Extended Access List Configuration With Packet Tracer

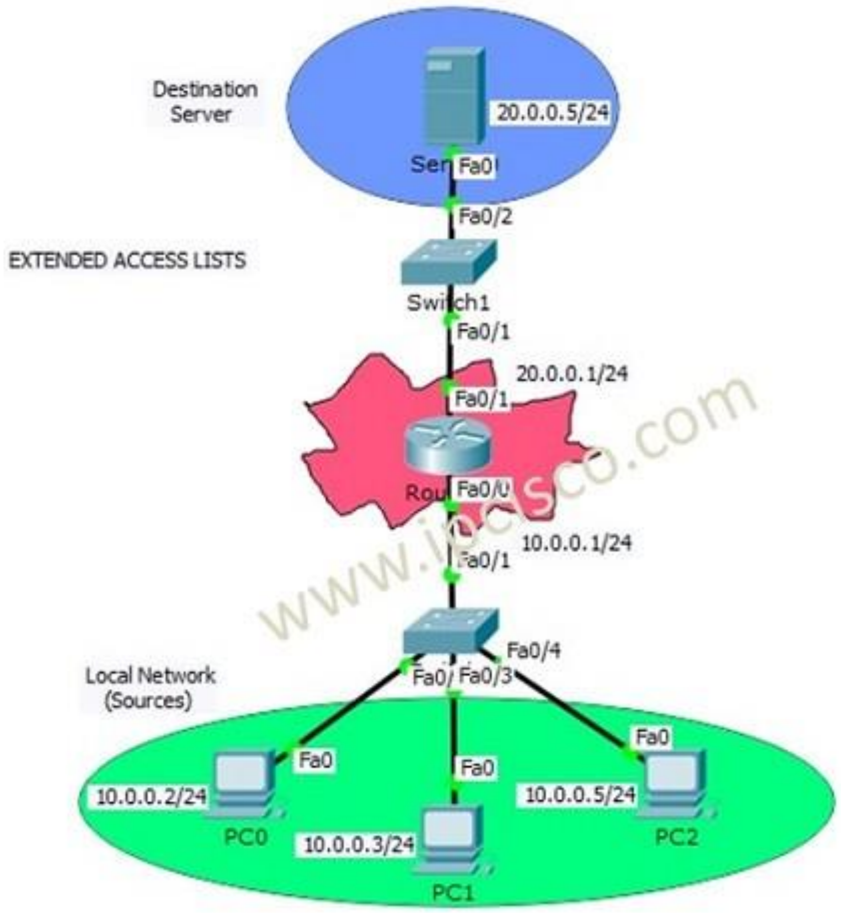
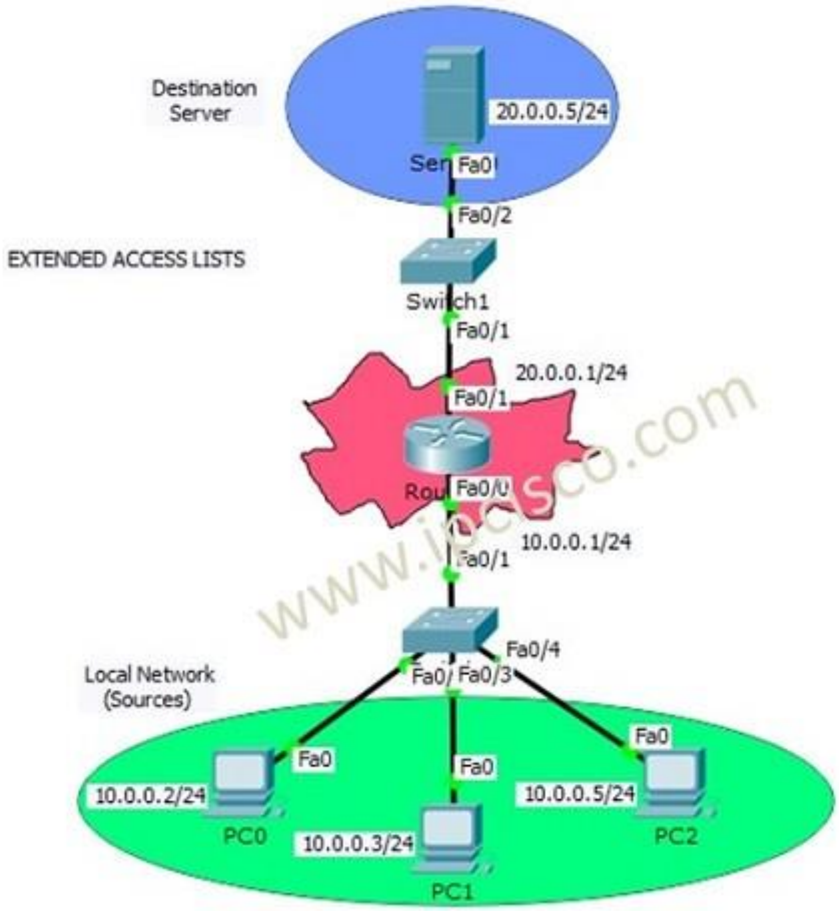


Table of Contents

□

Packet Tracer Extended Access Lists Configuration

In this lesson we will focus on **Cisco Extended ACL Configuration** with **Cisco Packet Tracer**. We will use the below topology for our packet tracer configuration.



You can **DOWNLOAD** the **Cisco Packet Tracer** example with **.pkt** format at the **End of This Lesson**.

Like **Standard ACL** configuration example, we will use one router, one destination server and 3 PCS in common. The switches in the topology will onlu used for port need.

Extended ACLs are a little complex if we compare with **Standard ACLs**. With **Extended ACLs**, we can restrict or allow specific things like **destination, protocol** or **port**.

In this **Cisco Extended ACL Configuration** example, we will **allow/deny ICMP protocol** through the server. As you know, **ICMP** is ping protocol. Here, PC0 and PC1 will be allowed and PC2 will be denied.

Extended Access-List Configuration

Let’s start to configure router for our **Cisco Extended ACL Configuration**.

For Extended ACLs, we can use **Extended Access-List Number** range **100 to 199**. Here, we will use 100.

```
Router # configure terminal
Router (config)# ip access-list extended 100
Router (config-ext-nacl)# permit icmp 10.0.0.0 0.0.0.3 host 20.0.0.5
Router (config-ext-nacl)# deny icmp host 10.0.0.5 host 20.0.0.5 host-unreachable
Router (config-ext-nacl)# end
Router # copy run start.
```

Standard Access List Configuration With Packet Tracer

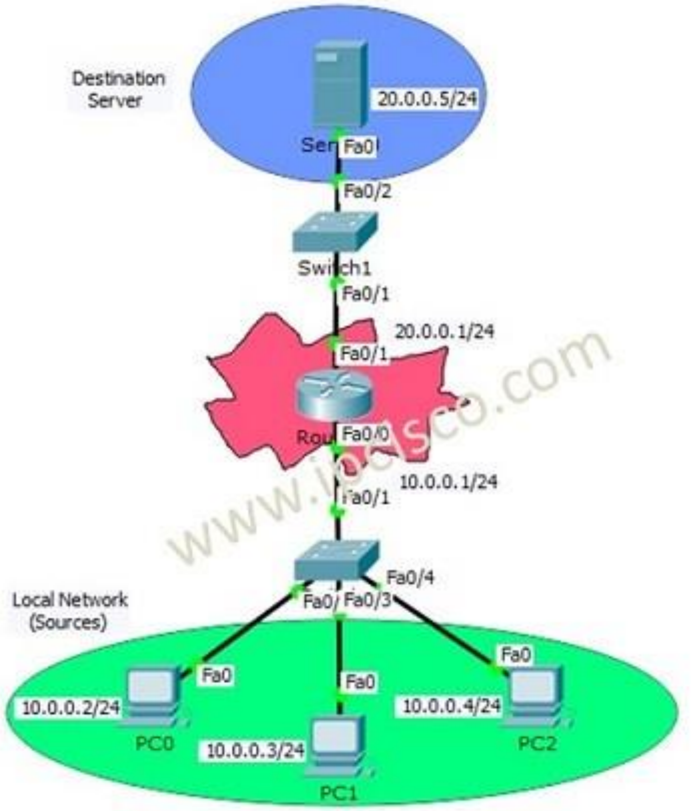


Table of Contents

□

Packet Tracer Standard Access List Configuration

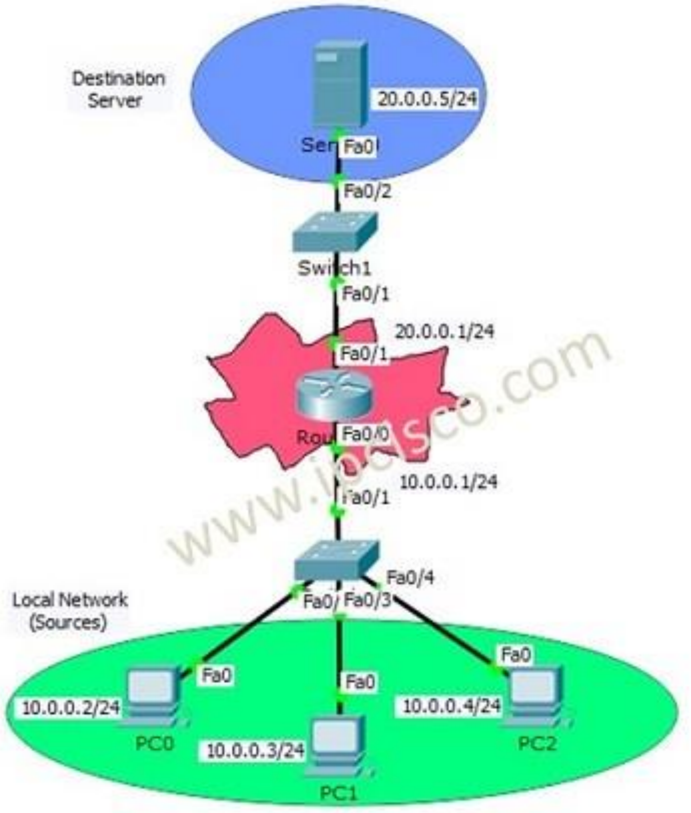
In this lesson we will see **Cisco Standard ACL Configuration** and how to configure **Standart Access-List** in Packet Tracer.
There are **three types Access Lists** in common. Thse access list types are :

- **Standard Access List**
- **Extended Access List**
- **Named Access List**

You can **DOWNLOAD** the **Cisco Packet Tracer** example with **.pkt** format at the **End of This Lesson**.

Standard Access-Lists are the simplest one. With Standard Access-List you can check only the source of the IP packets. On the other hand, with **Extended Access-Lists**, you can check source, destination, specific port and protocols. Lastly, with **Named Access-Lists**, you can use names instead of the numbers used in standard and extended ACLs. It do not have too much difference, but it is different with its named style.

In this lesson, we will focus on **Standart Access-List Configuration** with **Cisco Packet Tracer**. We will focus on the below topology.



Here, with our **Standard Access-List**, we will prohibit PC2 to access the server. But PC0 and PC1 can still access the server.

For our Standard Access-List, we can use the **ACL Number** 1 to 99. These numbers can be **100 to 199**, if you use extended ACLs.

Standard Access-List Configuration

Let’s start to do**Cisco Standard ACL Configuration**. We will configure the **Standard Access-List** on router .

```
Router # configure terminal
Router (config)# ip access-list standard 1
Router (config-std-nacl)# permit 10.0.0.2 0.0.0.0
Router (config-std-nacl)# permit 10.0.0.3 0.0.0.0
```

With this ACL configuration that we have written, we permit PC0 and PC1 to access the server. At the end of ACLs, there is an "**Implicit Deny**". These Implicit Deny, prohibits the other IP addresses. Because of the fact that we did not, allow PC2's IP address, it is autoamtically denied and can not access the server.

Here, there is no need to write but to show how to write deny, I will write the deny command also. As I said before, for this scenario, it is not necesary. But, you can write.

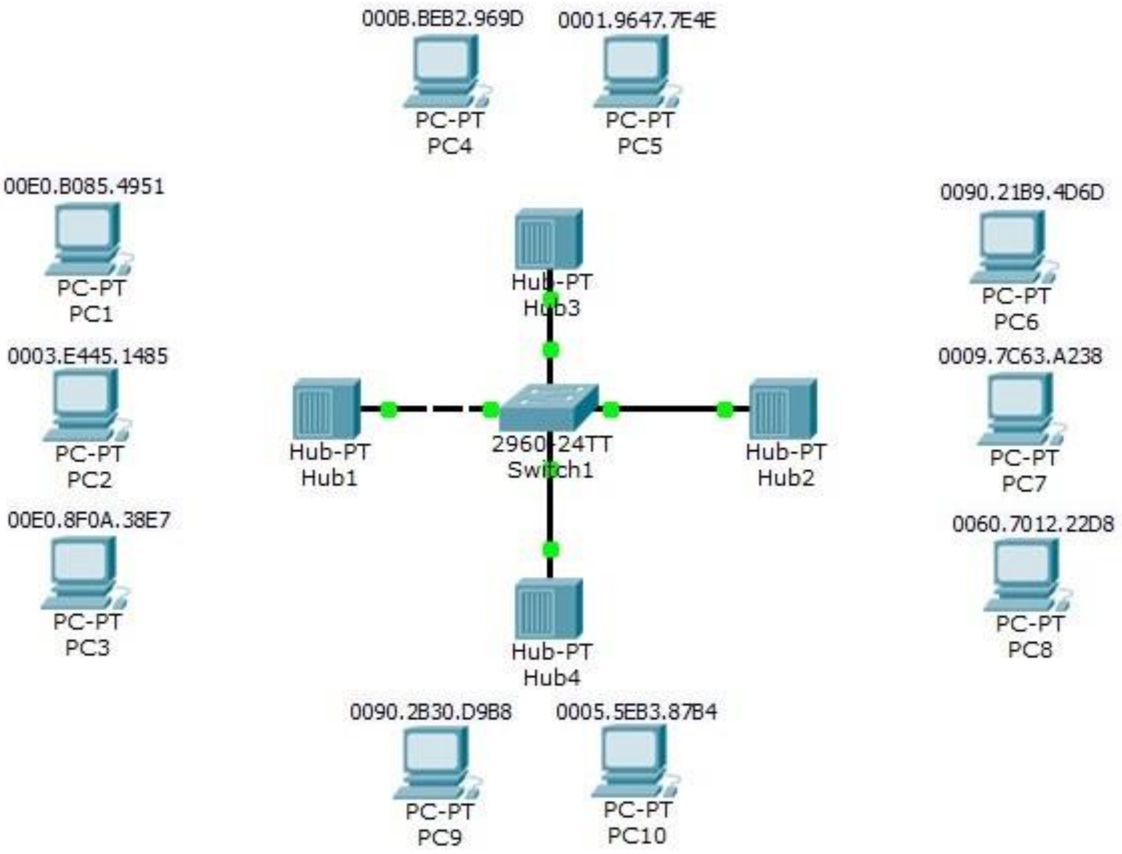
```
Router (config-std-nacl)# deny 10.0.0.4 0.0.0.0
Router (config-std-nacl)# end
Router # copy run start
```

Applying Standard Access-List to the Interface

After creating ACLs, we need to apply this ACL to the **interface**. For **Standard Access-List**, it is better to apply this ACL, close to the destination. So, for this configuration, we will apply our standard acceess list to the fastethernet 0/1 interface of the router.In other words, we will add ACL to the server face of the router.

You can also **DOWNLOAD** all the **Packet Tracer** examples with **.pkt** format in **Packet Tracer Labs**

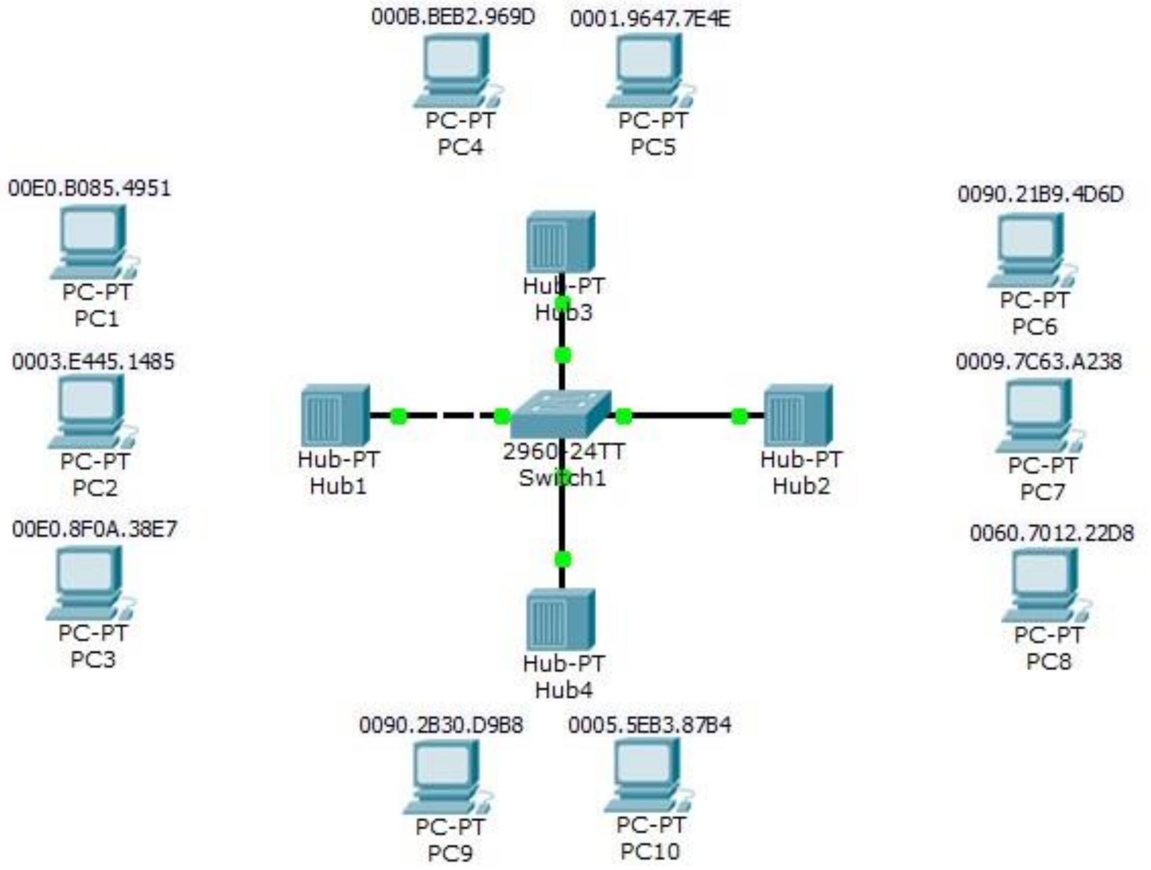
Switch Port Security Configuration with Cisco Packet Tracer



In this article, we will focus on detailed **Port Security** **Configuration**. For our **Port Security** **Configuration**, we will use the below topology. In this topology we will make examples for the configuration cases on Port Security.

