#router rip
R1(config-router)#network 10.0.0.0 *(Network to be advertised which is Directly Connected)*
R1(config-router)#network 15.0.0.0 *(Network to be advertised which is Directly Connected)*

Step 3(B): Enable the RIP protocol on the Router R2.

R2(config)#router rip
R2(config-router)#network 20.0.0.0 *(Network to be advertised which is Directly Connected)*
R2(config-router)#network 15.0.0.0 *(Network to be advertised which is Directly Connected)*

Step 4(A): Check the Routing table of the Router R1 after enabling RIP.

R1#sh ip route

R 20.0.0.0/8 [120/1] via 15.0.0.2, 00:04:42, Serial0
C 10.0.0.0/8 is directly connected, Ethernet0
C 15.0.0.0/8 is directly connected, Serial0

Step 4(B): Check the Routing table of the Router R2 after enabling RIP.

R2#sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0
R 10.0.0.0/8 [120/1] via 15.0.0.1, 00:01:12, Serial0
C 15.0.0.0/8 is directly connected, Serial0

Step 5(A): Make a Web Server.

1. Make a Web Page & Save it on Desktop.
2. Go to Start Button > All Programs > Administrative Tool > Internet Service Manager
3. Right Click on the Computer name & go to New tab > Web Site.
4. Follow the wizard and make the Web Server.

Step 5(B): Make a Ftp Server.

1. Make a Web Page & Save it on Desktop.
2. Go to Start Button > All Programs > Administrative Tool > Internet Service Manager
3. Right Click on the Computer name & go to New tab > FTP Site.
4. Follow the wizard and make the FTP Server.

Step 6: Defines a pool of global addresses to be allocated as needed.

R1(config)#ip nat pool abc 15.0.0.200 15.0.0.200 netmask 255.0.0.0

Step 7: Defines a standard IP access list permitting those inside local addresses that are to be translated.

R1(config)#access-list 1 permit 10.0.0.0 0.255.255.255

Step 8: Establishes dynamic source translation, specifying the access list defined in the prior step.

R1(config)#ip nat inside source list 1 pool abc overload

Step 9(A): Marks the interface as connected to the Inside Network.

R1(config)#int Ethernet 0
R1(config-if)#ip nat inside

Step 9(B): Marks the interface as connected to the Outside Network.

R1(config)#int serial 0
R1(config-if)#ip nat outside

Step 10(A): Verifying the Dynamic NAT Translation on Router R1 by debugging command.

R1#debug ip nat
IP NAT debugging is on

When Host 'A' pings to web server:

00:38:03: NAT: s=10.0.0.1->15.0.0.200, d=20.0.0.1 [440]
00:38:03: NAT: s=20.0.0.1, d=15.0.0.200->10.0.0.1 [406]

00:38:03: NAT*: s=10.0.0.1->15.0.0.200, d=20.0.0.1 [442]
00:38:03: NAT*: s=20.0.0.1, d=15.0.0.200->10.0.0.1 [407]

00:38:03: NAT*: s=10.0.0.1->15.0.0.200, d=20.0.0.1 [443]
00:38:04: NAT*: s=20.0.0.1, d=15.0.0.200->10.0.0.1 [408]

00:38:05: NAT*: s=10.0.0.1->15.0.0.200, d=20.0.0.1 [445]
00:38:06: NAT*: s=20.0.0.1, d=15.0.0.200->10.0.0.1 [409]

When Host 'B' pings to web server:

00:38:34: NAT*: s=10.0.0.2->15.0.0.200, d=20.0.0.1 [499]
00:38:34: NAT*: s=20.0.0.1, d=15.0.0.200->10.0.0.2 [415]

00:38:34: NAT*: s=10.0.0.2->15.0.0.200, d=20.0.0.1 [500]
00:38:34: NAT*: s=20.0.0.1, d=15.0.0.200->10.0.0.2 [416]

00:38:34: NAT*: s=10.0.0.2->15.0.0.200, d=20.0.0.1 [502]
00:38:39: NAT*: s=20.0.0.1, d=15.0.0.200->10.0.0.2 [417]

00:38:39: NAT*: s=10.0.0.2->15.0.0.200, d=20.0.0.1 [509]
00:38:39: NAT*: s=20.0.0.1, d=15.0.0.200->10.0.0.2 [418]

Step 10(B): Verifying the Dynamic PAT Translation on Router R1 by translation table.

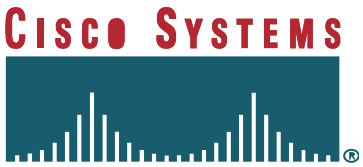
R1#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
tcp	**15.0.0.200:1041**	**10.0.0.1:1041**	**20.0.0.1:80**	**20.0.0.1:80**
tcp	**15.0.0.200:1042**	**10.0.0.2:1042**	**20.0.0.1:80**	**20.0.0.1:80**

Section 4

Switching

Etronics Solution Provider



By **M. Irfan Ghauri**
M. Rizwan

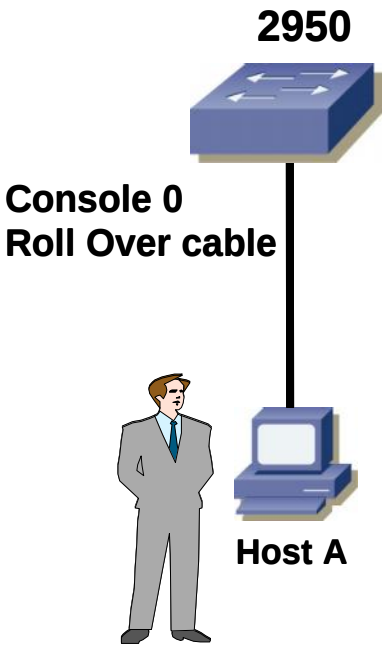
Lab # 11

2950 Switch Basic Native IOS

Objective

This lab includes basic commands of Native IOS on 2950 and 3550.

Diagram



By **M. Irfan Ghauri**
M. Rizwan

Configuration

Step 1: After connecting your PC to the Console Port.

Switch con0 is now available

Press RETURN to get started.

Switch> (**User Mode**)

Step 2: To Enter Into Privilege mode/Executive Mode From User Mode & Vice-Versa.

Switch>enable
Switch#

Switch#disable
Switch>

Step 3: To Enter Into Global Configuration Mode.

Switch#config t
Switch(config)#

Step 4: To change the Host Name of Switch.

Switch(config)#hostname 2950-SWA
2950-SWA(config)#

Step 5: Set the Message of the Day Banner

Switch(config)#banner motd # HELLO & WELCOME TO CISCO WORLD #

Step 6: Display the Version Information of the Switch.

2950-SWA#show version

Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I5Q3L2-M), Version 12.1(20)EA2, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Wed 19-May-04 05:06 by antonino
Image text-base: 0x00003000, data-base: 0x0082D44C

ROM: Bootstrap program is C2950 boot loader

2950 uptime is 7 hours, 11 minutes
System returned to ROM by power-on

System image file is "flash:c2950-i5q3l2-mz.121-20.EA2.bin"

cisco WS-C2950-24 (PowerPC) processor (revision L0) with 65526K/8192K bytes of memory.
Processor board ID CAT0805Z0CW
Last reset from warm-reset
Bridging software.
Running Layer2/3 Switching Image

Ethernet-controller 1 has 12 Fast Ethernet/IEEE 802.3 interfaces

Ethernet-controller 2 has 12 Fast Ethernet/IEEE 802.3 interfaces

Ethernet-controller 3 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 4 has 1 Gigabit Ethernet/IEEE 802.3 interface

24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

The password-recovery mechanism is enabled.
384K bytes of flash-simulated non-volatile configuration memory.

Base ethernet MAC Address: 00:0F:24:68:05:00

Motherboard assembly number: 73-5700-11
Power supply part number: 34-0966-04
Motherboard serial number: CAT08050JCX
Power supply serial number: DTH08042TFG
Model revision number: L0
Motherboard revision number: A0
Model number: WS-C2950-24-SMI
System serial number: CAT0805Z0CW

Configuration register is 0x10F

Step 7: Show contents of Current Configuration (RAM).

2950-SWA#show running-config

Building configuration...

Current configuration : 2146 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2950-SWA
!
<Output Omitted>
ip subnet-zero
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode dynamic desirable
!

```
interface FastEthernet0/2
 switchport mode dynamic desirable
!
<Output Omitted>
!
interface FastEthernet0/23
 switchport mode dynamic desirable
!
interface FastEthernet0/24
 switchport mode dynamic desirable
!
interface GigabitEthernet0/1
 switchport mode dynamic desirable
!
interface GigabitEthernet0/2
 switchport mode dynamic desirable
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip http server
!
<Output Omitted>
!
end
```

Step 8: Display the Flash Information.

