



CISCO

CCNA Certification

ICND2 Lab Guide

Version 2.0 Issue 1.01

www.firebrandtraining.com

ICND2

Interconnecting Cisco Networking Devices, Part 2

Version 2.0



Lab Guide

Issue v1.01

Table of Contents

Physical Topology Diagram

Lab 1-1: VLANs and Trunks Connections

Visual Topology

Command List

Task 1: Reload and check that the Switch is set to factory defaults.

Task 2: Basic switch set-up.

Task 3: Configure basic VLAN and Trunk connections.

Task 4: Troubleshoot Trunk failure.

Lab 1-2: Optimizing STP

Visual Topology

Command List

Task 1: Verify STP operation.

Task 2: Manipulating Root Bridge selection.

Task 3: Configuring Rapid Spanning-tree

Task 4: Using STP Portfast.

Lab 1-3: Configuring EtherChannel

Visual Topology

Command List

Task 1: EtherChannel configuration



Lab 3-1: Implementing EIGRP

Visual Topology

Command List

Task 1: Remote network connectivity.

Task 2: Configure EIGRP

Task 3: Using show commands to verify EIGRP parameters

Lab 3-2: Implementing EIGRP for IPv6

Visual Topology

Command Line

Task 1: Setting up IPv6 on the interface.

Task 2: Enabling EIGRP for IPv6.

Lab 4-1: Implementing OSPF in a Multi-area Environment

Visual Topology

Command Line

Task 1: Configuring a multi-area OSPF network.

Lab 4-2: Implementing OSPF for IPv6

Visual Topology

Command Line

Task 1: Enabling OSPFv3



Lab 5-1: Setting up a Serial Connection

Visual Topology

Command Line

Task 1: Using HDLC

Task 2: Configuring PPP

Task 3: Setting up PPP authentication

Lab 5-2: Establishing a Frame Relay Connection

Visual Topology

Command Line

Task 1: Setting up a basic Frame-relay link

Task 2: Supporting Frame-relay using sub-interfaces

Lab 6-1: SNMP and Syslog Basic Configuration

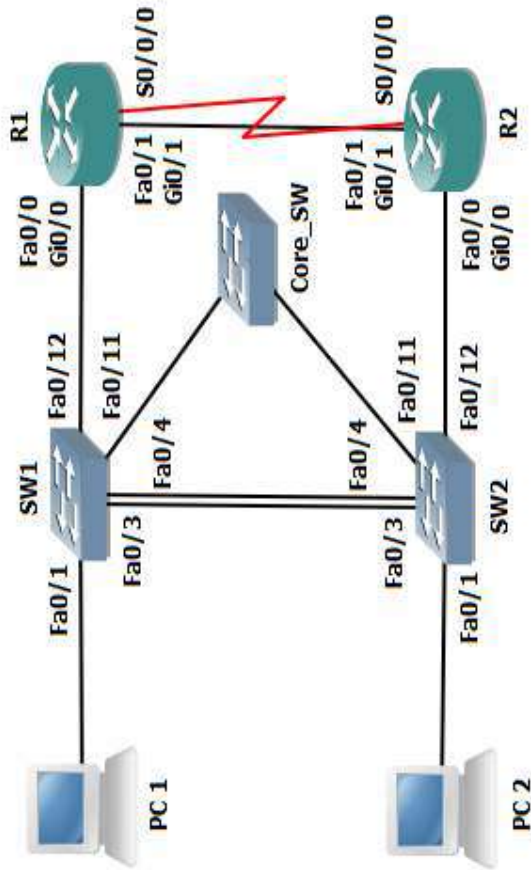
Visual Topology

Command Line

Task 1: Configure a Router for SNMP access

Task 2: Configure a Router for Syslog Services

Lab Answer Keys:



Connections Table

- PC - Switch Fa0/1
- SW1 Fa0/3 - SW2 Fa0/3
- SW1 Fa0/4 - SW2 Fa0/4
- SW1 Fa0/11 - Core_SW Fa0/X see note 1
- SW2 Fa0/11 - Core_SW Fa0/X see note 1
- SW1 Fa0/12 - R1 Fa0/0 or Gi0/0 see note 2
- SW2 Fa0/12 - R2 Fa0/0 or Gi0/0 see note 2
- R1 S0/0/0 - R2 S0/0/0
- R1 Fa0/1 or Gi0/1 - R2 Fa0/1 or Gi0/1 see note 2

Note 1

This topology supports 2 students, each student gets to configure PC1, SW1 & R1 or PC2, SW2 & R2. The Core Switch is managed by the instructor for all student connections.

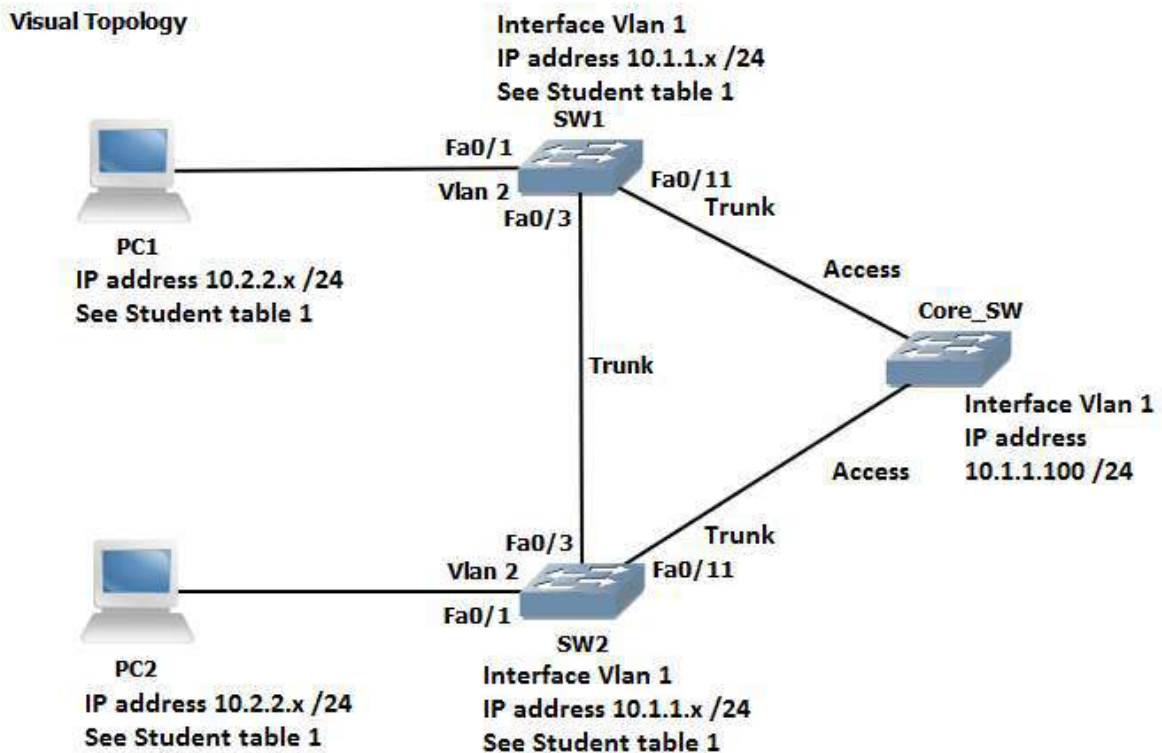
Students will need to work in pairs during some of the lab exercises.

Note 2

If R1 and R2 are 2811 routers then use Fa0/0 and Fa0/1

If R1 and R2 are 2901 routers then use Gi0/0 and Gi0/1

Lab 1-1: VLANs and Trunk Connections.



Command List

Command	Description
Configure Terminal	Enters global configuration mode
Copy run start	Saves your dynamic running config to NVRAM
Delete flash:vlan.dat	Deletes a file
Do <i>command</i>	Allows for the execution of commands located in a different mode
Enable	Enters privileged EXEC mode from user EXEC mode
End	Terminates configuration mode
Erase startup-config	Erases the startup-configuration from NVRAM
Exit	Exits current configuration mode
Hostname <i>name</i>	Sets a system name and is displayed within the system prompt
Interface <i>type/slot/id</i>	Enters the interface configuration mode
Interface Vlan 1	Enters the interface configuration (SVI) for Vlan 1 and allows you to set the management IP address for the switch
IP address <i>address & mask</i>	Set an IP address and also the network/subnet mask
Line console 0	Enters line console configuration mode
Logging synchronous	Prevents unsolicited messages from interfering when typing in your commands

Name <i>vlan name</i>	Used in vlan configuration mode to assign a descriptive name
Reload	Restarts the device
Show flash:	Displays the contents of the flash memory
Show startup-config	Displays the startup-config saved in NVRam
Show version	Displays hardware and software information
[no] Shutdown	Disables or enables an interface
Switchport access vlan <i>id</i>	Assigns a switchport to a data vlan
Switchport mode access	Puts the switchport into access mode
Switchport mode trunk	Puts the switchport into trunk mode
[no] Vlan <i>id</i>	Deletes or creates a vlan and enters vlan configuration mode

*** The instructor will assign you with a student ID (student 1 to 16).***

Please note that for this exercise students are expected to work in pairs.

Refer to the **Student Table 1** when allocating IP addresses and VLANs, failure to do so will result in IP address conflict messages and inconsistent lab results.

Student Table 1.

	Student ID	PC IP address & mask	Switch SVI (VLAN 1) IP address	VLAN assignments
Pair 1	Student 1	10.2.2.101 /24	10.1.1.1 /24	2 & 3
Pair 1	Student 2	10.2.2.102 /24	10.1.1.2 /24	2 & 3
Pair 2	Student 3	10.2.2.103 /24	10.1.1.3 /24	2, 4 & 5
Pair 2	Student 4	10.2.2.104 /24	10.1.1.4 /24	2, 4 & 5
Pair 3	Student 5	10.2.2.105 /24	10.1.1.5 /24	2, 6 & 7
Pair 3	Student 6	10.2.2.106 /24	10.1.1.6 /24	2, 6 & 7
Pair 4	Student 7	10.2.2.107 /24	10.1.1.7 /24	2, 8 & 9
Pair 4	Student 8	10.2.2.108 /24	10.1.1.8 /24	2, 8 & 9
Pair 5	Student 9	10.2.2.109 /24	10.1.1.9 /24	2, 10 & 11
Pair 5	Student 10	10.2.2.110 /24	10.1.1.10 /24	2, 10 & 11
Pair 6	Student 11	10.2.2.111 /24	10.1.1.11 /24	2, 12 & 13
Pair 6	Student 12	10.2.2.112 /24	10.1.1.12 /24	2, 12 & 13
Pair 7	Student 13	10.2.2.113 /24	10.1.1.13 /24	2, 14 & 15
Pair 7	Student 14	10.2.2.114 /24	10.1.1.14 /24	2, 14 & 15
Pair 8	Student 15	10.2.2.115 /24	10.1.1.15 /24	2, 16 & 17
Pair 8	Student 16	10.2.2.116 /24	10.1.1.16 /24	2, 16 & 17



Task 1: Reload and check that the Switch is set to factory defaults.

Step 1: Assign an IP address to your PC using the details listed in **Student Table 1**. The PC should be fitted with two network adapters check with the instructor if you are unsure which network adapter should be configured.

Step 2: Access the Switch Console port using the method and information provided by the instructor.

Enter into privilege mode and use the **erase startup-config** command to remove any previous saved configuration.

(If you see any other prompt or are asked for a password contact the instructor).

Step 3: Switches hold information about logical VLANs in a database stored in their flash memory and it is necessary to delete this database to reset the Switch back to factory defaults. **PLEASE BE VERY CAREFUL WHEN USING THE DELETE COMMAND.**

From privilege mode type in the following command and follow the system messages (if you are unsure what to do, contact the instructor before answering any of the system messages).

```
Switch#Delete flash:vlan.dat
```

confirm the deletion

Step 4: Reload the Switch.

confirm the reload

Please note the Switch may take a few minutes to reload.

NB. ASK THE INSTRUCTOR TO RESET THE CORE_SW BACK TO FACTORY DEFAULTS!

Task 2: Basic switch set-up

Step 1: Change the hostname of the Switch to either **SW1** or **SW2**

Step 2: Assign your Switch a management IP address using the values identified in the table below.

Device	IP Address	Mask	SVI (logical interface)
SW1	See Student Table 1	255.255.255.0	vlan 1
SW2	See Student Table 1	255.255.255.0	vlan 1

Remember to enable the SVI so the IP address is active.



Task 3: Configure basic VLAN and Trunk connections.

Step 1: Create the VLANs listed in **Student Table 1** and label Vlan2 with your pair name.

Example, **student 7** needs to create **VLANs 2, 8 and 9** and name Vlan 2, **Pair4**. Use the default names for the other Vlans created.

Step 2: Disable interface fa0/1 and put it into an access state

Hint....switchport mode ?

Step 3: Re-assign interface fa0/1 and place it into Vlan 2

Step 4: enable interface fa0/1

Step 5: Disable all other interfaces except fa0/1 and Vlan 1

Step 6: Configure interface fa0/3 and interface fa0/11 to support trunking without using a dynamic protocol trunking protocol.

Hint.....switchport mode ?

In the table below indicate which modes generate DTP messages.

Switchport mode access	
Switchport mode trunk	
Switchport mode dynamic auto	
Switchport mode dynamic desirable	

What is the command for disabling DTP?

Step 7: Enable interfaces fa0/3 and fa0/11 and disable DTP on all active interfaces.

Task 4: Troubleshooting Trunk failures

Step 1: Confirm with the instructor that the Core switch has been reset back to factory defaults?

Step 2: Ask the instructor to configure all of the ports on the Core switch as **ACCESS** ports.

When a switch has been reset to factory defaults and the ports have been set to access mode, what is the default allocated VLAN for the port?



Step 3: From privilege mode execute the following commands.

```
show interface fa0/3 switchport
```

```
show interface fa0/11 switchport
```

```
show interface fa0/1 switchport
```

Below are examples of output generated on SW1 but results should be similar on SW2 also.

```
SW1#sh interfaces fa0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
SW1#
```

Observe the Switchport status, Administrative mode, Operational mode.

What do you think the **Negotiation of Trunking: Off** line indicates?

```
SW1#sh interfaces fa0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
SW1#
```

```
SW1#sh int fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 2 (Pair1)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
SW1#
```

Interface Fa0/1 is attached to your PC.

Note that the Operational Mode is set to Static Access and the Access Mode VLAN is assigned to VLAN 2 with a name Pair1 (name will differ dependant on your pairings)



Step 4: ASK the Instructor to configure and enable the SVI (VLAN1) interface on the Core switch with an IP address of 10.1.1.100 /24.

Step 5: Ping 10.1.1.100 from you Switch

```
SW1#ping 10.1.1.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

SW1#
```

Explain, why the PING worked? Remembering that you have configured the switchport which connects you to the Core Switch as a Trunk link, however the Core Switch is configured in Static Access mode.

Step 6: From your PC ping 10.1.1.100.

```
PC>ping 10.1.1.100

Pinging 10.1.1.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

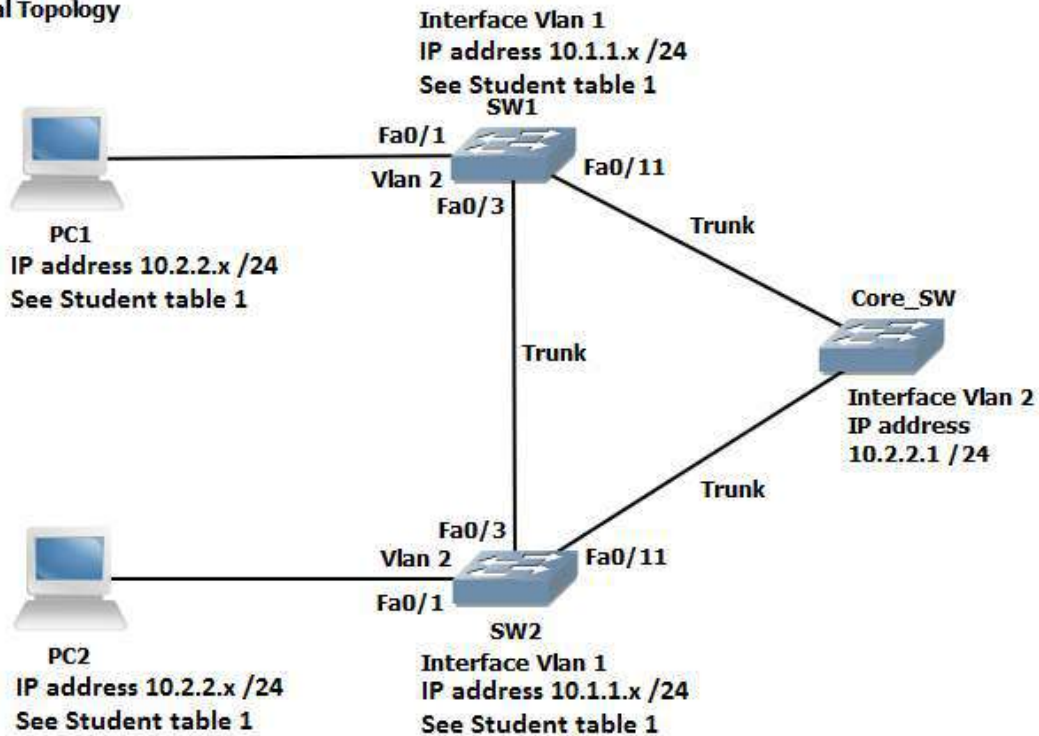
PC>|
```

Why does it fail?

Step 7: Save your running-config

Lab 1-2: Optimizing STP

Visual Topology



Command List

Commands	Description
Configure Terminal	Enters global configuration mode.
Copy run start	Saves the dynamic running-config to NVRAM.
[no] debug spanning-tree events	
Interface Fastethernet 0/0	Specifies interface fa0/0
Interface Gigabitethernet 0/0	Specifies interface gi0/0
Ping <i>ip-address or hostname</i>	Checks IP connectivity
Show Interface Fastethernet 0/0	Displays information about interface fa0/0
Show Interface Gigabitethernet 0/0	Displays information about interface gi0/0
Show IP Interface Brief	Displays a brief summary of the device interfaces
Show spanning-tree summary	STP summary of port states and operational status

Show spanning-tree vlan <i>id</i>	Displays spanning-tree information for a specified VLAN
Show spanning-tree vlan <i>id</i> root detail	Displays detailed spanning-tree status
Show vlan	
Shutdown/ No Shutdown	Disables or enable an interface
[no] spanning-tree bpduguard enable	Disable or enables the BPDU guard feature on a port
Spanning-tree mode rapid-PVST	Enables Per-VLAN rapid spanning-tree
Spanning-tree portfast	Enables STP portfast feature on a port
Spanning-tree vlan <i>id</i> root primary	Forces this switch to be the root bridge for a specified VLAN
Spanning-tree vlan <i>id</i> root secondary	Sets the switch to become the new root bridge if the current root bridge fails
Switchport mode trunk	Statically configures the port for trunking
Switchport nonegotiate	Disables DTP
Switchport trunk allowed vlan <i>vlan list</i>	Filters which VLAN's are permitted across a trunk connection.