You can **DOWNLOAD** the **Packet Tracer** example with **.pkt** format **HERE.**

You can download all Cisco Packet Tracer Labs on **Cisco Packet Tracer Labs** Page.



Switch Port Security Topology

Here we will use four scenario on four switch port. According to these scenarios, the below **Port Security** configuration will be done:

1.port

– max MAC 2
– 1 static MAC (PC1)
– 1 dynamic MAC (PC2)
– 1 violation (PC3)
– violation type shutdown

```
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 2
Switch(config-if)# switchport port-security mac-address 00E0.B085.4951
Switch(config-if)# switchport port-security mac-address 0003.e445.1485
Switch(config-if)# switchport port-security violation shutdown
```

2.port

– max MAC 2
– 2 dynamic MAC (PC6,PC7)
– 1 violation (PC8)
– violation type restrict

```
Switch(config)# interface fastEthernet 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 2
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security violation restrict
```

Basic Cisco Router Security Configuration

Table of Contents

How to Secure a Cisco Router Basically?

Security is an important concern for a network engineer. How can a network engineer provide security of a router? In this **Basic Cisco Router Security Configuration** lesson, we will talk about, how to **Secure a Router**. We sill see the **Router Security Steps** one by one. Let’s start.

Would you like to learn **Basic Cisco Router Configuration**?

Disabling Unused Ports

For a router basic security configuration, the first step is **shutdowning** all the **unused ports**. If you are using a port, it needs to be up. But if you don’t use any ports, then always disable (administratively down) these unused ports.

Shutdowning, in other words, disabling a port is very easy. You can do it with “**shutdown**” command under that interface.

```
Router(config)# interface fastethernet 0/0
Router(config-if)# shutdown
```

Enable and Enable Secret Passwords

The second important router security step is **passwords**. You should use passwords on your router.
Here, there are two passwords: **Enable** and **enable secret password**.

Enable password stores the password in clear text format. So, it is easy to see it. But ,enable secret password stores password in encrypted mode. So, it is more secure.

To **encrypt** all passwords in a router/switch, you can use “**service pasword-encryption**” command.
Let’s see how to configure this paswords on a router.

```
Router(config)# enable password 12345
Router(config)# enable secret 12345
Router(config)# service password-encryption
```

Configuring Telnet Access Password

Telnet is not a secure way of connecting to a router. But if you use telnet to connect a router, you should use telnet password.

To configure **Telnet Access** with password, you can use the below commands.

```
Router (config)# line vty 0 4
Router(config-line)# password 12345
Router(config-line)# login
```

Here, firstly we enter the **line vty mode** and then set the password string with password keyword. After that, we enter login command to activate it.

Configuring Console Access Password

Like telnet, you also need to configure **Console Access** password for a secure router. To do this, firstly you need to enter line **console mode** and then set the **password string**. Again, with the login keyword, you can activate it.

To configure **Console Access** with password, you can use the below commands.

```
Router(config)# line console 0
Router(config-line)# password 12345
Router(config-line)# login
```

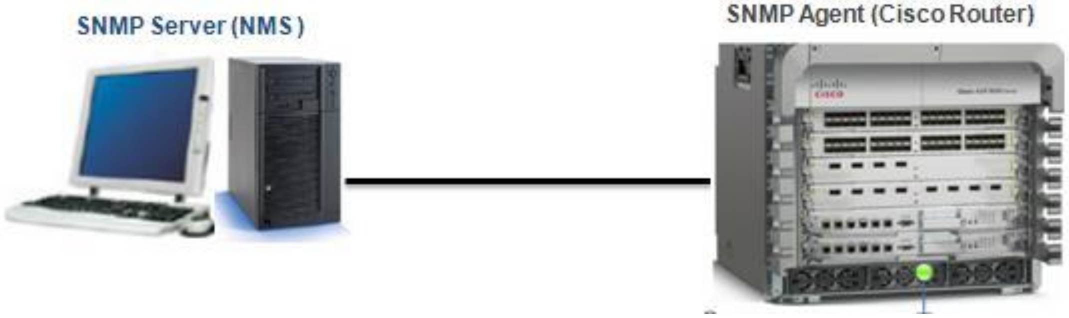
Configuring Auxiliary Port Access Password

Aux Port Access password is rarely used. But like telnet and console, you can configure its password in line aux mode.

To configure **Aux Port Access** with password, you can use the below commands.

- SNMP Configurations

SNMP Configuration On Cisco IOS



In this **Cisco SNMP Configuration Example**, we will see **how to configure SNMP** on Cisco **SNMP Agent** device. In this part I do not consider necessary what the **snmp agent** is. You already know that it is the device that we consider to manage with our **NMS (Network Management Server).**

Managing all the network devices are a very difficult. So managing the network devices in one location is very important in network world. This is done with a standard protocol **SNMP**. With SNMP you can manage your devices with a **NMS** remotely and in a central point. And the agent device also sends traps,notifications about alarms or exceeding some threshold values determined before for a good managed network.

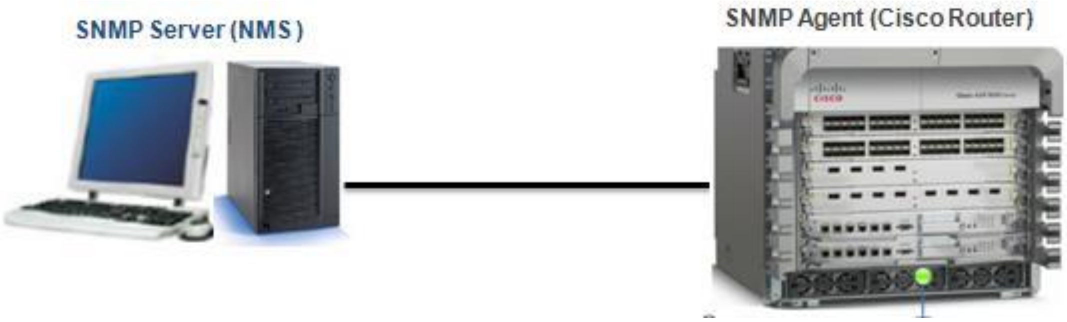


Table of Contents

SNMP Community Configuration

Like for all the vendor devices, to manage a **Cisco** devices from a central point we need SNMP. And to use SNMP, for **Cisco SNMP Configuration**, we need to enable this protocol. Enabling this protocol is done by creating a **community strings**. **Community strings** are used for the different access forms in SNMP. You can make the below configuration for different community string definitions.

```
Router (config)# snmp-server community public ro
Router (config)# snmp-server community ForYou ro
Router (config)# snmp-server community WithYourACL rw 10
Router (config)# snmp-server community HidenOne ro view noRouteTable
Router (config)# access-list 10 permit 192.168.100.1
```

Above, there are four community strings are defined. The first one can be for eveyone with only **read-only** access. The second one can be for you only. Here it is important to say that other vendors do not permit more than one **read-only community strings**.

The third community string above is the read-write one only allowed as the **access-list 10**. And the last one is the one that can be reached only with a certain user.

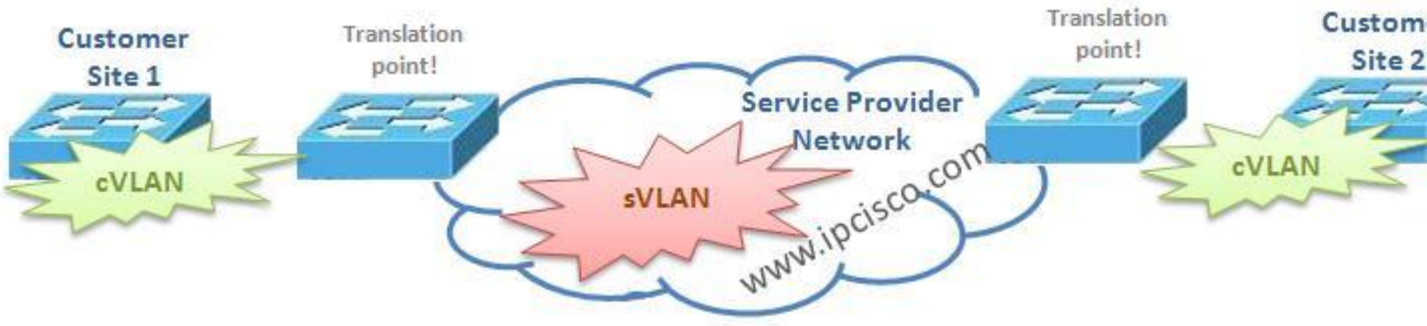
SNMP Trap Configuration

On our **Cisco SNMP Configuration** example, after defining community strings, it is time to configure something for **SNMP traps** that will inform SNMP Server during any trouble. To do this, use the below configuration commands.

```
Router (config)# snmp-server enable traps

Router (config)# snmp-server host 192.168.1.1 public
```

- ## VLAN Configurations

VLAN Mapping (VLAN Translation) on Cisco



On Cisco devices, VLAN mapping term is used for mentioning the swap of incoming VLAN id to a new VLAN id. In the below configuration examples, we will see Cisco configuration for this swapping. Lets check this configuration for a Cisco switch. The related congfiguration steps are:

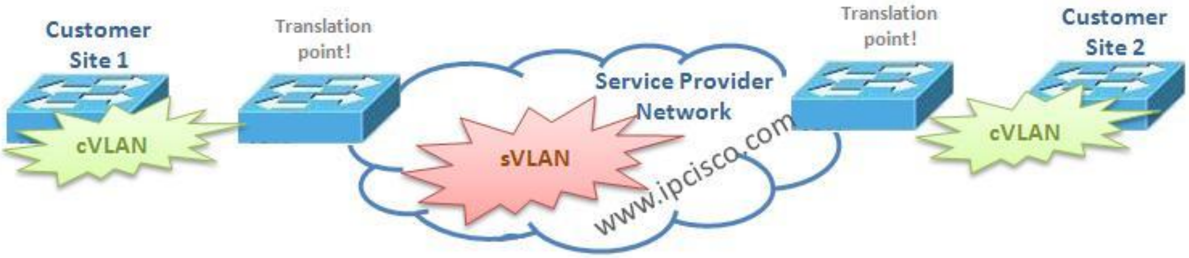
```
Switch# configure terminal

Switch(config)# interface interface-id

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport vlan mapping vlan-id translated-id

Switch(config-if)# end
```

And to verify, the below command scan be used:

```
Switch# show vlan mapping

Switch# copy running-config startup-config
```

As an example, we can configure the customer 10,20,30 and 40 VLANs(C-VLAN s) to the Service provider vlans(S-VLAN s),110,120,130 and 140.

```
Switch(config)# interface gigabiethernet 0/1

Switch(config-if)# switchport vlan mapping 10 110

Switch(config-if)# switchport vlan mapping 20 120

Switch(config-if)# switchport vlan mapping 30 130

Switch(config-if)# switchport vlan mapping 40 140

Switch(config-if)# exit
```



VLAN Mapping CVLAN SVLAN

Private VLAN Cisco Configuration Example

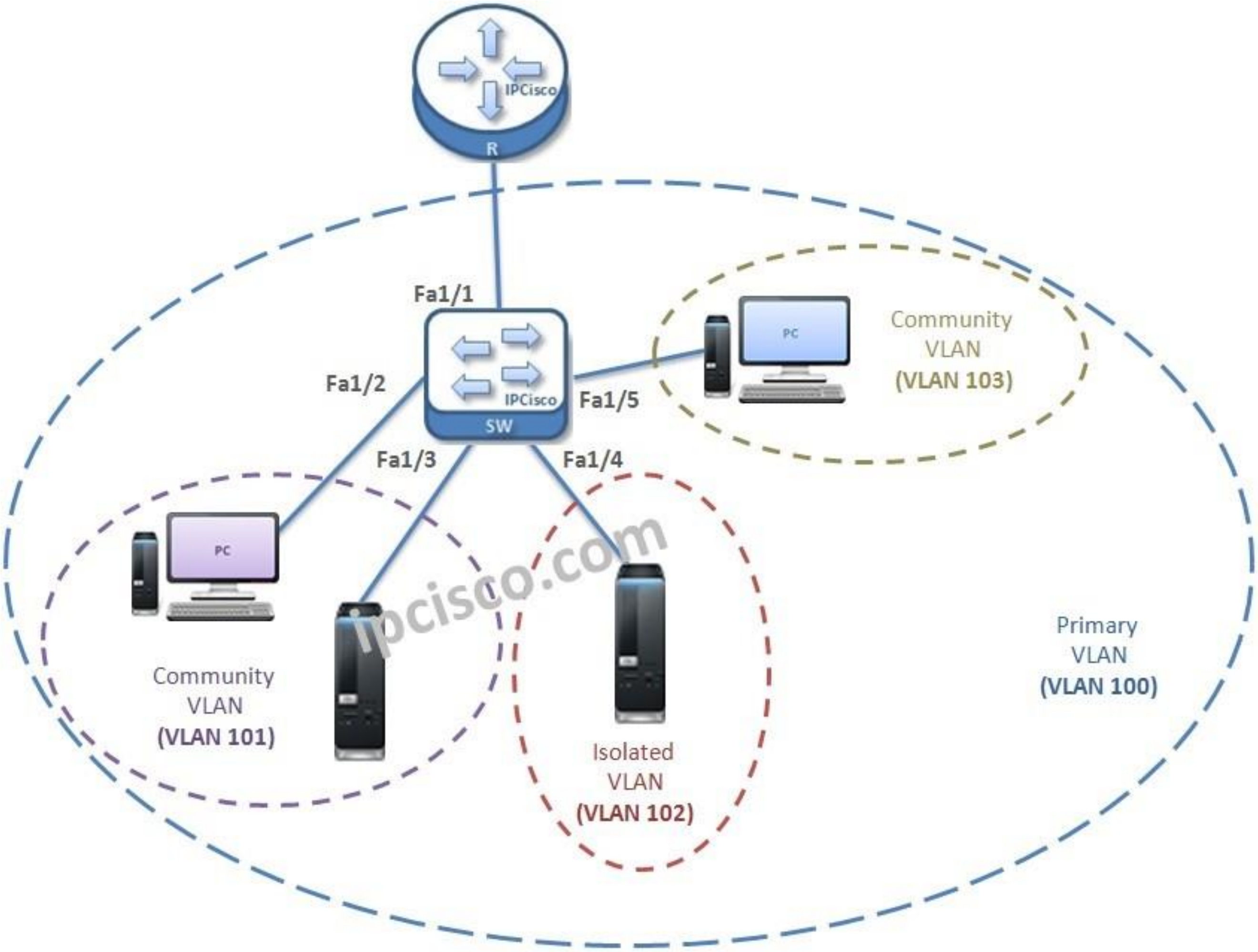
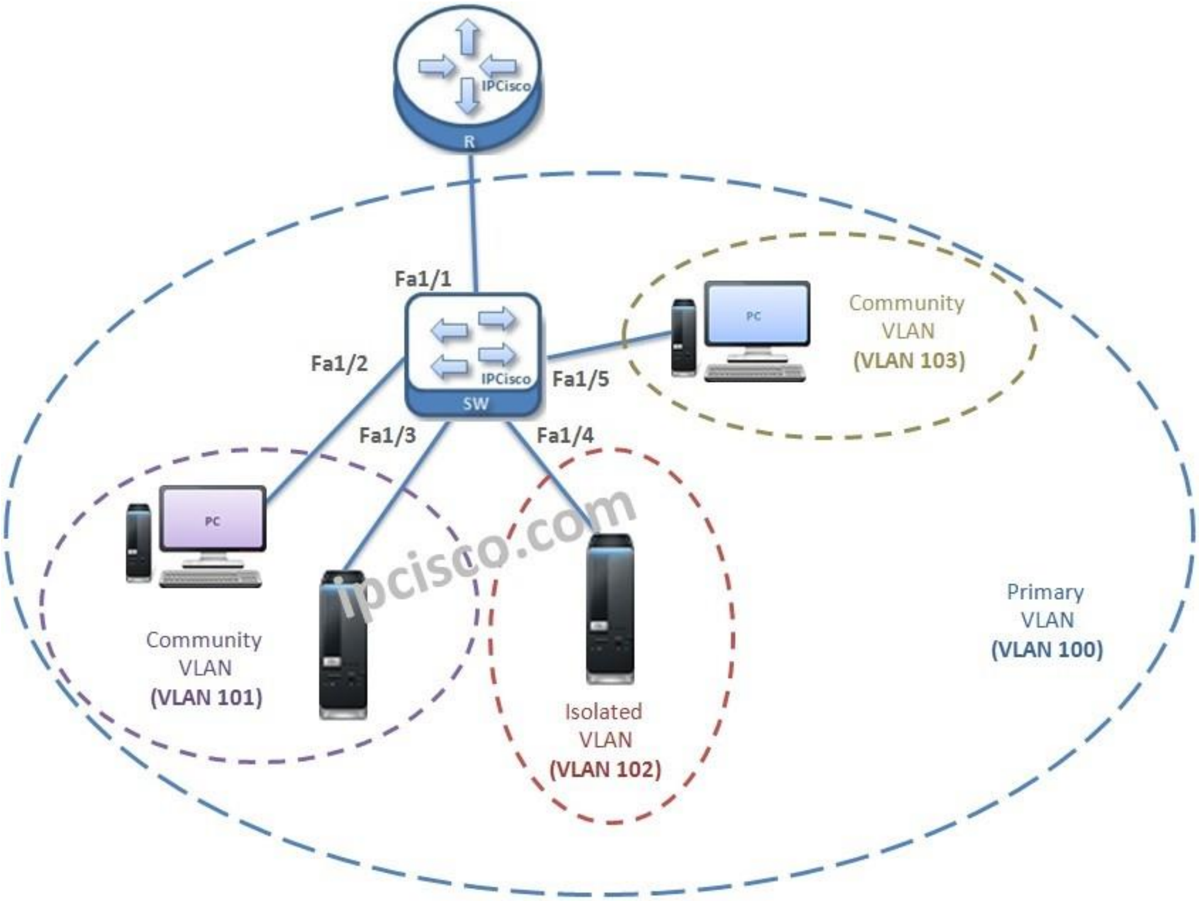


