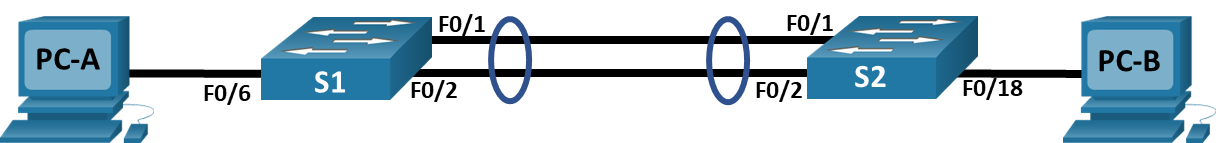
Lab - Implement EtherChannel **(Instructor Version)**

**Instructor Note**: Red font color or gray highlights indicate text that appears in the instructor copy only.

# Topology



# Addressing Table

| **Device** | **Interface** | **IP Address** | **Subnet Mask** |
| --- | --- | --- | --- |
| S1 | VLAN 10 | 192.168.10.11 | 255.255.255.0 |
| S2 | VLAN 10 | 192.168.10.12 | 255.255.255.0 |
| PC-A | NIC | 192.168.20.3 | 255.255.255.0 |
| PC-B | NIC | 192.168.20.4 | 255.255.255.0 |

# VLAN Table

| **VLAN** | **Name** | **Interface Assigned** |
| --- | --- | --- |
| 10 | Management | VLAN 10 |
| 20 | Clients | S1: F0/6  S2: F0/18 |
| 999 | Parking\_Lot | S1: F0/3-5, F0/7-24, G0/1-2  S2: F0/3-17, F0/19-24, G0/1-2 |
| 1000 | Native | N/A |

# Objectives

**Part 1: Build the Network and Configure Basic Device Settings**

**Part 2: Create VLANs and Assign Switch Ports**

**Part 3: Configure 802.1Q Trunks between the Switches**

**Part 4: Implement and Verify an EtherChannel between the switches**

# Background / Scenario

Link aggregation allows the creation of logical links that are comprised of two or more physical links. This provides increased throughput beyond using only one physical link. Link aggregation also provides redundancy if one of the links fails.

In this lab, you will configure EtherChannel, a form of link aggregation used in switched networks. You will configure EtherChannel using Link Aggregation Control Protocol (LACP).

**Note**: LACP is a link aggregation protocol that is defined by IEEE 802.3ad, and it is not associated with any specific vendor.

LACP allows Cisco switches to manage Ethernet channels between switches that conform to the 802.3ad protocol. You can configure up to 16 ports to form a channel. Eight of the ports are in active mode and the other eight are in standby mode. When any of the active ports fail, a standby port becomes active. Standby mode works only for LACP, not for PAgP.

**Note**: The switches used with CCNA hands-on labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

**Note**: Make sure that the switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

**Instructor Note**: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

# Required Resources

* 2 Switches (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
* 2 PCs (Windows with a terminal emulation program, such as Tera Term)
* Console cables to configure the Cisco IOS devices via the console ports
* Ethernet cables as shown in the topology

# Instructions

## Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the PC hosts and switches.

### Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

### Configure basic settings for each switch.

* + - 1. Assign a device name to the switch.

*Open configuration window*

switch(config)# **hostname S1**

* + - 1. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

S1(config)# **no ip domain-lookup**

* + - 1. Assign **class** as the privileged EXEC encrypted password.

S1(config)# **enable secret class**

* + - 1. Assign **cisco** as the console password and enable login.

S1(config)# **line console 0**

S1(config-line)# **password cisco**

S1(config-line)# **login**

* + - 1. Assign **cisco** as the VTY password and enable login.

S1(config)# **line vty 0 15**

S1(config-line)# **password cisco**

S1(config-line)# login

* + - 1. Encrypt the plaintext passwords.

S1(config)# service password-encryption

* + - 1. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

S1(config)# **banner motd $ Authorized Users Only! $**

* + - 1. Save the running configuration to the startup configuration file.

S1# **copy running-config startup-config**

* + - 1. Set the clock on the switch to today’s time and date.

S1# **clock set 15:30:00 27 Aug 2019**

**Note**: Use the question mark (**?**) to help with the correct sequence of parameters needed to execute this command.

* + - 1. Copy the running configuration to the startup configuration.