Student table 1

	Student ID	PC IP address & mask	Switch SVI (VLAN 1) IP address	VLAN
Pair 1	Student 1	10.2.2.101 /24	10.1.1.1 /24	2 & 3
Pair 1	Student 2	10.2.2.102 /24	10.1.1.2 /24	2 & 3
Pair 2	Student 3	10.2.2.103 /24	10.1.1.3 /24	2, 4 & 5
Pair 2	Student 4	10.2.2.104 /24	10.1.1.4 /24	2, 4 & 5
Pair 3	Student 5	10.2.2.105 /24	10.1.1.5 /24	2, 6 & 7
Pair 3	Student 6	10.2.2.106 /24	10.1.1.6 /24	2, 6 & 7
Pair 4	Student 7	10.2.2.107 /24	10.1.1.7 /24	2, 8 & 9
Pair 4	Student 8	10.2.2.108 /24	10.1.1.8 /24	2, 8 & 9
Pair 5	Student 9	10.2.2.109 /24	10.1.1.9 /24	2, 10 & 11
Pair 5	Student 10	10.2.2.110 /24	10.1.1.10 /24	2, 10 & 11
Pair 6	Student 11	10.2.2.111 /24	10.1.1.11 /24	2, 12 & 13
Pair 6	Student 12	10.2.2.112 /24	10.1.1.12 /24	2, 12 & 13
Pair 7	Student 13	10.2.2.113 /24	10.1.1.13 /24	2, 14 & 15
Pair 7	Student 14	10.2.2.114 /24	10.1.1.14 /24	2, 14 & 15
Pair 8	Student 15	10.2.2.115 /24	10.1.1.15 /24	2, 16 & 17
Pair 8	Student 16	10.2.2.116 /24	10.1.1.16 /24	2, 16 & 17

Student table 2

	Student ID	Spanning-tree root bridge primary	Spanning-tree root bridge secondary
Pair 1	Student 1	Vlan 2	Vlan 3
Pair 1	Student 2	Vlan 3	Vlan 2
Pair 2	Student 3	Vlan 4	Vlan 5
Pair 2	Student 4	Vlan 5	Vlan 4
Pair 3	Student 5	Vlan 6	Vlan 7
Pair 3	Student 6	Vlan 7	Vlan 6
Pair 4	Student 7	Vlan 8	Vlan 9
Pair 4	Student 8	Vlan 9	Vlan 8
Pair 5	Student 9	Vlan 10	Vlan 11
Pair 5	Student 10	Vlan 11	Vlan 10
Pair 6	Student 11	Vlan 12	Vlan 13
Pair 6	Student 12	Vlan 13	Vlan 12
Pair 7	Student 13	Vlan 14	Vlan 15
Pair 7	Student 14	Vlan 15	Vlan 14
Pair 8	Student 15	Vlan 16	Vlan 17
Pair 8	Student 16	Vlan 17	Vlan 16

Before starting the Lab, confirm with the Instructor that the Core Switch has been configured with all of its ports in trunk mode (see visual diagram) and a SVI (vlan2) has been set-up and enabled with the IP address 10.2.2.1 /24.

To prevent the unwanted propagation of the vlan database from the Core_SW ask the instructor to place the Core_SW into VTP transparent mode.

To aid with your understanding of the Lab exercise and how the Core switch is configured the running-config has been provided for you.

```
Core_SW#sh run
```

```
!
```

```
hostname Core_SW
```

```
!
```

```
vtp mode transparent
```

```
!
```

```
spanning-tree mode pvst
```

```
!
```


vlan 2  FIREBRAND

name Pair1

!

vlan 3

!

vlan 4

name Pair2

!

vlan 5

!

vlan 6

name Pair3

!

vlan 7

!

vlan 8

name Pair4

!

vlan 9

!

vlan 10

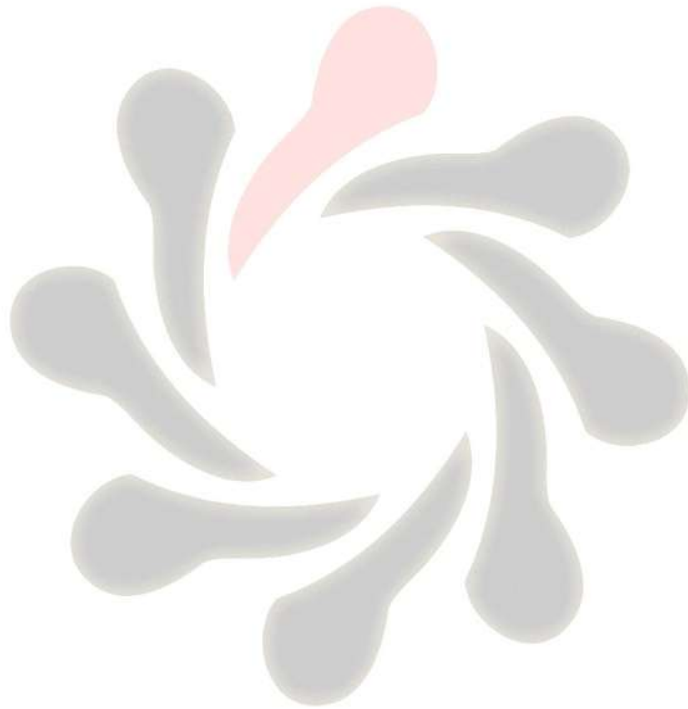
name Pair5

!

vlan 11

!

vlan 12



name Pair6  **FIREBRAND**

!

vlan 13

!

vlan 14

name Pair7

!

vlan 15

!

vlan 16

name Pair8

!

vlan 17

!

interface FastEthernet0/1

description Link to Student 1 Switch

switchport trunk allowed vlan 1-3

switchport mode trunk

switchport nonegotiate

!

interface FastEthernet0/2

description Link to Student 2 Switch

switchport trunk allowed vlan 1-3

switchport mode trunk

switchport nonegotiate

!





```
interface FastEthernet0/3
description Link to Student 3 Switch
switchport trunk allowed vlan 1-2,4-5
switchport mode trunk
switchport nonegotiate
```

!

```
interface FastEthernet0/4
description Link to Student 4 Switch
switchport trunk allowed vlan 1-2,4-5
switchport mode trunk
switchport nonegotiate
```

!

```
interface FastEthernet0/5
description Link to Student 5 Switch
switchport trunk allowed vlan 1-2,6-7
switchport mode trunk
switchport nonegotiate
```

!

```
interface FastEthernet0/6
description Link to Student 6 Switch
switchport trunk allowed vlan 1-2,6-7
switchport mode trunk
switchport nonegotiate
```

!





```
interface FastEthernet0/7
description Link to Student 7 Switch
switchport trunk allowed vlan 1-2,8-9
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/8
description Link to Student 8 Switch
switchport trunk allowed vlan 1-2,8-9
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/9
description Link to Student 9 Switch
switchport trunk allowed vlan 1-2,10-11
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/10
description Link to Student 10 Switch
switchport trunk allowed vlan 1-2,10-11
switchport mode trunk
switchport nonegotiate
!
```





interface FastEthernet0/11

description Link to Student 11 Switch

switchport trunk allowed vlan 1-2,12-13

switchport mode trunk

switchport nonegotiate

!

interface FastEthernet0/12

description Link to Student 12 Switch

switchport trunk allowed vlan 1-2,12-13

switchport mode trunk

switchport nonegotiate

!

interface FastEthernet0/13

description Link to Student 13 Switch

switchport trunk allowed vlan 1-2,14-15

switchport mode trunk

switchport nonegotiate

!

interface FastEthernet0/14

description Link to Student 14 Switch

switchport trunk allowed vlan 1-2,14-15

switchport mode trunk

switchport nonegotiate

!

interface FastEthernet0/15

description Link to Student 15 Switch





```
switchport trunk allowed vlan 1-2,16-17
```

```
switchport mode trunk
```

```
switchport nonegotiate
```

```
!
```

```
interface FastEthernet0/16
```

```
description Link to Student 16 Switch
```

```
switchport trunk allowed vlan 1-2,16-17
```

```
switchport mode trunk
```

```
switchport nonegotiate
```

```
!
```

```
interface Vlan1
```

```
no ip address
```

```
shutdown
```

```
!
```

```
interface Vlan2
```

```
ip address 10.2.2.1 255.255.255.0
```

```
!
```

```
end
```

```
-----Some output omitted-----
```





Task 1: Verify STP Operation.

Step 1: Confirm that you have interfaces fa0/1, fa0/3 and fa0/11 enabled.

Step 2: From your PC ping 10.2.2.1. This should be successful

```
PC>
PC>ping 10.2.2.1

Pinging 10.2.2.1 with 32 bytes of data:

Request timed out.
Reply from 10.2.2.1: bytes=32 time=0ms TTL=255
Reply from 10.2.2.1: bytes=32 time=0ms TTL=255
Reply from 10.2.2.1: bytes=32 time=0ms TTL=255

Ping statistics for 10.2.2.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

If the ping fails, check you have the correct IP address on your PC, fa0/1 is statically assigned to VLAN 2, the Trunk connection between your switch and the Core switch is operational.

Step 3: View the visual topology diagram and you will notice that a bridging loop exists between your switch, the Core switch and the switch which is being managed by the other student. Spanning-tree (STP) is enabled by default and will detect the presence of a loop and take the necessary steps to prevent the loop by blocking one of the ports.

Use the show spanning-tree vlan *id* to determine which switch is the current Root Bridge for VLAN 1, VLAN 2 and your unique student pair VLANs.

Student ID	Student Pair	Unique VLANs
Students 1 & 2	Pair 1	2 & 3
Students 3 & 4	Pair 2	4 & 5
Students 5 & 6	Pair 3	6 & 7
Students 7 & 8	Pair 4	8 & 9
Students 9 & 10	Pair 5	10 & 11
Students 11 & 12	Pair 6	12 & 13
Students 13 & 14	Pair 7	14 & 15
Students 15 & 16	Pair 8	16 & 17



Would you expect to see the same Root Bridge for all VLANs?

How is the Root Bridge elected?

The following outputs are for reference only, outputs will vary.

```
SW1#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
            Address    000D.BD0A.A4C6
            This bridge is the root
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
            Address    000D.BD0A.A4C6
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/3          Desg FWD 19        128.3    P2p
Fa0/11         Desg FWD 19        128.11   P2p

VLAN0002
  Spanning tree enabled protocol ieee
  Root ID    Priority    32770
            Address    000D.BD0A.A4C6
            This bridge is the root
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32770  (priority 32768 sys-id-ext 2)
            Address    000D.BD0A.A4C6
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/3          Desg FWD 19        128.3    P2p
Fa0/1          Desg FWD 19        128.1    P2p
Fa0/11         Desg FWD 19        128.11   P2p
```




```

SW2#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority    32769
              Address    000D.BD0A.A4C6
              Cost      19
              Port      3(FastEthernet0/3)
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769 (priority 32768 sys-id-ext 1)
              Address    0060.2FDB.2E65
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/3          Root FWD 19        128.3    P2p
Fa0/11        Desg FWD 19        128.11   P2p

VLAN0002
  Spanning tree enabled protocol ieee
  Root ID      Priority    32770
              Address    000D.BD0A.A4C6
              Cost      19
              Port      3(FastEthernet0/3)
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32770 (priority 32768 sys-id-ext 2)
              Address    0060.2FDB.2E65
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/3          Root FWD 19        128.3    P2p
Fa0/11        Desg FWD 19        128.11   P2p

```

Using the information obtained from your switch complete the table below.

Root Bridge ID for VLAN 1	
Root Bridge ID for VLAN 2	
Root Bridge ID for VLAN x (unique vlan in your student pair)	
Root Bridge ID for VLAN x (unique vlan in your student pair)	
Type of spanning-tree protocol	
Fa0/3 port role	
Fa0/3 port state	
Fa0/11 port role	
Fa0/11 port state	
Cost back to the Root Bridge	



Other show commands can be used to display information about Spanning-tree

Show spanning-tree summary (output for reference only)

```
SW2#  
SW2#sh spanning-tree summary  
Switch is in pvst mode  
Root bridge for:  
Extended system ID          is enabled  
Portfast Default            is disabled  
PortFast BPDU Guard Default is disabled  
Portfast BPDU Filter Default is disabled  
Loopguard Default          is disabled  
EtherChannel misconfig guard is disabled  
UplinkFast                  is disabled  
BackboneFast                is disabled  
Configured Pathcost method used is short  
  
Name                          Blocking Listening Learning Forwarding STP Active  
-----  
VLAN0001                       0           0           0           2           2  
VLAN0002                       0           0           0           2           2  
-----  
2 vlans                         0           0           0           4           4  
  
SW2#  
SW2#  
SW2#
```

Show spanning-tree vlan 1 root detail

SW1#sh spanning-tree vlan 1 root detail

VLAN0001

```
Root ID      Priority    32769  
Address      000D.BD0A.A4C6  
This bridge is the root  
Hello Time   2 sec    Max Age 20 sec    Forward Delay 15 sec
```

SW2#sh spanning-tree vlan 1 root detail

VLAN0001

```
Root ID      Priority    32769  
Address      000D.BD0A.A4C6  
Cost         19 (FastEthernet 0/3)  
Hello Time   2 sec    Max Age 20 sec    Forward Delay 15 sec
```



We can ascertain from the output of the previous commands that in this scenario **SW1** is clearly the **Root Bridge** and the best path to the Root Bridge for SW2 is via fa0/3 (root port).

Based on your results how did the switches decide which one of them should become the Root?

Task 2: Manipulating Root Bridge Selection.

In the previous task we used default settings, so the Root Bridge was elected based on the lowest MAC address.

Root bridge elections are pre-emptive and if a new switch is added to the network it can take over the role of the Root Bridge and influence the path decisions made by a switch when forwarding traffic. System administrators have the ability to manipulate the Root Bridge election and therefore create a more predictable switching environment.

Step 1:

Using the relevant commands force your switch to become the Root bridge and a backup Root Bridge for the VLANs indicated in the table below.

	Student ID	Spanning-tree root bridge primary	Spanning-tree root bridge secondary
Pair 1	Student 1	Vlan 2	Vlan 3
Pair 1	Student 2	Vlan 3	Vlan 2
Pair 2	Student 3	Vlan 4	Vlan 5
Pair 2	Student 4	Vlan 5	Vlan 4
Pair 3	Student 5	Vlan 6	Vlan 7
Pair 3	Student 6	Vlan 7	Vlan 6
Pair 4	Student 7	Vlan 8	Vlan 9
Pair 4	Student 8	Vlan 9	Vlan 8
Pair 5	Student 9	Vlan 10	Vlan 11
Pair 5	Student 10	Vlan 11	Vlan 10
Pair 6	Student 11	Vlan 12	Vlan 13
Pair 6	Student 12	Vlan 13	Vlan 12
Pair 7	Student 13	Vlan 14	Vlan 15
Pair 7	Student 14	Vlan 15	Vlan 14
Pair 8	Student 15	Vlan 16	Vlan 17
Pair 8	Student 16	Vlan 17	Vlan 16

Step 2: Verify step 1 using show commands.



Task 3: Configuring Rapid Spanning-tree

The default spanning-tree protocol on Cisco device is PVST+ (802.1D + 802.1Q) **Ask the Instructor to change the Core Switch.**

NB. You may need to wait for other students to catch up.

Step 1: Configure PVRST+

Step 2: Use an appropriate command to verify the change.

```
SW2#  
SW2#sh spanning-tree summary  
Switch is in rapid-pvst mode  
Root bridge for: SALES  
Extended system ID          is enabled  
Portfast Default            is disabled  
PortFast BPDU Guard Default is disabled  
Portfast BPDU Filter Default is disabled  
Loopguard Default          is disabled  
EtherChannel misconfig guard is disabled  
UplinkFast                  is disabled  
BackboneFast                is disabled  
Configured Pathcost method used is short
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	0	0	0	2	2
VLAN0002	0	0	0	2	2
2 vlans	0	0	0	4	4

```
SW2#
```

Step 3: Disable interface fa0/3

Step 4: Save your running-config

Task 4: Using STP Portfast

Spanning-tree portfast is used to transition a port straight from the spanning-tree blocking state to the spanning-tree forward state, it usually take less than 1 second for the port to become operational.

Step 1: Disable fa0/1 and configure it to use spanning-tree portfast.

Step 2: Run the following debug command.

Sw#debug spanning-tree events

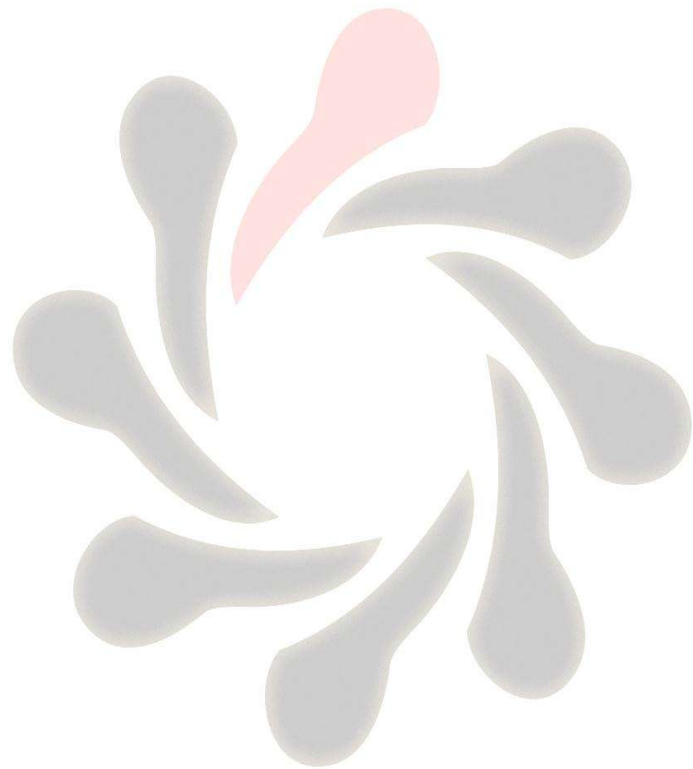


Step 3: Enable fa0/1 and monitor the output of the debug command.

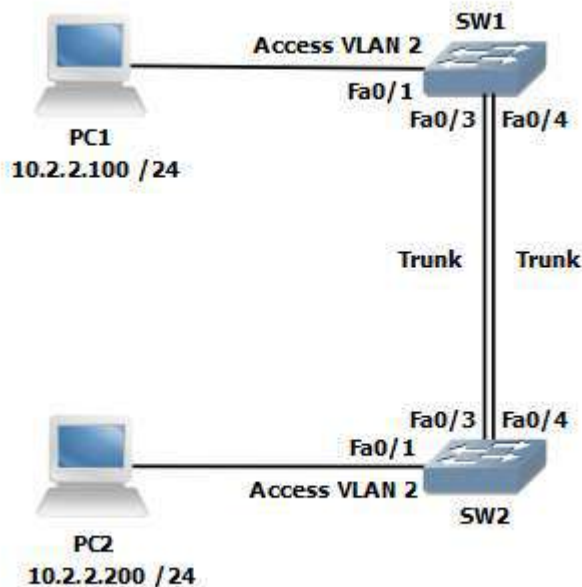
Look for a line similar to this, it should appear very soon after you enable the port.