Table of Contents

□

Cisco Private VLAN Configuration Example

For **Private VLAN** configuration, we will do a configuration example with one switch and one router. Here, we will use the same topology that we have used before for Private VLAN overview. Our topology, ports and VLANs will be like below:



We will do the below **Configuration** on the **Switch**, one by one.

For all Packet Tracer Examples and Files, you can check **Packet Tracer Labs** Page.

Cisco Private VLAN Configuration Steps

1. Set VTP Mode as “Transparent Mode”.

The first step is determination of the **VTP Mode** of the switch. It must be in **“Transparent Mode”**.

```
IPCisco# config terminal

IPCisco(config)# vtp mode transparent
```

2. Secondary VLANs Creation.

Secondly, we will create the **Secondary VLANs**.

```
IPCisco(config)# vlan 101

IPCisco(config-vlan)# private-vlan community

IPCisco(config-vlan)# end
```

```
IPCisco(config)# vlan 102

IPCisco(config-vlan)# private-vlan community

IPCisco(config-vlan)# end
```

```
IPCisco(config)# vlan 103

IPCisco(config-vlan)# private-vlan isolated

IPCisco(config-vlan)# end
```

3. Primary VLAN Creation.

In the step three, we will create **Primary VLAN**.

```
IPCisco(config)# vlan 100

IPCisco(config-vlan)# private-vlan primary

IPCisco(config-vlan)# end
```

For all Packet Tracer Examples and Files, you can check [Packet Tracer Labs] Page.

---

4. Association Secondary VLANs to Primary VLAN.

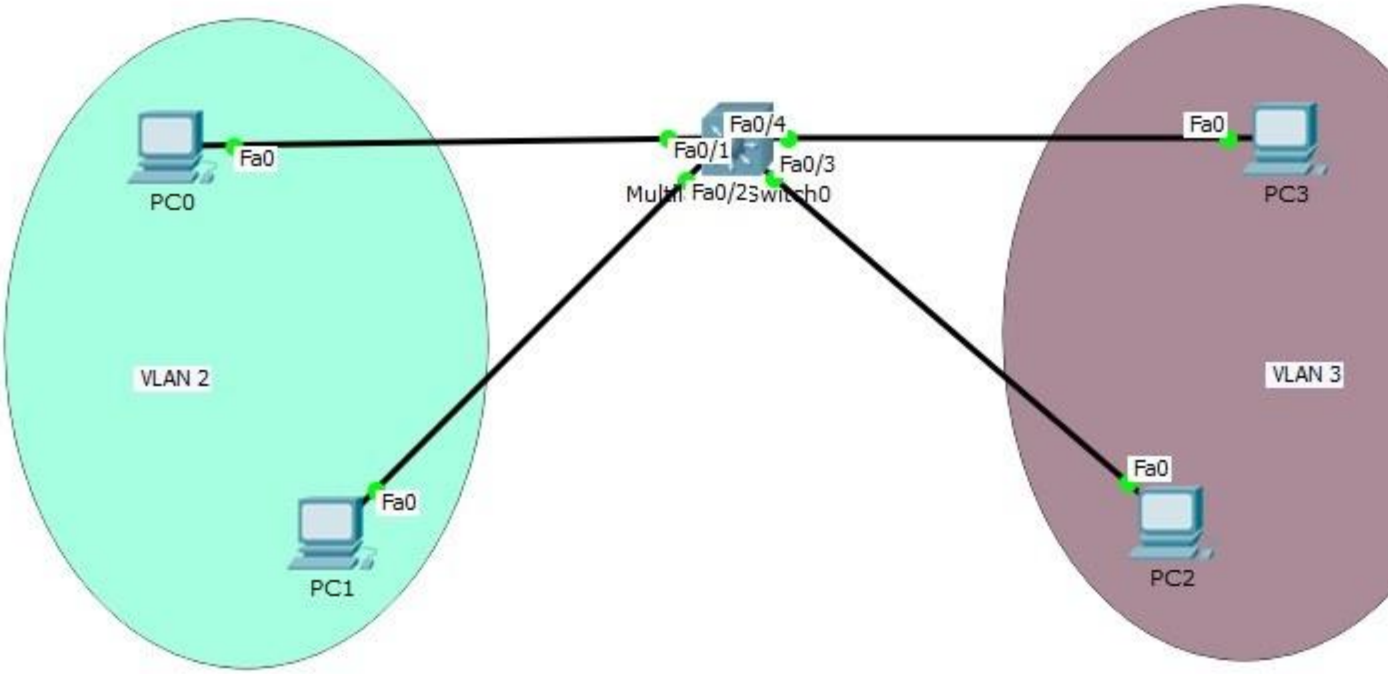
Secondary VLANs need to be **associated** to the **Primary VLAN**.In this step, we will associate Secondary VLANs to Primary VLANs.

```
IPCisco(config)# vlan 100

IPCisco(config-vlan)# private-vlan association 101-103

IPCisco(config-vlan)# end
```

After this step, we can use “show vlan private-vlan” command and we can see all the Secondary VLANs are associated with Primary VLAN.

```
IPCisco# show vlan private-vlan

Primary        Secondary      Type           Interfaces

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

100            101            community

100            102            community

100            103            isolated
```

Switch Virtual Interface Configuration on Packet Tracer



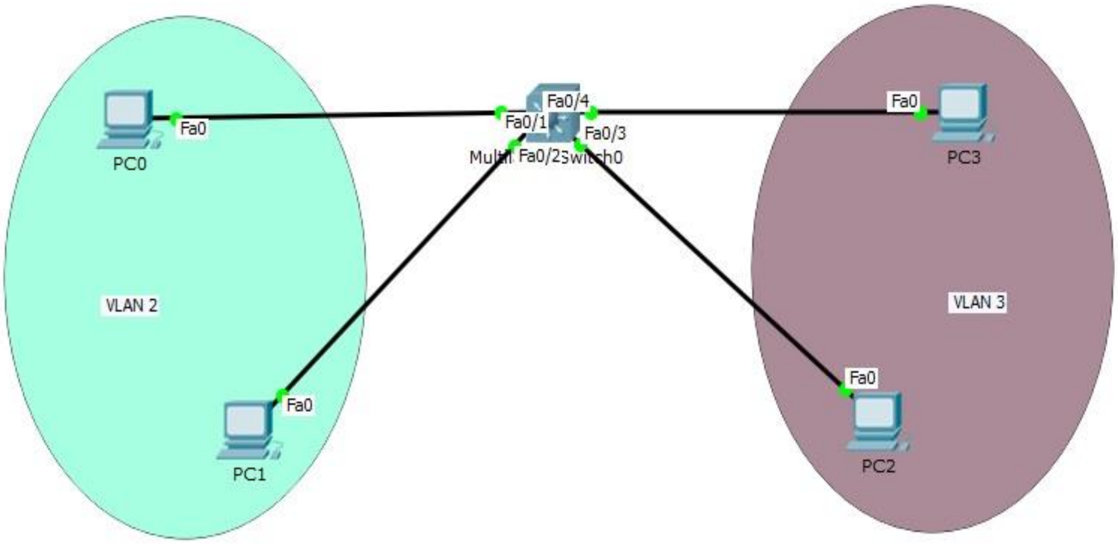
Theorically **switches** work in Layer 2 (Layer 2 switches). When you talk about switches, generally you do not think IP addresses. One of the ways that make a switch IP available is, configuring **Switch Virtual Interfaces (SVI)**. **Switch Virtual Interfaces (SVI)** is basically, an IP assigned VLAN, an interface for that **VLAN**. Here, we will see **SVI in Cisco**, **Cisco SVI Configuration**.

You can **DOWNLOAD** the **Cisco Packet Tracer** example with **.pkt** format **At the End of This Lessons**.

You can also **DOWNLOAD** all the **Packet Tracer** examples with **.pkt** format in **Packet Tracer Labs** section.

Here, the important point is the switch type. If the switch is layer 2 switch, then you can configure one Switch Virtual Interface (SVI). But, in Multilayer switches, you can configure **Switch Virtual Interfaces (SVI)**.

In this **Switch Virtual Interfaces (SVI)** Packet Tracer example, we will use a **Multi Layer Switch** and we will create two **VLANs**. In each VLAN, we will use 2 PCs. And in our Switch Virtual Interfaces (SVI) configuration, we will use two SVIs. After this configuration, Inter VLAN Routing will work and different VLANs can communicate.



Switch Virtual Interfaces (SVI)

Now, it is time to Switch Virtual Interface (SVI) configuration.

Cisco Hands On Course

Let's start with PC ip addresses. We will use the below IP addresses on these PCs. We will also configure the Gateway addresses of these PCs. The Gateway addresses are the addresses that we will configure as address of our **Switch Virtual Interfaces (SVI)**.

```
PC0 : 10.0.0.2 255.255.255.0 GW: 10.0.0.1
PC1 : 10.0.0.3 255.255.255.0 GW: 10.0.0.1
PC2 : 20.0.0.2 255.255.255.0 GW: 20.0.0.1
PC3 : 20.0.0.3 255.255.255.0 GW: 20.0.0.1
```

On Muti Layer switch, we will create **VLANs** and we will assign the ports to these VLANs.

```
MLSwitch (config-vlan) # vlan 2
MLSwitch (config-vlan) # vlan 3
MLSwitch (config-vlan) # exit
MLSwitch (config) # interface range fastEthernet 0/1-2
MLSwitch (config-if-range) # switchport mode access
MLSwitch (config-if-range) # switchport access vlan 2
MLSwitch (config-if-range) # exit
```

```
MLSwitch (config) # interface range fastEthernet 0/3-4
MLSwitch (config-if-range) # switchport mode access
MLSwitch (config-if-range) # switchport access vlan 3
MLSwitch (config-if-range) # exit
```

VLAN configurations of our **Switch Virtual Interface (SVI)** topology is OK now.Let’s verify our VLANs.

Inter VLAN Routing Configuration on Packet Tracer (Router on Stick)