*Close configuration window*

### Configure PC hosts.

Refer to the Addressing Table for PC host address information.

## Create VLANs and Assign Switch Ports

In Part 2, you will create VLANs as specified in the table above on both switches. You will then assign the VLANs to the appropriate interface and verify your configuration settings. Complete the following tasks on each switch.

### Create VLANs on the switches.

* + - 1. On both switches create and name the required VLANs from the VLAN Table above.

*Open configuration window*

S1(config)# **vlan 10**

S1(config-vlan)# **name Management**

S1(config-vlan)# **vlan 20**

S1(config-vlan)# **name Clients**

S1(config-vlan)# **vlan 999**

S1(config-vlan)# **name Parking\_Lot**

S1(config-vlan)# **vlan 1000**

S1(config-vlan)# **name Native**

S1(config-vlan)# **exit**

S2(config)# **vlan 10**

S2(config-vlan)# **name Management**

S2(config-vlan)# **vlan 20**

S2(config-vlan)# **name Clients**

S2(config-vlan)# **vlan 999**

S2(config-vlan)# **name Parking\_Lot**

S2(config-vlan)# **vlan 1000**

S2(config-vlan)# **name Native**

S2(config-vlan)# **exit**

* + - 1. Configure and activate the management interface on each switch using the IP address information in the Addressing Table.

S1(config)# **interface vlan 10**

S1(config-if)# **ip address 192.168.10.11 255.255.255.0**

S1(config-if)# **no shutdown**

S1(config-if)# **exit**

S2(config)# **interface vlan 10**

S2(config-if)# **ip address 192.168.10.12 255.255.255.0**

S2(config-if)# **no shutdown**

S2(config-if)# **exit**

* + - 1. Assign all unused ports on the switch to the Parking\_Lot VLAN, configure them for static access mode, and administratively deactivate them.

S1(config)# **interface range f0/3 - 4, f0/7 - 24, g0/1 - 2**

S1(config-if-range)# **switchport mode access**

S1(config-if-range)# **switchport access vlan 999**

S1(config-if-range)# **shutdown**

S2(config)# **interface range f0/3 - 17, f0/19 - 24, g0/1 - 2**

S2(config-if-range)# **switchport mode access**

S2(config-if-range)# **switchport access vlan 999**

S2(config-if-range)# **shutdown**

### Assign VLANs to the correct switch interfaces.

* + - 1. Assign used ports to the appropriate VLAN (specified in the VLAN table above) and configure them for static access mode.

S1(config)# **interface f0/6**

S1(config-if)# **switchport mode access**

S1(config-if)# **switchport access vlan 20**

S2(config)# **interface f0/18**

S2(config-if)# **switchport mode access**

S2(config-if)# **switchport access vlan 20**

* + - 1. Issue the **show vlan** **brief** command and verify that the VLANs are assigned to the correct ports.

S1# **show vlan brief**

VLAN Name Status Ports

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

1 default active Fa0/1, Fa0/2

10 Management active

20 Clients active Fa0/6

999 Parking\_Lot active Fa0/3, Fa0/4, Fa0/5, Fa0/7

Fa0/8, Fa0/9, Fa0/10, Fa0/11

Fa0/12, Fa0/13, Fa0/14, Fa0/15

Fa0/16, Fa0/17, Fa0/18, Fa0/19

Fa0/20, Fa0/21, Fa0/22, Fa0/23

Fa0/24, Gi0/1, Gi0/2

1000 Native active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

S2# **show vlan brief**

VLAN Name Status Ports

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

1 default active Fa0/1, Fa0/2

10 Management active

20 Clients active Fa0/18

999 Parking\_Lot active Fa0/3, Fa0/4, Fa0/5, Fa0/6

Fa0/7, Fa0/8, Fa0/9, Fa0/10

Fa0/11, Fa0/12, Fa0/13, Fa0/14

Fa0/15, Fa0/16, Fa0/17, Fa0/19

Fa0/20, Fa0/21, Fa0/22, Fa0/23

Fa0/24, Gi0/1, Gi0/2

1000 Native active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

*Close configuration window*

## Configure 802.1Q trunks between the switches.

In Part 3, you will manually configure interfaces F0/1 and F0/2 as 802.1Q trunks.

* + - 1. Change the switchport mode on the interfaces to force trunking. Use the **interface range** command to reduce the number of commands required. Make sure to do this on both switches.

