Linnéuniversitetet
Kalmar Växjö

Report

Assignment 2

Author: Andrei Neagu, Mohammed Sabbagh

Semester: V2020

Discipline: Computer Networks - administration

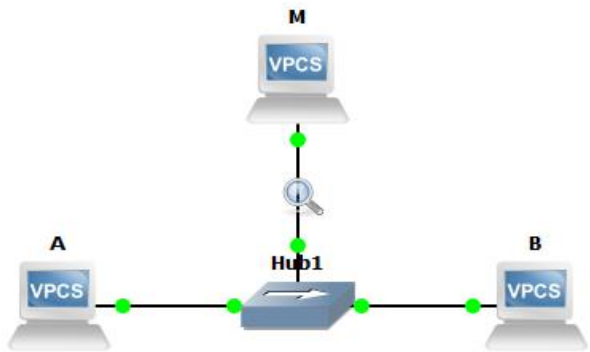
Course code: 1DV702

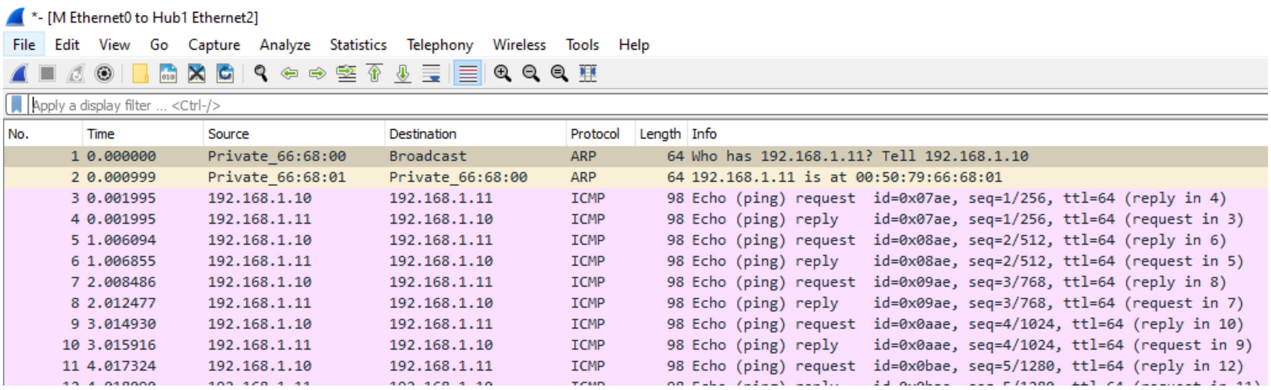
Contents

Part I - Segmentation Architecture Fundamentals

1.1 Hub vs. Switch Behaviour

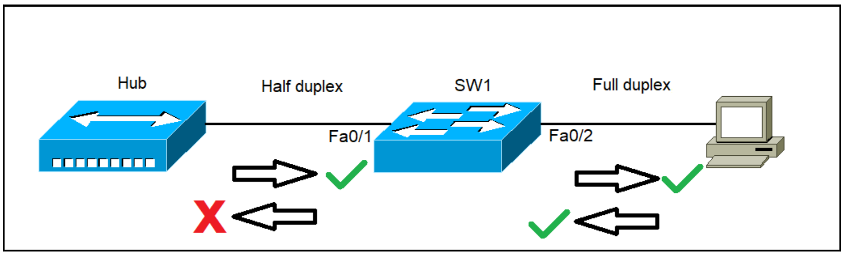
Traffic between A & B through a hub And M is capturing the traffic between them:





No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Private_66:68:00	Broadcast	ARP	64	Who has 192.168.1.11? Tell 192.168.1.10
2	0.000999	Private_66:68:01	Private_66:68:00	ARP	64	192.168.1.11 is at 00:50:79:66:68:01
3	0.001995	192.168.1.10	192.168.1.11	ICMP	98	Echo (ping) request id=0x07ae, seq=1/256, ttl=64 (reply in 4)
4	0.001995	192.168.1.11	192.168.1.10	ICMP	98	Echo (ping) reply id=0x07ae, seq=1/256, ttl=64 (request in 3)
5	1.006094	192.168.1.10	192.168.1.11	ICMP	98	Echo (ping) request id=0x08ae, seq=2/512, ttl=64 (reply in 6)
6	1.006855	192.168.1.11	192.168.1.10	ICMP	98	Echo (ping) reply id=0x08ae, seq=2/512, ttl=64 (request in 5)
7	2.008486	192.168.1.10	192.168.1.11	ICMP	98	Echo (ping) request id=0x09ae, seq=3/768, ttl=64 (reply in 8)
8	2.012477	192.168.1.11	192.168.1.10	ICMP	98	Echo (ping) reply id=0x09ae, seq=3/768, ttl=64 (request in 7)
9	3.014930	192.168.1.10	192.168.1.11	ICMP	98	Echo (ping) request id=0x0aae, seq=4/1024, ttl=64 (reply in 10)
10	3.015916	192.168.1.11	192.168.1.10	ICMP	98	Echo (ping) reply id=0x0aae, seq=4/1024, ttl=64 (request in 9)
11	4.017324	192.168.1.10	192.168.1.11	ICMP	98	Echo (ping) request id=0x0bae, seq=5/1280, ttl=64 (reply in 12)

1.1.1 Hub behavior

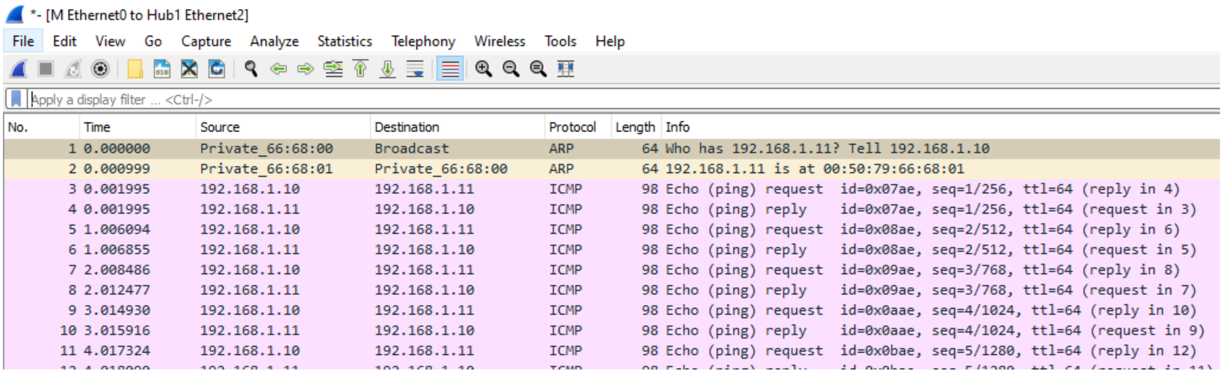


- <u>Half-duplex:</u> means that the Client can send and receive, but only one at a time. And both the sender and receiver can send any time, but only one can send it at any given time. The hub considered half-duplex, so the collisions will happen because of the nature of Ethernet's and will be handheld by the CSMA/CD methodology. The sender will listen to the medium and wait till it is idle then send. If the collision occurs, a random counter will start before a new transmission.

Full-duplex means that the Client can send and receive at the same time. And both the sender and receiver can send at any time. The Switch is considered as full-duplex, and each interface on the Switch considered a separate collision domain. That is why there are no collisions in full-duplex mode.

- Link Speed It is the maximum speed link between two nodes and measured in a bit per second.
  Auto-Negotiation is a signaling mechanism used by Ethernet over twisted pair by which two end devices. Both negotiate to choose the maximum standard transmission parameters (link speed, duplex mode, and flow control) they both supports.
  Normal Link Pulse (NLP): For the 10 Base-T standard, A link-test mechanism used to test the connection. If there is no network traffic, a 100-nanosecond pulse is sent every 16 milliseconds. This pulse called NLP. These pulses used to detect links between devices, and they are transmitted by the devices when they are not sending or receiving data. And used to check the compatibility of the devices as well, if there is no common technology, no link will be established.

- Unicast: Is sending data from one node (sender) to another one end node (receiver).
  Broadcast: Is sending data from one node (sender) to all end nodes (receivers)
  Multicast: Is sending Data from one node (sender) to a group of nodes(receivers).

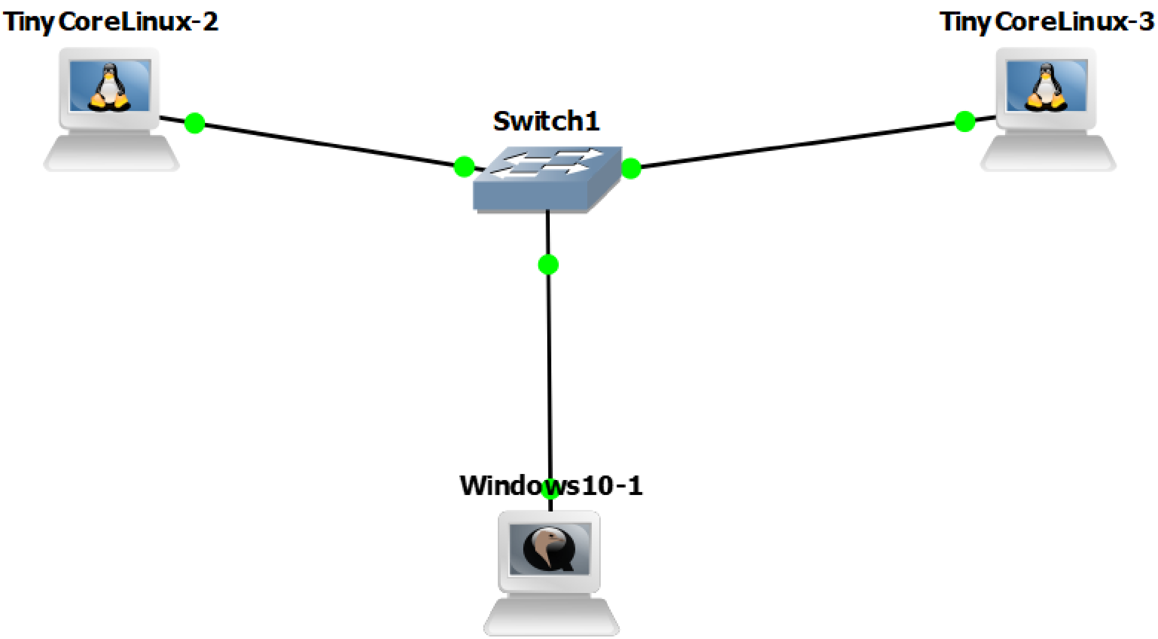

*- [M Ethernet0 to Hub1 Ethernet2]

