LAB MANUAL FOR CCNA  
Version 4.0

CONTENTS:

1. Basic Exercises

1.1 Lab Exercise 1: Entering user EXEC prompt on a Router and Exit
1.2 Lab Exercise 2: Introduction to Basic User Interface
1.3 Lab Exercise 3: Basic Show commands
1.4 Short Form Commands

2. Routing IOS Fundamental Exercises

2.1 Lab Exercise 1: Banner MOTD : Setting Message of the Day
2.2 Lab Exercise 2: Setting Host Name
2.3 Lab Exercise 3: Router Interface Configuration
2.4 Lab Exercise 4: Setting Bandwidth on an Interface
2.5 Lab Exercise 5: Setting Console Password
2.6 Lab Exercise 6: Setting Telnet Password
2.7 Lab Exercise 7: Setting Auxiliary Password to Router
2.8 Lab Exercise 8: Configuring Minimum password length
2.9 Lab Exercise 9: Implementing exec-timeout command
2.10 Lab Exercise 10: Copy Running Configuration to Startup Configuration
2.11 Lab Exercise 11: Router CDP Configuration
2.12 Lab Exercise 12: Show CDP Configuration
2.13 Lab Exercise 13: Show CDP neighbors
2.14 Lab Exercise 14: Bringing up a Router Interface
2.15 Lab Exercise 15: Set Keepalive Timers
2.16 Lab Exercise 16: Set Hostname and MOTD Banner
2.17 Lab Exercise 17: Console and Line Passwords
2.18 Lab Exercise 18: Host Table
2.19 Lab Exercise 19: Viewing ARP Entries
2.20 Lab Exercise 20: Telnet
2.21 Lab Exercise 21: TFTP
2.22 Lab Exercise 22: Configuring Cisco Routers for Syslog
2.23 Lab Exercise 23: Configure and Verify NTP

3. Exercises on Routing Fundamentals

3.1 Lab Exercise 1: Introduction to IP
3.2 Lab Exercise 2: Configuring Static routes
3.3 Lab Exercise 3: Implement and Verify Static Routes
3.4 Lab Exercise 4: Configuring Default route
3.5 Lab Exercise 5: Implement and Verify Default Routes
3.6 Lab Exercise 6: Configuring Loopback Interface
3.7 Lab Exercise 7: Connectivity Tests with Traceroute
3.8 Lab Exercise 8: Configuring RIP
3.9 Lab Exercise 9: Basic EIGRP Routing

4. Exercises on RIP/EIGRP Routing Scenarios
   4.1 Lab Exercise 1: RIP Routing Configuration Scenario
   4.2 Lab Exercise 2: Viewing IP RIP Information
   4.3 Lab Exercise 3: Configuring RIPv2
   4.4 Lab Exercise 4: RIP2 Routes
   4.5 Lab Exercise 5: EIGRP Routing Configuration Scenario
   4.6 Lab Exercise 6: EIGRP Troubleshooting Lab Scenario
   4.7 Lab Exercise 7: EIGRP Show Commands

5. Exercises on OSPF
   5.1 Lab Exercise 1: OSPF Configuration in Single Area
   5.2 Lab Exercise 2: OSPF Troubleshooting Lab Scenario-1
   5.3 Lab Exercise 3: OSPF Troubleshooting Lab Scenario-2
   5.4 Lab Exercise 4: OSPF Routing Configuration Scenario

6. Exercises on Access-Lists
   6.1 Lab Exercise 1: Creating a Standard Access List
   6.2 Lab Exercise 2: Applying an Access List to an Interface
   6.3 Lab Exercise 3: View Access List Entries
   6.4 Lab Exercise 4: Standard Access List Scenario Lab 1
   6.5 Lab Exercise 5: Configuring and Verifying Standard Access List
   6.6 Lab Exercise 6: Configuring and Verifying Extended Access List
   6.7 Lab Exercise 7: Configuring and Implementing Extended Access List
   6.8 Lab Exercise 8: Named Access-Lists

7. Exercises on Network Address Translation
   7.1 Lab Exercise 1: NAT Scenario 1
   7.2 Lab Exercise 2: NAT Scenario 2
   7.3 Lab Exercise 3: Dynamic NAT Scenario-1
   7.4 Lab Exercise 4: NAT and PAT

8. Exercises on HSRP
   8.1 Lab Exercise 1: To enable HSRP on a Router
   8.2 Lab Exercise 2: To disable HSRP on a Router
8.3 Lab Exercise 3: Configuring HSRP Priority, Delay and Preempt
8.4 Lab Exercise 4: Load Sharing with Multigroup HSRP (MHSRP)

9. Exercises on VPN (Virtual Private Network)
   9.1 Lab Exercise 1: Configuring site-to-site IPSEC VPN tunnel between routers

10. Exercises on DHCP
    10.1 Lab Exercise 1: Configuring cisco router as a DHCP Server
    10.2 Lab Exercise 2: DHCP client configuration

11. Exercises on PPP
    11.1 Lab Exercise 1: PPP Configuration

12. Exercises on Frame-Relay
    12.1 Lab Exercise 1: Configuring Frame-Relay without sub-interfaces
    12.2 Lab Exercise 2: Configuring Frame-Relay with point-to-point sub-interfaces
    12.3 Lab Exercise 3: Frame-Relay Show Commands

13. Exercises on IPv6
    13.1 Lab Exercise 1: Enabling IPv6 on a cisco router
    13.2 Lab Exercise 2: Enabling IPv6 on a cisco router interface
    13.3 Lab Exercise 3: Configuring IPv6 on a cisco router interface with IPv6 address in EUI format
    13.4 Lab Exercise 4: Configuring IPv6 on a cisco router interface with IPv6 address in general form
    13.5 Lab Exercise 5: Configuring loopback interface with IPv6 address
    13.6 Lab Exercise 6: Configuring IPv6 on two router interfaces connected directly and pinging the distant interface using console
    13.7 Lab Exercise 7: Configuring IPv6 static route
    13.8 Lab Exercise 8: Configuring IPv6 static default route
    13.9 Lab Exercise 9: Implement and verify IPv6 static route

    14.1 Lab Exercise 1: Enabling RIPng on a cisco router interface
    14.2 Lab Exercise 2: Enabling RIPng on two routers and pinging between them
    14.3 Lab Exercise 3: Entering RIPng router configuration mode and setting global parameters on a cisco router
14.4 Lab Exercise 4: Configuring EIGRPv6 on a router interface
14.5 Lab Exercise 5: Configuring EIGRPv6 on two routers and pinging between them
14.6 Lab Exercise 6: Enabling OSPF for IPv6 on a Cisco router interface
14.7 Lab Exercise 7: Configuring OSPF on two router interfaces
14.8 Lab Exercise 8: General IPv6 configuration on series router
14.9 Lab Exercise 9: Traceroute lab

15. Exercises on BGP

15.1 Lab Exercise 1: Basic BGP Configuration
15.2 Lab Exercise 2: Setting BGP attributes
15.3 Lab Exercise 3: Setting the BGP neighbor password
15.4 Lab Exercise 4: To disable the peer
15.5 Lab Exercise 5: Basic Configuration of a Peer Group
15.6 Lab Exercise 6: Configuring Multi Exit Discriminator Metric

