CCNA Routing & Switching Lab Workbook - Full-Scale Lab 1

Task 1.1

> You must load the initial configuration files for the section, **FS Lab-1 Initial**, which can be found in CCNA Routing & Switching Topology Diagrams and Initial Configurations.

Tasks

- Configure the hostname on all switches.
- Configure IP addresses on all switch management interfaces as follows:
  - Sw1 : 10.1.1.1/24
  - Sw2 : 10.1.1.2/24
  - Sw3 : 10.1.1.3/24
- Configure default-gateway 10.1.1.10 on all switches.
- Configure Sw1 as the telnet server using the password **cisco**.
- Configure the enable password **cisco** on Sw1.
- You should be able to telnet Sw1 from Sw2 and Sw3.

Configuration

By default, Cisco switches have VLAN 1 as their management VLAN. We can assign an IP address in the VLAN 1 interface, which is used to access that particular switch via remote access tools such as Telnet, SSH, etc.

The switch is a Layer 2 device, which should be configured with a default-gateway using the `ip default-gateway` command to make it accessible from different networks. Unlike a Layer 3 device, it cannot route the packets because it only works based on the destination mac address.

First, perform the basic configurations such as hostname, IP address, and default-gateway.

```
Sw1:
enable
!
```

```
configure terminal
!
hostname Sw1
!
interface vlan 1
 ip address 10.1.1.1 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.1.10
```

Sw2:

```
enable
!
configure terminal
!
hostname Sw2
!
interface vlan 1
 ip address 10.1.1.2 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.1.10
```

Sw3:

```
enable
!
configure terminal
!
hostname Sw3
!
interface vlan 1
 ip address 10.1.1.3 255.255.255.0
 no shutdown
!
ip default-gateway 10.1.1.10
```

Now configure Sw1 as the telnet server.

```
Sw1:

line vty 0 4
 password cisco
!
enable password cisco
```

Verification

Initially, we can check for the IP addressing and reachability information between all the switches in this topology. When it is successful, we can check for the telnet session to Sw1 from Sw2 and Sw3. We can use some kind of output modifier to get clean output, as shown here.

```
Sw1#show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  10.1.1.1        YES manual up                    up
!Sw1#ping 10.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/8 ms
!Sw1#ping 10.1.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.3, timeout is 2 seconds:.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/9 ms
!
!Sw2#show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  10.1.1.2        YES manual up                    up

!Sw2#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!Sw2#ping 10.1.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.3, timeout is 2 seconds:.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms
!
```

```
!Sw3#show ip interface brief | exclude unassigned

Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  10.1.1.3        YES manual up                    up
!Sw3#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!Sw3#ping 10.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

As required by the task, verify establishment of a telnet session from Sw2 and Sw3.

```
Sw2#telnet 10.1.1.1
Trying 10.1.1.1 ... Open



User Access Verification

Password:
Sw1>enable
Password: Sw1#
!
!Sw3#telnet 10.1.1.1
Trying 10.1.1.1 ... Open



User Access Verification

Password:
Sw1>enable
Password: Sw1#
```

We can also verify this by using the `show users` command to determine who is connected to Sw1 via telnet. Basically, it tells us who is connected to the telnet server using a telnet session.

```
Sw1#show users
```

```
    Line       User       Host(s)              Idle       Location
*   0 con 0                idle                 00:00:00
    1 vty 0                idle                 00:02:11 10.1.1.2
    2 vty 1                idle                 00:01:19 10.1.1.3
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 1

Task 1.2

Tasks

- Configure VLAN 100 and VLAN 200 on all switches.
- Configure any names for the VLANs.
- Associate VLANs on the ports as follows:
  - Sw1's Fa0/1 in VLAN 100
  - Sw2's Fa0/1 in VLAN 100
  - Sw2's Fa0/4 in VLAN 200
  - Sw3's Fa0/3 in VLAN 200
- Configure trunk ports if required.
- Configure IP addresses on the hosts as follows:
  - VLAN 100: 100.1.1.0/24
  - VLAN 200: 200.1.1.0/24
- Configure ISL encapsulation between Sw1 and Sw2, and 802.1Q encapsulation between Sw1 and Sw3.

Configuration

In this task, we are asked to configure VLAN 100, VLAN 200, and trunking on all the switches. We have four routers connected with three switches, which must be assigned in a particular VLAN. After VLAN configuration, we must configure trunk interfaces because we have multiple VLANs to pass through the switches. In trunking, there are two encapsulation types: ISL [Inter Switch Link] and IEEE802.1Q [dot1q]. ISL is the Cisco proprietary encapsulation method; it adds 30 bytes of extra overhead in the L2 frame, which usually is not preferred by Cisco switches. By default, 802.1q is enabled on the Cisco IOS switches. Optionally, we can change it to ISL by using the `switchport trunk enacpsulation isl` command.

Let's configure VLAN 100 and 200 on all the switches.

```
Sw1,Sw2 & Sw3:
```

```
vlan 100
name IT
exit
!
vlan 200
name Sales
exit
```

When configured, assign those VLANs in the particular ports as required by the task.

```
Sw1:
interface fa0/1
 switchport mode access
 switchport access vlan 100
Sw2:
interface fa0/1
 switchport mode access
 switchport access vlan 100
!
inter fa0/4
 switchport mode access
 switchport access vlan 200
Sw3:

interface fa0/3
 switchport mode access
 switchport access vlan 200
```

Now configure trunk and encapsulation types between switches.

```
Sw1:
interface fa0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface fa0/13
 switchport trunk encapsulation isl
 switchport mode trunk
Sw2:
interface fa0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
Sw3:

interface fa0/13
```

```
 switchport trunk encapsulation isl
 switchport mode trunk
```

The next step is to configure IP addresses on the host routers that correspond to the particular VLAN. When configured, we should have reachability between the devices that fall into the same VLAN ID.

```
R1:
interface fa0/1
 ip address 100.1.1.1 255.255.255.0
 no shutdown
R2:
interface fa0/1
 ip address 100.1.1.2 255.255.255.0
 no shutdown
R3:
interface fa0/1
 ip address 200.1.1.3 255.255.255.0
 no shutdown
R4:

interface fa0/1
 ip address 200.1.1.4 255.255.255.0
 no shutdown
```

Verification

Per the task requirements, we have configured VLAN 100 and 200 on all the switches and also configured the trunk ports as required. Now we have R1 and R2 assigned to VLAN 100, and R3 and R4 have been assigned to VLAN 200. Before we move on to the reachability test, we must verify which VLANs are created and how they are assigned to the switchports. Verify the VLANs and trunking first.

```
Sw1#show vlan


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

```
                                          Fa0/24, Gi0/1, Gi0/2
100  IT                               active    Fa0/1

200  Sales                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
!Sw1#show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/10      on               802.1q         trunking      1
Fa0/13      on               isl            trunking      1

Port        Vlans allowed on trunk
Fa0/10      1-4094
Fa0/13      1-4094

Port        Vlans allowed and active in management domain
Fa0/10      1,100,200
Fa0/13      1,100,200

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/10      100,200
Fa0/13      1,100,200
!
!Sw2#show vlan


VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gi0/1, Gi0/2
100  IT                               active    Fa0/1
200  Sales                            active    Fa0/4
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
!Sw2#show interfaces trunk
```

```
Port        Mode             Encapsulation  Status        Native vlan
Fa0/10      on               802.1q         trunking      1


Port        Vlans allowed on trunk
Fa0/10      1-4094

Port        Vlans allowed and active in management domain
Fa0/10      1,100,200

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/10      1,100,200
!
!Sw3#show vlan


VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
100  IT                               active    200  Sales                            active    Fa0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
!Sw3#show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/13      on               isl            trunking      1


Port        Vlans allowed on trunk
Fa0/13      1-4094

Port        Vlans allowed and active in management domain
Fa0/13      1,100,200

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/13      1,100,200
```

In the above output, we can see that there are two VLANs configured manually,

because others are default VLANs built in to the Cisco IOS. By default, VLAN 1 is considered the management VLAN, which can't be removed from the switch. VLAN-IDs from 1002 to 1005 are reserved for the token ring, one of the LAN technologies like Ethernet. It also cannot be removed from the switch. Additionally, when doing `show interface trunk` , we can see that there are two types of encapsulation types used for trunk: ISL and Dot1Q. By default, Cisco switches have a native VLAN of 1, which is usually considered to be the untagged VLAN, typically used for control plane traffic such as VTP, CDP, STP, BPDUs, etc. that does not need to be tagged by the switch.

Now we can check for the reachability between R1 and R2, and R3 and R4.

```
R1#ping 100.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.1.1.2, timeout is 2 seconds:.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
!
!R3#ping 200.1.1.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.1.4, timeout is 2 seconds:.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms
```

> The first packet of the initial ping is dropped because of the ARP process when the source host is trying to find the destination host MAC address. Subsequent packets are replied to normally.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 1

Task 1.3

Tasks

- Configure Sw1 to allow only VLAN 200 on its interface connected to Sw3.
- Configure Sw3 to allow only VLAN 200 on its interface connected to Sw1.
- Configure Sw1 and Sw2 to allow VLAN 100 and VLAN 200 on their trunk interface.
- Upon completing this task, R1 & R2 and R3 & R4 should communicate.

Configuration

In the previous task, we configured basic VLAN and trunking. By default, a trunk port forwards all the VLANs from a trunk that can be optimized by suppressing unnecessary VLANs on a trunk port. According to the task, we must configure Sw1 to allow VLAN 200 on its FastEthernet0/13 interface, and Sw1 and Sw2 must be configured to allow both VLANs 100 and 200 on its FastEthernet0/10 interface. We must also configure Sw3 to allow VLAN 200 on its FastEthernet0/13 interface.

```
Sw1:
interface FastEthernet0/10
 switchport trunk allowed vlan 100,200
!
interface FastEthernet0/13
 switchport trunk allowed vlan 200
Sw2:
interface FastEthernet0/10
 switchport trunk allowed vlan 100,200
Sw3:

interface FastEthernet0/13
 switchport trunk allowed vlan 200
```

Verification

We can filter the VLANs on an interface using the `switchport trunk allowed-vlan add | remove | none | except` commands. In this particular task, we have configured the trunk interfaces to allow only necessary VLANs. It can be verified by using the `show interface trunk` command as shown below.

```
Sw1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/10      on               802.1q         trunking      1
Fa0/13      on               isl            trunking      1

Port        Vlans allowed on trunk Fa0/10       100,200
Fa0/13      200

Port        Vlans allowed and active in management domain
Fa0/10      100,200
Fa0/13      200

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/10      100,200
Fa0/13      200
!
!Sw2#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/10      on               802.1q         trunking      1

Port        Vlans allowed on trunk Fa0/10       100,200

Port        Vlans allowed and active in management domain
Fa0/10      100,200

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/10      100,200
!
!Sw3#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/13      on               isl            trunking      1
```

```
Port        Vlans allowed on trunkFa0/13        200


Port        Vlans allowed and active in management domain
Fa0/13      200

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/13      200
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 1

Task 1.4

Tasks

- Modify the trunk port configurations as follows:
  - Configure Sw1 with DTP dynamic desirable mode for both trunk ports.
  - Configure Sw2 with DTP dynamic auto mode on its trunk port.
  - Configure Sw3 with DTP dynamic desirable mode on its trunk port.

Configuration

In the previous task, we configured all the trunk ports with static trunk, which can be replaced with Cisco's DTP (Dynamic Trunking Protocol). DTP has three modes: 1) auto, 2) on, and 3) desirable.

Basically, we are using auto and desirable mode where auto mode only responds to the trunking negotiation request, but desirable mode can initiate the trunk negotiation and respond as well.

```
Sw1:
interface FastEthernet0/10
 switchport mode dynamic desirable
 switchport trunk encapsulation negotiate
!
interface FastEthernet0/13
 switchport mode dynamic desirable
 switchport trunk encapsulation negotiate
Sw2:
interface FastEthernet0/10
 switchport mode dynamic auto
 switchport trunk encapsulation negotiate
Sw3:

interface FastEthernet0/13
 switchport mode dynamic desirable
```

```
switchport trunk encapsulation negotiate
```

Verification

We can verify the negotiated trunk by using the `show interface trunk` command in the privilege exec mode. Below are the command outputs for negotiated trunk verification.

```
Sw1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/10      desirable        n-isl
          trunking      1
Fa0/13      desirable        n-isl
          trunking      1
!Sw1#show interfaces fa0/10 switchport

Name: Fa0/10
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: isl
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<snip>
!Sw1#show interfaces fa0/13 switchport

Name: Fa0/13
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: isl
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<snip>
!
!Sw2#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/10      auto             n-isl
          trunking      1
```

```
!Sw2#show interfaces fa0/10 switchport

Name: Fa0/10
Switchport: EnabledAdministrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation:isl
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
!
!Sw3#show interfaces trunk


Port        Mode             Encapsulation  Status        Native vlanFa0/13      desirablen-isl
          trunking      1
!Sw3#show interfaces fa0/13 switchport

Name: Fa0/13
Switchport: EnabledAdministrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation:isl

Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
```

In the above output, we can see some additional parameters like `n-isl`, which means that the ISL encapsulation is negotiated by DTP. By default, Cisco switches use ISL as the trunking encapsulations when using DTP. In this task, we have the additional method of verifying trunking parameters using the `show interface <intf> switchport` command. It reveals the additional components of a trunk port such as Administrative mode, Operational mode, status of negotiation, etc.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 1

Task 1.5

Tasks

- Configure Sw1's Fa0/1 interface as a trunk, using encapsulation 802.1Q.
- Configure inter-VLAN routing with the router-on-a-stick model.
- Upon completing this task, R3 should reach R2 and R4.

Configuration

Because we have used different VLANs to connect the routers and the task is asking us to make them reachable, inter-VLAN routing should be in place to make them reachable. As we know, there should be at least one L3 device; that is, a router or L3-capable switch. So we are using R1 to perform inter-VLAN routing for VLAN 100 and VLAN 200. Make sure that the switchport connected to R1 is configured as static trunk because a router does not support DTP. Additionally, we must configure sub-interfaces on R1 on the basis of which VLANs we are trying to route to each other.

First, configure Sw1's Fa0/1 port as a trunk.

```
Sw1:

interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

Now configure R1 with the sub-interfaces and IP addressing for VLAN100 and VLAN200.

```
R1:

interface FastEthernet0/0
 no ip address
 no shutdown
```

```
!
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 ip address 100.1.1.1 255.255.255.0
!
interface FastEthernet0/0.200
 encapsulation dot1Q 200
 ip address 200.1.1.1 255.255.255.0
```

Set the default-gateway on R2, R3, and R4. Because we are using routers as the hosts, we must disable "ip routing" first and set the default gateway accordingly.

```
R2:
no ip routing
!
ip default-gateway 100.1.1.1
R3:
no ip routing
!
ip default-gateway 200.1.1.1
R4:

no ip routing
!
ip default-gateway 200.1.1.1
```

Verification

When configured, check the reachability between hosts in different VLANs.

```
R2#sh ip route
 Default gateway is 100.1.1.1

Host              Gateway           Last Use    Total Uses  Interface
ICMP redirect cache is empty
!R2#ping 200.1.1.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.1.4, timeout is 2 seconds:.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 36/36/36 ms
!R2#ping 200.1.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.1.3, timeout is 2 seconds:.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 28/29/32 ms
!
```

```
!R3#show ip route
Default gateway is 200.1.1.1


Host               Gateway           Last Use    Total Uses  Interface
ICMP redirect cache is empty
!    R3#ping 100.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.1.1.2, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/15/16 ms
!
!R4#show ip route
Default gateway is 200.1.1.1

Host               Gateway           Last Use    Total Uses  Interface
ICMP redirect cache is empty
!R4#ping 100.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.1.1.2, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 1

Task 1.6

Tasks

- Create VLAN 300 on Sw2.
- Configure Sw2 as the VTP server.
- Configure VTP parameters as follows:
  - VTP version: 2
  - VTP password: CCNA
  - VTP domain: INE_CISCO
- Configure Sw1 in VTP transparent mode.
- Configure Sw3 in VTP client mode.
- Assign VLAN 300 on the ports connected to R3 and R4.
- Upon completing this task, you should be able to ping from R3 to R4.

Configuration

In this task, we are asked to make Sw2 the VTP server where we can configure VLAN 300. After we configure identical VTP domains and passwords on the switches, it starts synchronizing and VLAN300 will be updated by the client (Sw3). Because we are using Sw1 as the VTP transparent device, it does not update its VLAN database with VLAN300; instead, it forwards the VLAN information to the Sw3. So to make R3 reachable R4 via VLAN300, we should create VLAN 300 on Sw1 manually.

Configure VLAN 300 in the database and assign it to the R4 connected interface. Also, configure VTP parameters according to the task requirement.

