Module 7 and 8 Assignment solutions

Sri Gnana Saravan.N

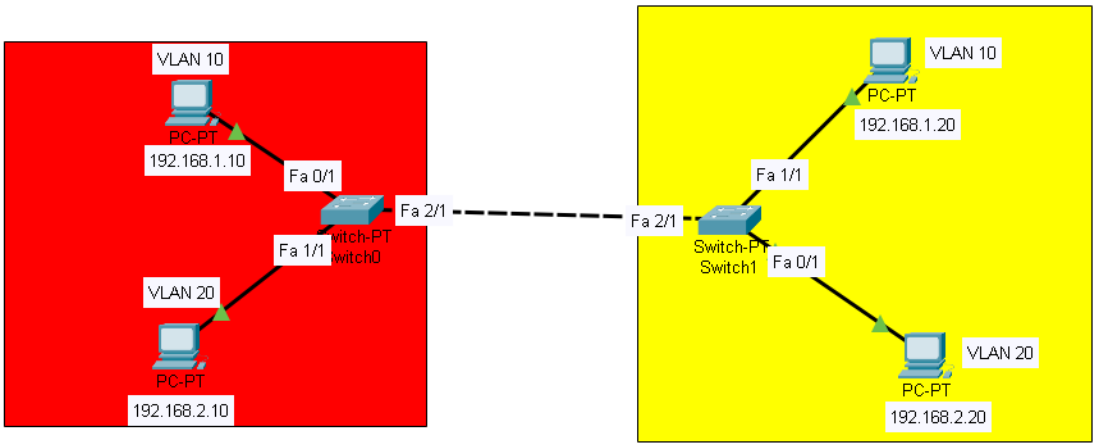
VIT Chennai

1. Use Cisco packet tracer for the below

Set up trunk ports between switches and try ping between different VLANs.

Solution:

Basic VLAN Setup:



Initial VLAN Setting in Switch:

```
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa1/1, Fa3/1, Fa4/1
                                                 Fa5/1
40   vlan_native_int                   active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Here all the ports are mapped to the VLAN 1 interface as default.

Creating new VLAN Interfaces:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name vlan_int1
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name vlan_int2
Switch(config-vlan)#
Switch(config-vlan)#exit
```

Configuring each port to the respective VLAN Interface:

```
Switch(config)#int f1/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#exit
```

After configuring the ports to the respective vlan:

```
Switch#show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa3/1, Fa4/1, Fa5/1
10   vlan_int1                           active    Fa1/1
20   vlan_int2                           active    Fa0/1
40   vlan_native_int                     active
```

Here the Other unused ports are mapped to the VLAN1 interface.We need to change the state of the ports down state using shut command and we need to assign all these ports to separate vlan.

```
Switch(config)#vlan 50
Switch(config-vlan)#name BLACKHOLE
Switch(config-vlan)#exit
Switch(config)#int range f3/1,f4/1,f5/1
Switch(config-if-range)#shut
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 50
Switch(config-if-range)#
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active
10   vlan_int1                           active    Fa1/1
20   vlan_int2                           active    Fa0/1
40   vlan_native_int                     active
50   BLACKHOLE                           active    Fa3/1, Fa4/1, Fa5/1
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
Switch#
```

You can see that,now there is no ports are assigned to the vlan1 interface.Here why we are assigning separate VLANS to every port?It is because for the security reasons.If the hacker are trying to access to the system files and it can be easily accessed if all the ports are assigned to the same network(Same VLAN Interface).So if we try to separate these system to different VLAN(different networks) then it may be tough to access the all the system files.

Pinging from PC1 to PC3(Connected across different switch but same VLAN):

```
C:\>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

Reply from 192.168.1.20: bytes=32 time=51ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 51ms, Average = 12ms
```

Pinging to the PC2 that is connected to the same switch:

```
C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

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

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Here you can see that even though the PC2 is connected to the same switch as PC1,ping fails.It is because the two different PC's are in the different VLAN(different broadcast domain).

2. Change the native VLAN on a trunk port. Test for VLAN mismatches and troubleshoot.

Solution:

Native VLAN Mismatch:

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa3/1, Fa4/1, Fa5/1
10   vlan_int1                         active    Fa0/1
20   vlan_int2                         active    Fa1/1
30   vlan_trunk_int                    active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet2/1 (30), with Switch
FastEthernet2/1 (1).
```

Here the native VLAN Problem occurs since the port that is connected to other switch have connected to the different VLAN.

