Lab-6: Basic CLI command, VLAN configuration and troubleshooting

Objective:

To provide hands-on experience in configuring switches using Cisco Packet Tracer, focusing on CLI commands, VLAN configuration, and troubleshooting.

CLI Commands:

In global configuration:

Create vlan:

```
vlan 10                          # Creating vlan and set its id
name room416                     # Set name for the Vlan
ex                               # Exit Vlan interface
```

Connect interface with vlan:

```
interface FastEthernet0/1        # Enter interface configuration

switchport mode access           # Set the interface to access mode

switchport access vlan 10        # Assign VLAN 10

no shutdown                      # Enable the interface

exit                             # Exit interface configuration mode
```

Input:

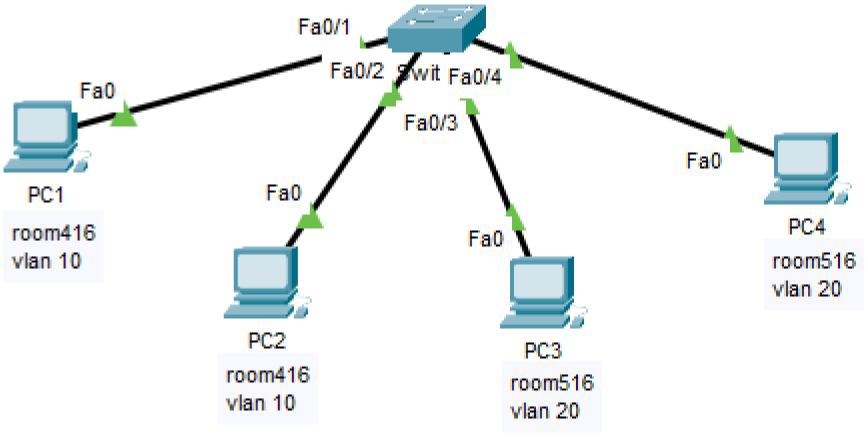
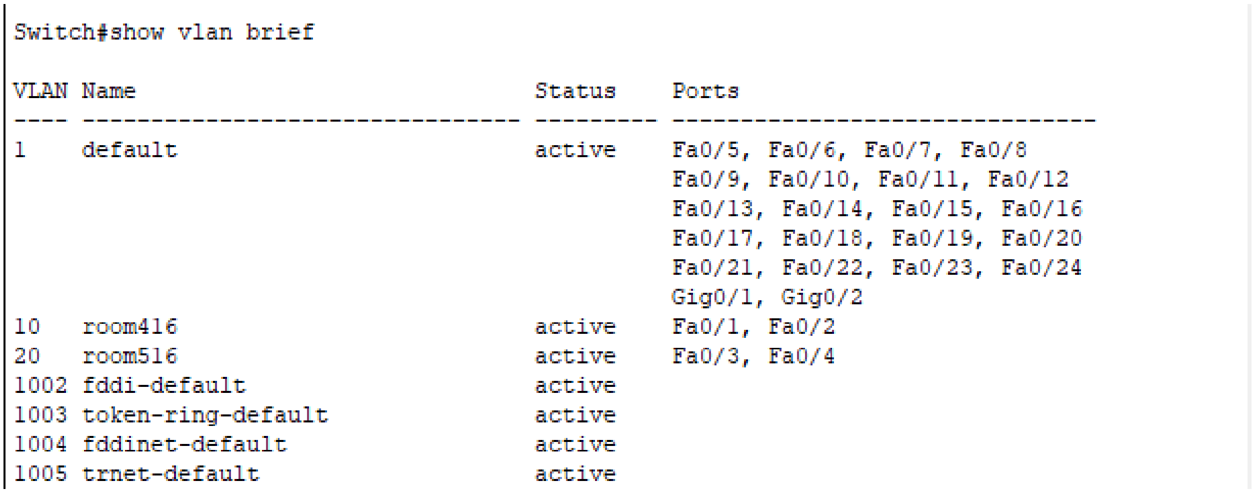


