PROJECT REPORT ON

IMPLEMENTATION OF INTER-VLAN COMMUNICATION

BY

ASHWIN PRAJAPATI
PARTH DODIA
SALONI BHAMBURE
SHREYAS BORSE

UNDER THE GUIDANCE OF

PROF. CHETNA SINGH

DEPARTMENT OF ELECTRONICS & TELECOMMUNICATION
K.J.SOMAIYA COLLEGE OF ENGINEERING,
VIDYAVIHAR, MUMBAI-400077.
(Autonomous College Affiliated to University of Mumbai)

(2018-19)

K.J.SOMAIYA COLLEGE OF ENGINEERING,
VIDYAVIHAR, MUMBAI -400077.
(Autonomous College Affiliated to University of Mumbai)

DEPARTMENT OF ELECTRONICS & TELECOMMUNICATION ENGINEERING

CERTIFICATE

This is to certify that the following students of sem VI

ASHWIN PRAJAPATI 1613061
PARTH DODIA 1613012
SALONI BHAMBURE 1613006
SHREYAS BORSE 1613061

have successfully completed the project titled "Inter Vlan routing methodologies" towards the partial fulfillment of degree of Bachelor of Technology in Electronics and Telecommunications of the University of Mumbai during academic year 2018-19.

Internal Guide

PROF.CHETNA SINGH **PROF. RUPALI**
PATIL
Examiner 1 **Examiner 2**

CONTENTS

ABSTRACT:

This mini-project focuses on the use of vlan, inter-vlan communication and its different methods of implementation. Vlan is basically a virtual lan which we can create in the same switch. It was first used when there was a need to optimize the use of switches and routers and to manage the broadcast traffic. This project describes the implementation of different Inter-VLAN communication methods and the objective behind the implementation of these new methods. We have discussed and implemented this methods using cisco packet tracer and hardware devices router-1841, switch-2960 and thereby this methods are compared based on parameters -Use of hardware, Ease of configuration, Latency. along with their applications.

1. INTRODUCTION:

Virtual LAN (VLAN) is a concept in which we can divide the devices logically on layer 2 (data link layer). VLAN is a logical group of network devices that appear to be on the same LAN. They are configured as if they are connected to the same physical connection even if they are located on a number of different LAN segments.

Layer 3 devices divide broadcast domain but broadcast domain can be divided by switches using the concept of VLAN.A broadcast domain is a network segment in which if a device broadcast a packet then all the devices in the same broadcast domain will receive it. The devices in the same broadcast domain will receive all the broadcast packet but it is limited to switches only as routers don't forward out the broadcast packet. Broadcast Frames can be switched on only the same VLAN ID's[1].

In scenarios where sensitive data may be broadcast on a network, VLANs can be created to enhance security by designating a broadcast to a specific VLAN. Only users that belong to a VLAN are able to access and manipulate the data on that VLAN.

VLAN ranges –

- VLAN 0, 4095: These are reserved VLAN which cannot be seen or used.
- VLAN 1: It is the default VLAN of switches. By default, all switch ports are in VLAN. This VLAN can't be deleted or edit but can be used.
- VLAN 2-1001: This is a normal VLAN range. We can create, edit and delete these VLAN.
- VLAN 1002-1005: These are CISCO defaults for token rings. These VLAN can't be deleted.
- VLAN 1006-4094: This is the extended range of VLAN.[1]

Advantages of using VLANs:

- Performance –The network traffic is full of broadcast and multicast. VLAN reduces the need to send such traffic to unnecessary destination. For example, If the traffic is intended for 2 users but as 10 devices are present in the same broadcast domain therefore all will receive the traffic and lead to wastage of bandwidth but by using VLANs, the broadcast or multicast packet will go to the intended users only.
- Formation of virtual groups – As there are different departments in every organisation namely sales, finance etc., VLANs can be very useful in order to group the devices logically according to their departments.
- Security – In the same network, sensitive data can be broadcast which can be accessed by the outsider but by creating VLAN, we can control broadcast domains, set up firewalls, restrict access. Also, VLANs can be used to inform the network manager of an intrusion. Hence, VLANs greatly enhance network security.
- Flexibility – VLAN provide flexibility to add, remove the number of host we want.
- Cost reduction – VLANs can be used to create broadcast domains which eliminate the need for expensive routers.[5]
- By using VLAN, the number of small size broadcast domain can be increased which are easy to handle as compared to a bigger broadcast domain

Ports: The port modes are defined as follows:

- Access Port — The frames received on the interface are assumed to not have a VLAN tag and are assigned to the specified VLAN. Access ports are used primarily for hosts and can only carry traffic for a single VLAN.
- Trunk Port — These switch ports belong to and carry the traffic of more than one VLAN. The frames received on the interface are assumed to have VLAN tags. Trunk ports are for links between switches or other network devices and are capable of carrying traffic for multiple VLANs. These are of great use if user wants to exchange traffic between more than one switches having more than one VLAN configured.[5]

1.1 INTRODUCTION TO INTERVLAN ROUTING:

To forward out the packets to different VLAN (from one VLAN to another) or broadcast domain, inter VLAN routing is needed. Through VLAN, different small size sub networks are created which are comparatively easy to handle.

A layer 2 network can be defined as a broadcast domain and this Layer 2 network can exist as a VLAN created on one or more switches in the network. These VLANS within the network are isolated from one and other so that packets destined for one VLAN do not cross over into another VLAN in the network. To be able to have packets from one VLAN transported into another VLAN a Layer 3 device is required whether this be a physical or a logical connection.[2]

There are several different ways Inter-VLAN routing can be configured, there could be a physical link for each VLAN from the Switch in the network to a router or a single trunk link from a switch to a router in the network to which is sometimes referred to as a Router on a Stick. Also a Multi-layer Switch can be configured to do all the work so no external router is required.

There are various ways in which inter-VLAN routing can be accomplished.Some of them are:

- Traditional inter-VLAN routing: Old Legacy Method
- Router-on-a-stick
- Multilayer Switch (3 Layer)[2]

2. LITERATURE SURVEY

2.1 OLD TOPOLOGY:

Historically, the first solution for inter-VLAN routing relied on routers with multiple physical interfaces. Each interface had to be connected to a separate network and configured with a distinct subnet. In this legacy approach, inter-VLAN routing is performed by connecting different physical router interfaces to different physical switch ports. The switch ports connected to the router are placed in access mode and each physical interface is assigned to a different VLAN. Each router interface can then accept traffic from the VLAN associated with the switch interface that it is connected to, and traffic can be routed to the other VLANs connected to the other interfaces.[1]

A router is connected to the switch using multiple interfaces, one for each VLAN. The interfaces on the router are configured as the default gateways for the VLANs configured on the switch. The ports that connect to the router from the switch are configured in access mode in their corresponding VLANs. This then allows each router interface to accept traffic from the VLAN associated with the connected switches interface. The traffic can then be routed to the appropriate VLAN.

