LAB 3 – VLAN : VTP : DTP : STP

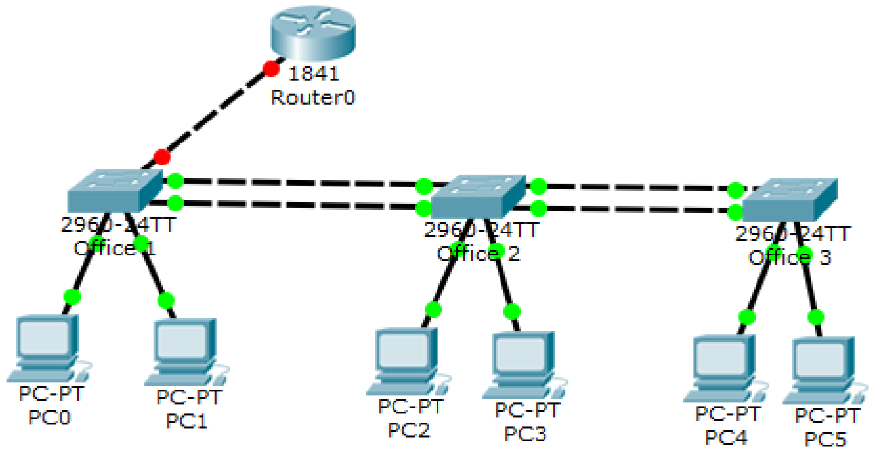
This lab explains how to use Packet Tracer for the practice of VLAN Configuration, VTP Server and Client configuration, DTP configuration, STP Configuration, Intra VLAN communication and Router on Stick Configuration.

Section A

Scenario and Initial Setup

A company has three offices which are all connected via layer 2 links. For redundancy purpose, each office has one more layer 2 link. The company has two departments: Sales & Management. In each office, we have one PC from each department. The Ethernet port of a router is used for inter VLAN communication.

Create a topology in packet tracer, as shown below:



PCs Configuration

Device	IP Address	Subnet Mask	Gateway	VLAN	Connected With
PC0	10.0.0.2	255.0.0.0	10.0.0.1	VLAN 10	Office 1 Switch on F0/1
PC1	20.0.0.2	255.0.0.0	20.0.0.1	VLAN 20	Office 1 Switch on F0/2
PC2	10.0.0.3	255.0.0.0	10.0.0.1	VLAN 10	Office 2 Switch on F0/1
PC3	20.0.0.3	255.0.0.0	20.0.0.1	VLAN 20	Office 2 Switch on F0/2
PC4	10.0.0.4	255.0.0.0	10.0.0.1	VLAN 10	Office 3 Switch on F0/1
PC5	20.0.0.4	255.0.0.0	20.0.0.1	VLAN 20	Office 3 Switch on F0/2

Office 1 Switch Configuration

Port	Connected To	VLAN	Link	Status
F0/1	With PC0	VLAN 10	Access	OK
F0/2	With PC1	VLAN 20	Access	OK
Gig0/1	With Router	VLAN 10,20	Trunk	OK
Gig0/2	With Switch2	VLAN 10,20	Trunk	OK
F0/24	With Switch2	VLAN 10,20	Trunk	STP - Blocked

Office 2 Switch Configuration

Port	Connected To	VLAN	Link	Status
F0/1	With PC0	VLAN 10	Access	OK
F0/2	With PC1	VLAN 20	Access	OK
Gig 0/2	With Switch1	VLAN 10,20	Trunk	OK
Gig 0/1	With Switch3	VLAN 10,20	Trunk	OK
F0/24	With Switch1	VLAN 10,20	Trunk	STP - Blocked
F0/23	With Switch3	VLAN 10,20	Trunk	STP - Blocked

Office 3 Switch Configuration

Port	Connected To	VLAN	Link	Status
F0/1	With PC0	VLAN 10	Access	OK
F0/2	With PC1	VLAN 20	Access	OK
Gig 0/1	With Switch2	VLAN 10,20	Trunk	OK
F0/24	With Switch1	VLAN 10,20	Trunk	STP - Blocked

