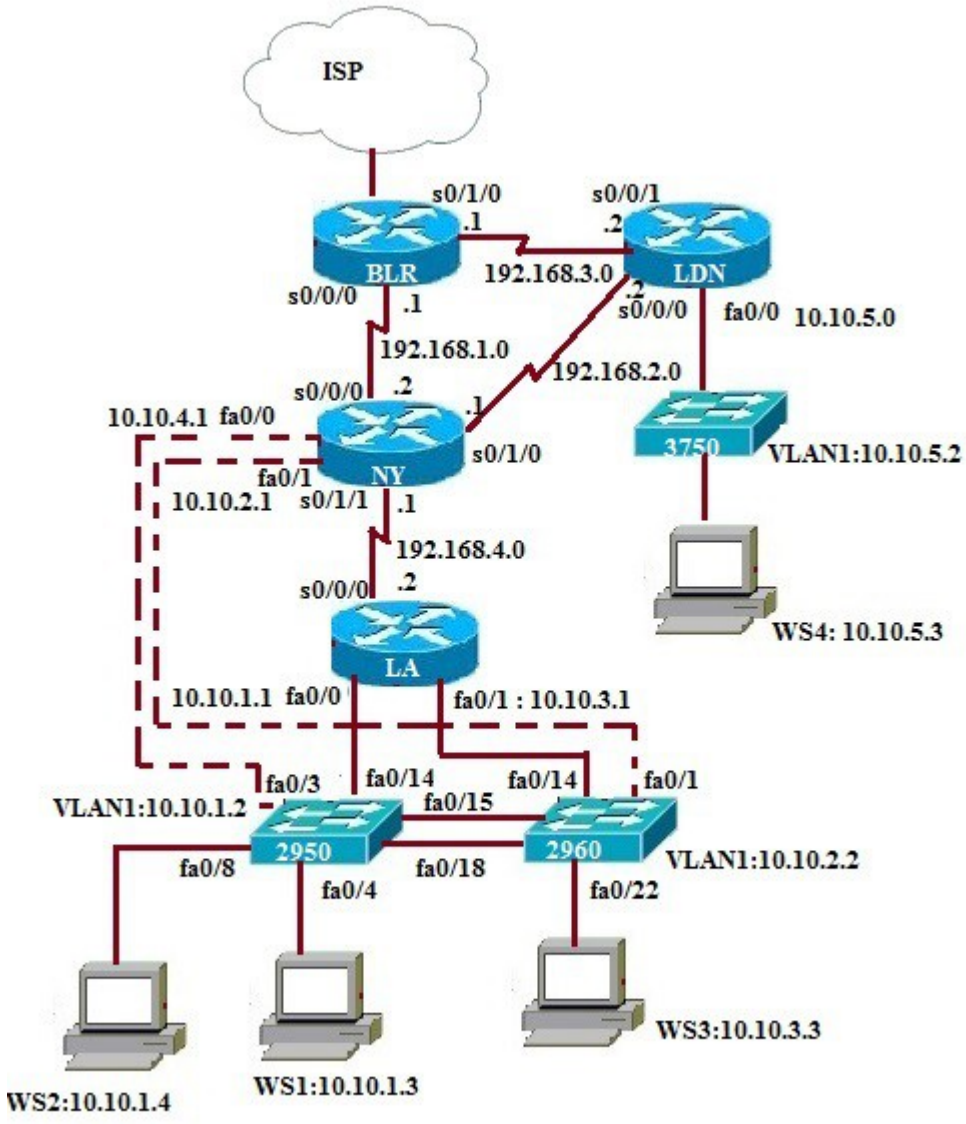
LAB MANUAL FOR CCENT

Version 4.0

CONTENTS:

1. BASIC EXERCISES

Note: *Please refer to the below default network Diagram for all the exercises given in this manual*



1.1: Lab Exercise 1: Entering User EXEC prompt on a Router, and exit

Description: A basic exercise, that shows how to enter into privileged EXEC prompt from user mode prompt, and exit from the same.

Instructions:

1. Enter into privileged mode
2. Get back to the user mode

BLR>

BLR>enable
Password: Cisco
BLR#disable
BLR>

Back

1.2: Lab Exercise 2: Introduction to Basic User Interface

Description: This exercise helps to get familiar with the user mode, privileged mode, CLI and basic commands.

Instructions:

1. Press enter to get the router prompt
2. In the user mode, type the command ? used to view all the commands in user mode
3. Enter into privileged mode
4. In the privileged mode, type the command ? to view all the commands in privileged mode
5. The command show ? displays all the show commands like show access-list, show banner, show cdp, show hosts, show flash, show protocols etc
6.The command show running-config displays the running configuration
7. Press space bar to view more information
8. The command "exit or disable" logs out the router

BLR>
BLR>?
BLR>enable
BLR#
BLR#?
BLR#show ?
BLR#show running-config
BLR#exit

Or

BLR#disable

Back

1.3: Lab Exercise 3: Basic show commands

Description: A basic exercise to get familiar and understand the various show commands available in the privileged mode.

Instructions:

1. Enter into privileged mode
2. Show running-config displays the active configuration in memory. The currently active configuration script running on the router is referred to as the running-config in the router's CLI
3. Show flash memory. Flash memory is a special kind of memory that contains the operating system

image file(s) on the router
4. Show history command displays all the past commands still present in router's memory
5. Show protocols command displays the protocols running on your router
6. Show version command displays critical information, such as router platform type, operating system revision, operating system last boot time and file location, amount of memory, number of interfaces, and configuration register
7. Show clock command displays the router's clock
8. Show hosts command displays list of hosts and all their interfaces IP Addresses
9. Show users command displays list of users who are connected to the router
10. Show interfaces command displays detailed information about each interface

BLR>enable
BLR#show running-config
BLR#show flash
BLR#show history
BLR#show protocols
BLR#show version
BLR#show clock
BLR#show hosts
BLR#show interfaces

Back

1.4 Short form commands

1. copy running-config startup-config command can be interpreted and used in short form as "copy run start" command.

2. show running-config command can be interpreted and used in short form as "show run" command.

3. show startup-config command can be interpreted and used in short form as "show start" command.

4. copy running-config tftp command can be interpreted and used in short form as "copy run tftp" command.

5. copy tftp startup-config command can be interpreted and used in short form as "copy tftp start" command.

Note: We can also use **UP ARROW** and **DOWN ARROW** keys to get the previously typed command in the simulator.

Back

2. ROUTING IOS FUNDAMENTAL EXERCISES

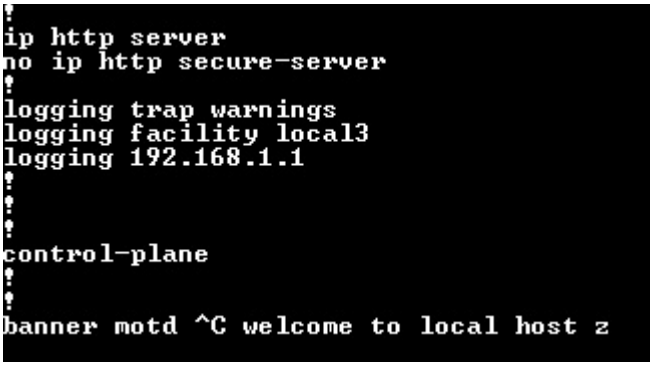
2.1: Lab Exercise 1: Banner MOTD-Setting message of the day

Description: This exercise helps in understanding the procedure of setting message of the day and the show banner command. Note that the banner is set in a single command line here. You can also use multi-line banner motd command.