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Private_66:68:00	Broadcast	ARP	64	Who has 192.168.1.11? Tell 192.168.1.10
2	0.000999	Private_66:68:01	Private_66:68:00	ARP	64	192.168.1.11 is at 00:50:79:66:68:01
3	0.001995	192.168.1.10	192.168.1.11	ICMP	98	Echo (ping) request id=0x07ae, seq=1/256, ttl=64 (reply in 4)
4	0.001995	192.168.1.11	192.168.1.10	ICMP	98	Echo (ping) reply id=0x07ae, seq=1/256, ttl=64 (request in 3)
5	1.006094	192.168.1.10	192.168.1.11	ICMP	98	Echo (ping) request id=0x08ae, seq=2/512, ttl=64 (reply in 6)
6	1.006855	192.168.1.11	192.168.1.10	ICMP	98	Echo (ping) reply id=0x08ae, seq=2/512, ttl=64 (request in 5)
7	2.008486	192.168.1.10	192.168.1.11	ICMP	98	Echo (ping) request id=0x09ae, seq=3/768, ttl=64 (reply in 8)
8	2.012477	192.168.1.11	192.168.1.10	ICMP	98	Echo (ping) reply id=0x09ae, seq=3/768, ttl=64 (request in 7)
9	3.014930	192.168.1.10	192.168.1.11	ICMP	98	Echo (ping) request id=0x0aae, seq=4/1024, ttl=64 (reply in 10)
10	3.015916	192.168.1.11	192.168.1.10	ICMP	98	Echo (ping) reply id=0x0aae, seq=4/1024, ttl=64 (request in 9)
11	4.017324	192.168.1.10	192.168.1.11	ICMP	98	Echo (ping) request id=0x0bae, seq=5/1280, ttl=64 (reply in 12)

The first line is a broadcast frame sent to all nodes connected to the hub. The rest are unicast traffic. Hub repeats the frames to all ports. And that's why M can capture traffic between A and B.
Hub is a layer2 medium and doesn't understand IP, so all devices need to know MAC addresses to communicate. A sends a broadcast asking about the MAC address for the IP address for client B. All Devices will drop the broadcast except B and will send back its MAC address to A as unicast.

1.1.2 Switch behavior

Because it is not possible to do the experiments in the lab due to coronavirus, I ran a simulation in GNS3. I have connected 2 Linux VMs to a switch and a Windows 10 VM. It works the same way it would work on site.



Experiment 1

2	0.327036	0c:38:69:77:e1:00	Broadcast	ARP	42 Who has 192.168.0.3? (ARP Probe)
8	1.326669	0c:38:69:77:e1:00	Broadcast	ARP	42 Who has 192.168.0.3? (ARP Probe)
20	2.328030	0c:38:69:77:e1:00	Broadcast	ARP	42 Who has 192.168.0.3? (ARP Probe)
21	3.327110	0c:38:69:77:e1:00	Broadcast	ARP	42 ARP Announcement for 192.168.0.3

After I assigned a private IP 192.168.0.3 on the Windows VM, I got ARP requests asking who has 192.168.0.3. I did not record other ARP traffic. All the VM's have their ARP tables statically assigned. Therefore, there is no need to broadcast requests to get the MAC address of the other nodes in the network. The Switch receives a frame and scans the CAM table to see if it knows the correct port. If a CAM entry is matched, the frame is forwarded to the correct port. In our case, when you start a switch, there is no CAM table, so the Switch sends broadcasts to all ports. It is not possible to capture other traffic because the other VMs have their ARP tables already configured. I do not know why the Windows VM sent a request asking who has 192.168.0.3 and then responded to it. The Switch floods the network with the packet that comes first.

There shouldn't have been any traffic in this experiment because the VMs have MAC IP maps statically assigned.

Experiment 2

2	0.336502	0c:38:69:77:e1:00	Broadcast	ARP	42 Who has 169.254.120.20? (ARP Probe)
3	0.337205	0c:38:69:77:e1:00	Broadcast	ARP	42 Who has 192.168.0.3? (ARP Probe)
9	1.336905	0c:38:69:77:e1:00	Broadcast	ARP	42 Who has 169.254.120.20? (ARP Probe)
10	1.337134	0c:38:69:77:e1:00	Broadcast	ARP	42 Who has 192.168.0.3? (ARP Probe)
19	2.336350	0c:38:69:77:e1:00	Broadcast	ARP	42 Who has 169.254.120.20? (ARP Probe)
20	2.336518	0c:38:69:77:e1:00	Broadcast	ARP	42 Who has 192.168.0.3? (ARP Probe)
23	3.365055	0c:38:69:77:e1:00	Broadcast	ARP	42 ARP Announcement for 169.254.120.20
24	3.365210	0c:38:69:77:e1:00	Broadcast	ARP	42 ARP Announcement for 192.168.0.3
73	47.944068	0c:38:69:b9:77:00	Broadcast	ARP	60 Who has 192.168.0.2? Tell 192.168.0.1
87	110.240469	0c:38:69:77:e1:00	Broadcast	ARP	42 Who has 192.168.0.1? Tell 192.168.0.3
88	110.241446	0c:38:69:b9:77:00	0c:38:69:77:e1:00	ARP	60 192.168.0.1 is at 0c:38:69:b9:77:00
93	113.939965	0c:38:69:77:e1:00	Broadcast	ARP	42 Who has 192.168.0.2? Tell 192.168.0.3
94	113.941061	0c:38:69:aa:69:00	0c:38:69:77:e1:00	ARP	60 192.168.0.2 is at 0c:38:69:aa:69:00
101	118.964689	0c:38:69:aa:69:00	0c:38:69:77:e1:00	ARP	60 Who has 192.168.0.3? Tell 192.168.0.2
102	118.965018	0c:38:69:77:e1:00	0c:38:69:aa:69:00	ARP	42 192.168.0.3 is at 0c:38:69:77:e1:00

In Experiment 2, the ARP tables are empty, the Linux VMs are sending pings, and the Switch is being reset. We can see the same ARP requests being flooded from the Switch, but now we also see requests from the other VMs. The Windows VM sends requests across the network as a broadcast, and the Windows VM receives requests from the other machines. An ARP request asks for the MAC address of the machines for the purpose of pairing them in a table. The reason why this additional traffic was captured is that the ARP tables were empty on all the VMs. The Switch records the source MAC address from all packets to populate the CAM table.

Conclusions

The package capture in Experiment 1 has no ARP requests from the VMs because the ARP entries in the table are statically added, the machines recognize the IP to MAC pairs, and there is no need for broadcasts. The capture in Experiment 2 contains ARP requests from all the machines because the ARP table is empty, and the demands are necessary for transmissions on the network.

A problem I found with the assignment is that my virtualized Switch does not have any way to connect to it, there is no console, I can't retrieve the CAM table. I can only answer how is populated using the screenshot below.

```
Ethernet switch Switch1 is always-on
  Running on server GNS3 VM (GNS3 VM) with port 3080
  Local ID is 4 and server ID is 9ba35403-622d-402c-ac2a-755b4ebdd274
  Console is on port 5003 and type is telnet
   Port Ethernet0 is in access  mode, with VLAN ID 1,
    connected to TinyCoreLinux-2 on port Ethernet0
   Port Ethernet1 is in access  mode, with VLAN ID 1,
    connected to TinyCoreLinux-3 on port Ethernet0
   Port Ethernet2 is in access  mode, with VLAN ID 1,
    connected to Windows10-1 on port Ethernet0
   Port Ethernet3 is empty
   Port Ethernet4 is empty
   Port Ethernet5 is empty
   Port Ethernet6 is empty
   Port Ethernet7 is empty
```

A CAM table looks like this, and this is not mine:

```
switch1#show mac address-table
          Mac Address Table
--------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0011.5ccc.5c00    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0009.5b44.9d2c    DYNAMIC     Fa0/1
   1    000f.66e3.352b    DYNAMIC     Fa0/1
```

Here we can see static entries and dynamic entries.

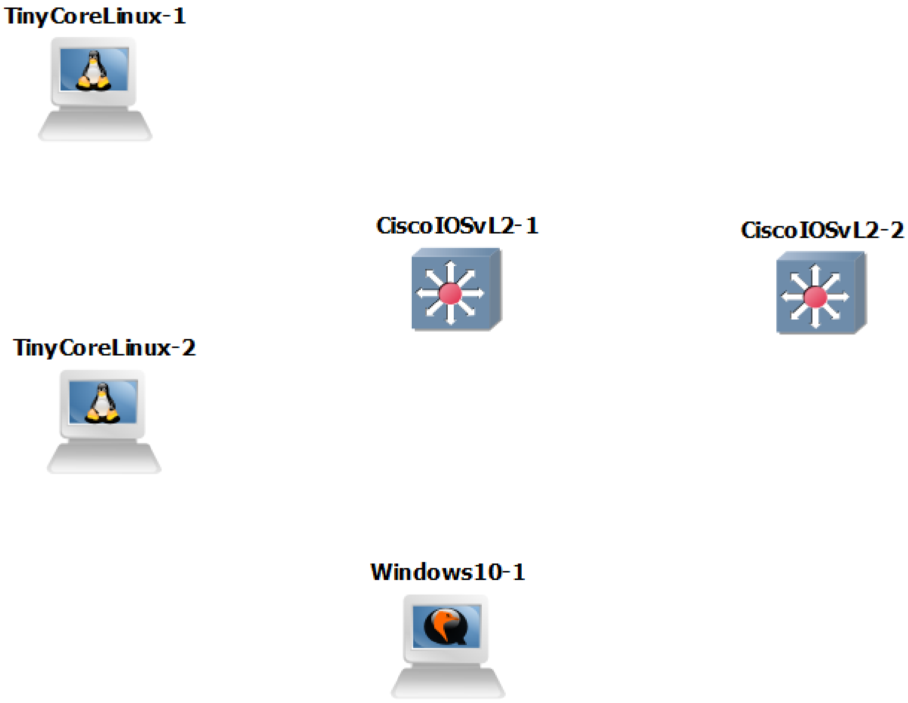
In my table, there would be only dynamic entries because we deleted all the static ones in Experiment 1. The Switch looks at the frames it receives and extracts the MAC addresses and maps them to its ports.