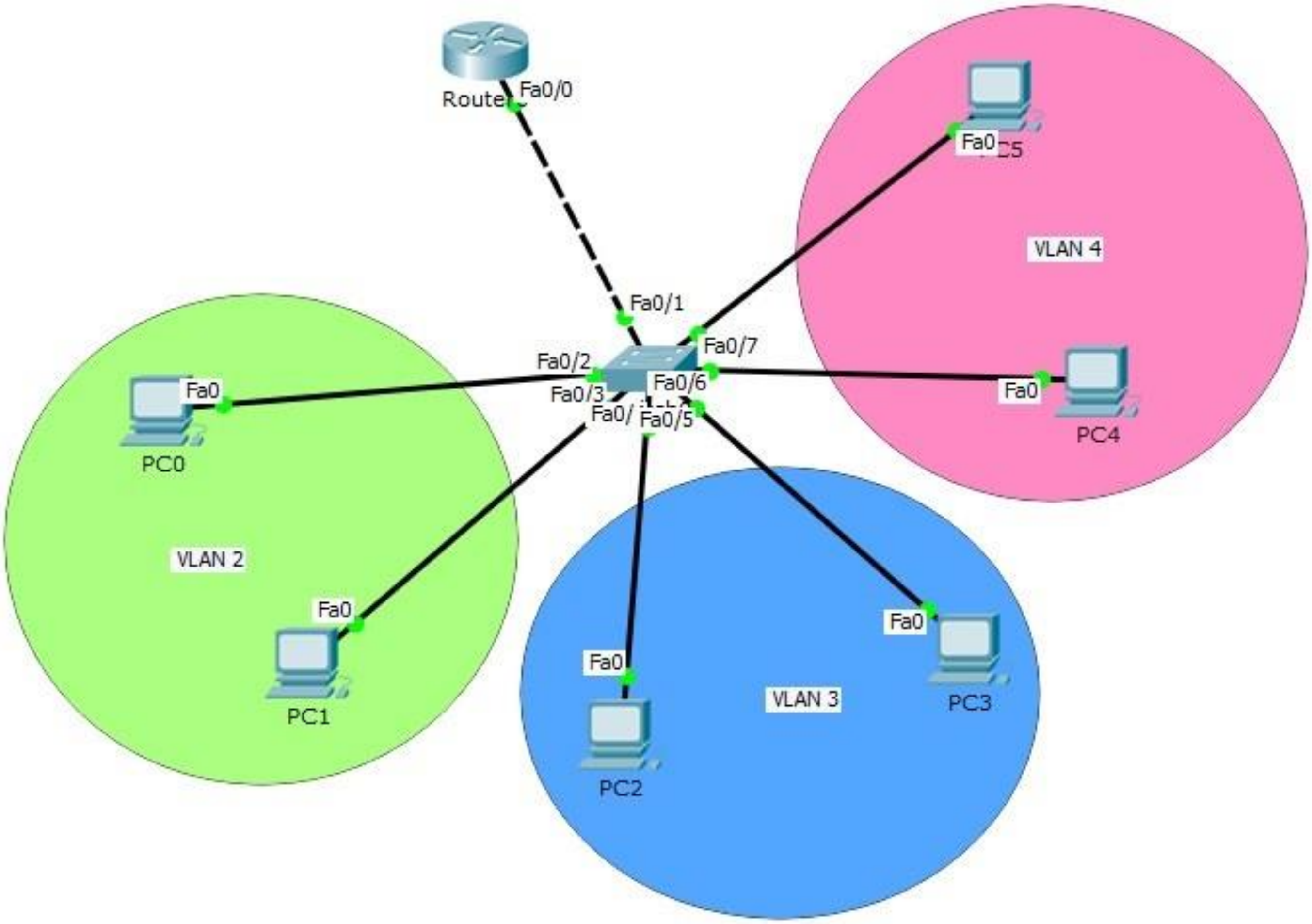


Table of Contents

□

Router on Stick Configuration on Packet Tracer

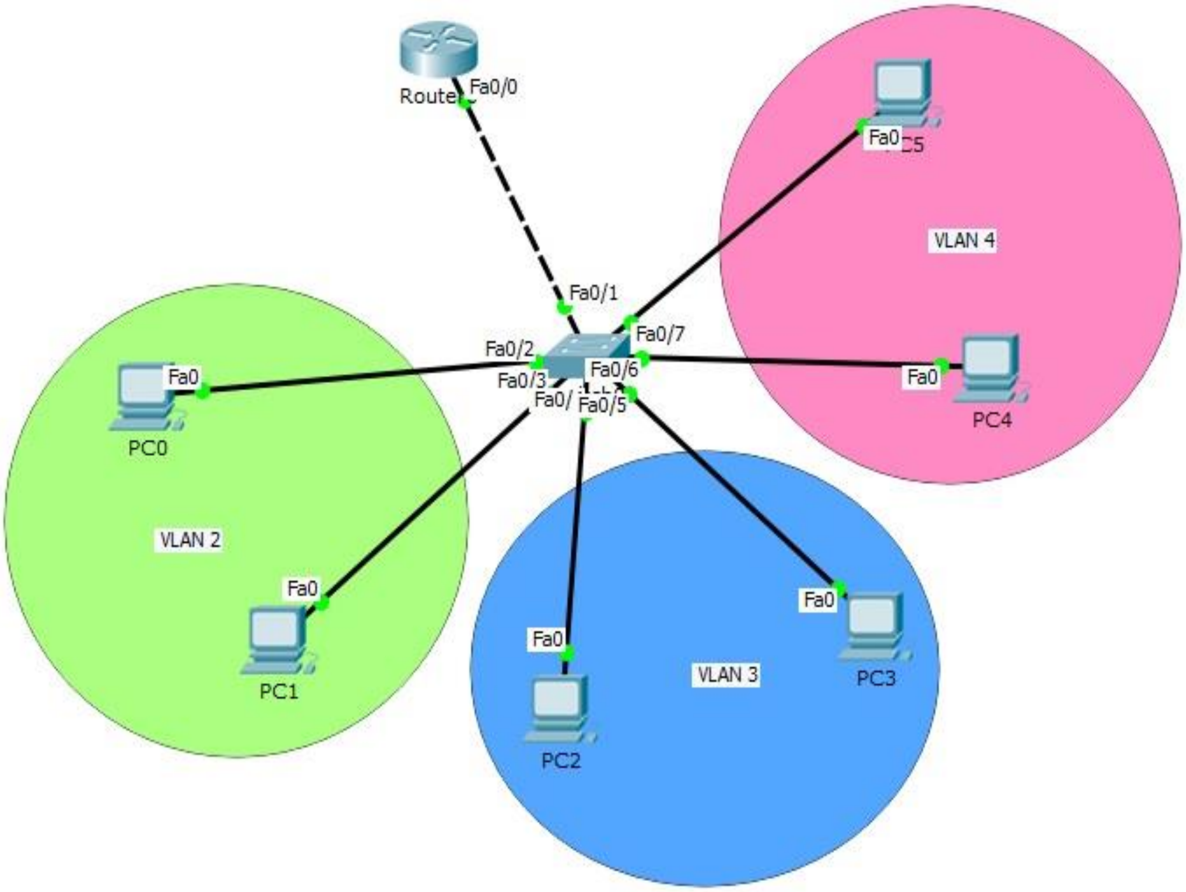
VLANs are the virtual LANS that provide divide your big network, into smaller pieces. Many companies use to divide their networks into different departments. We have discussed the basic logic of VLANs in the previous articles.As you know each **VLAN** is a seperate VLAN. Each of them is a single network. So at the beginning, there is no communication between VLAN. To enable the communication of these different sub networks, we need **Inter VLAN Routing**. In other words, this topology called “**Router on Stick**” topology. Inter VLAN Routing topology or Router on Stick topology is a very common topology for CCNA exams. We will learn Routing on Stick Topology and **Router on Stick Config** on this lesson.

You can **DOWNLOAD** the **Packet Tracer** example with **.pkt** format **At the End of This Lesson**.

You can also **DOWNLOAD** all the **Packet Tracer** examples with **.pkt** format in **Packet Tracer Labs** section.

You can download “Cisco Packet Tracer” in Tools section.

In this article, we will use the below Router on Stick topology and we will configure **Inter VLAN Routing** on Packet Tracer.



Router on Stick Topology

Router on Stick (Inter VLAN Routing) topology basically consist of one switch and a router. Here, the switch is the place that our VLANs exist and the router is the device that route the traffic.

Router on Stick Configuration Steps

For Router on Stick topology (Inter VLAN Routing) configuration, we will create router virtual interfaces under the router interfaces. Then, we will assign each of this virtual interface to a specific VLAN. We will also create our VLANs and configure the PCs on that VLAN.
For **Router on Stick topology** (Inter VLAN Routing), we will use one switch, one router and six PCs in **Packet Tracer**. And we will have 3 VLANs.

Let’s start to configure our **Router on Stick topology (Inter VLAN Routing)**.

IP Configurations For Inter VLAN Routing

We will use 10.0.0.0/24, 20.0.0.0/24 and 30.0.0.0/24 blocks for our **Packet Tracer Router on Stick** topology example. The first block will be for VLAN 2, the second will be for VLAN 3 and the last one will be for VLAN 4.

Firstly, we ll configure the IP addresses of the PCs on **Packet Tracer** like below.

PC0 : 10.0.0.2 255.255.255.0
GW : 10.0.0.1

PC1 : 10.0.0.3 255.255.255.0
GW : 10.0.0.1

PC2 : 20.0.0.2 255.255.255.0
GW : 20.0.0.1

PC3 : 20.0.0.3 255.255.255.0
GW : 20.0.0.1

PC4 : 30.0.0.2 255.255.255.0
GW : 30.0.0.1

PC5 : 30.0.0.3 255.255.255.0
GW : 30.0.0.1

Here, the gateway addresses of the PCs will be the IP address of router virtual interfaces. Each router virtual interface will have an IP addresses as gateway of one of the **VLANs**.

Creating VLANs

Now, let’s configure our VLANs and assign the interfaces to these VLANs. Firstly we will create VLAN 2,3 and 4. Then, we will enter the interface range and configure the interface range as access interface. Lastly, we will assign the interface to a specific VLAN with “**switchport access vlan**” command.

```
Switch (config) # vlan 2
Switch (config-vlan) # vlan 3
Switch (config-vlan) # vlan 4
Switch (config-vlan) # exit
Switch (config) # interface range fastEthernet 0/2-3
Switch (config-if-range) # switchport mode access
Switch (config-if-range) # switchport access vlan 2
Switch (config-if-range) # exit
Switch (config) # interface range fastEthernet 0/4-5
Switch (config-if-range) # switchport mode access
Switch (config-if-range) # switchport access vlan 3
Switch (config-if-range) # exit
Switch (config) # interface range fastEthernet 0/6-7
Switch (config-if-range) # switchport mode access
Switch (config-if-range) # switchport access vlan 4
Switch (config-if-range) # exit
```

Our VLAN configurations are OK on the switch now. Let’s verify the VLANs.

You can also **DOWNLOAD** all the **Packet Tracer** examples with **.pkt** format in **Packet Tracer Labs** section.

```
Switch# show vlan
```

```
VLAN Name Status Ports
—- ———————————————— ——— ———————————————-
1 default active 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, Gig0/1, Gig0/2
2 VLAN0002 active Fa0/2, Fa0/3
3 VLAN0003 active Fa0/4, Fa0/5
4 VLAN0004 active Fa0/6, Fa0/7
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup

AN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
—- —— ———- —— ——— ——— ———— —- ———— ——— ———
1 enet 100001 1500 – – – – – 0 0
2 enet 100002 1500 – – – – – 0 0
3 enet 100003 1500 – – – – – 0 0
4 enet 100004 1500 – – – – – 0 0
```

As you can see, for our **Router on Stick** topology, Interface Fa0/2 and Fa0/3 are the member of VLAN 2, Interface Fa0/4 and Fa0/5 are the member of VLAN 3, Interface Fa0/6 and Fa0/7 are the member of VLAN 4. Interface Fa0/1 is not on the VLAN table. Because it is our Trunking port.

Trunk Interface Configuration

It is time to configure the switch’s router face interface, interface 0/1. We will connect switch to the router, with this interface. This interface will be a trunk port. In our Router on Stick topology, **Trunk** interface will pass all our VLANs that we allowed.

```
Switch (config) # interface fastEthernet 0/1
Switch (config-if) # switchport mode trunk
Switch (config-if) # switchport trunk allowed vlan 2,3,4
Switch (config-if) # exit
```

Router on Stick Configuration

Our switch configuration is ok, on **Packet Tracer**. We can configure the router, Router on Stick now. On Router on Stick, we will configure Fa0/0 interface and the router virtual interfaces under this interface for Inter VLAN Routing.

```
Router (config) # interface fastEthernet 0/0
Router (config-if) # no shutdown
Router (config-if) # exit
```

Packet Tracer VLAN Configuration Example

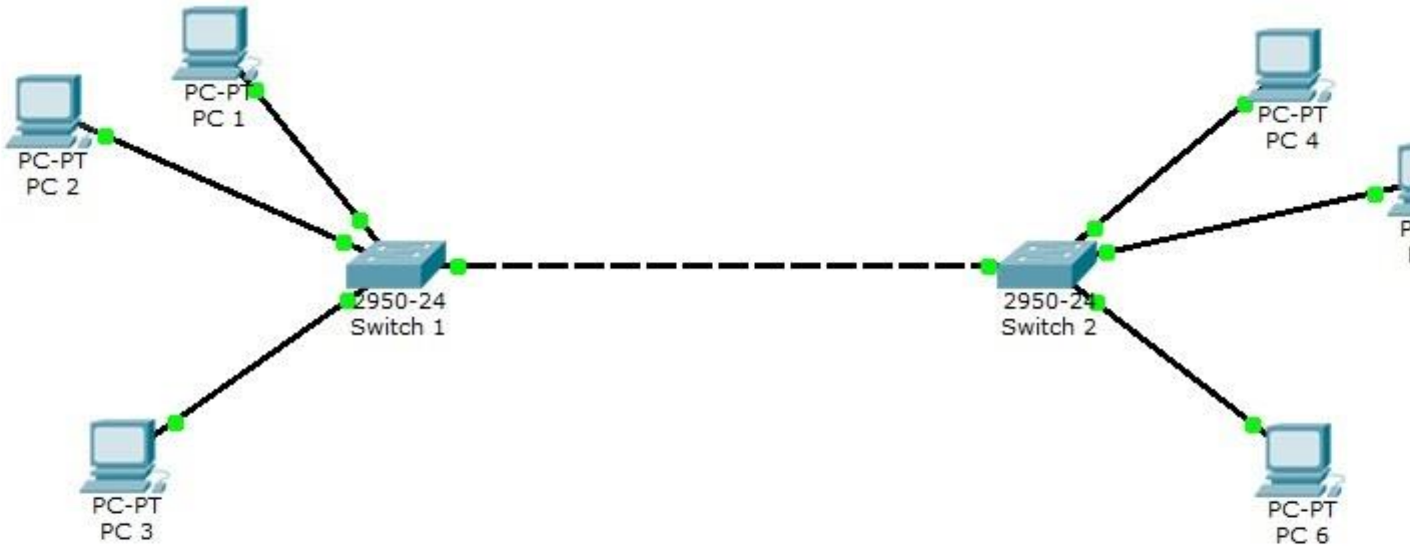
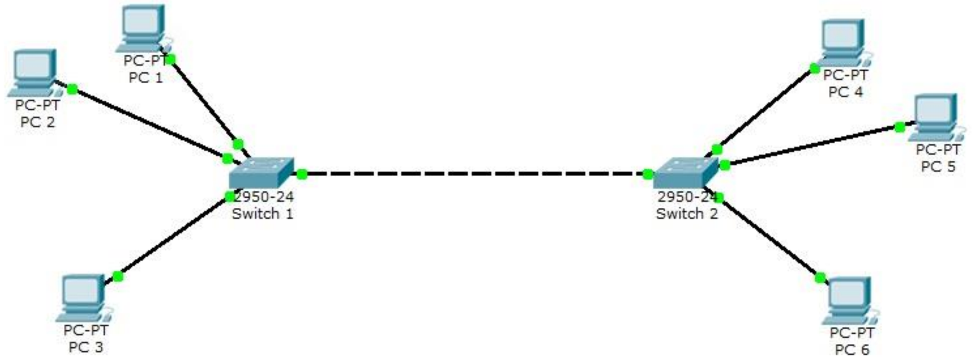


Table of Contents

☐

Packet Tracer VLAN Configuration

As an example, you can see a **VLAN topology** below. In this topology, 2 **Cisco Catalyst 2950-24** switches and 6 **PCs** are used.



Packet Tracer VLAN Topology Example

You can **DOWNLOAD** the **Cisco Packet Tracer** example with **.pkt** format **at the end of the lesson**.

For all Packet Tracer Examples and Files, you can check **Packet Tracer Labs** Page.

PC Configurations

For our **VLAN Configuration example**, we will set our PC IPaddresses as below. These ip addresses will be required at the end of this configuration example to test our configuration.

PC 1 –> 192.168.1.2 VLAN 2
PC 2 –> 192.168.1.3 VLAN 2
PC 3 –> 192.168.1.4 VLAN 3
PC 4 –> 192.168.1.6 VLAN 3
PC 5 –> 192.168.1.7 VLAN 3
PC 6 –> 192.168.1.8 VLAN 2

VLAN Configuration on Switch 1

After PC IP configurations, now, we can start our **VLAN Packet Tracer Configuration** steps. Here, we will follow the below steps:

1. We will set access ports that will access specific VLANs. We will do this with "**switchport mode access**" command under these interfaces.
2. We will also set the VLAN, that this port will access.
3. After that, we will set the trunk port that will carry multiple VLANs with "**swithcport mode trunk**" command.
4. Then we will also set this port with "**no negotiate**" command to prevent negotiation about the port role.
5. Laslty, we will set the allowed VLANs with "**switchport trunk allowed vlan**" command on this trunk and save our configuration.

```
Switch 1(config)# interface fastEthernet 0/2
Switch 1(config-if)# switchport mode access
Switch 1(config-if)# switchport access vlan 2

Switch 1(config)# interface fastEthernet 0/3
Switch 1(config-if)# switchport mode access
Switch 1(config-if)# switchport access vlan 2

Switch 1(config)# interface fastEthernet 0/4
Switch 1(config-if)# switchport mode access
Switch 1(config-if)# switchport access vlan 3

Switch 1(config)# interface fastEthernet 0/1
Switch 1(config-if)# switchport mode trunk
Switch 1(config-if)# switchport nonegotiate
Switch 1(config-if)# switchport trunk allowed vlan 2-4

Switch 1# copy running-config startup-config
```

VLAN Configuration on Switch 2

After configuring the first switch, we will configure switch 2 similar to switch 1 as below.

```
Switch 2(config)# interface fastEthernet 0/2
Switch 2(config-if)# switchport mode access
Switch 2(config-if)# switchport access vlan 3

Switch 2(config)# interface fastEthernet 0/3
Switch 2(config-if)# switchport mode access
Switch 2(config-if)# switchport access vlan 2

Switch 2(config)# interface fastEthernet 0/4
Switch 2(config-if)# switchport mode access
Switch 2(config-if)# switchport access vlan 2

Switch 2(config)# interface fastEthernet 0/1
Switch 2(config-if)# switchport mode trunk

Switch 2(config-if)# switchport nonegotiate

Switch 2(config-if)# switchport trunk allowed vlan 2-4

Switch 2# copy running-config startup-config
```

Checking VLAN Configuration

Our last step of **VLAN Packet Tracer Example** is configuration **verification**. to verify our VLAN Packet Tracer Configuration, we will use verification commands like “**show vlan brief**‟, “**show interfaces**‟, “**show interfaces trunk**” etc.

```
Switch# show vlan brief
VLAN Name Status Ports
—- ——————————— ——— ——————————-

1 default active Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9,
Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14,
Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19,
Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24

2 VLAN0002 active Fa0/2, Fa0/3

3 VLAN0003 active Fa0/4

1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
```

For all Packet Tracer Examples and Files, you can check **Packet Tracer Labs** Page.

- Spanning Tree Configurations

RSTP Configuration on Packet Tracer

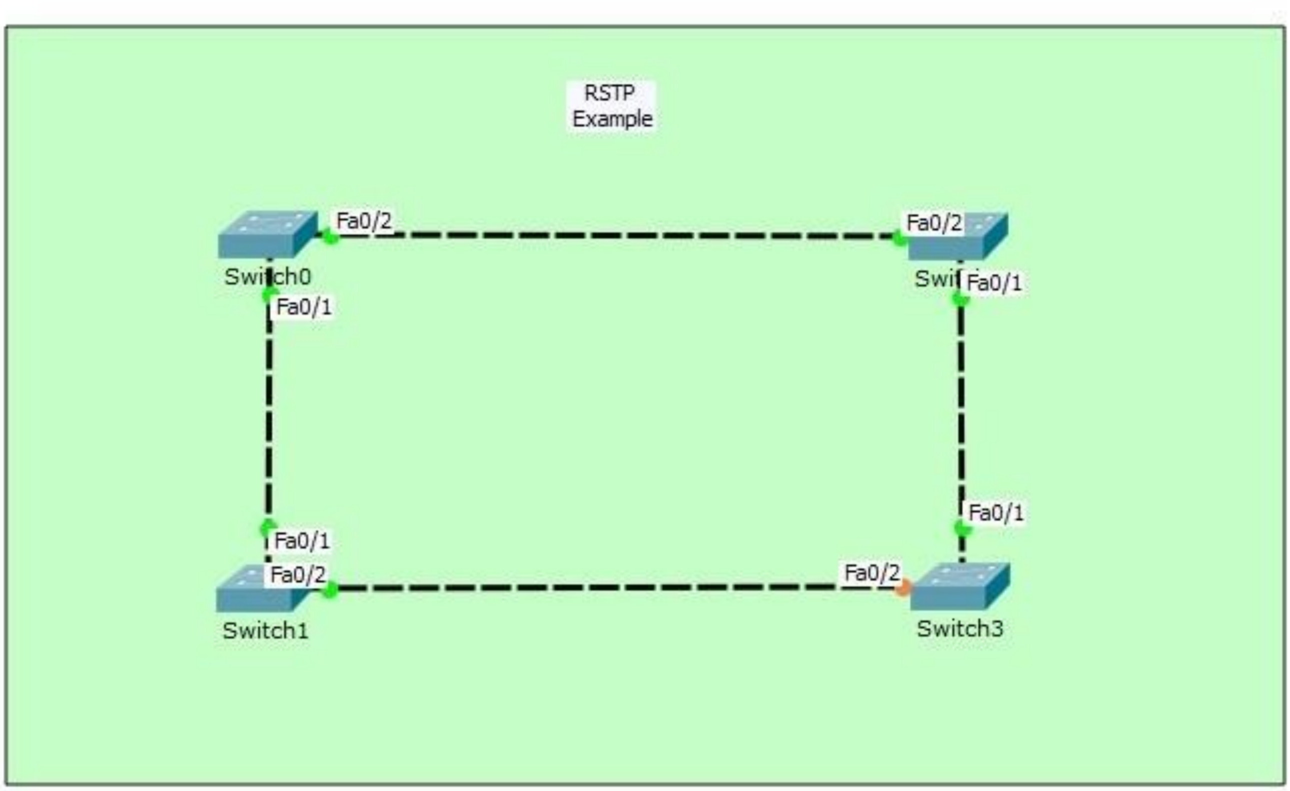


Table of Contents

Packet Tracer RSTP Configuration

As you know, **STP (Spanning Tree Protocol)** is the key protocol of Switching world. With **STP**, link redundancy is provided and switching loops are avoided.