Router Configuration

Port	Connected To	VLAN	Link	Status
Fa0/0	Office 1 Switch Gig 0/1	VLAN 10, 20	Trunk	Ok

VLAN Configuration

VLAN Number	VLAN Name	Gateway IP	PCs
10	Sales	10.0.0.1	PC0,PC2,PC4
20	Management	20.0.0.1	PC1,PC3,PC5

Assign IP Addresses to PCs

Assigning IP addresses is bit easy task in packet tracer. Just double Click on **PC-PT** and Click **Desktop** menu item and Click **IP Configuration** Select **Static** from radio option and fill IP address, subnet mask and default gateway IP in given input boxes. Use PC Configuration table above to assign correct IP address.

Section B

Configuring VTP Server and Client in Switch

This section explains basic concepts of VTP Protocol, VTP Domain, VTP Messages and VTP modes (Server mode, Transparent mode and Client mode) and how to configure VTP Server and VTP Clients.

VLAN Trunk Protocol (VTP) is a Cisco proprietary protocol used to share VLAN configuration across the network. Cisco created this protocol to share and synchronize their VLAN information throughout the network. Main goal of VTP is to manage all configured VLANs across the network.

In our scenario, we have only **3** switches. We can easily add or remove VLAN manually on all three switches. However this process could be more tedious and difficult if we have **50** switches. In a large network, we might make a mistake in VLAN configuration. We might forget to add a VLAN in one of the switch, or we may assign a wrong VLAN number. We may forget to remove a VLAN on one of the switch, whilst removing VLANs.

VTP is a life-saver protocol in this situation. With VTP, we can add or remove VLANs on one switch and this switch will propagate VLAN information to all other switches in network.

VTP Messages

VTP share VLANs information via VTP messages. VTP messages can only be propagate through the **trunk** connections. So we need to set up trunk connection between switches. VTP messages are propagated as layer 2 **multicast** frames.

VTP Domain

VTP domain is a group of switches that share same VLAN information. A switch can have a single domain. VTP messages include domain name. Switch only update VLAN information if it receive VTP message from same domain.

VTP can be configured in three different modes.

1. Server
2. Transparent
3. Client

VTP Server Mode

VTP Server can add, modify, and delete VLANs. It will propagate a VTP message containing all the changes from all of its trunk ports. If server receives a VTP message, it will incorporate the change and forward the message from all remaining trunk ports.

VTP Transparent Mode

VTP Transparent switch can also make change in VLANs but it will not propagate these changes to other switches. If transparent switch receives a VTP message, it will not incorporate the change and forward the message as it receives, from all remaining trunk ports.

VTP Client Mode

VTP client switch cannot change the VLAN configurations itself. It can only update its VLAN configuration through the VTP messages that it receive from VTP server. When it receives a VTP message, it incorporates the change and then forwards it to the remaining trunk ports.

Configuring VTP Server

We will configure **Office 1 Switch** as VTP Server. Double click on **Office 1 Switch** and Click **CLI** menu item and press **Enter key** to start CLI session.

By default all switches work as VTP server so we only need few commands to configure it. In the following commands we will:

- Set hostname to **`S1`**

- Set domain name to **`pditn18b`**
- Set password to **`test1234`**. (Password is case-sensitive)

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname S1
S1(config)# vtp mode server
Device mode already VTP SERVER.
S1(config)# vtp domain pditn18b
Changing VTP domain name from NULL to pditn18b
S1(config)# vtp password test1234
Setting device VLAN database password to test1234
```

Configure VTP Client

We will configure Office 2 Switch and Office 3 Switch as VTP client switch. Access **CLI** prompt of **Office 2 Switch** and execute following commands

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname S2
S2(config)# vtp mode client
Setting device to VTP CLIENT mode.
S2(config)# vtp domain pditn18b
Changing VTP domain name from NULL to pditn18b
S2(config)# vtp password test1234
Setting device VLAN database password to test1234
S2(config)#
```