16. Exercises on Route Redistribution

16.1 Lab Exercise 1: Route Redistribution for RIP
16.2 Lab Exercise 2: Route Redistribution for EIGRP
16.3 Lab Exercise 3: Route Redistribution for OSPF
16.4 Lab Exercise 4: Redistribution between EIGRP and OSPF
16.5 Lab Exercise 5: Redistribution between RIP and EIGRP

17. Exercises on MPLS

17.1 Lab Exercise 1: Configuring a Router for MPLS Forwarding and verifying the configuration of MPLS forwarding.
17.2 Lab Exercise 2: Enabling MPLS
17.3 Lab Exercise 3: Configuring MPLS LDP
17.4 Lab Exercise 4: Configuring MPLS using EIGRP
17.5 Lab Exercise 5: Configuring MPLS using OSPF
17.6 Lab Exercise 6: Configuring MPLS using RIP
17.7 Lab Exercise 7: MPLS show commands

18. Cisco Switch IOS

18.1 Logging into the switch
18.2 Lab Exercise 1: Introduction to Switch
18.3 Lab Exercise 2: Switch Console Password Assignment
18.4 Lab Exercise 3: Switch VTY Password Assignment
18.5 Lab Exercise 4: Switch Privileged password
18.6 Lab Exercise 5: Enable Fast Ethernet Interface on a Switch
18.7 Lab Exercise 6: Initial Switch Configuration
18.8 Lab Exercise 7: Basic Switch Interface Configuration
18.9 Lab Exercise 8: Catalyst 2960S Switch Configuration

19. Exercises on Spanning Tree Protocol
19.1 Lab Exercise 1: Enabling STP
19.2 Lab Exercise 2: Configuring Root Switch
19.3 Lab Exercise 3: Configuring Port-Priority
19.4 Lab Exercise 4: Configuring Switch Priority of a VLAN
19.5 Lab Exercise 5: Configuring STP Timers
19.6 Lab Exercise 6: Verifying STP

20. Exercises on Switch Configuration and VLAN

20.1 Lab Exercise 1: Basic Switch IP Configuration
20.2 Lab Exercise 2: Configure and verify port-security on switch
20.3 Lab Exercise 3: Troubleshooting a Switch
20.4 Lab Exercise 4: Switch Trunking Configuration
20.5 Lab Exercise 5: Creating and Deleting VLAN's
20.6 Lab Exercise 6: Configuring VTP on a Switch
20.7 Lab Exercise 7: Configuring VTP with a VTP Client
20.8 Lab Exercise 8: Troubleshooting lab with non matching domains
20.9 Lab Exercise 9: Troubleshooting lab with trunk functionality
20.10 Lab Exercise 10: VLANs Scenario
20.11 Lab Exercise 11: VTP Scenario
20.12 Lab Exercise 12: VLANs and Trunking
20.13 Lab Exercise 13: Routing between VLANs
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
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

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>
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

Below is the “show protocols” command output

```
BLR#show protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.0.10/24
FastEthernet0/1 is administratively down, line protocol is down
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.1.2/24
Serial0/1/0 is down, line protocol is down
  Internet address is 192.168.3.1/24
Serial0/1/1 is administratively down, line protocol is down
```

Below is the “show version “ command output

```
BLR#show version
Cisco 102 Software, 1841 Software (C880-3PWR-SEC-K9-M), Version 12.4(15)T17, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Tue 24-Jun-15 05:54 by psed_prel_32a
ROM: System Bootstrap, Version 12.3(0)T19, RELEASE SOFTWARE (fc1)
BLR uptime is 1 hour, 18 minutes
System returned to ROM by power-on
System image file is “flash://c1841-nmoeiosk9-mz.124-15.1T17.bin”

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.


If you require further assistance please contact us by sending email to export@cisco.com.

Cisco 1841 (revision 6.0) with 116736K/14336K bytes of memory.
Processor board ID PTH952M07B
2 FastEthernet interfaces
1 Serial interface
2 Serial(config=async) interfaces
DRAM configuration is 64 bits wide with parity disabled.
1916 bytes of NVRAM,
25488K bytes of ATA CompactFlash (Read/Write)
Configuration register is 0x2102
```
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.

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 banner 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
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
```

You can give “show running-config” command to check the output, where hostname changed to cisco from BLR

```
hostname cisco
```

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 255.255.255.0
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

By giving “show running-config” command you can view the ip address configured on the interfaces

```
interface FastEthernet0/0
  description Local Network
  ip address 192.168.0.130 255.255.255.0
  duplex auto
  speed auto

interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto

interface Serial0/0/0
  description WAN Link to NY Hub from BLR
  ip address 192.168.1.2 255.255.255.0

interface Serial0/1/0
  ip address 192.168.3.1 255.255.255.0
  clock rate 200000

interface Serial0/1/1
  no ip address
  shutdown
  clock rate 200000
```

<Output omitted for brevity>

2.4: Lab Exercise 4: Setting Bandwidth on an interface

**Description:** Bandwidth refers to the rate at which data is transferred over the communication link. You setup the bandwidth on a given interface (interface serial 0/0/0) to a specified value (64 kbps). You also set the clockrate to 64000. Note that bandwidth is represented in kbps whereas clock rate is entered in bps.

**Syntax:** bandwidth (interface):

The command bandwidth <kilobits> will set and communicate the bandwidth value for an interface to higher-level protocols.

**Ex:** bandwidth 64 will set the bandwidth to 64 kbps. Use no form of the command to set the
bandwidth to default value.

Instructions:

1. Enter to serial 0/0/0 mode of router BLR
2. Set bandwidth of serial 0/0/0 as 64 kbps
3. Set clockrate as 64000 bps

    BLR> enable
    BLR# configure terminal
    BLR(config)# interface serial 0/0/0
    BLR(config-if)# bandwidth 64
    BLR(config-if)# clock rate 64000 - This command applies to only DCE interfaces
    BLR(config-if)# exit
    BLR(config)# exit
    BLR# show interface s 0/0/0
    BLR# show interfaces

Below is the show interfaces serial 0/0/0” command output

| Serial0/0/0 is up, line protocol is up |
| Hardware is GT16K with integrated T1 CSU/DSU |
| Description: WAN Link to BLR Hub |
| Internet address is 192.168.1.2/24 |
| MTU 1500 bytes, BW 64 Kbit/sec, DLY 20000 usec, reliability 255/255, txload 7/255, rxload 11/255 |
| Encapsulation HDLC, loopback not set |
| Keepalive set (10 sec) |
| Last input 00:00:00, output 00:00:00, output hang never |
| Last clearing of "show interface" counters never |
| Input queue: 1/75/0/0 (size/max/drops/flushes); Total output drops: 0 |
| Queueing strategy: weighted fair |
| Output queue: 0/1000/64/0 (size/max total/threshold/drops) |
| Conversations: 0/1/256 (active/max active/max total) |
| Reserved Conversations 0/0 (allocated/max allocated) |
| Available Bandwidth 40 kilobits/sec |
| 5 minute input rate 3000 bits/sec, 5 packets/sec |
| 5 minute output rate 2000 bits/sec, 5 packets/sec |
| 1810 packets input, 100486 bytes, 0 no buffer |
| Received 183 broadcasts, 0 runts, 0 giants, 0 throttles |
| 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort |
| 1476 packets output, 79342 bytes, 0 underruns |
| 0 output errors, 0 collisions, 11 interface resets |

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: Set Hostname and MOTD Banner
Not Available in Demo Version

2.17: Lab Exercise 17: Configuring enable and secret password and service password-encryption
Not Available in Demo Version
2.18: Lab Exercise 18: Host Table
Not Available in Demo Version

2.19: Lab Exercise 19: Viewing ARP Entries
Not Available in Demo Version

2.20: Lab Exercise 19: Telnet
Not Available in Demo Version

2.21: Lab Exercise 20: TFTP
Not Available in Demo Version

2.22 Lab Exercise 22: Configuring Cisco Routers for Syslog
Not Available in Demo Version

2.23 Lab Exercise 23: 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 on router NY is shown below:

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK?</th>
<th>Method</th>
<th>Status</th>
<th>Prot</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet0/0</td>
<td>10.10.1.1</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>FastEthernet0/1</td>
<td>10.10.2.1</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Serial0/0/0</td>
<td>192.168.1.1</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Serial0/1/0</td>
<td>192.168.2.1</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Serial0/1/1</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM</td>
<td>administratively down</td>
<td>down</td>
</tr>
</tbody>
</table>
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

3.9: Lab Exercise 9: Basic EIGRP Routing

Not available in Demo Version

4. EXERCISES ON RIP/EIGRP 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 NY issue a ping and trace command to BLR and LDN
<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>NY</td>
<td>S0/0/0</td>
<td>192.168.1.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>S0/1/0</td>
<td>192.168.2.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>BLR</td>
<td>S0/0/0</td>
<td>192.168.1.2</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>S0/1/0</td>
<td>192.168.3.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>LDN</td>
<td>S0/0/0</td>
<td>192.168.2.2</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>S0/0/1</td>
<td>192.168.3.2</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

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 serial 0/1/0
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 LDN

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

On NY:

NY#ping 192.168.3.2
NY#ping 192.168.3.1
NY#trace 192.168.3.2
NY#trace 192.168.3.1

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

