101 CCNA Labs

with solutions

LAYOUT BY JOE MENDOLA

Local Area Networks

Wide Area Networks

IP Routing

Access Control Lists

Network Address Translation

Dynamic Host Configuration Protocol

IP and IOS Features

Cisco Router and Security Device Manager

Challenge Labs

Lab 1: Configuring standard VLANs on Catalyst Switches

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure standard VLANs 1-1001 on Cisco Catalyst IOS switches. In addition to this, you are also required to familiarize yourself with the commands available in Cisco IOS to validate and check your configurations.

Lab Purpose:

VLAN configuration is a fundamental skill. VLANs allow you to segment your network into multiple, smaller broadcast domains. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure VLANs on Cisco switches.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

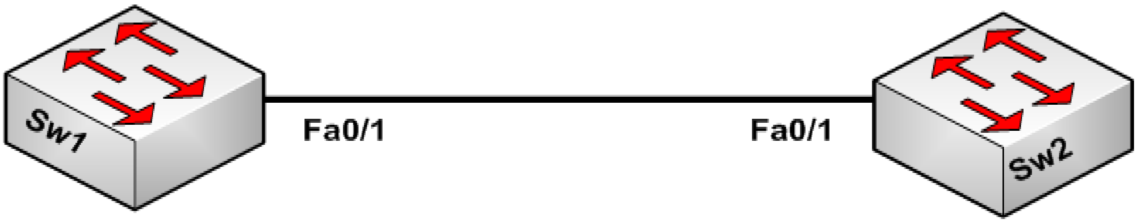
This lab has a difficulty rating of 4/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



VLAN Number	VLAN Name	Port
10	SALES	FastEthernet0/5
20	MANAGERS	FastEthernet0/6
30	ENGINEERS	FastEthernet0/7
40	SUPPORT	FastEthernet0/8

Task 1:

In preparation for VLAN configuration, configure a hostname on Sw1 as well as the VLANs depicted in the topology.

Task 2:

Configure ports FastEthernet0/5 – FastEthernet0/8 as access ports and assign them to the VLANs specified.

Task 3:

Verify your VLAN configuration using relevant show commands in Cisco IOS.

SOLUTION:

Lab 1 Configuration and Verification

Task 1:

```
Switch#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Switch(config)#hostname Sw1

Sw1(config)#vlan 10

Sw1(config-vlan)#name SALES

Sw1(config-vlan)#exit

Sw1(config)#vlan 20

Sw1(config-vlan)#name MANAGERS

Sw1(config-vlan)#exit

Sw1(config)#vlan 30

Sw1(config-vlan)#name ENGINEERS

Sw1(config-vlan)#exit

Sw1(config)#vlan 40

Sw1(config-vlan)#name SUPPORT
```

NOTE: By default, Cisco switches are VTP servers so no configuration is necessary for Server mode. Use the show vtp status command to look at the current VTP operating mode of the switch.

Task 2:

```
Sw1(config)#interface fastethernet0/5

Sw1(config-if)#switchport mode access
```

```
Sw1(config-if)#switchport access vlan 10

Sw1(config-if)#exit

Sw1(config)#interface fastethernet0/6

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 20

Sw1(config-if)#exit

Sw1(config-if)#interface fastethernet0/7

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 30

Sw1(config-if)#exit

Sw1(config-if)#interface fastethernet0/8

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 40
```

Task 3:

```
Sw1#show vlan brief

VLAN Name                             Status    Ports

---- -------------------------------- --------- -------------------------------

1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4

                                      Fa0/9,    Fa0/10, Fa0/11, Fa0/12

                                      Fa0/13,   Fa0/14, Fa0/15, Fa0/16

                                      Fa0/17,   Fa0/18, Fa0/19, Fa0/20

                                      Fa0/21,   Fa0/22, Fa0/23, Fa0/24

                                      Gi0/1,    Gi0/2

10   SALES                            active    Fa0/5

20   MANAGERS                         active    Fa0/6

30   ENGINEERS                        active    Fa0/7

40   SUPPORT                          active    Fa0/8
```

```
1002 fddi-default                    active

1003 token-ring-default              active

1004 fddinet-default                 active

1005 trnet-default                   active
```

Lab 2: Configuring extended VLANs on Catalyst Switches

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure extended VLANs 1006-4096 on Cisco Catalyst IOS switches. In addition to this, you are also required to familiarize yourself with the commands available in Cisco IOS to validate and check your configurations.

Lab Purpose:

VLAN configuration is a fundamental skill. VLANs allow you to segment your network into multiple, smaller broadcast domains. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure VLANs on Cisco switches.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

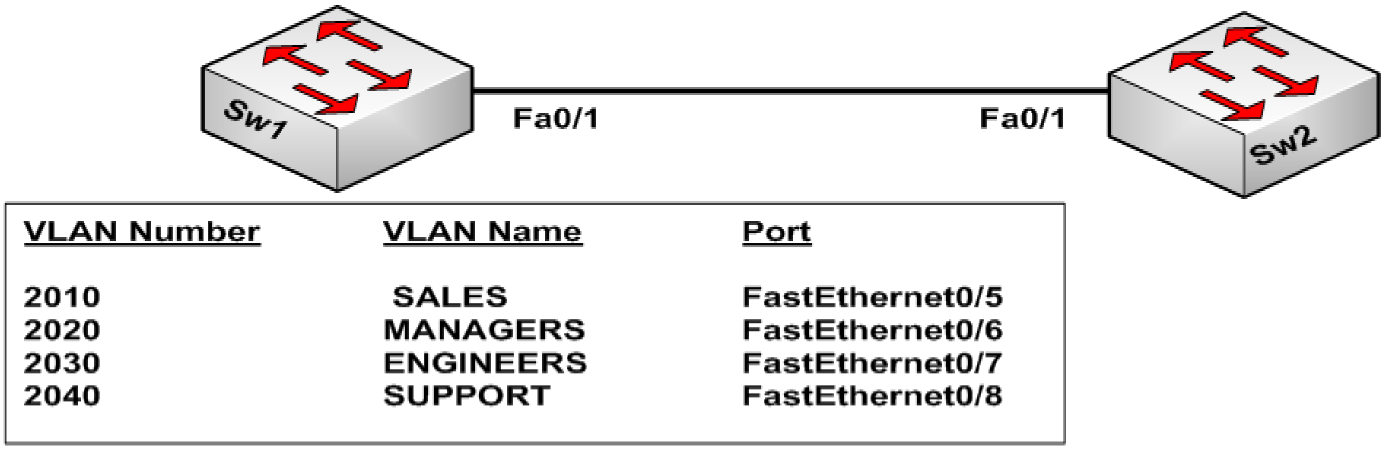
This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



VLAN Number	VLAN Name	Port
2010	SALES	FastEthernet0/5
2020	MANAGERS	FastEthernet0/6
2030	ENGINEERS	FastEthernet0/7
2040	SUPPORT	FastEthernet0/8

Task 1:

In preparation for VLAN configuration, configure a hostname on Sw1 as well as the VLANs depicted in the topology. Keep in mind that extended VLANs can only be configured on a switch in VTP Transparent mode.

Task 2:

Configure ports FastEthernet0/5 – FastEthernet0/8 as access ports and assign them to the VLANs specified.

Task 3:

Verify your VLAN configuration

SOLUTION:

Lab 2 Configuration and Verification

Task 1:

NOTE: By default, Cisco switches are VTP servers. Only standard range VLANS 1-1005 are configurable on VTP servers. To configure extended range VLANS (1006-4096) you must configure the switch as a VTP Transparent switch. Otherwise, you will get the following error message:

```
Sw1(config)#vlan 2010
Sw1(config-vlan)#end
Extended VLANs not allowed in VTP SERVER mode
Failed to commit extended VLAN(s) changes.
```

NOTE: Configuration files will be kept from previous labs. In order to remove them you can re-type the commands with the word 'no' in front.:

```
Sw1(config)#no vlan 2010
```

You may also need to reset the switch back to VTP mode server if appropriate.

```
Switch#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Switch(config)#hostname Sw1

Sw1(config)#vtp mode transparent

Setting device to VTP TRANSPARENT mode.

Sw1(config)#vlan 2010

Sw1(config-vlan)#name SALES

Sw1(config-vlan)#exit

Sw1(config)#vlan 2020
```

```
Sw1(config-vlan)#name MANAGERS

Sw1(config-vlan)#exit

Sw1(config)#vlan 2030

Sw1(config-vlan)#name ENGINEERS

Sw1(config-vlan)#exit

Sw1(config)#vlan 2040

Sw1(config-vlan)#name SUPPORT
```

Task 2:

```
Sw1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#interface fastethernet0/5

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 2010

Sw1(config-if)#exit

Sw1(config)#interface fastethernet0/6

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 2020

Sw1(config-if)#exit

Sw1(config-if)#interface fastethernet0/7

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 2030

Sw1(config-if)#exit

Sw1(config-if)#interface fastethernet0/8

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 2040
```

Task 3:

Sw1#**show vlan brief**

```
VLAN              Name                          Status    Ports
----              ----------------------------- --------- ----------------------------
1                 default                       active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                          Fa0/9,Fa0/10, Fa0/11, Fa0/12
                                                          Fa0/13, Fa0/14, Fa0/15,
                                                          Fa0/16
                                                          Fa0/17, Fa0/18, Fa0/19,
                                                          Fa0/20
                                                          Fa0/21, Fa0/22, Fa0/23,
                                                          Fa0/24
                                                          Gi0/1, Gi0/2
1002 fddi-default                               active
1003 token-ring-
default                                         active
1004 fddinet-default                            active
1005 trnet-default                              active
2010              SALES                         active    Fa0/5
2020              MANAGERS                      active    Fa0/6
2030              ENGINEERS                     active    Fa0/7
2040              SUPPORT                       active    Fa0/8
```

Lab 3: Configuring VTP Clients and Servers on Catalyst Switches

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure VTP Server and Client mode on Cisco Catalyst switches. By default, all Cisco switches are VTP Server devices.

Lab Purpose:

VTP Client and Server mode configuration is a fundamental skill. VLANs are configured on VTP Servers and VTP Clients receive VLAN information from the VTP Servers in the same VTP domain. VLAN sharing is possible by using a trunk between the switches. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure VTP Client and Server mode.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

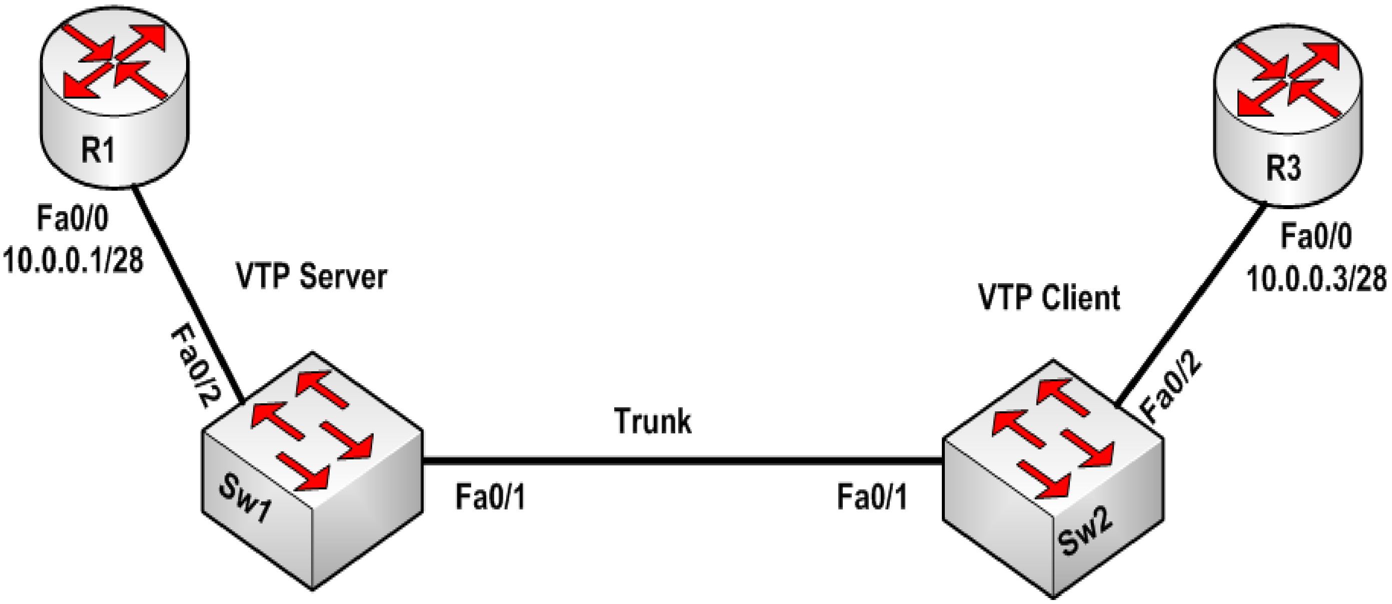
This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



VLAN Number	VLAN Name	Sw 1 & Sw 2 Interface
10	SALES	FastEthernet0/2
20	MANAGERS	

Task 1:

In preparation for VLAN configuration, configure a hostname on Sw1 as well as the VLANs depicted in the topology. Keep in mind that the default mode of operation of Cisco Catalyst switches is VTP Server mode.

Task 2:

Configure and verify Sw1 as a VTP Server switch and configure Sw2 as a VTP Client switch. Both switches should be in the VTP domain named CISCO.

Task 3:

Configure and verify FastEthernet0/1 between Sw1 and Sw2 as an 802.1q trunk

Task 4:

Configure and verify VLANs 10 and 20 on Sw1 with the names provided above. Assign FastEthernet0/2 on both Sw1 and Sw2 to VLAN 10. This interface should be configured as an access port.

Task 5:

Configure R1 and R3 FastEthernet0/0 interfaces with the IP addresses 10.0.0.1/28 and 10.0.0.3/28 respectively. Test connectivity via your VLANs by pinging R1 from R3 and vice versa.

SOLUTION:

Lab 3 Configuration and Verification

Task 1:

```
Switch#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Switch(config)#hostname Sw1

Sw1(config)#

Switch#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Switch(config)#hostname Sw2

Sw1(config)#

Router#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R1

R1(config)#

Router#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R3

R3(config)#
```

Task 2:

NOTE: By default, Cisco switches are VTP servers so no configuration is necessary for Server mode on Sw1. This can be verified using the show vtp status command. However, we do need to configure the domain.

```
Sw1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#vtp domain CISCO

Changing VTP domain name from Null to CISCO

Sw1(config)#
```

```
Sw2#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw2(config)#vtp mode client

Setting device to VTP CLIENT mode.

Sw2(config)#vtp domain CISCO

Changing VTP domain name from Null to CISCO

Sw2(config)#end

Sw1#show vtp status

VTP Version                     : 2
Configuration Revision          : 7
Maximum VLANs supported locally : 250
Number of existing VLANs        : 7
VTP Operating Mode              : Client
VTP Domain Name                 : CISCO
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x9D 0x1A 0x9D 0x16 0x9E 0xD1 0x38 0x59

Configuration last modified by 10.1.1.3 at 3-1-93 01:42:39
```

Task 3:

NOTE: By default Cisco switches default to 802.1q trunking so no explicit configuration is required.

```
Sw1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#interface fastethernet0/1

Sw1(config-if)#switchport mode trunk

Sw1#show interfaces trunk

Port      Mode        Encapsulation  Status      Native vlan

Fa0/1      on         802.1q       trunking     1

Port      Vlans allowed on trunk

Fa0/1      1-4094

Port      Vlans allowed and active in management domain
```

```
Fa0/1       1,10,20

Port        Vlans in spanning tree forwarding state and not pruned

Fa0/1       1,20

Sw2#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw2(config)#interface fastethernet0/1

Sw2(config-if)#switchport mode trunk

Sw2#show interfaces trunk

Port        Mode        Encapsulation  Status        Native vlan

Fa0/1       on          802.1q         trunking      1

Port        Vlans allowed on trunk

Fa0/1       1-4094

Port        Vlans allowed and active in management domain

Fa0/1       1,10,20

Port        Vlans in spanning tree forwarding state and not pruned

Fa0/1       1,20
```

Task 4:

```
Sw1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#vlan 10

Sw1(config-vlan)#name SALES

Sw1(config-vlan)#exit

Sw1(config)#vlan 20

Sw1(config-vlan)#name MANAGERS

Sw1(config-vlan)#exit

Sw1(config)#interface fastethernet0/2

Sw1(config-if)#switchport mode access
```

```
Sw1(config-if)#switchport access vlan 10

Sw1(config-if)#end

Sw1#

Sw1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
10   SALES                            active    Fa0/2
20   MANAGERS                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

Sw2#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw2(config)#interface fastethernet0/2

Sw2(config-if)#switchport mode access

Sw2(config-if)#switchport access vlan 10

Sw2(config-if)#end

Sw2#

Sw2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
10   SALES                            active    Fa0/2
20   MANAGERS                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Task 5:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#interface  fastethernet0/0

R1(config-if)#ip address 10.0.0.1 255.255.255.240

R1(config-if)#no shutdown

R1(config-if)#end

R1#

R3#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#interface  fastethernet0/0

R3(config-if)#ip address 10.0.0.3 255.255.255.240

R3(config-if)#no shutdown

R3(config-if)#end

R3#

R1#show ip interface brief

Interface              IP-Address      OK? Method Status            Protocol

FastEthernet0/0           10.0.0.1       YES manual up                 up

R1#ping 10.0.0.3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms
```

NOTE: The first PING packet times out due to ARP resolution. Subsequent packets will be successful.

```
R3#show ip interface brief

Interface              IP-Address      OK? Method Status            Protocol

FastEthernet0/0           10.0.0.3       YES manual up                 up
```

```
R3#ping 10.0.0.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

Lab 4: Configuring VTP Transparent Mode

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure VTP Transparent mode on Cisco Catalyst switches. By default, all Cisco switches are VTP Server devices.

Lab Purpose:

VTP Transparent mode configuration is a fundamental skill. VLANs configured on a switch in VTP Transparent mode are not automatically propagated to other switches within the same VTP domain as would be done by a VTP Server. Switches configured in VTP Transparent mode use a trunk to forward traffic for configured VLANs to other switches. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure VTP Transparent mode.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

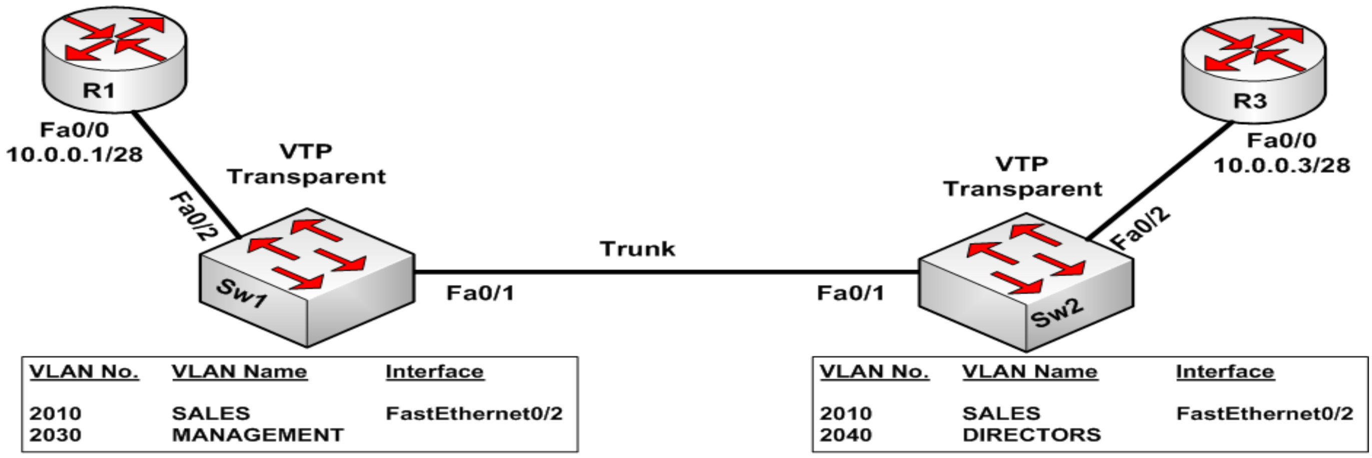
This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



VLAN No.	VLAN Name	Interface
2010	SALES	FastEthernet0/2
2030	MANAGEMENT	

VLAN No.	VLAN Name	Interface
2010	SALES	FastEthernet0/2
2040	DIRECTORS	

Task 1:

In preparation for VLAN configuration, configure a hostname on switches 1 and 2 and routers 1 and 3 as illustrated in the topology.

Task 2:

Configure and verify Sw1 and Sw2 in VTP Transparent mode. Both switches should be in the VTP domain named CISCO. Remember that switches must be in the same VTP domain to share VLAN information via a trunk.

Task 3:

Configure and verify FastEthernet0/1 between Sw1 and Sw2 as an 802.1q trunk.

Task 4:

Configure and verify VLANs 2010 and 2030 on Sw1 with the names provided above. Assign FastEthernet0/2 on Sw1 to VLAN 2010 as an access port. Configure and verify VLANs 2010 and 2040 on Sw2 with the names provided above. Assign FastEthernet0/2 on Sw2 to VLAN 2010 as an access port.

Task 5:

Configure R1 and R3 FastEthernet interfaces with the IP addresses 10.0.0.1/28 and 10.0.0.3/28 respectively. Test VLAN connectivity by pinging between R1 and R3.

SOLUTION:

Lab 4 Configuration and Verification

Task 1:

```
Switch#config t

Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Switch(config)#hostname Sw1

Sw1(config)#

Switch#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Switch(config)#hostname Sw2

Sw1(config)#

Router#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R1

R1(config)#

Router#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R3

R3(config)#
```

Task 2:

```
Sw1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#vtp mode transparent

Setting device to VTP TRANSPARENT mode.

Sw1(config)#end

Sw1#show vtp status

VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 250
Number of existing VLANs        : 5
VTP Operating Mode              : Transparent
VTP Domain Name                 : CISCO
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x9D 0x1A 0x9D 0x16 0x9E 0xD1 0x38 0x59

Configuration last modified by 10.1.1.3 at 3-1-93 01:42:39
```

```
Sw2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw2(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Sw2(config)#end
Sw2#show vtp status
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 250
Number of existing VLANs        : 5
VTP Operating Mode              : Transparent
VTP Domain Name                 : CISCO
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x9D 0x1A 0x9D 0x16 0x9E 0xD1 0x38 0x59
Configuration last modified by 10.1.1.3 at 3-1-93 01:42:45
```

Task 3:

NOTE: By default Cisco switches default to 802.1q trunking so no explicit configuration is required.

```
Sw1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#interface fastethernet0/1
Sw1(config-if)#switchport mode trunk
Sw2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw2(config)#interface fastethernet0/1
Sw2(config-if)#switchport mode trunk
```

Task 4:

```
Sw1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#vlan 2010

Sw1(config-vlan)#name SALES

Sw1(config-vlan)#exit

Sw1(config)#vlan 2030

Sw1(config-vlan)#name MANAGEMENT

Sw1(config-vlan)#exit

Sw1(config)#interface fastethernet0/2

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 2010

Sw1(config-if)#end

Sw1#

Sw1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
2010 SALES                            active    Fa0/2
2030 MANAGEMENT                       active

Sw2#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw2(config)#vlan 2010

Sw2(config-vlan)#name SALES

Sw2(config-vlan)#exit
```

```
Sw2(config)#vlan 2040

Sw2(config-vlan)#name DIRECTORS

Sw2(config-vlan)#exit

Sw2(config)#interface fastethernet0/2

Sw2(config-if)#switchport mode access

Sw2(config-if)#switchport access vlan 2010

Sw2(config-if)#end

Sw2#
```

```
Sw2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
2010 SALES                            active    Fa0/2
2040 DIRECTORS                        active
```

NOTE: By default switches configured for VTP Transparent mode do not exchange VLAN information. You can see in the above output that VLAN 2030 on Sw1 is not propagated to Sw2, and VLAN 2040 on Sw2 is not propagated to Sw1. In Transparent mode, all VLANs must be manually configured on all switches.

Task 5:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#interface  fastethernet0/0

R1(config-if)#ip address 10.0.0.1 255.255.255.240

R1(config-if)#no shutdown

R1(config-if)#end

R3#config t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#interface  fastethernet0/0

R3(config-if)#ip address 10.0.0.3 255.255.255.240

R3(config-if)#no shutdown

R3(config-if)#end

R1#show ip interface brief

Interface              IP-Address      OK? Method Status              Protocol

FastEthernet0/0            10.0.0.1       YES manual up                  up

R1#ping 10.0.0.3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms
```

NOTE: The first PING packet times out due to ARP resolution. Subsequent packets will be successful.

```
R3#show ip interface brief

Interface              IP-Address      OK? Method Status              Protocol

FastEthernet0/0            10.0.0.3       YES manual up                  up

R3#ping 10.0.0.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

Lab 5: Securing VTP Domains

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to secure VTP domains using Cisco Catalyst switches. By default, VTP domains are not password-protected.

Lab Purpose:

Securing the VTP domain is a fundamental skill. When VTP domains are not configured with a password, rogue switches can be added to the network and disrupt service. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure VTP passwords.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

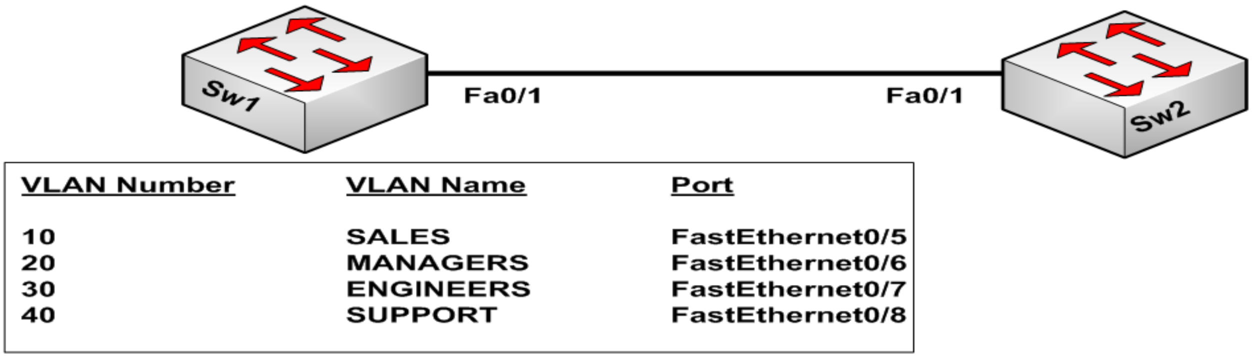
This lab has a difficulty rating of 4/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 5 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



VLAN Number	VLAN Name	Port
10	SALES	FastEthernet0/5
20	MANAGERS	FastEthernet0/6
30	ENGINEERS	FastEthernet0/7
40	SUPPORT	FastEthernet0/8

Task 1:

In preparation for VLAN configuration, configure a hostname on Sw1 and as depicted in the topology.

Task 2:

Configure and verify Sw1 as a VTP Server switch and configure Sw2 as a VTP Client switch. Both switches should be in the VTP domain named CISCO. Secure VTP messages with the VTP password CISCO.

Task 3:

Configure and verify FastEthernet0/1 between Sw1 and Sw2 as an 802.1q trunk.

Task 4:

Configure and verify VLANs 10 and 20 on Sw1 with the names provided above. Validate that these VLANs are still propagated to Sw2 after VTP has been secured.

SOLUTION:

Lab 5 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 3 Configuration and Verification Task 1

Task 2:

NOTE: By default, Cisco switches are VTP servers so no configuration is necessary for Server mode on Sw1. This can be verified using the show vtp status command. However, we do need to configure the domain.

```
Sw1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#vtp domain CISCO

Changing VTP domain name from Null to CISCO

Sw1(config)#vtp password CISCO

Setting device VLAN database password to CISCO

Sw1#show vtp status

VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 250
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : CISCO
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x00 0x7A 0x5E 0x47 0xF1 0xDD 0xB5 0x30

Sw2#config t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.

Sw2(config)#vtp mode client

Setting device to VTP CLIENT mode.

Sw2(config)#vtp domain CISCO

Changing VTP domain name from Null to CISCO

Sw1(config)#vtp password CISCO

Setting device VLAN database password to CISCO

Sw2(config)#end

Sw2#show vtp status

VTP Version                      : 2
Configuration Revision           : 0
Maximum VLANs supported locally  : 250
Number of existing VLANs         : 5
VTP Operating Mode               : Client
VTP Domain Name                  : CISCO
VTP Pruning Mode                 : Enabled
VTP V2 Mode                      : Disabled
VTP Traps Generation             : Disabled
MD5 digest                       : 0x9D 0x1A 0x9D 0x16 0x9E 0xD1 0x38 0x59
```

Task 3:

For reference information on configuring and verifying trunks, please refer to:

Lab 3 Configuration and Verification Task 3

Lab 3 Configuration and Verification Task 3

Task 4:

For reference information on configuring verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

NOTE: Make sure that the MD5 digest at the end of the output of the show vtp status command is the same when VTP passwords have been configured on switches within the same VTP domain.

Lab 6: Verifying Spanning-Tree Port States on Catalyst Switches

Lab Objective:

The objective of this lab exercise is to verify the different Spanning Tree port states, i.e. Listening, Learning, etc, and understand the IOS commands that can be used to determine the state of a port at any given time.

Lab Purpose:

Understanding the different Spanning-Tree protocol port states is a fundamental skill. In Spanning-Tree operation, ports transition from a Blocked state -> Listening state -> Learning state -> Forwarding state. A switched network is said to be converged when all ports are in the Forwarding or Blocking state. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know the different Spanning-Tree port states.

Certification Level:

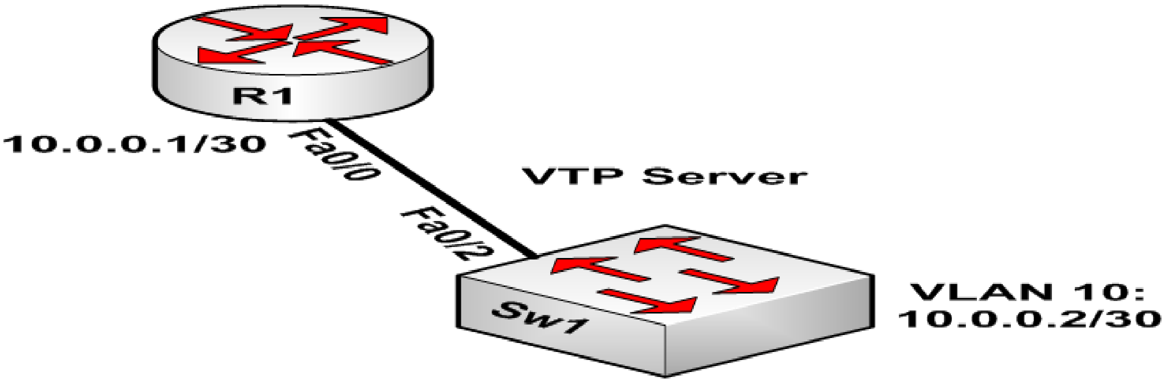
This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes



VLAN No.	VLAN Name	Interface
10	SALES	FastEthernet0/2

Task 1:

In preparation for VLAN configuration, configure a hostname on Sw1 and R1 as illustrated in the topology.

Task 2:

Configure and verify Sw1 as a VTP Server switch in a VTP domain named CISCO. The VTP domain should have a password of CISCO.

Task 3:

Configure VLAN 10 on Sw1 as illustrated in the topology. Configure FastEthernet0/2 on Sw1 as an access port in VLAN 10 and bring up the FastEthernet0/0 interface on router R1.

Configure the IP address on router R1 FastEthernet0/0 as illustrated in the topology and configure VLAN interface 10 with the IP address in the topology on switch Sw1. Verify IP connectivity using ping.

Task 4:

On Sw1, issue a shutdown and then a no shutdown command on FastEthernet0/2. Verify the transition of the Spanning-Tree state of the port to the Forwarding state. Make sure you see the interface in at least three different Spanning-Tree states.

SOLUTION:

Lab 6 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 3 Configuration and Verification Task 1

Task 2:

For reference information on configuring a VTP domain & password, please refer to:

Lab 3 Configuration and Verification Task 2

Lab 5 Configuration and Verification Task 2

Task 3:

For reference information on configuring standard VLANs, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 1 Configuration and Verification Task 2

Lab 2 Configuration and Verification Task 2

Lab 3 Configuration and Verification Task 1

Configure the IP address on router R1 FastEthernet0/0 as illustrated in the topology and configure VLAN interface 10 with the IP address in the topology on switch Sw1. Verify IP connectivity.

For reference information on configuring IP interfaces, please refer to:

Lab 3 Configuration and Verification Task 5

To add an IP address for VLAN 10 on the switch:

```
Sw1(config)#interface vlan 10

Sw1(config-if)#ip address 10.0.0.2 255.255.255.252

Sw1(config-if)#no shut

Sw1(config)#end
```

To check the IP address for VLAN 10 on the switch:

```
Sw1#show ip interface brief
```

NOTE: VLAN 1 is the default Management interface on Cisco switches. When configuring another interface with an IP address, it is good practice to shutdown interface VLAN1 and issue a no shutdown command on the new Management interface you are configuring.

Task 4:

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#int fastethernet0/2

Sw1(config-if)#shut

Sw1(config-if)#no shutdown

Sw1(config-if)#end

Sw1#

Sw1#show spanning-tree interface fastethernet 0/2

no spanning tree info available for FastEthernet0/2
```

After about 10-15 seconds, the port transitions to the Listen state as seen below:

```
Sw1#show spanning-tree interface fastethernet 0/2

Vlan              Role  Sts  Cost       Prio.Nbr  Type
----------------  ----  ---  ---------  --------  --------------------------------
VLAN0010          Desg  LIS  100        128.2     Shr
```

After about 10-15 seconds, the port transitions to the Learning state as seen below:

```
Sw1#show spanning-tree interface fastEthernet 0/2
Vlan              Role  Sts  Cost       Prio.Nbr  Type
----------------  ----  ---  ---------  --------  --------------------------------
VLAN0010          Desg  LRN  100        128.2     Shr
```

After about 10-15 seconds, the port transitions to the Forwarding state as seen below:

```
Sw1#show spanning-tree interface fastethernet 0/2
Vlan              Role   Sts   Cost        Prio.Nbr    Type
----------------  ----   ---   ---------   --------    --------------------------------
VLAN0010          Desg   FWD   100         128.2       Shr
```

Lab 7: Spanning-Tree Protocol Root Bridges Manually

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to manually configure a switch to become the Root Bridge for a particular VLAN. By default, all VLANs have a priority of 32,768 and the switch MAC addresses are used to determine the Spanning-Tree Root Bridge.

Lab Purpose:

VLAN Root Bridge configuration is a fundamental skill. It is always recommended that the Root Bridge be manually configured to ensure that the Layer 2 network is deterministic. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure a switch as a Root Bridge.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

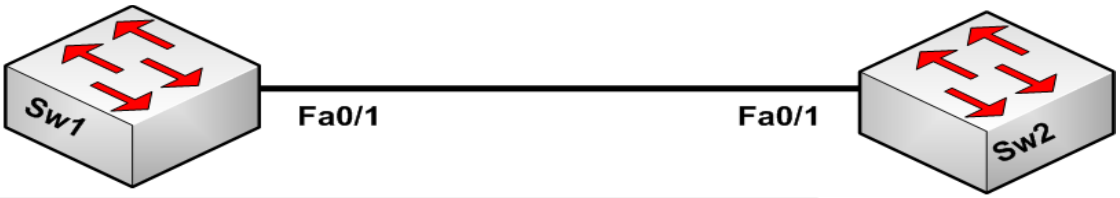
This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



VLAN Number	VLAN Name	Port
2010	SALES	FastEthernet0/5
2020	MANAGERS	FastEthernet0/6
2030	ENGINEERS	FastEthernet0/7
2040	SUPPORT	FastEthernet0/8

Task 1:

Based on the above topology, configure a hostname on Sw1 and Sw2 and configure the VLANs listed.

Task 2:

Configure the switches to support the VLANs listed in the topology. Configure the VLANs and check that they are visible on both switches. Configure FastEthernet0/1 on both switches as a trunk.

Task 3:

Configure switch Sw1 as Root Bridge for VLANs 2010 and 2030. Configure switch Sw2 as Root Bridge for VLANS 2020 and 2040. Use the second non-zero priority value for Root Bridges. Verify your configuration.

Task 4:

Verify your configuration with the appropriate show commands.

SOLUTION:

Lab 7 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 3 Configuration and Verification Task 1

Task 2:

NOTE: By default, Cisco switches are VTP servers. However, to configure the extended range of VLANs, i.e. VLANs 1006 and above, you need to configure the switch as a VTP Transparent switch.

For reference information on Transparent mode and extended VLANs, please refer to:

Lab 2 Configuration and Verification Task 1

Lab 4 Configuration and Verification Task 4

Task 3:

NOTE: Spanning-Tree priority values increment in amounts of 4096. The allowed values are illustrated on the switch if you issue an illegal value:

```
Sw1(config)#spanning-tree vlan 2010 priority 4192
% Bridge Priority must be in increments of 4096.
% Allowed values are:
  0     4096  8192  12288 16384 20480 24576 28672
```

```
32768 36864 40960 45056 49152 53248 57344 61440
```

```
Sw1(config)#spanning-tree vlan 2010 priority 8192

Sw1(config)#spanning-tree vlan 2030 priority 8192

Sw2(config)#spanning-tree vlan 2020 priority 8192

Sw2(config)#spanning-tree vlan 2040 priority 8192
```

Task 4:

NOTE: Use this command to verify the same for VLAN 2030, as well as for VLANs 2020 and 2040 on switch Sw2. In addition to this, you can also issue the show spanning-tree root command to view the Spanning-Tree Root Bridge for all VLANs in the domain. This is illustrated below:

```
Sw1#show spanning-tree root
                                         Root    Hello   Max                    Root
Vlan              Root ID                Cost    Time    Age   Fwd Dly          Port
----------------  --------------------   ------  ----- --- ---   ----------------
VLAN2010          10202 000d.bd06.4100   0       2       20    15
```

```
Sw1#show spanning-tree vlan 2010

VLAN2010

  Spanning tree enabled protocol ieee

  Root ID    Priority    10202

             Address     000d.bd06.4100

             This bridge is the root

             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    10202  (priority 8192 sys-id-ext 2010)

             Address     000d.bd06.4100

             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

             Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 100       128.2    Shr
```

Lab 8: Spanning-Tree Protocol Root Bridges using the IOS Macro

Lab Objective:

The objective of this lab exercise is to use the macro in Cisco IOS to configure a switch to automatically adjust its Spanning Tree priority for a particular VLAN, or group of VLANs, ensuring that it is most likely elected Root Bridge.

Lab Purpose:

VLAN Root Bridge configuration is a fundamental skill. It is always recommended that the Root Bridge be manually configured to ensure that the Layer 2 network is deterministic. However, the macro available in Cisco IOS can also be used. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure a switch as a Root Bridge using the macro available in Cisco IOS.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

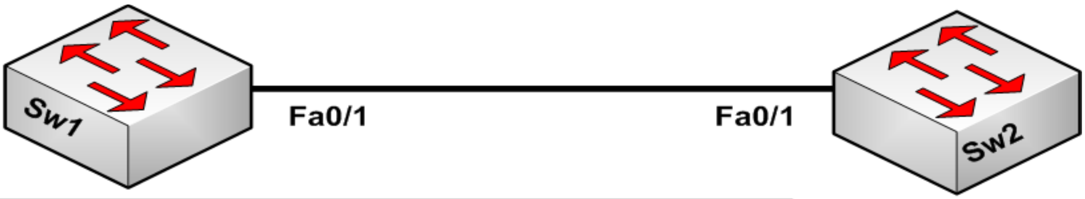
This lab has a difficulty rating of 10/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



VLAN Number	VLAN Name	Port
2010	SALES	FastEthernet0/5
2020	MANAGERS	FastEthernet0/6
2030	ENGINEERS	FastEthernet0/7
2040	SUPPORT	FastEthernet0/8

Task 1:

In preparation for VLAN configuration, configure a hostname on Sw1 and Sw2 and configure the VLANs depicted in the topology above.

Task 2:

Configure the switches to support the VLANs listed in the topology. Configure the VLANs and check that they are visible on both switches. Configure FastEthernet0/1 on both switches as a trunk.

Task 3:

Configure switch Sw1 as Root Bridge for VLANs 2010 and 2030. Configure switch Sw2 as Root Bridge for VLANS 2020 and 2040. Configure the switches to automatically update their priorities as follows:

(a) Switch Sw1 will always be the Root Bridge for VLANs 2010 and 2030 and switch Sw2 will always be the backup root for those VLANs.

(b) Switch Sw2 will always be the Root Bridge for VLANs 2020 and 2040 and switch Sw1 will always be the backup root for those VLANs.

Task 4:

Verify your configuration with the appropriate commands.

SOLUTION:

Lab 8 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 3 Configuration and Verification Task 1

Task 2:

> **NOTE:** By default, Cisco switches are VTP servers. However, to configure the extended range of VLANs, i.e. VLANs 1006 and above, you need to configure the switch as a VTP Transparent switch.

For reference information on Transparent mode and extended VLANs, please refer to:

Lab 2 Configuration and Verification Task 1

Lab 4 Configuration and Verification Task 4

Task 3:

> **NOTE:** The spanning-tree vlan <number> root primary command is a macro that allows Catalyst switches to automatically configure a Spanning-Tree priority value that ensures that the switch this command is issued on will most likely be elected Root Bridge. The spanning-tree vlan <number> root secondary is a macro that allows Catalyst switches to automatically configure a Spanning-Tree priority value that ensures that the switch this command is issued on will most likely be elected backup Root Bridge.

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#spanning-tree vlan 2010 root primary

Sw1(config)#spanning-tree vlan 2030 root primary

Sw1(config)#spanning-tree vlan 2020 root secondary

Sw1(config)#spanning-tree vlan 2040 root secondary

Sw1(config)#end

Sw1#

Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw2(config)#spanning-tree vlan 2020 root primary

Sw2(config)#spanning-tree vlan 2040 root primary

Sw2(config)#spanning-tree vlan 2010 root secondary

Sw2(config)#spanning-tree vlan 2030 root secondary

Sw2(config)#end

Sw2#
```

Task 4:

NOTE: Use this command to verify the same for VLAN 2030, as well as for VLANs 2020 and 2040 on switch Sw2. In addition to this, you can also issue the show spanning-tree root command to view the Spanning-Tree Root Bridge for all VLANs in the domain. This is illustrated below:

```
Sw1#show spanning-tree root
Fwd
                                       Root    Hello   Max   Vlan
                 Root ID               Cost    Time    Age   Dly    Root Port
----------------  --------------------  ------  -----   ---   ---    ----------------
VLAN2010         26586 000d.bd06.4100  0       2       20    15

Sw1#show spanning-tree vlan 2010

VLAN2010

  Spanning tree enabled protocol ieee
  Root ID    Priority    26586
             Address     000d.bd06.4100
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    26586  (priority 24576 sys-id-ext 2010)
             Address     000d.bd06.4100
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
Interface        Role  Sts  Cost      Prio.Nbr Type
---------------- ----  ---  --------- -------- --------------------------------
Fa0/2            Desg  FWD  100       128.2    Shr
```

NOTE: Notice the strange Priority value. This means that there is no switch in the switched LAN that has a priority that is numerically less than the manually set value of 28672. To test the macro, change the priority of VLAN 2010 on switch Sw2 to 20480 and then check the priority on Sw1 again. Try the reverse and change priorities on Sw1 and see Sw2 Spanning-Tree priority values change.

Lab 9: Assigning Multiple Instances to a VLAN Simultaneously

Lab Objective:

The objective of this lab exercise is to understand how to configure many interfaces that share the same common configuration at the same time without having to do them one at a time

Lab Purpose:

Configuring multiple interfaces on a switch at the same time is a fundamental skill. Some high end Cisco Catalyst switches can have in excess of 500 interfaces that may need to be configured almost identically. In such situations, configuring a single interface at a time would not be acceptable. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure multiple switch interfaces at the same time using user defined macros.

Certification Level:

This lab is suitable CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 10/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

You can use any standalone (single) switch to complete this lab. This lab is strictly about configuration syntax.

Task 1:

Configure a hostname of your liking on your lab switch, which should have at least 24 ports.

Task 2:

Configure VLAN 10 named SALES on the switch and VLAN 20 named TECH on the switch.

Task 3:

To simplify configuration tasks, you should create a macro called VLAN_10_Macro for configuring ports FastEthernet0/1 – FastEthernet0/12 that will be in VLAN 10 and a macro called VLAN_20_Macro for configuring ports FastEthernet0/13 – FastEthernet0/24 that will be in VLAN 20.

NOTE: Because this lab is to practice macro configuration, do NOT use the **interface range** command.

Task 4:

Configure interfaces FastEthernet0/1 – 12 and FastEthernet0/12 - 24 in VLAN 10 and VLAN 20, respectively, using the macro. These ports should be configured as Access ports.

Task 5:

Verify your configuration using the appropriate commands in Cisco IOS.

SOLUTION:

Lab 9 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 3 Configuration and Verification Task 1

Task 2:

For reference information on configuring standard VLANs, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 1 Configuration and Verification Task 2

Lab 2 Configuration and Verification Task 2

Lab 3 Configuration and Verification Task 1

Task 3:

```
Sw1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#define interface-range VLAN_10_Macro FastEthernet 0/1 - 12

Sw1(config)#define interface-range VLAN_20_Macro FastEthernet 0/13 -- 24

Sw1(config)#^Z

Sw1#
```

Task 4:

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#interface range macro VLAN_10_Macro

Sw1(config-if-range)#switchport mode access

Sw1(config-if-range)#switchport access vlan 10

Sw1(config-if-range)#exit

Sw1(config)#interface range macro VLAN_20_Macro

Sw1(config-if-range)#switchport mode access

Sw1(config-if-range)#switchport access vlan 20

Sw1(config-if-range)#end

Sw1#
```

Task 5:

```
Sw1#show vlan brief
VLAN         Name                             Status    Ports
----         -------------------------------- --------- -------------------------------
1            default                          active    Gi0/1, Gi0/2
2            VLAN0002                         active
10           SALES                            active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                        Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                        Fa0/9, Fa0/10, Fa0/11, Fa0/12
```

```
20      MANAGERS          active  Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                  Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                  Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002    fddi-default      active
1003    trcrf-default     active
1004    fddinet-default   active
1005    trbrf-default     active
```

Lab 10: Configuring Spanning-Tree Protocol for Access ports (Portfast)

Lab Objective:

The objective of this lab exercise is to configure Access ports to transition immediately to a Forwarding state, instead of going through the typical Spanning Tree states, i.e. Blocking, Listening, Learning, etc.

Lab Purpose:

Bypassing default Spanning-Tree port states is a fundamental skill. By default, it can take up to 60 seconds for a switch port to transition to the Forwarding state and begin forwarding frames. In most cases, this is acceptable; however, on a network with DHCP clients, for example, that need IP addressing information from a DHCP server, this duration may cause these clients to think the DHCP server is unavailable.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 4/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the any single switch for this lab. This lab is strictly about validating command syntax.

Task 1:

Configure a hostname of your liking on your lab switch, which should have at least 12 ports.

Task 2:

Configure VLAN 10 named SALES on the switch.

Task 3:

Configure ports FastEthernet0/1 and FastEthernet0/2 using the interface range command so that Spanning-Tree protocol transitions these interfaces into a forwarding state immediately. These interfaces should also be configured as access ports in VLAN 10.

Task 4:

Verify your configuration using the appropriate commands in Cisco IOS.

SOLUTION:

Lab 10 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 3 Configuration and Verification Task 1

Task 2:

For reference information on configuring verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#interface range fastethernet0/1 - 2

Sw1(config-if-range)#switchport mode access

Sw1(config-if-range)#switchport access vlan 10

Sw1(config-if-range)#spanning-tree portfast

%Warning: portfast should only be enabled on ports connected to a single

 host. Connecting hubs, concentrators, switches, bridges, etc... to this

 interface  when portfast is enabled, can cause temporary bridging loops.

 Use with CAUTION

%Portfast will be configured in 2 interfaces due to the range command
```

but will only have effect when the interfaces are in a non-trunking mode.

```
Sw1(config-if-range)#end

Sw1#
```

Task 4:

```
Sw1#show spanning-tree interface fastethernet 0/2 detail

 Port 2 (FastEthernet0/2) of VLAN0010 is forwarding

   Port path cost 100, Port priority 128, Port Identifier 128.2.

   Designated root has priority 4106, address 000d.bd06.4100

   Designated bridge has priority 4106, address 000d.bd06.4100

   Designated port id is 128.2, designated path cost 0

   Timers: message age 0, forward delay 0, hold 0

   Number of transitions to forwarding state: 1

   The port is in the portfast mode

   Link type is shared by default

   BPDU: sent 81, received 0
```

Lab 11: Configuring switch Access port security

Lab Objective:

The objective of this lab exercise is to configure basic switch security to prevent MAC address flooding on switch ports. This is accomplished by limiting the number of MAC entries that are allowed to be learned on a port. By default, there is no limit on MAC addresses that can be learned on a port.

Lab Purpose:

Port security is a fundamental skill. A Common Denial of Service technique used to cripple switched networks is MAC flooding. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure port security to mitigate MAC flooding attacks.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

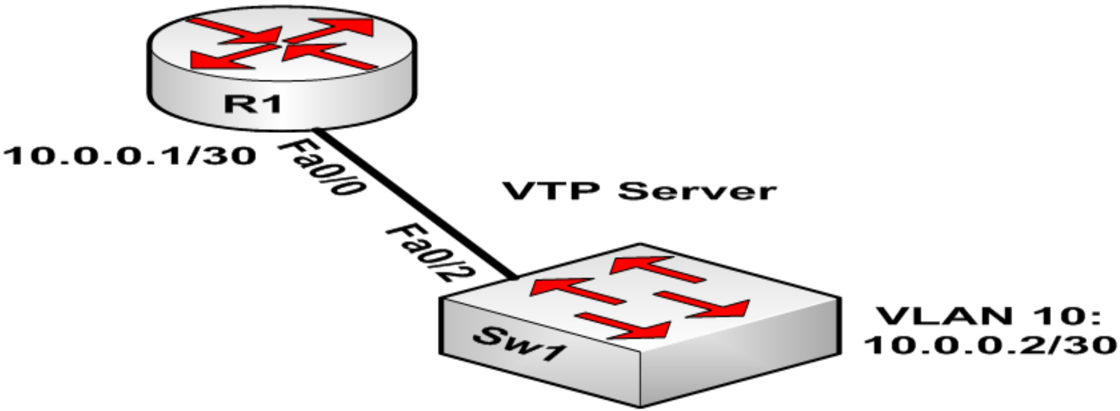
This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



VLAN No.	VLAN Name	Interface
10	SALES	FastEthernet0/2

Task 1:

Configure a hostname of Sw1 on your lab switch, and the hostname R1 on the router as illustrated in the topology.

Task 2:

Create VLAN 10 on switch Sw1 and assign port FastEthernet0/2 to this VLAN as an access port.

Task 3:

Configure IP address 10.0.0.1/30 on router R1's FastEthernet0/0 interface, and IP address 10.0.0.2/30 in switch Sw2's VLAN 10 interface. Verify that R1 can ping Sw1 and vice versa.

Task 4:

Configure port security on port FastEthernet0/2 on switch Sw1 so that only 1 MAC address is allowed to be learned on that interface. In the event of port security configuration violations, where more than 1 MAC address is observed on that interface, the switch should shut the interface down. Verify your configuration with port security commands in Cisco IOS.

SOLUTION:

Lab 11 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 3 Configuration and Verification Task 1

Task 2:

For reference information on configuring verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

For reference information on configuring IP interfaces, please refer to:

Lab 3 Configuration and Verification Task 5

Task 4:

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#interface fastethernet 0/2

Sw1(config-if)#switchport port-security

Sw1(config-if)#switchport port-security maximum 1

Sw1(config-if)#switchport port-security violation shutdown

Sw1(config-if)#end

Sw1#

Sw1#show port-security

Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action

                (Count)        (Count)      (Count)

---------------------------------------------------------------------------

    Fa0/2          1              0            0              Shutdown
```

```
-------------------------------------------------------------------------------

Total Addresses in System : 0

Max Addresses limit in System : 1024
```

NOTE: If you wanted to test your port security configuration, you could simply change the MAC address of FastEthernet0/0 on R1 to and then you would see a port security violation. For example:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface fastethernet0/0
R1(config-if)#mac-address 000a.bc01.2300
R1(config)#end
R1#

Sw1#show port-security
Secure Port     MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)        (Count)      (Count)
-------------------------------------------------------------------------------
    Fa0/2         1             0            1             Shutdown
-------------------------------------------------------------------------------
Total Addresses in System : 0
Max Addresses limit in System : 1024
Sw1#
Sw1#show interfaces fastethernet 0/2
FastEthernet0/2 is down, line protocol is down (err-disabled)
```

As can be seen in the output above, the violation counter has incremented and the interface is now in an err-disabled mode, which basically means it has been shut down due to a port security violation. To bring this interface back up, you need to issue a shutdown and then no shutdown under the interface.

Lab 12: Configuring advanced switch Access port security

Lab Objective:

The objective of this lab exercise is to ensure that learned MAC addresses on a secured port are retained in the switch NVRAM in the event of a reboot. By default, secured MAC addresses are flushed during switch reboots.

Lab Purpose:

Retaining learned secure MAC addresses is an advanced skill. When a Cisco Catalyst switch configured with port security reboots, learned secure MAC address entries are flushed and have to be re-learned when the switch comes back up. As a Cisco engineer, understanding advanced features will give you the edge over fellow CCNAs.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

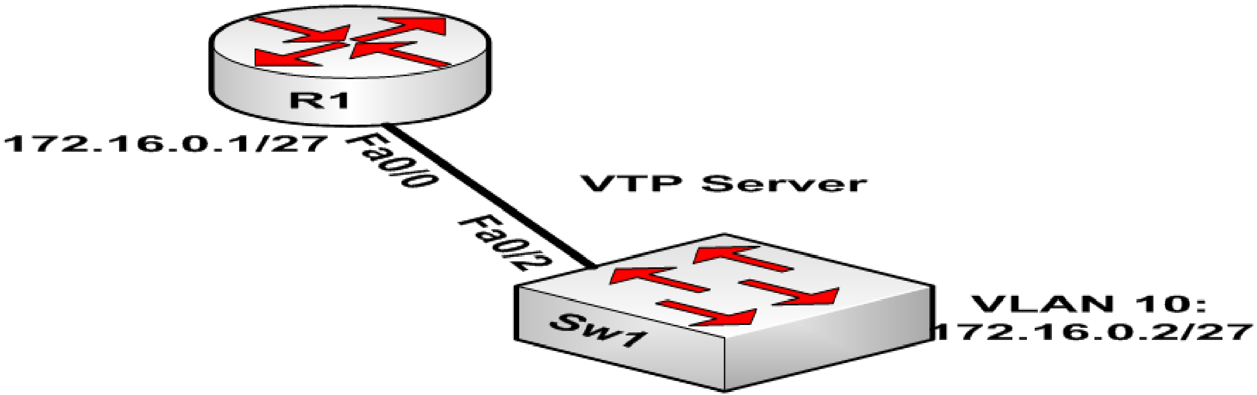
This lab has a difficulty rating of 10/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



VLAN No.	VLAN Name	Interface
10	SALES	FastEthernet0/2

Task 1:

Configure a hostname of Sw1 on your lab switch, and the hostname R1 on the router as illustrated in the topology.

Task 2:

Create VLAN 10 on switch Sw1 and assign port FastEthernet0/2 to this VLAN as an access port.

Task 3:

Configure IP address 172.16.0.1/27 on router R1's FastEthernet0/0 interface, and IP address 172.16.0.2/27 in switch Sw2's VLAN 10 interface. Verify that R1 can ping Sw1, and vice versa.

Task 4:

Configure port security on port FastEthernet0/2 on switch Sw1 so that any MAC addresses learned on that interface are written to the switch NVRAM. The NVRAM is the startup-configuration. Verify your configuration with port security commands in Cisco IOS.

SOLUTION:

Lab 12 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 3 Configuration and Verification Task 1

Task 2:

For reference information on configuring verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

For reference information on configuring IP interfaces, please refer to:

Lab 3 Configuration and Verification Task 5

NOTE: VLAN 1 is the default Management interface on Cisco switches. When configuring another interface with an IP address, it is good practice to shutdown interface VLAN1 and issue a no shutdown command on the new Management interface you are configuring.

Task 4:

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#interface fastethernet0/2

Sw1(config-if)#switchport port-security

Sw1(config-if)#switchport port-security violation shutdown

Sw1(config-if)#switchport port-security mac-address sticky

Sw1(config-if)#end

Sw1#

Sw1#copy startup-config running-config

Destination filename [running-config]?

2167 bytes copied in 2.092 secs (1036 bytes/sec)

Sw1#

Sw1#show port-security
```

```
Secure Port     MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action

                (Count)        (Count)      (Count)

---------------------------------------------------------------------------

    Fa0/2         1              1            0               Shutdown

---------------------------------------------------------------------------

Total Addresses in System : 1

Max Addresses limit in System : 1024

Sw1#

Sw1#

Sw1#show running-config interface fastethernet 0/2

Building configuration...

Current configuration : 254 bytes

!

interface FastEthernet0/2

 switchport port-security

 switchport port-security mac-address sticky

 switchport port-security mac-address sticky 0004.c058.5fc0

end
```

NOTE: When configuring port security, by default the learned MAC addresses are flushed when the switch in reloaded. To prevent this and ensure that the switch preserves MAC addresses that are dynamically learned via port security, you need to configure sticky learning. This configuration, in conjunction with the copy run start command, saves the learned MAC addresses to NVRAM. This means that when the switch is rebooted, the MAC address learned is not lost. The switch adds the switchport port-security mac-address sticky <mac-address> command dynamically under the interface for every sticky dynamically learned MAC address. So if 100 MAC addresses are learned this way, the switch would add 100 of these statements after the switchport port-security mac-address sticky command that you issued under the interface. Be very careful and this can create a very large configuration file in the real world!

Lab 13: Configuring advanced static switch Access port security

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure static MAC entries for port security. By default, MAC entries are learned dynamically on a switch port.

Lab Purpose:

Static port security MAC entries are an advanced skill. Static MAC address entries are manually configured by the administrator. As a Cisco engineer, understanding advanced features will give you the edge over fellow CCNAs.

Certification Level:

This lab is suitable for CCNA certification exam preparation.

Lab Difficulty:

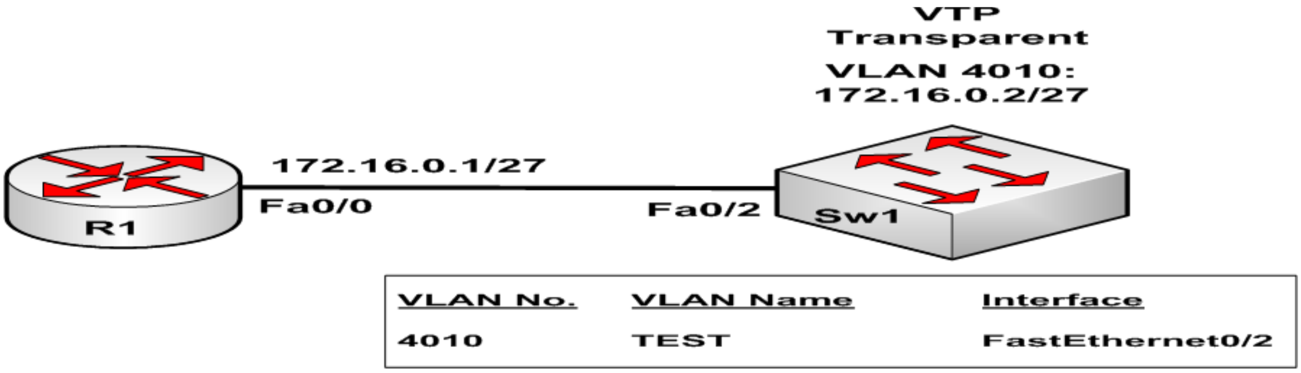
This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



VLAN No.	VLAN Name	Interface
4010	TEST	FastEthernet0/2

Task 1:

Configure a hostname of Sw1 on your lab switch, and the hostname R1 on the router as illustrated in the topology. Create VLAN 10 on switch Sw1 and assign port FastEthernet0/2 to this VLAN as an access port.

Task 2:

Configure IP address 172.16.0.1/27 on router R1's FastEthernet0/0 interface, and IP address 172.16.0.2/27 in switch Sw2's VLAN 10 interface. Verify that R1 can ping Sw1 and vice versa.

Task 3:

Configure port security on port FastEthernet0/5 on switch Sw1 for the following static MAC addresses:

abcd.1111.ab01

abcd.2222.cd01

abcd.3333.ef01

abcd.4444.ac01

The switch should restrict access to these ports for MAC addresses that are not known. Verify your configuration with port security commands in Cisco IOS.

SOLUTION:

Lab 13 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 3 Configuration and Verification Task 1

For reference information on Transparent mode and extended VLANs, please refer to:

Lab 2 Configuration and Verification Task 1

Lab 4 Configuration and Verification Task 4

Task 2:

For reference information on configuring IP interfaces, please refer to:

Lab 3 Configuration and Verification Task 5

NOTE: VLAN 1 is the default Management interface on Cisco switches. When configuring another interface with an IP address, it is good practice to shutdown interface VLAN1 and issue a no shutdown command on the new Management interface you are configuring.

Task 3:

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#interface fastethernet0/2

Sw1(config-if)#switchport port-security
```

```
Sw1(config-if)#switchport port-security maximum 4

Sw1(config-if)#switchport port-security mac-address 000a.1111.ab01

Sw1(config-if)#switchport port-security mac-address 000b.2222.cd01

Sw1(config-if)#switchport port-security mac-address 000c.3333.ef01

Sw1(config-if)#switchport port-security mac-address 000d.4444.ac01

Sw1(config-if)#end

Sw1#

Sw1#show port-security

Secure Port      MaxSecureAddr   CurrentAddr   SecurityViolation   Security Action

                (Count)        (Count)      (Count)

---------------------------------------------------------------------------

    Fa0/2          4              4            0             Shutdown

---------------------------------------------------------------------------

Total Addresses in System : 5

Max Addresses limit in System : 1024

Sw1#

Sw1#

Sw1#show port-security interface fastethernet 0/2

Port Security : Enabled

Port status : SecureUp

Violation mode : Shutdown

Maximum MAC Addresses : 4

Total MAC Addresses : 4

Configured MAC Addresses : 4

Sticky MAC Addresses : 0

Aging time : 0 mins

Aging type : Absolute
```

```
SecureStatic address aging : Disabled

Security Violation count : 0
```

NOTE: The requirements of this task seem pretty simple; however, a common mistake here is often made in the people forget that by default, the maximum number of addresses that can be secured is 1. Therefore, since we are given 4 MAC addresses, we need to increase the port security limit to 4. Otherwise, if you did not add the switchport port-security maximum 4 command, you would receive the following error when trying to add the second static MAC address for port security:

```
Sw1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#interface fastethernet0/2
Sw1(config-if)#switchport port-security
Sw1(config-if)#switchport port-security mac-address 000a.1111.ab01
Sw1(config-if)#switchport port-security mac-address 000b.2222.cd01
%Error: Cannot add secure address 000b.2222.cd01
%Error: Total secure addresses on interface reached its max limit of 1
%PSECURE: Internal Error in adding address
Sw1(config-if)#
```

Lab 14: Enabling Rapid Per-VLAN Spanning Tree

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure RPVST Spanning Tree protocol. By default, RPVST converges much faster than traditional STP.

Lab Purpose:

Rapid PVST configuration is a fundamental skill. RPVST converges much faster than traditional Spanning-Tree protocol. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure RPVST.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

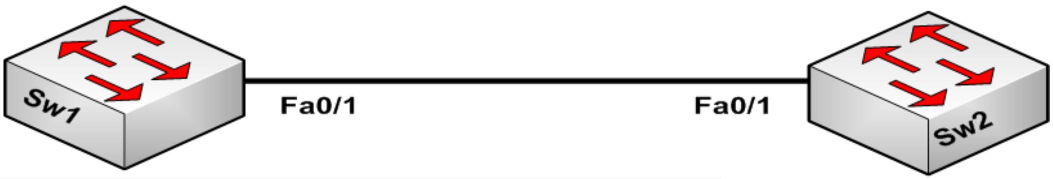
This lab has a difficulty rating of 4/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



VLAN Number	VLAN Name	Port
10	SALES	FastEthernet0/5
20	MANAGERS	FastEthernet0/6
30	ENGINEERS	FastEthernet0/7
40	SUPPORT	FastEthernet0/8

Task 1:

Configure a hostname on switches 1 and 2 as illustrated in the topology diagram above.

Task 2:

Configure and verify Sw1 as a VTP Server switch and configure Sw2 as a VTP Client switch. Both switches should be in the VTP domain named CISCO. Secure VTP messages with the password CISCO.

Task 3:

Configure and verify FastEthernet0/1 between Sw1 and Sw2 as an 802.1q trunk.

Task 4:

Configure and verify VLANs 10, 20, 30 and 40 on Sw1 with the names provided above. Validate that these VLANs are still propagated to Sw2 after VTP has been secured.

Task 5:

Verify that the switches are running in Per-VLAN Spanning Tree mode. This is the default mode for switches.

Task 6:

Update your switch to a Spanning Tree mode that ensures the fastest convergence for the Layer 2 network and verify your configuration.

SOLUTION:

Lab 14 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 3 Configuration and Verification Task 1

Task 2:

NOTE: By default, Cisco switches are VTP servers so no configuration is necessary for Server mode on Sw1. This can be verified using the show vtp status command. However, we do need to configure the domain.

For reference information on configuring the VTP Mode, please refer to:

Lab 4 Configuration and Verification Task 2

For reference information on configuring a VTP password, please refer to:

Lab 5 Configuration and Verification

Task 3:

For reference information on configuring and verifying trunks, please refer to:

Lab 3 Configuration and Verification Task 3

Lab 3 Configuration and Verification Task 3

Task 4:

For reference information on configuring verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

NOTE: Make sure that the MD5 digest at the end of the output of the show vtp status command is the same when VTP passwords have been configured on switches within the same VTP domain.

Task 5:

```
Sw1#show spanning-tree summary

Switch is in pvst mode

Root bridge for: VLAN0010, VLAN0020, VLAN0030, VLAN0040

EtherChannel misconfiguration guard is enabled

Extended system ID   is enabled

Portfast             is disabled by default

PortFast BPDU Guard  is disabled by default

Portfast BPDU Filter is disabled by default
```

```
Loopguard            is disabled by default
UplinkFast           is disabled
BackboneFast         is disabled
Pathcost method used is short
Name                 Blocking Listening Learning Forwarding STP Active
--------------------- -------- --------- -------- ---------- ----------
VLAN0010                  0        0        0         1          1
VLAN0020                  0        0        0         1          1
VLAN0030                  0        0        0         1          1
VLAN0040                  0        0        0         1          1
--------------------- -------- --------- -------- ---------- ----------
4 vlans                   0        0        0         4          4
```

Task 6:

```
Sw1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#spanning-tree mode rapid-pvst
Sw1(config)#^Z
Sw1#
Sw1#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0010, VLAN0020, VLAN0030, VLAN0040
EtherChannel misconfiguration guard is enabled
Extended system ID   is enabled
Portfast             is disabled by default
PortFast BPDU Guard  is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard            is disabled by default
```

```
UplinkFast          is disabled

BackboneFast        is disabled

Pathcost method used is short

Name                Blocking Listening Learning Forwarding STP Active

--------------------- -------- --------- -------- ---------- ----------

VLAN0010                0        0        0         1         1

VLAN0020                0        0        0         1         1

VLAN0030                0        0        0         1         1

VLAN0040                0        0        0         1         1

--------------------- -------- --------- -------- ---------- ----------

4 vlans              0        0        0         4         4
```

NOTE: Rapid Spanning Tree protocol enables the fastest convergence of Layer 2 switched networks.

Lab 15: Configuring and allowing inter-VLAN routing

Lab Objective:

The objective of this lab exercise is to configure a router to provide inter-VLAN communication. By default, hosts in one VLAN cannot communicate with hosts in another VLAN without a router routing between the two VLANs.

Lab Purpose:

Inter-VLAN routing configuration is a fundamental skill. Most networks typically have more than one VLAN and it is a requirement that hosts in these VLANs communicate with each other if the need arises. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure inter-VLAN routing.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

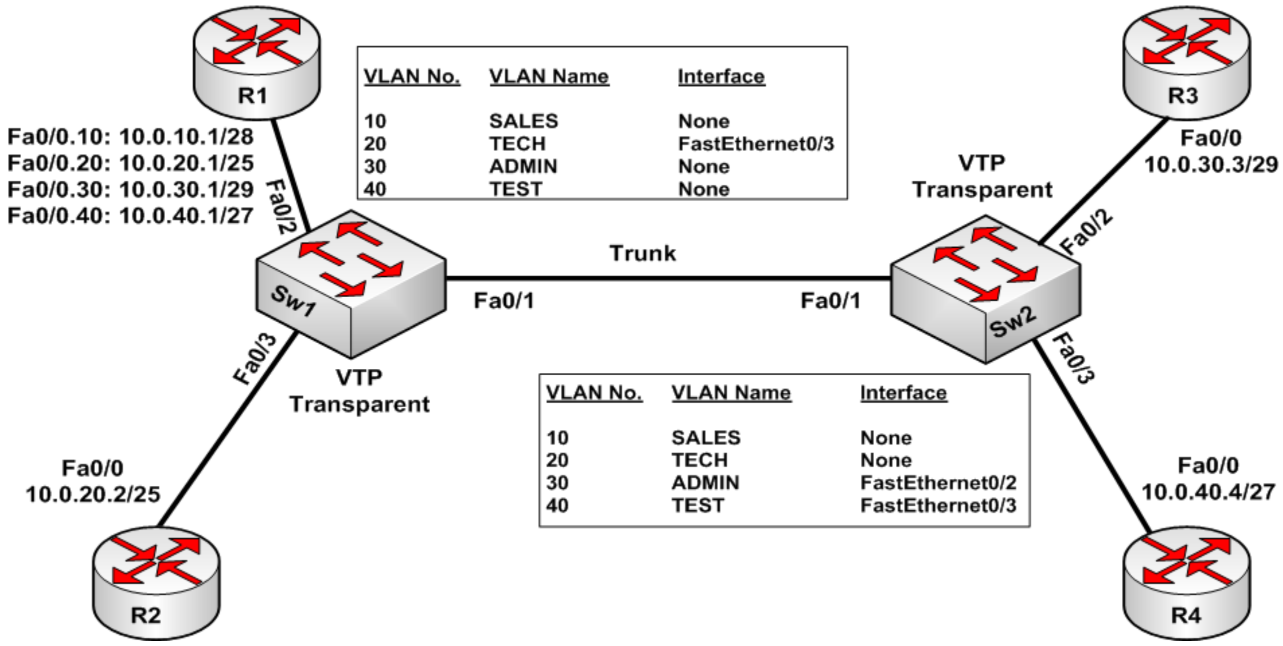
This lab has a difficulty rating of 9/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



VLAN No.	VLAN Name	Interface
10	SALES	None
20	TECH	FastEthernet0/3
30	ADMIN	None
40	TEST	None

VLAN No.	VLAN Name	Interface
10	SALES	None
20	TECH	None
30	ADMIN	FastEthernet0/2
40	TEST	FastEthernet0/3

Task 1:

Configure a hostname on switches 1 and 2 and routers 1 through 4 as illustrated in the topology above.

Task 2:

Configure and verify Sw1 and Sw2 as VTP Transparent switches. Both switches should be in the VTP domain named CISCO. Secure VTP messages with the password CISCO.

Task 3:

Configure and verify FastEthernet0/1 between Sw1 and Sw2 as an 802.1q trunk and configure VLANs as depicted in the topology above. Assign ports to depicted VLANs and configure Sw1 FastEthernet0/2 as a trunk. VLAN 20 should have untagged Ethernet Frames. Remember that on 802.1q trunks, only the native VLAN is untagged.

Task 4:

Configure IP addresses on routers R2, R3, and R4 as illustrated in the diagram.

Task 5:

Configure subinterfaces off FastEthernet0/0 in the corresponding VLANs on the diagram. Also configure interface VLAN 10 on switch Sw2 with the IP address 10.0.10.2/28.

Task 6:

Test network connectivity by pinging from R1 to routers R2, R3, and R4.

SOLUTION:

Lab 15 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 3 Configuration and Verification Task 1

Task 2:

For reference information on configuring verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

For reference information on configuring a VTP password, please refer to:

Lab 5 Configuration and Verification

Task 3:

```
Sw1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#interface fastethernet0/1

Sw1(config-if)#switchport mode trunk

Sw1(config-if)#exit

Sw1(config)#vlan 10

Sw1(config-vlan)#name SALES

Sw1(config-vlan)#exit

Sw1(config)#vlan 20

Sw1(config-vlan)#name TECH

Sw1(config-vlan)#exit

Sw1(config)#vlan 30

Sw1(config-vlan)#name ADMIN

Sw1(config-vlan)#exit
```

```
Sw1(config)#vlan 40
Sw1(config-vlan)#name TEST
Sw1(config-vlan)#exit
Sw1(config)#interface fastethernet0/2
Sw1(config-if)#switchport mode trunk
Sw1(config-if)#switchport trunk native vlan 20
Sw1(config-if)#exit
Sw1(config)#interface fastethernet0/3
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 20
Sw1(config-if)#end
Sw1#
Sw1#show interfaces trunk
Port      Mode        Encapsulation  Status       Native vlan
Fa0/1       on         802.1q        trunking     1
Fa0/2       on         802.1q        trunking     20
Port      Vlans allowed on trunk
Fa0/1       1-4094
Fa0/2       1-4094
Port      Vlans allowed and active in management domain
Fa0/1       1,10,20,30,40
Fa0/2       1,10,20,30,40
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,20,30,40
Fa0/2       1,20,30,40
Sw2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Sw2(config)#interface fastethernet0/1
Sw2(config-if)#switchport mode trunk
Sw2(config-if)#exit
Sw2(config)#vlan 10
Sw2(config-vlan)#name SALES
Sw2(config-vlan)#exit
Sw2(config)#vlan 20
Sw2(config-vlan)#name TECH
Sw2(config-vlan)#exit
Sw2(config)#vlan 30
Sw2(config-vlan)#name ADMIN
Sw2(config-vlan)#exit
Sw2(config)#vlan 40
Sw2(config-vlan)#name TEST
Sw2(config-vlan)#exit
Sw2(config)#interface fastethernet0/2
Sw2(config-if)#switchport mode access
Sw2(config-if)#switchport access vlan 30
Sw2(config-if)#exit
Sw2(config)#interface fastethernet0/3
Sw2(config-if)#switchport mode access
Sw2(config-if)#switchport access vlan 40
Sw2(config-if)#^Z
Sw2#
Sw2#show interfaces trunk
Port      Mode       Encapsulation  Status      Native vlan
Fa0/1      on        802.1q        trunking     1
```

```
Port        Vlans allowed on trunk

Fa0/1         1-4094

Port        Vlans allowed and active in management domain

Fa0/1         1,10,20,30,40

Port        Vlans in spanning tree forwarding state and not pruned

Fa0/1         1,20,30,40
```

Task 4:

For reference information on configuring IP interfaces, please refer to:

Lab 3 Configuration and Verification Task 5

Task 5:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#interface fastethernet 0/0

R1(config-if)#description "Connected To Switch Trunk Fa0/2"

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#interface fastethernet 0/0.10

R1(config-subif)#description Subinterface For VLAN 10

R1(config-subif)#encapsulation dot1Q 10

R1(config-subif)#ip address 10.0.10.1 255.255.255.240

R1(config-subif)#exit

R1(config)#interface fastethernet 0/0.20

R1(config-subif)#description Subinterface For VLAN 20

R1(config-subif)#encapsulation dot1Q 20 native

R1(config-subif)#ip address 10.0.20.1 255.255.255.128

R1(config-subif)#exit

R1(config)#interface fastethernet 0/0.30
```

```
R1(config-subif)#description Subinterface For VLAN 30

R1(config-subif)#ip address 10.0.30.1 255.255.255.248

R1(config-subif)#exit

R1(config)#interface fastethernet 0/0.40

R1(config-subif)#description Subinterface For VLAN 40

R1(config-subif)#encapsulation dot1Q 40

R1(config-subif)#ip address 10.0.40.1 255.255.255.224

R1(config-subif)#end

R1#

R1#show ip interface brief

Interface               IP-Address    OK?    Method    Status   Protocol

FastEthernet0/0            unassigned    YES    manual    up        up

FastEthernet0/0.10          10.0.10.1     YES    manual    up        up

FastEthernet0/0.20          10.0.20.1     YES    manual    up        up

FastEthernet0/0.30          10.0.30.1    YES     manual    up        up

FastEthernet0/0.40          10.0.40.1    YES     manual    up        up

Sw2(config)#interface vlan1

Sw2(config-if)#shutdown

Sw2(config)#interface vlan10

Sw2(config-if)#ip address 10.0.10.2 255.255.255.240

Sw2(config-if)#no shutdown

Sw2(config)#^Z

Sw2#

Sw2#show ip interface brief

Interface             IP-Address     OK? Method Status             Protocol

Vlan1                unassigned     YES NVRAM  administratively down down

Vlan10                10.0.10.2     YES manual up                 up
```

```
Sw2#
```

Task 6:

```
R1#ping 10.0.10.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.10.2, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms

R1#ping 10.0.20.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.20.2, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms

R1#ping 10.0.30.3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.30.3, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms

R1#ping 10.0.40.4

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.40.4, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms
```

NOTE: The first PING packet times out due to ARP resolution. Subsequent packets will be successful.

Lab 16: Restricting VLANs on Trunks and changing the VTP version

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to restrict VLANs traversing trunks. By default, all VLANs are allowed to traverse trunks.

Lab Purpose:

VLAN trunk restriction is a fundamental skill. By default, all VLANs traverse trunks. However, in some cases, this may result in unnecessary VLANs being propagated, and may pose a security risk. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to restrict VLANs traversing trunks.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

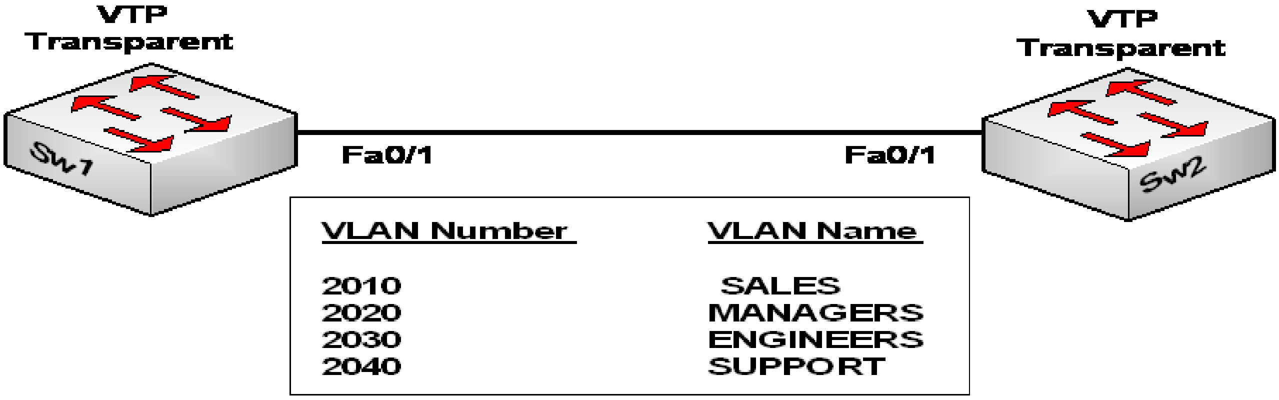
This lab has a difficulty rating of 7/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



VLAN Number	VLAN Name
2010	SALES
2020	MANAGERS
2030	ENGINEERS
2040	SUPPORT

Task 1:

In preparation for VLAN configuration, configure a hostname on switches 1 and 2 as illustrated in the topology.

Task 2:

Configure and verify Sw1 and Sw2 as VTP Transparent switches. Both switches should be in the VTP domain named CISCO. Configure the switches to use legacy VTP version 1. Configure FastEthernet0/1 as a trunk between switches Sw1 and Sw2.

Task 3:

Verify your VLAN configuration on either switch Sw1 or Sw2 and ensure they are identical.

Task 4:

Allow only VLAN 2040 to traverse the trunk link on switch Sw1 and verify your configuration.

SOLUTION:

Lab 16 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 3 Configuration and Verification Task 1

Task 2:

```
Sw1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#vtp mode transparent

Setting device to VTP TRANSPARENT mode.

Sw1(config)#vtp mode transparent

Sw1(config)#vtp domain CISCO

Changing VTP domain name from Null to CISCO

Sw1(config)#vtp version 1

Sw1(config)#vlan 2010

Sw1(config-vlan)#name SALES

Sw1(config-vlan)#exit

Sw1(config)#vlan 2020

Sw1(config-vlan)#name MANAGERS

Sw1(config-vlan)#exit

Sw1(config)#vlan 2030

Sw1(config-vlan)#name ENGINEERS
```

```
Sw1(config-vlan)#exit

Sw1(config)#vlan 2040

Sw1(config-vlan)#name SUPPORT

Sw1(config-vlan)#exit

Sw1(config)#interface fastethernet0/1

Sw1(config-if)#switchport mode trunk

Sw2#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw2(config)#vtp mode transparent

Setting device to VTP TRANSPARENT mode.

Sw2(config)#vtp mode transparent

Sw2(config)#vtp domain CISCO

Changing VTP domain name from Null to CISCO

Sw2(config)#vtp version 1

Sw2(config)#vlan 2010

Sw2(config-vlan)#name SALES

Sw2(config-vlan)#exit

Sw2(config)#vlan 2020

Sw2(config-vlan)#name MANAGERS

Sw2(config-vlan)#exit

Sw2(config)#vlan 2030

Sw2(config-vlan)#name ENGINEERS

Sw2(config-vlan)#exit

Sw2(config)#vlan 2040

Sw2(config-vlan)#name SUPPORT

Sw2(config-vlan)#exit

Sw2(config)#interface fastethernet0/1
```

```
Sw2(config-if)#switchport mode trunk
```

Task 3:

For reference information on configuring verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 4:

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#interface fastethernet0/1

Sw1(config-if)#switchport trunk allowed vlan 2040

Sw1(config-if)#^Z

Sw1#

Sw1#show interfaces trunk

Port       Mode        Encapsulation  Status       Native vlan

Fa0/1        on          802.1q          trunking      1

Port       Vlans allowed on trunk

Fa0/1        2040
```

NOTE: By default, ALL configured VLANs are allowed to traverse ALL configured trunk links. You can restrict certain VLANs to certain trunks by using the switchport trunk allowed vlan command.

Lab 17: Configuring a default gateway for routers and switches

Lab Objective:

The objective of this lab exercise is to configure routers and switches to be able to communicate with remote networks. By default, devices can only communicate with locally connected networks.

Lab Purpose:

Configuring a default gateway on routers and switches is a fundamental skill. Default gateways allow routers and switches to be reachable to and from remote subnets. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure a router or switch default gateway.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

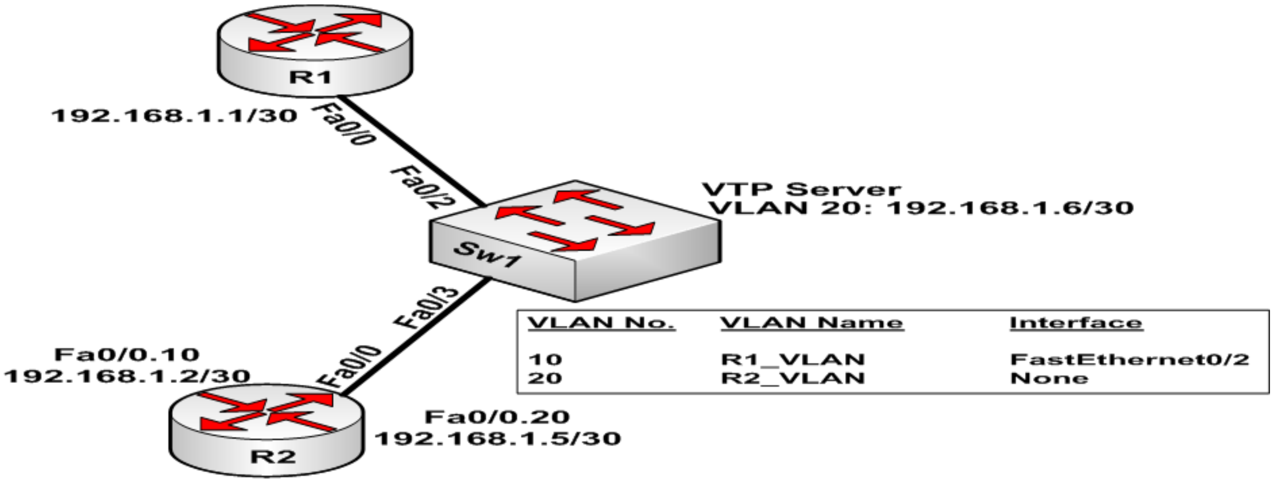
This lab has a difficulty rating of 4/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



VLAN No.	VLAN Name	Interface
10	R1_VLAN	FastEthernet0/2
20	R2_VLAN	None

Task 1:

Configure a hostname on switch 1 and routers R1 and R2 as illustrated in the topology above.

Task 2:

Configure switch Sw1 as a VTP Server and configure the VLANs as illustrated above. In addition, configure Sw1 interface FastEthernet0/3 as a trunk using 802.1q encapsulation. Ensure you place the correct switch interface into VLAN10.

Task 3:

Configure IP addressing on routers R1 and R2 and interface VLAN 20 on Sw1 as illustrated above. In addition to that, configure a default gateway on Sw1 of 192.168.1.5 and a default route on R1 via FastEthernet0/0.

Task 4:

Verify your configuration by pinging from Sw1 to R1's FastEthernet0/0 address of 192.168.1.1

SOLUTION:

Lab 17 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 3 Configuration and Verification Task 1

Task 2:

For reference information on configuring verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#interface  fastethernet0/0

R1(config-if)#ip address 192.168.1.1 255.255.255.252

R1(config-if)#exit

R1(config)#ip route 0.0.0.0 0.0.0.0 fastethernet0/0

R1(config)#^Z

R1#

R1#show ip interface brief

Interface                  IP-Address      OK? Method Status  Protocol

FastEthernet0/0            192.168.1.1     YES manual up      up

R2(config)#interface fastethernet 0/0

R2(config-if)#description "Connected To Switch Trunk Fa0/3"

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#interface fastethernet 0/0.10
```

```
R2(config-subif)#description Subinterface For VLAN 10

R2(config-subif)#encapsulation dot1Q 10

R2(config-subif)#ip address 192.168.1.2 255.255.255.252

R2(config-subif)#exit

R2(config)#interface fastethernet 0/0.20

R2(config-subif)#description Subinterface For VLAN 20

R2(config-subif)#encapsulation dot1Q 20 native

R2(config-subif)#ip address 192.168.1.5 255.255.255.252

R2(config-subif)#end

R2#

R2#show ip interface brief

Interface                IP-Address    OK?    Method    Status   Protocol

FastEthernet0/0             unassigned    YES    manual    up        up

FastEthernet0/0.10           192.168.1.2   YES    manual    up        up

FastEthernet0/0.20           192.168.1.5   YES    manual    up        up

Sw1(config)#interface vlan1

Sw1(config-if)#shutdown

Sw1(config)#interface vlan 20

Sw1(config-if)#ip address 192.168.1.6 255.255.255.252

Sw1(config-if)#no shutdown

Sw1(config-if)#interface fastethernet 0/3

Sw1(config-if)# exit

Sw1(config)# ip default-gateway 192.168.1.5

Sw1(config)# ^Z

Sw1#

Sw1#show ip interface brief

Interface              IP-Address     OK? Method Status           Protocol
```

```
Vlan1                  unassigned      YES NVRAM  administratively down down

Vlan20                  192.168.1.6     YES manual up                    up

Sw1#

Sw1#show ip redirects

Default gateway is 192.168.1.5

Host              Gateway           Last Use    Total Uses  Interface

ICMP redirect cache is empty
```

Task 4:

```
Sw1#ping 192.168.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1, timeout is 2 seconds:

..!!!

Success rate is 60 percent (3/5), round-trip min/avg/max = 1/3/4 ms
```

Notes -- on some models of 2950 the ping would only work after this command was added to fastethernet 0/3 on Sw1:

```
Sw1(config-if)#switchport trunk native vlan 20
```

Lab 18: Permitting Telnet access to Catalyst IOS switches

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure a switch to be access remotely via Telnet. By default, you can Telnet to a switch but cannot log in if no password has been set.

Lab Purpose:

Telnet access configuration is a fundamental skill. More often than not, switches are accessed and configured remotely via Telnet. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure a switch to allow an administrator to log in via Telnet.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

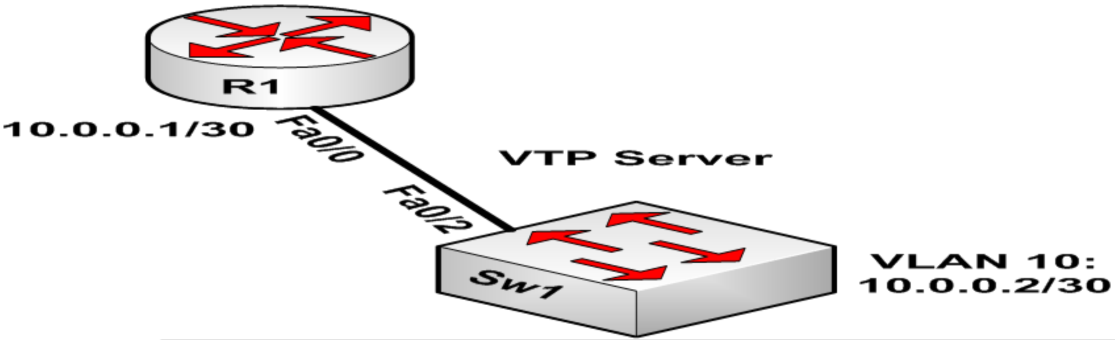
This lab has a difficulty rating of 4/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



VLAN No.	VLAN Name	Interface
10	SALES	FastEthernet0/2

Task 1:

Configure a hostname of Sw1 on your lab switch, and the hostname R1 on the router as illustrated in the topology.

Task 2:

Create VLAN 10 on switch Sw1 and assign port FastEthernet0/2 to this VLAN as an access port.

Task 3:

Configure IP address 10.0.0.1/30 on router R1's FastEthernet0/0 interface, and IP address 10.0.0.2/30 in switch Sw2's VLAN 10 interface. Verify that R1 can ping Sw1 and vice versa.

Task 4:

Configure Telnet access to Sw1 using a password of CISCO. The password is case-sensitive so take that into consideration in your configuration. Verify your configuration by creating a Telnet session from R1.

SOLUTION:

Lab 18 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 3 Configuration and Verification Task 1

Task 2:

For reference information on configuring verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

For reference information on configuring IP interfaces, please refer to:

Lab 3 Configuration and Verification Task 5

For reference information on using standard PING, please refer to:

Lab 15 Configuration and Verification Task

Task 4:

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#line vty 0 15

Sw1(config-line)#password CISCO

Sw1(config-line)#login

Sw1(config-line)#end

Sw1#
```

NOTE: Most people often forget the fact that switches typically have 16 VTY lines (numbered 0-15) unlike routers which typically have 5 VTY lines (numbered 0-4). Take care to remember this when configuring switches as you may leave some lines unsecured if you use line vty 0 4 as on a router.

```
R1#telnet 10.0.0.2

Trying 10.0.0.2 ... Open

User Access Verification

Password:
```

```
Sw1#

Sw1#
```

Lab 19: Configuring passwords on Catalyst switches

Lab Objective:

The objective of this lab exercise is to configure passwords that contain special characters, such as question marks, on switches. By default, the question mark invokes IOS help options for a command.

Lab Purpose:

Advanced password configuration is a fundamental skill. By default, when the question mark (?) is used, the Cisco IOS help menu displays possible options for completing the command being typed. This can become a problem if you want to configure a password such as C?sc0, for example. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure passwords with special characters.

Certification Level:

This lab is suitable for CCNA certification exam preparation.

Lab Difficulty:

This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes.

Lab Topology:

Use any single switch to complete this lab.

Task 1:

Configure an enable password or enable secret of **C?1sc0** on your Catalyst switch. If you find you cannot configure the password, try and remember the keys you need to type in before configuring special characters in a password.

Task 2:

Disable password encryption and verify your password shows up in the configuration as configured.

SOLUTION:

Lab 19 Configuration and Verification

Task 1:

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#enable password C?1sc0

Sw1(config)#end

Sw1#
```

NOTE: In order to use a question mark in a password on Cisco devices, you must type in CTNL/V (the CTRL key followed by the letter v) before you type in the question mark.

Task 2:

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#no service password-encryption

Sw1(config)#end

Sw1#

Sw1#show running-config

Building configuration...