Instructions:

1. Enter into privileged mode
2. Enter into global Configuration Mode
3. Set banner to: "Welcome to local host". Starting and ending character of the banner should be "Z" (Do not use quotes)
4. Use “show running-configgr” command to view the banner that has been set

BLR>enable
BLR#configure terminal
BLR(config)#banner motd Z Welcome to local host Z
BLR(config)#exit
BLR#show running-configuration



Back

2.2: Lab Exercise 2: Setting Host Name

Description: This basic exercise illustrates the steps required to set a hostname to a router.

Instructions:

1. Enter into privileged mode
2. Enter into global Configuration Mode
3. Set hostname as cisco

BLR>enable
BLR#configure terminal
BLR(config)#hostname cisco
BLR(config)#exit

BLR#show running-config

Back

2.3: Lab Exercise 3: Router Interface Configuration

Description: In this lab, you will learn to enable interfaces on a router i.e, configure Serial 0/0/0 and FastEthernet 0/0 interfaces on a router with specified IP Address and Subnet Mask.

Instructions:

1. Enter into privileged mode
2. Enter into global Configuration Mode
3. Set IP Address of Serial 0/0/0 as 192.168.1.2 and Subnet Mask as 255.255.255.5
4. Set IP Address of FastEthernet 0/0 as 192.168.0.130 and Subnet Mask as 255.255.255.0

BLR>enable
BLR#configure terminal
BLR(config)#interface serial 0/0/0
BLR(config-if)#ip address 192.168.1.2 255.255.255.0
BLR(config-if)#exit
BLR(config)#interface fastethernet 0/0
BLR(config-if)#ip address 192.168.0.130 255.255.255.0

2.4: Lab Exercise 4: Setting Bandwidth on an interface

Not Available in Demo Version

2.5: Lab Exercise 5: Setting Console Password

Not Available in Demo Version

2.6: Lab Exercise 6: Setting Telnet Password

Not Available in Demo Version

2.7: Lab Exercise 7: Setting Auxiliary Password to Router

Not Available in Demo Version

2.8: Lab Exercise 8: Configuring Minimum password length

Not Available in Demo Version

2.9: Lab Exercise 9: Implementing exec-timeout command

Not Available in Demo Version

2.10: Lab Exercise 10: Copy Running Configuration to Startup Configuration

Not Available in Demo Version

2.11: Lab Exercise 11: Router CDP Configuration

Not Available in Demo Version

2.12: Lab Exercise 12: Show CDP Configuration

Not Available in Demo Version

2.13: Lab Exercise 13: Show CDP Neighbors

Not Available in Demo Version

2.14: Lab Exercise 14: Bringing-up a router Interface

Not Available in Demo Version

2.15: Lab Exercise 15: Set Keepalive Timers

Not Available in Demo Version

2.16: Lab Exercise 16: Configuring enable and secret pasword and service password-encryption

Not Available in Demo Version

2.17: Lab Exercise 17: Host Table

Not Available in Demo Version

2.18: Lab Exercise 18: Viewing ARP Entries

Not Available in Demo Version

2.19: Lab Exercise 19: Telnet

Not Available in Demo Version

2.20: Lab Exercise 20: TFTP

Not Available in Demo Version

2.21 Lab Exercise 21: Configuring Cisco Routers for Syslog

Not Available in Demo Version

2.22 Lab Exercise 22: Configure and Verify NTP

Not Available in Demo Version

3. EXERCISES ON ROUTING FUNDAMENTALS

3.1: Lab Exercise 1: Introduction to IP

Description: This lab exercise is to learn assigning IP address to routers and pinging between them to test connectivity

Instructions:

1. Connect to router BLR, configure its ip address of serial interfaces
2. Connect to router NY, configure its ip address of serial interfaces.
3. Connect to router LD, configure its ip address of serial interfaces.
4. Use the command "show ip interface brief" to verify that the lines and protocols are up for all NY's interfaces
5. Display NY's running configuration to verify that the IP addresses appear
6. Display detailed IP information about each interface on NY

```
BLR>enable
BLR#configure terminal
BLR(config)#interface serial 0/0/0
BLR(config-if)#ip address 192.168.1.2 255.255.255.0
BLR(config-if)#no shutdown
BLR(config-if)#exit
BLR(config)#interface serial 0/1/0
BLR(config-if)#ip address 192.168.3.1 255.255.255.0
BLR(config-if)#no shut
BLR(config-if)#exit
```

```
NY>enable
Password:Cisco
NY#configure terminal
NY(config)#interface serial 0/0/0
NY(config-if)#ip address 192.168.1.1 255.255.255.0
NY(config-if)#no shutdown
NY(config-if)#exit
NY(config)#interface serial 0/1/0
NY(config-if)#ip address 192.168.2.1 255.255.255.0
NY(config-if)#no shutdown
```

```
LDN>enable
Password:Cisco
LDN#configure terminal
LDN(config)#interface serial 0/0/0
LDN(config-if)#ip address 192.168.2.2 255.255.255.0
LDN(config-if)#no shutdown
LDN(config-if)#exit
LDN(config)#interface serial 0/0/1
LDN(config-if)#ip address 192.168.3.2 255.255.255.0
LDN(config-if)#no shutdown
LDN(config-if)#exit
```


NY#ping 192.168.2.2
NY#ping 192.168.3.2
NY#show ip interface brief
NY#show running-config
NY#show ip interface

The sample output of "show ip interface brief" command is shown below

```
NY#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            10.10.1.1       YES NVRAM  up                    up

FastEthernet0/1            10.10.2.1       YES NVRAM  up                    up

Serial0/0/0                192.168.1.1     YES NVRAM  up                    up

Serial0/1/0                192.168.2.1     YES NVRAM  up                    up

Serial0/1/1                unassigned      YES NVRAM  administratively down down

NY#
```

Back

3.2: Lab Exercise 2: Configuring Static Routes

Description: Configure static route 10.10.1.0 mask 255.255.255.0 with next hop address of 192.168.1.1

Syntax: ip route prefix mask {address|interface} [distance]

prefix mask: It is the ip route prefix and mask for the destination.

address|interface: Use either the next hop router ip or the local router outbound interface used to reach the destination.

distance: It is the administrative distance and an optional parameter.