Now access **CLI** prompt of **Office 3 Switch** and enter following commands

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname S3
S3(config)# vtp mode client
Setting device to VTP CLIENT mode.
S3(config)# vtp domain pditn18b
Changing VTP domain name from NULL to pditn18b
S3(config)# vtp password test1234
Setting device VLAN database password to test1234
S3(config)#
```

We have configured VTP server and VTP client. At this moment, VTP client will not receive VTP messages from server. We need to configure DTP between switches.

Section C

This section explains VLAN Tagging, VLAN Trunking protocols (ISL & 802.1Q), DTP Modes (ON, DTP Mode Desirable, Auto, No-Negotiate & OFF) and VLAN Trunk configuration in detail.

In VLAN configuration, a switch port can operate in two mode; access and trunk. In access mode it can carry only single VLAN information while in trunk mode it can carry multiple VLANs information. **Access mode** is used to connect the port with **end devices** while **trunk mode** is used to connect two **switching devices**.

Access Link and Trunk Link

An access link can carry single VLAN information while trunk link can carry multiple VLANs information. Configuring VLANs on single switch does not require trunk link. It is required only when you configure VLANs across the multiple switches.

For example if we do not connect all switches in our network, we do not require to configure the trunk link. In this case PC0, PC2 and PC4 cannot communicate with each other. Although they all belongs to same VLAN group but they have no link to share this information.

Trunk link connections are used to connect multiple switches sharing same VLANs information.

You may think why we cannot use access link to connect these switches. We can use access links to connect switches but we will need to use one separate link for each VLAN. If we have 2 VLANs, we need 2 links.

With this implementation, we need links equal to VLANs that does not scale very well. For example if our design require 30 VLANs, we will have to use 30 links to connect switches.

Summary

- An access link can carry single VLAN information.
- Theoretically, we can use access link to connect switches.
- If we use access link to connect switches, we have to use links equal to VLANs.
- Due to scalability we do not use access link to connect the switches.
- A trunk link can carry multiple VLAN information.
- Practically we use trunk links to connect switches or switches to routers.

VLAN Tagging

Trunk links use VLAN tagging to carry the multiple VLANs traffic separately.

In VLAN tagging process, sender switch add a VLAN identifier header to the original Ethernet frame. Receiver switch read VLAN information from this header and remove it before forwarding to the associate ports. Thus original Ethernet frame remains unchanged. Destination PC receives it in its original shape.

VLAN Tagging process with example

- PC1 generates a broadcast frame.
- Office1 switch receives it and know that it is a broadcast frame for VLAN20.
- It will forward this frame from all of its port associated with VLAN20 including trunk links.
- While forwarding frame from access links, switch does not make any change in original frame. So any other port having same VLAN ID in switch will receive this frame in original shape.
- While forwarding frame from trunk links, switch adds a VLAN identifier header to the original frame. In our case switch will add a header indicating that this frame belongs to VLAN20 before forwarding it from trunk link.
- Office2 switch will receive this frame from trunk link.
- It will read VLAN identifier header to know the VLAN information.
- From header it will learn that this is a broadcast frame and belong to VLAN20.
- It will remove header after learning the VLAN information.
- Once header is removed, switch will have original broadcast frame.
- Now office2 switch has original broadcast frame with necessary VLAN information.
- Office2 Switch will forward this frame from all of its ports associated with VLAN20 including trunk links. For trunk link same process will be repeated.
- Any device connected in ports having VLAN20 ID in Office2 switch will receive original frame.

Now we know that in VLAN tagging process sender switch adds VLAN identifier header to the original frame while receive switch removes it after getting necessary VLAN information. Switches use VLAN trunking protocol for VLAN tagging process.

VLAN Trunking Protocol

Cisco switches supports two types of trunking protocols **ISL** and **802.1Q**.

ISL

ISL (Inter-Switch Link) is a Cisco proprietary protocol. It was developed a long time before the 802.1Q. It adds a 26-byte header (containing a 15-bit VLAN identifier) and a 4-byte CRC trailer to the frame.

802.1Q

It is an open standard protocol developed by IEEE. It inserts 4 byte tag in original Ethernet frame. Over time, 802.1Q has become the most popular trunking protocols.

Key difference between ISL and 802.1Q

- ISL was developed Cisco while 802.1Q was developed by IEEE.
- ISL is a proprietary protocol. It will works only in Cisco switches. 802.1Q is an open standard based protocol. It will works on all switches.
- ISL adds 26 bytes header and 4 byte trailer to the frame.
- 802.1Q inserts 4 byte tag in original frame.

802.1Q is a lightweight and advanced protocol with several enhanced security features. Even Cisco has adopted it as a standard protocol for tagging in newer switches. 2960 Switch supports only 802.1Q tagging protocol.

VLAN Trunk Configuration

We can configure trunking in Cisco switches by two ways: statically or dynamically. In static method, we need to configure trunking in interface statically; while in dynamic mode it automatically done by a DTP trunking protocol.

Dynamic Trunking Protocol

DTP [Dynamic Trunking Protocol] is a Cisco proprietary protocol. It automatically configures trunking on necessary ports. It operates in five modes.

DTP Modes

DTP Mode ON

In ON mode, interface is set to trunk, regardless whether remote end supports trunking or not. ON mode cause interface to generate DTP messages and tag frames based on trunk type.

DTP Mode Desirable

In Desirable mode, interface will generate the DTP messages and send them to other end. Interface will work as access link until it get replies from remote end. If reply messages indicate that remote device is trunking capable, DTP will change connection link from access link to Trunk. If the other end does not respond to DTP message, the interface will work as access link connection.

DTP Mode Auto

In auto mode interface works as access link and passively listen for DTP messages. Interface will change connection link to trunk, if it receives a DTP message from remote end.

DTP Mode No-Negotiate

In No-Negotiate mode, interface is set as trunk connection. Interface will tag frames but it will not generate DTP messages. DTP is a Cisco's proprietary protocol, thus a non Cisco device will not understand it. This mode is used to trunk connection between **Cisco device and a non Cisco device**.

DTP Mode OFF

In off mode interface is configured as access-link. No DTP message will be generated nor frames will be tagged. In our topology, we need to configure trunk on following interfaces:

Switch	Interfaces
Office 1	Gig0/1, Gig0/2, F0/24
Office 2	Gig0/1, Gig0/2, F0/23, F0/24
Office 3	Gig0/1, Gig0/2

By default, all interface on a switch starts as access link. **`switchport mode trunk`** command is used to change connection link in trunk. Run this command from interface mode. We will now change all necessary interfaces (given in above table) connection link in trunk.

Office 1 Switch