*Open configuration window*

S1(config)# **interface range f0/1-2**

S1(config-if-range)# **switchport mode trunk**

S2(config)# **interface range f0/1-2**

S2(config-if-range)# **switchport mode trunk**

* + - 1. As a part of the trunk configuration, set the native VLAN to 1000 on both switches. You may see error messages temporarily while the two interfaces are configured for different native VLANs.

S1(config-if-range)# **switchport trunk native vlan 1000**

S2(config-if-range)# **switchport trunk native vlan 1000**

* + - 1. As another part of trunk configuration, specify that VLANs 10, 20, and 1000 are allowed to cross the trunk.

S1(config-if-range)# **switchport trunk allowed vlan 10,20,1000**

S2(config-if-range)# **switchport trunk allowed vlan 10,20,1000**

* + - 1. Issue the **show interfaces trunk** command to verify the trunking ports, Native VLAN and allowed VLANs across the trunk.

S1# **show interfaces trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 1000

Fa0/2 on 802.1q trunking 1000

Port Vlans allowed on trunk

Fa0/1 10,20,1000

Fa0/2 10,20,1000

Port Vlans allowed and active in management domain

Fa0/1 10,20,1000

Fa0/2 10,20,1000

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 10,20,1000

Fa0/2 none

S2# **show interfaces trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 1000

Fa0/2 on 802.1q trunking 1000

Port Vlans allowed on trunk

Fa0/1 10,20,1000

Fa0/2 10,20,1000

Port Vlans allowed and active in management domain

Fa0/1 10,20,1000

Fa0/2 10,20,1000

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 10,20,1000

Fa0/2 10,20,1000

#### Question:

Why is the “Vlans in spanning tree forwarding state and not pruned” entry different for F0/1 and F0/2?

***Type your answers here.***

**In the example above spanning tree has placed F0/2 in the blocking state.**

*Close configuration window*

## Implement and Verify an EtherChannel between the switches.

* + - 1. Create a LACP-based EtherChannel using F0/1 and F0/2 using group number 1, with both switches actively negotiating the EtherChannel protocol. Use the **interface range** command to reduce the number of commands required.

*Open configuration window*

S1(config)# **interface range f0/1-2**

S1(config-if-range)# **channel-group 1 mode active**

S1(config-if-range)# **exit**

S2(config)# **interface range f0/1-2**

S2(config-if-range)# **channel-group 1 mode active**

S2(config-if-range)# **exit**

* + - 1. After the EtherChannel is configured, a virtual Port-Channel interface is automatically created. Now interface Port-Channel 1 represents the logical interface of the bundled physical ports F0/1 and F0/2. Additionally, the Port-Channel will inherit the configuration of the first physical port added to the EtherChannel.
      2. Issue the **show interfaces trunk** command to verify trunking is still in place

S1# **show interfaces trunk**

Port Mode Encapsulation Status Native vlan

Po1 on 802.1q trunking 1000

Port Vlans allowed on trunk

Po1 10,20,1000

Port Vlans allowed and active in management domain

Po1 10,20,1000

Port Vlans in spanning tree forwarding state and not pruned

Po1 10,20,1000

S2# **show interfaces trunk**

Port Mode Encapsulation Status Native vlan

Po1 on 802.1q trunking 1000

Port Vlans allowed on trunk

Po1 10,20,1000

Port Vlans allowed and active in management domain

Po1 10,20,1000

Port Vlans in spanning tree forwarding state and not pruned

Po1 10,20,1000

#### Question:

What does the port ‘Po1’ represent?

***Type your answers here.***

**The logical grouping of physical interfaces F0/1 and F0/2 is now seen as Port-channel 1 or Po1.**

* + - 1. Use the **show etherchannel summary** command to verify the EtherChannel configuration.