2950-SWA#dir

OR

2950-SWA#show flash:

Directory of flash: /

```
  2  -rwx         556   Mar 1 1993 00:18:07 +00:00  vlan.dat
  3  -rwx     4219426   Mar 1 1993 00:44:10 +00:00  c2950-i5q3l2-mz.121-20.EA2.bin
```

```
  4  -rwx         315   Mar 1 1993 00:45:44 +00:00  system_env_vars
  5  -rwx           0   Mar 1 1993 00:45:43 +00:00  env_vars
  8  drwx         192   Mar 1 1993 00:04:07 +00:00  c2950-i9q3l2-mz.121-14.EA1a
 87  -rwx         744   Mar 1 1993 00:26:17 +00:00  debug.text

15998976 bytes total (6026752 bytes free)
```

Step 9: To give the IP Address of Management Domain Interface OF 2950.

2950-SWA(config)#int vlan 1
2950-SWA(config-if)#ip address 10.0.0.10 255.0.0.0
2950-SWA(config-if)#no shutdown

Step 10: Display the information of Management VLAN Interface.

2950-SWA#sh int vlan 1

Vlan1 is up, line protocol is up
Hardware is EtherSVI, address is 000f.2468.0500 (bia 000f.2468.0500)

Internet address is 10.0.0.10/8
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00

Queueing strategy: fifo
Output queue: 0/40 (size/max)
<Output Omitted>

Step 11: Display the information of All Interfaces on the switch.

2950-SWA#sh ip int brief

Interface	IP-Address	OK	Method	Status	Protocol
Vlan1	**10.0.0.10**	**YES**	**manual**	**up**	**down**
FastEthernet0/1	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/23	unassigned	YES	unset	down	down
<Output Omitted>					
FastEthernet0/24	unassigned	YES	unset	down	down
GigabitEthernet0/1	unassigned	YES	unset	down	down
GigabitEthernet0/2	unassigned	YES	unset	down	down

Step 12: Set a IP Default Network In a Switched Network.

2950-SWA(config)#ip default-gateway 10.0.0.1

Step 13: Display the Status of the Interfaces on the switch.

2950-SWA#show interfaces status

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/2		notconnect	1	auto	auto	10/100BaseTX
<Output Omitted>						
Fa0/22		notconnect	1	auto	auto	10/100BaseTX

Fa0/23	notconnect	1	auto	auto	10/100BaseTX
Fa0/24	notconnect	1	auto	auto	10/100BaseTX
Gi0/1	notconnect	1	auto	auto	unknown
Gi0/2	notconnect	1	auto	auto	unknown

Step 14: Display the Detailed Information of Interfaces.

2950-SWA#show interfaces

OR

2950-SWA#show interfaces fastEthernet 0/1

FastEthernet0/1 is up, line protocol is up (connect)
Hardware is Fast Ethernet, address is 000f.2468.0501 (bia 000f.2468.0501)
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,

Encapsulation ARPA, loopback not set
Keepalive set (10 sec)

Auto-duplex, Auto-speed, media type is 100BaseTX
input flow-control is off, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00

Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
<Output Omitted>

Step 15: Display the Information of the Mode of Interfaces (Switchport).

2950-SWA#show interfaces switchport

OR

2950-SWA#show interfaces fastEthernet 0/1 switchport

Name: Fa0/1

Switchport: Enabled

Administrative Mode: dynamic desirable

Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
<Output Omitted>
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none

Step 16: Display the Detailed Information of Interfaces Capabilities.

2950-SWA#show interfaces capabilities

OR

2950-SWA#show interfaces fastEthernet 0/1 capabilities

FastEthernet0/1

Model:	WS-C2950-24
Type:	**10/100BaseTX**
Speed:	**10,100,auto**

Duplex:	**half,full,auto**
Trunk encap. type:	**802.1Q,ISL**
Trunk mode:	**on,off,desirable,nonegotiate**
Channel:	**yes**

<Output Omitted>

Step 17: Display the Information of the Trunk Interfaces (Ports).

2950-SWA#show interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/23	**desirable**	**n-802.1q**	**trunking**	**1**
Fa0/24	**desirable**	**n-802.1q**	**trunking**	**1**

Port	Vlans allowed on trunk
Fa0/23	**1-4094**
Fa0/24	**1-4094**

Port	Vlans allowed and active in management domain
Fa0/23	**1-2**
Fa0/24	**1-2**

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/23	**1-2**
Fa0/24	**2**

Step 18: Setting Of Speed, Duplex and Description On Interface.

2950-SWA(config)#int fastEthernet 0/1

2950-SWA(config-if)#speed 100

2950-SWA(config-if)#duplex full

2950-SWA(config-if)#description Fast-Ethernet-Port-1

Step 19: Configuring the Multiple Interfaces.

2950-SWA(config)#int range fastEthernet 0/1 - 5

2950-SWA(config-if-range)#switchport mode access

Step 26: Shown the MAC Address Table Information.

2950-SWA#show mac address-table dynamic

Mac Address Table

Vlan	Mac Address	Type	Ports
1	**0001.0262.fcc4**	**DYNAMIC**	**Fa0/1**

Total Mac Addresses for this criterion: 1

Step 20: Display the Information of CDP *(Cisco Discovery Protocol)*.

2950-SWA#sh cdp

Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
Sending CDPv2 advertisements is enabled

Step 21: Display the Information of CDP Enabled Interfaces.

2950-SWA#sh cdp interfaces

FastEthernet0/1 is up, line protocol is up
Encapsulation ARPA
Sending CDP packets every 60 seconds
Holdtime is 180 seconds

FastEthernet0/2 is down, line protocol is down

Encapsulation ARPA
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
<OUTPUT OMITTED>

FastEthernet0/23 is down, line protocol is down

Encapsulation ARPA
Sending CDP packets every 60 seconds
Holdtime is 180 seconds

FastEthernet0/24 is up, line protocol is up

Encapsulation ARPA
Sending CDP packets every 60 seconds
Holdtime is 180 seconds

GigabitEthernet0/1 is down, line protocol is down

Encapsulation ARPA
Sending CDP packets every 60 seconds
Holdtime is 180 seconds

GigabitEthernet0/2 is down, line protocol is down

Encapsulation ARPA
Sending CDP packets every 60 seconds
Holdtime is 180 seconds

Step 22: Enabled the CDP on the switch.

Switch(config)#cdp run

Step 23: Enable CDP on the Interface FastEthernet 0/1.

Switch(config)#interface fastethernet 0/1

Switch(config-if)#cdp enable

Step 24(A): Set the Line Console Password on the switch.

2950-SWA(config)#line console 0
2950-SWA(config-line)#password cisco
2950-SWA(config-line)#login

Step 24(B): Verification Line Console Password on the switch.

2950-SWA con0 is now available
Press RETURN to get started.
User Access Verification

Password:
2950-SWA>enable

Step 25(A): Set the privileged mode password in clear text.

2950-SWA(config)#enable password cisco

Step 25(B): Verifying the privileged mode password in clear text.

2950-SWA#disable
2950-SWA>enable
Password:
2950-SWA#

Step 26(A): Set the Privileged Mode password in encrypted form.

2950-SWA(config)#enable secret cisco

The enable secret you have chosen is the same as your enable password.
This is not recommended. **Re-enter the enable secret**.

2950-SWA(config)#enable secret cisco1

Step 26(B): Verifying the Privileged Mode password in encrypted form.

2950-SWA>enable
Password:

Step 27: Set the Line VTY Password on the switch.

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

Step 28: Display the Information of Dynamic Trunking Protocol (DTP).

2950-SWA#show dtp
Global DTP information
Sending DTP Hello packets every 30 seconds
Dynamic Trunk timeout is 300 seconds
4 interfaces using DTP

Step 29: Copy the Current Configuration Into Startup Configuration.