```
S1(config)# interface fastEthernet 0/24
S1(config-if)# switchport mode trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24,changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24,changed state to up
S1(config-if)# exit
S1(config)# interface gigabitEthernet 0/1
S1(config-if)# switchport mode trunk
S1(config-if)# exit
S1(config)# interface gigabitEthernet 0/2
S1(config-if)# switchport mode trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2,changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2,changed state to up
S1(config-if)# exit
S1(config)#
```

Office 2 Switch

```
S2(config)# interface gigabitEthernet 0/1
S2(config-if)# switchport mode trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,changed state to up
S2(config-if)# exit
S2(config)# interface gigabitEthernet 0/2
S2(config-if)# switchport mode trunk
S2(config-if)# exit
S2(config)# interface fastEthernet 0/23
S2(config-if)# switchport mode trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23,changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23,changed state to up
S2(config-if)# exit
S2(config)# interface fastEthernet 0/24
S2(config-if)# switchport mode trunk
S2(config-if)# exit
```

Office 3 Switch

```
S3(config)#  interface fastEthernet 0/24
S3(config-if)# switchport mode trunk
S3(config-if)# exit
S3(config)# interface gigabitEthernet 0/1
S3(config-if)# switchport mode trunk
S3(config-if)# exit
```

That's all the configurations we need. Now our trunk links are ready to move multiple VLANs traffic.

Section D

This final section explains how to create and assign VLAN, VLAN Membership (Static and Dynamic), Router on Stick and Spanning Tree Protocol (STP) in detail.

Creating VLAN

In Section B, Switch S1 was configured as VTP Server. S2 and S3 were configured as VTP clients. We only need to create VLANs in VTP Server. VTP Server will propagate this info to all VTP clients automatically.

`vlan` ***`vlan number`*** command is used to create the VLAN.

Office 1 Switch