```
Gateway of last resort is not set

C 192.168.4.0/24 is directly connected, Serial0/1/1
C 192.168.4.0/24 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
```

4.3: Lab Exercise 3: Configuring RIPV2

Not available in Demo Version

4.4: Lab Exercise 4: RIP2 Routes

Not available in Demo Version

4.5: Lab Exercise 5: EIGRP Routing Configuration Scenario

Not available in Demo Version
5. Exercises on OSPF

*Note*: Please refer to the below network Diagram for all the exercises in this section

**5.1: Lab Exercise 1: OSPF Configuration in Single Area**

**Description**: In OSPF single area, you configure OSPF network with an area ID. The configuration example uses four routers working in area 200.

![Network Diagram](image)

**IP Address Assignment Table**

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>NY</td>
<td>S0/1/0</td>
<td>192.168.4.0/24</td>
<td></td>
</tr>
<tr>
<td>LA</td>
<td>S0/0/0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDN</td>
<td>S0/0/0</td>
<td>192.168.2.0/24</td>
<td></td>
</tr>
<tr>
<td>BLR</td>
<td>S0/0/0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>S0/1/0</td>
<td>192.168.3.0/24</td>
<td></td>
</tr>
</tbody>
</table>
Instructions:

1. Based on the given network configuration, use appropriate commands to configure OSPF in networks 192.168.1.0, 192.168.2.0, 192.168.3.0 and 192.168.4.0 within area 200
2. Ping LDN and LA from NY and verify connectivity
3. Ping NY and LDN from LA and verify connectivity

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 serial 0/1/0
NY(config-if)#ip address 192.168.2.1 255.255.255.0
NY(config-if)# no shutdown
NY(config-if)#exit
NY(config)#interface serial 0/1/1
NY(config-if)#ip address 192.168.4.1 255.255.255.0
NY(config-if)# no shutdown
NY(config)#router ospf 1
NY(config-router)#network 192.168.1.0 0.0.0.255 area 200
NY(config-router)#network 192.168.2.0 0.0.0.255 area 200
NY(config-router)#network 192.168.4.0 0.0.0.255 area 200
NY(config-router)#exit
NY(config)#exit
NY#

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 ospf 1
BLR(config-router)#network 192.168.1.0 0.0.0.255 area 200
BLR(config-router)#network 192.168.3.0 0.0.0.255 area 200
BLR(config-router)#exit
BLR(config)#exit
BLR#

On LDN

LDN>enable
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)#router ospf 1
LDN(config-router)#network 192.168.2.0 0.0.0.255 area 200
LDN(config-router)#network 192.168.3.0 0.0.0.255 area 200
LDN(config-router)#exit
LDN(config)#exit
LDN#

On LA

LA>enable
LA#configure terminal
LA(config)#interface serial 0/0/0
LA(config-if)#ip address 192.168.4.2 255.255.255.0
LA(config-if)# no shutdown
LA(config-if)#exit
LA(config)#router ospf 1
LA(config-router)#network 192.168.4.0 0.0.0.255 area 200
LA(config-router)#exit
LA(config)#exit
LA#

On NY

NY#ping 192.168.3.2
NY#ping 192.168.4.2

On LA

LA#ping 192.168.1.1
5.2: Lab Exercise 2: OSPF Troubleshooting Lab Scenario-1

Description: In OSPF single area, you configure OSPF network with an area ID. The configuration example uses four routers working in area 200.

IP Address Assignment Table

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>NY</td>
<td>S0/0/0</td>
<td>192.168.1.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>S0/1/0</td>
<td>192.168.2.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>S0/1/1</td>
<td>192.168.4.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>LA</td>
<td>S0/0/0</td>
<td>192.168.4.2</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>BLR</td>
<td>S0/0/0</td>
<td>192.168.1.2</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>S0/1/0</td>
<td>192.168.3.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>LDN</td>
<td>S0/0/0</td>
<td>192.168.2.2</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>S0/0/1</td>
<td>192.168.3.2</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

Instructions:

1. Assign IP Addresses on all the devices as per the above table and bring all the interfaces to up state
2. On NY enable OSPF routing with process 1 and area as 200 for the network 192.168.2.0 and 192.168.4.0
3. On BLR enable OSPF routing with process 1 and area as 200 for the network 192.168.1.0 and 192.168.3.0
4. On LDN enable OSPF routing with process 1 and area as 200 for the network 192.168.2.0 and 192.168.3.0
5. On LA enable OSPF routing with process 1 and area as 200 for the network 192.168.4.0
6. Ping NY from BLR, you will see ping failure
7. Ping BLR from LDN, you will see ping success (This implies connectivity failure from BLR to NY)
8. Issue command on NY to see OSPF database
9. You will see that there is no link state entry for network 192.168.1.0, so enable OSPF routing on NY for this network
10. Ping NY from BLR, you will see ping success

Note: You need to assign the IP addresses and make the interfaces up (by issuing no shutdown commands at appropriate interfaces) for all the devices before proceeding with the following commands

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 serial 0/1/0
NY(config-if)#ip address 192.168.2.1 255.255.255.0
NY(config-if)# no shutdown
NY(config-if)#exit
NY(config)#interface serial 0/1/1
NY(config-if)#ip address 192.168.4.1 255.255.255.0
NY(config-if)# no shutdown
NY(config)#router ospf 1
NY(config-router)#network 192.168.2.0 0.0.0.255 area 200
NY(config-router)#network 192.168.4.0 0.0.0.255 area 200
NY(config-router)#exit
NY(config)#exit

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 ospf 1
BLR(config-router)#network 192.168.1.0 0.0.0.255 area 200
BLR(config-router)#network 192.168.3.0 0.0.0.255 area 200
BLR(config-router)#exit
BLR(config)#exit
BLR#

On LDN

LDN>enable
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)#router ospf 1
LDN(config-router)#network 192.168.2.0 0.0.0.255 area 200
LDN(config-router)#network 192.168.3.0 0.0.0.255 area 200
LDN(config-router)#exit
LDN(config)#exit
LDN#

On LA

LA>enable
LA#configure terminal
LA(config)#interface serial 0/0/0
LA(config-if)#ip address 192.168.4.2 255.255.255.0
LA(config-if)# no shutdown
LA(config-if)#exit
LA(config)#router ospf 1
LA(config-router)#network 192.168.4.0 0.0.0.255 area 200
LA(config-router)#exit
LA(config)#exit
LA#

BLR#ping 192.168.1.1
LDN#ping 192.168.1.2

On NY

NY#show ip ospf database
NY#configure terminal
NY(config)#router ospf 1
NY(config-router)#network 192.168.1.0 0.0.0.255 area 200
NY(config-router)#exit
NY(config)#exit
NY#

On BLR:

BLR#ping 192.168.1.1

“Show ip ospf database” command output for device NY is given below