Troubleshoot:

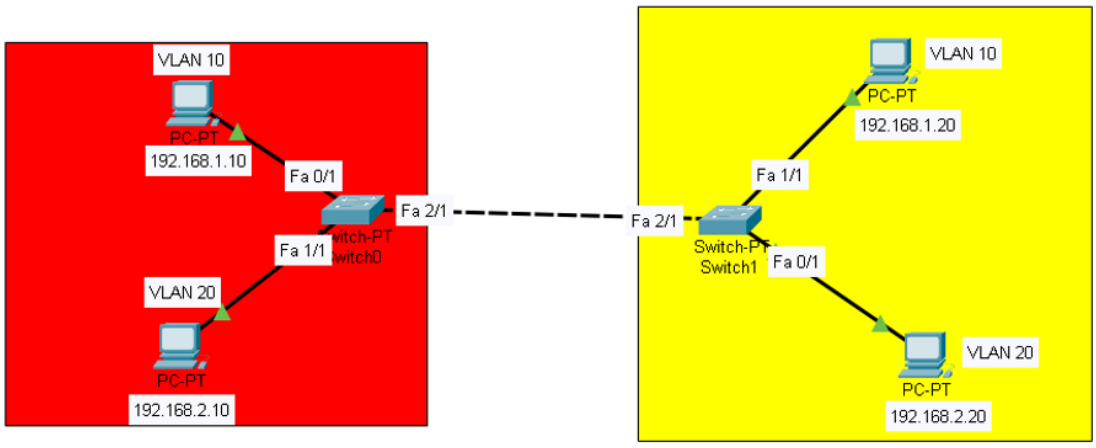
Both the ports of the native VLAN should be connected to the same VLAN(same network).

```
Switch(config-vlan)#nam
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet2/1 (1), with Switch
FastEthernet2/1 (40).

% Incomplete command.
Switch(config-vlan)#name vlan_native_int
Switch(config-vlan)#exit
Switch(config)#int f2/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 40
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#exit
```

So the both the ports are connected to the same VLAN.

3. You configured VLANs 10 and 20 on your switch and assigned ports to each VLAN.However, devices in VLAN 10 cannot communicate with devices in VLAN 20. Troubleshoot the issue.

Solution:

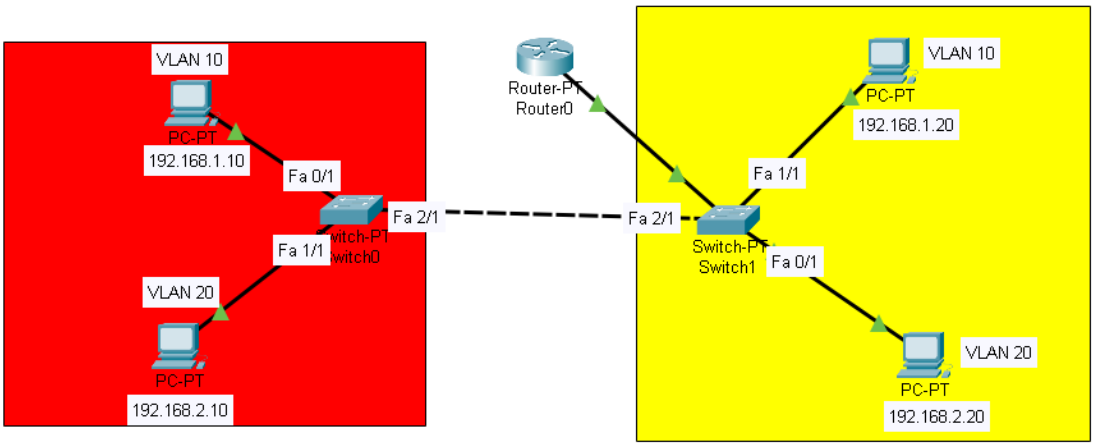


From the above set up,VLAN 10 and VLAN 20 are separate networks,So only using the switch we can’t able to communicate to the different network because switch is layer 2 device.