2950-SWA#copy running-config startup-config

Destination filename [startup-config]?
Building configuration...
[OK]

Lab # 12

Spanning Tree Protocol

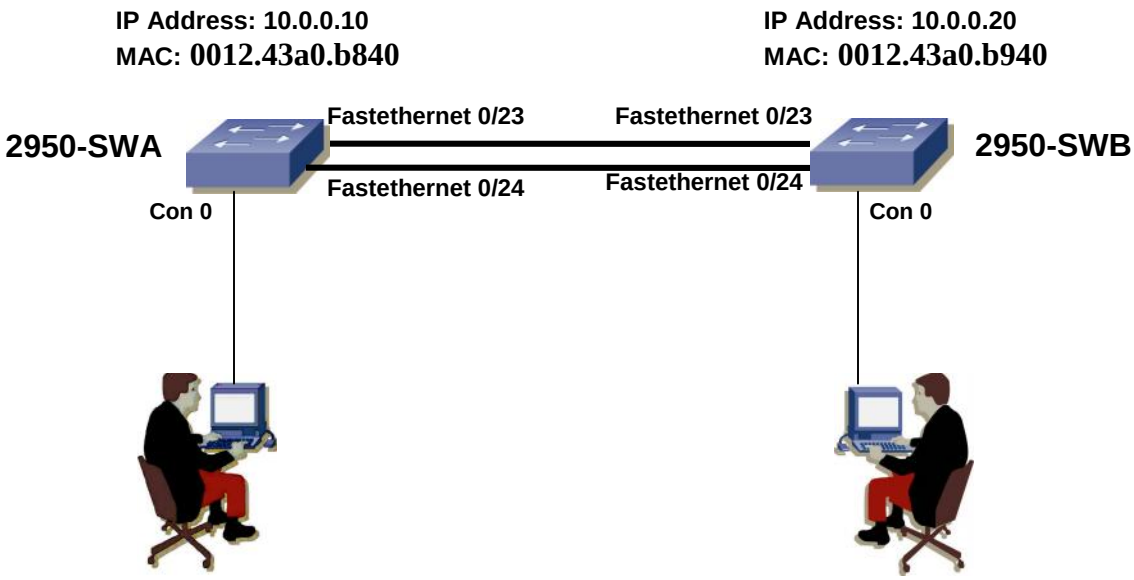
On

2950 Switch

Objective

Understanding the Spanning tree protocol operation in switched environment by creating a multiple or redundant link between switches.

Diagram



Etronics Solution Provider

By **M. Irfan Ghauri**
M. Rizwan

Procedure

1. Verifying the Spanning Tree Protocol on the 2950-SWA & 2950-SWB switches.
2. Changing Non Root Switch into Root Switch By Decreasing the priority.
3. Verifying the Spanning Tree Protocol on the 2950-SWA & 2950-SWB switches after changing priority.
4. Select Root Port on (Non-Root Switch) by Changing Cost of Port.
5. Verifying the Spanning Tree Protocol on the 2950-SWA & 2950-SWB switches after changing Cost of Port.

Configuration

Step 1(A): Verifying the Spanning Tree Protocol on the 2950-SWA switch.

2950-SWA#show spanning-tree

OR

2950-SWA#sh spanning-tree vlan 1

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0012.43a0.b840
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0012.43a0.b840
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/23	**Desg**	**FWD**	**19**	**128.23**	**P2p**
Fa0/24	**Desg**	**FWD**	**19**	**128.24**	**P2p**

Step 1(B): Verifying the detailed information of Spanning Tree Protocol on the 2950-SWA switch.

2950-SWA#show spanning-tree detail

OR

2950-SWA#sh spanning-tree vlan 1 detail

VLAN0001 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 32768, sysid 1, address 0012.43a0.b840
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag not set, detected flag not set
Number of topology changes 1 last change occurred 00:06:50 ago
from FastEthernet0/23
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0, aging 300

Port 23 (FastEthernet0/23) of VLAN0001 is forwarding
Port path cost 19, Port priority 128, Port Identifier 128.23.
Designated root has priority 32769, address 0012.43a0.b840
Designated bridge has priority 32769, address 0012.43a0.b840
Designated port id is 128.23, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 221, received 1

Port 24 (FastEthernet0/24) of VLAN0001 is forwarding
Port path cost 19, Port priority 128, Port Identifier 128.24.
Designated root has priority 32769, address 0012.43a0.b840
Designated bridge has priority 32769, address 0012.43a0.b840
Designated port id is 128.24, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 218, received 1

Step 2(A): Verifying the Spanning Tree Protocol on the 2950-SWB switch.

2950-SWB#show spanning-tree

OR

2950-SWB#show spanning-tree vlan 1

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0012.43a0.b840
Cost 19
Port 23 (FastEthernet0/23)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0012.43a0.b940
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/23	**Root**	**FWD**	**19**	**128.23**	**P2p**
Fa0/24	**Altn**	**BLK**	**19**	**128.24**	**P2p**

Step 2(B): Verifying the detailed information of Spanning Tree Protocol on the 2950-SWB switch.

2950-SWB#show spanning-tree detail

OR

2950-SWB#sh spanning-tree vlan 1 detail

VLAN0001 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 32768, sysid 1, address 0012.43a0.b940
Configured hello time 2, max age 20, forward delay 15

Current root has priority 32769, address 0012.43a0.b840
Root port is 23 (FastEthernet0/23), cost of root path is 19
Topology change flag not set, detected flag not set
Number of topology changes 0 last change occurred 00:06:03 ago
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0, aging 300

Port 23 (FastEthernet0/23) of VLAN0001 is forwarding
Port path cost 19, Port priority 128, Port Identifier 128.23.
Designated root has priority 32769, address 0012.43a0.b840
Designated bridge has priority 32769, address 0012.43a0.b840
Designated port id is 128.23, designated path cost 0
Timers: message age 2, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 1, received 182

Port 24 (FastEthernet0/24) of VLAN0001 is blocking
Port path cost 19, Port priority 128, Port Identifier 128.24.
Designated root has priority 32769, address 0012.43a0.b840
Designated bridge has priority 32769, address 0012.43a0.b840
Designated port id is 128.24, designated path cost 0
Timers: message age 2, forward delay 0, hold 0
Number of transitions to forwarding state: 0
Link type is point-to-point by default

Step 3: Changing Non Root Switch into Root Switch By decreasing the priority on 2950-SWB (Non-Root-Switch)

2950-SWB(config)#spanning-tree vlan 1 priority 4096

Step 4(A): Verifying the Spanning Tree Protocol on the 2950-SWB switch after Changing priority on 2950-SWB

2950-SWB#sh spanning-tree vlan 1

VLAN0001
Spanning tree enabled protocol ieee

Root ID Priority 4097
Address 0012.43a0.b940
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 4097 (priority 4096 sys-id-ext 1)
Address 0012.43a0.b940
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/23	**Desg**	**FWD**	**19**	**128.23**	**P2p**
Fa0/24	**Desg**	**FWD**	**19**	**128.24**	**P2p**

Step 4(B): Verifying the Spanning Tree Protocol on the 2950-SWA switch after Changing priority on 2950-SWB

2950-SWA#sh spanning-tree vlan 1

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 4097
Address 0012.43a0.b940
Cost 19
Port 23 (FastEthernet0/23)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0012.43a0.b840
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/23	**Root**	**FWD**	**19**	**128.23**	**P2p**
Fa0/24	**Altn**	**BLK**	**19**	**128.24**	**P2p**

Step 5: Select Root Port on (Non-Root Switch) by Changing Cost Of Port on 2950-SWA.

2950-SWA(config)#int fastEthernet 0/24
2950-SWA(config-if)#spanning-tree vlan 1 cost 18

Step 6: Verifying the Spanning Tree Protocol on the 2950-SWA switch after Changing Cost of Port.

2950-SWA#sh spanning-tree vlan 1

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 4097
Address 0012.43a0.b940
Cost 18
Port 24 (FastEthernet0/24)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0012.43a0.b840
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/23	**Altn**	**BLK**	**19**	**128.23**	**P2p**
Fa0/24	**Root**	**FWD**	**18**	**128.24**	**P2p**

Step 6: Verifying the Spanning Tree Protocol on the 2950-SWB switch after Changing Cost of Port.

2950-SWB#sh spanning-tree vlan 1

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 4097
Address 0012.43a0.b940
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 4097 (priority 4096 sys-id-ext 1)
Address 0012.43a0.b940
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/23	**Desg**	**FWD**	**19**	**128.23**	**P2p**
Fa0/24	**Desg**	**FWD**	**19**	**128.24**	**P2p**

Lab # 13

VLAN

&

VLAN Trunking Protocol

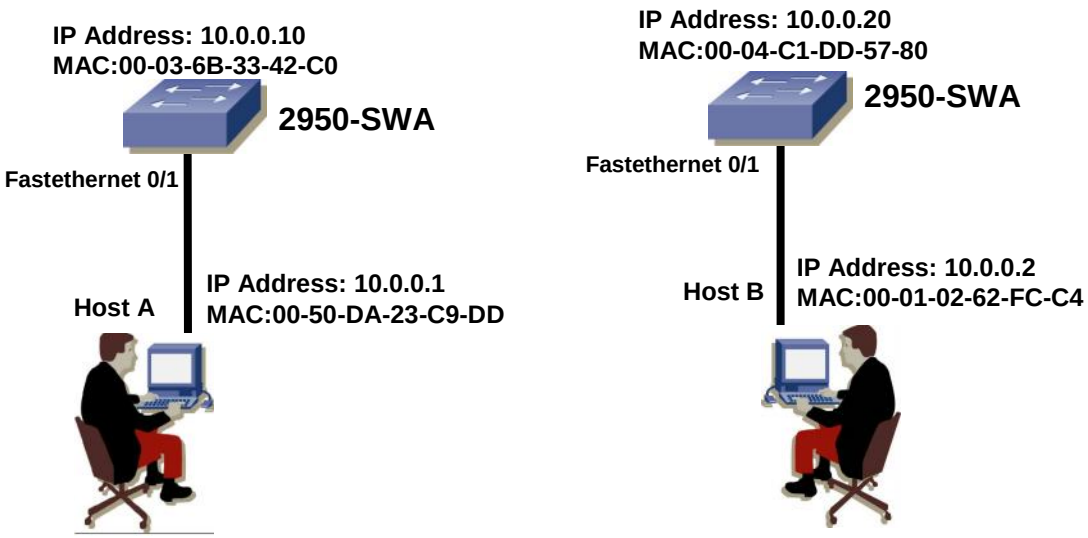
Objective

Understanding the VLAN operation in switched environment. The major concerns are,

1. To make Vlan's on 2950 switches & Vlan membership assignments to the ports.
2. VLAN Trunking Protocol (VTP).

i. VLAN

Diagram



Procedure

1. Connecting PC with 2950 switches and verified by Commands.
2. Display the results that all ports are the members of the native VLAN.
3. Create a VLAN # 2 on 2950 Switch.
4. Assign a VLAN Member-ship for a Port on 2950 Switch.
5. Verification of VLAN # 2.