Current configuration : 3093 bytes

!

version 12.1

no service pad

no service password-encryption

!

hostname Sw1

!

no logging console

enable password C?1sc0
```

Lab 20: Configuring back-to-back Serial connections

Lab Objective:

The objective of this lab exercise is to configure back-to-back Serial interfaces between two Cisco routers. By default, router Serial interfaces receive their clocking information from an external device such as a CSU/DSU.

Lab Purpose:

Back-to-back Serial interface configuration is a fundamental skill. Because routers typically receive clocking from an external device such as a CSU/DSU, it is imperative to understand how to bring up a back-to-back Serial connection between two routers to set up your home lab, for example. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure back-to-back Serial connections.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

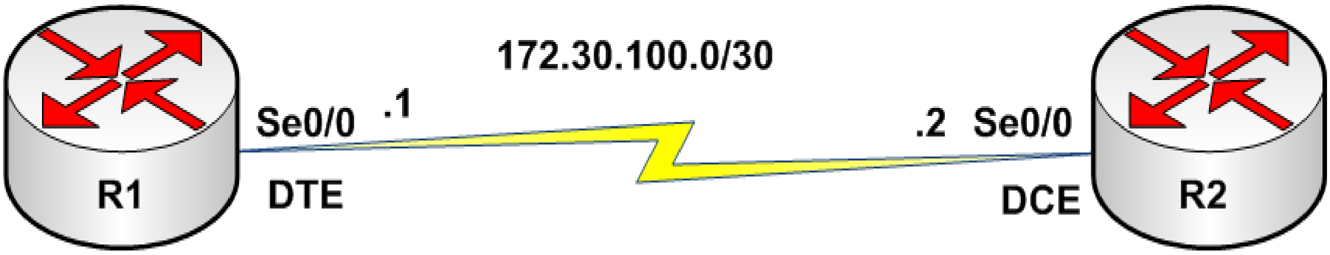
This lab has a difficulty rating of 3/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R2 as illustrated in the topology.

Task 2:

Enable the Serial interfaces on R1 and R2. The Serial0/0 interface on R2 is identified as the DCE in the topology. Use the appropriate show command to verify that this interface is indeed the DCE.

Task 3:

Configure the DCE interface on R2 to providing clocking to R1. The clock speed should be 256Kbps. Remember that 1Kbps = 1000bps. Verify that R1 receives clocking information from R2.

Task 4:

Configure IP addressing on R1 and R2 Serial0/0 interfaces as illustrated in the topology.

Task 5:

Verify your interface status and ping between R1 and R2 to validate connectivity.

SOLUTION:

Lab 20 Configuration and Verification

Task 1:

```
Router#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R1

R1(config)#

Router#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R2

R2(config)#
```

Task 2:

```
R1(config)#interface serial0/0

R1(config-if)#no shut

*Mar  1 00:36:47.282: %LINK-3-UPDOWN: Interface Serial0/0, changed state to down

R1(config-if)#end

R1#

R2(config)#interface serial0/0

R2(config-if)#no shut

*Mar  1 00:36:47.282: %LINK-3-UPDOWN: Interface Serial0/0, changed state to down
```

```
R2(config-if)#end

R2#

R2#show controllers serial 0/0

Interface Serial0/0

Hardware is PowerQUICC MPC860

DCE V.35, no clock
```

NOTE: The show controllers command will tell you whether the interface is the DCE side (which provides the clocking) or the DTE side (which receives the clocking) on a particular router interface.

Task 3:

```
R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#interface serial 0/0

R2(config-if)#clock rate 256000

R2(config-if)#end

R2#

R2#show controllers serial 0/0

Interface Serial0/0

Hardware is PowerQUICC MPC860

DCE V.35, clock rate 256000

R1#show controllers serial 0/2

Interface Serial0/0

Hardware is PowerQUICC MPC860

DTE V.35 TX and RX clocks detected.
```

Task 4:

```
R1#conf term

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#interface s0/0
```

```
R1(config-if)#ip address 172.30.100.1 255.255.255.252

R1(config-if)#end

R1#

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#interface serial 0/0

R2(config-if)#ip address 172.30.100.2 255.255.255.252

R2(config-if)#end

R2#
```

Task 5:

```
R1#show ip interface brief

Interface              IP-Address      OK? Method Status   Protocol

Serial0/0              172.30.100.1    YES manual up         up

R1#ping 172.30.100.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.30.100.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/12 ms

R2#show  ip interface brief

Interface              IP-Address      OK? Method Status  Protocol

Serial0/0              172.30.100.2    YES manual up        up

R2#ping 172.30.100.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.30.100.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/12 ms
```

Lab 21: Verifying Cisco HDLC Encapsulation

Lab Objective:

The objective of this lab exercise is to verify Cisco HDLC encapsulation, which is the default encapsulation method for WAN interfaces on Cisco IOS routers.

Lab Purpose:

Cisco HDLC verification is a fundamental skill. Cisco HDLC encapsulation is the default encapsulation on all Cisco router Serial interfaces. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to verify Cisco HDLC encapsulation.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

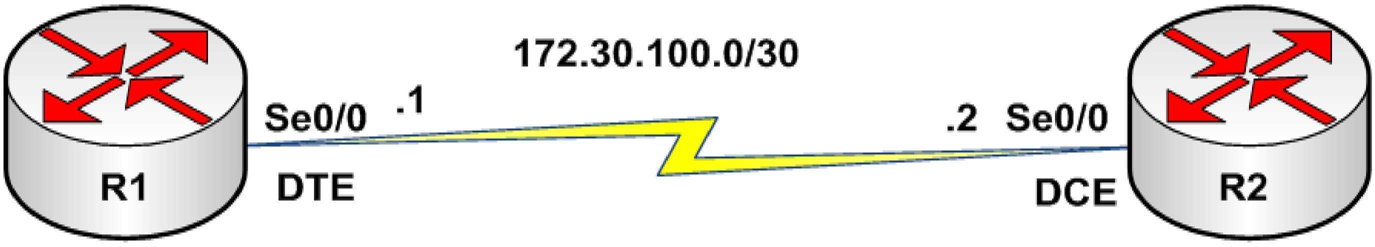
This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R2 as illustrated in the topology.

Task 2:

Enable the Serial interfaces on R1 and R2. The Serial0/0 interface on R2 is identified as the DCE in the topology. Configure the DCE interface on R2 to providing clocking to R1. The clock speed should be 256Kbps. Remember that 1Kbps = 1000bps. Verify that R2 is sending clocking information and that R1 receives this information from R2.

Task 3:

Configure IP addressing on R1 and R2 Serial0/0 interfaces as illustrated in the topology. Verify your interface encapsulation, which should be HDLC by default.

Task 4:

Enable debugging on the Cisco router to validate HDLC keepalive messages are being sent between the two routers. Ensure that you disable debugging when you are complete. Verify that HDLC messages are sent in the keepalive interval that is listed under the interface, which should be approximately every 10 seconds.

SOLUTION:

Lab 21 Configuration and Verification

Task 1:

```
Router#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R1

R1(config)#

Router#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R2

R2(config)#
```

Task 2:

```
R1(config)#interface serial0/0

R1(config-if)#no shut

*Mar  1 00:36:47.282: %LINK-3-UPDOWN: Interface Serial0/0, changed state to down

R1(config-if)#end

R1#

R2(config)#interface serial0/0

R2(config-if)#no shut

*Mar  1 00:36:47.282: %LINK-3-UPDOWN: Interface Serial0/0, changed state to down

R2(config-if)#end

R2#

R2#show controllers serial 0/0

Interface Serial0/0
```

```
Hardware is PowerQUICC MPC860
DCE V.35, no clock
```

NOTE: The show controllers command will tell you whether the interface is the DCE side (which provides the clocking) or the DTE side (which receives the clocking) on a particular router interface.

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface serial 0/0
R2(config-if)#clock rate 256000
R2(config-if)#end
R2#
R2#show controllers serial 0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 256000
R1#show controllers serial 0/2
Interface Serial0/0
Hardware is PowerQUICC MPC860
DTE V.35 TX and RX clocks detected.
```

Task 3:

```
R1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface s0/0
R1(config-if)#ip address 172.30.100.1 255.255.255.252
R1(config-if)#end
R1#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
R2(config)#interface serial 0/0
R2(config-if)#ip address 172.30.100.2 255.255.255.252
R2(config-if)#end
R2#
R1#show interfaces serial 0/0
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 172.30.100.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
R2#show interfaces serial 0/0
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 172.30.100.2/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
```

Task 4:

```
R1#debug serial interface
Serial network interface debugging is on
*Mar  1 01:17:34.686: Serial0/0: HDLC myseq 232, mineseen 232*, yourseen 230, line up
*Mar  1 01:17:44.686: Serial0/0: HDLC myseq 233, mineseen 233*, yourseen 231, line up
*Mar  1 01:17:54.687: Serial0/0: HDLC myseq 234, mineseen 234*, yourseen 232, line up
R1#
```

```
R1#

R1#undebug all

All possible debugging has been turned off
```

Lab 22: Configuring PPP Encapsulation

Lab Objective:

The objective of this lab exercise is to enable PPP encapsulation on Cisco router Serial interfaces and verify the state of the PPP-encapsulated interfaces. This lab also covers debugging PPP links to see the different states of PPP negotiation

Lab Purpose:

PPP configuration and verification is a fundamental skill. PPP is one of the most popular Layer 2 protocols used on WANs. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure and verify PPP encapsulation.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

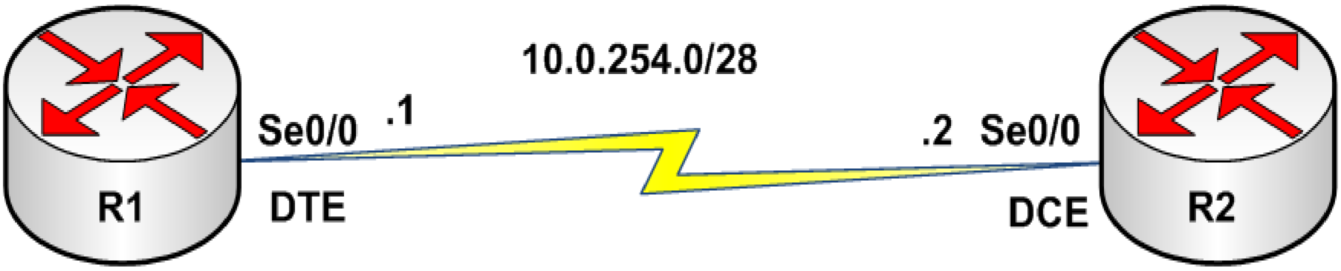
This lab has a difficulty rating of 4/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R2 as illustrated in the topology.

Task 2:

Enable the Serial interfaces on R1 and R2. The Serial0/0 interface on R2 is identified as the DCE in the topology. Use the appropriate show command to verify that this interface is indeed the DCE. Configure the DCE interface on R2 to providing clocking to R1. The clock speed should be 512Kbps. Verify that R1 receives clocking information from R2.

Task 3:

Enable PPP encapsulation on router R1 and R2 Seriaol0/0 interfaces. Configure IP addressing on R1 and R2 Serial0/0 interfaces as illustrated in the topology. Verify your interface encapsulation, which should now be PPP. Test connectivity between R1 and R2 by pinging between the routers over the PPP link.

Task 4:

Enable PPP link negotiation debugging on router R1. Next, issue the shutdown followed by the no shutdown command on Serial0/0. As the interface goes down and comes back up, you should observe the different phases of PPP link negotiation. Disable debugging when you are done.

SOLUTION:

Lab 22 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 20 Configuration and Verification Task 1

Lab 21 Configuration and Verification Task 1

Task 2:

For reference information on verifying DTE/DCE status, please refer to:

Lab 20 Configuration and Verification Task 2

Lab 21 Configuration and Verification Task 2

```
R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#interface serial 0/0

R2(config-if)#clock rate 512000

R2(config-if)#end

R2#

R2#show controllers serial 0/0
```

```
Interface Serial0/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 512000
R1#show controllers serial 0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DTE V.35 TX and RX clocks detected.
```

Task 3:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int s0/2
R1(config-if)#encapsulation ppp
R1(config-if)#ip address 10.0.254.1 255.255.255.240
R1(config-if)#^Z
R1#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface s0/0
R2(config-if)#encapsulation ppp
R2(config-if)#ip add 10.0.254.2 255.255.255.240
R2(config-if)#end
R2#
R1#show interfaces s0/0
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 10.0.254.1/28
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
R1#ping 10.0.254.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.254.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
R2#show interfaces s0/0
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 10.0.254.2/28
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
R2#ping 10.0.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.254.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
```

Task 4:

```
R1#debug ppp negotiation
PPP protocol negotiation debugging is on
R1#conf ter
```

```
Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s0/0

R1(config-if)#shut

*Mar  1 02:00:08.949: %LINK-5-CHANGED: Interface Serial0/0, changed state to administratively down

*Mar  1 02:00:08.949: Se0/0 PPP: Sending Acct Event[Down] id[4]

*Mar  1 02:00:08.949: Se0/0 CDPCP: State is Closed

*Mar  1 02:00:08.949: Se0/0 IPCP: State is Closed

*Mar  1 02:00:08.953: Se0/0 PPP: Phase is TERMINATING

*Mar  1 02:00:08.953: Se0/0 LCP: State is Closed

*Mar  1 02:00:08.953: Se0/0 PPP: Phase is DOWN

*Mar  1 02:00:08.953: Se0/0 IPCP: Remove route to 10.0.254.2

*Mar  1 02:00:09.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to down

R1(config-if)#no shut

*Mar  1 02:00:14.746: Se0/0 PPP: Outbound cdp packet dropped

*Mar  1 02:00:16.746: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up

*Mar  1 02:00:16.746: Se0/0 PPP: Using default call direction

*Mar  1 02:00:16.746: Se0/0 PPP: Treating connection as a dedicated line

*Mar  1 02:00:16.746: Se0/0 PPP: Session handle[A7000001] Session id[2]

*Mar  1 02:00:16.746: Se0/0 PPP: Phase is ESTABLISHING, Active Open

*Mar  1 02:00:16.750: Se0/0 LCP: O CONFREQ [Closed] id 22 len 10

*Mar  1 02:00:16.750: Se0/0 LCP:    MagicNumber 0x05CC8E89 (0x050605CC8E89)

*Mar  1 02:00:16.750: Se0/0 LCP: I CONFREQ [REQsent] id 2 len 10

*Mar  1 02:00:16.750: Se0/0 LCP:    MagicNumber 0x052E783E (0x0506052E783E)

*Mar  1 02:00:16.754: Se0/0 LCP: O CONFACK [REQsent] id 2 len 10

*Mar  1 02:00:16.754: Se0/0 LCP:    MagicNumber 0x052E783E (0x0506052E783E)

*Mar  1 02:00:16.754: Se0/0 LCP: I CONFACK [ACKsent] id 22 len 10
```

```
*Mar  1 02:00:16.754: Se0/0 LCP:    MagicNumber 0x05CC8E89 (0x050605CC8E89)

*Mar  1 02:00:16.754: Se0/0 LCP: State is Open

*Mar  1 02:00:16.758: Se0/0 PPP: Phase is FORWARDING, Attempting Forward

*Mar  1 02:00:16.758: Se0/0 PPP: Queue IPCP code[1] id[1]

*Mar  1 02:00:16.758: Se0/0 PPP: Discarded CDPCP code[1] id[1]

*Mar  1 02:00:16.762: Se0/0 PPP: Phase is ESTABLISHING, Finish LCP

*Mar  1 02:00:16.762: Se0/0 PPP: Phase is UP

*Mar  1 02:00:16.762: Se0/0 IPCP: O CONFREQ [Closed] id 1 len 10

*Mar  1 02:00:16.762: Se0/0 IPCP:    Address 10.0.254.1 (0x03060A00FE01)

*Mar  1 02:00:16.766: Se0/0 CDPCP: O CONFREQ [Closed] id 1 len 4

*Mar  1 02:00:16.766: Se0/0 PPP: Process pending ncp packets

*Mar  1 02:00:16.766: Se0/0 IPCP: Redirect packet to Se0/2

*Mar  1 02:00:16.766: Se0/0 IPCP: I CONFREQ [REQsent] id 1 len 10

*Mar  1 02:00:16.766: Se0/0 IPCP:    Address 10.0.254.2 (0x03060A00FE02)

*Mar  1 02:00:16.770: Se0/0 IPCP: O CONFACK [REQsent] id 1 len 10

*Mar  1 02:00:16.770: Se0/0 IPCP:    Address 10.0.254.2 (0x03060A00FE02)

*Mar  1 02:00:16.770: Se0/0 CDPCP: I CONFACK [REQsent] id 1 len 4

*Mar  1 02:00:16.774: Se0/0 PPP: Outbound cdp packet dropped

*Mar  1 02:00:16.774: Se0/0 IPCP: I CONFACK [ACKsent] id 1 len 10

*Mar  1 02:00:16.774: Se0/0 IPCP:    Address 10.0.254.1 (0x03060A00FE01)

*Mar  1 02:00:16.774: Se0/0 IPCP: State is Open

*Mar  1 02:00:16.778: Se0/0 IPCP: Install route to 10.0.254.2

*Mar  1 02:00:17.763: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to up

*Mar  1 02:00:18.741: Se0/0 CDPCP: I CONFREQ [ACKrcvd] id 2 len 4

*Mar  1 02:00:18.741: Se0/0 CDPCP: O CONFACK [ACKrcvd] id 2 len 4

*Mar  1 02:00:18.741: Se0/0 CDPCP: State is Open

R1(config-if)#end
```

```
*Mar  1 02:00:25.777: %SYS-5-CONFIG_I: Configured from console by consolee

R1#undebug all

All possible debugging has been turned off
```

Lab 23: PPP Authentication using PAP

Lab Objective:

The objective of this lab exercise is to configure two routers sharing a back-to-back Serial link encapsulated by PPP to authenticate each other using PAP. By default, PPP connections are not authenticated or secured.

Lab Purpose:

PPP PAP authentication configuration is a fundamental skill. One of the main reasons that PPP is so popular is because it has the capability to be secured and devices communicating using PPP can be authenticated. PAP authentication is the least preferred method to secure PPP as it sends usernames and passwords in clear text. However, as a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure PPP PAP authentication.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

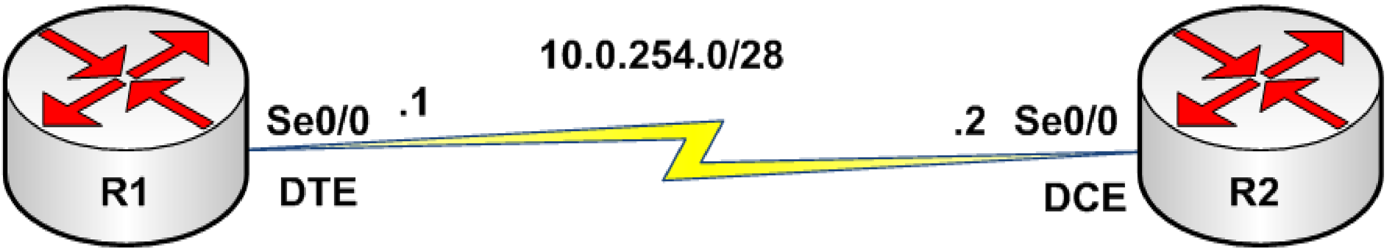
This lab has a difficulty rating of 6/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R2 as illustrated in the topology.

Task 2:

Enable the Serial interfaces on R1 and R2. The Serial0/0 interface on R2 is identified as the DCE in the topology. Use the appropriate commands to verify that this interface is indeed the DCE. Configure the DCE interface on R2 to providing clocking to R1. The clock speed should be 768Kbps. Again, remember that 1Kbps = 1000bps. Verify that R1 receives clocking information from R2.

Task 3:

Enable PPP encapsulation on router R1 and R2 Seriaol0/0 interfaces. Configure IP addressing on R1 and R2 Serial0/0 interfaces as illustrated in the topology.

Task 4:

Verify your interface encapsulation, which should now be PPP. Test connectivity between R1 and R2 by pinging between the routers.

Task 5:

Configure a username on routers R1 and R2. The user account should be the hostname of the remote router which will be authenticating with the local device. For example, on R1 the user account that will be used to authenticate router R2 will be R2. The password on both routers should be **PAP**.

Task 6:

Configure the Serial0/0 interfaces of R1 and R2 for PPP Authentication via PAP. Each router should send its configured hostname as the PAP username and the configured password of PAP should be used for PAP authentication between the routers.

Task 7:

Enable PPP authentication debugging on R1. Next, perform a shutdown followed by a no shutdown on Serial0/0. Verify that you see the two routers authenticating each other via PPP PAP. Disable debugging when you are done.

SOLUTION:

Lab 23 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 20 Configuration and Verification Task 1

Lab 21 Configuration and Verification Task 1

Task 2:

For reference information on verifying DTE/DCE status, please refer to:

Lab 20 Configuration and Verification Task 2

Lab 21 Configuration and Verification Task 2

For reference information on configuring DCE clocking, please refer to:

Lab 20 Configuration and Verification Task 3

Lab 21 Configuration and Verification Task 3

Task 3:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s0/2

R1(config-if)#encapsulation ppp

R1(config-if)#ip address 10.0.254.1 255.255.255.240

R1(config-if)#^Z

R1#

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#interface s0/0

R2(config-if)#encapsulation ppp

R2(config-if)#ip add 10.0.254.2 255.255.255.240

R2(config-if)#end

R2#
```

Task 4:

For reference information on verifying Serial encapsulation, please refer to:

Lab 21 Configuration and Verification Task 5

Lab 22 Configuration and Verification Task 5

Task 5:

```
R1#conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#username R2 password PAP
R1(config)#end
R1#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#username R1 password PAP
R2(config)#^Z
R2#
```

Task 6:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int s0/0
R1(config-if)#ppp authentication pap
R1(config-if)#ppp pap sent-username R1 password PAP
R1(config-if)#^Z
R1#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface serial0/0
R2(config-if)#ppp authentication pap
R2(config-if)#ppp pap sent-username R2 password PAP
R2(config-if)#end
R2#
```

Task 7:

```
R1#debug ppp authentication
```

```
PPP authentication debugging is on

R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s0/0

R1(config-if)#shut

R1(config-if)#

*Mar  1 02:24:04.158: %LINK-5-CHANGED: Interface Serial0/0, changed state to administratively down

*Mar  1 02:24:05.159: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to down

R1(config-if)#no shut

R1(config-if)#

*Mar  1 02:24:14.943: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up

*Mar  1 02:24:14.943: Se0/0 PPP: Using default call direction

*Mar  1 02:24:14.943: Se0/0 PPP: Treating connection as a dedicated line

*Mar  1 02:24:14.943: Se0/0 PPP: Session handle[BC000002] Session id[4]

*Mar  1 02:24:14.943: Se0/0 PPP: Authorization required

*Mar  1 02:24:14.951: Se0/0 PAP: Using hostname from interface PAP

*Mar  1 02:24:14.951: Se0/0 PAP: Using password from interface PAP

*Mar  1 02:24:14.951: Se0/0 PAP: O AUTH-REQ id 2 len 11 from "R1"

*Mar  1 02:24:14.951: Se0/0 PAP: I AUTH-REQ id 2 len 11 from "R2"

*Mar  1 02:24:14.951: Se0/0 PAP: Authenticating peer R2

*Mar  1 02:24:14.955: Se0/0 PPP: Sent PAP LOGIN Request

*Mar  1 02:24:14.955: Se0/0 PPP: Received LOGIN Response PASS

*Mar  1 02:24:14.959: Se0/0 PPP: Sent LCP AUTHOR Request

*Mar  1 02:24:14.959: Se0/0 PPP: Sent IPCP AUTHOR Request

*Mar  1 02:24:14.963: Se0/0 PAP: I AUTH-ACK id 2 len 5
```

```
*Mar  1 02:24:14.963: Se0/0 LCP: Received AAA AUTHOR Response PASS

*Mar  1 02:24:14.963: Se0/0 IPCP: Received AAA AUTHOR Response PASS

*Mar  1 02:24:14.967: Se0/0 PAP: O AUTH-ACK id 2 len 5

*Mar  1 02:24:14.967: Se0/0 PPP: Sent CDPCP AUTHOR Request

*Mar  1 02:24:14.971: Se0/0 PPP: Sent IPCP AUTHOR Request

*Mar  1 02:24:14.975: Se0/0 CDPCP: Received AAA AUTHOR Response PASS

*Mar  1 02:24:15.969: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to up

R1(config-if)#end

*Mar  1 02:24:22.339: %SYS-5-CONFIG_I: Configured from console by console

R1#

R1#undebug all

All possible debugging has been turned off
```

NOTE: By default, PAP sends usernames and passwords in clear text and is generally not considered a secure authentication means for PPP. The recommended and most common means to secure and authenticate via PPP is to use Challenge Handshake Authentication Protocol, or CHAP. In the above debug output, while the password is not shown, we can see the usernames "R1" and "R2" printed.

Lab 24: PPP Authentication using CHAP (Method # 1)

Lab Objective:

The objective of this lab exercise is to configure two routers sharing a back-to-back Serial link encapsulated by PPP to authenticate each other using default CHAP parameters on Cisco IOS. By default, PPP connections are not authenticated or secured.

Lab Purpose:

PPP CHAP authentication configuration is a fundamental skill. One of the main reasons that PPP is so popular is because it has the capability to be secured and devices communicating using PPP can be authenticated. CHAP authentication is the most preferred method to secure PPP as it does not send usernames and passwords in clear text. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure PPP CHAP authentication.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

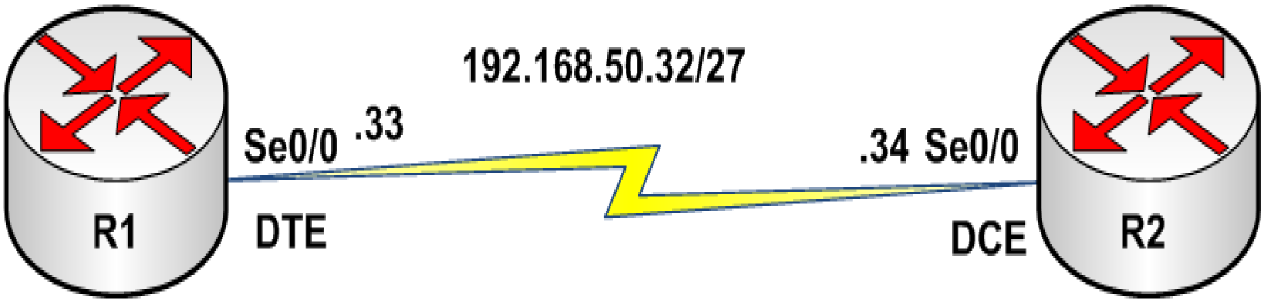
This lab has a difficulty rating of 4/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R2 as illustrated in the topology.

Task 2:

Enable the Serial interfaces on R1 and R2. The Serial0/0 interface on R2 is identified as the DCE in the topology. Use the appropriate command to verify that this interface is indeed the DCE. Configure the DCE interface on R2 to providing clocking to R1. The clock speed should be 768Kbps. Verify that R1 receives clocking information from R2.

Task 3:

Enable PPP encapsulation on router R1 and R2 Serial0/0 interfaces. Configure IP addressing on R1 and R2 Serial0/0 interfaces as illustrated in the topology.

Task 4:

Verify your interface encapsulation, which should now be PPP. Test connectivity between R1 and R2 by pinging between the routers.

Task 5:

Configure the Serial0/0 interfaces of R1 and R2 for PPP Authentication via CHAP. Both R1 and R2 should authenticate using their hostnames and the password **CHAP**.

Task 6:

Enable PPP authentication debugging on R2. Next, perform a shutdown followed by a no shutdown on Serial0/0. Verify that you see the two routers authenticating each other via PPP CHAP. Disable debugging when you are done.

SOLUTION:

Lab 24 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 20 Configuration and Verification Task 1

Lab 21 Configuration and Verification Task 1

Task 2:

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int s0/0
R2(config-if)#clock rate 1000000
R2(config-if)#end
R2#
R2#show contr s0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 1000000
R1#show controllers serial 0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DTE V.35 TX and RX clocks detected.
R1#
```

Task 3:

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int s0/0
R2(config-if)#encapsulation ppp
```

```
R2(config-if)# ip add 192.168.50.34 255.255.255.224

R2(config-if)#end

R2#

R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s0/0

R1(config-if)#encapsulation ppp

R1(config-if)#ip add 192.168.50.33 255.255.255.224

R1(config-if)#end

R1#
```

Task 4:

For reference information on verifying Serial encapsulation, please refer to:

Lab 21 Configuration and Verification Task 5

Lab 22 Configuration and Verification Task 5

```
R1#ping 192.168.50.34

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.50.34, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

R2#ping 192.168.50.33

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.50.33, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
```

Task 5:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.
```

```
R1(config)#username R2 password CHAP

R1(config)#int s0/0

R1(config-if)#ppp authentication chap

R1(config-if)#end

R1#

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#username R1 password CHAP

R2(config)#int s0/0

R2(config-if)#ppp authentication chap

R2(config-if)# ^Z

R2#
```

NOTE: By default, there is no need to configure a hostname to be used for CHAP authentication on Cisco IOS routers as they will use the hostname configured on the router. There is also no need to define a password to be used for authentication since CHAP does not send the passwords across the link like PAP. Therefore, a hash will be created using the configured passwords in the **username** command. These passwords must be identical on both routers, otherwise authentication will fail!

Task 6:

```
R1#debug ppp authentication

PPP authentication debugging is on

R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#interface serial0/0

R1(config-if)#shutdown

*Mar  1 03:04:40.496: %LINK-5-CHANGED: Interface Serial0/0, changed state to
administratively down

*Mar  1 03:04:41.497: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to down

R1(config-if)#no shutdown

*Mar  1 03:04:48.292: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
```

```
*Mar  1 03:04:48.292: Se0/0 PPP: Using default call direction
*Mar  1 03:04:48.292: Se0/0 PPP: Treating connection as a dedicated line
*Mar  1 03:04:48.292: Se0/0 PPP: Session handle[A3000003] Session id[5]
*Mar  1 03:04:48.292: Se0/0 PPP: Authorization required
*Mar  1 03:04:48.300: Se0/0 CHAP: O CHALLENGE id 1 len 23 from "R1"
*Mar  1 03:04:48.300: Se0/0 CHAP: I CHALLENGE id 1 len 23 from "R2"
*Mar  1 03:04:48.304: Se0/0 CHAP: Using hostname from unknown source
*Mar  1 03:04:48.304: Se0/0 CHAP: Using password from AAA
*Mar  1 03:04:48.304: Se0/0 CHAP: O RESPONSE id 1 len 23 from "R1"
*Mar  1 03:04:48.308: Se0/0 CHAP: I RESPONSE id 1 len 23 from "R2"
*Mar  1 03:04:48.308: Se0/0 PPP: Sent CHAP LOGIN Request
*Mar  1 03:04:48.312: Se0/0 PPP: Received LOGIN Response PASS
*Mar  1 03:04:48.312: Se0/0 PPP: Sent LCP AUTHOR Request
*Mar  1 03:04:48.316: Se0/0 PPP: Sent IPCP AUTHOR Request
*Mar  1 03:04:48.316: Se0/0 CHAP: I SUCCESS id 1 len 4
*Mar  1 03:04:48.316: Se0/0 LCP: Received AAA AUTHOR Response PASS
*Mar  1 03:04:48.320: Se0/0 IPCP: Received AAA AUTHOR Response PASS
*Mar  1 03:04:48.320: Se0/0 CHAP: O SUCCESS id 1 len 4
*Mar  1 03:04:48.324: Se0/0 PPP: Sent CDPCP AUTHOR Request
*Mar  1 03:04:48.324: Se0/0 PPP: Sent IPCP AUTHOR Request
*Mar  1 03:04:48.328: Se0/0 CDPCP: Received AAA AUTHOR Response PASS
*Mar  1 03:04:49.322: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to up
R1(config-if)#end
*Mar  1 03:04:55.308: %SYS-5-CONFIG_I: Configured from console by console
R1#undebug all
All possible debugging has been turned off
```

Lab 25: PPP Authentication using CHAP (Method # 2)

Lab Objective:

The objective of this lab exercise is to configure two routers sharing a back-to-back Serial link encapsulated by PPP to authenticate each other using default CHAP parameters on Cisco IOS. By default, PPP connections are not authenticated or secured.

Lab Purpose:

PPP CHAP authentication configuration is a fundamental skill. One of the main reasons that PPP is so popular is because it has the capability to be secured and devices communicating using PPP can be authenticated. CHAP authentication is the most preferred method to secure PPP as it does not send usernames and passwords in clear text. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure PPP CHAP authentication.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

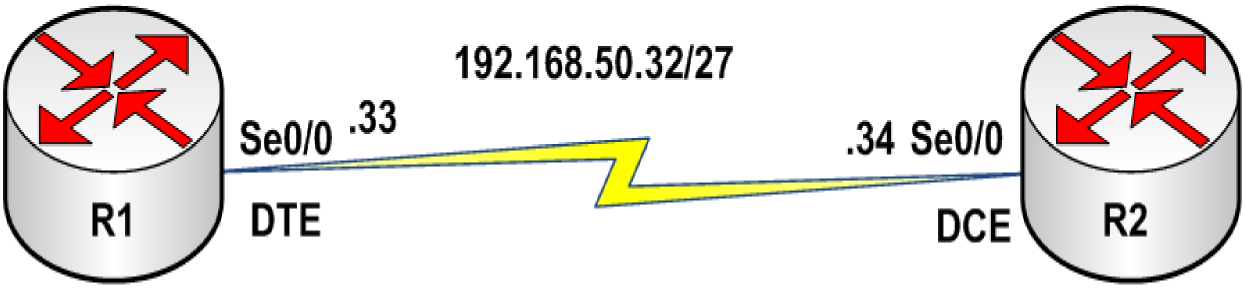
This lab has a difficulty rating of 6/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R2 as illustrated in the topology.

Task 2:

Enable the Serial interfaces on R1 and R2. The Serial0/0 interface on R2 is identified as the DCE in the topology. Use the appropriate show command to verify that this interface is indeed the DCE. Configure the DCE interface on R2 to providing clocking to R1. The clock speed should be 768Kbps. Verify that R1 receives clocking information from R2.

Task 3:

Enable PPP encapsulation on router R1 and R2 Serial0/0 interfaces. Configure IP addressing on R1 and R2 Serial0/0 interfaces as illustrated in the topology.

Task 4:

Verify your interface encapsulation, which should be PPP by default. Test connectivity between R1 and R2 by pinging between the routers.

Task 5:

Configure PPP CHAP authentication on R1 and R2. Configure R1 to use the CHAP username **Router1** with the password **MyPass**. Configure R2 to use the CHAP username **Router2** with the password **MyPass**.

Task 6:

Enable PPP authentication debugging on R1. Next, perform a shutdown followed by a no shutdown on Serial0/0. Verify that you see the two routers authenticating each other via PPP CHAP. Disable debugging when you are done.

SOLUTION:

Lab 25 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 20 Configuration and Verification Task 1

Lab 21 Configuration and Verification Task 1

Task 2:

For reference information on verifying DTE/DCE status, please refer to:

Lab 20 Configuration and Verification Task 2

Lab 21 Configuration and Verification Task 2

For reference information on configuring DCE clocking, please refer to:

Lab 21 Configuration and Verification Task 2

Task 3:

For reference information on enabling PPP encapsulation, please refer to:

Lab 22 Configuration and Verification Task 3

Lab 23 Configuration and Verification Task 3

Task 4:

For reference information on verifying Serial encapsulation, please refer to:

Lab 21 Configuration and Verification Task 5

Lab 22 Configuration and Verification Task 5

```
R1#ping 192.168.50.34

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.50.34, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

R2#ping 192.168.50.33

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.50.33, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
```

Task 5:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s0/0

R1(config-if)#ppp authentication chap

R1(config-if)#ppp chap ?

  hostname  Set alternate CHAP hostname

  password  Set default CHAP password

  refuse    Refuse to authenticate using CHAP

  wait      Wait for caller to authenticate first

R1(config-if)#ppp chap hostname Router1

R1(config-if)#ppp chap password MyPass

R1(config-if)#exit
```

```
R1(config)#username Router2 password MyPass
R1(config)#end
R1#
R2#configure ter
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interf ser 0/0
R2(config-if)#ppp authentication chap
R2(config-if)#ppp chap hostname Router2
R2(config-if)#ppp chap password MyPass
R2(config-if)#exit
R2(config)#username Router1 password MyPass
R2(config)#end
R2#
```

NOTE: By default, there is no need to configure a hostname to be used for CHAP authentication on Cisco IOS routers as they will use the hostname configured on the router. However, to use a different hostname, CHAP must be configured for that. This is performed using the ppp chap hostname and ppp chap password commands on the PPP interface used for CHAP authentication.

Task 6:

```
R2#debug ppp authentication
PPP authentication debugging is on
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int s0/0
R2(config-if)#shut
*Mar  1 03:54:08.805: %LINK-5-CHANGED: Interface Serial0/0, changed state to administratively down
*Mar  1 03:54:09.807: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to down
R2(config-if)#no shut
```

```
*Mar  1 03:54:15.861: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
*Mar  1 03:54:15.861: Se0/0 PPP: Using default call direction
*Mar  1 03:54:15.861: Se0/0 PPP: Treating connection as a dedicated line
*Mar  1 03:54:15.861: Se0/0 PPP: Session handle[D50000E3] Session id[229]
*Mar  1 03:54:15.861: Se0/0 PPP: Authorization required
*Mar  1 03:54:15.869: Se0/0 CHAP: O CHALLENGE id 181 len 28 from "Router2"
*Mar  1 03:54:15.869: Se0/0 CHAP: I CHALLENGE id 181 len 28 from "Router1"
*Mar  1 03:54:15.873: Se0/0 CHAP: Using hostname from interface CHAP
*Mar  1 03:54:15.877: Se0/0 CHAP: Using password from AAA
*Mar  1 03:54:15.877: Se0/0 CHAP: O RESPONSE id 181 len 28 from "Router2"
*Mar  1 03:54:15.877: Se0/0 CHAP: I RESPONSE id 181 len 28 from "Router1"
*Mar  1 03:54:15.881: Se0/0 PPP: Sent CHAP LOGIN Request
*Mar  1 03:54:15.881: Se0/0 PPP: Received LOGIN Response PASS
*Mar  1 03:54:15.885: Se0/0 PPP: Sent LCP AUTHOR Request
*Mar  1 03:54:15.885: Se0/0 PPP: Sent IPCP AUTHOR Request
*Mar  1 03:54:15.885: Se0/0 CHAP: I SUCCESS id 181 len 4
*Mar  1 03:54:15.889: Se0/0 LCP: Received AAA AUTHOR Response PASS
*Mar  1 03:54:15.889: Se0/0 IPCP: Received AAA AUTHOR Response PASS
*Mar  1 03:54:15.889: Se0/0 CHAP: O SUCCESS id 181 len 4
*Mar  1 03:54:15.893: Se0/0 PPP: Sent CDPCP AUTHOR Request
*Mar  1 03:54:15.897: Se0/0 PPP: Sent IPCP AUTHOR Request
*Mar  1 03:54:15.897: Se0/0 CDPCP: Received AAA AUTHOR Response PASS
*Mar  1 03:54:16.895: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to up
R2(config-if)#end
R2#
*Mar  1 03:54:21.114: %SYS-5-CONFIG_I: Configured from console by console
R2#undebug ppp authentication
```

```
PPP authentication debugging is off

R2#
```

Lab 26: Configuring Cisco Frame Relay

Lab Objective:

The objective of this lab exercise is to enable and validate basic Cisco Frame Relay on two routers using Serial interfaces. By default, all Serial interfaces have a default encapsulation type of Cisco HDLC.

Lab Purpose:

Cisco Frame Relay configuration and verification is a fundamental skill. Frame Relay is a Non Broadcast Multi Access technology that is commonly used in hub and spoke topologies. By default, Frame Relay will use Inverse ARP to map a remote IP address to a local DLCI. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure and verify Cisco Frame Relay encapsulation.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 3/10

Readiness Assessment:

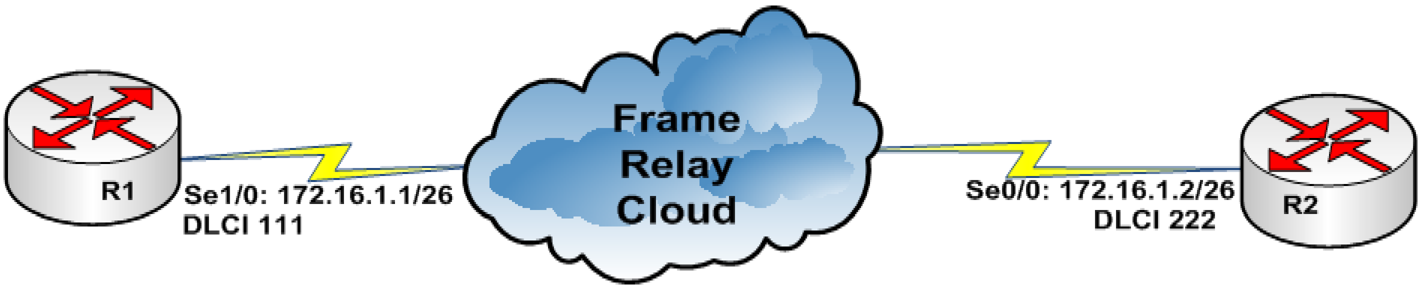
When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

In order to configure Frame Relay between two routers in your lab, you will need THREE routers! The first two routers will be regular routers, and the third will need to be configured as a Frame Relay switch. This can be any Cisco router that has at least two Serial interfaces. Please refer to **Appendix A: Cabling and configuring a Frame Relay Switch For Two Routers** for the appropriate configuration to issue on the Frame Relay switch.

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R2 as illustrated in the topology. Configure IP addresses on R1 and R2 Serial0/0 interfaces as illustrated in the topology.

Task 2:

Enable Cisco Frame Relay on router R1 and R2 Serial1/0 and 0/0 interfaces and verify Cisco Frame Relay encapsulation on the interfaces.

Task 3:

Verify that the Frame Relay DLCIs have been received from the Frame Relay switch. Next, validate that Inverse ARP has been used to dynamically map remote IP addresses to local DLCI values. Finally, test connectivity between R1 and R2 by pinging between the two routers.

SOLUTION:

Lab 26 Configuration and Verification

Task 1:

```
Router#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R1

R1(config)#interf ser1/0

R1(config-if)#ip add 172.16.1.1 255.255.255.192

R1(config-if)#no shut

R1(con

fig-if)#end

R1#

Router#conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#host R2

R2(config)#interface serial 0/0

R2(config-if)#ip address 172.16.1.2 255.255.255.192

R2(config-if)#no shut

R2(config-if)#^Z

R2#
```

Task 2:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s1/0

R1(config-if)#encap frame-relay

R1(config-if)#^Z

R1#

R1#show interfaces serial 1/0

Serial1/0 is up, line protocol is up

  Hardware is PowerQUICC Serial

  Internet address is 172.16.1.1/26

  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,

     reliability 255/255, txload 1/255, rxload 1/255

  Encapsulation FRAME-RELAY, loopback not set

  Keepalive set (10 sec)

  LMI enq sent  50, LMI stat recvd 8, LMI upd recvd 0, DTE LMI up

  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0

  LMI DLCI 1023  LMI type is CISCO  frame relay DTE

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.
```

```
R2(config)#int s0/0

R2(config-if)#encapsulation frame-relay

R2(config-if)#end

R2#

R2#sh int s0/0

Serial0/0 is up, line protocol is up

  Hardware is PowerQUICC Serial

  Internet address is 172.16.1.2/26

  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,

     reliability 255/255, txload 1/255, rxload 1/255

  Encapsulation FRAME-RELAY, loopback not set

  Keepalive set (10 sec)

  LMI enq sent  34, LMI stat recvd 2, LMI upd recvd 0, DTE LMI up

  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0

  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
```

NOTE: By default, Cisco encapsulation is the default Frame Relay encapsulation for Cisco router Frame-Relay enabled Serial interfaces. Therefore, to enable this encapsulation type, the only command required is the encapsulation frame-relay under the Serial interface. Cisco Frame Relay encapsulation uses LMI DLCI 1023 for signaling and defaults to an LMI type of CISCO.

Task 3:

```
R1#show frame-relay pvc

PVC Statistics for interface Serial0/0 (Frame Relay DTE)

              Active  Inactive  Deleted  Static
Local         1       0         0        0
Switched      0       0         0        0
Unused        0       0         0        0

DLCI = 111, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial1/0

  input pkts 12            output pkts 8            in bytes 551

  out bytes 395            dropped pkts 0           in pkts dropped 0

  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0          in BECN pkts 0          out FECN pkts 0

  out BECN pkts 0          in DE pkts 0            out DE pkts 0

  out bcast pkts 1        out bcast bytes 34

  5 minute input rate 0 bits/sec, 0 packets/sec

  5 minute output rate 0 bits/sec, 0 packets/sec

  pvc create time 00:06:30, last time pvc status changed 00:04:30

R2#show frame-relay pvc

PVC Statistics for interface Serial0/0 (Frame Relay DTE)

          Active  Inactive  Deleted  Static
Local       1       0         0        0
Switched    0       0         0        0
Unused      0       0         0        0

DLCI = 222, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0

  input pkts 1            output pkts 1           in bytes 34

  out bytes 34             dropped pkts 0          in pkts dropped 0

  out pkts dropped 0                out bytes dropped 0

  in FECN pkts 0          in BECN pkts 0          out FECN pkts 0

  out BECN pkts 0          in DE pkts 0            out DE pkts 0

  out bcast pkts 1        out bcast bytes 34

  5 minute input rate 0 bits/sec, 0 packets/sec

  5 minute output rate 0 bits/sec, 0 packets/sec

  pvc create time 00:03:55, last time pvc status changed 00:03:45
```

NOTE: Frame Relay DLCI information is provided by the local Frame Relay switch. You do not need to configure DLCI values on router interfaces manually.

```
R1#show frame-relay map

Serial1/0 (up): ip 172.16.1.2 dlci 111(0x6F,0x18F0), dynamic,

              broadcast,, status defined, active

R2#show frame-relay map

Serial0/0 (up): ip 172.16.1.1 dlci 222(0xDE,0x34E0), dynamic,
          broadcast,, status defined, active
```

NOTE: By default, Frame Relay uses Inverse ARP to dynamically map local DLCI values to remote IP addresses on the Frame Relay network. This dynamic mapping is illustrated by the keyword dynamic in the output of the show frame-relay map command. In the output above, the remote IP address on the Serial0/0 interface of either router has been dynamically mapped to the local DLCI value.

```
R1#ping 172.16.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms

R2#ping 172.16.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
```

Lab 27: Configuring IETF Frame Relay

The objective of this lab exercise is to enable and validate basic IETF Frame Relay on two routers using Serial interfaces. The default Frame Relay encapsulation type used by Cisco routers is Cisco Frame Relay encapsulation.

Lab Purpose:

IETF Frame Relay configuration and verification is a fundamental skill. Frame Relay is a Non Broadcast Multi Access technology that is commonly used in hub and spoke topologies. By default, Frame Relay will use Inverse ARP to map a remote IP address to a local DLCI. IETF Frame Relay encapsulation should be used when a non-Cisco Frame Relay switch is being used. When you configure IETF, it is also important to specify a non-Cisco LMI signaling type. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure and verify IETF Frame Relay encapsulation and non-Cisco LMI signaling.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 4/10

Readiness Assessment:

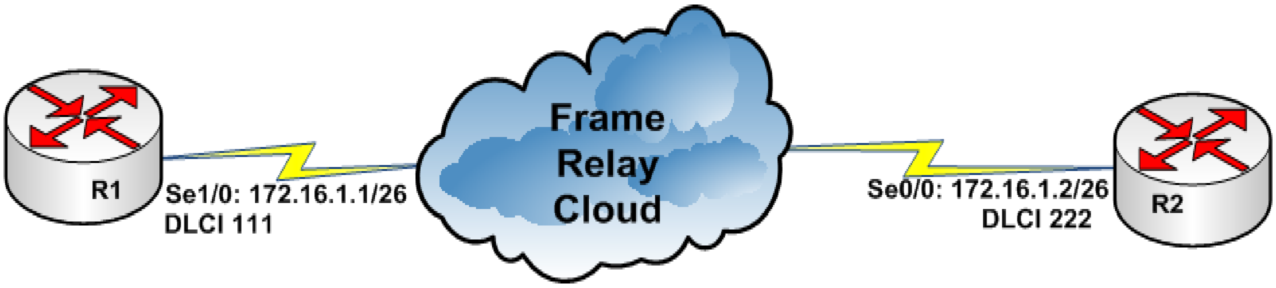
When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

IMPORTANT NOTE:

In order to configure Frame Relay between two routers in your lab, you will need THREE routers! The first two routers will be regular routers, and the third will need to be configured as a Frame Relay switch. This can be any Cisco router that has at least two Serial interfaces. Please refer to **Appendix A: Cabling and configuring a Frame Relay Switch For Two Routers** for the appropriate configuration to issue on the Frame Relay switch.

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R2 as illustrated in the topology. Configure IP addresses on R1 and R2 Serial0/0 interfaces as illustrated in the topology.

Task 2:

Enable IETF Frame Relay on router R1 and R2 Serial1/0 and 0/0 interfaces. In addition to that configure ANSI LMI signaling for the Frame Relay network. Verify IETF Frame Relay encapsulation on the interfaces.

Task 3:

Verify that the Frame Relay DLCIs have been received from the Frame Relay switch.

SOLUTION:

Lab 27 Configuration and Verification

Task 1:

For reference information on configuring hostnames and addresses, please refer to:

Lab 26 Configuration and Verification Task 1

Task 2:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int s1/0
R1(config-if)#encapsulation frame-relay ietf
R1(config-if)#frame-relay lmi-type ansi
R1(config-if)#end
R1#
R1#sh int s1/0
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 172.16.1.1/26
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY IETF, loopback not set
  Keepalive set (10 sec)
  LMI enq sent  178, LMI stat recvd 135, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 0  LMI type is ANSI Annex D  frame relay DTE
R2#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface serial 0/0
```

```
R2(config-if)#encap frame-relay ietf

R2(config-if)#frame-relay lmi-type ansi

R2(config-if)#^Z

R2#

R2#show interfaces serial 0/0

Serial0/0 is up, line protocol is up

  Hardware is PowerQUICC Serial

  Internet address is 172.16.1.2/26

  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,

     reliability 255/255, txload 1/255, rxload 1/255

  Encapsulation FRAME-RELAY IETF, loopback not set

  Keepalive set (10 sec)

  LMI enq sent  153, LMI stat recvd 119, LMI upd recvd 0, DTE LMI up

  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0

  LMI DLCI 0  LMI type is ANSI Annex D  frame relay DTE
```

NOTE: When IETF Frame Relay has been configured on a Frame Relay interface, the encapsulation type will show up as Encapsulation FRAME-RELAY IETF. In the same regard, when ANSI LMI signaling has been configured on a Frame Relay interface, the LMI type will show up as LMI type is ANSI Annex D. It is also important to note that while the CISCO LMI DLCI is 0, the ANSI (or Q933A) LMI DLCI will always be 0 as shown by the line LMI DLCI 0. Pay attention to these fields for the exam and in the real world. Not everyone will be using Cisco manufactured Frame Relay switches!

```
Active      Inactive  Deleted  Static
Local       0         1        0       0
Switched    0         0        0       0
Unused      0         0        0       0

DLCI = 111, DLCI USAGE = LOCAL, PVC STATUS = INACTIVE, INTERFACE = Serial0/0

  input pkts 246          output pkts 235          in bytes 12591

  out bytes 11266          dropped pkts 0          in pkts dropped 0

  out pkts dropped 0               out bytes dropped 0

  in FECN pkts 0          in BECN pkts 0          out FECN pkts 0

  out BECN pkts 0          in DE pkts 0            out DE pkts 0
  out bcast pkts 3         out bcast bytes 98

  5 minute input rate 0 bits/sec, 0 packets/sec

  5 minute output rate 0 bits/sec, 0 packets/sec

  pvc create time 00:27:41, last time pvc status changed 00:05:51
```

R2#**show frame-relay pvc**

```
PVC Statistics for interface Serial0/0 (Frame Relay DTE)

          Active  Inactive  Deleted  Static
Local     0       1         0        0
Switched  0       0         0        0
Unused    0       0         0        0

DLCI = 222, DLCI USAGE = LOCAL, PVC STATUS = INACTIVE, INTERFACE = Serial0/0

  input pkts 236           output pkts 244          in bytes 11296

  out bytes 12527          dropped pkts 0           in pkts dropped 0

  out pkts dropped 0                out bytes dropped 0

  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0

  out BECN pkts 0          in DE pkts 0             out DE pkts 0

  out bcast pkts 2         out bcast bytes 64

  5 minute input rate 0 bits/sec, 0 packets/sec

  5 minute output rate 0 bits/sec, 0 packets/sec

  pvc create time 00:26:18, last time pvc status changed 00:05:58
```

Lab 28: Configuring Static Frame Relay Maps

Lab Objective:

The objective of this lab exercise is to configure manual Frame Relay statements to map local DLCI values to remote IP addresses. This prevents the use of Inverse ARP and is the recommended way to configure Frame Relay. By default, Frame Relay uses Inverse ARP to map local DLCIs to remote IP addresses.

Lab Purpose:

Static Frame Relay map configuration is a fundamental skill. It is considered poor practice to rely on Inverse ARP to map local DLCIs to remote IP addresses. This default behavior should never be relied upon. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure and verify static Frame Relay maps.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

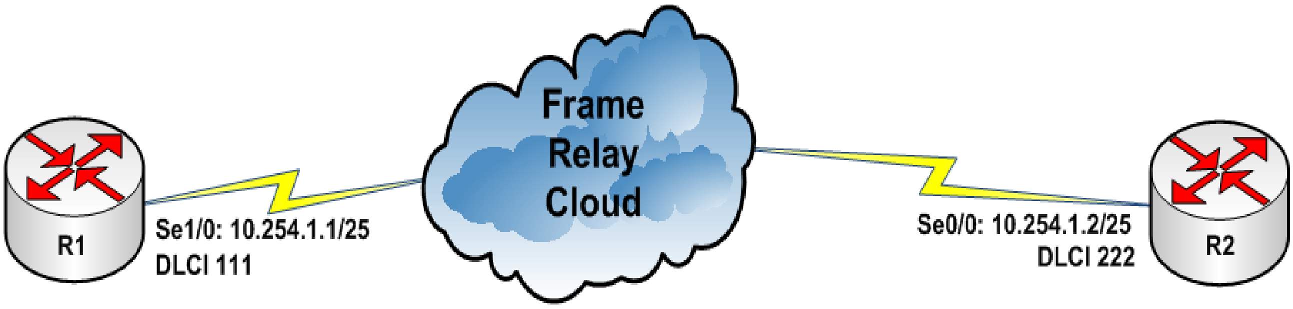
When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

IMPORTANT NOTE:

In order to configure Frame Relay between two routers in your lab, you will need THREE routers! The first two routers will be regular routers, and the third will need to be configured as a Frame Relay switch. This can be any Cisco router that has at least two Serial interfaces. Please refer to **Appendix A: Cabling and configuring a Frame Relay Switch For Two Routers** for the appropriate configuration to issue on the Frame Relay switch.

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R2 as illustrated in the topology. Configure IP addresses on R1 and R2 Serial0/0 interfaces as illustrated in the topology.

Task 2:

Enable Cisco Frame Relay on router R1 and R2 Serial1/0 and 0/0 interfaces. Verify Cisco Frame Relay encapsulation on the interfaces and that the Frame Relay DLCIs have been received from the Frame Relay switch.

Task 3:

Configure static Frame Relay map statements mapping the local DLCIs to the remote IP addresses on both R1 and R2. Verify your static mapping with the appropriate show commands. Finally, ping between R1 and R2 to validate your configuration and confirm IP connectivity between the two routers over the Frame Relay network.

SOLUTION:

Lab 28 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 26 Configuration and Verification Task 1

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s1/0

R1(config-if)#ip add 10.254.1.1 255.255.255.128

R1(config-if)#^Z

R2(config)#int s0/0

R2(config-if)#ip address 10.254.1.2 255.255.255.128

R2(config-if)#end

R2#
```

Task 2:

For reference information on enabling CISCO Frame Relay, please refer to:

Lab 26 Configuration and Verification Task 2

For reference information on verifying Frame Relay DLCIs, please refer to:

Lab 26 Configuration and Verification Task 3

Lab 27 Configuration and Verification Task 3

Task 3:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#interface ser 1/0

R1(config-if)#frame-relay map ip 10.254.1.2 111 broadcast

R1(config-if)#end

R1#

R1#show frame-relay map

Serial0/0 (up): ip 10.254.1.2 dlci 111(0x6F,0x18F0), static,

              broadcast,

              CISCO, status defined, inactive

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#int s0/0

R2(config-if)#frame-relay map ip 10.254.1.1 222 broadcast

R2(config-if)#^Z

R2#

R2#show frame-relay map

Serial0/0 (up): ip 10.254.1.1 dlci 222(0xDE,0x34E0), static,

              broadcast,

              CISCO, status defined, inactive
```

NOTE: Static Frame Relay mapping is the recommended method to map local DLCIs to remote IP addresses. When configuring a static Frame Relay map, specify the remote IP address you want to map to the local DLCI. At the end of the frame-relay map command, for the purposes of the CCNA, it is imperative that you issue the broadcast keyword. This keyword allows the Frame Relay PVC to support Broadcast and Multicast traffic, which it does not by default, because Frame Relay is a Non-Broadcast Multi-Access (NBMA) technology. A static Frame Relay map will always have the static keyword included in the output of the show frame-relay map command. If Broadcast & Multicast support has been enabled via the broadcast keyword in the frame-relay map command, the keyword will also appear in the output of the command frame-relay map as illustrated in the output above.

```
R1#ping 10.254.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.254.1.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms
```

```
R2#ping 10.254.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.254.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms
```

Lab 29: Configuring Frame Relay point-to-point Subinterfaces

Lab Objective:

The objective of this lab exercise is to configure Frame Relay point-to-point subinterfaces, assign DLCIs to these subinterfaces and verify connectivity between two Frame Relay routers. By default, no subinterfaces are configured.

Lab Purpose:

Frame Relay point-to-point subinterface configuration is a fundamental skill. Point-to-point subinterfaces are used between two - and only two - endpoints. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure Frame Relay point-to-point subinterfaces.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 6/10

Readiness Assessment:

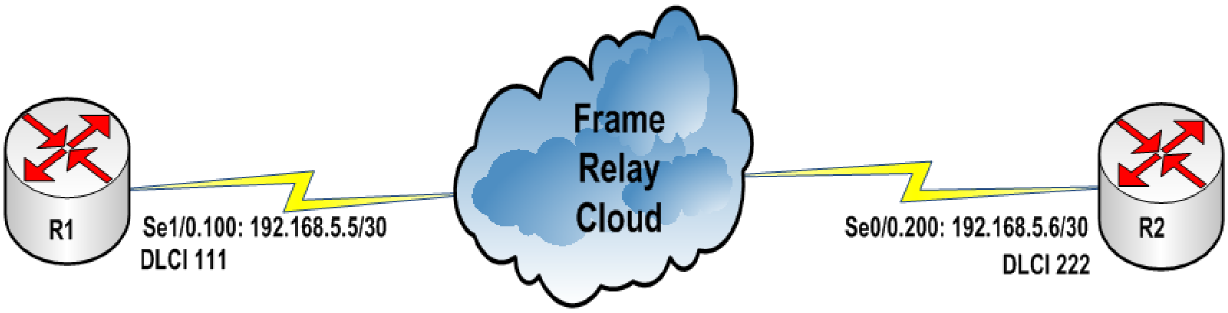
When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

IMPORTANT NOTE:

In order to configure Frame Relay between two routers in your lab, you will need THREE routers! The first two routers will be regular routers, and the third will need to be configured as a Frame Relay switch. This can be any Cisco router that has at least two Serial interfaces. Please refer to **Appendix A: Cabling and configuring a Frame Relay Switch For Two Routers** for the appropriate configuration to issue on the Frame Relay switch.

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R2 as illustrated in the topology. Enable Cisco Frame Relay encapsulation on the Serial1/0 and 0/0 interfaces of routers R1 and R2.

Task 2:

Configure a point-to-point subinterface S1/0.100 on R1 and assign this interface the IP address 192.168.5.5/30 and DLCI 111. Configure a point-to-point subinterface S0/0.200 on R2 and assign this interface the IP address 192.168.5.6/30 and DLCI 222.

Task 3:

Verify that the correct Frame Relay mapping for these DLCIs has been created and then test connectivity between R1 and R2 by pinging between the two routers over the Frame Relay network.

SOLUTION:

Lab 29 Configuration and Verification

Task 1:

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host R1
R1(config)#interface s1/0
R1(config-if)#encapsulation frame-relay
R1(config-if)#^Z
R1#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#int s0/0
R2(config-if)#encap frame-relay
R2(config-if)#end
R2#
```

Task 2:

```
R1#configure te
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int s1/0.100 ?
  multipoint      Treat as a multipoint link
  point-to-point  Treat as a point-to-point link
```

NOTE: Notice that you have the option of configuring either a multipoint subinterface or a point-to-point subinterface when configuring Frame Relay subinterfaces. In this case, we want point-to-point.

```
R1(config)#int s1/0.100 point-to-point
R1(config-subif)#ip address 192.168.5.5 255.255.255.252
```

```
R1(config-subif)#frame-relay interface-dlci 111

R1(config-fr-dlci)#end

R1#
```

NOTE: Also notice that we assign a DLCI to a point-to-point subinterface using the frame-relay interface-dlci command. You cannot use the frame-relay map command on a point-to-point subinterface. However, you can use the frame-relay interface-dlci command on a multipoint subinterface or physical interface. Multipoint subinterfaces behave and are configured in the same manner as physical interfaces.

```
R1#show ip interface brief

Interface                IP-Address      OK? Method Status   Protocol

Serial1/0                unassigned      YES manual  up       up

Serial1/0.100            192.168.5.5     YES manual  up       up

R2#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#interface serial 0/0.200 point-to-point

R2(config-subif)#ip address 192.168.5.6 255.255.255.252

R2(config-subif)#frame-relay interface-dlci 222

R2(config-fr-dlci)#^Z

R2#

R2#sh ip int bri

Interface                IP-Address      OK? Method Status Protocol

Serial0/0                unassigned      YES manual  up       up

Serial0/0.200            192.168.5.6     YES manual  up       up
```

Task 3:

```
R1#show frame-relay map

Serial1/0.100 (up): point-to-point dlci, dlci 111(0x6F,0x18F0), broadcast

          status defined, active

R1#ping 192.168.5.6

Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.5.6, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms

R2#show frame-relay map

Serial0/0.200 (up): point-to-point dlci, dlci 222(0xDE,0x34E0), broadcast

          status defined, active

R2#ping 192.168.5.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.5.5, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms
```

NOTE: Notice that unlike the output of the show frame-relay map command when using Inverse ARP or static DLCI mapping on physical interfaces, the same output does not provide the IP address mapped to the remote end for point-to-point subinterfaces. This is because there can only be two end points on a point-to-point connection unlike a physical or multipoint connection that can have more than two. Also notice that, by default, Broadcast and Multicast capabilities are enabled for the DLCIs.

Lab 30: Configuring Frame Relay Multipoint Subinterfaces

Lab Objective:

The objective of this lab exercise is to configure Frame Relay multipoint subinterfaces, assign DLCIs to these subinterfaces and verify connectivity between two Frame Relay routers. By default, no subinterfaces are configured.

Lab Purpose:

Frame Relay multipoint subinterface configuration is a fundamental skill. Multipoint subinterfaces behave and act in the same manner as physical interfaces. They can be used between two or more endpoints, such as in a hub and spoke topology. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure Frame Relay multipoint subinterfaces.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 6/10

Readiness Assessment:

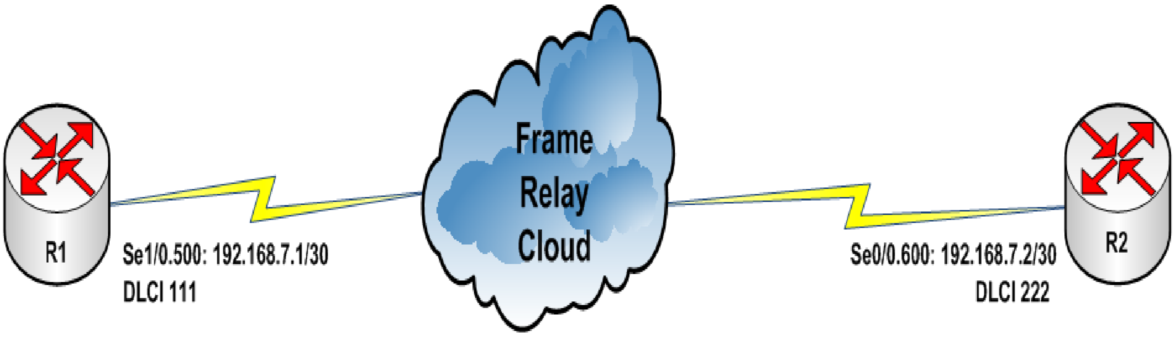
When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

IMPORTANT NOTE:

In order to configure Frame Relay between two routers in your lab, you will need THREE routers! The first two routers will be regular routers, and the third will need to be configured as a Frame Relay switch. This can be any Cisco router that has at least two Serial interfaces. Please refer to **Appendix A: Cabling and configuring a Frame Relay Switch For Two Routers** for the appropriate configuration to issue on the Frame Relay switch.

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R2 as illustrated in the topology. Enable Cisco Frame Relay encapsulation on the Serial0/0 and 1/0 interfaces of routers R1 and R2.

Task 2:

Configure a multipoint subinterface S1/0.500 on R1 and assign this interface the IP address 192.168.7.1/30 and DLCI 111. Configure a multipoint subinterface S0/0.600 on R2 and assign this interface the IP address 192.168.7.2/30 and DLCI 222.

Task 3:

Verify Frame Relay mapping for these DLCIs and test connectivity between R1 and R2 by pinging between the two routers over the Frame Relay network.

SOLUTION:

Lab 30 Configuration and Verification

Task 1:

```
Router#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#host R1

R1(config)#interface s1/0

R1(config-if)#encapsulation frame-relay

R1(config-if)#^Z

R1#

Router#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R2

R2(config)#int s0/0

R2(config-if)#encap frame-relay

R2(config-if)#end

R2#
```

Task 2:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s1/0.500 multipoint

R1(config-subif)#ip add 192.168.7.1 255.255.255.252

R1(config-subif)#frame-relay map ip 192.168.7.2 111 broadcast

R1(config-subif)#end

R1#

R1#show ip interface brief

Interface                  IP-Address      OK? Method Status                Protocol
```

```
Serial1/0              unassigned      YES manual up                 up
Serial1/0.500          192.168.7.1     YES manual up                 up
```

NOTE: Notice that the Serial1/0.500 subinterface is configured with the frame-relay map ip command in the same manner that a physical interface would be configured. Keep this in mind.

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int serial 0/0.600 multipoint
R2(config-subif)#ip address 192.168.7.2 255.255.255.252
R2(config-subif)#frame-relay map ip 192.168.7.1 222 broadcast
R2(config-subif)#end
R2#
R2#sh ip int brief
Interface              IP-Address      OK? Method Status             Protocol
Serial0/0              unassigned      YES manual up                 up
Serial0/0.600          192.168.7.2     YES manual up                 up
```

Task 3:

For reference information on verifying Frame Relay mapping, please refer to:

Lab 26 Configuration and Verification Task 3

Lab 27 Configuration and Verification Task 3

```
R1#ping 192.168.7.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms
R2#ping 192.168.7.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.1, timeout is 2 seconds:
```

```
!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms
```

Lab 31: Configuring Static Routing via Interfaces

Lab Objective:

The objective of this lab exercise is to configure static routes via Ethernet interfaces connected to a switch on two routers. This lab also goes through the validation of the configured static routes.

Lab Purpose:

Static route configuration is a fundamental skill. There are several methods to configure static routes on a Cisco router, and each way has its pros and cons. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure static routes via any of the methods available in Cisco IOS.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

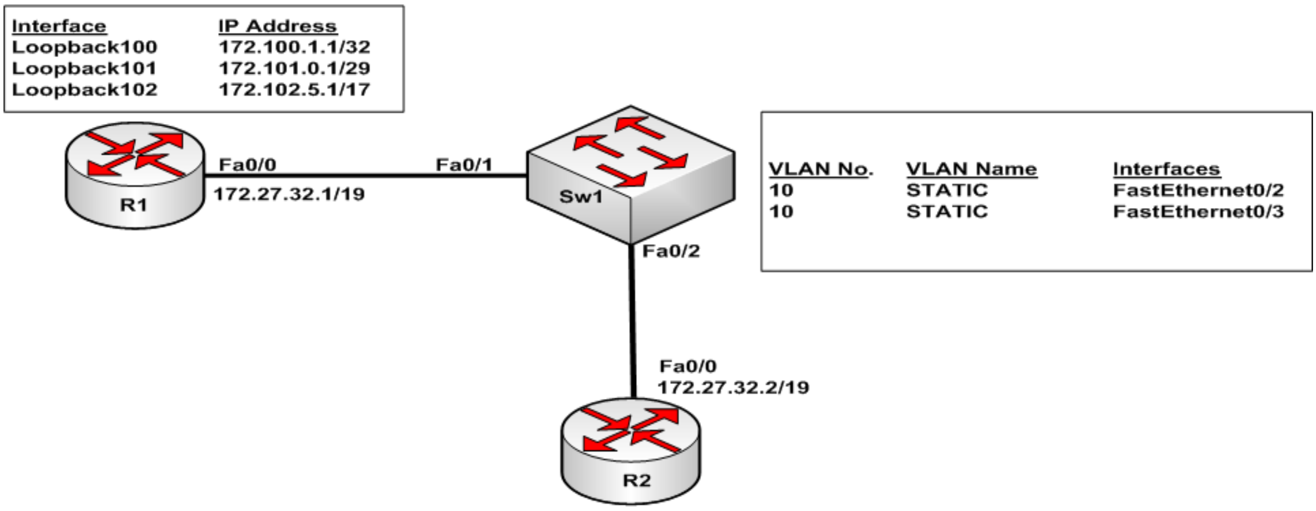
This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Interface	IP Address
Loopback100	172.100.1.1/32
Loopback101	172.101.0.1/29
Loopback102	172.102.5.1/17

VLAN No.	VLAN Name	Interfaces
10	STATIC	FastEthernet0/2
10	STATIC	FastEthernet0/3

Task 1:

Configure the hostnames on routers R1, R2, and Sw1 as illustrated in the topology.

Task 2:

Configure Sw2 as a VTP server and configure VLAN 10 named STATIC. Assign ports FastEthernet0/1 and FastEthernet0/2 to this VLAN.

Task 3:

Configure IP addresses 172.27.32.1/19 and 172.27.32.2/19 on R1 and R2 Fa0/0 interfaces respectively. In addition to that configure the Loopback interfaces on R1 with the IP addresses listed in the topology.

Task 4:

Configure static routes via the FastEthernet0/0 interface on R2 to all the subnets configured on the Loopback addresses configured on R1. Verify your static route configuration with appropriate commands. Ping each Loopback interface configured on R1 from R2 to validate your static route configuration.

SOLUTION:

Lab 31 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 20 Configuration and Verification Task 1

Lab 21 Configuration and Verification Task 1

Task 2:

For reference information on configuring standard VLANs, please refer to:

Lab 2 Configuration and Verification Task 2

Lab 3 Configuration and Verification Task 1

Task 3:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int fastether 0/0

R1(config-if)#ip address 172.27.32.1 255.255.224.0

R1(config-if)#no shutdown
```

```
R1(config-if)#end

R1#

R1#show ip interface brief

Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0            172.27.32.1     YES manual up                    up

R2#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#int fa0/0

R2(config-if)#ip add 172.27.32.2 255.255.224.0

R2(config-if)#no shu

R2(config-if)#^Z

R2#sh ip int brie

Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0            172.27.32.2     YES manual up                    up

R1#ping 172.27.32.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.27.32.2, timeout is 2 seconds:

.!!!!

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

R2#ping 172.27.32.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.27.32.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#interface loopback 100
```

```
R1(config-if)#ip address 172.100.1.1 255.255.255.255

R1(config-if)#exit

R1(config)#interface loopback 101

R1(config-if)#ip address 172.101.0.1 255.255.255.248

R1(config-if)#exit

R1(config)#interface loopback 102

R1(config-if)#ip address 172.102.5.1 255.255.128.0

R1(config-if)#^Z

R1#

R1#show ip interface brief

Interface              IP-Address      OK? Method Status              Protocol

FastEthernet0/0           172.27.32.1     YES manual up                  up

Loopback100               172.100.1.1     YES manual up                  up

Loopback101               172.101.0.1     YES manual up                  up

Loopback102               172.102.5.1     YES manual up                  up
```

NOTE: By default, Loopback interfaces will be enabled once you configure them. Therefore, there is no need to issue the no shutdown command when creating Loopbacks.

Task 4:

```
R2#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#ip route 172.100.1.1 255.255.255.255 fastethernet0/0

R2(config)#ip route 172.101.0.0 255.255.255.248 fastethernet0/0

R2(config)#ip route 172.102.0.0 255.255.128.0 fastethernet0/0

R2(config)#end

R2#

R2#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     172.102.0.0/17 is subnetted, 1 subnets
S       172.102.0.0 is directly connected, FastEthernet0/0
     172.100.0.0/32 is subnetted, 1 subnets
S       172.100.1.1 is directly connected, FastEthernet0/0
     172.101.0.0/29 is subnetted, 1 subnets
S       172.101.0.0 is directly connected, FastEthernet0/0
     172.27.0.0/19 is subnetted, 1 subnets
C       172.27.32.0 is directly connected, FastEthernet0/0
```

NOTE: The S in front of the route indicates that this is a static route as stated in the legend or key immediately following the show ip route command.

```
R2#sh ip route 172.100.1.1
Routing entry for 172.100.1.1/32
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly connected, via FastEthernet0/0
      Route metric is 0, traffic share count is 1
R2#sh ip route 172.101.0.1
Routing entry for 172.101.0.0/29
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly connected, via FastEthernet0/0
      Route metric is 0, traffic share count is 1
```

```
R2#sh ip route 172.102.5.1
Routing entry for 172.102.0.0/17
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly connected, via FastEthernet0/0
      Route metric is 0, traffic share count is 1
R2#ping 172.100.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.100.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/4/4 ms
R2#ping 172.101.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.101.0.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/4/4 ms
R2#ping 172.102.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.102.5.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/4/4 ms
```

NOTE: The first ping packet will always fail because of ARP resolution. Subsequent ping packets will pass.

Lab 32: Configuring Static Routing via IP addresses

Lab Objective:

The objective of this lab exercise is to configure static routes via next hop IP addresses on interfaces connected to a switch on two routers. This lab also goes through the validation of the configured static routes.

Lab Purpose:

Static route configuration is a fundamental skill. There are several methods to configure static routes on a Cisco router, and each way has its pros and cons. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure static routes via any of the methods available in Cisco IOS.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

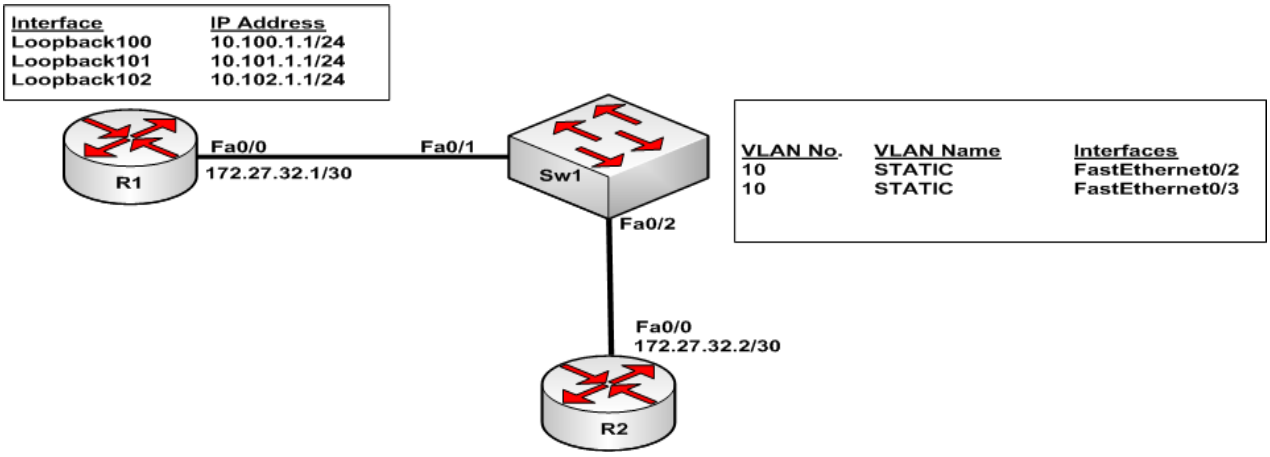
This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Interface	IP Address
Loopback100	10.100.1.1/24
Loopback101	10.101.1.1/24
Loopback102	10.102.1.1/24

VLAN No.	VLAN Name	Interfaces
10	STATIC	FastEthernet0/2
10	STATIC	FastEthernet0/3

Task 1:

Configure the hostnames on routers R1, R2, and Sw1 as illustrated in the topology.

Task 2:

Configure Sw2 as a VTP sever and configure VLAN 10 named STATIC. Assign ports FastEthernet0/1 and FastEthernet0/2 to this VLAN.

Task 3:

Configure IP addresses 172.27.32.1/30 and 172.27.32.2/30 on R1 and R2 Fa0/0 interfaces respectively. In addition to that configure the Loopback interfaces on R1 with the IP addresses in the topology.

Task 4:

Configure static routes via the next hop IP address of 172.27.32.1 on R2 to all the subnets configured on the Loopback addresses previously configured on R1. Verify your static route configuration. Ping each Loopback interface configured on R1 from R2 to validate your static route configuration.

SOLUTION:

Lab 32 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 20 Configuration and Verification Task 1

Lab 21 Configuration and Verification Task 1

Task 2:

For reference information on configuring standard VLANs, please refer to:

Lab 2 Configuration and Verification Task 2

Lab 3 Configuration and Verification Task 1

Task 3:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int fastether 0/0

R1(config-if)#ip address 172.27.32.1 255.255.255.252

R1(config-if)#no shutdown

R1(config-if)#end

R1#
```

```
R1#show ip interface brief

Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0            172.27.32.1     YES manual up                    up

R2#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#int fa0/0

R2(config-if)#ip add 172.27.32.2 255.255.255.252

R2(config-if)#no shu

R2(config-if)#^Z

R2#sh ip int brie

Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0            172.27.32.2     YES manual up                    up

R1#ping 172.27.32.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.27.32.2, timeout is 2 seconds:

.!!!!

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

R2#ping 172.27.32.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.27.32.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int loop 100

R1(config-if)#ip add 10.100.1.1 255.255.255.0

R1(config-if)#exit
```

```
R1(config)#int loop 101

R1(config-if)#ip add 10.101.1.1 255.255.255.0

R1(config-if)#exit

R1(config)#int loop 102

R1(config-if)#ip add 10.102.1.1 255.255.255.0

R1(config-if)#^Z

R1#

R1#sh ip int bri

Interface              IP-Address      OK? Method Status             Protocol

FastEthernet0/0            172.27.32.1     YES manual up                 up

Loopback100                10.100.1.1      YES manual up                 up

Loopback101                10.101.1.1      YES manual up                 up

Loopback102                10.102.1.1      YES manual up                 up
```

Task 4:

```
R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#ip route 10.100.1.0 255.255.255.0 172.27.32.1

R2(config)#ip route 10.101.1.0 255.255.255.0 172.27.32.1

R2(config)#ip route 10.102.1.0 255.255.255.0 172.27.32.1

R2(config)#end

R2#

R2#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.27.0.0/30 is subnetted, 1 subnets
C       172.27.32.0 is directly connected, FastEthernet0/0
     10.0.0.0/24 is subnetted, 3 subnets
S       10.102.1.0 [1/0] via 172.27.32.1
S       10.101.1.0 [1/0] via 172.27.32.1
S       10.100.1.0 [1/0] via 172.27.32.1
R2#ping 10.100.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R2#ping 10.101.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.101.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R2#ping 10.102.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.102.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

NOTE: Notice the difference in this ping versus the one where we used an interface as the next hop for static routing. Because an IP address has been specified, there is no ARP timeout for the first packet since the next hop Layer 3 address has been specified.

Lab 33: Configuring and Naming Static Routes

Lab Objective:

The objective of this lab exercise is to configure named static routes via next hop IP addresses on interfaces connected to a switch on two routers. This lab also goes through the validation of the configured static routes.

Lab Purpose:

Static route configuration is a fundamental skill. There are several methods to configure static routes on a Cisco router, and each way has its pros and cons. Naming the static routes allows you to easily identify what each static route is used for as you view the router configuration. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure named static routes via any of the methods available in Cisco IOS.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

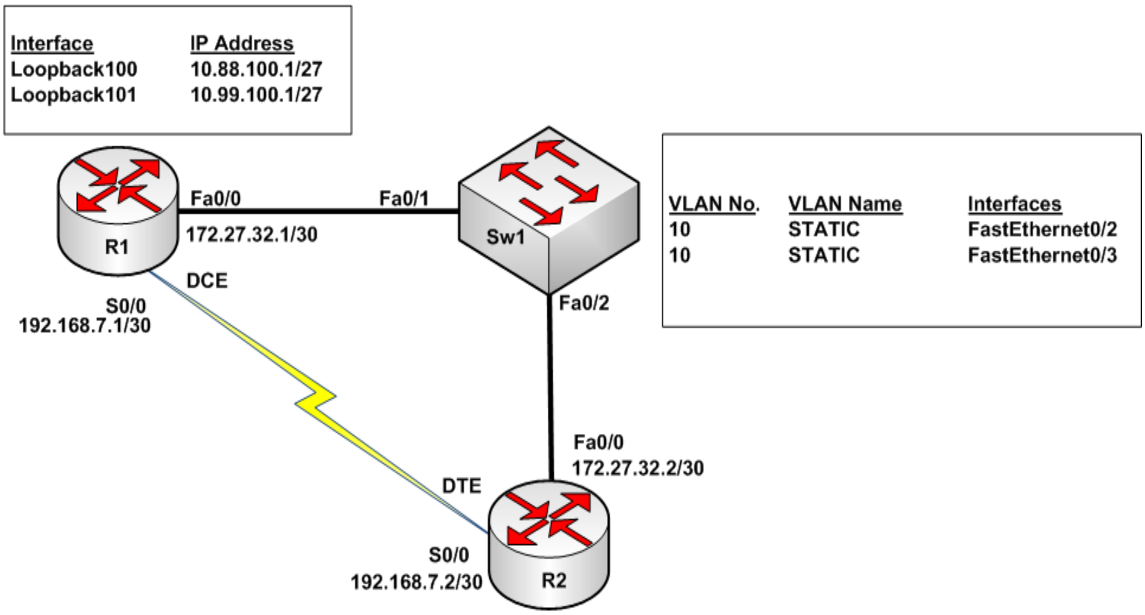
This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Interface	IP Address
Loopback100	10.88.100.1/27
Loopback101	10.99.100.1/27

VLAN No.	VLAN Name	Interfaces
10	STATIC	FastEthernet0/2
10	STATIC	FastEthernet0/3

Task 1:

Configure the hostnames on routers R1 and R2, as well as Sw1 as illustrated in the topology.

Task 2:

Configure Sw2 as a VTP sever and configure VLAN 10 named STATIC. Assign ports FastEthernet0/1 and FastEthernet0/2 to this VLAN. Configure the DCE interface Serial0/0 in R1 to provide clocking to R2 at a clock speed of 768Kbps.

Task 3:

Configure IP addresses 172.27.32.1/30 and 172.27.32.2/30 on R1 and R2 Fa0/0 interfaces respectively. Configure IP addresses 192.168.7.1/30 and 192.168.7.2/30 on R1 and R2 S0/0 interfaces respectively. In addition to that configure the Loopback interfaces on R1 with the IP addresses in the topology.

Task 4:

Configure a static route named LAN-ROUTE on R2 via interface FastEthernet0/0 with a next hop IP address of 172.27.32.1 to the 10.88.100.0/27 subnet. Configure a static route named WAN-ROUTE on R2 via Serial0/0 with a next hop IP address of 192.168.7.1 to the 10.99.100.0/27 subnet. Verify your static route configuration.

Task 5:

Ping each Loopback interface configured on R1 from R2 to verify your static route configuration.

SOLUTION:

Lab 33 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 20 Configuration and Verification Task 1

Lab 21 Configuration and Verification Task 1

Task 2:

For reference information on configuring standard VLANs, please refer to:

Lab 2 Configuration and Verification Task 2

Lab 3 Configuration and Verification Task 1

For reference information on verifying DTE/DCE status, please refer to:

Lab 20 Configuration and Verification Task 2

Lab 21 Configuration and Verification Task 2

For reference information on configuring DCE clocking, please refer to:

Lab 20 Configuration and Verification Task 3

Lab 21 Configuration and Verification Task 3

Lab 21 Configuration and Verification Task 2

Task 3:

For reference information on configuring IP interfaces, please refer to:

Lab 3 Configuration and Verification Task 5

Lab 31 Configuration and Verification Task 3

Task 4:

```
R2(config)#ip route 10.88.100.0 255.255.255.224 fa 0/0 172.27.32.1 name LAN-ROUTE

R2(config)#ip route 10.99.100.0 255.255.255.224 se 0/0 192.168.7.1 name WAN-ROUTE

R2(config)#end

R2#

R2#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

       ia - IS-IS inter area, * - candidate default, U - per-user static route

       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.27.0.0/24 is subnetted, 1 subnets

C       172.27.32.0 is directly connected, FastEthernet0/0

     10.0.0.0/27 is subnetted, 2 subnets

S       10.88.100.0 [1/0] via 172.27.32.1, FastEthernet0/0

S       10.99.100.0 [1/0] via 192.168.7.1, Serial0/0

     192.168.7.0/30 is subnetted, 1 subnets
```

```
C       192.168.7.0 is directly connected, Serial0/0
```

NOTE: The names configured on the static routes do not show in the output of the show ip route command. However, they do show in the running configuration. Naming static routes allows you to easily identify what configured static routes are being used for. This can be extremely helpful in a router where you have many static routes configured. You can simply issue the show run command and filter the output to include only statements that contain the word route as illustrated below.

```
R2#show running-config | include route
ip route 10.88.100.0 255.255.255.224 Ethernet0/0 172.27.32.1 name LAN-ROUTE
ip route 10.99.100.0 255.255.255.224 Serial0/0 192.168.7.1 name WAN-ROUTE
```

Task 5:

For reference information on how to ping, refer to the following:

Lab 32 Configuration and Verification Task 5

Lab 34: Configuring Default Static Routes

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure default static routes on Cisco IOS routers. By default, no default routes exist on Cisco IOS routers.

Lab Purpose:

Static default route configuration is a fundamental skill. Default routes are used to forward traffic to destinations where the router does not have a specific route to in its routing table. They can also be used to forward all external traffic (such as Internet traffic) to an Internet Service Provider, for example. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure static default routes.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 6/10

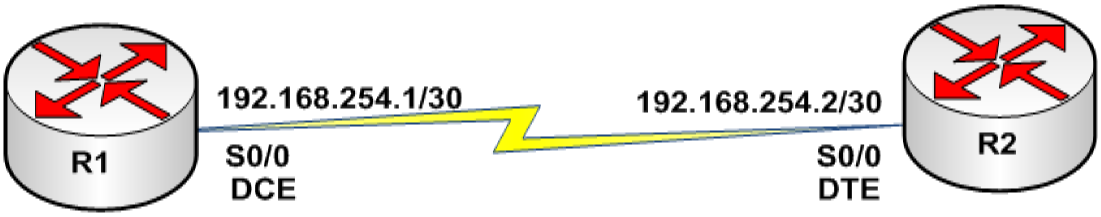
Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:

Interface	IP Address
Loopback100	172.18.0.1/23
Loopback101	10.100.100.1/26
Loopback102	192.168.30.1/29



Task 1:

Configure the hostnames on routers R1 and R2 as illustrated in the topology.

Task 2:

Configure a back-to-back Serial connection between R1 and R2 using PPP encapsulation. Configure the DCE interface Serial0/0 in R1 to provide clocking to R2 at a clock speed of 256Kbps.

Task 3:

Configure IP addresses 192.168.254.1/30 and 192.168.254.2/30 on R1 and R2 Serial0/0 interfaces respectively. Configure the Loopback interfaces on R1 with the IP addresses illustrated in the topology.

Task 4:

Configure a static route default route from R2 pointing to R1. Ping each Loopback interface configured on R1 from R2 to verify your static route configuration.

SOLUTION:

Lab 34 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 20 Configuration and Verification Task 1

Lab 21 Configuration and Verification Task 1

Task 2:

```
R1#conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int s0/0
R1(config)#encap ppp
R1(config)#clock rate 256000
R1(config-if)#end
R1#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface ser 0/0
R2(config)#encapsulation ppp
R2(config-if)#^Z
R2#
```

Task 3:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int s0/0
R1(config-if)#ip add 192.168.254.1 255.255.255.252
R1(config-if)#exit
R1(config)#interface loop 100
R1(config-if)#ip address 172.18.0.1 255.255.254.0
R1(config-if)#exit
R1(config)#interface loop 101
R1(config-if)#ip add 10.100.100.1 255.255.255.192
R1(config-if)#exit
R1(config)#int loo 102
R1(config-if)#ip address 192.168.30.1 255.255.255.248
R1(config-if)#^Z
```

```
R1#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int s0/0
R2(config)#encap ppp
R2(config-if)#ip add 192.168.254.2 255.255.255.252
R2(config-if)#end
R2#
R1#ping 192.168.254.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms
R2#ping 192.168.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms
```

Task 4:

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 serial0/0 192.168.254.1
R2(config)#end
R2#
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 192.168.254.1 to network 0.0.0.0
     192.168.254.0/30 is subnetted, 1 subnets
C       192.168.254.0 is directly connected, Serial0/0
     150.1.0.0/24 is subnetted, 1 subnets
C       150.1.1.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 192.168.254.1, Serial0/0
R2#ping 172.18.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.18.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/12/32 ms
R2#ping 10.100.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms
R2#ping 192.168.30.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms
```

Lab 35: Configuring RIP version 2

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure Routing Information Protocol version 2 on a Cisco IOS router.

Lab Purpose:

RIPv2 configuration is a fundamental skill. By default, when RIP is enabled on a Cisco router, both version 1 and version 2 updates are sent and received. Since RIPv1 is considered obsolete because of today's subnetted networks, it is imperative that you know how to enable RIPv2. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure and verify RIPv2.

Certification Level:

This lab is suitable for both CCENT and CCNA certification exam preparation

Lab Difficulty:

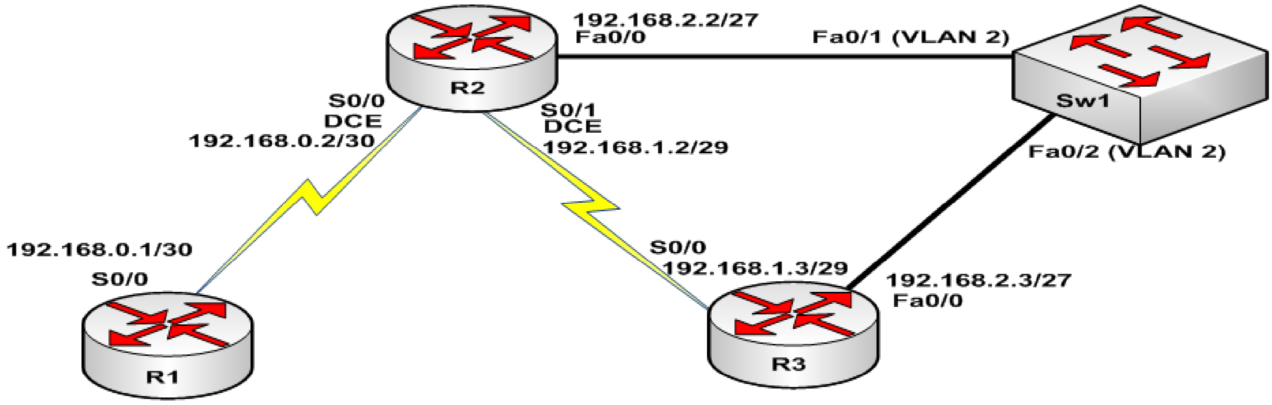
This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Interface	IP Address
Loopback 100	10.10.100.1/27
Loopback 101	10.10.101.1/26

Interface	IP Address
Loopback 100	10.30.100.1/29
Loopback 101	10.30.101.1/25

Task 1:

Configure the hostnames on routers R1 and R2 as illustrated in the topology.

Task 2:

Configure a back-to-back Serial connection between R1 and R2. Configure the DCE interface Serial0/0 in R2 to provide clocking to R1 at a clock speed of 2Mbps. Configure IP addresses 192.168.0.1/30 and 192.168.0.2/30 on R1 and R2 Serial0/0 interfaces respectively. Configure the Loopback interfaces on R1 with the IP addresses illustrated in the topology.

Task 3:

Enable RIPv2 on R1 and configure RIPv2 routing for the Loopback interfaces and the Serial0/0 interface. Verify on either R1 or R2 that RIPv2 has been enabled using the appropriate commands.

SOLUTION:

Lab 35 Configuration and Verification

Task 1:

```
Router#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#host R1

R1(config)#

Router#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#host R2

R2(config)#
```

Task 2:

```
R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#int s0/0

R2(config-if)#clock rate 2000000

R2(config-if)#end

R2#

R2#sh controllers s0/0

Interface Serial0/0

Hardware is PowerQUICC MPC860
```

```
DCE V.35, clock rate 2000000
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int s0/0
R1(config-if)#ip add 192.168.0.1 255.255.255.252
R1(config-if)#no shutdown
R1(config)#int loo 100
R1(config-if)#ip add 10.10.100.1 255.255.255.224
R1(config-if)#exit
R1(config)#int loo 101
R1(config-if)#ip add 10.10.101.1 255.255.255.192
R1(config-if)#end
R1#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int s0/0
R2(config-if)#ip address 192.168.0.2 255.255.255.252
R1(config-if)#no shutdown
R2(config-if)#end
R2#
R1#ping 192.168.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R2#ping 192.168.0.1
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

Task 3:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 10.0.0.0
R1(config-router)#network 192.168.0.0
R1(config-router)#end
R1#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.0.0
R2(config-router)#end
R2#
```

NOTE: When configuring RIP routing, you must use the version 2 keyword under RIP configuration mode. By default, if RIP is enabled and this keyword is not issued, the Cisco IOS router will enable both RIPv1 and RIPv2. RIPv1 will be enabled for inbound and outbound routing updates, and RIPv2 will be enabled only for inbound routing updates. This is illustrated below for a router configured for RIP routing without the version 2 keyword:

```
R1#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 9 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 1, receive any version
    Interface             Send  Recv  Triggered RIP  Key-chain
    Serial0/0             1     1 2
```

The next thing to remember when enabling RIP is to always specify the network at it major Classful boundary, regardless of the fact that it has been subnetted. For example, R1 has three Loopback interfaces: 10.10.100.1/27 and 10.10.101.1/26. Because these are part of the 10.0.0.0/8 subnet (which is a Class A address) the RIP network statement is configured using their major Classful boundary, and is configured as network 10.0.0.0 in RIP configuration mode.

```
R1#show ip protocols

Routing Protocol is "rip"

  Sending updates every 30 seconds, next due in 12 seconds

  Invalid after 180 seconds, hold down 180, flushed after 240

  Outgoing update filter list for all interfaces is not set

  Incoming update filter list for all interfaces is not set

  Redistributing: rip

  Default version control: send version 2, receive version 2

    Interface             Send  Recv  Triggered RIP  Key-chain

    Serial0/0             2     2

    Loopback100              2     2

    Loopback101              2     2

  Automatic network summarization is in effect

  Maximum path: 4

  Routing for Networks:

    10.0.0.0

    192.168.0.0

  Routing Information Sources:

    Gateway         Distance      Last Update

    192.168.0.2          120      00:02:47

  Distance: (default is 120)
```

Lab 36: RIPv2 Automatic Summarization

Lab Objective:

The objective of this lab exercise is for you to learn and understand automatic network summarization using Routing Information Protocol version 2 on a Cisco IOS router. By default, when RIP routing is enabled on for networks, it performs summarization at default network boundaries.

Lab Purpose:

RIPv2 configuration is a fundamental skill. By default, when RIP is enabled on a Cisco router, both version 1 and version 2 updates are sent and received. Since RIPv1 is considered obsolete because of today's subnetted networks, it is imperative that you know how to enable RIPv2. Also, because of the VLSM employed in the networks of today, automatic summarization is a default feature that should not be used. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to prevent automatic RIPv2 summarization.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

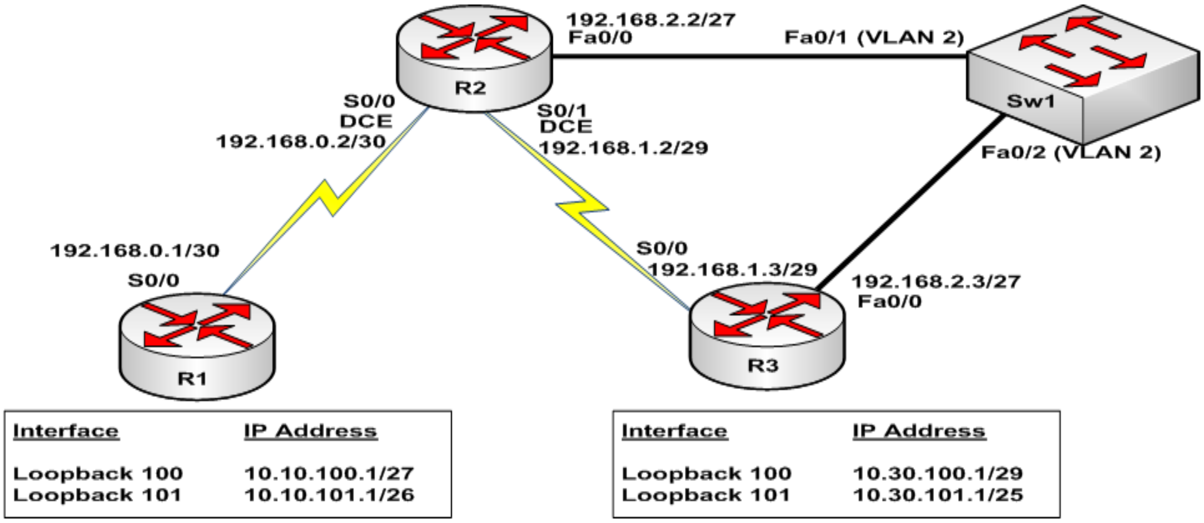
This lab has a difficulty rating of 10/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 30 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Interface	IP Address
Loopback 100	10.10.100.1/27
Loopback 101	10.10.101.1/26

Interface	IP Address
Loopback 100	10.30.100.1/29
Loopback 101	10.30.101.1/25

Task 1:

Configure the hostnames on routers R1, R2, R3 and Sw1 as illustrated in the topology.

Task 2:

Configure VLAN 2 named RIPv2-VLAN on Sw2 and assign ports FastEthernet0/1 and FastEthernet0/2 to this VLAN as access ports. Configure FastEthernet0/0 in R2 with the IP address 192.168.2.2/27 and FastEthernet0/0 on R3 with the IP address 192.168.2.3/27. Verify your VLAN and interface configuration by using ping.

Task 3:

Configure a back-to-back Serial connection between R1 and R2. Configure the DCE interface Serial0/0 in R2 to provide clocking to R1 at a clock speed of 128Kbps. Configure a back-to-back Serial connection between R2 and R3. Configure the DCE interface Serial0/1 in R2 to provide clocking to R3 at a clock speed of 128Kbps. Configure the IP addresses between R1 and R2 Serial interfaces and R2 and R3 Serial interfaces as illustrated in the topology. Ping from R1 to R2 and vice versa as well as from R2 to R3 and vice versa to validate your configuration.

Task 4:

Configure both R1 and R3 with the Loopback interface specified in the lab topology

Task 5:

Enable RIPv2 on R1, R2 and R3 for all subnets configured on the routers. Verify that RIPv2 has been enabled using the appropriate commands.

Task 6:

Look at the routing tables of R1, R2 and R3 and see if the 10.10.100.0/27 and 10.10.101.0/26 routes from R1 are present (check on R2 and R3) as well as if the 10.30.100.0/29 and 10.30.101.0/25 routes from R3 are present (check on R1 and R2). If you have configured the network as required, you will notice that you do not see these subnets, but instead only see a 10.0.0.0/8 subnet in the routing table.

Task 7:

Based on your studies, you know that RIPv2 performs automatic summarization at Classful boundaries. Armed with this knowledge, disable this behavior on R1, R2, and R3. To reset the routing tables, issue the clear ip route * command on routers R1, R2, and R3.

Task 8:

Look at the routing tables of R2 and R3 and verify that the 10.10.100.0/27 and 10.10.101.0/26 routes from R1 are now present. Next, look at the routing table of R1 and R2 and verify that the 10.30.100.0/29 and 10.30.101.0/25 routes from R3 are now present.

SOLUTION:

Lab 36 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

```
R2#conf

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#int fa 0/0

R2(config-if)#no shut

R2(config-if)#ip add 192.168.2.2 255.255.255.224

R2(config-if)#end

R2#

R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int fa 0/0

R3(config-if)#no shut

R3(config-if)#ip add 192.168.2.3 255.255.255.224

R3(config-if)#^Z

R3#

R2#ping 192.168.2.3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.3, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms

R2#ping 192.168.2.3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.3, timeout is 2 seconds:
```

```
!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

Task 3:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s0/0

R1(config-if)#ip add 192.168.0.1 255.255.255.252

R1(config-if)#no shutdown

R1(config-if)#end

R1#

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#int s0/0

R2(config-if)#clock rate 128000

R2(config-if)#ip address 192.168.0.2 255.255.255.252

R2(config-if)#no shut

R2(config-if)#exit

R2(config)#int s0/1

R2(config-if)#clock rate 128000

R2(config-if)#ip address 192.168.1.2 255.255.255.248

R2(config-if)#no shut

R2(config-if)#end

R2#

R1#ping 192.168.0.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.0.2, timeout is 2 seconds:

!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R2#ping 192.168.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int s0/0
R3(config-if)#ip add 192.168.1.3 255.255.255.248
R3(config-if)#no shutdown
R3(config-if)#end
R3#
R3#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms
R2#ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/20 ms
```

Task 4:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int lo 100
```

```
R1(config-if)#ip add 10.10.100.1 255.255.255.224
R1(config-if)#exit
R1(config)#int loo 101
R1(config-if)#ip add 10.10.101.1 255.255.255.192
R1(config-if)#end
R1#
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int loo 100
R3(config-if)#ip add 10.30.100.1 255.255.255.248
R3(config-if)#exit
R3(config)#int loo 101
R3(config-if)#ip add 10.30.101.1 255.255.255.128
R3(config-if)#^Z
R3#
```

Task 5:

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router rip
R3(config-router)#ver 2
R3(config-router)#network 10.0.0.0
R3(config-router)#network 192.168.1.0
R3(config-router)#network 192.168.2.0
R3(config-router)#^Z
R3#
R3#show ip protocols
Routing Protocol is "rip"
```

```
  Sending updates every 30 seconds, next due in 12 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface             Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0       2     2
    Serial0/0             2     2
    Loopback100           2     2
    Loopback101           2     2
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router rip
R2(config-router)#ver 2
R2(config-router)#net 192.168.0.0
R2(config-router)#net 192.168.1.0
R2(config-router)#net 192.168.2.0
R2(config-router)#end
R2#
R2#show ip prot
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 3 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface             Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0       2     2
    Serial0/0             2     2
    Serial0/1             2     2
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router rip
R1(config-router)#net 10.0.0.0
R1(config-router)#net 192.168.0.0
R1(config-router)#end
R1#
R1#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 18 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface             Send  Recv  Triggered RIP  Key-chain
    Serial0/0             2     2
    Loopback100           2     2
    Loopback101           2     2
```

Task 6:

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.10.100.0/27 is directly connected, Loopback100
C       10.10.101.0/26 is directly connected, Loopback101
     192.168.0.0/30 is subnetted, 1 subnets
C       192.168.0.0 is directly connected, Serial0/0
R    192.168.1.0/24 [120/1] via 192.168.0.2, 00:00:21, Serial0/0
R    192.168.2.0/24 [120/1] via 192.168.0.2, 00:00:21, Serial0/0
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
R    10.0.0.0/8 [120/1] via 192.168.0.1, 00:00:08, Serial0/0
                [120/1] via 192.168.1.3, 00:00:05, Serial0/1
                [120/1] via 192.168.2.3, 00:00:06, FastEthernet0/0
     192.168.0.0/30 is subnetted, 1 subnets
```

```
C       192.168.0.0 is directly connected, Serial0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/29 is directly connected, Serial0/1
R       192.168.1.0/24 [120/1] via 192.168.2.3, 00:00:06, FastEthernet0/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/27 is directly connected, FastEthernet0/0
R       192.168.2.0/24 [120/1] via 192.168.1.3, 00:00:06, Serial0/1
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.30.100.0/29 is directly connected, Loopback100
C       10.30.101.0/25 is directly connected, Loopback101
R    192.168.0.0/24 [120/1] via 192.168.1.2, 00:00:17, Serial0/0
                    [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/29 is directly connected, Serial0/0
R       192.168.1.0/24 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/27 is directly connected, FastEthernet0/0
R       192.168.2.0/24 [120/1] via 192.168.1.2, 00:00:17, Serial0/0
```

NOTE: Pay attention to the routes marked R as these are RIP routes. The [120/1] that follows the subnet indicates [Administrative Distance/Metric]. By default, the Administrative Distance for RIP is 120. The metric for the route, is based on the RIP metric -- which is hop count. Therefore, a metric of 1 means that the route is 1 hop away, a metric of 2 means that the route is 2 hops away, and so forth. The largest value you will ever see for RIP is 15, since this is the maximum amount of hops allowed in RIP. Make sure you familiarize yourself with the codes for Static, OSPF, EIGRP, and RIP routes for the CCNA certification.