Router is the device which can separate these networks and able to communicate to the different networks which will route the packets to destination ip.For any device to communicate over LAN or WAN,it need ip address,mac address,subnet mask,default gateway.Switch only keeps its mac address table which will not know about the destination ip.

Troubleshooting: Inter LAN Routing:

Connecting the switch to router will support the Inter LAN communication.This is called Inter LAN Routing.



Ensure that IEEE802.1Q is enabled in router.It basically tells to use the tagged vlan information to transmit data across ethernet.Add the IP Address for the sub interface

```
Router(config)#int f0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(conint f0/0.10iniip add 192.168.1.1 255.255.255.0
Router(config-subif)#exit
Router(config)#iip add 192encapsulation dot1Q 10encapsulatioip add 192.168.1.1 255.255.255.0ip add
192.168.2.1 255.255.255.0
```

Settings in Switch:

```
Switch(config)#int f3/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 40
Switch(config-if)#exit
Switch(config)#exit
```

Make sure that interface's state is up.Use no shut command to change the state to up.

```
C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

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

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>
C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.10: bytes=32 time=38ms TTL=127
Reply from 192.168.2.10: bytes=32 time<1ms TTL=127
Reply from 192.168.2.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 38ms, Average = 12ms
```

Now you can see that from 192.168.1.10 we can able to communicate to 192.168.2.10 which from different vlan.Router basically used that tagged vlan information to separate and route these packets to the respective vlans.

4. Configure a management VLAN and assign an IP address for remote access. Test SSH or Telnet access to the switch.

Solution:

Configuring a Management VLAN:

```
Switch(config)#vlan 100
Switch(config-vlan)#name MANAGEMENT
Switch(config-vlan)#exit
```

Assigning the Ethernet port 3 to the Management VLAN using switchport command and assign the IP to the port using ip address command.

```
Switch0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch0(config)#int f3/1
Switch0(config-if)#switchport mode access
Switch0(config-if)#switchport access vlan 50
Switch0(config-if)#exit
Switch0(config)#int f0/1
Switch0(config-if)#switchport mode access
Switch0(config-if)#switchport access vlan 100
Switch0(config-if)#exit
Switch0(config)#exit
Switch0#
%SYS-5-CONFIG_I: Configured from console by console

Switch0#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   vlan_int1                        active
20   vlan_int2                        active    Fa1/1
40   vlan_trunk_native                active
50   BLACKHOLE                        active    Fa3/1, Fa4/1, Fa5/1
100  MANAGEMENT                       active    Fa0/1
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch0#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet1/1        unassigned      YES manual up                    up
FastEthernet2/1        unassigned      YES manual up                    up
FastEthernet3/1        unassigned      YES manual administratively down down
FastEthernet4/1        unassigned      YES manual administratively down down
FastEthernet5/1        unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
Vlan100                192.168.1.50    YES manual up                    up
```

From PC1 through SSH connecting to the Switch remotely:

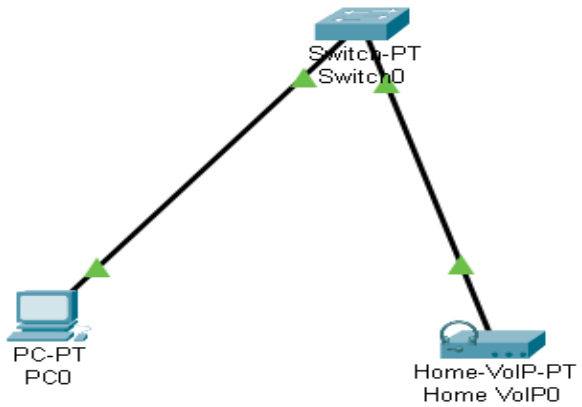
```
C:\>ssh saravan@192.168.10.10
Invalid Command.

C:\>ssh -l saravan 192.168.1.50

% Connection timed out; remote host not responding
C:\>ssh -l saravan 192.168.1.50

% Connection timed out; remote host not responding
C:\>ssh -l saravan 192.168.1.50

Password:
% Login invalid


Password:



Switch0#
Switch0#
Switch0#show vlan br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
10   vlan_int1                         active
20   vlan_int2                         active    Fa1/1
40   vlan_trunk_native                 active
50   BLACKHOLE                         active    Fa3/1, Fa4/1, Fa5/1
100  MANAGEMENT                        active    Fa0/1
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

A Management VLAN is a dedicated VLAN used to remotely manage a switch or network device using protocols like SSH, Telnet, SNMP, or HTTP/HTTPS. It allows network administrators to securely access and configure the switch without interfering with normal data traffic.

5. You have a Cisco switch and a VoIP phone that needs to be placed in a voice VLAN (VLAN 20). The data for the PC should remain in a separate VLAN (VLAN 10).Configure the switch port to support both voice and data traffic.

Solution:

Configuring the switch port for both data and voice using two separate VLANs