Instructions:

1. Enter into Global Configuration Mode
2. Disable IP Routing
3. Re-enable IP Routing
4. Configure a static route with destination sub network number as 10.10.1.0 with subnet mask as 255.255.255.0, and IP address of the next-hop router in the destination path to 192.168.1.1

BLR>enable
BLR#configure terminal
BLR(config)#no ip routing
BLR(config)#ip routing
BLR(config)#ip route 10.10.1.0 255.255.255.0 192.168.1.1

Note: "no ip routing" command used in the above exercise is used to remove any previously configured routing information.

3.3: Lab Exercise 3: Implement and Verify Static Routes

Not Available in Demo Version

3.4: Lab Exercise 4: Configuring Default Route

Not Available in Demo Version

3.5: Lab Exercise 5: Implement and Verify Default Routes

Not Available in Demo Version

3.6: Lab Exercise 6: Configuring Loopback Interface

Not Available in Demo Version

3.7: Lab Exercise 7: Connectivity Tests with Traceroute

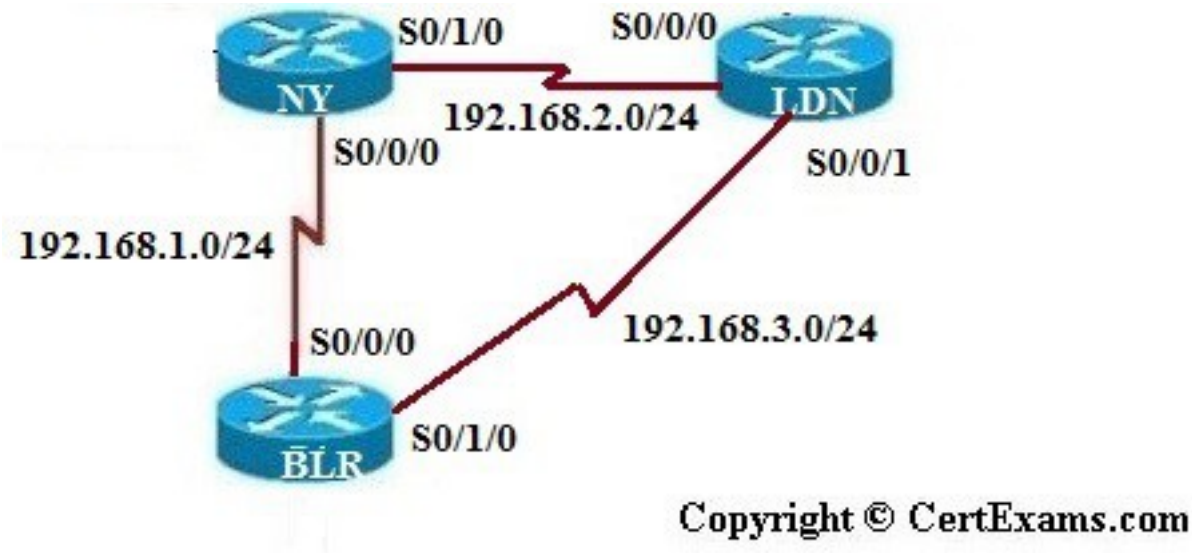
Not Available in Demo Version

3.8: Lab Exercise 8: Configuring RIP

Not Available in Demo Version

4. EXERCISES ON RIP Routing Scenarios

4.1: Lab Exercise 1: RIP Routing Configuration Scenario



Description: The purpose of this exercise is to configure RIP on all the devices and test for ping and trace commands.

The router rip command selects RIP as the routing protocol. The network command assigns a major network number that the router is directly connected to. The RIP routing process associates interface addresses with the advertised network number and begins RIP packet processing on the specified interfaces.

Instructions:

1. Assign the IP address of all the devices as given below
2. Bring all the interfaces to up
3. Configure RIP on all the devices
4. From BLR issue a ping and trace command to NY and LD

IP Address assignment table

Device	Interface	IP Address	Mask
NY	S0/0/0	192.168.1.1	255.255.255.0
	S0/1/0	192.168.2.1	255.255.255.0
BLR	S0/0/0	192.168.1.2	255.255.255.0
	S0/1/0	192.168.3.1	255.255.255.0
LDN	S0/0/0	192.168.2.2	255.255.255.0

	S0/0/1	192.168.3.2	255.255.255.0

On NY

```
NY>enable
NY#configure terminal
NY(config)#interface serial 0/0/0
NY(config-if)#ip address 192.168.1.1 255.255.255.0
NY(config-if)#no shutdown
NY(config-if)#exit
NY(config)#interface s0/1/0
NY(config-if)#ip address 192.168.2.1 255.255.255.0
NY(config-if)# no shutdown
NY(config-if)#exit
NY(config)#router rip
NY(config-router)#network 192.168.1.0
NY(config-router)#network 192.168.2.0
```

On BLR

```
BLR>enable
BLR#configure terminal
BLR(config)#interface serial 0/0/0
BLR(config-if)#ip address 192.168.1.2 255.255.255.0
BLR(config-if)# no shutdown
BLR(config-if)#exit
BLR(config)#interface serial 0/1/0
BLR(config-if)#ip address 192.168.3.1 255.255.255.0
BLR(config-if)#no shutdown
BLR(config-if)#exit
BLR(config)#router rip
BLR(config-router)#network 192.168.1.0
BLR(config-router)#network 192.168.3.0
```

On LD:

```
LDN>enable
LDN#configure terminal
LDN(config)#interface serial 0/0/0
LDN(config-if)#ip address 192.168.3.2 255.255.255.0
LDN(config-if)#no shutdown
LDN(config-if)#exit
LDN(config)#interface serial 0/0/1
LDN(config-if)#ip address 192.168.2.2 255.255.255.0
LDN(config-if)#no shutdown
LDN(config-if)#exit
```


LDN(config)#router rip
LDN(config-router)#network 192.168.3.0
LDN(config-router)#network 192.168.2.0

On BLR

BLR#ping 192.168.2.2
BLR#traceroute 192.168.2.2

BLR#ping 192.168.2.1
BLR#traceroute 192.168.2.1

Back

4.2: Lab Exercise 2: Viewing IP RIP Information

Description: The purpose of this exercise is to view important information on IP RIP.

Show ip route command displays the current state of the routing table and this command is to be used in EXEC mode.

"Show ip protocols" command displays the parameters and current state of the active routing protocol processes and this command is to be used in EXEC mode.

Instructions:

1. Enter global configuration mode, and enable RIP routing on the router
2. Associate network 192.168.1.0 with RIP routing process
3. Issue the command that displays all entries in the Routing Table
4. Type the command that displays information about the IP routing protocols.