Configuration

Step 1(A): Connecting PC with 2950 switch and verified by the Interface Command.

2950-SWA#sh interfaces fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 000b.5f03.f9c1 (bia 000b.5f03.f9c1)
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ARPA, loopback not set
Keepalive set (10 sec)

Full-duplex, 100Mb/s
<Output Omitted>

Step 1(B): Connecting PC with 2950 switch and verified by the MAC Address Table Command.

2950-SWA#show mac address-table dynamic

Mac Address Table

Vlan	Mac Address	Type	Ports
1	**0001.0262.fcc4**	**DYNAMIC**	**Fa0/1**

Total Mac Addresses for this criterion: 1

Step 2: Display the results that all ports are the members of the native VLAN.

2950-SWA#show vlan

OR

2950-SWA#show vlan id 1

VLAN	Name	Status	Ports
1	**default**	**active**	**Fa0/1, Fa0/2, Fa0/3, Fa0/4** **Fa0/5, Fa0/6, Fa0/7, Fa0/8** **Fa0/9, Fa0/10, Fa0/11, Fa0/12** **Fa0/13, Fa0/14, Fa0/15, Fa0/16** **Fa0/17, Fa0/18, Fa0/19, Fa0/20** **Fa0/21, Fa0/22, Fa0/23, Fa0/24** **Gi0/1, Gi0/2**

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	**enet**	**100001**	**1500**	**-**	**-**	**-**	**-**	**-**	**0**	**0**

<Output Omitted>

Step 3(A): Create a VLAN # 2 on 2950 Switch by VLAN Database command.

2950-SWA#vlan database
2950-SWA(vlan)#vlan 2 name esp

VLAN 2 added:
Name: esp
2950-SWA(vlan)#exit
APPLY completed.
Exiting....

Step 3(B): Create a VLAN # 2 on 2950 Switch by VLAN command.

2950-SWA(config)#vlan 2
2950-SWA(config-vlan)#name esp

Step 4: Assign a VLAN Member-ship for a Fast Ethernet Port 0/1 on 2950 Switch.

2950-SWA(config)#interface fastEthernet 0/1
2950-SWA(config-if)#switchport mode access
2950-SWA(config-if)#switchport access vlan 2

Step 5: Verification of VLAN # 2.

2950-SWA#show vlan

OR
2950-SWA#sh vlan id 2

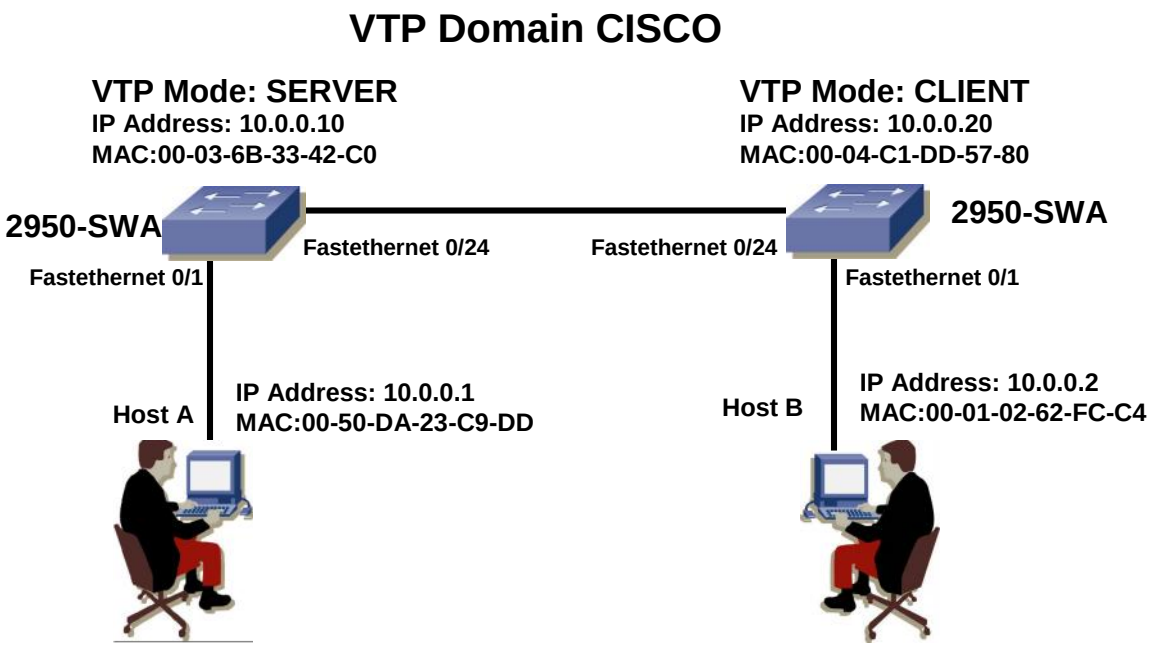
VLAN	Name	Status	Ports
2	**esp**	**active**	**Fa 0/1**

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
2	**enet**	**100002**	**1500**	**-**	**-**	**-**	**-**	**-**	**0**	**0**

<Output Omitted>

ii. VLAN Trunking Protocol (VTP)

Diagram



Procedure

1. Make a VTP domain CISCO on switches.
2. Make a VTP server to 2950-SWA and client to 2950-SWB.
3. Enable a Trunking on the fastEthernet ports 0/24 that connects both switches.
4. Verifying with VTP Status commands on switches.
5. Verifying the VTP Advertisements By Trigger Updates (make vlan's) On 2950-SWA switch.
6. Verifying the VTP Status on switches after triggered update.
7. Verifying the VLAN database on 2950-SWA switch after making VLAN's.
8. Verifying the VLAN datatbase consistency on 2950-SWB switch after making VLAN's on 2950-SWB switch.

Configuration

Step 1(A): Make a VTP Domain CISCO on 2950-SWA switch.

2950-SWA **(config)#vtp domain CISCO**
Changing VTP domain name from NULL to CISCO

Step 1(B): Make a VTP Domain CISCO on 2950-SWB switch.

2950-SWB(config)#vtp domain CISCO
Changing VTP domain name from NULL to CISCO

Step 2(A): Make a VTP Server to 2950-SWA switch.

2950-SWA(config)#vtp mode ?

```
client       Set the device to client mode.
server       Set the device to server mode.
transparent  Set the device to transparent mode.
```

2950-SWA(config)#vtp mode server
Device mode already VTP SERVER.

Step 2(B): Make a VTP Client to 2950-SWB switch.

2950-SWB(config)#vtp mode client
Setting device to VTP CLIENT mode.

Step 3(A): Enable a Trunking on the fastEthernet ports 0/24 of 2950-SWA switch.

2950-SWA(config)#int fastEthernet 0/24
2950-SWA(config-if)#switchport mode trunk

Step 3(B): Enable a Trunking on the fastEthernet ports 0/24 of 2950-SWB switch.

2950-SWB(config)#int fastEthernet 0/24
2950-SWB(config-if)#switchport mode trunk

Step 4(A): Verifying the VTP Status on 2950-SWA switch.

2950-SWA #sh vtp status

VTP Version : 2

Configuration Revision : 3
Maximum VLANs supported locally : 1005

Number of existing VLANs : 6

VTP Operating Mode : Server

VTP Domain Name : CISCO
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xD5 0x18 0x44 0xA3 0xAA 0x16 0xAE 0x35
Configuration last modified by 10.0.0.20 at 3-1-93 06:10:50
Local updater ID is 10.0.0.20 on interface Vl2 (lowest numbered VLAN interface found)

Step 4(B): Verifying the VTP Status on 2950-SWB switch.