When a user node sends a message to a user connected to a different VLAN, the message moves from their node to the access port that connects to the router on their VLAN. When the router receives the packet, it examines the packet's destination IP address and forwards it to the correct network using the access port for the destination VLAN. The switch now can forward the frame to the destination node since the router changed the VLAN information from the source VLAN to the destination VLAN.

In this form of inter-VLAN routing, the router has to have as many LAN interfaces as the number of VLANs configured on the switch. Therefore, if a switch has 10 VLANs, the router should have the same number of LAN interfaces.

One of the main disadvantages of legacy inter-VLAN routing is that it requires multiple physical interfaces on both the switch and the router. This means as the network grows, additional hardware is required, once exceeded the number of physical interfaces for either the router or switch.[5]

2.2 ROUTER ON STICK:

A typical switch can have up to 48 ports. This means, you can use that switch to route traffic between VLANs for up to 48 VLANs. In smaller networks this may be enough, but in larger enterprise networks, 48 VLANs may not be enough. this is not a desired behavior because you end up using too many physical interfaces, and sooner or later you will run out of interfaces.

Router-on-a-stick is a type of router configuration in which you are able to use a single physical interface to route traffic between multiple VLANs. The router interface is configured as a trunk link and is connected to a trunk switch port. The router is accepting the tagged traffic on the trunk interface and routes it internally using subinterfaces. Trunk links are able to accept multiple VLANs on one physical interface. Switches are able to recognize the VLAN used for a specific packet through the use of encapsulation protocols that encapsulate or tag the frames. The protocols used are 802.1Q (dot 1q). Subinterfaces are virtual interfaces associated with a single physical interface. These subinterfaces have their own IP address and VLAN assignment to be able to operate on a specific VLAN.[5]

2.3 MULTILAYER SWITCH:

Multi-layer switching combines layer 2 and 3 switching technologies and provides high-speed scalability with low latency. Multi-layer switching can move traffic at wire speed and also provide layer 3 routing. There is no performance difference between forwarding at different layers because the routing and switching is all hardware based.

Multi-layer switching can make routing and switching decisions based on the following

- MAC address in a data link frame
- Protocol field in the data link frame
- IP address in the network layer header
- Protocol field in the network layer header
- Port numbers in the transport layer header

Layer 3 switching is solely based on (destination) IP address stored in the header of IP datagram .The difference between a layer 3 switch and a router is the way the device is making the routing decision. Traditionally, routers use microprocessors to make forwarding decisions in software, while the switch performs only hardware-based packet switching. However, some traditional routers can have advanced hardware functions as well in some of the higher-end models.

Main problem of latency in previous two method can be resolved using L3 Switch.Here there is no need of individual subinterfaces as gateway Multilayer Switch has SVI interface,Switched Virtual interface
is a configured logical interface within L-3 switch compared to an external router to where a trunk is required.
A single SVI can be created for a Vlan. SVI for layer 3 switch provides both management and routing services while SVI on layer 2 switch provides only management services like creating vlans or telnet/SSH services. SVI is Virtual in that there is no physical port defined yet it can perform the same functions for the VLAN as a router interface .There is no need for a physical link.[2]

A **layer-3 switch** incorporates routing capability in addition to the layer-2 bridging found in a standard switch. The major difference between the packet forwarding operation of a router and that of a layer-3 switch is the actual implementation. In general-purpose routers, forwarding is usually implemented in software that runs on a microprocessor or a network processor, whereas a layer-3 switch performs the same operation using dedicated application-specific integrated circuit (ASIC) hardware.[5]

3. OBJECTIVE

To implement and study the inter-vlan communication methods discussed above and make comparative analysis.

4. METHODOLOGY

The above methods were carried out with help of

1. Cisco Packet Tracer:
   - This software is a visual simulation tool which enables the users to create network topologies and imitate modern computer networks.
   - Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, EIGRP, BGP,etc.
   - One can design the network simply by dragging and dropping the required router, switch, and the cable to connect them.

2. Hardware devices:

   Router :Cisco 1841 router

   Port or Connection Port Type: Color1

   1. The color codes are specific to cables shipped by Cisco Connected To: Cable Fast Ethernet (FE) RJ-45, yellow Ethernet hub Crossover to connect to a router Straight-through to connect to a switch T1/E1 WAN RJ-48C T1 or E1 network or CSU/DSU RJ-48 T1/E1 straight-through (Crossover to connect ot a PBX or any other equipment) Cisco serial (1T) 60-pin D-sub, blue CSU/DSU and serial network or equipment Cisco serial transition cable that matches the signaling protocol (EIA/TIA-232, EIA/TIA-449, V.35, X.21, or EIA/TIA-530) and the serial port operating mode (DTE or DCE). Refer to the Cisco Modular Access Router Cable Specifications document for information about selecting these cables. Cisco Smart serial (2T) Cisco Smart compact connector, blue CSU/DSU and serial network or equipment For WIC-2T and WIC-2A/S only DSL RJ-11C/RJ-14C Network demarcation device for service provider's DSL interface RJ-11 straight-through for 2-wire RJ-14 straight-through for 4-wire BRI S/T WAN (external NT12) 2. NT1 = Network Termination 1 RJ-45, orange NT1 device or PINX3 3. PINX = Private integrated network exchange RJ-45 straight-through BRI U WAN (built-in NT1) RJ-49C/CA-A11, orange ISDN network RJ-49 straight-through Analog modem RJ-11 PSTN RJ-11 straight-through 56/64-kbps CSU/DSU 8-pin modular RJ-48S interface RJ-48 straight-through.[3]

Switch :Cisco Catalyst 2960:

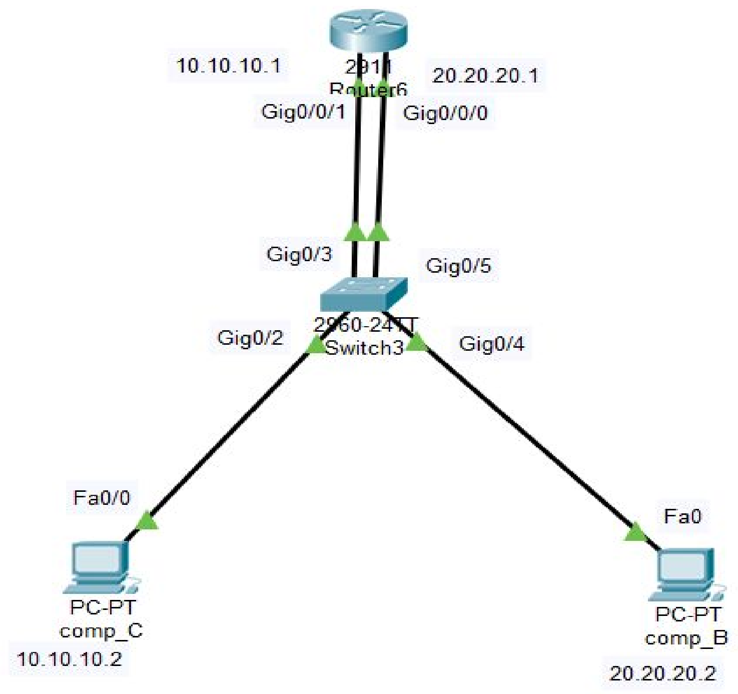
Cisco Catalyst 2960-X and 2960-XR Series Switches feature:

● 24 or 48 Gigabit Ethernet ports with line-rate forwarding performance .