```
S1(config)# vlan 10
S1(config-vlan)# exit
S1(config)# vlan 20
S1(config-vlan)# exit
S1(config)#
```

Assigning VLAN Membership

VLAN can be assigned statically or dynamically but at our level, we only need to use the static method to assign VLAN membership. **`switchport access vlan [`*`vlan number`*`]`** command is used to assign VLAN to the interface. Following commands will assign VLANs to the interfaces.

Office 1 Switch

```
S1(config)# interface fastEthernet 0/1
S1(config-if)# switchport access vlan 10
S1(config-if)# interface fastEthernet 0/2
S1(config-if)# switchport access vlan 20
```

Office 2 Switch

```
S2(config)# interface fastEthernet 0/1
S2(config-if)# switchport access vlan 10
S2(config-if)# interface fastEthernet 0/2
S2(config-if)# switchport access vlan 20
```

Office 3 Switch

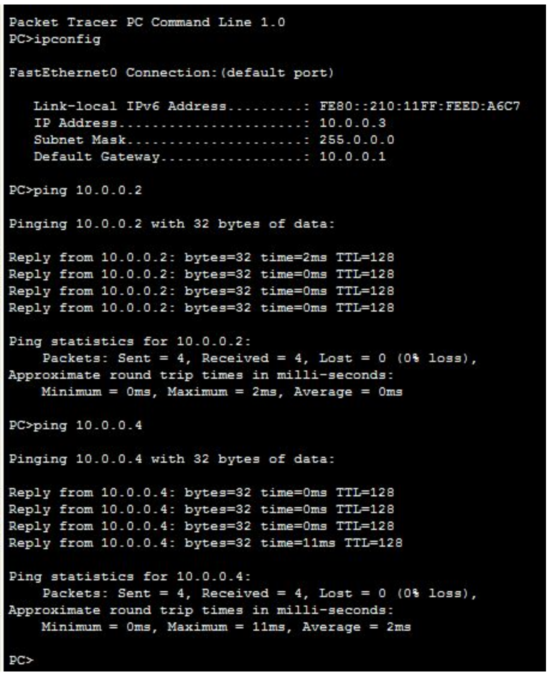
```
S3(config)# interface fastEthernet 0/1
S3(config-if)# switchport access vlan 10
S3(config-if)# interface fastEthernet 0/2
S3(config-if)# switchport access vlan 20
```

We have successfully assigned VLAN membership. It's time to test our configuration. To test this configuration, we will use *`ping`* command. *`ping`* command is used to test connectivity between two devices. As per our configuration, devices from same VLAN can communicate. Devices from different VLANs must not be able to communicate with each other without router.

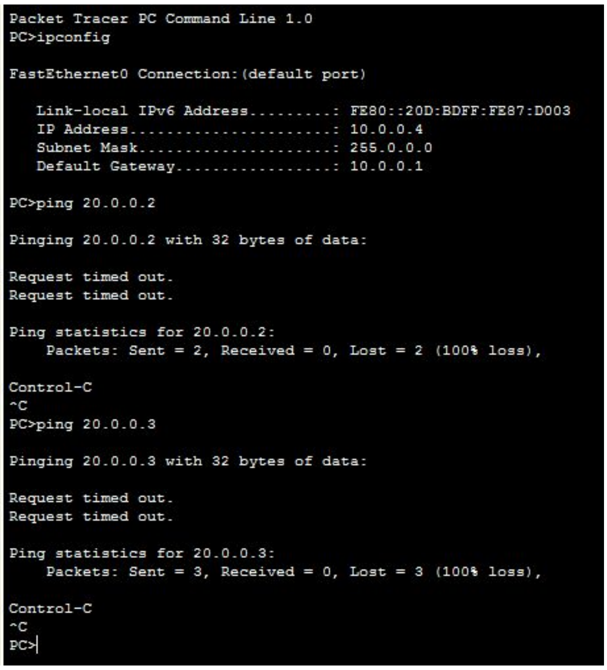
Testing VLAN configuration

Access PC(X) command prompt by Double click **PC(X)-PT** and click **Command Prompt**

We have two VLAN configurations VLAN 10 and VLAN 20. Let's test VLAN 10 first. In VLAN 10 we have three PCs with IP addresses: `10.0.0.2`, `10.0.0.3` and `10.0.0.4`. These PCs must be able to communicate with each other's. At this point, PCs from VLAN 10 should not be allowed to access PCs from VLAN 20. VLAN 20 also has three PCs `20.0.0.2`, `20.0.0.3` and `20.0.0.4`.



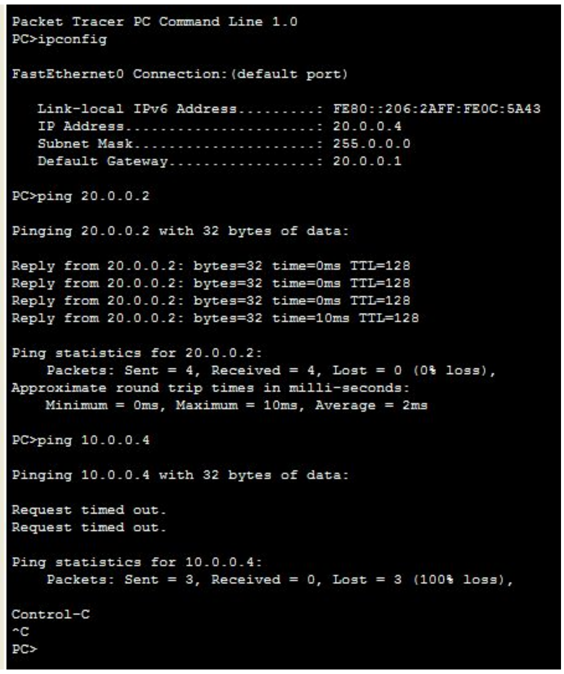
```
Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::210:11FF:FEED:A6C7
   IP Address......................: 10.0.0.3
   Subnet Mask.....................: 255.0.0.0
   Default Gateway.................: 10.0.0.1