NY>enable
NY#configure terminal
NY(config)#interface s 0/0/0
NY(config-if)#ip address 192.168.1.1 255.255.255.0
NY(config-if)#no shutdown
NY(config-if)#exit
NY(config)#router rip
NY(config-router)#network 192.168.1.0
NY(config-router)#exit
NY(config)#exit
NY#show ip route
NY#show ip protocols

Below is the show output of "show ip route" command


```
NY#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, Serial0/1/1
     10.0.0.0/24 is subnetted, 2 subnets
C       10.10.1.0 is directly connected, FastEthernet0/0
C       10.10.2.0 is directly connected, FastEthernet0/1
R    192.168.0.0/24 [120/1] via 192.168.1.2, 00:00:24, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/0
C    192.168.2.0/24 is directly connected, Serial0/1/0
NY#
```

Below is “show ip protocols” command output where ip protocol configured is RIP.

```
NY#show ip protocols
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 26 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 1, receive any version
    Interface             Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0       1     1 2
    FastEthernet0/1       1     1 2
    Serial0/0/0           1     1 2
    Serial0/1/0           1     1 2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
    192.168.0.0
    192.168.1.0
    192.168.2.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.2           120      00:04:29
    192.168.1.2           120      00:00:22
 --More--
  Distance: (default is 120)
```

Back

4.3: Lab Exercise 3: Configuring RIP V2

Not Available in Demo Version

4.4 : Lab Exercise 4: RIP2 Routes

Not Available in Demo Version

5. Exercises on Access-Lists

5.1: Lab Exercise 1: Creating a Standard Access List

Description: Create an access-list and configure the same according to a given set of rules.

Instructions:

1. Enter into Global Configuration Mode
2. Create an IP access-list to permit traffic from address 192.168.1.0 network and deny all other traffic. Use 1 as IP access-list number.
3. Create an access-list 2 that blocks only the single IP address 192.168.2.2
4. Type the command used for permitting packets from any IP Address. Use Access-list number as 2

```
NY>enable
NY#configure terminal
NY(config)#access-list 1 permit 192.168.1.0
NY(config)#access-list 2 deny 192.168.2.2
NY(config)#access-list 2 permit any
```

Back

5.2: Lab Exercise 2: Applying an Access List to an Interface

Description: Apply the access-list on both incoming and outgoing interfaces.

Instructions:

1. Enter into Interface Configuration Mode.
2. Use no shut down command on interface
3. Assuming that an access-list 1 is created, apply it to the interface Fastethernet0/0 as an inbound access-list
4. Apply an access-list 1 to interface serial 0/0/0 as an outbound access-list

```
NY>enable
NY#configure terminal
NY(config)#interface serial 0/0/0
NY(config-if)#no shutdown
NY(config-if)#ip access-group 1 in
NY(config-if)#ip access-group 1 out
```

Back

5.3: Lab Exercise 3: View Access List Entries

Description: Configure standard access-list #1 to permit ip 192.168.2.2 and view access-list entries by using appropriate show command.

Instructions:

1. Enter into Global Configuration Mode
2. Create an Access-list that permits traffic from address 192.168.2.2. Use access-list number 1. Exit from the global configuration mode
3. Use the show command to see the Access-list

```
NY>enable
NY#configure terminal
NY(config)#access-list 1 permit 192.168.2.2
NY(config)#exit
NY#show access-list
```

The screenshot of "show access-list" command output is shown below

Back

5.4: Lab Exercise 4: Standard Access List Scenario Lab 1

Not Available in Demo Version

5.5: Lab Exercise 5: Configuring and Verifying Standard Access List

Not Available in Demo Version

5.6: Lab Exercise 6: Configuring and Verifying Extended Access List

Not Available in Demo Version

5.7: Lab Exercise 7: Named Access-Lists

Not Available in Demo Version

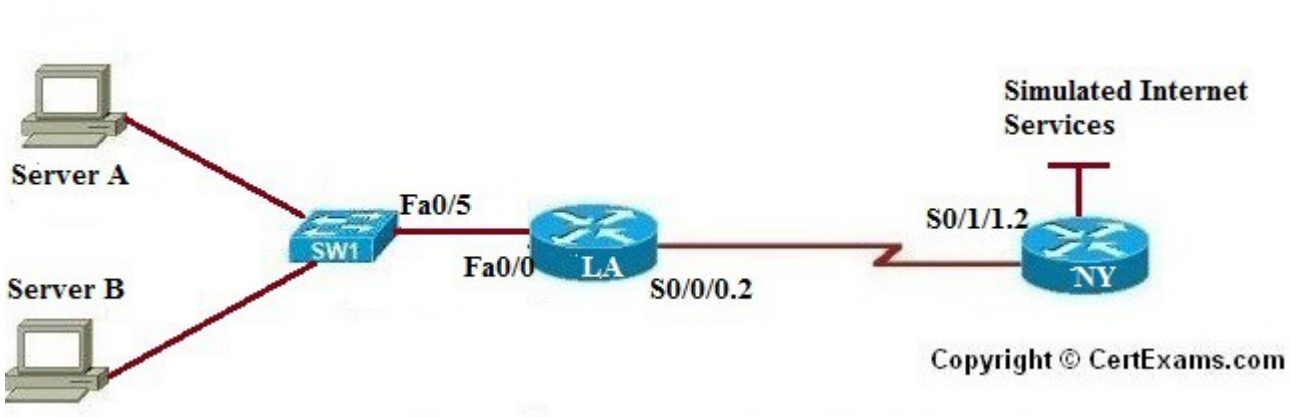
6. EXERCISES ON NETWORK ADDRESS TRANSLATION

NAT stands for Network Address Translation is used to perform address translation between two networks, which are identified as the inside network and the outside network in NAT terminology.i.e, there are primarily two ways a NAT can be defined in a network.

One is NAT inside, where we define the inside local, and inside global ip addresses; and the other is NAT outside, where we define the outside local, and outside global IP addresses.

Note: Please refer the below Network Diagram and IP Address Assignment Table for all the exercises in this section.

Network Diagram: Given Below



IP Address Assignment Table

Device	Interface	IP Address	Mask
NY	S0/1/1.2 Loopback0	209.165.201.17 192.31.7.1	255.255.255.252 255.255.255.255
LA	S0/0/0.2 Fa0/0	209.165.201.18 10.10.1.1	255.255.255.252 255.255.255.0
PC-A		10.10.1.3	255.255.255.0
PC-B		10.10.1.4	255.255.255.0

6.1: Lab Exercise 1: NAT Scenario 1

Description: The purpose of this exercise is to configure NAT on the source router (NAT inside source)

and test for connectivity by pinging a remote router.