1.1.3 Conclusions

A collision domain is a shared medium in which all the machines connected can see each other. A hub is one big collision domain. A switch separates the machines from each other that are connected to its ports; therefore, it breaks the collision domain. A hub is a layer one device, no intelligence, and a switch is a layer two device, limited intelligence. A hub is broadcasting packets across the network, creating noise, and a switch only sends packets towards the right destination eliminating traffic on the network.

A switch initially acts as a hub when the CAM table is empty. It broadcasts the packets across the network to retrieve the MAC addresses of the frames to map them to its ports. A switch can easily be made to act like a hub, however that defeats the purpose of a switch. A switch just must forward any packet and broadcast it across the network. The correct term for then the Switch broadcasts across its ports is flooding.

1.2 VLANs



Here I am using 2 Linux VMs in place of the laptops and 1 Windows VM in place of the PC, and this is used for packet capture.

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0, Gi1/1, Gi1/2, Gi1/3
                                                Gi2/0, Gi2/1, Gi2/2, Gi2/3
                                                Gi3/0, Gi3/1, Gi3/2, Gi3/3
10   VLAN 10                          active    Gi0/0, Gi0/1
20   VLAN 20                          active    Gi0/2, Gi0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

I have created VLAN 10 and VLAN 20, and I have attacked two ports on VLAN 10 and 2 ports on VLAN 20. This configuration is on both switches.

1.2.1 Single Switch

Experiment 1

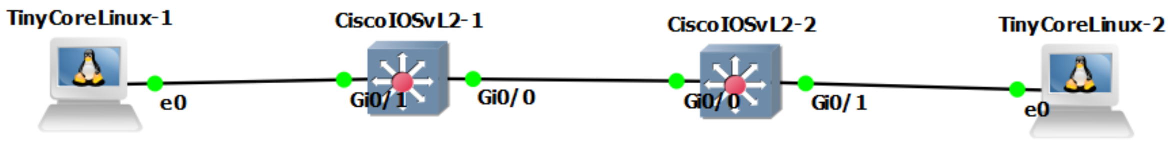
- When the Linux VM and the Windows VM are connected to VLAN 10, they are in the same subnet, and they can ping each other and can see broadcasts. When the Windows VM is connected to VLAN 20, the machines are not in the same domain anymore, and they will not be able to broadcast or ping messages to each other, they are in different VLANs.
- If we assign the same IP to one machine in VLAN 10 and another machine in VLAN 20, communication between machines in the same VLAN is possible, but it will create conflicts if the whole network is behind a NAT or Router.

Experiment 2

Here communication between the machines is not possible because they are in different VLANs.

1.2.2 Multiple Switches

This is the GNS3 setup.



To connect 2 VLANs, you need to set a port to trunk mode. On a Cisco router, you achieve that with the following commands. A trunk port is a port that is assigned to carry traffic for all the VLANs that are accessible by a specific switch, a process known as trunking. Trunk frames are encapsulated with IEEE 802.1Q.

```
switchport trunk encapsulation dot1q
```

```
switchport mode trunk
```

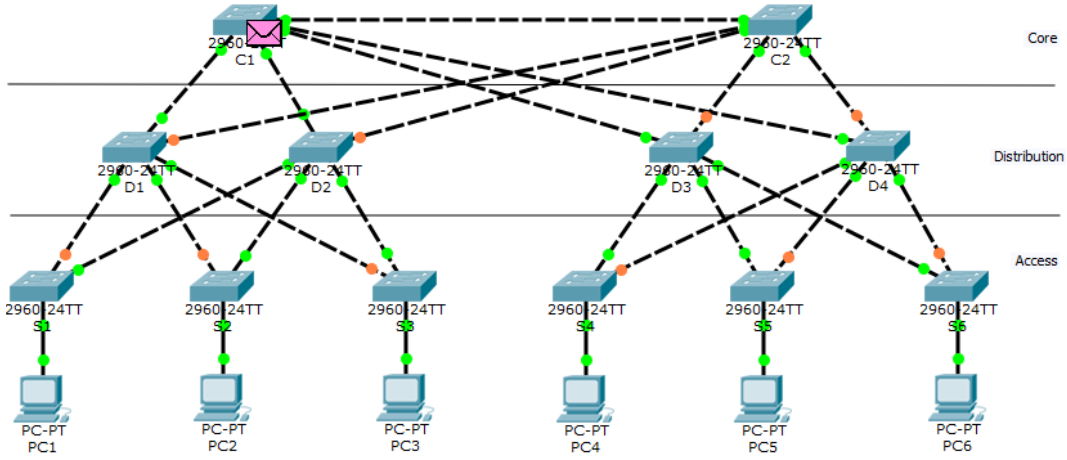
Without trunking, the machines connected in one VLAN cannot communicate with machines on a different VLAN.

After the configuration, the machines can ping each other.

1.3 Spanning Tree

Activity 5.1.3: Examining a Redundant Design

Task 1:



Task 2:

Step 1.

Step 2.

- because there is only one path, As the STP is blocking the other one.
- the loop-free path between PC1 and PC6: PC1-S1-D2-C1-D3-S6- PC6

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC1	ICMP	
	0.001	PC1	S1	ICMP	
	0.002	S1	D2	ICMP	
	0.003	D2	C1	ICMP	
	0.004	C1	D3	ICMP	
	0.005	D3	S6	ICMP	
	0.006	S6	PC6	ICMP	

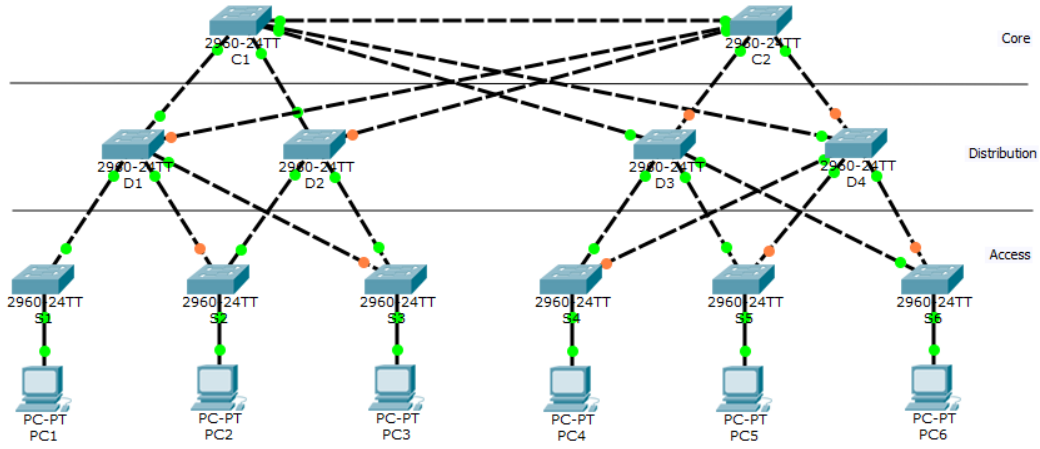
Step 3.

	0.013	PC2	S2	ICMP	
	0.014	S2	D2	ICMP	
	0.015	D2	C1	ICMP	
	0.016	C1	D3	ICMP	
	0.017	D3	S4	ICMP	
	0.018	S4	PC4	ICMP	
	0.019	PC4	S4	ICMP	

I have pinged from PC2 to PC4, and It has the same path in the old experiment in two-layer (distribution and core), but it was different in the access layer.

Task 3:

Step 1.

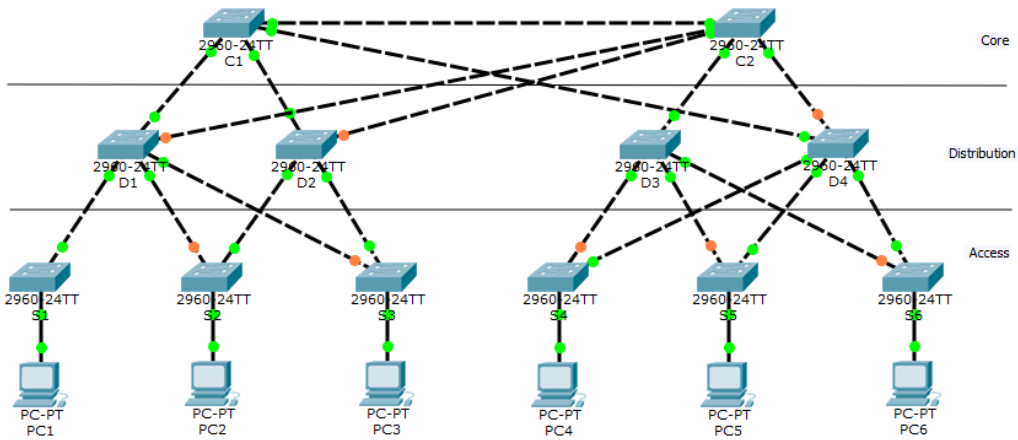


Step 2.

The new loop-free path between PC1 and PC6 is PC1-S1-D1-C1-D3-S6-PC6.