PC>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=2ms TTL=128
Reply from 10.0.0.2: bytes=32 time=0ms TTL=128
Reply from 10.0.0.2: bytes=32 time=0ms TTL=128
Reply from 10.0.0.2: bytes=32 time=0ms TTL=128

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

PC>ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:

Reply from 10.0.0.4: bytes=32 time=0ms TTL=128
Reply from 10.0.0.4: bytes=32 time=0ms TTL=128
Reply from 10.0.0.4: bytes=32 time=0ms TTL=128
Reply from 10.0.0.4: bytes=32 time=11ms TTL=128

Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 2ms

PC>
```



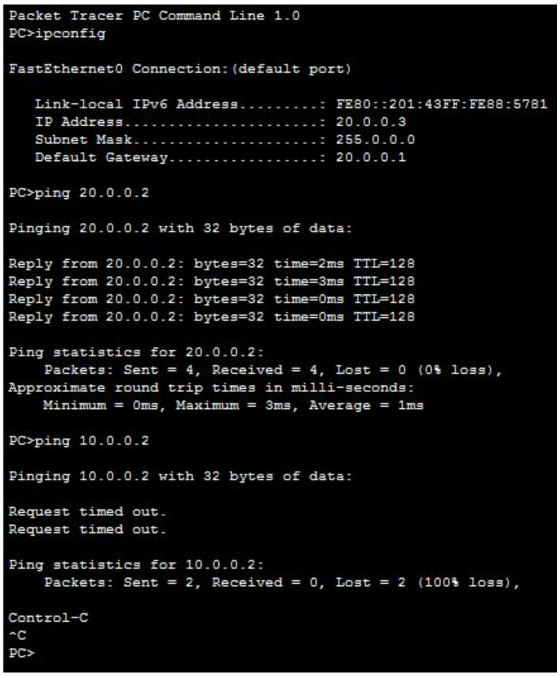
```
Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::20D:BDFF:FE87:D003
   IP Address......................: 10.0.0.4
   Subnet Mask.....................: 255.0.0.0
   Default Gateway.................: 10.0.0.1

PC>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 20.0.0.2:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
^C
PC>ping 20.0.0.3

Pinging 20.0.0.3 with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 20.0.0.3:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),

Control-C
^C
PC>
```

We have successfully implemented VLAN 10 now test VLAN 20.

Same as VLAN 10, PCs from VLAN 20 must be able to communicate with other PCs of same VLAN while they should not be able to access VLAN 10.