```
 NY#show ip ospf database

 OSPF Router with ID (192.31.7.1) (Process ID 1)
 Router Link States (Area 200)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADRU</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
<th>Link count</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.31.7.1</td>
<td>192.31.7.1</td>
<td>73</td>
<td>0x80000004</td>
<td>0x00E0DE</td>
<td>4</td>
</tr>
<tr>
<td>192.168.1.2</td>
<td>192.168.1.2</td>
<td>125</td>
<td>0x80000001</td>
<td>0x00F013</td>
<td>2</td>
</tr>
<tr>
<td>192.165.201.18</td>
<td>192.165.201.18</td>
<td>74</td>
<td>0x80000001</td>
<td>0x00D045</td>
<td>2</td>
</tr>
</tbody>
</table>
```
5.4: Lab Exercise 4: OSPF Routing Configuration Scenario

Not available in Demo Version

6. Exercises on Access-Lists

6.1: 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

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

Description: Apply access-list 1 to interface Ethernet 0 on R1. Apply the access-list on both incoming and outgoing interfaces.

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
6.3: 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.
3. Exit from the global configuration mode
4. 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

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

Not available in Demo Version

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

Not available in Demo Version

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

Not available in Demo Version

6.7: Lab Exercise 7: Configuring and Implementing Extended Access List

Not available in Demo Version

6.8: Lab Exercise 8: Named Access-Lists

Not available in Demo Version
7. 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**

![Network Diagram](image)

**IP Address Assignment Table**

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>NY</td>
<td>S0/1/1.2</td>
<td>209.165.201.17</td>
<td>255.255.255.252</td>
</tr>
<tr>
<td></td>
<td>Loopback0</td>
<td>192.31.7.1</td>
<td>255.255.255.255</td>
</tr>
<tr>
<td>LA</td>
<td>S0/0/0.2</td>
<td>209.165.201.18</td>
<td>255.255.255.252</td>
</tr>
<tr>
<td></td>
<td>Fa0/0</td>
<td>10.10.1.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>PC-A</td>
<td></td>
<td>10.10.1.3</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>PC-B</td>
<td></td>
<td>10.10.1.4</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

7.1: 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 ping a remote router.

**NAT Mapping Table for Inside Source**

<table>
<thead>
<tr>
<th>Inside Local</th>
<th>Inside Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.1.3</td>
<td>209.165.201.19</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Pro</th>
<th>Inside global</th>
<th>Inside local</th>
<th>Outside local</th>
<th>Outside global</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>209.165.201.19</td>
<td>10.10.1.3</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>---</td>
<td>209.165.201.20</td>
<td>10.10.1.4</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>

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

7.2: Lab Exercise 2: NAT Scenario 2

Description: The purpose of this lab is to configure NAT on the destination router (NAT outside source) and test for connectivity by pinging a remote router.

NAT Mapping Table for Outside Source

<table>
<thead>
<tr>
<th>Outside Local</th>
<th>Outside Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.1.3</td>
<td>209.165.201.3</td>
</tr>
<tr>
<td>10.10.1.4</td>
<td>209.165.201.4</td>
</tr>
</tbody>
</table>

Instructions:

1. Assign IP addresses on devices NY and LA as per the IP address assignment table
2. Enable routing on all routers.
3. Create IP NAT Mapping (Hint: use outside source static command) on LA
4. Define IP NAT Inside and IP NAT Outside interfaces on LA

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 200.165.201.0
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

LA>enable
LA#conf term
LA(config)#ip nat outside source static 10.10.1.3 209.165.201.19
LA(config)#ip nat outside 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

NY#:ping 209.165.201.19

7.3: Lab Exercise 3: Configuring Dynamic NAT Scenario I

Not available in Demo Version

7.4: Lab Exercise 4: NAT and PAT

Not available in Demo Version
8. Exercises on HSRP

Short Note On HSRP: HSRP is one of the so called FHRP or “First Hop Redundancy Protocols”. The other two FHRP protocols that are popularly known are VRRP (Virtual Router Redundancy Protocol) and GLBP (Gateway Load Balancing Protocol). In the labs, we cover HSRP.

Configuring HSRP: HSRP, or Hot Standby Routing Protocol, is a Cisco proprietary protocol that allows two or more routers to work together to represent a single virtual IP address to the end-user. Among the HSRP configured routers, one will work as Active and the others (one or more) work as Standby routers. The Active and Standby routers are determined by a set of rules. Only the virtual IP address that was created within the HSRP configuration along with a virtual MAC address is known to other hosts on the network.

The Active router is elected by considering the priority assigned (higher number means, higher priority). The default priority is 100. If two routers have the same priority, then the router with higher IP address will assume Active router role, and the other acquires Standby router role. Furthermore, if there are more than two routers in the group, the second highest IP address determines the standby router and the other router/routers are in the listen state.

Note: If both routers are set to the same priority, then the first router to come up will be the active router.

The labs provide hands-on experience in configuring HSRP using Cisco routers and verifying the HSRP configuration.

Note: When replying to traceroute command, the IP address of the physical interface is used, not the virtual IP address. Similarly, as per Cisco website, when a response for traceroute is received from a hop that runs HSRP, the reply must contain the active physical IP address and not the virtual ip address.

8.1: Lab Exercise 1: To enable HSRP on a Router

Description: This lab exercise demonstrates the necessary commands to enable the HSRP on a router.

Instructions: To achieve basic HSRP configuration, following needs to be done.

1. Configure IP address on the fa 0/0 interface of BLR and NY
2. Bring interface up (no shutdown)
3. Configure HSRP group and virtual IP address using the standby command

Configuration to enable HSRP on BLR is as follows