S1# **show etherchannel summary**

Flags: D - down P - bundled in port-channel

I - stand-alone s - suspended

H - Hot-standby (LACP only)

R - Layer3 S - Layer2

U - in use f - failed to allocate aggregator

M - not in use, minimum links not met

u - unsuitable for bundling

w - waiting to be aggregated

d - default port

Number of channel-groups in use: 1

Number of aggregators: 1

Group Port-channel Protocol Ports

------+-------------+-----------+-----------------------------------------------

1 Po1(SU) LACP Fa0/1(P) Fa0/2(P)

S2# **show etherchannel summary**

Flags: D - down P - bundled in port-channel

I - stand-alone s - suspended

H - Hot-standby (LACP only)

R - Layer3 S - Layer2

U - in use f - failed to allocate aggregator

M - not in use, minimum links not met

u - unsuitable for bundling

w - waiting to be aggregated

d - default port

Number of channel-groups in use: 1

Number of aggregators: 1

Group Port-channel Protocol Ports

------+-------------+-----------+-----------------------------------------------

1 Po1(SU) LACP Fa0/1(P) Fa0/2(P)

In the **show etherchannel summary** output the Portchannel is in "SU" this means the Portchannel is configured as layer-2 (S) and U stands for "in-use".  So the Portchannel is configured correctly and the physical ports are bundled. The flags, SU, indicate the etherchannel is Layer2 and in use.

*Close configuration window*

*End of document*

# Device Configs - Final

# Switch S1

S1# show run

Building configuration...

Current configuration : 3276 bytes

!

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname S1

!

boot-start-marker

boot-end-marker

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

system mtu routing 1500

!

!

no ip domain-lookup

!

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

!

interface Port-channel1

switchport trunk native vlan 1000

switchport trunk allowed vlan 10,20,1000

switchport mode trunk

!

interface FastEthernet0/1

switchport trunk native vlan 1000

switchport trunk allowed vlan 10,20,1000

switchport mode trunk

channel-group 1 mode active

!

interface FastEthernet0/2

switchport trunk native vlan 1000

switchport trunk allowed vlan 10,20,1000

switchport mode trunk

channel-group 1 mode active

!

interface FastEthernet0/3

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/4

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/5

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/6

switchport access vlan 20

switchport mode access

!

interface FastEthernet0/7

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/8

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/9

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/10

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/11

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/12

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/13

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/14

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/15

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/16

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/17

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/18

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/19

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/20

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/21

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/22

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/23

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/24

switchport access vlan 999

switchport mode access

shutdown

!

interface GigabitEthernet0/1

switchport access vlan 999

switchport mode access

shutdown

!

interface GigabitEthernet0/2

switchport access vlan 999

switchport mode access

shutdown

!

interface Vlan1

no ip address

!

interface Vlan10

ip address 192.168.10.11 255.255.255.0

!

ip http server

ip http secure-server

!

banner motd ^C Authorized Users Only! ^C

!

line con 0

password 7 14141B180F0B

login

line vty 0 4

password 7 14141B180F0B

login

line vty 5 15

login

vlan 10

name Management

vlan 20

name Clients

vlan 999

name Parking\_Lot

vlan 1000

name Native

exit

end

# Switch S2

S2# show run

Building configuration...

Current configuration : 3276 bytes

!

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname S2

!

boot-start-marker

boot-end-marker

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

system mtu routing 1500

!

!

no ip domain-lookup

!

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

!

interface Port-channel1

switchport trunk native vlan 1000

switchport trunk allowed vlan 10,20,1000

switchport mode trunk

!

interface FastEthernet0/1

switchport trunk native vlan 1000

switchport trunk allowed vlan 10,20,1000

switchport mode trunk

channel-group 1 mode active

!

interface FastEthernet0/2

switchport trunk native vlan 1000

switchport trunk allowed vlan 10,20,1000

switchport mode trunk

channel-group 1 mode active

!

interface FastEthernet0/3

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/4

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/5

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/6

switchport access vlan 20

switchport mode access

!

interface FastEthernet0/7

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/8

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/9

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/10

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/11

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/12

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/13

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/14

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/15

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/16

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/17

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/18

switchport access vlan 20

switchport mode access

!

interface FastEthernet0/19

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/20

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/21

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/22

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/23

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/24

switchport access vlan 999

switchport mode access

shutdown

!

interface GigabitEthernet0/1

switchport access vlan 999

switchport mode access

shutdown

!

interface GigabitEthernet0/2

switchport access vlan 999

switchport mode access

shutdown

!

interface Vlan1

no ip address

!

interface Vlan10

ip address 192.168.10.12 255.255.255.0

!

ip http server

ip http secure-server

!

banner motd ^C Authorized Users Only! ^C

!

line con 0

password 7 14141B180F0B

login

line vty 0 4

password 7 14141B180F0B

login

line vty 5 15

login

vlan 10

name Management

vlan 20

name Clients

vlan 999

name Parking\_Lot

vlan 1000

name Native

exit

end