```
Switch(config)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
Switch(config-if)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name VOICE_DATA
Switch(config-vlan)#vlan 10
Switch(config-vlan)#name DATA
Switch(config-vlan)#exit
Switch(config)#int f1/1
Switch(config-if)#switchport mode ?
  access   Set trunking mode to ACCESS unconditionally
  dynamic  Set trunking mode to dynamically negotiate access or trunk mode
  trunk    Set trunking mode to TRUNK unconditionally
Switch(config-if)#switchport mode
% Incomplete command.
Switch(config-if)#switchport voice vlan 20
Switch(config-if)#mls qos trust cos
```

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/1, Fa2/1, Fa3/1, Fa4/1
                                                Fa5/1
10   DATA                             active    Fa0/1
20   VOICE_DATA                       active    Fa1/1
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#show mls qos interface fa1/1
FastEthernet1/1
trust state: trust cos
trusted mode: trust cos
COS override: dis
default COS: 0
pass-through: none
trust device: none
```

6. Try Test-Connection and nslookup commands for below websites

www.google.com

www.facebook.com

www.amazon.com

www.github.com

vwwv.cisco.com

Solution:

Nslookup helps to troubleshoot DNS Related issues by providing information how domain name is resolved into ip address.

```
C:\Users\Priya>nslookup www.google.com
Server:  reliance.reliance
Address:  2405:201:e057:a913::c0a8:1d01

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4002:816::2004
          142.250.192.164


C:\Users\Priya>nslookup www.facebook.com
Server:  reliance.reliance
Address:  2405:201:e057:a913::c0a8:1d01

Non-authoritative answer:
Name:    star-mini.c10r.facebook.com
Addresses:  2a03:2880:f349:1:face:b00c:0:25de
          57.144.156.1
Aliases:  www.facebook.com


C:\Users\Priya>nslookup www.amazon.com
Server:  reliance.reliance
Address:  2405:201:e057:a913::c0a8:1d01

Non-authoritative answer:
Name:    d3ag4hukkh62yn.cloudfront.net
Addresses:  2600:9000:2241:4c00:7:49a5:5fd4:b121
          2600:9000:2241:d400:7:49a5:5fd4:b121
          2600:9000:2241:d200:7:49a5:5fd4:b121
          2600:9000:2241:ca00:7:49a5:5fd4:b121
          2600:9000:2241:fc00:7:49a5:5fd4:b121
          2600:9000:2241:8200:7:49a5:5fd4:b121
          2600:9000:2241:7c00:7:49a5:5fd4:b121
          2600:9000:2241:b000:7:49a5:5fd4:b121
          18.67.156.60
Aliases:  www.amazon.com
          tp.47cf2c8c9-frontier.amazon.com
```

7.Explore traceroute/tracert for different websites eg:google.com and analyse the parameters in the output and explore different options for traceroute command?

Solution:

It will tell us how many hops it takes to reach the server or destination ip.Intuitively it will tell how many network devices are in between the source and destination.

```
C:\Users\Priya>tracert www.google.com

Tracing route to www.google.com [2404:6800:4002:82f::2004]
over a maximum of 30 hops:

  1     5 ms     3 ms     2 ms  2405:201:e057:a913:c6e5:32ff:feb6:4c01
  2     *        *        *     Request timed out.
  3     7 ms     6 ms     6 ms  2405:203:400:100:172:31:0:144
  4     *        *        *     Request timed out.
  5    10 ms     5 ms     7 ms  2405:200:80c:3168:61::5
  6     *        *        *     Request timed out.
  7     9 ms     9 ms     7 ms  2405:200:801:900::1292
  8     *        *        *     Request timed out.
  9    24 ms     8 ms    11 ms  2001:4860:1:1::16a
 10    10 ms    11 ms     6 ms  2001:4860:1:1::16a
 11    11 ms     *        *     2404:6800:8202:40::1
 12     *        *       12 ms  2001:4860:0:1::1394
 13     *       10 ms     *     2001:4860:0:1::8824
 14    47 ms     *       45 ms  2001:4860::9:4001:67bc
 15    45 ms     *       47 ms  2001:4860:0:1::77d1
 16    46 ms    45 ms    42 ms  2001:4860:0:1::5e49
 17    45 ms    44 ms    43 ms  del12s11-in-x04.1e100.net [2404:6800:4002:82f::2004]

Trace complete.
```