Aug 15 17:10:45.529: STP: VLAN0002 Fa0/1 ->jump to forwarding from blocking

Step 4: Save your running-config



Lab 1-3: Configuring EtherChannel



Command List.

Command	Description
Channel-group <i>id</i> mode active	Configures an interface as EtherChannel bundle members using LACP in active mode.
Channel-group <i>id</i> mode passive	Configures an interface as EtherChannel bundle members using LACP in passive mode.
Configure Terminal	Enters global configuration mode.
Copy run start	Saves the dynamic running-config to NVRAM.
Interface range <i>range</i>	Enters interface range configuration mode
Show etherchannel port-channel	Displays port-channel interface information
Show Interface <i>interface</i>	Displays interface statistics
Show spanning-tree vlan <i>id</i>	Verifies spanning-tree information for a given VLAN

PC readiness: Assign the IP addresses used in the visual topology diagram for this exercise.

Task 1: EtherChannel Configuration

Step 1: Enable switchports fa0/1, fa0/3 and fa0/4 all other switchports should be shutdown.

Hint....Use the interface range command to speed up the process.

Step 2: Configure fa0/4 as a trunk connection.

Step 3: Validate that VLANs 1 and 2 are active on your switch



SW#sh vlan

Create vlan 2 if it doesn't exist.

Step 4: Because of the parallel links (fa0/3 & fa0/4) between the 2 switches spanning-tree will block one of the ports to prevent a loop.

Use an appropriate show command to verify this.

Step 5: Shutdown fa0/3 and fa0/4

Step 6:

SW1 only....

Configure fa0/3 and fa0/4 interfaces as part of an Etherchannel bundle. Use **1** as the port channel identifier and configure LACP in active mode.

SW2 only....

Configure fa0/3 and fa0/4 interfaces as part of an Etherchannel bundle. Use **1** as the port channel identifier and configure LACP in passive mode.

Step 7: Enable fa0/3 and fa0/4

Step 8:

SW1 only....

Execute

SW1#show spanning-tree vlan 2

```
SW1#sh spanning-tree vlan 2
VLAN0002
  Spanning tree enabled protocol rstp
  Root ID    Priority    24578
            Address    00E0.8FEE.948E
            Cost      9
            Port      27 (Port-channel 1)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32770 (priority 32768 sys-id-ext 2)
            Address    0090.0C23.95E5
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 20

Interface    Role  Sts  Cost    Prio.Nbr  Type
-----
Po1          Root  FWD  9        128.27    Shr
Fa0/1       Desg  FWD  19       128.1     P2p

SW1#
```

SW2 only



Execute

SW1#show spanning-tree vlan 1

```
SW2#
SW2#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
            Address    0090.0C23.95E5
            Cost        9
            Port        27 (Port-channel 1)
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
            Address    00E0.8FEE.948E
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  20

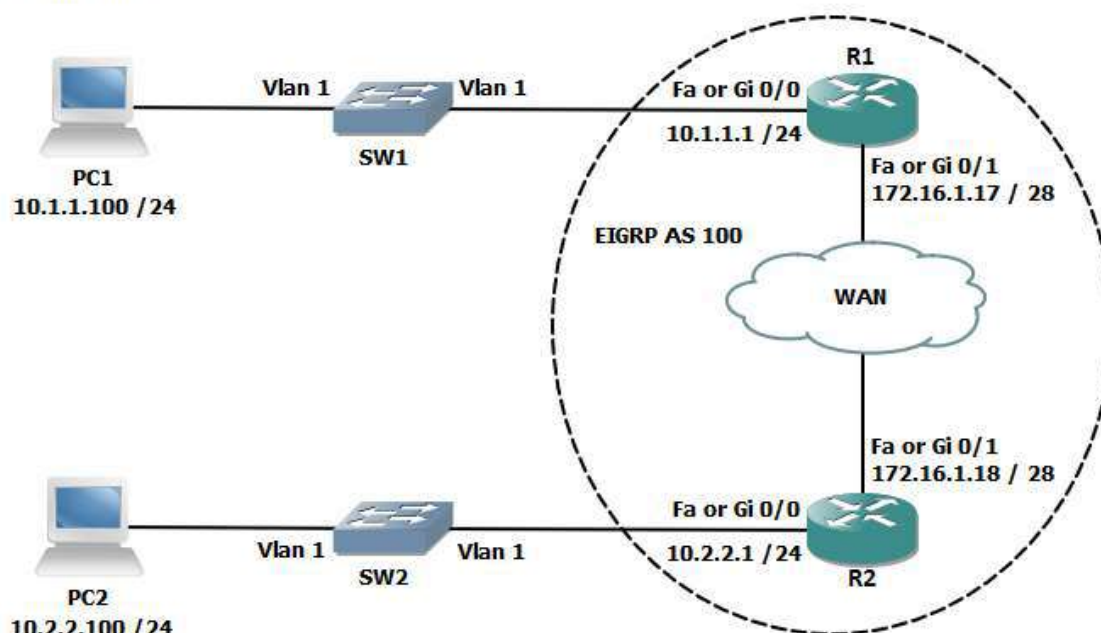
Interface          Role Sts Cost          Prio.Nbr Type
-----
Po1                 Root FWD 9             128.27 Shr
SW2#
```

Notice the Root port is now shown as **Po1**, which is the logical port created by the EtherChannel bundle.

Step 9: Save your running-config

Lab 3-1: Implementing EIGRP

Visual Topology



Command list.

Command	Description
debug eigrp neighbors	Debugs eigrp events
network <i>network [wildcard mask]</i>	Enables the routing protocol on the interfaces, an optional wildcard mask can be used to narrow down the interface list
no auto-summary	Disable auto-summarization at the classful boundary point.
no router eigrp <i>autonomous-system</i>	Disables the routing process
router eigrp <i>autonomous-system</i>	Enters the router configuring mode
show ip eigrp neighbors	Displays the contents of the neighbourship table
show ip eigrp topology	Displays the contents of the topology table, successors and feasible successors only.
show ip protocols	Displays details of active routing protocols
show ip route	Displays the contents of the IPv4 routing table (best paths)
undebug all	Turns off all debugging events



Task 1: Remote Network Connectivity.

Step 1: Access the CLI on your switch and shutdown all unused ports.

For this exercise, only fa0/1 and fa0/12 are used.

Step 2: Make sure both fa0/1 and fa0/12 are setup as access ports and assigned to VLAN1.

Hint.....Switchport mode access

Switchport access vlan 1

Step 3: Enable portfast of fa0/1 and fa0/12

Hint....spanning-tree portfast

Step 4: Enable fa0/1 and fa0/12

Step 5: Examine the IP address of your PC and if necessary change it to the following values.

PC1 10.1.1.100 / 24 default gateway 10.1.1.1

PC2 10.2.2.100 /24 default gateway 10.2.2.1

If your PC has two networking cards then type in the following commands at the system prompt to redirect traffic out of the correct interface.

PC1 c:\>route -p add 10.2.2.0 mask 255.255.255.0 10.1.1.1

PC2 c:\>route -p add 10.1.1.0 mask 255.255.255.0 10.2.2.1

Step 6: Access the CLI on your router.

Clear down any previous configuration, assign a host name of **R1** or **R2** and configure the following IP addresses.

R1 only....

fa0/0 or gi0/0 10.1.1.1 /24

fa0/1 or gi0/1 172.16.1.17 /28

R2 only....

fa0/0 or gi0/0 10.2.2.1 /24

fa0/1 or gi0/1 172.16.1.18 /28



Step 7: Enable both interfaces and check their status is up/up

Step 8: From your PC ping your default gateway, this should be successful!

Troubleshoot if the ping fails.

Step 9: From your PC ping the IP address of the other PC.

This should fail, why?

Task 2: Configure EIGRP.

Step 1: Access the CLI on the Router

Step 2: Enter the configuration mode for EIGRP using an autonomous system number of 100.

Do the autonomous system numbers need to match for the two routers to become neighbours?

Step 3: While in router configuration mode enter a network command which identifies the specific IP addresses configured on both ethernet interfaces.

Hint....Wildcard mask required

What networks will be advertised from R1 to R2 and R2 to R1?

Use the **show ip route** command to validate your answers and fill in the table below.

Source	Destination	Mask	Type: summary or connected	Exit interface

Step 4: Execute a command which prevents the auto-summarization at a classful boundary point.

Step 5: Use the **Show ip route** command and compare the results against the table in step 3.

Source	Destination	Mask	Type: summary or connected	Exit interface

Which routing protocols auto-summarize by default?

Task 3: Using Show Commands to Verify EIGRP Parameters

Step 1: Run the **sh ip eigrp nei** command and inspect the output.

How many neighbours do you have?

What is the purpose of the hold time value?

How often are hello packets sent?

Step 2: Run the **sh ip eigrp top** command and inspect the output.

How many entries do you have?

Do you have any feasible successors? If not why not?

What does the FD value represent? and how is it calculated?

Step 3: Run the **sh ip protocols** command and inspect the output.

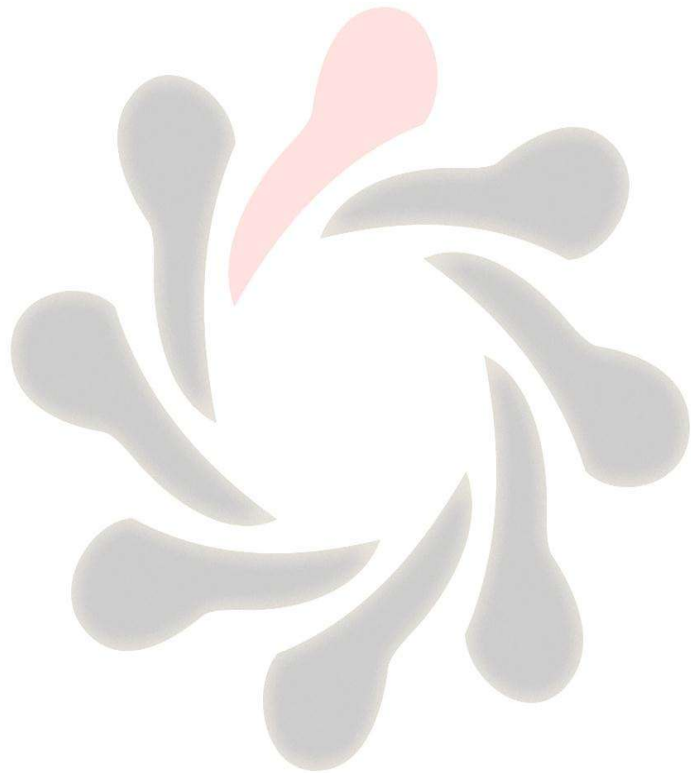
How many routing protocols are running?



What does **Distance: internal 90 external 170** signify?

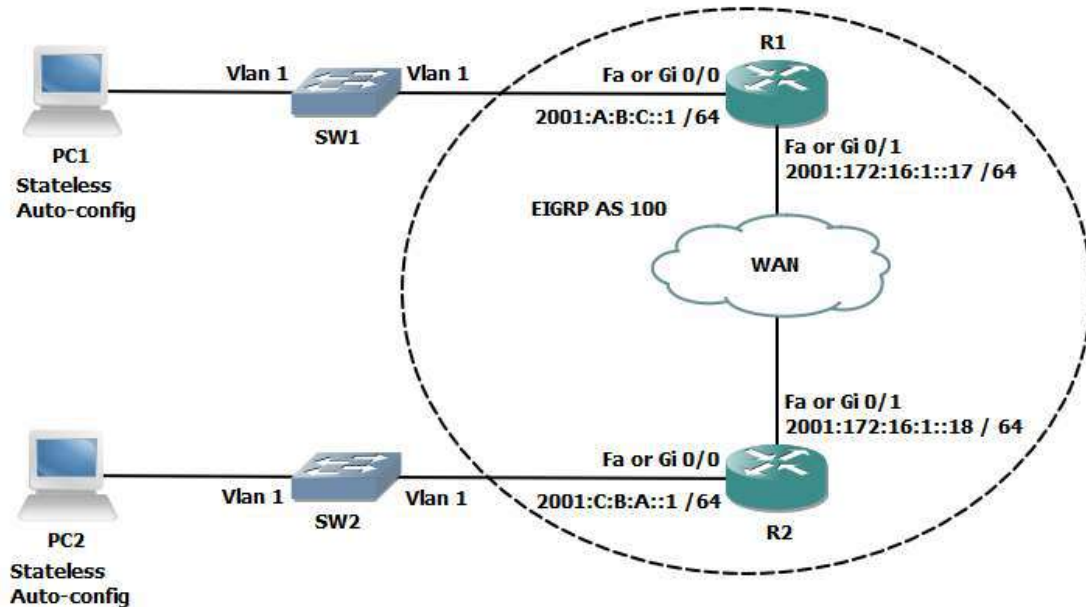
When would you change the **variance** value from its default of **1**?

Step 4: Save your running-config.



Lab 3-2: Implementing EIGRP for IPv6

Visual Topology



Command List

Command	Description
ipv6 address <i>address / mask</i>	Applies an IPv6 address to an interface
ipv6 eigrp <i>AS number</i>	Configures EIGRP for IPv6 on an interface
ipv6 router eigrp <i>AS number</i>	Enters the IPv6 EIGRP configuration mode
ipv6 unicast-routing	Enables IPv6 unicast-routing between interfaces
show ipv6 eigrp interfaces	Displays IPv6 EIGRP interfaces statistics
show ipv6 eigrp neighbors	Displays contents of the IPv6 EIGRP neighbours table
show ipv6 eigrp topology	Displays contents of the IPv6 EIGRP topology table
show ipv6 interface	Displays IPv6 interface setup
show ipv6 route	Displays contents of the IPv6 routing table (best paths)



Task 1: Setting up IPv6 on the Interface.

Step 1: Access the console port of the router.

Step 2: Assign the following IPv6 addresses.

Router	Interface	IPv6 address and mask
R1	fa0/0 or gi0/0	2001:A:B:C::1/64
R1	fa0/1 or gi0/1	2001:172:16:1::17/64
R2	fa0/0 or gi0/0	2001:C:B:A::1/64
R2	fa0/1 or gi0/1	2001:172:16:1::18/64

Step 3: Check the status of the interfaces and make sure they are up/up before continuing.

Step 4: Enter a command which enables routing between the interfaces.

Step 5: Examine the contents of the IPv6 routing table.

```
R1
R1#
R1#
R1#
R1#sh ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2001:A:B:C::/64 [0/0]
   via ::, FastEthernet0/0
L   2001:A:B:C::1/128 [0/0]
   via ::, FastEthernet0/0
C   2001:172:16:1::/64 [0/0]
   via ::, FastEthernet0/1
L   2001:172:16:1::17/128 [0/0]
   via ::, FastEthernet0/1
L   FE80::/10 [0/0]
   via ::, Null0
L   FF00::/8 [0/0]
   via ::, Null0
R1#
```

```
R2
R2#
R2#
R2#
R2#sh ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2001:C:B:A::/64 [0/0]
   via ::, FastEthernet0/0
L   2001:C:B:A::1/128 [0/0]
   via ::, FastEthernet0/0
C   2001:172:16:1::/64 [0/0]
   via ::, FastEthernet0/1
L   2001:172:16:1::18/128 [0/0]
   via ::, FastEthernet0/1
L   FE80::/10 [0/0]
   via ::, Null0
L   FF00::/8 [0/0]
   via ::, Null0
R2#
```

Step 6: Check whether or not your PC has automatically created a global IPv6 address.

```

c:\ Command Prompt
C:\Documents and Settings\Dave>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Autoconfiguration IP Address. . . : 169.254.92.119
    Subnet Mask . . . . . : 255.255.0.0
    IP Address. . . . . : 2001:a:b:c:2181:29a:69be:ca6e
    IP Address. . . . . : 2001:a:b:c:a00:27ff:fe39:c905
    IP Address. . . . . : fe80::a00:27ff:fe39:c905%4
    Default Gateway . . . . . : fe80::c000:23ff:fee0:0%4

Ethernet adapter Local Area Connection 2:

    Media State . . . . . : Media disconnected

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : fe80::5445:5245:444f%6
    Default Gateway . . . . . : 

Tunnel adapter Automatic Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : fe80::5efe:169.254.92.119%2
    Default Gateway . . . . . : 

C:\Documents and Settings\Dave>_
  
```

This is an example output on PC1 and please note the IPv6 addresses, both global and link-local addresses are present in the displayed output.

Based on the above information, can you run IPv4 and IPv6 on the same interface? And if I run IPv4 and IPv6 on the same router do I have separate routing, topology and neighborhood tables?

Task 2: Enabling EIGRP for IPv6.

Step 1: Enable EIGRP for IPv6 and set an autonomous number of 100.

NB: EIGRP can use a shutdown feature when you are in router configuration mode, execute the **no shutdown** just in case EIGRP isn't enabled by default.

Step 2: Use the appropriate commands to associate both the ethernet interfaces with the routing process you have just enabled. Very important you shutdown the interfaces before you apply the command, remember to enable the interface once you have configured them.

Step 3: Navigate through some of the show commands and examine the output details.



You should see similar displays to the following.

```
R1#
R1#sh ipv6 eigrp neighbor
EIGRP-IPv6 Neighbors for AS(100)
H  Address          Interface      Hold Uptime    SRTT  RTO  Q  Seq
                               (sec)          (ms)          Cnt  Num
0  Link-local address: Fa0/1          11 00:09:01    12   200  0   6
   FE80::C806:26FF:FE88:6

R1#
R1#
R1#
R1#
R1#sh ipv6 eigrp topology
EIGRP-IPv6 Topology Table for AS(100)/ID(10.1.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 2001:A:B:C::/64, 1 successors, FD is 28160
   via Connected, FastEthernet0/0
P 2001:172:16:1::/64, 1 successors, FD is 28160
   via Connected, FastEthernet0/1
P 2001:C:B:A::/64, 1 successors, FD is 30720
   via FE80::C806:26FF:FE88:6 (30720/28160), FastEthernet0/1

R1#
```

When using the **sh ipv6 eigrp nei** command please observe that the link-local address is shown instead of the global address.

```
R1#
R1#
R1#
R1#sh ipv6 protocol
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "eigrp 100"
EIGRP-IPv6 Protocol for AS(100)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
NSF-aware route hold timer is 240
Router-ID: 10.1.1.1
Topology : 0 (base)
  Active Timer: 3 min
  Distance: internal 90 external 170
  Maximum path: 16
  Maximum hopcount 100
  Maximum metric variance 1

Interfaces:
  FastEthernet0/0
  FastEthernet0/1
Redistribution:
  None

R1#
```

The output of the **sh ipv6 protocol** command references a number of key values which were also present in EIGRP for IPv4. However there is no mention of auto-summarization!