```
BLR>enable
BLR#configure terminal
BLR(config)#interface fastethernet 0/0
BLR(config-if)#ip address 192.168.0.130 255.255.255.0
BLR(config-if)#no shutdown
BLR(config-if)#standby 11 ip 192.168.0.100
```

Configuration to enable HSRP on NY is as follows
The **standby ip** interface configuration command activates HSRP on the configured interface. If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the address is learned through the standby function. In this example, HSRP is configured with group “11”. This group number can be any number between 0 and 255 (HSRP version 1) and the only requirement is that you must use the same number across devices in the same HSRP group.

### 8.2: Lab Exercise 2: To disable HSRP on a Router

**Description:** This lab exercise demonstrates the necessary commands to disable the HSRP on a router.

**Instructions:**

1. Configure IP address on the fa 0/0 interface of BLR
2. Bring interface up (no shutdown)
3. Configure no standby [group-number] ip [ip-address] interface configuration command to disable HSRP.

**On BLR**

```
BLR>enable
BLR#configure terminal
BLR(config)#interface fastethernet 0/0
BLR(config-if)#ip address 192.168.0.130 255.255.255.0
BLR(config-if)#no shutdown
BLR(config-if)#no standby 11 ip 192.168.0.100
```

### 8.3: Lab Exercise 3: Configuring HSRP Priority, Delay and Preempt

Not available in Demo Version

### 8.4: Lab Exercise 4: Load Sharing with Multigroup HSRP (MHSRP)

Not available in Demo Version
9. Exercises on VPN (Virtual Private Network)

9.1: Lab Exercise 1: Configuring site-to-site IPSEC VPN tunnel between routers

**Description:** This lab exercise explains how to setup and configure two routers to create a permanent secure site-to-site VPN tunnel over the Internet, using the IP Security (IPSec) protocol.

**Instructions:**

1. Configure the IP addresses of all the devices and bring the interface up
2. Apply static routing on NY and LA
3. Create interesting traffic on NY and LA
4. Configure IKE Phase 1 ISAKMP policy on NY and LA
5. Configure the IKE Phase 2 IPsec policy on NY and LA

**Step by step configuration for routers are given below**

**On NY**

1. Basic Interface configurations

   NY>enable
   NY#configure terminal
   NY(config)#interface fa0/1
   NY(config-if)#ip address 10.10.2.1 255.255.255.0
   NY(config-if)#no shutdown
   NY(config-if)#exit
   NY(config)#interface serial 0/1/1
   NY(config-if)#ip address 192.168.4.1 255.255.255.0
   NY(config-if)#no shutdown
   NY(config-if)#exit

   NY(config)#ip route 10.10.1.0 255.255.255.0 192.168.4.2

2. Configure Phase 1 (ISAKAMP) of IPSec so that a secure tunnel is established between
NY and LA

NY(config)#crypto isakmp policy 5
NY(config-isakmp)#hash sha
NY(config-isakmp)#authentication pre-share
NY(config-isakmp)#group 2
NY(config-isakmp)#lifetime 86400
NY(config-isakmp)#encryption 3des
NY(config-isakmp)#exit

3. Define a pre shared key for authentication with peer LA by using the following command:

NY(config)#crypto isakmp key 0 sim123 address 192.168.4.2

4. Configure IPSEC: To configure IPSec we need to do the following

- Create extended access-list
- Create IPSec Transform
- Create Crypto Map
- Apply crypto map to the public interface

1. Creating Access-list

NY(config)#ip access-list extended vpntraffic
NY(config-ext-nacl)#permit ip 10.10.2.0 0.0.0.255 10.10.1.0 0.0.0.255
NY(config-ext-nacl)#exit

2. Create IPSEC Transform (ISAKMP PHASE 2 POLICY)

NY(config)#crypto ipsec transform-set trnsset esp-3des esp-md5-hmac
NY(cfg-crypto-trans)#exit

3. Create Crypto Map

NY(config)#crypto map crmap 10 ipsec-isakmp
NY(config-crypto-map)#set peer 192.168.4.2
NY(config-crypto-map)#set transform-set trnsset
NY(config-crypto-map)#match address vpntraffic
NY(config-crypto-map)#exit

4. Apply Crypto Map To The Public Interface

NY(config)#interface serial 0/1/1
NY(config-if)#crypto map crmap
NY(config-if)#end
NY#show crypto map
NY#show crypto isakmp key
NY#show crypto ipsec transform-set
NY#show crypto isakmp policy

The output of “show crypto map” command is given below

```
NY#show crypto map
Crypto Map "crmap" 10 ipsec-isakmp
   Peer = 192.168.4.2
   Extended IP access list vpntraffic
   access-list vpntraffic permit ip 10.10.2.0 0.0.0.255 10.10.1.0 0.0.0.0

   Current peer: 192.168.4.2
   Security association lifetime: 4608000 kilobytes/3600 seconds
   PFS (Y/N): N
   Transform sets={
      trnset,
   }
   Interfaces using crypto map crmap:
      Serial0/1/1
```

The output of “show crypto isakmp key” command is given below

```
NY#show crypto isakmp key
Keyring Hostname/Address Preshared Key
   default 192.168.4.2 sim123
```

The output of “show crypto ipsec transform-set” is given below

```
NY#show crypto ipsec transform-set
Transform set trnset: { esp-3des esp-md5-hmac } will negotiate = { Tunnel, },
```

The output of “show crypto isakmp policy” is given below

```
NY#show crypto isakmp policy
Global IKE policy Protection suite of priority 5
      encryption algorithm: Three key triple DES
      hash algorithm: Secure Hash Standard
      authentication method: Pre-Shared Key
      Diffie-Hellman group: #2 (1024 bit)
      lifetime: 86400 seconds, no volume limit

Default protection suite
      encryption algorithm: DES - Data Encryption Standard (56 bit keys)
      hash algorithm: Secure Hash Standard
      authentication method: Rivest-Shamir-Adleman Signature
      Diffie-Hellman group: #1 (1024 bit)
      lifetime: 86400 seconds, no volume limit
```

On LA

```
LA> enable
LA#configure terminal
LA(config)#interface serial 0/0/0
LA(config-if)#ip address 192.168.4.2 255.255.255.0
LA(config-if)#no shutdown
```
LA(config-if)#exit
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)#ip route 10.10.2.0 255.255.255.0 192.168.4.1

LA(config)#crypto isakmp policy 5
LA(config-isakmp)#hash sha
LA(config-isakmp)#authentication pre-share
LA(config-isakmp)#group 2
LA(config-isakmp)#lifetime 86400
LA(config-isakmp)#encryption 3des
LA(config-isakmp)#exit

LA(config)#crypto isakmp key 0 sim123 address 192.168.4.1

LA(config)#ip access-list extended vpntraffic
LA(config-ext-acl)#permit ip 10.10.1.0 0.0.0.255 10.10.2.0 0.0.0.255
LA(config-ext-acl)#exit

LA(config)#crypto ipsec transform-set trnsset esp-3des esp-md5-hmac
LA(cfg-crypto-trans)#exit
LA(config)#crypto map crmap 10 ipsec-isakmp
LA(config-crypto-map)#set peer 192.168.4.1
LA(config-crypto-map)#set transform-set trnsset
LA(config-crypto-map)#match address vpntraffic
LA(config-crypto-map)#exit

LA(config)#interface serial 0/0/0
LA(config-if)#crypto map crmap
LA(config-if)#end
LA#show crypto map
LA#show crypto isakmp key
LA#show crypto ipsec transform-set
LA#show crypto isakmp policy