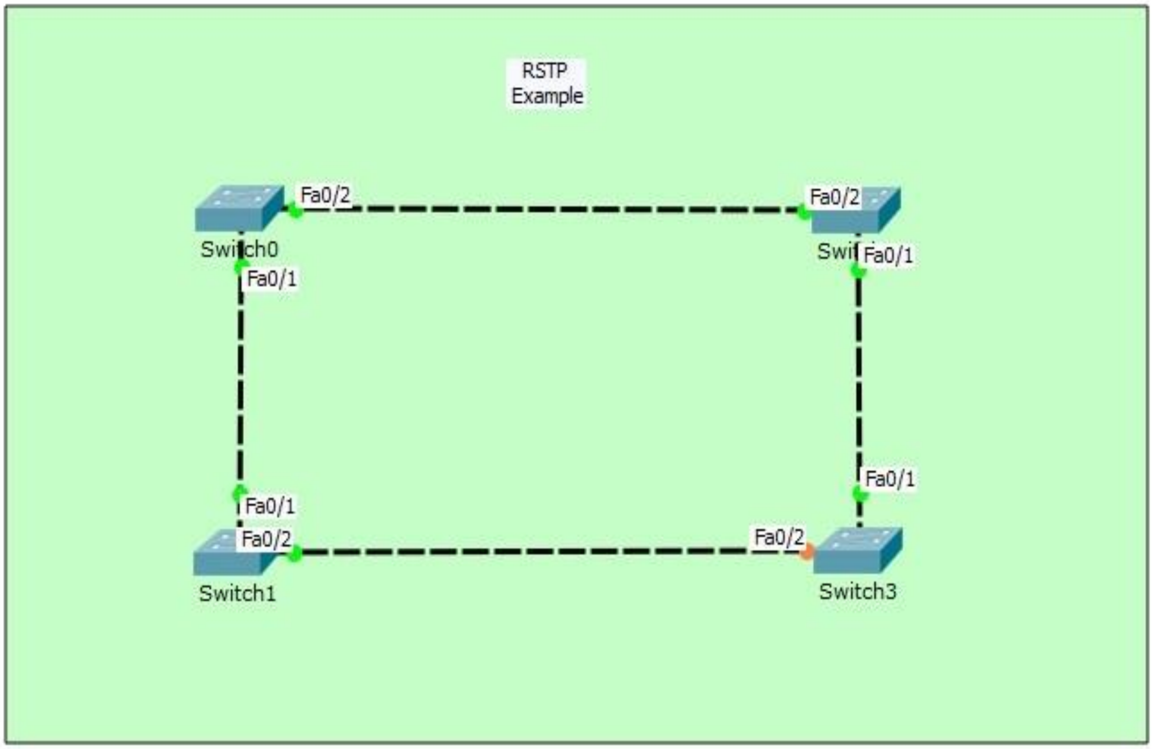
STP has different versions. One of the STP version is **RSTP (Rapid Spanning Tree Protocol)**. Like it name, RSTP (Rapid Spanning Tree Protocol) is the fastest converged version of STP.

In this example, we will configure **RSTP (Rapid Spanning Tree Protocol)** with Packet Tracer.

You can **DOWNLOAD** the **Cisco Packet Tracer** example with **.pkt** format **At the End of This Lesson**.

For all Packet Tracer Examples and Files, you can check **Packet Tracer Labs** Page.

For our **RSTP (Rapid Spanning Tree Protocol)** example, we will use the below switching topology.



RSTP Configuration Topology

STP (Spanning Tree Protocol) has four states. These STP states are; Blocking, Listenning, Learning and Forwarding. With RSTP (Rapid Spanning Tree Protocol), the Spanning Tree state Blocking and Listenning are bypassed. The RSTP states that starting with discarded, go through the learning and forwarding.

In **STP (Spanning Tree Protocol)**, **Blocking State** is **20 seconds**, **Listenning State** is **15 seconds** and **Learning State** is **15 seconds**. So, for STP, going through forwarding states needs **50 seconds**. This total time is **15 seconds** in **RSTP (Rapid Spanning Tree Protocol)**. Because RSTP, **bypasses** the Blocking and Listenning states.

RSTP Confgiuration

Let's start to configure **RSTP (Rapid Spanning Tree Protocol)** on Cisco Packet Tracer.

```
Switch0(config)# spanning-tree mode ?
pvst Per-Vlan spanning tree mode
rapid-pvst Per-Vlan rapid spanning tree mode
```

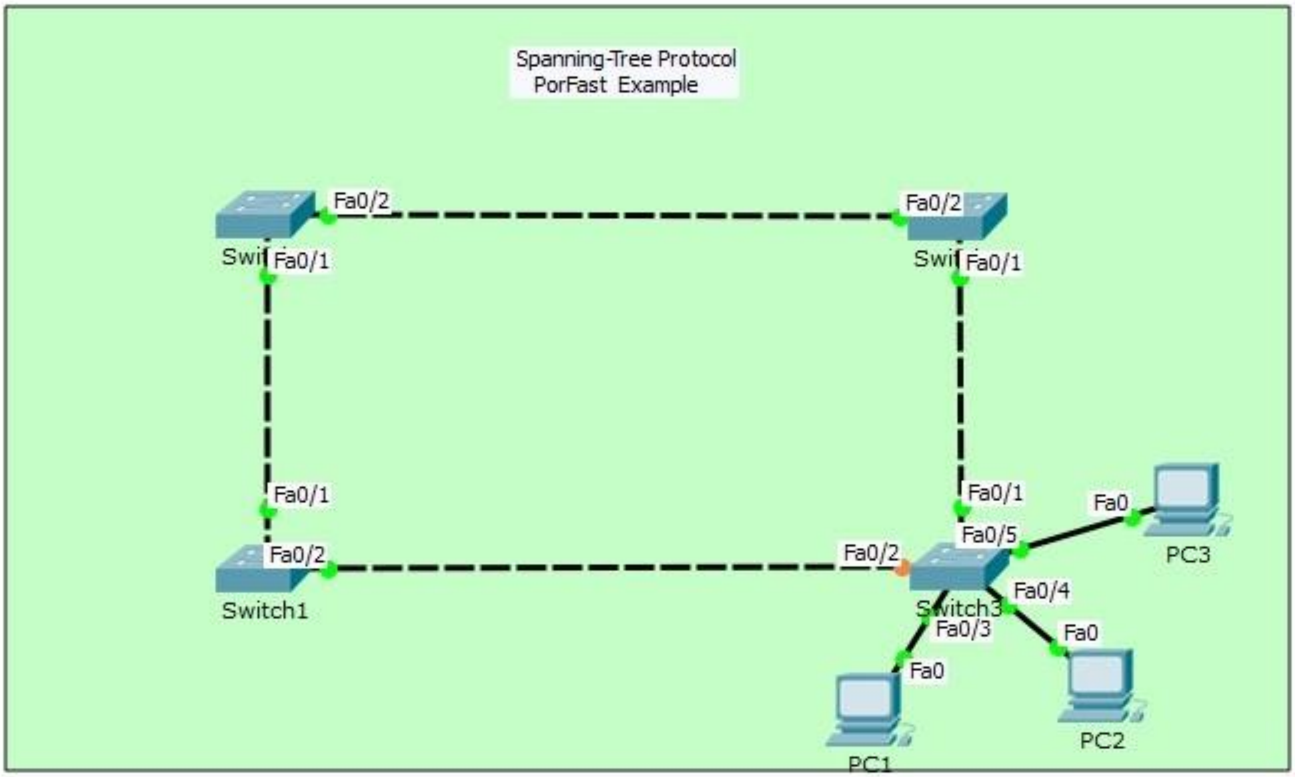
```
Switch0 (config)# spanning-tree mode rapid-pvst
```

```
Switch0 (config)# end

Switch0 # copy running-config startup-config
```

```
Switch1 (config)# spanning-tree mode rapid-pvst

Switch1 (config)# end

Switch1 # copy running-config startup-config
```

For all Packet Tracer Examples and Files, you can check **Packet Tracer Labs** Page

STP Portfast Configuration with Packet Tracer



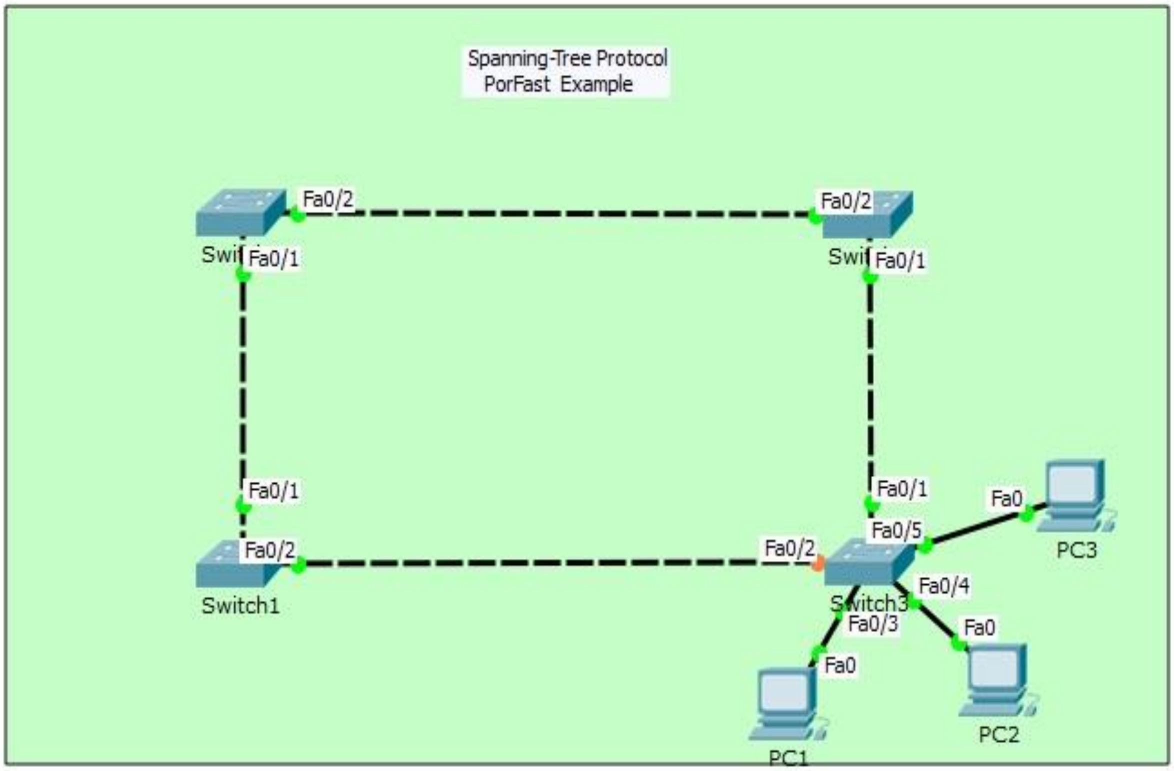
STP Portfast Configuration with Packet Tracer

In **STP (Spanning Tree Protocol)** there are Blocking State, Listenning State, Learning State and Forwarding State. With STP Portfast, Listenning State and Learning State bypassed.

The access ports of the switches that connect to hosts can configured with **STP Portfast**. And with STP Portfast, the host ports rapidly goes to Forwarding State. Here, host means, PCs, Laptops, IP Phone and other user equipments.

You can **DOWNLOAD** the **Cisco Packet Tracer** example with **.pkt** format **At the End of This Lesson**.

For our STP Portfast configuration, we will use the below topology on Packet Tracer.



STP Portfast Topology

Before STP Portfast configuration, let’s check the STP behaviour withot STP Portfast.

You can delete the link of PC2 and then reconnect it for checikng the behaviour of STP without STP Portfast. After this process, you will see STP states one by one.

```
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0006.2A11.24CC
             Cost        38
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000A.4139.1675
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg LSN 19        128.4    P2p
```

```
Fa0/5               Desg FWD 19        128.5    P2p
```

```
Switch# show spanning-tree

VLAN0001

  Spanning tree enabled protocol ieee

  Root ID    Priority    32769

             Address     0006.2A11.24CC

             Cost        38

             Port        1(FastEthernet0/1)

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


  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)

             Address     000A.4139.1675

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

             Aging Time  20


Interface           Role Sts Cost      Prio.Nbr Type

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

Fa0/1               Root FWD 19        128.1    P2p

Fa0/2               Altn BLK 19        128.2    P2p

Fa0/3               Desg FWD 19        128.3    P2p

Fa0/4               Desg LRN 19        128.4    P2p

Fa0/5               Desg FWD 19        128.5    P2p
```

```
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0006.2A11.24CC
             Cost        38
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000A.4139.1675
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- -----------------------------
---
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
```

STP (Spanning Tree Protocol) Example on Packet Tracer

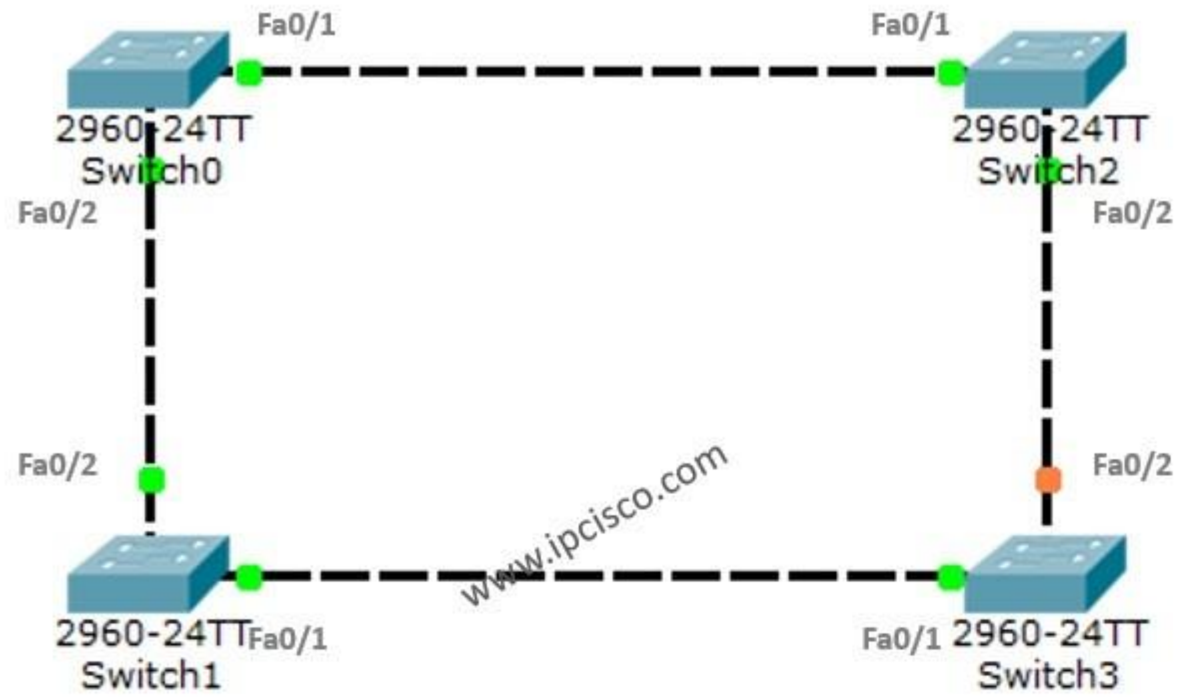


Table of Contents

□

Packet Tracer STP Configuration

In this post, instead of detaily talk about **STP (Spanning Tree Protocol)**, we will focus on a basic **Switching Loop** topology and how **STP** mechanism helps to avoid this Switching Loop.

You can **DOWNLOAD** the **Packet Tracer** example with **.pkt** format **HERE**.