Do any IPv6 routing protocols support auto-summarization at the classful boundary point and if not, why not?

Step 4: Disable EIGRP for IPv6

```
R(config)#no ipv6 router eigrp 100
```

```
R(config)#int range fa0/0 - 1
```

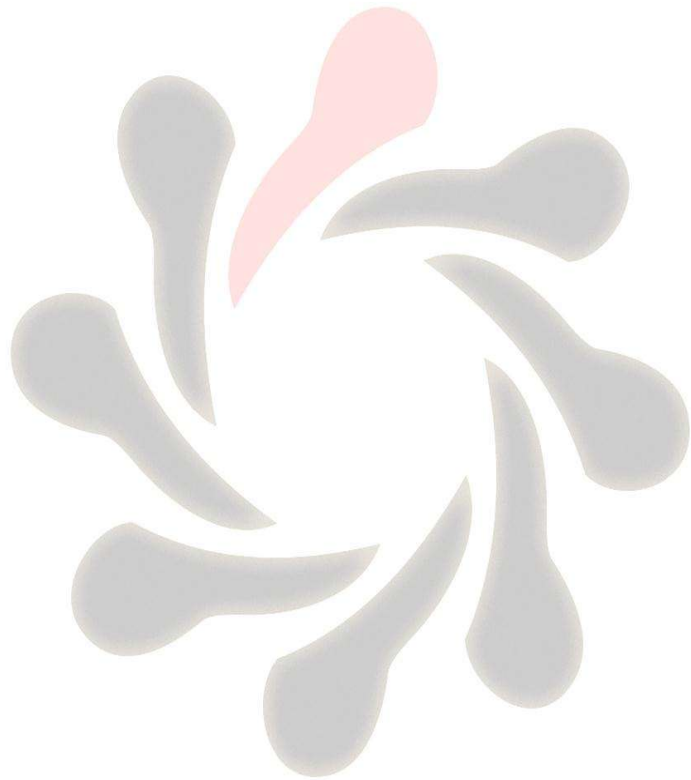
```
R(config-if-range)#shut
```

```
R(config-if-range)#no ipv6 eigrp 100
```



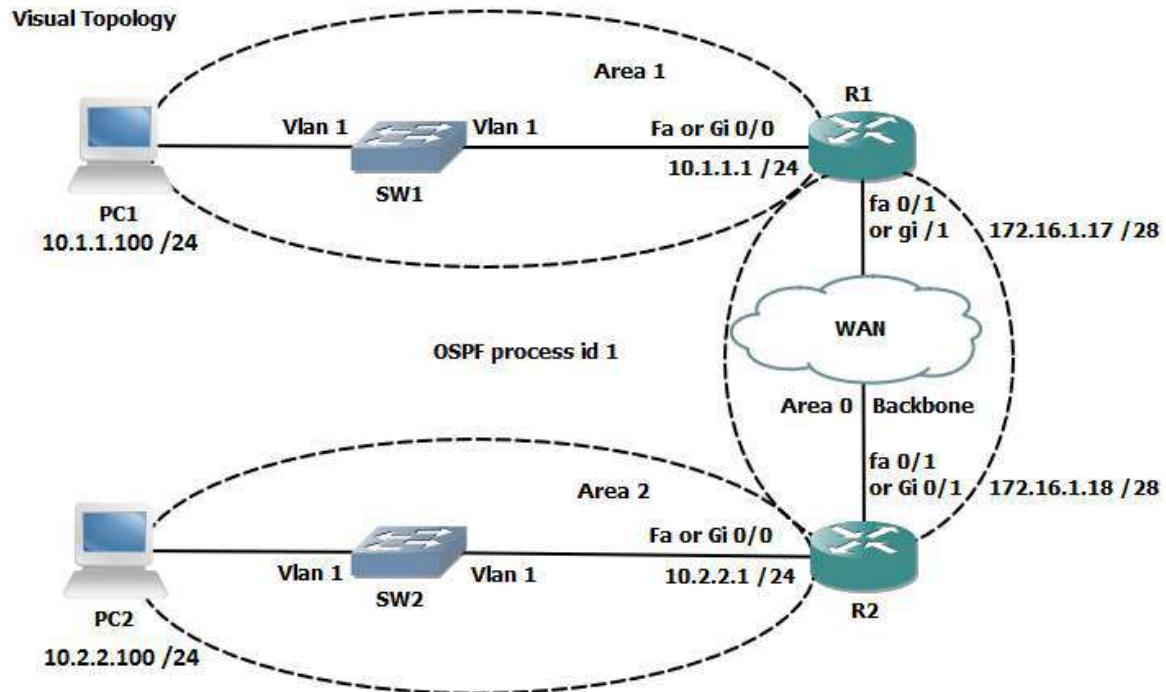
R(config-if-range)#no shut

Step 5: Save your running-config



Lab 4-1: FIREBRAND

Implementing OSPF in a Multi-area Environment.



Command List

Command	Description
network <i>address wildcard mask</i> area <i>id</i>	Specifies which interfaces are OSPF capable and links them to an OSPF area
router ospf <i>process id</i>	Enters the OSPF router configuration mode
show ip ospf interfaces brief	Displays OSPF interface information
show ip ospf neighbor	Displays the contents of the adjacency table
show ip protocols	Display information about active running protocols.
show ip route	Displays the contents of the IPv4 routing table. (best paths)
show ip route ospf	Filters the output display to only show OSPF entries in the routing table.



Task 1: Configuring a Multi-area OSPF Network

Step 1: Access the CLI on your router

Step 2: Check that your IPv4 addresses are still in place and create interface loopback0 and assign the IP address from the table below.

R#sh ip int brief

C:\>ipconfig

Rectify any IPv4 address problems

Router	Interface	IPv4 address	Mask
R1	fa0/0 or gi0/0	10.1.1.1	255.255.255.0
R1	fa0/1 or gi 0/1	172.16.1.17	255.255.255.240
R1	loopback 0	1.1.1.1	255.255.255.255
R2	fa0/0 or gi0/0	10.2.2.1	255.255.255.0
R2	fa0/1 or gi0/1	172.16.1.18	255.255.255.240
R2	loopback 0	2.2.2.2	255.255.255.255

Step 3: Enter the OSPF router configuration mode and assign a process id of **1**

Do process IDs need to match for routers to form an adjacency?

Step 4: Use the **Network** command with an explicit wildcard mask to enable the ethernet and the loopback interfaces. Use the table below for their area assignment.

Router	Interface	Area
R1	fa0/0 or gi0/0	1
R1	fa0/1 or gi0/1	0
R1	loopback 0	0
R2	fa0/0 or gi0/0	2
R2	fa0/1 or gi0/1	0
R2	loopback 0	0

Step 5: Enter the **sh ip protocol** command and write down the router ID

Why did the router select this value.



Is there another way of controlling the router ID and if so, how?

Step 6: Run the `sh ip ospf nei` command (these are example outputs)

```
R1#
R1#
R1#sh ip ospf nei

Neighbor ID      Pri   State           Dead Time   Address      Interface
2.2.2.2          1    FULL/DR         00:00:34   172.16.1.18  FastEthernet0/1
R1#
R1#
R1#
R1#
R1#
R1#
```

```
R2#
R2#
R2#sh ip ospf nei

Neighbor ID      Pri   State           Dead Time   Address      Interface
1.1.1.1          1    FULL/BDR        00:00:33   172.16.1.17  FastEthernet0/1
R2#
R2#
R2#
R2#
R2#
```

Note that both the router ID and the actual IP address of the neighbours interface are displayed using this command. The top picture displays a neighbour with a router ID of 2.2.2.2 and a connecting interface of 172.16.1.18.

Why do we see a DR and BDR in the pictures above but below we see a DR and DRother?

```
R1#
R1#sh ip ospf nei

Neighbor ID      Pri   State           Dead Time   Address      Interface
2.2.2.2          1    FULL/DR         00:00:39   172.16.1.18  FastEthernet0/1
R1#
R1#
```

```
R2#sh ip ospf nei

Neighbor ID      Pri   State           Dead Time   Address      Interface
1.1.1.1          0    FULL/DROTHER    00:00:36   172.16.1.17  FastEthernet0/1
R2#
R2#
R2#
```



Using the **sh ip protocol** command we can find out information about the OSPF configuration.

Run this command on your router and analyze the result.

```
R1#
R1#sh ip protocol
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  It is an area border router
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    1.1.1.1 0.0.0.0 area 0
    10.1.1.1 0.0.0.0 area 1
    172.16.1.17 0.0.0.0 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    2.2.2.2          110           00:06:56
  Distance: (default is 110)
```

This display clearly identifies the Router ID, which networks (interfaces) are allocated to which areas, and a maximum equal cost load balancing of up to 4 paths.

Why is it an Area Border Router (ABR) ?

Step 7: View the contents of the IPv4 routing table and would you expect to see any OSPF entries?

```
R1#
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

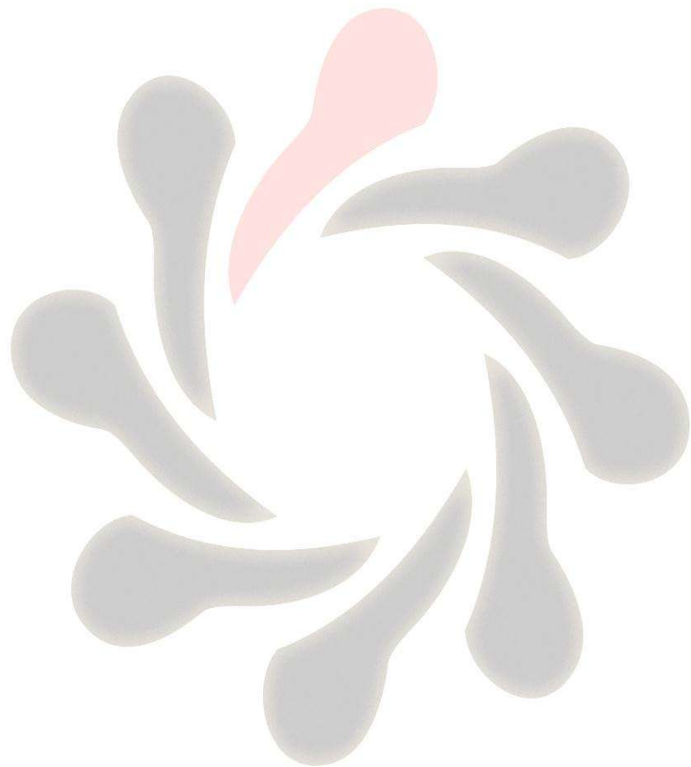
  1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
  2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/2] via 172.16.1.18, 00:17:04, FastEthernet0/1
 10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/24 is directly connected, FastEthernet0/0
C       10.1.1.1/32 is directly connected, FastEthernet0/0
O IA    10.2.2.0/24 [110/2] via 172.16.1.18, 00:17:04, FastEthernet0/1
       172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.16/28 is directly connected, FastEthernet0/1
L       172.16.1.17/32 is directly connected, FastEthernet0/1
R1#
```



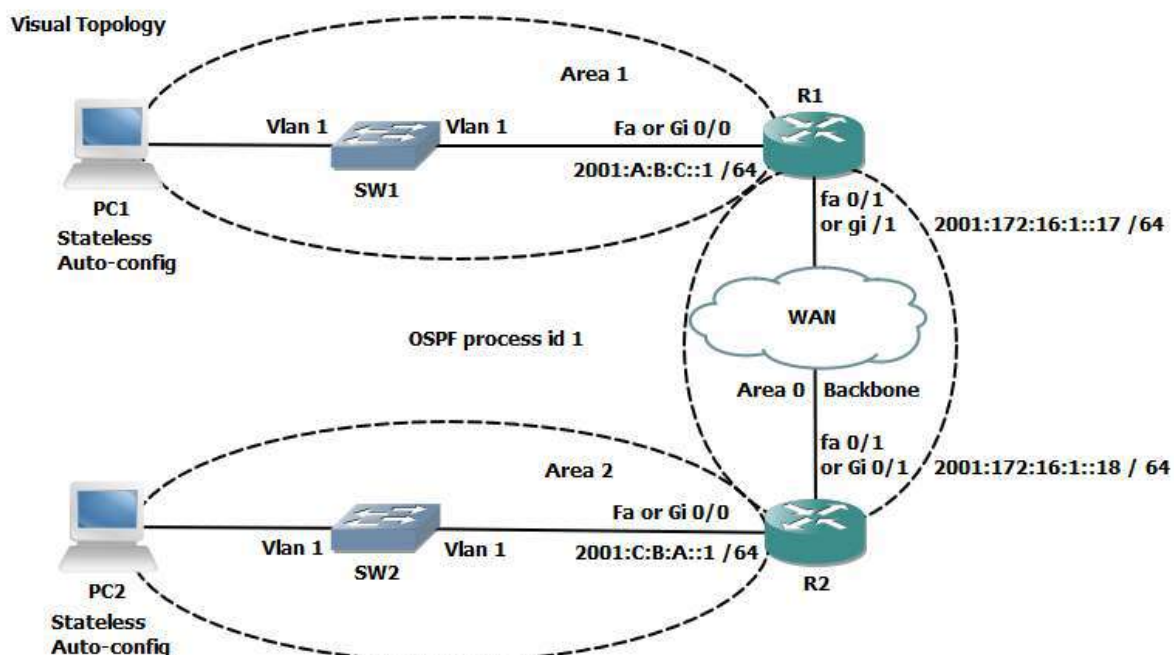
You should observe OSPF generated **O** and **O IA** entries in your routing table.

Explain the difference between the two?

Step 7: Save your running-config.



Lab 4-2: Implementing OSPF for IPv6



Command Line

Command	Description
ipv6 ospf <i>process id</i> area <i>id</i>	Enables OSPFv3 on an interface
ipv6 router ospf <i>process id</i>	Enters the OSPFv3 configuration mode
router-id <i>id</i>	Set a 32 bit router-id (dotted decimal notation)
Show ipv6 ospf interface brief	Displays interfaces that are enabled for OSPFv3
show ipv6 ospf neighbor	Displays the contents of the OSPFv3 neighbours table
show ipv6 route ospf	Displays any OSPFv3 entries contained in the IPv6 routing table (best paths)

Task 1: Enabling OSPFv3 for IPv6.

Step 1: Access the CLI on your router

Step 2: Confirm you still have your IPv6 addresses configured.

R#sh ipv6 int brief



Router	Interface	IPv6 address and mask
R1	fa0/0 or gi0/0	2001:A:B:C::1/64
R1	fa0/1 or gi0/1	2001:172:16:1::17/64
R2	fa0/0 or gi0/0	2001:C:B:A::1/64
R2	fa0/1 or gi0/1	2001:172:16:1::18/64

Step 3: Your router will once again be configure to act as an ABR, use the table below to identify the area ID and also the Router ID to be used.

Router	Router-ID	Interface	Area
R1	1.1.1.1	fa0/0 or gi0/0	1
R1		fa0/1 or gi0/1	0
R2	2.2.2.2	fa0/0 or gi0/0	2
R2		fa0/1 or gi0/1	0

Enter into the OSPFv3 router configuration mode using a process-id of **1**.

Step 4: While in the router configuration mode configure the unique router-ID listed in the table above.

Step 5: Navigate to the interface configuration mode and enable OSPFv3 for process 1.

Step 6: Use the **sh ipv6 ospf int brief** command to verify your configuration.

```

R1#
R1#sh ipv6 ospf interface brief
Interface  PID  Area      Intf ID  Cost  State Nbrs F/C
Fa0/1     1    0         4        1    DR    1/1
Fa0/0     1    1         3        1    DR    0/0
R1#
R1#
R1#
R1#
R1#
R1#

```

```

R2#
R2#
R2#sh ipv6 ospf interface brief
Interface  PID  Area      Intf ID  Cost  State Nbrs F/C
Fa0/1     1    0         4        1    BDR   1/1
Fa0/0     1    2         3        1    DR    0/0
R2#
R2#
R2#
R2#
R2#

```

Step 7: Analyze the contents of the adjacency table using the **sh ipv6 ospf nei** command.

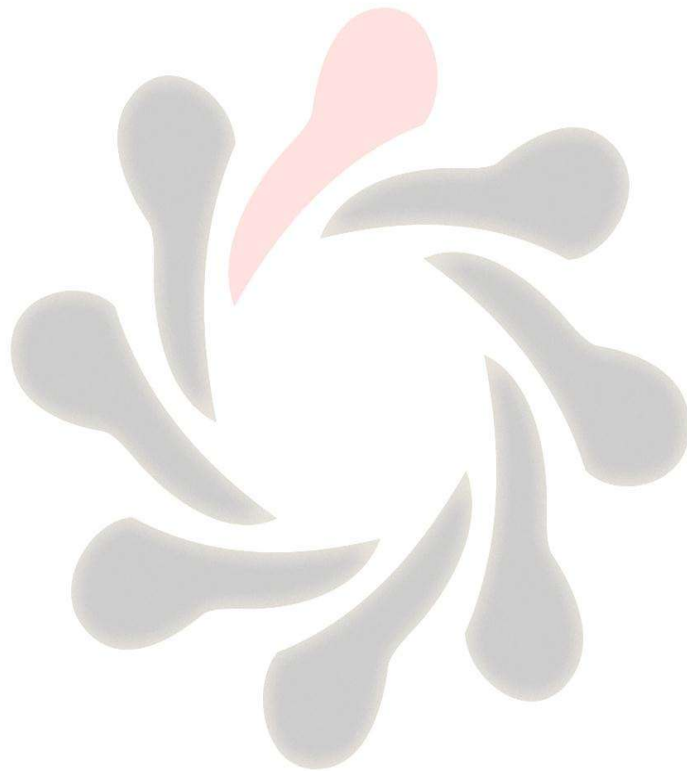
The output looks very similar to OSPFv2 running on IPv4.



Step 8: Use the appropriate command to display all active IPv6 routing protocols.

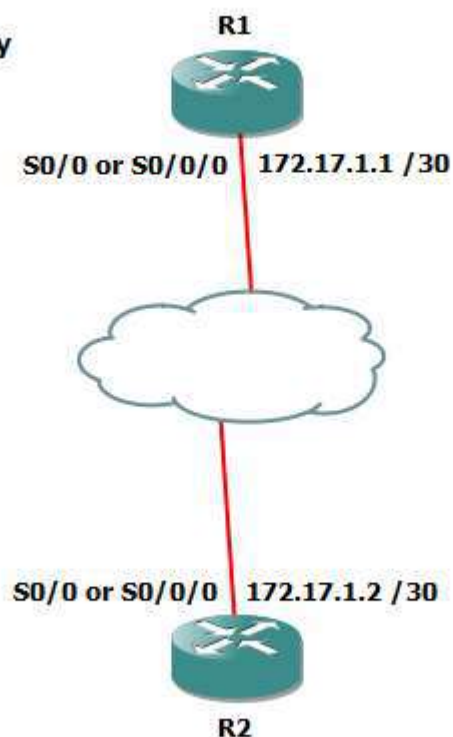
Based on the output displayed, does OSPFv3 have the same administrative distance as OSPFv2?