```
Show crypto map crmap 10 ipsec-isakmp
Peer = 192.168.4.1
Extended IP access list vpntraffic
access-list vpntraffic permit ip 10.10.1.0 0.0.0.255 10.10.2.0 0.0.0.255
Current peer: 192.168.4.1
Security association lifetime: 6000000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={
    trnsset.
}
Interfaces using crypto map crmap:
    Serial0/0/0
```

Version 4.0 Copyright © 2002 - 2019 CertExams.com 38
Here the interesting traffic means traffic that needs to be encrypted, rest of the traffic goes unencrypted. From Site1's perspective, all the traffic with source address from internal network 10.10.1.0/24 and destination network 10.10.2.0/24 will be regarded as interesting traffic, and vice versa from Site2's perspective.

Back
10. Exercises on DHCP

10.1: 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#
10.2: 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.

```bash
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#config 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
```
11. Exercises on PPP

11.1: Lab Exercise 1: PPP Configuration

**Description:** This exercise helps to understand how Point to Point Protocol encapsulation works. Configure PPP across a point-to-point network as shown in the network diagram below.

**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
```
12. Exercises on Frame-Relay

12.1: Lab Exercise 1: Configuring Frame-Relay without sub-interfaces

**Description:** Configure frame-relay without using sub-interfaces. This configuration example uses full mesh topology.

Note that on a frame-relay network without sub-interfaces, the LMI-type is automatically
detected. Similarly, PVC DLCIs are learned through CMS status messages. There is no need to specify the same explicitly. On the other hand, in a FR network with point-to-point sub-interface configurations, you need to specify the interface-dlci number.

Instructions:

**IP Address Assignment Table:**

<table>
<thead>
<tr>
<th>Device-Interface</th>
<th>IP Address/Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLR-S0/0/0</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>BLR-S0/1/0</td>
<td>192.168.2.1/24</td>
</tr>
<tr>
<td>NY-S0/0/0</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>NY-S0/1/1</td>
<td>192.168.4.1/24</td>
</tr>
<tr>
<td>LA-S0/0/0</td>
<td>192.168.2.2/24</td>
</tr>
<tr>
<td>LA-S0/0/1</td>
<td>192.168.3.2/24</td>
</tr>
</tbody>
</table>

1. Specify frame-relay on S0/0 of Venus
2. Specify frame-relay on S0/0 of Saturn
3. Specify frame-relay on S0/0 of Jupiter

```
BLR>enable
BLR#configure terminal
BLR(config)#interface serial 0/0/0
BLR(config-if)# encapsulation frame-relay
BLR(config-if)#ip address 192.168.1.2 255.255.255.0
BLR(config-if)#exit
BLR(config)#interface serial 0/1/0
BLR(config-if)# encapsulation frame-relay
BLR(config-if)#ip address 192.168.3.1 255.255.255.0
BLR(config-if)^z
BLR#

NY>enable
NY#configure terminal
NY(config)#interface serial 0/0/0
NY(config-if)# encapsulation frame-relay
NY(config-if)#ip address 192.168.1.1 255.255.255.0
NY(config-if)#exit
NY(config)#interface serial 0/1/0
NY(config-if)# encapsulation frame-relay
NY(config-if)#ip address 192.168.3.1 255.255.255.0
NY(config-if)^z

LDN>enable
LDN#configure terminal
LDN(config)#interface serial 0/0/0
LA(config-if)# encapsulation frame-relay
LDN(config-if)#ip address 192.168.2.2 255.255.255.0
LDN(config-if)#exit
```
12.2: Lab Exercise 2: Configuring Frame-Relay with point-to-point sub-interfaces

**Description:** Configure frame-relay using point-to-point sub-interfaces. This example uses 4 routers connected together in the form of a star using sub-interfaces.

Note that on a frame-relay network without sub-interfaces, the LMI-type is automatically detected. Similarly, PVC DLCIs are learned through CMS status messages. There is no need to specify the same explicitly. On the otherhand, in a FR network with point-to-point sub-interface configurations, you need to specify the interface-dlci number.

**Instructions:**

**IP Address Assignment Table:**

<table>
<thead>
<tr>
<th>Device-Interface-Sub Interface</th>
<th>IP Address/Mask</th>
</tr>
</thead>
</table>

Copyright © CertExams.com
NY-S0/0/0.1 | 192.160.1.1/24  
NY-S0/0/1.1 | 192.160.2.1/24  
NY-S0/1/0.1 | 192.160.3.1/24  
BLR-S0/0/0.1 | 192.160.1.2/24  
London-S0/0/0.1 | 192.160.2.2/24  
LA-S0/0/0.1 | 192.160.3.2/24  

**Router NY:**

1. Enter sub-interface configuration mode for s0/0.1  
2. Specify ip address  
3. Specify interface-dlci number 62  
4. Exit  
5. Specify hostname  
6. Enter sub-interface configuration mode for s0/1.1  
7. Specify ip address  
8. Specify interface-dlci number 63  
9. Exit  
10. Specify hostname  
11. Enter sub-interface configuration mode for s1/0.1  
12. Specify ip address  
13. Specify interface-dlci number 64  
14. Exit  

**Router BLR:**

1. Specify hostname  
2. Specify frame-relay encapsulation  
3. Enter sub-interface configuration mode for s0/0.1  
4. Specify ip address  
5. Specify interface-dlci number 62  
6. Exit  

**Router London:**

1. Specify frame-relay encapsulation  
2. Enter sub-interface configuration mode for s0/0.1  
3. Specify ip address  
4. Specify interface-dlci number 63  
5. Exit  

**Router LA:**

1. Specify hostname  
2. Specify frame-relay encapsulation  
3. Enter sub-interface configuration mode for s0/0.1  
4. Specify ip address  
5. Specify interface-dlci number 64
6. Exit

NY> enable
NY# conf term
NY(config)# interface serial 0/0/0
NY(config-if)# encapsulation frame-relay
NY(config-if)# exit
NY(config)# interface serial 0/0/0.1 point-to-point
NY(config-subif)# ip address 192.160.1.1 255.255.255.0
NY(config-subif)# frame-relay interface-dlci 62
NY(config-subif)# exit
NY(config)# interface serial 0/0/1.1 point-to-point
NY(config-subif)# ip address 192.160.2.1 255.255.255.0
NY(config-subif)# frame-relay interface-dlci 63
NY(config-subif)# exit
NY(config)# interface serial 0/1/0.1 point-to-point
NY(config-subif)# ip address 192.160.3.1 255.255.255.0
NY(config-subif)# frame-relay interface-dlci 64
NY(config-subif)#^z
NY# copy running-config startup-config