● 4 fixed 1 Gigabit Ethernet Small Form-Factor Pluggable (SFP) uplinks or 2 fixed 10 Gigabit Ethernet SFP+ uplinks ● PoE+ support with a power budget of up to 740W and Perpetual PoE ● Cisco IOS LAN Base1 or LAN Lite1 and Cisco IOS IP Lite2 ● Device management with web UI, over-the-air access via Bluetooth, Command-Line Interface (CLI), Simple Network Management Protocol (SNMP), and RJ-45 or USB console access ● Network management with Cisco Prime® , Cisco Network Plug and Play, and Cisco DNA Center ● Stacking with FlexStack-Plus and FlexStack-Extended ● Layer 3 features with routed access (Open Shortest Path First [OSPF]), static routing, and Routing Information Protocol (RIP) ● Visibility with Domain Name System as an Authoritative Source (DNS-AS) and Full (Flexible) NetFlow ● Security with 802.1X, Serial Port Analyzer (SPAN) and Bridge Protocol Data Unit (BPDU) Guard ● Reliability with higher Mean Time Between Failures (MTBF) and Enhanced Limited Lifetime Warranty (E-LLW) ● Resiliency with optional dual field-replaceable power supplies[3]

4.1 OLD TOPOLOGY

The network topology for the old legacy inter-vlan communication implemented is as follows:



OVERVIEW OF OLD TOPOLOGY:

1)COMP_C and COMP_B are in two different VLANs.

2)Both the PC's are connected to the router vis switch through two distinct physical interfaces for each VLAN respectively.

3)Assigned IP address 10.10.10.2 to COMP_C with default subnet mask as 255.0.0.0.

4)The default gateway for the COMP_C is 10.10.10.1 which is the interface Gig0/0 of the router.

5)Assigned IP address 20.20.20.2 to COMP_B with default subnet mask as 255.0.0.0.

6)The default gateway for the COMP_B is 20.20.20.1 which is the interface Gig0/1 of the router.

7)Created two VLANs : VLAN2 and VLAN3

8)Configured the Switch ports to access the specified VLAN, Gig0/2 to VLAN 2 and Gig0/4 to VLAN 3.

9) On Router, configured its interfaces with the default gateways corresponding to the VLANs. That is; on Gig0/0 -10.10.10.1 and on Gig0/1 – 20.20.20.1 ...[2]

Accomplished the above steps with the CLI commands shown below:

1) Switch Configuration:

COM6 - PuTTY

```
RACK1-SW1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
RACK1-SW1(config)#interface range gi0/4-5
RACK1-SW1(config-if-range)#switchport access vlan 2
RACK1-SW1(config-if-range)#switchport mode access
RACK1-SW1(config-if-range)#
RACK1-SW1(config-if-range)#exit
RACK1-SW1(config)#interface vlan 3
RACK1-SW1(config-if)#exit
Apr  5 08:42:10.207: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan3, changed state tswitchport access vlan 3
                      ^
% Invalid input detected at '^' marker.

RACK1-SW1(config-if)#
RACK1-SW1(config-if)#switchport access vlan 3
                      ^
% Invalid input detected at '^' marker.

RACK1-SW1(config-if)#interface range 0/2-3
                                     ^
% Invalid input detected at '^' marker.

RACK1-SW1(config)#interface range gi0/2-3
RACK1-SW1(config-if-range)#switchport access vlan 3
RACK1-SW1(config-if-range)#switchport mode access
RACK1-SW1(config-if-range)#exit
RACK1-SW1(config)#exit
RACK1-SW1#
Apr  5 08:43:24.662: %SYS-5-CONFIG_I: Configured from console by admin on consoleshow vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/6, Gi0/7, Gi0/8, Gi0/9
                                                Gi0/10, Gi0/11, Gi0/12
2    comp_B                           active    Gi0/4, Gi0/5
3    comp_C                           active    Gi0/2, Gi0/3
10   USER VLAN                        active
20   ROUTER VLAN                      active
30   ACCESS POINT VLAN                active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

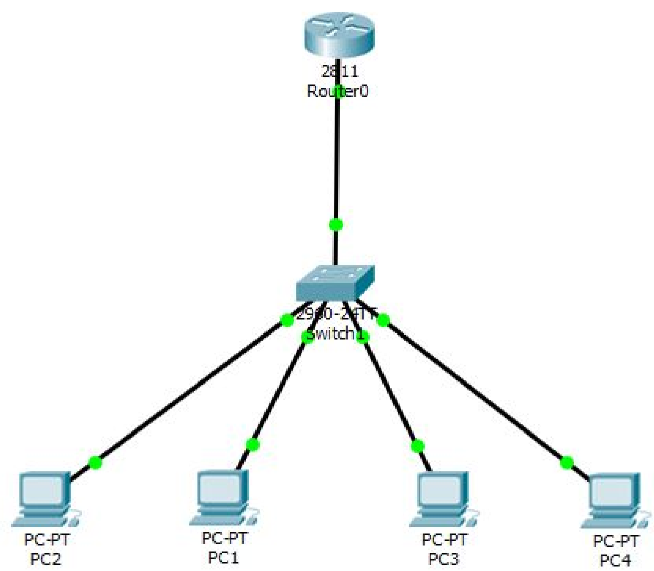
2)Router Configuration:

COM7 - PuTTY

```
R2(config)#interface Gi0/0/1
R2(config-if)#ip address 10.10.10.1 255.0.0.0
R2(config-if)#exit
R2(config)#interface Gi0/0/1
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface Gi0/0/0
R2(config-if)#ip address 20.20.20.1 255.0.0.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*Apr  5 08:50:10.585: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed st
ate to downexit
R2#s
*Apr  5 08:50:14.851: %SYS-5-CONFIG_I: Configured from console by admin on conso
lehowi
*Apr  5 08:50:16.647: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed st
ate to up
*Apr  5 08:50:17.646: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEth
ernet0/0/0, changed state to up brief
       ^
% Invalid input detected at '^' marker.

R2#show ip brief
            ^
% Invalid input detected at '^' marker.