Here it tells that totally takes 17 hops to reach the destination. If you see high round-trip times it might indicate network congestion.

```
C:\Users\Priya>tracert -w 500 www.google.com

Tracing route to www.google.com [2404:6800:4002:813::2004]
over a maximum of 30 hops:

  1     5 ms     3 ms     2 ms  2405:201:e057:a913:c6e5:32ff:feb6:4c01
  2     *        *        *     Request timed out.
  3     9 ms     9 ms    10 ms  2405:203:400:100:172:31:0:144
  4     *        *        *     Request timed out.
  5    12 ms     7 ms     6 ms  2405:200:80c:3168:61::5
  6     *        *        *     Request timed out.
  7     7 ms     5 ms     6 ms  2405:200:801:900::1296
  8     *        *        *     Request timed out.
  9     9 ms     8 ms    10 ms  2001:4860:1:1::16a
 10    13 ms    10 ms     7 ms  2404:6800:8135::1
 11     *        *        *     Request timed out.
 12     9 ms     9 ms     8 ms  2001:4860:0:1::40bc
 13    45 ms    45 ms    50 ms  2001:4860::9:4001:67bd
 14     *        *        *     Request timed out.
 15    43 ms    41 ms    43 ms  2001:4860:0:1::25c9
 16    42 ms    41 ms    43 ms  del11s08-in-x04.1e100.net [2404:6800:4002:813::2004]

Trace complete.
```

-w tells the wait timeout for each reply.

-4 will force use IPv4 -6 will force use IPv6.

8.Implement ACLs to restrict traffic based on source and destination ports.Test rules by simulating legitimate and unauthorized traffic. Create an extended ACL to block specific applications, such as HTTP or FTP traffic.Test the ACL rules by attempting to access blocked services.

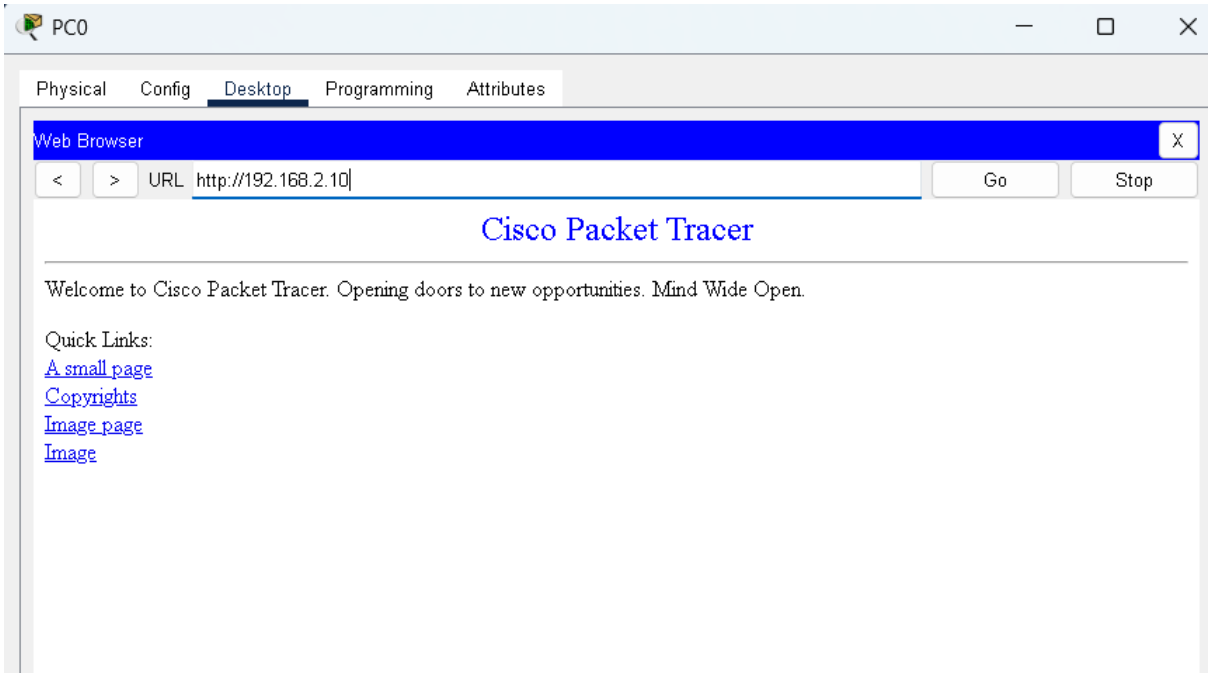
Solution:

Creating an extended ACL to block specific applications such as HTTP or FTP:

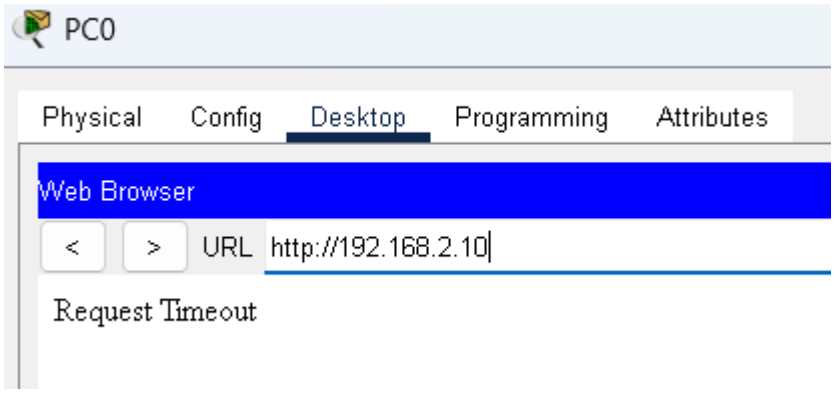
```
Router#
Router#show access-lists
Extended IP access list saravan_AL
    10 deny tcp host 192.168.1.10 host 192.168.2.10 eq www
    20 permit ip any any
```

```
C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.2.10: bytes=32 time=10ms TTL=127
Reply from 192.168.2.10: bytes=32 time<1ms TTL=127
Reply from 192.168.2.10: bytes=32 time<1ms TTL=127
Reply from 192.168.2.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

Before Blocking:



After blocking:

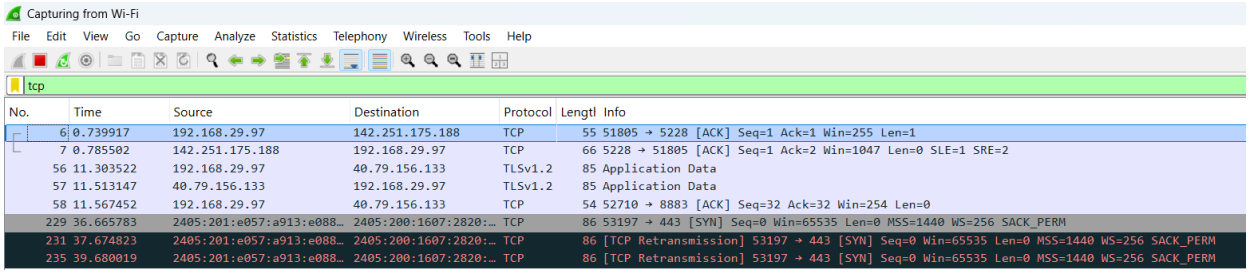


An Access Control List (ACL) is a set of rules used to control network traffic by filtering packets based on specific criteria. ACLs are used in networking devices like routers and switches to enhance security, restrict access to certain resources.

9. Use Wireshark to capture and analyze DNS, TCP, UDP traffic and packet header,packet flow, options and flags?