BLR> enable
BLR# configure terminal
BLR(config)# interface serial 0/0/0
BLR(config-if)# encapsulation frame-relay
BLR(config-if)# exit
BLR(config)# interface serial 0/0/0.1 point-to-point
BLR(config-subif)# ip address 192.160.1.2 255.255.255.0
BLR(config-subif)# frame-relay interface-dlci 62
BLR(config-subif)#^z
BLR# copy running-config startup-config

LDN> enable
LDN# configure terminal
LDN(config)# interface serial 0/0/0
LDN(config-if)# encapsulation frame-relay
LDN(config-if)# exit
LDN(config)# interface serial 0/0/0.1 point-to-point
LDN(config-subif)# ip address 192.160.2.2 255.255.255.0
LDN(config-subif)# frame-relay interface-dlci 63
LDN(config-subif)#^z
LDN# copy running-config startup-config

LA> enable
LA# configure terminal
LA(config)# interface serial 0/0/0
LA(config-if)# encapsulation frame-relay
LA(config-if)# exit
LA(config)# interface serial 0/0/0.1 point-to-point
LA(config-subif)# ip address 192.160.3.2 255.255.255.0
12.3: Lab Exercise 3: Frame-Relay with Show Commands

Not available in Demo Version
13. Exercises on Ipv6

13.1: 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.

13.2: 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
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.

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

Not available in Demo Version

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

Not available in Demo Version

13.5: Lab Exercise 5: Configuring loopback interface with IPv6 address

Not available in Demo Version

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

Not available in Demo Version

13.7: Lab Exercise 7: Configuring IPv6 static route

Not available in Demo Version

13.8: Lab Exercise 8: Configuring IPv6 static default route

Not available in Demo Version

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

Not available in Demo Version

14.1: 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

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.

“show ipv6 rip” and “show ipv6 protocols” command output is given below

NY# show ipv6 rip
RIP process "pname1", port 521, multicast-group FF02::9, pid 181
   Administrative distance is 120. Maximum paths is 16
   Updates every 30 seconds, expire after 180
   Holddown lasts 0 seconds, garbage collect after 120
   Split horizon is on; poison reverse is off
   Default routes are not generated
   Periodic updates 0, trigger updates 0
Interfaces:
   Serial0/0/0
Redistribution:
   None
14.2: 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

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

Not available in Demo Version

14.4: Lab Exercise 4: Configuring EIGRPv6 on a router interface

Not available in Demo Version

14.5: Lab Exercise 5: Configuring EIGRPv6 on two routers and pinging between them

Not available in Demo Version

14.6: Lab Exercise 6: Enabling OSPF for IPv6 on a cisco router interface

Not available in Demo Version
15. Exercises on BGP

15.1: Lab Exercise 1 Basic BGP Configuration

Note: This Lab has three sections

I: Basic BGP Configuration

Description: Describes the commands for forming BGP neighbor relationships and advertising networks.

Instructions:

1. Assign the IP addresses to all the devices as per the diagram.
2. Bring all the interfaces to up.
3. Issue network command on all the devices to identify the networks to be advertised by the BGP process.
4. Issue neighbor command on Router NY to identify each neighbor and its AS.

On NY:

```
NY> enable
NY# conf term
NY(config)# int 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)# int serial 0/1/1
NY(config-if)# ip address 192.168.4.1 255.255.255.0
NY(config-if)# no shutdown
NY(config-if)# exit
NY(config)# router bgp 300
NY(config-router)# network 192.168.4.0
NY(config-router)# network 192.168.1.0
NY(config-router)# exit
NY(config)# exit
NY#
```

On BLR

```
BLR> enable
BLR# conf term
BLR(config)# int 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)# router bgp 100
BLR(config-router)# network 192.168.1.0
BLR(config-router)# exit
BLR(config)# exit
BLR#
```

On LA

```
LA> enable
LA# conf term
LA(config)# int serial 0/0/0
LA(config-if)# ip address 192.168.4.2 255.255.255.0
LA(config-if)# no shutdown
LA(config-if)# exit
LA(config)# router bgp 200
LA(config-router)# network 192.168.4.0
LA(config-router)# exit
LA(config)# exit
LA#
```
II: Managing and Verifying the BGP Configuration

Description: This section explains the common BGP commands used to view the status of BGP neighbor relationships and the routes learned through these relationships.

Instructions:

1. Enter into privileged mode
2. Issue show ip bgp command to display the bgp routing table
3. Issue show ip bgp summary command to display the status of all bgp sessions.
4. Issue show ip bgp neighbor command to displays TCP and BGP connection to neighbors.

BGP show command output is given below

```
On NY

NY>enable
NY#conf term
NY(config)#router bgp 300
NY(config-router)# neighbor 192.168.1.2 remote-as 100
NY(config-router)# neighbor 192.168.4.2 remote-as 200
NY(config-router)#exit
NY(config)#exit

On NY

NY>enable
NY#show ip bgp
NY#show ip bgp summary
NY#show ip bgp neighbors

BGP show command output is given below

```

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.4.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>U</th>
<th>AS</th>
<th>MsgRcd</th>
<th>MsgSent</th>
<th>ThldUp</th>
<th>InqOut</th>
<th>Up/Down</th>
<th>State/PfxRec</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.2</td>
<td>4</td>
<td>100</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>never Active</td>
</tr>
<tr>
<td>192.168.4.2</td>
<td>4</td>
<td>200</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>never Active</td>
</tr>
</tbody>
</table>

```
III: Resetting neighbors

Description: Describes the methods for resetting BGP neighbor relationships.

Instructions:

1. Enter into router configuration mode
2. Issue clear ip bgp command to reset session between the neighbors.

On NY:

NY>enable
NY#conf term
NY(config)#router bgp 300
NY(config-router)#clear ip bgp 192.168.1.2
NY(config-router)#clear ip bgp *

15.2: Lab Exercise 2: Setting BGP attributes

Description: This lab exercise explains to set the weight and local preference attribute of the
BGP.

Instructions:

1. On NY set BGP weight attribute of the neighbor (BLR) as 200
2. Also set the default local preference of neighbor BLR to 100
3. Verify the configuration of attributes by giving show ip bgp command.

On NY

NY>enable
NY#conf term
NY(config)#router bgp 300
NY(config-router)#neighbor 192.168.1.2 weight 200
NY(config-router)#bgp default local-preference 100
NY(config-router)#exit
NY(config)#exit
NY#show ip bgp

15.3: Lab Exercise 3: Setting the BGP neighbor password

Not available in Demo Version

15.4: Lab Exercise 4: To disable the peer

Not available in Demo Version

15.5: Lab Exercise 5: Basic configuration of a peer group

Not available in Demo Version

15.6: Lab Exercise 6: Configuring Multi Exit Discriminator Metric

Not available in Demo Version
16. Exercises On Route Redistribution

16.1: Lab Exercise 1: Route Redistribution for RIP

**Description:** This lab exercise demonstrates the command for redistributing EIGRP, OSPF, and Static routes into RIP.

**Instructions:**

1. Enter into router configuration mode
2. Issue command to redistribute all EIGRP routes into RIP
3. Issue command to redistribute all OSPF routes into RIP
4. Issue command to redistribute all Static routes into RIP

**On NY:**

```
NY>enable
NY#conf term
NY(config)#router rip
NY(config-router)#redistribute eigrp 100 metric 1
NY(config-router)#redistribute ospf 1 metric 1
NY(config-router)#redistribute static metric 1
NY(config-router)#exit
NY(config)#
```

**NOTE:** Metric command can also be given in following way (Using the default-metric command saves work because it eliminates the need for defining the metric separately for each redistribution.)