R2#show ip interface br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   20.20.20.1      YES manual up                    up
GigabitEthernet0/0/1   10.10.10.1      YES manual up                    up
GigabitEthernet0/1/0   unassigned      YES NVRAM  administratively down down
R2#
```

2. ROUTER ON STICK:

The network topology for the router on stick inter-vlan communication implemented is as follows:



In order to form a trunk link with our switch it is necessary to create one sub-interface for every VLAN configured on our switch. After creating the sub-interface, we assign an IP address to it and set the encapsulation type to 802.1q along with the VLAN to which the subinterface belongs.

[2]

OVERVIEW OF ROUTER ON STICK METHOD:

1)COMP_C and COMP_B are in two different VLANs.

2)Both the PC's are connected to the router via switch through two distinct physical interfaces for each VLAN respectively.

3)Assigned IP address 10.10.10.2 to COMP_C with default subnet mask as 255.0.0.0.

4)The default gateway for the COMP_C is 10.10.10.1 which is the interface Gig0/0 of the router.

5)Assigned IP address 20.20.20.2 to COMP_B with default subnet mask as 255.0.0.0.

6)The default gateway for the COMP_B is 20.20.20.1 even this is the interface Gig0/0 of the router.

Important steps:

1) Use **interface** *port_int.sub_interface* command in global configuration mode to create a unique subinterface for each VLAN to be routed.
2) Use the **encapsulation dot1q** *vlan_id* command to enable 802.1Q trunking and associate each VLAN with the subinterface.
3) Assign the ip address to the subinterfaces of the respective VLANs.
4) **show ip interface brief** command shows the list of ip addresses existing in the router.[5]

Router configuration:

COM7 - PuTTY

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int gi0/0/0.2
R2(config-subif)#no ip address
R2(config-subif)#encapsulation dot1Q 2
R2(config-subif)#ip address 20.20.20.1 255.0.0.0
R2(config-subif)#exit
R2(config)#int gi0/0/0.3
R2(config-subif)#no ip address

% Configuring IP routing on a LAN subinterface is only allowed if that
subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q,
or ISL vLAN.

R2(config-subif)#encapsulation dot1Q 3
R2(config-subif)#ip address 10.10.10.1 255.0.0.0
R2(config-subif)#^Z
R2#
*Apr  5 10:48:25.676: %SYS-5-CONFIG_I: Configured from console by admin on consolesh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES manual up                    up
GigabitEthernet0/0/0.2 20.20.20.1      YES manual up                    up
GigabitEthernet0/0/0.3 10.10.10.1      YES manual up                    up
GigabitEthernet0/0/0.5 unassigned      YES manual up                    up
GigabitEthernet0/0/0.8 unassigned      YES unset  up                    up
GigabitEthernet0/0/0.9 unassigned      YES unset  up                    up
GigabitEthernet0/0/1   unassigned      YES manual down                  down
GigabitEthernet0/1/0   unassigned      YES NVRAM  administratively down down
R2#
```