NAT Mapping Table for Inside Source

Inside Local	Inside Global
10.10.1.3	209.165.201.19
10.10.1.4	209.165.201.20

Instructions:

1. Assign IP addresses to all the devices as per the IP address assignment table
2. Enable routing on all routers.
3. Create IP NAT Mapping (Hint: use inside source static command) on LA
4. Define IP NAT Inside and IP NAT Outside interfaces on LA
5. Test for Connectivity by issuing ping command

Three steps are required to configure static NAT:

1. Configure private/public IP address mapping using the ip nat inside source static PRIVATE_IP PUBLIC_IP command
2. Configure the router's inside interface using the ip nat inside command
3. Configure the router's outside interface using the ip nat outside command

```
NY>enable
NY#conf term
NY(config)#interface serial 0/1/1.2
NY(config-subif)#ip address 209.165.201.17 255.255.255.252
NY(config-subif)#no shutdown
NY(config-subif)#exit
NY(config)#router rip
NY(config-router)#network 209.165.201.0
NY(config-router)#exit

LA>enable
LA#configure terminal
LA(config)#interface fastethernet 0/0
LA(config-if)#ip address 10.10.1.1 255.255.255.0
LA(config-if)#no shutdown
LA(config-if)#exit
LA(config)#interface serial 0/0/0.2
LA(config-subif)#ip address 209.165.201.18 255.255.255.252
LA(config-subif)#no shutdown
LA(config-subif)#exit
LA(config)#router rip
LA(config-router)#network 209.165.201.0
LA(config-router)#network 10.10.1.0
```



```
LA>enable
LA#conf term
LA(config)#ip nat inside source static 10.10.1.3 209.165.201.19
LA(config)#ip nat inside source static 10.10.1.4 209.165.201.20
LA(config)#interface serial 0/0/0.2
LA(config-subif)#ip nat outside
LA(config-subif)#exit
LA(config)#interface fastethernet 0/0
LA(config-if)#ip nat inside
LA(config-if)#exit
LA(config)#exit
```

"show ip nat translations" command output is shown below

```
LA#show ip nat translations
Pro Inside global     Inside local       Outside local      Outside global
--- 209.165.201.19    10.10.1.3          ---                ---
--- 209.165.201.20    10.10.1.4          ---                ---
LA#
```

Here, we are telling the router LA to perform NAT on packets coming into the router on the inside interface Fa0/0. More specifically the router would identify which of these packets have a source IP address of 10.10.1.3 and would change it to 209.165.201.19 before forwarding the packet out the outside interface serial0/0/0.2.

```
NY#:ping 209.165.201.19
```

Back

6.2: Lab Exercise 2: NAT Scenario 2

Not Available in Demo Version

6.3: Lab Exercise 3: Configuring Dynamic NAT Scenario I

Not Available in Demo Version

6.4: Lab Exercise 4: NAT and PAT

Not Available in Demo Version

7. Exercises on DHCP

7.1: Lab Exercise 1: Configuring cisco router as a DHCP Server

Description: This lab exercise demonstrates the required commands for DHCP Server configuration on a cisco router.

Instructions:

1. Issue service dhcp command on router LA that enables and disables the DHCP server feature on router. By default, this is enabled.
2. Create an addressing pool for dhcp.
3. Issue network command that specifies the range of IP addresses to be assigned to clients.
4. Assign the domain-name to the client.
5. In order to resolve Host names to IP addresses, client computers require the IP addresses of DNS (Domain Name Service) servers. Use dns-server command that allows assigning upto 8 DNS server addresses to the client, but however in simulator only 1 address is allowed.
6. Specify the default-router address using default-router command that allows assigning upto 8 default-gateway addresses to the client for this range of addresses.
7. Specify the duration of the lease, which if omitted results to default 1 day.

```
LA>enable
LA#con ter
LA(config)#service dhcp
LA(config)#ip dhcp pool newpool
LA(config-dhcp)#network 192.168.100.0 255.255.255.0
LA(config-dhcp)#domain-name xyz.com
LA(config-dhcp)#dns-server 192.168.100.2
LA(config-dhcp)#default-router 192.168.100.1
LA(config-dhcp)#lease 2
LA(config-dhcp)#exit
LA(config)#exit
LA#show ip dhcp pool
```

```
LA#show ip dhcp pool

Pool newpool :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 192.168.100.1        192.168.100.1    - 192.168.100.254   0
LA#
```

Back

7.2: Lab Exercise 2: DHCP client configuration

Description: This lab exercise demonstrates DHCP client configuration i.e, Configuring an interface on the router to use DHCP to acquire its IP address.

Instructions:

1. Configure DHCP server on LA router.
2. Enter into interface configuration mode on router NY with appropriate commands.
3. Use the command "ip address dhcp" that configures the specified interface to acquire its IP Address from the DHCP server, verify the same using "show ip interface brief" on the router.

```
LA>enable
LA#con ter
LA(config)#service dhcp
LA(config)#ip dhcp pool newpool
LA(config-dhcp)#network 192.168.100.0 255.255.255.0
LA(config-dhcp)#domain-name xyz.com
LA(config-dhcp)#dns-server 192.168.100.2
LA(config-dhcp)#default-router 192.168.100.1
LA(config-dhcp)#lease 2
LA(config-dhcp)#exit
LA(config)#exit
LA#show ip dhcp pool
```

```
NY>enable
NY#configure terminal
NY(config)#interface fastethernet 0/1
NY(config-if)#ip address dhcp
NY(config-if)#exit
NY(config)#exit
NY#show ip interface brief
```

```
NY#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            10.10.4.1       YES NVRAM  up                    up
FastEthernet0/0.1          unassigned      YES unset  up                    up
FastEthernet0/0.2          unassigned      YES unset  up                    up
FastEthernet0/1            unassigned      YES DHCP   up                    up
Serial0/0/0                192.168.1.1     YES NVRAM  up                    up
Serial0/1/0                192.168.2.1     YES NVRAM  up                    up
Serial0/1/1                192.168.4.1     YES NVRAM  up                    up
Serial0/1/1.2              209.165.201.17  YES NVRAM  up                    up
Loopback0                  192.31.7.1      YES NVRAM  up                    up
Loopback1                  unassigned      YES NVRAM  up                    up
```


Note: DHCP provides dynamic addressing information to hosts on a network. It allows devices to dynamically acquire their addressing information. The main purpose of the DHCP server is to provide IP configuration parameters to hosts such as the default gateway, domain name, Domain Name System – DNS.

DHCP uses UDP protocol. Port 67 for requests and 68 for replies.

Note that as per cisco 12.2 release, only ethernet interfaces are supported for DHCP.

Back

8. Exercises on PPP

8.1: Lab Exercise 1: PPP Configuration

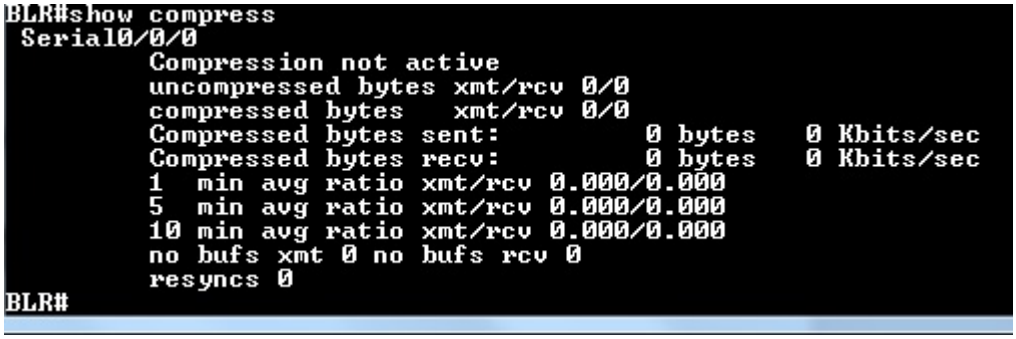
Description: This exercise helps to understand how Point to Point Protocol encapsulation works .