2950-SWB#sh vtp status

VTP Version : 2

Configuration Revision : 3
Maximum VLANs supported locally : 250

Number of existing VLANs : 6

VTP Operating Mode : Client

VTP Domain Name : CISCO
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xD5 0x18 0x44 0xA3 0xAA 0x16 0xAE 0x35
Configuration last modified by 10.0.0.20 at 3-1-93 06:10:50

Step 5: Verifying the VTP Advertisements By Trigger Updates (Add/ Delete/ Modify vlan's) On 2950-SWA switch.

2950-SWA(config)#vlan 25
2950-SWA(config-vlan)#vlan 50
2950-SWA(config-vlan)#vlan 75
2950-SWA(config-vlan)#vlan 100

Step 6(A): Verifying the VTP Status on 2950-SWA switch after triggered update.

2950-SWA#sh vtp status

VTP Version : 2

Configuration Revision : 7
Maximum VLANs supported locally : 1005

Number of existing VLANs : 10

VTP Operating Mode : Server

VTP Domain Name : CISCO
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xD5 0x18 0x44 0xA3 0xAA 0x16 0xAE 0x35
Configuration last modified by 10.0.0.20 at 3-1-93 06:10:50

Local updater ID is 10.0.0.20 on interface Vl2 (lowest numbered VLAN interface found)
2950-SWA#

Step 6(B): Verifying the VTP Status on 2950-SWB switch after triggered update.

2950-SWB#sh vtp status

VTP Version : 2

Configuration Revision : 7
Maximum VLANs supported locally : 250

Number of existing VLANs : 10

VTP Operating Mode : Client

VTP Domain Name : CISCO
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xD5 0x18 0x44 0xA3 0xAA 0x16 0xAE 0x35
Configuration last modified by 10.0.0.20 at 3-1-93 06:10:50

Step 7: Verifying the VLAN datatbase on 2950-SWA switch after making VLAN's.

2950-SWA#show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
2	esp	active	Fa0/1
25	**VLAN0025**	**active**	
50	**VLAN0050**	**active**	

75 VLAN0075 active
100 VLAN0100 active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
2	**enet**	**100002**	**1500**	**-**	**-**	**-**	**-**	**-**	**0**	**0**
25	**enet**	**100025**	**1500**	**-**	**-**	**-**	**-**	**-**	**0**	**0**
50	**enet**	**100050**	**1500**	**-**	**-**	**-**	**-**	**-**	**0**	**0**
75	**enet**	**100075**	**1500**	**-**	**-**	**-**	**-**	**-**	**0**	**0**
100	**enet**	**100100**	**1500**	**-**	**-**	**-**	**-**	**-**	**0**	**0**
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

<Output Omitted>

Step 8: Verifying the VLAN datatbase consistency on 2950-SWB switch after making VLAN's on 2950-SWA switch.

2950-SWB#show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
2	**esp**	**active**	**Fa0/1**
25	**VLAN0025**	**active**	
50	**VLAN0050**	**active**	
75	**VLAN0075**	**active**	

100 VLAN0100 active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup

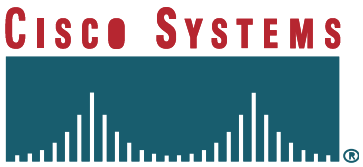
VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
2	**enet**	**100002**	**1500**	**-**	**-**	**-**	**-**	**-**	**0**	**0**
25	**enet**	**100025**	**1500**	**-**	**-**	**-**	**-**	**-**	**0**	**0**
50	**enet**	**100050**	**1500**	**-**	**-**	**-**	**-**	**-**	**0**	**0**
75	**enet**	**100075**	**1500**	**-**	**-**	**-**	**-**	**-**	**0**	**0**
100	**enet**	**100100**	**1500**	**-**	**-**	**-**	**-**	**-**	**0**	**0**
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	srb	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

<Output Omitted>

Section 5

WAN

Etronics Solution Provider



By **M. Irfan Ghauri**
M. Rizwan

Lab # 14

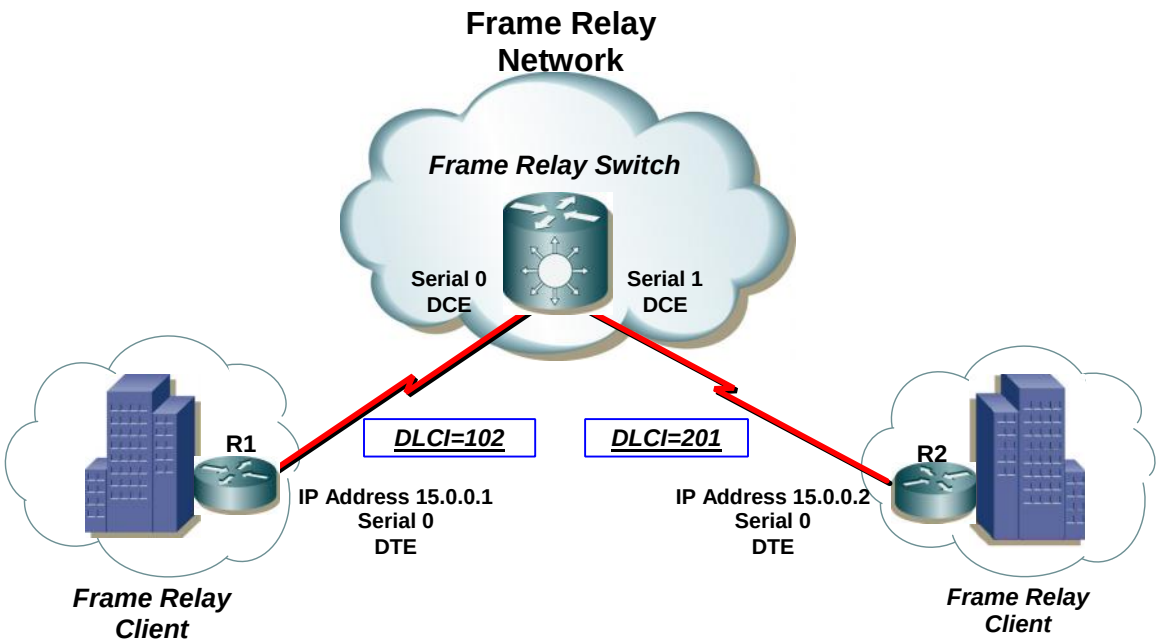
FRAME RELAY

Objective

To establish a Frame Relay PVC connection.

- Frame Relay is a standard that defines the process for sending data over a public data network.
- Frame Relay is a connection-oriented data link technology that is streamlined to provide high performance & efficiency.
- Frame Relay connections operate over virtual circuits.

Diagram



Procedure

1. Configuring the FR Switch.
2. Configuring & Assigning the IP addresses to the FR Clients (R1 & R2).
3. Verifying the Frame Relay Operation by commands.
4. Verifying the connectivity of both FR Clients.

Configuration

Step 1: Configuring the FR switch.

FR-SWITCH(config)#frame-relay switching

FR-SWITCH(config)#int s0
FR-SWITCH(config-if)#no ip address
FR-SWITCH(config-if)#no shutdown
FR-SWITCH(config-if)#encapsulation frame-relay
FR-SWITCH(config-if)#frame-relay intf-type dce
FR-SWITCH(config-if)#clock rate 64000
FR-SWITCH(config-if)#frame-relay route 102 int s1 201

FR-SWITCH(config)#int s1
FR-SWITCH(config-if)#no ip address
FR-SWITCH(config-if)#no shutdown
FR-SWITCH(config-if)#encapsulation frame-relay
FR-SWITCH(config-if)#frame-relay intf-type dce
FR-SWITCH(config-if)#clock rate 64000
FR-SWITCH(config-if)#frame-relay route 201 int s0 102

Step 2(A): Assigning the IP addresses to the FR Client Router R1.

R1(config)#interface serial 0
R1(config-if)#ip address 15.0.0.1 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#encapsulation frame-relay

Step 2(B): Assigning the IP addresses to the FR Client Router R2.

R2(config)#interface serial 0
R2(config-if)#ip address 15.0.0.2 255.0.0.0
R2(config-if)#no shutdown
R2(config-if)#encapsulation-frame-relay

Step 3(A): Verifying the Frame Relay Operation by commands.

FR Client

The **show frame-relay pvc** command displays the status of each configured connection, as well as traffic statistics.

The **show frame-relay map** command displays the DLCI-protocol address map entries, as well as information about the connection.

The **show frame-relay lmi** command displays LMI traffic statistics.

FR Switch

The **show frame-relay route** command displays the status of each configured virtual circuit connection, as well as their status and route to other interface.