Step 9: Save your running-config.



Lab 5-1: Setting up a Serial Connection.

Visual Topology



Command Line

Command	Description
debug ppp authentication	Displays the PPP authentication process in real time
debug ppp negotiation	Displays the PPP negotiation packet exchange
encapsulation HDLC	Enables HDLC encapsulation on an interface
encapsulation PPP	Enables PPP encapsulation on an interface
Hostname	Sets a system name and changes the prompt output.
PPP authentication chap	Enable PPP authentication CHAP in an interface
no debug all	Turns off all current debugging screens
username <i>username</i> password <i>password</i>	Sets up a local user account



Task 1: Using HDLC

Step 1: Access the CLI on the router.

Step 2: Shutdown the ethernet interface connecting the two routers together, for this exercise we are going to configure a serial link between the two.

Step 3: Using the information contained in the visual topology diagram configure your serial interface with the appropriate IP address.

Step 4: Run the **sh int s0/0/0 or s0/0** command and study the output to ascertain the layer 2 frame encapsulation, default should be HDLC.

Step 5: In the classroom we are using a back-to-back serial cable and one end will act as the DTE and the other end will be the DCE.

The DCE provides the synchronous clocking signal and requires the clock rate to be set.

R(config-if)**clock rate 256000**

Step 6: Enable the serial interface and PING the IP address of the peer end.

The PING should be successful!

Task 2: Configuring PPP.

Once you are happy with the connection disable the serial interface so we can change the encapsulation to PPP.

PPP provides optional features not available with HDLC such as authentication and will allow communication with a non-Cisco peer device unlike the default Cisco version of HDLC.

Step 1: Disable the serial interface and apply a command which changes the encapsulation to PPP, enable the serial interface and check you once again have connectivity between the two routers.

Task 3: Setting up PPP Authentication.

PPP supports different types of authentication, PAP and CHAP, in this task we are going to configure the more secure option out of the two, CHAP.

Step 1: Create a local user account

R1 only....

R1(config)#**username R2 password cisco**



R2 only....

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

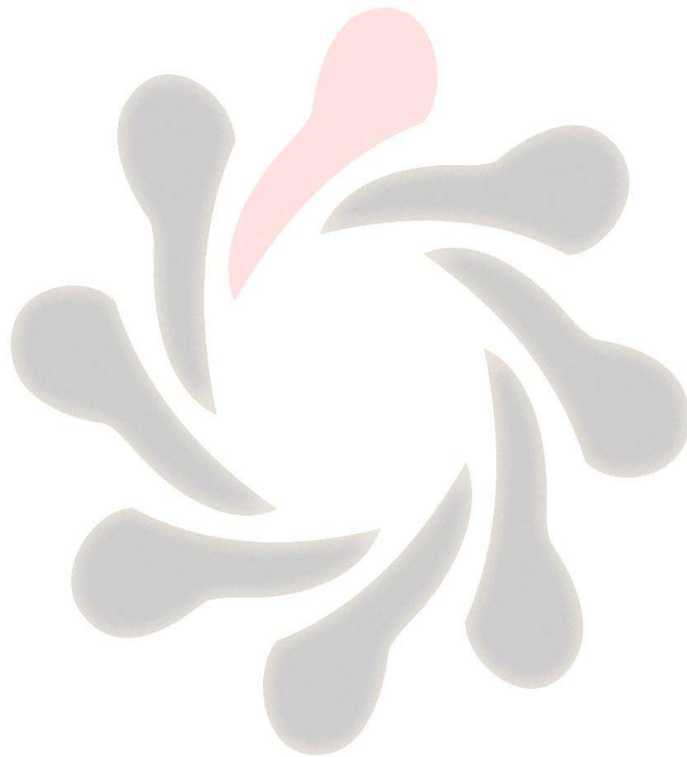
The username will need to match the hostname of the peer end and the password needs to be the same at both ends of the connection.

Step 2: Shutdown the serial interface.

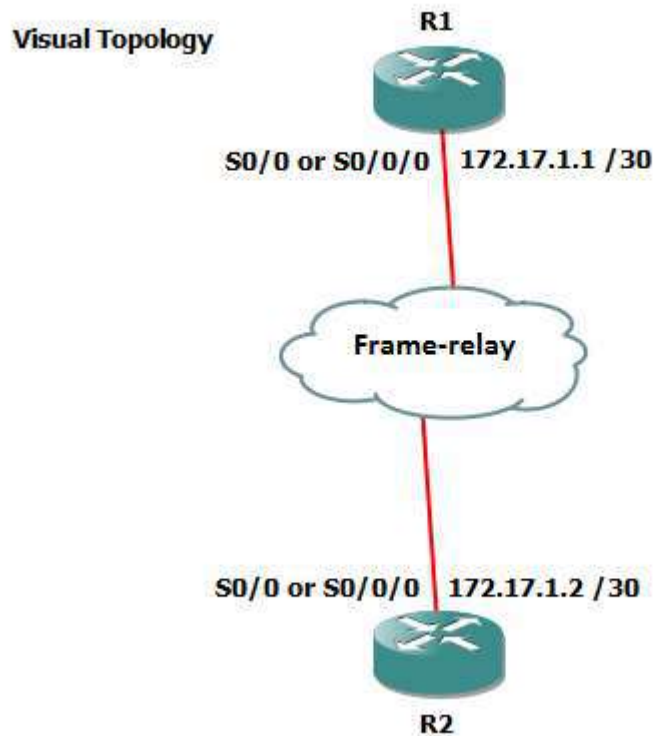
Step 3: Run a debug command to observe the authentication handshaking process

Step 4: Enable the serial interface

Step 5: Save your running-config



Lab 5-2: Establishing a Frame-relay Connection.



Command Line

Command	Description
encapsulation Frame-relay	Enables Frame-relay encapsulation on an interface
Frame-relay interface-dlci <i>dlci</i>	Assigns a DLCI to an interface or subinterface
Interface <i>interface.subinterface</i> point-to-point	Creates a frame-relay point-to-point subinterface
Show frame-relay lmi	Display LMI statistics
Show frame-relay pvc	Displays PVC characteristics
Show frame-relay map	Displays the mapping between the local DLCI and the next hop IP address.

Task 1: Setting up a Basic Frame-relay Link.

Step 1: Access the CLI on the router.

Step 2: Disable the serial interface



Step 3: Remove the current IP address

```
R(config-if)#no IP address
```

Step 4: Change the encapsulation to Frame-relay

Task 2: Supporting Frame-relay using Subinterfaces

In this task the two routers will take on different frame-relay roles, R1 will act as the Frame-relay DCE and R2 will become a Frame-relay DTE

Step 1: R1 only....

The following commands will setup Frame-relay switching, Frame-relay DCE and a frame-relay point-to-point subinterface on router R1.

```
R1(config)#frame-relay switching  
R1(config)#interface s0/0.111 point-to-point  
R1(config-subif)#ip address 172.17.1.1 255.255.255.252  
R1(config-subif)#frame-relay interface-dlci 111  
R1(config-fr-dlci)#end  
R1#conf t  
R1(config)#interface s0/0  
R1(config-if)#frame-relay intf-type dce  
R1(config-if)#no shut
```

Step 1: R2 only.... Acting as a Frame-relay DTE client.

```
R2(config)#interface s0/0.111 point-to-point  
R2(config-subif)#ip address 172.17.1.2 255.255.255.252  
R2(config-subif)#frame-relay interface-dlci 111  
R2(config-fr-dlci)#end  
R2#conf t  
R2(config)#interface s0/0  
R2(config-if)#no shut
```



Step 2: Execute the `sh frame-relay pvc` command.

Below are example snapshots.

```
R1#
R1#
R1#
R1#sh frame-relay pvc

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

      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 = Serial0/0.111

input pkts 16          output pkts 26          in bytes 4205
out bytes 7244        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 20    out bcast bytes 6700
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 00:22:44, last time pvc status changed 00:02:59
R1#
```

```
R2#sh fra
R2#sh 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 = Serial0/0.111

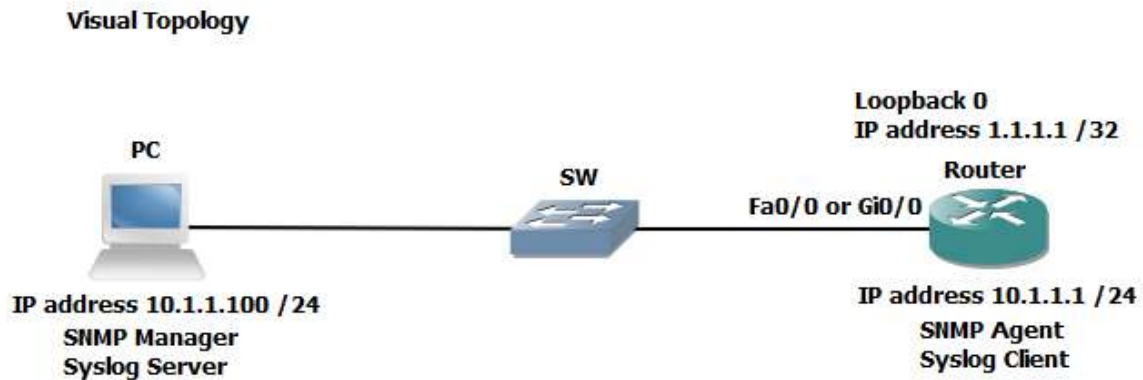
input pkts 17          output pkts 15          in bytes 4540
out bytes 3870        dropped pkts 0          in pkts dropped 0
out pkts dropped 0    out bytes dropped 0
in FECN pkts 0        in BECN pkts 0        out FECN pkts 0
out BECN pkts 0      in DE pkts 0          out DE pkts 0
out bcast pkts 10    out bcast bytes 3350
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 00:08:49, last time pvc status changed 00:08:25
R2#
R2#
R2#
```

What are the 3 possible states of a PVC?

When are frame marked DE?

Step 3: Ping the IP address of the Peer device, this should be successful!

Lab 6-1: SNMP & Syslog Basic Configuration.



Command Line

Command	Description
Interface Loopback0	Creates a Loopback interface
Logging <i>ip address</i>	Sends syslog messages to a host
Logging trap <i>severity</i>	Limits the syslog messages being sent to the syslog server based on severity level
Show logging	Displays the contents of the standard syslog buffer
Snmp-server community <i>string</i> [ro rw]	Defines the community string with either read-only or read-write access
Snmp-server contact <i>name</i>	Defines a system contact value
Snmp-server location <i>location</i>	Defines a system location value

Task 1: Configure a Router for SNMP access.

Step 1: Access the CLI on your router and assign an IP address of 10.1.1.1 /24 on the Fa0/0 or Gi0/0 interface.

Step 2: Create a Loopback interface and assign it an IP address of 1.1.1.1 /32

Step 3: Disable any interfaces connecting the two partnering routers together.



Step 4: Assign an IP address of 10.1.1.100 /24 to the PC and check you have IP connectivity between the PC and your router.

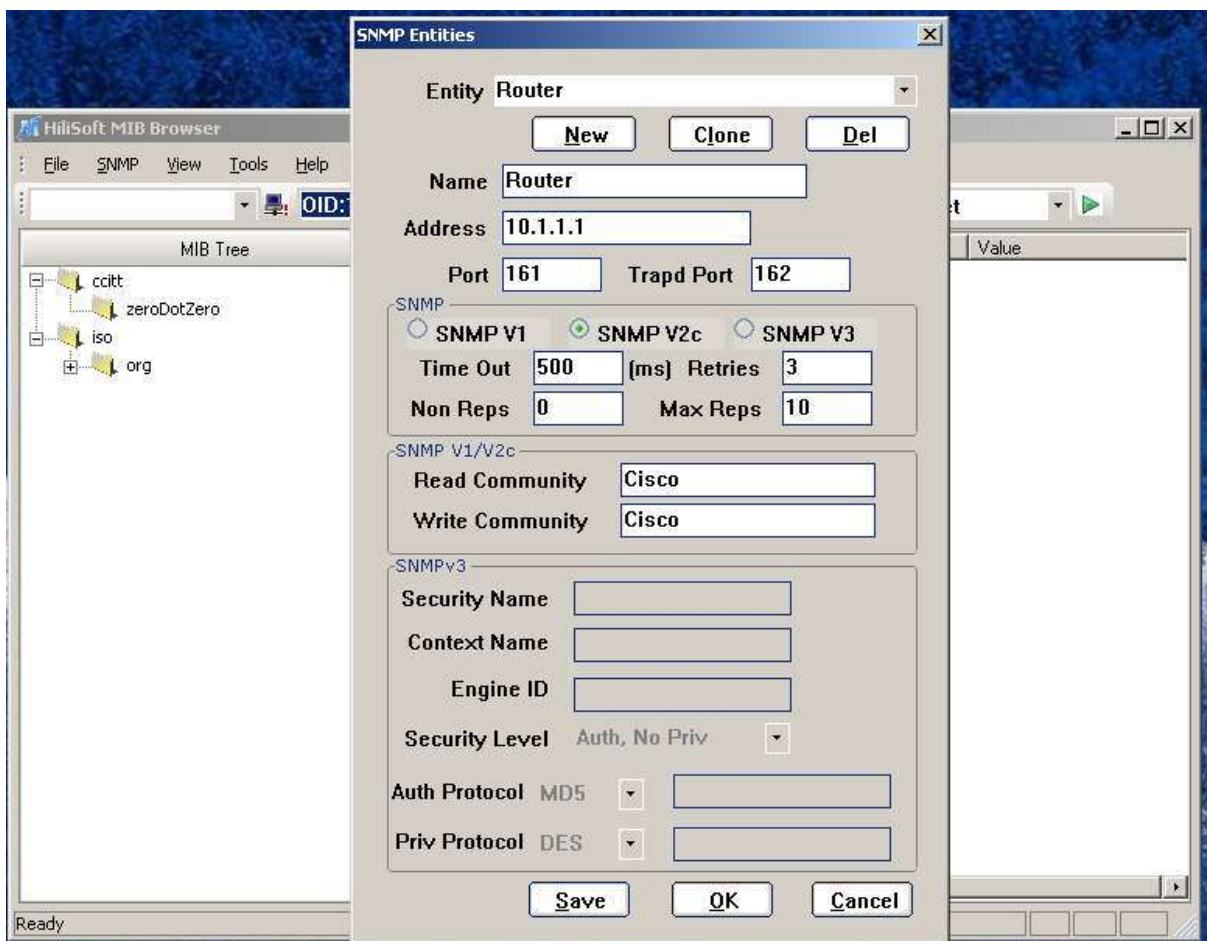
Troubleshoot any issues if found and check you have spanning-tree portfast installed on the switch ports connecting your router and PC to each other.

Step 5: On the router define a community string with of **Cisco** with read-write privileges.

Step 6: On the router define an SNMP contact of John Smith and an SNMP location of Wyboston Lakes.

Step 7: Launch the application **HillSoft MIB Browser** found on your PC.

Click **Tools>SNMP Entities** and fill in the appropriate fields to retrieve data from your router.

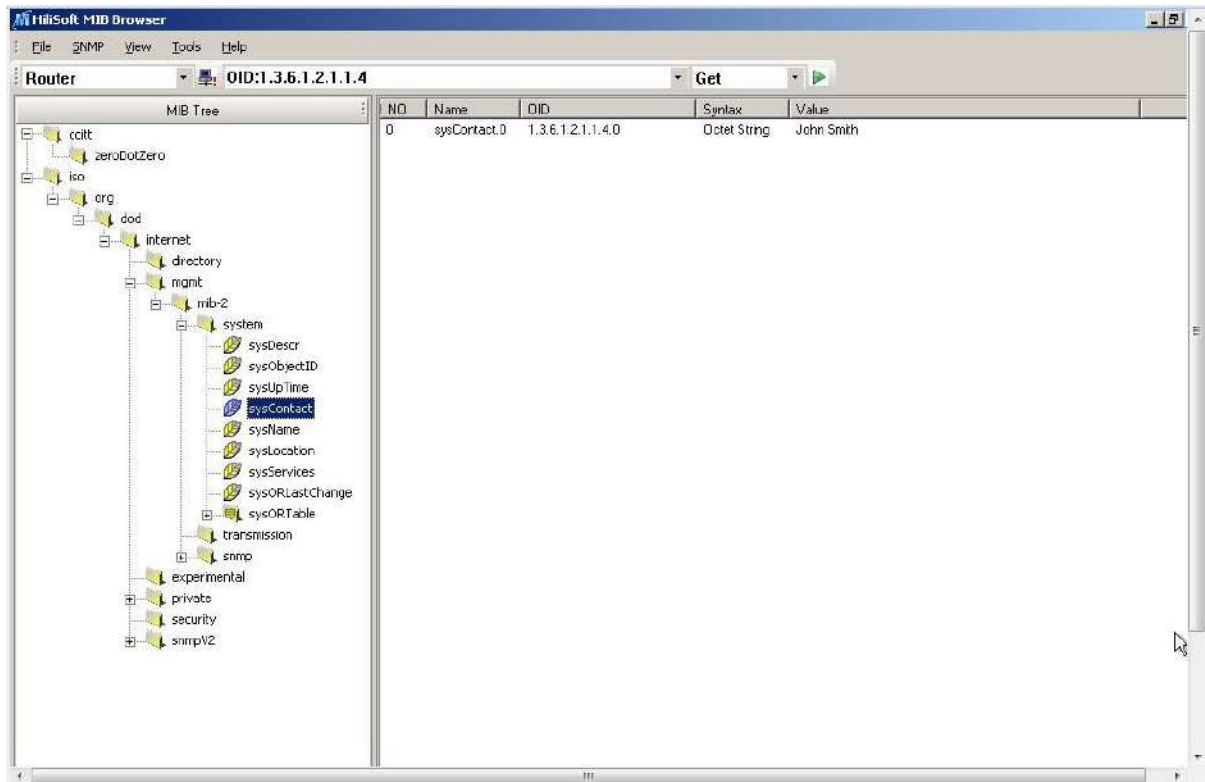


Click **OK**

Are Community Strings case sensitive ?

Step 8: In the MIB view navigate to **iso>org>dod>internet>mgmt>mib-2>system**

Select the **sysContact** and click on the green arrow to **get** the system contact name configured on your router.



Can you see the sysContact string **John Smith** ?

Navigate to the **sysLocation** and check that **Wyboston Lakes** appear.