Instructions:

1. Configure for PPP on router BLR Serial 0/0/0
2. Configure "stac" compression on BLR
3. Configure for PPP on router NY serial 0/0/0
4. Configure "stac" compression on NY
5. Verify PPP compression by using show compress command

```
NY>enable
NY#configure terminal
NY(config)#interface serial 0/0/0
NY(config-if)#ip address 192.168.1.1 255.255.255.0
NY(config-if)#encapsulation ppp
NY(config-if)#compress stac

BLR>enable
BLR#configure terminal
BLR(config)#interface serial 0/0/0
BLR(config-if)#ip address 192.168.1.2 255.255.255.0
BLR(config-if)#encapsulation ppp
BLR(config-if)#compress stac
BLR(config-if)#exit
BLR(config)#exit
BLR#show compress
```

Back

9. Exercises on IPv6

9.1: Lab Exercise 1: Enabling IPv6 on a cisco router

Description: This lab demonstrates the steps required to enable ipv6 on a Cisco router.

Instructions

1. Enter into privileged mode on router NY.
2. Enter into global configuration mode.
3. Enter the command "ipv6 unicast-routing" that enables the forwarding of IPv6 unicast datagrams globally on the router.

NY>enable
NY#configure terminal
NY(config)#ipv6 unicast-routing
NY(config)#exit
NY#exit
NY>

Note: The first step of enabling IPv6 on a Cisco router is the activation of IPv6 traffic forwarding to forward unicast IPv6 packets between network interfaces. By default, IPv6 traffic forwarding is disabled on Cisco routers.

The **ipv6 unicast-routing** command is used to enable the forwarding of IPv6 packets between interfaces on the router.

Back

9.2: Lab Exercise 2: Enabling IPv6 on cisco router interface

Description: This lab demonstrates the steps required to enable ipv6 on a cisco router interface.

Instructions

1. Enter into privileged mode on router NY

2. Enter into global configuration mode.
3. Enter the command "ipv6 unicast-routing" that enables the forwarding of IPv6 unicast datagrams globally on the router.
4. Enter into interface configuration mode and then use the command "ipv6 enable" to enable ipv6 processing on the interface and the command also automatically configures an IPv6 link-local address on the interface.

```
NY>enable
NY#configure terminal
NY(config)#ipv6 unicast-routing
NY(config)#interface serial 0/0/0
NY(config-if)#ipv6 enable
NY(config-if)#exit
NY(config)#exit
```

Note: To configure a router so that it uses only link local addresses, you only have to give ipv6 enable command. Issuing an ipv6 address command automatically configure link local addresses.

Back

9.3: Lab Exercise 3: Configuring IPv6 on a cisco router interface with IPv6 address in EUI-format

Not Available in Demo Version

9.4: Lab Exercise 4: Configuring IPv6 on a cisco router interface with IPv6 address in general form

Not Available in Demo Version

9.5: Lab Exercise 5: Configuring loopback interface with Ipv6 address

Not Available in Demo Version

9.6: Lab Exercise 6: Configuring IPv6 on two router interfaces connected directly and pinging the distant interface using console

Not Available in Demo Version

9.7: Lab Exercise 7: Configuring IPv6 static route

Not Available in Demo Version

9.8: Lab Exercise 8: Configuring IPv6 static default route

Not Available in Demo Version

9.9: Lab Exercise 9: Implement and verify IPv6 static route

10. Exercises on IPv6 Routing Protocols

10.1: Lab Exercise 1: Enabling RIPng on a cisco router interface

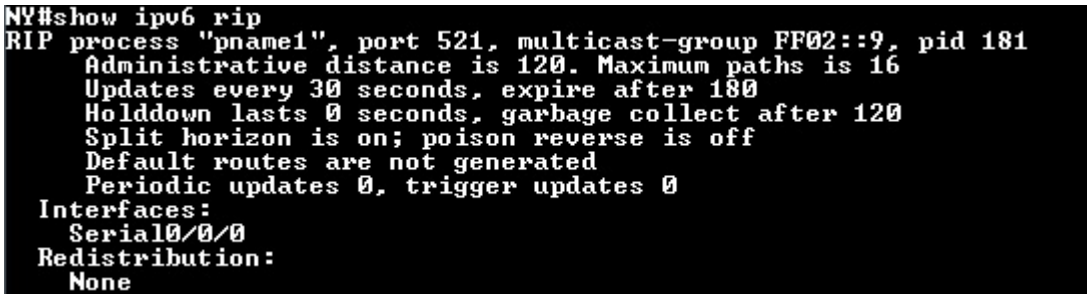
Description: This lab exercise demonstrates enabling RIPng for IPv6 (next-generation RIP protocol) on a router interface.

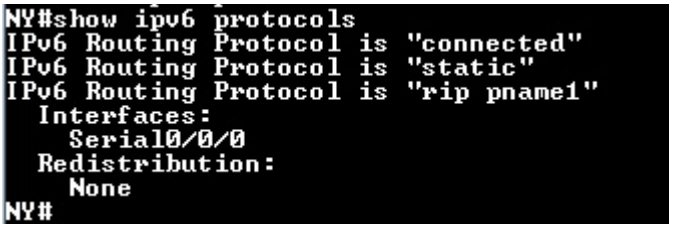
Instructions:

1. Enter into privileged mode on router NY.
2. Enter into global configuration mode.
3. Enter the command "ipv6 unicast-routing" that enables the forwarding of IPv6 unicast datagrams globally on the router.
4. Enter into interface configuration mode and then use the command "ipv6 rip <name> enable command to enable the specified RIP routing process on an interface.
5. Issue "show ipv6 rip" command that displays information about the configured RIP routing processes.

```
NY>enable
NY#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
NY(config)#ipv6 unicast-routing
NY(config)#interface serial 0/0/0
NY(config-if)#ipv6 rip pname1 enable
NY(config-if)#exit
NY(config)#exit
NY#show ipv6 rip
NY#show ipv6 protocols
```

The screenshot of “show ipv6 rip” and “show ipv6 protocols” command output is shown below





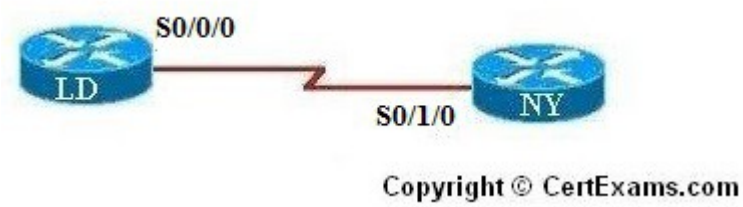
Note: ipv6 rip <name> enable command enables the specified IPv6 RIP routing process on an interface.

The process name is only significant within the router, and allows you to run more than one RIP process if you want to. Because it is only locally significant, every router can have a different RIP process name without conflict, although we generally don't recommend this, as it can become confusing to manage.

Back

10.2: Lab Exercise 2: Enabling RIPng on two routers and pinging between them

Description: This lab exercise demonstrates testing the connectivity using ping between two routers configured with RIP routing processes.