Switching Loop is an unwanted problem in a network. Then, what is Switching Loop? **Switching Loop** is the situation, in which there are two **layer 2** path between two layer 2 endpoint(switch, brigde). Switches creates broadcast storms from every port and switch rebroadcast again and again. Because of teh fact that there is no **TTL(time to live)** mechanism on layer 2, this continues forever.

To avoid this unwanted **Switching Loops**, there are some mechanisms. One of the most common name of this mechanisms is **STP(Spanning Tree Protocol)**.

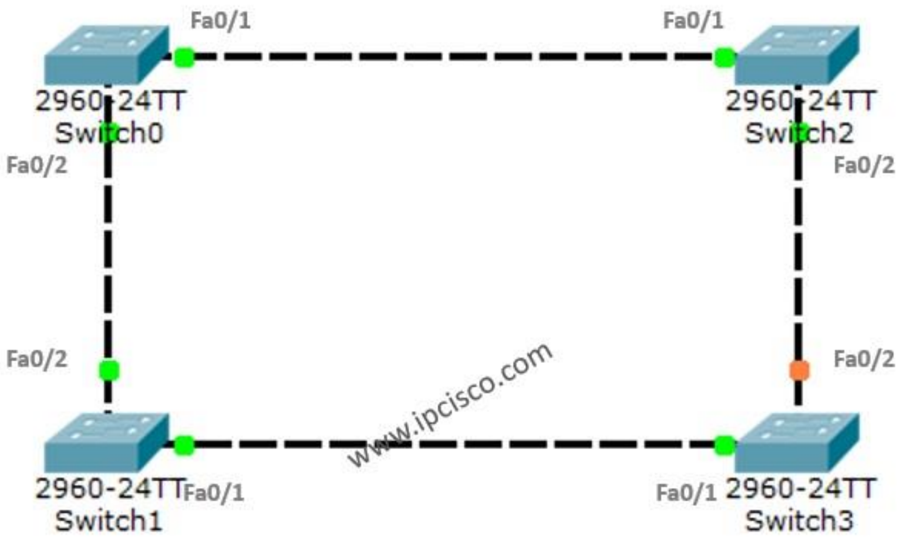
Acording to this protocol, in the switching topology, a **Root Bridge** is selected. And then the connected port of the switches are classified. The port classification and their meaning are like below:

– **Root Port :** The port to the Root Bridge
– **Designated Port :** The other port thatis not Root Port
– **Non Designated (Blocked) Port :** In a segment, other port than the Designated Port

The selection process is done orderly. First **Root Bridge** is selected, secondly **Root Ports** on all the switches, then **Designated Ports** are selected, and lastly the remainning ports become **Non-Designated Port**, meaning **Blocking Port**.

STP Example on Packet Tracer

For STP example with PAcket Tracer, we will use the below switch topology.



STP Example Topology

As you can see after connecting the switches together in the Loop position, one of the ports become blocking. Because by default STP is enabled and it is avoiding us any Switching Loop. To understand more detailly let’s check the show screenshots.

<u>On Switch0</u>

```
Switch0#show spanning-tree

VLAN0001

  Spanning tree enabled protocol ieee

  Root ID    Priority    32769
```

```
             Address     0001.C90E.EDC0

             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     0001.C90E.EDC0

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

             Aging Time  20



Interface        Role Sts Cost      Prio.Nbr Type

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

Fa0/1            Desg FWD 19        128.1    P2p

Fa0/2            Desg FWD 19        128.2    P2p
```

```
Switch0#show spanning-tree active

VLAN0001

  Spanning tree enabled protocol ieee

  Root ID    Priority    32769

             Address     0001.C90E.EDC0

             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     0001.C90E.EDC0
```

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

                 Aging Time  20



Interface         Role Sts Cost      Prio.Nbr Type

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

Fa0/1            Desg FWD 19        128.1    P2p

Fa0/2            Desg FWD 19        128.2    P2p
```

As we can see above, the addresses are for the Root and the Bridge part. So, Switch0 is selected as **Root Bridge**. The Root Bridge is selected according to the Bridge ID, The Bridge ID is the MAC address of the Switch. So, the lower one is selected as Root Bridge. This is Switch0.

The two port of Switch0 are normally Designated Port. Because all the ports on Root Bridge is always choosen as **Designated Port**.

Both of these ports are in Forwarding State, this means that they are ready to send the traffic. As a recall, as you know there are four states of an STP port. These are:

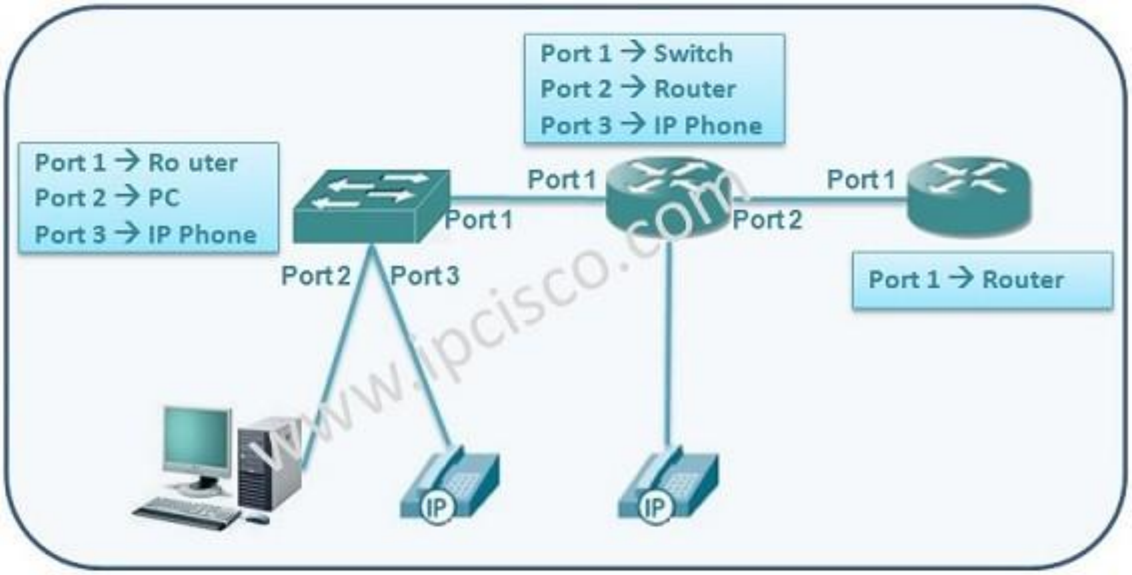
– **Blocking** (20 seconds)
– **Listening** (15 second)
– **Learning** (15 second)
– **Forwarding**

You can also use the following commands to check the spanning-tree information.

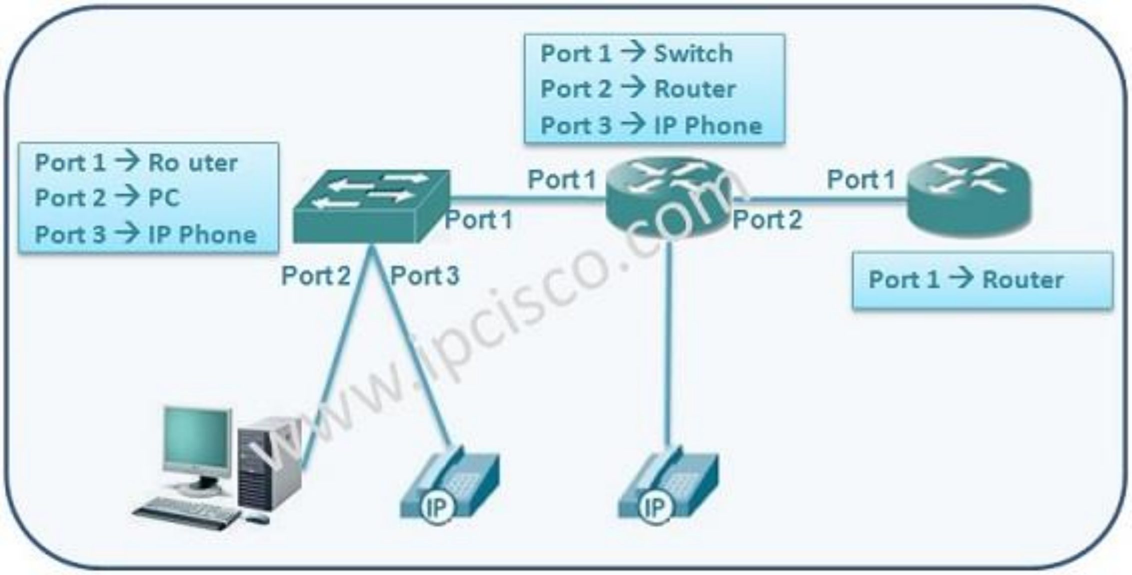
```
Switch0#show spanning-tree interface fa0/1

Vlan              Role Sts Cost      Prio.Nbr Type

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

VLAN0001          Desg FWD 19        128.1     P2p
```

- Neighbor Discovery Configurations

LLDP Configuration on Cisco



In this configuration lesson, we will focus on **Cisco LLDP Configuration**. To understand **LLDP** better, let's check the configuration of **LLDP on the Cisco IOS**. The most important commands related with **LLDP configuration** is showed below.



LLDP Configuration Topology

LLDP is **disabled** by **default**. To enable LLDP on the device, use **"lldp run"** on the global configuration mode. Again, **"no lldp run"** is used to disable lldp on that device.

```
RouterA(config)# lldp run

RouterA(config)# no lldp run
```

To specify the TLVs on the device, use **“lldp med-tlv-select tlv”** command. Here, tlv can be inventory-management, power-management, network-policy, location etc.

```
RouterA(config)# lldp med-tlv-select tlv
```

Like other protocols, **LLDP** (**Link Layer Discovery Protocol**) has also timers. The default values of **reinit** is **2**, **timer** is **30** and **holdtime** is **120**. **Reinit** is the initialization delay. **Timer** is the update time. And **holdtime** is the time that it waits without an update and then discards the entry.

LLDP timers can be configured like below:

```
RouterA(config)# lldp reinit 2
RouterA(config)# lldp timer 30
RouterA(config)# lldp holdtime 120
```

You can disable or enable receiving and transmitting the LLDP packets on a specific interface. To do this, use **“lldp transmit”** and **“lldp**

receive" commands under that interface. To disable, you can also use the no versions of this commands.

```
RouterA(config)# interface fastethernet 0/1
RouterA(config-if)# lldp transmit
RouterA(config-if)# lldp receive
```

```
RouterA(config)# interface fastethernet 0/2
RouterA(config-if)# no lldp transmit
RouterA(config-if)# no lldp receive
```

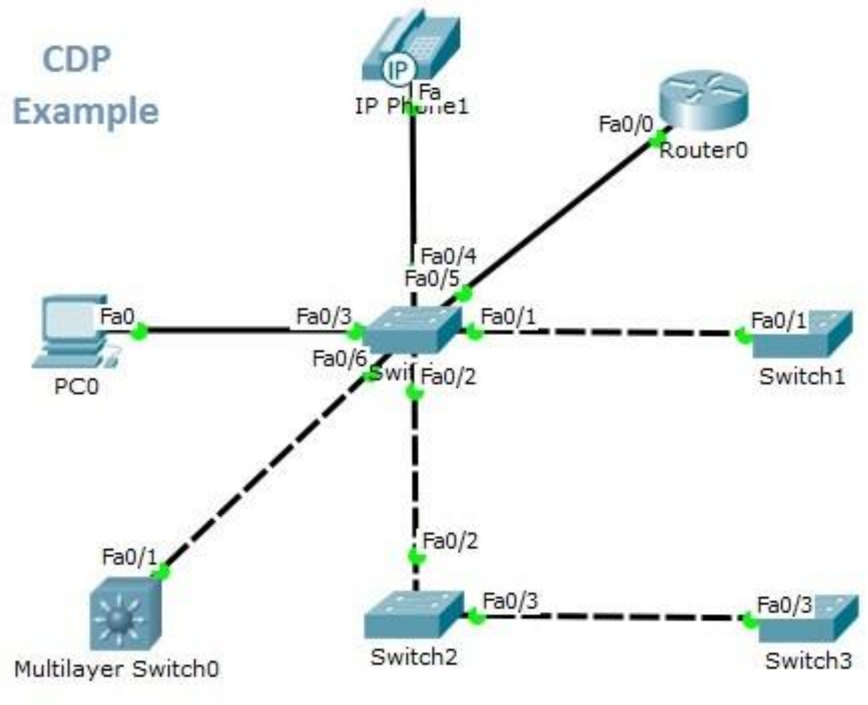
To see the lldp related information on the device, use the below show commands:

```
RouterA# show lldp
RouterA# show lldp traffic
RouterA# show lldp entry entry
RouterA# show lldp interface interface-id
RouterA# show lldp neighbors interface-id
RouterA# show lldp errors
```

To reset the lldp counters to zero, use **"clear lldp counters"** command.

```
RouterA# clear lldp counters
```

CDP Configuration with Packet Tracer



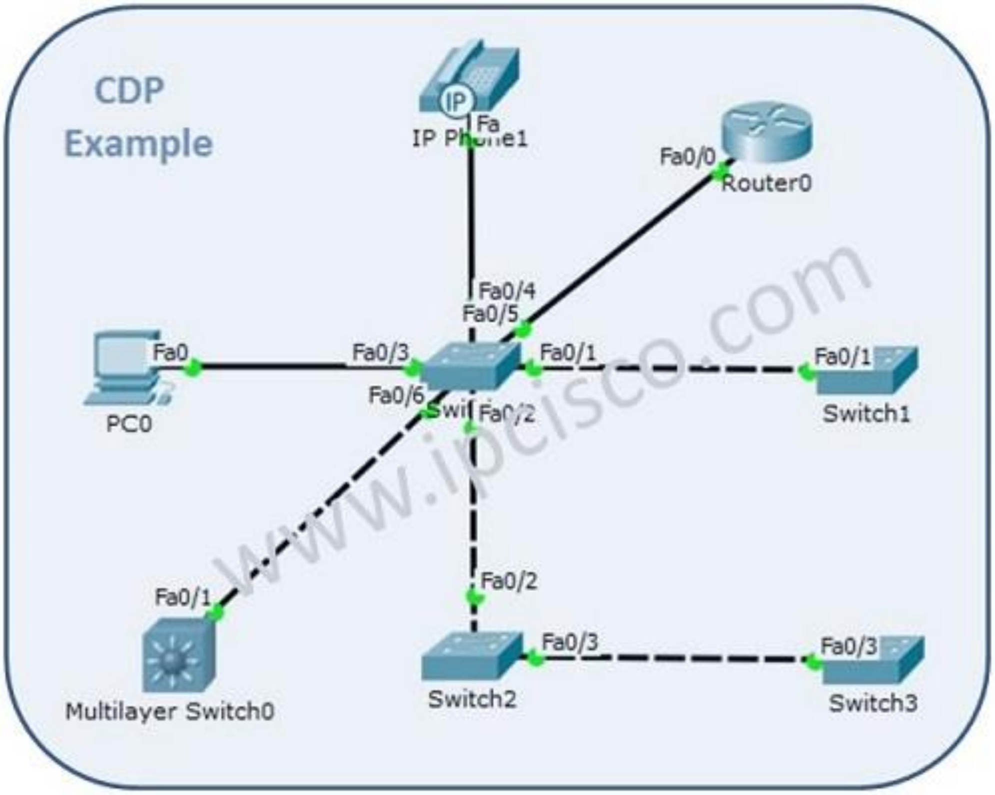
Packet Tracer CDP Configuration

As we have talked about in the previous lesson, CDP is a Cisco proprietary **Neighbor Discovery Protocol**. In this article, we will discuss **how to configure CDP** in Cisco IOS, we will learn **CDP Cisco Configuration**. LLDP is a standard neighbour discovery protocol. In another lesson we will also **configure LLDP**.

You can **DOWNLOAD** the **Packet Tracer** example with **.pkt** format **HERE.**

For all Packet Tracer Examples and Files, you can check **Packet Tracer Labs** Page.

For our example, the below topology is used.



CDP Configuration Topology

Above, there is a L2 swith, a L3 switch, a router, an IP Phone and a PC are connected to the central switch.

We will not talk about the configuration of the central switch, but we will talk about the general **CDP configuration commands.**

To **enable CDP globally**, use **"cdp run"** on the router configuration mode.

```
Switch(config)# cdp run
```

To **enable CDP** on a specific interface, use **"cdp enable"** command on the interface configuration mode. By **default** CDP is already **enabled**. You can also disable CDP by using **"no cdp enable"** command.

```
Switch(config-if)# cdp enable
Switch(config-if)# no cdp enable
```

To configure cdp **Hello** time and **Hold** time, you can use the below commands. Time is mentioned as seconds.

```
Switch(config)# cdp timer 50
Switch(config)# cdp holdtime 100
```

To **clear** the CDP table, use the **“clear cdp table”** command.