0.025	PC1	S1	ICMP
0.027	S1	D1	ICMP
0.029	D1	C1	ICMP
0.031	C1	D3	ICMP
0.033	D3	S6	ICMP
0.035	S6	PC6	ICMP

Step 3.



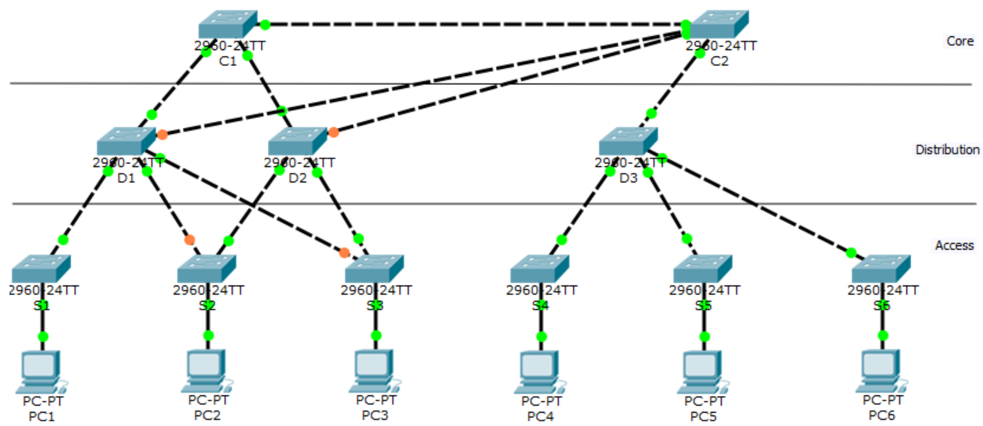
Now, as in the figure above, the link from D3 to C2 is active after the deletion.

Step 4.

The new loop-free path between PC1 and PC6 is PC1-S1-D1-C1-D4-S6-PC6.

0.001	PC1	S1	ICMP
0.003	S1	D1	ICMP
0.005	D1	C1	ICMP
0.007	C1	D4	ICMP
0.009	D4	S6	ICMP
0.011	S6	PC6	ICMP

Step 5.



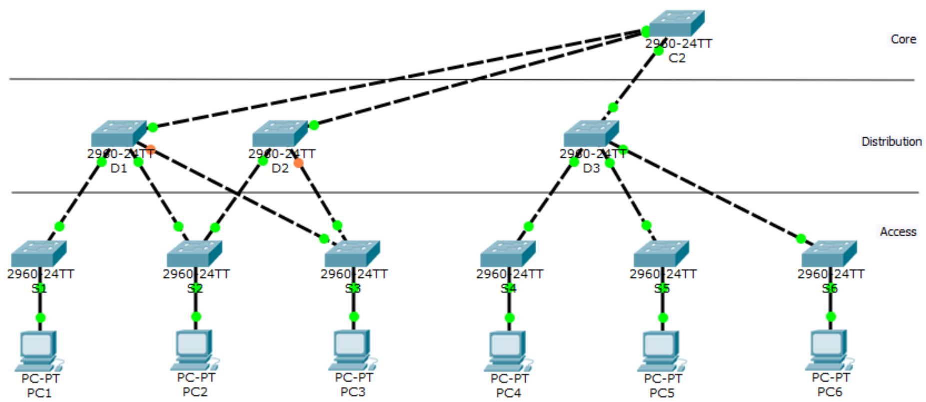
Step 6.

The new loop-free path between PC1 and PC6 is PC1-S1-D1-C1-C2-D3-S6-PC6.

0.003	PC1	S1	ICMP
0.005	S1	D1	ICMP
0.007	D1	C1	ICMP
0.009	C1	C2	ICMP
0.011	C2	D3	ICMP
0.013	D3	S6	ICMP
0.015	S6	PC6	ICMP

The new is there is only one distribution point below C2, which is D3 no redundant way.

Step 7.



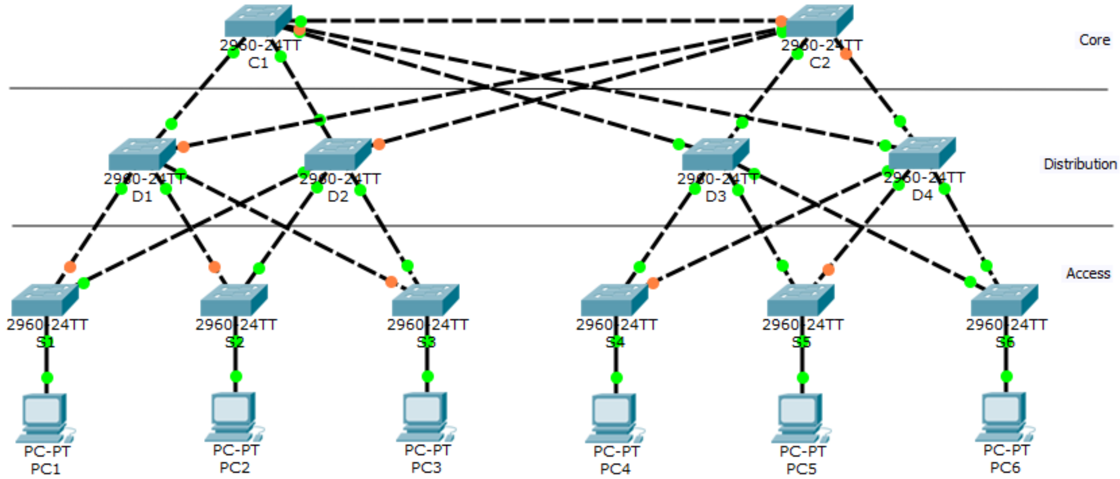
Step 8.

The new loop-free path between PC1 and PC6 is PC1-S1-D1-C2-D3-S6-PC6.

Activity 5.2.5: Configuring STP

Task 1:

Step 1.



Step 2. Done

Step 3.

The root bridge is switch S6.

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.968	--	S6	STP	
	0.969	S6	PC6	STP	
	0.969	S6	D4	STP	
	0.969	S6	D3	STP	

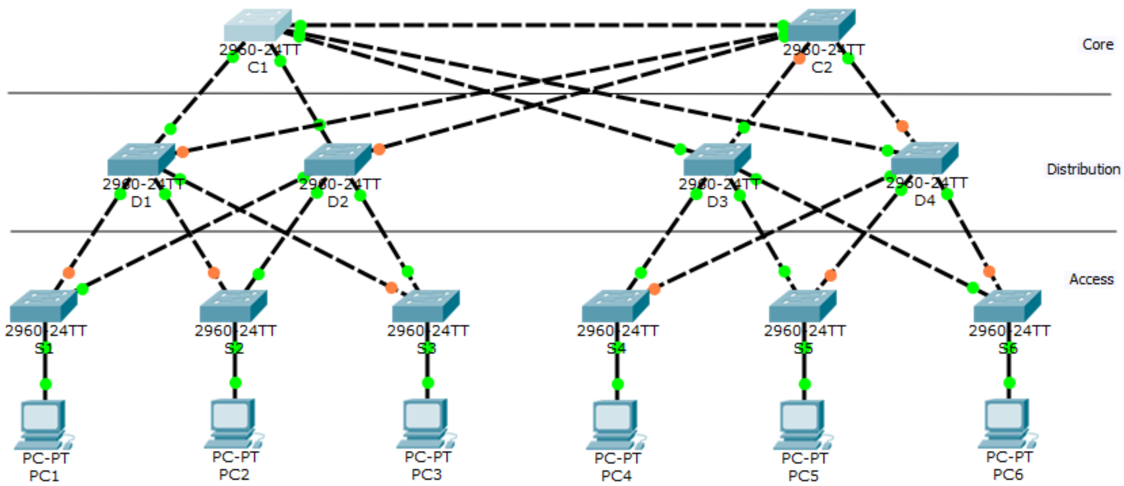
The reason why is because it not located in the core layer.

Task 2:

Step 1.

```
C1(config)#spanning-tree vlan 1 priority 4096
C1(config)#
```

Step 2.



Step 3. Done

Step 4.

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.110	--	C1	STP	
	0.111	C1	D1	STP	
	0.111	C1	D4	STP	
	0.111	C1	D3	STP	
	0.111	C1	C2	STP	
	0.111	C1	D2	STP	

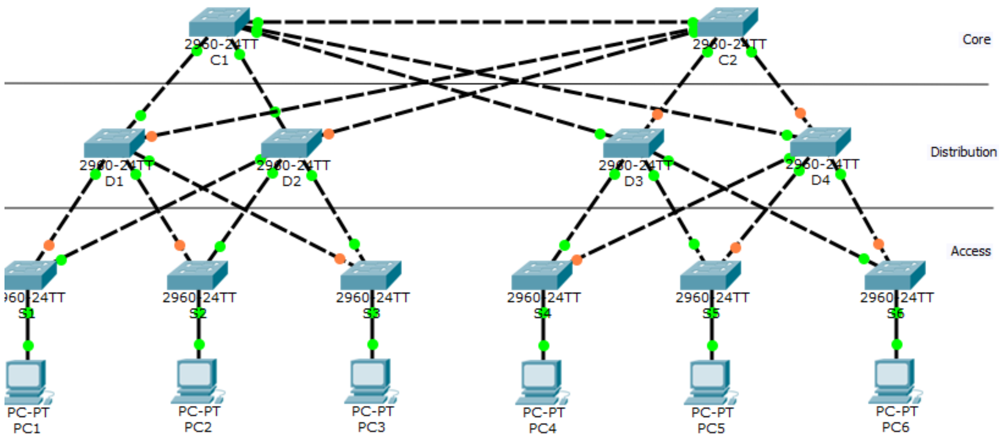
Step 5. Done

Task 3:

Step 1.

```
C2(config)#spanning-tree vlan 1 priority 8192
C2(config)#
```

Step 2.



Step 3.

All C2 links to distribution layers blocked (amber) because that C2 is a redundant root for C1 and will work if C1 has a failure.