Task 7:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#router rip

R1(config-router)#no auto-summary

R1(config-router)#^Z

R1#

R1#cle ip rou *

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#router rip

R2(config-router)#no auto-summary

R2(config-router)#end

R2#

R2#cle ip ro *

R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#router rip

R3(config-router)#no auto-summary

R3(config-router)#end

R3#

R3#clear ip route *
```

Task 8:

```
R1#show ip ro
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 5 subnets, 5 masks
R       10.0.0.0/8 [120/1] via 192.168.0.2, 00:01:16, Serial0/0
C       10.10.100.0/27 is directly connected, Loopback100
C       10.10.101.0/26 is directly connected, Loopback101
R       10.30.100.0/29 [120/2] via 192.168.0.2, 00:00:19, Serial0/0
R       10.30.101.0/25 [120/2] via 192.168.0.2, 00:00:19, Serial0/0
     192.168.0.0/30 is subnetted, 1 subnets
C       192.168.0.0 is directly connected, Serial0/0
     192.168.1.0/29 is subnetted, 1 subnets
R       192.168.1.0 [120/1] via 192.168.0.2, 00:00:19, Serial0/0
     192.168.2.0/27 is subnetted, 1 subnets
R       192.168.2.0 [120/1] via 192.168.0.2, 00:00:19, Serial0/0
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 4 subnets, 4 masks
R       10.10.100.0/27 [120/1] via 192.168.0.1, 00:00:11, Serial0/0
R       10.10.101.0/26 [120/1] via 192.168.0.1, 00:00:11, Serial0/0
R       10.30.100.0/29 [120/1] via 192.168.2.3, 00:00:11, FastEthernet0/0
                       [120/1] via 192.168.1.3, 00:00:10, Serial0/1
R       10.30.101.0/25 [120/1] via 192.168.2.3, 00:00:11, FastEthernet0/0
                       [120/1] via 192.168.1.3, 00:00:10, Serial0/1
     192.168.0.0/30 is subnetted, 1 subnets
C       192.168.0.0 is directly connected, Serial0/0
     192.168.1.0/29 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, Serial0/1
     192.168.2.0/27 is subnetted, 1 subnets
C       192.168.2.0 is directly connected, FastEthernet0/0
R3#sh ip ro
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 5 subnets, 5 masks
```

```
R       10.0.0.0/8 [120/1] via 192.168.1.2, 00:02:25, Serial0/0
                 [120/1] via 192.168.2.2, 00:02:21, FastEthernet0/0
R       10.10.100.0/27 [120/2] via 192.168.2.2, 00:00:09, FastEthernet0/0
                   [120/2] via 192.168.1.2, 00:00:08, Serial0/0
R       10.10.101.0/26 [120/2] via 192.168.2.2, 00:00:10, FastEthernet0/0
                   [120/2] via 192.168.1.2, 00:00:08, Serial0/0
C       10.30.100.0/29 is directly connected, Loopback100
C       10.30.101.0/25 is directly connected, Loopback101
     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
R       192.168.0.0/30 [120/1] via 192.168.2.2, 00:00:10, FastEthernet0/0
                   [120/1] via 192.168.1.2, 00:00:08, Serial0/0
R       192.168.0.0/24 [120/1] via 192.168.2.2, 00:02:21, FastEthernet0/0
                   [120/1] via 192.168.1.2, 00:02:25, Serial0/0
     192.168.1.0/29 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, Serial0/0
     192.168.2.0/27 is subnetted, 1 subnets
C       192.168.2.0 is directly connected, FastEthernet0/0
```

Lab 37: Debugging and Verifying RIP version 2 Updates

Lab Objective:

The objective of this lab exercise is for you to learn and understand how RIPv2 updates are sent. Unlike RIPv1, RIPv2 sends updates using Multicast.

Lab Purpose:

RIPv2 update debugging is a fundamental skill. By default, RIPv2 sends updates via Multicast. You can use debugging commands to troubleshoot network and routing problems. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to verify RIPv2 updates using debugging commands.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

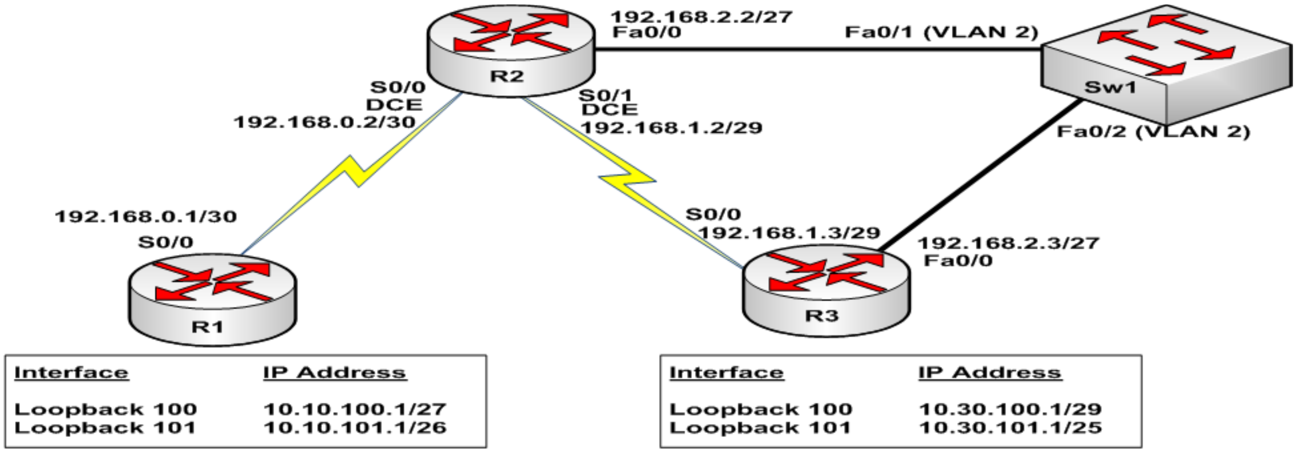
This lab has a difficulty rating of 7/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Interface	IP Address
Loopback 100	10.10.100.1/27
Loopback 101	10.10.101.1/26

Interface	IP Address
Loopback 100	10.30.100.1/29
Loopback 101	10.30.101.1/25

Task 1:

This lab will only use 2 routers. Configure the hostnames on routers R1 and R2 as illustrated in the topology.

Task 2:

Configure a back-to-back Serial connection between R1 and R2. Configure the DCE interface Serial0/0 in R2 to provide clocking to R1 at a clock speed of 2Mbps.

Task 3:

Configure IP addresses 192.168.0.1/30 and 192.168.0.2/30 on R1 and R2 Serial0/0 interfaces respectively. Configure the Loopback interfaces on R1 with the IP addresses illustrated in the topology.

Task 4:

Enable RIPv2 for the Serial0/0 interface on R2 and the Serial 0/0 and Loopback interfaces on R1.

Task 5:

Enable debugging on R1 and R2 and verify that RIPv2 updates are being sent out of all RIPv2-enabled networks. Keep in mind that by default RIP sends updates every 30 seconds, so you will typically see updates within that time frame. Familiarize yourself with the output of the debugs. Be sure to disable debugging when done.

SOLUTION:

Lab 37 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring DCE clocking, please refer to:

Lab 35 Configuration and Verification Task 2

Task 3:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s0/0

R1(config-if)#ip add 192.168.0.1 255.255.255.252

R1(config-if)#no shutdown

R1(config)#int loo 100

R1(config-if)#ip add 10.10.100.1 255.255.255.224

R1(config-if)#exit

R1(config)#int loo 101

R1(config-if)#ip add 10.10.101.1 255.255.255.192

R1(config-if)#end

R1#

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#int s0/0
```

```
R2(config-if)#ip address 192.168.0.2 255.255.255.252

R1(config-if)#no shutdown

R2(config-if)#end

R2#

R1#ping 192.168.0.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.0.2, timeout is 2 seconds:

!!!!!

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

R2#ping 192.168.0.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:

!!!!!

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

Task 4:

```
R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#router rip

R2(config-router)#version 2

R2(config-router)#net 192.168.0.0

R2(config-router)#end

R2#

R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#router rip

R1(config-router)#net 10.0.0.0

R1(config-router)#net 192.168.0.0
```

```
R1(config-router)#end

R1#
```

Task 5:

```
R1#debug ip rip events

RIP event debugging is on

*Mar  1 02:13:44.358: RIP: sending v2 update to 224.0.0.9 via Loopback101 (10.10.101.1)

*Mar  1 02:13:44.358: RIP: Update contains 2 routes

*Mar  1 02:13:44.358: RIP: Update queued

*Mar  1 02:13:44.358: RIP: Update sent via Loopback101

*Mar  1 02:13:44.362: RIP: ignored v2 packet from 10.10.101.1 (sourced from one of our addresses)

*Mar  1 02:13:46.189: RIP: sending v2 update to 224.0.0.9 via Loopback100 (10.10.100.1)

*Mar  1 02:13:46.189: RIP: Update contains 2 routes

*Mar  1 02:13:46.189: RIP: Update queued

*Mar  1 02:13:46.189: RIP: Update sent via Loopback100

*Mar  1 02:13:46.193: RIP: ignored v2 packet from 10.10.100.1 (sourced from one of our addresses)

*Mar  1 02:13:46.962: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (192.168.0.1)

*Mar  1 02:13:46.962: RIP: Update contains 2 routes

*Mar  1 02:13:46.962: RIP: Update queued

*Mar  1 02:13:46.962: RIP: Update sent via Serial0/0

R1#undebug all

All possible debugging has been turned off

R2#debug ip rip events

RIP event debugging is on

*Mar  1 02:15:49.395: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (192.168.0.2) - suppressing null update

*Mar  1 02:15:56.186: RIP: received v2 update from 192.168.0.1 on Serial0/0

*Mar  1 02:15:56.186: RIP: Update contains 2 routes
```

```
*Mar  1 02:16:15.790: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (192.168.0.2) - suppressing null update

*Mar  1 02:16:25.422: RIP: received v2 update from 192.168.0.1 on Serial0/0

*Mar  1 02:16:25.422: RIP: Update contains 2 routes

R2#undebug ip rip events

RIP event debugging is off
```

NOTE: There are two other options available when it comes to debugging RIP. These are:

```
R1#debug ip rip ?
  database  RIP database events
  events    RIP protocol events
  trigger   RIP trigger extension
  <cr>
```

Play around with these options and familiarize yourself with the information they print. Also, remember that debugging is very processor intensive, and can do more harm than good in a live network, so always make sure you disable debugging when you have captured the information you were looking for.

Lab 38: Passive Interfaces for RIPv2 Updates

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to prevent RIPv2 from sending unnecessary updates by using passive interfaces.

Lab Purpose:

Preventing unnecessary RIPv2 updates using passive interfaces is a fundamental skill. By default, RIPv2 sends updates via Multicast on all interfaces for which RIPv2 has been enabled. For example, it is not possible to ever have another device connected to a Loopback interface, so it is a waste of router processing power to have RIPv2 continuously send updates to a Loopback interface. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to prevent RIPv2 sending unnecessary updates.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

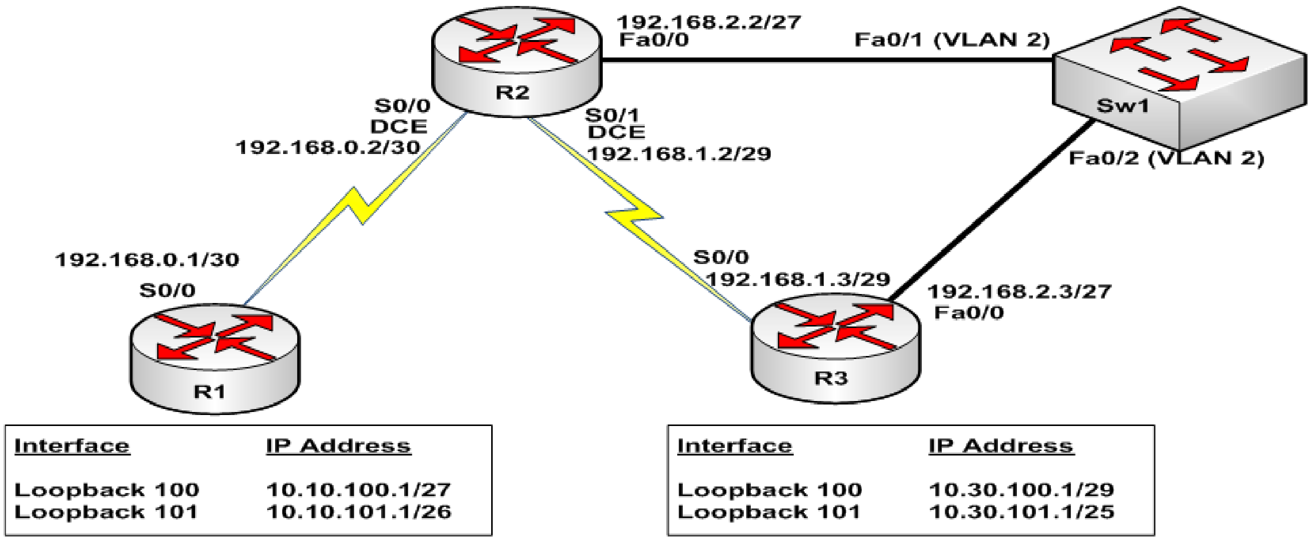
This lab has a difficulty rating of 7/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Interface	IP Address
Loopback 100	10.10.100.1/27
Loopback 101	10.10.101.1/26

Interface	IP Address
Loopback 100	10.30.100.1/29
Loopback 101	10.30.101.1/25

Task 1:

This lab will only use 2 routers. Configure the hostnames on routers R1 and R2 as illustrated in the topology.

Task 2:

Configure a back-to-back Serial connection between R1 and R2. Configure the DCE interface Serial0/0 in R2 to provide clocking to R1 at a clock speed of 2Mbps.

Task 3:

Configure IP addresses 192.168.0.1/30 and 192.168.0.2/30 on R1 and R2 Serial0/0 interfaces respectively. Configure the Loopback interfaces on R1 with the IP addresses illustrated in the topology. Enable RIPv2 for the Serial0/0 interface on R1 and the Loopback subnets.

Task 4:

First, use the show ip protocols command to see the interfaces on which RIPv2 is sending updates. Next, enable debugging on R1 and verify that RIPv2 updates are being sent on all RIPv2-enabled interfaces. When you have verified this, disable debugging.

Task 5:

Prevent RIPv2 from sending updates on the Loopback interfaces. Verify your configuration by enabling debugging. Disable debugging when done.

SOLUTION:

Lab 38 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring DCE clocking, please refer to:

Lab 35 Configuration and Verification Task 2

Task 3:

For reference information on configuring Loopback interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

For reference information on configuring RIPv2, please refer to:

Lab 35 Configuration and Verification Task 4

Lab 36 Configuration and Verification Task 5

Lab 37 Configuration and Verification Task 4

Task 4:

```
R1#show ip protocols

Routing Protocol is "rip"

  Sending updates every 30 seconds, next due in 19 seconds

  Invalid after 180 seconds, hold down 180, flushed after 240

  Outgoing update filter list for all interfaces is not set

  Incoming update filter list for all interfaces is not set

  Redistributing: rip

  Default version control: send version 2, receive version 2

    Interface             Send  Recv  Triggered RIP  Key-chain

    Serial0/0               2     2

    Loopback100             2     2
```

```
   Loopback101          2    2

R1#debug ip rip

RIP protocol debugging is on

*Mar  1 03:09:46.237: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (192.168.0.1)

*Mar  1 03:09:46.237: RIP: build update entries

*Mar  1 03:09:46.237:   10.10.100.0/27 via 0.0.0.0, metric 1, tag 0

*Mar  1 03:09:46.237:   10.10.101.0/26 via 0.0.0.0, metric 1, tag 0

*Mar  1 03:09:53.248: RIP: sending v2 update to 224.0.0.9 via Loopback101 (10.10.101.1)

*Mar  1 03:09:53.248: RIP: build update entries

*Mar  1 03:09:53.248:   10.10.100.0/27 via 0.0.0.0, metric 1, tag 0

*Mar  1 03:09:53.248:   192.168.0.0/30 via 0.0.0.0, metric 1, tag 0

*Mar  1 03:09:53.252: RIP: ignored v2 packet from 10.10.101.1 (sourced from one of our
addresses)

*Mar  1 03:10:09.070: RIP: sending v2 update to 224.0.0.9 via Loopback100 (10.10.100.1)

*Mar  1 03:10:09.070: RIP: build update entries

*Mar  1 03:10:09.070:   10.10.101.0/26 via 0.0.0.0, metric 1, tag 0

*Mar  1 03:10:09.070:   192.168.0.0/30 via 0.0.0.0, metric 1, tag 0

*Mar  1 03:10:09.074: RIP: ignored v2 packet from 10.10.100.1 (sourced from one of our
addresses)

R1#

R1#undebug ip rip

RIP protocol debugging is off
```

NOTE: Pay particular note to the fact that RIPv2 is sending updates via the Loopback interfaces as illustrated:

```
*Mar  1 03:09:53.248: RIP: sending v2 update to 224.0.0.9 via Loopback101 (10.10.101.1)
*Mar  1 03:10:09.070: RIP: sending v2 update to 224.0.0.9 via Loopback100 (10.10.100.1)
```

Loopback interfaces are logical interfaces that have the majority of the characteristics of physical interfaces. However, one important thing to remember is that no host can ever reside on a subnet configured for a Loopback interface. If you assign a Loopback interface as /24 subnet mask, for example, you are simply wasting valuable IP address space. Given that no host can every reside on the same subnet as a Loopback interface, it is a waste of router resources to have a routing protocol send updates to a Loopback interface, as there will never be another router (or other device) that will ever respond back to these updates. Hence, when you configure Loopback interfaces, it is always considered best practice to disable routing protocols sending updates on them using the passive-interface command as illustrated.

Task 5:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#router rip

R1(config-router)#passive-interface loopback 100

R1(config-router)#passive-interface loopback 101

R1(config-router)#end

R1#

R1#show ip protocols

Routing Protocol is "rip"

  Sending updates every 30 seconds, next due in 5 seconds

  Invalid after 180 seconds, hold down 180, flushed after 240

  Outgoing update filter list for all interfaces is not set

  Incoming update filter list for all interfaces is not set

  Redistributing: rip

  Default version control: send version 2, receive version 2

    Interface             Send  Recv  Triggered RIP  Key-chain

    Serial0/0             2     2

R1#debug ip rip

RIP protocol debugging is on

R1#

*Mar  1 03:20:02.355: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (192.168.0.1)

*Mar  1 03:20:02.355: RIP: build update entries

*Mar  1 03:20:02.355:   10.10.100.0/27 via 0.0.0.0, metric 1, tag 0

*Mar  1 03:20:02.355:   10.10.101.0/26 via 0.0.0.0, metric 1, tag 0
```

```
R1#

*Mar  1 03:20:28.974: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (192.168.0.1)

*Mar  1 03:20:28.974: RIP: build update entries

*Mar  1 03:20:28.974:   10.10.100.0/27 via 0.0.0.0, metric 1, tag 0

*Mar  1 03:20:28.974:   10.10.101.0/26 via 0.0.0.0, metric 1, tag 0

R1#undebug all

All possible debugging has been turned off
```

NOTE: Suppose you have a router with 1 Serial interface and 600 Loopback interfaces. Given such a scenario, issuing the passive-interface command for every one of those Loopback interfaces would take a great deal of time. Fortunately, Cisco recognized this and created the passive-interface default command in Cisco IOS. When this command is issued, all interfaces are configured passive. In order to send updates on a particular interface, you would negate that interface as not being passive by issuing the no passive-interface command followed by the interface(s) you want to send routing protocol updates on. This is illustrated below:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router rip
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface serial0/0
R1(config-router)#end
R1#
```

The above configuration makes all interfaces configured for RIP passive with the exeption of interface Serial0/0. Make sure you remember this command, not only for the purposes of the CCNA exam, but for use in the real world.

Lab 39: Summarizing Routes with RIPv2

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to summarize routes with RIPv2. Route summarization allows the size of routing tables to be reduced by advertising a summary route for a range of multiple specific routes.

Lab Purpose:

Route summarization is a fundamental skill. With the subnetted networks of today, routing tables can grow very large due to the sheer number of network entries. In order to reduce the burden of extremely large routing tables on routers, route summarization can be used. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure a RIPv2 route summarization.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

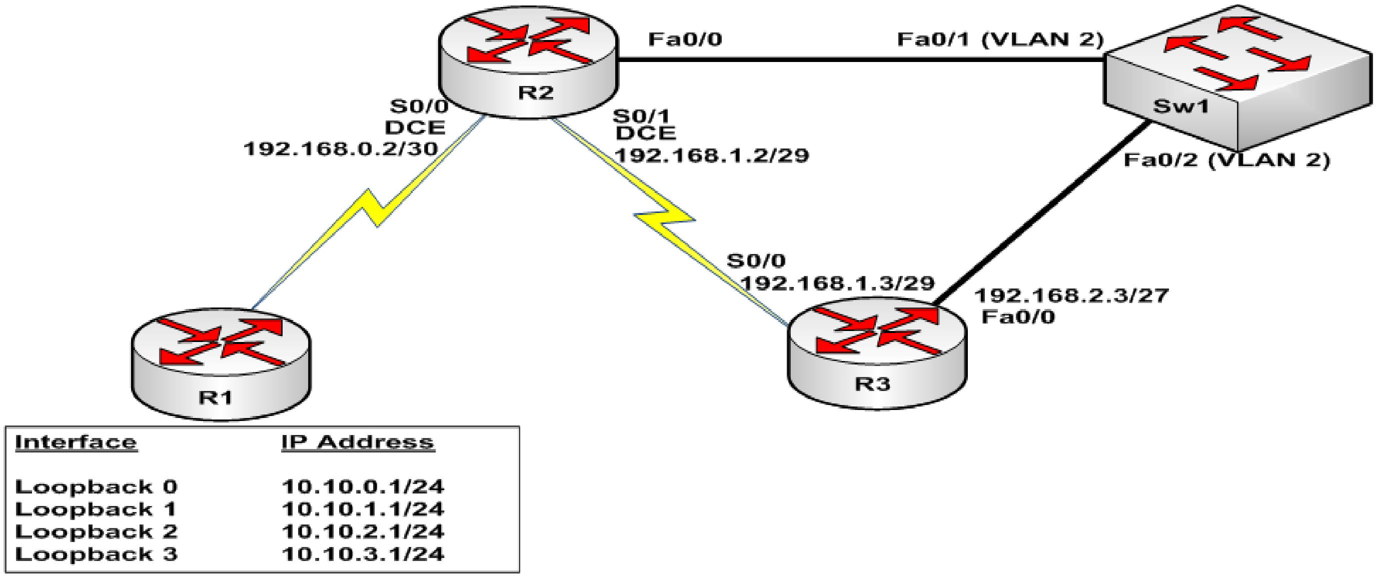
This lab has a difficulty rating of 10/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Interface	IP Address
Loopback 0	10.10.0.1/24
Loopback 1	10.10.1.1/24
Loopback 2	10.10.2.1/24
Loopback 3	10.10.3.1/24

Task 1:

Configure the hostnames on routers R1, R2, R3 and Sw1 as illustrated in the topology.

Task 2:

Configure VLAN 2 named RIPv2-VLAN on Sw2 and assign ports FastEthernet0/1 and FastEthernet0/2 to this VLAN as access ports. Configure FastEthernet0/0 in R2 with the IP address 192.168.2.2/27 and FastEthernet0/0 on R3 with the IP address 192.168.2.3/27. Verify your VLAN and interface configuration by using ping.

Task 3:

Configure a back-to-back Serial connection between R1 and R2. Configure the DCE interface Serial0/0 in R2 to provide clocking to R1 at a clock speed of 128Kbps. Configure a back-to-back Serial connection between R2 and R3. Configure the DCE interface Serial0/1 in R2 to provide clocking to R3 at a clock speed of 128Kbps. Configure the IP addresses between R1 and R2 Serial interfaces and R2 and R3 Serial interfaces as illustrated in the topology. Ping from R1 to R2 and vice versa as well as from R2 to R3 and vice versa to validate your configuration.

Task 4:

Configure the Loopback interfaces on R1 with the IP addresses illustrated in the topology.

Task 5:

Enable RIPv2 on R1, R2 and R3 for all subnets configured on the routers. Verify that RIPv2 has been enabled using the appropriate commands. Verify that R2 and R3 can see the R1 Loopback subnets in their routing tables

Task 6:

Configure R1 to summarize the Loopback interfaces subnets and advertise a single route to R2 and R3 that encompasses the IP address range of the Loopback interfaces. Clear the routing table on R1 after you are done. Finally, validate that a summary address has been accepted and is in the RIP database.

Task 7:

Verify that both R2 and R3 now see a single route for the 10.10.0.0/24 through 10.10.3.0/24 subnets. Ping an IP address within this range from R2 and R3 to ensure that there is network connectivity.

SOLUTION:

Lab 39 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

For reference information on configuring DCE clocking, please refer to:

Lab 21 Configuration and Verification Task 2

Lab 35 Configuration and Verification Task 2

For reference information on configuring IP interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

Task 4:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#interface loopback 0

R1(config-if)#ip address 10.10.0.1 255.255.255.0

R1(config-if)#exit

R1(config)#interface loopback 1

R1(config-if)#ip address 10.10.1.1 255.255.255.0

R1(config-if)#exit

R1(config)#interface loopback 2

R1(config-if)#ip address 10.10.2.1 255.255.255.0

R1(config-if)#exit

R1(config)#interface loopback 3

R1(config-if)#ip address 10.10.3.1 255.255.255.0

R1(config-if)#^Z

R1#

R1#show ip interface brief

Interface              IP-Address      OK? Method Status  Protocol

Serial0/0              192.168.0.1      YES manual up       up

Loopback0                10.10.0.1      YES manual up       up

Loopback1                10.10.1.1      YES manual up       up

Loopback2                10.10.2.1      YES manual up       up

Loopback3                10.10.3.1      YES manual up       up
```

Task 5:

For reference information on configuring RIPv2, please refer to:

Lab 35 Configuration and Verification Task 4

Lab 36 Configuration and Verification Task 5

Lab 37 Configuration and Verification Task 4

```
R2#show ip route rip

   10.0.0.0/24 is subnetted, 4 subnets

R      10.10.0.0 [120/1] via 192.168.0.1, 00:00:17, Serial0/0

R      10.10.1.0 [120/1] via 192.168.0.1, 00:00:17, Serial0/0

R      10.10.2.0 [120/1] via 192.168.0.1, 00:00:17, Serial0/0

R      10.10.3.0 [120/1] via 192.168.0.1, 00:00:17, Serial0/0

R3#show ip route rip

   10.0.0.0/24 is subnetted, 4 subnets

R      10.10.0.0 [120/2] via 192.168.2.2, 00:00:13, FastEthernet0/0

             [120/2] via 192.168.1.2, 00:00:00, Serial0/0

R      10.10.1.0 [120/2] via 192.168.2.2, 00:00:13, FastEthernet0/0

             [120/2] via 192.168.1.2, 00:00:00, Serial0/0

R      10.10.2.0 [120/2] via 192.168.2.2, 00:00:13, FastEthernet0/0

             [120/2] via 192.168.1.2, 00:00:00, Serial0/0

R      10.10.3.0 [120/2] via 192.168.2.2, 00:00:13, FastEthernet0/0

             [120/2] via 192.168.1.2, 00:00:00, Serial0/0

   192.168.0.0/30 is subnetted, 1 subnets

R      192.168.0.0 [120/1] via 192.168.1.2, 00:00:00, Serial0/0

              [120/1] via 192.168.2.2, 00:00:13, FastEthernet0/0
```

Task 6:

NOTE: This is the stage at which you get tested on your subnetting skill. In subnetting, you should have also learned how to summarize networks and create a single summary address. The task here is to summarize the 10.10.0.0/24, 10.10.1.0/24, 10.10.2.0/24, and 10.10.3.0/24 subnets. In order to create your summary address, identify the first octet that does not have the same Decimal value. Based on our provided subnets, this would be the third octet of each of the provided address. The first and second octets all match -- i.e. they are all 10.10, but the third octet is 1 on the first address, 2 on the second, 3 on the third, and 4 on the fourth. Write out the Decimal values of the third octet of the subnets provided in Binary notation. This would be as follows:

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
0	0	0	0	0	0	0	0

0	0	0	0	0	0	0	1
0	0	0	0	0	0	1	0
0	0	0	0	0	0	1	1

The last value under which all four bits are the same is 4. Therefore, to determine the summary address, insert a value of 1 all the way through the column with the 4 in it and add those bits up. The answer will be the Decimal value which you will use to create the summary address subnet mask. This is illustrated as follows:

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
1	1	1	1	1	1	0	0

The subnet mask for your summarized network would be 128 + 64 + 32 + 16 + 8 + 4, which equals 252. The summary address would then be written as 10.10.0.0 255.255.252.0 or 10.10.0.0/22. To configure RIPv2 to send this summary address instead of the four 10.10.x.x/24 network entries, use the ip summary-address rip command under the interface RIPv2 uses to send updates to other RIPv2 routers as illustrated below.

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s0/0

R1(config-if)#ip summary-address rip 10.10.0.0 255.255.252.0

R1(config-if)#end

R1#

R1#show running-config interface serial 0/0

Building configuration...

Current configuration : 130 bytes

!

interface Serial0/0

 ip address 192.168.0.1 255.255.255.252

 ip summary-address rip 10.10.0.0 255.255.252.0

end

R1#

R1#show ip rip database

10.0.0.0/8    auto-summary

10.10.0.0/22    int-summary
```

```
10.10.0.0/24    directly connected, Loopback0
10.10.1.0/24    directly connected, Loopback1
10.10.2.0/24    directly connected, Loopback2
10.10.3.0/24    directly connected, Loopback3
192.168.0.0/24    auto-summary
192.168.0.0/30    directly connected, Serial0/0
192.168.1.0/24    auto-summary
192.168.1.0/29
   [1] via 192.168.0.2, 00:00:02, Serial0/0
192.168.2.0/24    auto-summary
192.168.2.0/27
   [1] via 192.168.0.2, 00:00:02, Serial0/0
```

Task 7:

```
R2#show ip route rip
    10.0.0.0/22 is subnetted, 1 subnets
R       10.10.0.0 [120/1] via 192.168.0.1, 00:00:00, Serial0/0
R2#
R2#ping 10.10.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R3#show ip route rip
    10.0.0.0/22 is subnetted, 1 subnets
R       10.10.0.0 [120/2] via 192.168.2.2, 00:00:23, FastEthernet0/0
                  [120/2] via 192.168.1.2, 00:00:22, Serial0/0
    192.168.0.0/30 is subnetted, 1 subnets
```

```
R       192.168.0.0 [120/1] via 192.168.1.2, 00:00:22, Serial0/0
                    [120/1] via 192.168.2.2, 00:00:23, FastEthernet0/0
R3#
R3#ping 10.10.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/15/20 ms
```

Lab 40: RIPv2 Split Horizon

Lab Objective:

The objective of this lab exercise is for you to learn and understand the effects of Split Horizon in a typical hub and spoke topology.

Lab Purpose:

Configuring and troubleshooting Split Horizon is a fundamental skill. RIPv2 is a Distance Vector protocol, and as such uses Split Horizon to prevent routing loops. Split Horizon mandates that RIPv2 will not send updates back out of the interface on which they were received. In newer versions of Cisco IOS software, Split Horizon is disabled by default for Frame Relay and SMDS. However, in the real world, you may encounter routers running older Cisco IOS software which do have Split Horizon enabled by default. It is for the preparation of such scenarios that you should be knowledgeable about Split Horizon. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to address Split Horizon issues in RIPv2.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

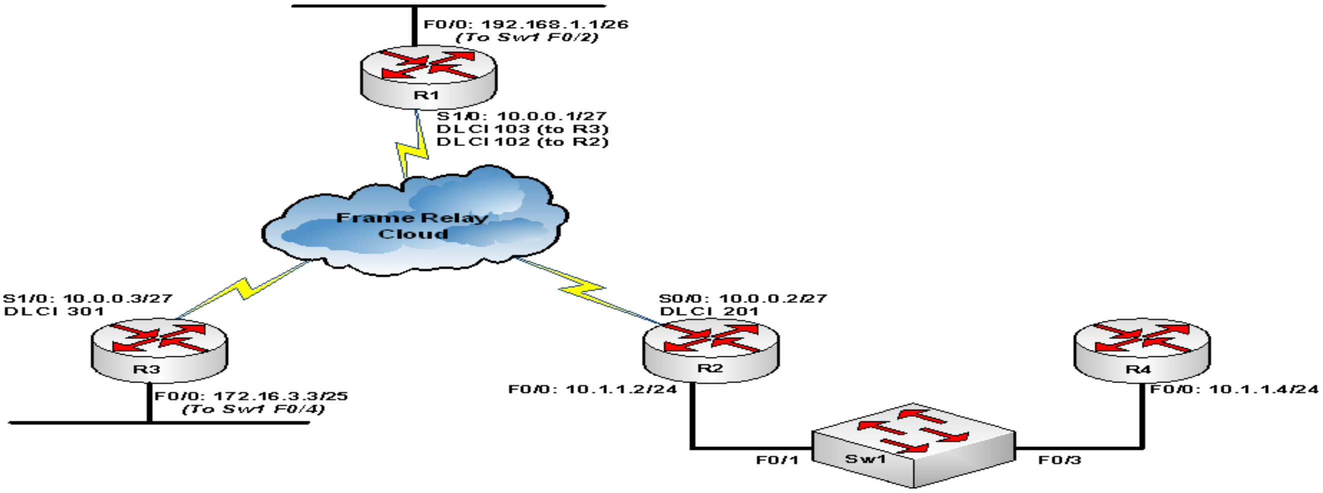
IMPORTANT NOTE:

In order to configure Frame Relay between two routers in your lab, you will need THREE routers! The first two routers will be regular routers, and the third will need to be configured as a Frame Relay switch. This can be any Cisco router that has at least two Serial interfaces.

Please refer to **Appendix B: Cabling and configuring a Frame Relay Switch For Three Routers** for the appropriate configuration to issue on the Frame Relay switch.

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

This lab will only be performed on routers R1, R2, and R3. Configure the hostnames on routers R1, R2, and R3 as illustrated in the topology.

Task 2:

Configure the switch in the topology with the hostname Sw1. Enable F0/1, F0/2, and F0/4 on Sw1 so that when you bring up the router interfaces connected to those switch ports they can come up.

Task 3:

Configure IP addresses on the Fa0/0 interfaces on R1, R2, and R3. Make sure you enable these interfaces. Verify that the Fa0/0 interfaces on all three routers are up.

Task 4:

Configure Frame Relay on R1, R2, and R3. Use the IP addresses in the topology for their respective Serial interfaces. Use the default Frame Relay encapsulation of Cisco.

Task 5:

Create a static Frame Relay map on each router for the two other routers. Verify your static Frame Relay maps. You can also use ping to test connectivity between the routers to double-check your Frame Relay mapping.

Task 6:

Enable RIPv2 on R1, R2, and R3 for all the subnets configured on those respective routers. Be sure to prevent RIPv2 from automatically summarizing at Classful network boundaries on all routers.

Task 7:

Check your IP routing tables. If you have configured everything as required, you will be receiving all routes on all routers. You can also use ping to test connectivity between the routers to double-check your routing.

Task 8:

Generally, if you are working on a hub and spoke network running RIPv2 and the router is running a Cisco IOS image that has Split Horizon disabled by default, you do not want to enable that feature unless you have very good cause to do so. However, in order to better understand Split Horizon, enable this feature on the Serial interface of R1 and clear the ip routing tables of all three routers.

Having done so, check the routing table of R3 and you will see the 10.1.1.0/24 route is no longer present. Next, check the routing table of R2 and you will see that the 172.16.3.0/25 route is no longer present. Finally, check the routing table of R1 and you will see both these routes. Because Split Horizon has been enabled, R1 will not send updates out the same interface it received them. Make sure you understand Split Horizon!

SOLUTION:

Lab 40 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

```
Switch#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Switch(config)#hostname Sw1

Sw1(config)#interface fastethernet0/1

Sw1(config-if)#no shutdown

Sw1(config-if)#exit

Sw1(config)#interface fastethernet0/3

Sw1(config-if)#no shutdown

Sw1(config-if)#end

Sw1#
```

Task 3:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int fa0/0

R1(config-if)#ip address 192.168.1.1 255.255.255.192

R1(config-if)#no shutdown

R1(config-if)#end

R1#

R1#show ip interface brief

Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        192.168.1.1     YES manual up                    up

Serial0/0              unassigned      YES unset  administratively down down

Serial0/1              unassigned      YES unset  administratively down down

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#int fa0/0

R2(config-if)#ip add 10.1.1.2 255.255.255.0

R2(config-if)#no shut

R2(config-if)#end

R2#

R2#show ip int brie

Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0           10.1.1.2     YES manual up                    up

Serial0/0              unassigned      YES unset  administratively down down

Serial0/1              unassigned      YES unset  administratively down down

R3#config term

Enter configuration commands, one per line.  End with CNTL/Z.
```

```
R3(config)#int fa0/0

R3(config-if)#ip address 172.16.3.3 255.255.255.128

R3(config-if)#no shutdown

R3(config-if)#end

R3#

R3#show ip interface brief

Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0         172.16.3.3      YES manual up                    up

Serial0/0              unassigned      YES unset  administratively down down

Serial0/1              unassigned      YES unset  administratively down down
```

Task 4:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s1/0

R1(config-if)#no shut

R1(config-if)#ip address 10.0.0.1 255.255.255.224

R1(config-if)#encapsulation frame-relay

R1(config-if)#end

R1#

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#int s0/0

R2(config-if)#no shut

R2(config-if)#encap frame-relay

R2(config-if)#ip address 10.0.0.2 255.255.255.224

R2(config-if)#^Z

R2#
```

```
R3#conf term

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int s1/0

R3(config-if)#ip address 10.0.0.3 255.255.255.224

R3(config-if)#encapsulation fram

R3(config-if)#no shut

R3(config-if)#end

R3#
```

Task 5:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s1/0

R1(config-if)#frame-relay map ip 10.0.0.2 102 broadcast

R1(config-if)#frame-relay map ip 10.0.0.3 103 broadcast

R1(config-if)#end

R1#

R1#show frame-relay map

Serial1/0 (up): ip 10.0.0.2 dlci 102(0x66,0x1860), static,

              broadcast,

              CISCO, status defined, inactive

Serial1/0 (up): ip 10.0.0.3 dlci 103(0x67,0x1870), static,

              broadcast,

              CISCO, status defined, inactive

R2#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#int s0/0

R2(config-if)#frame-relay map ip 10.0.0.1 201 broadcast
```

```
R2(config-if)#frame-relay map ip 10.0.0.3 201 broadcast
R2(config-if)#end
R2#
R2#show frame-relay map
Serial0/0 (up): ip 10.0.0.1 dlci 201(0xC9,0x3090), static,
              broadcast,
              CISCO, status defined, active
Serial0/0 (up): ip 10.0.0.3 dlci 201(0xC9,0x3090), static,
              broadcast,
              CISCO, status defined, active
R3#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int s1/0
R3(config-if)#frame-rel map ip 10.0.0.1 301 broad
R3(config-if)#frame-rel map ip 10.0.0.2 301 broad
R3(config-if)#^Z
R3#
R3#show frame-relay map
Serial1/0 (up): ip 10.0.0.1 dlci 301(0x12D,0x48D0), static,
              broadcast,
              CISCO, status defined, active
Serial1/0 (up): ip 10.0.0.2 dlci 301(0x12D,0x48D0), static,
              broadcast,
              CISCO, status defined, active
```

Task 6:

```
R1#config
Configuring from terminal, memory, or network [terminal]? term
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router rip
R1(config-router)#ver 2
R1(config-router)#no auto-summary
R1(config-router)#net 192.168.1.0
R1(config-router)#net 10.0.0.0
R1(config-router)#end
R1#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 10.0.0.0
R2(config-router)#no auto-sum
R2(config-router)#^Z
R2#
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router rip
R3(config-router)#ver 2
R3(config-router)#net 172.16.3.0
R3(config-router)#net 10.0.0.0
R3(config-router)#no auto-summary
R3(config-router)#end
R3#
```

Task 7:

```
R1#sh ip route rip
```

```
     172.16.0.0/25 is subnetted, 1 subnets
R       172.16.3.0 [120/1] via 10.0.0.3, 00:00:18, Serial1/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R       10.1.1.0/24 [120/1] via 10.0.0.2, 00:00:07, Seria 1/0
```

R2#**show ip route rip**

```
     172.16.0.0/25 is subnetted, 1 subnets
R       172.16.3.0 [120/2] via 10.0.0.3, 00:00:11, Serial0/0
     192.168.1.0/26 is subnetted, 1 subnets
R       192.168.1.0 [120/1] via 10.0.0.1, 00:00:11, Serial0/0
```

R3#**show ip route rip**

```
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R       10.1.1.0/24 [120/2] via 10.0.0.2, 00:00:00, Serial1/0
     192.168.1.0/26 is subnetted, 1 subnets
R       192.168.1.0 [120/1] via 10.0.0.1, 00:00:00, Serial1/0
```

Task 8:

R1#**conf t**

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#**int s1/0**

R1(config-if)#**ip split-horizon**

R1(config-if)#**end**

R1#

R1#**clear ip route ***

R1#

R1#**show ip route rip**

```
     172.16.0.0/25 is subnetted, 1 subnets
R       172.16.3.0 [120/1] via 10.0.0.3, 00:00:24, Serial1/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
```

```
R       10.1.1.0/24 [120/1] via 10.0.0.2, 00:00:09, Serial1/0

R2#clear ip route *

R2#

R2#show ip route rip

     192.168.1.0/26 is subnetted, 1 subnets

R       192.168.1.0 [120/1] via 10.0.0.1, 00:00:01, Serial0/0

R3#clear ip route *

R3#

R3#show ip route rip

     192.168.1.0/26 is subnetted, 1 subnets

R       192.168.1.0 [120/1] via 10.0.0.1, 00:00:03, Serial1/0
```

Lab 41: Configuring Basic EIGRP Routing

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to enable basic EIGRP routing using a single Autonomous System.

Lab Purpose:

Enabling basic EIGRP routing is a fundamental skill. EIGRP is an advanced Distance Vector routing protocol. It is also a Cisco proprietary protocol that runs over IP protocol number 88. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to enable basic EIGRP routing.

Certification Level:

This lab is suitable for CCENT & CCNA certification exam preparation

Lab Difficulty:

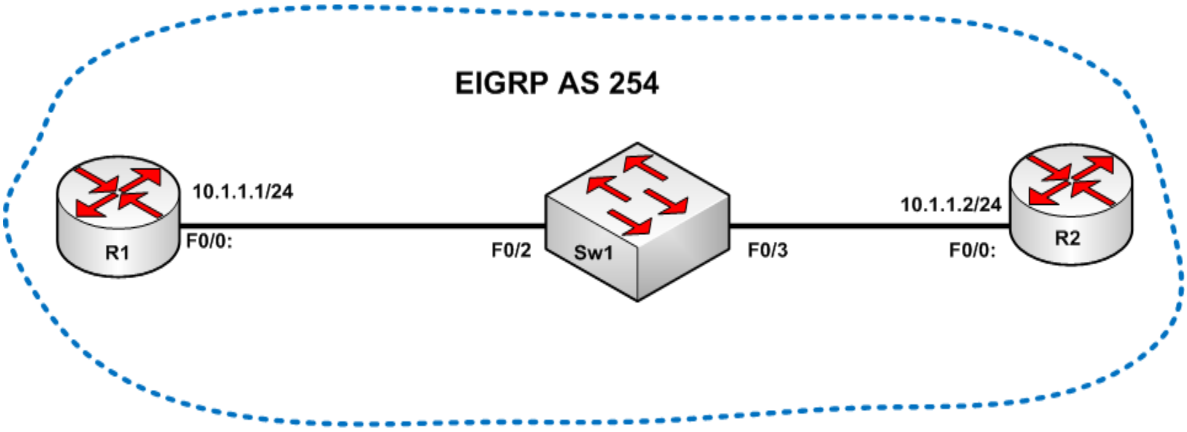
This lab has a difficulty rating of 4/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1, R2, and Sw1 as illustrated in the topology.

Task 2:

Configure VLAN 10 named EIGRP_VLAN on Sw1. Keep in mind that, by default, Sw1 will be a VTP server so you can simply create the VLAN and assign it the name provided. Next, assign ports FastEthernet0/2 and FastEthernet0/3 on Sw1 to VLAN 10 as access ports and enable those ports.

Task 3:

Configure the F0/0 interfaces on R1 and R2 with the IP addresses in the topology and bring up the interfaces. Perform a ping from R1 to R2 and vice versa and ensure that the routers can ping each other.

Task 4:

Enable EIGRP on R1 and R2 for the subnet configured on their F0/0 interfaces. Make sure that EIGRP uses Autonomous System number 254 as illustrated in the topology.

Task 5:

Verify that an EIGRP adjacency has formed between R1 and R2 using appropriate commands.

SOLUTION:

Lab 41 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int fa0/0
R1(config-if)#ip add 10.1.1.1 255.255.255.0
R1(config-if)#end
R1#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int fa0/0
R2(config-if)#ip add 10.1.1.2 255.255.255.0
R2(config-if)#^Z
R2#
R2#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 = 1/3/4 ms
R2#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 = 4/4/4 ms
```

Task 4:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#router eigrp 254

R1(config-router)#network 10.0.0.0

R1(config-router)#end

R1#

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#router eigrp 254

R2(config-router)#network 10.0.0.0

R2(config-router)#end

R2#

*Mar  1 00:11:46.782: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 254: Neighbor 10.1.1.1
(FastEthernet0/0) is up: new adjacency

R2#
```

NOTE: When configuring EIGRP, you must use an Autonomous System Number. This can be any number from 1 through 65535. This is configured as follows:

```
R1(config)#router eigrp ?
  <1-65535>  Autonomous system number
```

In addition, when you configure EIGRP, you will see an adjancency form if EIGRP has been configured correctly. This will be indicated by the log message printed on the console:

```
*Mar  1 00:11:46.782: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 254: Neighbor 10.1.1.1
(FastEthernet0/0) is up: new adjacency
```

Task 5:

```
R1#show ip eigrp neighbors

IP-EIGRP neighbors for process 254

H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq

                                            (sec)         (ms)       Cnt Num
```

```
0   10.1.1.2             Fa0/0           13 00:07:40    1  4500  0  1

R1#

R2#show ip eigrp neighbors

IP-EIGRP neighbors for process 254

H   Address              Interface       Hold Uptime   SRTT   RTO  Q  Seq

                                 (sec)         (ms)      Cnt Num

0   10.1.1.1             Fa0/0           13 00:04:56  862  5000  0  1

R2#
```

Lab 42: Configuring EIGRP Routing Using Wildcard Masks

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to enable EIGRP routing using a single Autonomous System while using a wildcard mask for EIGRP network statements.

Lab Purpose:

Enabling basic EIGRP routing using wildcard masks is a fundamental skill. EIGRP is an advanced Distance Vector routing protocol. It is also a Cisco proprietary protocol that runs over IP protocol number 88. Wildcard masks allow EIGRP to be enabled for certain subnets within a major subnet and provide greater control for establish EIGRP neighbor adjacencies. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to enable basic EIGRP routing while using wildcard masks.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

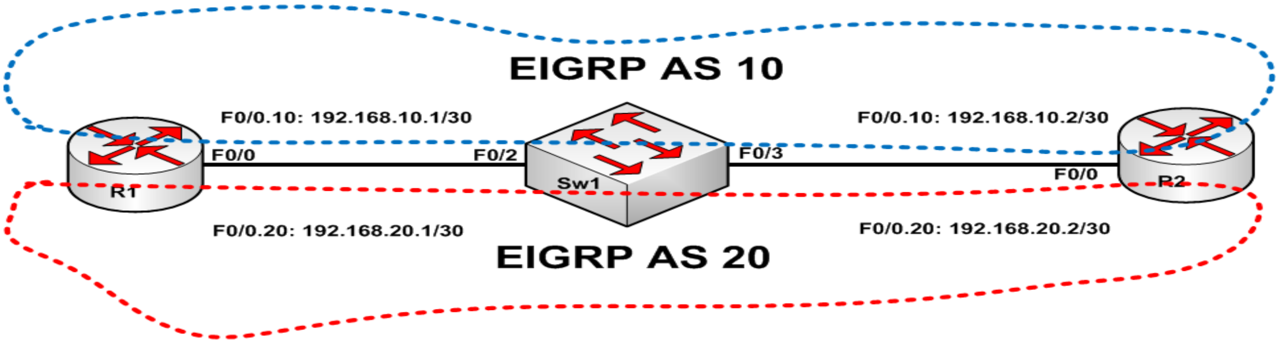
This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1, R2, and Sw1 as illustrated in the topology.

Task 2:

Configure VLAN 10 named EIGRP_10 and VLAN 20 named EIGRP_20 on Sw1. Next, configure Sw1 F0/2 and F0/3 as trunks. These should be connected to R1 and R2 F0/0 interfaces, respectively.

Task 3:

Configure subinterfaces Fa0/0.10 and F0/0.20 on R1 and R2. Subinterface Fa0/0.10 on either router should be associated with VLAN 10 and subinterface Fa0/0.20 on either router should be associated with VLAN 20. Configure IP addresses on both the subinterfaces as illustrated in the topology.

Task 4:

Ping between R1 and R2 on subinterface Fa0/0.10 and Fa0/0.20 to verify IP connectivity.

Task 5:

Enable EIGRP using Autonomous System 10 between R1 and R2 F0/0.10 subinterfaces. EIGRP using Autonomous System 10 should only be enabled for these interfaces. Use a wildcard mask to achieve this.

Task 6:

EIGRP using Autonomous System 20 between R1 and R2 F0/0.20 subinterfaces. EIGRP using Autonomous System 10 should only be enabled for these interfaces. Use a wildcard mask to achieve this.

Task 7:

Verify that you have two EIGRP adjacencies on R1 and R2. One adjacency should be for EIGRP using Autonomous System 10 and the other for EIGRP using Autonomous System 20.

SOLUTION:

Lab 42 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

```
Sw1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#vlan 10
Sw1(config-vlan)#name EIGRP_10
Sw1(config-vlan)#exit
Sw1(config)#vlan 20
Sw1(config-vlan)#name EIGRP_20
Sw1(config-vlan)#exit
Sw1(config)#int f0/2
Sw1(config-if)#switchport mode trunk
Sw1(config-if)#no shut
Sw1(config-if)#exit
Sw1(config)#int f0/3
Sw1(config-if)#switchport mode trunk
Sw1(config-if)#no shut
Sw1(config-if)#^Z
Sw1#show interfaces trunk
Port      Mode       Encapsulation  Status       Native vlan
Fa0/2      on        802.1q         trunking     1
Fa0/3      on        802.1q         trunking     1
Port      Vlans allowed on trunk
```

```
Fa0/2       1-4094

Fa0/3       1-4094

Port       Vlans allowed and active in management domain

Fa0/2       1,10,20

Fa0/3       1,10,20

Port       Vlans in spanning tree forwarding state and not pruned

Fa0/2       1,10,20

Fa0/3       1,10,20

Sw1#show vlan id 10

VLAN Name                             Status    Ports

---- -------------------------------- --------- -------------------------------

10   EIGRP_10                         active    Fa0/2, Fa0/3

Sw1#show vlan id 20

VLAN Name                             Status    Ports

---- -------------------------------- --------- -------------------------------

20   EIGRP_20                         active    Fa0/2, Fa0/3
```

Task 3:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int fa0/0

R1(config-if)#no shutdown

R1(config-if)#int fa0/0.10

R1(config-subif)#encapsulation dot1q 10

R1(config-subif)#ip address 192.168.10.1 255.255.255.252

R1(config-subif)#exit

R1(config)#int fa0/0.20

R1(config-subif)#encapsulation dot1q 20
```

```
R1(config-subif)#ip address 192.168.20.1 255.255.255.252
R1(config-subif)#end
R1#
R1#show ip int bri
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0              unassigned      YES manual up                    up
FastEthernet0/0.10         192.168.10.1     YES manual up                    up
FastEthernet0/0.20         192.168.20.1     YES manual up                    up
Serial0/0                  unassigned      YES NVRAM  administratively down down
Serial0/1                  unassigned      YES NVRAM  administratively down down
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int fa0/0
R2(config-if)#no shutdown
R2(config-if)#int fa0/0.10
R2(config-subif)#encapsulation dot1q 10
R2(config-subif)#ip address 192.168.10.2 255.255.255.252
R2(config-subif)#exit
R2(config)#int fa0/0.20
R2(config-subif)#encapsulation dot1q 20
R2(config-subif)#ip address 192.168.20.2 255.255.255.252
R2(config-subif)#end
R2#
R2#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0              unassigned      YES manual up                    up
FastEthernet0/0.10         192.168.10.2     YES manual up                    up
```

```
FastEthernet0/0.20        192.168.20.2    YES manual up                  up
Serial0/0                 unassigned      YES NVRAM  administratively down down
Serial0/1                 unassigned      YES NVRAM  administratively down down
```

Task 4:

```
R1#ping 192.168.10.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms

R1#ping 192.168.20.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms
```

Task 5:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#router eigrp 10

R1(config-router)#network 192.168.10.0 0.0.0.3

R1(config-router)#end

R1#

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#router eigrp 10

R2(config-router)#network 192.168.10.0 0.0.0.3

R2(config-router)#^Z

*Mar  1 00:52:23.436: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 192.168.10.1
(FastEthernet0/0.10) is up: new adjacency
```

```
R2#
```

NOTE: Understanding wildcard masks is an essential requirement for both the purposes of the CCNA certification as well as in the real world. To determine the wildcard mask, you can simply subtract the network mask for the network on which you want to enable a specific EIGRP Autonomous System from the Broadcast mask. This concept is illustrated in the subtraction table shown below:

Broadcast Mask	255	255	255	255
[minus] **Subnet Mask**	255	255	255	252
[equals] **Wildcard Mask**	0	0	0	3

In our example, the subnet mask of the 192.168.1.0/30 subnet is 255.255.255.252. If this is subtracted from the Broadcast mask of 255.255.255.255 the result is 0.0.0.3, which is the wildcard mask we use to enable EIGRP for this subnet. Take some time to practice configuring wildcard masks for different subnetted networks.

Task 6:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#router eigrp 20

R1(config-router)#net 192.168.20.0 0.0.0.3

R1(config-router)#end

R1#

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#router eigrp 20

R2(config-router)#network 192.168.20.0 0.0.0.3

R2(config-router)#^Z

*Mar  1 01:08:55.887: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 20: Neighbor 192.168.20.1
(FastEthernet0/0.20) is up: new adjacency

R2#
```

Task 7:

```
R1#show ip eigrp neighbors

IP-EIGRP neighbors for process 10
```

```
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.10.2            Fa0/0.10        12 00:18:51    1  4500  0  1
IP-EIGRP neighbors for process 20
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.20.2            Fa0/0.20        12 00:02:20    1  4500  0  1
R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.10.1            Fa0/0.10        10 00:17:58 1907  5000  0  1
IP-EIGRP neighbors for process 20
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.20.1            Fa0/0.20        11 00:01:26  452  2712  0  1
```

Lab 43: EIGRP Automatic Summarization

Lab Objective:

The objective of this lab exercise is for you to learn and understand how EIGRP performs automatic summarization at Classful network boundaries.

Lab Purpose:

Dealing with EIGRP automatic summarization is a fundamental skill. EIGRP is an advanced Distance Vector routing protocol. It is also a Cisco proprietary protocol that runs over IP protocol number 88. Because of the VLSM employed in the networks of today, automatic summarization is a default feature that should not be used. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to enable basic EIGRP routing.

Certification Level:

This lab is suitable for CCENT & CCNA certification exam preparation

Lab Difficulty:

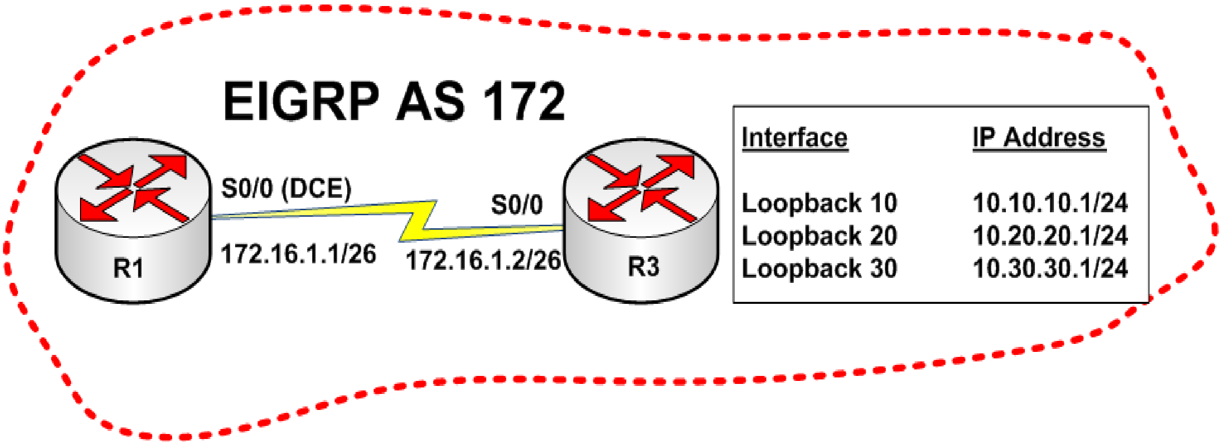
This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R3, as illustrated in the topology. Since R1 S0/0 is the DCE end of the back-to-back Serial connection, configure R1 to send R3 clocking information at a rate of 256Kbps. Configure the IP addresses for R1 and R3 S0/0 interfaces as specified in the topology and ping between the routers to verify connectivity based on your configuration.

Task 2:

Configure the Loopback interfaces on R3 as illustrated in the topology.

Task 3:

Enable EIGRP using Autonomous System 172 on both R1 and R3 and configure EIGRP network statements for R1 and R3 S0/0 interfaces and for the Loopback interfaces on R3.

Task 4:

On R1, verify the EIGRP routes you are receiving from R3. You should notice that you only have one route, which is 10.0.0.0/8 for the three Loopback interfaces configured on R3.

Task 5:

Configure R3 so that it does not perform automatic summarization at Classful boundaries and clear the IP routing table on R3 and R1 using the clear ip route * command.

Task 6:

On R1, verify the EIGRP routes you are receiving from R3. You should now have three routes for the 10.x.x.x/24 Loopback interfaces configured on R3 and advertised by EIGRP. Ping these IP addresses to verify connectivity.

SOLUTION:

Lab 43 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s0/0

R1(config-if)#no shutdown

R1(config-if)#clock rate 256000

R1(config-if)#ip address 172.16.1.1 255.255.255.192

R1(config-if)#end

R1#

R3#config ter

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int s0/0

R3(config-if)#no shutdown

R3(config-if)#ip address 172.16.1.2 255.255.255.192

R3(config-if)#^Z

R3#

R1#ping 172.16.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:

!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms

R3#ping 172.16.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
```

Task 2:

```
R3#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int lo 10

R3(config-if)#ip address 10.10.10.1 255.255.255.0

R3(config-if)#exit

R3(config)#int lo 20

R3(config-if)#ip address 10.20.20.1 255.255.255.0

R3(config-if)#exit

R3(config)#int lo 30

R3(config-if)#ip address 10.30.30.1 255.255.255.0

R3(config-if)#^Z

R1#
```

Task 3:

```
R1#conf terminal

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#router eigrp 172

R1(config-router)# network 172.16.1.0

R1(config-router)#end

R1#

R3#conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#router eigrp 172

R3(config-router)#network 10.0.0.0

R3(config-router)#network 172.16.1.0

R3(config-router)#^Z

*Mar  1 01:52:35.842: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 172: Neighbor 172.16.1.1
(Serial0/0) is up: new adjacency
```

Task 4:

```
R1#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

       ia - IS-IS inter area, * - candidate default, U - per-user static route

       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C       172.16.1.0/26 is directly connected, Serial0/0

C       172.16.3.0/25 is directly connected, FastEthernet0/0

D    10.0.0.0/8 [90/2297856] via 172.16.1.3, 00:04:24, Serial0/0
```

NOTE: Pay attention to the routing protocol keywords. Notice that Internal EIGRP routes are labeled with a D. A code type of D EX would be for External EIGRP routes.

Task 5:

```
R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#router eigrp 172

R3(config-router)#no auto-summary
```

```
R3(config-router)#end

*Mar  1 02:01:30.535: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 172: Neighbor 172.16.1.1
(Serial0/0) is down: summary configured

*Mar  1 02:01:30.599: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 172: Neighbor 172.16.1.1
(Serial0/0) is up: new adjacency
```

> **NOTE:** By default, in a manner similar to RIP, EIGRP will perform automatic summarization at Classful boundaries. It is considered good practice to disable this default feature.When you disable automatic summarization, the EIGRP adjacencies are reset, so be careful when performing this, especially in a production network environment. This is printed to the console as follows:
>
> ```
> *Mar  1 02:01:30.535: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 172: Neighbor 172.16.1.1
> (Serial0/0) is down: summary configured
> *Mar  1 02:01:30.599: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 172: Neighbor 172.16.1.1
> (Serial0/0) is up: new adjacency
> ```

Task 6:

```
R1#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

       ia - IS-IS inter area, * - candidate default, U - per-user static route

       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C       172.16.1.0/26 is directly connected, Serial0/0

C       172.16.3.0/25 is directly connected, FastEthernet0/0

     10.0.0.0/24 is subnetted, 3 subnets

D       10.30.30.0 [90/2297856] via 172.16.1.3, 00:05:37, Serial0/0

D       10.20.20.0 [90/2297856] via 172.16.1.3, 00:05:37, Serial0/0

D       10.10.10.0 [90/2297856] via 172.16.1.3, 00:05:37, Serial0/0
```

```
R1#ping 10.10.10.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms

R1#ping 10.20.20.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.20.20.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms

R1#ping 10.30.30.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.30.30.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
```

Lab 44: Passive Interfaces for EIGRP Updates

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to prevent EIGRP from sending unnecessary updates by using passive interfaces.

Lab Purpose:

Preventing unnecessary EIGRP updates using passive interfaces is a fundamental skill. By default, EIGRP sends updates via Multicast on all interfaces for which EIGRP has been enabled. This means that EIGRP adjacencies will form on all interfaces for which EIGRP has been enabled. In some cases, this may not be desirable and should be prevented. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to prevent EIGRP from sending unnecessary updates.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

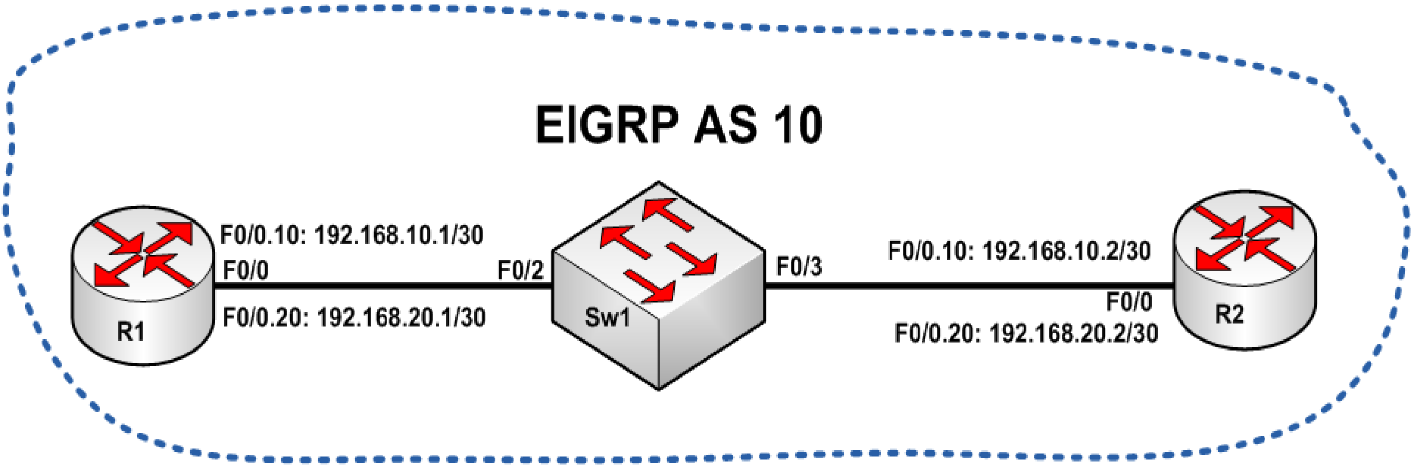
This lab has a difficulty rating of 7/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1, R2, and Sw1 as illustrated in the topology.

Task 2:

Configure VLAN 10 named EIGRP_10 and VLAN 20 named EIGRP_20 on Sw1. Next, configure Sw1 F0/2 and F0/3 as trunks. These should be connected to R1 and R2 F0/0 interfaces, respectively.

Task 3:

Configure subinterfaces Fa0/0.10 and F0/0.20 on R1 and R2. Subinterface Fa0/0.10 on either router should be associated with VLAN 10 and subinterface Fa0/0.20 on either router should be associated with VLAN 20. Configure IP addresses on both the subinterfaces as illustrated in the topology.

Task 4:

Ping between R1 and R2 on subinterface Fa0/0.10 and Fa0/0.20 to verify IP connectivity.

Task 5:

Enable EIGRP using Autonomous System 10 on R1 and R2 F0/0.10 and F0/0.20 subinterfaces and verify that you have two EIGRP neighbor adjacencies on R1 and R2, one through the F0/0.10 and the other through the Fa0/0.20 subinterface. On either R1 or R2, verify that you have two EIGRP adjacencies to your peer router.

Task 6:

Prevent EIGRP from forming an adjacency via Fa0/0.20 on R1 and R2. Verify that you now only have one EIGRP neighbor adjacency on R1 and R2, only through each F0/0.10 subinterface.

SOLUTION:

Lab 44 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 21 Configuration and Verification Task 1

Lab 35 Configuration and Verification Task 1

Task 2:

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#vlan 10

Sw1(config-vlan)#name EIGRP_10

Sw1(config-vlan)#exit

Sw1(config)#vlan 20

Sw1(config-vlan)#name EIGRP_20

Sw1(config-vlan)#exit

Sw1(config)#int f0/2

Sw1(config-if)#switchport mode trunk

Sw1(config-if)#no shut

Sw1(config-if)#exit

Sw1(config)#int f0/3

Sw1(config-if)#switchport mode trunk

Sw1(config-if)#no shut

Sw1(config-if)#^Z

Sw1#show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
```

```
Fa0/2     on          802.1q        trunking     1
Fa0/3     on          802.1q        trunking     1
Port      Vlans allowed on trunk
Fa0/2      1-4094
Fa0/3      1-4094
Port      Vlans allowed and active in management domain
Fa0/2      1,10,20
Fa0/3      1,10,20
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/2      1,10,20
Fa0/3      1,10,20
Sw1#show vlan id 10
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
10   EIGRP_10                         active    Fa0/2, Fa0/3
Sw1#show vlan id 20
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
20   EIGRP_20                         active    Fa0/2, Fa0/3
```

Task 3:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int fa0/0
R1(config-if)#no shutdown
R1(config-if)#int fa0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 192.168.10.1 255.255.255.252
```

```
R1(config-subif)#exit

R1(config)#int fa0/0.20

R1(config-subif)#encapsulation dot1q 20

R1(config-subif)#ip address 192.168.20.1 255.255.255.252

R1(config-subif)#end

R1#

R1#show ip int bri

Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0            unassigned      YES manual up                    up

FastEthernet0/0.10         192.168.10.1    YES manual up                    up

FastEthernet0/0.20         192.168.20.1    YES manual up                    up

Serial0/0              unassigned      YES NVRAM  administratively down down

Serial0/1              unassigned      YES NVRAM  administratively down down

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#int fa0/0

R2(config-if)#no shutdown

R2(config-if)#int fa0/0.10

R2(config-subif)#encapsulation dot1q 10

R2(config-subif)#ip address 192.168.10.2 255.255.255.252

R2(config-subif)#exit

R2(config)#int e0/0.20

R2(config-subif)#encapsulation dot1q 20

R2(config-subif)#ip address 192.168.20.2 255.255.255.252

R2(config-subif)#end

R2#

R2#show ip interface brief
```

```
Interface                IP-Address      OK? Method Status               Protocol
FastEthernet0/0              unassigned      YES manual up                   up
FastEthernet0/0.10        192.168.10.2    YES manual up                   up
FastEthernet0/0.20        192.168.20.2    YES manual up                   up
Serial0/0                unassigned      YES NVRAM  administratively down down
Serial0/1                unassigned      YES NVRAM  administratively down down
```

Task 4:

```
R1#ping 192.168.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms
R1#ping 192.168.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms
```

Task 5:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router eigrp 10
R1(config-router)#network 192.168.10.0
R1(config-router)#network 192.168.20.0
R1(config-router)#end
R1#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
R2(config)#router eigrp 10

R2(config-router)#network 192.168.10.0

R2(config-router)#network 192.168.20.0

R2(config-router)#end

*Mar  1 01:30:18.438: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 192.168.10.1
(FastEthernet0/0.10) is up: new adjacency

*Mar  1 01:30:22.124: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 192.168.20.1
(FastEthernet0/0.20) is up: new adjacency

R2#

R2#

R2#show ip eigrp neighbors

IP-EIGRP neighbors for process 10

H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq

                                            (sec)         (ms)       Cnt Num

1   192.168.20.1            Fa0/0.20          11 00:02:31 1779  5000  0  2

0   192.168.10.1            Fa0/0.10          12 00:02:34  809  4854  0  1
```

Task 6:

```
R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#router eigrp 10

R2(config-router)#passive-interface e0/0.20

R2(config-router)#

*Mar  1 01:34:53.925: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 192.168.20.1
(FastEthernet0/0.20) is down: interface passive

R2(config-router)#end

R2#

R2#show ip eigrp neighbors

IP-EIGRP neighbors for process 10

H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
```

```
                              (sec)       (ms)      Cnt Num

0   192.168.10.1          Fa0/0.10        11 00:04:46  647  3882  0  3

R2#
```

NOTE: When configuring passive interfaces under EIGRP, it is important to know that this needs only be applied to either side of the adjacency to prevent routing updates on that interface. In our example, specifying FastEthernet0/0.20 in R2 as passive dropped the adjacency on R1 and R2 FastEthernet0/0.20 dropping.

Lab 45: Summarizing Routes with EIGRP

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to summarize routes with EIGRP. Route summarization allows the size of routing tables to be reduced by advertising a summary route for a range of multiple specific routes.

Lab Purpose:

Route summarization is a fundamental skill. With the subnetted networks of today, routing tables can grow very large due to the sheer number of network entries. In order to reduce the burden of extremely large routing tables on routers, route summarization can be used. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure a EIGRP route summarization.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

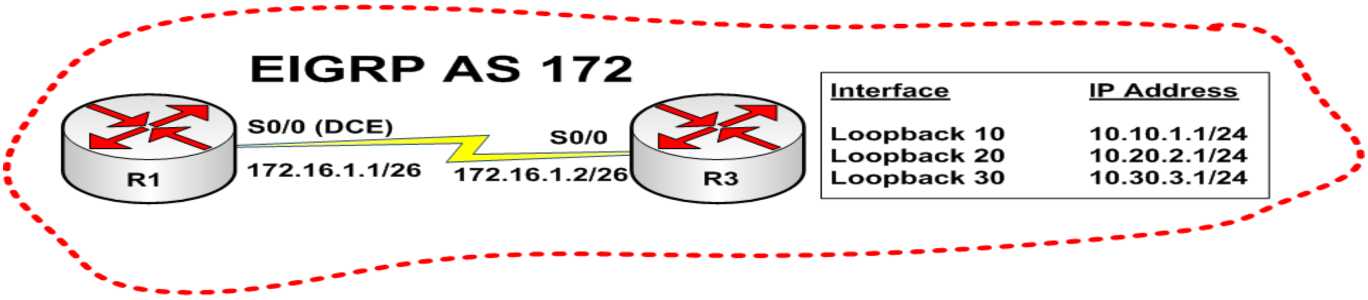
This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R3, as illustrated in the topology. Since R1 S0/0 is the DCE end of the back-to-back Serial connection, configure R1 to send R3 clocking information at a rate of 256Kbps. Configure the IP addresses for R1 and R3 S0/0 interfaces as specified in the topology and ping between the routers to verify connectivity based on your configuration.

Task 2:

Configure the Loopback interfaces on R3 as illustrated in the topology.

Task 3:

Enable EIGRP using Autonomous System 172 on both R1 and R3 and configure EIGRP network statements for R1 and R3 S0/0 interfaces and for the Loopback interfaces on R3. Ensure that EIGRP does not perform automatic summarization at Classful network boundaries.

Task 4:

On R1, verify the EIGRP routes you are receiving from R3. You should have three routes for the 10.x.x.x/24 Loopback interfaces configured on R3 and advertised by EIGRP. Ping these IP addresses to verify connectivity.

Task 5:

Configure R3 send a summarized route for the 10.x.x.x/24 Loopback interfaces to R1.

Task 6:

Verify the EIGRP routes you are receiving from R3 on R1. You should now have one route for the 10.x.x.x/24 Loopback interfaces configured on R3 and advertised by EIGRP. Ping these IP addresses to verify connectivity.

SOLUTION:

Lab 45 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

For reference information on configuring DCE clocking, please refer to:

Lab 21 Configuration and Verification Task 2

Lab 35 Configuration and Verification Task 2

Task 2:

For reference information on configuring Loopback interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

Lab 39 Configuration and Verification Task 4

Lab 43 Configuration and Verification Task 2

Task 3:

For reference information on enabling EIGRP, please refer to:

Lab 41 Configuration and Verification Task 4

Lab 42 Configuration and Verification Task 5

Lab 44 Configuration and Verification Task 5

Task 4:

```
R1#show ip route eigrp

     10.0.0.0/24 is subnetted, 3 subnets

D       10.30.3.0 [90/2297856] via 172.16.1.2, 00:00:33, Serial0/0

D       10.20.2.0 [90/2297856] via 172.16.1.2, 00:00:34, Serial0/0

D       10.10.1.0 [90/2297856] via 172.16.1.2, 00:00:34, Serial0/0

R1#ping 10.10.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms

R1#ping 10.20.2.1

Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.20.2.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms

R1#ping 10.30.3.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.30.3.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
```

Task 5:

NOTE: For a refresher on how to create a summary address, you can refer to Lab 39 Configuration and Verification Task 6. Using the same concept in that example, our second octet in Binary notation for the three Loopback interface subnets on R3 would be written as follows:

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
0	0	0	0	1	0	1	0
0	0	0	1	0	1	0	0
0	0	0	0	0	0	1	0
0	0	0	1	1	1	1	0

The last value under which all four bits are the same is 32. Therefore, to determine the summary address, insert a value of 1 all the way through the column with the 4 in it and add those bits up. The answer will be the Decimal value which you will use to create the summary address subnet mask. This is illustrated as follows:

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
1	1	1	0	0	0	0	0

The subnet mask for your summarized network would be 128 + 64 + 32 which equals 224. The summary address would then be written as 10.0.0.0 255.255.224.0 or 10.0.0.0/11. To configure EIGRP to send this summary address instead of the three 10.x.x.x/24 network entries, use the ip summary-address eigrp <as-number> command under the interface EIGRP uses to send updates to other RIPv2 routers as illustrated below. Do not forget to add the Autonomous System Number when configuring EIGRP route summarization.

```
R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int s0/0

R3(config-if)#ip summ

R3(config-if)#ip summary-address eigrp 172 10.0.0.0 255.224.0.0
```

```
R3(config-if)#end

*Mar  1 02:39:48.125: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 172: Neighbor 172.16.1.1
(Serial0/0) is down: summary configured

*Mar  1 02:39:50.305: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 172: Neighbor 172.16.1.1
(Serial0/0) is up: new adjacency

R3#

R3#show running-config interface s0/0

Building configuration...

Current configuration : 134 bytes

!

interface Serial0/0

 ip address 172.16.1.2 255.255.255.192

 ip summary-address eigrp 172 10.0.0.0 255.224.0.0 5

 no fair-queue

end
```

NOTE: As can be seen in the output above, when an EIGRP summary address is configured, the EIGRP neighbor adjacencies via that interface are reset. Be careful when doing this in a production network environment. Because of this, there is no need to issue the clear ip route * as we did when we configured RIP summarization. Also notice that under the interface configuration, even though we issued the command ip summary-address eigrp 172 10.0.0.0 255.224.0.0 there is an additional 5 at the end. This is because EIGRP summary routes have a default Administrative Distance of 5. This can be viewed on the router perfoming the summarization as follows:

```
R3#show ip ro eigrp
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
D       10.0.0.0/11 is a summary, 00:00:13, Null0

R3#show ip eigrp topology
IP-EIGRP Topology Table for AS(172)/ID(172.16.3.3)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.0.0.0/11, 1 successors, FD is 128256
        via Summary (128256/0), Null0
```

Summary routes in EIGRP will always point to the Null0 interface which is simply a logical black-hole interface in Cisco IOS routers. Detailed knowledge of Null0 is beyond the scope of this course, so don't worry too much about it; however, be familiar with the fact that EIGRP summary routes will be automatically created and use Null0.

Task 6:

```
R1#show ip route eigrp

     10.0.0.0/11 is subnetted, 1 subnets

D       10.0.0.0 [90/2297856] via 172.16.1.2, 00:03:20, Serial0/0

R1#ping 10.10.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms

R1#ping 10.20.2.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.20.20.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms

R1#ping 10.30.3.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.30.30.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
```

NOTE: EIGRP summary routes have an Administrative Distance of 5. This can be verified using the show ip route command.

Lab 46: Verifying the EIGRP Database

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to verify the EIGRP database using the appropriate Cisco IOS commands.

Lab Purpose:

Verifying the EIGRP database is a fundamental skill. EIGRP is an advanced Distance Vector protocol that incorporates features from both Distance Vector and Link State routing protocols. The EIGRP database is a feature of Link State routing protocols. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to verify routes in the EIGRP database.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

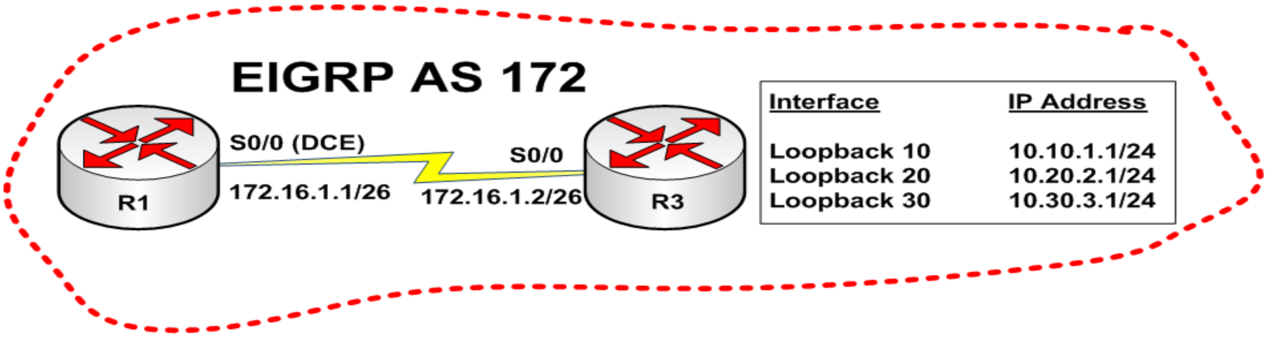
This lab has a difficulty rating of 6/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Interface	IP Address
Loopback 10	10.10.1.1/24
Loopback 20	10.20.2.1/24
Loopback 30	10.30.3.1/24

Task 1:

Configure the hostnames on routers R1 and R3, as illustrated in the topology. Since R1 S0/0 is the DCE end of the back-to-back Serial connection, configure R1 to send R3 clocking information at a rate of 256Kbps. Configure the IP addresses for R1 and R3 S0/0 interfaces as specified in the topology and ping between the routers to verify connectivity based on your configuration.

Task 2:

Configure the Loopback interfaces on R3 as illustrated in the topology.

Task 3:

Enable EIGRP using Autonomous System 172 on both R1 and R3 and configure EIGRP network statements for R1 and R3 S0/0 interfaces and for the Loopback interfaces on R3. Ensure that EIGRP does not perform automatic summarization at Classful network boundaries.

Task 4:

On R1, verify the state of the received routes in the EIGRP database using the appropriate show commands. To take a more detailed look, also verify the EIGRP database information of the 10.20.20.0/24 subnet.

SOLUTION:

Lab 46 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

For reference information on configuring DCE clocking, please refer to:

Lab 21 Configuration and Verification Task 2

Lab 35 Configuration and Verification Task 2

Task 2:

For reference information on configuring Loopback interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

Lab 39 Configuration and Verification Task 4

Lab 43 Configuration and Verification Task 2

Task 3:

For reference information on enabling EIGRP, please refer to:

Lab 41 Configuration and Verification Task 4

Lab 42 Configuration and Verification Task 5

Lab 44 Configuration and Verification Task 5

Task 4:

```
R1#show ip route eigrp

     10.0.0.0/24 is subnetted, 3 subnets
```

```
D       10.30.30.0 [90/2297856] via 172.16.1.2, 00:00:33, Serial0/0

D       10.20.20.0 [90/2297856] via 172.16.1.2, 00:00:34, Serial0/0

D       10.10.10.0 [90/2297856] via 172.16.1.2, 00:00:34, Serial0/0

R1#ping 10.10.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms

R1#ping 10.20.2.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.20.20.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms

R1#ping 10.30.3.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.30.30.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms

R1#show ip eigrp topology

IP-EIGRP Topology Table for AS(172)/ID(17.16.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,

       r - reply Status, s - sia Status

P 10.30.30.0/24, 1 successors, FD is 2297856

        via 172.16.1.2 (2297856/128256), Serial0/0

P 10.20.20.0/24, 1 successors, FD is 2297856

        via 172.16.1.2 (2297856/128256), Serial0/0

P 10.10.10.0/24, 1 successors, FD is 2297856
```

```
        via 172.16.1.2 (2297856/128256), Serial0/0

P 172.16.1.0/26, 1 successors, FD is 2169856

        via Connected, Serial0/0
```

The output of the show ip eigrp topology command will show you, the EIGRP router ID of the local router, the route metric, Feasible Distance, Successors, and Fesible Successors (if applicable). These are core EIGRP components that you are expected to know. Take some time to familiarize yourself with the information contained in the output of this command.

```
R1#show ip eigrp topology 10.20.2.0 255.255.255.0

IP-EIGRP (AS 172): Topology entry for 10.20.2.0/24

  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 2297856

  Routing Descriptor Blocks:

  172.16.1.2 (Serial0/0), from 172.16.1.2, Send flag is 0x0

      Composite metric is (2297856/128256), Route is Internal

      Vector metric:

        Minimum bandwidth is 1544 Kbit

        Total delay is 25000 microseconds

        Reliability is 255/255

        Load is 1/255

        Minimum MTU is 1500

        Hop count is 1
```

The output of the show ip eigrp topology [network] [mask] command will show you who the route is from, the composite metric of theroute and the components included in the calculation of the metric, such as bandwitch, delay, reliability, load and MTU. It also includes the hop count of the route. Again, these are core EIGRP components that you are expected to know. Therefore, take some time to familiarize yourself with the information contained in the output of this command.

Lab 47: EIGRP Split Horizon

Lab Objective:

The objective of this lab exercise is for you to learn and understand the effects of Split Horizon in a typical hub and spoke topology.

Lab Purpose:

Configuring and troubleshooting Split Horizon is a fundamental skill. EIGRP is an advanced Distance Vector protocol, and as such uses Split Horizon to prevent routing loops. Split Horizon mandates that EIGRP will not send updates back out of the interface on which they were received. While this default feature is generally a good thing, it can have a disastrous effect on traditional hub and spoke topologies. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to address Split Horizon issues in EIGRP.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 8/10

Readiness Assessment:

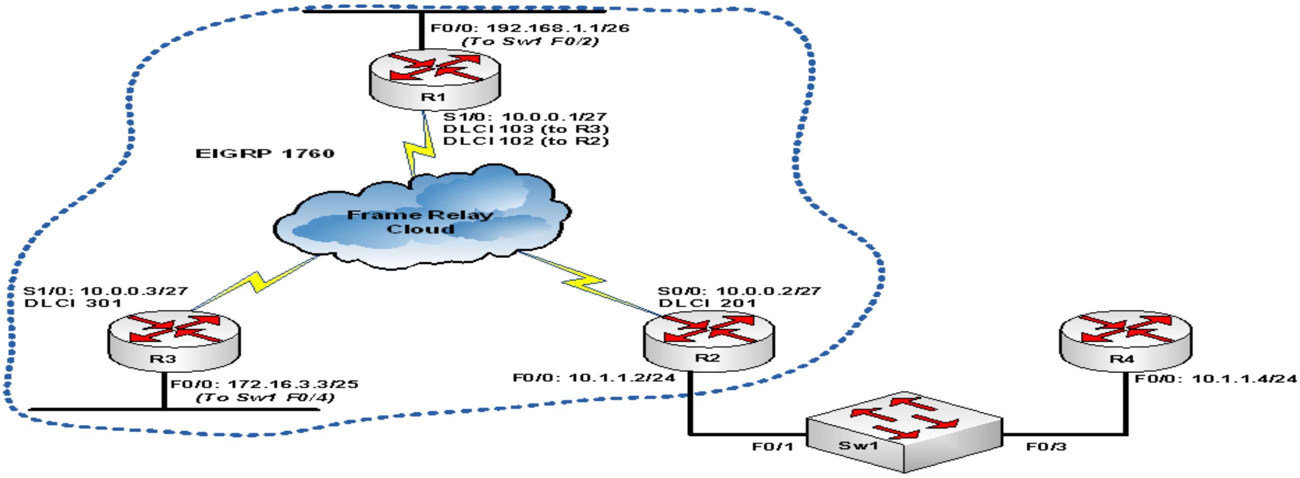
When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

IMPORTANT NOTE:

In order to configure Frame Relay between two routers in your lab, you will need THREE routers! The first two routers will be regular routers, and the third will need to be configured as a Frame Relay switch. This can be any Cisco router that has at least two Serial interfaces. Please refer to **Appendix B: Cabling and configuring a Frame Relay Switch For Three Routers** for the appropriate configuration to issue on the Frame Relay switch.

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

This lab will only be performed on R1, R2, and R3. Configure the hostnames on routers R1, R2, and R3 as above.

Task 2:

Configure the switch in the topology with the hostname Sw1. Enable F0/1, F0/2, and F0/4 on Sw1 so that when you bring up the router interfaces connected to those switch ports they can come up.

Task 3:

Configure IP addresses on the Fa0/0 interfaces on R1, R2, and R3. Make sure you enable these interfaces and they are up.

Task 4:

Configure Frame Relay on R1, R2, and R3. Use the IP addresses in the topology for their respective Serial interfaces. Use the default Frame Relay encapsulation of Cisco. Configure static Frame Relay maps between R1, R2, and R3, so that each router has a static Frame Relay map to the other two routers on the Frame Relay network.

Task 5:

Enable EIGRP in AS 1760 on R1, R2, and R3 for all the subnets configured on those respective routers. Be sure to prevent EIGRP from automatically summarizing at Classful network boundaries.

Task 6:

If you have configured everything as requested, you will not be able to see the 10.1.1.0/24 route via EIGRP on R3 nor will you be able to see the 172.16.3.0/25 route via EIGRP on R2. However, R1 will have both routes. Verify that this is the case using the appropriate commands.

Task 7:

Based on your studies, you know that the reason you are not seeing the 10.1.1.0/24 route via EIGRP on R3 and the 172.16.3.0/25 route via EIGRP on R2 is because these routes are both sent to R1 via EIGRP, but since Distance Vector protocols do not send routing information back out of the same interface they received it, R1 will not send the routing information for 10.1.1.0/24 to R3 or the routing information for 172.16.3.0/25 since the routing information was received on the same interface. To prevent this from happening, disable this default feature.

Task 8:

Now verify that you can see the 10.1.1.0/24 route via EIGRP on R3 and the 172.16.3.0/25 route via EIGRP on R2. Ping 10.1.1.1 from R3 and 172.16.3.3 from R2 to verify network connectivity.

SOLUTION:

Lab 47 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 21 Configuration and Verification Task 1

Lab 35 Configuration and Verification Task 1

Task 2:

```
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Sw1
Sw1(config)#interface fastethernet0/1
Sw1(config-if)#no shutdown
Sw1(config-if)#exit
Sw1(config)#interface fastethernet0/2
Sw1(config-if)#no shutdown
Sw1(config-if)#exit
Sw1(config)#interface fastethernet0/4
Sw1(config-if)#no shutdown
Sw1(config-if)#end
Sw1#
```

Task 3:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int fa0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.192
R1(config-if)#no shutdown
R1(config-if)#end
```

```
R1#
R1#show ip interface brief
Interface            IP-Address      OK? Method Status              Protocol
FastEthernet0/0         192.168.1.1     YES manual up                   up
Serial1/0            unassigned      YES unset  administratively down down
Serial0/1            unassigned      YES unset  administratively down down
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int fa0/0
R2(config-if)#ip add 10.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#end
R2#
R2#show ip int brie
Interface            IP-Address      OK? Method Status              Protocol
FastEthernet0/0         10.1.1.2       YES manual up                   up
Serial0/0            unassigned      YES unset  administratively down down
Serial0/1            unassigned      YES unset  administratively down down
R3#config term
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int fa0/0
R3(config-if)#ip address 172.16.3.3 255.255.255.128
R3(config-if)#no shutdown
R3(config-if)#end
R3#
R3#show ip interface brief
Interface            IP-Address      OK? Method Status              Protocol
```

```
FastEthernet0/0          172.16.3.3      YES manual up                   up
Serial/0               unassigned      YES unset  administratively down down
Serial0/1              unassigned      YES unset  administratively down down
```

Task 4:

For reference information on verifying Frame Relay mapping, please refer to:

Lab 40 Configuration and Verification Task 4

Lab 40 Configuration and Verification Task 5

```
R1#show frame-relay map
Serial1/0(up): ip 10.0.0.2 dlci 102(0x66,0x1860), static,
              broadcast,
              CISCO, status defined, active
Serial1/0 (up): ip 10.0.0.3 dlci 103(0x67,0x1870), static,
              broadcast,
              CISCO, status defined, active
```

```
R2#show frame-relay map
Serial0/0 (up): ip 10.0.0.1 dlci 201(0xC9,0x3090), static,
              broadcast,
              CISCO, status defined, active
Serial0/0 (up): ip 10.0.0.3 dlci 201(0xC9,0x3090), static,
              broadcast,
              CISCO, status defined, active
```

```
R3#show frame-relay map
Serial1/0 (up): ip 10.0.0.1 dlci 301(0x12D,0x48D0), static,
              broadcast,
              CISCO, status defined, active
Serial1/0 (up): ip 10.0.0.2 dlci 301(0x12D,0x48D0), static,
              broadcast,
         CISCO, status defined, active
```

Task 5:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router eigrp 1760
R1(config-router)#no auto-summary
R1(config-router)#net 10.0.0.0
R1(config-router)#network 192.168.1.0
R1(config-router)#end
R1#
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router eigrp 1760
R2(config-router)#no auto-summary
R2(config-router)#network 10.0.0.0
R2(config-router)#network 10.1.1.0
R2(config-router)#^Z
R2#
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router eigrp 1760
R3(config-router)#no auto-summary
R3(config-router)#network 10.0.0.0
R3(config-router)#network 172.16.3.0
R3(config-router)#^Z
R3#
R1#show ip eigrp neighbors
```

```
IP-EIGRP neighbors for process 1760
H   Address               Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                          (sec)         (ms)       Cnt Num
1   10.0.0.2              Se1/0           165 00:01:07   24   200  0  2
0   10.0.0.3              Se1/0           153 00:01:25  124   744  0  2
```

R2#**show ip eigrp neighbors**

```
IP-EIGRP neighbors for process 1760
H   Address               Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                          (sec)         (ms)       Cnt Num
0   10.0.0.1              Se0/0           128 00:00:53  911  5000  0  4
```

R3#**show ip eigrp neighbors**

```
IP-EIGRP neighbors for process 1760
H   Address               Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                          (sec)         (ms)       Cnt Num
0   10.0.0.1              Se1/0           156 00:02:20    8   200  0  4
```

Task 6:

R3#**show ip route eigrp**

```
     192.168.1.0/26 is subnetted, 1 subnets
D       192.168.1.0 [90/2195456] via 10.0.0.1, 00:10:53, Serial1/0
```

R2#**show ip route eigrp**

```
     192.168.1.0/26 is subnetted, 1 subnets
D       192.168.1.0 [90/2195456] via 10.0.0.1, 00:10:55, Serial0/0
```

R1#**show ip route eigrp**

```
     172.16.0.0/25 is subnetted, 1 subnets
D       172.16.3.0 [90/2195456] via 10.0.0.3, 00:12:23, Serial1/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.1.1.0/24 [90/2195456] via 10.0.0.2, 00:12:04, Serial1/0
```

Task 7:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s1/0

R1(config-if)#no ip split-horizon eigrp 1760

R1(config-if)#end

R1#

*Mar  1 01:20:39.104: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1760: Neighbor 10.0.0.2
(Serial1/0) is down: split horizon changed

*Mar  1 01:20:39.108: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1760: Neighbor 10.0.0.3
(Serial1/0) is down: split horizon changed

*Mar  1 01:20:39.677: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1760: Neighbor 10.0.0.3
(Serial1/0) is up: new adjacency

*Mar  1 01:21:34.122: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1760: Neighbor 10.0.0.2
(Serial1/0) is up: new adjacency
```

NOTE: When you disable (or re-enable) Split Horizon on an interface, all EIGRP adjacencies that have been established via that interface are reset as indicated in the output above. You can verify the neighbors have reestablished successfully using the show ip eigrp neighbors command as illustrated in the following output.