```
Switch# clear cdp table
```

To **verify CDP**, you can use general CDP verification commands below:

```
Switch# show cdp
Switch# show cdp interface
Switch# show cdp neighbors
Switch# show cdp entry
Switch# show cdp traffic
```

In our topology, for the central switch, **“show cdp neighbours”** and **“show cdp interface”** command outputs are showed below.

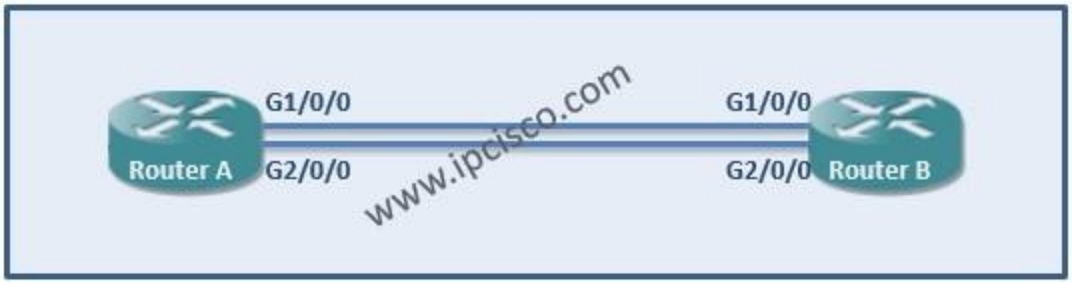
```
Switch>show cdp neighbors
```

```
Capability Codes: R – Router, T – Trans Bridge, B – Source Route Bridge
S – Switch, H – Host, I – IGMP, r – Repeater, P – Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
IP Phone Fas 0/4 124 H P 7960
Switch Fas 0/6 124 3560 Fas 0/1
Switch Fas 0/2 124 S 2960 Fas 0/2
Router Fas 0/5 124 R C2800 Fas 0/0
Switch Fas 0/1 124 S 2950 Fas 0/1
```

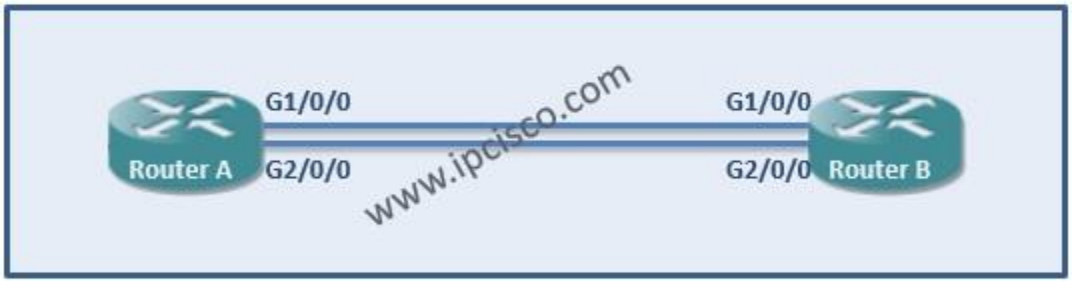
For all Packet Tracer Examples and Files, you can check **Packet Tracer Labs** Page.

- EtherChannel Configurations

LACP Configuration on Cisco Devices



We have learned **LACP** and **Link Aggregation** before detailly and in this article we will focus **LACP Cisco Configuration**. We will make a link aggregation protocol with two ports in one bundle. You can use more port up to **8 ports** in Cisco devices.



Link Aggregation on Cisco Devices

In our **LACP Cisco Configuration** example, we will use the **G1/0/0** and the **G2/0/0** ports to configure link aggregation. The basic configuration steps are below.

On RouterA

```
RouterA> enable
RouterA# configure terminal
RouterA (config)# interface port-channel 1
RouterA (config-if)# lacp max-bundle 2
RouterA (config-if)# ip address 192.168.0.1 255.255.255.0
RouterA (config-if)# interface g1/0/0
RouterA (config-if)# no ip address
RouterA (config-if)# channel-group 1 mode active
RouterA (config-if)# exit
RouterA (config)# interface g2/0/0
RouterA (config-if)# no ip address
RouterA (config-if)# channel-group 1 mode active
RouterA (config-if)# end
```

- First Hop Redundancy Configurations

VRRP Configuration on Cisco

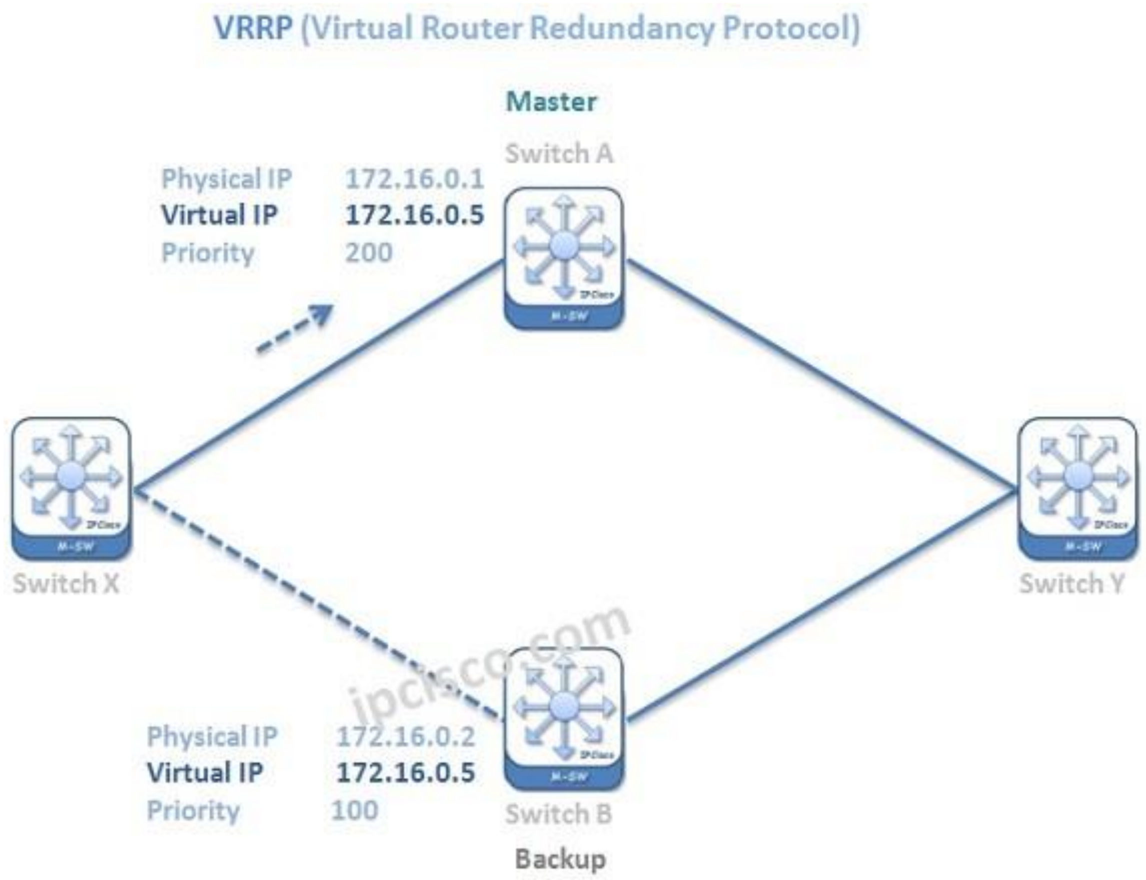


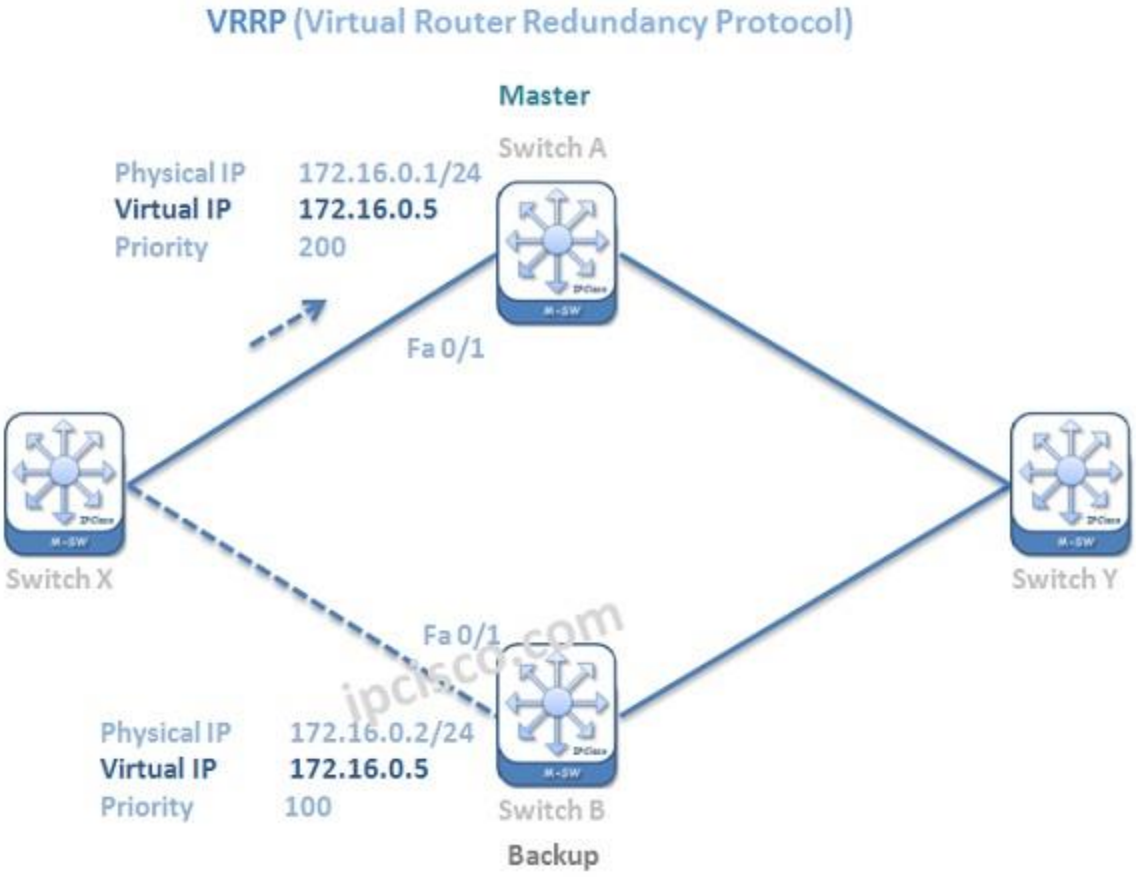
Table of Contents

□

How to Configure VRRP on Cisco Switches?

In this **VRRP example**Cisco Configuration Example, we will work on **Cisco IOS** and configure **VRRP (Virtual Router Redundancy Protocol)** on **Cisco Routers. Configuring VRRP Protocol** is like configuring Cisco Proprietary protocol HSRP. There are only small command differences.

For our **VRRP Cisco Configuration Example**, we will use the below topology:



Now, let’s configure **VRRP Protocol** on **Cisco Routers** and learn VRRP better.

You can also check **Cisco HSRP Configuration Example**

IP Address Configuration

The first step of our VRRP Cisco Configuration is the IP address configuration on interfaces.

```
Switch A (config)# int fa0/1
Switch A (config-if)# no switchport
Switch A (config-if)# ip address 172.16.0.1 255.255.255.0
Switch A (config-if)# no shutdown
```

```
Switch B (config)# int fa0/1
Switch B (config-if)# no switchport
Switch B (config-if)# ip address 172.16.0.2 255.255.255.0
Switch B (config-if)# no shutdown
```

VRRP Process Creation with Virtual IP

VRRP process is created with the **VRRP Group ID** and the **Virtual IP Address**.Here, our **VRRP Group ID** is 1 and our **Virtual IP** address is 172.16.0.5.

```
Switch A (config-if)# vrrp 1 ip 172.16.0.5

Switch B (config-if)# vrrp 1 ip 172.16.0.5
```

VRRP Group Description

Like all descriptions, in **VRRP**, we can use description to give our VRRP group a memorable description.

```
Switch A (config-if)# vrrp 1 description Our-vrrp

Switch B (config-if)# vrrp 1 description Our-vrrp
```

VRRP Priority

For **Master/Backup** selection, **VRRP** priorities are configured. To manuplate VRRP selection and determine a Master manually, **VRRP Priority** values are important. The default one is 100 and the highest one is elected as VRRP Master.