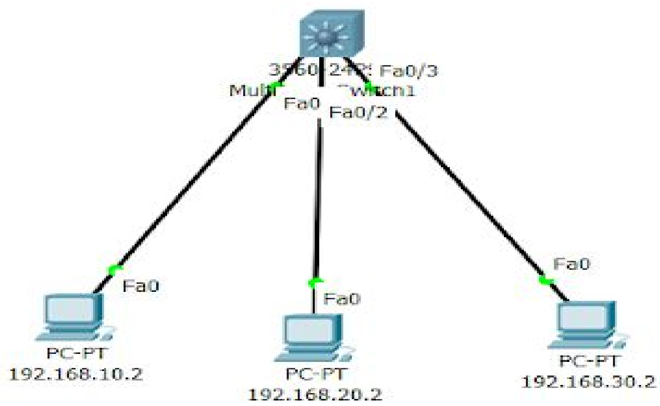
Switch Configuration:

```
RACK1-SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RACK1-SW1(config)#int gi0/3
RACK1-SW1(config-if)#no switchport access vlan 3
RACK1-SW1(config-if)#exit
RACK1-SW1(config)#int gi0/4
RACK1-SW1(config-if)#no switchport access vlan 2
RACK1-SW1(config-if)#^Z
RACK1-SW1#sh v
Apr  5 10:23:03.471: %SYS-5-CONFIG_I: Configured from console by admin on consolelan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/3, Gi0/4, Gi0/6, Gi0/7
                                                Gi0/8, Gi0/9, Gi0/10, Gi0/11
                                                Gi0/12
2    comp_B                           active    Gi0/5
3    comp_C                           active    Gi0/2
10   USER VLAN                        active
20   ROUTER VLAN                      active
30   ACCESS POINT VLAN                active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

3. MULTILAYER SWITCH (Using L3 SW as a switch) :

Process of Inter Vlan Routing by Layer 3 Switch –

The SVI created for the respective Vlan acts a default gateway for that Vlan just
like the sub-interface of the router
(in the process of Router On a stick). If the packet is to be delivered to different vlan
i.e inter Vlan Routing is to be performed on layer 3 switch then
first the packet is delivered to layer 3 switch and then to destination
just like in the process of router on a stick.[5][6]

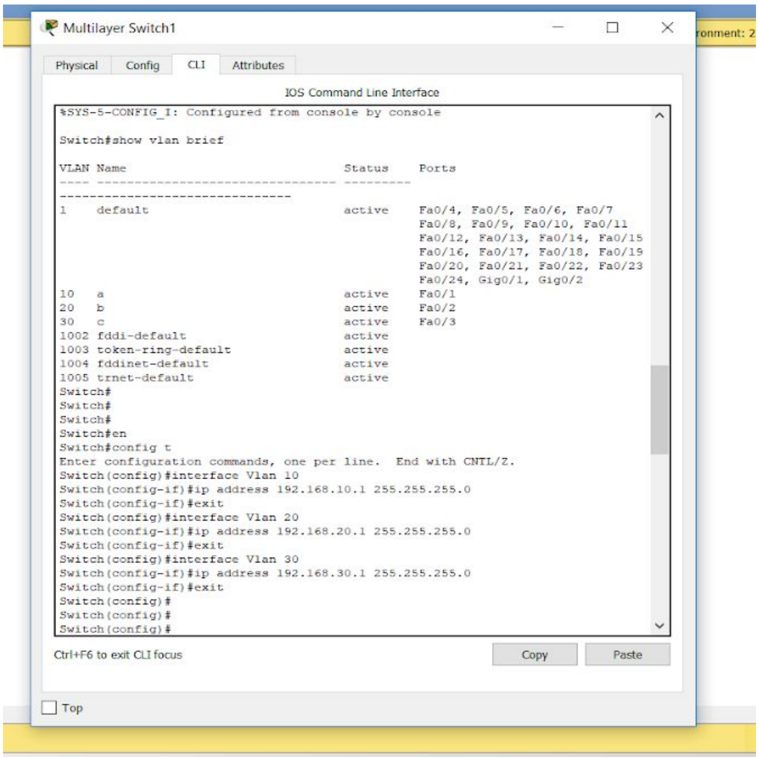


OVERVIEW OF MULTILAYER SWITCH METHOD:

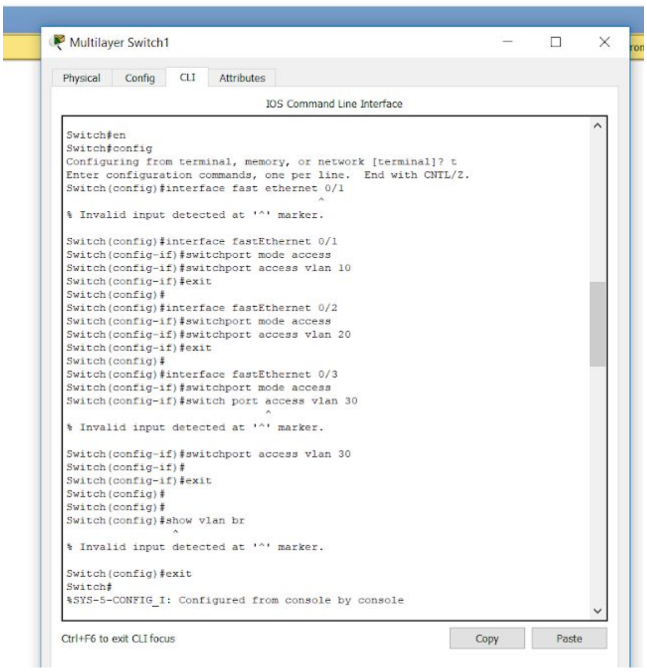
Here is a topology in which we have a layer 3 switch connected to
host devices namely PC1, PC2, PC3.

1) The hosts PC1, PC2,PC3 will be in
Vlan 10 VLAN 20 VLAN 30. Giving IP address to All hosts.
2) Naming all vlan
3) Assigning Fast ethernet ports of device and L3 switch
4) Interface Vlan-> mode access-> access vlan
5) SVI Created
6) Interface Vlan->assigning IP and Subnet mask.
7) TO use L3 for routing-> command IP routing
8) Ping from PC1 to PC3.[2]

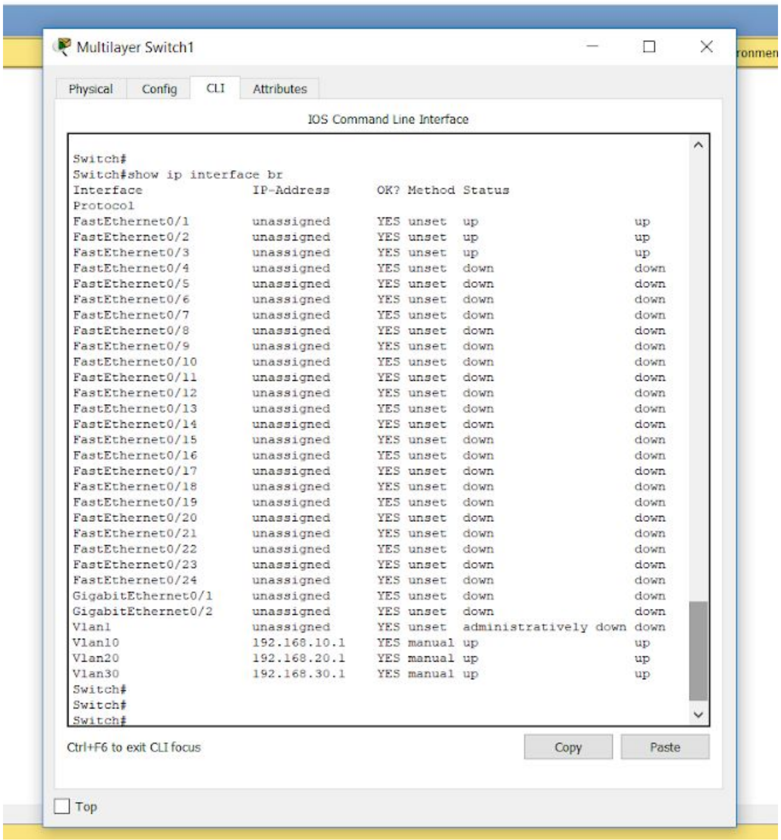
Vlan configuration:



Interfacing fast Ethernet port:



IP BRIEF:



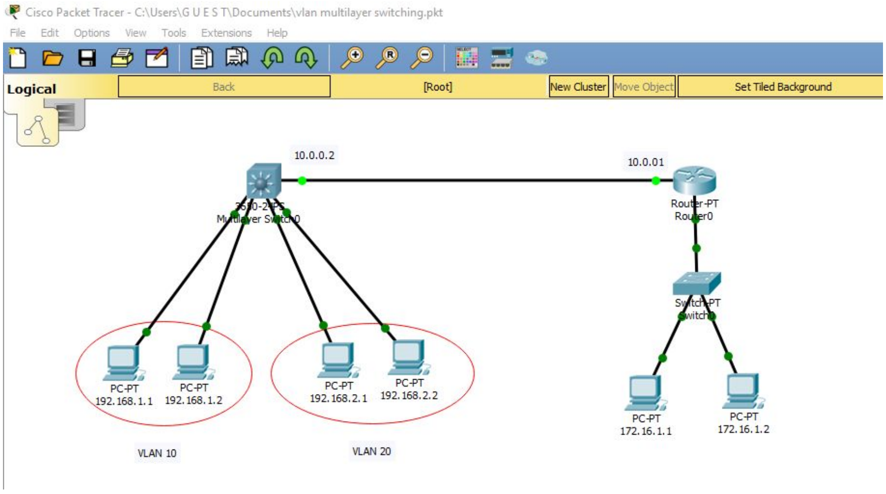
At the end to enable ip route on L3 switch :

switch#ip routing

4.4) MULTILAYER SWITCH (Using switch as a router):

In this method we would modify the network used in M3 and use one of the port of the layer 3 switch as a router port. To use that port as router port we need to configure that port from switch port to router port. We will use “no switchport” command to do this. Thus we can operate the L3 switch as a router and it can communicate using IP addresses. For communicating between the two sites, we used RIP(dynamic routing). We can also use other routing protocols. This method is widely used for WAN. Procedure Is Same As Above Method.[1][2]

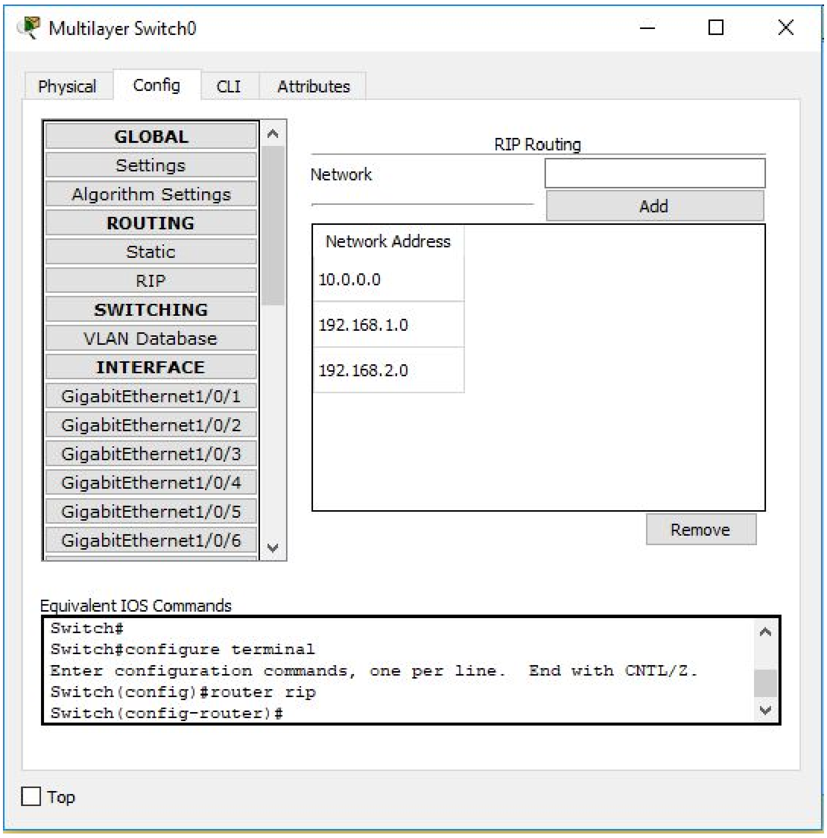
The following figure shows the network;



Overview of Configuration of L3 switch method 2:

1. Create two vlans(vlan 10,vlan 20).
2. Assign two end users on each vlan
3. Configure a port of the multilayer switch as router port
4. Create another network
5. Establish connection between that port and the other network.
6. Use RIP protocol for communication.
7. Ping to check the connection between the networks.

RIP table of the multilayer switch:

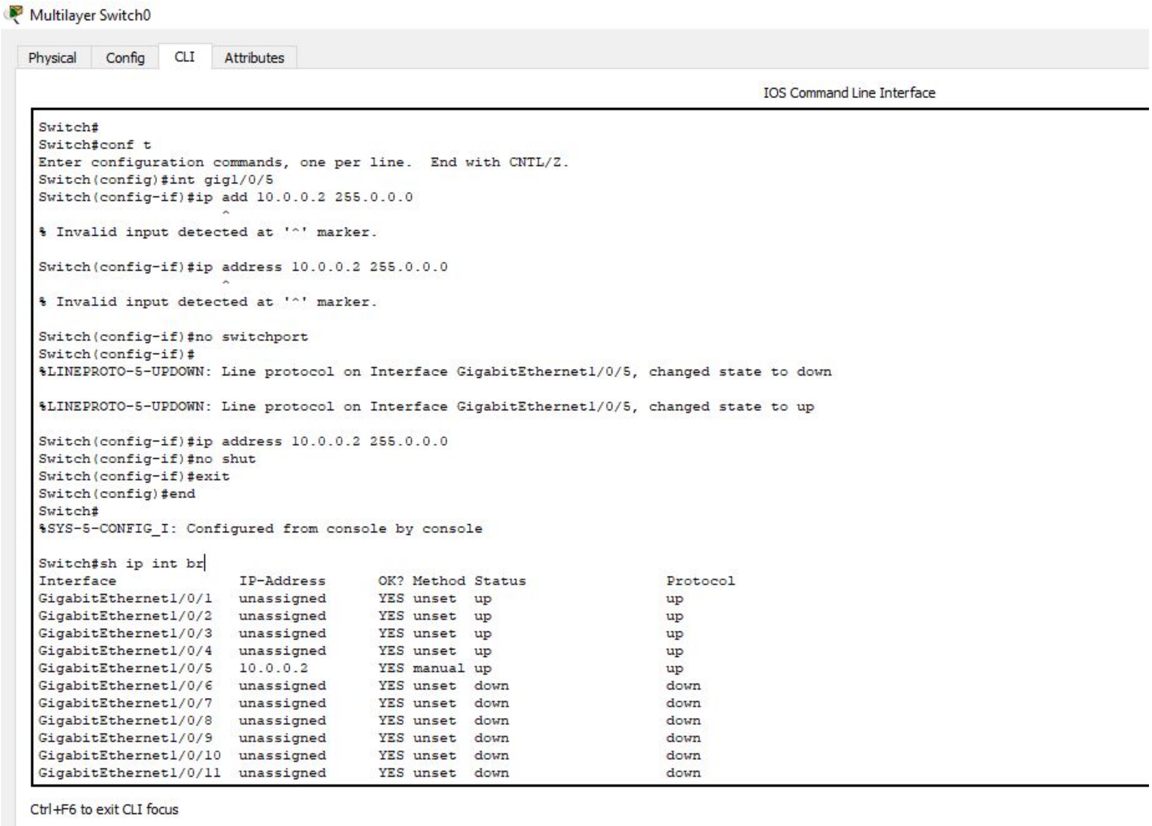


Code:

```
Switch#

Switch#conf t

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

Switch(config)#int gig1/0/5

Switch(config-if)#ip add 10.0.0.2 255.0.0.0

^

% Invalid input detected at '^' marker.

Switch(config-if)#no switchport

Switch(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to down


%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to up


Switch(config-if)#ip address 10.0.0.2 255.0.0.0

Switch(config-if)#no shut

Switch(config-if)#exit

Switch(config)#end

Switch#
```

[3]

CLI SWITCH:



5. RESULT:

Analysis of the Inter-Vlan Communication Methods

Metric	Old Legacy	Router-On-A-Stick	Multilayer Switch
No. of Physical Interfaces	One Physical Interface per VLAN	One Physical Interface for many VLANs	One Physical Interface per VLAN
Port Mode	Access Mode	Trunk Mode	Access Mode
Cost	More Expensive	Less Expensive	Cost Effective
Admin Complexity	Less Complex Configuration	Complex Configuration	Less Complex Configuration
Components Required	Router, Switch and End Devices	Router, Switch and End Devices	Multilayer Switch and End Devices
Application	Used mostly in smaller networks example LAN.	Used where more number of vlans are to be used.	Mostly used in WAN connections

5. Comment on the output of each method:

OLD LEGACY:

The first solution of inter-VLAN routing is known as legacy inter-VLAN routing.

One of the main disadvantages of legacy inter-VLAN routing is that it requires multiple physical interfaces on both the switch and the router.

Router On Stick:

Router-on-a-stick only requires the configuration of one single physical interface on the router in order to route traffic between multiple VLANs.

The router interface is configured to operate as a trunk link between the router and the switch.

Multilayer Switching:

One of the main advantages of using multi-layer switching is the ability to scale at a rapid pace. The above mentioned inter-VLAN routing are limited by the number of the ports on the network device. However, Layer 3 switches are not subjected to the same limitations.

The second benefit of Layer 3 switching is that all routing is performed internally and never leaves the switch. This avoids the some of the limitations of using a single trunk link such as only being able to accommodate a limited amount of traffic on one physical interface.[5]

6. OUTPUT:

Connection establishment and trace route of the methods.

1)Old-Legacy Connection Establishment:

Command Prompt

```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\WC-NEW-LAB>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:
Reply from 20.20.20.2: bytes=32 time<1ms TTL=127
Reply from 20.20.20.2: bytes=32 time<1ms TTL=127
Reply from 20.20.20.2: bytes=32 time=1ms TTL=127
Reply from 20.20.20.2: bytes=32 time<1ms TTL=127

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\WC-NEW-LAB>tracert 20.20.20.2

Tracing route to 20.20.20.2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  10.10.10.1
  2     1 ms     1 ms    <1 ms  20.20.20.2

Trace complete.