Sw2:

```
vtp mode server
vtp domain INE_CISCO
vtp password CCNA
vtp version 2
```

```
!
vlan 300
exit
!
interface Fa0/4
 switchport access vlan 300
```

Now configure Sw1 in VTP transparent mode and Sw3 in VTP client mode. Also, assign VLAN 300 on the R3 connected port on Sw3.

```
Sw1:
vtp mode transparent
vtp domain INE_CISCO
vtp password CCNA
vtp version 2
!
vlan 300
exit
Sw3:

vtp mode client
vtp domain INE_CISCO
vtp password CCNA
vtp version 2
!
interface Fa0/3
 switchport access vlan 300
```

Verification

First, check for the VTP synchronization using the `vtp status` privilege exec mode command. You should see the configuration revision number matching among all the switches.

```
Sw2#show vtp status
 VTP Version                     : running VTP2
Configuration Revision           : 6
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
VTP Operating Mode              : Server VTP Domain Name                 : INE_CISCO
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8D 0x03 0xE4 0xAB 0xD5 0x30 0x03 0xAC
```

```
Configuration last modified by 10.1.1.2 at 3-4-93 00:10:49
Local updater ID is 10.1.1.2 on interface Vl1 (lowest numbered VLAN interface found)
!Sw2#show vtp password
 VTP Password:CCNA
!
!Sw1#show vtp status
VTP Version capable             : 1 to 3VTP version running             : 2
VTP Domain Name                 : INE_CISCO
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0019.2f45.ec00
Configuration last modified by 10.1.1.1 at 3-4-93 00:08:25

Feature VLAN:
--------------VTP Operating Mode               : Transparent
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 8
Configuration Revision            : 0
MD5 digest                        : 0x28 0x6A 0xD9 0xFD 0xEF 0x4D 0x26 0x0D
                                    0xF2 0x1D 0x4E 0xC2 0x77 0xDB 0x3A 0xCB
!Sw1#show vtp password
VTP Password:CCNA
!
!Sw3#show vtp status
 VTP Version                     : running VTP2
Configuration Revision          : 6
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
VTP Operating Mode              : ClientVTP Domain Name                 : INE_CISCO
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x5C 0x3B 0xCF 0xD7 0xED 0x0E 0xB1 0x70
Configuration last modified by 10.1.1.3 at 3-4-93 00:39:33
!Sw3#show vtp password
 VTP Password:CCNA
```

All the switches have been configured with identical VTP parameters, and it seems that VLAN 300 has been updated on Sw3's VLAN database. Let's verify it and ping from R3 to R4.

```
Sw3#show vlan
```

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gi0/1, Gi0/2
100  IT                                active
200  Sales                             active    300  VLAN0300                         active    Fa0/3
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
!
!R3#ping 200.1.1.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.1.4, timeout is 2 seconds:.....

Success rate is 0 percent (0/5)
```

In the above output, the ping from R3 to R4 is not successful because we have not added VLAN 300 in the allowed-list on the trunk interfaces. So, allow VLAN 300 on each trunk interface.

```
Sw2:
interface FastEthernet0/10
 switchport trunk allowed vlan add 300
Sw1:
interface FastEthernet0/10
 switchport trunk allowed vlan add 300
!
interface FastEthernet0/13
 switchport trunk allowed vlan add 300
Sw3:

interface FastEthernet0/13
 switchport trunk allowed vlan add 300
```

Again, ping from R3 to R4. It should be successful after we allow VLAN 300 on all the trunk ports.

```
R3#ping 200.1.1.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.1.4, timeout is 2 seconds:.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 1

Task 1.7

Tasks

- Enable Fa0/16 interfaces on Sw2 and Sw3.
- Configure all the switches in rapid-PVST mode.
- Configure Sw1 as the root bridge for VLAN 200. Do not change the bridge priority.
- Configure Sw3 as the secondary root bridge for VLAN 200 without changing the bridge priority.
- Verify spanning-tree root and blocked ports for VLAN 200.

Configuration

By default, Cisco switches run PVST (Per-VLAN Spanning Tree) protocol to prevent Layer 2 loops. In this task, we are asked to change the mode to Rapid-PVST because it has the faster convergence capability. First, configure all the switches for Rapid-PVST mode.

```
All Switches:

spanning-tree mode rapid-pvst
```

Instead of using the `priority` command, we can change the root bridge preference using the `spanning-tree vlan <vlan-id> root primary | secondary` command. In this task, we are asked to make Sw1 the root bridge and Sw3 the root secondary for VLAN 200.

```
Sw1:

spanning-tree vlan 200 root primary
Sw3:

spanning-tree vlan 200 root secondary
```

Verification

The next step is to check for the spanning-tree mode, root bridge, costs, etc. Additionally, we can verify the spanning-tree root and blocked ports by using `show spanning-tree root | blockedports".

```
Sw1#show spanning-tree summary  | inc mode
Switch is in rapid-pvst mode
!Sw1#show spanning-tree vlan 200

VLAN0200  Spanning tree enabled protocol rstp
  Root ID Priority    24776
Address     0019.2f45.ec00
            This bridge is the root
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24776  (priority 24576 sys-id-ext 200) Address     0019.2f45.ec00
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  300 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------------- --- --------- -------- --------------------------------
Fa0/10           Desg FWD 19        128.12   P2p
Fa0/13           Desg FWD 19        128.15   P2p
!
!Sw2#show spanning-tree vlan 200

VLAN0200
  Spanning tree enabled protocol rstp Root ID    Priority    24776
Address     0019.2f45.ec00
Cost        19
Port        10 (FastEthernet0/10)
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32968  (priority 32768 sys-id-ext 200) Address     000c.8581.a500
```

```
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/10              Root FWD 19        128.10   P2p

Fa0/16              Desg FWD 19        128.16   P2p
!Sw2#show spanning-tree vlan 200 root


                                        Root    Hello Max Fwd
Vlan                Root ID             Cost    Time  Age Dly  Root Port
---------------- ------------------- --------- ----- --- ---  ------------
VLAN0200         24776 0019.2f45.ec00        19    2   20  15  Fa0/10

!
!Sw3#show spanning-tree summary | inc mode
Switch is in rapid-pvst mode
!Sw3#show spanning-tree vlan 200

VLAN0200
  Spanning tree enabled protocol rstp Root ID    Priority    24776
Address     0019.2f45.ec00
Cost        19
Port        13 (FastEthernet0/13)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32968  (priority 32768 sys-id-ext 200) Address     000e.830d.f680
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/13              Root FWD 19        128.13   P2p Fa0/16              Altn BLK 19        128.16   P2p

!Sw3#show spanning-tree vlan 200 root


                                        Root    Hello Max Fwd
Vlan                Root ID             Cost    Time  Age Dly  Root Port
---------------- ------------------- --------- ----- --- ---  ------------
VLAN0200         24776 0019.2f45.ec00        19    2   20  15  Fa0/13

!Sw3#show spanning-tree vlan 200 blockedports
```

```
Name                 Blocked Interfaces List
-------------------- ------------------------------------
VLAN0200             Fa0/16
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 1

Task 1.8

Tasks

- Enable interfaces Fastethernet0/11 on Sw1 and Sw2 and Fastethernet0/14 on Sw1 and Sw3.
- Configure those ports as trunks using encapsulation dot1q.
- Configure Sw1 to allow VLAN 200 on its Fa0/11 and Fa0/14 interfaces.
- Configure Sw3 to elect Fa0/14 as the root port.
- Configure Sw1 to elect Fa0/11 of Sw2 as the root port.

Configuration

In this task, we are asked to configure port priority and STP cost to change the default root port election. Basically, port priority is configured on the root bridge in STP, whereas the STP cost can be configured on the local switch to influence the desired root port election.

Until we configure things like port priority and cost, the STP gives preference to the lowest port priority among the uplinks that are connected to the same upstream bridge. If there are multiple upstream bridges, the STP will elect the root port based on the lower bridge identifier among the upstream bridges.

Let's configure the switches according to the task requirements. First, enable the interfaces that are required for this task.

```
Sw1:
interface fa0/11
 no shutdown
!
interface fa0/14
 no shutdown
Sw2:
interface fa0/11
 no shutdown
```

```
Sw3:

interface fa0/14
 no shutdown
```

Configure trunk interfaces and allow VLAN 200 through the trunks as required.

```
Sw1:
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed-vlan 200
!
interface FastEthernet0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed-vlan 200
Sw2:
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
Sw3:

interface FastEthernet0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

The next step is to configure lower port priority on Sw1's Fa0/11 port and higher STP cost on the Fa0/14 interface of Sw3 for VLAN 200.

```
Sw1:
interface FastEthernet0/11
 spanning-tree vlan 200 port-priority 0
Sw3:

interface FastEthernet0/13
 spanning-tree vlan 200 cost 100
```

Verification

Before configuring STP port priority and cost, the output would look like this.

```
Sw2#sh spanning-tree vlan 200


VLAN0200
  Spanning tree enabled protocol rstp
  Root ID     Priority    24776
              Address     0019.2f45.ec00
              Cost        19 Port        10 (FastEthernet0/10)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32968  (priority 32768 sys-id-ext 200)
              Address     000c.8581.a500
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/10              Root FWD 19        128.10   P2p
 Fa0/11              Altn BLK 19        128.11   P2p

Fa0/16              Desg FWD 19        128.16   P2p
!
!Sw3#sh spanning-tree vlan 200

VLAN0200
  Spanning tree enabled protocol rstp
  Root ID     Priority    24776
              Address     0019.2f45.ec00
              Cost        19 Port        13 (FastEthernet0/13)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32968  (priority 32768 sys-id-ext 200)
              Address     000e.830d.f680
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/13              Root FWD 19        128.13   P2p
 Fa0/14              Altn BLK 19        128.14   P2p

Fa0/16              Altn BLK 19        128.16   P2p
```

After changing default port priority and cost values on Sw1 and Sw3, the root ports

are changed.

```
Sw2#sh spanning-tree vlan 200

VLAN0200
  Spanning tree enabled protocol rstp
  Root ID    Priority    24776
             Address     0019.2f45.ec00
             Cost        19 Port        11 (FastEthernet0/11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32968  (priority 32768 sys-id-ext 200)
             Address     000c.8581.a500
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/10              Altn BLK 19        128.10   P2p
Fa0/11              Root FWD 19        128.11   P2p

Fa0/16              Desg FWD 19        128.16   P2p

Sw3#show spanning-tree vlan 200

VLAN0200
  Spanning tree enabled protocol rstp
  Root ID    Priority    24776
             Address     0019.2f45.ec00
             Cost        19 Port        14 (FastEthernet0/14)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32968  (priority 32768 sys-id-ext 200)
             Address     000e.830d.f680
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/13              Altn BLK 100       128.13   P2p
Fa0/14              Root FWD 19        128.14   P2p

Fa0/16              Altn BLK 19        128.16   P2p
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 1

Task 1.9

Tasks

- Configure Sw2 to allow only one MAC address on its interfaces connected to R2 and R4.
- You should statically assign the MAC address of R2 on the Fa0/1 interface.
- Configure Sw2 to dynamically learn MAC addresses on its Fa0/4 interface, but it should look like a static MAC entry.
- Configure Sw2 to shut down its port if an unauthorized MAC is learned on a secure port.

Configuration

To limit number of MAC addresses on a Cisco switchport, we can apply a port security mechanism that prevents any unauthorized host from connecting to the switch. In this particular task, we are asked to perform two types of port security configuration. The first task asks us to configure a static MAC entry for port security, and the second task asks us to configure sticky MAC address configuration. A sticky MAC entry can be considered the static MAC address binding, which converts the dynamically learned MAC address to the static configuration.

Sw2:

```
interface FastEthernet0/1
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation shutdown
 switchport port-security mac-address 001a.6c30.8fdf
!
interface FastEthernet0/4
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation shutdown
```

```
switchport port-security mac-address sticky
```

Verification

First, verify port-security in the interface.

```
Sw2#sh port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 001a.6c30.8fdf:100
Security Violation Count   : 0
!Sw2#sh port-security interface fa0/4
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 001c.589e.7ae1:300
Security Violation Count   : 0
!Sw2#sh port-security

Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)         (Count)
---------------------------------------------------------------------------
Fa0/1              1             1                0          Shutdown
Fa0/4              1             1                0          Shutdown

---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 5120
```

In the above output, we can see the configured parameters of port security. The violation mode is "shutdown" and the Maximum MAC address is up to 1 by default.

Now configure the Fa0/1 interfaces of R1 and R4 with some different MAC address.

```
R2:

interface FastEthernet0/1
 mac-address 1234.1234.1234
!R4

interface FastEthernet0/1
 mac-address 1234.1234.1234
```

The Fa0/1 and Fa0/4 interfaces have gone to the "err-disable" state because of port security violation. Take a look at the log messages.

```
Sw2#
*Mar  8 15:16:55.346: %PM-4-ERR_DISABLE:
psecure-violation error detected on Fa0/1, putting Fa0/1 in err-disable state
*Mar  8 15:16:55.354:
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 1234.1234.1234 on port FastEt
*Mar  8 15:16:56.346: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*Mar  8 15:16:57.354: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
!*Mar  8 15:19:01.894: %PM-4-ERR_DISABLE:
psecure-violation error detected on Fa0/4, putting Fa0/4 in err-disable state
*Mar  8 15:19:01.898:
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 1234.1234.1234 on port FastEt
*Mar  8 15:19:02.894: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down
*Mar  8 15:19:03.898: %LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to down
Sw2#show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0Last Source Address:Vlan    : 1234.1234.1234:100
Security Violation Count   : 1
!Sw2#show port-security interface fa0/4
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
```

```
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1Last Source Address:Vlan    : 1234.1234.1234:300
Security Violation Count   : 1
!Sw2#show port-security

Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/1              1            11
         Shutdown       Fa0/4              1            11
         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 5120
```

Unlike earlier outputs, we can see the violation count on both the secure ports. If the number of attempts increases, the violation count will also increase. Optionally, we can tell the switchport not to shut the ports down, rather than just restricting or protecting the ports that usually prevent unauthorized access without shutting the ports down. The restrict mode also sends the SNMP trap if an unauthorized MAC address is seen on the secure port.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 1

Task 1.10

Tasks

- Configure EtherChannel on Sw1, Sw2, and Sw3 as follows:
  - Configure PAgP between Sw1 and Sw2.
  - Configure LACP between Sw1 and Sw3.
- In both configurations, only Sw1 should be able to initiate the channel.

Configuration

Basically, Cisco switches support two types of EtherChannel protocol. PAgP is the Cisco proprietary protocol that is used to aggregate two or more links in a channel in a Cisco-only environment. It has three modes:

- Auto
- On
- Desirable

LACP is an open standard that can be used between Cisco and non-Cisco devices to bundle multiple interfaces in a channel.

In this task, we are asked to configure PAgP on the FastEthernet0/10 and 11 interfaces between Sw1 and Sw2. Likewise, LACP must be configured on the FastEthernet0/13 and 14 interfaces between Sw1 and Sw3. Moreover, we are asked to configure Sw1 to initiate the EtherChannel. So, the "active" state for LACP and the "desirable" state for PAgP must be configured on Sw1.

Initially, make sure that the configuration regarding VLAN allowed-list and trunking encapsulation are identical on both interfaces.

Sw1:

```
interface range FastEthernet0/10 - 11
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,200,300
```

```
 switchport mode trunk
!
interface range FastEthernet0/13 - 14
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,200,300
 switchport mode trunk
Sw2:
interface range FastEthernet0/10 - 11
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,200,300
 switchport mode trunk
Sw3:

interface range FastEthernet0/13 - 14
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,200,300
 switchport mode trunk
```

Now configure EtherChannel as required by the task.

```
Sw1:
interface range FastEthernet0/10 - 11
 channel-group 1 mode desirable
!
interface range FastEthernet0/13 - 14
 channel-group 2 mode active
Sw2:
interface range FastEthernet0/10 - 11
 channel-group 1 mode auto
Sw3:

interface range FastEthernet0/13 - 14
 channel-group 2 mode passive
```

Verification

The next step is to verify the EtherChannel on all the switches.

```
Sw1#show etherchannel summary

Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
```

```
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)          PAgP      Fa0/10(P)   Fa0/11(P)
   2      Po2(SU)          LACP      Fa0/13(P)   Fa0/14(P)
```

After we define the channel-group number, it automatically creates the corresponding port-channel interface, which is indicated as "Po" in the above output. In this particular output, both the Po1 and Po2 are in "SU" state, which indicates that the port channel is Layer 2 and is working correctly. Similarly, we can check the same on Sw2 and Sw3.

```
Sw2#show etherchannel summary

Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)          PAgP      Fa0/10(P)   Fa0/11(P)
!
!Sw3#show etherchannel summary
```

```
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
2      Po2(SU)         LACP      Fa0/13(P)   Fa0/14(P)
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 2

Task 2.1

> You must load the initial configuration files for the section, **FS Lab-2 Initial**, which can be found in CCNA Routing & Switching Topology Diagrams and Initial Configurations.

Tasks

- Configure hostnames on all the routers.
- Disable domain name lookup on all the routers.
- Configure IP addresses on the connected and Loopback0 interfaces as shown in the diagram.
- After configuring addressing, test the point-to-point reachability.
- Configure R1 as a telnet server, using the privilege level 15 password to access the router.
  - **Username: ccna**
  - **Password: cisco**
  - Do not set the enable password as part of this task.
  - After configuring, you should be able to telnet to R1 from R2 and R4.
  - Upon completing the task, verify user's session on R1.