Instructions:

1. Enter into privileged mode on router London (LD).
2. Enter into global configuration mode.
3. Enter the command "ipv6 unicast-routing" that enables the forwarding of IPv6 unicast datagrams globally on the router.
4. Enter into interface configuration mode and then assign IPv6 address on the interface.
and then use the command "ipv6 rip <name> enable command to enable the specified RIP routing process on an interface.
5. Use the command "no shutdown" to start the protocol and issue copy run start config command
6. Enter into privileged mode on router Newyork (NY).
7. Enter into global configuration mode.
8. Enter the command "ipv6 unicast-routing" that enables the forwarding of IPv6 unicast datagrams globally on the router.
9. Enter into interface configuration mode and then assign IPv6 address on the interface.
and then use the command "ipv6 rip <name> enable command to enable the specified RIP routing process on an interface.
10. Use the command "no shutdown" to start the protocol and issue copy run start config command
11. Ping LDN from NY and test for connectivity.

```
LDN>enable
LDN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
LDN(config)#ipv6 unicast-routing
LDN(config)#interface serial 0/0/0
LDN(config-if)#ipv6 address 2001:3abc:d00:4ab:2::1/64
LDN(config-if)#ipv6 rip process1 enable
LDN(config-if)#no shutdown
LDN(config-if)#exit
LDN(config)#exit

NY>enable
NY#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
NY(config)#ipv6 unicast-routing
NY(config)#interface serial 0/1/0
NY(config-if)#ipv6 address 2001:3abc:d00:4ab:2::2/64

NY(config-if)#ipv6 rip process1 enable
NY(config-if)#no shutdown
NY(config-if)#exit
NY(config)#exit

NY#ping ipv6 2001:3abc:d00:4ab:2::1
```

Back

10.3: Lab Exercise 3: Entering RIPng router configuration mode and setting global parameters on a cisco router

Not Available in Demo Version

10.4: Lab Exercise 4: Traceroute lab

Not Available in Demo Version

10.5: Lab Exercise 5: General IPv6 configuration on cisco router

Not Available in Demo Version

11. Exercises On MPLS

11.1: Lab Exercise 1: Configuring a Router for MPLS Forwarding and verifying the configuration of MPLS forwarding.

Description: MPLS forwarding on Cisco routers requires that Cisco Express Forwarding be enabled. This lab exercise demonstrates the necessary commands to enable the Cisco Express Forwarding.

Instructions:

1. Enable privileged EXEC mode.
2. Enter into configuration mode
3.Enable the Cisco express forwarding on the router.

```
BLR>enable
BLR#conf term
BLR(config)#ip cef
BLR(config)#exit
```

Back

11.2: Lab Exercise 2: Enabling MPLS

Description: The following example shows how to configure MPLS hop-by-hop forwarding on the interface.

Instructions:

1. Enable privileged EXEC mode.
2. Enter into configuration mode
3. Enable the Cisco express forwarding on the router
4. Enter into interface configuration mode
5. Configures MPLS hop-by-hop forwarding on the interface.
6. Exit interface configuration mode

```
BLR>enable
BLR#conf term
BLR(config)#ip cef
BLR(config)#interface s 0/0/0
BLR(config-if)#mpls ip
BLR(config-if)#exit
BLR(config)#exit
```

Note: Router(config)#mpls ip

The above command configures MPLS hop-by-hop forwarding globally.
The 'mpls ip'command is enabled by default; you do not have to specify this command.Globally enabling MPLS forwarding does not enable it on the router interfaces. You must enable MPLS forwarding on the interfaces as well as for the router.

Use of the **mpls ip** command on an interface triggers the transmission of discovery Hello messages for the interface. When two platforms are directly connected by multiple packet links, the same label distribution protocol (LDP or TDP) must be configured for all of the packet interfaces connecting the platforms.

Back

11.3 Lab Exercise 3: Configuring MPLS LDP

Not Available in Demo Version

11.4: Lab Exercise 4: Configuring MPLS using RIP

Not Available in Demo Version

11.5: Lab Exercise 5: MPLS Show commands

Not Available in Demo Version

12. CISCO SWITCH IOS

12.1 Logging In To The Switch

When Catalyst switches are configured from the CLI that runs on the console or a remote terminal, the Cisco IOS Software provides a CLI called the EXEC. The EXEC interprets the commands that are entered and carries out the corresponding operations.

For security purposes, the EXEC has the following two levels of access to commands:

1. User mode: Typical tasks include those that check the status of the switch, such as some basic show commands.

2. Privileged mode: Typical tasks include those that change the configuration of the switch. This mode is also known as enable mode. If you have the password that gets you to this privileged enable mode, you basically will have access to all possible device configuration commands.

To change from user EXEC mode to privileged EXEC mode, enter the enable command.
The switch then prompts for the enable password if one is configured. Enter the correct enable password.
By default, the enable password is not configured.

12.2: Lab Exercise 1: Introduction to switch

Description: A basic exercise to get familiar with the different commands related to switch. The switch initial startup status can be verified using the below status commands:

Instructions:

1. Connect to switch and you should see the user mode prompt
2. Show version command displays the IOS version of the switch
3. Show interfaces command displays the interfaces of the switch
4. Show running-config displays the running configuration

```
LA-2950>enable
Password:CCNA
LA-2950#show version
LA-2950#show interfaces
LA-2950#show running-config
```

Show version: Displays the configuration of the system hardware and the currently loaded IOS software version information , the screenshot of "show version" command is given below.

Show running-config: Displays the current active running configuration of the switch. This command requires privileged EXEC mode access. The screenshot of "show running-config" command is given below.

```
LA-2950#show running-config
Building configuration...

Current configuration : 1712 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname LA-2950
!
aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
enable secret 5 $1$Jjfn$.rfVfzuQI/Ua9f61PRZXX/
!
username networkadmin privilege 15 secret 5 $1$hAoN$AMieiPvJ7mb0ixrlI04Du.
username netmonitor secret 5 $1$YEmb$Vl8kMjdubiUUK6EexC2OZ/
ip subnet-zero
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
```

<Output omitted for brevity>

Show interfaces: Displays statistics and status information of all the interfaces on the switch.


```
LA-2950#show interfaces
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 0017.e091.b780 (bia 0017.e091.b780)
  Internet address is 10.10.1.2/24
  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
  Last input 00:00:00, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 1000 bits/sec, 1 packets/sec
  5 minute output rate 11000 bits/sec, 13 packets/sec
     1758 packets input, 314535 bytes, 0 no buffer
     Received 100 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 8 ignored
     46340 packets output, 14691341 bytes, 0 underruns
     0 output errors, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
FastEthernet0/1 is down, line protocol is down (notconnect)
  Hardware is Fast Ethernet, address is 0017.e091.b781 (bia 0017.e091.b781)
  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)
  Auto-duplex, Auto-speed, media type is 100BaseTX
  input flow-control is unsupported output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 01:03:33, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
 --More--
[Connection to 10.10.1.2 closed by foreign host]
LDN#
```

<Output omitted for brevity>

Back

12.3: Lab Exercise 2: Switch Console Password Assignment

Description: Lab Exercise explains the concept of configuring switch console password assignment.