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1760
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                    (sec)         (ms)       Cnt Num
1   10.0.0.2                Se1/0           131 00:00:50 1512  5000  0  4
0   10.0.0.3                Se1/0           131 00:01:44   13   200  0  5
```

Task 8:

```
R2#show ip route eigrp

     172.16.0.0/25 is subnetted, 1 subnets

D       172.16.3.0 [90/2707456] via 10.0.0.1, 00:00:05, Serial0/0

     192.168.1.0/26 is subnetted, 1 subnets

D       192.168.1.0 [90/2195456] via 10.0.0.1, 00:00:05, Serial0/0

R2#ping 172.16.3.3

Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.3.3, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/32/40 ms

R3#show ip route eigrp

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

D       10.1.1.0/24 [90/2707456] via 10.0.0.1, 00:00:47, Serial1/0

     192.168.1.0/26 is subnetted, 1 subnets

D       192.168.1.0 [90/2195456] via 10.0.0.1, 00:00:47, Serial1/0

R3#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 = 24/27/32 ms
```

Lab 48: Configuring OSPF on Point-to-Point Networks

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to enable OSPF on point-to-point network types. These include HDLC and PPP.

Lab Purpose:

Enabling OSPF on point-to-point network types is a fundamental skill. OSPF is the most popular Interior Gateway Protocol (IGP) and it is imperative to understand how OSPF adjacencies are established on point-to-point network types. OSPF uses the concept of Areas. In order for two OSPF-enabled routers to establish an adjacency, they must reside in the same OSPF Area. Unlike EIGRP which uses Autonomous System Numbers, OSPF is enabled using a locally significant Process ID. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to enable OSPF on point-to-point network types.

Certification Level:

This lab is suitable for CCENT & CCNA certification exam preparation

Lab Difficulty:

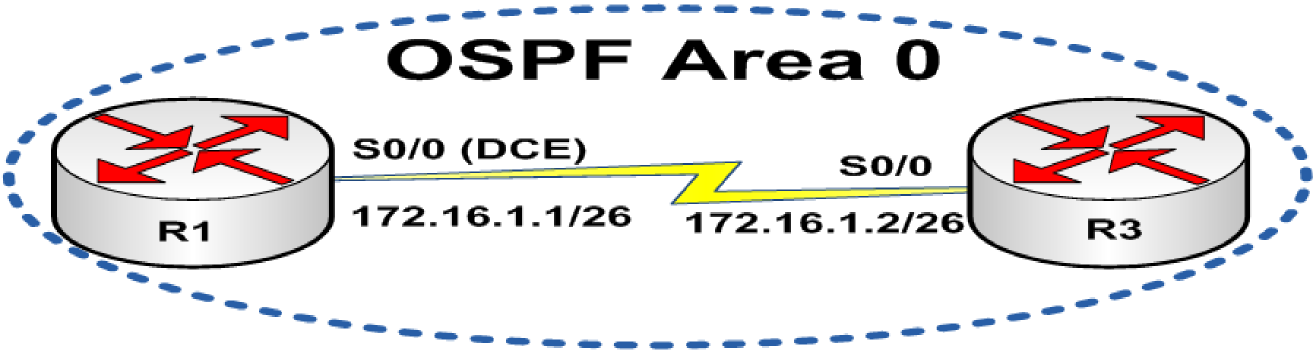
This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R3 as illustrated in the topology.

Task 2:

Configure R1 S0/0 which is a DCE to provide a clock rate of 768Kbps to R3. Enable PPP on the link between R1 and R3 configure the IP addresses illustrated in the topology.

Task 3:

Enable OSPF in Area 0 between R1 and R3. For R1, use an OSPF Process ID of 1. For R3 use an OSPF Process ID of 3. Verify your OSPF adjacency has formed between R1 and R3. Also verify that the default network type for the PPP link between R1 and R3 is point-to-point.

SOLUTION:

Lab 48 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 21 Configuration and Verification Task 1

Lab 35 Configuration and Verification Task 1

Task 2:

R1#**conf t**

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#**int s0/0**

```
R1(config-if)#clock rate 768000

R1(config-if)#encapsulation ppp

R1(config-if)#ip address 172.16.1.1 255.255.255.192

R1(config-if)#no shut

R1(config-if)#end

R1#

R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int s0/0

R3(config-if)#ip address 172.16.1.2 255.255.255.192

R3(config-if)#encap ppp

R3(config-if)#no shutdown

R3(config-if)#^Z

R3#

R1#ping 172.16.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:

!!!!!

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

R3#ping 172.16.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
```

Task 3:

NOTE: Unlike EIGRP configuration where wildcard masks following network statements are optional, in OSPF you MUST use a wildcard mask with your network statements. To determine the wildcard mask, you can simply subtract the network mask for the network on which you want to enable OSPF from the Broadcast mask. This concept is illustrated in the subtraction table shown below:

Broadcast Mask	255	255	255	255
[minus] **Subnet Mask**	255	255	255	192
[equals] **Wildcard Mask**	0	0	0	63

In our example, the subnet mask of the 172.16.1.0/26 subnet is 255.255.255.192. If this is subtracted from the Broadcast mask of 255.255.255.255 the result is 0.0.0.63, which is the wildcard mask we use to enable OSPF for this subnet. Take some time to practice configuring wildcard masks for different subnets.

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#router ospf 1

R1(config-router)#network 172.16.1.0 0.0.0.63 area 0

R1(config-router)#end

R1#

R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#router ospf 3

R3(config-router)#network 172.16.1.0 0.0.0.63 area 0

R3(config-router)#^Z

R3#

R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface

172.16.1.2        0   FULL/  -        00:00:36    172.16.1.2      Serial0/0

R1#show ip ospf interface serial 0/0

Serial0/0 is up, line protocol is up

  Internet Address 172.16.1.1/26, Area 0

  Process ID 1, Router ID 172.16.1.1, Network Type POINT_TO_POINT, Cost: 64

  Transmit Delay is 1 sec, State POINT_TO_POINT,

  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
    oob-resync timeout 40
    Hello due in 00:00:06
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.1.2
  Suppress hello for 0 neighbor(s)
```

NOTE: When verifying OSPF adjacencies, always ensure that neighbors are in the FULL state for point-to-point networks. If they are in any other state, you will need to perform some troubleshooting to identify the root cause of the issue. Take a moment to look at the detail contained in the output of the show ip ospf interface serial 0/0 command. From this output, we can determine that the OSPF network type is point-to-point: Network Type POINT_TO_POINT; the interface has an OSPF metric, or cost of 64: Cost: 64; and at the very botton, there is one OSPF neighbor with which an OSPF adjacency has been created via this interface as depicted in the line Adjacent with neighbor 172.16.1.2.

Lab 49: Configuring OSPF on Broadcast Networks

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to enable OSPF on Broadcast network types. These include Ethernet and Token Ring.

Lab Purpose:

Enabling OSPF on Broadcast network types is a fundamental skill. OSPF is the most popular Interior Gateway Protocol (IGP) and it is imperative to understand how OSPF adjacencies are established on Broadcast network types. OSPF uses the concept of Areas. In order for two OSPF-enabled routers to establish an adjacency, they must reside in the same OSPF Area. Unlike EIGRP which uses Autonomous System Numbers, OSPF is enabled using a locally significant Process ID. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to enable OSPF on point-to-point network types.

Certification Level:

This lab is suitable for CCENT & CCNA certification exam preparation

Lab Difficulty:

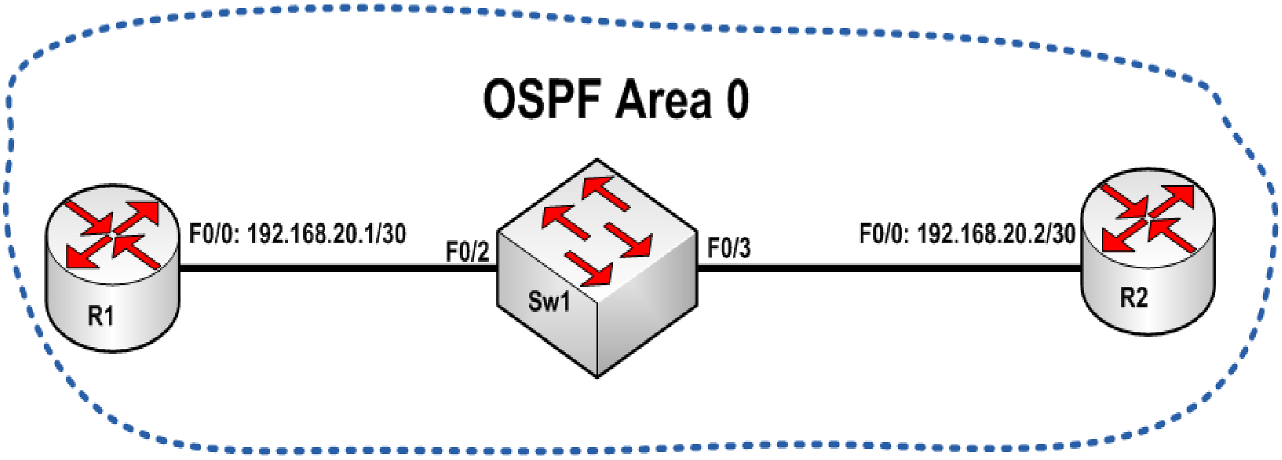
This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1, R2 and Sw1 as illustrated in the topology.

Task 2:

Configure VLAN 4010 on Sw1 and name it OSPF_VLAN. Assign ports FastEthernet0/2 and FastEthernet0/3 to this VLAN as access ports. Configure IP addresses on R1 and R2 FastEthernet0/0 interfaces and enable them.

Task 3:

Enable OSPF in Area 0 between R1 and R2. For R1, use an OSPF Process ID of 1 and for R2; use an OSPF Process ID of 2. Verify your OSPF adjacency has formed between R1 and R3. Also verify that the default network type for the Ethernet link between R1 and R3 is Broadcast.

SOLUTION:

Lab 49 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

```
Sw1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Sw1(config)#vlan 4010
Sw1(config-vlan)#name OSPF_VLAN
Sw1(config-vlan)#exit
Sw1(config)#
Sw1(config)#interface fastethernet0/2
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 4010
Sw1(config-if)#no shut
Sw1(config-if)#exit
Sw1(config)#interface fastethernet0/2
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 4010
Sw1(config-if)#no shut
Sw1(config-if)#end
Sw1#
Sw1#show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
```

```
                                        Fa0/17, Fa0/18, Fa0/19, Fa0/20

                                        Fa0/21, Fa0/22, Fa0/23, Fa0/24

                                        Gi0/1, Gi0/2

1002 fddi-default                     active

1003 token-ring-default                 active

1004 fddinet-default                   active

1005 trnet-default                     active

4010 OSPF_VLAN                          active      Fa0/2, Fa0/3

Sw1#

R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int fa0/0

R1(config-if)#ip address 192.168.20.1 255.255.255.252

R1(config-if)#no shut

R1(config-if)#end

R1#

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#int fast 0/0

R2(config-if)#ip add 192.168.20.2 255.255.255.252

R2(config-if)#no shut

R2(config-if)#^Z

R2#

R2#

R1#ping 192.168.20.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
```

```
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms
```

Task 3:

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 2
R2(config-router)#network 192.168.20.0 0.0.0.3 area 0
R2(config-router)#^Z
R2#
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#network 192.168.20.0 0.0.0.3 area 0
R1(config-router)#end
R1#
Mar  1 01:53:20.828: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.20.2 on FastEthernet0/0
from LOADING to FULL, Loading Done
R1#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.20.2      1   FULL/DR         00:00:37    192.168.20.2    Ethernet0/0
R1#show ip ospf interface fastethernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 192.168.20.1/30, Area 0
  Process ID 1, Router ID 192.168.20.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 192.168.20.2, Interface address 192.168.20.2
  Backup Designated router (ID) 192.168.20.1, Interface address 192.168.20.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
    oob-resync timeout 40

    Hello due in 00:00:04

  Index 1/1, flood queue length 0

  Next 0x0(0)/0x0(0)

  Last flood scan length is 1, maximum is 1

  Last flood scan time is 0 msec, maximum is 0 msec

  Neighbor Count is 1, Adjacent neighbor count is 1

    Adjacent with neighbor 192.168.20.2  (Designated Router)

  Suppress hello for 0 neighbor(s)
```

NOTE: On Broadcast and Non-Broadcast Multi-Access Networks, OSPF elects a Designated Router and a Backup Designated router for the subnet. So when you are verifying OSPF adjacencies on these network types, make sure that the state is either FULL/DR, FULL/BDR, or FULL/DROTHER. The output of the show ip ospf interface command shows that the elected DR is R2: Designated Router (ID) 192.168.20.2, and that R1 is the BDR: Backup Designated router (ID) 192.168.20.1.

Lab 50: Configuring OSPF on Non-Broadcast Networks

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to enable OSPF on Non-Broadcast network types. These include Frame Relay and SMDS.

Lab Purpose:

Enabling OSPF on Non-Broadcast network types is a fundamental skill. OSPF is the most popular Interior Gateway Protocol (IGP) and it is imperative to understand how OSPF adjacencies are established on Non-Broadcast network types. OSPF uses the concept of Areas. In order for two OSPF-enabled routers to establish an adjacency, they must reside in the same OSPF Area. Unlike EIGRP which uses Autonomous System Numbers, OSPF is enabled using a locally significant Process ID. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to enable OSPF on point-to-point network types.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

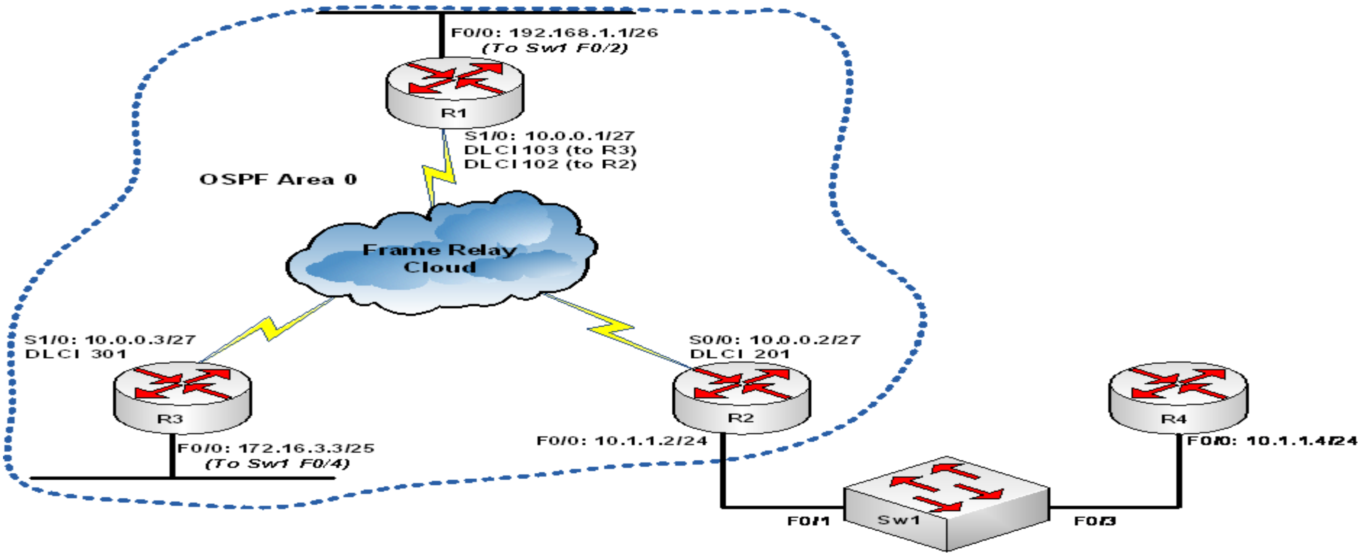
This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

This lab will only be concerned with configuration on R1, R2, and R3. To begin with, configure the hostnames on routers R1, R2 and R3 as illustrated in the topology.

Task 2:

Enable the Serial interfaces of R1, R2, and R3 for Frame Relay encapsulation and use static maps for each router to the other two routers. For example, create a static Frame Relay map on R1 to both R2 and R3.

Task 3:

Enable OSPF in Area 0 between R1, R2 and R3. You know that Frame Relay is a NBMA technology, therefore, the default OSPF Network Type would be Non-Broadcast, therefore use this as a hint to establish OSPF adjacencies. As another hint, R1 should have an adjacency to R2 and R3, and R2 and R3 should each have an adjacency to R1.

Task 4:

Verify the correct OSPF network type on any router Serial interface. Finally, verify that OSPF adjacencies have been established. You need to complete your OSPF configuration to establish adjacencies.

SOLUTION:

Lab 50 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 21 Configuration and Verification Task 1

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on verifying Frame Relay mapping, please refer to:

Lab 40 Configuration and Verification Task 4

Lab 40 Configuration and Verification Task 5

```
R1#show frame-relay map

Serial1/0 (up): ip 10.0.0.2 dlci 102(0x66,0x1860), static,

            broadcast,

            CISCO, status defined, active

Serial1/0 (up): ip 10.0.0.3 dlci 103(0x67,0x1870), static,

            broadcast,

            CISCO, status defined, active
```

```
R2#show frame-relay map

Serial0/0 (up): ip 10.0.0.1 dlci 201(0xC9,0x3090), static,

            broadcast,

            CISCO, status defined, active

Serial0/0 (up): ip 10.0.0.3 dlci 201(0xC9,0x3090), static,

            broadcast,

            CISCO, status defined, active
```

```
R3#show frame-relay map

Serial1/0 (up): ip 10.0.0.1 dlci 301(0x12D,0x48D0), static,

            broadcast,
            CISCO, status defined, active
Serial1/0 (up): ip 10.0.0.2 dlci 301(0x12D,0x48D0), static,
            broadcast,
            CISCO, status defined, active
```

Task 3:

For reference information wildcard masks, please refer to:

Lab 42 Configuration and Verification Task 5

Lab 48 Configuration and Verification Task 3

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#network 10.0.0.0 0.0.0.31 area 0
R1(config-router)#^Z
R1#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 2
R2(config-router)#network 10.0.0.0 0.0.0.31 area 0
R2(config-router)#end
R2#
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router ospf 3
R3(config-router)#network 10.0.0.0 0.0.0.31 area 0
R3(config-router)#^Z
R3#
```

Task 4:

NOTE: If you were to issue the show ip ospf neighbor command after having issued the above commands, you would notice that the neighbor list was empty as can be seen on R3:

```
R3#show ip ospf neighbor

R3#
```

This is because on NBMA networks, OSPF is expecting to discover neighbors using Unicast rather than Multicast (which is the default). In other words, OSPF needs to be configured with specific neighbors using the neighbor command in OSPF configuration mode. This is a very important concept to commit to mind. Make sure you understand and remember this! To establish the neighbors for OSPF, consider the fact that R1 is the hub and R2 and R3 are spoke routers in a typical hub and spoke network. Therefore, R1 needs to have two neighbor statements for R2 and R3, and R2 and R3 each need to have a neighbor statement for R1. This is illustrated below.

```
R1#show ip ospf interface serial 1/0

Serial1/0 is up, line protocol is up

  Internet Address 10.0.0.1/27, Area 0

  Process ID 1, Router ID 192.168.1.1, Network Type NON_BROADCAST, Cost: 64

  Transmit Delay is 1 sec, State DR, Priority 1

  Designated Router (ID) 192.168.1.1, Interface address 10.0.0.1

  Backup Designated router (ID) 172.16.3.3, Interface address 10.0.0.3

  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5

    oob-resync timeout 120

    Hello due in 00:00:00

  Index 1/1, flood queue length 0

  Next 0x0(0)/0x0(0)

  Last flood scan length is 1, maximum is 1

  Last flood scan time is 4 msec, maximum is 4 msec

  Neighbor Count is 2, Adjacent neighbor count is 2

    Adjacent with neighbor 10.1.1.2

    Adjacent with neighbor 172.16.3.3  (Backup Designated Router)

  Suppress hello for 0 neighbor(s)
```

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#neighbor 10.0.0.2
R1(config-router)#neighbor 10.0.0.3
R1(config-router)#^Z
R1#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 2
R2(config-router)#neighbor 10.0.0.1
R2(config-router)#end
R2#
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router ospf 3
R3(config-router)#neighbor 10.0.0.1
R3(config-router)#^Z
R3#
R1#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.1.2          1   FULL/DROTHER    00:01:37    10.0.0.2        Serial1/0
172.16.3.3        1   FULL/BDR        00:01:58    10.0.0.3        Serial1/0
R2#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.1       1   FULL/DR         00:01:54    10.0.0.1        Serial0/0
R3#show ip ospf neighbor
```

```
Neighbor ID     Pri   State           Dead Time   Address         Interface

192.168.1.1       1   FULL/DR         00:01:41    10.0.0.1        Serial1/0
```

NOTE: Based on the above neighbor relationships, we can determine that R1 is the Designated Router, and R3 is the Backup Designated Router. R2 is neither DR nor BDR and is listed as DROTHER.

Lab 51: Configuring OSPF Point-to-Multipoint Networks

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to enable OSPF on Point-to-Multipoint network types. Unlike other OSPF network types, there is no default Point-to-Multipoint network type. This must be manually enabled.

Lab Purpose:

Enabling OSPF on Point-to-Multipoint network types is a fundamental skill. OSPF is the most popular Interior Gateway Protocol (IGP) and it is imperative to understand how OSPF adjacencies are established on Point-to-Multipoint network types. Point-to-Multipoint network types are typically used in a hub and spoke environment on NBMA technologies such as Frame Relay. OSPF uses the concept of Areas. In order for two OSPF-enabled routers to establish an adjacency, they must reside in the same OSPF Area. Unlike EIGRP which uses Autonomous System Numbers, OSPF is enabled using a locally significant Process ID. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to enable OSPF on point-to-point network types.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

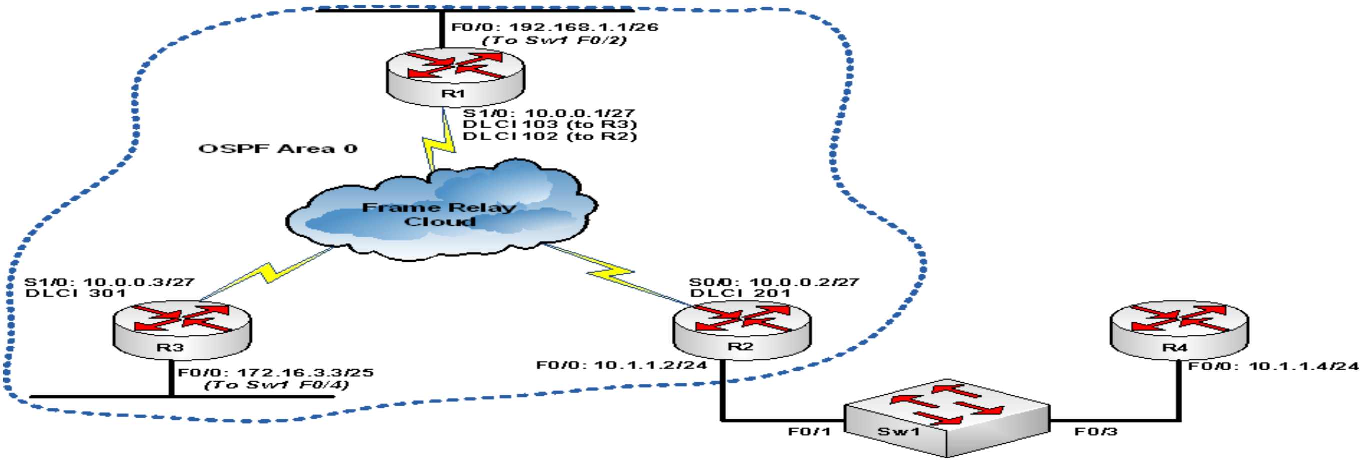
This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 15 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

This lab will only be concerned with configuration on R1, R2, and R3. To begin with, configure the hostnames on routers R1, R2 and Sw1 as illustrated in the topology.

Task 2:

Enable the Serial interfaces of R1, R2, and R3 for Frame Relay encapsulation and use static maps for each router to the other two routers. For example, create a static Frame Relay map on R1 to both R2 and R3.

Task 3:

Enable OSPF in Area 0 between R1, R2 and R3. You know that Frame Relay is a NBMA technology; however, to prevent having to manually configure static neighbor statements as was performed in the previous lab, change the default OSPF network to Point-to-Multipoint.

Task 4:

Verify the configured OSPF point-to-multipoint network type on any router Serial interface. Finally, verify that OSPF adjacencies have been established.

SOLUTION:

Lab 51 Configuration and Verification

Task 1:

```
Router#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R1

R1(config)#end
```

```
R1#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#end
R2#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R3
R3(config)#end
R3#
```

Task 2:

For reference information on verifying Frame Relay mapping, please refer to:

Lab 40 Configuration and Verification Task 4

Lab 40 Configuration and Verification Task 5

```
R1#show frame-relay map
Serial1/0 (up): ip 10.0.0.2 dlci 102(0x66,0x1860), static,
              broadcast,
              CISCO, status defined, active
Serial1/0 (up): ip 10.0.0.3 dlci 103(0x67,0x1870), static,
              broadcast,
              CISCO, status defined, active
R2#show frame-relay map
Serial0/0 (up): ip 10.0.0.1 dlci 201(0xC9,0x3090), static,
              broadcast,
              CISCO, status defined, active
Serial0/0 (up): ip 10.0.0.3 dlci 201(0xC9,0x3090), static,
              broadcast,

              CISCO, status defined, active

R3#show frame-relay map

Serial1/0 (up): ip 10.0.0.1 dlci 301(0x12D,0x48D0), static,

              broadcast,

              CISCO, status defined, active

Serial1/0 (up): ip 10.0.0.2 dlci 301(0x12D,0x48D0), static,

              broadcast,

              CISCO, status defined, active
```

Task 3:

NOTE: By default, when OSPF is enabled on Frame Relay networks, the default OSPF network types will be non-broadcast.This means that manual neighbor statememts will need to be configured (as in the previous lab exercise) to establish OSPF adjacencies. To work around this, a point-to-multipoint network type can be specified for Frame Relay hub and spoke networks, such as the topology used in this lab exercise. This is done using the ip ospf network interface configuration command for the interface connected to the NBMA network as shown below:

```
R1(config)#int s1/0
R1(config-if)#ip ospf network ?
  broadcast           Specify OSPF broadcast multi-access network
  non-broadcast       Specify OSPF NBMA network
  point-to-multipoint  Specify OSPF point-to-multipoint network
  point-to-point      Specify OSPF point-to-point network
```

As is illustrated in the above output, using the ip ospf network command allows you to manually configure a network as a different type than the default OSPF network. For example, this command can be issued on a FastEthernet interface enabled for OSPF to force that interface to operate as a point-to-point OSPF interface (which means there will ne no DR/BDR election) versus the default OSPF network type of Broadcast.

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#router ospf 1

R1(config-router)#network 10.0.0.0 0.0.0.31 area 0

R1(config-router)#exit

R1(config)#int s1/0

R1(config-if)#ip ospf network point-to-multipoint
```

```
R1(config-if)#end

R1#

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#router ospf 2

R2(config-router)#network 10.0.0.0 0.0.0.31 area 0

R2(config-router)#exit

R2(config)#int s0/0

R2(config-if)#ip ospf network point-to-multipoint

R2(config-if)#end

R2#

R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#router ospf 3

R3(config-router)#network 10.0.0.0 0.0.0.31 area 0

R3(config-router)#exit

R3(config)#int s1/0

R3(config-if)#ip ospf network point-to-multipoint

R3(config-if)#^Z

R3#
```

Task 4:

```
R1#show ip ospf interface serial 1/0

Serial1/0 is up, line protocol is up

  Internet Address 10.0.0.1/27, Area 0

  Process ID 1, Router ID 192.168.1.1, Network Type POINT_TO_MULTIPOINT, Cost: 64

  Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,

  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
```

```
    oob-resync timeout 120
    Hello due in 00:00:22
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 4 msec, maximum is 4 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 172.16.3.3
    Adjacent with neighbor 10.1.1.2
  Suppress hello for 0 neighbor(s)
```

NOTE: As can be seen in the output above, the OSPF network type is now point-to-multipoint as specified by the Network Type POINT_TO_MULTIPOINT output even though this interface is connected to a Frame Relay network. Also notice the fact that there is no DR/BDR elected on a point-to-multipoint network type just like there is no DR/BDR elected on a point-to-point network type.

```
R1#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.3.3        0   FULL/  -        00:01:45    10.0.0.3        Serial1/0
10.1.1.2          0   FULL/  -        00:01:53    10.0.0.2        Serial0/1
R2#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.1       0   FULL/  -        00:01:51    10.0.0.1        Serial0/0
R3#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.1       0   FULL/  -        00:01:31    10.0.0.1        Serial1/0
```

Lab 52: Configuring Multi-Area OSPF

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to enable OSPF using more than one Area.

Lab Purpose:

Enabling multi-area OSPF is a fundamental skill. When configuring multi-area OSPF, it is imperative to remember that all Area's must be connected to the OSPF backbone Area, which is Area 0. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to enable multi-area OSPF.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

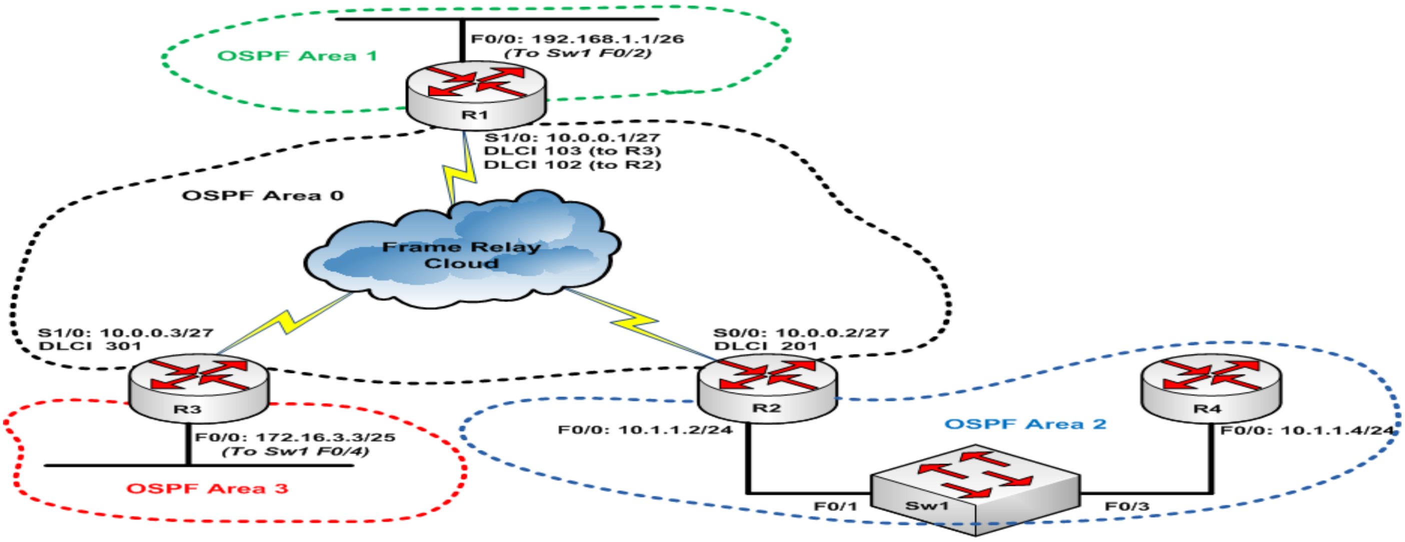
This lab has a difficulty rating of 10/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 30 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

To begin with, configure the hostnames on routers R1, R2, R3, R4 and Sw1 as illustrated in the topology.

Task 2:

Enable the Serial interfaces of R1, R2, and R3 for Frame Relay encapsulation and use static maps for each router to the other two routers. For example, create a static Frame Relay map on R1 to both R2 and R3.

Task 3:

Configure VLAN 2 on Sw1 and assign it the name OSPF_VLAN. Assign interfaces FastEthernet0/1 and FastEthernet0/3 to this VLAN.

Task 4:

Enable OSPF in Area 0 between R1, R2 and R3 Serial interfaces. Use the point-to-multipoint OSPF network type. Verify OSPF adjacencies on the routers.

Task 5:

Configure IP addressing and OSPF Area 1 on R1 FastEthernet0/0 interface and OSPF Area 3 on R3 FastEthernet0/0 interface as illustrated in the topology.

Task 6:

Configure OSPF Area 2 between R2 and R4 FastEthernet0/0 interfaces. Verify OSPF adjacencies on R2 and R4.

Task 7:

Verify your OSPF routes using the show ip route command. Look at the routing tables of all routers.

Task 8:

Check the OSPF database on R1 and R4. Use the show ip ospf database command. Familiarize yourself with the contents of the OSPF database.

SOLUTION:

Lab 52 Configuration and Verification

Task 1:

```
Router#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R1

R1(config)#end

R1#

Router#conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#end
R2#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R3
R3(config)#end
R3#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R4
R4(config)#end
R4#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Sw1
Sw1(config)#end
Sw1#
```

Task 2:

For reference information on verifying Frame Relay mapping, please refer to:

Lab 40 Configuration and Verification Task 4

Lab 40 Configuration and Verification Task 5

```
R1#show frame-relay map
Serial1/0 (up): ip 10.0.0.2 dlci 102(0x66,0x1860), static,
              broadcast,
              CISCO, status defined, active
```

```
Serial1/0 (up): ip 10.0.0.3 dlci 103(0x67,0x1870), static,
            broadcast,
            CISCO, status defined, active
R2#show frame-relay map
Serial0/0 (up): ip 10.0.0.1 dlci 201(0xC9,0x3090), static,
            broadcast,
            CISCO, status defined, active
Serial0/0 (up): ip 10.0.0.3 dlci 201(0xC9,0x3090), static,
            broadcast,
            CISCO, status defined, active
```

Task 3:

```
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#vlan 1
Sw1(config-vlan)#name OSPF_VLAN
Sw1(config-vlan)#exit
Sw1(config)#interface fastethernet0/1
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 2
Sw1(config-if)#no shutdown
Sw1(config-if)#exit
Sw1(config)#interface fastethernet0/3
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 2
Sw1(config-if)#no shutdown
Sw1(config-if)#end
Sw#
```

```
Sw1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
2    OSPF_VLAN                        active    Fa0/1, Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Task 4:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#router ospf 1

R1(config-router)#network 10.0.0.0 0.0.0.31 area 0

R1(config-router)#exit

R1(config)#int s1/0

R1(config-if)#ip ospf network point-to-multipoint

R1(config-if)#end

R1#

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#router ospf 2

R2(config-router)#network 10.0.0.0 0.0.0.31 area 0

R2(config-router)#exit

R2(config)#int s0/0

R2(config-if)#ip ospf network point-to-multipoint

R2(config-if)#end

R2#
```

```
R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#router ospf 3

R3(config-router)#network 10.0.0.0 0.0.0.31 area 0

R3(config-router)#exit

R3(config)#int s1/0

R3(config-if)#ip ospf network point-to-multipoint

R3(config-if)#^Z

R3#

R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface

172.16.3.3        0   FULL/  -        00:01:45    10.0.0.3        Serial1/0

10.1.1.2          0   FULL/  -        00:01:53    10.0.0.2        Serial1/0

R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface

192.168.1.1       0   FULL/  -        00:01:51    10.0.0.1        Serial0/0

R3#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface

192.168.1.1       0   FULL/  -        00:01:31    10.0.0.1        Serial1/0
```

Task 5:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int fa0/0

R1(config-if)#ip address 192.168.1.1 255.255.255.192

R1(config-if)#exit

R1(config)#router ospf 1

R1(config-router)#network 192.168.1.0 0.0.0.63 area 1
```

```
R1(config-router)#^Z
R1#
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int fa0/0
R3(config-if)#ip address 172.16.3.3 255.255.255.128
R3(config-if)#exit
R3(config)#router ospf 3
R3(config-router)#network 172.16.3.3 0.0.0.127 area 3
R3(config-router)#end
R3#
```

Task 6:

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int fa0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.0
R2(config-if)#exit
R2(config)#router ospf 2
R2(config-router)#network 10.1.1.0 0.0.0.255 area 2
R2(config-router)#end
R2#
R4#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#int fa0/0
R4(config-if)#ip address 10.1.1.4 255.255.255.0
R4(config-if)#no shut
R4(config-if)#exit
```

```
R4(config)#router ospf 4

R4(config-router)#network 10.1.1.0 0.0.0.255 area 2

R4(config-router)#^Z

*Mar  1 00:02:10.009: %OSPF-5-ADJCHG: Process 4, Nbr 10.1.1.2 on Ethernet0/0 from
LOADING to FULL, Loading Done

R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface

192.168.1.1       0   FULL/  -        00:01:30    10.0.0.1        Serial0/0

10.1.1.4          1   FULL/BDR        00:00:34    10.1.1.4        FasrEthernet0/0

r4#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface

10.1.1.2          1   FULL/DR         00:00:32    10.1.1.2        FastEthernet0/0

r4#
```

Task 7:

```
R1#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

       ia - IS-IS inter area, * - candidate default, U - per-user static route

       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/25 is subnetted, 1 subnets

O IA    172.16.3.0 [110/74] via 10.0.0.3, 00:06:47, Serial1/0

     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks

O       10.0.0.2/32 [110/64] via 10.0.0.2, 00:06:47, Serial1/0

O       10.0.0.3/32 [110/64] via 10.0.0.3, 00:06:47, Serial1/0
```

```
O IA    10.1.1.0/24 [110/65] via 10.0.0.2, 00:02:53, Serial1/0
C       10.0.0.0/27 is directly connected, Serial1/0
     192.168.1.0/26 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     172.16.0.0/25 is subnetted, 1 subnets
O IA    172.16.3.0 [110/138] via 10.0.0.1, 00:01:18, Serial0/0
     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
O       10.0.0.3/32 [110/128] via 10.0.0.1, 00:07:30, Serial0/0
C       10.1.1.0/24 is directly connected, FastEthernet0/0
C       10.0.0.0/27 is directly connected, Serial0/0
O       10.0.0.1/32 [110/64] via 10.0.0.1, 00:07:30, Serial0/0
     192.168.1.0/26 is subnetted, 1 subnets
O IA    192.168.1.0 [110/74] via 10.0.0.1, 00:01:18, Serial0/0
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     172.16.0.0/25 is subnetted, 1 subnets
C       172.16.3.0 is directly connected, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
O       10.0.0.2/32 [110/128] via 10.0.0.1, 00:07:54, Serial1/0
O IA    10.1.1.0/24 [110/129] via 10.0.0.1, 00:04:00, Serial1/0
C       10.0.0.0/27 is directly connected, Serial0/1
O       10.0.0.1/32 [110/64] via 10.0.0.1, 00:07:54, Serial1/0
     192.168.1.0/26 is subnetted, 1 subnets
O IA    192.168.1.0 [110/74] via 10.0.0.1, 00:07:54, Serial1/0
r4#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     172.16.0.0/25 is subnetted, 1 subnets
O IA    172.16.3.0 [110/139] via 10.1.1.2, 00:02:08, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O IA    10.0.0.2/32 [110/1] via 10.1.1.2, 00:02:08, FastEthernet0/0
O IA    10.0.0.3/32 [110/129] via 10.1.1.2, 00:02:08, FastEthernet0/0
```

```
C       10.1.1.0/24 is directly connected, FastEthernet0/0

O IA    10.0.0.1/32 [110/65] via 10.1.1.2, 00:02:08, FastEthernet0/0

     192.168.1.0/26 is subnetted, 1 subnets

O IA    192.168.1.0 [110/75] via 10.1.1.2, 00:02:10, FastEthernet0/0
```

NOTE: When looking at the routing table, routes marked O are intra-area OSPF routes, i.e. routes within the same OSPF Area. Routes that are marked O IA are inter-area OSPF routes, i.e routes between OSPF Area. Make sure you note which routes are O and which are O IA and validate that this is correct based on the topology we just configured.

Task 8:

R1#**show ip ospf database**

```
                OSPF Router with ID (192.168.1.1) (Process ID 1)
                        Router Link States (Area 0)
Link ID                 ADV Router  Age  Seq#       Checksum Link count
10.1.1.2                10.1.1.2    739  0x80000005 0x00A996 2
172.16.3.3              172.16.3.3  1126 0x80000004 0x007461 2
192.168.1.1             192.168.1.1 974  0x80000008 0x0016AF 3
                     Summary Net Link States (Area 0)
Link ID                 ADV Router  Age  Seq#       Checksum
10.1.1.0                10.1.1.2    500  0x80000003 0x00809F
172.16.3.0              172.16.3.3  1122 0x80000001 0x00909F
192.168.1.0             192.168.1.1 1066 0x80000001 0x009CFF
                        Router Link States (Area 1)
Link ID                 ADV Router  Age  Seq#       Checksum Link count
192.168.1.1             192.168.1.1 1070 0x80000003 0x00DA49 1
                     Summary Net Link States (Area 1)
Link ID                 ADV Router  Age  Seq#       Checksum
10.0.0.1                192.168.1.1 1071 0x80000001 0x00E3E2
10.0.0.2                192.168.1.1 1072 0x80000001 0x005C29
10.0.0.3                192.168.1.1 1072 0x80000001 0x005232
10.1.1.0                192.168.1.1 500  0x80000003 0x005F23
172.16.3.0              192.168.1.1 1072 0x80000001 0x00B393
```

r4#**show ip ospf database**

```
                 OSPF Router with ID (10.1.1.4) (Process ID 4)
                        Router Link States (Area 2)
Link ID                 ADV Router  Age  Seq#       Checksum Link count
10.1.1.2                10.1.1.2    474  0x80000002 0x00D820 1
10.1.1.4                10.1.1.4    332  0x80000003 0x00CF23 1
                         Net Link States (Area 2)
Link ID                 ADV Router  Age  Seq#       Checksum
10.1.1.2                10.1.1.2    475  0x80000001 0x00A758
                     Summary Net Link States (Area 2)
Link ID                 ADV Router  Age  Seq#       Checksum
10.0.0.1                10.1.1.2    706  0x80000001 0x000AD9
10.0.0.2                10.1.1.2    706  0x80000001 0x007DA5
10.0.0.3                10.1.1.2    706  0x80000001 0x007829
172.16.3.0              10.1.1.2    706  0x80000001 0x00D98A
192.168.1.0             10.1.1.2    706  0x80000001 0x00C2F6
```

NOTE: Understanding the information printed in the OSPF database is key to understanding the operation of OSPF. The show ip ospf database shows the router ID of the router this command is issued on, as well as the locally significant OSPF process ID that has been enabled on the router. It also shows the different types of OSPF LSAs and the routes associated with those LSA types, and the OSPF Areas. In addition to this, each Link ID listed in the OSPF database is identified by the originator of the LSA under the column named ADV Router.

Lab 53: Manually configuring the OSPF router ID

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to manually configure the OSPF router ID.

Lab Purpose:

Manually configuring the OSPF router ID is a fundamental skill. By default, if only physical interfaces are configured on a router, the highest IP address of those interfaces is used as the OSPF router ID. However, if both Loopback and physical interfaces are configured, then the Loopback interfaces are preferred when Cisco IOS selects the router ID for OSPF. However, the recommended method to select an OSPF router ID is to manually configure it. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to manually configure an OSPF router ID.

Certification Level:

This lab is suitable for CCENT & CCNA certification exam preparation

Lab Difficulty:

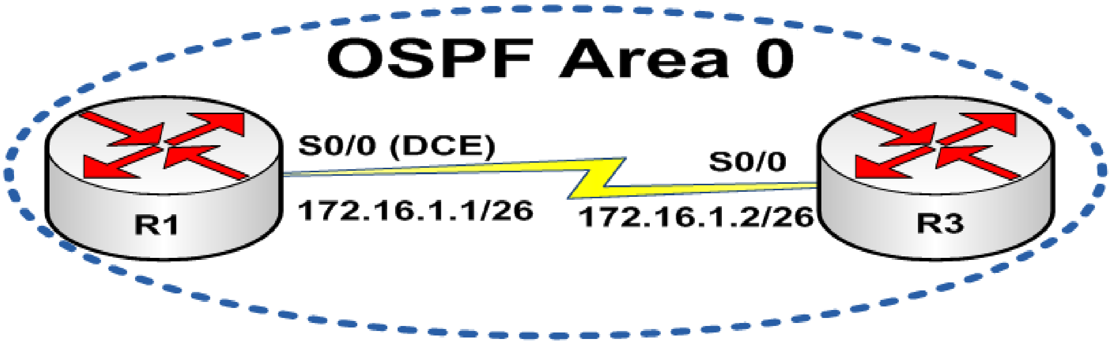
This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R3 as illustrated in the topology.

Task 2:

Configure R1 S0/0 which is a DCE to provide a clock rate of 768Kbps to R3. Configure the IP addresses on the Serial interfaces of R1 and R3 as illustrated in the topology.

Task 3:

Enable OSPF in Area 0 between R1 and R3. For R1, use an OSPF Process ID of 1. For R3 use an OSPF Process ID of 3. Verify your OSPF adjacency has formed between R1 and R3. Make a mental note the OSPF router ID being used at this time when the adjacency between R1 and R3 has been established.

Task 4:

Manually configure an OSPF router ID of 1.1.1.1 on R1 and 3.3.3.3 on R3. Reset the OSPF process on R1 and R3 by issuing the clear ip ospf process command. Verify that the OSPF adjacency has reestablished between R1 and R3. Verify that the OSPF neighbor IP addresses are now showing as the manually configured router IDs instead of the physical interface IP addresses.

SOLUTION:

Lab 53 Configuration and Verification

Task 1:

```
Router#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R1

R1(config)#end

Router#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R3

R3(config)#end
```

Task 2:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s0/0
```

```
R1(config-if)#clock rate 768000

R1(config-if)#ip address 172.16.1.1 255.255.255.192

R1(config-if)#no shut

R1(config-if)#end

R1#

R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int s0/0

R3(config-if)#ip address 172.16.1.2 255.255.255.192

R3(config-if)#no shutdown

R3(config-if)#^Z

R3#
```

Task 3:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#router ospf 1

R1(config-router)#network 172.16.1.0 0.0.0.63 area 0

R1(config-router)#^Z

R1#

R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#router ospf 3

R3(config-router)#network 172.16.1.0 0.0.0.63 area 0

R3(config-router)#end

*Mar  1 01:51:39.406: %OSPF-5-ADJCHG: Process 3, Nbr 192.168.1.1 on Serial0/0 from
LOADING to FULL, Loading Done

R1#show ip ospf neighbor detail

 Neighbor 172.16.3.3, interface address 172.16.1.2
```

```
    In the area 0 via interface Serial0/0
    Neighbor priority is 0, State is FULL, 12 state changes
    DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x52
    LLS Options is 0x1 (LR)
    Dead timer due in 00:00:35
    Neighbor is up for 00:01:04
    Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
R3#show ip ospf neighbor detail
 Neighbor 192.168.1.1, interface address 172.16.1.1
    In the area 0 via interface Serial0/0
    Neighbor priority is 0, State is FULL, 6 state changes
    DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x52
    LLS Options is 0x1 (LR)
    Dead timer due in 00:00:39
    Neighbor is up for 00:00:48
    Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

NOTE: The show ip ospf neighbor detail provides detailed information of OSPF neighbors. It provides the neighbor router ID as well as the interface on which the neighbor was discovered, amongst other things. In addition to that, it will also provide the IP address of the routers that are DR and BDR respectively on Broadcast or NBMA network types as illustrated below. Familiarize yourself with the information provided by this command.

```
r4#show ip ospf neighbor detail
 Neighbor 10.1.1.2, interface address 10.1.1.2
    In the area 2 via interface FastEthernet0/0
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.1.1.2 BDR is 10.1.1.4
    Options is 0x52
    LLS Options is 0x1 (LR)
    Dead timer due in 00:00:33
    Neighbor is up for 00:36:56
    Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Task 4:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#router ospf 1

R1(config-router)#router-id 1.1.1.1

Reload or use "clear ip ospf process" command, for this to take effect

R1(config-router)#end

R1#

R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#router ospf 3

R3(config-router)#router-id 3.3.3.3

Reload or use "clear ip ospf process" command, for this to take effect

R3(config-router)#end

R3#

R3#clear ip ospf process

Reset ALL OSPF processes? [no]: yes

*Mar  1 01:58:27.875: %OSPF-5-ADJCHG: Process 3, Nbr 1.1.1.1 on Serial0/0 from FULL to
DOWN, Neighbor Down: Interface down or detached

*Mar  1 01:58:27.959: %OSPF-5-ADJCHG: Process 3, Nbr 1.1.1.1 on Serial0/0 from LOADING
to FULL, Loading Done
```

NOTE: Whenever you manually change the OSPF router ID for an established OSPF adjacency, the change is not immediate and you either have to reboot the router or reset the OSPF process as indicated in the message that is printed on the console when we configured the router ID on R3:

Reload or use "clear ip ospf process" command, for this to take effect

After resetting the OSPF process, a new adjacency is reestablished and both routers use the configured router IDs.

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface

3.3.3.3           0   FULL/  -        00:00:37    172.16.1.2      Serial0/0
```

```
R3#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface

1.1.1.1           0   FULL/  -        00:00:39    172.16.1.1      Serial0/0
```

Lab 54: Debugging OSPF Adjacencies

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to debug OSPF adjacencies.

Lab Purpose:

Debugging OSPF adjacencies is a fundamental troubleshooting skill. Using debugging, you can identify issues that may be causing OSPF to stop operating. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to decipher OSPF adjacency debugging messages..

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

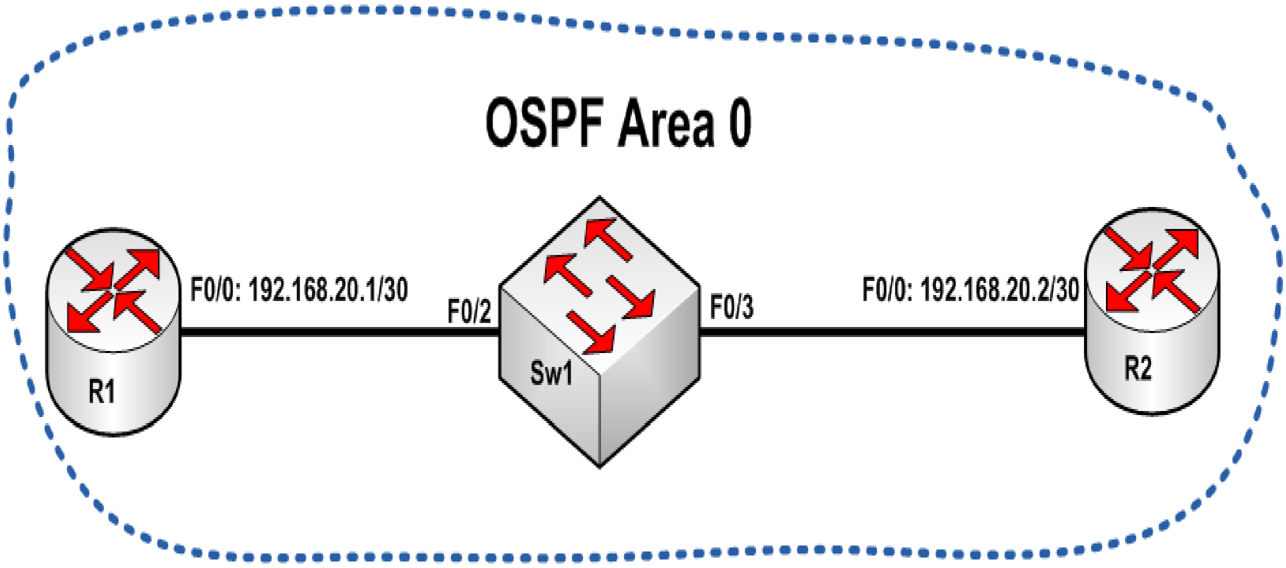
This lab has a difficulty rating of 7/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1, R2 and Sw1 as illustrated in the topology.

Task 2:

Configure VLAN 4010 on Sw1 and name it OSPF_VLAN. Assign ports FastEthernet0/2 and FastEthernet0/3 to this VLAN as access ports. Configure IP addressing on R1 and R2 FastEthernet0/0 interfaces.

Task 3:

Enable OSPF in Area 0 between R1 and R2. For R1, use an OSPF Process ID of 1 and for R2; use an OSPF Process ID of 2. Verify your OSPF adjacency has formed between R1 and R3. Also verify that the default network type for the Ethernet link between R1 and R3 is Broadcast.

Task 4:

Enable OSPF adjacency debugging on R1 using the debug ip ospf adj command. Reset the OSPF process on R2. As the OSPF adjacency reestablishes, verify that you can see the different states that OSPF transitions through as it moves to the FULL state.

SOLUTION:

Lab 54 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 21 Configuration and Verification Task 1

Lab 35 Configuration and Verification Task 1

Task 2:

```
Sw1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#vtp mode transparent

Setting device to VTP TRANSPARENT mode.

Sw1(config)#vlan 4010

Sw1(config-vlan)#name OSPF_VLAN

Sw1(config-vlan)#exit

Sw1(config)#

Sw1(config)#interface fastethernet0/2

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 4010

Sw1(config-if)#no shut

Sw1(config-if)#exit

Sw1(config)#interface fastethernet0/2

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 4010

Sw1(config-if)#no shut

Sw1(config-if)#end

Sw1#

Sw1#show vlan brief
```

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
4010 OSPF_VLAN                        active    Fa0/2, Fa0/3

Sw1#
```

For reference information on configuring IP interfaces, please refer to:

Lab 3 Configuration and Verification Task 5

Lab 31 Configuration and Verification Task 3

Task 3:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#router ospf 1

R1(config-router)#network 192.168.20.0 0.0.0.3 area 0

R1(config-router)#end

R1#

R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#router ospf 2

R2(config-router)#network 192.168.20.0 0.0.0.3 area 0

R2(config-router)#^Z

*Mar  1 02:10:48.305: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.20.1 on FastEthernet0/0
from LOADING to FULL, Loading Done

R2#
```

```
R2#show ip ospf interface fastethernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 192.168.20.2/30, Area 0
  Process ID 2, Router ID 10.1.1.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 192.168.20.1, Interface address 192.168.20.1
  Backup Designated router (ID) 10.1.1.2, Interface address 192.168.20.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 4
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.20.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

Task 4:

```
R2#debug ip ospf adj
OSPF adjacency events debugging is on
R2#clear ip ospf process
Reset ALL OSPF processes? [no]: yes
*Mar  1 02:13:21.660: OSPF: Elect BDR 0.0.0.0
*Mar  1 02:13:21.660: OSPF: Elect DR 0.0.0.0
*Mar  1 02:13:21.660:        DR: none    BDR: none
*Mar  1 02:13:21.660: OSPF: Remember old DR 192.168.20.1 (id)
*Mar  1 02:13:21.721: OSPF: Interface FastEthernet0/0 going Up
```

```
*Mar  1 02:13:21.721: OSPF: i_up : interface is down

*Mar  1 02:13:21.725: OSPF: 2 Way Communication to 192.168.20.1 on
FastEthernet0/0, state 2WAY

*Mar  1 02:13:21.725: OSPF: Backup seen Event before WAIT timer on FastEthernet0/0

*Mar  1 02:13:21.725: OSPF: DR/BDR election on FastEthernet0/0

*Mar  1 02:13:21.725: OSPF: Elect BDR 10.1.1.2

*Mar  1 02:13:21.729: OSPF: Elect DR 192.168.20.1

*Mar  1 02:13:21.729: OSPF: Elect BDR 10.1.1.2

*Mar  1 02:13:21.729: OSPF: Elect DR 192.168.20.1

*Mar  1 02:13:21.729:        DR: 192.168.20.1 (Id)   BDR: 10.1.1.2 (Id)

*Mar  1 02:13:21.729: OSPF: Send DBD to 192.168.20.1 on FastEthernet0/0 seq 0x1614 opt
0x52 flag 0x7 len 32

*Mar  1 02:13:21.733: OSPF: Rcv DBD from 192.168.20.1 on Ethernet0/0 seq 0xEB3
opt 0x52 flag 0x7 len 32  mtu 1500 state EXSTART

*Mar  1 02:13:21.737: OSPF: NBR Negotiation Done. We are the SLAVE

*Mar  1 02:13:21.737: OSPF: Send DBD to 192.168.20.1 on FastEthernet0/0 seq 0xEB3 opt
0x52 flag 0x0 len 32

*Mar  1 02:13:21.741: OSPF: Rcv DBD from 192.168.20.1 on FastEthernet0/0 seq 0xEB4 opt
0x52 flag 0x3 len 172  mtu 1500 state EXCHANGE

*Mar  1 02:13:21.741: OSPF: Send DBD to 192.168.20.1 on FastEthernet0/0 seq 0xEB4 opt
0x52 flag 0x0 len 32

*Mar  1 02:13:21.749: OSPF: Rcv DBD from 192.168.20.1 on FastEthernet0/0 seq
0xEB5 opt 0x52 flag 0x1 len 32  mtu 1500 state EXCHANGE

*Mar  1 02:13:21.749: OSPF: Exchange Done with 192.168.20.1 on FastEthernet0/0

*Mar  1 02:13:21.749: OSPF: Send LS REQ to 192.168.20.1 length 84 LSA count 7

*Mar  1 02:13:21.749: OSPF: Send DBD to 192.168.20.1 on FastEthernet0/0 seq 0xEB5 opt
0x52 flag 0x0 len 32

*Mar  1 02:13:21.753: OSPF: Rcv LS UPD from 192.168.20.1 on FastEthernet0/0 length 332
LSA count 7

*Mar  1 02:13:21.757: OSPF: Synchronized with 192.168.20.1 on FastEthernet0/0, state FULL

*Mar  1 02:13:21.757: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.20.1 on
FastEthernet0/0 from LOADING to FULL, Loading Done
```

```
*Mar  1 02:13:26.544: OSPF: Rcv LS UPD from 192.168.20.1 on FastEthernet0/0 length 64
LSA count 1

*Mar  1 02:13:27.001: OSPF: Rcv LS UPD from 192.168.20.1 on FastEthernet0/0 length 64
LSA count 1R2#undebug all

All possible debugging has been turned off

R2#
```

NOTE: From the output above, we can clearly see OSPF transition from the 2WAY state to the EXSTART state, to the EXCHANGE state, and finally to the FULL state. Because this is a Broadcast network type, a DR and BDR router are also elected. If this were a point-to-point, or point-to-multipoint network type, we would not see the DR and BDR election taking place.

Lab 55: Configuring and Applying Standard Numbered ACLs

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to create and apply standard numbered Access Control Lists.

Lab Purpose:

Configuring and applying standard ACLs is a fundamental skill. Standard ACLs filter based on source address and should be applied as close to the destination as possible. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to create and apply standard numbered ACLs.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

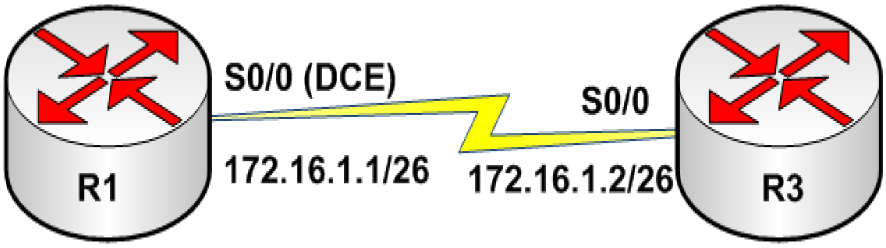
This lab has a difficulty rating of 7/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Interface	IP Address
Loopback10	10.10.10.3/25
Loopback20	10.20.20.3/28
Loopback30	10.30.30.3/29

Task 1:

Configure the hostnames on routers R1 and R3 as illustrated in the topology.

Task 2:

Configure R1 S0/0 which is a DCE to provide a clock rate of 768Kbps to R3. Configure the IP addresses on the Serial interfaces of R1 and R3 as illustrated in the topology. Configure a static default route on R1 pointing to R3 over the Serial connection between the two routers. Also configure a static default route on R3 pointing to R1 via the Serial connection between the two routers. Configure the Loopback interfaces specified in the diagram on R1 and R3.

Task 3:

To test connectivity, ping R1 from R3 Serial0/0, Loopback10, Loopback20 and Loopback30 interfaces. To ping from the Loopback interfaces, use the **ping <ip_address> source <interface>** command.

Task 4:

On R1, create a standard numbered ACL to prevent inbound traffic from the Loopback20 subnet on R3, but explicitly allow all inbound traffic from Loopback10 and Loopback30 subnets on R3. Apply this ACL inbound on Serial0/0. Now, try to ping R1 from R3 Serial0/0, Loopback10, Loopback20, and Loopback30 using the **ping <ip_address> source <interface>.** If you have configured this correctly, only Loopback10 and Loopback30 should still be able to ping.

SOLUTION:

Lab 55 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 21 Configuration and Verification Task 1

Lab 35 Configuration and Verification Task 1

Task 2:

```
R1#conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s0/0

R1(config-if)#no shutdown

R1(config-if)#clock rate 768000

R1(config-if)#ip add 172.16.1.2 255.255.255.192

R1(config-if)#end

R1#

R3#config term

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int s0/1

R3(config-if)#ip address 172.16.1.2 255.255.255.192

R3(config-if)#no shut

R3(config-if)#end

R3#

R1#ping 172.16.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:

!!!!!

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

R1#

R3#ping 172.16.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

!!!!!

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

R3#

R1#config t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 serial0/0 172.16.1.2
R1(config-if)#end
R1#
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip route 0.0.0.0 0.0.0.0 serial0/0 172.16.1.1
R3(config)#int loo 10
R3(config-if)#ip address 10.10.10.3 255.255.255.128
R3(config-if)#exit
R3(config)#int loo 20
R3(config-if)#ip address 10.20.20.3 255.255.255.240
R3(config-if)#exit
R3(config)#int loo 30
R3(config-if)#ip address 10.30.30.3 255.255.255.248
R3(config-if)#end
R3#
```

Task 3:

```
R3#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
R3#ping 172.16.1.1 source loopback10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.10.10.3
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
R3#ping 172.16.1.1 source loopback20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.20.20.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
R3#ping 172.16.1.1 source loopback30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.30.30.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

Task 4:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 10 remark 'Permit From R3 Loopback10'
R1(config)#access-list 10 permit 10.10.10.0 0.0.0.127
R1(config)#access-list 10 remark 'Deny From R3 Loopback20'
R1(config)#access-list 10 deny   10.20.20.0 0.0.0.15
R1(config)#access-list 10 remark 'Permit From R3 Loopback30'
R1(config)#access-list 10 permit 10.30.30.0 0.0.0.7
R1(config)#int s0/0
R1(config-if)#ip access-group 10 in
R1(config)#end
R1#
```

```
R1#show ip access-lists

Standard IP access list 10

    10 permit 10.10.10.0, wildcard bits 0.0.0.127

    20 deny   10.20.20.0, wildcard bits 0.0.0.15

    30 permit 10.30.30.0, wildcard bits 0.0.0.7
```

NOTE: The wildcard masks uses in ACLs are configured in the same way as those for EIGRP and OSPF. To determine the wildcard mask, you can simply subtract the network mask for the network on which you want to match with the ACL from the Broadcast mask. This concept is illustrated in the subtraction table shown below:

Broadcast Mask	255	255	255	255
[minus] **Subnet Mask**	255	255	255	128
[equals] **Wildcard Mask**	0	0	0	127

In our example, the subnet mask of the 10.10.10.0/25 subnet is 255.255.255.128. If this is subtracted from the Broadcast mask of 255.255.255.255 the result is 0.0.0.127, which is the wildcard mask we use to use in the ACL match for this subnet. Using the same concept, the subnet mask of the10.20.20.0/28 subnet is 255.255.255.240. If we use the above table to determine the wildcard mask, we would get the following:

Broadcast Mask	255	255	255	255
[minus] **Subnet Mask**	255	255	255	240
[equals] **Wildcard Mask**	0	0	0	15

And finally, the subnet mask of the 10.30.30.0/29 subnet is 255.255.255.248. If we used the same table to get the wildcard mask, we would end up with the following:

Broadcast Mask	255	255	255	255
[minus] **Subnet Mask**	255	255	255	252
[equals] **Wildcard Mask**	0	0	0	7

It is extremely important to practice creating wildcards for ACLs. Take time out to practice these until you are extremely comfortable with them. ACLs are a very important part of the CCNA certification and in the real world.

While it is not mandatory, I prefer to use the access-list [number] remark [description] statement so that I know which ACL line is matching what. This makes it easier for you. You may or may not want to do so, but I feel that is it good practice to do so. Do whatever you feel comfortable doing.

```
R3#ping 172.16.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

U.U.U
```

```
Success rate is 0 percent (0/5)
R3#ping 172.16.1.1 source loopback10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.10.10.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R3#ping 172.16.1.1 source loopback20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.20.20.3
U.U.U
Success rate is 0 percent (0/5)
R3#ping 172.16.1.1 source loopback30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.30.30.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

NOTE: Whenever you see a ping fail and the router shows U.U.U it is typically because your ping request was administratively prohibited by an ACL on the other end.

The second lesson to be learned in this exercise is that even though our ACL configuration focused on R3 Loopback10, Loopback20, and Loopback30, because we did not explicitly allow the Serial0/0 subnet between R1 and R3, this is implicitly denied at the end of the ACL. Keep this in mind, i.e. if traffic is not explicitly permitted, it is implicitly denied. It is very important to understand this aspect in regards to Access Control Lists. The explicitly configured statements show as matches against ACL entries, but implicit deny matches do not.

```
R1#show access-lists
Standard IP access list 10
    10 permit 10.10.10.0, wildcard bits 0.0.0.127 (15 matches)
    20 deny   10.20.20.0, wildcard bits 0.0.0.15 (11 matches)
    30 permit 10.30.30.0, wildcard bits 0.0.0.7 (15 matches)
```

Lab 56: Configuring and Applying Standard Named ACLs

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to create and apply standard named Access Control Lists.

Lab Purpose:

Configuring and applying standard ACLs is a fundamental skill. Standard ACLs filter based on source address and should be applied as close to the destination as possible. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to create and apply standard numbered ACLs.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

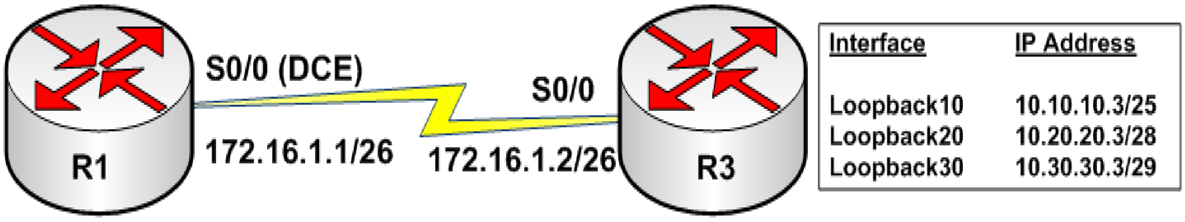
This lab has a difficulty rating of 7/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Interface	IP Address
Loopback10	10.10.10.3/25
Loopback20	10.20.20.3/28
Loopback30	10.30.30.3/29

Task 1:

Configure the hostnames on routers R1 and R3 as illustrated in the topology.

Task 2:

Configure R1 S0/0 which is a DCE to provide a clock rate of 768Kbps to R3. Configure the IP addresses on the Serial interfaces of R1 and R3 as illustrated in the topology. Configure a static default route on R1 pointing to R3 over the Serial connection between the two routers. Also configure a static default route on R3 pointing to R1 via the Serial connection between the two routers. Configure the Loopback interfaces specified in the diagram on R3.

Task 3:

To test connectivity, ping R1 from R3 Serial0/0, Loopback10, Loopback20 and Loopback30 interfaces. To ping from the Loopback interfaces, use the **ping <ip_address> source <interface>** command.

Task 4:

On R1, create a standard named ACL to prevent inbound traffic from the Loopback10 and Loopback30 subnet on R3, but explicitly allow all inbound traffic from Serial0/0 and Loopback20 subnets on R3. This ACL should be named LOOPBACK-10-30-ACL. Apply this ACL inbound on Serial0/0. Now, try to ping R1 from R3 Serial0/0, Loopback10, Loopback20, and Loopback30 using the **ping <ip_address> source <interface>** command. If you have configured this correctly, only ping from Serial0/0 and Loopback20 will work.

SOLUTION:

Lab 56 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 21 Configuration and Verification Task 1

Lab 35 Configuration and Verification Task 1

Task 2:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s0/0

R1(config-if)#no shutdown

R1(config-if)#clock rate 768000

R1(config-if)#ip add 172.16.1.2 255.255.255.192

R1(config-if)#end

R1#

R3#config term

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int s0/1

R3(config-if)#ip address 172.16.1.2 255.255.255.192

R3(config-if)#no shut
```

```
R3(config-if)#end

R3#

R1#ping 172.16.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:

!!!!!

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

R1#

R3#ping 172.16.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

!!!!!

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

R3#

R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#ip route 0.0.0.0 0.0.0.0 serial0/0 172.16.1.2

R1(config-if)#end

R1#

R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#ip route 0.0.0.0 0.0.0.0 serial0/0 172.16.1.1

R3(config)#int loo 10

R3(config-if)#ip address 10.10.10.3 255.255.255.128

R3(config-if)#exit

R3(config)#int loo 20

R3(config-if)#ip address 10.20.20.3 255.255.255.240
```

```
R3(config-if)#exit

R3(config)#int loo 30

R3(config-if)#ip address 10.30.30.3 255.255.255.248

R3(config-if)#end

R3#
```

Task 3:

```
R3#ping 172.16.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms

R3#ping 172.16.1.1 source loopback10

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

Packet sent with a source address of 10.10.10.3

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms

R3#ping 172.16.1.1 source loopback20

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

Packet sent with a source address of 10.20.20.3

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

R3#ping 172.16.1.1 source loopback30

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

Packet sent with a source address of 10.30.30.3
```

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

Task 4:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list standard LOOPBACK-10-30-ACL
R1(config-std-nacl)#remark 'Deny Traffic From R3 Loopback10'
R1(config-std-nacl)#deny 10.10.10.0 0.0.0.127
R1(config-std-nacl)#remark 'Permit Traffic From R3 Loopback20'
R1(config-std-nacl)#permit 10.20.20.0 0.0.0.15
R1(config-std-nacl)#remark 'Deny Traffic From R3 Loopback30'
R1(config-std-nacl)#deny 10.30.30.0 0.0.0.7
R1(config-std-nacl)#remark 'Permit Traffic From Serial0/0 Subnet'
R1(config-std-nacl)#permit 172.16.1.0 0.0.0.63
R1(config-std-nacl)#exit
R1(config)#int s0/0
R1(config-if)#ip access-group LOOPBACK-10-30-ACL in
R1(config-if)#end
R1#
R3#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R3#ping 172.16.1.1 source loop 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
```

```
Packet sent with a source address of 10.10.10.3

U.U.U

Success rate is 0 percent (0/5)

R3#ping 172.16.1.1 source loop 20

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

Packet sent with a source address of 10.20.20.3

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

R3#ping 172.16.1.1 source loop 30

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

Packet sent with a source address of 10.30.30.3

U.U.U

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

NOTE: Take note of the different syntax for creating a named ACL versus a numbered ACL. Named ACLs perform the same way as numbered ACLs but allow for easier identification of what the ACL is used for because they can be assigned a name. You can view named ACLs using the same commands as you would for numbered ACLs.

```
R1#show ip access-lists LOOPBACK-10-30-ACL
Standard IP access list LOOPBACK-10-30-ACL
    10 deny   10.10.10.0, wildcard bits 0.0.0.127 (11 matches)
    20 permit 10.20.20.0, wildcard bits 0.0.0.15 (15 matches)
    30 deny   10.30.30.0, wildcard bits 0.0.0.7 (11 matches)
    40 permit 172.16.1.0, wildcard bits 0.0.0.63 (15 matches)
```

To view ACLs applied to an interface, you can either use the show run interface <name> command or the show ip interface <name> command as illustrated below:

```
R1#show running-config interface serial 0/0
Building configuration...

Current configuration : 139 bytes
!
interface Serial0/0
 ip address 172.16.1.1 255.255.255.192
 ip access-group LOOPBACK-10-30-ACL in
 clock rate 768000
 no fair-queue
```

```
end

R1#show ip interface serial 0/0
Serial0/0 is up, line protocol is up
  Internet address is 172.16.1.1/26
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is LOOPBACK-10-30-ACL
```

Lab 57: Configuring and Applying Extended Numbered ACLs Inbound

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to create and apply extended numbered Access Control Lists.

Lab Purpose:

Configuring and applying extended ACLs is a fundamental skill. Extended ACLs filter based on source and destination address, as well as Layer 4 protocols TCP and UDP. Extended ACLs and should be applied as close to the source as possible. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to create and apply extended numbered ACLs.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

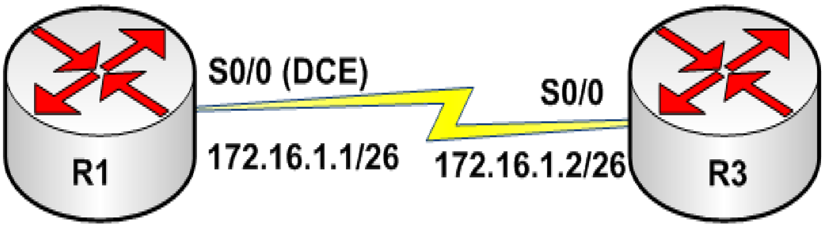
This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Interface	IP Address
Loopback10	10.10.10.3/25
Loopback20	10.20.20.3/28
Loopback30	10.30.30.3/29

Task 1:

Configure the hostnames on routers R1 and R3 as illustrated in the topology.

Task 2:

Configure R1 S0/0 which is a DCE to provide a clock rate of 768Kbps to R3. Configure the IP addresses on the Serial interfaces of R1 and R3 as illustrated in the topology.

Task 3:

Configure a static default route on R1 pointing to R3 over the Serial connection between the two routers. Also configure a static default route on R3 pointing to R1 via the Serial connection between the two routers. Configure the Loopback interfaces specified in the diagram on R1 and R3.

Task 4:

To test connectivity, ping R1 from R3 Serial0/0, Loopback10, Loopback20 and Loopback30 interfaces. To ping from the Loopback interfaces, use the **ping <ip_address> /source <interface>** command.

Task 5:

Configure both R1 and R3 to allow Telnet connections. A password of CISCO should for Telnet access. Also configure an enable secret of CISCO on both routers.

Task 6:

Configure a numbered extended ACL on R1 to allow Telnet from R3 Loopback10 and Loopback30 networks. Explicitly configure the extended ACL to deny Telnet from R3 Loopback20 but allow ping traffic from R3 Loopback20. When done, apply this ACL inbound on R1 Serial0/0 interface.

Telnet to R1 from R3 Loopback10, Loopback 20, and Loopback30 interfaces using the **telnet <ip_address> /source-interface <name>**command. If your ACL has been configured correctly, Telnet should be allowed on from Loopback10 and Loopback30 only.

Ping R1 from Loopback10, Loopback 20, and Loopback30 interfaces using the **ping <ip_address> /source <interface>** command. If your ACL has been configured correctly, Ping should only work when you ping from R3 Loopback20.

SOLUTION:

Lab 57 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 21 Configuration and Verification Task 1

Lab 35 Configuration and Verification Task 1

Task 2:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s0/0

R1(config-if)#no shutdown

R1(config-if)#clock rate 768000

R1(config-if)#ip add 172.16.1.1 255.255.255.192

R1(config-if)#end

R1#

R3#config term

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int s0/0

R3(config-if)#ip address 172.16.1.2 255.255.255.192

R3(config-if)#no shut

R3(config-if)#end

R3#

R1#ping 172.16.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:

!!!!!

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

```
R1#

R3#ping 172.16.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

!!!!!

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

R3#
```

Task 3:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#ip route 0.0.0.0 0.0.0.0 serial0/0 172.16.1.2

R1(config-if)#end

R1#

R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#ip route 0.0.0.0 0.0.0.0 serial0/0 172.16.1.1

R3(config)#int loo 10

R3(config-if)#ip address 10.10.10.3 255.255.255.128

R3(config-if)#exit

R3(config)#int loo 20

R3(config-if)#ip address 10.20.20.3 255.255.255.240

R3(config-if)#exit

R3(config)#int loo 30

R3(config-if)#ip address 10.30.30.3 255.255.255.248

R3(config-if)#end

R3#
```

Task 4:

```
R3#ping 172.16.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms

R3#ping 172.16.1.1 source loopback10

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

Packet sent with a source address of 10.10.10.3

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms

R3#ping 172.16.1.2 source loopback20

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

Packet sent with a source address of 10.20.20.3

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

R3#ping 172.16.1.2 source loopback30

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

Packet sent with a source address of 10.30.30.3

!!!!!

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

Task 5:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.
```

```
R1(config)#enable secret CISCO

R1(config)#line vty 0 4

R1(config-line)#password CISCO

R1(config-line)#login

R1(config-line)#end

R1#

R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#enable secret CISCO

R3(config)#line vty 0 4

R3(config-line)#password CISCO

R3(config-line)#login

R3(config-line)#end

R3#
```

Task 6:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#access-list 150 remark 'Allow Telnet For R3 Loopback10'

R1(config)#access-list 150 permit tcp 10.10.10.0 0.0.0.127 any eq telnet

R1(config)#access-list 150 remark 'Deny Telnet For R3 Loopback20'

R1(config)#access-list 150 deny   tcp 10.20.20.0 0.0.0.15 any eq telnet

R1(config)#access-list 150 remark 'Allow Telnet For R3 Loopback30'

R1(config)#access-list 150 permit tcp 10.30.30.0 0.0.0.7 any eq telnet

R1(config)#access-list 150 remark 'Allow PING For R3 Loopback20'

R1(config)#access-list 150 permit icmp 10.20.20.0 0.0.0.15 any echo

R1(config)#int s0/0

R1(config-if)#ip access-group 150 in
```

```
R1(config-if)#end

R1#
```

NOTE: Extended ACLs have the capability to match on Layer 4 protocol information. This means that you must know your well-known TCP and UDP port numbers. Fortunately, instead of having TCP and UDP port numbers, Cisco IOS ACLs allow you to use keywords for common protocols. For example, you can use the keyword telnet instead of having to use port number 23 to configure an ACL to match on Telnet traffic. However, if you do decide to use a port number, Cisco IOS automatically converts it to the common name as illustrated below:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 100 permit tcp any any eq 23
R1(config)#access-list 100 permit tcp any any eq 80
R1(config)#access-list 100 permit tcp any any eq 179
R1(config)#access-list 100 permit udp any any eq 520
R1(config)#access-lis 100 permit 88 any any
R1(config)#access-lis 100 permit 89 any any
R1(config)#end
R1#
R1#show ip access-lists 100
Extended IP access list 100
    10 permit tcp any any eq telnet
    20 permit tcp any any eq www
    30 permit tcp any any eq bgp
    40 permit udp any any eq rip
    50 permit eigrp any any
    60 permit ospf any any
```

As can be seen, while we configured the ACL using port numbers, IOS converted it to common names.

```
R3#telnet 172.16.1.1 /source-interface loopback10

Trying 172.16.1.1 ... Open

User Access Verification

Password:

R1#

R3#telnet 172.16.1.1 /source-interface loopback20

Trying 172.16.1.1 ...

% Destination unreachable; gateway or host down

R3#telnet 172.16.1.1 /source-interface loopback30

Trying 172.16.1.1 ... Open

User Access Verification
```

```
Password:

R1#

R3#ping 172.16.1.1 source loopback 20

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

Packet sent with a source address of 10.20.20.3

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
```

NOTE: When you see the message % Destination unreachable; gateway or host down when trying to Telnet to a host, it is typically because there is an ACL preventing Telnet to this device. Based on our configuration, everything works, and if we looked at the ACL configured on R1, we would see matches against it as follows:

```
R1#show ip access-lists 150
Extended IP access list 150
    10 permit tcp 10.10.10.0 0.0.0.127 any eq telnet (66 matches)
    20 deny tcp 10.20.20.0 0.0.0.15 any eq telnet (3 matches)
    30 permit tcp 10.30.30.0 0.0.0.7 any eq telnet (465 matches)
    40 permit icmp 10.20.20.0 0.0.0.15 any echo (15 matches)
```

Lab 58: Configuring and Applying Extended Named ACLs Inbound

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to create and apply extended numbered Access Control Lists.

Lab Purpose:

Configuring and applying extended ACLs is a fundamental skill. Extended ACLs filter based on source and destination address, as well as Layer 4 protocols TCP and UDP. Extended ACLs should be applied as close to the source as possible. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to create and apply extended named ACLs.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

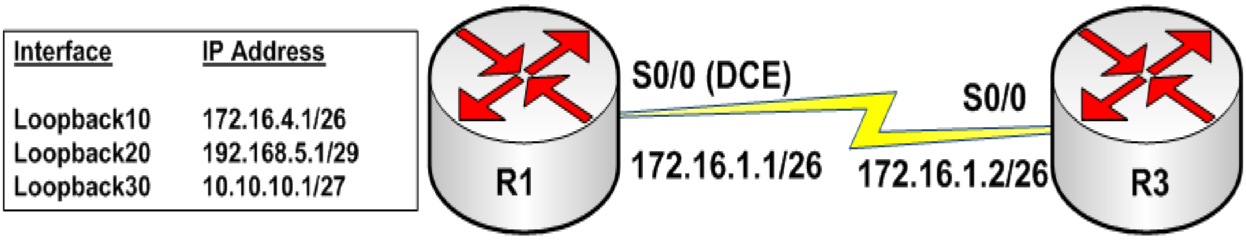
This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Interface	IP Address
Loopback10	172.16.4.1/26
Loopback20	192.168.5.1/29
Loopback30	10.10.10.1/27

Task 1:

Configure the hostnames on routers R1 and R3 as illustrated in the topology.

Task 2:

Configure R1 S0/0 which is a DCE to provide a clock rate of 768Kbps to R3. Configure the IP addresses on the Serial interfaces of R1 and R3 as illustrated in the topology. Configure the Loopback interfaces on R1.

Task 3:

Configure RIPv2 on R1 and R3 for Serial0/0 on both routers and the 172.16.4.0/26 Loopback10 on R1.

Configure EIGRP using AS 10 on R1 and R3 for Serial0/0 on both routers and the 192.168.5.0/29 Loopback20 on R1.

Configure OSPF using process 10 using Area 0on R1 and R3 Serial0/0 on both routers and the 10.10.10.0/27 Loopback30 on R1.

Task 4:

Verify your configuration using show ip route on R3 to ensure all three routes are seen via the different configured routing protocols. To test connectivity, ping the three Loopback interfaces on R1 from R3. These should all be reachable.

Task 5:

Configure a named extended ACL on R3 called ROUTING-ACL. This ACL should deny RIPv2, allow EIGRP, deny OSPF, and allow all other IP traffic. Apply this ACL inbound on R3 Serial0/0.

Task 6:

Issue the **clear ip route *** command followed by the show ip route command on R3 and look at the routing table again. If you have configured this ACL correctly, you should only have the EIGRP route in the routing table.

SOLUTION:

Lab 58 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 21 Configuration and Verification Task 1

Lab 35 Configuration and Verification Task 1

Task 2:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s0/0

R1(config-if)#no shutdown

R1(config-if)#clock rate 768000

R1(config-if)#ip add 172.16.1.1 255.255.255.192

R1(config-if)#exit

R1(config)#int lo10

R1(config-if)#ip address 172.16.4.1 255.255.255.192

R1(config-if)#exit

R1(config)#int lo20

R1(config-if)#ip address 192.168.5.1 255.255.255.248

R1(config-if)#exit

R1(config)#int lo30

R1(config-if)#ip address 10.10.10.1 255.255.255.224

R1(config-if)#exi

R1#

R3#config term

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int s0/0
```

```
R3(config-if)#ip address 172.16.1.2 255.255.255.192

R3(config-if)#no shut

R3(config-if)#end

R3#
```

Task 3:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#router rip

R1(config-router)#version 2

R1(config-router)#network 172.16.1.0

R1(config-router)#network 172.16.4.0

R1(config-router)#no auto-summary

R1(config-router)#exit

R1(config)#router eigrp 10

R1(config-router)#network 172.16.1.0 0.0.0.63

R1(config-router)#network 192.168.5.0

R1(config-router)#no auto-summary

R1(config-router)#exit

R1(config)#router ospf 10

R1(config-router)#network 172.16.1.0 0.0.0.63 area 0

R1(config-router)#network 10.10.10.0 0.0.0.31 area 0

R1(config-router)#end

R1#

R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#router rip

R3(config-router)#ver 2
```

```
R3(config-router)#net 172.16.1.0

R3(config-router)#no auto-sum

R3(config-router)#exit

R3(config)#router eigrp 10

R3(config-router)#network 172.16.1.0

R3(config-router)#no auto-summary

*Mar  1 03:18:45.296: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 172.16.1.1
(Serial0/0) is up: new adjacency

R3(config)#router ospf 10

R3(config-router)#network 172.16.1.0 0.0.0.63 area 0

R3(config-router)#end

*Mar  1 03:19:08.550: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.5.1 on Serial0/0 from
LOADING to FULL, Loading Done
```

Task 4:

```
R3#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

       ia - IS-IS inter area, * - candidate default, U - per-user static route

       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/26 is subnetted, 2 subnets

R       172.16.4.0 [120/1] via 172.16.1.1, 00:00:06, Serial0/0

C       172.16.1.0 is directly connected, Serial0/0

     192.168.5.0/29 is subnetted, 1 subnets

D       192.168.5.0 [90/2297856] via 172.16.1.1, 00:03:16, Serial0/0
```

```
     10.0.0.0/32 is subnetted, 1 subnets
O       10.10.10.1 [110/65] via 172.16.1.1, 00:07:53, Serial0/0
R3#ping 172.16.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.4.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/16 ms
R3#ping 192.168.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
R3#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
```

Task 5:

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip access-list extended ROUTING-ACL
R3(config-ext-nacl)#remark 'Deny RIP (UDP Port 520)'
R3(config-ext-nacl)#deny udp any any eq 520
R3(config-ext-nacl)#remark 'Permit EIGRP (IP Protocol 88)'
R3(config-ext-nacl)#permit 88 any any
R3(config-ext-nacl)#remark 'Deny OSPF (IP Protocol 89)'
R3(config-ext-nacl)#deny 89 any any
```

```
R3(config-ext-nacl)#remark 'Permit All Other IP Traffic'

R3(config-ext-nacl)#permit ip any any

R3(config-ext-nacl)#exit

R3(config)#int s0/0

R3(config-if)#ip access-group ROUTING-ACL in

R3(config-if)#^Z

R3#
```

NOTE: Notice that I used the IP protocol numbers 88 and 89 for EIGRP and OSPF, respectively instead of the keywords eigrp and ospf. Even though I did so, Cisco IOS will convert these to the common names which is what you will see when you issue the show access-lists command.

Task 6:

```
R3#clear ip route *

R3#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

       ia - IS-IS inter area, * - candidate default, U - per-user static route

       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/26 is subnetted, 1 subnets

C       172.16.1.0 is directly connected, Serial0/0

     192.168.5.0/29 is subnetted, 1 subnets

D       192.168.5.0 [90/2297856] via 172.16.1.1, 00:00:03, Serial0/0
```

NOTE: You may be wondering why the OSPF neighbor did not immediately go down when you applied the ACL inbound. This is because the adjacency is only removed when the OSPF dead timer expires. Therefore, after a few seconds, you should see the following message on your console:

```
*Mar  1 03:34:01.683: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.5.1 on Serial0/0 from
FULL to DOWN, Neighbor Down: Dead timer expired
```

The reason we need to issue the clear ip route * command is because RIP routes only get removed from the routing tables after the timers expire. This will be a few minutes. Therefore, if you ever see a RIP route that is older than 30 seconds, RIP hold-down timers have kicked in, as illustrated in the following output:

```
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/26 is subnetted, 2 subnets
R       172.16.4.0 [120/1] via 172.16.1.1, 00:03:05, Serial0/0
```

Based on our configuration tasks, we know the ACL is working because we can ping R3 from R1 and the ACL on R3 shows matches for configured rules as follows:

```
R1>ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

R3#show ip access-lists ROUTING-ACL
Extended IP access list ROUTING-ACL
    10 deny udp any any eq rip (80 matches)
    20 permit eigrp any any (453 matches)
    30 deny ospf any any (135 matches)
    40 permit ip any any (15 matches)
```

Lab 59: Configuring and Applying Extended Numbered ACLs

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to create and apply extended numbered Access Control Lists.

Lab Purpose:

Configuring and applying extended ACLs is a fundamental skill. Extended ACLs filter based on source and destination address, as well as Layer 4 protocols TCP and UDP. Extended ACLs and should be applied as close to the source as possible. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to create and apply extended numbered ACLs.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

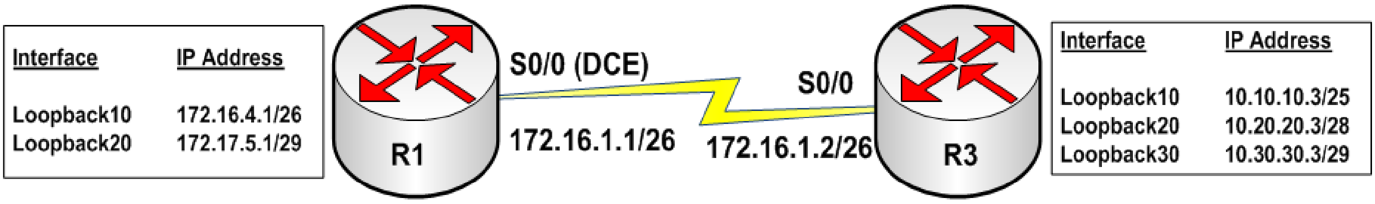
This lab has a difficulty rating of 10/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R3 as illustrated in the topology.

Task 2:

Configure R1 S0/0 which is a DCE to provide a clock rate of 768Kbps to R3. Configure the IP addresses on the Serial interfaces of R1 and R3 as illustrated in the topology.

Task 3:

Configure a static default route on R1 pointing to R3 over the Serial connection between the two routers. Also configure a static default route on R3 pointing to R1 via the Serial connection between the two routers. Configure the Loopback interfaces specified in the diagram on R1 and R3.

Task 4:

To test connectivity, ping R1 from R3 Serial0/0, Loopback10, Loopback20 and Loopback30 interfaces. To ping from the Loopback interfaces, use the **ping <ip_address> /source <interface**> command.

Task 5:

Configure both R1 and R3 to allow Telnet connections. A password of CISCO should for Telnet access.

Task 6:

Configure a numbered extended ACL on R3 to allow Telnet from R1 Loopback10 to R3 Loopback20 and Loopback30. Add another line to the extended ACL to only allow ping traffic from R1 Loopback20 to R3 Loopback10. Apply this ACL inbound on R3 Serial0/0.

To test your Telnet ACL configuration, Telnet from R1 Loopback10 to R3 Loopback10, Loopback20 and Loopback30. If you have configured your ACL correctly, only Telnet sessions to Loopback20 and Loopback30 will work.

Task 7:

To test your ping ACL configuration, ping from R1 Loopback20 to R3 Loopback10, Loopback20 and Loopback30. If you have configured your ACL correctly, only ping from R1 Loopback10 to R3 Loopback20 should work. Use the **ping <ip_address> /source <interface>** command to send pings from the Loopback interfaces.

SOLUTION:

Lab 59 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring DCE clocking, please refer to:

Lab 57 Configuration and Verification Task 2

Lab 58 Configuration and Verification Task 2

Task 3:

R1#**config t**

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#**ip route 0.0.0.0 0.0.0.0 serial0/0 172.16.1.2**

```
R1(config)#int lo10
R1(config-if)#ip address 172.16.4.1 255.255.255.192
R1(config-if)#exit
R1(config)#int lo20
R1(config-if)#ip address 172.17.5.1 255.255.255.248
R1(config-if)#end
R1#
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip route 0.0.0.0 0.0.0.0 serial0/0 172.16.1.1
R3(config)#int loo 10
R3(config-if)#ip address 10.10.10.3 255.255.255.128
R3(config-if)#exit
R3(config)#int loo 20
R3(config-if)#ip address 10.20.20.3 255.255.255.240
R3(config-if)#exit
R3(config)#int loo 30
R3(config-if)#ip address 10.30.30.3 255.255.255.248
R3(config-if)#end
R3#
```

Task 4:

For reference information on sourcing traffic from other interfaces, please refer to:

Lab 55 Configuration and Verification Task 4

Lab 56 Configuration and Verification Task 5

Lab 57 Configuration and Verification Task 4

Lab 57 Configuration and Verification Task 6

Task 5:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#enable secret CISCO

R1(config)#line vty 0 4

R1(config-line)#password CISCO

R1(config-line)#login

R1(config-line)#end

R1#

R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#enable secret CISCO

R3(config)#line vty 0 4

R3(config-line)#password CISCO

R3(config-line)#login

R3(config-line)#end

R3#
```

Task 6:

```
R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#access-list 180 remark 'R1 Loop10->R3 Loop20'

R3(config)#access-list 180 per tcp 172.16.4.0 0.0.0.63 10.20.20.0 0.0.0.15 eq telnet

R3(config)#access-list 180 remark 'R1 Loop10->R3 Loop30'

R3(config)#access-list 180 per tcp 172.16.4.0 0.0.0.63 10.30.30.0 0.0.0.7 eq telnet

R3(config)#access-list 180 per icmp 172.17.5.0 0.0.0.7 10.10.10.0 0.0.0.127 echo

R3(config)#access-list 180 per icmp 172.17.5.0 0.0.0.7 10.10.10.0 0.0.0.127 echo-reply

R3(config)#int s0/0

R3(config-if)#ip access-group 180 in
```

```
R3(config-if)#end
R3#
R1#telnet 10.10.10.3 /source-interface loopback 10
Trying 10.10.10.3 ...
% Destination unreachable; gateway or host down
R1#telnet 10.20.20.3 /source-interface loopback 10
Trying 10.20.20.3 ... Open
User Access Verification
Password:
R3#
R1#telnet 10.30.30.3 /source-interface loopback 10
Trying 10.30.30.3 ... Open
User Access Verification
Password:
R3#
```

Task 7:

```
R1#ping 10.10.10.3 source loopback20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.3, timeout is 2 seconds:
Packet sent with a source address of 172.17.5.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
R1#ping 10.20.20.3 source loopback20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.20.3, timeout is 2 seconds:
Packet sent with a source address of 172.17.5.1
U.U.U
```

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

R1#ping 10.30.30.3 source loopback20

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.30.30.3, timeout is 2 seconds:

Packet sent with a source address of 172.17.5.1

U.U.U

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

Lab 60: Configuring and Applying Extended Named ACLs Outbound

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to create and apply extended numbered Access Control Lists.

Lab Purpose:

Configuring and applying extended ACLs is a fundamental skill. Extended ACLs filter based on source and destination address, as well as Layer 4 protocols TCP and UDP. Extended ACLs and should be applied as close to the source as possible. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to create and apply extended ACLs in the outbound direction.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

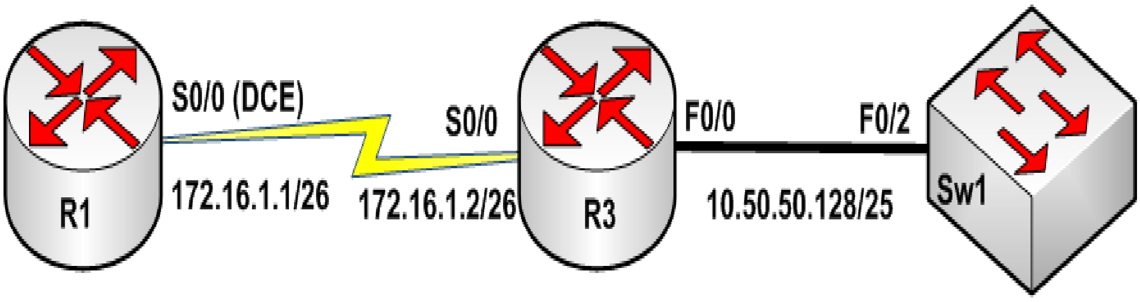
This lab has a difficulty rating of 10/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1, R3 and Sw1 as illustrated in the topology.