Configuration

```
R1:
enable
!
configure terminal
!
hostname R1
!
no ip domain-lookup
!
interface Loopback0
```

```
 ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.1.124.1 255.255.255.0
 no shutdown
!
interface Serial1/0
 ip address 10.1.134.1 255.255.255.0
 no shutdown
!
interface Serial1/1
 ip address 10.1.12.1 255.255.255.0
 clock rate 64000
 no shutdown
!
interface Serial1/3
 ip address 10.1.14.1 255.255.255.0
 clock rate 128000
 no shutdown
!
username ccna privilege 15 secret cisco
!
line vty 0 4
login local
```

R2:

```
enable
!
configure terminal
!
hostname R2
!
no ip domain-lookup
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.1.124.2 255.255.255.0
 no shutdown
!
interface Serial0/1/0
 ip address 10.1.12.2 255.255.255.0
 no shutdown
```

R3:

```
enable
!
```

```
configure terminal
!
hostname R3
!
no ip domain-lookup
!
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
!
interface Serial0/0/0
 ip address 10.1.134.3 255.255.255.0
 no shutdown
```

R4:

```
enable
!
configure terminal
!
hostname R4
!
no ip domain-lookup
!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.1.124.4 255.255.255.0
 no shutdown
!
interface Serial1/0
 ip address 10.1.134.4 255.255.255.0
 no shutdown
!
interface Serial1/3
 ip address 10.1.14.4 255.255.255.0
 no shutdown
```

Verification

Hostname is an identity of a router that can be explicitly configured using the `hostname` global configuration command. Likewise, we configured the `no ip domain-lookup` command to avoid unnecessary name resolution. After that, we configured IP addresses on the connected and Loopback0 interfaces on all the routers. So, to

verify IP addresses and interface status, we can issue commands such as `show ip interface brief` and `show run interface <intf>` . Also, use output modifiers with `| exclude` , `| include` commands for the clear output.

```
R1#show ip interface brief | exclude unassigned
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.1.124.1      YES manual up                    up
Serial1/0                  10.1.134.1      YES manual up                    up
Serial1/1                  10.1.12.1       YES manual up                    up
Serial1/3                  10.1.14.1       YES manual up                    up
Loopback0                  1.1.1.1         YES manual up                    up
!
!R1#show run interface FastEthernet 0/0
Building configuration...

Current configuration : 95 bytes
!
interface FastEthernet0/0
 ip address 10.1.124.1 255.255.255.0
 duplex auto
 speed auto
 end
!R1#ping 10.1.124.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.2, timeout is 2 seconds:
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!R1#ping 10.1.124.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.4, timeout is 2 seconds:
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!R1#ping 10.1.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
!R1#ping 10.1.14.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.14.4, timeout is 2 seconds:
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms
!
!R2#show ip interface brief | exclude unassigned
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.1.124.2      YES manual up                    up
Serial0/1/0                10.1.12.2       YES manual up                    up
Loopback0                  2.2.2.2         YES manual up                    up
!R2#ping 10.1.124.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.1, timeout is 2 seconds:
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!R2#ping 10.1.124.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.4, timeout is 2 seconds:
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!R2#ping 10.1.12.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.12.1, timeout is 2 seconds:
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
!
!R3#show ip interface brief | exclude unassigned
Interface                  IP-Address      OK? Method Status                Protocol
Serial0/0/0                10.1.134.3      YES manual up                    up
Serial0/1/0                10.1.1.3        YES manual up                    up
!R3#ping 10.1.134.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.134.1, timeout is 2 seconds:
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
!R3#ping 10.1.134.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.134.4, timeout is 2 seconds:
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
!
!R4#show ip interface brief | exclude unassigned
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.1.124.4      YES manual up                    up
Serial1/0                  10.1.134.4      YES manual up                    up
Serial1/3                  10.1.14.4       YES manual up                    up
!R4#ping 10.1.124.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.1, timeout is 2 seconds:
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 1/27/124 ms
!R4#ping 10.1.124.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.2, timeout is 2 seconds:
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!R4#ping 10.1.134.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.134.1, timeout is 2 seconds:
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
!R4#ping 10.1.134.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.134.3, timeout is 2 seconds:
```

```
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 28/30/32 ms


!R4#ping 10.1.14.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.14.1, timeout is 2 seconds:
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms
```

After verifying point-to-point reachability, we are asked to configure R1 as the telnet server. To secure the password configured for the telnet, we can use the "secret" option instead of the "password" option when creating the privilege level 15 password. The "secret" option will secure the password with type 5 encryption, which cannot be seen in the running configuration.

When configuring telnet, you have multiple options for configuring username and password. By default, no password is set for the telnet connection. We can configure the password directly under the line configuration, but it is not considered a secure method. An alternative is to create a local user database without the privilege level command. When configured, it will take us into the user mode when making telnet sessions, and we will require the enable password to get into privilege mode.

A third option is to create a username and password with the privilege level 15 option. This will take us into the privilege mode with level 15 authorization, and the enable password will not be required during telnet session establishment. It is important to remember to apply `login local` command under the line mode if you have chosen the second or third configuration option.

Configuration

```
R1:

username ccna privilege 15 secret cisco
!
line vty 0 4
login local
```

Verification

```
R2#telnet 10.1.124.1
Trying 10.1.124.1 ... Open
```

```
User Access Verification

Username: ccna
Password: R1#
!R4#telnet 10.1.124.1
Trying 10.1.124.1 ... Open

User Access Verification

Username: ccna
Password: R1#
!
!R1#show running-config | include username
username ccna privilege 15 secret 5 $1$w3Hp$YIngTxHRU9S1bGTh30q0q.
!R1#show users
    Line       User       Host(s)              Idle       Location
*  0 con 0                 idle                 00:00:00    514 vty 0 ccna
       idle                 00:00:05 10.1.124.2
515 vty 1 ccna        idle                 00:08:00 10.1.124.4
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 2

Task 2.2

Tasks

- Configure R3 as a telnet server.
- Configure a banner on R3 that will be shown if someone accesses it via telnet.
- Configure the username and password without the privilege level option.
  - **Username: ccna**
  - **Password: cisco**
- Configure the enable password **cisco**.
- Secure all the passwords with type 7 encryption.
- Upon completing this task, you should be able to access R3 from R1 and R4.

Configuration

In this task, we need to configure the local user database without the privilege level 15 option. Therefore, the enable password is mandatory to get into the privilege mode of R3. The enable password can be set in two ways: **enable password** and **enable secret**. The first option will set a clear text password that can be seen in the running configuration. To secure the password with type 7 encryption, the **service password-encryption** command has been configured in the global configuration mode. However, the second enable password option will secure the password with type 5 encryption.

```
R3:


username ccna password cisco
!
enable password cisco
!
service password-encryption
!
line vty 0 4
login local
```

```
!
banner motd #
Welcome to INE CCNA R&S Workbook #
```

Verification

As the task requires, telnet R3 from R1 and R4.

```
R1#telnet 10.1.134.3
Trying 10.1.134.3 ... Open
Welcome to INE CCNA R&S Lab

User Access Verification

Username: ccna
Password: R3>enable
Password:  R3#
!R4#telnet 10.1.134.3
Trying 10.1.134.3 ... Open
Welcome to INE CCNA R&S Lab

User Access Verification

Username: ccna
Password: R3>enable
Password:  R3#
!
!R3#sh running-config | inc username
username ccna password 7 1511021F0725
!R3#show running-config | include enable
enable password 7 094F471A1A0A
```

As expected, we can see that all the passwords are type 7 encrypted, which cannot be seen in the running configuration.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 2

Task 2.3

Tasks

- Configure the enable password **ccna** on R3, and secure it with type 5 encryption. Do not remove the previously configured enable password.
- Configure the console password **ciscoccna** on R3.
- Telnet to R3 from R4 and verify preference for enable password types.

Configuration

In this task, we are asked to configure the enable secret password to enter the privilege level 15 mode. The enable secret option secures the password with type 5 encryption. Previously, we configured **enable password** on the same router. Now we have both types of enable passwords configured. Look at the following configuration to verify which type of password it prefers.

```
R3:

enable secret cisco
!
line console 0
password cisco
```

Verification

```
R3#show run | inc enable
enable secret 5 $1$f9Bl$.TacnnFEnE81yp/cxucJ11
enable password 7 094F471A1A0A
!R4#telnet 10.1.134.3
Trying 10.1.134.3 ... Open

Welcome to INE CCNA R&S Lab
```

```
User Access Verification

Username: ccna
Password:
R3>enable Password:

Password: R3#
```

When making a telnet session on R3, it prefers the password configured with **enable secret**.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 2

Task 2.4

Tasks

- Configure a static route on R2 for the destination network 4.4.4.4/32.
- Configure a static route on R4 for the destination network 2.2.2.2/32.
- Configure a static route on R1 for the destination networks 4.4.4.4/32 and 2.2.2.2/32.
- Both the routers should take their serial links as primary route.
- Verify your outputs using the `show ip protocols` and `show ip route` commands.
- Upon completing this task, you should be able to ping from R2's Loopback0 interface to R4's loopback network.

Configuration

In the IP routing section, we have two types of routing: **static routing** and **dynamic routing**. Static routes are usually configured by manually entering destination and next-hop information. In this task, we are asked to configure static routes on R2 for R4's /32 prefix and vice versa. Make sure that the static entries are configured with serial interface next-hop address. Also, R1 is in between of R2 and R4, so the static route entry for both the prefixes are required on it also.

```
R2:
ip route 4.4.4.4 255.255.255.255 10.1.12.1
R1:
ip route 2.2.2.2 255.255.255.255 10.1.12.2
ip route 4.4.4.4 255.255.255.255 10.1.14.4
R4:

ip route 2.2.2.2 255.255.255.255 10.1.14.1
```

Verification

```
R2#show ip route static

Codes: L - local, 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, H - NHRP, l - LISP
   a - application route
   + - replicated route, % - next hop override

Gateway of last resort is not set

  4.0.0.0/32 is subnetted, 1 subnets
S        4.4.4.4 [1/0] via 10.1.12.1
!R2#ping 4.4.4.4 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 2.2.2.2
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 44/44/44 ms
!R4#show ip route static
Codes: L - local, 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, H - NHRP, l - LISP
   a - application route
   + - replicated route, % - next hop override

Gateway of last resort is not set

  2.0.0.0/32 is subnetted, 1 subnets
S        2.2.2.2 [1/0] via 10.1.14.1
!R4#ping 2.2.2.2 source Loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 4.4.4.4
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 40/42/44 ms
!
!R1#show ip route static | beg Gateway
Gateway of last resort is not set

  2.0.0.0/32 is subnetted, 1 subnets
S        2.2.2.2 [1/0] via 10.1.12.2
```

```
4.0.0.0/32 is subnetted, 1 subnets
S        4.4.4.4 [1/0] via 10.1.14.4
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 2

Task 2.5

Tasks

- Configure additional loopback interfaces on R3 as follows:
  - Loopback33: 33.33.33.33/32
  - Loopback133: 133.133.133.133/32
- Configure static default routes on R1 and R4 so that they can reach to R3's loopback networks with a single route entry.
- Verify the routing table after configuration.

Configuration

In this task, we are allowed to write one route for the both destinations. Usually we configure default routing with 0.0.0.0/0 destination if there are multiple destinations. When verifying a static default route, we can see that the route is denoted with "S*", which is the default route with 0.0.0.0/0 destination.

```
R3:
interface Loopback33
 ip address 33.33.33.33 255.255.255.255
!
interface Loopback133
 ip address 133.133.133.133 255.255.255.255
R1


ip route 0.0.0.0 0.0.0.0 10.1.134.3
R1


ip route 0.0.0.0 0.0.0.0 10.1.134.3
```

Verification

```
R1#show ip route static | begin Gateway
Gateway of last resort is 10.1.134.3 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 10.1.134.3
    2.0.0.0/32 is subnetted, 1 subnets
S       2.2.2.2 [1/0] via 10.1.12.2
    4.0.0.0/32 is subnetted, 1 subnets
S       4.4.4.4 [1/0] via 10.1.14.4
!
!R4#show ip route static | begin Gateway
Gateway of last resort is 10.1.134.3 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 10.1.134.3

    2.0.0.0/32 is subnetted, 1 subnets
S       2.2.2.2 [1/0] via 10.1.14.1
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 2

Task 2.6

Tasks

- Configure additional interfaces as follows:
  - Configure Loopback11 interface with the IP address 11.11.11.11/32 on R1.
  - Configure Loopback22 interface with the IP address 22.22.22.22/32 on R2.
  - Configure Loopback44 interface with the IP address 44.44.44.44/32 on R4.
- Configure RIP version 2 on R1, R3, and R4.
- Do not advertise Loopback0 networks into RIP.
- Disable the auto-summarization feature on all routers.
- Verify reachability from R3 to R1 and R4's loopback interfaces.
- Verify things like RIP timers, advertised networks, etc.
- Enable RIP debugging and verify the route propagation process.

Configuration

```
R1:
interface Loopback11
 ip address 11.11.11.11 255.255.255.255
!
router rip
version 2
no auto-summary
network 11.0.0.0
network 10.0.0.0
end
R2:
inter Loopback22
 ip address 22.22.22.22 255.255.255.255
!
router rip
version 2
no auto-summary
```

```
network 22.0.0.0
network 10.0.0.0
end
R4:

interface Loopback44
 ip address 44.44.44.44 255.255.255.255
!
router rip
version 2
no auto-summary
network 44.0.0.0
network 10.0.0.0
end
```

Verification

```
R1#show ip int brief | ex una
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.1.124.1      YES manual up                    up
Serial1/0                  10.1.134.1      YES manual up                    up
Serial1/1                  10.1.12.1       YES manual up                    up
Serial1/3                  10.1.14.1       YES manual up                    up
Loopback0                  1.1.1.1         YES manual up                    up
Loopback11                 11.11.11.11     YES manual up                    up
!R1#show ip route rip
Codes: L - local, 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, H - NHRP, l - LISP
   a - application route
   + - replicated route, % - next hop override

Gateway of last resort is 10.1.134.3 to network 0.0.0.0

    22.0.0.0/32 is subnetted, 1 subnets
R       22.22.22.22 [120/1] via 10.1.12.2, 00:00:23, Serial1/1
    44.0.0.0/32 is subnetted, 1 subnets
R       44.44.44.44 [120/1] via 10.1.134.4, 00:00:20, Serial1/0
                [120/1] via 10.1.14.4, 00:00:11, Serial1/3
 !R1#show ip protocols | section Networks
Routing for Networks:
Routing for Networks:
```

```
10.0.0.0
 11.0.0.0
!R1#debug ip rip
*Sep  7 17:36:26.787: RIP: sending v2 update to 224.0.0.9 via Serial1/3 (10.1.14.1)
*Sep  7 17:36:26.787: RIP: build update entries
*Sep  7 17:36:26.787:   10.1.12.0/24 via 0.0.0.0, metric 1, tag 0
*Sep  7 17:36:26.787:   10.1.124.0/24 via 0.0.0.0, metric 1, tag 0
*Sep  7 17:36:26.787:   10.1.134.0/24 via 0.0.0.0, metric 1, tag 0
*Sep  7 17:36:26.787:   11.11.11.11/32 via 0.0.0.0, metric 1, tag 0
*Sep  7 17:36:26.787:   22.22.22.22/32 via 0.0.0.0, metric 2, tag 0
!*Sep  7 17:39:04.123: RIP: received v2 update from 10.1.14.4 on Serial1/3
*Sep  7 17:39:04.123:      10.1.124.0/24 via 0.0.0.0 in 1 hops
*Sep  7 17:39:04.123:      10.1.134.0/24 via 0.0.0.0 in 1 hops
*Sep  7 17:39:04.123:      22.22.22.22/32 via 0.0.0.0 in 2 hops
*Sep  7 17:39:04.123:      44.44.44.44/32 via 0.0.0.0 in 1 hops
<snip>
!
!R2#show ip interface brief | exclude unassigned
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.1.124.2      YES manual up                    up
Serial0/1/0                10.1.12.2       YES manual up                    up
Loopback0                  2.2.2.2         YES manual up                    up
Loopback22                 22.22.22.22     YES manual up                    up
!R2#show ip route rip
Codes: L - local, 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, H - NHRP, l - LISP
   a - application route
   + - replicated route, % - next hop override

Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
R        10.1.14.0/24 [120/1] via 10.1.124.4, 00:00:23, FastEthernet0/0
                      [120/1] via 10.1.124.1, 00:00:04, FastEthernet0/0
                      [120/1] via 10.1.12.1, 00:00:03, Serial0/1/0
R        10.1.134.0/24 [120/1] via 10.1.124.4, 00:00:23, FastEthernet0/0
                       [120/1] via 10.1.124.1, 00:00:04, FastEthernet0/0
                       [120/1] via 10.1.12.1, 00:00:03, Serial0/1/0
  11.0.0.0/32 is subnetted, 1 subnets
R        11.11.11.11 [120/1] via 10.1.124.1, 00:00:04, FastEthernet0/0
```

```
                [120/1] via 10.1.12.1, 00:00:03, Serial0/1/0
  44.0.0.0/32 is subnetted, 1 subnets
R        44.44.44.44 [120/1] via 10.1.124.4, 00:00:23, FastEthernet0/0
!R2#show ip protocols | section Networks
Routing for Networks:
Routing for Networks:10.0.0.0
22.0.0.0
!
!R4#show ip interface brief | exclude unassigned
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.1.124.4      YES manual up                    up
Serial1/0                  10.1.134.4      YES manual up                    up
Serial1/3                  10.1.14.4       YES manual up                    up
Loopback0                  4.4.4.4         YES manual up                    up
Loopback44                 44.44.44.44     YES manual up                    up
!R4#show ip route rip
Codes: L - local, 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, H - NHRP, l - LISP
   a - application route
   + - replicated route, % - next hop override

Gateway of last resort is 10.1.134.3 to network 0.0.0.0

  10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
R        10.1.12.0/24 [120/1] via 10.1.134.1, 00:00:14, Serial1/0
                [120/1] via 10.1.124.2, 00:00:08, FastEthernet0/0
                [120/1] via 10.1.124.1, 00:00:19, FastEthernet0/0
                [120/1] via 10.1.14.1, 00:00:13, Serial1/3
  11.0.0.0/32 is subnetted, 1 subnetsR        11.11.11.11 [120/1] via 10.1.134.1, 00:00:14, Serial1/0
                [120/1] via 10.1.124.1, 00:00:19, FastEthernet0/0
                [120/1] via 10.1.14.1, 00:00:13, Serial1/3
  22.0.0.0/32 is subnetted, 1 subnets
R        22.22.22.22 [120/1] via 10.1.124.2, 00:00:08, FastEthernet0/0
!R4#show ip protocols | sec Networks
Routing for Networks:
Routing for Networks: 10.0.0.0
 44.0.0.0
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 2

Task 2.7

Tasks

- Configure RIP authentication as follows:
  - Simple password authentication between R1 and R4.
  - Message digest authentication between R1 and R2.
  - Use password **cisco** for both authentication types.
- Verify authentication status.

Configuration

Basically, we have two types of RIP authentication: plain text and MD5.

In this task, we are asked to configure plain text authentication between R1 and R4, and message digest authentication between R1 and R2. To configure RIP authentication, the first step is to configure key chain, which is a group of key-id and string password. In the interface-specific mode, we can define whether we will configure clear text or message digest authentication. Upon configuring the authentication, we should be able to see the RIP routes as earlier.