```
Switch A (config-if)# vrrp 1 priority 200

Switch B (config-if)# vrrp 1 priority 100
```

It is not required to configure **VRRP Priority** for switch B, because it is the default value. Here, we write this command to show you only.

VRRP Authentication

To configure **VRRP authentication,** we will use the below command on switches. Our password is CISCO.

GLBP Configuration on Cisco

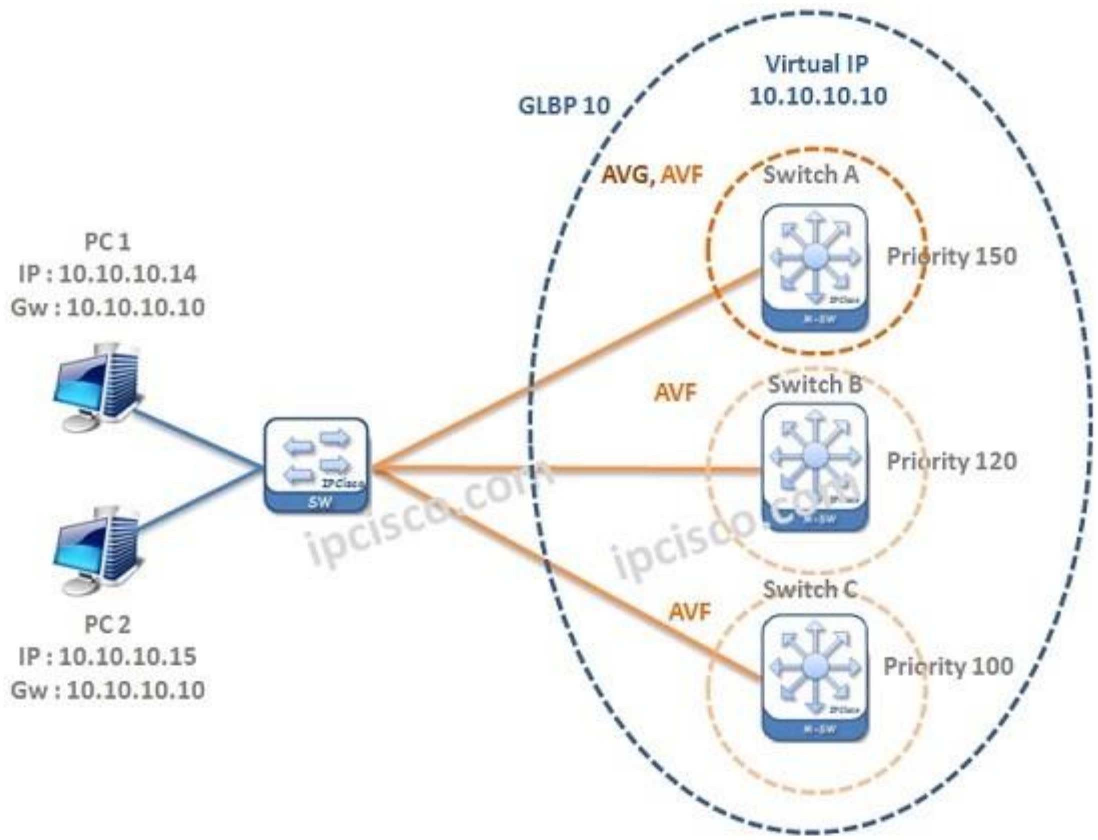


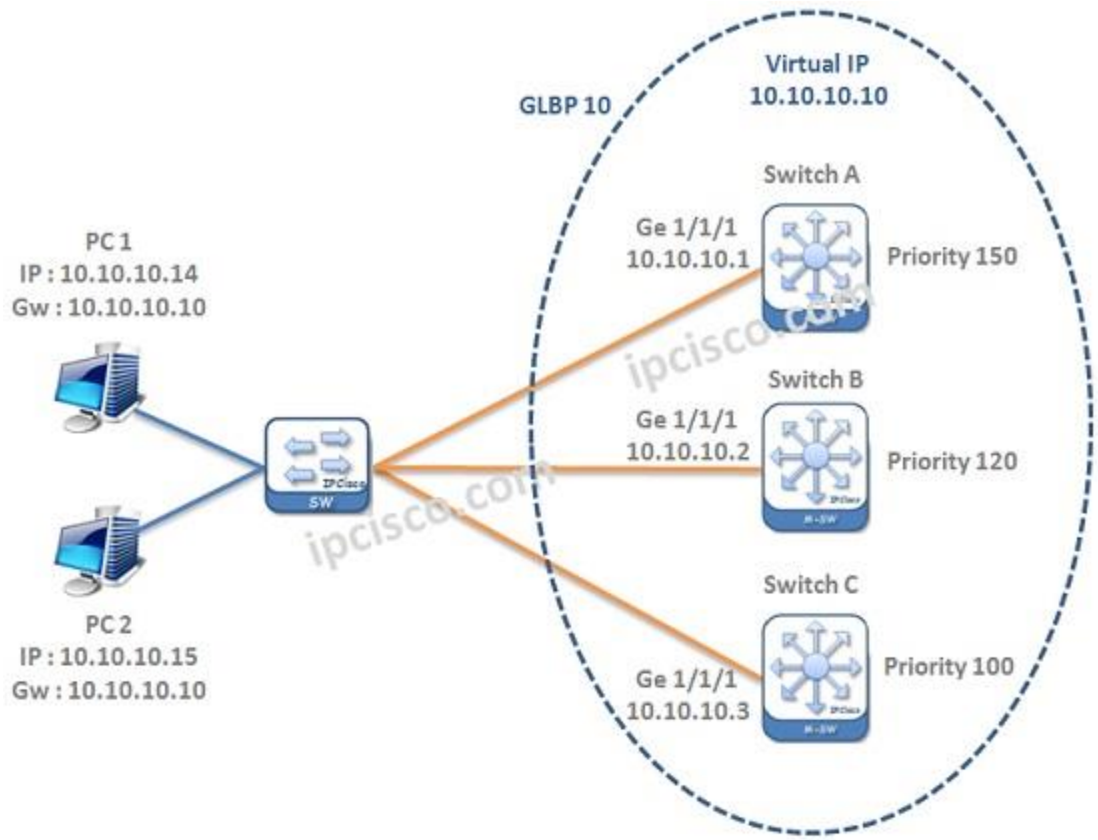
Table of Contents

□

GLBP Cisco Configuration Example

GLBP is a **Cisco Proprietary** Firsth Hop Redundancy Protocol. In this lesson, we will configure GLBP on Cisco devices with a **GLBP Example Topology.**

For our **GLBP Example**, we will use the below topology.



For **GLBP Cisco Configuration**, there are some steps. These steps are given below one by one:

1. Interface Configurations
2. GLBP Group Configuration with Group ID and Virtaul IP
3. GLBP Priority Configuration
4. Setting GLBP Preeption
5. Setting GLBP Load Balancing Option
6. Saving the configuration
7. GLBP Verification

Now, let’s start and learn How to Do **GLBP Cisco Configuration** practically.

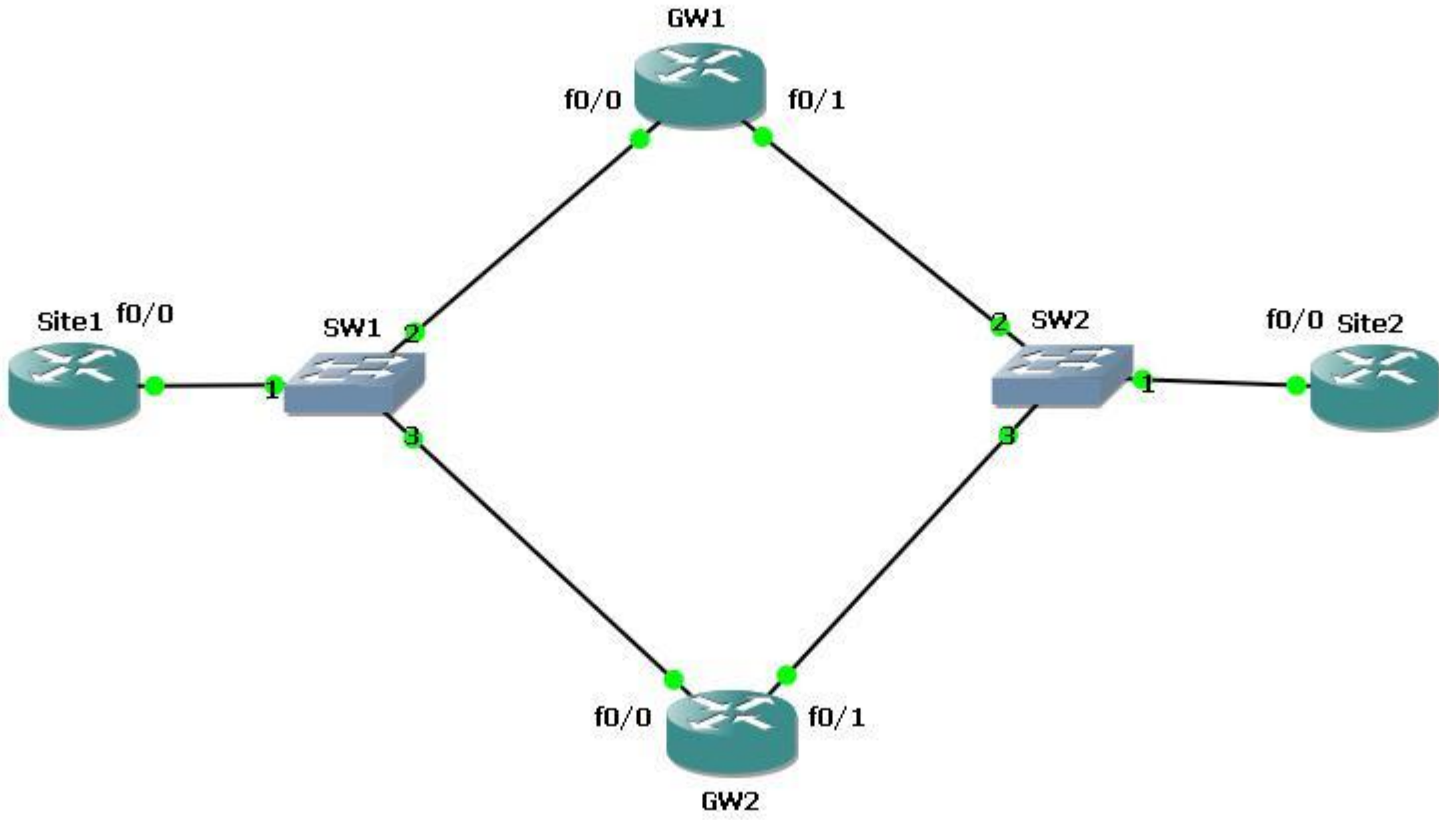
Interface Configurations

Interface configuration is the basic IP configurations of switch ports. Here, our swicthes are Layer 3 switch.

```
Switch A# configure

Switch A(config)# interface Gigabitethernet 1/1/1
Switch A(config-if)# ip address 10.10.10.1 255.255.255.0

Switch A(config-if)# no shutdown
```

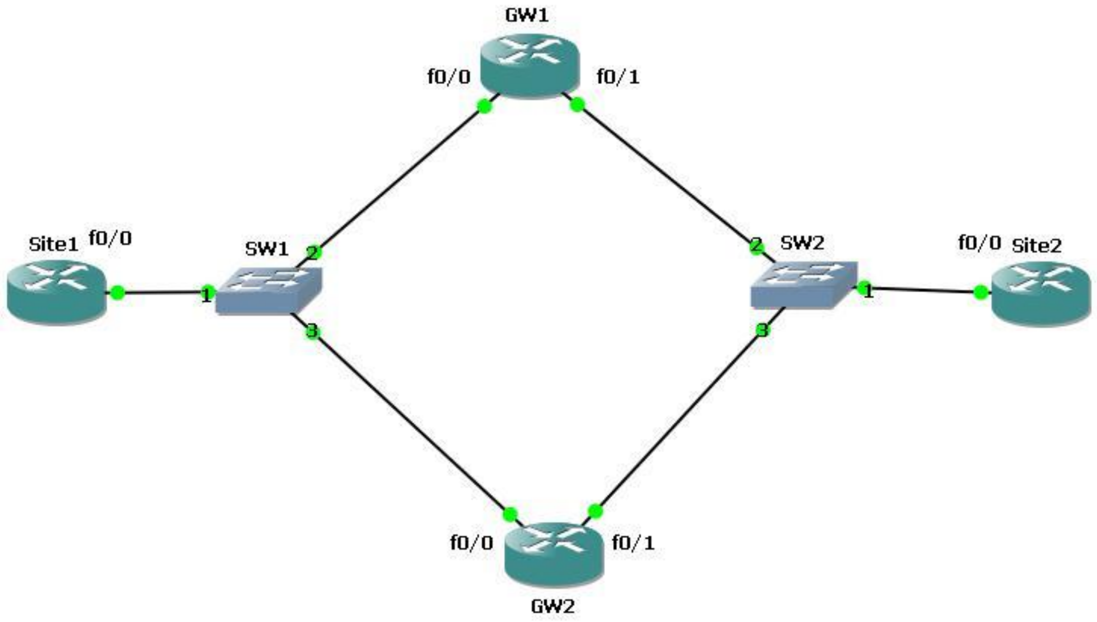
```
Switch B# configure

Switch B(config)# interface Gigabitethernet 1/1/1

Switch B(config-if)# ip address 10.10.10.2 255.255.255.0

Switch B(config-if)# no shutdown
```

HSRP Configuration on Cisco IOS



HSRP Configuration Example on Cisco Routers

In this section we will do an **HSRP Configuration** to understand the issue better. To do this wewill use the below topology. At the end of this article, you will find the GNS3 configuration lab of this lesson.



HSRP Example Topology

Before the **HSRP (Hot Standby Router Protocol)** configuration, we must prepare our topology. We will change the router names and we will assigned the ip addresses of the router interfaces.

For the left side of the topology, we will use 10.10.10.0 network and for the right side, we will use 10.10.20.0 network. All the interfaces connected to the layer 2 swicth will be assigned with the ip addresses related to its connected port. For example the fa0/0 interface of the Site1 router will be assigned the ip address 10.10.10.1 and the GW1's and GW2's fa0/0 ip addresses will be 10.10.10.2 and 10.10.10.3 orderly.

After interface configuration, we will configure a static route on each Site1 and Site2. In this static route we will use two virtual ip addresses that we will explain in this article. This virtual addresses will be 10.10.10.10 and 10.10.20.20.

```
Site1(config)# ip route 10.10.20.0 255.255.255.0 10.10.10.10
```

```
Site2(config)# ip route 10.10.10.0 255.255.255.0 10.10.20.20
```

Now our configuration is ready to **HSRP configuration**. Let’s start on one side(left) on GW1 and GW2 and after that we will configure a second HSRP configuration for the other side(right).

GW1

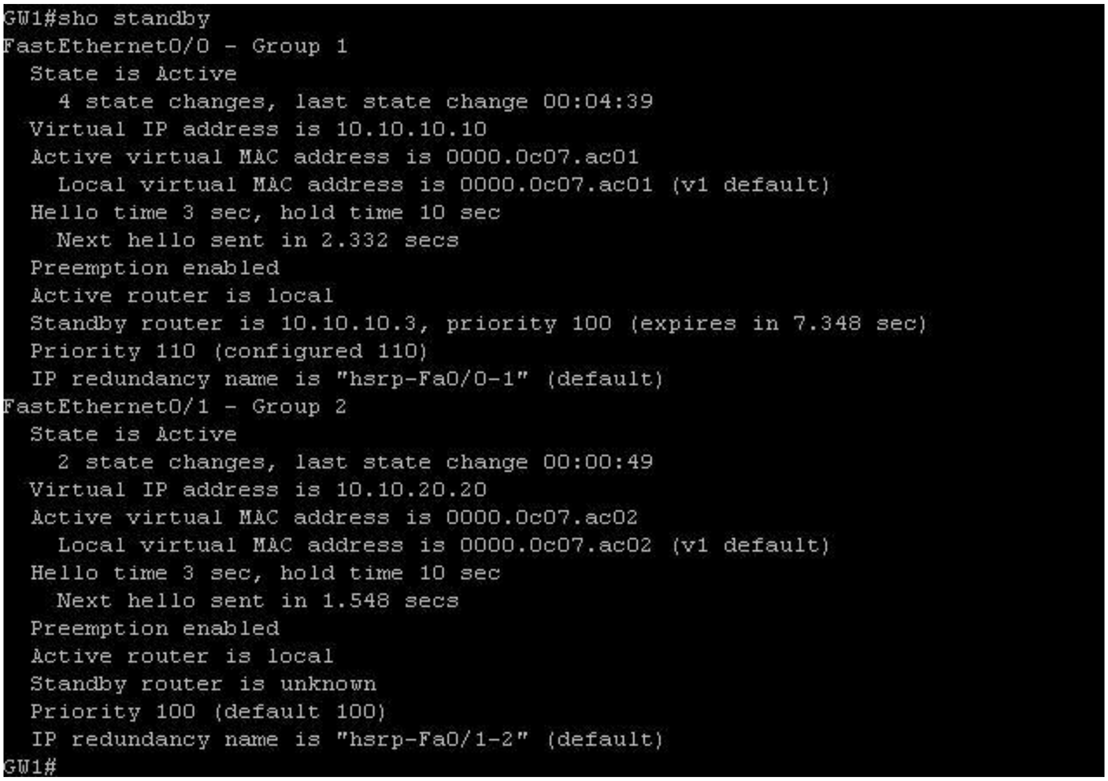
```
GW1(config)# interface fastethernet 0/0

GW1(config-if)# standby 1 ip 10.10.10.10

GW1(config-if)# standby 1 preempt

GW1(config-if)# standby 1 priority 110

GW1(config-if)# standby 1 track fa0/1

GW1(config-if)# exit

GW1(config)# interface fastethernet 0/1

GW1(config-if)# standby 1 ip 10.10.20.20

GW1(config-if)# standby 1 preempt

GW1(config-if)# exitGW2
```

GW2

```
GW2(config)# interface fastethernet 0/0

GW2(config-if)# standby 1 ip 10.10.10.10

GW2(config-if)# standby 1 preempt

GW2(config-if)# standby 1 priority 100

GW2(config-if)# standby 1 track fa0/1

GW2(config-if)# exit

GW2(config)# interface fastethernet 0/1
```

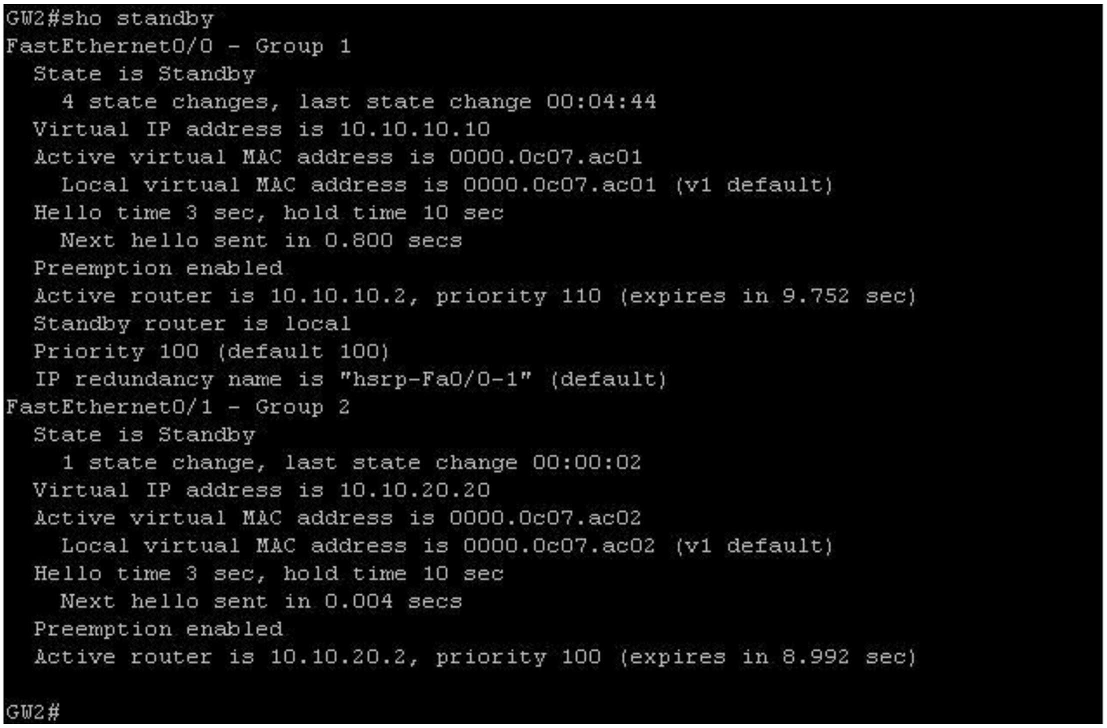
```
GW2(config-if)# standby 1 ip 10.10.20.20

GW2(config-if)# standby 1 preempt

GW2(config-if)# exit
```

You do not need to do this configuration for both sides, but in this configuration, we do it for both sites. After this you can check the configuration with **“show standby”** command on GW1 and GW2. As you see below, for both redundancy configuration GW1 is the active router and the GW2 is the standby.



```
GW1#sho standby
FastEthernet0/0 - Group 1
  State is Active
    4 state changes, last state change 00:04:39
  Virtual IP address is 10.10.10.10
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.332 secs
  Preemption enabled
  Active router is local
  Standby router is 10.10.10.3, priority 100 (expires in 7.348 sec)
  Priority 110 (configured 110)
  IP redundancy name is "hsrp-Fa0/0-1" (default)
FastEthernet0/1 - Group 2
  State is Active
    2 state changes, last state change 00:00:49
  Virtual IP address is 10.10.20.20
  Active virtual MAC address is 0000.0c07.ac02
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.548 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Fa0/1-2" (default)
GW1#
```

Show Standby On Active Router (HSRP)



```
GW2#sho standby
FastEthernet0/0 - Group 1
  State is Standby
    4 state changes, last state change 00:04:44
  Virtual IP address is 10.10.10.10
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.800 secs
  Preemption enabled
  Active router is 10.10.10.2, priority 110 (expires in 9.752 sec)
  Standby router is local
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Fa0/0-1" (default)
FastEthernet0/1 - Group 2
  State is Standby
    1 state change, last state change 00:00:02
  Virtual IP address is 10.10.20.20
  Active virtual MAC address is 0000.0c07.ac02
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.004 secs
  Preemption enabled
  Active router is 10.10.20.2, priority 100 (expires in 8.992 sec)

GW2#
```

Show Standby On Standby Router (HSRP)