```
Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::206:2AFF:FE0C:5A43
   IP Address......................: 20.0.0.4
   Subnet Mask.....................: 255.0.0.0
   Default Gateway.................: 20.0.0.1

PC>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time=0ms TTL=128
Reply from 20.0.0.2: bytes=32 time=0ms TTL=128
Reply from 20.0.0.2: bytes=32 time=0ms TTL=128
Reply from 20.0.0.2: bytes=32 time=10ms TTL=128

Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

PC>ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 10.0.0.4:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),

Control-C
^C
PC>
```



```
Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::201:43FF:FE88:5781
   IP Address......................: 20.0.0.3
   Subnet Mask.....................: 255.0.0.0
   Default Gateway.................: 20.0.0.1

PC>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time=2ms TTL=128
Reply from 20.0.0.2: bytes=32 time=3ms TTL=128
Reply from 20.0.0.2: bytes=32 time=0ms TTL=128
Reply from 20.0.0.2: bytes=32 time=0ms TTL=128

Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

PC>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 10.0.0.2:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
^C
PC>
```

Configure Router on Stick

Typically routers are configured to receive data on one physical interface and forward that data from another physical interface based on its configuration. Each VLAN has a layer 3 address that should be configured as default gateway address on all its devices. In our scenario we reserved IP address 10.0.0.1 for VLAN 10 and 20.0.0.1 for VLAN 20.

With default configuration, we need two physical interfaces on router to make intra-VLAN communication. Due to the high price of a router, it’s not a cost effective solution to use a physical interface of router for each VLAN. Usually a router has one or two Ethernet interface. For example, if we have 50 VLANs, we would need nearly 25 routers in order to make intra-VLANs communication. To deal with situation, we use Router on Stick.

Router on Stick is router that supports trunk connection and has an ability to switch frames between the VLANs on this trunk connection. On this router, a single physical interface is sufficient to make communication between both VLANs.

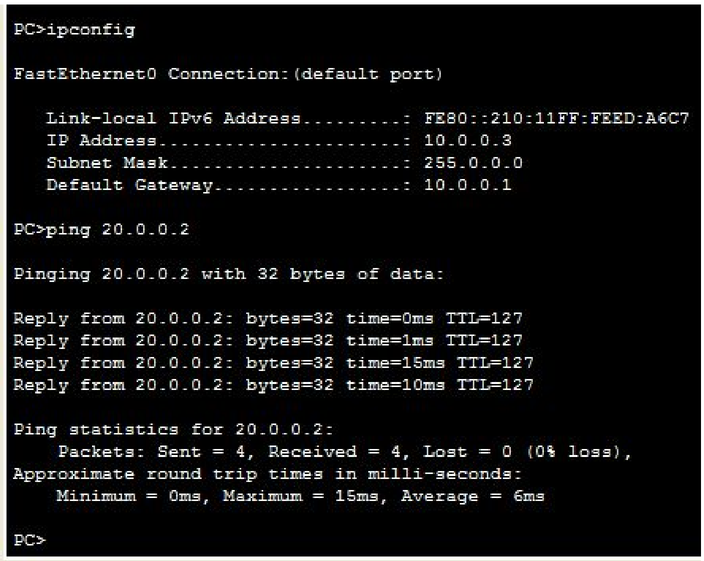
Access command prompt of Router

To configure Router on Stick we have to access CLI prompt of Router. Click **Router** and Click **CLI** from menu items and Press **Enter key** to access the CLI

Run following commands in same sequence to configure Router on Stick

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastEthernet 0/0
Router(config-if)# no ip address
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface fastEthernet 0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 10.0.0.1 255.0.0.0
Router(config-subif)# exit
Router(config)# interface fastEthernet 0/0.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 20.0.0.1 255.0.0.0
Router(config-subif)# exit
```