R1:

```
key chain TEST
 key 1
 key-string cisco
!
interface Serial1/3
 ip rip authentication mode text
 ip rip authentication key-chain TEST
!
interface Serial1/1
 ip rip authentication mode md5
 ip rip authentication key-chain TEST
```

R4:

```
key chain TEST
 key 1
 key-string cisco
!
interface Serial1/3
 ip rip authentication mode text
 ip rip authentication key-chain TEST
R2:

key chain TEST
 key 1
 key-string cisco
!
interface Serial0/1/0
 ip rip authentication mode md5
 ip rip authentication key-chain TEST
```

Verification

```
R1#show ip protocols | beg Default

Default version control: send version 2, receive version 2
Interface              Send  Recv  Triggered RIP  Key-chain
FastEthernet0/0        2     2
Serial1/0              2     2
Serial1/1              2     2                   TEST
            Serial1/3              2     2                   TEST

Loopback11             2     2
Automatic network summarization is not in effect
    Maximum path: 4
Routing for Networks:
    10.0.0.0
    11.0.0.0
Routing Information Sources:
Gateway         Distance      Last Update
10.1.14.4            120      00:00:22
10.1.12.2            120      00:00:27
10.1.124.4           120      00:00:12
10.1.124.2           120      00:00:12
Distance: (default is 120)
!R2#debug ip rip
RIP protocol debugging is onSep  9 11:32:55.190: RIP: received packet with text authentication cisco
```

```
Sep  9 11:32:55.190: RIP: received v2 update from 10.1.14.4 on Serial1/3
Sep  9 11:32:55.190:      10.1.124.0/24 via 0.0.0.0 in 1 hops
Sep  9 11:32:55.190:      22.22.22.22/32 via 0.0.0.0 in 2 hops
Sep  9 11:32:55.190:      44.44.44.44/32 via 0.0.0.0 in 1 hops
!Sep  9 11:32:58.594: RIP: received packet with MD5 authentication

Sep  9 11:32:58.594: RIP: received v2 update from 10.1.12.2 on Serial1/1
Sep  9 11:32:58.594:      10.1.124.0/24 via 0.0.0.0 in 1 hops
Sep  9 11:32:58.594:      22.22.22.22/32 via 0.0.0.0 in 1 hops
Sep  9 11:32:58.594:      44.44.44.44/32 via 0.0.0.0 in 2 hops
```

Initially, we can see the authentication key-chain using the `show ip protocols` command, and we can also debug RIP for the additional real-time messages. Therefore, `debug ip rip` shows the type of authentication being used on each interface.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 2

Task 2.8

Tasks

- Configure EIGRP 99 on the point-to-point network between R1 & R4 & frame-relay network.
- Use specific wildcard mask when advertising connected networks.
- Advertise 10.1.124.0/24 and Loopback0 interface on R1 and R4.
- Disable auto-summarization feature on all the EIGRP routers.
- Verify EIGRP neighbor table, topology table and routing table on R3.
- Upon completing this task, you should be able to ping from each others Loopback0 networks.

Configuration

In this task, we are asked to configure EIGRP in AS 99 on the frame-relay backbone and the point-to-point link between R1 and R4. At first, configure EIGRP in AS 99 on R1,R3 and R4.

```
R3:
router eigrp 99
no auto-summary
network 3.3.3.3 0.0.0.0
network 10.1.134.0 0.0.0.255
R1:
router eigrp 99
no auto-summary
network 1.1.1.1 0.0.0.0
network 10.1.124.0 0.0.0.255
network 10.1.134.0 0.0.0.255
network 10.1.14.0 0.0.0.255
R4

router eigrp 99
```

```
no auto-summary
network 4.4.4.4 0.0.0.0
network 10.1.124.0 0.0.0.255
network 10.1.134.0 0.0.0.255
network 10.1.14.0 0.0.0.255
```

Verification

At first, check for neighbor table on all the EIGRP routers. In this table, we can find the neighbors information as shown below:

```
R3#show ip eigrp neighbors

EIGRP-IPv4 Neighbors for AS(99)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   10.1.134.4              Se0/0/0                 175 00:01:52   27   162  0  17
0   10.1.134.1              Se0/0/0                 178 00:02:31   21   126  0  18
!
!R1#sh ip eigrp neighbors

EIGRP-IPv4 Neighbors for AS(99)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   10.1.124.4              Fa0/0                    11 00:00:12    3   100  0  29
3   10.1.14.4               Se1/3                    27 14:11:13   14  1170  0  28
2   10.1.134.4              Se1/0                   173 14:23:27   21  1170  0  27
0   10.1.134.3              Se1/0                   167 14:24:06  277  1662  0  12
!
!R4#show ip eigrp neighbors

EIGRP-IPv4 Neighbors for AS(99)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   10.1.124.1              Fa0/0                    12 00:02:37    4   100  0  30
3   10.1.14.1               Se1/3                    25 14:13:38   15  1170  0  29
2   10.1.134.1              Se1/0                   159 14:25:52  228  1368  0  28
1   10.1.134.3              Se1/0                   179 14:25:52  345  2070  0  12
```

Once the neighbors are established, we can look into the EIGRP topology table on R3 where all the routes learnt from both the neighbors are recorded. Upon getting routing information from the different neighbors, EIGRP calculates best path on the basis of the **FD [Feasible Distance]** value which is the total metric between source

and destination. The primary route is typically called a **successor route** in EIGRP and the backup routes are called **feasible successor**. Multiple routes can be installed in the routing table if the metric of two or more routes are equal. In this case EIGRP does load balance between the multiple paths. By default, EIGRP supports **4** equal cost paths, which can be configured up to **16** using **maximum-paths** command.

```
R3#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(99)/ID(133.133.133.133)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
   r - reply Status, s - sia Status
P 10.1.124.0/24, 2 successors, FD is 2172416
    via 10.1.134.1 (2172416
/28160), Serial0/0/0    via 10.1.134.4 (2172416
/28160), Serial0/0/0P 10.1.14.0/24, 2 successors, FD is 21024000
    via 10.1.134.1 (21024000
/20512000), Serial0/0/0    via 10.1.134.4 (21024000
/20512000), Serial0/0/0P 4.4.4.4/32, 1 successors, FD is 2297856
    via 10.1.134.4 (2297856
/128256), Serial0/0/0
    via 10.1.134.1 (2300416/156160), Serial0/0/0
P 10.1.134.0/24, 1 successors, FD is 2169856
    via Connected, Serial0/0/0
P 3.3.3.3/32, 1 successors, FD is 128256
    via Connected, Loopback0P 1.1.1.1/32, 1 successors, FD is 2297856
    via 10.1.134.1 (2297856
/128256), Serial0/0/0
    via 10.1.134.4 (2300416/156160), Serial0/0/0
```

In the above output, we saw two paths to get to 10.1.124.0/24 network. The total metric, i.e. Feasible Distance is 2172416 and the distance from neighboring device, i.e. Advertised Distance is 28160. In this case, both the routes have same FD values which does mean that both the routes are going to be installed in the routing table after DUAL calculation.

```
R3#show ip route eigrp
Codes: L - local, 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, H - NHRP, l - LISP
   a - application route
   + - replicated route, % - next hop override
```

```
Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
D        1.1.1.1 [90/2297856] via 10.1.134.1, 00:24:58, Serial0/0/0
      4.0.0.0/32 is subnetted, 1 subnets
D        4.4.4.4 [90/2297856] via 10.1.134.4, 00:24:24, Serial0/0/0
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
D        10.1.14.0/24 [90/21024000] via 10.1.134.4, 00:12:45, Serial0/0/0
                      [90/21024000
] via 10.1.134.1, 00:12:45, Serial0/0/0
D        10.1.124.0/24 [90/2172416] via 10.1.134.4, 00:24:58, Serial0/0/0
                       [90/2172416
] via 10.1.134.1, 00:24:58, Serial0/0/0
```

Like we discussed above, both the paths have been installed in the routing table, which will be equal cost load balanced. The load balancing can be verified using "traceroute" to the 10.1.124.2 address.

```
R3#traceroute 10.1.124.2
Type escape sequence to abort.
Tracing the route to 10.1.124.2
VRF info: (vrf in name/id, vrf out name/id)
1 10.1.134.1 16 msec 10.1.134.4 16 msec
 10.1.134.1 16 msec

2 10.1.124.2 16 msec *  12 msec
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 2

Task 2.9

Tasks

- Configure EIGRP hello and hold timers to 10 and 30 second between R1 and R4.
- Suppress "Hello" messages where EIGRP neighborship is not required.
- Verify EIGRP timers on both routers.

Configuration

By default, EIGRP has hello and hold intervals of 5 and 15 seconds in the point-to-point and broadcast network. We can manually change it by using the `ip hello interval eigrp` interface-specific command and setting the desired hello interval. Unlike OSPF, EIGRP still forms neighborship if the hello and hold intervals are different on either end. In the case of non-broadcast networks such as Frame Relay and ATM, the hell0 and hold intervals are 60 and 180 seconds.

The `passive-interface` command is configured under the router-specific mode to suppress hello messages where unnecessary. In this case, we are running EIGRP on the LAN interfaces (that is, the FastEthernet0/0 interfaces of both R1 and R4). Therefore, the hello message are unnecessary on these interfaces and we need to configure the `passive-interface` command under the eigrp 99 router-specific mode.

```
R1:
interface Serial1/3
 ip hello-interval eigrp 99 10
 ip hold-time eigrp 99 30
!
router eigrp 99
 passive-interface FastEthernet0/0
R4:

interface Serial1/3
 ip hello-interval eigrp 99 10
 ip hold-time eigrp 99 30
```

```
!
router eigrp 99
 passive-interface FastEthernet0/0
```

Verification

```
R1#show ip eigrp interfaces detail Serial1/3
EIGRP-IPv4 Interfaces for AS(99)
                        Xmit Queue   PeerQ        Mean   Pacing Time   Multicast    Pending
Interface              Peers  Un/Reliable  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Se1/3                    1        0/0       0/0          15       5/195        255           0
Hello-interval is 10, Hold-time is 30
Split-horizon is enabled
Next xmit serial <none>
Packetized sent/expedited: 2/0
Hello's sent/expedited: 10805/2
Un/reliable mcasts: 0/0  Un/reliable ucasts: 2/3
Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 0
Retransmissions sent: 0  Out-of-sequence rcvd: 0
Topology-ids on interface - 0
Authentication mode is not set
!
!R4#show ip eigrp interfaces detail Serial1/3
EIGRP-IPv4 Interfaces for AS(99)
                        Xmit Queue   PeerQ        Mean   Pacing Time   Multicast    Pending
Interface              Peers  Un/Reliable  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Se1/3                    1        0/0       0/0          15       5/195        251           0
Hello-interval is 10, Hold-time is 30

Split-horizon is enabled
Next xmit serial <none>
Packetized sent/expedited: 2/0
Hello's sent/expedited: 10948/2
Un/reliable mcasts: 0/0  Un/reliable ucasts: 3/3
Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 0
Retransmissions sent: 0  Out-of-sequence rcvd: 0
Topology-ids on interface - 0
Authentication mode is not set
```

Because we were able to see the neighborship between R1 and R4 via FastEthernet link, it was removed after we configured **passive-interface** for the FastEthernet0/0 interface under the EIGRP 99 process. Because we already had

neighborship between R1 and R4 via serial link, the EIGRP hellos need not be sent over the FastEthernet0/0 link. Verify the neighborship on R1 and R4 again.

```
R1#show ip eigrp neighbors

EIGRP-IPv4 Neighbors for AS(99)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
3   10.1.14.4               Se1/3                    28 14:32:37   15  1170  0  30
2   10.1.134.4              Se1/0                   164 14:44:52   21  1170  0  31
0   10.1.134.3              Se1/0                   152 14:45:31  226  1356  0  12
!
!R4#show ip eigrp neighbors

EIGRP-IPv4 Neighbors for AS(99)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
3   10.1.14.1               Se1/3                    22 14:34:45   15  1170  0  31
2   10.1.134.1              Se1/0                   146 14:46:59  189  1140  0  32
1   10.1.134.3              Se1/0                   129 14:46:59  280  1680  0  12
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 2

Task 2.10

Tasks

- Configure OSPF on the broadcast network in area 0.
- Advertise Loopback0 networks of R1, R2, and R4 in OSPF area 0.
- Configure the serial point-to-point link between R1 and R4 in OSPF area 1.
- Upon completing this task, you should be able to see the 4.4.4.4/32 route in the OSPF routing table.
- Do not remove existing static routes.

Configuration

We know that the OSPF works on the basis of area hierarchy to minimize LSA flooding. In this task, we are asked to configure OSPF area 0 in the broadcast network between R1, R2, and R4. The task also asks us to configure area 1 OSPF on the point-to-point link between R1 and R4. In the broadcast network, OSPF elects one DR and BDR per segment, but in the case of the point-to-point serial link, DR and BDR election is not performed.

```
R1:
router ospf 1
network 1.1.1.1 0.0.0.0 area 0
network 10.1.14.0 0.0.0.255 area 1
network 10.1.124.0 0.0.0.255 area 0
R2:
router ospf 1
network 2.2.2.2 0.0.0.0 area 0
network 10.1.124.0 0.0.0.255 area 0
R4


router ospf 1
network 4.4.4.4 0.0.0.0 area 0
network 10.1.124.0 0.0.0.255 area 0
```

```
network 10.1.14.0 0.0.0.255 area 0
```

Verification

First, check for the neighbor relationship between all the router interfaces. By default, OSPF picks the highest loopback IP address as the router-id if it has not been configured manually. In the following outputs, we can see that the point-to-point serial connectivity does not have DR/BDR status because it does not perform DR/BDR election. In the case of broadcast networks, there are DR/BDR elections.

```
R1#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
22.22.22.22       1   FULL/BDR        00:00:39    10.1.124.2      FastEthernet0/0
44.44.44.44       1   FULL/DROTHER    00:00:37    10.1.124.4      FastEthernet0/0
44.44.44.44       0   FULL/  -        00:00:37    10.1.14.4       Serial1/3
!
!R2#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
11.11.11.11       1   FULL/DR         00:00:30    10.1.124.1      FastEthernet0/0
44.44.44.44       1   FULL/DROTHER    00:00:34    10.1.124.4      FastEthernet0/0
!
!R4#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
11.11.11.11       1   FULL/DR         00:00:36    10.1.124.1      FastEthernet0/0
22.22.22.22       1   FULL/BDR        00:00:36    10.1.124.2      FastEthernet0/0
11.11.11.11       0   FULL/  -        00:00:39    10.1.14.1       Serial1/3
```

The next section of this task is to check for the routing table of OSPF. Frst check for the routing table of R2.

```
R2#show ip route ospf
Codes: L - local, 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, H - NHRP, l - LISP
```

```
    a - application route
    + - replicated route, % - next hop override

Gateway of last resort is not set

  1.0.0.0/32 is subnetted, 1 subnets
O        1.1.1.1 [110/2] via 10.1.124.1, 00:13:52, FastEthernet0/0
  10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O IA     10.1.14.0/24 [110/782] via 10.1.124.4, 00:09:55, FastEthernet0/0

                   [110/782] via 10.1.124.1, 00:10:02, FastEthernet0/0
```

In the above output, we can see that the prefix 10.1.14.0/24 has been learned as an inter-area route because we have configured it under area 1. The prefix 1.1.1.1/32 has been configured for area 0 in the OSPF, so it is learned as the intra-area "O" route. Because of the static route configured in the earlier tasks, OSPF is unable to put the 4.4.4.4/32 prefix in the routing table because its administrative distance is higher than the static route. The tasks restricts us from removing existing static routes, but we have another option for configuring the **floating static route** to get that particular prefix in the OSPF routing table.

Let's verify the static route configured for the 4.4.4.4/32 prefix.

```
R2#show ip route static
Codes: L - local, 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, H - NHRP, l - LISP
   a - application route
   + - replicated route, % - next hop override

Gateway of last resort is not set

  4.0.0.0/32 is subnetted, 1 subnets
S        4.4.4.4 [1/0
] via 10.1.12.1
```

Now configure the floating static route with an administrative distance value of 111, because the OSPF has 110 as its AD value.

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip route 4.4.4.4 255.255.255.255 10.1.12.1 111
```

Verify the OSPF routing table again.

```
R2#show ip route ospf
Codes: L - local, 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, H - NHRP, l - LISP
   a - application route
   + - replicated route, % - next hop override

Gateway of last resort is not set

    1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1 [110/2] via 10.1.124.1, 00:29:06, FastEthernet0/0
    4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/2] via 10.1.124.4, 00:01:03, FastEthernet0/0

    10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O IA    10.1.14.0/24 [110/782] via 10.1.124.4, 00:25:09, FastEthernet0/0
                   [110/782] via 10.1.124.1, 00:25:16, FastEthernet0/0
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 2

Task 2.11

Tasks

- Configure router-ids to reflect their Loopback0 IP addresses.
- Configure OSPF hello and dead intervals of 5 and 20 seconds on the link between R1 and R4.
- Configure OSPF to elect DR for R1 and BDR for R2. R4 should be seen as DROTHER. Do not change the router-id.
- Verify OSPF DR and BDR status on R1 and R2.
- Verify OSPF neighborship and routes.

Configuration

By default, OSPF chooses the highest loopback interface IP address as its router-id. We can configure the router-id with the `router-id` command under the OSPF instance.