Step 4. Done

Task 4:

Step 1.

```
D1(config)#spanning-tree vlan 1 priority 12288
D2(config)#spanning-tree vlan 1 priority 12288
D3(config)#spanning-tree vlan 1 priority 12288
D4(config)#spanning-tree vlan 1 priority 12288
```

Step 2.

Activity Results

Congratulations Guest! You completed the activity.

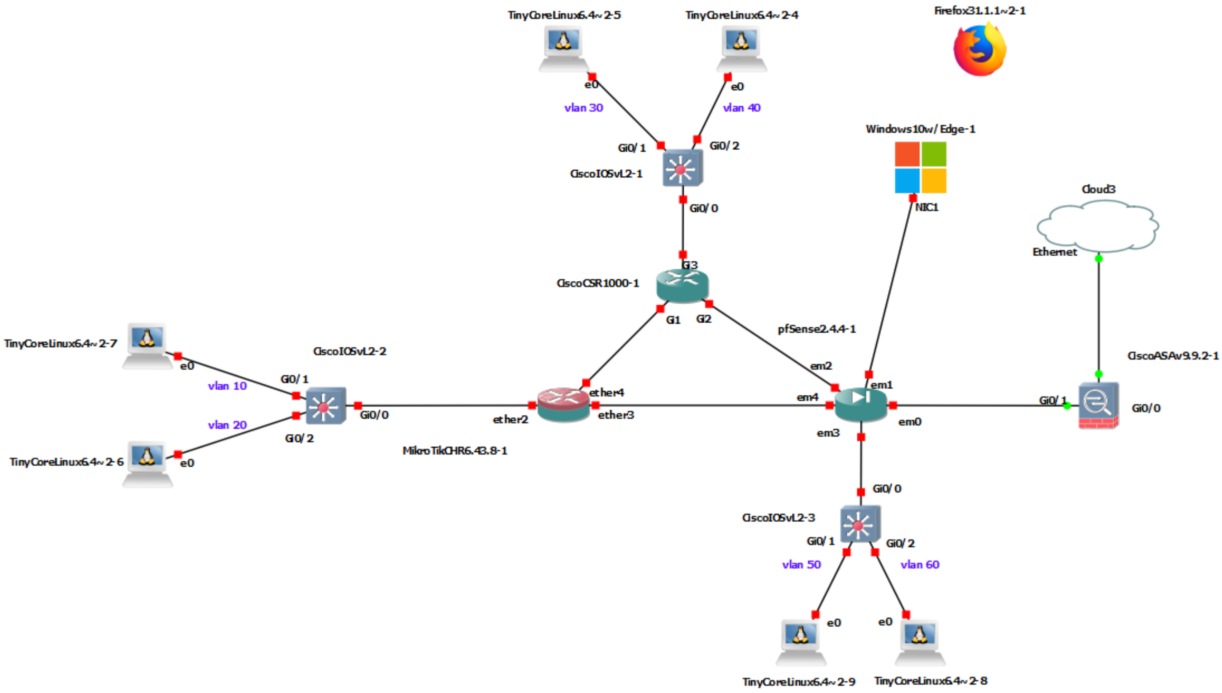
Overall Feedback | Assessment Items | Connectivity Tests

Congratulations on completing this activity!

Part II - Addressing and Routing Architecture

2.1 Preparation

2.2 IP Addressing



The best suitable subnet for this topology is class B, which will meet the requirements.

Subnet Name	Hosts needed	Host available	Network address	CIDR	Subnet Mask	Host range	Broadcast
VLAN 10	58	62	172.16.10.0	/26	255.255.255.192	172.16.10.1 - 172.16.10.62	172.16.10.63
VLAN 20	12	14	172.16.20.0	/28	255.255.255.240	172.16.20.1 - 172.16.20.14	172.16.20.15
VLAN 30	201	254	172.16.30.0	/24	255.255.255.0	172.16.30.1 - 172.16.30.254	172.16.30.255
VLAN 40	414	510	172.16.40.0	/23	255.255.254.0	172.16.40.1 - 172.16.41.254	172.16.41.255
VLAN 50	109	126	172.16.50.0	/25	255.255.255.128	172.16.50.1 - 172.16.50.126	172.16.50.127
VLAN 60	54	62	172.16.60.0	/26	255.255.255.192	172.16.60.1 - 172.16.60.62	172.16.60.0
RM-RC	2	2	172.16.1.0	/30	255.255.255.252	172.16.1.1 - 172.16.1.2	172.16.1.3
RM-RP	2	2	172.16.1.4	/30	255.255.255.252	172.16.1.5 - 172.16.1.6	172.16.1.7
RC-RP	2	2	172.16.1.8	/30	255.255.255.252	172.16.1.9 - 172.16.1.10	172.16.1.11
RP-RASA	2	2	172.16.1.12	/30	255.255.255.252	172.16.1.13 - 172.16.1.14	172.16.1.15
ASA-IE	2	2	212.157.74.96	/30	255.255.255.252	212.157.74.97- 212.157.74.98	212.157.74.99

R= Router M=MikroTikCHR C=Cisco P=pfSense ASA=CiscoASA

The above table demonstrates the networks and subnets that will be used in the topology. The network 172.16.0.0 /16 was the base of our subnetting.

First, I have started with the switches. I have configured each Switch with two VLAN interfaces and one trunk interface. The port to the Router is a trunk port. And each pc in a VLAN for the test.

```
interface GigabitEthernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/1
 switchport access vlan 10
 switchport mode access
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/2
 switchport access vlan 20
 switchport mode access
 media-type rj45
 negotiation auto
!
```

```
switch2#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/3, Gi1/0, Gi1/1, Gi1/2
                                                Gi1/3, Gi2/0, Gi2/1, Gi2/2
                                                Gi2/3, Gi3/0, Gi3/1, Gi3/2
                                                Gi3/3
10   VLAN0010                         active    Gi0/1
20   VLAN0020                         active    Gi0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
```

The picture above for a switch has two VLAN (10,20) configured on it and one interface trunk.

Second, I started with the routers. I configured each interface with the corresponding IP address.

And for every interface that has the Switch, I have created two sub-interfaces for each VLAN.

```
[admin@MikroTik] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   172.16.10.1/26     172.16.10.0     VLAN10
 1   172.16.20.1/28     172.16.20.0     VLAN20
 2   172.16.1.1/30      172.16.1.0      ether1
 3   172.16.1.5/30      172.16.1.4      ether3
```

```
interface GigabitEthernet1
 ip address 172.16.1.2 255.255.255.252
 negotiation auto
 no mop enabled
 no mop sysid
!
interface GigabitEthernet2
 ip address 172.16.1.9 255.255.255.252
 negotiation auto
 no mop enabled
 no mop sysid
!
interface GigabitEthernet3
 no ip address
 negotiation auto
 no mop enabled
 no mop sysid
!
interface GigabitEthernet3.30
 encapsulation dot1Q 30
 ip address 172.16.30.1 255.255.255.0
!
interface GigabitEthernet3.40
 encapsulation dot1Q 40
 ip address 172.16.40.1 255.255.254.0
!
```

The images above show the interfaces with the IP addresses and the sub-interfaces VLAN.

Third, the DHCP setup.

Cisco router:

I started with Cisco by creating two pools for each VLAN network and its default gateway and DNS server.

```
ip dhcp pool vlan30
 network 172.16.30.0 255.255.255.0
 default-router 172.16.30.1
 dns-server 8.8.8.8
!
ip dhcp pool vlan40
 network 172.16.40.0 255.255.254.0
 default-router 172.16.40.1
 dns-server 8.8.8.8
```

The pc on the VLAN 30 will sends a DHCP request through the trunk port in the Switch to the Router on its sub-interface interface Gi 3.30. Then the Router will respond with an IP offer to the pc.

```
nameserver 8.8.8.8
eth0      Link encap:Ethernet  HWaddr 0C:92:37:12:37:00
          inet addr:172.16.30.2  Bcast:172.16.30.255  Mask:255.255.255.0
          inet6 addr: fe80::e92:37ff:fe12:3700/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:3352 (3.2 KiB)
```

Mikrotik router:

I have used the WinBox to configure the Router as it allows o access to the GUI interface.

Then the same as Cisco.

DHCP Server

DHCP | Networks | Leases | Options | Option Sets | Alerts

DHCP Config | DHCP Setup

Name	Interface	Relay	Lease Time	Address Pool
DHCP-1	VLAN10		00:10:00	VLAN10
DHCP-2	VLAN20		00:10:00	VLAN20

DHCP Server

DHCP | Networks | Leases | Options | Option Sets | Alerts

Address	Gateway	DNS Servers
172.16.10.0/26	172.16.10.1	8.8.8.8
172.16.20.0/28	172.16.20.1	8.8.8.8

DHCP Server

DHCP | Networks | Leases | Options | Option Sets | Alerts

Check Status

	Address	MAC Address	Client ID	Server	Active Address	Active MAC Addre...	Active Hos...	Expires After	Status
D	172.16.10.62	0C:92:37:44:67:00	1:c:92:37:44:67:0	DHCP-1	172.16.10.62	0C:92:37:44:67:00	box	00:09:56	bound

```
gns3@box:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 0C:92:37:44:67:00
          inet addr:172.16.10.62  Bcast:172.16.10.63  Mask:255.255.255.192
```

The picture above shows the setup of the DHCP on the MikroTik router and the leased IP for the Client.

PfSense router:

I connect to the LAN with Firefox on the em1 interface, and I browse to the management page. I have configured the interfaces with a proper IP address as I plan on the table above.

I have created two VLAN (50,60), and I assigned them to the interface that is connected to the Switch.

Then configure the DHCP server and the pool for each of the VLAN. And after that, it offers IP addresses to the clients corresponding to their VLAN.