C:\Users\WC-NEW-LAB>
```

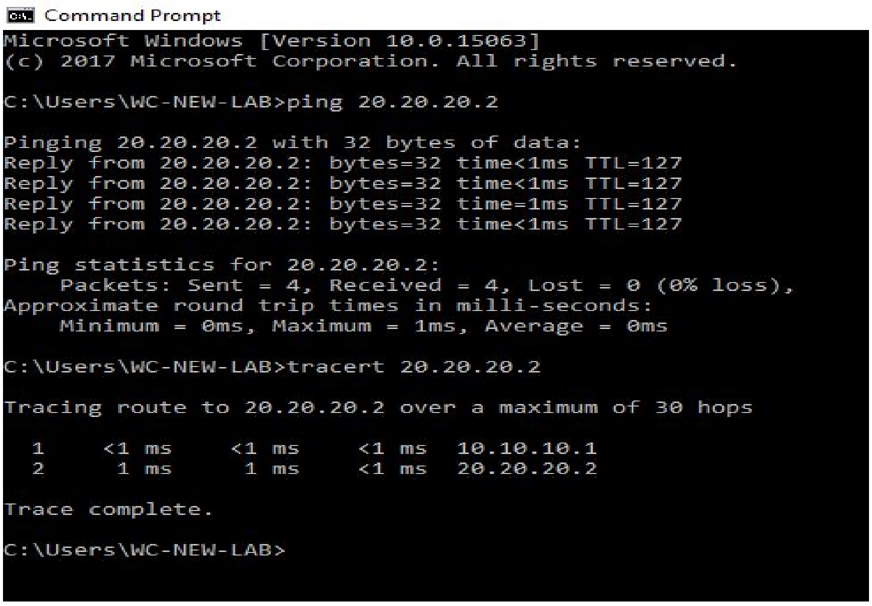
2)Router on Stick Connection Establishment:

Command Prompt

```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\WC-NEW-LAB>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:
Reply from 20.20.20.2: bytes=32 time<1ms TTL=127
Reply from 20.20.20.2: bytes=32 time<1ms TTL=127
Reply from 20.20.20.2: bytes=32 time=1ms TTL=127
Reply from 20.20.20.2: bytes=32 time<1ms TTL=127

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\WC-NEW-LAB>tracert 20.20.20.2

Tracing route to 20.20.20.2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  10.10.10.1
  2     1 ms     1 ms    <1 ms  20.20.20.2

Trace complete.

C:\Users\WC-NEW-LAB>
```

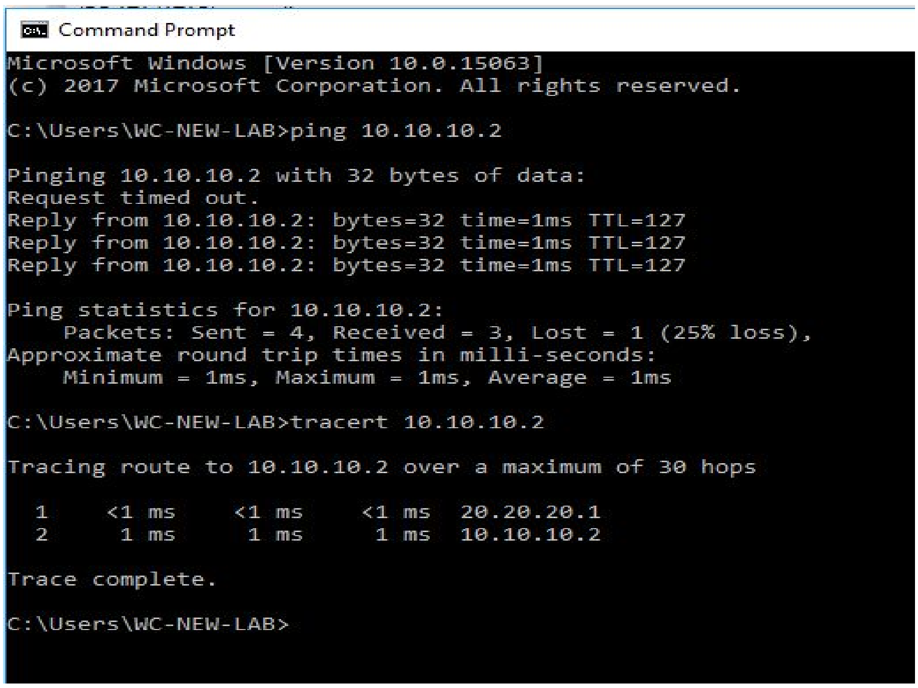
2) ROUTER ON STICK:

OUTPUT PC 1



```
Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\WC-NEW-LAB>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:
Reply from 20.20.20.2: bytes=32 time<1ms TTL=127
Reply from 20.20.20.2: bytes=32 time<1ms TTL=127
Reply from 20.20.20.2: bytes=32 time=1ms TTL=127
Reply from 20.20.20.2: bytes=32 time<1ms TTL=127

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\WC-NEW-LAB>tracert 20.20.20.2

Tracing route to 20.20.20.2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  10.10.10.1
  2     1 ms     1 ms    <1 ms  20.20.20.2

Trace complete.