Let's configure the router-id and other tasks on all the OSPF routers. Make sure to clear the OSPF neighborship with `clear ip ospf process` for the changes to take effect.

```
R1:
router ospf 1
router-id 1.1.1.1
!
interface Serial1/3
ip ospf hello-interval 5
ip ospf dead-interval 20
!
interface FastEthernet0/0
ip ospf priority 255
R2:
router ospf 1
router-id 2.2.2.2
```

```
!
interface FastEthernet0/0
ip ospf priority 254
R4:
router ospf 1
router-id 4.4.4.4
!
interface Serial1/3
ip ospf hello-interval 5
ip ospf dead-interval 20
On all routers:

clear ip ospf process
```

Verification

```
R1#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface 2.2.2.2 254
   FULL/BDR        00:00:37    10.1.124.2      FastEthernet0/0
4.4.4.4           1   FULL/DROTHER    00:00:38    10.1.124.4      FastEthernet0/0
4.4.4.4           0   FULL/  -        00:00:18    10.1.14.4       Serial1/3
!
!R2#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface 1.1.1.1 255
   FULL/DR         00:00:36    10.1.124.1      FastEthernet0/0
4.4.4.4           1   FULL/DROTHER    00:00:38    10.1.124.4      FastEthernet0/0
R2#
!
!R4#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface 1.1.1.1 255
   FULL/DR         00:00:36    10.1.124.1      FastEthernet0/0 2.2.2.2 254
   FULL/BDR        00:00:32    10.1.124.2      FastEthernet0/0
1.1.1.1           0   FULL/  -        00:00:16    10.1.14.1       Serial1/3
```

In the above output, R4 is shown as DROTHER by both R1 and R2. We can also see that the point-to-point link has 20 seconds of dead-interval as required by the

task. For further verification on the hello and dead timers, issue the following command.

```
R1#show ip ospf interface Serial 1/3 | inc Hello
 Timer intervals configured, Hello 5, Dead 20
, Wait 20, Retransmit 5
    Hello due in 00:00:03
```

Again, verify the OSPF routes on R2.

```
R2#show ip route ospf

Codes: L - local, 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, H - NHRP, l - LISP
   a - application route
   + - replicated route, % - next hop override

Gateway of last resort is not set

  1.0.0.0/32 is subnetted, 1 subnets
O        1.1.1.1 [110/2] via 10.1.124.1, 00:08:06, FastEthernet0/0
  4.0.0.0/32 is subnetted, 1 subnets
O        4.4.4.4 [110/2] via 10.1.124.4, 00:08:06, FastEthernet0/0
  10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O IA     10.1.14.0/24 [110/782] via 10.1.124.4, 00:08:06, FastEthernet0/0
                [110/782] via 10.1.124.1, 00:08:06, FastEthernet0/0
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 3

Task 3.1

> You must load the initial configuration files for the section, **FS Lab-3 Initial**, which can be found in CCNA Routing & Switching Topology Diagrams and Initial Configurations.

Tasks

- Configure IP addresses on all the routers as shown in the diagram.
- Configure R1 as the DHCP server as follows:
  - Network: 192.168.1.0/24
  - Default Gateway: 192.168.1.1
  - Primary DNS Sever: 8.8.8.8
  - Secondary DNS Server: 8.8.4.4
  - Lease: 12 hours
- Allocate IPv4 addresses, from 192.168.1.50 to 192.168.1.60.
- The DHCP server should not to use the rest of the IPs from this subnet.
- Configure Host A and Host B to obtain their IP from DHCP server.

Configuration

Cisco IOS can be configured as the DHCP server to allocate dynamic IPs to the hosts. The recent Cisco IOS runs DHCP service by default, and we can just create the pool with its attributes. In this task, we have been given the DHCP parameters to be configured, and Host A and Host B should receive IP addresses dynamically from R1 (the DHCP server). At first, configure IP addressing and test the point-to-point reachability between the devices.

```
R1:
interface FastEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 no shutdown
!
interface FastEthernet0/1
```

```
 ip address 10.1.13.1 255.255.255.0
 no shutdown
R2:
 interface FastEthernet0/0
 ip address 192.168.1.3 255.255.255.0
 no shutdown
!
interface FastEthernet0/1
 ip address 10.1.24.2 255.255.255.0
 no shutdown
R3:
interface FastEthernet0/1
 ip address 10.1.13.3 255.255.255.0
R4:

interface FastEthernet0/1
 ip address 10.1.24.4 255.255.255.0
```

Now configure R1 as the DHCP server for the 192.168.1.0/24 network.

```
R1:

ip dhcp pool TEST
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 8.8.8.8 8.8.4.4
 lease 0 12
!
ip dhcp excluded-address 192.168.1.1 192.168.1.49
ip dhcp excluded-address 192.168.1.61 192.168.1.254
```

Verification

Initially, Host A and Host B need to be configured for DHCP using the `ip address dhcp` command under their respective interfaces. Then, both hosts will get their IP address from R1, which is the DHCP server in our case. To verify the DHCP process, we can run `show ip dhcp binding` on the server, and we can also see the IPv4 address on both hosts.

```
Host_A:
enable
configure terminal
interface FastEthernet0/10ip address dhcp
```

```
Host_B:
enable
configure terminal
interface FastEthernet0/13ip address dhcp
```

Verify IP address assignment and default-gateway on both hosts. Make sure to enable `ip domain lookup` on both hosts before checking for whether name-server addresses were received from the DHCP server.

```
Host_A#show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/10       192.168.1.50    YES DHCP   up                    up

!Host_A#show ip route
Default gateway is 192.168.1.1

Host               Gateway           Last Use    Total Uses  Interface
ICMP redirect cache is empty
!Host_A(config)#ip domain lookup
Host_A(config)#do ping ine.com
Translating"ine.com"...domain server (8.8.8.8
)
!
!Host_B#show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/13       192.168.1.51    YES DHCP   up                    up
!Host_B#show ip route
Default gateway is 192.168.1.1

Host               Gateway           Last Use    Total Uses  Interface
ICMP redirect cache is empty
!Host_B(config)#ip domain lookup
Host_B(config)#do ping ine.com
Translating"ine.com"...domain server (8.8.8.8
)
```

In the above output, we can see that the hosts are pointing toward their primary DNS server address, 8.8.8.8. Because we have pinged a domain name that does not exist anywhere in this lab, you should not expect reachability to the domain ine.com. Technically, if the primary DNS server fails, the secondary will take care of each and every DNS request.

Also, check for DHCP binding table on R1.

```
R1#show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.1.50        0063.6973.636f.2d30.    Sep 27 2014 09:19 PM    Automatic
                    3030.632e.3835.3831.
                    2e61.3530.302d.4661.
                    302f.3130
192.168.1.51        0063.6973.636f.2d30.    Sep 27 2014 09:19 PM    Automatic

                    3030.652e.3833.3064.
                    2e66.3638.302d.4661.
                    302f.3133
```

In the above output, we can see the DHCP binding of the IP address and the hardware addresses of individual hosts. If required, the binding database can be cleared using the `clear ip dhcp binding *` privilege exec command.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 3

Task 3.2

Tasks

- Configure R1 as the telnet server as follows:
  - Use the username **cisco** and the password **ine** with type 5 encryption.
  - Do not use enable password.
  - Upon successful login, you should have a privilege level of 15.
- Configure R2 as the telnet server as follows:
  - Use the username **cisco** and the password **ine** with type 7 encryption.
  - Use the enable password **cisco**.
  - Upon successful login, you should have a privilege level of 15.

Configuration

Telnet uses TCP as its transport and port 23 as the service identification number. A Cisco router can be configured with the telnet server feature so that administrators can access the router remotely. Among the various approaches to configuring authentication methods, we are asked to configure two types of authentication in this task. The difference between the two configurations here is with the enable password and with the "privilege 15" argument in the local user database.

If the username is created with the "secret" option, the IOS will secure a local user password with type 5 encryption. Alternately, if the "password" option is used when creating the local user, the password will not be encrypted and can be seen when issuing `show running-config`. So, to secure the password with type 7 encryption, the `service password-encryption` command must be configured in the global configuration mode, which would secure the entire password of the router with type 7 encryption.

R1:

```
username cisco privilege 15 secret ine
!
line vty 0 4
login local
```

```
R2:

username cisco password ine
!
enable password cisco
!
service password-encryption
!
line vty 0 4
login local
```

Verification

```
Host_A#telnet 192.168.1.2
Trying 192.168.1.2 ... Open

User Access Verification

Username: cisco
Password: R1#show privilege
Current privilege level is 15
!R1#show run | include username
username cisco privilege 15 secret 5 $1$efns$7libORXdvOoHhmBgTIpVu0
```

As required by the task, we can get in to R1's privilege 15 mode without using the enable password because of the `privilege` command used along with the username and password. Additionally, we can also see the type 5 encrypted password because the "secret" keyword is used instead of the "password" option. Now, try to log in to R2.

```
Host_A#telnet 192.168.1.3
Trying 192.168.1.3 ... Open

User Access Verification

Username: cisco
Password: R2>enable
Password:
R2#
!R2#show privilege
 Current privilege level is 15
```

```
!R2#show run | include username
username cisco password 7 12100B12
```

We must pass through the enable password, which is required to get in to the privilege level 15 mode. Also, the encryption is 7 here, unlike in the previous task.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 3

Task 3.3

Tasks

- Configure SSH version 2 on R1.
- Use 1024-bit key module for SSH.
- Configure the domain name cisco.com
- Authenticate SSH clients using the username **ccna** and the password **cisco**.
- The password should be secured with type 5 encryption.
- To meet the security standard, do not allow telnet connection on it.
- Host A and Host B should be able to SSH on R1.

Configuration

SSH stands for Secure Shell, which uses TCP port 22. SSH provides secure communication to access remote network devices. Communication between the client and server is encrypted in both SSH version 1 and SSH version 2. To configure SSH, we should configure hostname, domain name, and privilege 15 username and password. Additionally, we can filter the remote communication protocol using "transport input" line configuration mode. It has components such as "all", "telnet", "ssh", and "none". In our case, we need to use "transport input ssh," which allows only the SSH connection refusing the telnet communication. By default, SSH version 1.99 is enabled as soon as we generate the crypto key, which can be changed using the `ip ssh version` global configuration command.

R1:

```
ip domain name cisco.com
!
username ccna privilege 15 secret cisco
!
crypto key generate rsa
!
line vty 0 4
```

```
login local
transport inpout ssh
```

Verification

Initially, let's verify the public/private key generated by the router to provide secure remote connection to its clients. After that, we can test whether the clients can make the telnet or SSH connection or both.

```
R1#show crypto key mypubkey rsa
% Key pair was generated at: 09:36:07 UTC Sep 28 2014 Key name: R1.cisco.com
Key type: RSA KEYS
 Storage Device: private-config
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00DA49EB
  98E90303 2A9D4E61 04F7A5FD 5676101B A418DF43 8152E500 A7BD5A8C D9E7211A
  5911D137 2C021856 86921553 0004E12D E042959B 44D163AE D118943C 4A9AC410
  64F599CE 938C9CEA 9FD31943 37683E4C 39579D12 331AD4DC E9C23E90 018ECFA3
  0A6E67C8 60BC7B60 CECDD623 2201B06B 2199158B 3978700F 57DDCF61 39020301 0001
% Key pair was generated at: 09:36:13 UTC Sep 28 2014 Key name: R1.cisco.com.server
Key type: RSA KEYS
Temporary key
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D9E1F2 88C959BA
  09200311 673967C7 CA0F985B 8CF9912C 8BC1A53E 41CE7D15 BB1C0344 6AD52BE4
  9317CDAC 18A98C29 C3B3938D A0FF55B4 934B21F3 EEB878FA 2C0766F5 BAE73F13
  168844FD 97186DEA B588D3BF 8C55EB08 84CC2787 7F232CBE 43020301 0001
! R1#show ip ssh
 SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa
, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDaSeuY6QMDKp1OYQT3pf1WdhAbpBjfQ4FS5QCnvVqM
2echGlkR0TcsAhhWhpIVUwAE4S3gQpWbRNFjrtEYlDxKmsQQZPWZzpOMnOqf0xlDN2g+TDlXnRIzGtTc
6cI+kAGOz6MKbmfIYLx7YM7N1iMiAbBrIZkVizl4cA9X3c9hOQ==
!R1#show run | include username ccna
username ccna privilege 15 secret 5 $1$hA4Y$4etFqNGtGyXMJX6xO.Tx31
```

```
!
!Host_A#telnet 192.168.1.2
Trying 192.168.1.2 ... % Connection refused by remote host
```

The telnet connection has been denied by R1 because we have allowed only the SSH connection using the `transport input` command. Now try to log in to R1 using SSH.

```
Host_A#ssh -l ccna 192.168.1.2

Password:
R1#
!
!Host_B#ssh -l ccna 192.168.1.2

Password:
R1#
!
!R1#show users
Line       User       Host(s)              Idle      Location
*  0 con 0                 idle                 00:00:00
514 vty 0     ccna       idle                 00:00:16 192.168.1.51
515 vty 1     ccna       idle                 00:00:08 192.168.1.50


  Interface    User               Mode         Idle     Peer Address
```

Both the hosts are logged in to R1 using the username **ccna** as required.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 3

Task 3.4

Tasks

- Configure Sw1 for CDP.
- It should see Host A and Host B via CDP.

Configuration

CDP stands for Cisco Discovery Protocol, a Cisco proprietary neighbor discovery protocol. In open standard version, we can use LLDP (Link Layer Detection Protocol) where a multi-vendor environment exists. CDP exchanges its hello message every 60 seconds and has a hold time of 180 seconds. CDP provides information about the remote Cisco devices such as hostname, outgoing/remote interfaces, IP address, and capability. By default, Cisco routers and switches run CDP, which can be configured in the global configuration mode or at an interface-specific level.

```
Sw1:

cdp run
```

Verification

```
Sw1#show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Host_B           Fas 0/13          126             S I   WS-C3550- Fas 0/13
Host_A           Fas 0/10          166             S I   WS-C3550- Fas 0/10
```

```
R2              Fas 0/2          123            R B S I 1841      Fas 0/0
R1.cisco.com    Fas 0/1          172            R B S I 2811      Fas 0/0
```

In the above output, Sw1 can see Host_A via its Fas0/10 interface, whereas it can see Host_B via its Fas0/13 interface. The capability of both hosts are Switch and IGMP device, and both hosts are Cisco 3550 switches. We can examine the neighborship in more detail below.

```
Sw1#show cdp neighbors fa0/10 detail

-------------------------Device ID: Host_A
Entry address(es):  IP address: 192.168.1.50
Platform: Cisco WS-C3550-24,  Capabilities:Switch IGMP
 Interface:FastEthernet0/10
,  Port ID (outgoing port): FastEthernet0/10Holdtime : 162 sec

Version :
Cisco IOS Software, C3550 Software (C3550-IPSERVICESK9-M), Version 12.2(50)SE, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Sat 28-Feb-09 04:04 by weiliu

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27, value=00000000FFFFFFFF010221FF0000000000000000C858
VTP Management Domain: ''
Duplex: full
Management address(es):
  IP address: 192.168.1.50
!
!Sw1#show cdp neighbors fa0/13 detail

-------------------------Device ID: Host_B
Entry address(es):  IP address: 192.168.1.51
Platform: Cisco WS-C3550-24,  Capabilities:Switch IGMP
 Interface:FastEthernet0/13
,  Port ID (outgoing port): FastEthernet0/13Holdtime : 168 sec

Version :
Cisco IOS Software, C3550 Software (C3550-IPSERVICESK9-M), Version 12.2(50)SE, RELEASE SOFTWARE (fc1)

Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Sat 28-Feb-09 04:04 by weiliu

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27, value=00000000FFFFFFFF010221FF0000000000000000E830
VTP Management Domain: ''
```

```
Duplex: full
Management address(es):
  IP address: 192.168.1.51
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 3

Task 3.5

Task

- Configure loopback1 interface on R1 and R2 using **1.1.1.1/32** network on both the routers.
- Configure HSRP on R1 and R2 as follows:
  - HSRP virtual router IP address will be **192.168.1.1**.
  - Set group number **1** and use the MD5 authentication password **cisco**.
  - R1 should be elected as the Active HSRP router.
  - If R1 fails, R2 should take over and make sure that R1 will take its "active" role back when it comes online.
  - Check and verify failover pinging **1.1.1.1** from Host A.

Configuration

HSRP is a Cisco proprietary gateway redundancy protocol that uses UDP port 1985. An HSRP router has "active" and "standby" roles; whichever has the higher priority is considered the "active" router, and the rest of the routers are considered "standby." The active router replies to the ARP request destined for the virtual gateway MAC address. When the active router fails, the standby router automatically takes over the active role and starts to reply to the ARP request made by the clients.

R2:

```
interface Loopback1
 ip address 1.1.1.1 255.255.255.0
!
interface FastEthernet0/0
 standby 1 ip 192.168.1.1
 standby 1 preempt
 standby 1 authentication md5 key-string cisco
```

R1:

```
interface Loopback1
 ip address 1.1.1.1 255.255.255.0
!
interface FastEthernet0/0
 standby 1 ip 192.168.1.1
 standby 1 preempt
 standby 1 priority 101
 standby 1 authentication md5 key-string cisco
```

Verification

In the above tasks, we configured HSRP and assigned priority on R1 so that it would take its active role. Additionally, the "preempt" feature tells R1 to take its role back if it comes back from a failure. Likewise, the strongest method is MD5 for authentication, which is more secure than clear-text password authentication. Now we can verify the HSRP using the `show standby` and `show standby brief` commands on R1 and R2. Also, we can ping 1.1.1.1 continuously and make R1 fail and check whether R2 takes over the active role or not.

```
R1#show standby
FastEthernet0/0 - Group 1 State is Active
    2 state changes, last state change 00:12:05 Virtual IP address is 192.168.1.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.160 secs Authentication MD5, key-string
  Preemption enabled  Active router is local
  Standby router is 192.168.1.3, priority 100 (expires in 10.496 sec) Priority 101 (configured 101)
  Group name is "hsrp-Fa0/0-1" (default)
!R1#show standby brief

                     P indicates configured to preempt.
                      |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Fa0/0       1    101 P Active  local           192.168.1.3     192.168.1.1
!
!R2#show standby

FastEthernet0/0 - Group 1 State is Standby
    1 state change, last state change 00:09:46 Virtual IP address is 192.168.1.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.120 secs
```

```
 Authentication MD5, key-string


   Preemption enabled Active router is 192.168.1.2, priority 101 (expires in 8.768 sec)
   Standby router is local Priority 100 (default 100)
   Group name is "hsrp-Fa0/0-1" (default)
! R2#show standby brief
                     P indicates configured to preempt.
                     |
Interface    Grp  Pri P State   Active          Standby         Virtual IP
Fa0/0        1    100 P Standby 192.168.1.2     local           192.168.1.1
```

Now, ping 1.1.1.1 from Host A and shut down the Fastethernet0/0 interface on R1. When we shut down the port, R2 will take the active role.

```
Host_A#ping 1.1.1.1 repeat 1000 size 18000


Type escape sequence to abort.
Sending 1000, 18000-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.
!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!Success rate is 99 percent (999/1000), round-trip min/avg/max = 40/41/76 ms
```

After re-enabling the FastEthernet0/0 interface on R1, we can see that R1 has taken the active role again because of the preemption feature enabled on it.

```
R1#show standby brief


                 P indicates configured to preempt.
                 |
```

```
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Fa0/0       1    101 P Active  local           192.168.1.3     192.168.1.1
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 3

Task 3.6

Tasks

- Configure an additional Loopback8 interface on R3 and assign the **8.8.8.8/32** address.
- Configure OSPF on all the routers using process-id **1**. Advertise all the networks, including loopbacks.
- Configure R3 as the DNS server and map R4's Loopback0 with the domain name **www.ine.com**.
- Verify pinging "**www.ine.com**" from Host A and Host B.

Configuration

A Cisco router can be configured as the DNS server, which can be used to map a particular address to the given domain name. To configure a router as a DNS server, we need to make it reachable from the hosts. Before configuring DNS service on R3, configure OSPF on all the routers as required by the task.