MRPR Interface (opt3, em4)

Status	up
MAC Address	0c:92:37:37:88:04
IPv4 Address	172.16.1.6
Subnet mask IPv4	255.255.255.252
IPv6 Link Local	fe80::e92:37ff:fe37:8804%em4
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	0/3 (0 B/304 B)
In/out packets (pass)	0/3 (0 B/304 B)
In/out packets (block)	0/0 (0 B/0 B)
In/out errors	0/0
Collisions	0

INVLAN50 Interface (opt4, em3.50)

Status	up
MAC Address	0c:92:37:37:88:03
IPv4 Address	172.16.50.1
Subnet mask IPv4	255.255.255.128
IPv6 Link Local	fe80::e92:37ff:fe37:8803%em3.50
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	2/42 (656 B/4 KiB)
In/out packets (pass)	2/42 (656 B/4 KiB)
In/out packets (block)	0/0 (0 B/0 B)
In/out errors	0/0
Collisions	0

```
gns3@box:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 0C:92:37:C5:E3:00
          inet addr:172.16.60.2  Bcast:172.16.60.63  Mask:255.255.255.192
```

Status / DHCP Leases

Leases

	IP address	MAC address	Hostname	Description	Start	End	Online	Le
	172.16.50.2	0c:92:37:aa:57:00	box		2020/05/01 17:42:12	2020/05/01 19:42:12	offline	ac
	172.16.60.2	0c:92:37:c5:e3:00	box		2020/05/01 17:42:11	2020/05/01 19:42:11	offline	ac
	192.168.1.100	0c:92:37:8e:9a:00	box		2020/05/01 17:05:56	2020/05/01 19:05:56	online	ac

Leases in Use

Interface	Pool Start	Pool End	# of leases in use
LAN	192.168.1.100	192.168.1.199	1
INVLAN50	172.16.50.2	172.16.50.126	1
INVLAN60	172.16.60.2	172.16.60.62	1

So every node will send a DHCP request asking for IP, and the Router will respond with the corresponding address with the IP address that matches the VLAN ID on the Switch.

2.3 IP Routing

I have chosen to use the OSPF protocol to route all Router and make network reachable from anywhere.

First, I have configured the OSPF protocol on all routers, and as a result of that, I was able to reach any part of the network.

I have added a static route for both (CiscoCSR and Mikrotik) for the unknown network (0.0.0.0 0.0.0.0) to the port that faced Pfsense.

I have added NAT role for each Router, and a result of that the clients on each VLAN able to reach the internet (NOTE: at this point, I was connecting the Pfsense directly to the internet I haven't join ASA yet).

After configuring the DNS, the static route, and NAT on each Router, I was able to reach the internet.

At this point, I disconnect the Pfsense from the internet, and I connected to the ASA that will be the WAN interface.

IN ASA, I configure the outside interface with DHCP to get into from my cloud connection. I have added a security level. I have added a static route for the internet.

I have created a user account for ASA with privilege 15 to be able to connect to it remotely.

I have copied the ASDM image to ASA, and I have allowed the traffic from my pc to ASA to manage it throw ASDM.

I configured the interface between ASA and Pfsense with the network (192.168.2.0/30) and named it as inside. I have added a proper access role and a NAT for the inside network to access the internet from the outside interface.

I have configured the OSPF protocol on ASA to reach the hole inside the network.

In the end, I was able to reach the internet from any node in the network :

For example: (Client in vlan 10)➔(switch+Microtik router)➔(Pfsense router)➔(ASA)

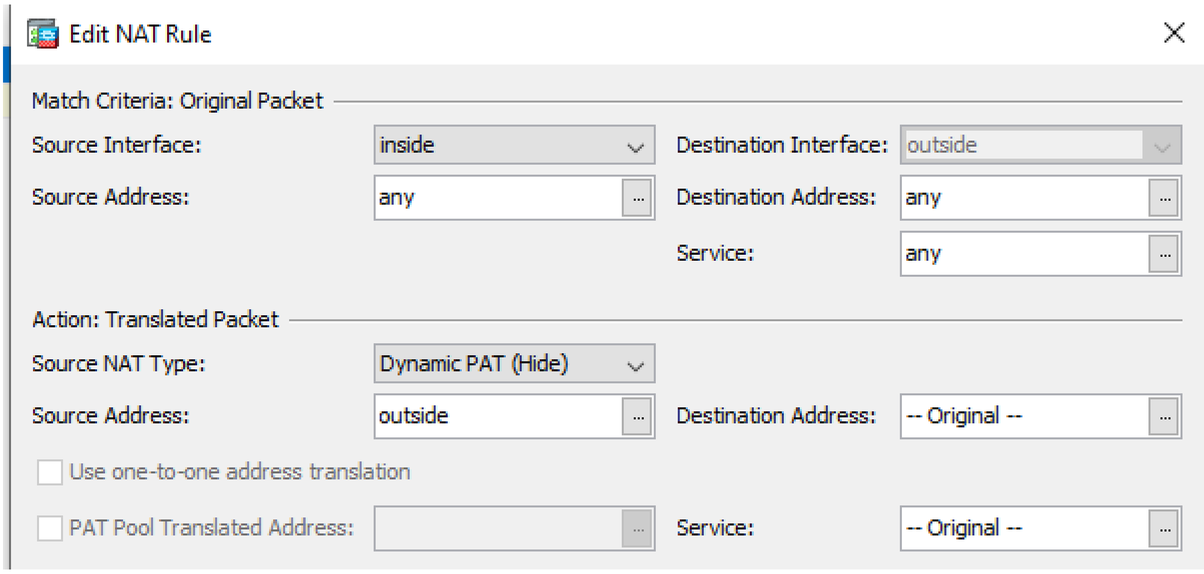
The interfaces in ASA (two interfaces outside and inside):

Interface Status

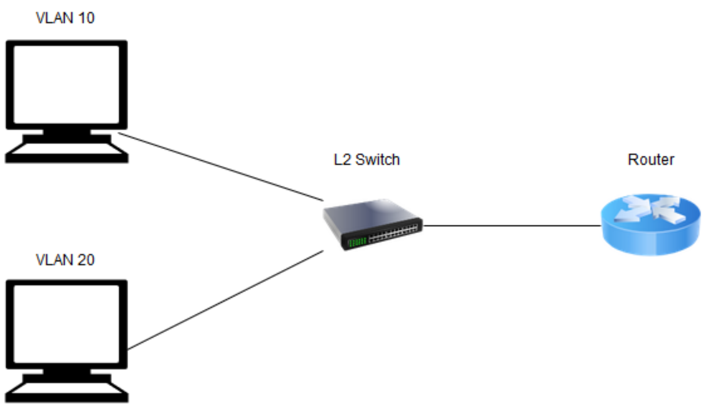
Interface	IP Address/Mask	Line	Link	Kbps
inside	192.168.2.1/30	up	up	0
outside	192.168.140.145/24	up	up	63

Interface	Name	...	Route...	State	Security Level	IP Address	Subnet Mask Prefix Length	Secondary VLAN	Redundant	Group	Type	MTU
GigabitEthernet0/0	outside			Enabled	0	192.168.140.145 (DHCP)	255.255.255.0 (DHCP)		No		Hardware	1,500
GigabitEthernet0/1	inside			Enabled	100	192.168.2.1	255.255.255.252		No		Hardware	1,500

The NAT role in ASA to allow inside the network to access the internet :



- **The technique to route two VLANs on an L2 switch**



In the setup above, we have 2 VLANs on the L2 Switch, and the Switch is connected with a single interface to a router. Because the Switch is operating on the 2nd level, with mac addresses, there is no way for the VLANs to talk with each other, and we require another device to do the routing. The Router behind the Switch will do this job. Firstly, we need to assign the link between the Switch and the Router the trunk mode, with access to VLAN 10 and VLAN 20. The Router and the L2 Switch are connected using a single interface. To solve this problem, we must create two sub-interfaces and specify the VLAN that they belong to. Now the Router can see the different VLANs and pinging is possible.

The benefit of this approach is that we can use an L2 Switch that is cheaper than an L3 switch.

The drawbacks are that the traffic going to the Router is limited by the link between the L2 Switch and the Router, it will always be slower than an L3 Switch. Another drawback is that the Router is an added point of failure. If money is of no concern, an L3 Switch is a superior approach.

[Reference]

From the same segment:

Ping & traceroute from VLAN 10 to VLAN 20 :

```
gns3@box:~$ ping 172.16.20.14
PING 172.16.20.14 (172.16.20.14): 56 data bytes
64 bytes from 172.16.20.14: seq=0 ttl=63 time=9.426 ms
64 bytes from 172.16.20.14: seq=1 ttl=63 time=9.244 ms
64 bytes from 172.16.20.14: seq=2 ttl=63 time=8.718 ms
^C
--- 172.16.20.14 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 8.718/9.129/9.426 ms
gns3@box:~$ traceroute 172.16.20.14
traceroute to 172.16.20.14 (172.16.20.14), 30 hops max, 38 byte packets
 1  172.16.10.1 (172.16.10.1)  3.837 ms  4.003 ms  4.078 ms
 2  172.16.20.14 (172.16.20.14)  8.967 ms  8.300 ms  7.782 ms
gns3@box:~$
```

Ping & traceroute from VLAN 30 to VLAN 40 :

```
gns3@box:~$ ping 172.16.40.2
PING 172.16.40.2 (172.16.40.2): 56 data bytes
64 bytes from 172.16.40.2: seq=0 ttl=63 time=15.376 ms
64 bytes from 172.16.40.2: seq=1 ttl=63 time=9.104 ms
64 bytes from 172.16.40.2: seq=2 ttl=63 time=9.027 ms
^C
--- 172.16.40.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 9.027/11.169/15.376 ms
gns3@box:~$ traceroute 172.16.40.2
traceroute to 172.16.40.2 (172.16.40.2), 30 hops max, 38 byte packets
 1  172.16.30.1 (172.16.30.1)  3.557 ms  3.754 ms  6.157 ms
 2  172.16.40.2 (172.16.40.2)  13.451 ms  10.766 ms  8.574 ms
```