Task 2:

Configure R1 S0/0 which is a DCE to provide a clock rate of 768Kbps to R3. Configure the IP addresses on the Serial interfaces of R1 and R3 as illustrated in the topology.

Task 3:

Configure a static default route on R1 pointing to R3 over the Serial connection between the two routers. Also configure a static default route on R3 pointing to R1 via the Serial connection between the two routers.

Task 4:

Configure VLAN 50 on Sw1 and assign it the name ACL-VLAN. Assign port FastEthernet0/2 to this VLAN. Configure interface VLAN50 with the IP address 10.50.50.130/25 and configure a default gateway on the switch to 10.50.50.129. Also, configure interface F0/0 on R3 with the IP address 10.50.50.129 and enable this interface.

Task 5:

Create an extended named ACL called SWITCH-ACL on R3. This ACL should:

- Permit all ICMP traffic from 10.50.50.128/25 to the interface address of R1 S0/0 (172.16.1.1)
- Deny all WWW traffic from 10.50.50.128/25 to the 172.16.1.0/26 subnet
- Permit all TELNET traffic from the interface address of Sw1 (10.50.50.130 to the interface address of R1 S0/0
- Permit all IP traffic from 10.50.50.128/25 to the interface address of R1 S0/0
- Deny all IP traffic from the interface address of Sw1 to the 172.16.1.0/26 subnet

Apply this ACL outbound on R3 S0/0.

Task 6:

To test your ACL configuration by performing ping and Telnet exercises as we done in previous labs and verify matches against your ACL using the show ip access-list SWITCH-ACL command.

SOLUTION:

Lab 60 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring DCE clocking, please refer to:

Lab 57 Configuration and Verification Task 2

Lab 58 Configuration and Verification Task 2

Task 3:

For reference information on configuring static routes, please refer to:

Lab 31 Configuration and Verification Task 4

Lab 32 Configuration and Verification Task 3

Lab 33 Configuration and Verification Task 4

Lab 34 Configuration and Verification Task 4

Task 4:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

For reference information on configuring IP interfaces, please refer to:

Lab 3 Configuration and Verification Task 5

Lab 31 Configuration and Verification Task 3

Task 5:

```
R3#conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
R3(config)#ip access-list extended SWITCH-ACL

R3(config-ext-nacl)#permit icmp 10.50.50.128 0.0.0.127 host 172.16.1.1

R3(config-ext-nacl)#deny tcp 10.50.50.128 0.0.0.127 172.16.1.0 0.0.0.63 eq www

R3(config-ext-nacl)#permit tcp host 10.50.50.130 host 172.16.1.1 eq telnet

R3(config-ext-nacl)#permit ip 10.50.50.128 0.0.0.127 host 172.16.1.1

R3(config-ext-nacl)#deny ip host 10.50.50.130 172.16.1.0 0.0.0.63

R3(config-ext-nacl)#exit

R3(config)#int s0/0

R3(config-if)#ip access-group SWITCH-ACL out

R3(config-if)#end

R3#
```

Task 6:

```
R3#show ip access-lists SWITCH-ACL

Extended IP access list SWITCH-ACL

   10 permit icmp 10.50.50.128 0.0.0.127 host 172.16.1.1 (15 matches)

   20 deny tcp 10.50.50.128 0.0.0.127 172.16.1.0 0.0.0.63 eq www (2 matches)

   30 permit tcp host 10.50.50.130 host 172.16.1.1 eq telnet (75 matches)

   40 permit ip 10.50.50.128 0.0.0.127 host 172.16.1.1 (30 matches)

   50 deny ip host 10.50.50.130 172.16.1.0 0.0.0.63 (5 matches)
```

Lab 61: Restricting Inbound Telnet Access using Extended ACLs

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to create and apply extended Access Control Lists to restrict Telnet access to a router or switch.

Lab Purpose:

Configuring and applying extended ACLs to restrict Telnet access is a fundamental skill. Extended ACLs filter based on source and destination address, as well as Layer 4 protocols TCP and UDP. Extended ACLs and should be applied as close to the source as possible. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to restrict inbound Telnet traffic to the router or switch using ACLs.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

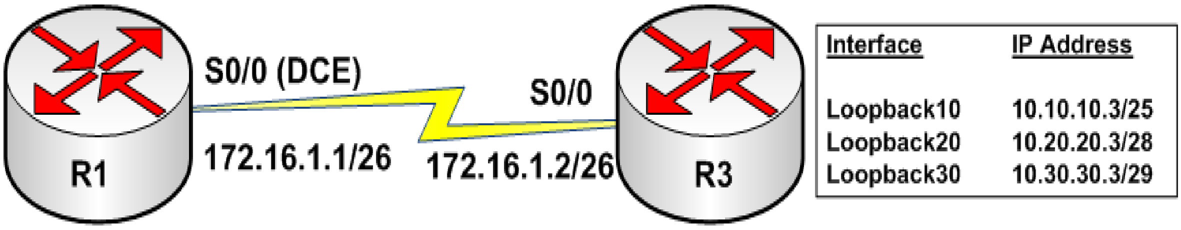
This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Interface	IP Address
Loopback10	10.10.10.3/25
Loopback20	10.20.20.3/28
Loopback30	10.30.30.3/29

Task 1:

Configure the hostnames on routers R1 and R3 as illustrated in the topology.

Task 2:

Configure R1 S0/0 which is a DCE to provide a clock rate of 2Mbps to R3. Configure the IP addresses on the Serial interfaces of R1 and R3 as illustrated in the topology.

Task 3:

Configure a static default route on R1 pointing to R3 over the Serial connection between the two routers. Next, configure the Loopback interfaces specified in the diagram on R3. Finally, configure R1 to allow Telnet sessions. Use a password of CISCO for Telnet login.

Task 4:

To test connectivity, ping R1 from R3 Loopback10, Loopback20 and Loopback30 interfaces.

Task 5:

Create an extended named ACL called TELNET-IN on R1. This ACL should permit Telnet traffic from host 10.10.10.3 to any IP address on R1; deny Telnet from host 10.20.20.3 to any IP address on R1; permit Telnet from host 10.30.30.3 to any IP address on R1. Apply this ACL to the Telnet lines on R1 for inbound traffic.

Task 6:

To test your ACL configuration, Telnet to R1 from R3 Loopback10, Loopback20, and Loopback30 interfaces using the **telnet <ip_address> /source-interface <interface>** command. If your ACL configuration is correct, only Telnet from R3 Loopback10 and Loopback20 should work. Verify matches against your ACL.

SOLUTION:

Lab 61 Configuration and Verification

Task 1:

```
Router#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R1

R1(config)#

Router#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R3

R3(config)#
```

Task 2:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s0/0
```

```
R1(config-if)#no shutdown
R1(config-if)#clock rate 2000000
R1(config-if)#ip add 172.16.1.1 255.255.255.192
R1(config-if)#end
R1#
R3#config term
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int s0/0
R3(config-if)#ip address 172.16.1.2 255.255.255.192
R3(config-if)#no shut
R3(config-if)#end
R3#
R1#ping 172.16.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R1#
R3#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R3#
```

Task 3:

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
R1(config)#ip route 0.0.0.0 0.0.0.0 serial0/0 172.16.1.2

R1(config)#line vty 0 4

R1(config-line)#password CISCO

R1(config-line)#login

R1(config-line)#end

R1#

R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int loo 10

R3(config-if)#ip address 10.10.10.3 255.255.255.128

R3(config-if)#exit

R3(config)#int loo 20

R3(config-if)#ip address 10.20.20.3 255.255.255.240

R3(config-if)#exit

R3(config)#int loo 30

R3(config-if)#ip address 10.30.30.3 255.255.255.248

R3(config-if)#exit

R3(config)#line vty 0 4

R3(config-line)#password CISCO

R3(config-line)#login

R3(config-line)#end

R3#
```

Task 4:

```
R1#ping 10.10.10.3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.3, timeout is 2 seconds:

!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R1#ping 10.20.20.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.20.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
R1#ping 10.30.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.30.30.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 5:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list extended TELNET-IN
R1(config-ext-nacl)#remark 'Permit Telnet From Host 10.10.10.3'
R1(config-ext-nacl)#permit tcp host 10.10.10.3 any eq 23
R1(config-ext-nacl)#remark 'Deny Telnet From Host 10.20.20.3'
R1(config-ext-nacl)#deny tcp host 10.20.20.3 any eq 23
R1(config-ext-nacl)#remark 'Permit Telnet From Host 10.30.30.3'
R1(config-ext-nacl)#permit tcp host 10.30.30.3 any eq 23
R1(config-ext-nacl)#exit
R1(config)#line vty 0 4
R1(config-line)#access-class TELNET-IN in
R1(config-line)#end
R1#
```

Task 6:

```
R3#telnet 172.16.1.1 /source-interface loopback 10

Trying 172.16.1.1 ... Open

User Access Verification

Password:

R1#

R3#telnet 172.16.1.1 /source-interface loopback 20

Trying 172.16.1.1 ...

% Connection refused by remote host

R3#telnet 172.16.1.1 /source-interface loopback 30

Trying 172.16.1.1 ... Open

User Access Verification

Password:

R1#
```

NOTE: The access-class command is used to apply ACLs to the router or switch VTY lines to prevent inbound Telnet and/or SSH sessions to the device. This is not the same as using ACLs that are applied to interfaces to prevent Telnet and/or SSH sessions to the device. Make a mental note of this.

Based on our example above, we can see matches to our ACL rules as follows:

```
R1#sh ip access-lists TELNET-IN
Extended IP access list TELNET-IN
    10 permit tcp host 10.10.10.3 any eq telnet (2 matches)
    20 deny tcp host 10.20.20.3 any eq telnet (1 match)
    30 permit tcp host 10.30.30.3 any eq telnet (2 matches)
```

Lab 62: Restricting Outbound Telnet Access using Extended ACLs

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to create and apply extended Access Control Lists to restrict Telnet access from a router or switch.

Lab Purpose:

Configuring and applying extended ACLs to restrict Telnet access is a fundamental skill. Extended ACLs filter based on source and destination address, as well as Layer 4 protocols TCP and UDP. Telnet traffic sourced from the router or switch cannot be filtered using outbound interface ACLs. Instead, because the VTY lines are used, this is where the ACL restrictions should be applied. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to create and apply extended numbered ACLs.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

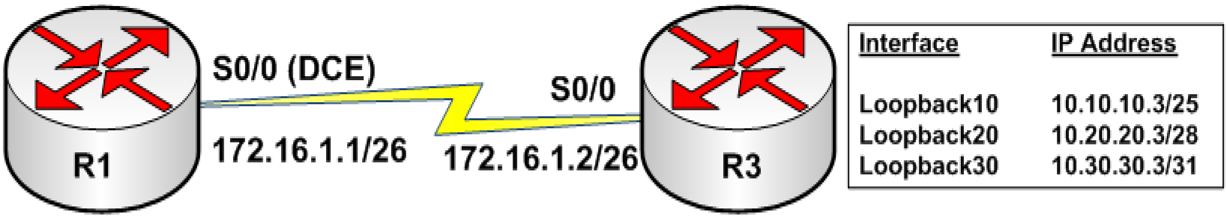
This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Interface	IP Address
Loopback10	10.10.10.3/25
Loopback20	10.20.20.3/28
Loopback30	10.30.30.3/31

Task 1:

Configure the hostnames on routers R1 and R3 as illustrated in the topology.

Task 2:

Configure R1 S0/0 which is a DCE to provide a clock rate of 768Kbps to R3. Configure the IP addresses on the Serial interfaces of R1 and R3 as illustrated in the topology.

Task 3:

Configure a static default route on R1 pointing to R3 over the Serial connection between the two routers. Configure the Loopback interfaces specified in the diagram on R3. Configure R3 to allow Telnet sessions. Use a password of CISCO for Telnet login.

Task 4:

To test connectivity, Telnet from R1 to R3 Loopback10, Loopback20 and Loopback30 interfaces.

Task 5:

Create an extended named ACL called TELNET-OUT on R1. This ACL should deny all Telnet traffic to 10.10.10.0/25; permit Telnet to 10.20.20.0/28; deny Telnet traffic to 10.30.30.0/29. Apply this ACL to the Telnet lines on R1 for outbound Telnet traffic originated from the router.

Task 6:

To test your ACL configuration, Telnet from R1 from R3 Loopback10, Loopback20, and Loopback30 interfaces. If your ACL configuration is correct, only Telnet from R3 Loopback20 should work.

SOLUTION:

Lab 62 Configuration and Verification

Task 1:

```
Router#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R1

R1(config)#

Router#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname R3

R3(config)#
```

Task 2:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int s0/0

R1(config-if)#no shutdown
```

```
R1(config-if)#clock rate 2000000

R1(config-if)#ip add 172.16.1.1 255.255.255.192

R1(config-if)#end

R1#

R3#config term

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int s0/0

R3(config-if)#ip address 172.16.1.2 255.255.255.192

R3(config-if)#no shut

R3(config-if)#end

R3#

R1#ping 172.16.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:

!!!!!

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

R1#

R3#ping 172.16.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

!!!!!

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

R3#
```

Task 3:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#ip route 0.0.0.0 0.0.0.0 serial0/0 172.16.1.2
```

```
R1(config)#line vty 0 4

R1(config-line)#password CISCO

R1(config-line)#login

R1(config-line)#end

R1#

R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int loo 10

R3(config-if)#ip address 10.10.10.3 255.255.255.128

R3(config-if)#exit

R3(config)#int loo 20

R3(config-if)#ip address 10.20.20.3 255.255.255.240

R3(config-if)#exit

R3(config)#int loo 30

R3(config-if)#ip address 10.30.30.3 255.255.255.248

R3(config-if)#exit

R3(config)#line vty 0 4

R3(config-line)#password CISCO

R3(config-line)#login

R3(config-line)#end

R3#
```

Task 4:

```
R1>telnet 10.10.10.3

Trying 10.10.10.3 ... Open

User Access Verification

Password:

R3#
```

```
R1>telnet 10.20.20.3

Trying 10.20.20.3 ... Open

User Access Verification

Password:

R3#

R1>telnet 10.30.30.3

Trying 10.30.30.3 ... Open

User Access Verification

Password:

R3#
```

Task 5:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#ip access-list extended TELNET-OUT

R1(config-ext-nacl)#remark 'Deny Traffic To 10.10.10.0/25'

R1(config-ext-nacl)#deny ip any 10.10.10.0 0.0.0.127

R1(config-ext-nacl)#remark 'Permit Traffic To 10.20.20.0/28'

R1(config-ext-nacl)#permit ip any 10.20.20.0 0.0.0.15

R1(config-ext-nacl)#remark 'Deny Traffic To 10.30.30.0/29'

R1(config-ext-nacl)#deny ip any 10.30.30.0 0.0.0.7

R1(config-ext-nacl)#exit

R1(config)#line vty 0 4

R1(config-line)#access-class TELNET-OUT out

R1(config-line)#end

R1#
```

Task 6:

For reference information on completing Task 6, please use the **telnet** command from R1

Lab 63: Debugging Network Traffic Using Extended ACLs

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to create extended Access Control Lists to troubleshoot the network using the debug ip packet command.

Lab Purpose:

Limiting debugging to specific traffic types using ACLs is a fundamental skill. Extended ACLs can be configured to match on source and destination address, as well as Layer 4 protocols TCP and UDP. Using extended ACLs, you can debug specific types of traffic to troubleshoot a network. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to create and debug using extended numbered ACLs.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

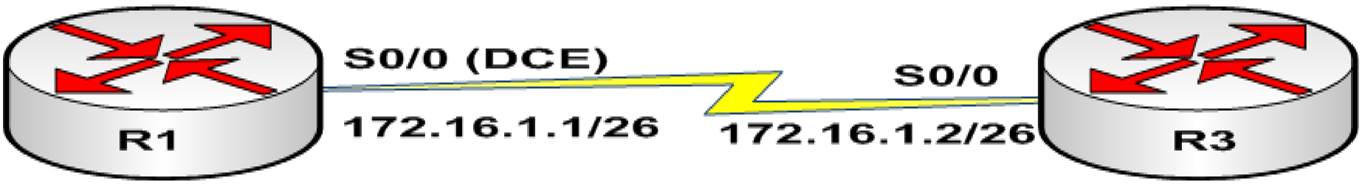
This lab has a difficulty rating of 6/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 5 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R3 as illustrated in the topology.

Task 2:

Configure R1 S0/0 which is a DCE to provide a clock rate of 768Kbps to R3. Configure the IP addresses on the Serial interfaces of R1 and R3 as illustrated in the topology.

Task 3:

Configure an extended ACL on R1 to match and permit all ICMP traffic. Use ACL number 111.

Task 4:

Enable detailed debugging on R1 using the debug ip packet 111 detail command. This ACL specifies that we are only going to be limiting debugging to the traffic type specified in the ACL, which is ICMP.

Task 5:

Ping R2 from R1. You should see some detailed information printed on the Console on R1 based on your debugging. When you are done, disable debugging on R1.

SOLUTION:

Lab 63 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring DCE clocking, please refer to:

Lab 57 Configuration and Verification Task 2

Lab 58 Configuration and Verification Task 2

Task 3:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#access-list 111 remark 'Permit all ICMP traffic'

R1(config)#access-list 111 permit icmp any any

R1(config)#end

R1#
```

Task 4:

```
R1#debug ip packet 111 detail

IP packet debugging is on (detailed) for access list 111

R1#
```

Task 5:

```
R1#ping 172.16.1.2
```

```
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms

R1#

*Mar  1 01:10:16.600: IP: tableid=0, s=172.16.1.1 (local), d=172.16.1.2 (Serial0/0),
routed      via FIB

*Mar  1 01:10:16.600: IP: s=172.16.1.1 (local), d=172.16.1.2 (Serial0/0), len 100, sending

*Mar  1 01:10:16.604:     ICMP type=8, code=0

*Mar  1 01:10:16.608: IP: tableid=0, s=172.16.1.2 (Serial0/0), d=172.16.1.1 (Serial0/0),
routed via RIB

*Mar  1 01:10:16.608: IP: s=172.16.1.2 (Serial0/0), d=172.16.1.1 (Serial0/0), len 100, rcvd
3

*Mar  1 01:10:16.608:     ICMP type=0, code=0

*Mar  1 01:10:16.608: IP: tableid=0, s=172.16.1.1 (local), d=172.16.1.2 (Serial0/0), routed
via FIB

*Mar  1 01:10:16.608: IP: s=172.16.1.1 (local), d=172.16.1.2 (Serial0/0), len 100, sending

*Mar  1 01:10:16.612:     ICMP type=8, code=0

*Mar  1 01:10:16.616: IP: tableid=0, s=172.16.1.2 (Serial0/0), d=172.16.1.1 (Serial0/0),
routed via RIB

*Mar  1 01:10:16.616: IP: s=172.16.1.2 (Serial0/0), d=172.16.1.1 (Serial0/0), len 100, rcvd
3

*Mar  1 01:10:16.616:     ICMP type=0, code=0

R1#undebug all

All possible debugging has been turned off
```

NOTE: Based on the ping , we can see that ICMP Type 8, Code 0 messages are being sent from R1 to R3 and ICMP Type 0, Code 0 messages are being sent from R3 to R1. You are required to know the different ICMP Type Codes for the Cisco CCNA exam, so if you are not sure what these two codes are, now would be a good time to look them up. Make sure you commit the ICMP Types and Codes to memory.

Lab 64: Logging ACL Matches

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure Access Control Lists to log traffic that matches any particular entry within the configured ACL.

Lab Purpose:

Logging traffic based on ACL rule configuration is a fundamental skill. Both named and numbered standard and extended ACLs can be configured to log information on matches against their configured rules. This logging can be performed locally (on the router or switch) or remotely (to a SYSLOG server). As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure ACLs to log information against configured rules.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

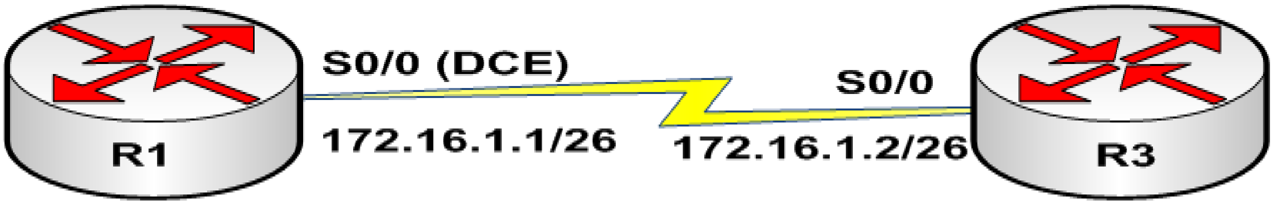
This lab has a difficulty rating of 6/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 5 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and R3 as illustrated in the topology.

Task 2:

Configure R1 S0/0 which is a DCE to provide a clock rate of 768Kbps to R3. Configure the IP addresses on the Serial interfaces of R1 and R3 as illustrated in the topology.

Task 3:

Enable local logging on R3. The logging level should be for informational messages only.

Task 4:

Configure an extended named ACL on R3 to permit all Telnet and ICMP traffic types. This ACL should log when Telnet or ICMP traffic matches it. Configure this ACL with the name MyACL and apply it inbound on R3 Serial0/0.

Task 5:

Clear the logs on R3 using the clear log command. Ping R3 from R1 and check log on R3 with the show log command. If you have configured the ACL correctly, you will have a log message about the ACL line permitting ICMP traffic to R3. Telnet to R3 from R1 and check log on R3 with the **show log** command. If you have configured the ACL correctly, you will have a log message about the ACL line permitting Telnet traffic to R3.

SOLUTION:

Lab 64 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring DCE clocking, please refer to:

Lab 57 Configuration and Verification Task 2

Lab 58 Configuration and Verification Task 2

Task 3:

```
R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#logging on

R3(config)#logging buffered informational

R3(config)#end

R3#
```

NOTE: When configuring logging, it is always good practice to enable logging with the logging on command. When logging messages to the buffer on the router, the options available are:

```
R3#conf t
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#logging buffered ?
```

```
<0-7>              Logging severity level
<4096-2147483647>  Logging buffer size
alerts             Immediate action needed           (severity=1)
critical           Critical conditions               (severity=2)
debugging          Debugging messages                (severity=7)
emergencies        System is unusable                (severity=0)
errors             Error conditions                  (severity=3)
informational      Informational messages            (severity=6)
notifications      Normal but significant conditions (severity=5)
warnings           Warning conditions                (severity=4)
xml                Enable logging in XML to XML logging buffer
<cr>
```

If you specify a Severity of 5 (Notifications) then the router or switch will log all messages up to and including that severity level. In other words, the device will log message levels 1 through 5, inclusive. To see debugging output, you must enable a Severity of 7. When logging debugging messages, ensure that there is enough buffer space to for these messages. Use the logging buffered <4096-2147483647> command to specify the buffer size.

Task 4:

```
R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#ip access-list extended MyACL

R3(config-ext-nacl)#permit tcp any any eq telnet log

R3(config-ext-nacl)#permit icmp any any log

R3(config-ext-nacl)#exit

R3(config)#int s0/0

R3(config-if)#ip access-group MyACL in

R3(config-if)#end

R3#

R3#show ip access-lists

Extended IP access list MyACL

    10 permit tcp any any eq telnet log

    20 permit icmp any any log
```

Task 5:

For information on how to ping or Telnet from Cisco routers, please see the following:

Lab 62 Configuration and Verification Task 2

Lab 62 Configuration and Verification Task 4

```
R3#show log

Syslog logging: enabled (0 messages dropped, 1 messages rate-limited, 0 flushes, 0 overruns, xml disabled)

    Console logging: disabled

    Monitor logging: level debugging, 0 messages logged, xml disabled

    Buffer logging: level informational, 6 messages logged, xml disabled

    Logging Exception size (4096 bytes)

    Count and timestamp logging messages: disabled

    Trap logging: level informational, 35 message lines logged

Log Buffer (4096 bytes):

*Mar  1 01:29:00.370: %SEC-6-IPACCESSLOGDP: list MyACL permitted icmp 172.16.1.1 -> 172.16.1.2 (0/0), 1 packet

*Mar  1 01:29:54.771: %SEC-6-IPACCESSLOGP: list MyACL permitted tcp 172.16.1.1(17218) -> 172.16.1.2(23), 1 packet

*Mar  1 01:30:16.751: %SEC-6-IPACCESSLOGDP: list MyACL permitted icmp 172.16.1.1 -> 172.16.1.2 (8/0), 1 packet

*Mar  1 01:30:23.186: %SEC-6-IPACCESSLOGP: list MyACL permitted tcp 172.16.1.1(60418) -> 172.16.1.2(23), 1 packet
```

Lab 65: Configuring Static Network Address Translation

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure static NAT.

Lab Purpose:

NAT configuration is a fundamental skill. Static NAT provides a one-to-one translation between a private IP address (RFC 1918) and a public IP address. Static NAT is typically used to provide access to private inside hosts from outside hosts or networks. When static NAT is configured, outside hosts or networks connect to devices on the inside using a public or external IP address. This hides the private IP addresses of hosts on the inside. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure static NAT.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

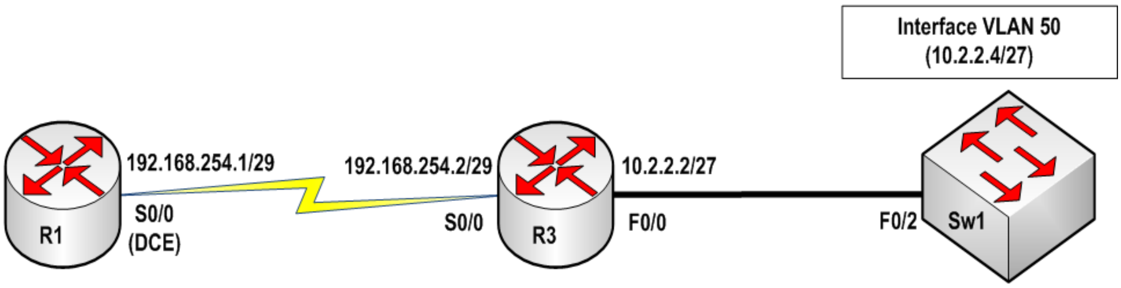
This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1, R3 and Sw1 as illustrated in the topology.

Task 2:

Configure R1 S0/0 which is a DCE to provide a clock rate of 256Kbps to R3. Configure the IP addresses on the Serial interfaces of R1 and R3 as illustrated in the topology.

Task 3:

Configure VLAN 50 named NAT_VLAN on Sw1. Assign the FastEthernet0/2 interface on Sw1 to this VLAN. Also, configure Sw1 to allow Telnet access using a password of CISCO.

Task 4:

Configure interface VLAN 50 on Sw1 and assign it the IP address illustrated in the topology. The default gateway on Sw1 should be 10.2.2.2. Next, configure interface FastEthernet0/0 in R3 and assign it the IP address illustrated in the topology.

Task 5:

Test connectivity by pinging from R1 to R3 and pinging from R3 to Sw1. These should all be successful. However, since R1 does not know about the 10.2.2.0/27 subnet, Sw1 will not be able to ping R1. Verify this.

Task 6:

Configure R3 F0/0 as the inside NAT interface and S0/0 as the outside NAT interface. Next, create a static NAT statement on R3 mapping the inside address of 10.2.2.4 (Sw1 interface VLAN 50) to the outside address of 192.168.254.4.

Task 7:

Ping from Sw1 to R1 and verify that the ping is successful. Next, Telnet from R1 to 192.168.254.4 and verify that you connect to Sw1 via the NAT configured on R3.

Lab 65 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring DCE clocking, please refer to:

Lab 57 Configuration and Verification Task 2

Lab 58 Configuration and Verification Task 2

For reference information on configuring IP interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

Task 3:

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#vlan 50

Sw1(config-vlan)#name NAT_VLAN

Sw1(config-vlan)#exit

Sw1(config)#int f0/2

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 50

Sw1(config-if)#no shutdown

Sw1(config-if)#exit

Sw1(config)#line vty 0 15

Sw1(config-line)#password CISCO

Sw1(config-line)#login

Sw1(config-line)#end
```

```
Sw1#

Sw1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
50   NAT_VLAN                         active    Fa0/2
1002 fddi-default                     active
1003 trcrf-default                    active
1004 fddinet-default                  active
1005 trbrf-default                    active
```

Task 4:

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#int vlan 1

Sw1(config-if)#shutdown

Sw1(config-if)#exit

Sw1(config)#int vlan 50

Sw1(config-if)#no shutdown

Sw1(config-if)#ip address 10.2.2.4 255.255.255.224

Sw1(config-if)#exit

Sw1(config)#ip default-gateway 10.2.2.2

Sw1(config)#end

Sw1#

R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int fa0/0

R3(config-if)#no shutdown

R3(config-if)#ip address 10.2.2.2 255.255.255.224
```

```
R3(config-if)#end
R3#
```

Task 5:

```
R1#ping 192.168.254.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R3#ping 192.168.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R3#ping 10.2.2.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.4, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/3/4 ms
Sw1#ping 10.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
Sw1#ping 192.168.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:
.....
```

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

Task 6:

```
R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int fa0/0

R3(config-if)#ip nat inside

R3(config-if)#exit

R3(config)#int s0/0

R3(config-if)#ip nat outside

R3(config-if)#exit

R3(config)#ip nat inside source static 10.2.2.4 192.168.254.4

R3(config)#end

R3#

R3#show ip nat translations

Pro Inside global      Inside local       Outside local      Outside global

--- 192.168.254.4      10.2.2.4           ---                ---
```

Task 7:

```
Sw1#ping 192.168.254.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms

R1#telnet 192.168.254.4

Trying 192.168.254.4 ... Open

User Access Verification

Password:

Sw1#
```

NOTE: You can look at translations statistics using the show ip nat statistics command. If you are having issues with NAT, this command can show you the hits versus the misses, which indicates successful versus unsuccessful translations. Use those counters to troubleshoot Network Address Translation.

```
R3#show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial0/0
Inside interfaces:
  FastEthernet0/0
Hits: 53  Misses: 0
Expired translations: 0
Dynamic mappings:
```

Also keep in mind that because we configured static NAT, we will not see any dynamic NAT mappings or translation statistics until we configure dynamic NAT.

Lab 66: Configuring Dynamic Network Address Translation

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure dynamic NAT using a pool of IP addresses for translation.

Lab Purpose:

NAT configuration is a fundamental skill. Dynamic NAT provides dynamic one-to-one translation between private IP addresses (RFC 1918) and public IP addresses. Dynamic NAT is typically used to provide inside private hosts with access to public or external networks without revealing the private IP addresses of the inside hosts. When dynamic NAT is used, hosts on the outside cannot access hosts on the inside. In other words, dynamic NAT works only when traffic is coming from hosts on the inside. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure dynamic NAT.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

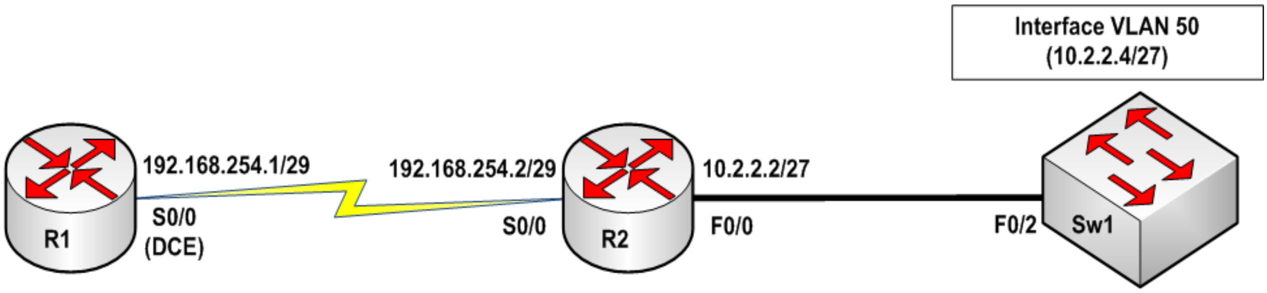
This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1, R2 and Sw1 as illustrated in the topology.

Task 2:

Configure R1 S0/0 which is a DCE to provide a clock rate of 256Kbps to R2. Configure the IP addresses on the Serial interfaces of R1 and R2 as illustrated in the topology.

Task 3:

Configure VLAN 50 named NAT_VLAN on Sw1. Assign the FastEthernet0/2 interface on Sw1 to this VLAN. Also, configure R1 to allow Telnet access using a password of CISCO.

Task 4:

Configure interface VLAN 50 on Sw1 and assign it the IP address illustrated in the topology. The default gateway on Sw1 should be 10.2.2.2. Next, configure interface FastEthernet0/0 in R2 and assign it the IP address illustrated in the topology.

Task 5:

Test connectivity by pinging from R1 to R2 and pinging from R2 to Sw1. These should all be successful. However, since R1 does not know about the 10.2.2.0/27 subnet, Sw1 will not be able to ping R1 or vice versa.

Task 6:

Configure R2 F0/0 as the inside NAT interface and S0/0 as the outside NAT interface. Next, create an ACL to permit all IP traffic from the 10.2.2.0/27 subnet to any destination. You can use either a named or numbered ACL.

Task 7:

Create a NAT pool called Dynamic-NAT. The starting IP address in this pool should be 192.168.254.3 and the ending IP address in this pool should be 192.168.254.6. This should have the same prefix length as the Serial0/0 subnet.

Task 8:

Configure NAT to translate all address specified in the ACL you created to the pool you created in Task 7.

Task 9:

Ping R1 from Sw1. Next, ping R1 from the FastEthernet0/0 interface of R2 using the **ping <ip_address> source <interface>** command. If you have configured your NAT translation, the ping should be successful. Use the **show ip nat translations** command to verify your dynamic NAT translations.

SOLUTION:

Lab 66 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring DCE clocking, please refer to:

Lab 57 Configuration and Verification Task 2

Lab 58 Configuration and Verification Task 2

For reference information on configuring IP interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

Task 3:

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#vlan 50

Sw1(config-vlan)#name NAT_VLAN

Sw1(config-vlan)#exit

Sw1(config)#int f0/2

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 50

Sw1(config-if)#no shutdown
```

```
Sw1(config-if)#exit

Sw1(config)#line vty 0 15

Sw1(config-line)#password CISCO

Sw1(config-line)#login

Sw1(config-line)#end

Sw1#

Sw1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
50   NAT_VLAN                         active    Fa0/2
1002 fddi-default                     active
1003 trcrf-default                    active
1004 fddinet-default                  active
1005 trbrf-default                    active
```

Task 4:

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#int vlan 1

Sw1(config-if)#shutdown

Sw1(config-if)#exit

Sw1(config)#int vlan 50

Sw1(config-if)#no shutdown

Sw1(config-if)#ip address 10.2.2.4 255.255.255.224

Sw1(config-if)#exit

Sw1(config)#ip default-gateway 10.2.2.2

Sw1(config)#end

Sw1#
```

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int fa0/0
R2(config-if)#no shutdown
R2(config-if)#ip address 10.2.2.2 255.255.255.224
R2(config-if)#end
R2#
```

Task 5:

```
R1#ping 192.168.254.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R2#ping 192.168.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R2#ping 10.2.2.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.4, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/3/4 ms
Sw1#ping 10.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

Sw1#ping 192.168.254.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:

.....

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

Task 6:

```
R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#int fa0/0

R2(config-if)#ip nat inside

R2(config-if)#exit

R2(config)#int s0/0

R2(config-if)#ip nat outside

R2(config-if)#exit

R2(config)#ip access-list extended NAT-ACL

R2(config-ext-nacl)#remark 'Permit The 10.2.2.0/27 Subnet To Be NATd'

R2(config-ext-nacl)#permit ip 10.2.2.0 0.0.0.31 any

R2(config-ext-nacl)#end

R2#
```

Task 7:

```
R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#ip nat pool Dynamic-NAT 192.168.254.3 192.168.254.6 prefix-length 29

R2(config)#^Z

R2#
```

Task 8:

```
R2#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#ip nat inside source list NAT-ACL pool Dynamic-NAT

R2(config)#end

R2#

R2#show ip nat statistics

Total active translations: 0 (0 static, 0 dynamic; 0 extended)

Outside interfaces:

  Serial0/0

Inside interfaces:

  FastEthernet0/0

Hits: 53  Misses: 0

Expired translations: 0

Dynamic mappings:

-- Inside Source

[Id: 1] access-list NAT-ACL pool Dynamic-NAT refcount 0

 pool Dynamic-NAT: netmask 255.255.255.248

        start 192.168.254.3 end 192.168.254.6

        type generic, total addresses 4, allocated 0 (0%), misses 0
```

Task 9:

```
Sw1#ping 192.168.254.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms

R2#ping 192.168.254.1 source fastethernet0/0
```

```
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:

Packet sent with a source address of 10.2.2.2

!!!!!

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

R2#show ip nat translations

Pro Inside global      Inside local       Outside local      Outside global

--- 192.168.254.3      10.2.2.4           ---                ---

--- 192.168.254.4      10.2.2.2           ---                ---

R2#show ip nat statistics

Total active translations: 2 (0 static, 2 dynamic; 0 extended)

Outside interfaces:

  Serial0/0

Inside interfaces:

  FastEthernet0/0

Hits: 91  Misses: 2

Expired translations: 0

Dynamic mappings:

-- Inside Source

[Id: 1] access-list NAT-ACL pool Dynamic-NAT refcount 2

 pool Dynamic-NAT: netmask 255.255.255.248

        start 192.168.254.3 end 192.168.254.6

        type generic, total addresses 4, allocated 2 (50%), misses 0
```

NOTE: Now that we have dynamic NAT configured, and we have pinged R1 from the F0/0 interface of R2 as well as from Sw1, we can see two dynamic translations in the NAT table. The first is a translation of the inside address 10.2.2.4 to the outside address of 192.168.254.3, and the second is the translation of the inside address 10.2.2.2 to the outside address of 192.168.254.3. Because the NAT pool only have 4 total IP addresses allocated, we can see that ½ the pool is in use as specified in the line type generic, total addresses 4, allocated 2 (50%), misses 0. Pay attention to the information printed by this command and commit it to memory.

Lab 67: Configuring interface-based Port Address Translation

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure interface-based PAT.

Lab Purpose:

PAT configuration is a fundamental skill. PAT provides many-to-one translation using random port numbers. This means that multiple inside hosts can use the same outside address to communicate with external devices, while hiding their private IP addresses. Like dynamic NAT, PAT works in one direction only: from the inside to the outside. Interface-based PAT translates all private IP addresses to the outside interface on the router. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure interface-based Port Address Translation.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

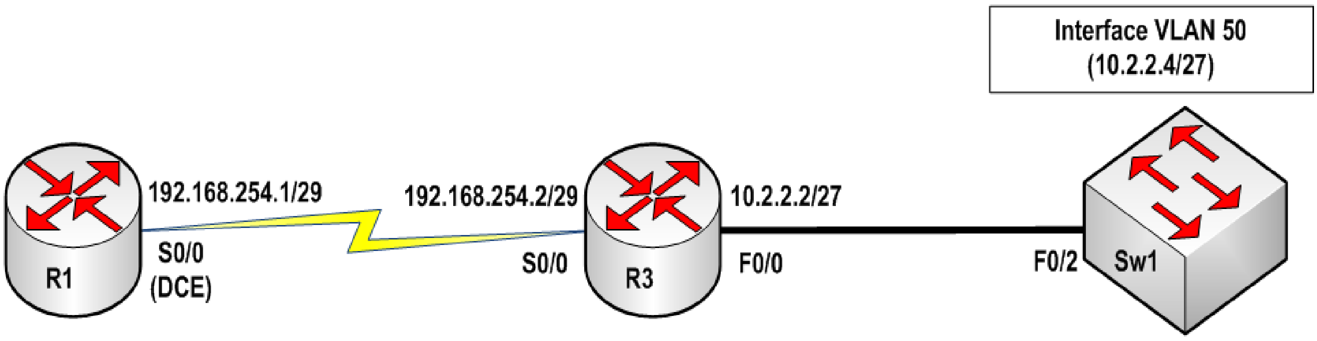
This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1, R2 and Sw1 as illustrated in the topology.

Task 2:

Configure R1 S0/0 which is a DCE to provide a clock rate of 256Kbps to R2. Configure the IP addresses on the Serial interfaces of R1 and R2 as illustrated in the topology.

Task 3:

Configure VLAN 50 named NAT_VLAN on Sw1. Assign the FastEthernet0/2 interface on Sw1 to this VLAN. Also, configure R1 to allow Telnet access using a password of CISCO.

Task 4:

Configure interface VLAN 50 on Sw1 and assign it the IP address illustrated in the topology. The default gateway on Sw1 should be 10.2.2.2. Next, configure interface FastEthernet0/0 in R2 and assign it the IP address illustrated in the topology.

Task 5:

Test connectivity by pinging from R1 to R2 and pinging from R2 to Sw1. These should all be successful. However, since R1 does not know about the 10.2.2.0/27 subnet, Sw1 will not be able to ping R1 or vice versa.

Task 6:

Create an ACL to permit only ICMP and Telnet traffic from the 10.2.2.0/27 subnet to any destination. You can create either a named or numbered ACL to complete this task.

Task 7:

Configure R2 F0/0 as the inside interface for NAT and S0/0 as the outside interface for NAT. Next, configure PAT to translate all IP addresses specified in the ACL you configured in Task 6 to the S0/0 interface of R2.

Task 8:

Ping R1 from Sw1. Also, perform a Telnet from Sw1 to R1. If you have configured interface-based PAT correctly, the ping and Telnet should work. Check the NAT translation table on R2 using the **show ip nat translations** command.

SOLUTION:

Lab 67 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring DCE clocking, please refer to:

Lab 57 Configuration and Verification Task 2

Lab 58 Configuration and Verification Task 2

For reference information on configuring IP interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

Task 3:

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#vlan 50

Sw1(config-vlan)#name NAT_VLAN

Sw1(config-vlan)#exit

Sw1(config)#int f0/2

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 50

Sw1(config-if)#no shutdown

Sw1(config-if)#exit

Sw1(config)#line vty 0 15

Sw1(config-line)#password CISCO

Sw1(config-line)#login

Sw1(config-line)#end

Sw1#

Sw1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
50   NAT_VLAN                         active    Fa0/2
1002 fddi-default                     active
1003 trcrf-default                    active
1004 fddinet-default                  active
1005 trbrf-default                    active
```

Task 4:

```
Sw1#conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#int vlan 1
Sw1(config-if)#shutdown
Sw1(config-if)#exit
Sw1(config)#int vlan 50
Sw1(config-if)#no shutdown
Sw1(config-if)#ip address 10.2.2.4 255.255.255.224
Sw1(config-if)#exit
Sw1(config)#ip default-gateway 10.2.2.2
Sw1(config)#end
Sw1#
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int fa0/0
R3(config-if)#no shutdown
R3(config-if)#ip address 10.2.2.2 255.255.255.224
R3(config-if)#end
R3#
```

Task 5:

```
R1#ping 192.168.254.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R3#ping 192.168.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R3#ping 10.2.2.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.4, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/3/4 ms
Sw1#ping 10.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
Sw1#ping 192.168.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Task 6:

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 140 remark 'Permit ICMP Traffic For NAT'
Sw1(config)#access-list 140 permit icmp 10.2.2.0 0.0.0.31 any
Sw1(config)#access-lis 140 permit tcp 10.2.2.0 0.0.0.31 any eq telnet
R3(config)#end
R3#
R3#show ip access-lists 140
Extended IP access list 140
```

```
    10 permit icmp 10.2.2.0 0.0.0.31 any

    20 permit tcp 10.2.2.0 0.0.0.31 any eq telnet
```

Task 7:

```
R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int fa0/0

R3(config-if)#ip nat inside

R3(config-if)#exit

R3(config)#int s0/0

R3(config-if)#ip nat outside

R3(config-if)#exit

R3(config)#ip nat inside source list 140 interface serial 0/0 overload

R3(config)#end

R3#
```

NOTE: Port Address Translation (or NAT Overload) is enabled by using the overload keyword in the ip nat inside souce list command. This allows the router to overload address translation to the specified interface or IP address. Do not forget to issue this keyword when configuring PAT. Otherwise, you will have created dynamic NAT and will run out of addresses after the very first translation.

Task 8:

Perform a ping and then telnet from Sw1 and then disconnect from the telnet session.

```
Sw1#ping 192.168.254.1

Sw1#telnet 192.168.254.1

R3#

R3#show ip nat translations

Pro Inside global      Inside local       Outside local       Outside global

tcp 192.168.254.2:11777 10.2.2.4:11777    192.168.254.1:23   192.168.254.1:23

icmp 192.168.254.2:4176 10.2.2.4:4176     192.168.254.1:4176 192.168.254.1:4176

icmp 192.168.254.2:4177 10.2.2.4:4177     192.168.254.1:4177 192.168.254.1:4177
icmp 192.168.254.2:4178 10.2.2.4:4178    192.168.254.1:4178 192.168.254.1:4178

icmp 192.168.254.2:4179 10.2.2.4:4179    192.168.254.1:4179 192.168.254.1:4179

icmp 192.168.254.2:4180 10.2.2.4:4180    192.168.254.1:4180 192.168.254.1:4180
```

NOTE: Notice that there is only one translation for Telnet but there are five translations for Ping. This is because a dynamic translation is created for every ping packet sent. By default, Cisco routers and switches will send five ping packets. You can tell they are from the same ping because the port numbers are sequential.

Also, by using interface based PAT, R1 will see all packets (Ping and Telnet) being sourced from the Serial0/0 interface of R3. If we enabled the debug ip packet detail command on R1, we would see the following for Telnet:

```
*Mar  1 01:07:45.127:     TCP src=23, dst=12289, seq=2994196370, ack=125681435,
win=4085 ACK PSH
*Mar  1 01:07:45.272: IP: tableid=0, s=192.168.254.2 (Serial0/0), d=192.168.254.1
(Serial0/0), routed via RIB
```

In a similar manner, we would also see the following for pings from Sw2:

```
*Mar  1 01:08:40.907: IP: s=192.168.254.2 (Serial0/0), d=192.168.254.1 (Serial0/0), len
100, rcvd 3
*Mar  1 01:08:40.907:     ICMP type=8, code=0
*Mar  1 01:08:40.907: IP: tableid=0, s=192.168.254.1 (local), d=192.168.254.2
(Serial0/0), routed via FIB
*Mar  1 01:08:40.907: IP: s=192.168.254.1 (local), d=192.168.254.2 (Serial0/0), len 100,
sending
*Mar  1 01:08:40.907:     ICMP type=0, code=0
```

R#**show ip nat statistics**

```
Total active translations: 5 (0 static, 5 dynamic; 5 extended)

Outside interfaces:

  Serial0/0

Inside interfaces:

  FastEthernet0/0

Hits: 153  Misses: 23

Expired translations: 16

Dynamic mappings:

-- Inside Source

[Id: 3] access-list 140 interface Serial0/0 refcount 5
```

Lab 68: Configuring pool-based Port Address Translation

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure pool-based PAT.

Lab Purpose:

PAT configuration is a fundamental skill. PAT provides many-to-one translation using random port numbers. This means that multiple inside hosts can use the same outside address to communicate with external devices, while hiding their private IP addresses. Like dynamic NAT, PAT works in one direction only: from the inside to the outside. Interface-based PAT translates all private IP addresses to the outside interface on the router. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure interface-based Port Address Translation.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

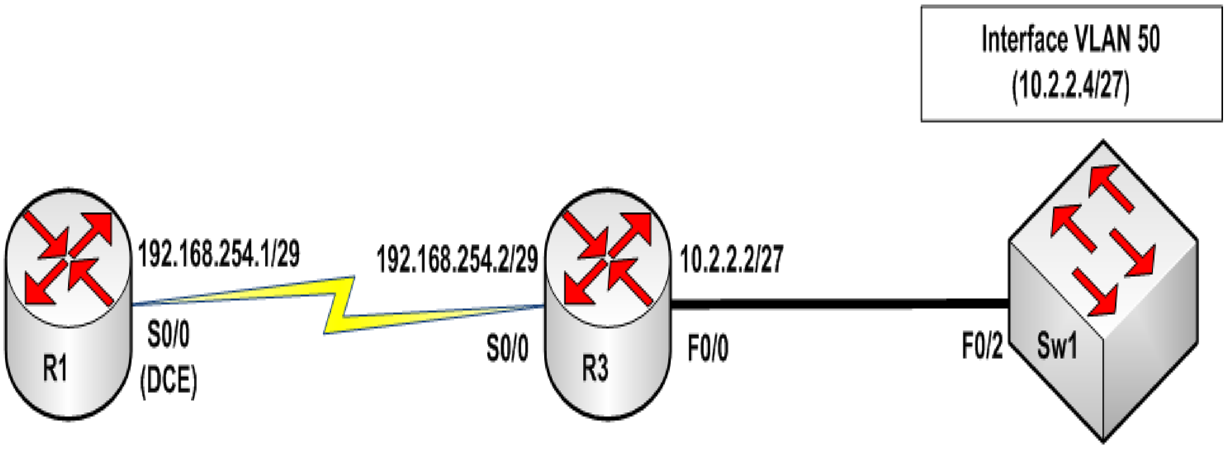
This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1, R2 and Sw1 as illustrated in the topology.

Task 2:

Configure R1 S0/0 which is a DCE to provide a clock rate of 256Kbps to R2. Configure the IP addresses on the Serial interfaces of R1 and R2 as illustrated in the topology.

Task 3:

Configure VLAN 50 named NAT_VLAN on Sw1. Assign the FastEthernet0/2 interface on Sw1 to this VLAN. Also, configure R1 to allow Telnet access using a password of CISCO.

Task 4:

Configure interface VLAN 50 on Sw1 and assign it the IP address illustrated in the topology. The default gateway on Sw1 should be 10.2.2.2. Next, configure interface FastEthernet0/0 in R2 and assign it the IP address illustrated in the topology.

Task 5:

Test connectivity by pinging from R1 to R2 and pinging from R2 to Sw1. These should all be successful. However, since R1 does not know about the 10.2.2.0/27 subnet, Sw1 will not be able to ping R1 or vice versa.

Task 6:

Create an ACL to permit all IP traffic from the 10.2.2.0/27 subnet to the 192.168.254.0/29 subnet. You can create either a named or numbered ACL to complete this task.

Task 7:

Configure R2 F0/0 as the inside interface for NAT and S0/0 as the outside interface for NAT. Next, configure a pool called PAT-POOL to be used for PAT translation. This pool should have both a single starting and ending IP address of 192.168.254.4. Use the same subnet mask as that of S0/0 for this pool.

Task 8:

Configure PAT on R2 to translate traffic specified in the ACL configured in Task 6 to the pool named PAT-POOL. Telnet from Sw1 to R1. If you have configured PAT correctly, this should work. The same applies for ping from Sw1 or the Fa0/0 interface of R2 to R1.

Task 9:

Check the NAT translation table on R2 using the **show ip nat translations** command.

SOLUTION:

Lab 68 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring DCE clocking, please refer to:

Lab 57 Configuration and Verification Task 2

Lab 58 Configuration and Verification Task 2

For reference information on configuring IP interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

Task 3:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 4:

For reference information on configuring IP interfaces, please refer to:

Lab 3 Configuration and Verification Task 5

Lab 31 Configuration and Verification Task 3

Task 5:

```
R1#ping 192.168.254.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.254.2, timeout is 2 seconds:

!!!!!

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

R2#ping 192.168.254.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:

!!!!!

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

R2#ping 10.2.2.4

Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.2.2.4, timeout is 2 seconds:

..!!!

Success rate is 60 percent (3/5), round-trip min/avg/max = 1/3/4 ms

Sw1#ping 10.2.2.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

Sw1#ping 192.168.254.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:

.....

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

Task 6:

```
R2#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#ip access-list extended NAT-ACL

R2(config-ext-nacl)#remark 'NAT Traffic from 10.2.2.0/27 To 192.168.254.0/29'

R2(config-ext-nacl)#permit ip 10.2.2.0 0.0.0.31 192.168.254.0 0.0.0.7

R2(config-ext-nacl)#^Z

R2#
```

Task 7:

```
R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#int fa0/0

R2(config-if)#ip nat inside

R2(config-if)#exit
```

```
R2(config)#int s0/0

R2(config-if)#ip nat outside

R2(config-if)#exit

R2(config)#ip nat pool PAT-POOL 192.168.254.4 192.168.254.4 netmask
255.255.255.240

R2(config)#end

R2#
```

Task 8:

```
R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#ip nat inside source list NAT-ACL pool PAT-POOL overload

R2(config)#end

R2#
```

NOTE: Again, do not forget to issue the overload keyword when configuring NAT overload or PAT.

```
Sw1#ping 192.168.254.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/12 ms

Sw1#telnet 192.168.254.1

Trying 192.168.254.1 ... Open

User Access Verification

Password:

R1#
```

Task 9:

```
R2#show ip nat translations

Pro Inside global      Inside local       Outside local      Outside global
```

```
icmp 192.168.254.2:4813 10.2.2.4:4813     192.168.254.1:4813 192.168.254.1:4813
icmp 192.168.254.2:4814 10.2.2.4:4814     192.168.254.1:4814 192.168.254.1:4814
icmp 192.168.254.2:4815 10.2.2.4:4815     192.168.254.1:4815 192.168.254.1:4815
icmp 192.168.254.2:4816 10.2.2.4:4816     192.168.254.1:4816 192.168.254.1:4816
icmp 192.168.254.2:4817 10.2.2.4:4817     192.168.254.1:4817 192.168.254.1:4817
tcp 192.168.254.2:12801 10.2.2.4:12801    192.168.254.1:23   192.168.254.1:23
R2#
R2#show ip nat statistics
Total active translations: 6 (0 static, 6 dynamic; 6 extended)
Outside interfaces:
  Serial0/0
Inside interfaces:
  FastEthernet0/0
Hits: 250  Misses: 40
Expired translations: 32
Dynamic mappings:
-- Inside Source
[Id: 3] access-list 140 interface Serial0/0 refcount 6
[Id: 4] access-list NAT-ACL pool PAT-POOL refcount 0
 pool PAT-POOL: netmask 255.255.255.248
        start 192.168.254.4 end 192.168.254.4
        type generic, total addresses 1, allocated 0 (0%), misses 0
```

Lab 69: Configuring IOS DHCP Clients

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to Cisco IOS DHCP Clients.

Lab Purpose:

Configuring the Cisco IOS DHCP client feature is a fundamental skill. DHCP provides dynamic addressing information to hosts on a network. Typically, physical DHCP servers (such as Microsoft Windows servers) are used to provide addressing information to DHCP clients (which are devices that request configuration via DHCP). In most cases, DHCP clients are typically computers and other such devices, however, it is also possible to configure Cisco IOS devices to act as DHCP clients and automatically receive configuration information from a DHCP server. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure the Cisco IOS DHCP client feature.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

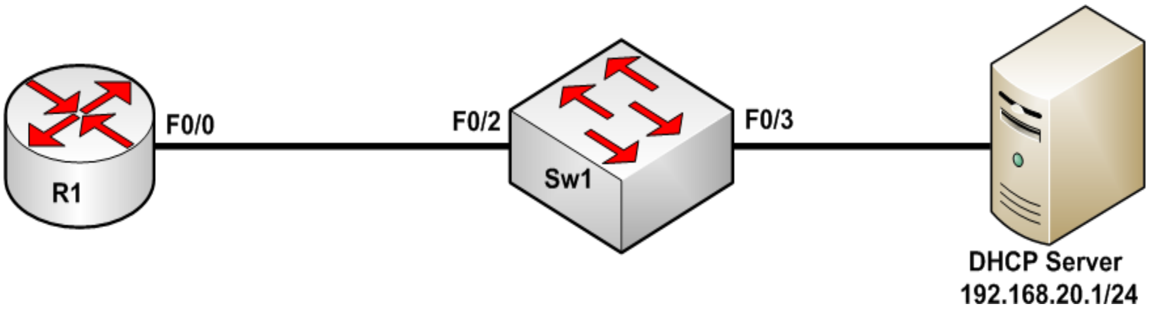
When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

In order to test DHCP functionality, you will need a DHCP server configured and ready to provide IP addressing information. However, this may not be possible, so the purpose of this lab exercise is to be able to configure the IOS DHCP client feature. The solutions guide will provide information on what you would look for if this was a real network with a functioning DHCP server.

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and Sw1 as illustrated in the topology.

Task 2:

Configure VLAN 100 on Sw1 and name it DHCP_VLAN. Assign port Fa0/2 and Fa0/3 to this VLAN. To prevent DHCP request timeouts, enable the ports to automatically transition to the Spanning Tree Forwarding state.

Task 3:

Assuming the DHCP server is correctly configured, configure R1 F0/0 to receive IP addressing via DHCP. Verify that R1 has received automatic configuration information via DHCP

SOLUTION:

Lab 69 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

```
Sw1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#vlan 100

Sw1(config-vlan)#name DHCP_VLAN

Sw1(config-vlan)#exit

Sw1(config)#interface range fastethernet0/2 -- 3

Sw1(config-if-range)#switchport mode access

Sw1(config-if-range switchport access vlan 100

Sw1(config-if-range)#spanning-tree portfast

%Warning: portfast should only be enabled on ports connected to a single

 host. Connecting hubs, concentrators, switches, bridges, etc... to this

 interface  when portfast is enabled, can cause temporary bridging loops.

 Use with CAUTION

%Portfast will be configured in 2 interfaces due to the range command
```

but will only have effect when the interfaces are in a non-trunking mode.

```
Sw1(config-if-range)#no shutdown

Sw1(config-if-range)#end

Sw1#
```

Task 3:

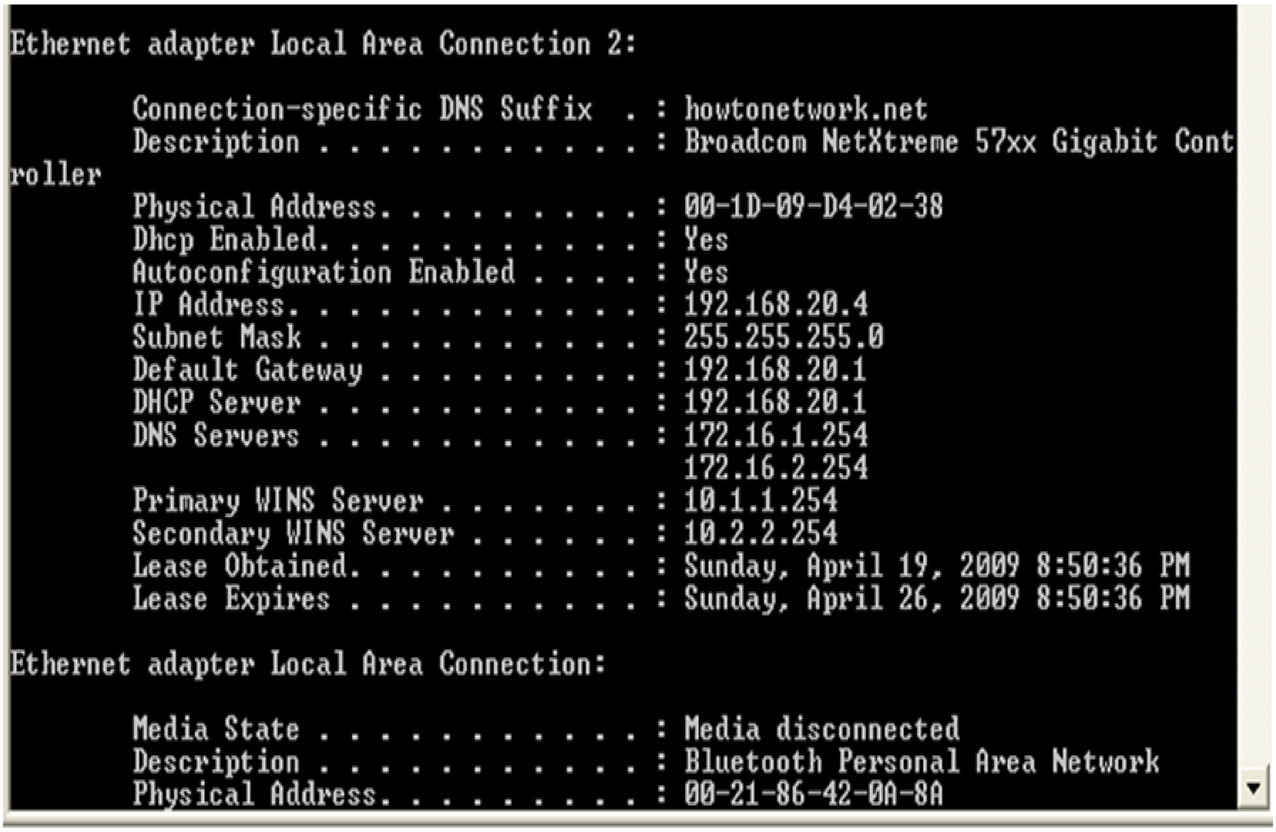
```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int fa0/0

R1(config-if)#ip address dhcp

R1(config-if)#no shutdown

R1(config-if)#end

*Mar  1 02:25:29.029: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up

*Mar  1 02:25:30.030: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

*Mar  1 02:25:33.164: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned
DHCP address 192.168.20.3, mask 255.255.255.0, hostname R1

R1#
```

NOTE: When you see the log message %DHCP-6-ADDRESS_ASSIGN: you know that your device has been assigned an IP address via DHCP. Verify that the interface specified is the one you configured for DHCP.

```
R1#show ip interface fastethernet 0/0

FastEthernet0/0 is up, line protocol is up

  Internet address is 192.168.20.3/24

  Broadcast address is 255.255.255.255

  Address determined by DHCP

R1#show dhcp server

   DHCP server: ANY (255.255.255.255)

    Leases:   2

    Offers:   2      Requests: 2     Acks: 2     Naks: 0
```

```
Declines: 0      Releases: 3     Bad:  0

DNS0:   172.16.1.254,   DNS1:  172.16.2.254

NBNS0:  10.1.1.254,   NBNS1: 10.2.2.254

Subnet: 255.255.255.0   DNS Domain: howtonetwork.net
```

NOTE: From the above output, we can see that the DHCP server provided us with two DNS servers as specified by the line: DNS0:   172.16.1.254,   DNS1: 172.16.2.254 as well as two WINS servers, as specified by the line NBNS0: 10.1.1.254,   NBNS1: 10.2.2.254. The Subnet mask is /24 and the DNS domain provided is howtonetwork.net. If a workstation, such as a Windows-based computer were provided IP addressing information from the same DHCP server and we issued ipconfig /all at the command prompt, we would see:



```
Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : howtonetwork.net
        Description . . . . . . . . . . . : Broadcom NetXtreme 57xx Gigabit Cont
roller
        Physical Address. . . . . . . . . : 00-1D-09-D4-02-38
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.20.4
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.20.1
        DHCP Server . . . . . . . . . . . : 192.168.20.1
        DNS Servers . . . . . . . . . . . : 172.16.1.254
                                            172.16.2.254
        Primary WINS Server . . . . . . . : 10.1.1.254
        Secondary WINS Server . . . . . . : 10.2.2.254
        Lease Obtained. . . . . . . . . . : Sunday, April 19, 2009 8:50:36 PM
        Lease Expires . . . . . . . . . . : Sunday, April 26, 2009 8:50:36 PM

Ethernet adapter Local Area Connection:

        Media State . . . . . . . . . . . : Media disconnected
        Description . . . . . . . . . . . : Bluetooth Personal Area Network
        Physical Address. . . . . . . . . : 00-21-86-42-0A-8A
```

Lab 70: Configuring IOS DHCP Server

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure the Cisco IOS DHCP Server.

Lab Purpose:

Configuring the Cisco IOS DHCP server is a fundamental skill. DHCP provides dynamic addressing information to hosts on a network. Typically, physical DHCP servers (such as Microsoft Windows servers) are used to provide addressing information to DHCP clients (which are devices that request configuration via DHCP). However, Cisco IOS routers can also be configured to act as DHCP servers and provide dynamic addressing to DHCP clients. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure the Cisco IOS DHCP server.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 7/10

Readiness Assessment:

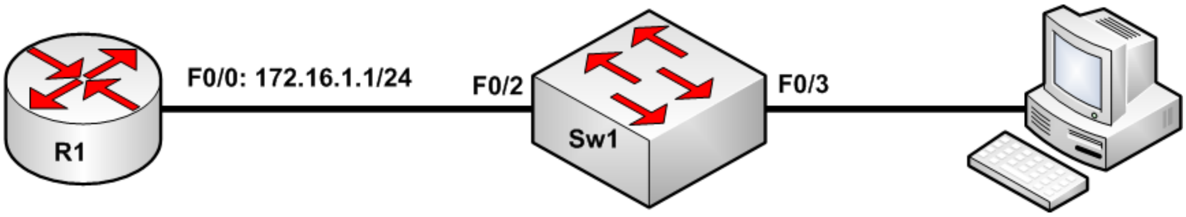
When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

In order to test DHCP functionality, you will need a workstation DHCP client configured to receive IP addressing information via DHCP. If you do not have a DHCP client, feel free to substitute it with another Cisco IOS router configured as a DHCP client as illustrated in the previous lab.

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1 and Sw1 as illustrated in the topology.

Task 2:

Configure VLAN 50 named DHCP_VLAN on Sw1. Assign the FastEthernet0/2 and FastEthernet0/3 interfaces on Sw1 to this VLAN. Ensure that the ports immediately transition to the Spanning Tree Forwarding state.

Task 3:

Configure R1 as a Cisco IOS DHCP server with the following settings:

DHCP Pool Name: CCNA-DHCP-POOL

DHCP Network: 172.16.1.0/24

DNS Server: 10.1.1.254

WINS Server: 10.2.2.254

Default Gateway: 172.16.1.1

DNS Domain: howtonetwork.net

DHCP Lease Time: 5 days 30 minutes

Task 4:

Verify your DHCP configuration on the connected workstation (or other DHCP client) and also verify that your Cisco IOS DHCP server is showing a leased DHCP address.

SOLUTION:

Lab 70 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

```
Sw1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#vlan 50

Sw1(config-vlan)#name DHCP_VLAN

Sw1(config-vlan)#exit
```

```
Sw1(config)#interface range fastethernet0/2 -- 3
Sw1(config-if-range)#switchport mode access
Sw1(config-if-range switchport access vlan 50
Sw1(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast will be configured in 2 interfaces due to the range command
 but will only have effect when the interfaces are in a non-trunking mode.
Sw1(config-if-range)#no shutdown
Sw1(config-if-range)#end
Sw1#
```

Task 3:

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip dhcp pool CCNA-DHCP-POOL
R1(dhcp-config)#network 172.16.1.0 255.255.255.0
R1(dhcp-config)#dns-server 10.1.1.254
R1(dhcp-config)#netbios-name-server 10.2.2.254
R1(dhcp-config)#default-router 172.16.1.1
R1(dhcp-config)#domain-name howtonetwork.net
R1(dhcp-config)#lease 5 0 30
R1(dhcp-config)#end
R1#show ip dhcp pool CCNA-DHCP-POOL
Pool CCNA-DHCP-POOL :
Utilization mark (high/low)  : 100 / 0
Subnet size (first/next)     : 0 / 0
```

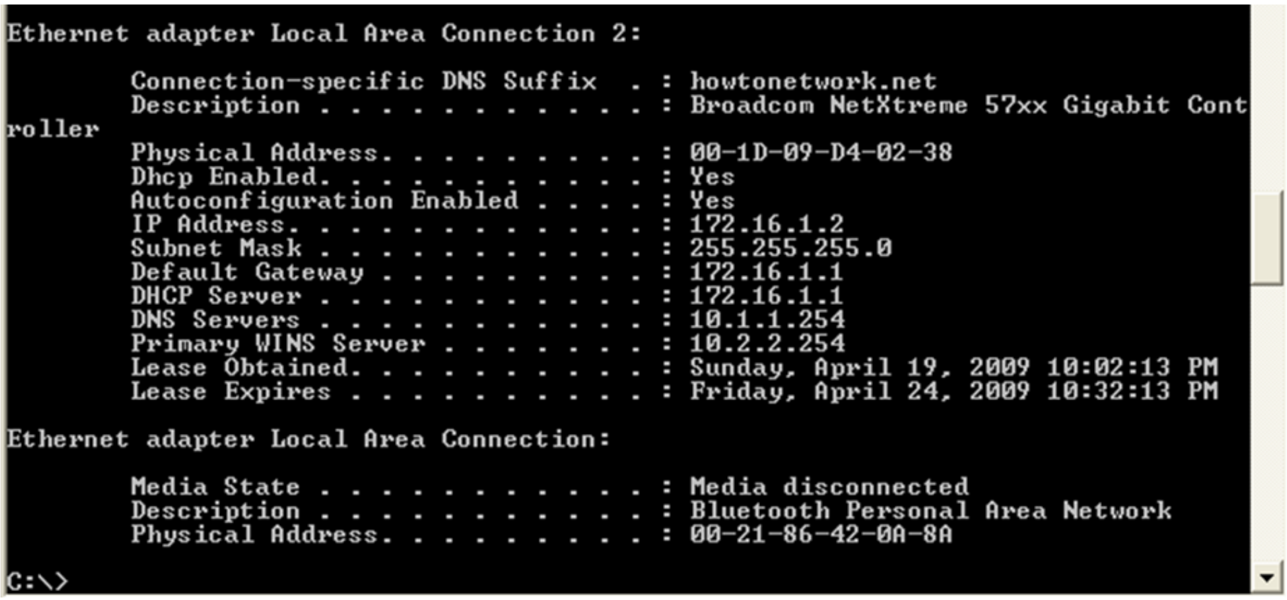
```
Total addresses              : 254
Leased addresses             : 0
Pending event                : none

 1 subnet is currently in the pool :

 Current index      IP address range              Leased addresses

 172.16.1.1         172.16.1.1     - 172.16.1.254     0
```

Task 4:

R1#**show ip dhcp binding**

```
Bindings from all pools not associated with VRF:

IP address        Client-ID/            Lease expiration       Type

                Hardware address/

                User name

172.16.1.2        0100.1d09.d402.38       Mar 06 1993 04:12 AM    Automatic
```

The ipconfig /all on a Windows-based workstation would show the following:



```
Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : howtonetwork.net
        Description . . . . . . . . . . . : Broadcom NetXtreme 57xx Gigabit Cont
roller
        Physical Address. . . . . . . . . : 00-1D-09-D4-02-38
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 172.16.1.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.16.1.1
        DHCP Server . . . . . . . . . . . : 172.16.1.1
        DNS Servers . . . . . . . . . . . : 10.1.1.254
        Primary WINS Server . . . . . . . : 10.2.2.254
        Lease Obtained. . . . . . . . . . : Sunday, April 19, 2009 10:02:13 PM
        Lease Expires . . . . . . . . . . : Friday, April 24, 2009 10:32:13 PM

Ethernet adapter Local Area Connection:

        Media State . . . . . . . . . . . : Media disconnected
        Description . . . . . . . . . . . : Bluetooth Personal Area Network
        Physical Address. . . . . . . . . : 00-21-86-42-0A-8A

C:\>
```

NOTE: If you have configured another Cisco IOS device as a DHCP client to test your configuration, you should see the following output:

R1#**show dhcp server**

```
   DHCP server: ANY (255.255.255.255)
    Leases:   2
    Offers:   2      Requests: 2     Acks: 2     Naks: 0
    Declines: 0      Releases: 3     Bad:  0
    DNS0:   172.16.1.254,   DNS1:  172.16.2.254
    NBNS0:  10.1.1.254,   NBNS1: 10.2.2.254
```

Subnet: 255.255.255.0 DNS Domain: howtonetwork.net

Lab 71: Forwarding DHCP requests to remote DHCP Servers

Lab Objective:

The objective of this lab exercise is for you to learn and understand how Cisco IOS routers forward DHCP requests to remote DHCP servers.

Lab Purpose:

Configuring Cisco IOS routers to forward DHCP requests to remote DHCP servers is a fundamental skill. In some cases, DHCP servers are located in a central location (such as the Headquarters) and DHCP requests from local clients need to be forwarded on to these servers. By default, Cisco IOS routers do not forward Broadcast traffic. Therefore, since DHCP requests are broadcast packets, configuration is required on the Cisco IOS devices to forward these Broadcasts to the DHCP servers. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure Cisco IOS routers to forward DHCP requests to remote DHCP servers.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 7/10

Readiness Assessment:

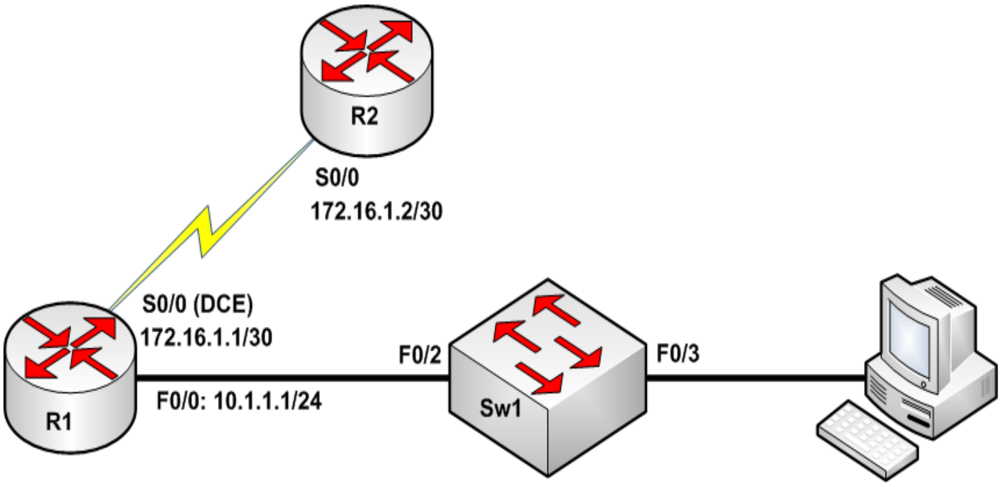
When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

In order to test DHCP functionality, you will need a workstation DHCP client configured to receive IP addressing information via DHCP. If you do not have a DHCP client, feel free to substitute it with another Cisco IOS router configured as a DHCP client as illustrated in the previous lab.

Lab Topology:

Please use the following topology to complete this lab exercise:



Task 1:

Configure the hostnames on routers R1, R2 and Sw1 as illustrated in the topology.

Task 2:

Configure R1 to provide clocking information for R2 at a speed of 256Kbps. Configure the IP addresses on R1 and R2 S0/0 interface as illustrated in the topology.

Task 3:

Configure VLAN 3000 named DHCP_VLAN on Sw1. Assign the FastEthernet0/2 and FastEthernet0/3 interfaces on Sw1 to this VLAN. Ensure that the ports immediately transition to the Spanning Tree Forwarding state.

Task 4:

Configure R2 as a Cisco IOS DHCP server with the following settings:

DHCP Pool Name: REMOTE-DHCP-POOL

DHCP Network: 10.1.1.0/24

DNS Server: 192.168.1.254

WINS Server: 172.30.1.254

Default Gateway: 10.1.1.1

DNS Domain: howtonetwork.net

DHCP Lease Time: 8 days

Task 5:

Configure R1 to forward DHCP requests from DHCP clients connected to F0/0 to R2 (the IOS DHCP server).

Task 6:

Verify your DHCP configuration on the connected workstation (or other DHCP client) and also verify that your Cisco IOS DHCP server is showing a leased DHCP address.

SOLUTION:

Lab 71 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring DCE clocking, please refer to:

Lab 21 Configuration and Verification Task 2

Lab 35 Configuration and Verification Task 2

Task 3:

```
Sw1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#vtp mode transparent

Setting device to VTP TRANSPARENT mode.

Sw1(config)#vlan 3000

Sw1(config-vlan)#name DHCP_VLAN

Sw1(config-vlan)#exit

Sw1(config)#interface range fastethernet0/2 -- 3

Sw1(config-if-range)#switchport mode access

Sw1(config-if-range switchport access vlan 3000

Sw1(config-if-range)#spanning-tree portfast

%Warning: portfast should only be enabled on ports connected to a single
```

```
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast will be configured in 2 interfaces due to the range command
 but will only have effect when the interfaces are in a non-trunking mode.
Sw1(config-if-range)#no shutdown
Sw1(config-if-range)#end
Sw1#
```

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 4:

```
R2#config term
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip dhcp pool REMOTE-DHCP-POOL
R2(dhcp-config)#network 10.1.1.0 /24
R2(dhcp-config)#dns-server 192.168.1.254
R2(dhcp-config)#netbios-name-server 172.30.1.254
R2(dhcp-config)#default-router 10.1.1.1
R2(dhcp-config)#lease 8
R2(dhcp-config)#end
R2#
```

Task 5:

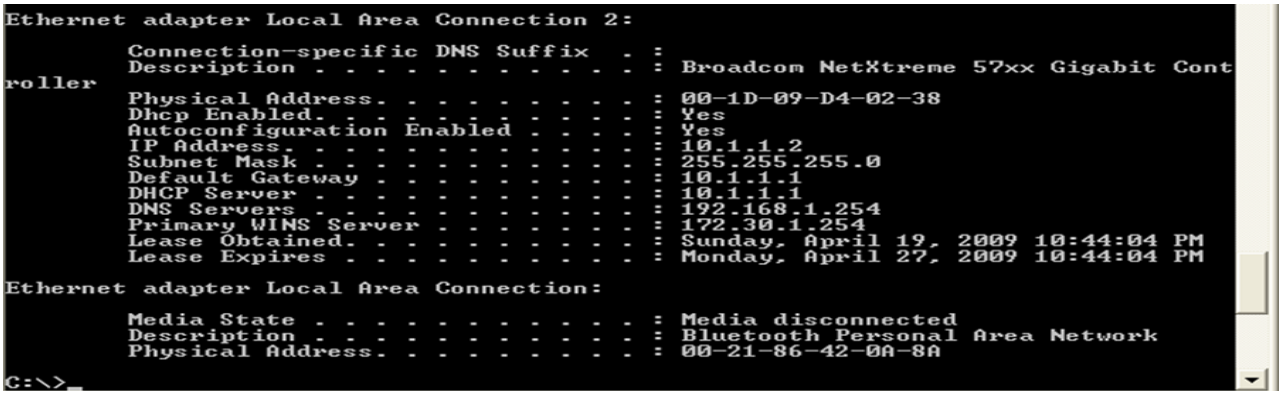
```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int fastethernet0/0
R1(config-if)#ip helper-address 172.16.1.2
```

```
R1(config-if)#end

R1#
```

NOTE: The ip helper-address command is used to point an interface connected to a subnet with DHCP clients to a remote DHCP server. You can specify more tha one DHCP server with this command; however, the first configured on will always be tried first.

Task 6:

```
R1#show ip dhcp pool REMOTE-DHCP-POOL
Pool REMOTE-DHCP-POOL              :
Utilization mark (high/low)        : 100 / 0
Subnet size (first/next)           : 0 / 0
Total addresses                    : 254
Leased addresses                   : 1
Pending event                      : none

 1 subnet is currently in the pool :

 Current index       IP address range                  Leased addresses

 10.1.1.3           10.1.1.1        - 10.1.1.254        1

R1#show ip dhcp binding

Bindings from all pools not associated with VRF:

IP address         Client-ID/            Lease expiration         Type

                Hardware address/

                User name

10.1.1.2          0100.1d09.d402.38       Mar 09 1993 04:27 AM     Automatic
```



```
Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Broadcom NetXtreme 57xx Gigabit Cont
roller
        Physical Address. . . . . . . . . : 00-1D-09-D4-02-38
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.1.1.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.1.1.1
        DHCP Server . . . . . . . . . . . : 10.1.1.1
        DNS Servers . . . . . . . . . . . : 192.168.1.254
        Primary WINS Server . . . . . . . : 172.30.1.254
        Lease Obtained. . . . . . . . . . : Sunday, April 19, 2009 10:44:04 PM
        Lease Expires . . . . . . . . . . : Monday, April 27, 2009 10:44:04 PM

Ethernet adapter Local Area Connection:

        Media State . . . . . . . . . . . : Media disconnected
        Description . . . . . . . . . . . : Bluetooth Personal Area Network
        Physical Address. . . . . . . . . : 00-21-86-42-0A-8A

C:\>_
```

NOTE: If you decided to use another Cisco IOS device as a DHCP client, you can check your DHCP configuration by issuing the show dhcp server command as illustrated in the following output:

```
R4#show dhcp server
   DHCP server: ANY (255.255.255.255)
   Leases:   3
   Offers:   3      Requests: 3     Acks: 3     Naks: 0
   Declines: 0      Releases: 6     Bad:  0
   DNS0:   192.168.1.254,   DNS1:  0.0.0.0
   NBNS0:  172.30.1.254,   NBNS1: 0.0.0.0
   Subnet: 255.255.255.0   DNS Domain: howtonetwork.net
```

Lab 72: Configuring command aliases in IOS devices

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure and use aliases within the Cisco IOS.

Lab Purpose:

Configuring and using aliases is a fundamental skill. Aliases are customized names assigned to Cisco IOS commands that can be used in place of long commands. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure and use aliases on Cisco IOS devices.

Certification Level:

This lab is suitable for CCENT & CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 3/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use any single router or switch to complete this lab.

Task 1:

Configure the hostname on your router or switch.

Task 2:

Configure the following aliases on your device:

ALIAS	**REAL Cisco IOS COMMAND**
int	show ip interfaces brief
save	copy running-config startup-config
proc	show processes cpu

Task 3:

Verify your configured aliases. Now, test your aliases and validate that they operate as expected.

SOLUTION:

Lab 72 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#alias exec int show ip interface brief

R1(config)#alias exec save copy running-config startup-config

R1(config)#alias exec proc show processes cpu

R1(config)#end

R1#
```

Task 3:

```
R1#show aliases

Exec mode aliases:

  h                    help

  lo                   logout

  p                    ping

  r                    resume

  s                    show

  u                    undebug

  un                   undebug

  w                    where

  int                  show ip interface brief
  save              copy running-config startup-config

  proc              show processes cpu

R1#int

Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        unassigned      YES manual administratively down down

Serial0/0              unassigned      YES NVRAM  administratively down down

Serial0/1              unassigned      YES manual administratively down down

R1#save

Destination filename [startup-config]?

Building configuration...

[OK]

R1#proc

CPU utilization for five seconds: 0%/0%; one minute: 4%; five minutes: 1%

 PID Runtime(ms)   Invoked      uSecs    5Sec   1Min   5Min TTY Process

   1           0         2          0  0.00%  0.00%  0.00%   0 Chunk Manager

   2           0       110          0  0.00%  0.00%  0.00%   0 Load Meter

 [output truncated for brevity]
```

Lab 73: Configuring Local Name Resolution on Cisco IOS devices

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure name resolution on Cisco IOS devices.

Lab Purpose:

Configuring name resolution on Cisco IOS devices is a fundamental skill. Name resolution can be used to provide hostname to Layer 3 address mapping instead of DNS service. It is typically used in small networks with a few internetwork devices. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure name resolution on Cisco IOS devices.

Certification Level:

This lab is suitable for CCNA certification exam preparation

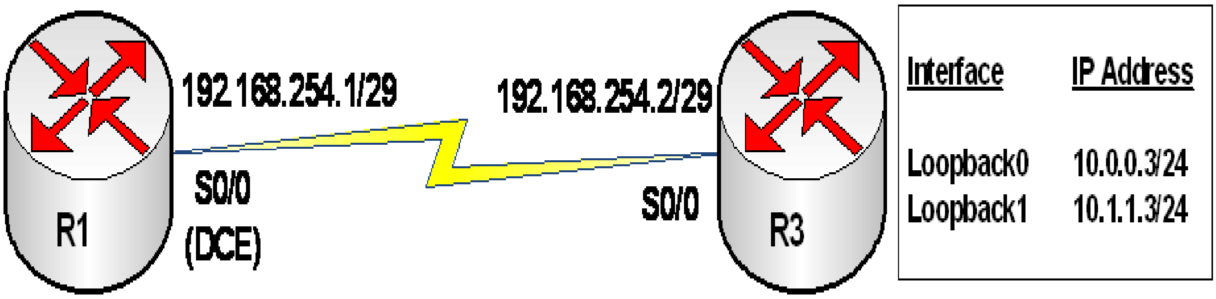
Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:



Interface	IP Address
Loopback0	10.0.0.3/24
Loopback1	10.1.1.3/24

Please use the following topology to complete this lab:

Task 1:

Configure the hostnames on your router or switch.

Task 2:

Configure R1 to provide clocking to R3 at rate of 256Kbps. Next, configure the IP addresses on R1 and R3 as illustrated in the network topology.

Task 3:

Configure R1 with a static default route pointing to R3. Next, configure the two Loopback interfaces on R2 as illustrated in the network topology.

Task 4:

Configure local host name resolution on R1 for R3 Loopback0 and Loopback1. Use the IP addresses of the Loopback interfaces and the hostnames R3-LOOP0 and R3-LOOP1, respectively on R1.

Task 5:

Test your configuration by pinging R3-LOOP0 and R3-LOOP1. These hostnames should be resolved to the IP addresses of the Loopback0 and Loopback1 interfaces on R3, respectively.

SOLUTION:

Lab 73 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring DCE clocking, please refer to:

Lab 20 Configuration and Verification Task 3

Lab 21 Configuration and Verification Task 3

Lab 21 Configuration and Verification Task 2

Lab 35 Configuration and Verification Task 2

Task 3:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0 192.168.254.3

R1(config)#end

R1#

R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int lo 0

R3(config-if)#ip add 10.0.0.3 255.255.255.0

R3(config-if)#exit

R3(config)#int lo 1

R3(config-if)#ip add 10.1.1.3 255.255.255.0

R3(config-if)#exit

R3(config)#end

R3#
```

Task 4:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#ip host R3-LOOP0 10.0.0.3

R1(config)#ip host R3-LOOP1 10.1.1.3

R1(config)#end

R1#

R1#show host

Default domain is not set

Name/address lookup uses domain service

Name servers are 255.255.255.255

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate

       temp - temporary, perm - permanent

       NA - Not Applicable None - Not defined

Host                    Port  Flags      Age Type   Address(es)

R3-LOOP0                    None  (perm, OK)  0   IP    10.0.0.3

R3-LOOP1                    None  (perm, OK)  0   IP    10.1.1.3
```

Task 5:

```
R1#ping R3-LOOP0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/16 ms

R1#ping R3-LOOP1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.3, timeout is 2 seconds:

!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/12 ms
```

Lab 74: Configuring Domain Name Resolution on Cisco IOS devices

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure DNS on Cisco IOS devices.

Lab Purpose:

Configuring DNS on Cisco IOS devices is a fundamental skill. DNS provides hostname to Layer 3 address resolution. DNS servers are typically used in large networks with a lot of hosts and internetworking devices. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure DNS on Cisco IOS devices.

Certification Level:

This lab is suitable for CCENT & CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 3/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 5 minutes

IMPORTANT NOTE:

The objective of this lab is to simply familiarize you with the steps required to configure a Cisco IOS device to communicate with a DNS server. Because there will be no real DNS server configured against which to perform testing, the sole objective of this lab is command familiarity.

Lab Topology:

Please use any single router or switch to complete this lab.

Task 1:

Configure a hostname your router or switch.

Task 2:

Configure your router of switch as part of the howtonetwork.net domain. For name resolution, your device should forward traffic to DNS servers 172.16.1.254 or 172.17.1.254.

SOLUTION:

Lab 74 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#ip domain-name howtonetwork.net

R1(config)#ip name-server 172.16.1.254 172.17.1.254

R1(config)#ip domain-lookup

R1(config)#end

R1#
```

NOTE: If an actual DNS server was available and was providing name resolution, we could ping or connect to devices based on their hostnames as illustrated below:

```
R1#ping R3

Translating "R3.howtonetwork.net"...domain server (172.16.1.254) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/16 ms

R1#telnet R3
Translating "R3"...domain server (172.16.1.254) [OK]
Trying R3.howtonetwork.net (192.168.254.3)... Open


User Access Verification

Password:
R3#
```

Lab 75: Configuring IOS Device Logging to a SYSLOG server

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure Cisco IOS devices to send log messages to a SYSLOG server.

Lab Purpose:

Configuring Cisco IOS devices to send logging information to a SYSLOG server is a fundamental skill. In most networks, a SYSLOG server is present and devices are configured to send log messages to this central repository. Users or groups managing this central repository can therefore see alarms from devices and act accordingly to address the issues. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure Cisco IOS devices to send log messages to SYSLOG servers.

Certification Level:

This lab is suitable for CCENT & CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

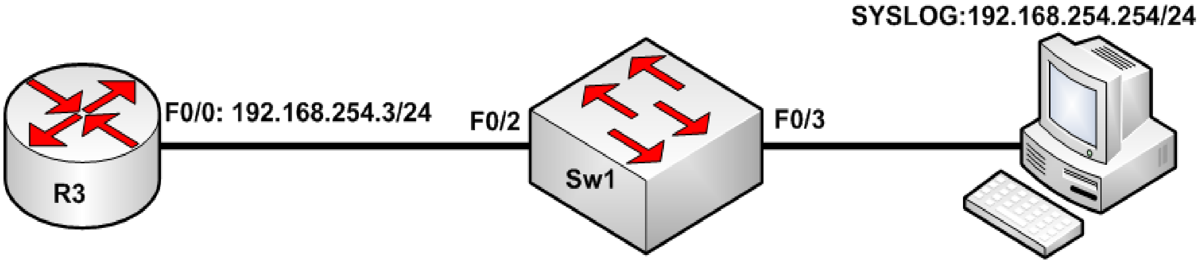
When you are ready for your certification exam, you should complete this lab in no more than 5 minutes

IMPORTANT NOTE:

The objective of this lab is to simply familiarize you with the steps required to configure a Cisco IOS device to send log messages to a SYSLOG server. Because there will be no real SYSLOG server configured against which to perform testing, the sole objective of this lab is command familiarity.

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure the hostnames on R3 and Sw1 as illustrated below.

Task 2:

At this stage, we know that by default, all interfaces on a Cisco Catalyst switch are in VLAN 1. Therefore, simply enable interfaces FastEthernet0/2 and FastEthernet0/3 on Sw1.

Task 3:

Configure R3 to send SYSLOG messages up to Level 7 to the SYSLOG server 192.168.254.254.

Task 4:

Verify your SYSLOG configuration on R3 using the show logging command.

SOLUTION:

Lab 75 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

```
Sw1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#interface fastethernet0/2

Sw1(config-if)#no shutdown

Sw1(config-if)#exit

Sw1(config)#interface fastethernet0/3

Sw1(config-if)#no shutdown

Sw1(config-if)#^Z

Sw1#
```

Task 3:

```
R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#logging trap debugging

R3(config)#logging host 192.168.254.254

R3(config)#end

R3#
```

NOTE: When configuring logging levels, you can use the number or the keyword for the specific level for which you want to enable logging. You can view the correlation between numbers and keywords by using a question mask after the logging trap command as illustrated below:

```
R3(config)#logging trap ?
<0-7>                     Logging severity level
alerts                    Immediate action needed          (severity=1)
critical                  Critical conditions              (severity=2)
debugging                 Debugging messages               (severity=7)
emergencies               System is unusable               (severity=0)
errors                    Error conditions                 (severity=3)
informational Informational messages                       (severity=6)
notifications             Normal but significant conditions (severity=5)
warnings                  Warning conditions               (severity=4)
```

Task 4:

```
R3#show logging

Syslog logging: enabled (0 messages dropped, 1 messages rate-limited, 0 flushes, 0 overruns,
xml disabled)

    Console logging: disabled

    Monitor logging: level debugging, 0 messages logged, xml disabled

    Buffer logging: disabled, xml disabled

    Logging Exception size (4096 bytes)

    Count and timestamp logging messages: disabled

    Trap logging: level debugging, 33 message lines logged

        Logging to 192.168.254.254, 1 message lines logged, xml disabled
```

NOTE: Logging using a level of 7 indicates that the device will send logs for all other levels. If we has a SYSLOG server and performed a configuration task on this router, we would see the log messages on the SYSLOG server.

Lab 76: Configuring User Privileges on Cisco IOS Devices

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure user privileges on devices.

Lab Purpose:

Configuring user privilege levels on Cisco IOS devices is a fundamental skill. Users can be configured with certain privilege levels that allow them to execute certain commands. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure user privilege levels on Cisco IOS devices.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

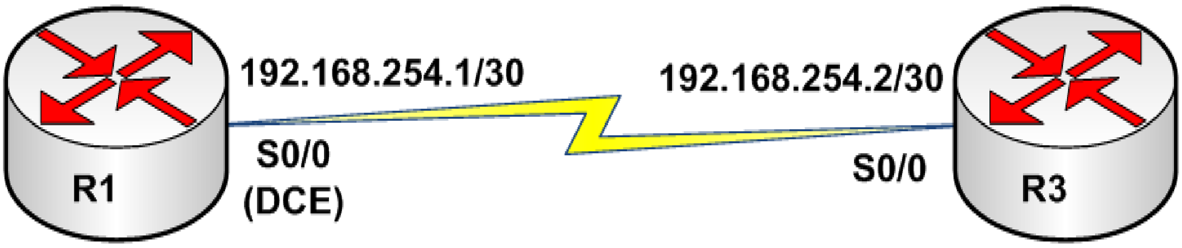
This lab has a difficulty rating of 6/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure the hostnames on R1 and R3 as illustrated in the topology.

Task 2:

Configure R1 to provide clocking to R3 at rate of 2Mbps. Next, configure the IP addresses on R1 and R3 as illustrated in the network topology.

Task 3:

Configure the VTY lines on R3 to allow users to log into the router based on locally configured usernames and passwords. Also, configure the enable secret of SAFE on R3.

Task 4:

Configure R3 with the following user accounts:

Username	Password	Privilege Level
admin	cisco	15
test	cisco	1

Connect via Telnet from R1 to R3. First, log in with the username admin and check your privilege level and the router prompt after login. Next, log in with the username text and check your privilege level and the router prompt after login. Do you notice any differences?

SOLUTION:

Lab 76 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring DCE clocking, please refer to:

Lab 20 Configuration and Verification Task 3

Lab 21 Configuration and Verification Task 3

Lab 21 Configuration and Verification Task 2

Lab 35 Configuration and Verification Task 2

Task 3:

```
R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#line vty 0 4

R3(config-line)#login local

R3(config-line)#end

R3#
```

NOTE: The login local command specifies that the device should use the local database for user authentication. When configured, you must also configure username and password pairs to be used to gain access to the device.

Task 4:

```
R3#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#username admin privilege 15 password cisco

R3(config)# username test privilege 1 password cisco

R3(config)#end

R3#

R1#telnet 192.168.254.3

Trying 192.168.254.3 ... Open

User Access Verification

Username: admin

Password:

R3#

R1#telnet 192.168.254.3

Trying 192.168.254.3 ... Open

User Access Verification

Username: test

Password:

R3>
```

NOTE: Notice how user admin is automatically in Privileged Exec mode after successful login, as illustrated by the # sign; however, we can see that user test (who has a privilege level of 1) is automatically put into User Exec mode after successful login, as illustrated by the > sign.

Lab 77: Configuring Command & Password privilege Levels on devices

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure privilege levels for certain commands and passwords on Cisco IOS devices.

Lab Purpose:

Configuring user privilege levels on Cisco IOS devices is a fundamental skill. Users can be configured with certain privilege levels that allow them to execute certain commands. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure user privilege levels on Cisco IOS devices.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 6/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use any single Cisco IOS router or switch to complete the following lab.

Task 1:

Configure a hostname of your liking on your Cisco IOS router or switch. It may be easier to use a router for this lab.

Task 2:

Configure a level 15 secret of **cisco456** on your device.

Task 3:

Issue the show ip interface brief command from User Exec mode, i.e. where you see the > sign after the device name. Verify that this command works and you do see the current interface status.

Task 4:

Configure the show ip interface brief command to work only for users with Level 15 access.

Task 5:

If you are connected via the console, type in the command disable to return to User Exec mode (i.e. where you see the > sign after the device hostname). Next, issue the **show ip interfaces brief** command. If you have configured your device correctly, this command will no longer work in User Exec mode.

Task 6:

Next, type in enable and type is the Level 15 password of **cisco456**. Attempt to issue the show ip interface brief command. If your configuration is correct, this will work.

SOLUTION:

Lab 77 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#enable secret level 15 cisco456

R1(config)#^Z

R1#
```

Task 3:

```
R1>show ip interface brief

Interface                IP-Address      OK? Method Status                Protocol

Ethernet0/0              unassigned      YES manual administratively down down

Serial0/0                unassigned      YES manual administratively down down

Serial0/1                unassigned      YES manual administratively down down
```

Task 4:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#privilege exec level 15 show ip interface brief
```

```
R1(config)#end

R1#
```

NOTE: The privilege exec command is used to set different privilege levels for commands. By default, the show ip interfaces brief command has a privilege level of 1 which means that it can be issued from the User Exec prompt; i.e. the > prompt after the hostname of the device.

Task 5:

```
R1#disable

R1>show ip interface brief

    ^

% Invalid input detected at '^' marker.
```

Task 6:

```
R1>enable

Password:

R1#show ip interface brief

Interface                  IP-Address      OK? Method Status                Protocol

Ethernet0/0                unassigned      YES manual administratively down down

Serial0/0                  unassigned      YES manual administratively down down

Serial0/1                  unassigned      YES manual administratively down down
```

Lab 78: Configuring MOTD Banners

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure message of the day banners on Cisco IOS devices.

Lab Purpose:

MOTD banner configuration is a fundamental skill. The MOTD banner is displayed to all terminals connected and is useful for sending messages that affect all users. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure an MOTD banner.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 6/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use any Cisco IOS device to complete this lab.

Task 1:

Configure a hostname of your liking on your device.

Task 2:

Configure the device MOTD banner exactly as follows:

##

This is a private system. If you have connected to this device

accidentally, please disconnect immediately!

##

Task 3:

If you are connected to the device via the console port, issue the command quit to reset the console. Now connect back to the device (hit Enter) and you should see the MOTD banner.

SOLUTION:

Lab 78 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#banner motd %

Enter TEXT message.  End with the character '%'.
```

```
##################################################

This is a private system. If you have connected to this device

accidentally, please disconnect immediately!

##################################################

%

R1(config)#end

R1#
```

NOTE: Be careful not to use the delimiting character in your banner configuration. Most people have a tendancy to use the # symbol as a delimiting character, and then forget and use it in their banner configuration, resulting in an incomplete banner on the device. Practice configuring banners with other delimiting characters as well.