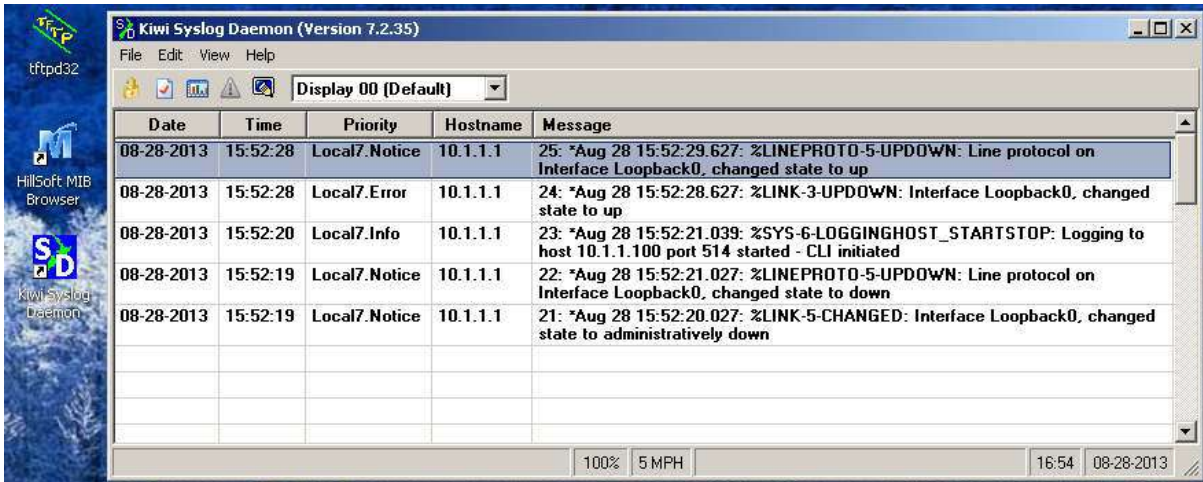
Task 2: Configure a Router for Syslog Services.

Step 1: Access the CLI on your router and configure it to send syslog messages to your PC.

Step 2: At the PC run the Kiwi Syslog server (icon on desktop)

Step 3: Disable and enable the Loopback interface a couple of times to generate syslog messages.

Step 4: Observe the syslog messages captured by the Kiwi syslog server.

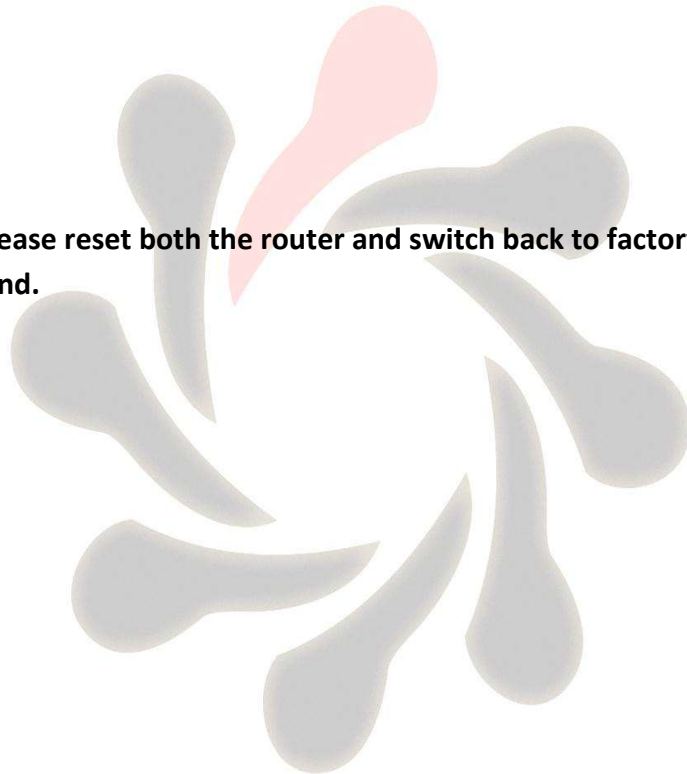


Date	Time	Priority	Hostname	Message
08-28-2013	15:52:28	Local7.Notic	10.1.1.1	25: *Aug 28 15:52:29.627: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
08-28-2013	15:52:28	Local7.Error	10.1.1.1	24: *Aug 28 15:52:28.627: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
08-28-2013	15:52:20	Local7.Info	10.1.1.1	23: *Aug 28 15:52:21.039: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.1.1.100 port 514 started - CLI initiated
08-28-2013	15:52:19	Local7.Notic	10.1.1.1	22: *Aug 28 15:52:21.027: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to down
08-28-2013	15:52:19	Local7.Notic	10.1.1.1	21: *Aug 28 15:52:20.027: %LINK-5-CHANGED: Interface Loopback0, changed state to administratively down

From the output of the syslog server, what severity levels are recorded when the loopback interface changes states.

Once you have complete this lab, Please reset both the router and switch back to factory defaults using the following command.

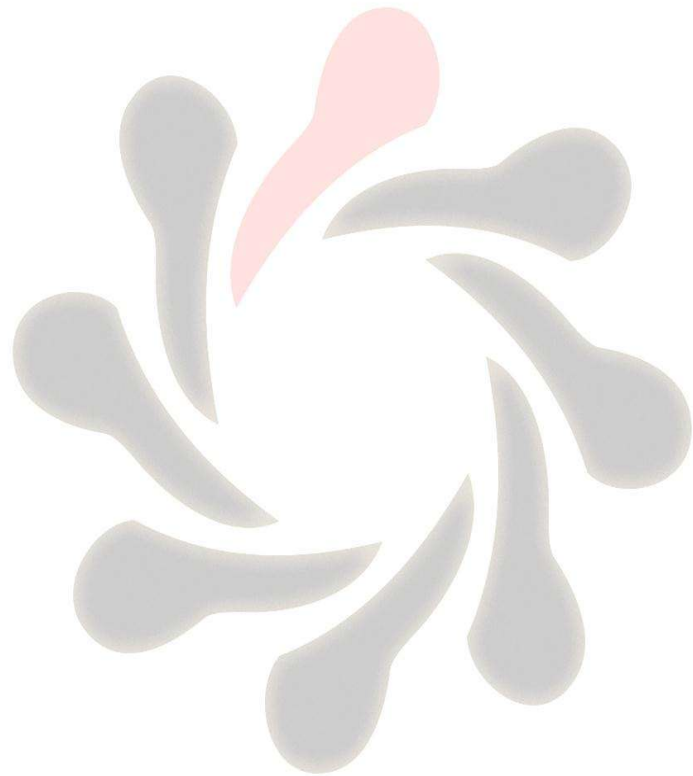
#erase startup-config





Lab Answer Keys:

Please note that not all of the Lab exercise steps are shown in the Lab Answer Keys section and it should be used for reference only.





Lab 1-1: VLANs and Trunk Connections.

Task 1: Reload and check that the Switch is set to factory defaults.

Step 1: Assign an IP address to your PC using the details listed in the visual topology diagram. The PC should be fitted with two network adapters, check with the instructor if you are unsure which network adapter should be configured.

Step 2: Access the Switch Console port using the method and information provided by the instructor.

Enter into privilege mode and use the **erase startup-config** command to remove any previous saved configuration.

Switch>enable

Switch#erase-config

Confirm action and do not save if prompted.

Step 3: Deleting the vlan database

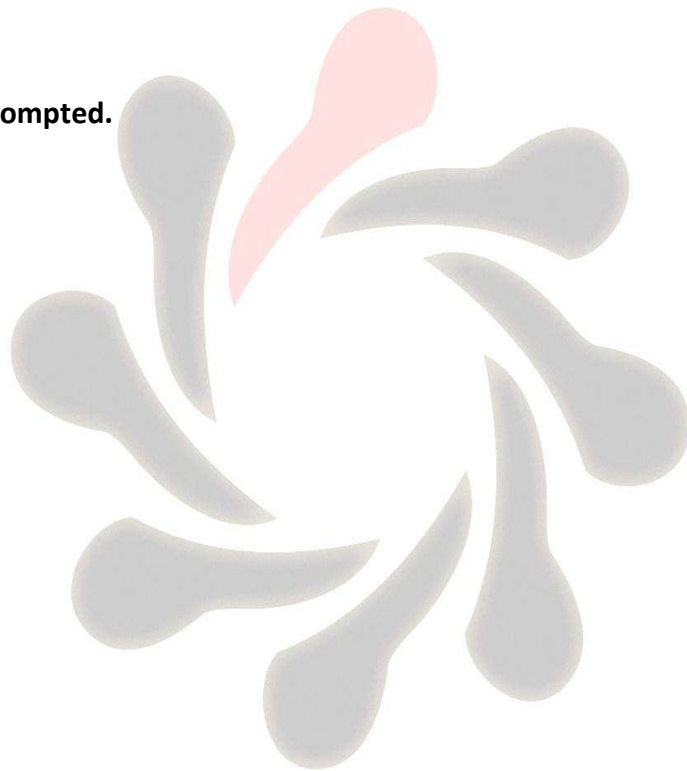
Switch#Delete flash:vlan.dat

confirm the deletion

Step 4: Reload the Switch.

Switch#reload

confirm the reload





Task 2: Basic switch set-up

Step 1: Change the hostname of the Switch to either **SW1** or **SW2**

```
Switch(config)#hostname SW1
```

or

```
Switch(config)#hostname SW2
```

Step 2: Assign your Switch a management IP address using the values identified in the table below.

Device	IP Address	Mask	SVI (logical interface)
SW1	See Student table 1	255.255.255.0	vlan 1
SW2	See Student table 1	255.255.255.0	vlan 1

Remember to enable the SVI so the IP address is active.

```
SW1(config)#interface vlan 1
```

```
SW1(config-if)#ip address 10.1.1.x 255.255.255.0
```

```
SW1(config-if)#no shut
```

or

```
SW2(config)#interface vlan 1
```

```
SW2(config-if)#ip address 10.1.1.x 255.255.255.0
```

```
SW2(config-if)#no shut
```

Task 3: Configure basic VLAN and Trunk connections.

Step 1: Create Vlan 2 and label it with a name of PAIRx

```
SW(config)#vlan 2
```

```
SW(config-vlan)#name PAIRx
```

Step 2: Disable interface fa0/1 and put it into an access state

```
SW(config)#int fa0/1
```

```
SW(config-if)#shut
```

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



Step 3: Re-assign interface fa0/1 and place it into Vlan 2

SW(config-if)#switchport access vlan 2

Step 4: enable interface fa0/1

SW(config-if)#no shut

Step 5: Disable all other interfaces except fa0/1 and Vlan 1

SW(config)#int range fa0/2 - 24

SW(config-if-range)#shut

Step 6: Configure interface fa0/3 and interface fa0/11 to support trunking without using a dynamic protocol trunking protocol.

SW(config)#int fa0/3

SW(config-if)#switchport mode trunk

In the table below indicate which modes generate DTP messages.

Active will send DTP messages, Passive will only receive.

Switchport mode access	Active	operational state access only
Switchport mode trunk	Active	operational state trunk only
Switchport mode dynamic auto	Passive	operational state either trunk or access
Switchport mode dynamic desirable	Active	operational state either trunk or access

What is the command for disabling DTP?

SW(config-if)#switchport nonegotiate

Step 7: Enable interfaces fa0/3 and fa0/11 and disable DTP on all active interfaces.

SW(config)#int range fa0/1, fa0/3, fa0/11

SW(config-if-range)#switchport nonegotiate

SW(config-if-range)#no shut



Task 4: Troubleshooting Trunk failures

Step 2: Ask the instructor to configure all of the ports on the Core switch as **ACCESS** ports.

When a switch has been reset to factory defaults and the ports have been set to access mode, what is the default allocated VLAN for the port?

VLAN 1

Step 3: From privilege mode execute the following commands.

```
show interface fa0/3 switchport
```

```
show interface fa0/11 switchport
```

```
show interface fa0/1 switchport
```

Below are examples of output generated on SW1 but results should be similar on SW2 also.

```
SW1#sh interfaces fa0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
SW1#
```

Observe the Switchport status, Administrative mode, Operational mode.

What do you think the **Negotiation of Trunking: Off** line indicates?

DTP is turned off



Step 4: ASK the Instructor to configure and enable the SVI (VLAN1) interface on the Core switch with an IP address of 10.1.1.100 /24.

Step 5: Ping 10.1.1.100 from you Switch

```
SW1#ping 10.1.1.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

SW1#
```

Explain, why the PING worked? Remembering that you have configured the switchport which connects you to the Core Switch as a Trunk link, however the Core Switch is configured in Static Access mode.

The switches will still communicate with each other if their operational states are different. Our configuration shows the Core Switch set to access mode vlan 1 and your switch set to Trunk with a native vlan of 1, and because the PING originates from vlan 1 your switch will send the PING frame down the trunk link untagged which will then be received at the core switch.

Step 6: From your PC ping 10.1.1.100.

```
PC>ping 10.1.1.100

Pinging 10.1.1.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>|
```

Why does it fail?

The PC is connected to switchport fa0/1 which was reassigned to vlan 2 earlier in the exercise, ports placed in vlan 2 can only communicate to other ports in vlan 2 unless layer 3 routing has been configured.



Step 7: Save your running-config

SW#copy run start





Lab 1-2: Optimizing STP

Task 1: Verify STP Operation.

Confirm with the Instructor that the Core Switch has been configured with all of its ports in trunk mode (see visual diagram) and a SVI (vlan2) has been set-up and enabled with the IP address 10.2.2.1 /24

Step 1: Confirm that you have interfaces fa0/1, fa0/3 and fa0/11 enabled.

SW#sh ip int brief

Step 3:.

Would you expect to see the same Root Bridge for both VLANs?

Yes.

All switches are using defaults bridge priorities for all vlans.

How is the Root Bridge elected?

Lowest BID

The BID is a combination of a 16 bit bridge priority and a 48 bit base mac address. The bridge priority is the primary selection criteria and is set to 32768 by default, the mac address will only be used to determine the Root Bridge if the priorities are equal on all switches involved in the spanning-tree instance.

```

SW2#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
            Address    000D.BD0A.A4C6
            Cost      19
            Port      3(FastEthernet0/3)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
            Address    0060.2FDB.2E65
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 20

Interface          Role Sts Cost      Prio.Nbr Type
-----
Fa0/3              Root FWD 19        128.3   P2p
Fa0/11             Desg FWD 19        128.11  P2p

VLAN0002
  Spanning tree enabled protocol ieee
  Root ID    Priority    32770
            Address    000D.BD0A.A4C6
            Cost      19
            Port      3(FastEthernet0/3)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32770  (priority 32768 sys-id-ext 2)
            Address    0060.2FDB.2E65
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 20

Interface          Role Sts Cost      Prio.Nbr Type
-----
Fa0/3              Root FWD 19        128.3   P2p
Fa0/11             Desg FWD 19        128.11  P2p

```

Using the information obtained from your switch complete the table below.

Table values are based on the output above and should be used for reference only.

Root Bridge ID for VLAN 1	32769.000D.BD0A.A4C6
Root Bridge ID for VLAN 2	32770.000D.BD0A.A4C6
Type of spanning-tree protocol	IEEE (default Cisco PVST+)
Fa0/3 port role	Root
Fa0/3 port state	Forwarding
Fa0/11 port role	Designated
Fa0/11 port state	Forwarding
Cost back to the Root Bridge	19



Based on your results how did the switches decide which one of them should become the Root?

Best (lowest values) BID

Task 2: Manipulating Root Bridge Selection.

In the previous task we used default settings, so the Root Bridge was elected based on the lowest MAC address.

Root bridge elections are pre-emptive and if a new switch is added to the network it can take over the role of the Root Bridge and influence the path decisions made by a switch when forwarding traffic. System administrators have the ability to manipulate the Root Bridge election and therefore create a more predictable switching environment.

Step 1:

SW1 only.....

****IMPORTANT, the following commands illustrate the use of the command structure****

Using the relevant commands, force the switch to become the Root bridge for VLAN 1 and a backup Root Bridge for VLAN 2 if SW2 fails.

SW1(config)#spanning-tree vlan 1 root primary (use the vlan identify in the table)

SW1(config)#spanning-tree vlan 2 root secondary (use the vlan identify in the table)

SW2 only.....

Using the relevant commands, force the switch to become the Root bridge for VLAN 2 and a backup Root Bridge for VLAN 1 if SW1 fails.

SW2(config)#spanning-tree vlan 1 root secondary (use the vlan identify in the table)

SW2(config)#spanning-tree vlan 2 root primary (use the vlan identify in the table)

Task 3: Configuring Rapid Spanning-tree

Step 1: Configure PVRST+

SW(config)#spanning-tree mode rapid-pvst



Step 3: Disable interface fa0/3

```
SW(config)#int fa0/3
```

```
SW(config-if)#shut
```

Step 4: Save your running-config

```
SW#copy run start
```

Task 4: Using STP Portfast

Spanning-tree portfast is used to transition a port straight from the spanning-tree blocking state to the spanning-tree forward state, it usually take less than 1 second for the port to become operational.

Step 1: Disable fa0/1 and configure it to use spanning-tree portfast.

```
SW(config)#int fa0/1
```

```
SW(config-if)#shut
```

```
SW(config-if)spanning-tree portfast
```

Step 3: Enable fa0/1 and monitor the output of the debug command.

```
SW(config-if)#no shut
```

Look for a line similar to this, it should appear very soon after you enable the port.

```
Aug 15 17:10:45.529: STP: VLAN0002 Fa0/1 ->jump to forwarding from blocking
```

Step 4: Save your running-config

```
SW#copy run start
```



Lab 1-3: Configuring EtherChannel

Task 1: EtherChannel Configuration

Step 1: Enable switchports fa0/1, fa0/3 and fa0/4 all other switchports should be shutdown.

```
SW(config)#int range fa0/1, fa0/3 - 4
```

```
SW(config-if-range)#no shut
```

Step 2: Configure fa0/4 as a trunk connection.

```
SW(config)#int fa0/4
```

```
SW(config-if)#shut
```

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

```
SW(config-if)#no shut
```

Step 4: Because of the parallel links (fa0/3 & fa0/4) between the 2 switches spanning-tree will block one of the ports to prevent a loop.

Use an appropriate show command to verify this.

```
SW#sh spanning-tree summary
```

Look for a blocked port on one of the switches.

Step 5: Shutdown fa0/3 and fa0/4

```
SW(config)#int range fa0/3 - 4
```

```
SW(config-if-range)#shut
```

Step 6:

SW1 only....

Configure fa0/3 and fa0/4 interfaces as part of an Etherchannel bundle. Use **1** as the port channel identifier and configure LACP in active mode.

```
SW1(config-if-range)#channel-group 1 mode active
```

```
SW1(config-if-range)#no shut
```




SW2 only....