Ping & traceroute from VLAN 50 to VLAN 60 :

```
gns3@box:~$ ping 172.16.60.2
PING 172.16.60.2 (172.16.60.2): 56 data bytes
64 bytes from 172.16.60.2: seq=0 ttl=63 time=8.096 ms
64 bytes from 172.16.60.2: seq=1 ttl=63 time=7.780 ms
64 bytes from 172.16.60.2: seq=2 ttl=63 time=8.649 ms
^C
--- 172.16.60.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 7.780/8.175/8.649 ms
gns3@box:~$ traceroute  172.16.60.2
traceroute to 172.16.60.2 (172.16.60.2), 30 hops max, 38 byte packets
 1  172.16.50.1 (172.16.50.1)  6.414 ms  3.486 ms  4.394 ms
 2  172.16.60.2 (172.16.60.2)  10.393 ms  8.474 ms  7.966 ms
```

From different segments:

Ping & traceroute from VLAN 10 to VLAN 30 and VLAN 50 :

```
gns3@box:~$ ping 172.16.30.2
PING 172.16.30.2 (172.16.30.2): 56 data bytes
64 bytes from 172.16.30.2: seq=0 ttl=62 time=17.315 ms
64 bytes from 172.16.30.2: seq=1 ttl=62 time=8.366 ms
^C
--- 172.16.30.2 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 8.366/12.840/17.315 ms
gns3@box:~$ traceroute 172.16.30.2
traceroute to 172.16.30.2 (172.16.30.2), 30 hops max, 38 byte packets
 1  172.16.10.1 (172.16.10.1)  3.599 ms  5.804 ms  4.410 ms
 2  172.16.1.2 (172.16.1.2)  5.593 ms  6.180 ms  6.460 ms
 3  172.16.30.2 (172.16.30.2)  8.587 ms  9.149 ms  7.915 ms
gns3@box:~$ ping 172.16.50.2
PING 172.16.50.2 (172.16.50.2): 56 data bytes
64 bytes from 172.16.50.2: seq=0 ttl=62 time=15.640 ms
64 bytes from 172.16.50.2: seq=1 ttl=62 time=8.775 ms
64 bytes from 172.16.50.2: seq=2 ttl=62 time=9.353 ms
^C
--- 172.16.50.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 8.775/11.256/15.640 ms
gns3@box:~$ traceroute  172.16.50.2
traceroute to 172.16.50.2 (172.16.50.2), 30 hops max, 38 byte packets
 1  172.16.10.1 (172.16.10.1)  3.630 ms  3.787 ms  4.212 ms
 2  172.16.1.6 (172.16.1.6)  4.131 ms  3.942 ms  4.179 ms
 3  172.16.50.2 (172.16.50.2)  7.643 ms  7.500 ms  6.480 ms
gns3@box:~$
```

Ping & traceroute from VLAN 30 to VLAN 20 and VLAN 60 :

```
gns3@box:~$ ping 172.16.20.14
PING 172.16.20.14 (172.16.20.14): 56 data bytes
64 bytes from 172.16.20.14: seq=0 ttl=62 time=12.647 ms
64 bytes from 172.16.20.14: seq=1 ttl=62 time=8.415 ms
^C
--- 172.16.20.14 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 8.415/10.531/12.647 ms
gns3@box:~$ traceroute  172.16.20.14
traceroute to 172.16.20.14 (172.16.20.14), 30 hops max, 38 byte packets
 1  172.16.30.1 (172.16.30.1)  5.616 ms  5.792 ms  4.003 ms
 2  172.16.1.1 (172.16.1.1)  5.870 ms  4.705 ms  4.170 ms
 3  172.16.20.14 (172.16.20.14)  10.211 ms  7.193 ms  11.143 ms
gns3@box:~$ traceroute  172.16.60.2
traceroute to 172.16.60.2 (172.16.60.2), 30 hops max, 38 byte packets
 1  172.16.30.1 (172.16.30.1)  4.984 ms  4.883 ms  4.778 ms
 2  172.16.1.10 (172.16.1.10)  6.459 ms  4.209 ms  4.431 ms
 3  172.16.60.2 (172.16.60.2)  13.144 ms  7.890 ms  8.604 ms
gns3@box:~$ ping 172.16.60.2
PING 172.16.60.2 (172.16.60.2): 56 data bytes
64 bytes from 172.16.60.2: seq=0 ttl=62 time=11.667 ms
64 bytes from 172.16.60.2: seq=1 ttl=62 time=11.358 ms
64 bytes from 172.16.60.2: seq=2 ttl=62 time=8.342 ms
^C
--- 172.16.60.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 8.342/10.455/11.667 ms
gns3@box:~$
```

Ping & traceroute from VLAN 50 to VLAN 10 and VLAN 40 :

```
gns3@box:~$ ping 172.16.10.62
PING 172.16.10.62 (172.16.10.62): 56 data bytes
64 bytes from 172.16.10.62: seq=0 ttl=62 time=10.679 ms
64 bytes from 172.16.10.62: seq=1 ttl=62 time=8.009 ms
^C
--- 172.16.10.62 ping statistics ---
3 packets transmitted, 2 packets received, 33% packet loss
round-trip min/avg/max = 8.009/9.344/10.679 ms
gns3@box:~$ traceroute  172.16.10.62
traceroute to 172.16.10.62 (172.16.10.62), 30 hops max, 38 byte packets
 1  172.16.50.1 (172.16.50.1)  4.960 ms  3.902 ms  4.213 ms
 2  172.16.1.5 (172.16.1.5)  3.081 ms  4.277 ms  4.058 ms
 3  172.16.10.62 (172.16.10.62)  8.558 ms  9.408 ms  11.549 ms
gns3@box:~$ ping 172.16.40.2
PING 172.16.40.2 (172.16.40.2): 56 data bytes
64 bytes from 172.16.40.2: seq=0 ttl=62 time=9.861 ms
64 bytes from 172.16.40.2: seq=1 ttl=62 time=8.866 ms
64 bytes from 172.16.40.2: seq=2 ttl=62 time=7.478 ms
^C
--- 172.16.40.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 7.478/8.735/9.861 ms
gns3@box:~$ traceroute  172.16.40.2
traceroute to 172.16.40.2 (172.16.40.2), 30 hops max, 38 byte packets
 1  172.16.50.1 (172.16.50.1)  4.690 ms  4.043 ms  4.165 ms
 2  172.16.1.9 (172.16.1.9)  6.056 ms  4.102 ms  6.141 ms
 3  172.16.40.2 (172.16.40.2)  8.751 ms  8.060 ms  8.833 ms
gns3@box:~$
```

From different Client to the internet:

Ping & traceroute from VLAN 10 to the internet :

```
gns3@box:~$ ping google.com
PING google.com (216.58.207.206): 56 data bytes
64 bytes from 216.58.207.206: seq=0 ttl=126 time=42.737 ms
64 bytes from 216.58.207.206: seq=1 ttl=126 time=42.158 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 42.158/42.447/42.737 ms
gns3@box:~$ traceroute google.com
traceroute to google.com (216.58.207.206), 30 hops max, 38 byte packets
 1  172.16.10.1 (172.16.10.1)  3.890 ms  4.056 ms  4.027 ms
 2  172.16.1.6 (172.16.1.6)  3.940 ms  3.963 ms  9.462 ms
 3  192.168.140.2 (192.168.140.2)  8.135 ms  6.685 ms  8.176 ms
 4^C
```

Ping & traceroute from VLAN 30 to the internet :

```
gns3@box:~$ ping google.com
PING google.com (216.58.207.238): 56 data bytes
64 bytes from 216.58.207.238: seq=0 ttl=126 time=40.385 ms
64 bytes from 216.58.207.238: seq=1 ttl=126 time=40.866 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 40.385/40.625/40.866 ms
gns3@box:~$ traceroute google.com
traceroute to google.com (216.58.207.238), 30 hops max, 38 byte packets
 1  172.16.30.1 (172.16.30.1)  28.322 ms  4.583 ms  4.111 ms
 2  172.16.1.10 (172.16.1.10)  5.679 ms  4.182 ms  3.999 ms
 3  192.168.140.2 (192.168.140.2)  6.842 ms  6.011 ms  7.870 ms
 4  *^C
```

Ping & traceroute from VLAN 60 to the internet :

```
gns3@box:~$ ping google.com
PING google.com (216.58.211.14): 56 data bytes
64 bytes from 216.58.211.14: seq=0 ttl=127 time=42.894 ms
64 bytes from 216.58.211.14: seq=1 ttl=127 time=43.067 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 42.894/42.980/43.067 ms
gns3@box:~$ traceroute google.com
traceroute to google.com (216.58.207.206), 30 hops max, 38 byte packets
 1  172.16.50.1 (172.16.50.1)  3.831 ms  4.161 ms  4.080 ms
 2  192.168.140.2 (192.168.140.2)  7.512 ms  5.004 ms  8.827 ms
 3  *^C
```

MikroTik routing table and OSPF database and neighbor tables :

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 A S  0.0.0.0/0                          172.16.1.6                1
 1 ADC  172.16.1.0/30      172.16.1.1      ether4                    0
 2 ADC  172.16.1.4/30      172.16.1.5      ether3                    0
 3 ADo  172.16.1.8/30                      172.16.1.2              110
 4 ADC  172.16.10.0/26     172.16.10.1     VLAN10                    0
 5 ADC  172.16.20.0/28     172.16.20.1     VLAN20                    0
 6 ADo  172.16.30.0/24                     172.16.1.2              110
 7 ADo  172.16.40.0/23                     172.16.1.2              110
 8 ADo  172.16.50.0/25                     172.16.1.2              110
 9 ADo  172.16.60.0/26                     172.16.1.2              110
10 ADo  192.168.2.0/30                     172.16.1.2              110
[admin@MikroTik] > routing ospf route print
 # DST-ADDRESS        STATE         COST                                   GATEWAY          INTERFACE
 0 172.16.1.0/30      intra-area    10                                     0.0.0.0          ether4
 1 172.16.1.4/30      intra-area    10                                     0.0.0.0          ether3
 2 172.16.1.8/30      intra-area    11                                     172.16.1.2       ether4
 3 172.16.10.0/26     intra-area    10                                     0.0.0.0          VLAN10
 4 172.16.20.0/28     intra-area    10                                     0.0.0.0          VLAN20
 5 172.16.30.0/24     intra-area    11                                     172.16.1.2       ether4
 6 172.16.40.0/23     intra-area    11                                     172.16.1.2       ether4
 7 172.16.50.0/25     intra-area    21                                     172.16.1.2       ether4
 8 172.16.60.0/26     intra-area    21                                     172.16.1.2       ether4
 9 192.168.2.0/30     intra-area    21                                     172.16.1.2       ether4
[admin@MikroTik] > routing ospf neighbor print
 0 instance=default router-id=172.16.40.1 address=172.16.1.2 interface=ether4 priority=1 dr-address=172.16.1.1
   backup-dr-address=172.16.1.2 state="Full" state-changes=5 ls-retransmits=0 ls-requests=0 db-summaries=0
   adjacency=31m14s