Task 3:

```
Press RETURN to get started.

##################################################

This is a private system. If you have connected to this device

accidentally, please disconnect immediately!

##################################################

R1>
```

Lab 79: Enabling HTTP access to Cisco IOS devices

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to enable HTTP access to devices.

Lab Purpose:

HTTP access to Cisco IOS devices is a fundamental skill. Using HTTP, it is possible to view information on a Cisco IOS device as well as perform basic configuration tasks. Keep in mind, however, that this is not SDM configuration, but a legacy means of HTTP access which pre-dates SDM. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure HTTP access to legacy Cisco IOS devices.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 7/10

Readiness Assessment:

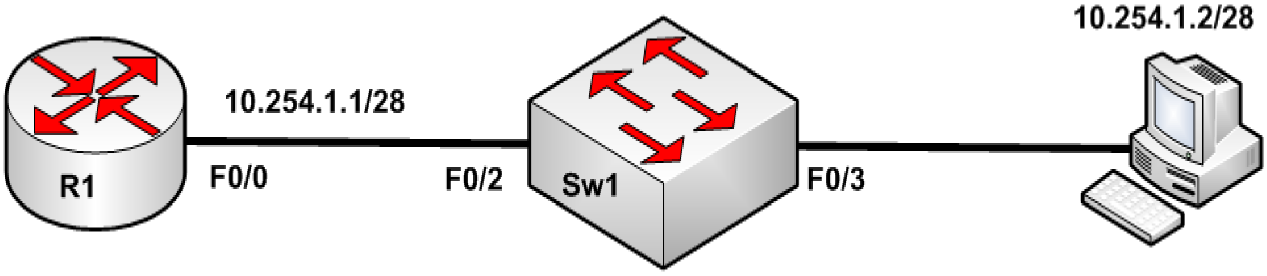
When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

The objective of this lab is to simply familiarize you with the steps required to configure a Cisco IOS device to allow HTTP access. You may not have a PC connected to device to test this configuration; however, the solutions guide will provide relevant screenshots on what you would expect to see when you access a device via HTTP.

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure the hostnames on R1 and Sw1 as illustrated in the topology.

Task 2:

Configure VLAN 20 on Sw1 and assign it the name HTTP_VLAN. Next, configure ports FastEthernet0/2 and FastEthernet0/3 on Sw1 as access ports within this VLAN.

Task 3:

Configure the IP address of your router and PC as illustrated in the topology.

Task 4:

Configure R1 to allow HTTP access. HTTP users should authenticate locally on the router using the username ADMIN and the password CISCO. Ensure that the user has the highest privilege level on Cisco IOS. Using the Web browser on the PC, HTTP to the IP address 10.254.1.1 and verify that you log in successfully.

SOLUTION:

Lab 79 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

For reference information on configuring IP interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

Lab 56 Configuration and Verification Task 2

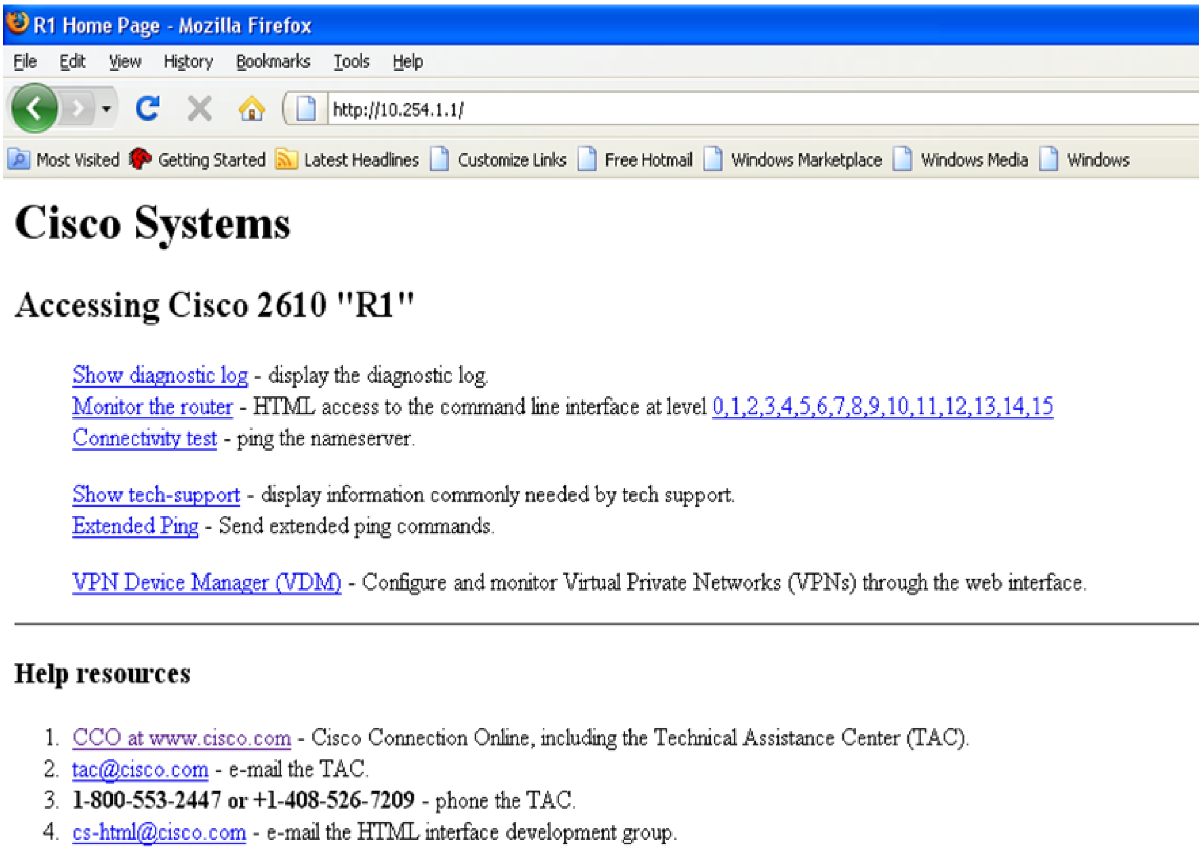
Task 4:

```
Sw1#config te

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#ip http server

Sw1(config)#ip http authentication local

Sw1(config)#username ADMIN privilege 15 password CISCO

Sw1(config)#end

R1#
```

NOTE: Because you will be accessing the device via HTTP, ensure that you set the privilege level of the HTTP administrator to 15. This is a commonly forgotten task. Remember it.

Task 5:

If you had access to the device via a PC in your lab, expect to see something similar to the following when you connect to it via HTTP:


R1 Home Page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://10.254.1.1/
Most Visited Getting Started Latest Headlines Customize Links Free Hotmail Windows Marketplace Windows Media Windows

Cisco Systems

Accessing Cisco 2610 "R1"

Show diagnostic log - display the diagnostic log.
Monitor the router - HTML access to the command line interface at level 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
Connectivity test - ping the nameserver.

Show tech-support - display information commonly needed by tech support.
Extended Ping - Send extended ping commands.

VPN Device Manager (VDM) - Configure and monitor Virtual Private Networks (VPNs) through the web interface.

Help resources

1. CCO at www.cisco.com - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - e-mail the TAC.
3. **1-800-553-2447** or **+1-408-526-7209** - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.

You could then navigate using the browser and perform basic configurations as well as basic diagnostic testing on the device. Keep in mind that this is the HTTP access method for devices that are not supported by SDM.

Lab 80: Changing the Configuration Register on Cisco IOS devices

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to change the configuration register value on Cisco IOS devices.

Lab Purpose:

Changing the configuration register is a fundamental skill. The configuration register is typically changed when performing a password recovery procedure on a Cisco IOS device. The settings within the configuration register are used to change the default behavior of Cisco IOS devices. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to change and verify the configuration register.

Certification Level:

This lab is suitable for CCENT & CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 4/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 5 minutes

Lab Topology:

Please use any single router or switch to complete this lab.

Task 1:

Configure any desired hostname on your device.

Task 2:

Verify the current setting of the configuration register using the show version command. The configuration register will be at the very end of the output from this command.

Task 3:

Change the configuration register value to 102 and save your configuration. Verify that your new configuration register will be used after your device has been rebooted.

SOLUTION:

Lab 80 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

```
R1#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IK9O3S3-M), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 15:23 by dchih
ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
R1 uptime is 2 hours, 12 minutes
System returned to ROM by power-on
System image file is "flash:c2600-ik9o3s3-mz.123-26.bin"
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
```

```
export@cisco.com.
cisco 2610 (MPC860) processor (revision 0x203) with 61440K/4096K bytes of memory.
Processor board ID JAD05090GA8 (596408632)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
```

Task 3:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#config-register 0x102
R1(config)#end
R1#
R1#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IK9O3S3-M), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 15:23 by dchih
ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
R1 uptime is 2 hours, 13 minutes
System returned to ROM by power-on
System image file is "flash:c2600-ik9o3s3-mz.123-26.bin"
```

```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
cisco 2610 (MPC860) processor (revision 0x203) with 61440K/4096K bytes of memory.
Processor board ID JAD05090GA8 (596408632)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102 (will be 0x102 at next reload)
```

NOTE: The Configuration Register is always in Hexadecimal format. Therefore, always remember to issue the 0x before specifying the desired Configurations Register value. This is often forgotten, so ensure you remember it!

Lab 81: Cisco Discovery Protocol

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to enable CDP and adjust CDP timers.

Lab Purpose:

Understanding CDP is a fundamental skill. CDP is a proprietary Cisco protocol that can be used for device discovery as well as internetwork troubleshooting. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to enable and use CDP in internetwork discovery and troubleshooting.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

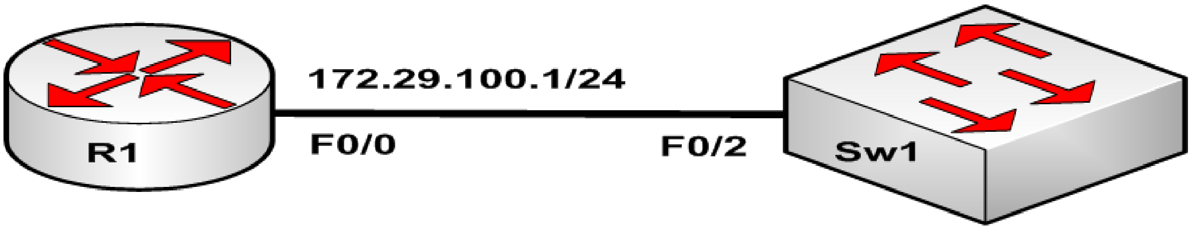
This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure hostnames on R1 and Sw1 as illustrated in the topology.

Task 2:

Configure an IP address of 172.29.100.1/24 on R1 F0/0.

Task 3:

Configure VLAN 200 on Sw1 and name it CDP_VLAN. Configure interface VLAN 200 on Sw1 and assign it the IP address 172.29.100.2/24. Assign port FastEthernet0/2 on Sw1 to this VLAN.

Task 4:

Enable CDP on R1 and Sw1 globally. Configure R1 and Sw1 to send CDP packets every 10 seconds.

Task 5:

Use CDP and see detailed information about Sw1 from R1. Familiarize yourself with the information provided.

SOLUTION:

Lab 81 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int fa0/0

R1(config-if)#ip address 172.29.100.1 255.255.255.0

R1(config-if)#no shut

R1(config-if)#^Z

R1#
```

Task 3:

```
Sw1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#vlan 200

Sw1(config-vlan)#name CDP_VLAN

Sw1(config-vlan)#exit

Sw1(config)#interface vlan 1

Sw1(config-if)#shut

Sw1(config-if)#exit
```

```
Sw1(config)#int vlan 200

Sw1(config-if)#no shut

Sw1(config-if)#ip address 172.29.100.2 255.255.255.0

Sw1(config-if)#exit

Sw1(config)#int f0/2

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 200

Sw1(config-if)#end

Sw1#

Sw1#ping 172.29.100.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.29.100.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/203/1000 ms

Sw1#
```

Task 4:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#cdp run

R1(config)#cdp timer 10

R1(config)#^Z

R1#

R1#show cdp interface fastethernet 0/0

FastEthernet0/0 is up, line protocol is up

  Encapsulation ARPA

  Sending CDP packets every 10 seconds

  Holdtime is 180 seconds
```

```
Sw1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#cdp run

Sw1(config)#cdp timer 10

Sw1(config)#end

Sw1#

Sw1#show cdp interface fastethernet 0/2

FastEthernet0/2 is up, line protocol is up

  Encapsulation ARPA

  Sending CDP packets every 10 seconds

  Holdtime is 180 seconds
```

Task 5:

```
R1#show cdp neighbors detail

-------------------------

Device ID: Sw1

Entry address(es):

  IP address: 172.29.100.2

Platform: cisco WS-C2950G-24-EI,  Capabilities: Switch IGMP

Interface: FastEthernet0/0,  Port ID (outgoing port): FastEthernet0/2

Holdtime : 178 sec

Version :

Cisco Internetwork Operating System Software

IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(13)EA1, RELEASE SOFTWARE (fc1)

Copyright (c) 1986-2003 by cisco Systems, Inc.

Compiled Tue 04-Mar-03 02:14 by yenanh

advertisement version: 2

Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27,
value=00000000FFFFFFFF010221FF000000000000000DBD064100FF0000
```

VTP Management Domain: 'CISCO'

Duplex: full

NOTE: The show cdp neighbors detail command provides detailed information about devices. This is a very useful troubleshooting command as you can find out the IP addresses (and more) of connected devices and access them remotely. Try this command on Sw1 and see the information you find out about R1. Familiarize yourself with the contents of this command for both routers and switches.

Lab 82: Configuring Cisco IOS routers for SDM

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure Cisco IOS routers for SDM.

Lab Purpose:

Understanding Cisco SDM is a fundamental skill. SDM is a web-based application that can be used to configure routers as well as troubleshoot internetworks. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure the router in preparation for SDM.

Certification Level:

This lab is suitable for CCENT & CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

In order to use SDM, you must have an SDM-capable router. The following routers support SDM:

- Cisco Small Business 101, 106, and 107
- Cisco 1701, 1710, 1711, 1712, 1721, 1751, 1751-V, 1760 and 1870V
- Cisco 1801, 1802, 1803, 1811, and 1812
- Cisco 1841
- Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and Cisco 2691

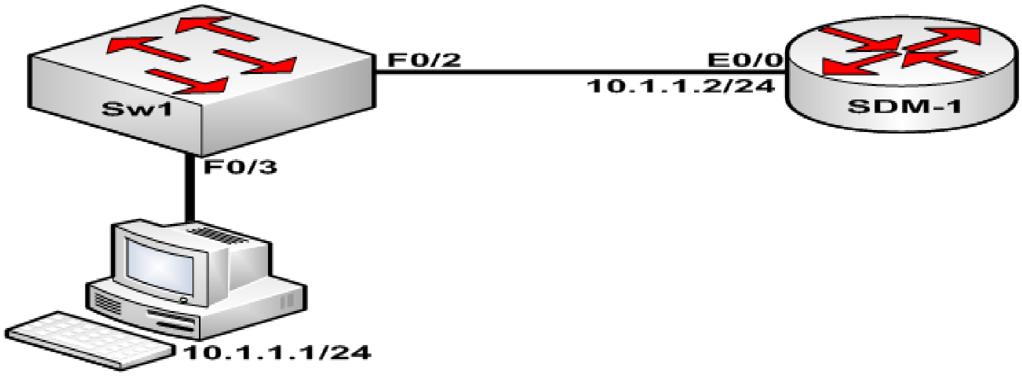
Multiservice Routers

- Cisco 2801, 2811, 2821, and 2851
- Cisco 3620, 3640, 3661, and 3662
- Cisco 3725 and 3745
- Cisco 3825 and 3845
- Cisco 7204VXR, 7206VXR and 7301

The objective of this lab exercise is to familiarize your with the SDM GUI and how to navigate through it. As long as you have one of the platforms listed above, the configuration tasks and GUI navigation will be the same. These lab exercises are based on a Cisco 3640 router with two 10Mbps Ethernet interfaces and two Serial interfaces, but can be completed on any one of the above routers with similar interfaces. Substitute the interfaces in these lab exercises with the ones you have on your router.

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure hostnames on Sw1 as illustrated in the topology.

Task 2:

Configure VLAN 200 on Sw1 and assign it the name SDM_VLAN. Next, configure the E0/0 interface of SDM-1 with the IP address of 10.1.1.2/24. Ensure that the PC has the IP address 10.1.1.1/24 configured on the correct NIC.

Task 3:

Configure SDM-1 to accept HTTP connections in preparation for SDM access to the device. Configure local database authentication for HTTP using the username ADMIN and secret CISCO. Ensure this account has the highest privilege level available on Cisco IOS routers.

Task 4:

Connect to the device via your Web Browser or the SDM application installed on your workstation. Use the login credentials you just configured to log into the device and take a moment to glance at the options available on the SDM device home page.

Task 5:

Using SDM, configure the router name as SDM-1.

SOLUTION:

Lab 82 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

```
Sw1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Sw1(config)#vlan 200

Sw1(config-vlan)#name SDM_VLAN

Sw1(config-vlan)#exit

Sw1(config)#interface vlan 1

Sw1(config-if)#shut

Sw1(config-if)#exit

Sw1(config)#int vlan 200

Sw1(config-if)#no shut

Sw1(config-if)#ip address 10.1.1.254 255.255.255.0

Sw1(config-if)#exit

Sw1(config)#int f0/2

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 200

Sw1(config-if)#exit
```

```
Sw1(config)#int f0/3

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 200

Sw1(config-if)#end

Sw1#
```

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

For reference information on configuring IP interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

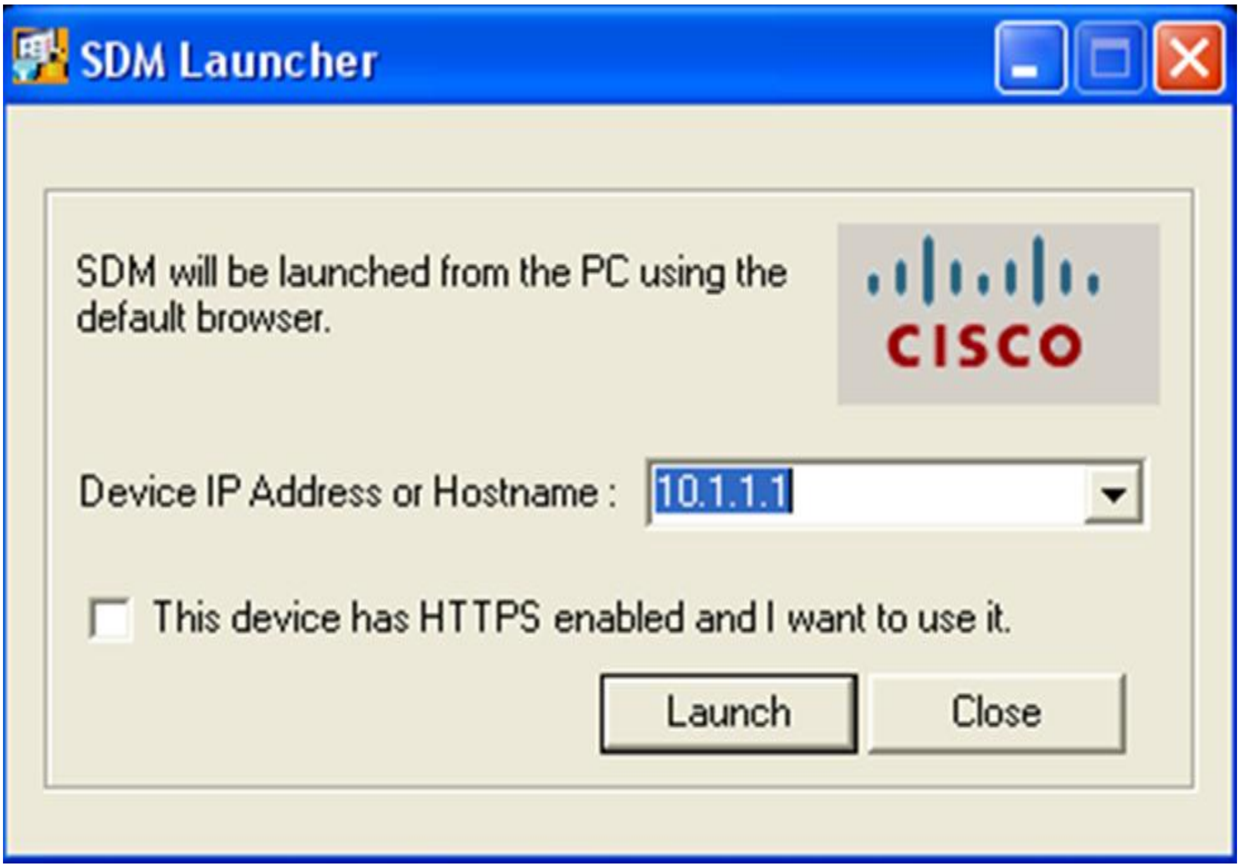
Lab 56 Configuration and Verification Task 2

Task 3

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#ip http server

R1(config)#ip http authentication local

R1(config)#username ADMIN privilege 15 secret CISCO

R1(config)#end

R1#
```

Task 4:

If you are using the SDM application installed on your desktop, open up the appliacation and type in the IP address or device name of the device you wish to connect to and click on the **Launch** button as follows:

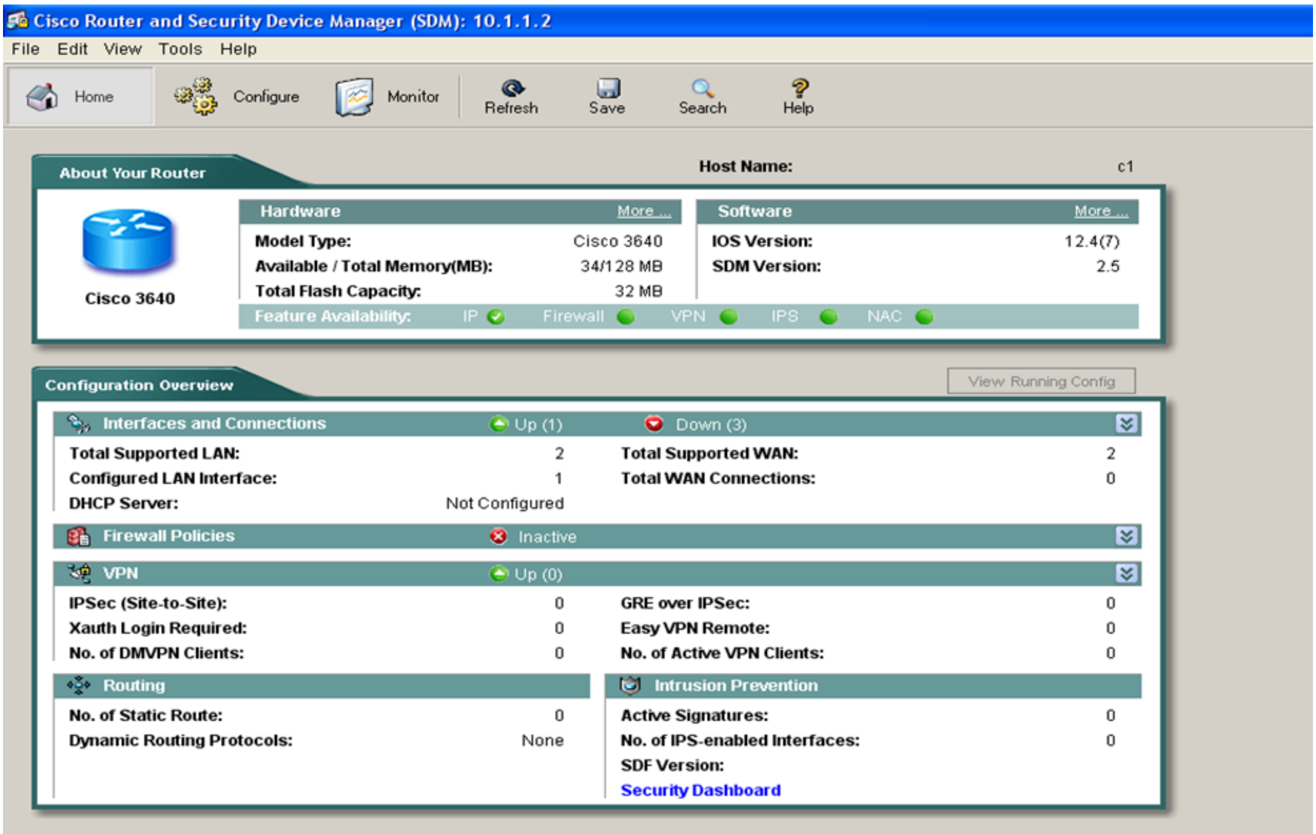


SDM will be launched from the PC using the default browser.

Device IP Address or Hostname : 10.1.1.1

□ This device has HTTPS enabled and I want to use it.

NOTE: The output below will vary depending on the specific router platform you are using, available interfaces, memory, etc; however, the overall look and feel will be just the same.



Cisco Router and Security Device Manager (SDM): 10.1.1.2
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help

About Your Router

Host Name: c1

Cisco 3640

Hardware	More ...
Model Type:	Cisco 3640
Available / Total Memory(MB):	34/128 MB
Total Flash Capacity:	32 MB

Software	More ...
IOS Version:	12.4(7)
SDM Version:	2.5

Feature Availability: IP ✓ Firewall ● VPN ● IPS ● NAC ●

Configuration Overview

Interfaces and Connections — Up (1) — Down (3)

Total Supported LAN:	2	Total Supported WAN:	2
Configured LAN Interface:	1	Total WAN Connections:	0
DHCP Server:	Not Configured		

Firewall Policies — Inactive

VPN — Up (0)

IPSec (Site-to-Site):	0	GRE over IPSec:	0
Xauth Login Required:	0	Easy VPN Remote:	0
No. of DMVPN Clients:	0	No. of Active VPN Clients:	0

Routing

No. of Static Route:	0
Dynamic Routing Protocols:	None

Intrusion Prevention

Active Signatures:	0
No. of IPS-enabled Interfaces:	0
SDF Version:	

Security Dashboard

Task 5:

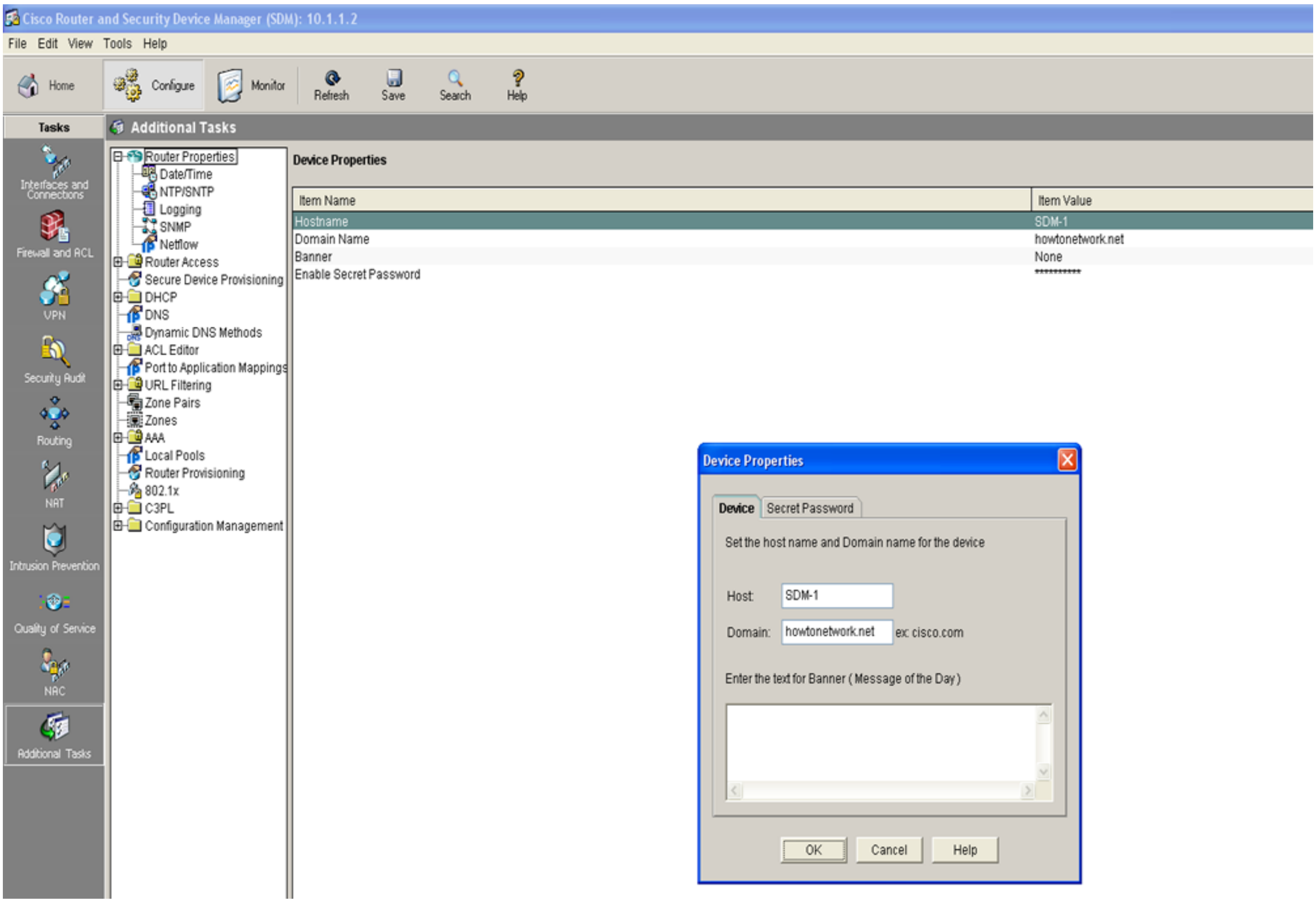
To complete this task you need to navigate to the router properties as follows:

1. On the top menu (next to Home) click on **Configure**.

2. Under **Tasks**, click on **Additional Tasks**.

3. Next, click on **Router Properties**.

4. Click on **Edit** at the far right and adjust the parameters as desired.



Device Properties

Item Name	Item Value
Hostname	SDM-1
Domain Name	howtonetwork.net
Banner	None
Enable Secret Password	**********

Set the host name and Domain name for the device

Host: SDM-1

Domain: howtonetwork.net ex: cisco.com

Enter the text for Banner (Message of the Day)

From the page above, you can configure the router hostname, DNS Domain, enable secret, as well as the MOTD banner. Make it a point to familiarize yourself with the configuration tasks that can be performed here. When you have configured the desired hostname (and any other parameters, click on OK and the configuration will be saved onto the router.

Lab 83: Using Cisco SDM to configure IP interfaces

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure IP interfaces using Cisco SDM.

Lab Purpose:

Understanding Cisco SDM is a fundamental skill. SDM is a web-based application that can be used to configure routers as well as troubleshoot internetworks. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure IP interfaces using SDM.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

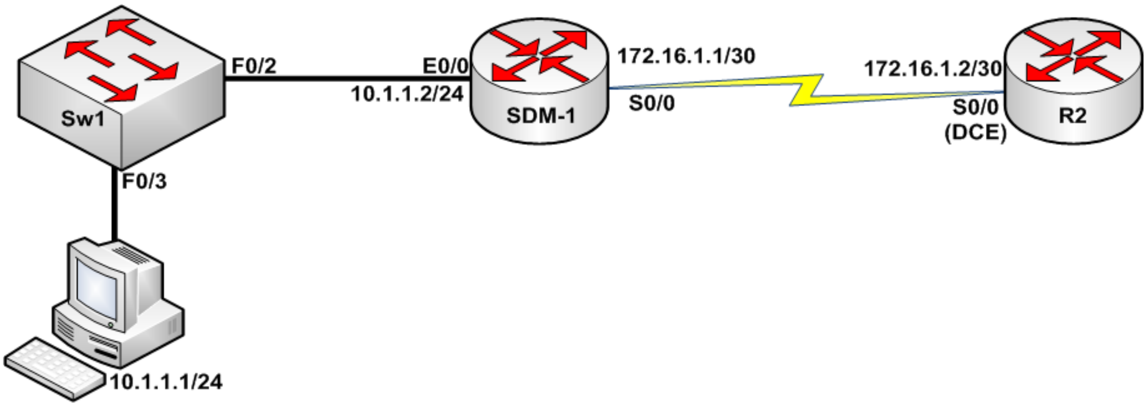
In order to use SDM, you must have an SDM-capable router. The following routers support SDM:

- Cisco Small Business 101, 106, and 107
- Cisco 1701, 1710, 1711, 1712, 1721, 1751, 1751-V, 1760 and 1870V
- Cisco 1801, 1802, 1803, 1811, and 1812
- Cisco 1841
- Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and Cisco 2691 Multiservice Routers
- Cisco 2801, 2811, 2821, and 2851
- Cisco 3620, 3640, 3661, and 3662
- Cisco 3725 and 3745
- Cisco 3825 and 3845
- Cisco 7204VXR, 7206VXR and 7301

The objective of this lab exercise is to familiarize your with the SDM GUI and how to navigate through it. As long as you have one of the platforms listed above, the configuration tasks and GUI navigation will be the same. These lab exercises are based on a Cisco 3640 router with two 10Mbps Ethernet interfaces and two Serial interfaces, but can be completed on any one of the above routers with similar interfaces. Substitute the interfaces in these lab exercises with the ones you have on your router.

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure hostnames on Sw1 and R2 as illustrated in the topology.

Task 2:

Configure VLAN 200 on Sw1 and assign it the name SDM_VLAN. Next, configure the E0/0 interface of SDM-1 with the IP address of 10.1.1.2/24. Ensure that the PC has the IP address 10.1.1.1/24 configured on the correct NIC.

Task 3:

Using the CLI configure the S0/0 interface of R2 with the IP address specified in the topology. Enable this interface and provide clocking to SDM-1 at 2Mbps.

Task 4:

Using SDM, configure the S0/0 interface of SDM-1 with the IP address specified in the topology.

Task 5:

Verify your interface status in SDM and ping between the routers.

SOLUTION:

Lab 83 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

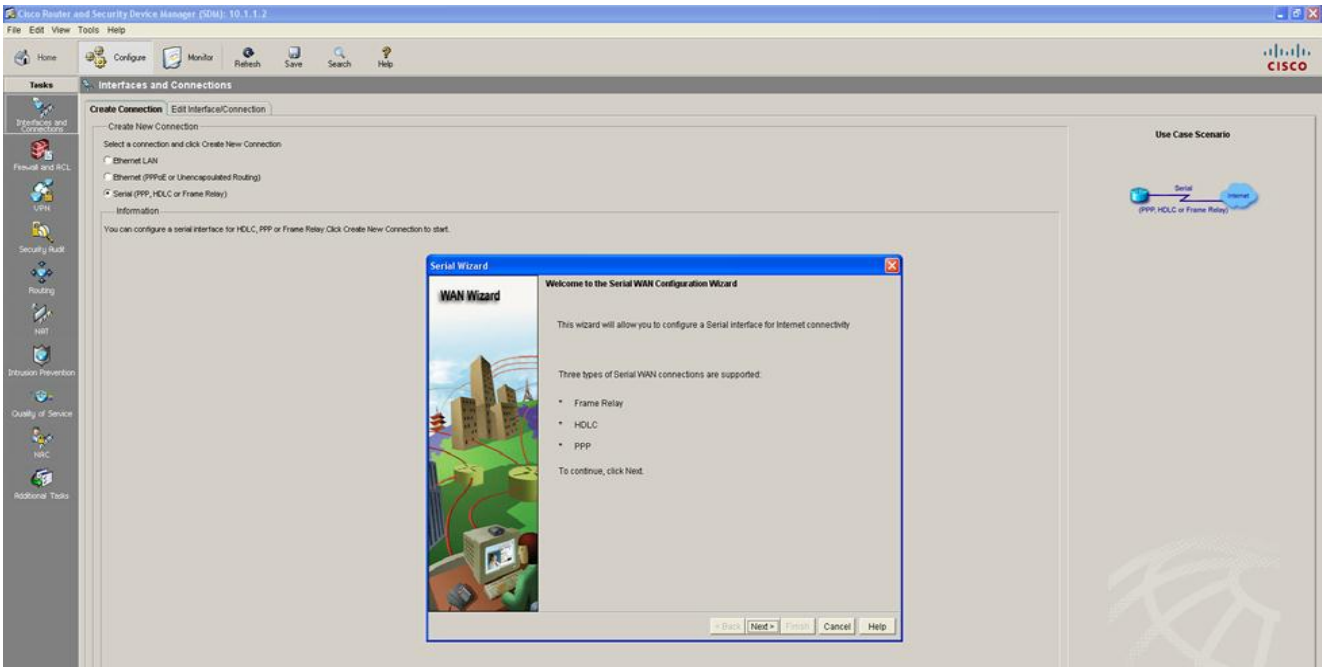
Task 3:

```
R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#int s0/0

R2(config-if)#ip address 172.16.1.2 255.255.255.252

R2(config-if)#clock rate 2000000

R2(config-if)#no shutdown

R2(config-if)#end

R2#
```

Task 4:

To complete this task you need to navigate to the router properties as follows:

1. On the top menu click on **Configure**.
2. Under **Tasks**, click on **Interfaces and Connections**.
3. Next, click on **Create Connection**.
4. Click on the **Serial (PPP, HDLC or Frame Relay)** radio button.
5. At the bottom of the page, click on **Create New Connection**.



Interfaces and Connections

Create Connection | Edit Interface/Connection

Create New Connection

Select a connection and click Create New Connection

○ Ethernet LAN

○ Ethernet (PPPoE or Unencapsulated Routing)

● Serial (PPP, HDLC or Frame Relay)

Information

You can configure a serial interface for HDLC, PPP or Frame Relay Click Create New Connection to start.

Welcome to the Serial WAN Configuration Wizard

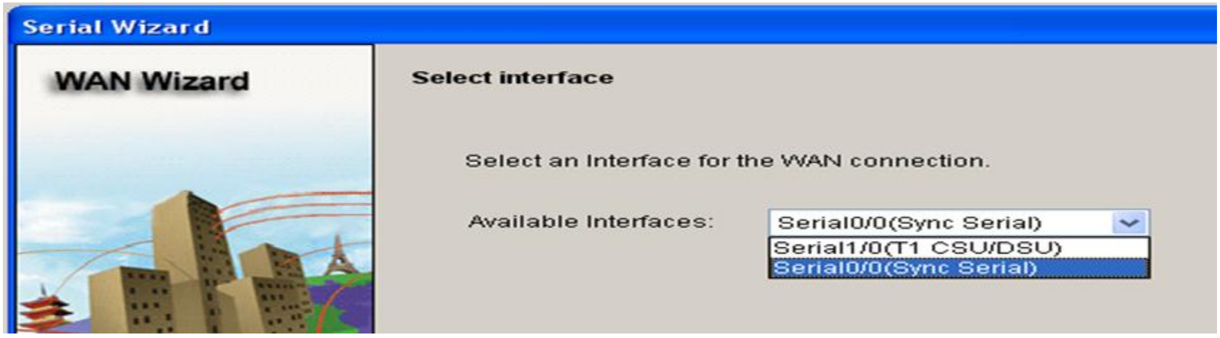
This wizard will allow you to configure a Serial interface for Internet connectivity

Three types of Serial WAN connections are supported:

- Frame Relay
- HDLC
- PPP

To continue, click Next.

6. Next, select the interface you want to configure from the drop-down menu:



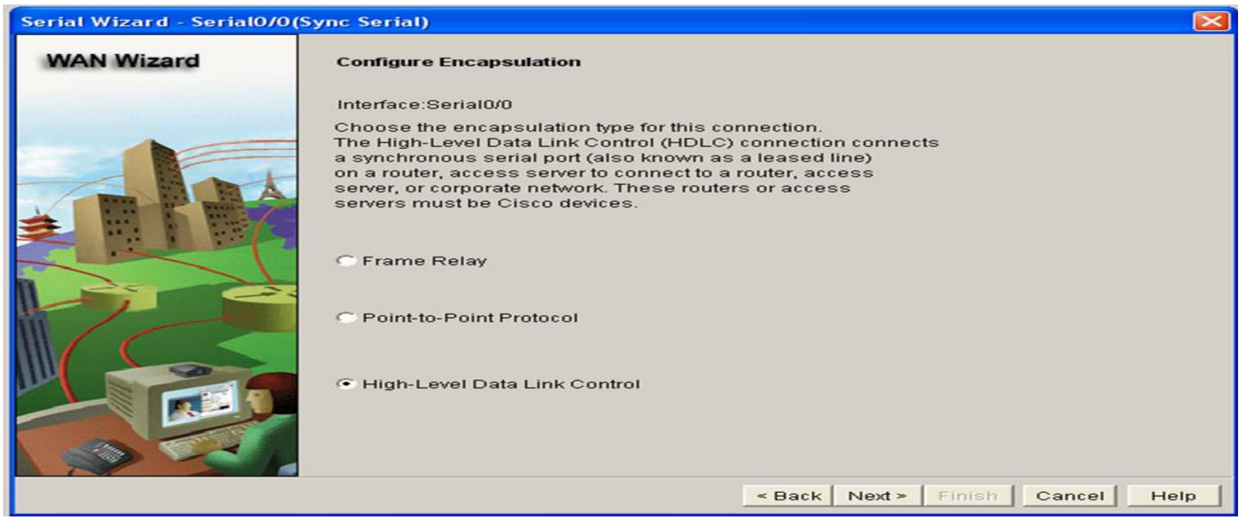
Select interface

Select an Interface for the WAN connection.

Available Interfaces: Serial0/0(Sync Serial)

Serial1/0(T1 CSU/DSU)
Serial0/0(Sync Serial)

7. Select the desired interface encapsulation type from the available options:



Configure Encapsulation

Interface:Serial0/0

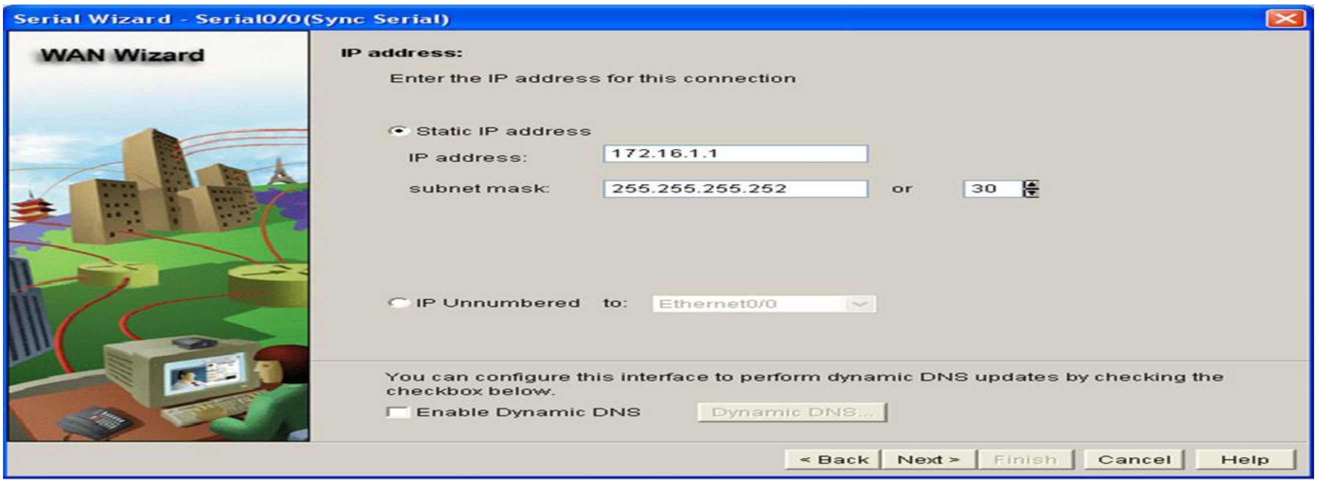
Choose the encapsulation type for this connection.
The High-Level Data Link Control (HDLC) connection connects
a synchronous serial port (also known as a leased line)
on a router, access server to connect to a router, access
server, or corporate network. These routers or access
servers must be Cisco devices.

○ Frame Relay

○ Point-to-Point Protocol

● High-Level Data Link Control

8. Configure the desired IP address for the interface:



IP address:

Enter the IP address for this connection

● Static IP address

IP address: 172.16.1.1

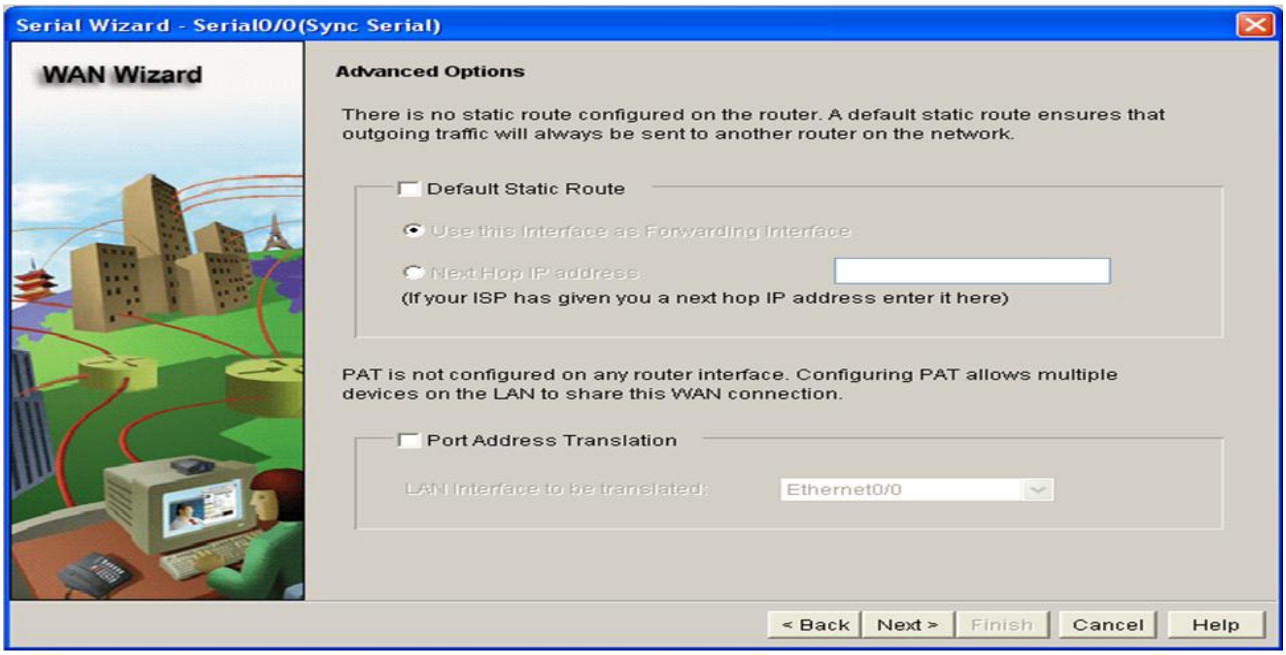
subnet mask: 255.255.255.252 or 30

○ IP Unnumbered to: Ethernet0/0

You can configure this interface to perform dynamic DNS updates by checking the checkbox below.

□ Enable Dynamic DNS

9. Optionally, you can configure a default static route or Port Address Translation:



Advanced Options

There is no static route configured on the router. A default static route ensures that outgoing traffic will always be sent to another router on the network.

□ Default Static Route

● Use this Interface as Forwarding Interface

○ Next Hop IP address

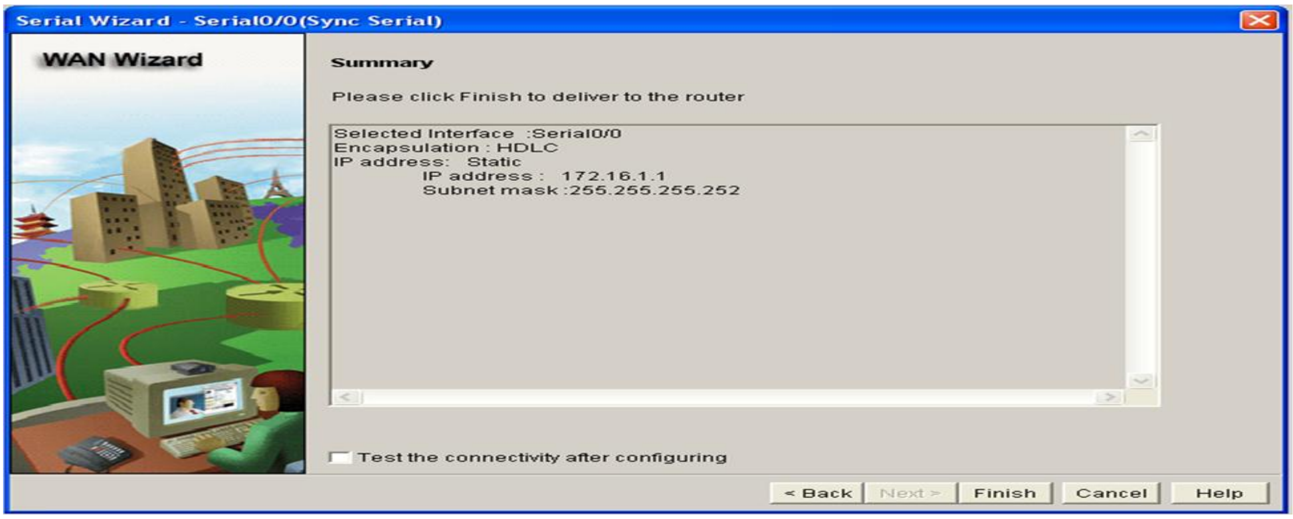
(If your ISP has given you a next hop IP address enter it here)

PAT is not configured on any router interface. Configuring PAT allows multiple devices on the LAN to share this WAN connection.

□ Port Address Translation

LAN Interface to be translated: Ethernet0/0

10.Click **Finish** when you're done.



Serial Wizard - Serial0/0(Sync Serial)
WAN Wizard
Summary
Please click Finish to deliver to the router
Test the connectivity after configuring
< Back
Next >
Finish
Cancel
Help

```
Selected Interface  :Serial0/0
Encapsulation : HDLC
IP address:  Static
          IP address :   172.16.1.1
          Subnet mask :255.255.255.252
```

□ Test the connectivity after configuring

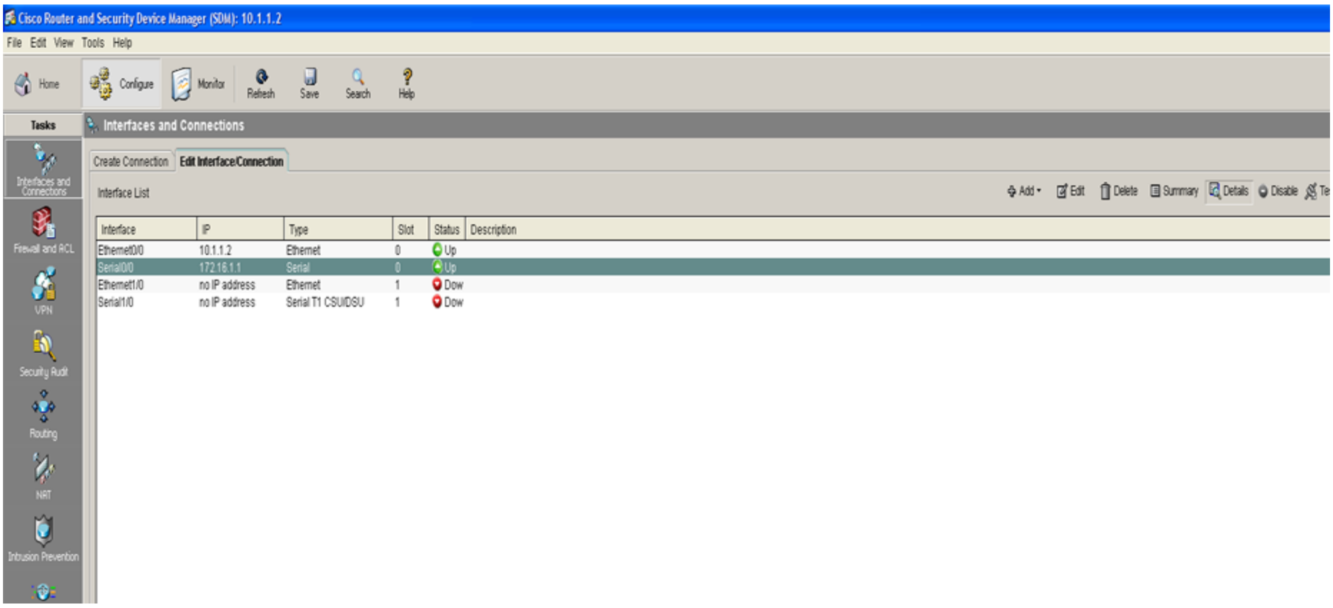
Task 5:

To complete this task you need to navigate to the router properties as follows:

1. On the top menu click on **Configure**.

2. Under **Tasks**, click on **Interfaces and Connections**.

3. Next, click on **Edit Interface/Connection**. You should see the S0/0 status as up.



Interface	IP	Type	Slot	Status	Description
Ethernet0/0	10.1.1.2	Ethernet	0	Up	
Serial0/0	172.16.1.1	Serial	0	Up	
Ethernet1/0	no IP address	Ethernet	1	Dow	
Serial1/0	no IP address	Serial T1 CSU/DSU	1	Dow	

```
R2>ping 172.16.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/5 ms
```

Lab 084: Using Cisco SDM to configure Multi-Area OSPF Routing

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure IP OSPF using Cisco SDM.

Lab Purpose:

Understanding Cisco SDM is a fundamental skill. SDM is a web-based application that can be used to configure routers as well as troubleshoot internetworks. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure multi-area OSPF using SDM.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

In order to use SDM, you must have an SDM-capable router. The following routers support SDM:

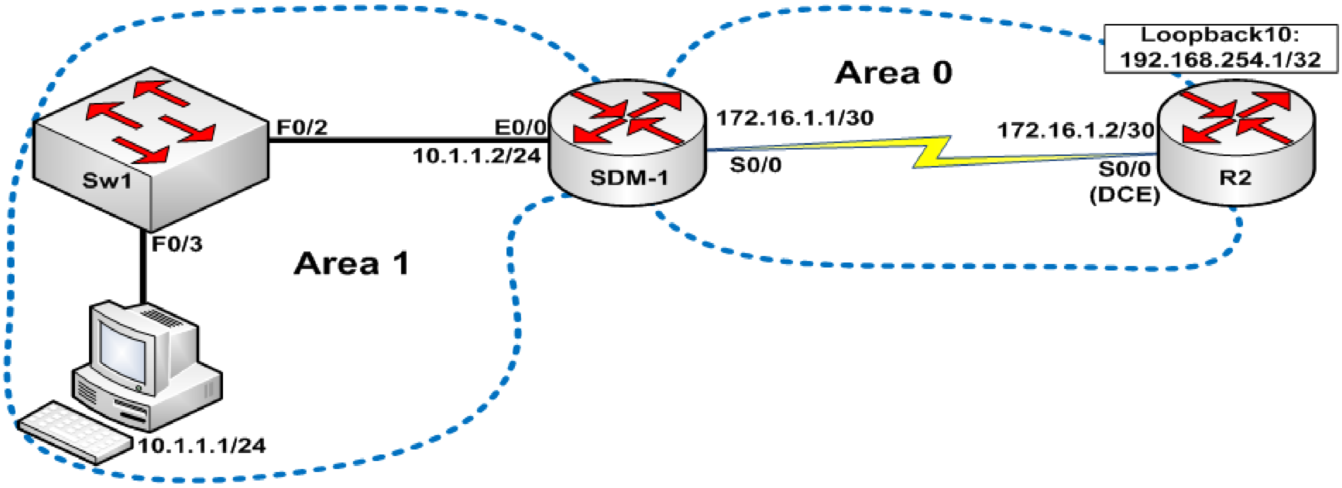
- Cisco Small Business 101, 106, and 107
- Cisco 1701, 1710, 1711, 1712, 1721, 1751, 1751-V, 1760 and 1870V
- Cisco 1801, 1802, 1803, 1811, and 1812
- Cisco 1841
- Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and Cisco 2691 Multiservice Routers
- Cisco 2801, 2811, 2821, and 2851
- Cisco 3620, 3640, 3661, and 3662

- Cisco 3725 and 3745
- Cisco 3825 and 3845
- Cisco 7204VXR, 7206VXR and 7301

The objective of this lab exercise is to familiarize your with the SDM GUI and how to navigate through it. As long as you have one of the platforms listed above, the configuration tasks and GUI navigation will be the same. These lab exercises are based on a Cisco 3640 router with two 10Mbps Ethernet interfaces and two Serial interfaces, but can be completed on any one of the above routers with similar interfaces. Substitute the interfaces in these lab exercises with the ones you have on your router.

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure hostnames on Sw1 and R2 as illustrated in the topology.

Task 2:

Configure VLAN 200 on Sw1 and assign it the name SDM_VLAN. Next, configure the E0/0 interface of SDM-1 with the IP address of 10.1.1.2/24. Ensure that the PC has the IP address 10.1.1.1/24 configured on the correct NIC.

Task 3:

Using the CLI configure the S0/0 interface of R2 with the IP address specified in the topology. Enable this interface and provide clocking to SDM-1 at 2Mbps. Configure Loopback10 on R2 with the IP address 192.168.254.1/32

Task 4:

Using SDM, configure the S0/0 interface of SDM-1 with the IP address specified in the topology.

Task 5:

Configure OSPF process ID 2 on R2. Configure Serial0/0 in Area 0 and Loopback0 in Area 2.

Task 6:

Using SDM, configure Serial0/0 in SDM-1 in Area 0 and Ethernet0/0 in Area 1. Use a process ID of 1. Verify that you can ping the Loopback0 interface of R2 via SDM. Finally, verify that R2 is seeing the OSPF routes from SDM-1.

SOLUTION:

Lab 84 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

For reference information on configuring DCE clocking, please refer to:

Lab 21 Configuration and Verification Task 2

Lab 35 Configuration and Verification Task 2

For reference information on configuring Loopback interfaces, please refer to:

Lab 39 Configuration and Verification Task 4

Lab 43 Configuration and Verification Task 2

Task 4:

For reference information on using SDM to configure & verify interfaces, please refer to:

Lab 83 Configuration and Verification Task 4

Lab 83 Configuration and Verification Task 5

Task 5:

```
R2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config-if)#router ospf 2

R2(config-router)#net 172.16.1.2 0.0.0.3 area 0

R2(config-router)#net 192.168.254.1 0.0.0.0 area 1

R2(config-router)#end

R2#
```

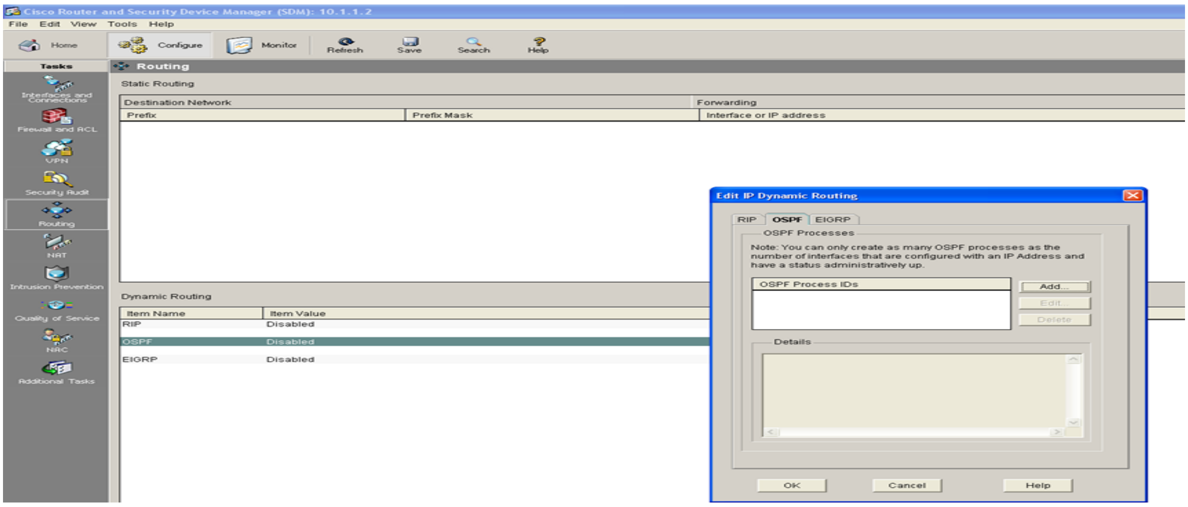
Task 6:

To complete this task you need to navigate to the router properties as follows:

1. On the top menu click on **Configure**.

2. Under **Tasks**, click on **Routing**.

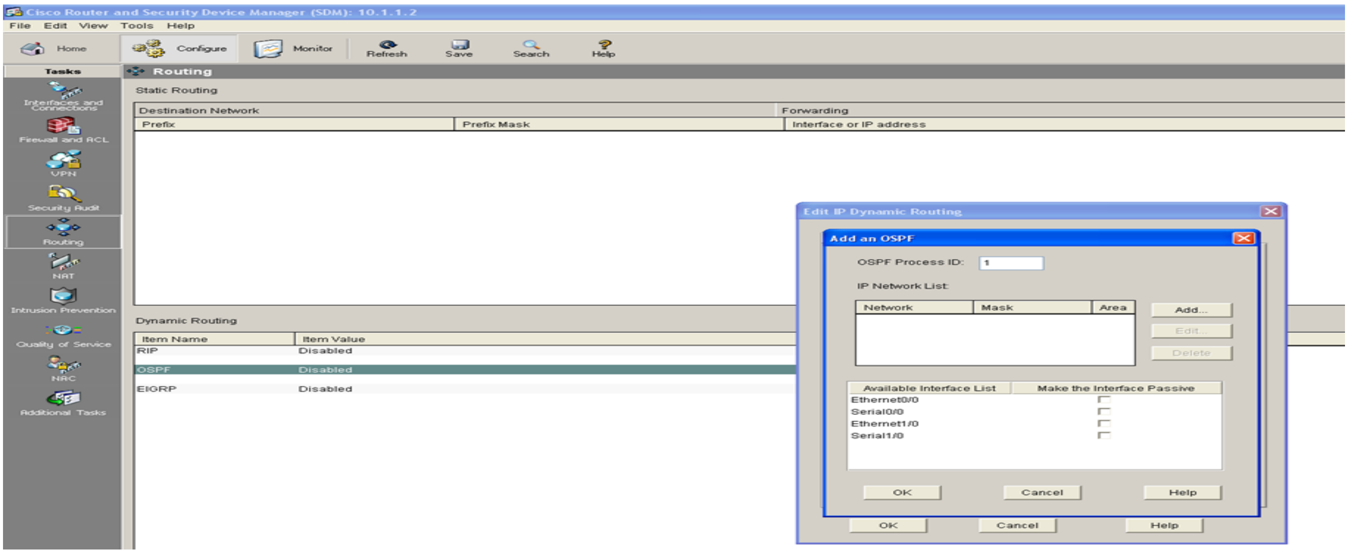
3. Next, highlight **OSPF** and click on **Edit**.



Item Name	Item Value
RIP	Disabled
OSPF	Disabled
EIGRP	Disabled

Note: You can only create as many OSPF processes as the number of interfaces that are configured with an IP Address and have a status administratively up.

4. Click on the **Add** to configure an OSPF process ID. Add the OSPF process ID as illustrated. Notice that you also have the option to configure certain interfaces as passive at this point in the configuration.



Static Routing

Destination Network		Forwarding
Prefix	Prefix Mask	Interface or IP address

Dynamic Routing

Item Name	Item Value
RIP	Disabled
OSPF	Disabled
EIGRP	Disabled

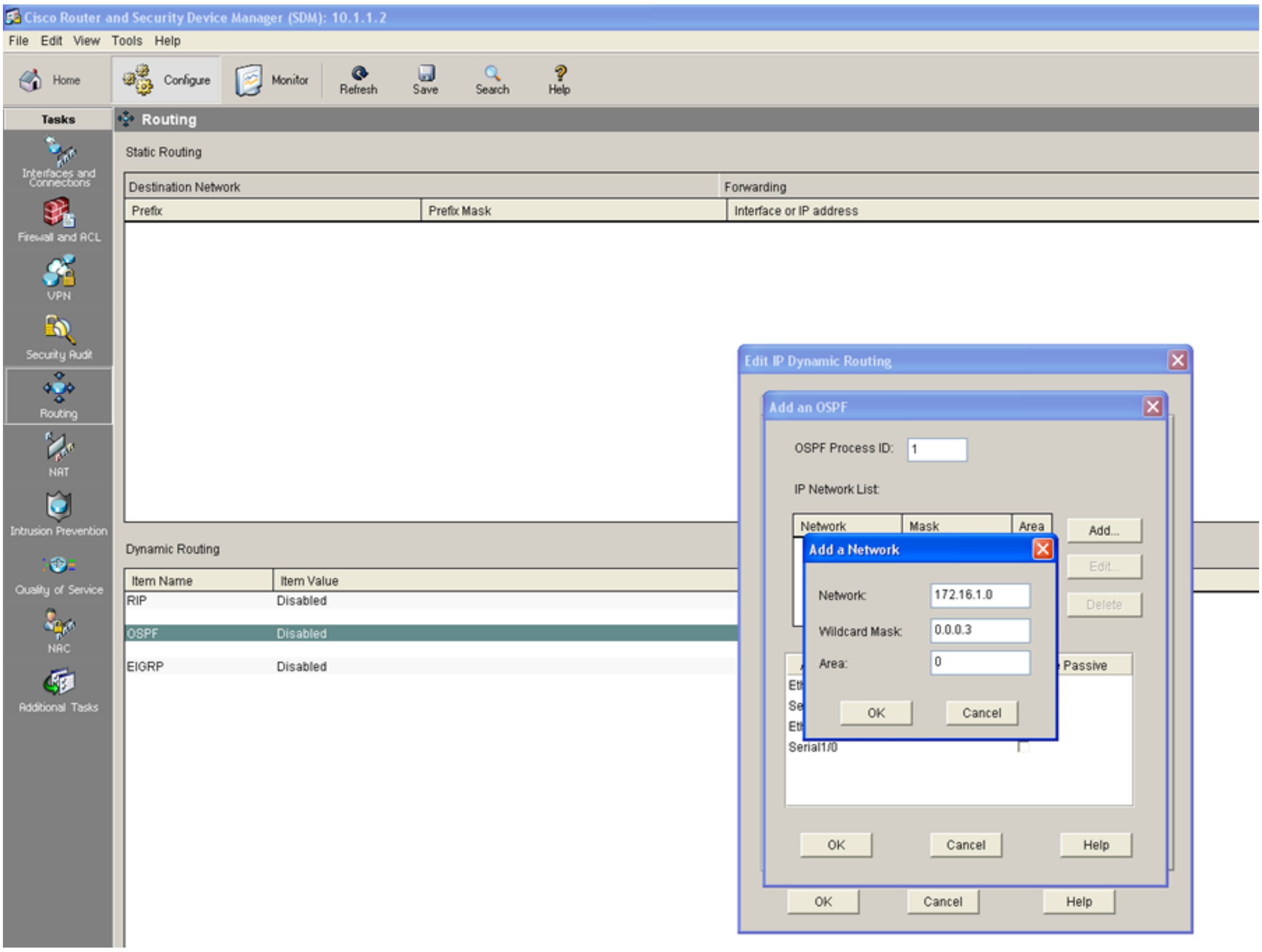
OSPF Process ID: 1

IP Network List

Network	Mask	Area

Available Interface List	Make the Interface Passive
Ethernet0/0	□
Serial0/0	□
Ethernet1/0	□
Serial1/0	□

5. Under **IP Network List**, click **Add** and add the network, wildcard mask and OSPF Area ID. Click **OK**. Repeat the same for the 10.1.1.0/24 subnet that will be in OSPF Area 1 and click **OK** when complete.



Static Routing

Destination Network		Forwarding
Prefix	Prefix Mask	Interface or IP address

Dynamic Routing

Item Name	Item Value
RIP	Disabled
OSPF	Disabled
EIGRP	Disabled

OSPF Process ID: 1

IP Network List

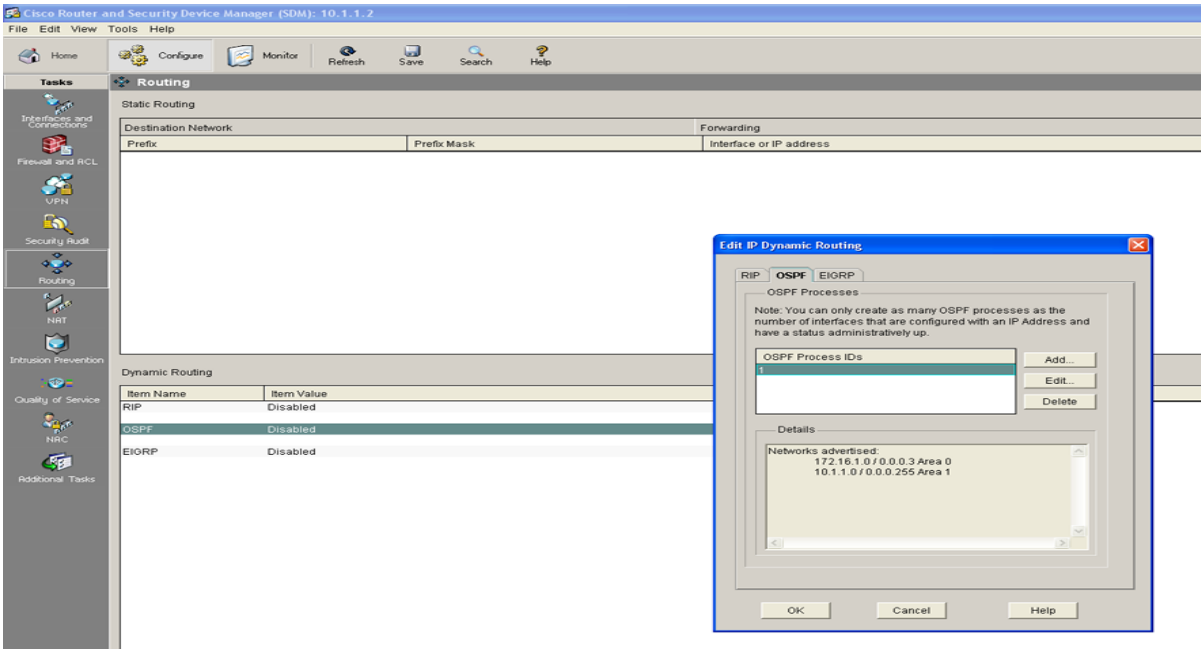
Network	Mask	Area

Network: 172.16.1.0

Wildcard Mask: 0.0.0.3

Area: 0

6. After you have added you network statements, click **OK** to return to the main screen. Here you can see a summary of your OSPF configuration for a specific process ID.



Cisco Router and Security Device Manager (SDM): 10.1.1.2

Routing

Static Routing

Destination Network		Forwarding
Prefix	Prefix Mask	Interface or IP address

Dynamic Routing

Item Name	Item Value
RIP	Disabled
OSPF	Disabled
EIGRP	Disabled

Edit IP Dynamic Routing

OSPF Processes

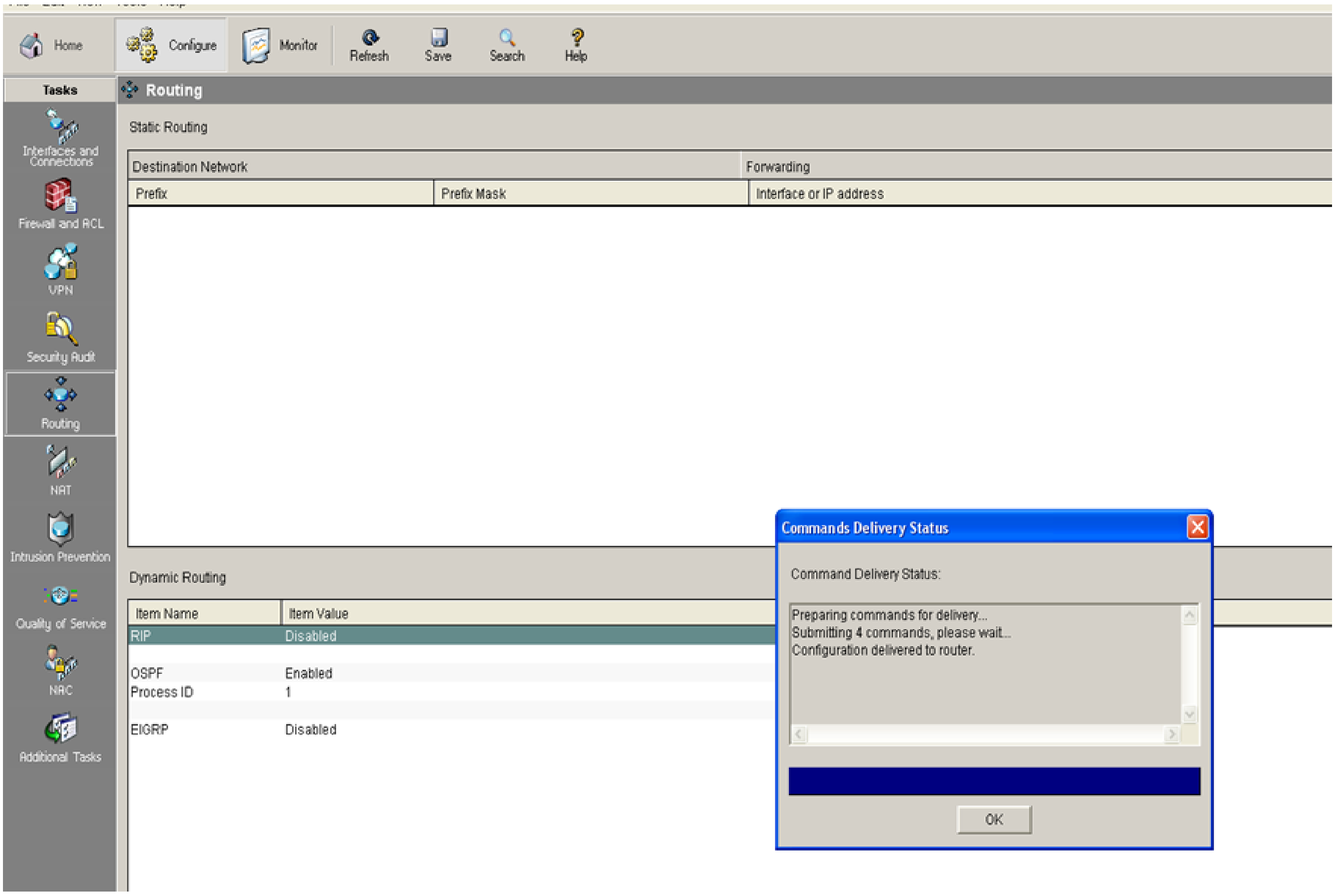
Note: You can only create as many OSPF processes as the number of interfaces that are configured with an IP Address and have a status administratively up.

OSPF Process IDs
1

Details

```
Networks advertised:
         172.16.1.0 / 0.0.0.3 Area 0
         10.1.1.0 / 0.0.0.255 Area 1
```

7. If you are satisfied with your configuration, click **OK** and the configuration is loaded to the router.



Routing

Static Routing

Destination Network		Forwarding
Prefix	Prefix Mask	Interface or IP address

Dynamic Routing

Item Name	Item Value
RIP	Disabled
OSPF	Enabled
Process ID	1
EIGRP	Disabled

Commands Delivery Status

Command Delivery Status:

```
Preparing commands for delivery...
Submitting 4 commands, please wait...
Configuration delivered to router.
```

8. Once complete, we can see the adjaceny has established on R2

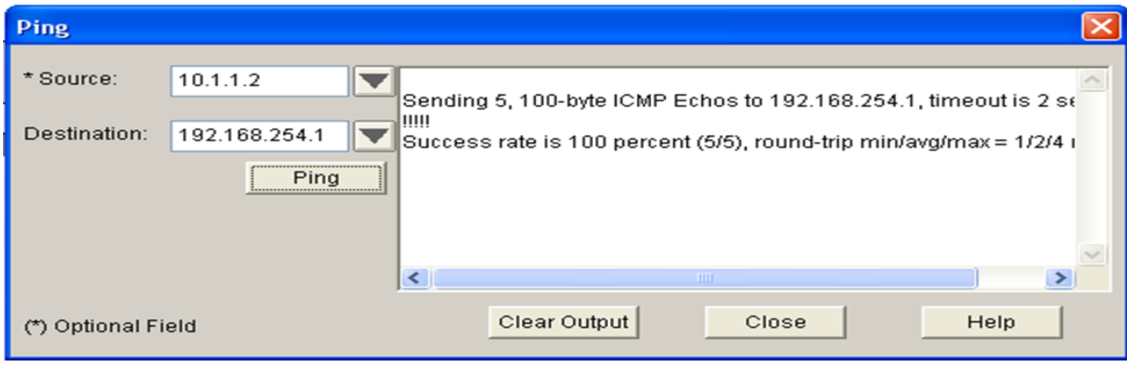
R2#**show ip ospf neighbor**

```
Neighbor ID     Pri   State           Dead Time   Address         Interface

172.16.1.1        0   FULL/  -        00:00:37    172.16.1.1       Serial0/0
```

R2#**show ip route ospf**

```
     10.0.0.0/24 is subnetted, 1 subnets

O IA    10.1.1.0 [110/74] via 172.16.1.1, 00:08:30, Serial0/0
```

From the top level menu under **Tools** - ping the Loopback0 interface of R2 as follows:



* Source: 10.1.1.2

Destination: 192.168.254.1

```
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 se
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ı
```

Lab 85: Using Cisco SDM to configure IP EIGRP Routing

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure EIGRP using Cisco SDM.

Lab Purpose:

Understanding Cisco SDM is a fundamental skill. SDM is a web-based application that can be used to configure routers as well as troubleshoot internetworks. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure IP EIGRP routing using SDM.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

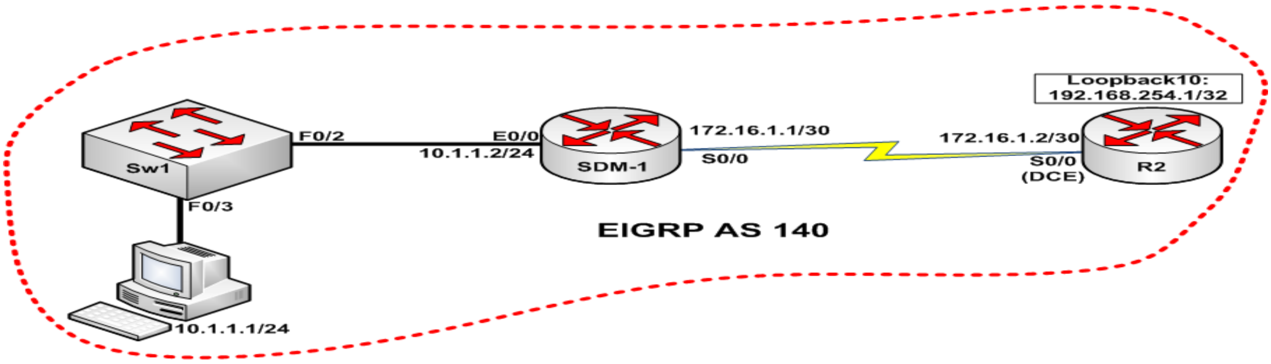
In order to use SDM, you must have an SDM-capable router. The following routers support SDM:

- Cisco Small Business 101, 106, and 107
- Cisco 1701, 1710, 1711, 1712, 1721, 1751, 1751-V, 1760 and 1870V
- Cisco 1801, 1802, 1803, 1811, and 1812
- Cisco 1841
- Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and Cisco 2691 Multiservice Routers
- Cisco 2801, 2811, 2821, and 2851
- Cisco 3620, 3640, 3661, and 3662
- Cisco 3725 and 3745
- Cisco 3825 and 3845
- Cisco 7204VXR, 7206VXR and 7301

The objective of this lab exercise is to familiarize your with the SDM GUI and how to navigate through it. As long as you have one of the platforms listed above, the configuration tasks and GUI navigation will be the same. These lab exercises are based on a Cisco 3640 router with two 10Mbps Ethernet interfaces and two Serial interfaces, but can be completed on any one of the above routers with similar interfaces. Substitute the interfaces in these lab exercises with the ones you have on your router.

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure hostnames on Sw1 and R2 as illustrated in the topology.

Task 2:

Configure VLAN 200 on Sw1 and assign it the name SDM_VLAN. Next, configure the E0/0 interface of SDM-1 with the IP address of 10.1.1.2/24. Ensure that the PC has the IP address 10.1.1.1/24 configured on the correct NIC.

Task 3:

Using the CLI configure the S0/0 interface of R2 with the IP address specified in the topology. Enable this interface and provide clocking to SDM-1 at 2Mbps. Configure Loopback10 on R2 with the IP address 192.168.254.1/32

Task 4:

Using SDM, configure the S0/0 interface of SDM-1 with the IP address specified in the topology.

Task 5:

Configure EIGRP using AS 140 on R2. Configure Serial0/0 and Loopback0 for EIGRP routing.

Task 6:

Using SDM, configure EIGRP using AS 140 on SDM-1. Ensure that the Serial0/0 and Ethernet0/0 subnets are configured for EIGRP routing. Use SDM ping to ensure you can ping the Loopback0 interface on R2. Finally, verify the EIGRP adjacency on R2 and the IP routing table.

SOLUTION:

Lab 85 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

For reference information on configuring DCE clocking, please refer to:

Lab 21 Configuration and Verification Task 2

Lab 35 Configuration and Verification Task 2

For reference information on configuring Loopback interfaces, please refer to:

Lab 39 Configuration and Verification Task 4

Lab 43 Configuration and Verification Task 2

Task 4:

For reference information on using SDM to configure & verify interfaces, please refer to:

Lab 83 Configuration and Verification Task 4

Lab 83 Configuration and Verification Task 5

Task 5:

For reference information on enabling EIGRP, please refer to:

Lab 41 Configuration and Verification Task 4

Lab 42 Configuration and Verification Task 5

Lab 44 Configuration and Verification Task 5

Task 6:

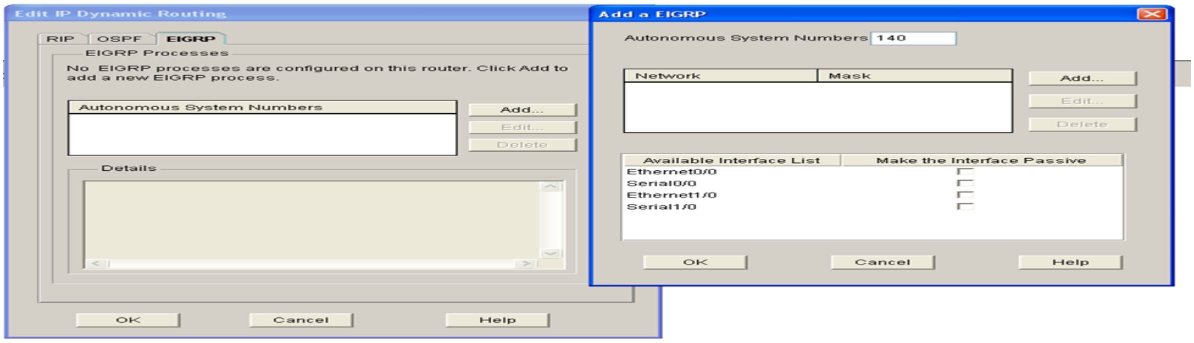
To complete this task you need to navigate to the router properties as follows:

1. On the top menu click on **Configure**.

2. Under Tasks, click on **Routing**.

3. Next, highlight **EIGRP** and click on **Edit**.

4. Next to **Autonmous System Numbers**, click **Add** and key in the EIGRP AS Number.

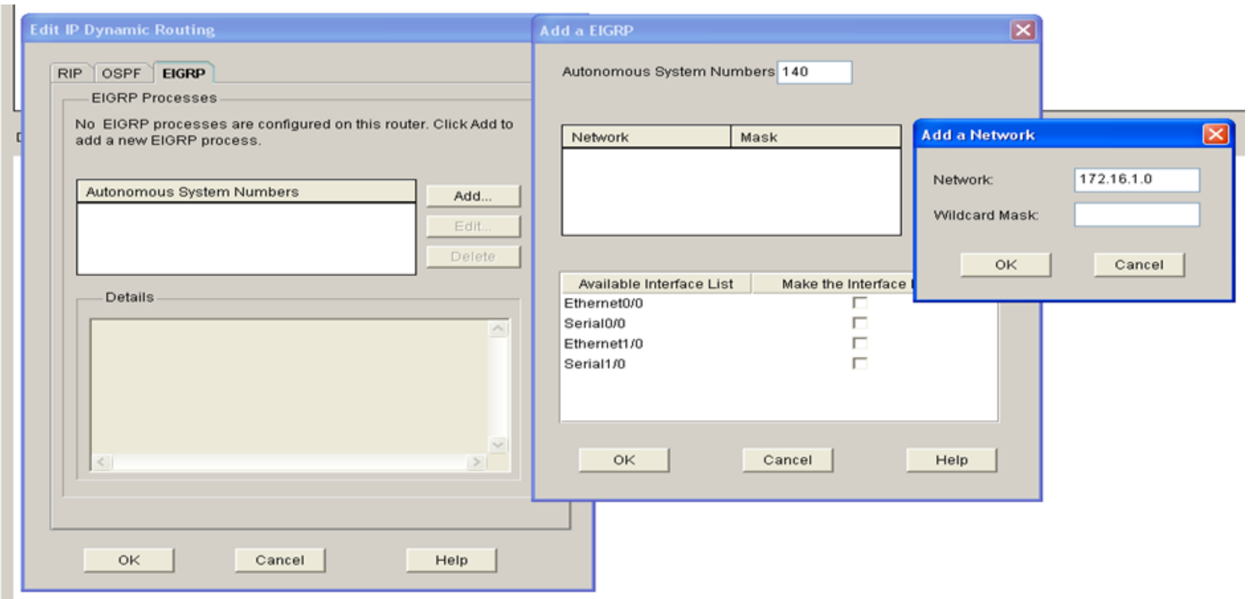


No EIGRP processes are configured on this router. Click Add to add a new EIGRP process.

Autonomous System Numbers 140

Available Interface List	Make the Interface Passive
Ethernet0/0	□
Serial0/0	□
Ethernet1/0	□
Serial1/0	□

5. Next click **Add** to add network entries for EIGRP. Notice that you have the option to specify wildcard masks.



No EIGRP processes are configured on this router. Click Add to add a new EIGRP process.

Autonomous System Numbers 140

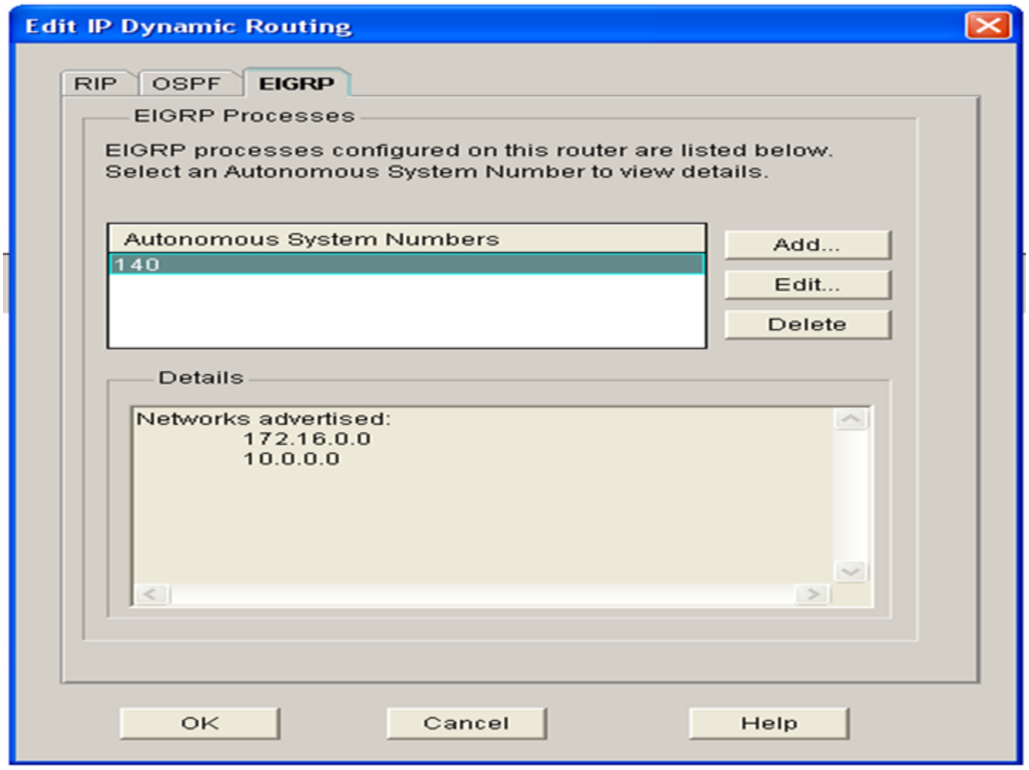
Ethernet0/0 □
Serial0/0 □
Ethernet1/0 □
Serial1/0 □

Network: 172.16.1.0
Wildcard Mask:

6. Perform the same configuration tasks for the 10.1.1.0/24 subnet.

7. Next, click **OK** and you return to the main EIGRP configuration menu.

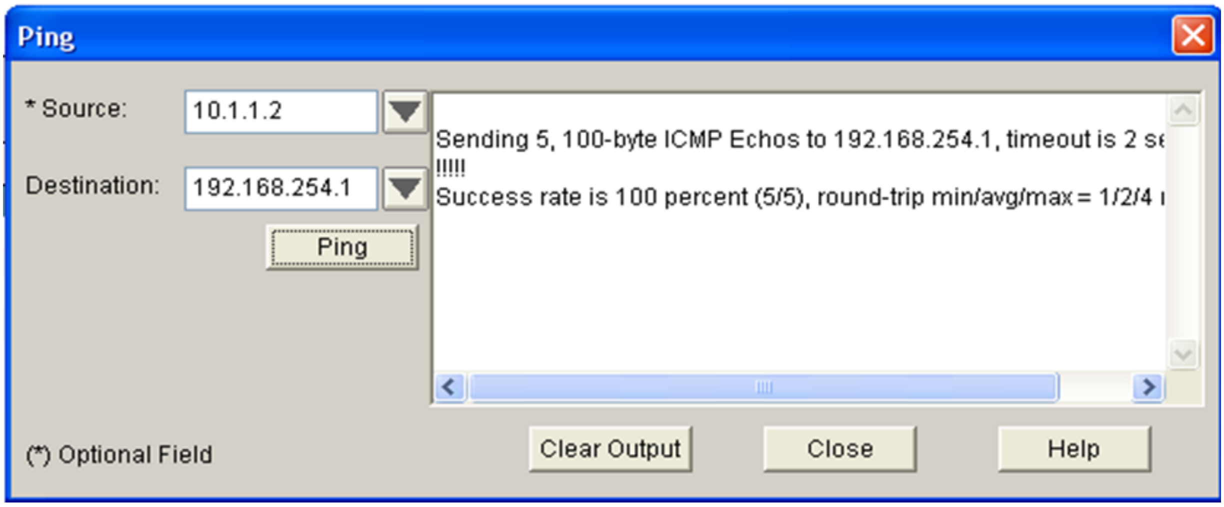
NOTE: By default, EIGRP will disable automatic network summarization when configured via SDM. Therefore, if you looked at the actual running-config on SDM-1, you would see the no auto-summary command included.



EIGRP processes configured on this router are listed below. Select an Autonomous System Number to view details.

140

Networks advertised:
172.16.0.0
10.0.0.0



Source: 10.1.1.2

Destination: 192.168.254.1

```
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 se
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 r
```

```
R2#show ip eigrp neighbors

IP-EIGRP neighbors for process 140

H   Address              Interface      Hold Uptime   SRTT   RTO  Q  Seq

                                 (sec)        (ms)       Cnt Num

0   172.16.1.1             Se0/0           14 00:06:41    4   200  0  2
```

```
R2#show ip route eigrp

    10.0.0.0/24 is subnetted, 1 subnets

D       10.1.1.0 [90/2195456] via 172.16.1.1, 00:06:42, Serial0/0
```

Lab 86: Using Cisco SDM to configure RIP version 2 Routing

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure RIPv2 using Cisco SDM.

Lab Purpose:

Understanding Cisco SDM is a fundamental skill. SDM is a web-based application that can be used to configure routers as well as troubleshoot internetworks. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure RIP version 2 routing using SDM.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

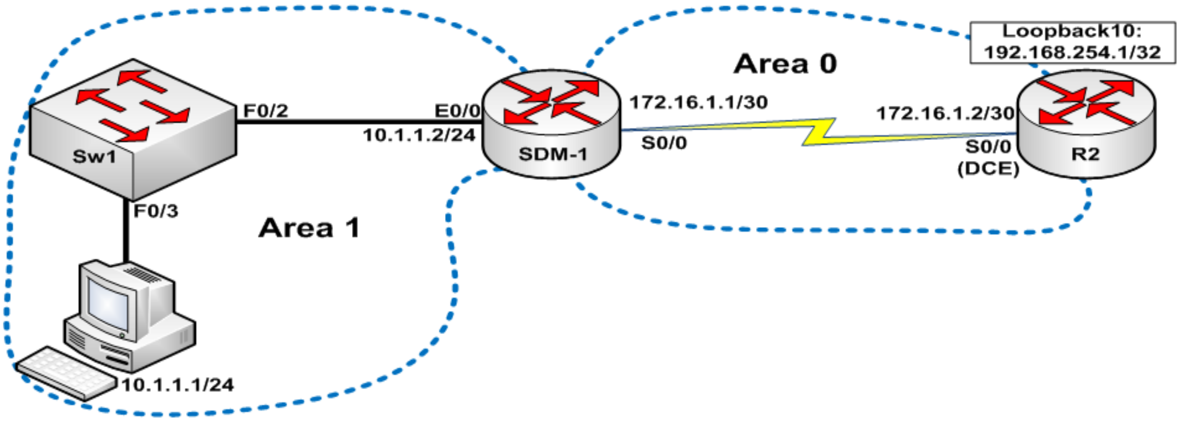
In order to use SDM, you must have an SDM-capable router. The following routers support SDM:

- Cisco Small Business 101, 106, and 107
- Cisco 1701, 1710, 1711, 1712, 1721, 1751, 1751-V, 1760 and 1870V
- Cisco 1801, 1802, 1803, 1811, and 1812
- Cisco 1841
- Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and Cisco 2691 Multiservice Routers
- Cisco 2801, 2811, 2821, and 2851
- Cisco 3620, 3640, 3661, and 3662
- Cisco 3725 and 3745
- Cisco 3825 and 3845
- Cisco 7204VXR, 7206VXR and 7301

The objective of this lab exercise is to familiarize your with the SDM GUI and how to navigate through it. As long as you have one of the platforms listed above, the configuration tasks and GUI navigation will be the same. These lab exercises are based on a Cisco 3640 router with two 10Mbps Ethernet interfaces and two Serial interfaces, but can be completed on any one of the above routers with similar interfaces. Substitute the interfaces in these lab exercises with the ones you have on your router.

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure hostnames on Sw1 and R2 as illustrated in the topology.

Task 2:

Configure VLAN 200 on Sw1 and assign it the name SDM_VLAN. Next, configure the E0/0 interface of SDM-1 with the IP address of 10.1.1.2/24. Ensure that the PC has the IP address 10.1.1.1/24 configured on the correct NIC.

Task 3:

Using the CLI configure the S0/0 interface of R2 with the IP address specified in the topology. Enable this interface and provide clocking to SDM-1 at 2Mbps. Configure Loopback10 on R2 with the IP address 192.168.254.1/32

Task 4:

Using SDM, configure the S0/0 interface of SDM-1 with the IP address specified in the topology.

Task 5:

Configure RIPv2 using on R2. Configure Serial0/0 and Loopback0 for RIPv2 routing.

Task 6:

Using SDM, configure RIPv2 on SDM-1. Ensure that the Serial0/0 and Ethernet0/0 subnets are configured for RIPv2 routing. Finally, verify the RIPv2 routes on R2.