Fig: Assigning different vlan to pcs

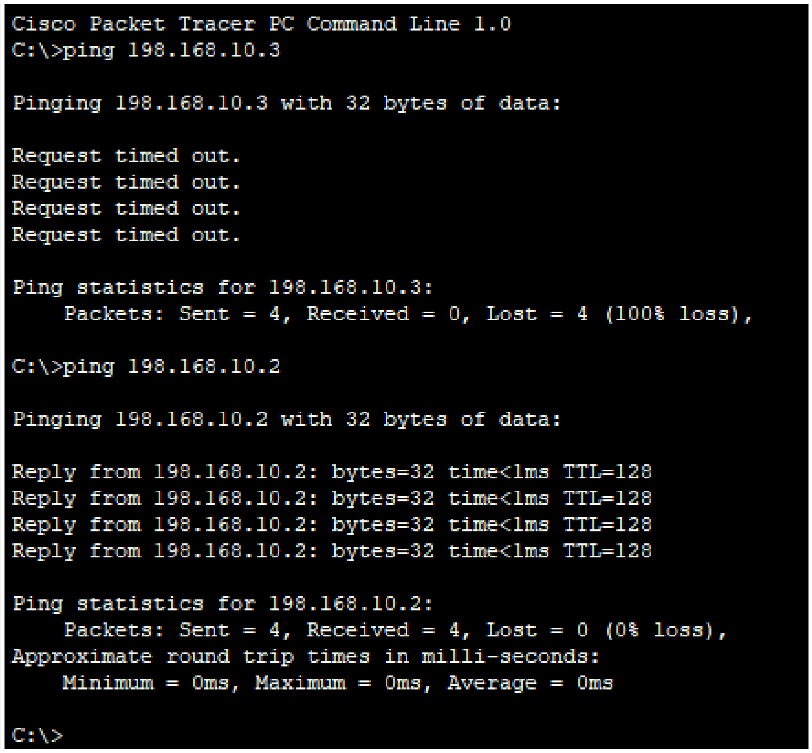
Output:



```
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
                                                Gig0/1, Gig0/2
10   room416                          active    Fa0/1, Fa0/2
20   room516                          active    Fa0/3, Fa0/4
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Fig: Vlan brief



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 198.168.10.3

Pinging 198.168.10.3 with 32 bytes of data:

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

Ping statistics for 198.168.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 198.168.10.2

Pinging 198.168.10.2 with 32 bytes of data:

Reply from 198.168.10.2: bytes=32 time<1ms TTL=128
Reply from 198.168.10.2: bytes=32 time<1ms TTL=128
Reply from 198.168.10.2: bytes=32 time<1ms TTL=128
Reply from 198.168.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 198.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fig: ping send from pc1 to pc3 and pc2

Lab-7: Basic CLI command, Interface configuration and Routing protocol (Static routing, RIP, OSPF)

Objective:

To gain hands-on experience by configuring routers using Cisco Packet Tracer, focusing on CLI commands for basic setup, interface configuration, and routing protocols.

Section A: Static routing

CLI command:

```
ip route 20.0.0.0 255.0.0.0 40.40.40.2
```

Input:

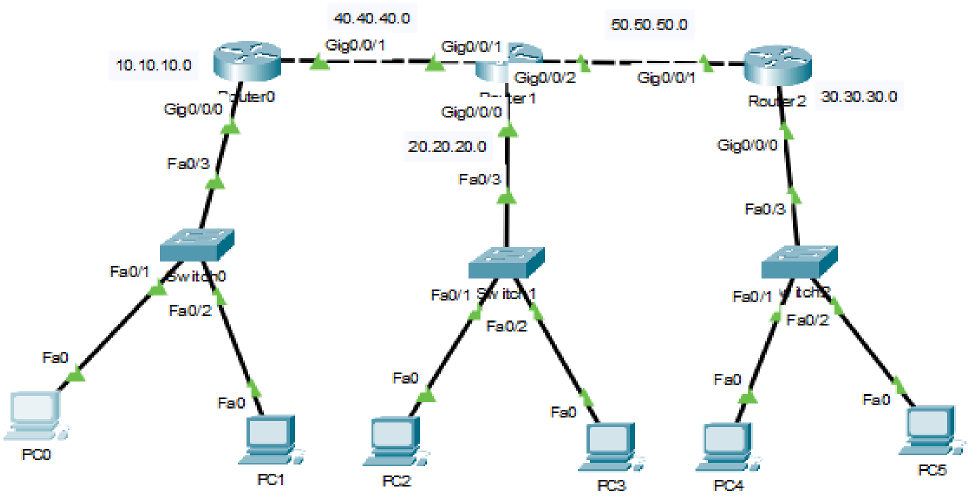
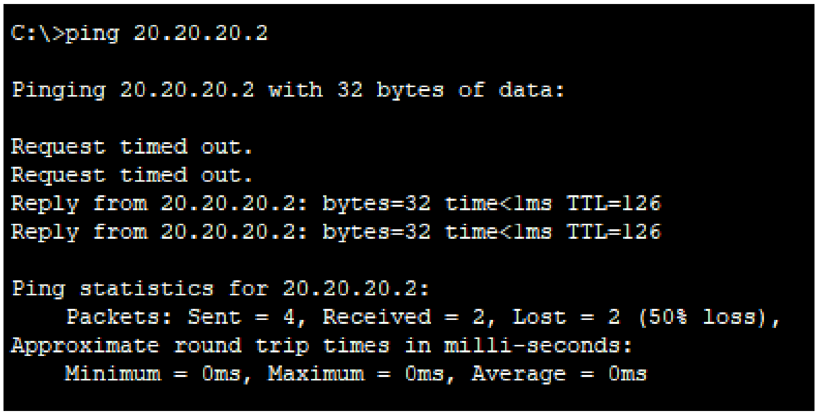


Fig: Static routing connection

Output:



```
C:\>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 20.20.20.2: bytes=32 time<1ms TTL=126
Reply from 20.20.20.2: bytes=32 time<1ms TTL=126

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fig: sending ping from pc0 to pc3

Section B: RIP routing

CLI command:

```
router rip
network 10.0.0.0
network 20.0.0.0
```

Input:

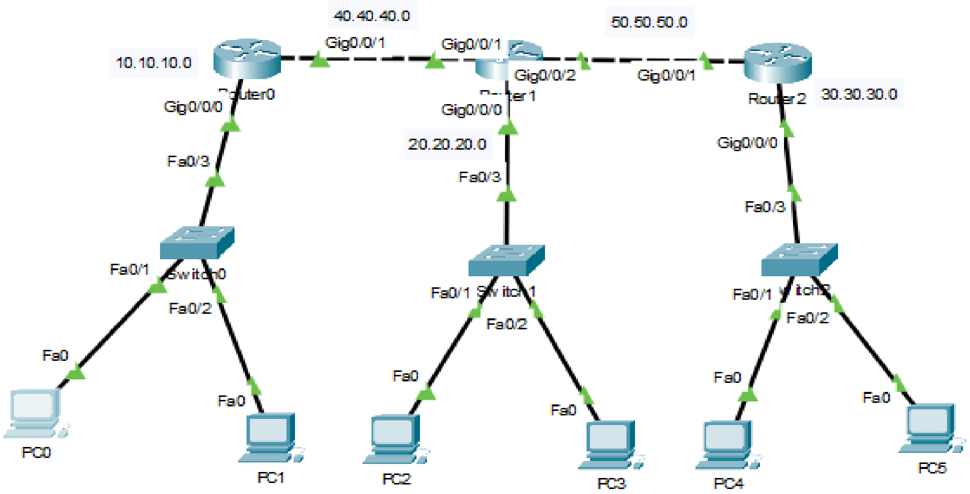
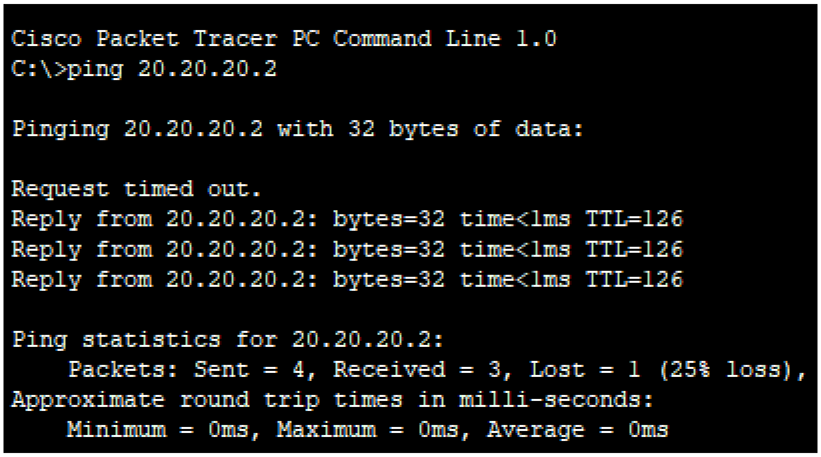