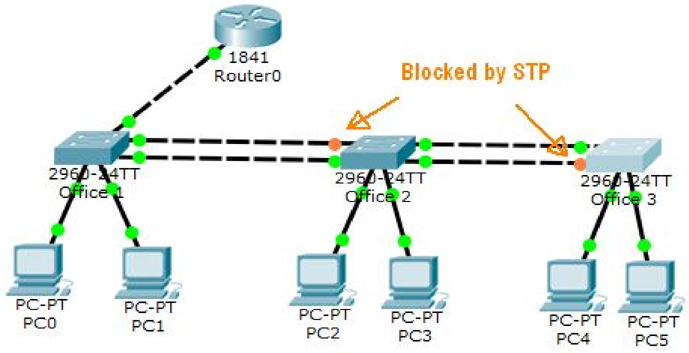
- In above configuration, we broke up single physical interface [FastEthernet 0/0] into two logical interfaces, known as sub-interfaces. A router can support up to 1000 interfaces
- By default interface link works as access link. We need to change it into trunk link. encapsulation commands specify the trunk type and associate VLAN with sub-interface.
- In next step we assigned IP address to our sub-interface.



```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::210:11FF:FEED:A6C7
   IP Address......................: 10.0.0.3
   Subnet Mask.....................: 255.0.0.0
   Default Gateway.................: 10.0.0.1

PC>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time=0ms TTL=127
Reply from 20.0.0.2: bytes=32 time=1ms TTL=127
Reply from 20.0.0.2: bytes=32 time=15ms TTL=127
Reply from 20.0.0.2: bytes=32 time=10ms TTL=127

Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 6ms

PC>
```

That's all configuration we need to switch VLANs. Now we can test different VLAN communications. To test intra VLANs communication open command prompt of PC and ping the PC of other VLAN. PC2 [10.0.0.3] from VLAN 10 can now access PC1 [20.0.0.2] from VLAN 20.

Spanning Tree Protocol (STP)



STP is a layer 2 protocol, used for removing loops. For backup purpose we typically create backup links for important resources. In our scenario, all offices have backup links that create loops in topology. STP automatically removes layer 2 loops. STP multicasts frame that contain information about switch interfaces. These frames are called BPDU (Bridge Protocol Data Units). Switch use BPDUs to learn network topology. If it found any loop, it will automatically remove that. To remove loop, STP disables port or ports that are causing it. *(may differ to yours)*

APPENDIX: VLAN VTP DTP commands cheat sheet

Command	Description
Switch(config)# vtp mode server	Configure Switch as VTP Server
Switch(config)# vtp mode client	Configure Switch as VTP Client
Switch(config)# vtp mode transparent	Configure Switch as VTP Transparent
Switch(config)# no vtp mode Configure	Switch to default VTP Server Mode
Switch(config)# vtp domain domain-name	Set VTP Domain name.
Switch(config)# vtp password password	Set VTP password. Password is case sensitive
Switch# show vtp status	Display VTP status including general information
Switch# show vtp counters	Show VTP counters of switch
Switch(config-if)# switchport mode trunk	Change interface mode in Trunk
Switch(config)# vlan 10	Create VLAN and associate number ID 10 with it
Switch(config-vlan)# name Sales	Assign name to VLAN
Switch(config-vlan)# exit	Return in Global configuration mode from VLAN configuration mode
Switch(config)# interface fastethernet 0/1	Enter in interface configuration mode
Switch(config-if)# switchport mode access	Set interface link type to access link
Switch(config-if)# switchport access vlan 10	Assign this interface to VLAN 10
Switch# show vlan	Displays VLAN information
Switch# show vlan brief	Displays VLAN information in short
Switch# show vlan id 10	Displays information VLAN ID 10 only
Switch# show vlan name sales	Displays information about VLAN named sales only
Switch(config)# interface fastethernet 0/8	Enter in Interface configuration mode
Switch(config-if)# no switchport access vlan 10	Removes interface from VLAN 10 and reassigns it to the default VLAN - VLAN 1
Switch(config-if)# exit	Move back to Global configuration mode
Switch(config)# no vlan 10	Delete VLAN 10 from VLAN database
Switch# copy running-config startup-config	Saves the running configuration in NVRAM