Use the line console 0 command, followed by the password and login subcommands, to require login and establish a login password on the console terminal or on a VTY port. By default, login is not enabled on the console or on VTY ports.

Instructions:

1. Enter global configuration mode
2. Enter line sub-configuration mode
3. Set the console password to "consolepass"
4. Exit line configuration mode

LA-2950>enable
LA-2950#configure terminal
LA-2950(config)#line console 0
LA-2950(config-line)#password consolepass
LA-2950(config-line)#exit

By giving “show running-config” command you can view the console password assigned

<Output omitted for brevity>

Back

12.4: Lab Exercise 3: Switch VTY password assignment

Not Available in Demo Version

12.5: Lab Exercise 4: Switch Privileged Password Assignment

Not Available in Demo Version

12.6: Lab Exercise 5: Enable FastEthernet Interface on a switch

Not Available in Demo Version

12.7: Lab Exercise 6: Initial Switch configuration

Not Available in Demo Version

12.8: Lab Exercise 7: Basic Switch Interface Configuration

Not Available in Demo Version

12.9: Lab Exercise 8: Catalyst Switch Configuration

Not Available in Demo Version

13. EXERCISES ON SWITCH CONFIGURATION AND VLAN

13.1: Lab Exercise 1: Basic Switch IP Configuration

Description: The lab exercise explains the concept of configuring IP address on switch

Instructions:

1. Enter user Exec mode
2. Enter privileged Exec mode
3. Assign an ip address 10.10.1.2 255.255.255.0
4. Assign default gateway route 10.10.1.1
5. Exit switch configuration mode

```
LA-2950>enable
LA-2950#configure terminal
LA-2950(config)#interface vlan 1
LA-2950(config-if)#ip address 10.10.1.2 255.255.255.0
LA-2950(config-if)#exit
LA-2950(config)#ip default-gateway 10.10.1.1
LA-2950(config)#end
LA-2950#show running-config
```

Explanation: A default gateway allows devices on a network to communicate with devices on another network. Without it, the network is isolated from the outside. Basically, devices send data that is bound for other networks (one that does not belong to its local IP range) through the default gateway.

LA-2950 , vlan1 interface is configured with ip address as 10.10.1.2 255.255.255.0 and default-gateway as 10.10.1.1

Back

13.2: Lab Exercise 2: Configure and verify port-security on switch

Description: Lab exercise explains the configuration of port-security on switches

Notes: Port security is disabled by default. **switchport port-security** command is used to enable it. Port security feature does not work on three types of ports.

- Trunk ports
- Ether channel ports
- Switch port analyzer ports

Port security work on host port. In order to configure port security we need to set it as host port. It could be done easily by ***switchport mode access*** command.

Instructions:

1. Move in privilege exec mode
2. Move in global configuration mode
3. Move in interface mode

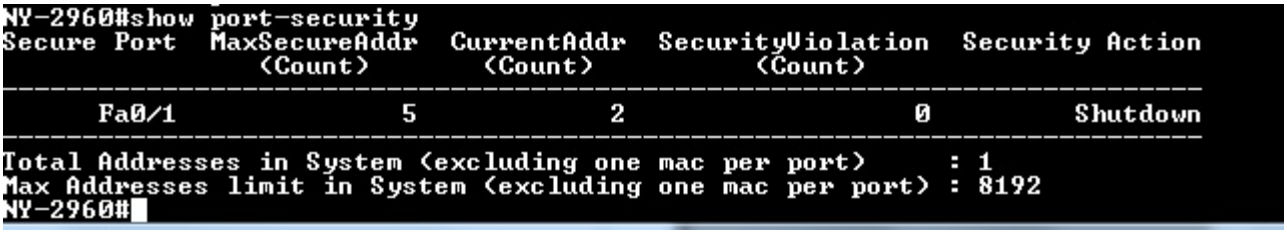
4. Assign port as host port
5. Enable port security feature on this port
6. Set limit for hosts that can be associated with interface. Default value is 1.
7. Set security violation mode. Default mode is shutdown.
8. Enters a secure MAC address for the interface. You can use this command to enter the maximum number of secure MAC addresses.
9. Enable sticky learning on the interface
10. Verify the configuration by show command "**show port-security**"
11. Also give "**show port-security interface fastethernet** *0/1*"

```
NY-2960>enable
 Password:Cisco
NY-2960#configure terminal
NY-2960(config)#interface fastethernet 0/1
NY-2960(config-if)#switchport mode access
NY-2960(config-if)#switchport port-security
NY-2960(config-if)#switchport port-security maximum 5
NY-2960(config-if)#switchport port-security violation shutdown
NY-2960(config-if)#switchport port-security mac-address 2222.3333.4444
NY-2960(config-if)#switchport port-security mac-address sticky
NY-2960(config-if)#end
NY-2960#show port-security
NY-2960#show port-security interface fastethernet 0/1
```

Explanation: The "switchport port-security maximum <no. of addresses>" command sets the maximum number of secure MAC addresses for the port (default is 1) . To configure a static entry for the MAC address table, use the mac address-table static command. To delete the static entry, use the no form of this command.
mac address-table static mac-address vlan vlan-id {drop| interface{ethernetslot/port|port-channelnumber[.subinterface-number]} [auto-learn]

In this lab port security is configured on port fa 0/1. The switch will learn the MAC address of the device connected to port fa 0/1 and will allow only that device to connect to the port in future.

The sample output of "show port-security" and "show port-security interface fastethernet 0/1**"** is shown below



```
NY-2960#show port-security interface fastEthernet 0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 5
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 001b.d43f.8baf:1
Security Violation Count   : 0

NY-2960#
```

Back

13.3: Lab Exercise 3: Troubleshooting a Switch

Not Available in Demo Version

13.4: Lab Exercise 4: Switch Trunking Configuration

Not Available in Demo Version

13.5: Lab Exercise 5: Creating and Deleting VLAN's

Not Available in Demo Version

13.6: Lab Exercise 6: Configuring VTP on a Switch

Not Available in Demo Version

13.7: Lab Exercise 7: Configuring VTP with a VTP Client

Description: This lab exercise demonstrates configuring VTP with a VTP client.

Not Available in Demo Version

13.8: Lab Exercise 8: Troubleshooting lab with non-matching domains

Not Available in Demo Version

13.9: Lab Exercise 9: Troubleshooting lab with trunk functionality

Not Available in Demo Version

13.10: Lab Exercise 10: VLANs Scenario

Not Available in Demo Version

13.11: Lab Exercise 11: VTP (VLAN Trunking Protocol) Scenario

Not Available in Demo Version

13.12: Lab Exercise 12: VLANs and Trunking

Not Available in Demo Version

13.13: Lab Exercise 13: Routing between VLANs(Router on a Stick)

Not Available in Demo Version