Lab # 15

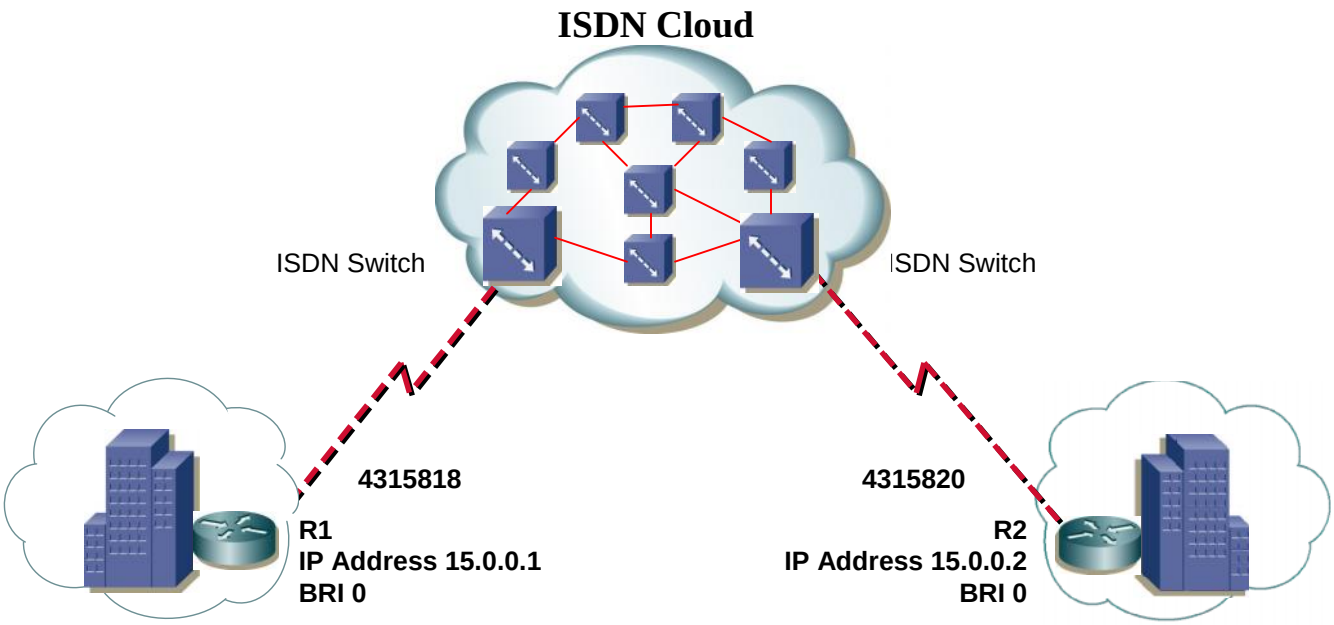
Integrated Services Digital Network (ISDN)

Objective

Configuring ISDN for DDR (Dial-on-Demand Routing).
DDR means that

1. **Connects when needed**
2. **Disconnects when finished**

Diagram



Procedure

1. Make a simple ISDN Call Configuration on Routers.
2. Verifying the R1's configuration by pinging the R2.
3. Displays the status of an ISDN connection at Routers
4. Displays the status of an ISDN connection at Routers.
5. Displays the dialer information of an ISDN connection at Routers.
6. Displays statistics for the BRI interface configured at Routers.
7. To disconnect the current isdn session.
8. Displays statistics for the BRI interface configured at Router R1 after disconnecting the line.

Configuration

Step 1(A): Maka a simple ISDN Call Configuration on R1.

Router(config)#hostname R1
R1(config)#username R2 password esp
R1(config)# isdn switch-type vn3
R1(config)#dialer-list 1 protocol ip permit

R1(config)#interface bri 0
R1(config-if)#ip address 15.0.0.1 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication chap
R1(config-if)# dialer-group 1
R1(config-if)# dialer map ip 15.0.0.2 name R2 4315820

Step 1(B): Maka a simple ISDN Call Configuration on R2.

Router(config)#hostname R2
R2(config)#username R1 password esp
R2(config)# isdn switch-type vn3
R2(config)#dialer-list 1 protocol ip permit

R2(config)#interface bri 0
R2(config-if)#ip address 15.0.0.2 255.0.0.0
R2(config-if)#no shutdown
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication chap
R2(config-if)# dialer-group 1
R2(config-if)# dialer map ip 15.0.0.1 name R1 4315818

Step 2: Verifying the R1's configuration by pinging the R2.

RouterA#ping 15.0.0.2

Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 36/38/40 ms
00:06:54: %ISDN-6-LAYER2UP: Layer 2 for Interface BR0, TEI 97 changed to up
00:06:56: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up
00:06:56: %ISDN-6-CONNECT: Interface BRI0:1 is now connected to 4315820

Step 3(A): Displays the status of an ISDN connection at Router R1.

R1#show isdn status

Global ISDN Switchtype = vn3

ISDN BRI0 interface

dsl 0**, interface ISDN Switchtype = vn3**
Layer 1 Status:
ACTIVE
Layer 2 Status:
TEI = 97, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
Layer 3 Status:
1 Active Layer 3 Call(s)

Activated dsl 0 CCBs = 1

CCB:callid=0x8007, sapi=0x0, ces=0x1, B-chan=1

Total Allocated ISDN CCBs = 1

Step 3(B): Displays the status of an ISDN connection at Router R2.

R2#show isdn status

Global ISDN Switchtype = vn3

ISDN BRI0 interface

dsl 0**, interface ISDN Switchtype = vn3**

Layer 1 Status:

ACTIVE

Layer 2 Status:

TEI = 106, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED

Layer 3 Status:

1 Active Layer 3 Call(s)

Activated dsl 0 CCBs = 1

CCB:callid=0x7, sapi=0x0, ces=0x1, B-chan=1

Total Allocated ISDN CCBs = 1

Step 4(A): Displays the dialer information of an ISDN connection at Router R1.

R1#show dialer

BRI0 - dialer type = ISDN

Dial String	Successes	Failures	Last called	Last status
4315820	**7**	**0**	**00:00:16**	**successful**

0 incoming call(s) have been screened.

0 incoming call(s) rejected for callback.

BRI0:1 - dialer type = ISDN

Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Dial reason: ip (s=10.0.0.1, d=10.0.0.2)

Time until disconnect 105 secs

Connected to 4315820 (R2)

BRI0:2 - dialer type = ISDN

Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)

Dialer state is idle

Step 4(B): Displays the dialer information of an ISDN connection at Router R2.

R2#show dialer

BRI0 - dialer type = ISDN

Dial String	Successes	Failures	Last called	Last status
4315818	**0**	**0**	**never**	**-**

0 incoming call(s) have been screened.
0 incoming call(s) rejected for callback.

BRI0:1 - dialer type = ISDN
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Time until disconnect 68 secs
Connected to 4315818 (R1)

BRI0:2 - dialer type = ISDN

Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Step 5(A): Displays statistics for the BRI interface configured at Router R1.

R1#show int bri0

BRI0 is up, line protocol is up (spoofing)
Hardware is BRI
Internet address is 15.0.0.1/8
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set
<OutputOmitted>

Step 5(B): Displays statistics for the BRI interface configured at Router R2.

R2#show int bri0

BRI0 is up, line protocol is up (spoofing)

Hardware is BRI

Internet address is 15.0.0.2/8

MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set
<OutputOmitted>

Step 6: To disconnect the current isdn session.

R1#clear int bri0

00:07:58: %ISDN-6-DISCONNECT: Interface BRI0:1 disconnected from 4315820 RouterB, call lasted 62 seconds
00:07:58: %LINK-3-UPDOWN: Interface BRI0:1, changed state to down
00:07:59: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed state to down

Step 7: Displays statistics for the BRI interface configured at Router R1 after disconnecting the line.

R1#show int bri0

BRI0 is up (spoofing), line protocol is up (spoofing)
Hardware is BRI
Internet address is 10.0.0.1/8
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255

Encapsulation PPP, loopback not set
<OutputOmitted>

Step 8: Verifying the ISDN Operations by other commands.

The **show isdn active** command displays current call information.

The **show isdn history** command displays the information of all calls.

The **debug isdn q921** command shows ISDN Layer 2 messages.

The **debug isdn q931** command shows ISDN call setup and teardown activity.

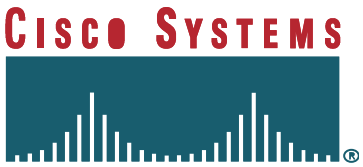
The **debug ppp authentication** command displays the PPP authentication protocol messages.