SOLUTION:

Lab 86 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

For reference information on configuring DCE clocking, please refer to:

Lab 21 Configuration and Verification Task 2

Lab 35 Configuration and Verification Task 2

For reference information on configuring Loopback interfaces, please refer to:

Lab 39 Configuration and Verification Task 4

Lab 43 Configuration and Verification Task 2

Task 4:

For reference information on using SDM to configure & verify interfaces, please refer to:

Lab 83 Configuration and Verification Task 4

Lab 83 Configuration and Verification Task 5

Task 5:

For reference information on configuring RIPv2, please refer to:

Lab 36 Configuration and Verification Task 5

Lab 37 Configuration and Verification Task 4

Task 6:

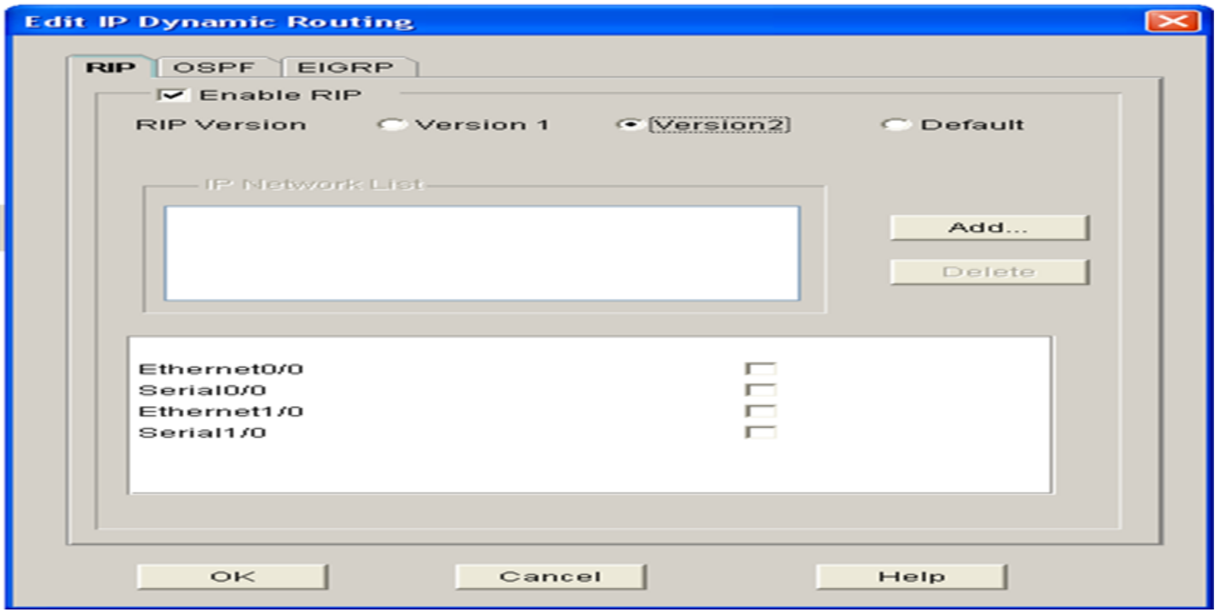
To complete this task you need to navigate to the router properties as follows:

1. On the top menu click on **Configure**.

2. Under Tasks, click on **Routing**.

3. Next, highlight **RIP** and click on **Edit**.

4. Check the **Enable RIP** checkbox and click on the **Version 2** radio box to configure RIPv2.



Edit IP Dynamic Routing

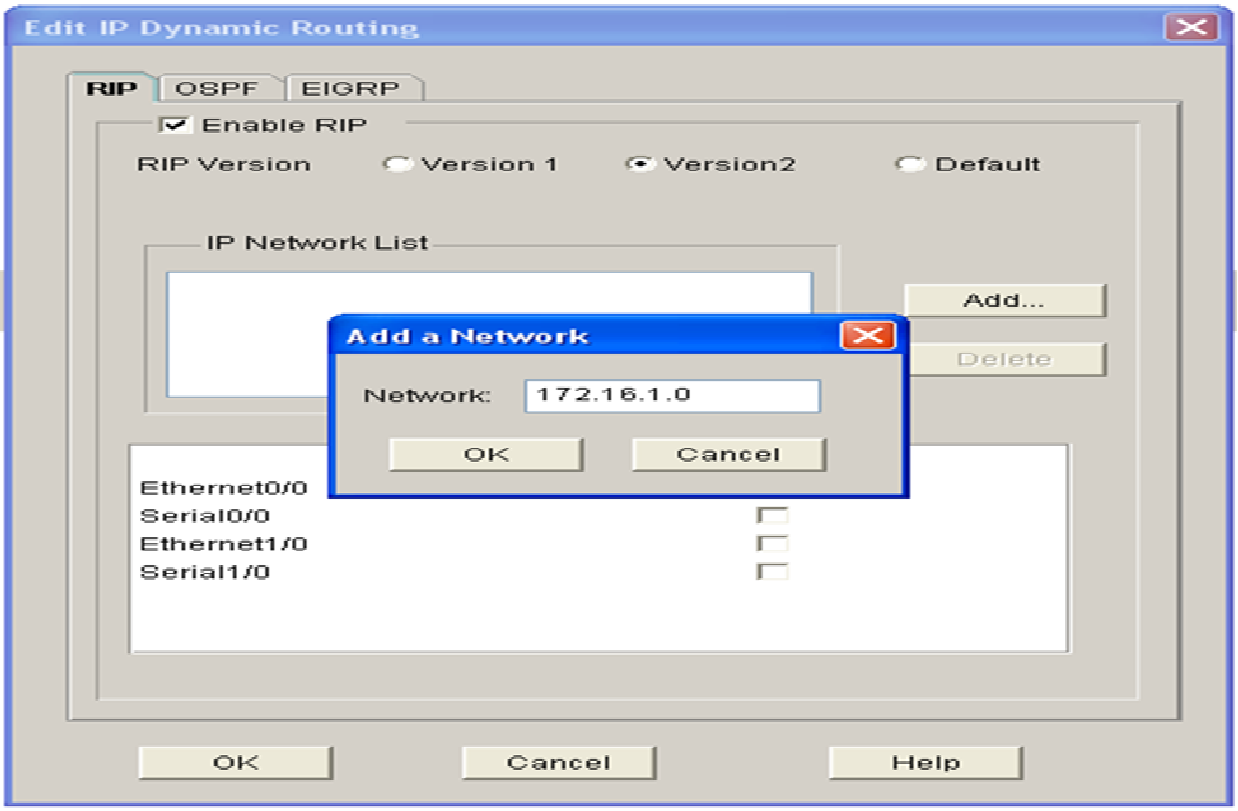
☑ Enable RIP

RIP Version ○ Version 1 ● Version2 ○ Default

IP Network List

Ethernet0/0 □
Serial0/0 □
Ethernet1/0 □
Serial1/0 □

5. Next click on **Add** and enter in the networks you want RIPv2 to advertise.



Edit IP Dynamic Routing

☑ Enable RIP

RIP Version ○ Version 1 ● Version2 ○ Default

IP Network List

Add a Network

Network: 172.16.1.0

Ethernet0/0
Serial0/0 □
Ethernet1/0 □
Serial1/0 □

6. Repeat step 5 for the 10.1.1.0/24 subnet and click **OK** when complete.

R2#**show ip route rip**

```
     10.0.0.0/24 is subnetted, 1 subnets
R       10.1.1.0 [120/1] via 172.16.1.1, 00:00:09, Serial0/0
R2#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
```

Lab 87: Using Cisco SDM to configure and apply extended ACLs

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure and apply extended Access Control Lists using Cisco SDM.

Lab Purpose:

Understanding Cisco SDM is a fundamental skill. SDM is a web-based application that can be used to configure routers as well as troubleshoot internetworks. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure and apply extended ACLs using SDM.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

In order to use SDM, you must have an SDM-capable router. The following routers support SDM:

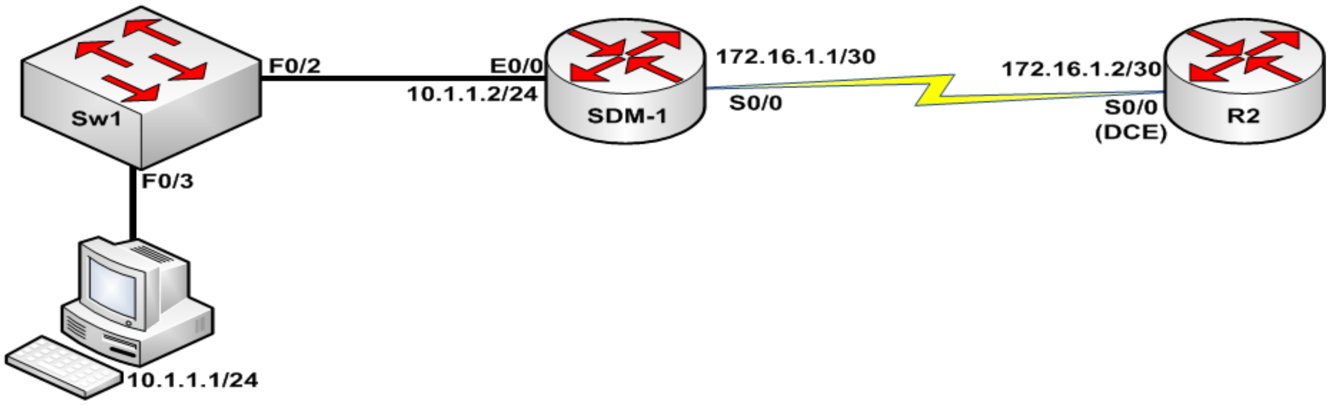
- Cisco Small Business 101, 106, and 107

- Cisco 1701, 1710, 1711, 1712, 1721, 1751, 1751-V, 1760 and 1870V
- Cisco 1801, 1802, 1803, 1811, and 1812
- Cisco 1841
- Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and Cisco 2691 Multiservice Routers
- Cisco 2801, 2811, 2821, and 2851
- Cisco 3620, 3640, 3661, and 3662
- Cisco 3725 and 3745
- Cisco 3825 and 3845
- Cisco 7204VXR, 7206VXR and 7301

The objective of this lab exercise is to familiarize your with the SDM GUI and how to navigate through it. As long as you have one of the platforms listed above, the configuration tasks and GUI navigation will be the same. These lab exercises are based on a Cisco 3640 router with two 10Mbps Ethernet interfaces and two Serial interfaces, but can be completed on any one of the above routers with similar interfaces. Substitute the interfaces in these lab exercises with the ones you have on your router.

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure hostnames on Sw1 and R2 as illustrated in the topology.

Task 2:

Configure VLAN 200 on Sw1 and assign it the name SDM_VLAN. Next, configure the E0/0 interface of SDM-1 with the IP address of 10.1.1.2/24. Ensure that the PC has the IP address 10.1.1.1/24 configured on the correct NIC.

Task 3:

Using the CLI configure the S0/0 interface of R2 with the IP address specified in the topology. Enable this interface and provide clocking to SDM-1 at 2Mbps. Configure Loopback10 on R2 with the IP address 192.168.254.1/32

Task 4:

Using SDM, configure the S0/0 interface of SDM-1 with the IP address specified in the topology. Ping and. Telnet from R2 to SDM-1 and verify that this works.

Task 5:

Configure an extended ACL numbered 140 that allows all ICMP traffic and denies all Telnet traffic. Apply this ACL inbound on the Serial0/0 interface of SDM-1.

Task 6:

Ping and. Telnet from R2 to SDM-1 and verify that this works after the ACL has been applied on SDM-1 S0/0. If you have configured this correctly, ping will work, but Telnet access will not work.

SOLUTION:

Lab 87 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

For reference information on configuring DCE clocking, please refer to:

Lab 21 Configuration and Verification Task 2

Lab 35 Configuration and Verification Task 2

For reference information on configuring Loopback interfaces, please refer to:

Lab 39 Configuration and Verification Task 4

Lab 43 Configuration and Verification Task 2

Task 4:

For reference information on using SDM to configure & verify interfaces, please refer to:

Lab 83 Configuration and Verification Task 4

Lab 83 Configuration and Verification Task 5

```
R2#ping 172.16.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

!!!!!

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

R2#telnet 172.16.1.1

Trying 172.16.1.1 ... Open

User Access Verification

Password:

SDM-1#
```

Task 5:

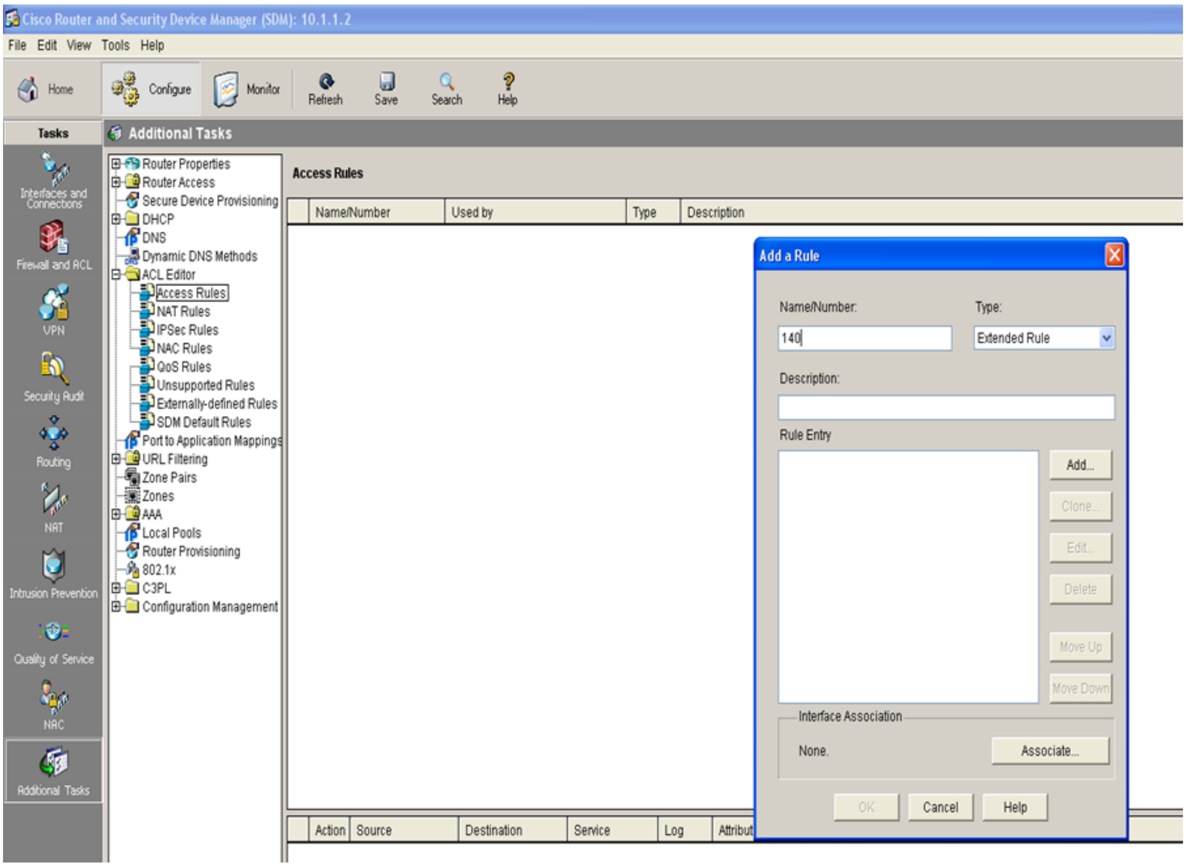
To complete this task you need to navigate to the router properties as follows:

1. On the top menu click on **Configure**.

2. Under Tasks, click on **Additional Tasks**.

3. Next, click on **ACL Editor** and highlight **Access Rules**.

4. Click on the **Add** in the top right hand corner and enter the ACL name/number and description.



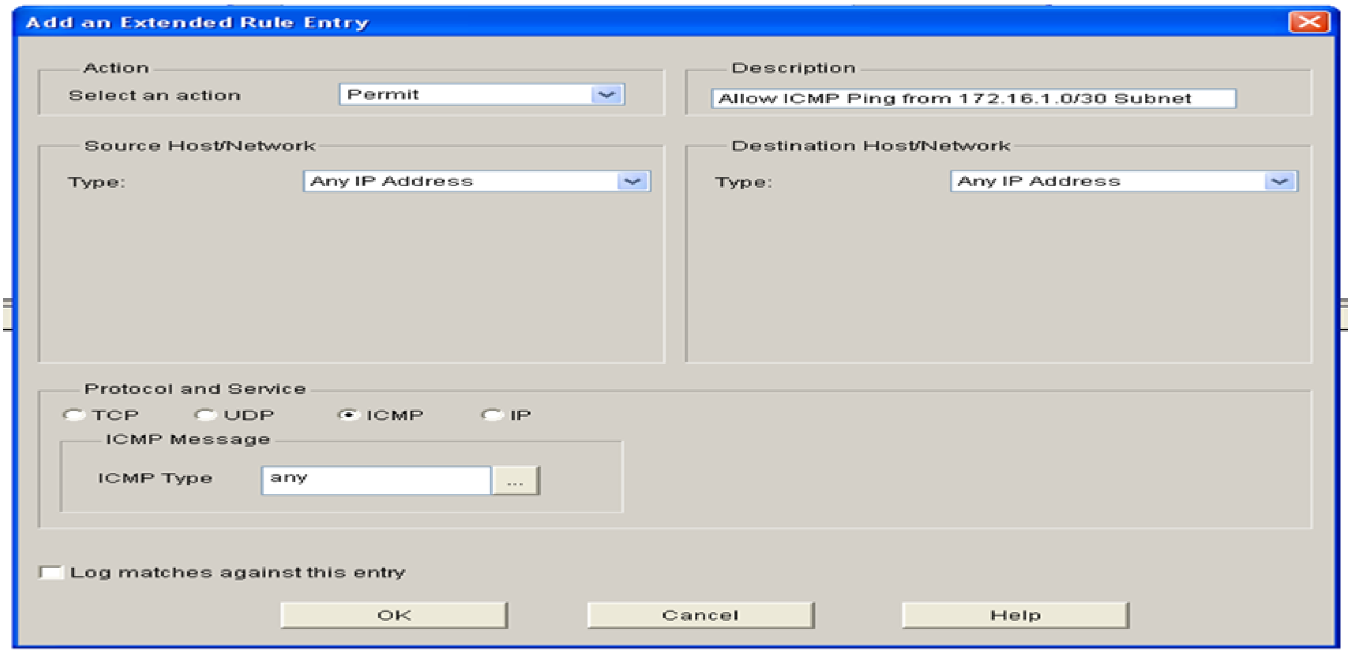
Name/Number: 140

Type: Extended Rule

Description:

Interface Association: None.

5. Next, add a meaningful description and click on **Add** to add a new entry. The first entry we will create will be to permit ICMP ping traffic, so select an action item of **Permit** from the Action drop-down menu.



Select an action: Permit

Description: Allow ICMP Ping from 172.16.1.0/30 Subnet

Source Host/Network Type: Any IP Address

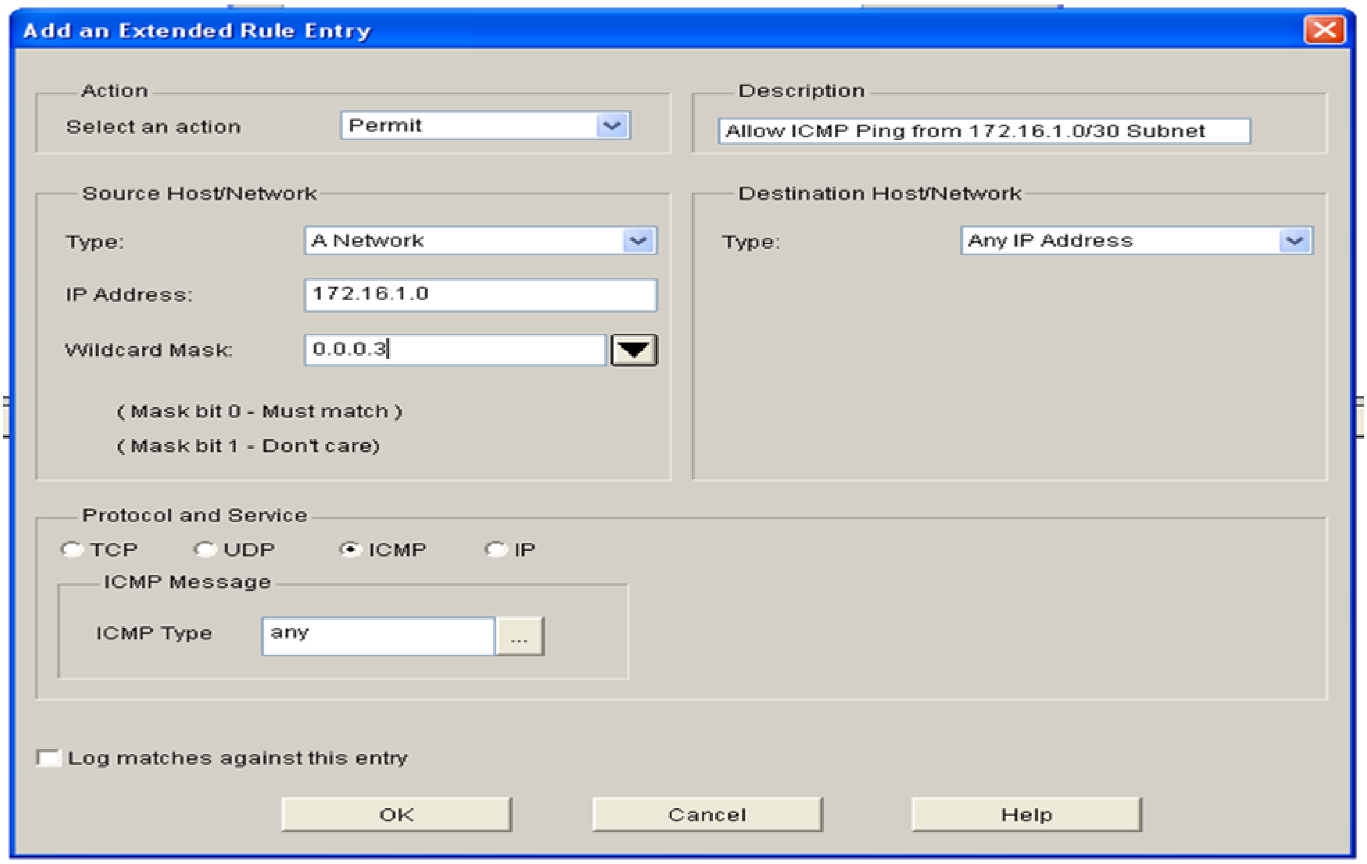
Destination Host/Network Type: Any IP Address

○ TCP ○ UDP ● ICMP ○ IP

ICMP Type: any

□ Log matches against this entry

6. Next, specify the source network of the ICMP pings, which will be 172.16.1.0/30. The destination will be any since we want to allow R2 to ping any interface on SDM-1. Don't forget the wildcard mask.



Add an Extended Rule Entry

Action

Select an action: Permit

Description

Allow ICMP Ping from 172.16.1.0/30 Subnet

Source Host/Network

Type: A Network

IP Address: 172.16.1.0

Wildcard Mask: 0.0.0.3

(Mask bit 0 - Must match)

(Mask bit 1 - Don't care)

Destination Host/Network

Type: Any IP Address

Protocol and Service

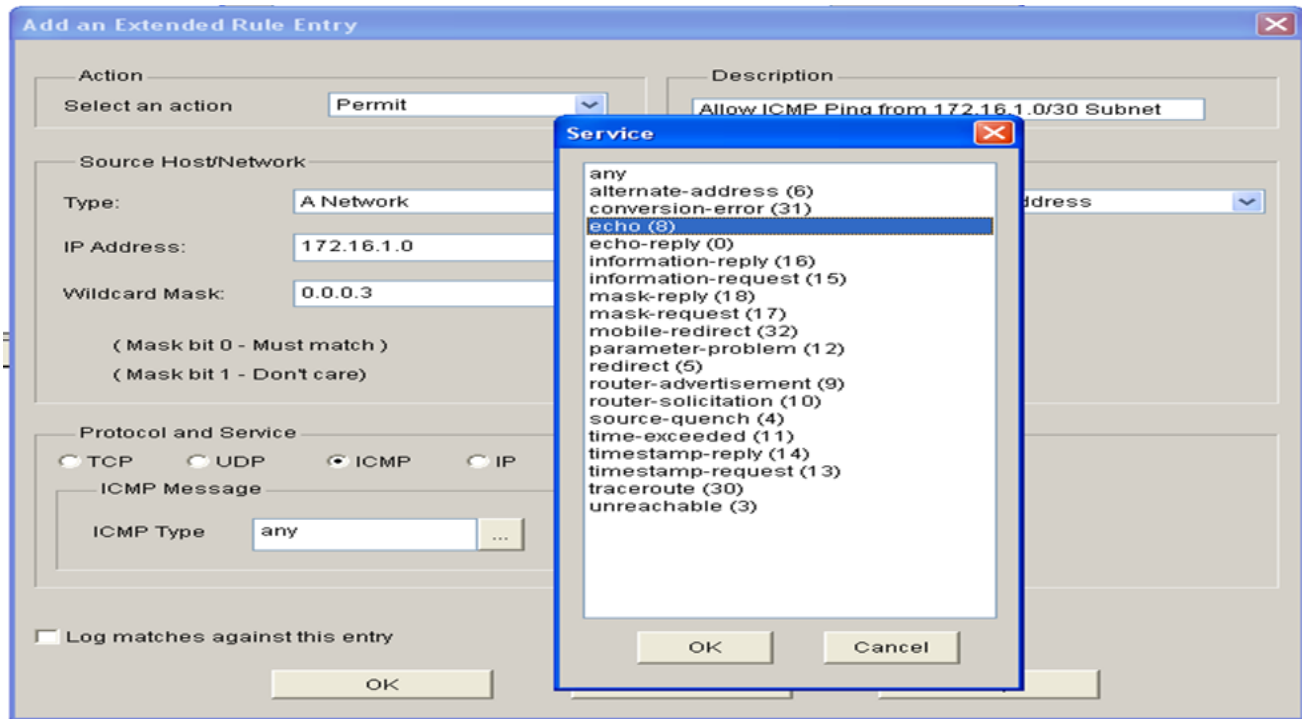
○ TCP ○ UDP ● ICMP ○ IP

ICMP Message

ICMP Type: any

□ Log matches against this entry

7. Next, under the **Protocol and Service** section, click on the radio box that says **ICMP**. For ICMP type, click on the box next to any for a pop-up menu of the different ICMP types.



Add an Extended Rule Entry

Action

Select an action: Permit

Description

Allow ICMP Ping from 172.16.1.0/30 Subnet

Source Host/Network

Type: A Network

IP Address: 172.16.1.0

Wildcard Mask: 0.0.0.3

(Mask bit 0 - Must match)

(Mask bit 1 - Don't care)

Protocol and Service

○ TCP ○ UDP ● ICMP ○ IP

ICMP Message

ICMP Type: any

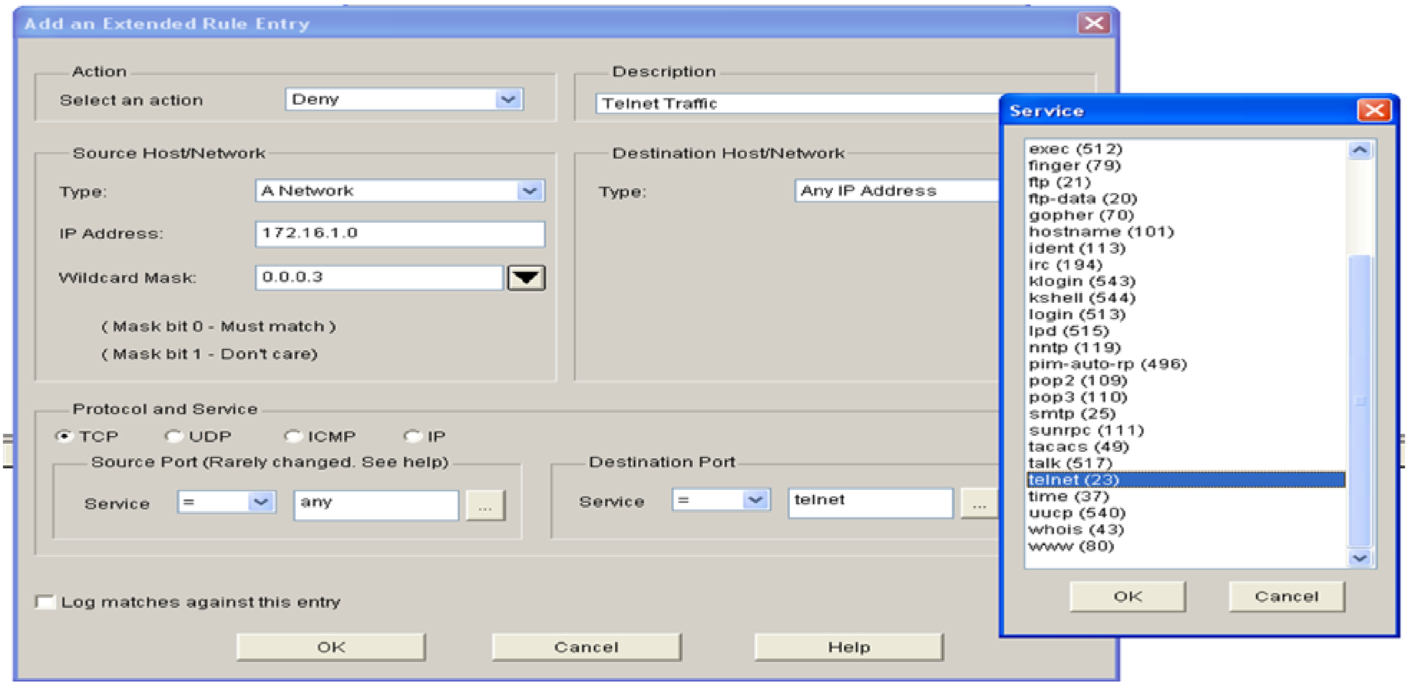
□ Log matches against this entry

Service

any
alternate-address (6)
conversion-error (31)
echo (8)
echo-reply (0)
information-reply (16)
information-request (15)
mask-reply (18)
mask-request (17)
mobile-redirect (32)
parameter-problem (12)
redirect (5)
router-advertisement (9)
router-solicitation (10)
source-quench (4)
time-exceeded (11)
timestamp-reply (14)
timestamp-request (13)
traceroute (30)
unreachable (3)

8. Select **echo (8)** and click **OK**. Repeat steps 6 and 7 and add **echo-reply (0).** Click **OK** when complete.

9. Repeat the same steps to create a deny statement in the ACL for Telnet traffic.



Add an Extended Rule Entry

Action — Select an action: Deny

Description: Telnet Traffic

Source Host/Network — Type: A Network; IP Address: 172.16.1.0; Wildcard Mask: 0.0.0.3

(Mask bit 0 - Must match)
(Mask bit 1 - Don't care)

Destination Host/Network — Type: Any IP Address

Protocol and Service — ● TCP ○ UDP ○ ICMP ○ IP

Source Port (Rarely changed. See help) — Service = any

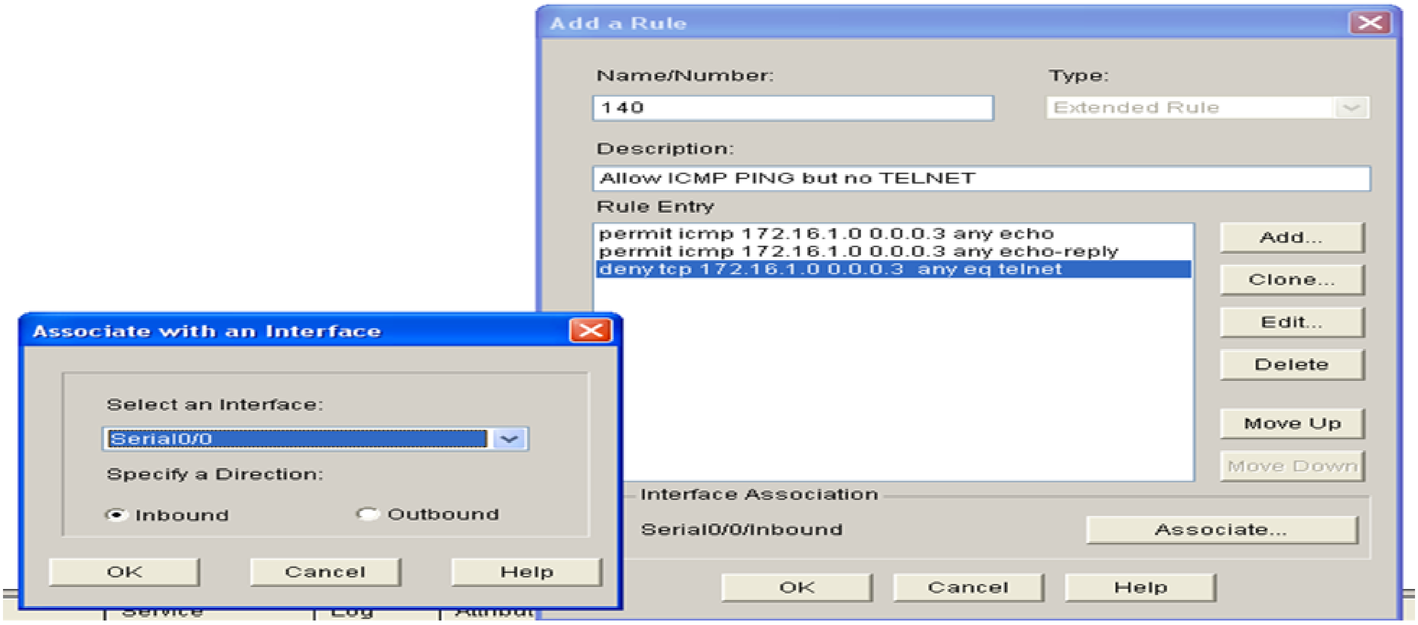
Destination Port — Service = telnet

□ Log matches against this entry

10.After you are done, click **Associate** on the next configuration screen to associate the ACL with an interface.

11.Select **Serial0/0** in the **Select an Interface** screen and ensure that direction is inbound. Click **OK**.

12.Click **OK** again and the configuration will be sent to the router.



Add a Rule

Name/Number: 140

Type: Extended Rule

Description: Allow ICMP PING but no TELNET

Rule Entry

```
permit icmp 172.16.1.0 0.0.0.3 any echo
permit icmp 172.16.1.0 0.0.0.3 any echo-reply
deny tcp 172.16.1.0 0.0.0.3  any eq telnet
```

Interface Association: Serial0/0/inbound

Associate with an Interface

Select an Interface: Serial0/0

Specify a Direction: ● Inbound ○ Outbound

Now, you can try and ping and Telnet from R2. Ping will work, but Telnet will not work as illustrated below. If Telnet is working or ICMP is not working for you, please check your configuration.

```
R2#ping 172.16.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

!!!!!

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

R2#telnet 172.16.1.1

Trying 172.16.1.1 ...

% Destination unreachable; gateway or host down
```

Lab 88 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int fa0/0

R1(config-if)#ip address dhcp

R1(config-if)#end

R1#
```

Task 4:

For reference information on using SDM to configure & verify interfaces, please refer to:

Lab 83 Configuration and Verification Task 4

Lab 83 Configuration and Verification Task 5

Task 5:

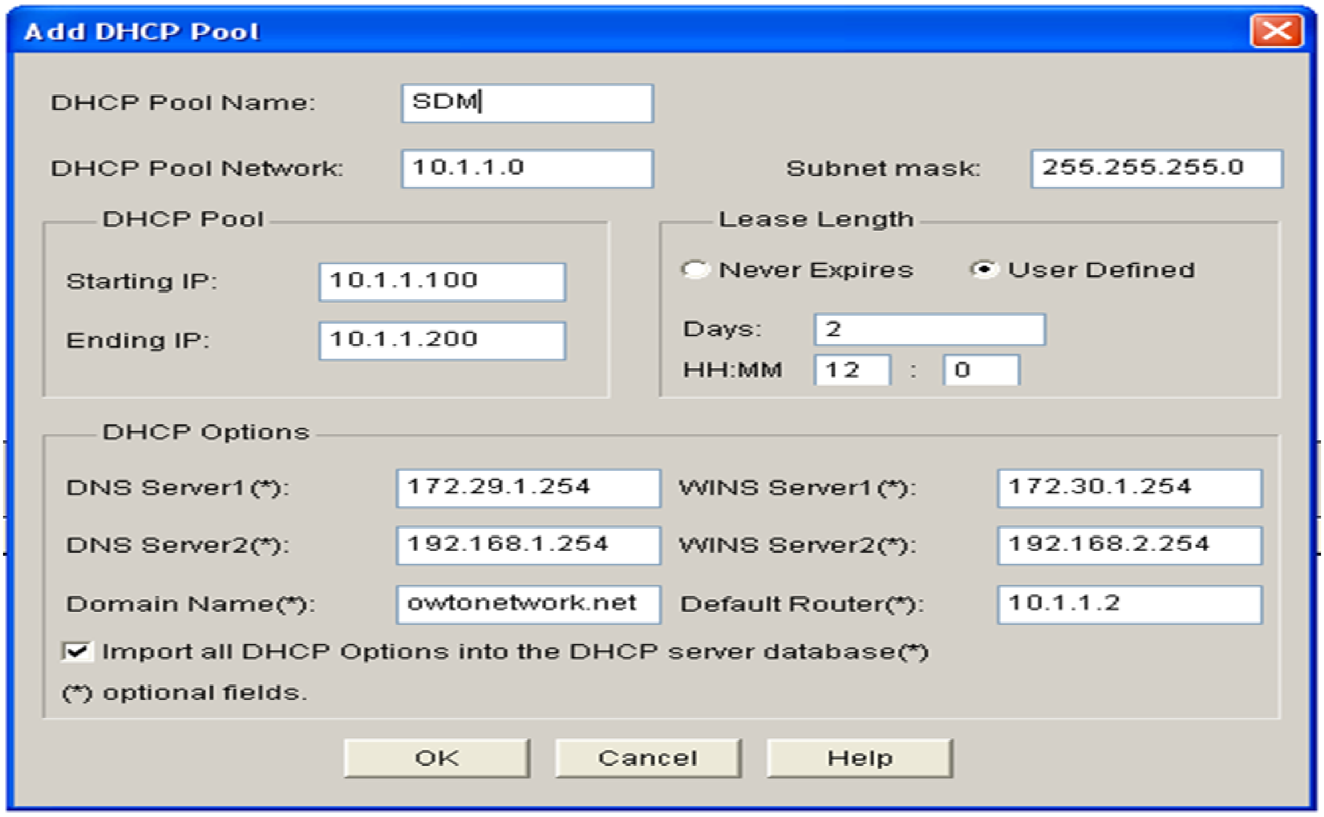
To complete this task you need to navigate to the router properties as follows:

1. On the top menu click on **Configure**.

2. Under Tasks, click on **Additional Tasks**.

3. Next, click on **DHCP** to expand the options and click on **DHCP Pools**.

4. Click on the **Add** in the top right hand corner and type in the relevant DHCP options.



Add DHCP Pool

DHCP Pool Name: SDM

DHCP Pool Network: 10.1.1.0

Subnet mask: 255.255.255.0

DHCP Pool

Starting IP: 10.1.1.100

Ending IP: 10.1.1.200

Lease Length

○ Never Expires ● User Defined

Days: 2

HH:MM 12 : 0

DHCP Options

DNS Server1 (*): 172.29.1.254

WINS Server1 (*): 172.30.1.254

DNS Server2(*): 192.168.1.254

WINS Server2(*): 192.168.2.254

Domain Name(*): owtonetwork.net

Default Router(*): 10.1.1.2

☑ Import all DHCP Options into the DHCP server database(*)

(*) optional fields.

5. Click **OK** when complete.

6. The configuration is copied to the router. Click **OK** to confirm and complete the configuration.

Task 6:

```
R1#

*Mar  1 06:39:20.990: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned
DHCP address 10.1.1.101, mask 255.255.255.0, hostname R1

R1#show dhcp server

   DHCP server: ANY (255.255.255.255)

    Leases:   1

    Offers:   1      Requests: 1     Acks: 1     Naks: 0

    Declines: 0      Releases: 0     Bad:  0

    DNS0:   172.29.1.254,   DNS1:  192.168.1.254

    NBNS0:  172.30.1.254,   NBNS1: 192.168.2.254

    Subnet: 255.255.255.0   DNS Domain: howtonetwork.net
```

Lab 88: Using Cisco SDM to configure Cisco IOS DHCP Server

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure the Dynamic Host Configuration Protocol using Cisco SDM.

Lab Purpose:

Understanding Cisco SDM is a fundamental skill. SDM is a web-based application that can be used to configure routers as well as troubleshoot internetworks. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure the Cisco IOS DHCP server using SDM.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

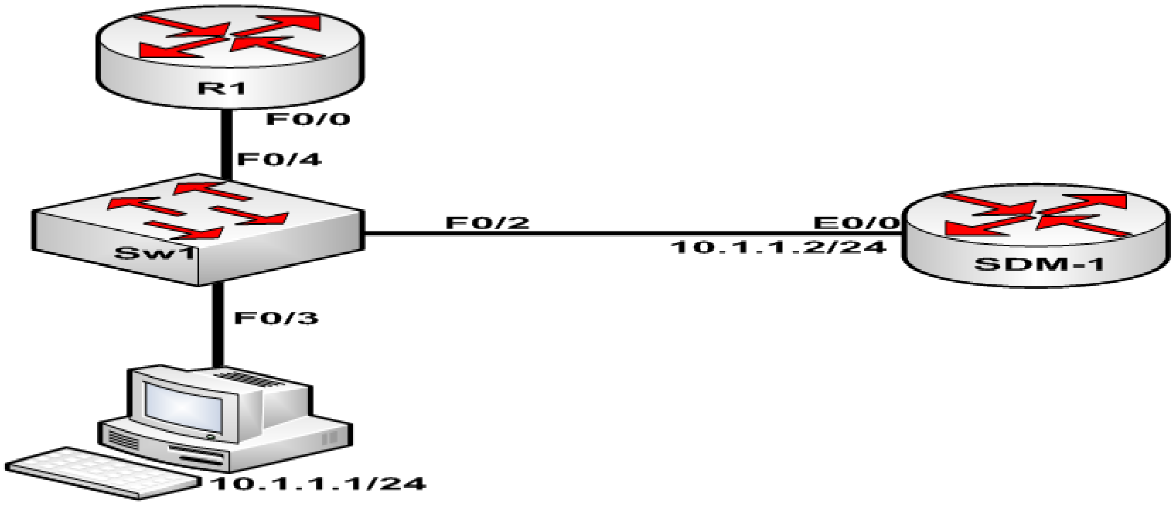
In order to use SDM, you must have an SDM-capable router. The following routers support SDM:

- Cisco Small Business 101, 106, and 107
- Cisco 1701, 1710, 1711, 1712, 1721, 1751, 1751-V, 1760 and 1870V
- Cisco 1801, 1802, 1803, 1811, and 1812
- Cisco 1841
- Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and Cisco 2691 Multiservice Routers
- Cisco 2801, 2811, 2821, and 2851
- Cisco 3620, 3640, 3661, and 3662
- Cisco 3725 and 3745
- Cisco 3825 and 3845
- Cisco 7204VXR, 7206VXR and 7301

The objective of this lab exercise is to familiarize your with the SDM GUI and how to navigate through it. As long as you have one of the platforms listed above, the configuration tasks and GUI navigation will be the same. These lab exercises are based on a Cisco 3640 router with two 10Mbps Ethernet interfaces and two Serial interfaces, but can be completed on any one of the above routers with similar interfaces. Substitute the interfaces in these lab exercises with the ones you have on your router.

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure hostnames on Sw1 and R1 as illustrated in the topology.

Task 2:

Configure VLAN 4000 on Sw1 and assign it the name SDM_VLAN. Next, configure the E0/0 interface of SDM-1 with the IP address of 10.1.1.2/24. Ensure that the PC has the IP address 10.1.1.1/24 configured on the correct NIC. Assign ports FastEthernet0/2 – FastEthernet0/4 to VLAN 4000.

Task 3:

Configure R1 F0/0 to receive IP address information via DHCP.

Task 4:

Using SDM, configure the S0/0 interface of SDM-1 with the IP address specified in the topology. Ping and. Telnet from R2 to SDM-1 and verify that this works.

Task 5:

Using SDM, configure a DHCP pool called SDM on router SDM-1 with the following parameters:

Network:	10.1.1.0/24. The addresses that DHCP should lease must be 10.1.1.100 - 10.1.1.200
Domain:	howtonetwork.net
DNS:	172.29.1.254 and 192.168.1.254
WINS:	172.30.1.254 and 192.168.2.254
Lease:	2 days 12 hours
Gateway:	10.1.1.2

Task 6:

Verify your DHCP configuration using SDM and on router R1.

SOLUTION:

Lab 88 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

```
R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int fa0/0

R1(config-if)#ip address dhcp

R1(config-if)#end

R1#
```

Task 4:

For reference information on using SDM to configure & verify interfaces, please refer to:

Lab 83 Configuration and Verification Task 4

Lab 83 Configuration and Verification Task 5

Task 5:

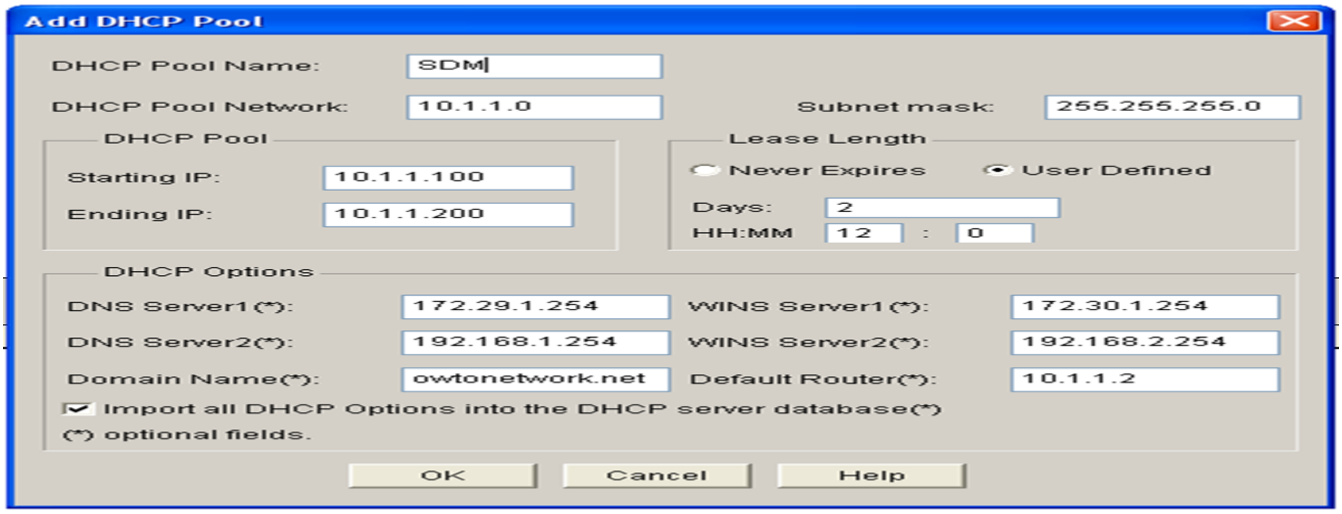
To complete this task you need to navigate to the router properties as follows:

1. On the top menu click on **Configure**.

2. Under Tasks, click on **Additional Tasks**.

3. Next, click on **DHCP** to expand the options and click on **DHCP Pools**.

4. Click on the **Add** in the top right hand corner and type in the relevant DHCP options.



DHCP Pool Name: SDM

DHCP Pool Network: 10.1.1.0

Subnet mask: 255.255.255.0

DHCP Pool

Starting IP: 10.1.1.100

Ending IP: 10.1.1.200

Lease Length

○ Never Expires ● User Defined

Days: 2

HH:MM 12 : 0

DHCP Options

DNS Server1(*): 172.29.1.254

WINS Server1(*): 172.30.1.254

DNS Server2(*): 192.168.1.254

WINS Server2(*): 192.168.2.254

Domain Name(*): owtonetwork.net

Default Router(*): 10.1.1.2

☑ Import all DHCP Options into the DHCP server database(*)

(*) optional fields.

5. Click **OK** when complete.

6. The configuration is copied to the router. Click **OK** to confirm and complete the configuration.

Task 6:

```
R1#

*Mar  1 06:39:20.990: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned
DHCP address 10.1.1.101, mask 255.255.255.0, hostname R1

R1#show dhcp server

   DHCP server: ANY (255.255.255.255)

    Leases:   1

    Offers:   1      Requests: 1     Acks: 1     Naks: 0

    Declines: 0      Releases: 0     Bad:  0

    DNS0:   172.29.1.254,   DNS1:  192.168.1.254

    NBNS0:  172.30.1.254,   NBNS1: 192.168.2.254

    Subnet: 255.255.255.0   DNS Domain: howtonetwork.net
```

Lab 89: Using Cisco SDM to configure DNS servers

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure the router to communicate with a DNS server via Cisco SDM.

Lab Purpose:

Understanding Cisco SDM is a fundamental skill. SDM is a web-based application that can be used to configure routers as well as troubleshoot internetworks. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure Domain Name Service using SDM.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

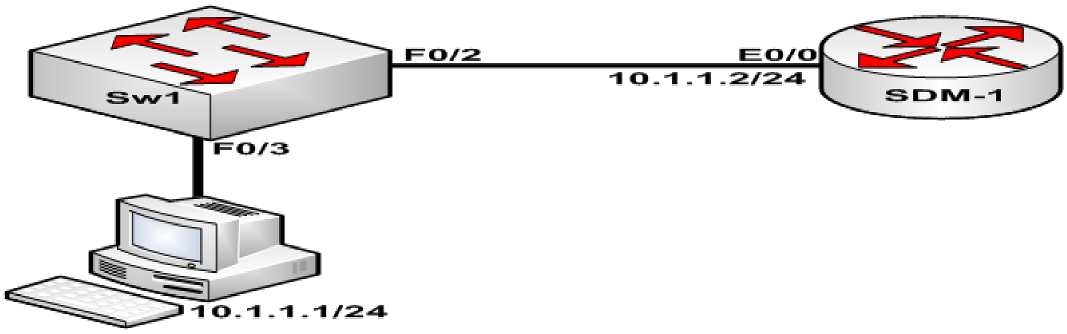
In order to use SDM, you must have an SDM-capable router. The following routers support SDM:

- Cisco Small Business 101, 106, and 107
- Cisco 1701, 1710, 1711, 1712, 1721, 1751, 1751-V, 1760 and 1870V
- Cisco 1801, 1802, 1803, 1811, and 1812
- Cisco 1841
- Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and Cisco 2691 Multiservice Routers
- Cisco 2801, 2811, 2821, and 2851
- Cisco 3620, 3640, 3661, and 3662
- Cisco 3725 and 3745
- Cisco 3825 and 3845
- Cisco 7204VXR, 7206VXR and 7301

The objective of this lab exercise is to familiarize your with the SDM GUI and how to navigate through it. As long as you have one of the platforms listed above, the configuration tasks and GUI navigation will be the same. These lab exercises are based on a Cisco 3640 router with two 10Mbps Ethernet interfaces and two Serial interfaces, but can be completed on any one of the above routers with similar interfaces. Substitute the interfaces in these lab exercises with the ones you have on your router.

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure the hostname on Sw1 as illustrated in the topology.

Task 2:

Configure VLAN 4000 on Sw1 and assign it the name SDM_VLAN. Next, configure the E0/0 interface of SDM-1 with the IP address of 10.1.1.2/24. Ensure that the PC has the IP address 10.1.1.1/24 configured on the correct NIC. Assign ports FastEthernet0/2 and FastEthernet0/3 to VLAN 4000.

Task 3:

Using SDM, configure SDM-1 to send DNS requests to servers 10.254.1.1 and 10.254.2.2.

SOLUTION:

Lab 89 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

To complete this task you need to navigate to the router properties as follows:

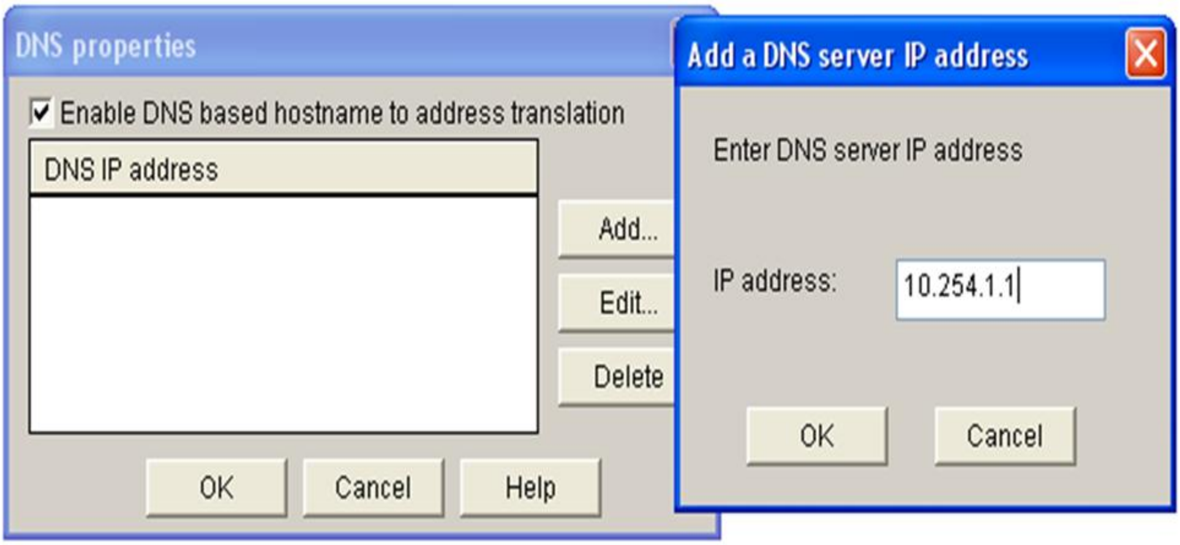
1. On the top menu click on **Configure**.

2. Under Tasks, click on **Additional Tasks**.

3. Next, click on **DNS**

4. Click on the **Add** in the top right hand corner.

5. On the **DNS Properties** pop-up page, click **Add** to add a new DNS server.



☑ Enable DNS based hostname to address translation

IP address: 10.254.1.1

6. Click **OK** when done and repeat the same steps to add the second DNS server.

Lab 90: Using Cisco SDM to configure Network Address Translation

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure static Network Address Translation using Cisco SDM.

Lab Purpose:

Understanding Cisco SDM is a fundamental skill. SDM is a web-based application that can be used to configure routers as well as troubleshoot internetworks. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure Network Address Translation using SDM.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

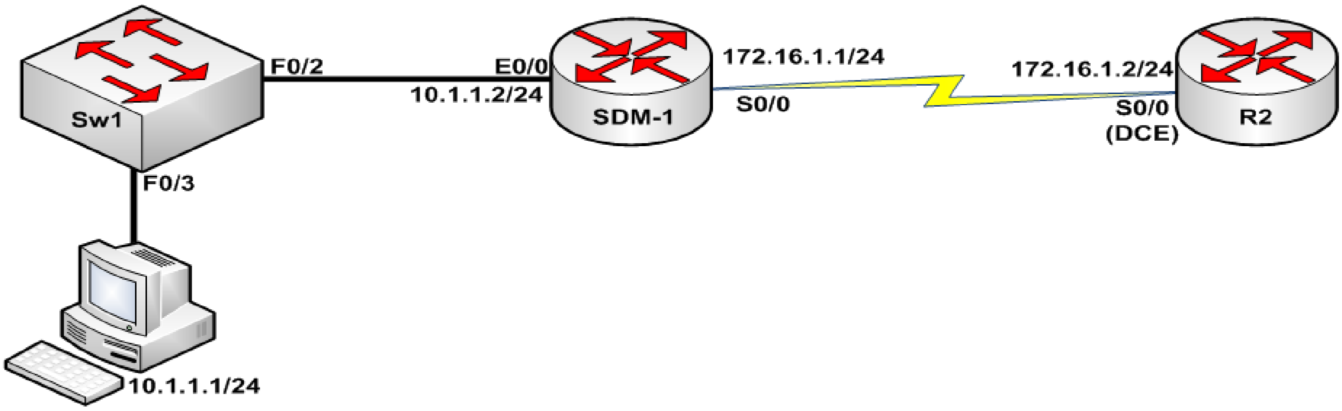
In order to use SDM, you must have an SDM-capable router. The following routers support SDM:

- Cisco Small Business 101, 106, and 107
- Cisco 1701, 1710, 1711, 1712, 1721, 1751, 1751-V, 1760 and 1870V
- Cisco 1801, 1802, 1803, 1811, and 1812
- Cisco 1841
- Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and Cisco 2691 Multiservice Routers
- Cisco 2801, 2811, 2821, and 2851
- Cisco 3620, 3640, 3661, and 3662
- Cisco 3725 and 3745
- Cisco 3825 and 3845
- Cisco 7204VXR, 7206VXR and 7301

The objective of this lab exercise is to familiarize your with the SDM GUI and how to navigate through it. As long as you have one of the platforms listed above, the configuration tasks and GUI navigation will be the same. These lab exercises are based on a Cisco 3640 router with two 10Mbps Ethernet interfaces and two Serial interfaces, but can be completed on any one of the above routers with similar interfaces. Substitute the interfaces in these lab exercises with the ones you have on your router.

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure the hostname on Sw1 as illustrated in the topology.

Task 2:

Configure VLAN 4000 on Sw1 and assign it the name SDM_VLAN. Next, configure the E0/0 interface of SDM-1 with the IP address of 10.1.1.2/24. Ensure that the PC has the IP address 10.1.1.1/24 configured on the correct NIC. Assign ports FastEthernet0/2 and FastEthernet0/3 to VLAN 4000. Configure an IP address of 10.1.1.254 on interface VLAN 4000 on Sw1.

Task 3:

Using the CLI configure the S0/0 interface of R2 with the IP address specified in the topology. Enable this interface and provide clocking to SDM-1 at 2Mbps.

Task 4:

Using SDM, configure the S0/0 interface of SDM-1 with the IP address specified in the topology. Ping from R2 to SDM-1 and verify that this works. Try to ping and Telnet to the 10.1.1.254 address assigned to Sw1 interface VLAN 4000 from R2. At this point, neither will work because there is no route to the 10.1.1.0/24 subnet.

Task 5:

Using SDM, configure the S0/0 interface of SDM-1 as the NAT outside interface and the E0/0 interface as the NAT inside interface. In addition, configure a static NAT translation for 10.1.1.254 to 172.16.1.254 for Telnet ONLY.

Task 6:

To test and validate your configuration, Telnet to IP address 172.16.1.254 from R2. Based on your NAT configuration, verify that you are connected to Sw1.

SOLUTION:

Lab 90 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

For reference information on configuring DCE clocking, please refer to:

Lab 21 Configuration and Verification Task 2

Lab 35 Configuration and Verification Task 2

For reference information on configuring IP interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

Lab 56 Configuration and Verification Task 2

Task 4:

For reference information on using SDM to configure & verify interfaces, please refer to:

Lab 83 Configuration and Verification Task 4

Lab 83 Configuration and Verification Task 5

```
R2#ping 172.16.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

!!!!!

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

R2#ping 10.1.1.254

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.254, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

R2#telnet 10.1.1.254

Trying 10.1.1.254 ...

% Destination unreachable; gateway or host down
```

Task 5:

To complete this task you need to navigate to the router properties as follows:

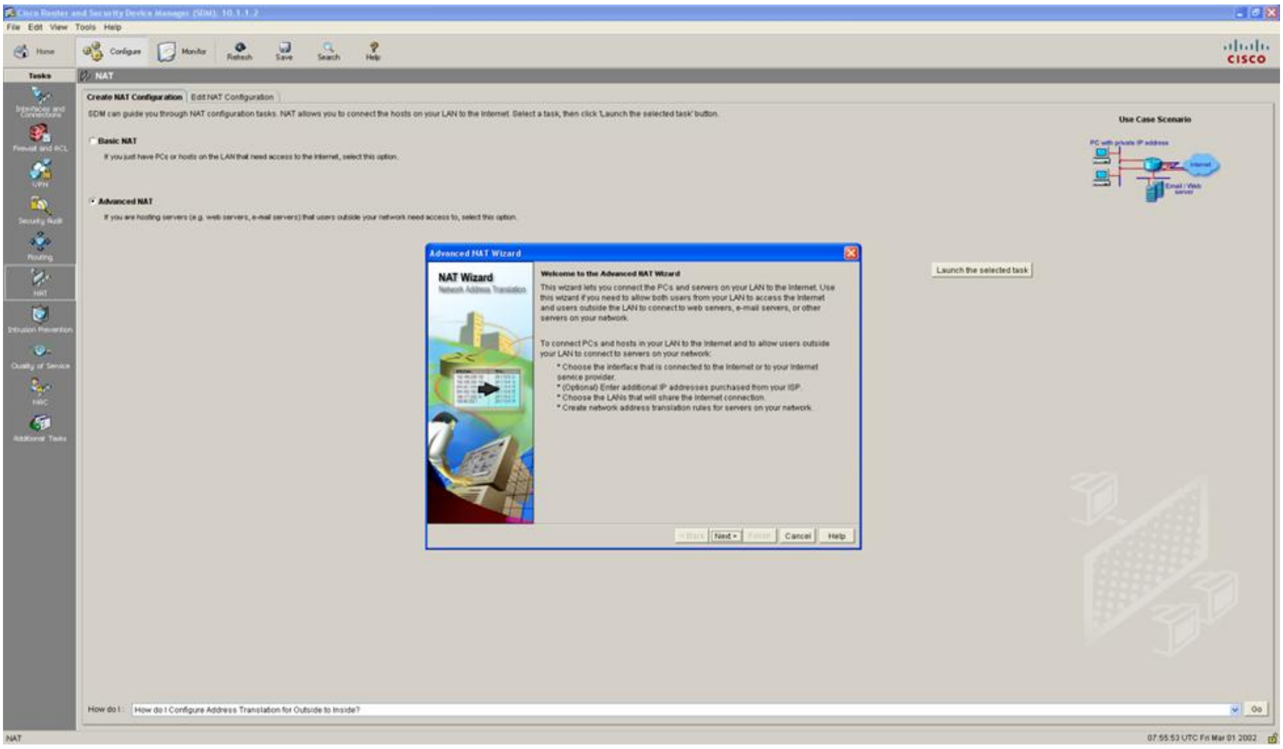
1. On the top menu click on **Configure**.

2. Under Tasks, click on **NAT**.

3. Next, click on the **Create NAT Configuration** tab.

4. Click on the **Advanced NAT** radio box.

5. Next, Click the **Launch the selected task** button to launch the Wizard.



Cisco Router and Security Device Manager (SDM): 10.1.1.2
File Edit View Tools Help
Home Configure Monitor Refresh Save Search Help
Tasks
NAT
Create NAT Configuration
Edit NAT Configuration
Use Case Scenario
Launch the selected task
< Back
Next >
Finish
Cancel
Help

SDM can guide you through NAT configuration tasks. NAT allows you to connect the hosts on your LAN to the Internet. Select a task, then click 'Launch the selected task' button.

○ Basic NAT

If you just have PCs or hosts on the LAN that need access to the Internet, select this option.

● Advanced NAT

If you are hosting servers (e.g. web servers, e-mail servers) that users outside your network need access to, select this option.

Advanced NAT Wizard

NAT Wizard
Network Address Translation

Welcome to the Advanced NAT Wizard

This wizard lets you connect the PCs and servers on your LAN to the Internet. Use this wizard if you need to allow both users from your LAN to access the Internet and users outside the LAN to connect to web servers, e-mail servers, or other servers on your network.

To connect PCs and hosts in your LAN to the Internet and to allow users outside your LAN to connect to servers on your network:

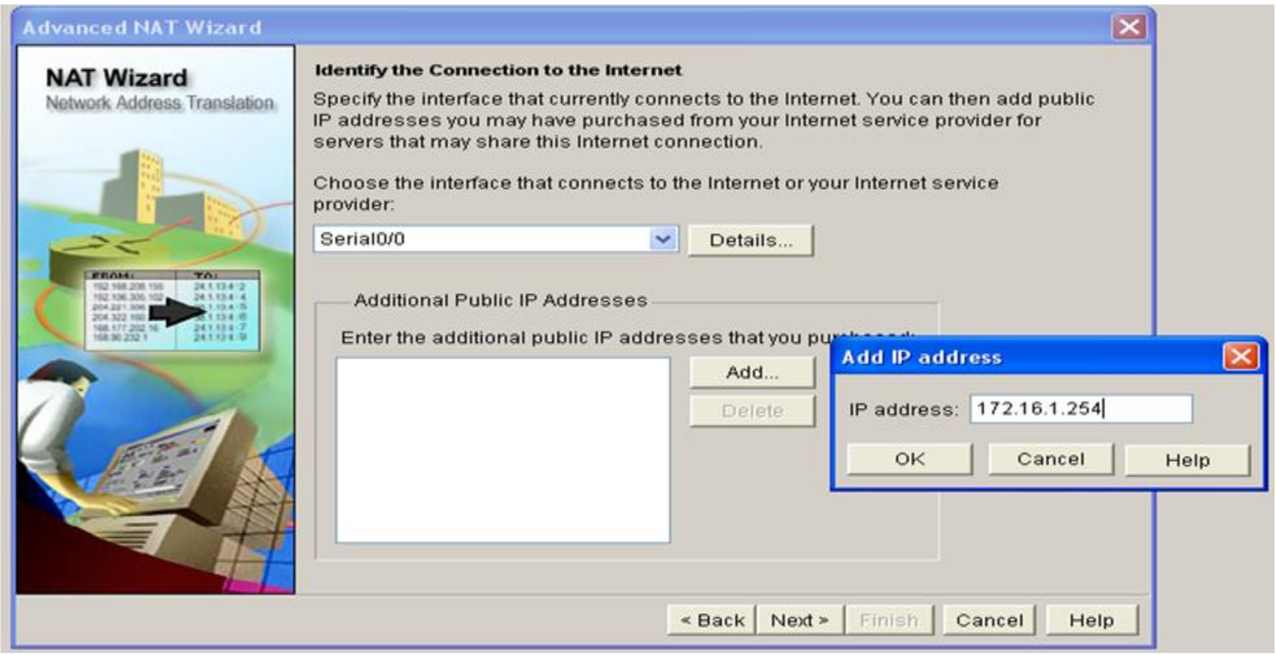
* Choose the interface that is connected to the Internet or to your Internet service provider.
* (Optional) Enter additional IP addresses purchased from your ISP.
* Choose the LANs that will share the Internet connection.
* Create network address translation rules for servers on your network.

How do I: How do I Configure Address Translation for Outside to Inside?

6. Click on **Next**

7. Leave the drop-down menu for your Internet interface at Serial0/0

8. Click on **Add** to add an additional public IP addres and type in 172.16.1.254 which we will use for static NAT.



Identify the Connection to the Internet

Specify the interface that currently connects to the Internet. You can then add public IP addresses you may have purchased from your Internet service provider for servers that may share this Internet connection.

Choose the interface that connects to the Internet or your Internet service provider:

Serial0/0

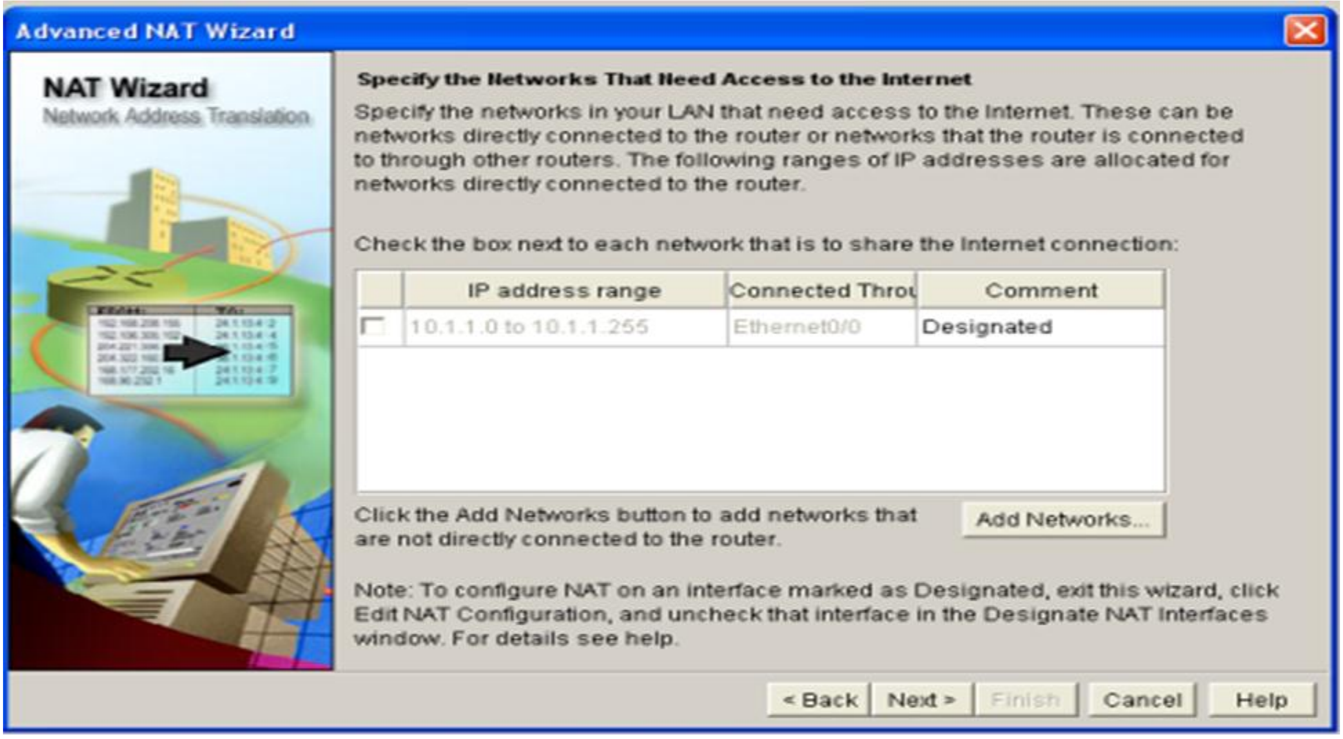
Additional Public IP Addresses

Enter the additional public IP addresses that you pu

IP address: 172.16.1.254

9. Click on **OK** and click **Next**.

10. Ignore the following page and click **Next**.



Specify the Networks That Need Access to the Internet

Specify the networks in your LAN that need access to the Internet. These can be networks directly connected to the router or networks that the router is connected to through other routers. The following ranges of IP addresses are allocated for networks directly connected to the router.

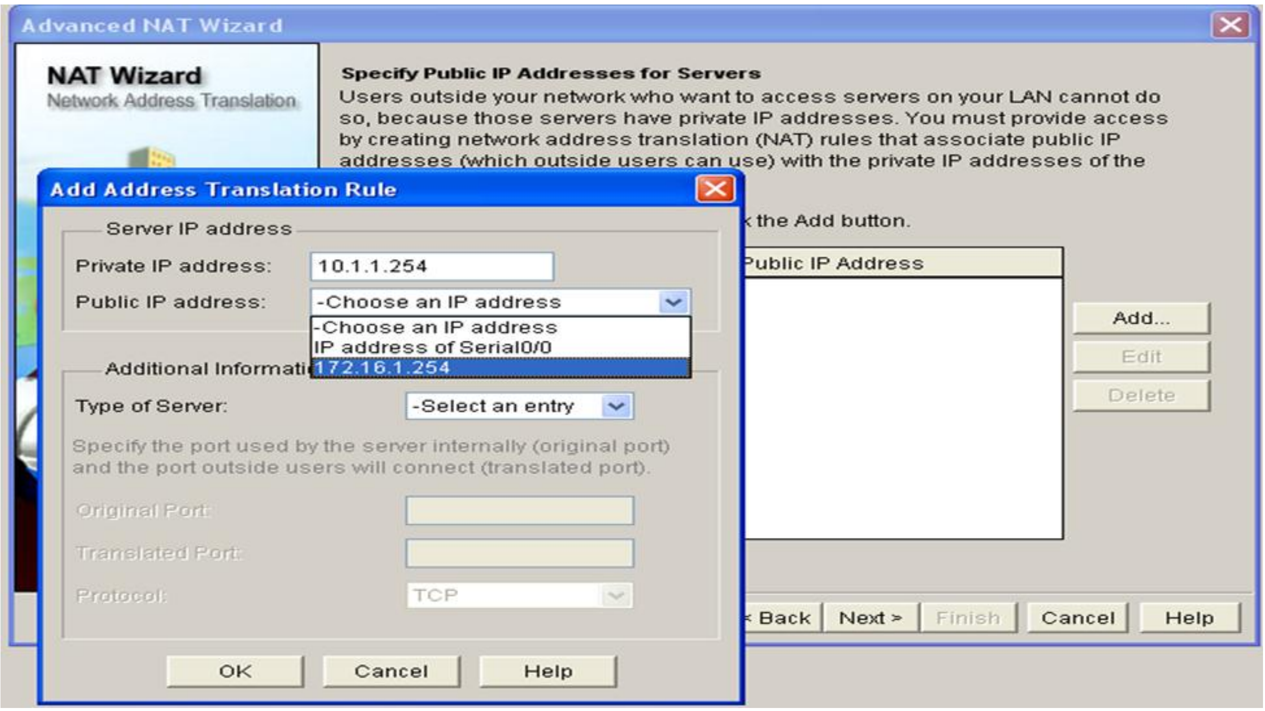
Check the box next to each network that is to share the Internet connection:

	IP address range	Connected Throu	Comment
□	10.1.1.0 to 10.1.1.255	Ethernet0/0	Designated

Click the Add Networks button to add networks that are not directly connected to the router.

Note: To configure NAT on an interface marked as Designated, exit this wizard, click Edit NAT Configuration, and uncheck that interface in the Designate NAT Interfaces window. For details see help.

11. On the Specify Publick IP addresses for Servers page, click **Add**. In the **Private IP address** space put in the private IP address of 10.1.1.254. In the Public IP address drop-down menu, select the IP address 172.16.1.254 we created earlier.



Specify Public IP Addresses for Servers

Users outside your network who want to access servers on your LAN cannot do so, because those servers have private IP addresses. You must provide access by creating network address translation (NAT) rules that associate public IP addresses (which outside users can use) with the private IP addresses of the

the Add button.

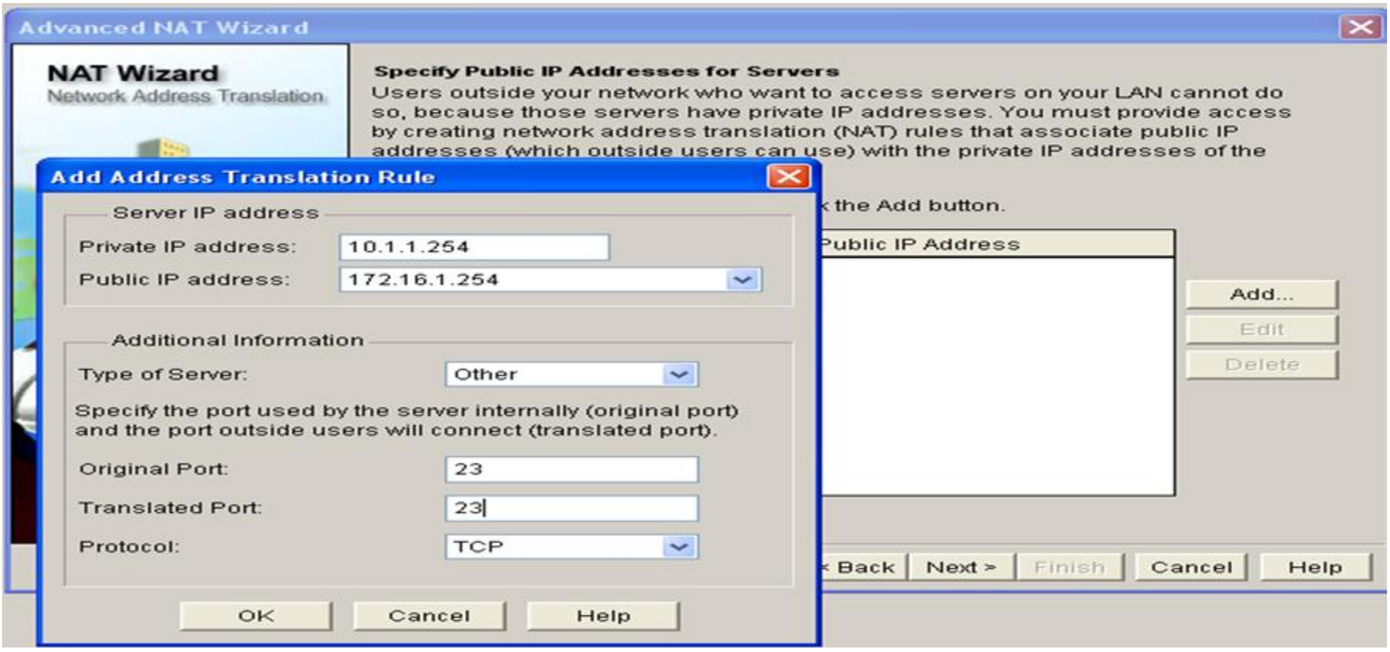
Private IP address: 10.1.1.254

Public IP address: -Choose an IP address

Type of Server: -Select an entry

Specify the port used by the server internally (original port) and the port outside users will connect (translated port).

12. Under **Type of Server** select Other. For **Original Port** and **Translated Port** type in 23 and for **Protocol** select **TCP**. We are doing this because we are configuring Telnet access to Sw1. Telnet uses TCP port 23.



Advanced NAT Wizard

NAT Wizard
Network Address Translation

Specify Public IP Addresses for Servers
Users outside your network who want to access servers on your LAN cannot do so, because those servers have private IP addresses. You must provide access by creating network address translation (NAT) rules that associate public IP addresses (which outside users can use) with the private IP addresses of the

k the Add button.

Public IP Address

Add Address Translation Rule

Server IP address

Private IP address: 10.1.1.254

Public IP address: 172.16.1.254

Additional Information

Type of Server: Other

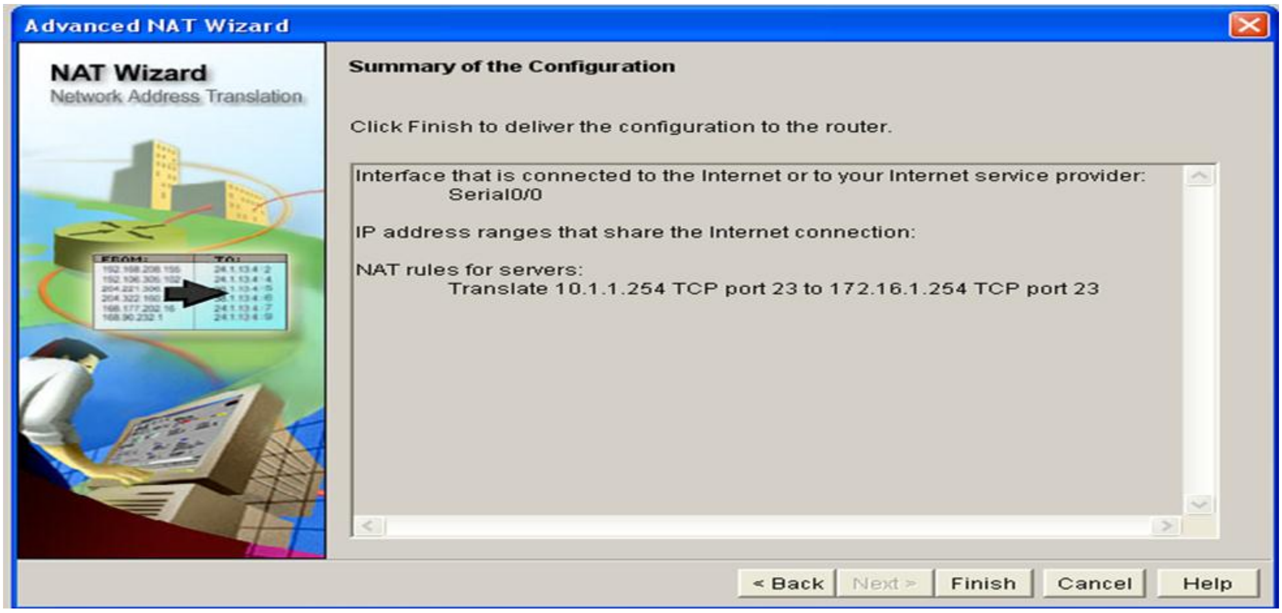
Specify the port used by the server internally (original port) and the port outside users will connect (translated port).

Original Port: 23

Translated Port: 23

Protocol: TCP

13. Click **OK** and then click **Next**. You will arrive at the screen below. Click on the **Finish** button to complete your configuration and SDM will copy and save it to the router. Your NAT configuration is complete.



Advanced NAT Wizard

NAT Wizard
Network Address Translation

Summary of the Configuration

Click Finish to deliver the configuration to the router.

```
Interface that is connected to the Internet or to your Internet service provider:
        Serial0/0

IP address ranges that share the Internet connection:

NAT rules for servers:
        Translate 10.1.1.254 TCP port 23 to 172.16.1.254 TCP port 23
```

Task 6:

R2#**telnet 172.16.1.254**

Trying 172.16.1.254 ... Open

User Access Verification

```
Password:

Sw1>
```

Lab 91: Using Cisco SDM to configure Port Address Translation

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure Port Address Translation using Cisco SDM.

Lab Purpose:

Understanding Cisco SDM is a fundamental skill. SDM is a web-based application that can be used to configure routers as well as troubleshoot internetworks. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure Port Address Translation using SDM.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

In order to use SDM, you must have an SDM-capable router. The following routers support SDM:

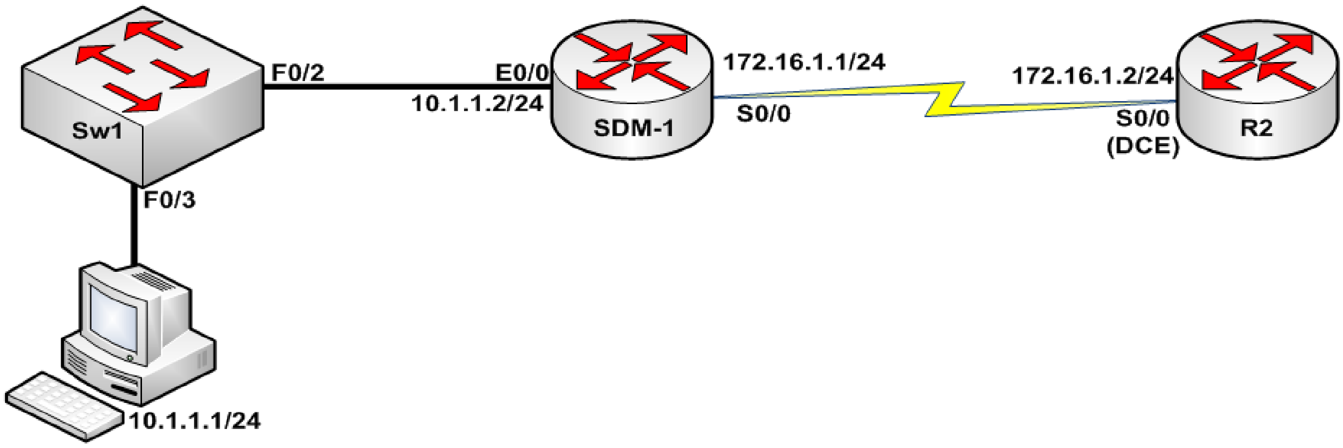
- Cisco Small Business 101, 106, and 107
- Cisco 1701, 1710, 1711, 1712, 1721, 1751, 1751-V, 1760 and 1870V
- Cisco 1801, 1802, 1803, 1811, and 1812
- Cisco 1841
- Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and Cisco 2691 Multiservice Routers
- Cisco 2801, 2811, 2821, and 2851
- Cisco 3620, 3640, 3661, and 3662

- Cisco 3725 and 3745
- Cisco 3825 and 3845
- Cisco 7204VXR, 7206VXR and 7301

The objective of this lab exercise is to familiarize your with the SDM GUI and how to navigate through it. As long as you have one of the platforms listed above, the configuration tasks and GUI navigation will be the same. These lab exercises are based on a Cisco 3640 router with two 10Mbps Ethernet interfaces and two Serial interfaces, but can be completed on any one of the above routers with similar interfaces. Substitute the interfaces in these lab exercises with the ones you have on your router.

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure the hostname on Sw1 as illustrated in the topology.

Task 2:

Configure VLAN 25 on Sw1 and assign it the name SDM_VLAN. Next, configure the E0/0 interface of SDM-1 with the IP address of 10.1.1.2/24. Ensure that the PC has the IP address 10.1.1.1/24 configured on the correct NIC. Assign ports FastEthernet0/2 and FastEthernet0/3 to VLAN 25. Configure an IP address of 10.1.1.254 on interface VLAN 25 on Sw1.

Task 3:

Using the CLI configure the S0/0 interface of R2 with the IP address specified in the topology. Enable this interface and provide clocking to SDM-1 at 768Kbps.

Task 4:

Using SDM, configure the S0/0 interface of SDM-1 with the IP address specified in the topology. Ping from R2 to SDM-1 and verify that this works. Try to ping and Telnet from Sw1 to R2. At this point, neither will work because there is no route to the 10.1.1.0/24 subnet present on R2.

Task 5:

Using SDM, configure the S0/0 interface of SDM-1 as the NAT outside interface and the E0/0 interface as the NAT inside interface. In addition, configure PAT for the 10.1.1.0/24 subnet to the Serial0/0 interface of SDM-1.

Task 6:

To test your configuration, ping and Telnet to R2 from Sw1. If your configuration is correct, both tests should work.

SOLUTION:

Lab 91 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

For reference information on configuring DCE clocking, please refer to:

Lab 21 Configuration and Verification Task 2

Lab 35 Configuration and Verification Task 2

For reference information on configuring IP interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

Lab 56 Configuration and Verification Task 2

Task 4:

For reference information on using SDM to configure & verify interfaces, please refer to:

Lab 83 Configuration and Verification Task 4

Lab 83 Configuration and Verification Task 5

Task 5:

To complete this task you need to navigate to the router properties as follows:

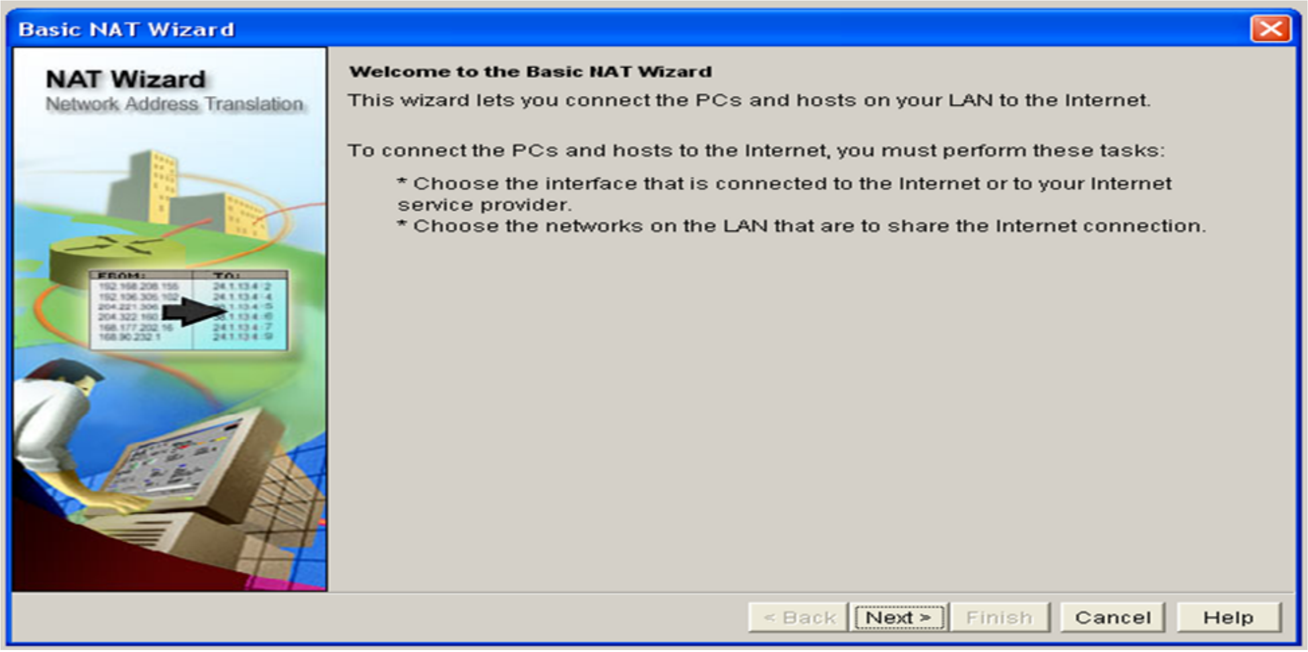
1. On the top menu click on **Configure**.

2. Under Tasks, click on **NAT**.

3. Next, click on the **Create NAT Configuration** tab.

4. Click on the **Basic NAT** radio box.

5. Next, Click the **Launch the selected task** button to launch the Wizard.



Welcome to the Basic NAT Wizard

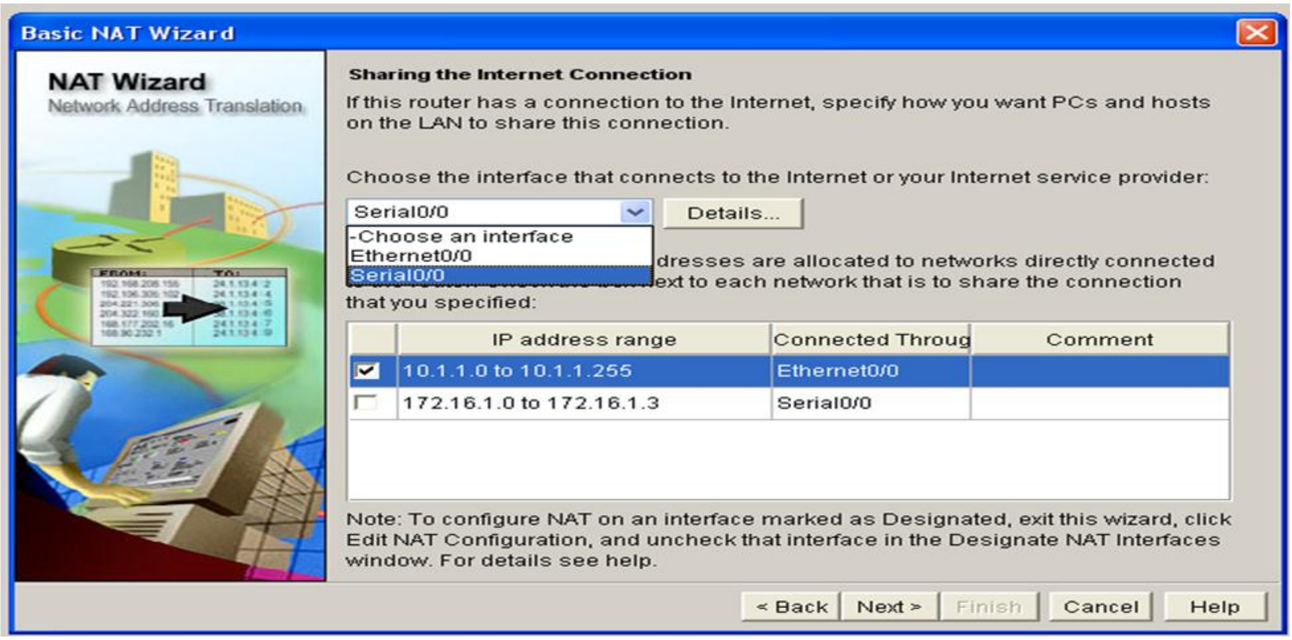
This wizard lets you connect the PCs and hosts on your LAN to the Internet.

To connect the PCs and hosts to the Internet, you must perform these tasks:

* Choose the interface that is connected to the Internet or to your Internet service provider.
* Choose the networks on the LAN that are to share the Internet connection.

6. Click **Next**.

7. On the drop-down menu for the interface that connects to the Internet, select Serial0/0 and then check the box for the Ethernet0/0 subnet, which is our private IP address space. Then click **Next**.



Sharing the Internet Connection

If this router has a connection to the Internet, specify how you want PCs and hosts on the LAN to share this connection.

Choose the interface that connects to the Internet or your Internet service provider:

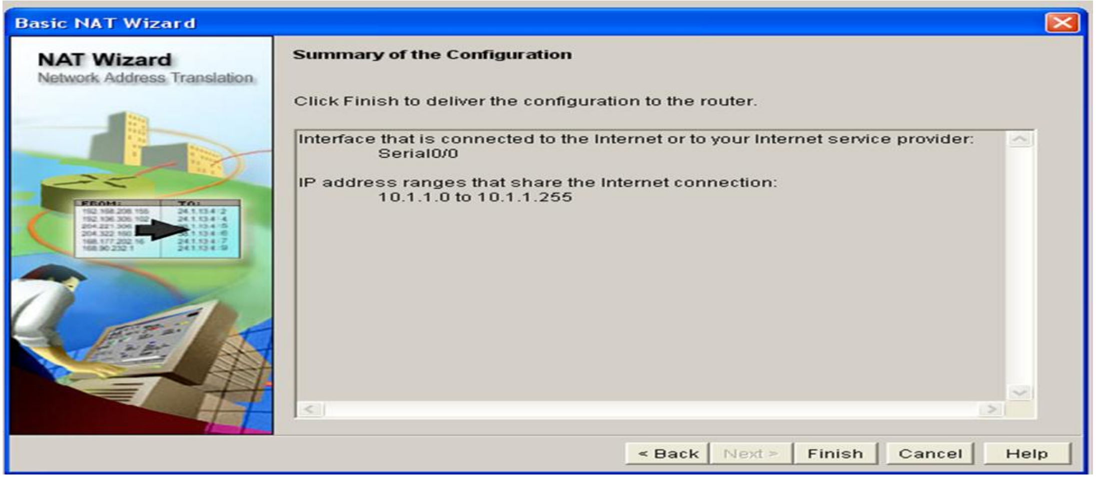
Serial0/0

dresses are allocated to networks directly connected ext to each network that is to share the connection that you specified:

	IP address range	Connected Throug	Comment
☑	10.1.1.0 to 10.1.1.255	Ethernet0/0	
☐	172.16.1.0 to 172.16.1.3	Serial0/0	

Note: To configure NAT on an interface marked as Designated, exit this wizard, click Edit NAT Configuration, and uncheck that interface in the Designate NAT Interfaces window. For details see help.

8. The **Summary of the Configuration** page appears. Click Finish to send the configuration to the router.



Summary of the Configuration

Click Finish to deliver the configuration to the router.