C:\Users\WC-NEW-LAB>
```

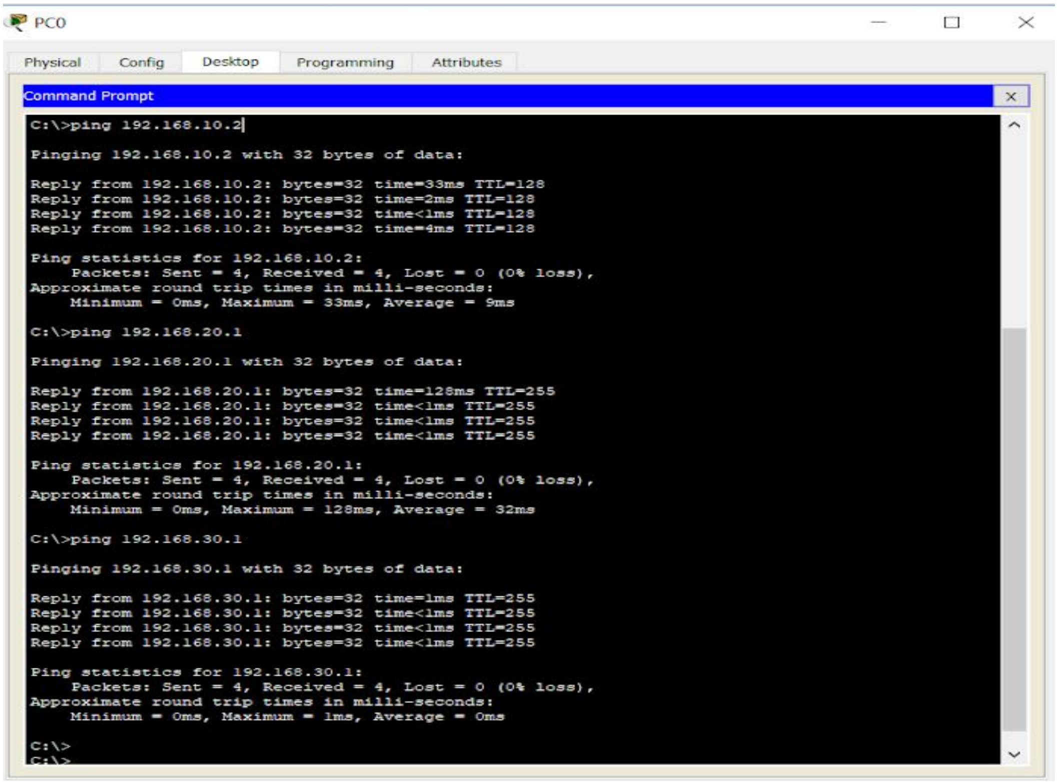
OUTPUT PC2:



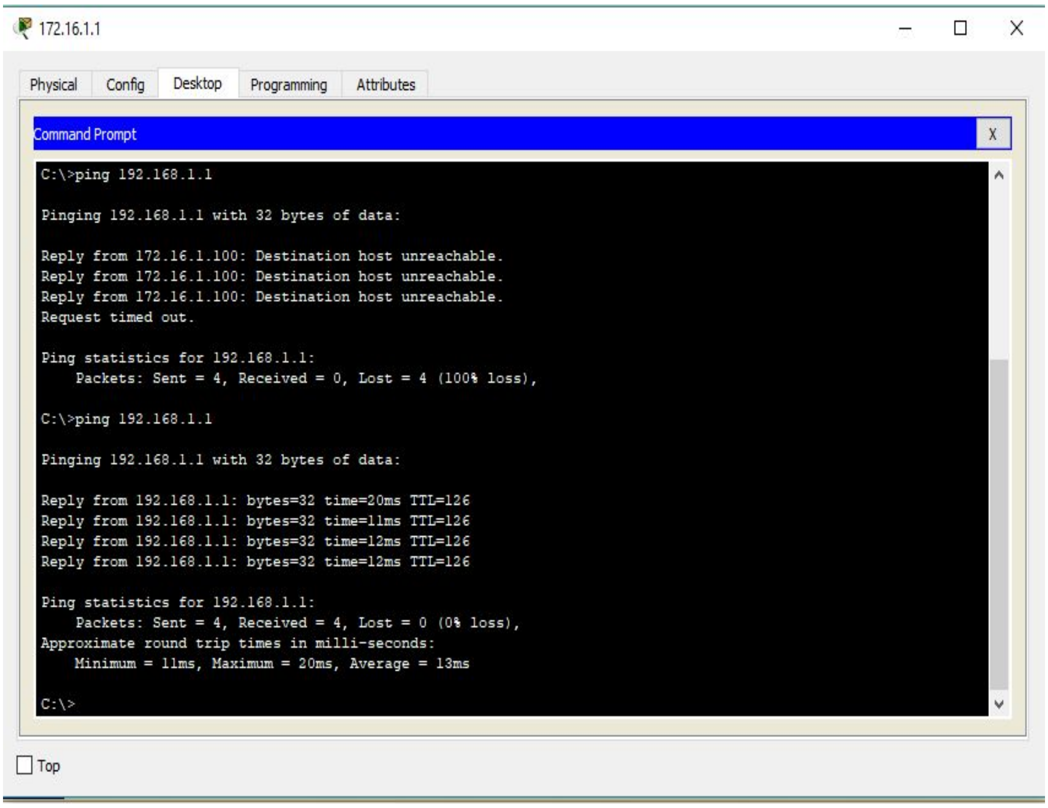
```
Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\WC-NEW-LAB>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:
Request timed out.
Reply from 10.10.10.2: bytes=32 time=1ms TTL=127
Reply from 10.10.10.2: bytes=32 time=1ms TTL=127
Reply from 10.10.10.2: bytes=32 time=1ms TTL=127

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\WC-NEW-LAB>tracert 10.10.10.2

Tracing route to 10.10.10.2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  20.20.20.1
  2     1 ms     1 ms     1 ms  10.10.10.2

Trace complete.

C:\Users\WC-NEW-LAB>
```

3) MULTILAYER SWITCH OUTPUT

A)


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>ping 192.168.10.2
Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=33ms TTL=128
Reply from 192.168.10.2: bytes=32 time=2ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time=4ms TTL=128
Ping statistics for 192.168.10.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 33ms, Average = 9ms
C:\>ping 192.168.20.1
Pinging 192.168.20.1 with 32 bytes of data:
Reply from 192.168.20.1: bytes=32 time=128ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.20.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 128ms, Average = 32ms
C:\>ping 192.168.30.1
Pinging 192.168.30.1 with 32 bytes of data:
Reply from 192.168.30.1: bytes=32 time=1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.30.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
C:\>

B)


172.16.1.1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 172.16.1.100: Destination host unreachable.
Reply from 172.16.1.100: Destination host unreachable.
Reply from 172.16.1.100: Destination host unreachable.
Request timed out.
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=20ms TTL=126
Reply from 192.168.1.1: bytes=32 time=11ms TTL=126
Reply from 192.168.1.1: bytes=32 time=12ms TTL=126
Reply from 192.168.1.1: bytes=32 time=12ms TTL=126
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 11ms, Maximum = 20ms, Average = 13ms
C:\>
Top

7. CONCLUSION:

Implemented Old Legacy Routing, Router on Stick, Multilayer Switch on Packet Tracer and verified the Old Legacy and Router On Stick by implementing them practically on hardware using Cisco Switches and Routers.

In old legacy method several ports are used on the switch in access mode and for each Vlan a separate physical interface is required .

The drawback of old Legacy method is removed in Router on Stick method where only one port (Trunk) is used for several Vlans.

But in both the above mentioned methods we require more hardware devices. This increases the cost and complexity of network.

Thus we use another method which is multilayer switching. This method focuses on using only one switch which can be used as a switch and as a router.

8.FUTURE SCOPE: A Network Architecture can be build Using Inter-VLAN Routing and Secure Campus Area Network (CAN).Redundant link configuration can be used[6].

9.REFERENCES:

[1].https://searchnetworking.techtarget.com/answer/What-is-interVLAN-routing

[2].https://www.youtube.com/watch?v=GvYfi-mmtmA&t=155s

[3]https://www.cisco.com/c/en/us/td/docs/routers/access/1800/1841/hardware/quick/guide/1800qsg.pdf

[4]https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-s-series-switches/data_sheet_c78-726680.pdf

[5]https://www.researchgate.net/publication/329033784_The_Proposed_Roles_of_VLAN_and_Inter-VLAN_Routing_in_Effective_Distribution_of_Network_Services_in_Ebonyi_State_University

[6]https://www.ijcseonline.org/pub_paper/18-IJCSE-03028.pdf