The **debug ppp negotiation** command displays information on PPP link establishment

Section 6

Appendix

Etronics Solution Provider



By **M. Irfan Ghauri**
M. Rizwan

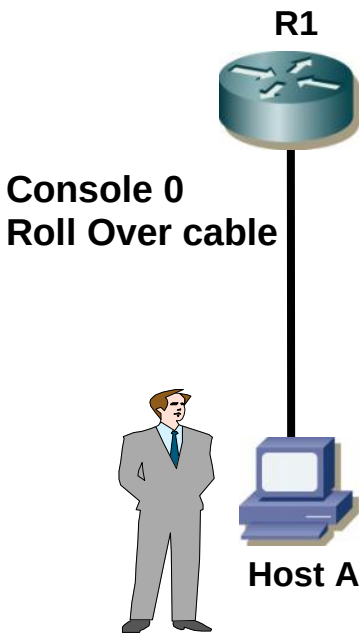
Lab # 16

Password Recovery

Objective

This lab demonstrates how to recover the password of 2500 series Routers. Password Recovery procedure allows you to regain administrative control over the device.

Diagram



Procedure

1. Attach a PC with terminal emulation software to the Router's Console port.
2. Turn off the Router, and turn it on and press the Break Key on the PC within 60 seconds of turning on the Router.
3. Enter the command to By-Pass the NVRAM on the > prompt and initialize the Router by command.
4. Enter no in response to the System Configuration dialog prompts.
5. Enter into the Router and copy the configuration from the NVRAM, change the password & change the value of the configuration register & save the configuration into NVRAM again and reload the Router.

Configuration

Step 1: Attach a PC with terminal emulation software to the Router's Console Port.

The configuration register value is 0x2102 by-default. It's mean that whenever the Router boots, it will read the contents of the NVRAM. So, we need to by-pass the NVRAM at the time of startup for the password recovery.

Step 2: Turn off the Router, and turn it on and press the Break Key on the PC within 60 seconds of turning on the Router.

The > **prompt** with no Router name appears at the Router screen.

Step 3: Enter the command to By-Pass the NVRAM on the > prompt and initialize the Router by command.

> o/r 0x2142 (to boot from flash)
> i (initialize the Router)

Step 4: **Enter no in response to the System Configuration dialog prompts until the following message appears.**

Press RETURN to get started!

Step 5: **Enter into the Router and copy the configuration from the NVRAM, change the password & change the value of the configuration register & save the configuration into NVRAM again and reload the Router.**

Router#copy stratup-config running-config
Router(config)#no enable password
Router(config)#enable password cisco
Router(config)#configuration-register 0x2102
Router#write memory (Equivalent Command of **copy running-config startup-config**)
Router#reload

Lab # 17

Port Security

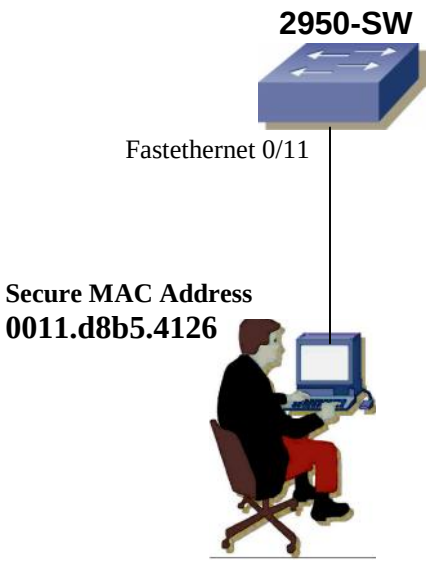
On 2950 Switch

Objective

This lab demonstrates the concept of port security mechanism on Switch.

In the port security, we can limit the number of Mac addresses on each port and can define violation method.

Diagram



By **M. Irfan Ghauri**
M. Rizwan

Procedure

1. Enable the port Security of the Interfaces.
2. Define the Max Mac Addresses on the Interface.
3. Verifying the Port Security of the Interface.
4. Note Messages at run time after security violation occurred.
5. Verifying the Port Security of the Interface after violation occurred.

Configuration

Step 1: Enable the port Security of the Interfaces.

Switch(config)#int fastEthernet 0/11
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security

Step 2: Define the Max Mac Addresses on the Interface.

Switch(config-if)#switchport port-security maximum 1

(The switch then automatically learns the Mac address on port # 11.This is called 'Sticky learned').

Step 3: Verifying the Port Security of the Interface.

Switch# sh port-security

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation	Security Action
Fa0/11	**1**	**1**	**0**	**Shutdown**

Step 4: Note Messages at run time after security violation occurred.

(Plugged–in any host at fast Ethernet 0/11 that has a Mac-address other than the one which is defined above in Step 3).

00:38:33: %PM-4-ERR_DISABLE: **psecure-violation error detected on Fa0/11**, putting Fa0/11 in err-disable state
00:38:33: %PORT_SECURITY-2-PSECURE_VIOLATION: **Security violation occurred**, **caused by MAC address 0011.d8e2.89da on port FastEthernet0/11**.
00:38:34: %LINEPROTO-5-UPDOWN: **Line protocol on Interface FastEthernet0/11, changed state to down**
00:38:35: %LINK-3-UPDOWN: **Interface FastEthernet0/11, changed state to down**

Step 5: Verifying the Port Security of the Interface after violation occurred.

Switch#sh port-security

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation	Security Action
Fa0/11	**1**	**1**	**1**	**Shutdown**

Lab # 18

TFTP Server

Objective

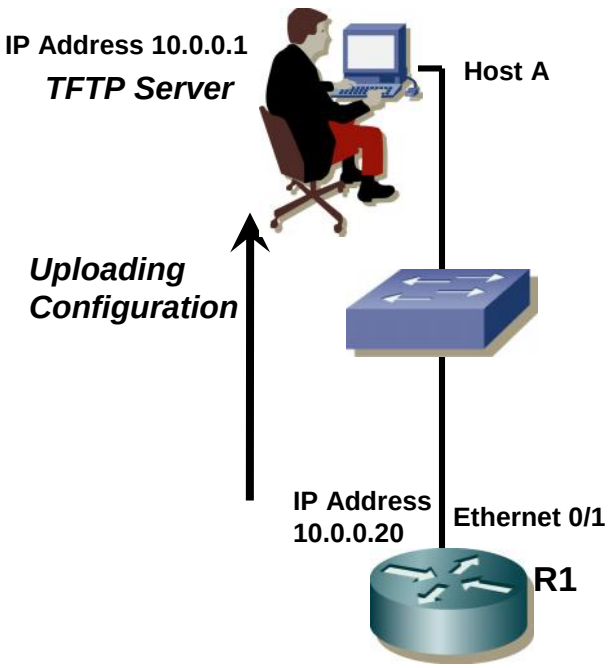
This lab demonstrates how you can backup your configuration as well as upload your configuration.

The demonstrations include:

1. Uploading Configuration to the TFTP Server.
2. Downloading Configuration from the TFTP Server.

i. Uploading Configuration from Router to the TFTP Server

Diagram

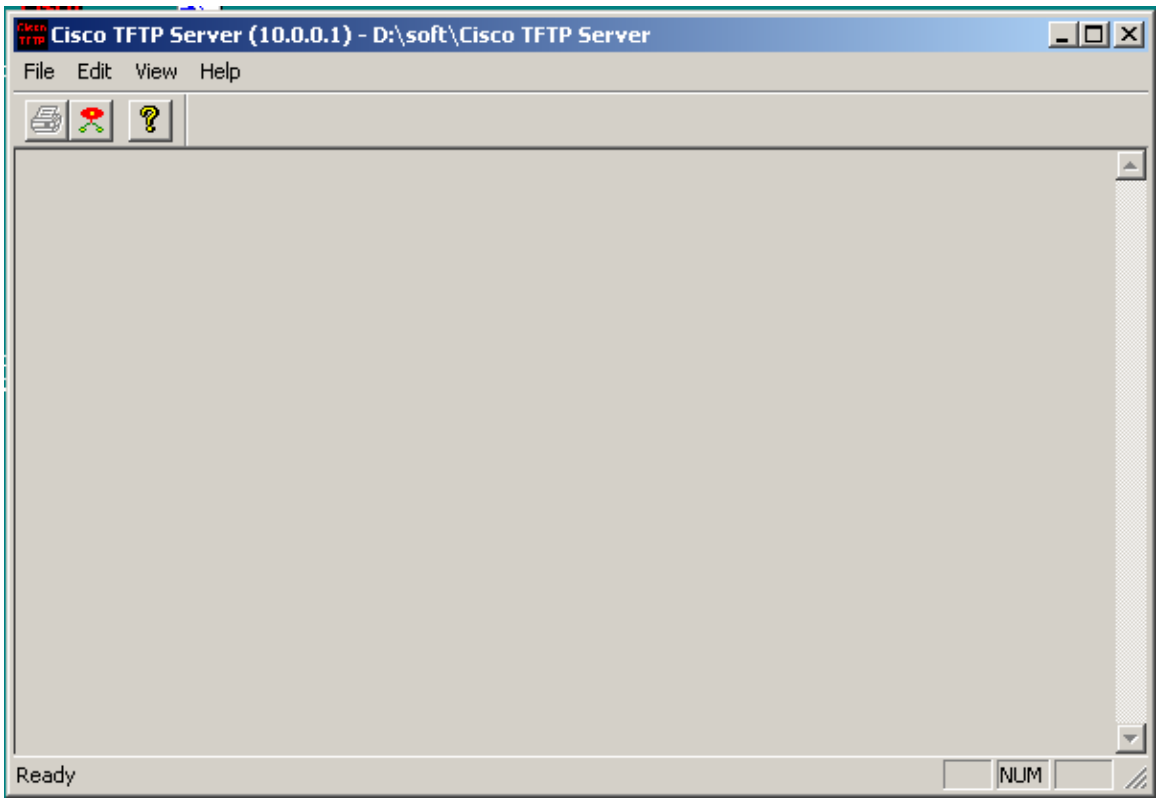


Procedure

1. Make a TFTP Server to Host ‘A’.
2. Verification of connectivity of PC & Router by ping command.
3. Upload the NVRAM Configuration into TFTP Server.
4. Verifying the uploaded configuration from the TFTP Server.