```
R1:
router ospf 1
 network 10.1.13.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
R2:
router ospf 1
 network 10.1.24.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
R3:
router ospf 1
 network 3.3.3.3 0.0.0.0 area 0
 network 8.8.8.8 0.0.0.0 area 0
 network 10.1.13.0 0.0.0.255 area 0
R4:

router ospf 1
```

```
 network 4.4.4.4 0.0.0.0 area 0
 network 10.1.24.0 0.0.0.255 area 0
```

After verifying routing and reachability, we can configure DNS service and map the domain name with the IP address as required.

```
R3:

ip dns server
!
ip host www.ine.com 4.4.4.4
```

Verification

Because we have already configured the DNS server IP address to the hosts via DHCP, we do not need to set it explicitly to resolve the domain name.

```
Host_A#ping www.ine.com
Translating "www.ine.com"...domain server (8.8.8.8) [OK]

Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 4.4.4.4
, timeout is 2 seconds:
!!!!! Success rate is 100 percent (5/5)
, round-trip min/avg/max = 1/2/4 ms
!
!Host_B#ping www.ine.com
Translating "www.ine.com"...domain server (8.8.8.8) [OK]

Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 4.4.4.4
, timeout is 2 seconds:
!!!!! Success rate is 100 percent (5/5)
, round-trip min/avg/max = 1/3/8 ms
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 3

Task 3.7

Tasks

- Configure R1 to filter Host B from reaching the DNS server IP address.
- It should check only the source IP address.
- Host A should still be able to reach the DNS server.

Configuration

An Access Control List is a packet filtering mechanism that allows a router to filter packets based on the ACL entries in sequential order. There are two types of ACL: standard and extended. We can use ACL numbers from 1 through 99 when configuring standard access lists.

Standard ACL filters packets based on the source IP address of a packet; we usually apply it nearest to the destination because it does not check for the packet destination. If applied nearest to the source, issues can arise caused by unnecessary traffic filtering, unlike Extended ACL.

R1:

```
access-list 1 deny host 192.168.1.51
access-list 1 permit any
!
interface FastEthernet0/1
ip access-group 1 out
```

Verification

To verify that the ACL entry is working correctly, ping from Host B to the destination 8.8.8.8, which is the DNS server IP address. Likewise, initiate the ping from Host A; it should be reachable because we have restricted Host B to get to 8.8.8.8.

```
Host_B#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:U.U.U
Success rate is 0 percent (0/5)
!Host_B#ping www.ine.com
Translating "www.ine.com"...domain server (8.8.8.8) (8.8.4.4)
% Unrecognized host or address, or protocol not running.
```

Because the DNS server is not reachable from Host B, a ping to www.ine.com fails, lacking name resolution. The secondary DNS 8.8.4.4 does not exist anywhere within this lab; it has been configured to test the DHCP process for the secondary DNS only.

```
Host_A#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!Host_A#ping www.ine.com
Translating "www.ine.com"...domain server (8.8.8.8) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!
!R1#show access-lists

Standard IP access list 110 deny   192.168.1.51 (12 matches
)20 permit any (12 matches
)
```

In the above output we can see that the packet matches, which indicates that 12 packets are generated from Host B and 6 packets are generated from Host A.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 3

Task 3.8

Tasks

- Configure R4 as the HTTP server.
- Authenticate HTTP using the username **cisco** and the password **ine**.
- Configure R2 to filter HTTP traffic from Host A to **4.4.4.4**.
- The rest of the devices should not be restricted by the rule.

Configuration

Extended ACL filters packets based on the source and destination IP and TCP/UDP port numbers, which provides a lot more flexibility in packet filtering. It can be applied nearest to the source and destination because it has the ability to determine where the packet is destined to. So, we can use extended ACL where we have a specific need to filter packets on the basis of destination application port numbers, like HTTP, FTP, DNS, etc. We can use ACL numbers from 100 through 199 when configuring extended access lists.

```
R4:
ip http server
ip http authentication local
!
username cisco privilege 15 password ine
R2:

access-list 101 deny tcp host 192.168.1.50 host 4.4.4.4 eq 80
access-list 101 permit ip any any
!
interface FastEthernet0/0
ip access-group 101 in
```

Verification

To check the HTTP filtering, initiate telnet from Host A and Host B to 4.4.4.4 using port 80. We can also verify the HTTP connection status on R4. Additionally, check for the ACL status to determine the packets that are matching with the deny statement.

```
Host_A#telnet 4.4.4.4 80
Trying 4.4.4.4, 80 ... % Destination unreachable; gateway or host down
!
!Host_B#telnet 4.4.4.4 80
Trying 4.4.4.4, 80 ... Open


[Connection to 4.4.4.4 closed by foreign host]
!
!R4#show ip http server connection



HTTP server current connections:
local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes
4.4.4.4:80        192.168.1.51:26133 0           0


!
!R2#show access-lists

Extended IP access list 101 10 deny tcp host 192.168.1.50 host 4.4.4.4 eq www (1 match)


20 permit ip any any (206 matches)
```

In the above output, we can see that "1" packet is being matched by the deny statement, which indicates that the HTTP from Host A is being denied by the ACL.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 3

Task 3.9

Tasks

- Configure R3 as the HTTP server.
- Authenticate HTTP using the username **cisco** and the password **ine**.
- Configure named ACL on R1 to filter HTTP traffic from Host B to **3.3.3.3**.
- The rest of the devices should not be restricted by the rule.

Configuration

In ACL, there are numbered and named configurations. Like numbered ACLs, named ACLs also have the same kind of ACL categories: standard named and extended named. The only difference between these two approaches is ease of modification in individual ACL statements. We use slightly different syntax for the named ACL than for the numbered ACL. Additionally, we can give any appropriate name according to the naming convention for any ACL instances.

```
R3:
ip http server
ip http authentication local
!
username cisco privilege 15 password ine
R1:

ip access-list extended DENY_HTTP
 deny tcp host 192.168.1.51 host 3.3.3.3 eq 80
 permit ip any any
!
interface FastEthernet0/0
ip access-group DENY_HTTP in
```

Verification

To check the HTTP filtering, initiate a telnet session from Host A and Host B to 3.3.3.3 using port 80. We can also verify the HTTP connection status on R3. Additionally, check for the ACL status to verify the packets that are matching with the deny statement.

```
Host_A#telnet 3.3.3.3 80
Trying 3.3.3.3, 80 ... Open
!
!Host_B#telnet 3.3.3.3 80
Trying 3.3.3.3, 80 ... % Destination unreachable; gateway or host down
!
!R3#show ip http server connection


HTTP server current connections:
local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes
3.3.3.3:80        192.168.1.50:20787 0           0


!
!R1#show access-lists DENY_HTTP
Extended IP access list DENY_HTTP 10 deny tcp host 192.168.1.51 host 3.3.3.3 eq www (1 match)


20 permit ip any any (153 matches)
```

In the above ACL output, we can see that "1" packet is being matched with the permit statement of the ACL DENY_HTTP.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 3

Task 3.10

Tasks

- Remove OSPF configuration from R3 and R4.
- Configure static NAT on R1 to translate Host A with the 10.1.13.50 address.
- Upon completing this task, you should be able to ping the 3.3.3.3 address.

Configuration

Network Address Translation is a mechanism of translating private IP addresses into the public IP addresses to allow inside hosts to access the Internet from the internal LAN. In reality, the global network does not know the inside hosts, which are configured with private IP addresses. So, without having address translation the users cannot access the Internet. NAT can be used to accomplish such a goal.

There are three types of NAT:

1.Static NAT

2.Dynamic NAT

3.PAT

In this task, we are asked to configure one to one mapping, static NAT, which translates a single host with the given public IP addresses. We are not using any public IP address here because the private address ranges have been used in this lab.

Initially, remove OSPF configuration from R3 and R4 and configure a static route to R3's loopback interface on R1 (because the task requires reachability from Host A to 3.3.3.3).

```
R3 & R4:
no router ospf 1
R1:
```

```
interface FastEthernet0/0
ip nat inside
!
interface FastEthernet0/1
ip nat outside
!
ip route 3.3.3.3 255.255.255.255 10.1.13.3
!
ip nat inside source static 192.168.1.50 10.1.13.50
```

Verification

To verify this task, we can initiate a ping or telnet session from Host A to 3.3.3.3. When it is initiated, we should see the translation hits on R1 when doing `show ip nat translation` .

```
Host_A#ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
!Host_A#telnet 3.3.3.3
Trying 3.3.3.3 ... Open


Password required, but none set

[Connection to 3.3.3.3 closed by foreign host]
!
!R1#show ip nat translations

Pro Inside global      Inside local       Outside local      Outside global
icmp 10.1.13.50:1      192.168.1.50:1     3.3.3.3:1          3.3.3.3:1
tcp 10.1.13.50:44369   192.168.1.50:44369 3.3.3.3:23         3.3.3.3:23

--- 10.1.13.50         192.168.1.50       ---                ---
```

Optionally, we can enable `debug ip packet` on R3 to determine which IP is coming as the source address.

```
R3#debug ip packet

IP packet debugging is on
!
```

```
!Host_A#ping 3.3.3.3 repeat 1


Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:!
Success rate is 100 percent (1/1), round-trip min/avg/max = 4/4/4 ms
!
!
R3#
Oct  9 10:11:20.736: IP: s=10.1.13.50 (FastEthernet0/1), d=3.3.3.3, len 100, input feature, MCI Check(94), rtype 0,
Oct  9 10:11:20.736: IP: tableid=0, s=10.1.13.50 (FastEthernet0/1), d=3.3.3.3 (Loopback0), routed via RIB
Oct  9 10:11:20.736: IP: s=10.1.13.50 (FastEthernet0/1), d=3.3.3.3, len 100, rcvd 4
Oct  9 10:11:20.736: IP: s=10.1.13.50 (FastEthernet0/1), d=3.3.3.3, len 100, stop process pak for forus packet

Oct  9 10:11:20.736: IP: s=3.3.3.3 (local), d=10.1.13.50 (FastEthernet0/1), len 100, sending
Oct  9 10:11:20.736: IP: s=3.3.3.3 (local), d=10.1.13.50 (FastEthernet0/1), len 100, sending full packet
R3#
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 3

Task 3.11

Tasks

- Remove static NAT configuration on R1.
- Configure dynamic NAT on R1 using a network pool of **10.1.13.11 - 10.1.13.20**.
- Both the hosts should be able to reach **3.3.3.3**.

Configuration

Dynamic NAT is configured when you have multiple hosts with private IP addresses that need to be exposed to the Internet. We basically create a pool of public IP address ranges and bind it to the private address range using ACL. Whichever host comes first picks the first address from the pool and gets translated. In this task, we have two hosts, which would just require two public IP addresses, but we have 10 addresses in this pool, which allows translation up to 10 hosts.

First, remove static NAT configuration on R1, because static NAT always takes preference over dynamic.

```
R1:

no ip nat inside source static 192.168.1.50 10.1.13.50
```

The first step is to configure standard ACL specifying Host A and Host B addresses in the source. Make sure that the interface-specific NAT configurations were already made in the previous task.

```
access-list 1 permit host 192.168.1.50
access-list 1 permit host 192.168.1.51
```

The next step is to configure the NAT pool using given addresses, which are used to translate the inside host's addresses. We can also use the "prefix-length" option

instead of the "netmask" option in the pool statement.

```
ip nat pool TEST_POOL 10.1.13.11 10.1.13.20 netmask 255.255.255.0
```

Now, bind the ACL with the pool named "TEST_POOL" that we created above.

```
ip nat inside source list 1 pool TEST_POOL
```

Verification

When verifying NAT, we always need to initiate traffic from the sources. In this task, we have two active hosts that need to be translated by the NAT using dynamic pool.

```
Host_A#ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds: .!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/4/4 ms
!
!Host_B#ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds: .!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/4/4 ms
!
!R1#show ip nat translation

Pro Inside global     Inside local       Outside local      Outside global
icmp 10.1.13.11:5     192.168.1.50:5     3.3.3.3:5          3.3.3.3:5
--- 10.1.13.11        192.168.1.50       ---                ---
icmp 10.1.13.12:0     192.168.1.51:0     3.3.3.3:0          3.3.3.3:0

--- 10.1.13.12        192.168.1.51       ---                ---
```

Additionally, we can debug NAT events and analyze which source is getting translated with which public IP address from the NAT pool. Enable `debug ip nat` on R1 and initiate ping from both the hosts.

```
R1#debug ip nat
!
!Host_A#ping 3.3.3.3

Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
!
!Host_B#ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
 Oct 10 04:08:21.680: NAT*: s=192.168.1.50->10.1.13.11, d=3.3.3.3 [26]
Oct 10 04:08:21.684: NAT*: s=3.3.3.3, d=10.1.13.11->192.168.1.50 [26]
Oct 10 04:08:21.688: NAT*: s=192.168.1.50->10.1.13.11, d=3.3.3.3 [27]
Oct 10 04:08:21.688: NAT*: s=3.3.3.3, d=10.1.13.11->192.168.1.50 [27]
Oct 10 04:08:21.692: NAT*: s=192.168.1.50->10.1.13.11, d=3.3.3.3 [28]
Oct 10 04:08:21.696: NAT*: s=3.3.3.3, d=10.1.13.11->192.168.1.50 [28]
Oct 10 04:08:21.696: NAT*: s=192.168.1.50->10.1.13.11, d=3.3.3.3 [29]
Oct 10 04:08:21.700: NAT*: s=3.3.3.3, d=10.1.13.11->192.168.1.50 [29]
Oct 10 04:08:21.700: NAT*: s=192.168.1.50->10.1.13.11, d=3.3.3.3 [30]
Oct 10 04:08:21.704: NAT*: s=3.3.3.3, d=10.1.13.11->192.168.1.50 [30]
!
!Oct 10 04:08:36.428: NAT*: s=192.168.1.51->10.1.13.12, d=3.3.3.3 [5]
Oct 10 04:08:36.432: NAT*: s=3.3.3.3, d=10.1.13.12->192.168.1.51 [5]

Oct 10 04:08:36.432: NAT*: s=192.168.1.51->10.1.13.12, d=3.3.3.3 [6]
Oct 10 04:08:36.436: NAT*: s=3.3.3.3, d=10.1.13.12->192.168.1.51 [6]
Oct 10 04:08:36.440: NAT*: s=192.168.1.51->10.1.13.12, d=3.3.3.3 [7]
Oct 10 04:08:36.440: NAT*: s=3.3.3.3, d=10.1.13.12->192.168.1.51 [7]
Oct 10 04:08:36.444: NAT*: s=192.168.1.51->10.1.13.12, d=3.3.3.3 [8]
Oct 10 04:08:36.444: NAT*: s=3.3.3.3, d=10.1.13.12->192.168.1.51 [8]
Oct 10 04:08:36.448: NAT*: s=192.168.1.51->10.1.13.12, d=3.3.3.3 [9]
Oct 10 04:08:36.452: NAT*: s=3.3.3.3, d=10.1.13.12->192.168.1.51 [9]
```

In the above debug output, we can see that Host A is being translated with 10.1.13.11 and Host B is being translated with 10.1.13.12.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 3

Task 3.12

Tasks

- Configure Port Address Translation on R1.
- Use the previously configured pool to translate internal host addresses.

Configuration

PAT stands for Port Address Translation, and it translates private addresses on the basis of port number rather than IP addresses. In PAT, a public IP can translate up to 64,000 ports. We can configure PAT using NAT Pool or tell a router to use its outside interface IP address to translate the internal addresses. In this task, we are asked to use the previously configured NAT pool, which has addresses ranging from 10.1.13.11 to 10.1.13.20. By default, PAT uses the first address until it runs out of its available port numbers. When it reaches its maximum port, it uses the next available IP address (10.1.13.12).

In this task, we are using a previously configured pool, so we simply need to add the "overload" argument at the end of NAT command.

```
R1:

ip nat inside source list 50 pool TEST_POOL overload
```

When we configure the overload keyword in the existing nat command, it provides an error message stating "**%Dynamic mapping in use, cannot change**". To avoid this, we can clear NAT using the `clear ip nat translation *` command and reapply the configuration.

Verification

Like we did in earlier tasks, initiate ping from both hosts and check for the NAT table

on R1.

```
Host_A>ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
!
!Host_B>ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
!
!R1#show ip nat translations

Pro Inside global      Inside local       Outside local      Outside global icmp 10.1.13.12:7
      192.168.1.50:7     3.3.3.3:7          3.3.3.3:7 icmp 10.1.13.12:2
      192.168.1.51:2     3.3.3.3:2          3.3.3.3:2
```

Now, both hosts are using the same outside IP address but different port numbers to get translated. Optionally, we can eliminate the concept of pool if we have only one global IP address. In this task, we configured PAT using pool because it was already configured in the previous task. If we have a single address and need to configure PAT, we can directly overload an interface instead of a pool.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 4

Task 4.1

> You must load the initial configuration files for the section, **FS Lab-4 Initial**, which can be found in CCNA Routing & Switching Topology Diagrams and Initial Configurations.

Tasks

- Configure PPP authentication as follows:
  - Configure one-way PAP authentication between R1 and R4.
  - R1 should be PAP server and R4 should be configured as PAP client.
  - Use the password **cisco** whenever required.
  - Configure two-way CHAP authentication between R1 and R2.
  - Authenticate R2 using **ccna** and the password **cisco**.
  - Upon completing this task, verify point-to-point reachability.

Configuration

By default, Cisco runs HDLC encapsulation on its serial interface, which is one of the point-to-point encapsulation types that belongs to the OSI data link layer sub layer LLC. In this task, we focus more on the PPP (Point-to-Point Protocol) authentication section, which is configured to provide a level of security on the point-to-point serial connection. We have two types of authentication in PPP:

1. PAP (Password Authentication Protocol)
2. CHAP (Challenge Handshake Authentication Protocol)

Technically, we can configure one-way or two-way authentication in both authentication types. In one-way authentication, one of the routers acts as the server and another acts as the client. In two-way authentication, both routers have both server and client roles.

In this task, we are asked to configure one-way PAP authentication between R1 and R4, and we need to configure two-way CHAP authentication between R1 and R2.

First, configure PAP authentication between R1 and R4 as required by the task.