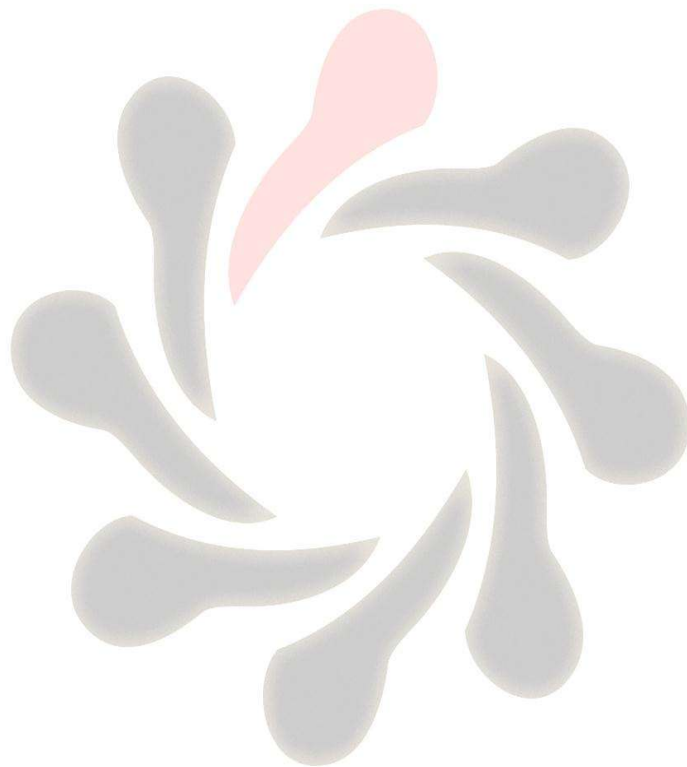
Configure fa0/3 and fa0/4 interfaces as part of an Etherchannel bundle. Use **1** as the port channel identifier and configure LACP in passive mode.

SW2(config-if-range)#channel-group 1 mode passive

SW2(config-if-range)#no shut

Step 9: Save your running-config

SW#copy run start





Lab 3-1: Implementing EIGRP

Task 1: Remote Network Connectivity.

Step 1: Access the CLI on your switch and shutdown all unused ports.

```
SW(config)#int range fa0/1 - 24
```

```
SW(config-if-range)#shut
```

Step 2: Make sure both fa0/1 and fa0/12 are setup as access ports and assigned to VLAN1.

```
SW(config)#int range fa0/1, fa0/12
```

```
SW(config-if-range)#switchport mode access
```

```
SW(config-if-range)#switchport access vlan 1
```

Step 3: Enable portfast of fa0/1 and fa0/12

```
SW(config-if-range)#spanning-tree portfast
```

Step 4: Enable fa0/1 and fa0/12

```
SW(config-if-range)#no shut
```

Step 6: Access the CLI on your router.

Clear down any previous configuration, assign a host name of **R1** or **R2** and configure the following IP addresses.

```
Router#erase startup-config
```

```
Router#reload
```

confirm reload

R1 only....

```
Router>en
```

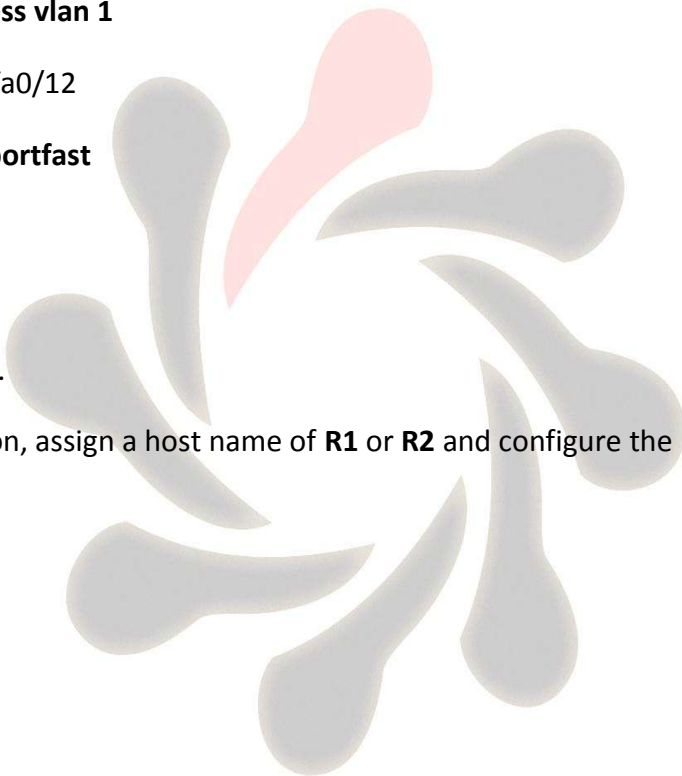
```
Router#conf t
```

```
Router(config)#host R1
```

```
R1(config)#int fa0/0
```

or

```
R1(config)#int gi0/0
```





```
R1(config-if)#ip address 10.1.1.1 255.255.255.0
```

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

```
R1(config-if)#int fa0/1
```

or

```
R1(config-if)#int gi0/1
```

```
R1(config-if)#ip address 172.16.1.17 255.255.255.240
```

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

R2 only....

```
Router>en
```

```
Router#conf t
```

```
Router(config)#host R2
```

```
R2(config)#int fa0/0
```

or

```
R2(config)#int gi0/0
```

```
R2(config-if)#ip address 10.2.2.1 255.255.255.0
```

```
R2(config-if)#no shut
```

```
R2(config-if)#int fa0/1
```

or

```
R2(config-if)#int gi0/1
```

```
R2(config-if)#ip address 172.16.1.18 255.255.255.240
```

```
R2(config-if)#no shut
```

Step 9: From your PC ping the IP address of the other PC.

This should fail, why?

Because you don't have a path to the remote subnet in your routing table.





Task 2: Configure EIGRP.

Step 1: Access the CLI on the Router

Step 2: Enter the configuration mode for EIGRP using an autonomous system number of 100.

```
R(config)#router eigrp 100
```

```
R(config-router)#
```

Do the autonomous system numbers need to match for the two routers to become neighbours?

YES

EIGRP neighbours need to agree on a number of parameters before they exchange routing information.

AS number

K values (metrics being used)

Peer devices on the same logical IP subnet

Authentication policy (not used or MD5)

Step 3: While in router configuration mode enter a network command which identifies the specific IP addresses configured on both ethernet interfaces.

R1 only....

```
R1(config-router)#network 10.1.1.1 0.0.0.0
```

```
R1(config-router)#network 172.16.1.17 0.0.0.0
```

R2 only....

```
R2(config-router)#network 10.2.2.1 0.0.0.0
```

```
R2(config-router)#network 172.16.1.18 0.0.0.0
```

What networks will be advertised from R1 to R2 and R2 to R1?

Summarized 10.0.0.0 /8



Step 4: Execute a command which prevents the auto-summarization at a classful boundary point.

R(config-router)#no auto-summary

Which routing protocols auto-summarize by default?

Distance vector based protocols

RIP v1

RIP v2

IGRP

EIGRP

Task 3: Using Show Commands to Verify EIGRP Parameters

Step 1: Run the **sh ip eigrp nei** command and inspect the output.

How many neighbours do you have?

You should see 1 neighbour

What is the purpose of the hold time value?

15 seconds by default on LAN connections, if I don't receive an hello packet from an established neighbour for 15 seconds, I assume the neighbour has gone off line and I recalculate my topology table.

How often are hello packets sent?

5 seconds by default on LAN connections, used to discovery neighbours and also a keepalive mechanism.

Step 2: Run the **sh ip eigrp top** command and inspect the output.

How many entries do you have?

Should see 3, two local networks and one remote.

Do you have any feasible successors? If not why not?

NO because you only have 1 viable path to your remote network.



What does the FD value represent? and how is it calculated?

Feasible Distance is the metric value to any destination, it is calculated by adding the advertised distance (reported distance) to the calculated link distance between you and your neighbour. The K values control which metric components are used.

Step 3: Run the **sh ip protocols** command and inspect the output.

How many routing protocols are running?

1 (no dynamic routing protocols are enabled by default)

What does **Distance: internal 90 external 170** signify?

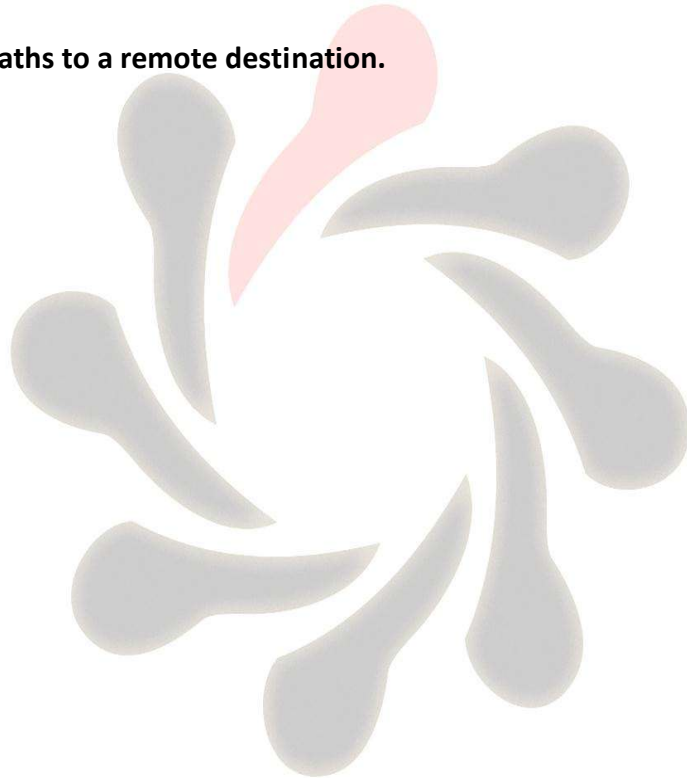
Administrative distances used for internal and external (redistributed) routes.

When would you change the **variance** value from its default of **1**?

You want to support unequal cost paths to a remote destination.

Step 4: Save your running-config.

R#copy run start





Lab 3-2: Implementing EIGRP for IPv6

Task 1: Setting up IPv6 on the Interface.

Step 2: Assign the following IPv6 addresses.

R1 only....

```
R1(config)#int fa0/0
```

or

```
R1(config)#int gi0/0
```

```
R1(config-if)#ipv6 address 2001:a:b:c::1/64
```

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

```
R1(config-if)#int fa0/1
```

or

```
R1(config-if)#int gi0/1
```

```
R1(config-if)#ipv6 address 2001:172:16:1::17/64
```

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

R2 only....

```
R2(config)#int fa0/0
```

or

```
R2(config)#int gi0/0
```

```
R2(config-if)#ipv6 address 2001:c:b:a::1/64
```

```
R2(config-if)#no shut
```

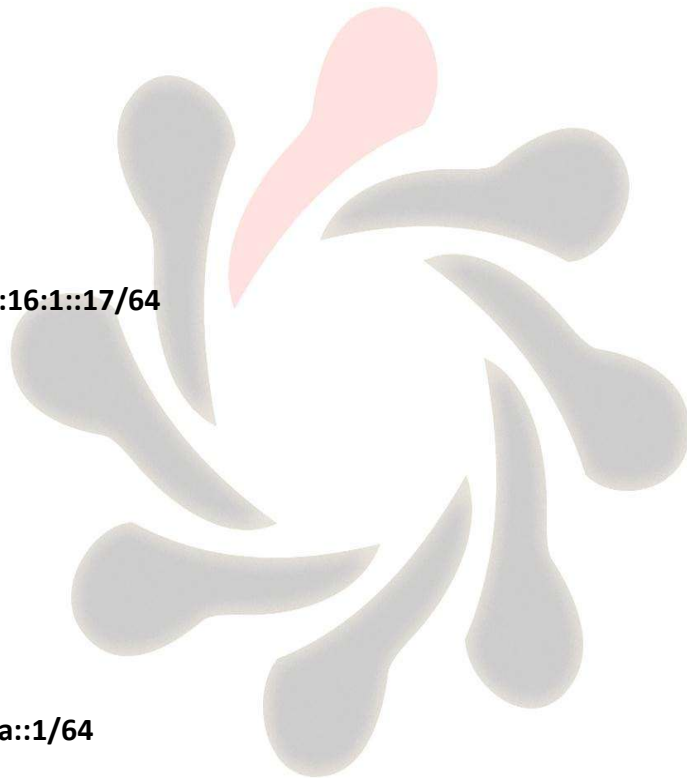
```
R2(config-if)#int fa0/1
```

or

```
R2(config-if)#int gi0/1
```

```
R2(config-if)#ipv6 address 2001:172:16:1::18/64
```

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



Router	Interface	IPv6 address and mask
R1	fa0/0 or gi0/0	2001:A:B:C::1/64
R1	fa0/1 or gi0/1	2001:172:16:1::17/64
R2	fa0/0 or gi0/0	2001:C:B:A::1/64
R2	fa0/1 or gi0/1	2001:172:16:1::18/64

Step 3: Check the status of the interfaces and make sure they are up/up before continuing.

R#sh ipv6 int brief

Step 4: Enter a command which enables routing between the interfaces.

R(config)#ipv6 unicast-routing

Step 5: Examine the contents of the IPv6 routing table.

R#sh ipv6 route

```

R1
R1#
R1#
R1#
R1#
R1#sh ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C 2001:A:B:C::/64 [0/0]
  via ::, FastEthernet0/0
L 2001:A:B:C::1/128 [0/0]
  via ::, FastEthernet0/0
C 2001:172:16:1::/64 [0/0]
  via ::, FastEthernet0/1
L 2001:172:16:1::17/128 [0/0]
  via ::, FastEthernet0/1
L FE80::/10 [0/0]
  via ::, Null0
L FF00::/8 [0/0]
  via ::, Null0
R1#

```

```

R2
R2#
R2#
R2#
R2#sh ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C 2001:C:B:A::/64 [0/0]
  via ::, FastEthernet0/0
L 2001:C:B:A::1/128 [0/0]
  via ::, FastEthernet0/0
C 2001:172:16:1::/64 [0/0]
  via ::, FastEthernet0/1
L 2001:172:16:1::18/128 [0/0]
  via ::, FastEthernet0/1
L FE80::/10 [0/0]
  via ::, Null0
L FF00::/8 [0/0]
  via ::, Null0
R2#

```




Step 6: Check whether or not your PC has automatically created a global IPv6 address.

C:\>ipconfig

```
c:\ Command Prompt
C:\Documents and Settings\Dave>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . : 
    Autoconfiguration IP Address. . . . : 169.254.92.119
    Subnet Mask . . . . . : 255.255.0.0
    IP Address. . . . . : 2001:a:b:c:2181:29a:69be:ca6e
    IP Address. . . . . : 2001:a:b:c:a00:27ff:fe39:c905
    IP Address. . . . . : fe80::a00:27ff:fe39:c905%4
    Default Gateway . . . . . : fe80::c000:23ff:fee0:0%4

Ethernet adapter Local Area Connection 2:

    Media State . . . . . : Media disconnected

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix . . . : 
    IP Address. . . . . : fe80::5445:5245:444f%6
    Default Gateway . . . . . : 

Tunnel adapter Automatic Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix . . . : 
    IP Address. . . . . : fe80::5efe:169.254.92.119%2
    Default Gateway . . . . . : 

C:\Documents and Settings\Dave>
```

This is an example output on PC1 and please note the IPv6 addresses, both global and link-local addresses are present in the displayed output.

Based on the above information, can you run IPv4 and IPv6 on the same interface? And if I run IPv4 and IPv6 on the same router do I have separate routing, topology and neighbourship tables?

Yes, you can run both IPv4 and IPv6 on the same interface (dual stacking).

IPv4 and IPv6 protocols require separate processing tables, you can't place an IPv4 route into an IPv6 table and vice versa.

Task 2: Enabling EIGRP for IPv6.

Step 1: Enable EIGRP for IPv6 and set an autonomous number of 100.

R(config)#ipv6 router eigrp 100

R(config-router)#no shutdown

NB: EIGRP can use a shutdown feature when you are in router configuration mode, execute the **no shutdown** just in case EIGRP isn't enabled by default.



Step 2: Use the appropriate commands to associate both the ethernet interfaces with the routing process you have just enabled. Very important you shutdown the interfaces before you apply the command, remember to enable the interface once you have configured them.

```
R(config)#int range fa0/0 - 1
```

or

```
R(config)#int range gi0/0 - 1
```

```
R(config-if-range)#shut
```

```
R(config-if-range)#ipv6 eigrp 100
```

```
R(config-if-range)#no shut
```

Step 3: Navigate through some of the show commands and examine the output details.

The output of the **sh ipv6 protocol** command references a number of key values which were also present in EIGRP for IPv4. However there is no mention of auto-summarization!

Do any IPv6 routing protocols support auto-summarization at the classful boundary point and if not, why not?

IPv6 is a classless routable protocol, there is no concept of classful boundaries so auto-summarization doesn't exist.

Step 4: Disable EIGRP for IPv6

```
R(config)#no ipv6 router eigrp 100
```

```
R(config)#int range fa0/0 - 1
```

```
R(config-if-range)#shut
```

```
R(config-if-range)#no ipv6 eigrp 100
```

```
R(config-if-range)#no shut
```

Step 5: Save your running-config

```
R#copy run start
```



Lab 4-1:

Implementing OSPF in a Multi-area Environment.

Task 1: Configuring a Multi-area OSPF Network

Step 2: Check that your IPv4 addresses are still in place and create interface loopback0 and assign the IP address from the table below.

R#sh ip int brief

R(config)#int loopback 0

R1 only....

R1(config-if)#ip address 1.1.1.1 255.255.255.255

R2 only....

R2(config-if)#ip address 2.2.2.2 255.255.255.255

C:\>ipconfig

Rectify any IPv4 address problems

Router	Interface	IPv4 address	Mask
R1	fa0/0 or gi0/0	10.1.1.1	255.255.255.0
R1	fa0/1 or gi 0/1	172.16.1.17	255.255.255.240
R1	loopback 0	1.1.1.1	255.255.255.255
R2	fa0/0 or gi0/0	10.2.2.1	255.255.255.0
R2	fa0/1 or gi0/1	172.16.1.18	255.255.255.240
R2	loopback 0	2.2.2.2	255.255.255.255

Step 3: Enter the OSPF router configuration mode and assign a process id of 1

R(config)#router ospf 1

R(config-router)#

Do process IDs need to match for routers to form an adjacency?

NO, the process ID is locally significant.



Step 4: Use the **Network** command with an explicit wildcard mask to enable the ethernet and the loopback interfaces. Use the table below for their area assignment.

Router	Interface	Area
R1	fa0/0 or gi0/0	1
R1	fa0/1 or gi0/1	0
R1	loopback 0	0
R2	fa0/0 or gi0/0	2
R2	fa0/1 or gi0/1	0
R2	loopback 0	0

R1 only....

R1(config-router)#network 10.1.1.1 0.0.0.0 area 1

R1(config-router)#network 172.16.1.17 0.0.0.0 area 0

R2 only....

R2(config-router)#network 10.2.2.1 0.0.0.0 area 2

R2(config-router)#network 172.16.1.18 0.0.0.0 area 0

Step 5: Enter the **sh ip protocol** command and write down the router ID

Why did the router select this value.

Used the ip address of the loopback address.

Is there another way of controlling the router ID and if so, how?