Configuration

Step 1: Make a TFTP Server to Host ‘A’.



Step 2: Verification of connectivity of PC & Switch by ping command.

R1#ping 10.0.0.1

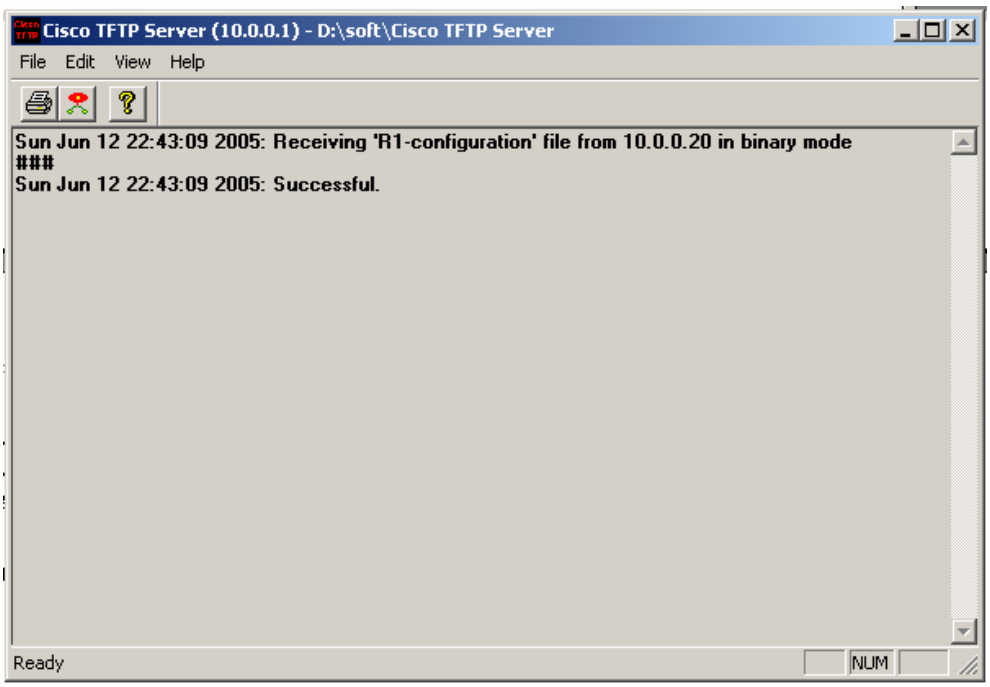
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Step 3: Upload the NVRAM Configuration into TFTP Server.

R1#copy startup-config tftp

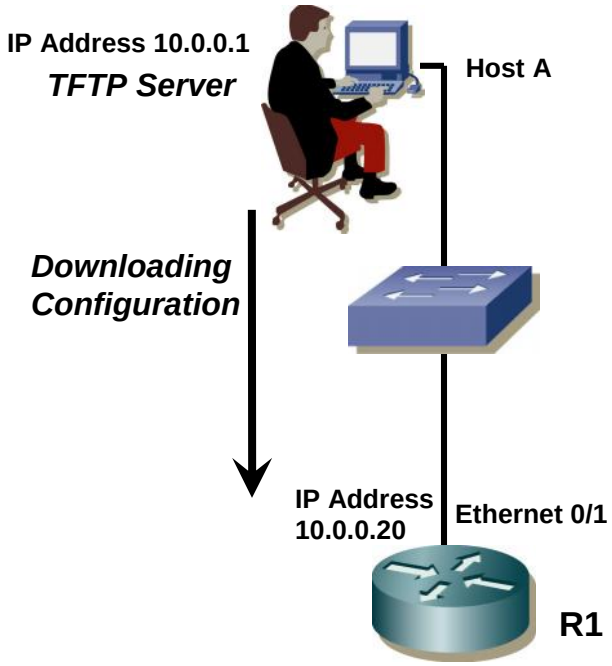
Remote host []? 10.0.0.1
Name of configuration file to write [r1-confg]? R1-configuration
Write file R1-configuration on host 10.0.0.1? [confirm]
Writing R1-configuration !! [OK]

Step 4: Verifying the uploaded configuration from the TFTP Server.



ii. Downloading Configuration to Router from the TFTP Server

Diagram

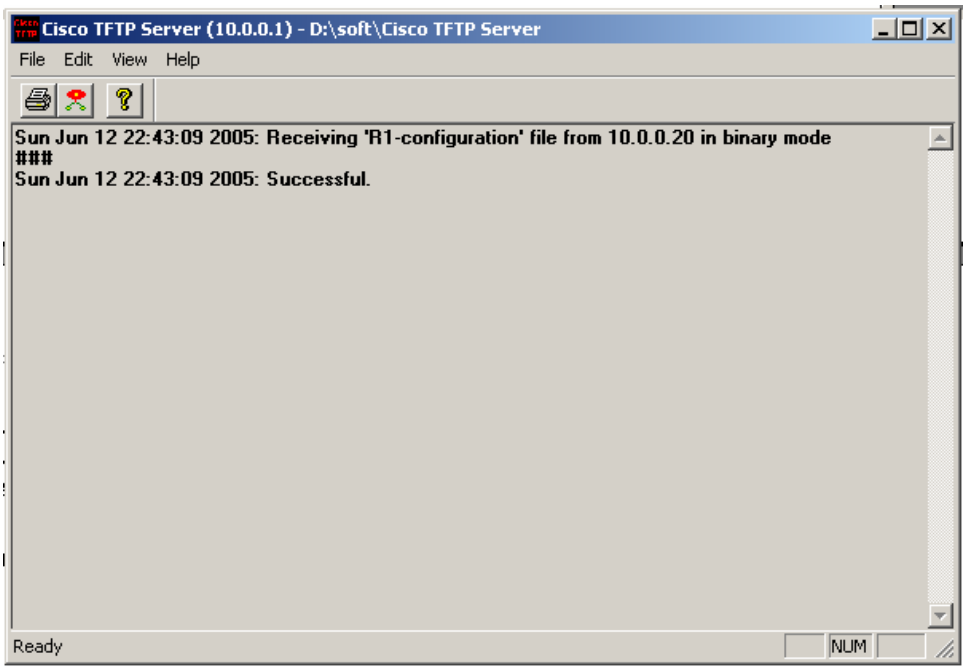


Procedure

1. Make a TFTP Server to Host ‘A’.
2. Remove the Configuration from the NVRAM and reload the Router.
3. Give the IP Address to the Router.
4. Verification of connectivity of PC & Router by ping command.
5. Download the NVRAM Configuration from the TFTP Server.
6. Verifying the uploaded configuration from the TFTP Server.

Configuration

Step 1: Make a TFTP Server to Host 'A'.



Step 2: Remove the Configuration from the NVRAM & reload the Router.

R1#write erase
[OK]

R1#reload

Proceed with reload? [confirm]

%SYS-5-RELOAD: Reload requested
System Bootstrap, Version 11.0(10c), SOFTWARE
Copyright (c) 1986-1996 by cisco Systems
<Output Omitted>

Step 3: Give the IP Address to the Router.

Router(config)#int ethernet 0
Router(config-if)#ip address 10.0.0.20 255.0.0.0

Step 4: Verification of connectivity of PC & Switch by ping command.

Router#ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms

Step 5: Download the NVRAM Configuration from TFTP Server.

Router#copy tftp running-config

Host or network configuration file [host]?
Address of remote host [255.255.255.255]? 10.0.0.1
Name of configuration file [router-confg]? R1-configuration
Configure using R1-configuration from 10.0.0.1? [confirm]
Loading R1-configuration from 10.0.0.1 (via Ethernet0): !
[OK - 1076/32723 bytes]
R1#
%SYS-5-CONFIG: Configured from R1-configuration by console tftp from 10.0.0.1

Step 6(A): Verifying the uploaded configuration by the command.

R1#show running-config

Step 6(B): Verifying the uploaded configuration from the TFTP Server.