```
NY(config)#router rip
NY(config-router)#redistribute eigrp 100
NY(config-router)#redistribute ospf 1
NY(config-router)#redistribute static
NY(config-router)#default-metric 1
```

16.2: Lab Exercise 2: Route Redistribution for EIGRP

**Description:** This lab exercise demonstrates the command for redistributing RIP, OSPF, and Static routes into EIGRP.

**NOTE:** EIGRP need five metrics when redistributing other protocols: bandwidth, delay, reliability, load, and MTU

**Instructions:**
1. Enter into router configuration mode
2. Issue command to redistribute all RIP routes into EIGRP
3. Issue command to redistribute all OSPF routes into EIGRP
4. Issue command to redistribute all static routes into EIGRP.

On NY:

NY>enable
NY#conf term
NY(config)#router eigrp 1
NY(config-router)#redistribute rip metric 2000 200 255 1 1500
NY(config-router)#redistribute ospf 1 metric 2000 200 255 1 1500
NY(config-router)#redistribute static metric 2000 200 255 1 1500
NY(config-router)#exit
NY(config)#

NOTE: Metric command can also be given in following way (Using the default-metric command saves work because it eliminates the need for defining the metric separately for each redistribution.)

NY(config)#router eigrp 1
NY(config-router)#redistribute rip
NY(config-router)#redistribute ospf
NY(config-router)#redistribute static
NY(config-router)#default-metric 10000 100 255 1 1500

16.3: Lab Exercise 3: Route Redistribution for OSPF

Not available in Demo Version

16.4: Lab Exercise 4: Redistribution between EIGRP and OSPF

Not available in Demo Version

16.5: Lab Exercise 5: Redistribution between RIP and EIGRP

Not available in Demo Version
17. Exercises On MPLS

17.1: 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

17.2: 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.

17.3: Lab Exercise 3: Configuring MPLS LDP

Not available in Demo Version

17.4: Lab Exercise 4: Configuring MPLS using EIGRP

Not available in Demo Version

17.5: Lab Exercise 5: Configuring MPLS using OSPF

Not available in Demo Version

17.6: Lab Exercise 6: Configuring MPLS using RIP

Not available in Demo Version

17.7: Lab Exercise 7: MPLS Show commands

Not available in Demo Version
18. CISCO SWITCH IOS

18.1 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.

![Console](image)

18.2: 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.
Show interfaces: Displays statistics and status information of all the interfaces on the switch.
18.3: 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#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>

18.4: Lab Exercise 3: Switch VTY password assignment

Not available in Demo Version

18.5: Lab Exercise 4: Switch Setting Privileged Password

Not available in Demo Version

18.6: Lab Exercise 5: Enable Fast Ethernet Interface on a switch

Not available in Demo Version

18.7: Lab Exercise 6: Initial Switch configuration

Not available in Demo Version

18.8: Lab Exercise 7: Basic Switch Interface Configuration

Not available in Demo Version

18.9: Lab Exercise 8: Catalyst Switch Configuration

Not available in Demo Version
19. Exercises on Spanning Tree Protocol

19.1: Lab Exercise 1: Enabling STP

**Description:** This lab exercise demonstrates the necessary commands to enable and disable spanning tree protocol on a switch.

**Instructions:**

1. Enter into configuration mode on LA-2950
2. Issue command "spanning-tree vlan <vlan-num>" to enable spanning-tree on a specified VLAN
3. Issue no form of the command "spanning-tree vlan <vlan-num>" to disable spanning-tree on the VLAN specified.

```
LA-2950>enable
LA-2950#configure terminal
LA-2950(config)#spanning-tree vlan 1
LA-2950(config)#no spanning-tree vlan 1
LA-2950(config)#exit
LA-2950#
```

**Note:** Spanning Tree Protocol (STP) is enabled by default on modern switches. It is possible to disable or enable the Spanning Tree Protocol (STP) when required.

19.2: Lab Exercise 2: Configuring Root Switch

**Description :** This lab exercise demonstrates the necessary commands to configure the root switch.

**Instructions:**

1. Enter into configuration mode on LA-2950
2. Issue the command "spanning-tree vlan <vlan-num> root" that modifies the switch priority from the default 32768 to a lower value to allow the switch to become the root switch for VLAN 1
3. Verify the configuration using “show spanning-tree” command.

```
LA-2950>enable
LA-2950#configure terminal
LA-2950(config)#spanning-tree vlan 1 root
LA-2950(config)#exit
LA-2950#show spanning-tree
```

**Explanation:** The command "show spanning-tree" includes information about the following:
1. VLAN number
2. Root bridge priority, MAC address
3. Bridge timers (Max Age, Hello Time, Forward Delay)

Below screenshot displays output from "show spanning-tree"

**19.3: Lab Exercise 3: Configuring Port-Priority**

Not available in Demo Version

**19.4: Lab Exercise 4: Configuring the switch priority of a VLAN**

Not available in Demo Version

**19.5: Lab Exercise 5: Configuring STP Timers**

Not available in Demo Version

**19.6: Lab Exercise 6: Verifying STP**
20. EXERCISES ON SWITCH CONFIGURATION AND VLAN

20.1: 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

20.2: 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”

**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 3/0/1. The switch will learn the MAC address of the device connected to port fa 3/0/1 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 3/0/1” is shown below

```
NY-2960#show port-security
Secure Port  MaxSecureAddr Count CurrentAddr Count SecurityViolation Count Security Action
Fa0/1  5 2 0 Shutdown

Total Addresses in System (excluding one mac per port) : 1
Max Addresses limit in System (excluding one mac per port) : 8192
```

NY-2960#enqueue
### 20.3: Lab Exercise 3: Troubleshooting a Switch

Not available in Demo Version

### 20.4: Lab Exercise 4: Switch Trunking Configuration

Not available in Demo Version

### 20.5: Lab Exercise 5: Creating and Deleting VLAN's

Not available in Demo Version

### 20.6: Lab Exercise 6: Configuring VTP on a Switch

Not available in Demo Version

### 20.7: Lab Exercise 7: Configuring VTP with a VTP Client

Not available in Demo Version

### 20.8: Lab Exercise 8: Troubleshooting lab with non-matching domains

Not available in Demo Version

### 20.9: Lab Exercise 9: Troubleshooting lab with trunk functionality

Not available in Demo Version

### 20.10: Lab Exercise 10: VLANs Scenario

Not available in Demo Version
20.11: Lab Exercise 11: VTP (VLAN Trunking Protocol) Scenario

Not available in Demo Version

20.12: Lab Exercise 12: VLANs and Trunking

Not available in Demo Version

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

Not available in Demo Version