```
Interface that is connected to the Internet or to your Internet service provider:
          Serial0/0

IP address ranges that share the Internet connection:
          10.1.1.0 to 10.1.1.255
```

Task 6:

```
Sw1>ping 172.16.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms

Sw1>telnet 172.16.1.2

Trying 172.16.1.2 ... Open

User Access Verification

Password:

R2#
```

NOTE: If we were to look at the PAT translations on SDM-1 using the CLI, we would see:

```
SDM-1#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 172.16.1.1:1231   10.1.1.254:1231    172.16.1.2:1231    172.16.1.2:1231
icmp 172.16.1.1:1232   10.1.1.254:1232    172.16.1.2:1232    172.16.1.2:1232
icmp 172.16.1.1:1233   10.1.1.254:1233    172.16.1.2:1233    172.16.1.2:1233
icmp 172.16.1.1:1234   10.1.1.254:1234    172.16.1.2:1234    172.16.1.2:1234
icmp 172.16.1.1:1235   10.1.1.254:1235    172.16.1.2:1235    172.16.1.2:1235
```

Lab 92: Using Cisco SDM to manager users, passwords and privileges

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure user and password pairs, as well as assign privileges to users logging onto the router using Cisco SDM.

Lab Purpose:

Understanding Cisco SDM is a fundamental skill. SDM is a web-based application that can be used to configure routers as well as troubleshoot internetworks. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure users, passwords and privileges using SDM.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

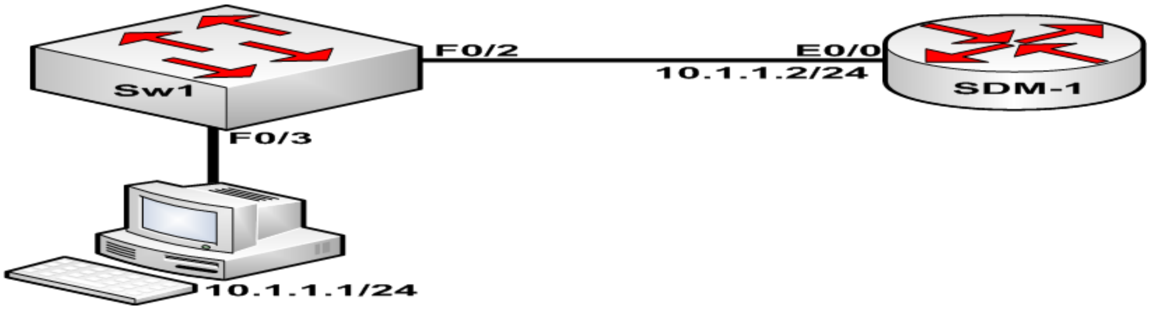
In order to use SDM, you must have an SDM-capable router. The following routers support SDM:

- Cisco Small Business 101, 106, and 107
- Cisco 1701, 1710, 1711, 1712, 1721, 1751, 1751-V, 1760 and 1870V
- Cisco 1801, 1802, 1803, 1811, and 1812
- Cisco 1841
- Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and Cisco 2691 Multiservice Routers
- Cisco 2801, 2811, 2821, and 2851
- Cisco 3620, 3640, 3661, and 3662
- Cisco 3725 and 3745
- Cisco 3825 and 3845
- Cisco 7204VXR, 7206VXR and 7301

The objective of this lab exercise is to familiarize your with the SDM GUI and how to navigate through it. As long as you have one of the platforms listed above, the configuration tasks and GUI navigation will be the same. These lab exercises are based on a Cisco 3640 router with two 10Mbps Ethernet interfaces and two Serial interfaces, but can be completed on any one of the above routers with similar interfaces. Substitute the interfaces in these lab exercises with the ones you have on your router.

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure the hostname on Sw1 as illustrated in the topology.

Task 2:

Configure VLAN 105 on Sw1 and assign it the name SDM_VLAN. Next, configure the E0/0 interface of SDM-1 with the IP address of 10.1.1.2/24. Ensure that the PC has the IP address 10.1.1.1/24 configured on the correct NIC. Assign ports FastEthernet0/2 and FastEthernet0/3 to VLAN 105.

Task 3:

Using SDM, configure the username TESTUSER with a password of TESTPASS. This user should be assigned a privilege level of 15 onto router SDM-1.

SOLUTION:

Lab 92 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

To complete this task you need to navigate to the router properties as follows:

1. On the top menu click on **Configure**.

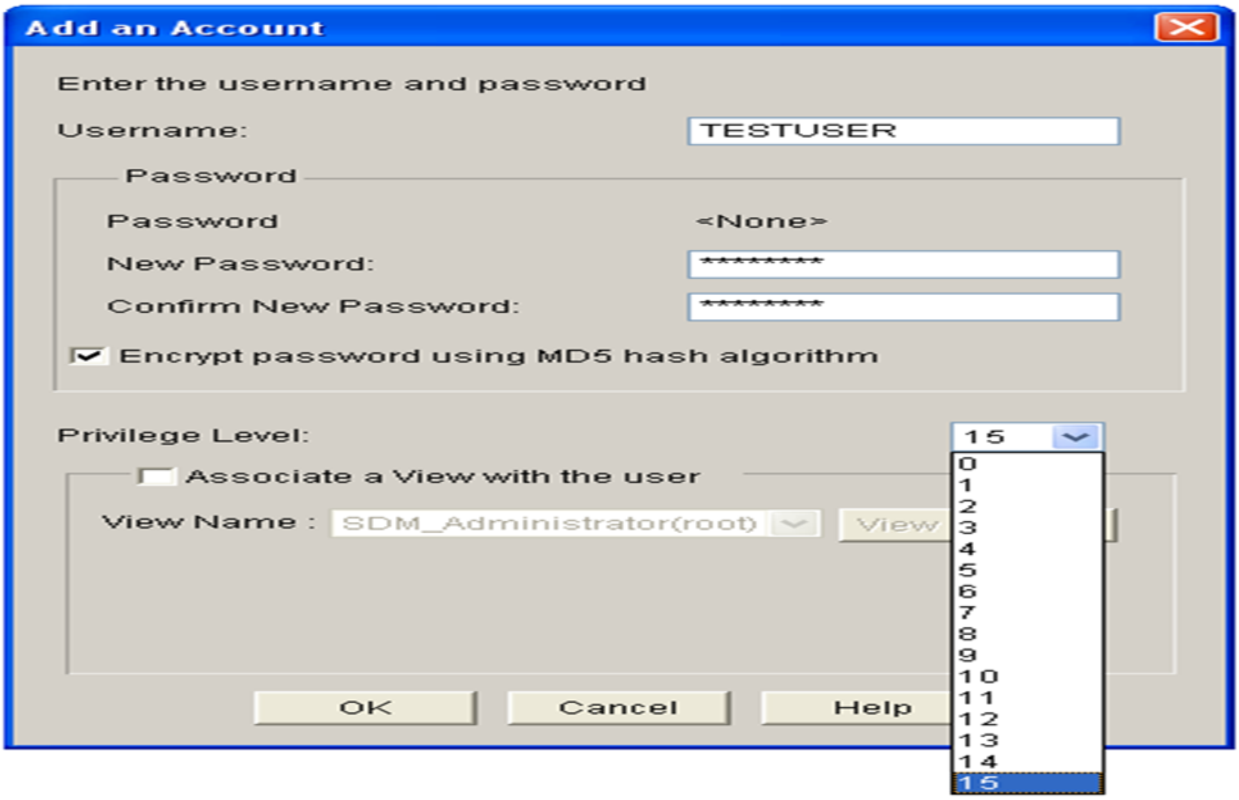
2. Under Tasks, click on **Additional Tasks**.

3. Next, expand the **Router Access** selection.

4. Click on **User Accounts/View**

5. On the right hand side, click **Add**.

6. Enter the username and password and **15** from the Privilege Level drop-down menu. Once complete, click **OK**.



Add an Account

Enter the username and password

Username: TESTUSER

Password

Password <None>

New Password: *********

Confirm New Password: *********

☑ Encrypt password using MD5 hash algorithm

Privilege Level: 15

□ Associate a View with the user

View Name : SDM_Administrator(root)

Lab 93: Using Cisco SDM to restrict Telnet and SSH access to routers

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to configure and restrict Telnet and SSH access to Cisco IOS routers using Cisco SDM.

Lab Purpose:

Understanding Cisco SDM is a fundamental skill. SDM is a web-based application that can be used to configure routers as well as troubleshoot internetworks. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to configure restricting Telnet and SSH access to routers using SDM.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

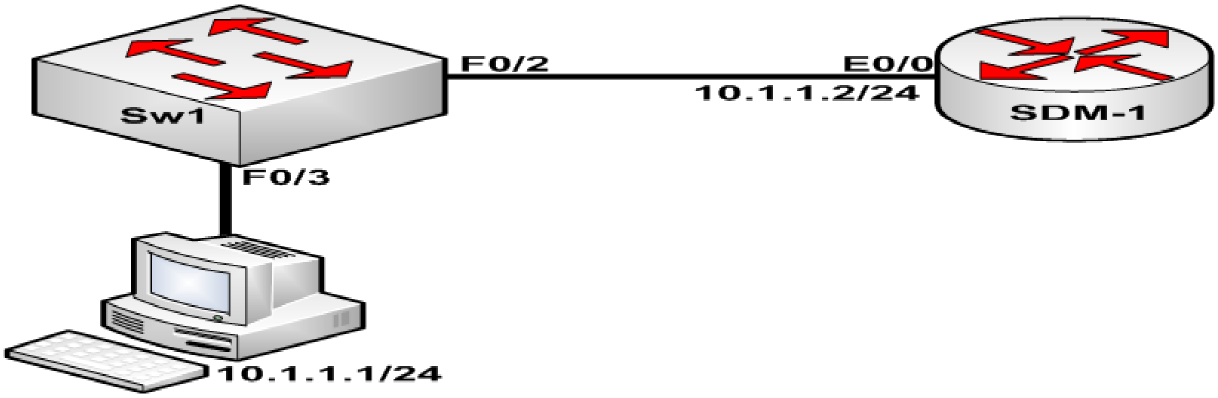
In order to use SDM, you must have an SDM-capable router. The following routers support SDM:

- Cisco Small Business 101, 106, and 107
- Cisco 1701, 1710, 1711, 1712, 1721, 1751, 1751-V, 1760 and 1870V
- Cisco 1801, 1802, 1803, 1811, and 1812
- Cisco 1841
- Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and Cisco 2691 Multiservice Routers
- Cisco 2801, 2811, 2821, and 2851
- Cisco 3620, 3640, 3661, and 3662
- Cisco 3725 and 3745
- Cisco 3825 and 3845
- Cisco 7204VXR, 7206VXR and 7301

The objective of this lab exercise is to familiarize your with the SDM GUI and how to navigate through it. As long as you have one of the platforms listed above, the configuration tasks and GUI navigation will be the same. These lab exercises are based on a Cisco 3640 router with two 10Mbps Ethernet interfaces and two Serial interfaces, but can be completed on any one of the above routers with similar interfaces. Substitute the interfaces in these lab exercises with the ones you have on your router.

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure the hostname on Sw1 as illustrated in the topology.

Task 2:

Configure VLAN 105 on Sw1 and assign it the name SDM_VLAN. Next, configure the E0/0 interface of SDM-1 with the IP address of 10.1.1.2/24. Ensure that the PC has the IP address 10.1.1.1/24 configured on the correct NIC. Assign ports FastEthernet0/2 and FastEthernet0/3 to VLAN 105.

Task 3:

Using SDM, allow Telnet and SSH access to router SDM-1 from the 10.1.1.0/24 subnet using a standard ACL.

SOLUTION:

Lab 93 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

To complete this task you need to navigate to the router properties as follows:

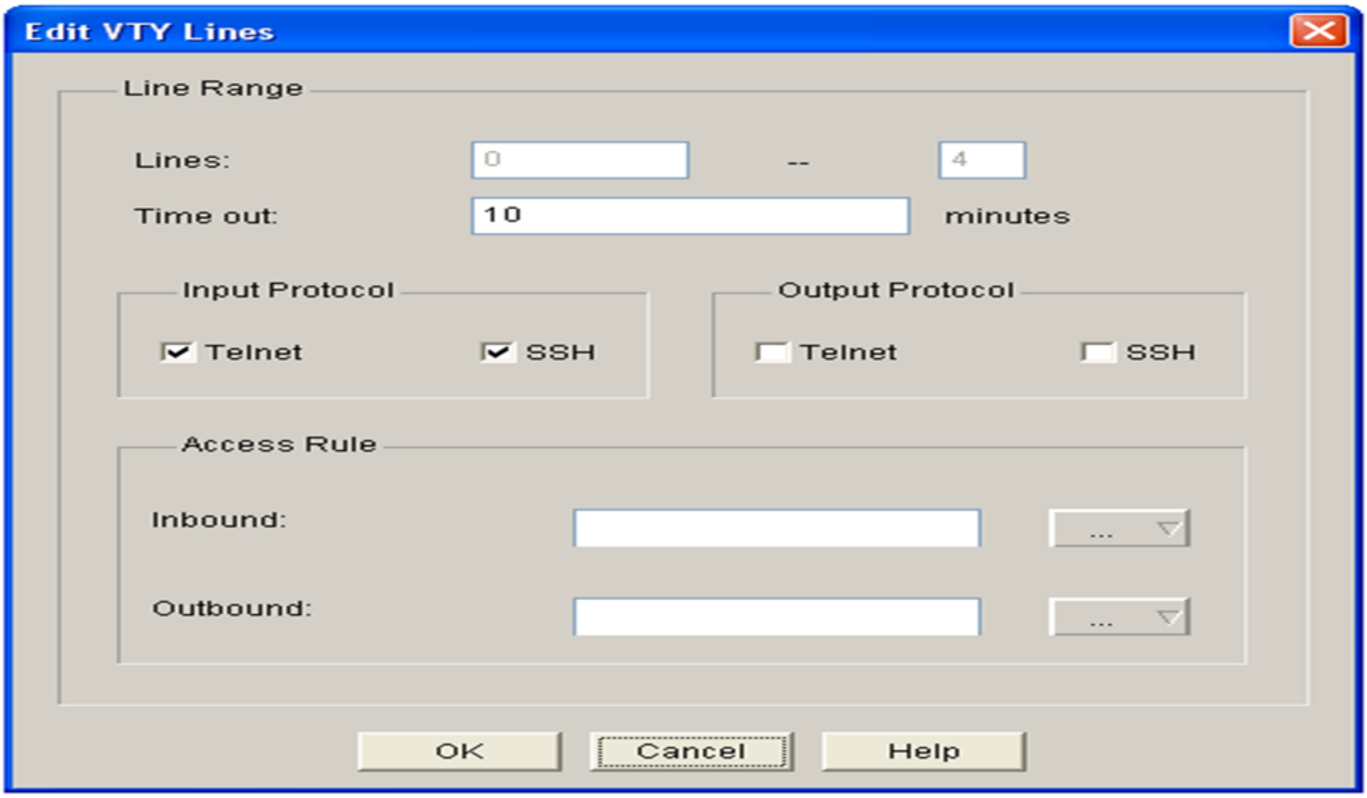
1. On the top menu click on **Configure**.

2. Under Tasks, click on **Additional Tasks**.

3. Next, expand the **Router Access** selection.

4. Click on **VTY**

5. On the right hand side, click **Edit**.



Edit VTY Lines

Line Range

Lines: 0 -- 4

Time out: 10 minutes

Input Protocol

☑ Telnet ☑ SSH

Output Protocol

□ Telnet □ SSH

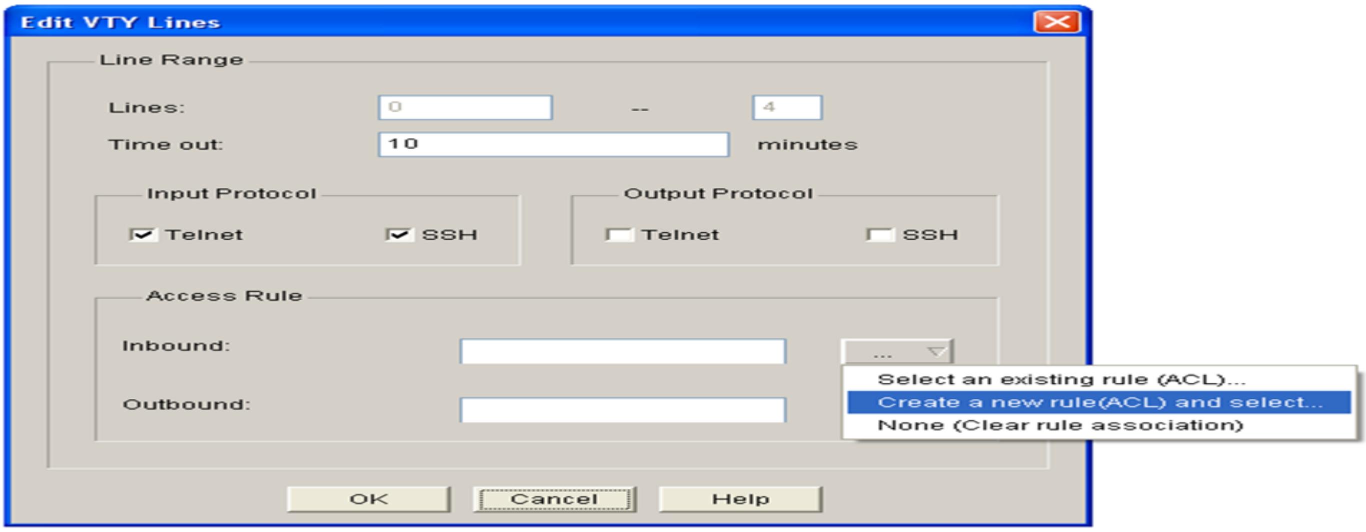
Access Rule

Inbound:

Outbound:

6. Check that the **Telnet** and **SSH** boxes under **Input Protocol** have a check mark against them. This is the default.

7. Under **Access Rule**, right-click the radio box on the same line as the **Inbound** access rule statement. Doing so will allow you to create an ACL that can be used to restrict Telnet and SSH access to the router.



Edit VTY Lines

Line Range

Lines: 0 -- 4

Time out: 10 minutes

Input Protocol: ☑ Telnet ☑ SSH

Output Protocol: □ Telnet □ SSH

Access Rule

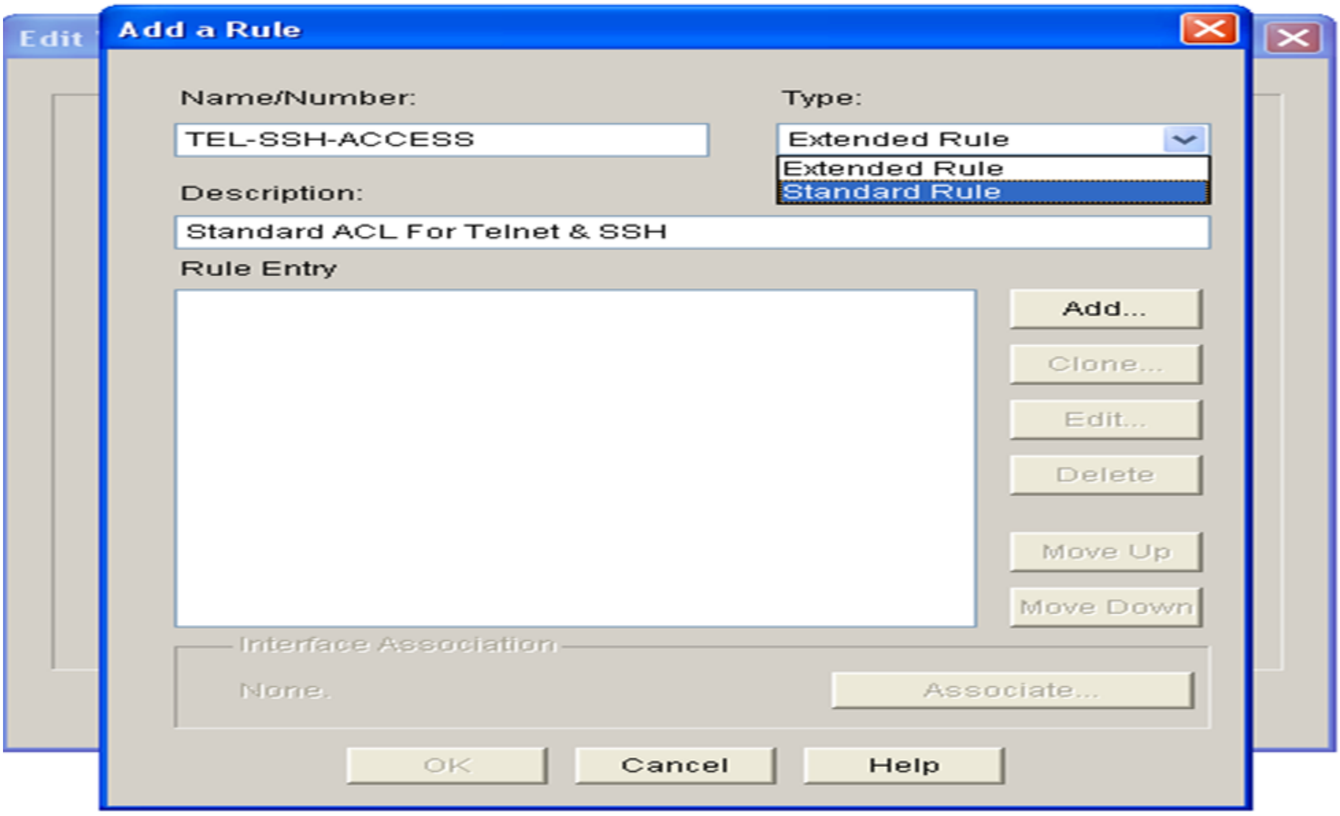
Inbound:

Outbound:

...
Select an existing rule (ACL)...
Create a new rule(ACL) and select...
None (Clear rule association)
OK
Cancel
Help

8. Click on **Create a new rule (ACL) and select...**

9. Assign a name or number to your ACL, and under the **Type** drop-down menu, select **Standard Rule**. You should also add a meaningful description to the ACL you are about to create as illustrated below.



Add a Rule

Name/Number: TEL-SSH-ACCESS

Type: Extended Rule

Description: Standard ACL For Telnet & SSH

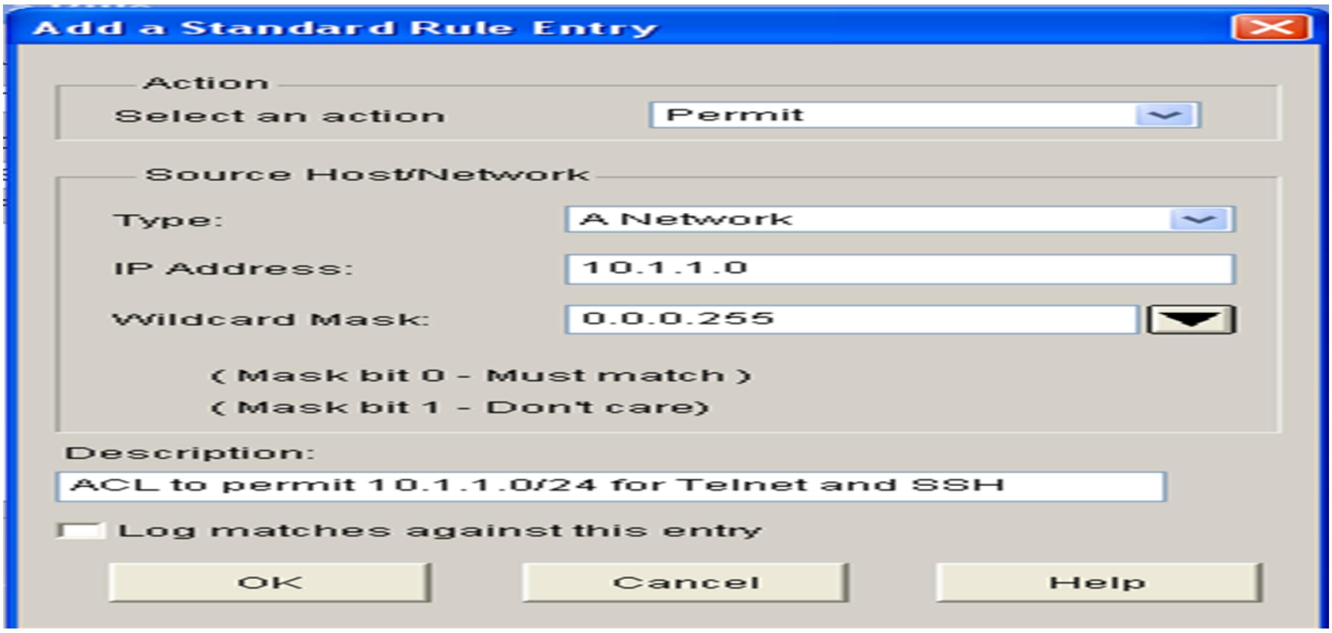
Rule Entry

Interface Association

None.

10. Under **Rule Entry**, click on the **Add** button.

11. Enter the network and wildcard mask. You can also chose to log when packets match this ACL.



Add a Standard Rule Entry
Action
Source Host/Network
(Mask bit 0 - Must match)
(Mask bit 1 - Don't care)
OK
Cancel
Help

Select an action: Permit

Type: A Network

IP Address: 10.1.1.0

Wildcard Mask: 0.0.0.255

Description: ACL to permit 10.1.1.0/24 for Telnet and SSH

□ Log matches against this entry

12. Click **OK** to return to the main menu.

13. Click **OK** again and the commands are sent to the router.

Lab 94: Managing configuration files with Cisco SDM

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to manage router configuration files with Cisco SDM.

Lab Purpose:

Understanding Cisco SDM is a fundamental skill. SDM is a web-based application that can be used to configure routers as well as troubleshoot internetworks. As a Cisco engineer, as well as in the Cisco CCNA exam, you will be expected to know how to manage configuration files on routers using SDM.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

This lab has a difficulty rating of 5/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 10 minutes

IMPORTANT NOTE:

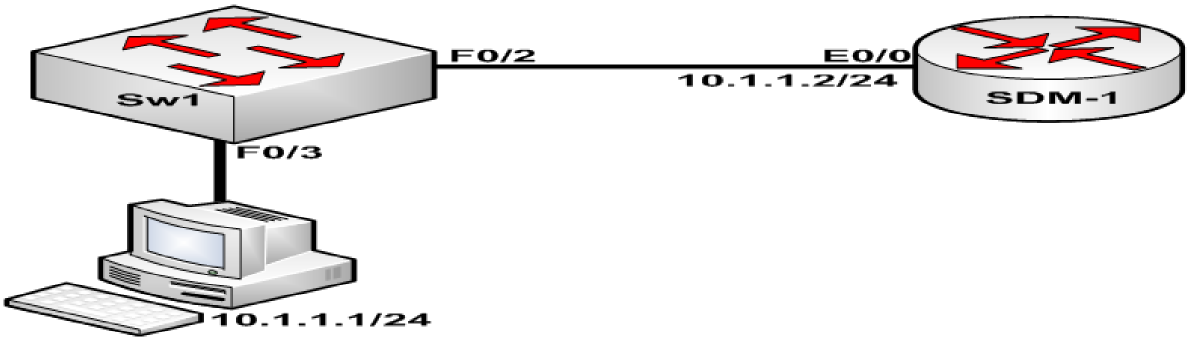
In order to use SDM, you must have an SDM-capable router. The following routers support SDM:

- Cisco Small Business 101, 106, and 107
- Cisco 1701, 1710, 1711, 1712, 1721, 1751, 1751-V, 1760 and 1870V
- Cisco 1801, 1802, 1803, 1811, and 1812
- Cisco 1841
- Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and Cisco 2691 Multiservice Routers
- Cisco 2801, 2811, 2821, and 2851
- Cisco 3620, 3640, 3661, and 3662
- Cisco 3725 and 3745
- Cisco 3825 and 3845
- Cisco 7204VXR, 7206VXR and 7301

The objective of this lab exercise is to familiarize your with the SDM GUI and how to navigate through it. As long as you have one of the platforms listed above, the configuration tasks and GUI navigation will be the same. These lab exercises are based on a Cisco 3640 router with two 10Mbps Ethernet interfaces and two Serial interfaces, but can be completed on any one of the above routers with similar interfaces. Substitute the interfaces in these lab exercises with the ones you have on your router.

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure the hostname on Sw1 as illustrated in the topology.

Task 2:

Configure VLAN 105 on Sw1 and assign it the name SDM_VLAN. Next, configure the E0/0 interface of SDM-1 with the IP address of 10.1.1.2/24. Ensure that the PC has the IP address 10.1.1.1/24 configured on the correct NIC. Assign ports FastEthernet0/2 and FastEthernet0/3 to VLAN 105.

Task 3:

Using Cisco SDM, type in the following configuration to the current configuration on the router:

interface loopback 191

ip address 192.168.19.1 255.255.255.255

Task 4:

Verify that your configuration has been merged with the current configuration on the router.

SOLUTION:

Lab 94 Configuration and Verification

Task 1:

For reference information on configuring hostnames, please refer to:

Lab 35 Configuration and Verification Task 1

Task 2:

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3:

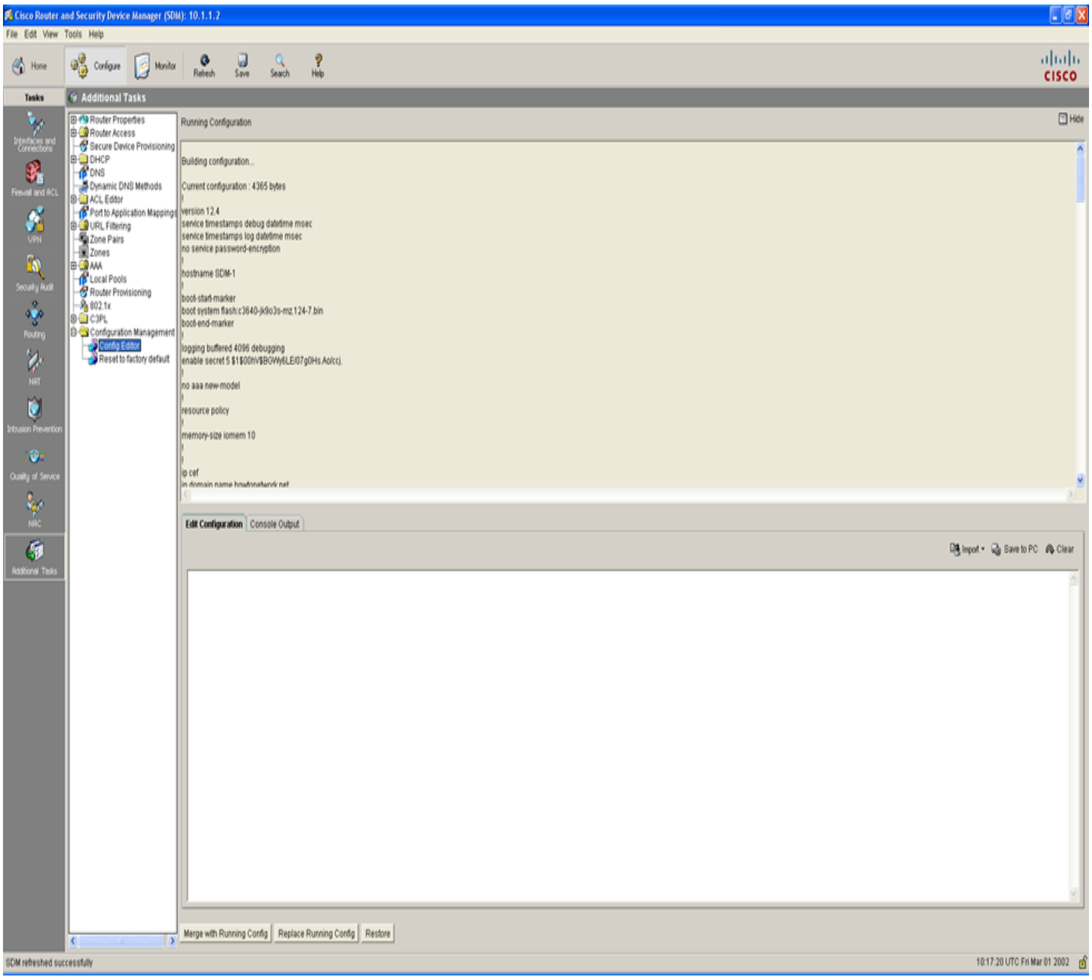
To complete this task you need to navigate to the router properties as follows:

1. On the top menu click on **Configure**.

2. Under Tasks, click on **Additional Tasks**.

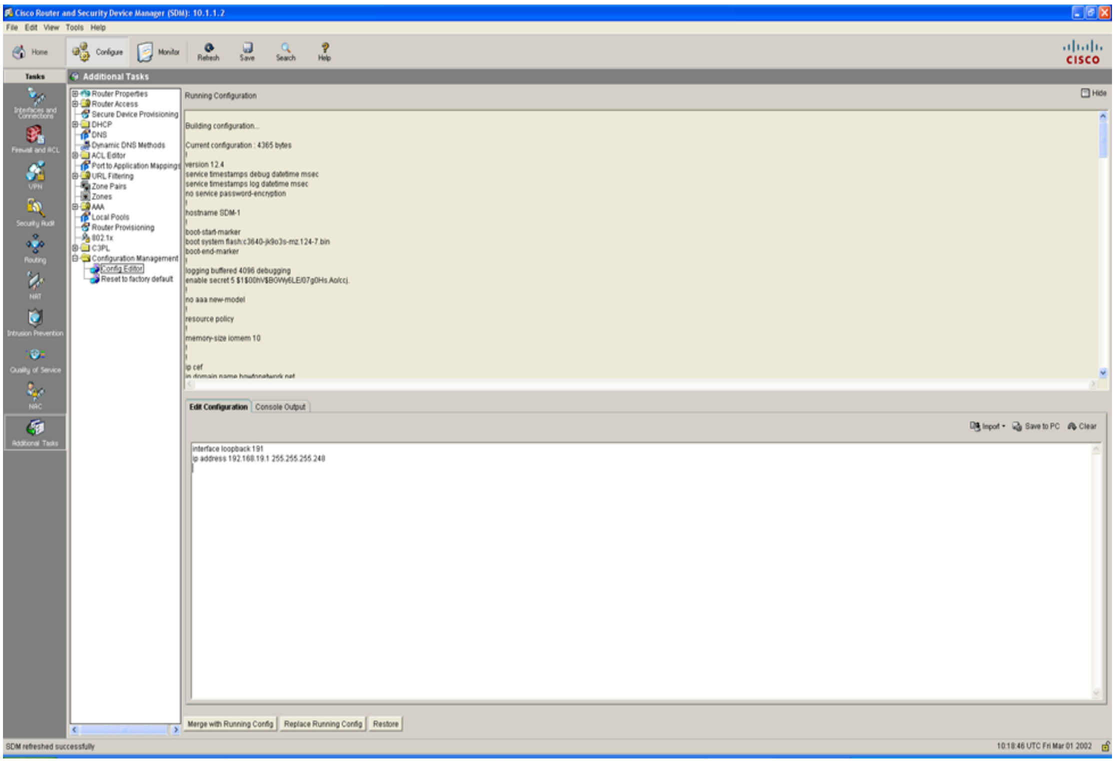
3. Next, expand the **Configuration Management** selection.

4. Click on **Config Editor.** You should now be able to see running-config on the router.



```
Building configuration...

Current configuration : 4365 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SDM-1
!
boot-start-marker
boot system flash:c3640-jk9o3s-mz.124-7.bin
boot-end-marker
!
logging buffered 4096 debugging
enable secret 5 $1$00hV$BGWy6LE/07g0Hs.Ao/cj.
!
no aaa new-model
!
resource policy
!
memory-size iomem 10
!
!
ip cef
ip domain name howtonetwork.net
```

5. Under **Edit Configuration**, type in the configuration provided for the new Loopback interface



Running Configuration

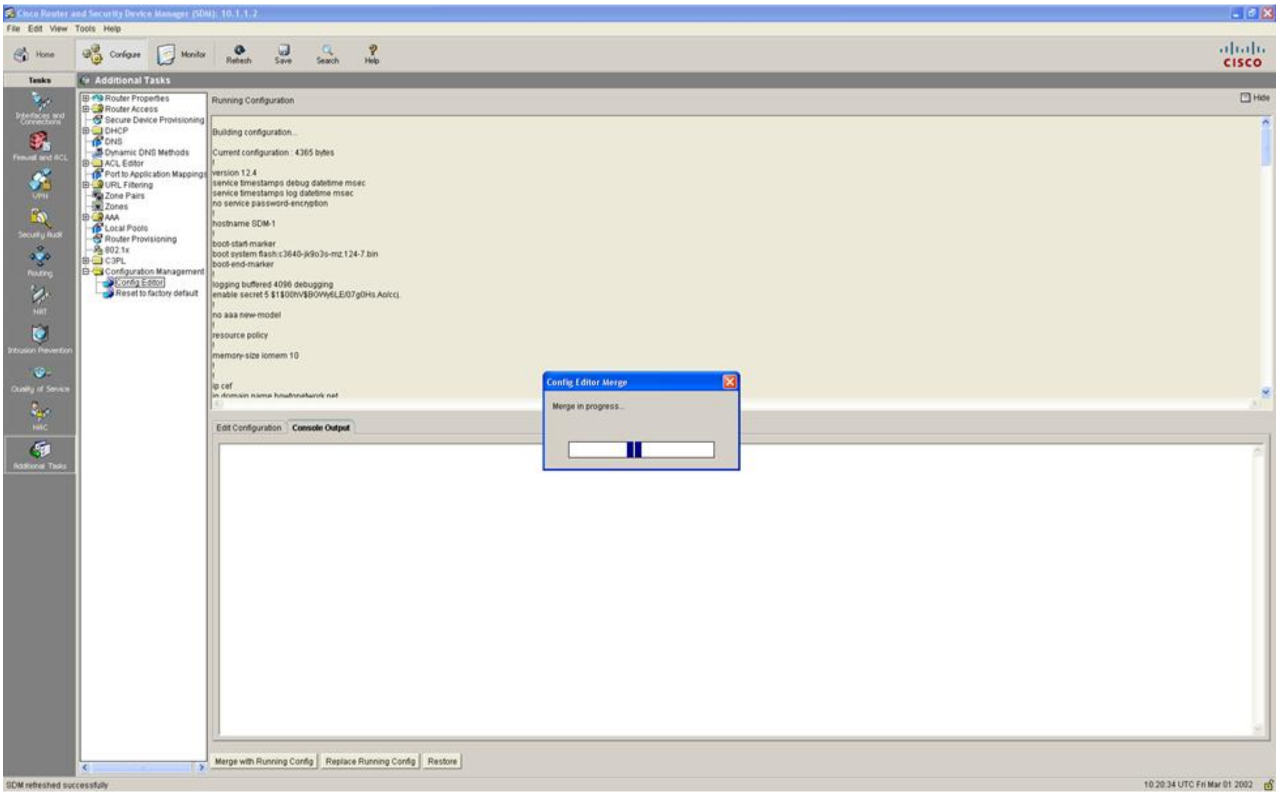
```
Building configuration...

Current configuration : 4365 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SDM-1
!
boot-start-marker
boot system flash:c3640-jk9o3s-mz.124-7.bin
boot-end-marker
!
logging buffered 4096 debugging
enable secret 5 $1$00hV$BGWy6LE/07g0Hs.Ao/cc/.
!
no aaa new-model
!
resource policy
!
memory-size iomem 10
!
!
ip cef
ip domain name howtonetwork.net
```

Edit Configuration | Console Output

```
interface loopback 191
ip address 192.168.19.1 255.255.255.248
```

6. Next, click on the **Merge with Running Config** radio button.

7. Click **Yes** when asked if you are sure and want to continue.



Running Configuration

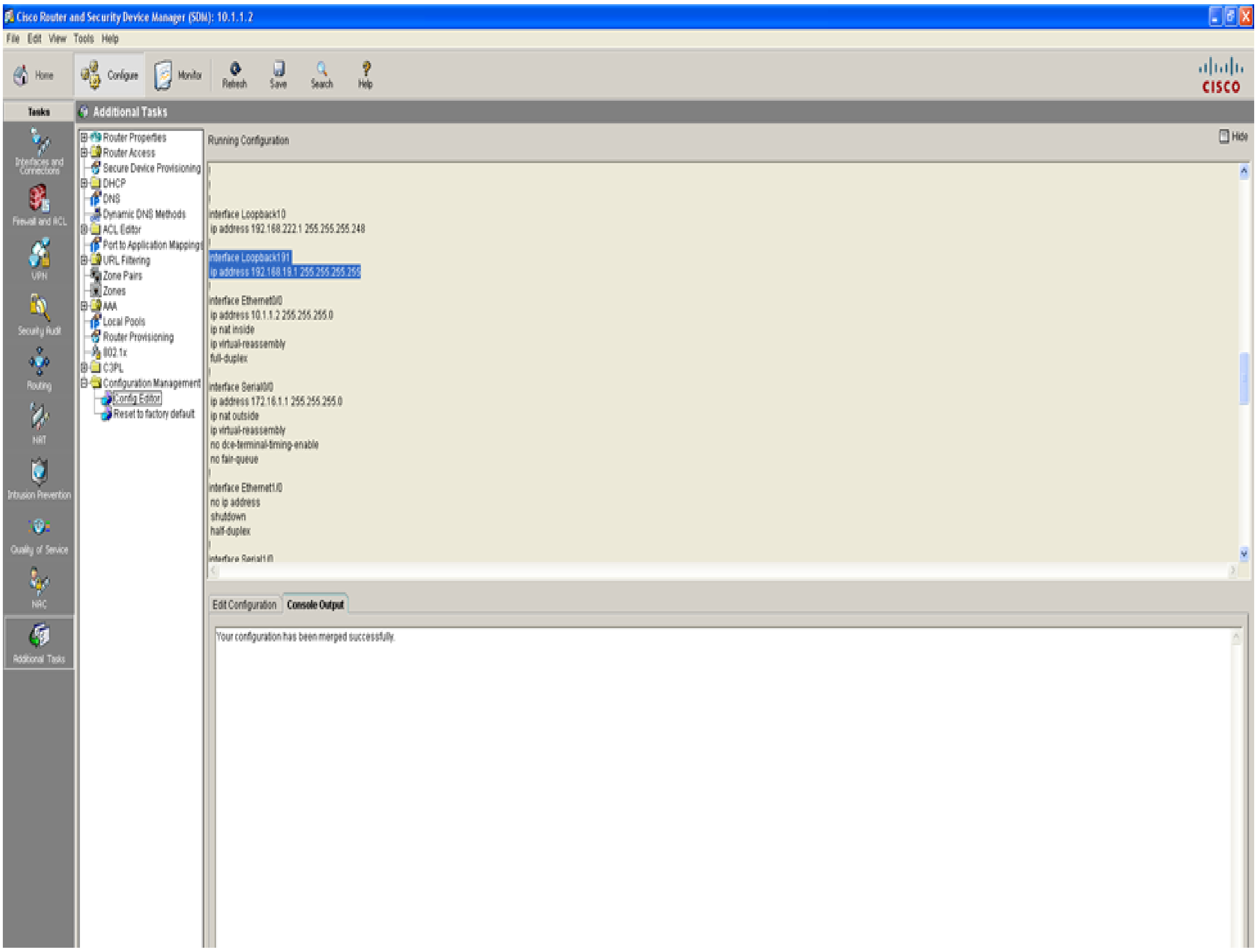
```
Building configuration...

Current configuration : 4365 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SDM-1
!
boot-start-marker
boot system flash:c3640-jk9o3s-mz.124-7.bin
boot-end-marker
!
logging buffered 4096 debugging
enable secret 5 $1$00hV$BGWy6LE/07g0Hs.Ao/cc/.
!
no aaa new-model
!
resource policy
!
memory-size iomem 10
!
!
ip cef
ip domain name howtonetwork.net
```

Config Editor Merge

Merge in progress...

8. Cisco SDM merges your configuration with that of the current router configuration. It may take a few minutes.

9. Once complete you will get a confirmation message from Console Output that the merge was successful. If you scroll down the running config at this time, you will see your new configuration on the router.



Running Configuration

```
!
!
!
interface Loopback10
 ip address 192.168.222.1 255.255.255.248
!
interface Loopback191
 ip address 192.168.19.1 255.255.255.255
!
interface Ethernet0/0
 ip address 10.1.1.2 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 full-duplex
!
interface Serial0/0
 ip address 172.16.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 no dce-terminal-timing-enable
 no fair-queue
!
interface Ethernet1/0
 no ip address
 shutdown
 half-duplex
!
interface Serial1/0
```

Console Output:

```
Your configuration has been merged successfully.
```

Challenge Lab 1: DHCP, inter-VLAN routing and RIPv2

Lab Objective:

This is a challenge lab designed to test and validate the skills you have acquired throughout this lab guide on DHCP, inter-VLAN routing and RIP version 2.

Lab Purpose:

The purpose of this lab is to reinforce DHCP, inter-VLAN routing and RIP version 2 configuration.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

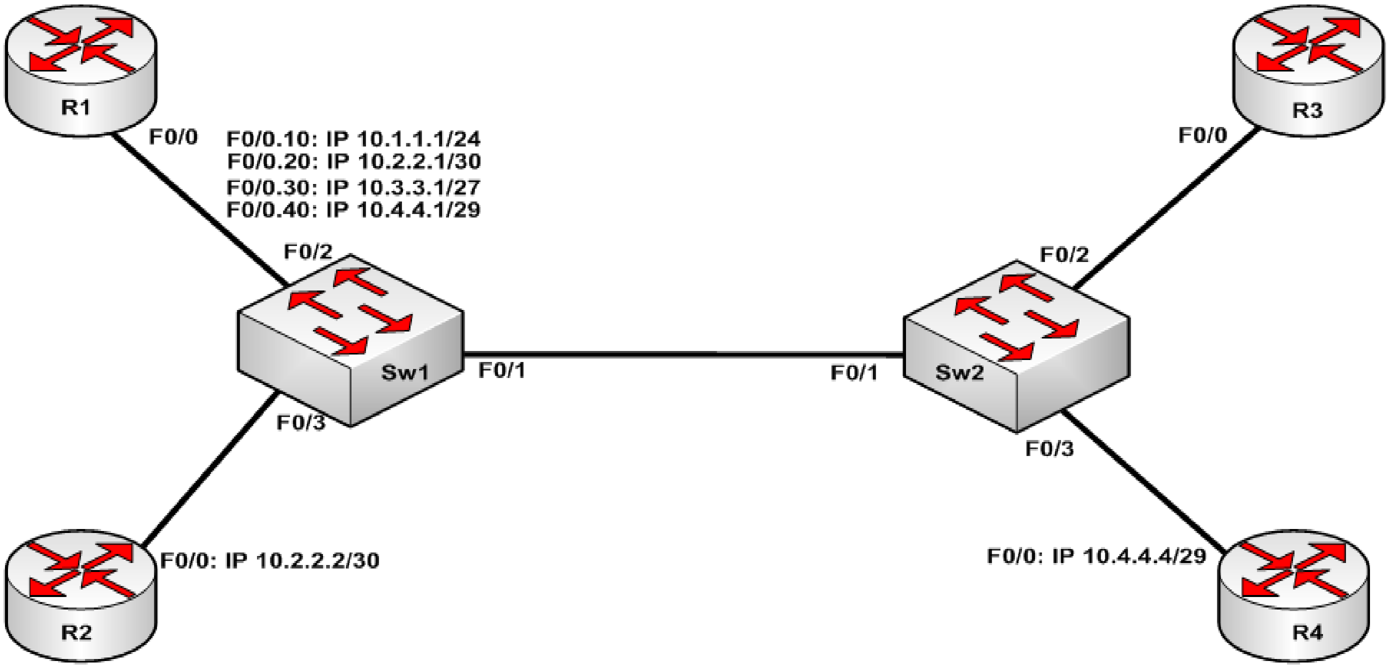
This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure the hostname on all devices as illustrated in the network topology.

Task 2:

Configure Sw1 as a VTP server and Sw2 as a VTP client switch. Both switches should be in VTP domain CISCO. Configure the F0/1 interfaces on both switches as trunk link. Verify that your trunk link is operation and propagating all VLAN information.

Task 3:

Configure the following VLANs on Sw1:

VLAN Number	**VLAN Name**
10	VLAN-10
20	VLAN-20
30	VLAN-30
40	VLAN-40

Task 4:

Make sure your VLAN information propagates to Sw2. Next, configure Sw1 Fa0/2 as a trunk link and Fa0/3 in VLAN 20. Configure Sw2 Fa0/2 in VLAN 30 and Fa0/3 in VLAN 40.

Task 5:

Configure IP addresses as specified in the topology on routers R2 and R4. On Sw1 and Sw2, configure interface VLAN 10 with an IP address of 10.1.1.2/24 and 10.1.1.3/24 respectively for Sw1 and Sw2. The default gateway both all switches should be 10.1.1.1.

Task 6:

Configure subinterfaces on R1 as illustrated in the topology. Ensure that Fa0/0.10 is in VLAN 10, Fa0/0.20 is in VLAN 20, Fa0/0.30 is in VLAN 30, and Fa0/0.40 is in VLAN 40.

Task 7:

Configure R1 as a Cisco IOS DHCP server for the 10.3.3.0/27 subnet. The domain name should be howtonetwork.net; the default gateway should be 10.3.3.1; the DHCP lease should be for 7 days. Next, configure R3 to receive IP addressing on F0/0 via DHCP.

Task 8:

Configure RIP version 2 on R1, R2, R3 and R4. Make sure there is no automatic summarization.

Task 9:

If you have configured everything correctly, all routers and all switches should be able to ping each other. Verify this to see if you have completed the lab successfully.

SOLUTION:

Challenge Lab 1: Configuration Hints

Task 1 Hints & References

For reference information on configuring hostnames, please refer to:

Lab 21 Configuration and Verification Task 1

Lab 35 Configuration and Verification Task 1

Task 2 Hints & References

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

For reference information on configuring a VTP Domain, please refer to:

Lab 3 Configuration and Verification Task 2

Lab 5 Configuration and Verification Task 2

For reference information on configuring and verifying trunks, please refer to:

Lab 3 Configuration and Verification Task 3

Lab 3 Configuration and Verification Task 3

Task 3 Hints & References

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 4 Hints & References

For reference information on configuring and verifying trunks, please refer to:

Lab 3 Configuration and Verification Task 3

Lab 3 Configuration and Verification Task 3

Task 5 Hints & References

For reference information on configuring IP interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

Lab 56 Configuration and Verification Task 2

Task 6 Hints & References

For reference information on LAN subinterfaces, please refer to:

Lab 15 Configuration and Verification Task 5

Task 7 Hints & References

For reference information on IOS DHCP Client & Server configuration, please refer to:

Lab 70 Configuration and Verification Task 3

Lab 71 Configuration and Verification Task 4

Task 8 Hints & References

Remember that automatic summarization at Classful boundaries is a default RIP feature. Disable it.

For reference information on disabling RIPv2 automatic summarization, please refer to:

Lab 36 Configuration and Verification Task 7

Task 9 Hints & References

For reference information on using standard PING, please refer to:

Lab 15 Configuration and Verification Task 6

For reference information on sourcing traffic from other interfaces, please refer to:

Lab 55 Configuration and Verification Task 4

Lab 56 Configuration and Verification Task 5

Lab 57 Configuration and Verification Task 4

Lab 57 Configuration and Verification Task 6

Lab 59 Configuration and Verification Task 6

Challenge Lab 2: VTP, STP and OSPF

Lab Objective:

This is a challenge lab designed to test and validate the skills you have acquired throughout this lab guide on VTP, STP and OSPF.

Lab Purpose:

The purpose of this lab is to reinforce VTP, STP and OSPF configuration.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

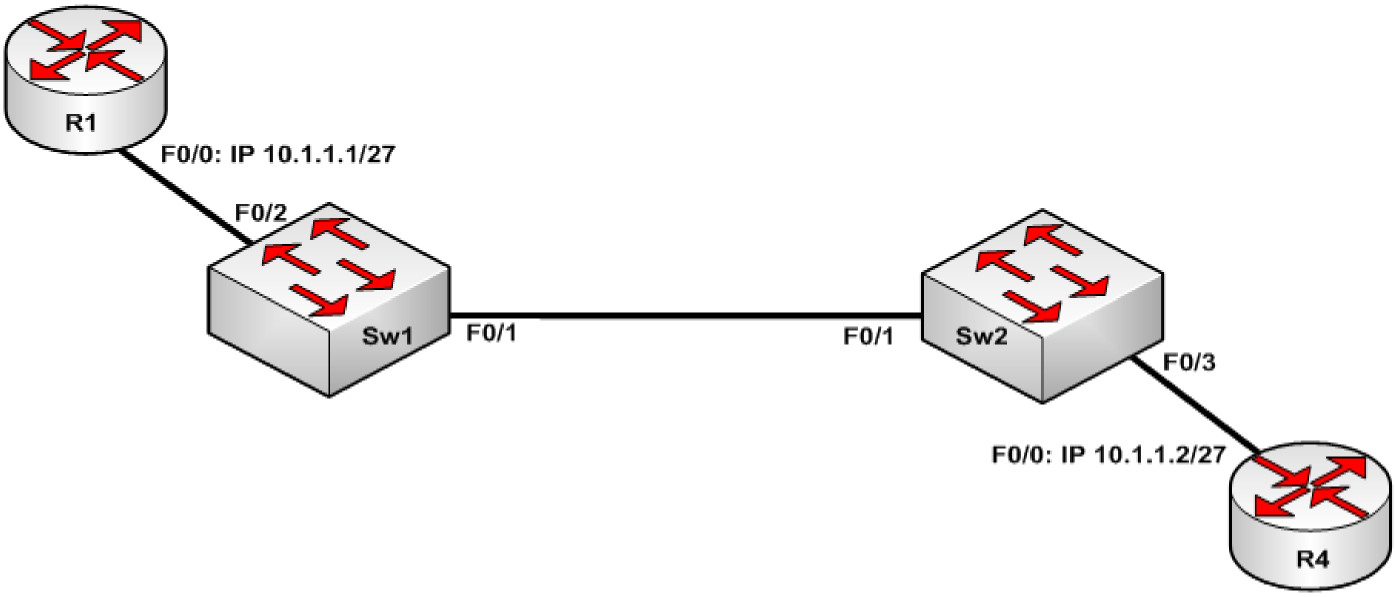
This lab has a difficulty rating of 8/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure the hostname on all devices as illustrated in the network topology.

Task 2:

Configure Sw1 and Sw2 to support extended range VLANs. Both switches should be in the VTP domain CISCO with a VTP password of HOWTONETWORK. In addition to that, both switches should only send VTP version 2 updates.

Task 3:

Configure the following VLANs on Sw1 and Sw2

VLAN Number	**VLAN Name**
4010	VLAN-4010
4020	VLAN-4020
4030	VLAN-4030
4040	VLAN-4040

Task 4:

Assign port Fa0/2 on Sw1 and Fa0/3 on Sw2 to VLAN 4040. These ports should be configured to transition immediately to a Spanning Tree forwarding state. Ports Fa0/1 on Sw1 and Sw2 should be configured a trunk link; however, this trunk link must only allow the VLANs configured on the switches.

Task 5:

Configure IP addresses as specified in the topology on routers R1 and R4. Verify these routers can ping each other.

Task 6:

Configure Sw1 to be the Root Bridge for VLANs 4010 and 4030 with a priority of 4096. Configure Sw2 to be the root bridge for VLANs 4020 and 4040 using the built-in Cisco macro. Verify the Root Bridge states using the correct Spanning Tree commands.

Task 7:

Configure OSPF Area 0 between R1 and R4 on the 10.1.1.0/27 subnet. Ensure that an OSPF adjacency forms and a DR and BDR is elected on the subnet. Verify your configuration with the appropriate OSPF commands.

SOLUTION:

Challenge Lab 2: Configuration Hints

Task 1 Hints & References

For reference information on configuring hostnames, please refer to:

Lab 21 Configuration and Verification Task 1

Lab 35 Configuration and Verification Task 1

Task 2 Hints & References

For reference information on changing VTP version & password, please refer to:

Lab 5 Configuration and Verification Task 2

Lab 16 Configuration and Verification Task 2

Task 3 Hints & References

By default all Catalyst switches are VTP server devices; however VTP servers do not supported extended VLAN ranges so you need to update your switch VTP mode to create the extended range VLANs.

For reference information on configuring extended VLANs, please refer to:

Lab 4 Configuration and Verification Task 4

Task 4 Hints & References

By default, all ports have to go through the typical Spanning Tree states of Blocking, Listening, Learning, Forwarding, etc; however, portfast allows a port to transition immediately to a Forwarding state.

For reference information on Spanning Tree PortFast, please refer to:

Lab 10 Configuration and Verification Task 2

Task 5 Hints & References

For reference information on configuring IP interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

Lab 56 Configuration and Verification Task 2

Task 6 Hints & References

The STP root bridge can be changed manually using the spanning-tree vlan [id] priority command or via an in-built macro using the spanning-tree vlan [id] root [primary|secondary] commands.

For reference information on Spanning Tree Priority, please refer to:

Lab 7 Configuration and Verification Task 3

Lab 8 Configuration and Verification Task 3

Task 7 Hints & References

For reference information wildcard masks, please refer to:

Lab 42 Configuration and Verification Task 5

Lab 48 Configuration and Verification Task 3

For reference information OSPF configuration, please refer to:

Lab 52 Configuration and Verification Task 4

Lab 53 Configuration and Verification Task 3

Lab 54 Configuration and Verification Task 3

Challenge Lab 3: EIGRP, PAT, ACLs and Banners

Lab Objective:

This is a challenge lab designed to test and validate the skills you have acquired throughout this lab guide on EIGRP, PAT, ACLs and Banners.

Lab Purpose:

The purpose of this lab is to reinforce EIGRP, PAT, ACLs and Banner configuration.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

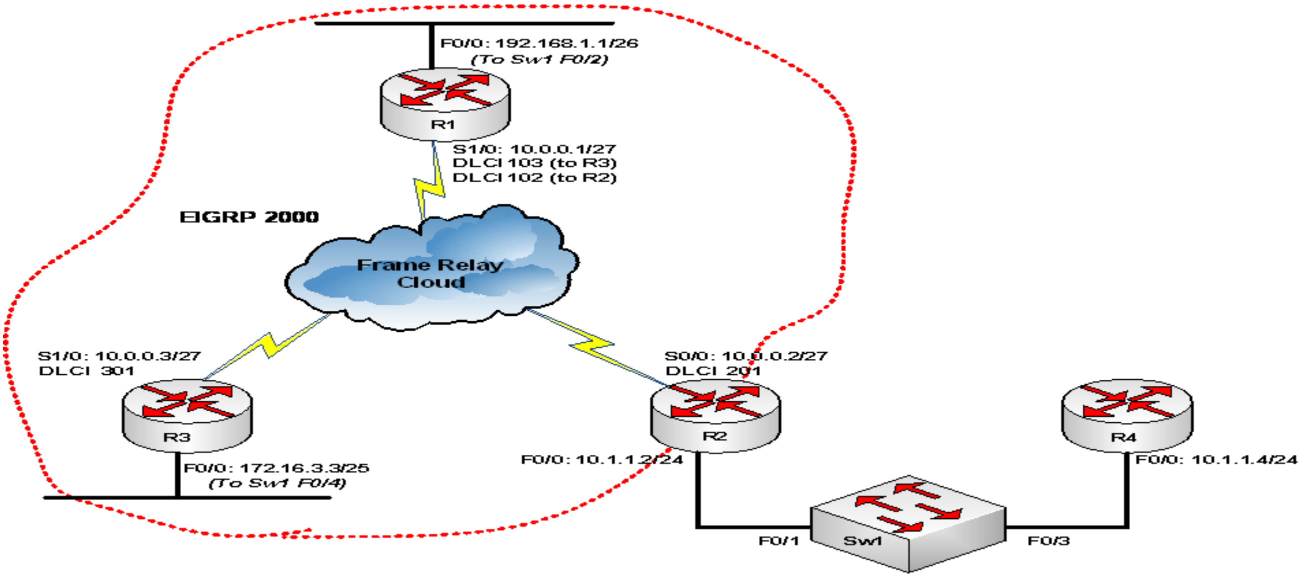
This lab has a difficulty rating of 10/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure the hostname on all devices as illustrated in the network topology.

Task 2:

Configure VLAN 2000 on Sw1 and name it EIGRP_VLAN. Add ports FastEthernet0/1 and FastEthernet0/3 to this VLAN. Next, enable ports FastEthernet0/2 and FastEthernet0/4 on Sw1 so that R1 and R3 F0/0 interfaces come up.

Task 3:

Configure R1, R2 and R3 over the Frame Relay network using static Frame Relay maps. Each router must have a static Frame Relay map to the other two routers on the Frame Relay network.

Task 4:

Configure the IP addresses for R1, R2, R3, and R4 F0/0 interfaces as illustrated in the topology. Ping between R2 and R4 to ensure you have network connectivity.

Task 5:

Enable EIGRP AS 2000 for R1 S1/0 and F0/0 interfaces, R3 S1/0 and F0/0 interfaces, and for R2 S0/0 interface only. Do NOT advertise the R2 F0/0 subnet via EIGRP. You MUST use a wildcard mask on R2 to prevent this from happening.

Task 6:

At this point, you should have EIGRP routes for all subnets except for the 10.1.1.0/24 subnet. If either R1 or R3 is seeing this route via EIGRP, check your configuration on R2 as instructed in Task 5.

Task 7:

Configure R4 with a default static route of 10.1.1.2. Configure R1 and R3 to accept Telnet login using a password of CISCO. In addition, configure both R1 and R3 with the following MOTD banner:

%%%%%%%%%%%%%%%%%%%%%%%%%%%%

Congratulations! Your PAT configuration works!

%%%%%%%%%%%%%%%%%%%%%%%%%%%%

Task 8:

Configure PAT on R2 so that ping traffic from 10.1.1.0/24 to 172.16.3.0/25 and 192.168.1.0/26 is translated to the IP address of R2 S0/0 interface. Ping 192.168.1.1 and 172.16.3.3 from R4. If configured correctly, these will work.

Task 9:

Configure PAT on R2 so that Telnet traffic from 10. 1.1.0/24 to 10.0.0.0/27 is translated to the IP address of R2 S0/0 interface. Telnet to R2 and R3 from R4. If configured correctly, this will work.

SOLUTION:

Challenge Lab 3: Configuration Hints

Task 1 Hints & References

For reference information on configuring hostnames, please refer to:

Lab 21 Configuration and Verification Task 1

Lab 35 Configuration and Verification Task 1

Task 2 Hints & References

To bring up the interfaces, you need to perform a no shutdown command on the interface.

For reference information on configuring and verifying VLANs, please refer to:

Lab 1 Configuration and Verification Task 3

Lab 2 Configuration and Verification Task 3

Task 3 Hints & References

Each router must have two Frame Relay map statements similar to the following:

Serial1/0 (up): ip **[IP ADDRESS]** dlci **[DLCI](**0x66,0x1860), static,

broadcast,

CISCO, status defined, active

Serial1/0 (up): ip **[IP ADDRESS]** dlci **[DLCI](**0x67,0x1870), static,

broadcast,

CISCO, status defined, active

For reference information on verifying Frame Relay mapping, please refer to:

Lab 26 Configuration and Verification Task 3

Lab 27 Configuration and Verification Task 3

Lab 40 Configuration and Verification Task 4

Lab 40 Configuration and Verification Task 5

Task 4 Hints & References

For reference information on using standard PING, please refer to:

Lab 15 Configuration and Verification Task 6

Task 5 Hints & References

Your EIGRP configuration on R2 would be:

```
router eigrp 2000

 no auto-summary

 network 10.0.0.0 0.0.0.31
```

If you did not use the wildcard mask, EIGRP would advertise the entire 10.0.0.0/8 network, which would include the 10.1.1.0/24 subnet. Since that is prohibited in the lab, you must use the EIGRP wildcard mask.

For reference information wildcard masks, please refer to:

Lab 42 Configuration and Verification Task 5

Lab 48 Configuration and Verification Task 3

For reference information on enabling EIGRP, please refer to:

Lab 41 Configuration and Verification Task 4

Lab 42 Configuration and Verification Task 5

Lab 44 Configuration and Verification Task 5

For reference information on verifying EIGRP adjacencies, please refer to:

Lab 41 Configuration and Verification Task 5

Lab 42 Configuration and Verification Task 7

Task 6 Hints & References

Use the show ip route eigrp or the show ip route command to verify routing information.

Task 7 Hints & References

You need to use the ip route 0.0.0.0 0.0.0.0 [interface|ip address] command

For reference information on configuring static routes, please refer to:

Lab 31 Configuration and Verification Task 4

Lab 32 Configuration and Verification Task 3

Lab 33 Configuration and Verification Task 4

Lab 34 Configuration and Verification Task 4

To configure an MOTD banner, you need to use the banner motd command. Be careful not to use your delimiting character in the banner configuration!

For reference information on configuring banners, please refer to:

Lab 78 Configuration and Verification Task 2

Task 8 Hints & References

You need to configure an extended ACL for the PAT traffic. Your ACL would be similar to the following:

```
ip access-list extended NAT-ACL

   permit icmp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.127 echo

   permit icmp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.127 echo-reply

   permit icmp 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.63 echo

   permit icmp 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.63 echo-reply
```

You then need to use this ACL in the ip nat inside command and PAT traffic to S0/0

For reference information on NAT, please refer to:

Lab 65 Configuration and Verification Task 6

Lab 66 Configuration and Verification Task 7

Lab 67 Configuration and Verification Task 7

Lab 68 Configuration and Verification Task 7

Lab 59 Configuration and Verification Task 6

Task 9 Hints & References

You need to add to the ACL you created in Task 8 to complete this task

```
ip access-list extended NAT-ACL

   permit tcp 10.1.1.0 0.0.0.255 10.0.0.0 0.0.0.31 eq telnet
```

Alternatively, you can create a second PAT configuration altogether:

```
ip nat inside source-list TELNET-NAT-ACL interface Serial0/0 overload

ip nat inside source-list PING-NAT-ACL interface Serial0/0 overload
```

```
!
ip access-list extended NAT-ACL
   permit tcp 10.1.1.0 0.0.0.255 10.0.0.0 0.0.0.31 eq telnet
!
ip access-list extended PING-NAT-ACL
   permit icmp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.127 echo
   permit icmp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.127 echo-reply
   permit icmp 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.63 echo
   permit icmp 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.63 echo-reply
```

Whichever method you use, as long as it meets the requirements, you're fine.

For reference information on configuring NAT, please refer to:

Lab 65 Configuration and Verification Task 6

Lab 66 Configuration and Verification Task 8

Lab 67 Configuration and Verification Task 7

Challenge Lab 4: Multi-Area OSPF, Frame Relay, LAN Switching

Lab Objective:

This is a challenge lab designed to test and validate the skills you have acquired throughout this lab guide on Multi-Area OSPF, Frame Relay and LAN switching

Lab Purpose:

The purpose of this lab is to reinforce Multi-Area OSPF, Frame Relay and LAN switching.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

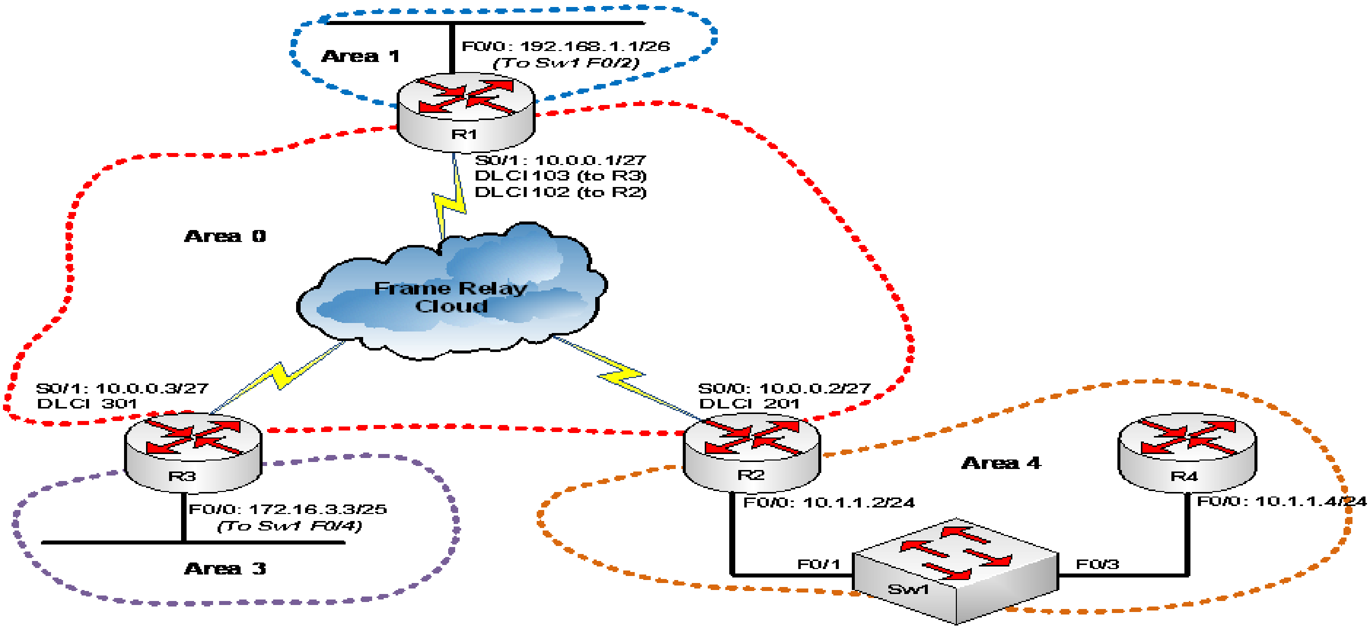
This lab has a difficulty rating of 10/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 30 minutes

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure the hostname on all devices as illustrated in the network topology.

Task 2:

Configure VLAN 75 on Sw1 and name it OSPF_VLAN. To simply switch port configuration, configure a macro called NETWORK-PORTS on Sw1 for ports FastEthernet0/1 and FastEthernet0/3. Using this macro, configure ports FastEthernet0/1 and FastEthernet0/3 as access ports in VLAN 75. Ensure that these ports immediately transition to the forwarding state.

Task 3:

Configure the IP addresses on R2 and R4 F0/0 interfaces as illustrated in the topology. Configure interface VLAN 75 on Sw1 with the IP address 10.1.1.254/24. Sw1 should have a default gateway of 10.1.1.2.

Task 4:

Configure R1, R2 and R3 over the Frame Relay network using static Frame Relay maps. Each router must have a static Frame Relay map to the other two routers on the Frame Relay network. Use the IP addresses provided.

Task 5:

Configure R1 and R3 F0/0 interfaces. Enable these interfaces on the routers. Also, enable ports FastEthernet0/2 and FastEthernet0/4 on Sw1 so that these interfaces come up.

Task 6:

Configure OSPF and assign interfaces to Areas illustrated in the network topology. On the Frame Relay network, change the default OSPF network type to the most suitable network type for NBMA networks. On all routers, configure the OSPF router ID as x.x.x.x, where x is the router number. For example, on R1 you would configure the OSFP router ID as 1.1.1.1, on R2 you would configure it as 2.2.2.2, etc.

Task 7:

Verify your OSPF adjacencies on all routers. Ensure you can ping all subnets from all routers.

SOLUTION:

Challenge Lab 4: Configuration Hints

Task 1 Hints & References

For reference information on configuring hostnames, please refer to:

Lab 21 Configuration and Verification Task 1

Lab 35 Configuration and Verification Task 1

Task 2 Hints & References

For reference information on configuring standard VLANs, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 1 Configuration and Verification Task 2

Lab 2 Configuration and Verification Task 2

Lab 3 Configuration and Verification Task 1

You also need to configure an interface macro to complete this task.

For reference information on configuring interface macros, please refer to:

Lab 9 Configuration and Verification Task 3

Task 3 Hints & References

For reference information on switch default gateways, please refer to:

Lab 17 Configuration and Verification Task 3

Task 4 Hints & References

Each router must have two Frame Relay map statements similar to the following:

```
Serial1/0 (up): ip [IP ADDRESS] dlci [DLCI](0x66,0x1860), static,
              broadcast,
              CISCO, status defined, active
Serial1/0 (up): ip [IP ADDRESS] dlci [DLCI](0x67,0x1870), static,
              broadcast,
              CISCO, status defined, active
```

For reference information on verifying Frame Relay mapping, please refer to:

Lab 26 Configuration and Verification Task 3

Lab 27 Configuration and Verification Task 3

Lab 40 Configuration and Verification Task 4

Lab 40 Configuration and Verification Task 5

Task 5 Hints & References

You need to issue the no shutdown command to bring up the interfaces.

For reference information on configuring IP interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

Lab 56 Configuration and Verification Task 2

Task 6 Hints & References

You need to change from the NONBROADCAST network type to POINT_TO_MULTIPOINT using the ip ospf network point-to-multipoint command on the router Serial interfaces.

For reference information OSPF point-to-multipoint networks, please refer to:

Lab 52 Configuration and Verification Task 3

For reference information OSPF configuration, please refer to:

Lab 52 Configuration and Verification Task 4

Lab 53 Configuration and Verification Task 3

Lab 54 Configuration and Verification Task 3

Task 7 Hints & References

For reference information OSPF configuration, please refer to:

Lab 52 Configuration and Verification Task 4

Lab 53 Configuration and Verification Task 3

Lab 54 Configuration and Verification Task 3

Challenge Lab 5: EIGRP Summarization, Static NAT, ACLs

Lab Objective:

This is a challenge lab designed to test and validate the skills you have acquired throughout this lab guide on EIGRP summarization, static NAT configuration and Access Control Lists.

Lab Purpose:

The purpose of this lab is to reinforce EIGRP summarization, static NAT configuration and Access Control Lists.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

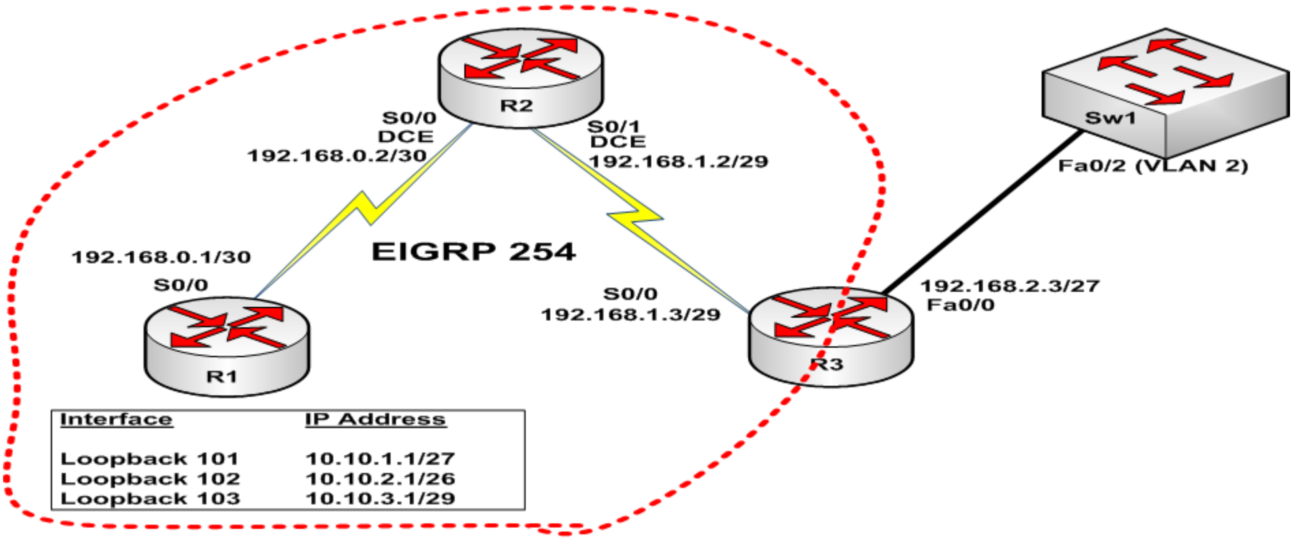
This lab has a difficulty rating of 10/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

Lab Topology:

Please use the following topology to complete this lab.



Interface	IP Address
Loopback 101	10.10.1.1/27
Loopback 102	10.10.2.1/26
Loopback 103	10.10.3.1/29

Task 1:

Configure the hostname on all devices as illustrated in the network topology.

Task 2:

Configure VLAN 2 on Sw1 and name it EIGRP_VLAN. Assign port FastEthernet0/2 to this VLAN. In addition, configure interface VLAN 2 on Sw1 and assign it the IP address 192.168.2.4. Sw1 should have a default gateway of 192.168.2.3 configured.

Task 3:

Configure the Loopback interfaces on R2 as illustrated in the topology. Configure the IP addressing on the Serial interfaces of R1, R2 and R3. Make sure that the DCE interfaces provide clocking at 512Kbps.

Task 4:

Configure EIGRP AS 254 on R1 Loopback interfaces and S0/0, on R2 S0/0 and S0/1 interfaces, and on R3 S0/0. Do NOT configure EIGRP for R3 F0/0. Use a wildcard mask on R3 EIGRP configuration to prevent this.

Task 5:

At this point, you should have EIGRP routes for all subnets except for the 192.168.2.0/27 subnet. Next, configure R1 to send a summary address via EIGRP for the three Loopback interfaces. This summary address should be advertised out of S0/0. Verify that R2 and R3 now see a single route for the three Loopback interfaces on R1, but can still ping all of them.

Task 6:

Configure static NAT on R3 so that the private IP address of 192.168.2.4 (which is Sw1) is translated to the public IP address of 192.168.1.4. Configure Sw1 to allow Telnet connections using the username ADMIN with a password of CISCO.

Task 7:

Sw1 should not be able to ping all other devices in the network. Verify that it can. In addition, Telnet from R1 and R2 to 192.168.1.4 and verify that you connect to Sw1 via the NAT translation. If not, check your configuration.

SOLUTION:

Challenge Lab 5: Configuration Hints

Task 1 Hints & References

For reference information on configuring hostnames, please refer to:

Lab 21 Configuration and Verification Task 1

Lab 35 Configuration and Verification Task 1

Task 2 Hints & References

For reference information on configuring standard VLANs, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 1 Configuration and Verification Task 2

Lab 2 Configuration and Verification Task 2

Lab 3 Configuration and Verification Task 1

Task 3 Hints & References

For reference information on configuring IP interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

Lab 56 Configuration and Verification Task 2

Task 4 Hints & References

Your EIGRP configuration on R2 would be:

```
router eigrp 254

 no auto-summary

 network 192.168.1.0 0.0.0.7
```

If you did not use the wildcard mask, EIGRP would advertise the entire 192.168.0.0/16 network, which would include the 192.168.2.0/27 subnet. Since that is prohibited in the lab, you must use the EIGRP wildcard mask.

For reference information wildcard masks, please refer to:

Lab 42 Configuration and Verification Task 5

Lab 48 Configuration and Verification Task 3

For reference information on enabling EIGRP, please refer to:

Lab 41 Configuration and Verification Task 4

Lab 42 Configuration and Verification Task 5

Lab 44 Configuration and Verification Task 5

Task 5 Hints & References

Your summary address configuration for this task would be as follows:

```
interface Serial0/0

 ip summary-address eigrp 254 10.10.0.0 255.255.252.0
```

You need to be comfortable summarizing IP addresses. Practice makes perfect!

For reference information on RIPv2 and EIGRP route summarization, please refer to:

Lab 39 Configuration and Verification Task 6

Lab 45 Configuration and Verification Task 5

Task 6 Hints & References

You need to use the ip nat inside source static command to complete this task.

For reference information on configuring NAT, please refer to:

Lab 65 Configuration and Verification Task 6

Lab 66 Configuration and Verification Task 8

Lab 67 Configuration and Verification Task 7

Task 7 Hints & References

For reference information on using standard PING, please refer to:

Lab 15 Configuration and Verification Task 6

Challenge Lab 6: PPP Authentication, Static Routing, DNS, SYSLOG

Lab Objective:

This is a challenge lab designed to test and validate the skills you have acquired throughout this lab guide on PPP authentication, static routing, DNS and SYSLOG.

Lab Purpose:

The purpose of this lab is to reinforce PPP authentication, static routing, DNS and SYSLOG.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

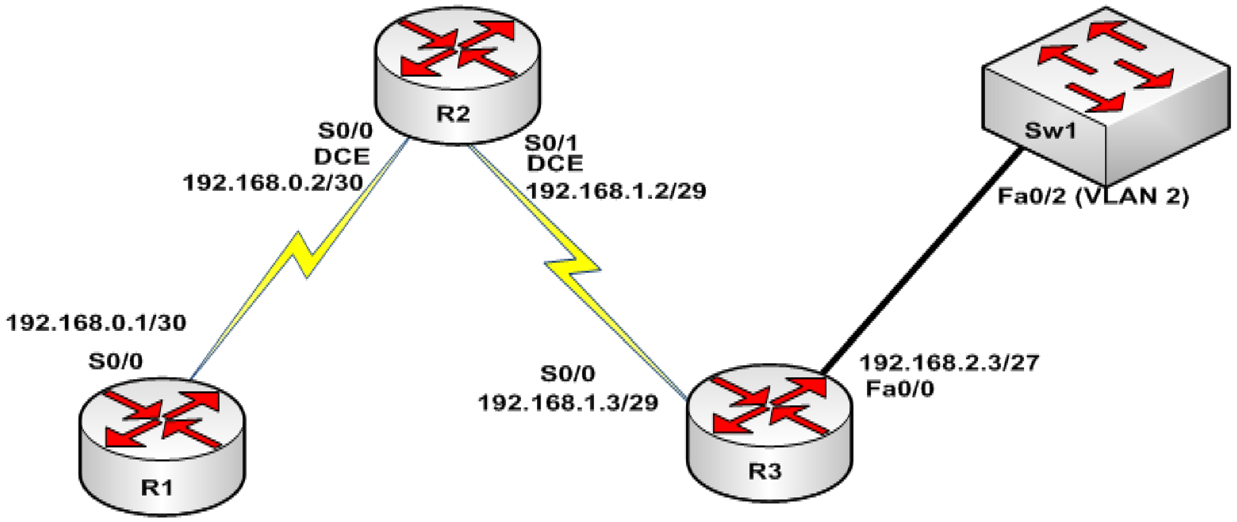
This lab has a difficulty rating of 10/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

Lab Topology:

Please use the following topology to complete this lab.



Interface	IP Address
Loopback 101	10.10.1.1/27
Loopback 102	10.10.2.1/26
Loopback 103	10.10.3.1/29

Task 1:

Configure the hostname on all devices as illustrated in the network topology.

Task 2:

Configure VLAN 2 on Sw1 and name it EIGRP_VLAN. Assign port FastEthernet0/2 to this VLAN. In addition, configure interface VLAN 2 on Sw1 and assign it the IP address 192.168.2.4. Sw1 should have a default gateway of 192.168.2.3

Task 3:

Configure the Loopback interfaces on R2 as illustrated in the topology. Configure the IP addressing on the Serial interfaces of R1, R2 and R3. Make sure that the DCE interfaces provide clocking at 2Mbps.

Task 4:

Configure the link between R1 and R2 to use PPP encapsulation. This link should also use PPP CHAP authentication using the password CISCO123 for both routers. When complete, make sure R1 and R2 can still ping each other.

Task 5:

Configure the link between R2 and R3 to use PPP encapsulation. This link should also use PPP PAP authentication using the password CISCO456 for both routers. The routers should send their hostnames as PAP usernames. When complete, make sure R2 and R3 can still ping each other.

Task 6:

Configure a default static route on R1 pointing to the IP address of R2. Configure a default static route on R3 pointing to the IP address of R2.

Task 7:

Configure the following 4 static routes to R2 as follows:

Network / Subnet	Next-Hop For Static Route
10.10.1.0/27	R1 Serial0/0
10.10.2.0/26	R1 Serial0/0
10.10.3.0/29	R1 Serial0/0
192.168.2.0/27	R3 Serial0/0

After your static routing configuration is complete, make sure all devices in the network can ping each other. If they cannot, then you need to check your configuration.

Task 8:

Configure Sw1 as a part of the DNS domain howtonetwork.net. Configure name resolution via DNS on Sw1 by an imaginary DNS server with the IP address 192.168.254.1. Enable DNS lookups on Sw1.

Task 8:

Configure R1, R2 and R3 to log all level 5 messages to an imaginary SYSLOG server with the IP address 10.1.254.1.

SOLUTION:

Challenge Lab 6: Configuration Hints

Task 1 Hints & References

For reference information on configuring hostnames, please refer to:

Lab 21 Configuration and Verification Task 1

Lab 35 Configuration and Verification Task 1

Task 2 Hints & References

For reference information on configuring standard VLANs, please refer to:

Lab 1 Configuration and Verification Task 1

Lab 1 Configuration and Verification Task 2

Lab 2 Configuration and Verification Task 2

Lab 3 Configuration and Verification Task 1

Task 3 Hints & References

For reference information on configuring IP interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

Lab 56 Configuration and Verification Task 2

Task 4 Hints & References

For reference information on enabling PPP Authentication, please refer to:

Lab 23 Configuration and Verification Task 5

Lab 24 Configuration and Verification Task 5

Lab 25 Configuration and Verification Task 5

Task 5 Hints & References

For reference information on enabling PPP Authentication, please refer to:

Lab 23 Configuration and Verification Task 5

Lab 24 Configuration and Verification Task 5

Lab 25 Configuration and Verification Task 5

Task 6 Hints & References

To complete this task you need to use the ip route command.

For reference information on configuring static routes, please refer to:

Lab 31 Configuration and Verification Task 4

Lab 32 Configuration and Verification Task 3

Lab 33 Configuration and Verification Task 4

Lab 34 Configuration and Verification Task 4

Task 7 Hints & References

You need to use the ip route command to complete this task. The subnet masks for the networks are:

10.10.1.0 255.255.255.224

10.10.2.0 255.255.255.192

10.10.3.0 255.255.255.248

192.168.2.0 255.255.255.224

For reference information on configuring static routes, please refer to:

Lab 31 Configuration and Verification Task 4

Lab 32 Configuration and Verification Task 3

Lab 33 Configuration and Verification Task 4

Lab 34 Configuration and Verification Task 4

Task 8 Hints & References

For reference information on configuring DNS, please refer to:

Lab 74 Configuration and Verification Task 2

Challenge Lab 7: Subnetting, Summarization, Static Routing and ACLs

Lab Objective:

This is a challenge lab designed to test and validate the skills you have acquired throughout this lab guide on subnetting, static routing and ACLs.

Lab Purpose:

The purpose of this lab is to reinforce route summarization, static routing and ACLs.

Certification Level:

This lab is suitable for CCNA certification exam preparation

Lab Difficulty:

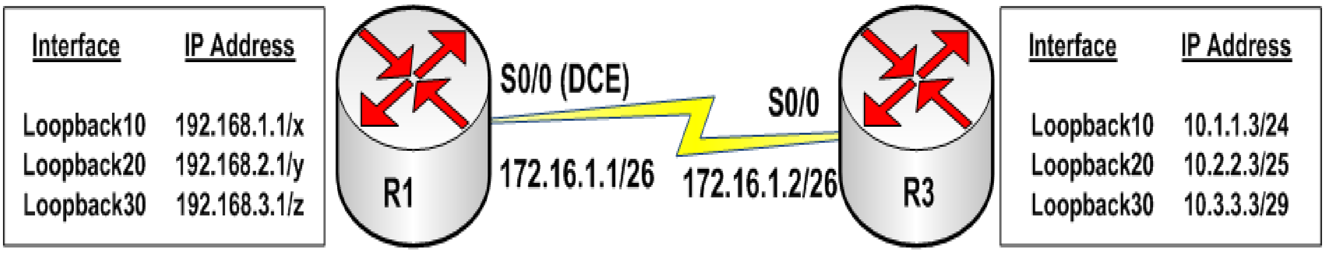
This lab has a difficulty rating of 10/10

Readiness Assessment:

When you are ready for your certification exam, you should complete this lab in no more than 20 minutes

Lab Topology:

Please use the following topology to complete this lab.



Task 1:

Configure the hostname on R1 and R3 devices as illustrated in the network topology.

Task 2:

Configure the Loopback interfaces on R3 as illustrated in the network topology.

Task 3:

Configure a SINGLE static route on R1 for the three 10.x.x.x subnets on R3. Do NOT use a default route. This route should be as specific as possible. Do NOT use 10.0.0.0/16 as the static route.

Task 4:

Configure the Loopbacks on R1 as follows:

- For Loopback10, replace x with a subnet mask that can support 59 hosts
- For Loopback20, replace y with a subnet mask that can support 22 hosts
- For Loopback30, replace z with a subnet mask that can support 5 hosts

Task 5:

Configure a SINGLE static route on R3 for the three 192.168.x.x subnets on R1. Do NOT use a default route. This route should be as specific as possible. Do NOT use 192.168.0.0/16 as the static route.

Task 6:

Configure a named ACL on R1 that does the following:

- Permits Telnet traffic from 10.1.1.0/24 to 192.168.1.0/x
- Permits Ping traffic from 10.2.2.0/25 to 192.168.2.0/y
- Permits HTTP traffic from 10.3.3.0/29 to 192.168.3.0/z
- Permits RIPv2 traffic from host 172.16.1.2 to host 172.16.1.1
- Denies Traceroute traffic from the 10.x.x.x subnets to the 192.168.x.x subnets (using a single line!)
- Denies DNS traffic from 10.3.3.0/29 to 172.16.1.0/30
- Permits IP traffic from the any source to any destination - which must be LOGGED!

Apply this ACL inbound on R1 S0/0.

Task 7:

Configure a named ACL on R3 that does the following:

- Denies EIGRP traffic from 172.16.1.0/30 to any destination
- Denies OSPF traffic from 172.16.1.0/30 to any destination
- Permits FTP traffic from 10.1.1.0/24 and 10.3.3.0/29 to host 192.168.2.1/y
- Denies HTTPS traffic from any source to 192.168.3.0/z
- Permit IP traffic from any source to any destination – which must be LOGGED!

Apply this ACL outbound on R3 S0/0.

SOLUTION:

Challenge Lab 7: Configuration Hints

Task 1 Hints & References

For reference information on configuring hostnames, please refer to:

Lab 21 Configuration and Verification Task 1

Lab 35 Configuration and Verification Task 1

Task 2 Hints & References

For reference information on configuring IP interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

Lab 56 Configuration and Verification Task 2

Task 3 Hints & References

You need to be solid in subnetting to complete this task. Your summary would be 10.0.0.0 255.252.0.0 or 10.0.0.0/14 in CIDR notation. If you got it, you're right on the money!

For reference information on configuring static routes, please refer to:

Lab 31 Configuration and Verification Task 4

Lab 32 Configuration and Verification Task 3

Lab 33 Configuration and Verification Task 4

Lab 34 Configuration and Verification Task 4

Task 4 Hints & References

You need to be solid in subnetting to complete this task. The Loopbacks should be:

192.168.1.1 255.255.255.192 or 192.168.1.1/26

192.168.2.1 255.255.255.224 or 192.168.2.1/27

192.168.3.1 255.255.255.248 or 192.168.3.1/29

For reference information on configuring IP interfaces, please refer to:

Lab 31 Configuration and Verification Task 3

Lab 56 Configuration and Verification Task 2

Task 5 Hints & References

Again, you need to be solid with subnetting to complete this task. The route would be:

192.168.0.0 255.255.252.0 or 192.168.0.0/22 in CIDR notation

Task 6 Hints & References

Use an extended ACL to complete this task

For reference information on configuring ACL logging, please refer to:

Lab 64 Configuration and Verification Task 4

For reference information on configuring ACLs, please refer to:

Lab 62 Configuration and Verification Task 5

Lab 62 Configuration and Verification Task 5

Lab 63 Configuration and Verification Task 4

Lab 64 Configuration and Verification Task 4

Task 7 Hints & References

For reference information on configuring ACL logging, please refer to:

Lab 64 Configuration and Verification Task 4

For reference information on configuring ACLs, please refer to:

Lab 62 Configuration and Verification Task 5

Lab 62 Configuration and Verification Task 5

Lab 63 Configuration and Verification Task 4

Lab 64 Configuration and Verification Task 4

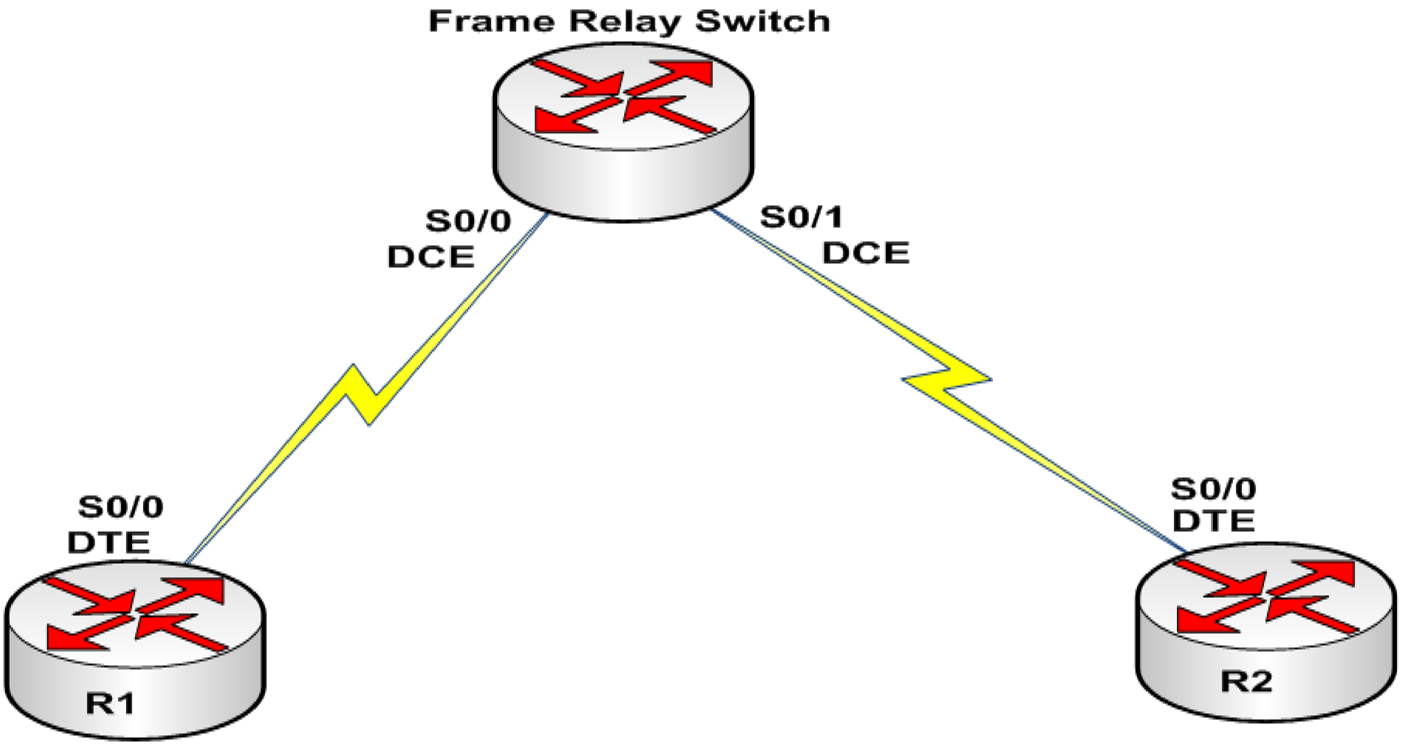
APPENDIX

Appendix A:

Cabling and configuring a Frame Relay Switch for Two Routers

Figure 1:

Frame Relay Physical Lab Cabling



Frame Relay Switch Configuration

```
hostname FR-SWITCH

!

frame-relay switching

!

interface serial0/0

description 'Connected to R1 Serial0/0'

encapsulation frame-relay

frame-relay intf-type dce

frame-relay route 111 interface serial0/1 222

clock rate 256000
```

```
no shutdown

!

interface serial0/1

description 'Connected to R2 Serial0/0'

encapsulation frame-relay

frame-relay intf-type dce

frame-relay route 222 interface serial0/0 111

clock rate 256000

no shutdown

!

end
```

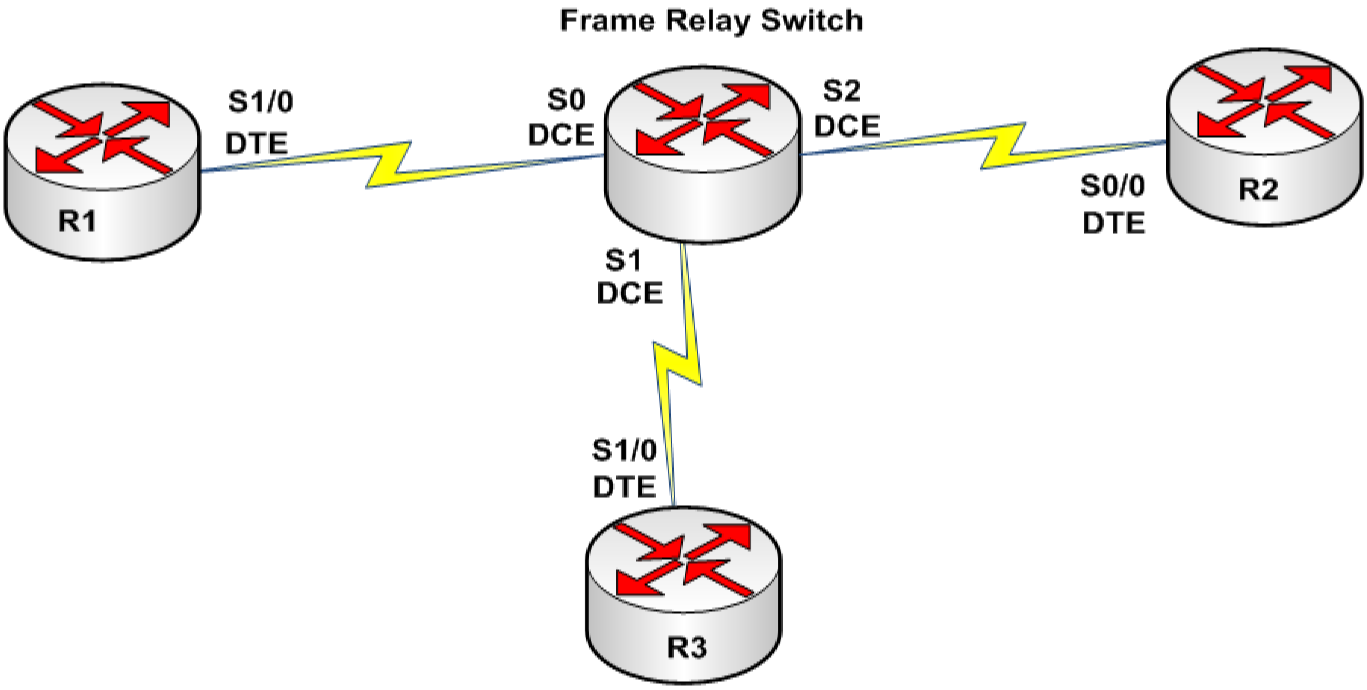
NOTE: This Frame Relay Switch configuration is based on the configuration of a Cisco 2610 IOS router with two Serial interfaces. The router is running a basic Enterprise IOS image.

Appendix B:

Cabling and configuring a Frame Relay Switch for Three Routers

Figure 1:

Frame Relay Physical Lab Cabling



Frame Relay Switch Configuration

```
hostname FR-SWITCH

!

frame-relay switching

interface serial0

description 'Connected to R1 Serial1/0'

encapsulation frame-relay

frame-relay intf-type dce

frame-relay route 103 interface serial1 301

frame-relay route 102 interface serial2 201

clock rate 800000

no shutdown

!

interface serial1

description 'Connected to R3 Serial1/0'

encapsulation frame-relay

frame-relay intf-type dce

frame-relay route 301 interface serial0 103

clock rate 800000

no shutdown

!

serial2

description 'Connected to R2 Serial0/0'

encapsulation frame-relay

frame-relay intf-type dce

frame-relay route 201 interface serial0 102

clock rate 115200
```

```
no shutdown

!

end
```

NOTE: This Frame Relay Switch configuration is based on the configuration of a Cisco 2521 IOS router with four Serial interfaces. The router is running a basic Enterprise IOS image.