Fig: RIP routing connection

Output:



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

Request timed out.
Reply from 20.20.20.2: bytes=32 time<1ms TTL=126
Reply from 20.20.20.2: bytes=32 time<1ms TTL=126
Reply from 20.20.20.2: bytes=32 time<1ms TTL=126

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fig: sending ping from pc1 to pc4

Lab-8: standard and extended Access control list

Objective:

The objective of this lab is to study the basics of Standard and Extended Access Control Lists (ACLs) and configure them in different network scenarios using Cisco Packet Tracer.

Introduction to ACLs:

Access Control Lists (ACLs) are used to filter network traffic based on a set of rules. They can be applied to routers to control which packets are allowed or denied through an interface. ACLs operate in sequential order, where each packet is compared to the ACL statements in order, until a match is found or the implicit "deny all" rule applies.

Purpose of ACLs:

Limit network traffic to improve performance

Enhance security by controlling access to network resources

Control routing updates

Filter packets for debugging

Types of ACLs:

Standard ACL:

Criteria for filtering: Based only on the source IP address.

ACL Number Range: 1-99, 1300-1999 (Expanded range).

Usage: Typically used to block or allow traffic from specific hosts or networks.

Extended ACL:

Criteria for filtering: Based on both source and destination IP addresses, protocols (e.g., TCP, UDP, ICMP), and ports.

ACL Number Range: 100-199, 2000-2699 (Expanded range).

Usage: More specific filtering that can be used to block/allow specific services, applications, and traffic between networks.

A. Standard ACL:

CLI command

access-list 10 deny host 192.168.20.2
access-list 10 permit any
interface GigabitEthernet0/0/0
 ip access-group 10 in

Input:

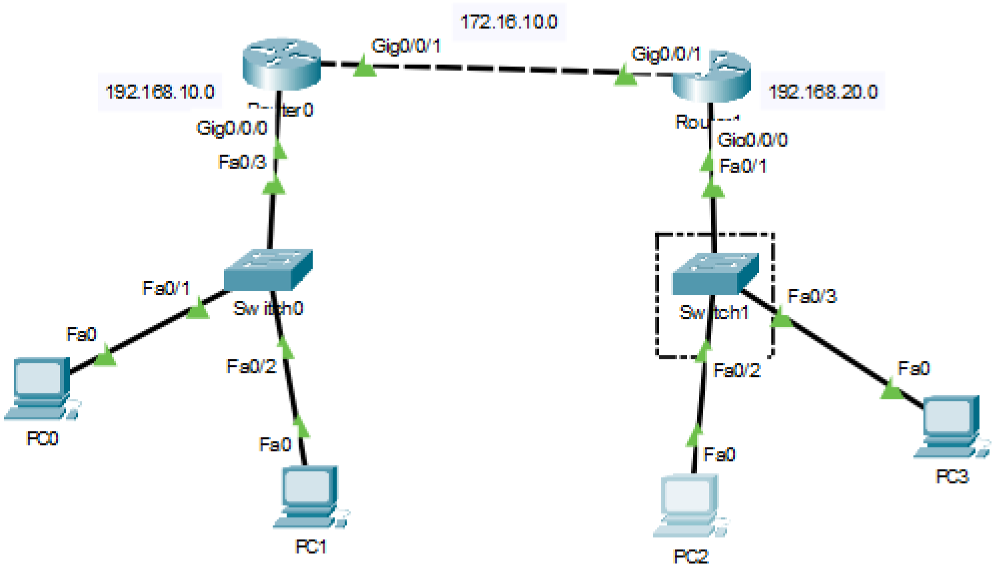
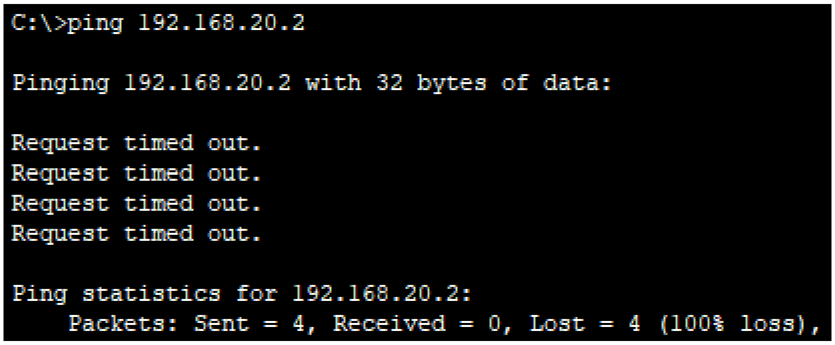


Fig: standard ACL

Output:



```
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

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

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fig: sending ping from pc0 to pc2

Lab-9: VLAN trunk protocol (VTP)

Objective:

The objective of this lab is to study the basic switch and router configuration commands, understand VLANs, trunks, and VLAN Trunking Protocol (VTP), and learn how to configure VLANs and VTP on Cisco switches using Cisco Packet Tracer.

Theory:

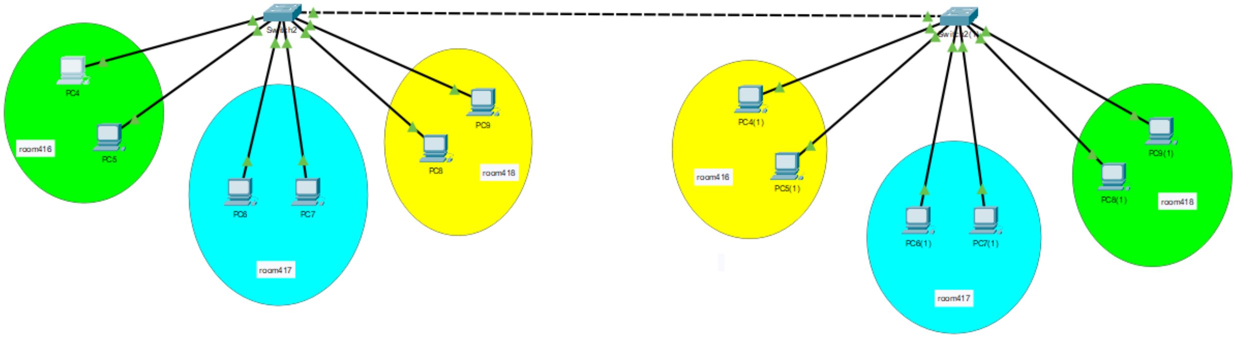
VTP is a Cisco proprietary protocol that helps manage VLANs across multiple switches by sharing VLAN information. There are three modes in VTP:

Server Mode: Switches can create, modify, and delete VLANs.

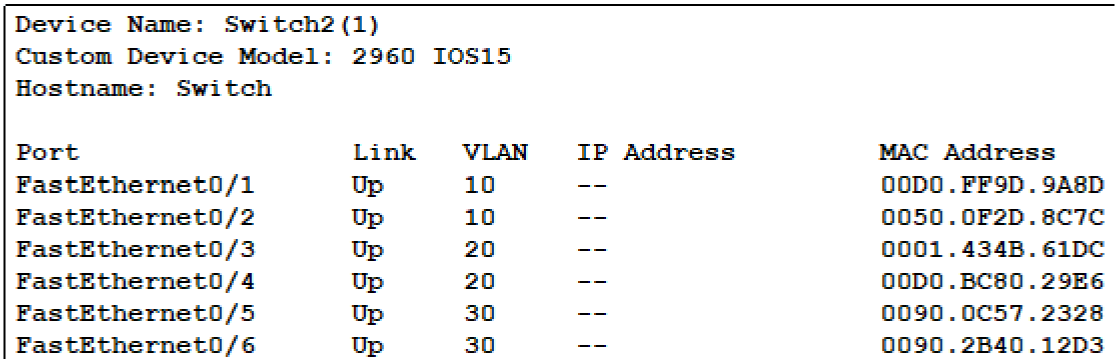
Client Mode: Switches receive VLAN information from VTP servers but cannot make changes.

Transparent Mode: Switches pass VLAN information but do not participate in VTP.

Input:



Output:



```
Device Name: Switch2(1)
Custom Device Model: 2960 IOS15
Hostname: Switch

Port                    Link    VLAN    IP Address            MAC Address
FastEthernet0/1         Up      10      --                    00D0.FF9D.9A8D
FastEthernet0/2         Up      10      --                    0050.0F2D.8C7C
FastEthernet0/3         Up      20      --                    0001.434B.61DC
FastEthernet0/4         Up      20      --                    00D0.BC80.29E6
FastEthernet0/5         Up      30      --                    0090.0C57.2328
FastEthernet0/6         Up      30      --                    0090.2B40.12D3
```

Lab-10: VLAN (Virtual Local AreaNetwork) with VTP and STP

Objective:

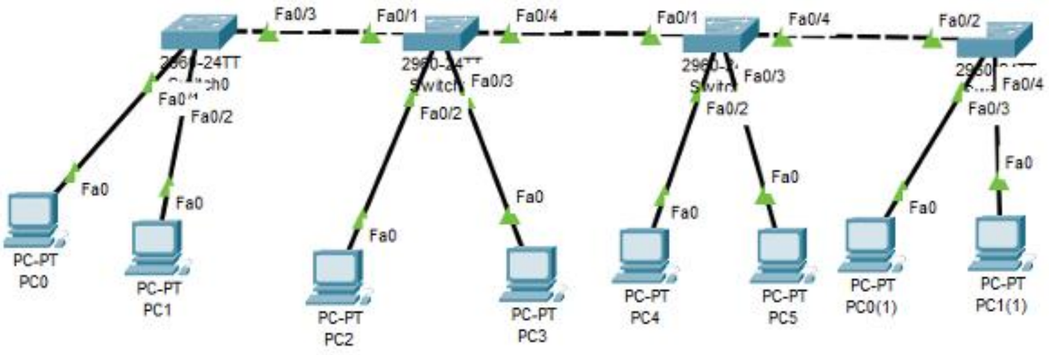
The objectives of this lab are:

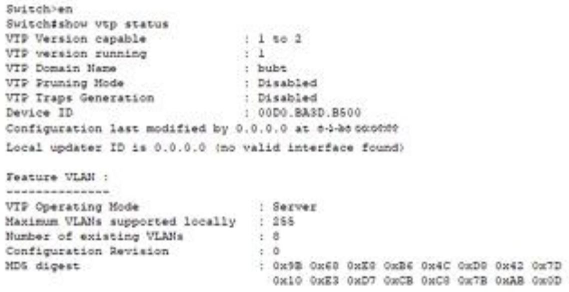
- To configure VLANs across multiple switches
- To implement VTP for VLAN synchronization
- To observe and verify Spanning Tree Protocol (STP) operations
- To analyze loop prevention in switched networks
- To test connectivity and switching behavior in redundant topologies

Theory:

A VLAN enables segmentation of a physical LAN into separate logical broadcast domains, improving security, efficiency, and network management. VLANs allow users to be grouped logically even if not physically adjacent

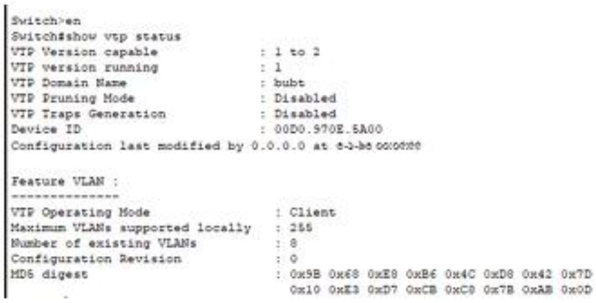
Input/Output:





```
Switch>en
Switch#show vtp status
VTP Version capable              : 1 to 2
VTP version running              : 1
VTP Domain Name                  : bubt
VTP Pruning Mode                 : Disabled
VTP Traps Generation             : Disabled
Device ID                        : 00D0.BA3D.B500
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
--------------
VTP Operating Mode                 : Server
Maximum VLANs supported locally    : 255
Number of existing VLANs           : 8
Configuration Revision             : 0
MD5 digest                         : 0x9B 0x68 0xE8 0xB6 0x4C 0xD8 0x42 0x7D
                                     0x10 0xE3 0xD7 0xCB 0xC8 0x7B 0xAB 0x0D
```



```
Switch>en
Switch#show vtp status
VTP Version capable              : 1 to 2
VTP version running              : 1
VTP Domain Name                  : bubt
VTP Pruning Mode                 : Disabled
VTP Traps Generation             : Disabled
Device ID                        : 00D0.970E.5A00
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN :
--------------
VTP Operating Mode                 : Client
Maximum VLANs supported locally    : 255
Number of existing VLANs           : 8
Configuration Revision             : 0
MD5 digest                         : 0x9B 0x68 0xE8 0xB6 0x4C 0xD8 0x42 0x7D
                                     0x10 0xE3 0xD7 0xCB 0xC8 0x7B 0xAB 0x0D
```

Lab-11: Wireless Router Configuration

Objective:

The objective of this lab is to configure a wireless router, secure wireless networks using WEP, WPA, and WPA2, establish wireless connections, and configure a wireless access point (AP) using Cisco Packet Tracer.

Theory:

Wireless networks provide connectivity without physical cabling, enabling mobility and flexible deployment. Wireless routers act as central devices that distribute network access using radio frequency signals. Securing wireless networks is essential to prevent unauthorized access and data interception.

A. WEP (Wired Equivalent Privacy)

- First-generation wireless security
- Uses static keys
- Considered weak and easily cracked

B. WPA (Wi-Fi Protected Access)

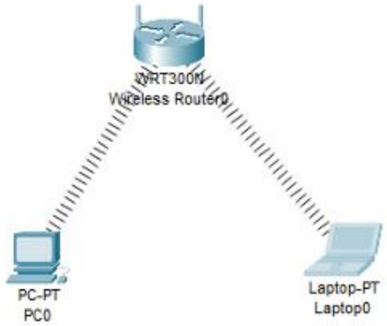
- Improved security over WEP
- Uses TKIP encryption

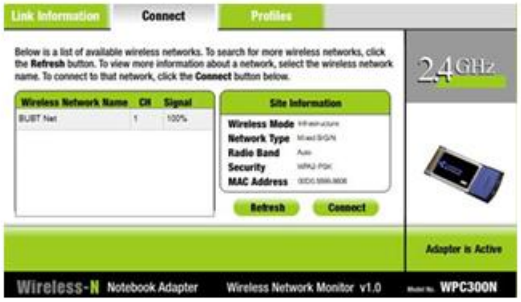
C. WPA2

- Most secure and widely used
- Uses AES encryption

These protocols secure wireless communication and prevent unauthorized access.

Input/Output:





Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
BUBT Net	1	100%

Site Information

Wireless Mode Infrastructure
Network Type Mixed B/G/N
Radio Band Auto
Security WPA2-PSK
MAC Address [illegible]

Adapter is Active

Wireless-N Notebook Adapter Wireless Network Monitor v1.0 Model No. WPC300N