Solution:

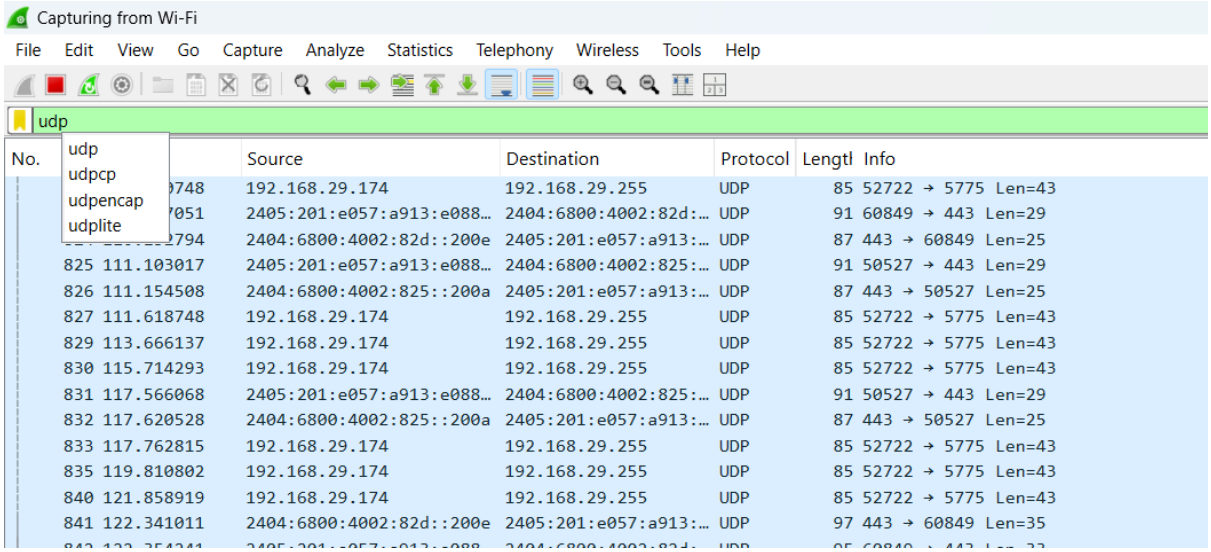
Using display filters like tcp,dns,udp to filter out the packets

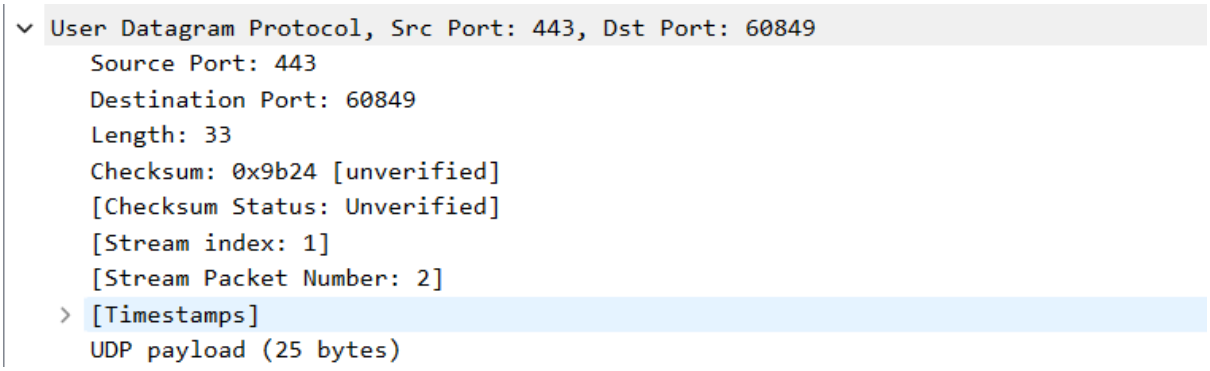



```
Transmission Control Protocol, Src Port: 51805, Dst Port: 5228, Seq: 1, Ack: 1, L
    Source Port: 51805
    Destination Port: 5228
    [Stream index: 0]
    [Stream Packet Number: 1]
  > [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 1]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1343435411
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3607842998
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 255
```

It starts the transaction using SYN packet and uses Sequence number for the ordered packet reception.Also it uses Acknowledgement for error detection,If the ACK is not received,it will resend the packets.TCP follows the 3 way handshake.

For udp:





UDP is connectionless protocol,it just needs Source and Destination port to transmit the packets,whenever the speed is required udp is used.