```
R1:
username R4 password 0 cisco
!
interface Serial1/3
 encapsulation ppp
 ppp authentication pap
R4:

interface Serial1/3
 encapsulation ppp
 ppp pap sent-username R4 password cisco
```

In the above configuration, R1 has been configured with username and password for the authentication. By default, PAP client sends its hostname as the username. So, the hostname must be configured as username on the PAP server. Additionally, the `ppp authentication pap` command enforces the router to be PAP server. Now, configure CHAP authentication between R1 and R2.

```
R1:
username ccna password 0 cisco
!
interface Serial1/1
 encapsulation ppp
 ppp authentication chap
 ppp chap password 0 cisco
R2:

username R1 password 0 cisco
!
interface Serial0/1/0
 encapsulation ppp
 ppp authentication chap
 ppp chap hostname ccna
 ppp chap password 0 cisco
```

Verification

When configuring PPP authentication, the line protocol of both the routers goes into the down state, lacking complete authentication. When configured, the line protocol will come in both ends. So, we can check for the point-to-point reachability and the

server/client status by using the `show users` privilege exec command.

```
R1#ping 10.1.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
!
!R1#ping 10.1.14.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.14.4, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

Basic reachability is fine in both the directions. Now, check for the server/client relationship using the `show users` command.

```
R1#show users
Line       User           Host(s)              Idle      Location
*  0 con 0                 idle                 00:00:00

Interface    User               Mode         Idle     Peer Address
Se1/1        ccna               Sync PPP     00:00:05 10.1.12.2
Se1/3        R4                 Sync PPP     00:00:06 10.1.14.4

!
!R2#show users
Line       User       Host(s)              Idle      Location
*  0 con 0                 idle                 00:00:00

Interface    User               Mode         Idle     Peer Address
Se0/1/0      R1                 Sync PPP     00:00:01 10.1.12.1
!
!R4#show users
Line       User       Host(s)              Idle      Location
*  0 con 0                 idle                 00:00:00

Interface    User               Mode         Idle     Peer Address
Se1/3                           Sync PPP     00:00:05 10.1.14.1
```

In the above output, we can see that R1 is acting as the server and authenticating R2 and R4. Likewise, R2 is acting as the server for R1 and authenticating using username "R1." Finally, R4 is acting as only the client because we have not

configured it as a server. In other words, we have not configured R4 with the `ppp authentication pap/chap` interface-specific command. Moreover, we can also verify the entire process of PPP authentication using the `debug ppp authentication` command.

Enable debugging for the PPP authentication on R1 and shut/unshut R4s Serial1/3 interface to see the authentication process.

```
R1#debug ppp authentication
PPP authentication debugging is on
!
!
R4(config)#inter s1/3
R4(config-if)#shutR4(config-if)#no shut
!
R1#
*Oct 11 10:40:13.598: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/3, changed state to down
*Oct 11 10:40:13.598: %LINK-3-UPDOWN: Interface Serial1/3, changed state to down
*Oct 11 10:40:19.094: %LINK-3-UPDOWN: Interface Serial1/3, changed state to up
*Oct 11 10:40:19.098: Se1/3 PPP: Using default call direction
*Oct 11 10:40:19.098: Se1/3 PPP: Treating connection as a dedicated line
*Oct 11 10:40:19.098: Se1/3 PPP: Session handle[99000024] Session id[33]
*Oct 11 10:40:19.138: Se1/3 PAP: I AUTH-REQ id 1 len 13 from "R4"
*Oct 11 10:40:19.138: Se1/3 PAP: Authenticating peer R4
*Oct 11 10:40:19.138: Se1/3 PPP: Sent PAP LOGIN Request
*Oct 11 10:40:19.142: Se1/3 PPP: Received LOGIN Response PASS
*Oct 11 10:40:19.146: Se1/3 PAP: O AUTH-ACK id 1 len 5

!
*Oct 11 10:40:19.146: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/3, changed state to up
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 4

Task 4.2

Tasks

- Configure Frame Relay on R1, R3, and R4 as follows:
  - Configure R3 as the Frame Relay hub.
  - R1 and R4 should be configured as spokes. Use sub-interface on R1 and R4.
  - Disable inverse ARP on all routers.
  - Configure manual Frame Relay mapping between hub and spokes.
  - Configure IP addressing as shown in the diagram.
  - Configure Frame Relay point-to-point between R1 and R4.
  - Use DLCI information as shown in the diagram.

Configuration

Frame Relay is a multipoint WAN technology that allows service providers to offer multi-site WAN service to customers. We can configure Frame Relay either in multipoint or point to point. If we have more than two sites to connect with, multipoint configuration should be used; otherwise, a point-to-point connection will work between two sites.

In our first task, we are asked to configure multipoint Frame Relay between R3, R1, and R4, where R3 will act as the hub and R1 and R4 will be configured as spokes. This means that we will have a direct Permanent Virtual Circuit between R3-R1 and R3-R4. Additionally, we must disable inverse ARP and configure manual Frame Relay mapping to and from R3. By default, serial interfaces run Frame Relay inverse ARP, which can be disabled using the `no frame-relay inverse-arp` interface-specific command. Make sure to use sub-interfaces on R1 and R4 to provision the interface for the next task of point-to-point Frame Relay between R1 and R4. We do not need to disable inverse ARP on R1 and R4 because it is disabled in the sub-interfaces by default.

In the second task, we are asked to configure Frame Relay point-to-point between

R1 and R4. It has a different incoming and outgoing DLCI defined by the pre-configured Frame Relay switch. So, it has a different Virtual Circuit, which is point-to-point to each other, unlike in the previous task.

Now, configure multipoint Frame Relay on R1, R3, and R4.

```
R3:
interface Serial0/0/0
 ip address 10.1.134.3 255.255.255.0
 encapsulation frame-relay
 no frame-relay inverse-arp
 frame-relay map ip 10.1.134.1 131
 frame-relay map ip 10.1.134.4 341
R1:
interface Serial1/0
 encapsulation frame-relay
 no shutdown
!
interface Serial1/0.13 multipoint
 ip address 10.1.134.1 255.255.255.0
 frame-relay map ip 10.1.134.3 131
R4:

interface Serial1/0
 encapsulation frame-relay
 no shutdown
!
interface Serial1/0.43 multipoint
 ip address 10.1.134.4 255.255.255.0
 frame-relay map ip 10.1.134.3 341
```

We have configured sub-interfaces on R1 and R4 because we need to configure Frame Relay point-to-point using the same main interface. So, whenever there are different requirements to be fulfilled using the same interface, we can proceed with the sub-interface and the available configuration options for multipoint or point-to-point when creating sub-interfaces. Also, recall that we do not need to disable inverse ARP on R1 and R4 because they are using sub-interfaces.

The next step is to configure point-to-point Frame Relay between R1 and R4.

```
R1:
interface Serial1/0.14 point-to-point
 ip address 10.1.104.1 255.255.255.0
 frame-relay interface-dlci 141
R4:
```

```
interface Serial1/0.41 point-to-point
 ip address 10.1.104.4 255.255.255.0
 frame-relay interface-dlci 141
```

Verification

Before testing reachability, we should verify mapping between the configured devices. Unless there is proper mapping of IP and DLCI, the local router cannot reach the other end.

```
R3#show frame-relay map
 Serial0/0/0 (up): ip 10.1.134.1 dlci 131 (0x83,0x2030), static
,
              CISCO, status defined, active Serial0/0/0 (up): ip 10.1.134.4 dlci 341 (0x155,0x5450), static
,
              CISCO, status defined, active
!
!R1#show frame-relay map
  Serial1/0.13 (up): ip 10.1.134.3 dlci 131 (0x83,0x2030), static
,
               CISCO, status defined, active Serial1/0.14 (up): point-to-point dlci, dlci 141
(0x8D,0x20D0), broadcast
          status defined, active
!
!R4#show frame-relay map
 Serial1/0.41 (up): point-to-point dlci, dlci 141
(0x8D,0x20D0), broadcast
          status defined, active Serial1/0.43 (up): ip 10.1.134.3 dlci 341 (0x155,0x5450), static
,
               CISCO, status defined, active
```

In the above outputs, R3 has two static mappings to IPs from same subnet because they are multipoint peers. However, R1 and R4 have multipoint and point-to-point mappings that can be distinguished on the basis of destinations mapped with the DLCI. There is no destination defined in the point-to-point mapping because it has only one possible destination. But in the multipoint configuration, there can be more than one destination.

Now we should have reachability between all the routers within a single network.

```
R3#ping 10.1.134.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.134.1, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms
!R3#ping 10.1.134.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.134.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/58/60 ms
!
!R1#ping 10.1.134.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.134.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms
!R1#ping 10.1.104.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.104.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/58/60 ms
!
!R4#ping 10.1.134.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.134.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/58/60 ms
!R4#ping 10.1.104.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.104.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms
```

We have successful reachability as expected. The only problem is that R1 cannot reach 10.1.134.4 and R4 cannot reach 10.1.134.3 because there is no Frame Relay mapping. Even if we enable inverse ARP on both device interfaces, they cannot establish a virtual circuit because they do not have direct PVC configured on a Frame Relay switch. The remaining option is to configure the static mapping on R1 for R4 via multipoint link and vice versa.

First, check the reachability between R1 and R4 on multipoint Frame Relay. Then add the static Frame Relay mapping on both routers and check for reachability again.

```
R1#ping 10.1.134.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.134.4, timeout is 2 seconds:.....
```

```
Success rate is 0 percent (0/5)
!
R1(config)#interface s1/0.13R1(config-subif)#frame-relay map ip 10.1.134.4 131
!R1#show frame-relay map
Serial1/0.13 (up): ip 10.1.134.4 dlci 131(0x83,0x2030), static,
              CISCO, status defined, active
Serial1/0.13 (up): ip 10.1.134.3 dlci 131(0x83,0x2030), static,
              CISCO, status defined, active
Serial1/0.14 (up): point-to-point dlci, dlci 141(0x8D,0x20D0), broadcast
          status defined, active
!R1#ping 10.1.134.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.134.4, timeout is 2 seconds:
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 112/115/120 ms

!
!R4#ping 10.1.134.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.134.1, timeout is 2 seconds:.....
Success rate is 0 percent (0/5)
!
R4(config)#interface s1/0.43R4(config-subif)#frame-relay map ip 10.1.134.1 341
!R4#show frame-relay map

Serial1/0.41 (up): point-to-point dlci, dlci 141(0x8D,0x20D0), broadcast
          status defined, activeSerial1/0.43 (up): ip 10.1.134.1 dlci 341(0x155,0x5450), static,
              CISCO, status defined, active
Serial1/0.43 (up): ip 10.1.134.3 dlci 341(0x155,0x5450), static,
              CISCO, status defined, active
!R4#ping 10.1.134.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.134.1, timeout is 2 seconds:
!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 112/114/124 ms
```

In the above output, look at the latency between the R1 and R4 ping report. It's twice the usual latency seen on R3 when pinging to its spokes. This is because of indirect VCs that exist between R1 and R3, and R3 and R4. When ping is initiated from 10.1.134.1, it is sent to the R3 first, and then R3 will forward the packet to R4 and vice versa. If we were to ping from R1 to R4 via its point-to-point Frame Relay link, it would ping with half of the delay that is seen in the above output.

```
R1#ping 10.1.104.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.104.4, timeout is 2 seconds:
```

```
!!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 56/58/60 ms
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 4

Task 4.3

Tasks

- Configure IPv6 addressing on R1, R2, and R4 as shown in the diagram.
- Verify the point-to-point reachability after configuration is complete.

Configuration

IPv6 is the next-generation addressing protocol that was developed as a replacement for IP version 4, which had limited address space. IP version 6 has 128-bit addresses, which is a huge address range. Basically, there are two types of addressing in IPv6:

1. Link Local Addresses
2. Global Unicast Addresses

In this task, we will assign global unicast addresses as shown in the diagram. After configuration, the interface will automatically generate its link local address on the basis of its MAC address. When creating a link local address, an interface puts FFFE within the MAC address to make a 64-bit host address. Usually, a routing protocol uses the link local address as its next hop, instead of the global unicast addresses.

```
R1:

interface Serial1/1
 ipv6 address 2001:10:1:12::1/64
R2:

interface Serial0/1/0
 ipv6 address 2001:10:1:12::2/64
R4:

interface Serial1/3
ipv6 address 2001:10:1:14::4/64
```

Verification

To verify, we have some verification commands and reachability tests. Check for the interface status, as in IP version 4.

```
R1#show ipv6 interface brief | exclude FastEthernet|unassigned
Serial1/0              [up/up]
Serial1/0.13           [up/up]
Serial1/0.14           [up/up]
Serial1/1              [up/up] FE80::221:A0FF:FE7E:7E10
    2001:10:1:12::1
Serial1/2              [up/up]
Serial1/3              [up/up] FE80::221:A0FF:FE7E:7E10

    2001:10:1:14::1
Vlan1                  [up/up]
```

Because the serial is has point-to-point protocol and does not use MAC addressing, both IPv6-enabled interfaces are referring to the FastEthernet0/0 MAC address to make their link local address.

```
R1#show interfaces fa0/0 | inc bia
 Hardware is MV96340 Ethernet, address is 0021.a07e.7e10 (bia 0021.a07e.7e10)
```

In this MAC address, we have 24 OUI bits, and the remaining 24 bits are vendor code (that is, 0021.A0 and 7E.7E10). But this is quite different from the link local address. In reality, IPv6 takes the MAC address but it inverts the 7th bit of the MAC

address as shown below.

Let's convert the OUI portion of the MAC into binary.

0000 00**0**0 0010 0001 1010 0000

When inverting 7th bit, it looks like 0000 00**1**0 0010 1010 0000. As a result, the MAC is converted to 0221.A0. Finally, the link local address would look like FE80::221:A0FF:FE7E:7E10.

Now, verify the same on R2 and R4.

```
R2#show ipv6 interface brief | exclude FastEthernet|unassigned

Serial0/0/0            [up/up]
Serial0/1/0            [up/up] FE80::21A:2FFF:FE6A:A264
    2001:10:1:12::2
!R2#show interfaces fastEthernet 0/0 | inc bia
 Hardware is Gt96k FE, address is 001a.2f6a.a264 (bia 001a.2f6a.a264)
!
!R4#show ipv6 interface brief | exclude FastEthernet|unassigned

Serial1/0              [up/up]
Serial1/0.41           [up/up]
Serial1/0.43           [up/up]
Serial1/1              [administratively down/down]
Serial1/2              [up/up]
Serial1/3              [up/up] FE80::21B:54FF:FED4:E840
    2001:10:1:14::4
Vlan1                  [up/up]
!R4#show interfaces fastEthernet 0/0 | include bia
 Hardware is MV96340 Ethernet, address is 001b.54d4.e840 (bia 001b.54d4.e840)
```

As required by the task, check the reachability.

```
R1#ping 2001:10:1:14::4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:10:1:14::4, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
!R1#ping 2001:10:1:12::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:10:1:12::2, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
```

As expected, both the segments are reachable from R1.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 4

Task 4.4

Tasks

- Configure static routing on R2 and R4.
- Verify reachability between R2 and R4.

Configuration

As with IPv4, IPv6 also supports static and dynamic routing protocols. By default, IPv6 routing is disabled on most of the IOSs. So we must first enable IPv6 routing using the `ipv6 unicast-routing` global configuration command.

In this task, we are asked to configure static routing between R2 and R4. Because R1 is connected to both segments, we do not need to write static routes on it.

```
R1:
ipv6 unicast-routing
R2:
ipv6 unicast-routing
ipv6 route 2001:10:1:14::/64 2001:10:1:12::1
R4:

ipv6 unicast-routing
ipv6 route 2001:10:1:12::/64 2001:10:1:14::1
```

Verification

Before verifying reachability, we have some routing specific verification commands. Check for a couple of outputs, and then proceed to check for reachability.

```
R1#show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
```

```
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, la - LISP alt
       lr - LISP site-registrations, ld - LISP dyn-eid, a - Application
C   2001:10:1:12::/64 [0/0]
     via Serial1/1, directly connected
L   2001:10:1:12::1/128 [0/0]
     via Serial1/1, receive
C   2001:10:1:14::/64 [0/0]
     via Serial1/3, directly connected
L   2001:10:1:14::1/128 [0/0]
     via Serial1/3, receive
L   FF00::/8 [0/0]
     via Null0, receive
!
!R2#show ipv6 route
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, la - LISP alt
       lr - LISP site-registrations, ld - LISP dyn-eid, a - Application
C   2001:10:1:12::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:10:1:12::2/128 [0/0]
     via Serial0/1/0, receiveS   2001:10:1:14::/64 [1/0]
via 2001:10:1:12::1
L   FF00::/8 [0/0]
     via Null0, receive
!R2#show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "application"
IPv6 Routing Protocol is "ND"IPv6 Routing Protocol is "static
"
!
!R4#show ipv6 route
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
```

```
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, la - LISP alt
       lr - LISP site-registrations, ld - LISP dyn-eid, a - Application
S   2001:10:1:12::/64 [1/0]
     via 2001:10:1:14::1
C   2001:10:1:14::/64 [0/0]
     via Serial1/3, directly connected
L   2001:10:1:14::4/128 [0/0]
     via Serial1/3, receive
L   FF00::/8 [0/0]
     via Null0, receive
!R4#show ipv6 protocol
R4#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "application"
IPv6 Routing Protocol is "ND"IPv6 Routing Protocol is "static
"
!R4#ping 2001:10:1:12::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:10:1:12::2, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 4

Task 4.5

Tasks

- Configure additional interfaces on R2 and R4 as follows:
  - Configure IPv6 address **2001:2:2:2::2/128** on R2's Loopback0 interface.
  - Configure IPv6 address **2001:4:4:4::4/128** on R4's Loopback0 interface.
- Configure RIPng on all routers.
- Verify routes and reachability upon completing this task.

Configuration

As with IPv4, several IGPs are designed for IPv6: RIPng, EIGRPv6, and OSPFv3. There are no functional differences between RIPv2 and RIPng; the only difference is protocol stack and configuration syntax. In this task, we are asked to configure RIPng on all routers and establish reachability between the loopback interfaces of R2 and R4.

Unlike with IPv4, we do not have `network` command in IPv6. Instead of defining the network under the routing instance, we just need to apply the routing protocol under the interfaces. First, configure additional IPv6 addresses as required in the task.