Router-ID command in the router configuration mode

Step 6: Run the **sh ip ospf nei** command (these are example outputs)

```
R1#
R1#
R1#sh ip ospf nei
Neighbor ID      Pri   State           Dead Time   Address        Interface
2.2.2.2          1     FULL/DR         00:00:34   172.16.1.18   FastEthernet0/1
R1#
R1#
R1#
R1#
R1#
```

```

R2#
R2#
R2#sh ip ospf nei
Neighbor ID      Pri   State           Dead Time   Address      Interface
1.1.1.1          1     FULL/BDR        00:00:33   172.16.1.17  FastEthernet0/1
R2#
R2#
R2#
R2#
R2#

```

Note that both the router ID and the actual IP address of the neighbours interface are displayed using this command. The top picture displays a neighbour with a router ID of 2.2.2.2 and a connecting interface of 172.16.1.18.

Why do we see a DR and BDR in the pictures above but below we see a DR and DROther?

The router detects from the interface type that an election for a DR, BDR and DROther needs to take place.

In the first set of output displays both routers are using the default ip ospf priority of 1 and out of the two routers one will demote itself to a BDR.

The second set of output displays one router with an ip ospf priority of 0, which means it will not participate in the election process and take on the role of DROther.

```

R1#
R1#sh ip ospf nei
Neighbor ID      Pri   State           Dead Time   Address      Interface
2.2.2.2          1     FULL/DR         00:00:39   172.16.1.18  FastEthernet0/1
R1#
R1#

```

```

R2#sh ip ospf nei
Neighbor ID      Pri   State           Dead Time   Address      Interface
1.1.1.1          0     FULL/DROTHER    00:00:36   172.16.1.17  FastEthernet0/1
R2#
R2#
R2#

```



Using the **sh ip protocol** command we can find out information about the OSPF configuration.

Run this command on your router and analyze the result.

```
R1#
R1#sh ip protocol
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  It is an area border router
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    1.1.1.1 0.0.0.0 area 0
    10.1.1.1 0.0.0.0 area 1
    172.16.1.17 0.0.0.0 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    2.2.2.2          110          00:06:56
  Distance: (default is 110)
```

This display clearly identifies the Router ID, which networks (interfaces) are allocated to which areas, and a maximum equal cost load balancing of up to 4 paths.

Why is it an Area Border Router (ABR) ?

OSPF interfaces are placed in different area's

Step 7: View the contents of the IPv4 routing table and would you expect to see any OSPF entries?

Yes, advertised from the other router

You should observe OSPF generated **O** and **O IA** entries in your routing table.

Explain the difference between the two?

O entries represent intra-area routes, routes which originate inside your area

O IA entries represent inter-area routes, routes which originate within OSPF but from a different area

Step 7: Save your running-config.

R#copy run start



Lab 4-2: Implementing OSPF for IPv6

Task 1: Enabling OSPFv3 for IPv6.

Step 1: Access the CLI on your router

Step 2: Confirm you still have your IPv6 addresses configured.

R#sh ipv6 int brief

Router	Interface	IPv6 address and mask
R1	fa0/0 or gi0/0	2001:A:B:C::1/64
R1	fa0/1 or gi0/1	2001:172:16:1::17/64
R2	fa0/0 or gi0/0	2001:C:B:A::1/64
R2	fa0/1 or gi0/1	2001:172:16:1::18/64

Step 3: Your router will once again be configure to act as an ABR, use the table below to identify the area ID and also the Router ID to be used.

Router	Router-ID	Interface	Area
R1	1.1.1.1	fa0/0 or gi0/0	1
R1		fa0/1 or gi0/1	0
R2	2.2.2.2	fa0/0 or gi0/0	2
R2		fa0/1 or gi0/1	0

Enter into the OSPFv3 router configuration mode using a process-id of **1**.

R(config)#ipv6 router ospf 1

Step 4: While in the router configuration mode configure the unique router-ID listed in the table above.

R1 only....

R1(config-router)#router-id 1.1.1.1

R2 only.....

R2(config-router)#router-id 2.2.2.2



Step 5: Navigate to the interface configuration mode and enable OSPFv3 for process 1.

R1 only.....

R1(config)#int fa0/0

or

R1(config)#int gi0/0

R1(config-if)#ipv6 ospf 1 area 1

R1(config-if)#int fa0/1

or

R1(config-if)#int gi0/1

R1(config-if)#ipv6 ospf 1 area 0

R2 only.....

R2(config)#int fa0/0

or

R2(config)#int gi0/0

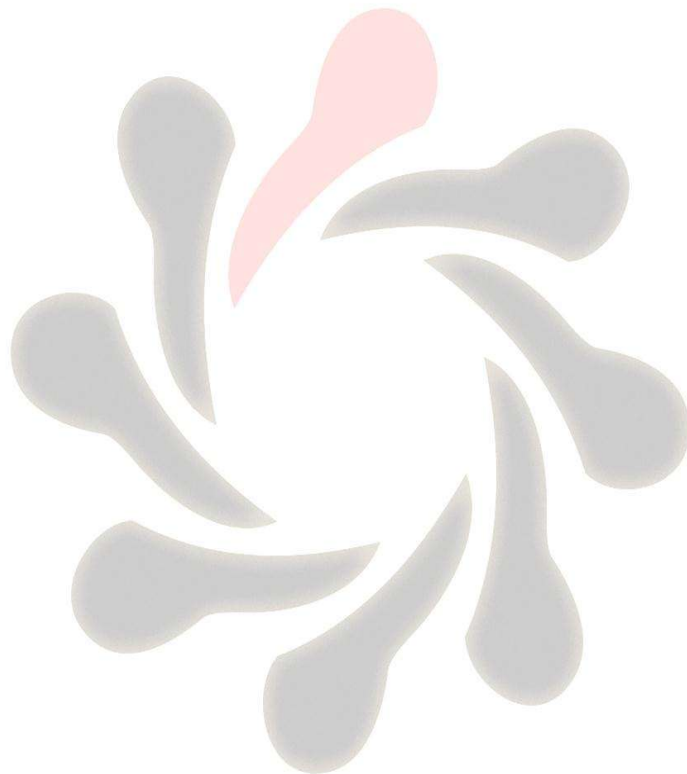
R2(config-if)#ipv6 ospf 1 area 2

R2(config-if)#int fa0/1

or

R2(config-if)#int gi0/1

R2(config-if)#ipv6 ospf 1 area 0



Step 8: Use the appropriate command to display all active IPv6 routing protocols.

R#sh ipv6 protocols

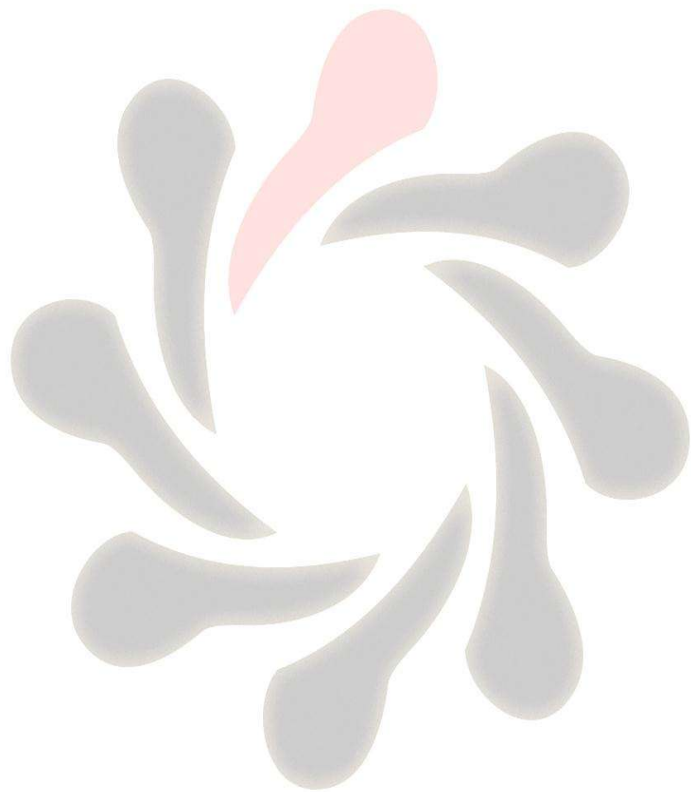
Based on the output displayed, does OSPFv3 have the same administrative distance as OSPFv2?

Yes, both use a default administrative distance of 110



Step 9: Save your running-config.

R#copy run start



Lab 5-1: Setting up a Serial Connection.

Task 1: Using HDLC

Step 2: Shutdown the ethernet interface connecting the two routers together, for this exercise we are going to configure a serial link between the two.

```
R(config)#int fa0/1
```

or

```
R(config)#int gi0/1
```

```
R(config-if)#shut
```

Step 3: Using the information contained in the visual topology diagram configure your serial interface with the appropriate IP address.

R1 only....

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

or

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

```
R1(config-if)#ip address 172.17.1.1 255.255.255.252
```

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

R2 only....

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

or

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

```
R2(config-if)#ip address 172.17.1.2 255.255.255.252
```

```
R2(config-if)#no shut
```





Step 4: Run the **sh int s0/0/0** or **s0/0** command and study the output to ascertain the layer 2 frame encapsulation, default should be HDLC.

R#sh int s0/0/0

or

R#sh int s0/0

Step 5: In the classroom we are using a back-to-back serial cable and one end will act as the DTE and the other end will be the DCE.

The DCE provides the synchronous clocking signal and requires the clock rate to be set.

R(config-if)clock rate 256000

Step 6: Enable the serial interface and PING the IP address of the peer end.

The PING should be successful!

YES

Task 2: Configuring PPP.

Once you are happy with the connection disable the serial interface so we can change the encapsulation to PPP.

PPP provides optional features not available with HDLC such as authentication and will allow communication with a non-Cisco peer device unlike the default Cisco version of HDLC.

Step 1: Disable the serial interface and apply a command which changes the encapsulation to PPP, enable the serial interface and check you once again have connectivity between the two routers.

R(config)#int s0/0/0

or

R(config)#int s0/0

R(config-if)#shut

R(config-if)#encap ppp

R(config-if)#no shut



Task 3: Setting up PPP Authentication.

PPP supports different types of authentication, PAP and CHAP, in this task we are going to configure the more secure option out of the two, CHAP.

Step 1: Create a local user account

R1 only....

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

R2 only....

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

The username will need to match the hostname of the peer end and the password needs to be the same at both ends of the connection.

Step 2: Shutdown the serial interface.

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

or

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

```
R(config-if)#shut
```

```
R(config-if)#end
```

Step 3: Run a debug command to observe the authentication handshaking process

```
R#debug ppp auth
```

Step 4: Enable the serial interface

```
R#conf t
```

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

or

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

```
R(config-if)#no shut
```

Step 5: Save your running-config

```
R#copy run start
```

Lab 5-2: Establishing a Frame-relay Connection

Task 1: Setting up a Basic Frame-relay Link.

Step 2: Disable the serial interface

```
R(config-if)#shut
```

Step 3: Remove the current IP address

```
R(config-if)#no IP address
```

Step 4: Change the encapsulation to Frame-relay

```
R(config-if)#encap frame-relay
```

Task 2: Supporting Frame-relay using Subinterfaces

In this task the two routers will take on different frame-relay roles, R1 will act as the Frame-relay DCE and R2 will become a Frame-relay DTE

Step 1: R1 only....

The following commands will setup Frame-relay switching, Frame-relay DCE and a frame-relay point-to-point subinterface on router R1.

```
R1(config)#frame-relay switching
```

```
R1(config)#interface s0/0.111 point-to-point
```

```
R1(config-subif)#ip address 172.17.1.1 255.255.255.252
```

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

```
R1(config-fr-dlci)#end
```

```
R1#conf t
```

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

```
R1(config-if)#frame-relay intf-type dce
```

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

Step 1: R2 only.... Acting as a Frame-relay DTE client.

```
R2(config)#interface s0/0.111 point-to-point
```

```
R2(config-subif)#ip address 172.17.1.1 255.255.255.252
```

```
R2(config-subif)#frame-relay interface-dlci 111
```

```
R2(config-fr-dlci)#end
```

```
R2#conf t
```

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

```
R2(config-if)#no shut
```

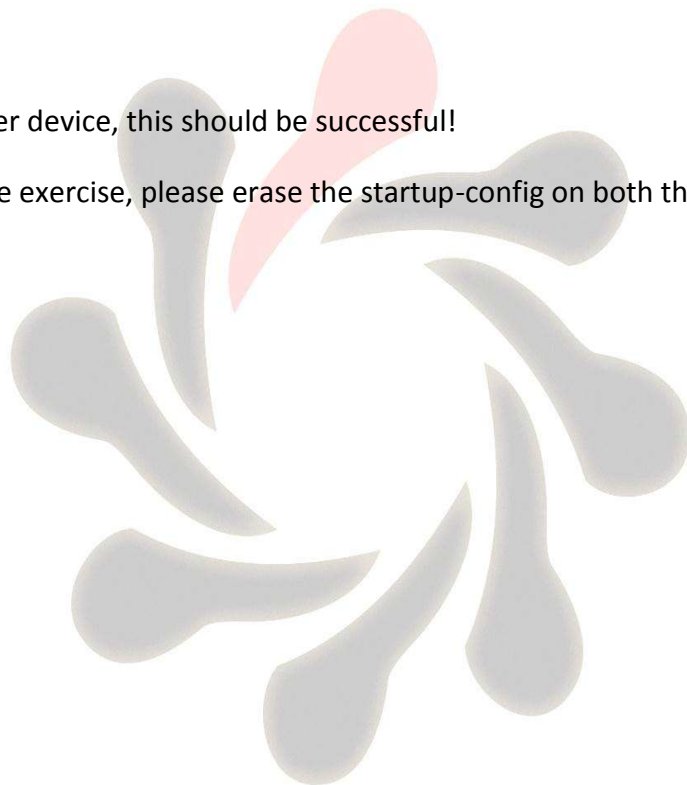
Step 2: Execute the **sh frame-relay pvc** command.

```
R#sh frame-relay pvc
```

Step 3: Ping the IP address of the Peer device, this should be successful!

Step 4: Once you have completed the exercise, please erase the startup-config on both the router and the switch.

```
R#erase startup-config
```





Lab 6-1: SNMP & Syslog Basic Configuration.

Task 1: Configure a Router for SNMP access.

Step 1: Access the CLI on your router and assign an IP address of 10.1.1.1 /24 on the Fa0/0 or Gi0/0 interface.

```
R>enable
```

```
R#conf t
```

```
R(config)#interface fa0/0 or Gi0/0
```

```
R(config-if)#ip address 10.1.1.1 255.255.255.0
```

```
R(config-if)#no shut
```

Step 2: Create a Loopback interface and assign it an IP address of 1.1.1.1 /32

```
R(config-if)#Interface Loopback 0
```

```
R(config-if)#ip address 1.1.1.1 255.255.255.255
```

Step 3: Disable any interfaces connecting the two partnering routers together.

```
R(config-if)#interface fa0/1 or Gi0/1
```

```
R(config-if)#shut
```

```
R(config-if)#interface s0/0/0 or s0/0
```

```
R(config-if)#shut
```

Step 5: On the router define a community string with of **Cisco** with read-write privileges.

```
R(config)#snmp-server community Cisco rw
```

```
R(config)#snmp-server community Cisco ro
```

Step 6: On the router define an SNMP contact of John Smith and an SNMP location of Wyboston Lakes.

```
R(config)#snmp-server contact John Smith
```

```
R(config)#snmp-server location Wyboston Lakes
```

Step 7:

Are Community Strings case sensitive ?

Yes they are

Task 2: Configure a Router for Syslog Services.

Step 1: Access the CLI on your router and configure it to send syslog messages to your PC.

```
R(config)#logging 10.1.1.100
```

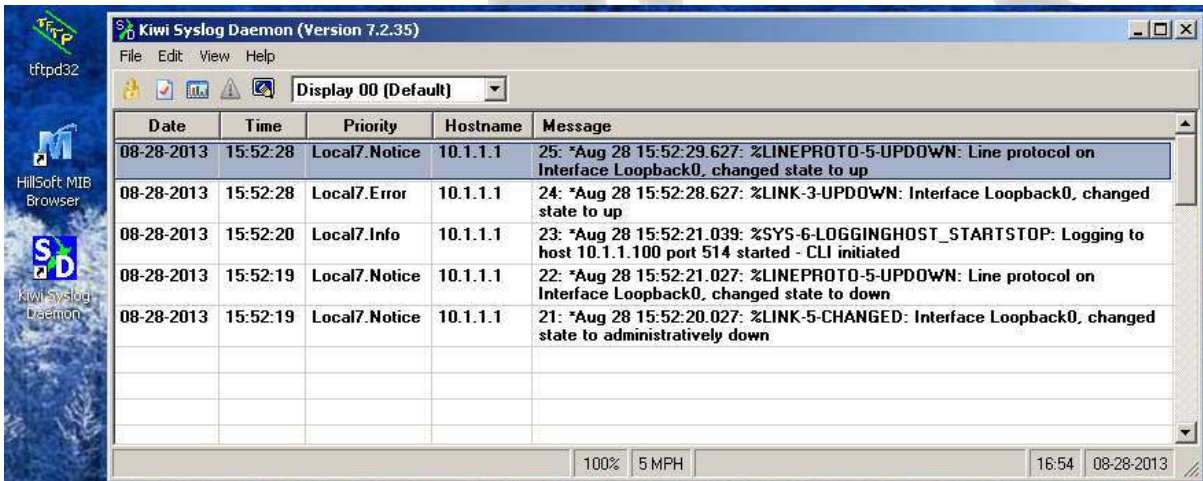
Step 3: Disable and enable the Loopback interface a couple of times to generate syslog messages.

```
R(config)#int loopback 0
```

```
R(config-if)#shut
```

```
R(config-if)#no shut
```

Step 4: Observe the syslog messages captured by the Kiwi syslog server.



Date	Time	Priority	Hostname	Message
08-28-2013	15:52:28	Local7.Notic	10.1.1.1	25: *Aug 28 15:52:29.627: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
08-28-2013	15:52:28	Local7.Error	10.1.1.1	24: *Aug 28 15:52:28.627: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
08-28-2013	15:52:20	Local7.Info	10.1.1.1	23: *Aug 28 15:52:21.039: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.1.1.100 port 514 started - CLI initiated
08-28-2013	15:52:19	Local7.Notic	10.1.1.1	22: *Aug 28 15:52:21.027: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to down
08-28-2013	15:52:19	Local7.Notic	10.1.1.1	21: *Aug 28 15:52:20.027: %LINK-5-CHANGED: Interface Loopback0, changed state to administratively down

From the output of the syslog server, what severity levels are recorded when the loopback interface changes states.

%LINK-3-UPDOWN (severity level 3 ERROR)

%LINK-5-CHANGED (severity level 5 NOTIFICATION)

%SYS-6-LOGGINGHOST_STARTSTOP (severity level 6 INFORMATIONAL)



Once you have complete this lab, Please reset both the router and switch back to factory defaults using the following command.

```
#erase startup-config
```