```
R2:
interface Loopback0
 ipv6 address 2001:2:2:2::2/128
R4:

interface Loopback0
 ipv6 address 2001:4:4:4::4/128
```

Now enable the RIPng instance globally and apply it under the interfaces.

```
R1:
```

```
ipv6 router rip TEST
!
interface Serial1/1
 ipv6 rip TEST enable
!
interface Serial1/3
 ipv6 rip TEST enable
R2:
ipv6 router rip TEST
!
interface Serial0/1/0
 ipv6 rip TEST enable
!
interface Loopback0
 ipv6 rip TEST enable
R4:

ipv6 router rip TEST
!
interface Serial1/3
 ipv6 rip TEST enable
!
interface Loopback0
 ipv6 rip TEST enable
```

Verification

There are various methods for verifying a routing protocol configuration on Cisco IOS. The protocol status and routes can be verified, and a reachability test is also a good idea after you can see the routes in the routing table. Because we have already gone through the RIP version 2 lab in earlier sections, it should be fairly easy to understand the outputs and their attributes.

```
R1#show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "application"
IPv6 Routing Protocol is "ND"IPv6 Routing Protocol is "rip TEST"
  Interfaces:Serial1/1
Serial1/3
  Redistribution:
    None
!
!R2#show ipv6 protocols
```

```
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "application"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "static"IPv6 Routing Protocol is "rip TEST"
  Interfaces:Serial0/1/0
Loopback0
  Redistribution:
    None
!R2#show ipv6 route rip
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, la - LISP alt
       lr - LISP site-registrations, ld - LISP dyn-eid, a - Application
R   2001:4:4:4::4/128 [120/3]     viaFE80::221:A0FF:FE7E:7E10
, Serial0/1/0
!R2#ping 2001:4:4:4::4 source Loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:4:4:4::4, timeout is 2 seconds:
Packet sent with a source address of 2001:2:2:2::2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
!
!R4#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "application"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "static"IPv6 Routing Protocol is "rip TEST"
  Interfaces:Serial1/3
Loopback0
  Redistribution:
    None
!R4#show ipv6 route rip
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, la - LISP alt
       lr - LISP site-registrations, ld - LISP dyn-eid, a - Application
```

```
R   2001:2:2:2::2/128 [120/3]      via FE80::221:A0FF:FE7E:7E10
, Serial1/3
!R4#ping 2001:2:2:2::2 source Loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:2:2:2::2, timeout is 2 seconds:
Packet sent with a source address of 2001:4:4:4::4
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms
```

In the above output, both R2 and R4 are referring to the same link local address because R1 has allocated the same MAC address of FastEthernet0/0 to its serial interfaces when generating link local address. Unlike with static routing, we can see the link local address as the next hop instead of the global unicast address.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 4

Task 4.6

Tasks

- Configure EIGRPv6 in AS 1 on R1, R2, and R4.
- Advertise Loopback0 interfaces of R2 and R4 into EIGRPv6
- Verify routes and reachability upon completing this task.

Configuration

In this task, we are asked to configure EIGRP version 6 even though RIPng has already been configured for all the networks. After we configure EIGRP and advertise the loopback interfaces on R2 and R4, the administrative distance value will be compared between these two protocols. We know that EIGRPv6 has an administrative distance of 90 and RIP has an administrative distance of 120. So, EIGRPv6 will take preference over the RIPng learned routes. According to the task requirement, configure EIGRPv6 on all routers.

```
R1:
ipv6 router eigrp 1
!
interface Serial1/1
 ipv6 eigrp 1
!
interface Serial1/3
 ipv6 eigrp 1
R2:
ipv6 router eigrp 1
!
interface Serial0/1/0
 ipv6 eigrp 1
!
interface Loopback0
 ipv6 eigrp 1
R4:
```

```
ipv6 router eigrp 1
!
interface Serial1/3
 ipv6 eigrp 1
!
interface Loopback0
 ipv6 eigrp 1
```

Verification

In the above configuration, EIGRP version 6 has been enabled on the specific interfaces, including loopback interfaces where RIPng is running. Verify neighborship for EIGRP version 6 and check for routes and reachability.

```
R1#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "application"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip TEST"
  Interfaces:
    Serial1/1
    Serial1/3
  Redistribution:
    NoneIPv6 Routing Protocol is "eigrp 1"
EIGRP-IPv6 Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  NSF-aware route hold timer is 240
  Router-ID: 10.1.134.1
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 16
    Maximum hopcount 100
    Maximum metric variance 1

  Interfaces: Serial1/1
Serial1/3
  Redistribution:
    None
!R1#show ipv6 eigrp neighbor
EIGRP-IPv6 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   Link-local address:     Se1/3                    11 00:07:36   40  1182  0  4
```

```
FE80::21B:54FF:FED4:E840

0   Link-local address:     Se1/1                   12 00:08:13   32  1182  0  4
FE80::21A:2FFF:FE6A:A264
!R1#show ipv6 route eigrp
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, la - LISP alt
       lr - LISP site-registrations, ld - LISP dyn-eid, a - Application D   2001:2:2:2::2/128 [90
/20640000]
     via FE80::21A:2FFF:FE6A:A264, Serial1/1 D   2001:4:4:4::4/128 [90
/20640000]
     via FE80::21B:54FF:FED4:E840, Serial1/3
!R1#ping 2001:2:2:2::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:2:2:2::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
!R1#ping 2001:4:4:4::4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:4:4:4::4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
```

We can see that R1 has neighborship via EIGRP version 6, with R2 and R4 using their link local addresses. When checking for the routing table, the next hops are link local. Similar outputs can be seen in R2 and R4 as well. As we discussed above, EIGRPv6 has been given preference over RIPng routes. This can be verified by looking at the routing table specific to RIPng.

```
R1#show ipv6 route rip

IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
```

```
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, la - LISP alt
       lr - LISP site-registrations, ld - LISP dyn-eid, a - Application
```

No routes have been installed in the RIPng routing table. However, we can see the routes learned by RIPng in its routing database. However, it is not installed in the routing table because of the EIGRPv6 lower administrative distance value.

```
R1#show ipv6 rip database
RIP process "TEST", local RIB 2001:2:2:2::2/128, metric 2
     Serial1/1/FE80::21A:2FFF:FE6A:A264, expires in 176 secs 2001:4:4:4::4/128, metric 2

     Serial1/3/FE80::21B:54FF:FED4:E840, expires in 156 secs
 2001:10:1:12::/64, metric 2
     Serial1/1/FE80::21A:2FFF:FE6A:A264, expires in 176 secs
 2001:10:1:14::/64, metric 2
     Serial1/3/FE80::21B:54FF:FED4:E840, expires in 156 secs
```

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 4

Task 4.7

Tasks

- Configure additional loopback interfaces as follows:
  - On R2, configure Loopback1 using IPv6 address **2001:22:22:22::22/128**.
  - On R4, configure Loopback1 using IPv6 address **2001:44:44:44::44/128**.
- Configure OSPFv3 on R1, R2, and R4, and advertise Loopback1 interfaces of R2 and R4 in area 0.
- When configuration is complete, verify end-to-end reachability.

Configuration

As in earlier tasks, we are asked to configure OSPFv3 on all IPv6 routers. Unlike the EIGRPv6 task, we will not have dependency with other protocols when configuring OSPFv3 on these routers. R2 and R4 have different loopback interfaces that are specifically configured for OSPF version 3 route advertisement. When configuring OSPFv3, it will use an IPv4 style router-id, but if there are no IPv4 addresses on local routers, it cannot pick the router-id lacking IPv4 addresses. In this task, we can configure the router-id manually.

```
R1:
ipv6 router ospf 1
 router-id 1.1.1.1
!
interface Serial1/1
 ipv6 ospf 1 area 0
!
interface Serial1/3
 ipv6 ospf 1 area 0
R2:
ipv6 router ospf 1
 router-id 2.2.2.2
!
```

```
interface Serial0/1/0
 ipv6 ospf 1 area 0
!
interface Loopback1
 ipv6 ospf 1 area 0
R4:

ipv6 router ospf 1
 router-id 4.4.4.4
!
interface Serial1/3
 ipv6 ospf 1 area 0
!
interface Loopback1
 ipv6 ospf 1 area 0
```

Verification

Likewise, we can verify OSPFv3 neighborship and then the routing table before verifying end-to-end reachability.

```
R1#show ipv6 ospf neighbor


        OSPFv3 Router with ID (1.1.1.1) (Process ID 1)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
4.4.4.4           0   FULL/  -        00:00:36    13              Serial1/3
2.2.2.2           0   FULL/  -        00:00:35    5               Serial1/1
!    R1#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "application"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip TEST"
  Interfaces:
    Serial1/1
    Serial1/3
  Redistribution:
    None
IPv6 Routing Protocol is "eigrp 1"
EIGRP-IPv6 Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  NSF-aware route hold timer is 240
  Router-ID: 10.1.134.1
```

```
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 16
    Maximum hopcount 100
    Maximum metric variance 1

  Interfaces:
    Serial1/1
    Serial1/3
  Redistribution:
    None IPv6 Routing Protocol is "ospf 1"
  Router ID 1.1.1.1
  Number of areas: 1 normal, 0 stub, 0 nssa
  Interfaces (Area 0): Serial1/3
Serial1/1
  Redistribution:
    None
!R1# show ipv6 route ospf
IPv6 Routing Table - default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, la - LISP alt
       lr - LISP site-registrations, ld - LISP dyn-eid, a - Application
O   2001:22:22:22::22/128 [110/781]
     via FE80::21A:2FFF:FE6A:A264, Serial1/1O   2001:44:44:44::44/128 [110/781]
     via FE80::21B:54FF:FED4:E840, Serial1/3
!R1#ping  2001:22:22:22::22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:22:22:22::22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
!R1#ping  2001:44:44:44::44

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:44:44:44::44, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

As expected, both IPv6 prefixes are being learned by R1, and there is also end-to-

end reachability.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 5

Task 5.1

> You must load the initial configuration files for the section, **FS Lab-5 Initial**, which can be found in CCNA Routing & Switching Topology Diagrams and Initial Configurations.

Tasks

- Enable TFTP service on the TFTP server.
- Copy the filename **TEST** from the TFTP server to the flash memory of R1.
- Verify the contents of the filename **TEST**.

Configuration

In this task, we need to configure Sw2 as a TFTP server so that we can back up and restore the configuration and IOS images of R1. Because of the lack of flash memory space, we cannot perform an IOS backup test because the router has a huge file size; but we will test how the configuration or IOS images can be restored to the local flash memory. Instead of the IOS image, we will use the filename "TEST" for the necessary test.

First, configure Sw2 as a TFTP server and locate the file named "TEST" in its flash memory.

```
TFTP-SERVER
:


tftp-server flash:TEST.text
```

Now copy the file TEST from the TFTP server to the flash memory of R1.

```
R1#copy tftp: flash:
Address or name of remote host []? 192.168.1.10Source filename []?TEST.text
```

```
Destination filename [TEST.text]?
Accessing tftp://192.168.1.10/TEST.text...Loading TEST.text from 192.168.1.10 (via FastEthernet0/0): !
[OK - 2427 bytes]
2427 bytes copied in 0.364 secs (6668 bytes/sec)
```

Verification

To verify the contents in the file named TEST, we use the `more` command, which displays the contents as required by the task. For testing purpose, the TEST file has been created with the entire configuration of the TFTP server, which is Sw2 in our case.

```
R1#more flash:TEST.text

!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname TFTP-SERVER
!
!
no aaa new-model
ip subnet-zero
no ip domain-lookup
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
```

```
!
!
interface FastEthernet0/1
 switchport mode dynamic desirable
!
interface FastEthernet0/2
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/3
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/4
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/5
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/6
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/7
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/8
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/9
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/10
 switchport mode dynamic desirable
!
interface FastEthernet0/11
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/12
 switchport mode dynamic desirable
```

```
 shutdown
!
interface FastEthernet0/13
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/14
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/15
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/16
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/17
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/18
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/19
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/20
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/21
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/22
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/23
 switchport mode dynamic desirable
 shutdown
!
```

```
interface FastEthernet0/24
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/1
 switchport mode dynamic desirable
!
interface GigabitEthernet0/2
 switchport mode dynamic desirable
!
interface Vlan1
 ip address 192.168.1.10 255.255.255.0
!
ip classless
ip http server
ip http secure-server
!
!
!
control-plane
!
!
line con 0
line vty 5 15
!
end
```

Likewise, we can upload the TEST file from the local flash memory to the TFTP server, but we have configured a switch as a TFTP server and it may not support full features as real TFTPs do. So, the entire process remains the same. The only difference here would be command syntax. You can use `copy flash:TEST.text tftp:` instead of the above command to back up the TEST file on the TFTP server.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 5

Task 5.3

Tasks

- Load the IOS on the flash memory from both the native IOS and ROM monitor mode.

Configuration

We can load the IOS image on the flash memory when it is necessary to upgrade the existing IOS with a newer version, or if the IOS crashed unexpectedly. When upgrading the IOS image, it is very easy to pull the IOS from the TFTP server; but if the IOS has already crashed and there is no way to get to the IOS CLI, we have ROMMON mode, also called the Mini IOS of the Cisco router. It helps us execute some basic commands and pull the IOS image from the TFTP server. At first, configure R1 to load the IOS image from its TFTP server. In our case, there is no actual IOS image. Instead, we have the IOS.bin file as an IOS image.

```
R1#copy tftp: flash:
Address or name of remote host [192.168.1.10]? Source filename [IOS.bin]?

Destination filename [IOS.bin]?
Accessing tftp://192.168.1.10/IOS.bin...Loading IOS.bin from 192.168.1.10 (via FastEthernet0/0): !

[OK - 2511 bytes]

2511 bytes copied in 0.496 secs (5063 bytes/sec)

R1#
```

Another option for installing the IOS image on the flash memory is to use ROM monitor commands and pull the IOS from the TFTP server. Like we did earlier, reload the router and press Ctrl+Break" to get into ROM monitor mode. When the router gets into the ROMMON mode, we can use the commands as follows.

```
ROMMON1>IP_ADDRESS=192.168.1.1
ROMMON2>IP_SUBNET_MASK=255.255.255.0
ROMMON3>DEFAULT_GATEWAY=192.168.1.10
ROMMON4>TFTP_SERVER=192.168.1.10
ROMMON5>TFTP_FILE=IOS.bin
ROMMON6>tftpdnld
```

Upon completing these steps, the router can get the IOS image from the TFTP server.

CCNA Routing & Switching Lab Workbook - Full-Scale Lab 5

Task 5.2

Tasks

- Assume that you have forgotten the console password of R1, and recover it without erasing the entire configuration on R1.

Configuration

We can recover the console password on Cisco routers, bypassing the startup configuration, because all the configuration-related items are stored in the startup-config file inside the NVRAM. To recover the password, we should bypass the NVRAM temporarily, which we can do by changing the configuration-register value in ROM monitor mode. After it is bypassed it will load the running-config, and we can see it as if it were a blank router just purchased from Cisco. After entering into the CLI of the router, we can copy the startup-config into the running-config, which is the primary/temporary memory of the router. After it is copied, we can change the password to avoid lockout during next reload. Additionally, we should configure the config-register value back to its default state.

By default, the config-register value is 0X2102, which tells a router to load NVRAM contents on the RAM. If the configuration register value is configured as 0X2142, the NVRAM content is bypassed and you will not be asked for authentication credentials.

First, reload the router and press Ctrl+Break within 60 seconds, which enforces the router to get into ROM monitor mode, also called ROMMON mode.

```
ROMMON1>confreg 0x2142
ROMMON2>reset
```

After the router is rebooted, it will bypass the NVRAM contents and we can copy the startup-config into the running-config and change the password.

```
Router>enable
Router#copy startup-config running-config
Destination filename [running-config]? 1541 bytes copied in 0.484 secs (3184 bytes/sec)
R1#
```

Now the startup-config has been copied into the running-config, which also copies the forgotten password. So the next step is to change the password and configuration-register value back to the default state.

```
R1:

line console 0
password cisco
!
config-register 0X2102
!
wr
```

Now we can reload the router and use the newly set password.

CCNA Routing & Switching Lab Workbook - CCNA Routing & Switching Lab Resources

CCNA Routing & Switching Topology Diagrams and Initial Configurations

Welcome!

Thank you for using this workbook as part of your preparations for pursuing your CCNA certification. The sections and tasks within this workbook are designed to give you hands-on experience with the majority of topics covered in the CCNA Routing & Switching exams.

Diagrams and Configurations

All diagrams and configurations are available to download by clicking the **Resources** button in the upper-right corner of this page. Individual lab diagrams are also included with the first task of each lab.

Feedback

Please let us know how we're doing! In the upper-right corner of your screen, you will see a **Feedback** link. If you found any errors in this workbook or have any suggestions for improvement, we'd like to know. Also, if you enjoyed this workbook, we'd like to know that as well.

CCNP SWITCH Workbook - CCNP Switch Workbook Introduction

CCNA/CCNP Rack Rental Guide

Click here to access the CCNA/CCNP Rack Rental Guide.