 1 instance=default router-id=192.168.2.2 address=172.16.1.6 interface=ether3 priority=1 dr-address=172.16.1.6
   backup-dr-address=0.0.0.0 state="Init" state-changes=1 ls-retransmits=0 ls-requests=0 db-summaries=0
[admin@MikroTik] >
```

Cisco CSR routing table and OSPF database and neighbor tables :

```
Router#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 172.16.1.10 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.1.10
      172.16.0.0/16 is variably subnetted, 13 subnets, 7 masks
C        172.16.1.0/30 is directly connected, GigabitEthernet1
L        172.16.1.2/32 is directly connected, GigabitEthernet1
O        172.16.1.4/30 [110/11] via 172.16.1.10, 00:32:55, GigabitEthernet2
                       [110/11] via 172.16.1.1, 00:32:56, GigabitEthernet1
C        172.16.1.8/30 is directly connected, GigabitEthernet2
L        172.16.1.9/32 is directly connected, GigabitEthernet2
O        172.16.10.0/26 [110/11] via 172.16.1.1, 00:32:56, GigabitEthernet1
O        172.16.20.0/28 [110/11] via 172.16.1.1, 00:32:56, GigabitEthernet1
C        172.16.30.0/24 is directly connected, GigabitEthernet3.30
L        172.16.30.1/32 is directly connected, GigabitEthernet3.30
C        172.16.40.0/23 is directly connected, GigabitEthernet3.40
L        172.16.40.1/32 is directly connected, GigabitEthernet3.40
O        172.16.50.0/25 [110/11] via 172.16.1.10, 00:32:55, GigabitEthernet2
O        172.16.60.0/26 [110/11] via 172.16.1.10, 00:32:55, GigabitEthernet2
      192.168.2.0/30 is subnetted, 1 subnets
O        192.168.2.0 [110/11] via 172.16.1.10, 00:32:55, GigabitEthernet2
```

```
Router#sh ip ospf database

            OSPF Router with ID (172.16.40.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.10.1     172.16.10.1     212         0x80000004 0x007073 4
172.16.40.1     172.16.40.1     8           0x80000009 0x00164B 4
192.168.2.2     192.168.2.2     219         0x8000000C 0x007E9D 5

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
172.16.1.1      172.16.10.1     212         0x80000002 0x00D552
172.16.1.10     192.168.2.2     149         0x80000002 0x00656E
Router#sh ip os
Router#sh ip ospf nei
Router#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.2.2       1   FULL/DR         00:00:33    172.16.1.10     GigabitEthernet2
172.16.10.1       1   FULL/DR         00:00:33    172.16.1.1      GigabitEthernet1
Router#
```

Pfsense routing table and OSPF database and neighbor tables :

pfSense.localdomain - [

Certificate error https://192.168.1.1/diag_routes.php

IPv4 Routes

Destination	Gateway	Flags	Use	Mtu	Netif
default	192.168.2.1	UGS	11020	1500	em0
127.0.0.1	link#8	UH	158	16384	lo0
172.16.1.0/30	172.16.1.9	UG1	0	1500	em2
172.16.1.4/30	link#5	U	31	1500	em4
172.16.1.6	link#5	UHS	0	16384	lo0
172.16.1.8/30	link#3	U	28	1500	em2
172.16.1.10	link#3	UHS	0	16384	lo0
172.16.10.0/26	172.16.1.9	UG1	0	1500	em2
172.16.20.0/28	172.16.1.9	UG1	0	1500	em2
172.16.30.0/24	172.16.1.9	UG1	0	1500	em2
172.16.40.0/23	172.16.1.9	UG1	0	1500	em2
172.16.50.0/25	link#11	U	15	1500	em3.5(
172.16.50.1	link#11	UHS	0	16384	lo0
172.16.60.0/26	link#12	U	1	1500	em3.6(
172.16.60.1	link#12	UHS	0	16384	lo0
192.168.1.0/24	link#2	U	4981	1500	em1
192.168.1.1	link#2	UHS	0	16384	lo0
192.168.2.0/30	link#1	U	1	1500	em0
192.168.2.1	0c:fc:fd:83:3e:00	UHS	1752	1500	em0
192.168.2.2	link#1	UHS	0	16384	lo0

Quagga OSPF Neighbors

```
Neighbor ID     Pri State           Dead Time Address         Interface          RXmtL RqstL DBsmL
172.16.40.1       1 Full/DR           35.154s 172.16.1.9      em2:172.16.1.10        0     0     0
```

Quagga OSPF Routes

```
============ OSPF network routing table ============
N    172.16.1.0/30         [11] area: 0.0.0.0
                           via 172.16.1.9, em2
N    172.16.1.4/30         [10] area: 0.0.0.0
                           directly attached to em4
N    172.16.1.8/30         [10] area: 0.0.0.0
                           directly attached to em2
N    172.16.10.0/26        [21] area: 0.0.0.0
                           via 172.16.1.9, em2
N    172.16.20.0/28        [21] area: 0.0.0.0
                           via 172.16.1.9, em2
N    172.16.30.0/24        [11] area: 0.0.0.0
                           via 172.16.1.9, em2
N    172.16.40.0/23        [11] area: 0.0.0.0
                           via 172.16.1.9, em2
N    172.16.50.0/25        [10] area: 0.0.0.0
                           directly attached to em3.50
N    172.16.60.0/26        [10] area: 0.0.0.0
                           directly attached to em3.60
N    192.168.2.0/30        [10] area: 0.0.0.0
                           directly attached to em0
```

Cisco ASA routing table and OSPF database and neighbor tables :

```
ciscoasa# sh route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 192.168.140.2 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.140.2, outside
O        172.16.1.0 255.255.255.252 [110/21] via 192.168.2.2, 00:00:38, inside
O        172.16.1.4 255.255.255.252 [110/20] via 192.168.2.2, 00:00:38, inside
O        172.16.1.8 255.255.255.252 [110/20] via 192.168.2.2, 00:00:38, inside
O        172.16.10.0 255.255.255.192
           [110/31] via 192.168.2.2, 00:00:38, inside
O        172.16.20.0 255.255.255.240
           [110/31] via 192.168.2.2, 00:00:38, inside
O        172.16.30.0 255.255.255.0 [110/21] via 192.168.2.2, 00:00:38, inside
O        172.16.40.0 255.255.254.0 [110/21] via 192.168.2.2, 00:00:38, inside
O        172.16.50.0 255.255.255.128
           [110/20] via 192.168.2.2, 00:00:38, inside
O        172.16.60.0 255.255.255.192
           [110/20] via 192.168.2.2, 00:00:38, inside
C        192.168.2.0 255.255.255.252 is directly connected, inside
L        192.168.2.1 255.255.255.255 is directly connected, inside
C        192.168.140.0 255.255.255.0 is directly connected, outside
L        192.168.140.145 255.255.255.255 is directly connected, outside
```

```
ciscoasa# sh ospf database


            OSPF Router with ID (192.168.140.145) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.10.1     172.16.10.1     1419        0x80000005 0x6e74 4
172.16.40.1     172.16.40.1     17          0x8000000c 0xed71 4
192.168.2.2     192.168.2.2     380         0x80000013 0xefb4 5
192.168.140.145 192.168.140.145 378         0x80000002 0xdc63 1

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
172.16.1.1      172.16.10.1     1419        0x80000003 0xd353
172.16.1.9      172.16.40.1     17          0x80000002 0x 23a
192.168.2.2     192.168.2.2     380         0x80000001 0xfe8e
ciscoasa# sh ospf ne


Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.2.2       1   FULL/DR         0:00:36    192.168.2.2     inside
```

Part III - Management Architecture

3.1 Remote Management

3.1.1 Telnet configuration on cisco router:

```
Router(config)#enable password cisco
Router(config)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#exec-ti
Router(config-line)#exec-timeout 30
Router(config-line)#login
Router(config-line)#login
Router(config-line)#
```

The term "**VTY**" stood for **Virtual teletype and** used to get Telnet or SSH access to Cisco devices.

"0 – 4" means five simultaneous virtual connections to the same device.

And the password to be able to log in. And after 30 minutes, the session will be ended if it is idle.

I have established a telnet connection from the Client in VLAN 20 to Cisco's route:

```
eth0      Link encap:Ethernet  HWaddr 0C:FC:FD:78:4B:00
          inet addr:172.16.20.14  Bcast:172.16.20.15  Mask:255.255.255.240
          inet6 addr: fe80::efc:fdff:fe78:4b00/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8 errors:4 dropped:0 overruns:0 frame:4
          TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1138 (1.1 KiB)  TX bytes:3814 (3.7 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:200 (200.0 B)  TX bytes:200 (200.0 B)

gns3@box:~$ telnet 172.16.1.2

Entering character mode
Escape character is '^]'.


User Access Verification

Password:
Router>en
Password:
Router#
```

3.1.2 SSH configuration on ASA:

There is two way to do it from the console CLI or the ASDM GUI:

We need to have a crypto key to allow SSH and I used RSA modulus1024

Then we enable the local authentication for SSH.

And add a local user account with admin privilege if you don't have one.

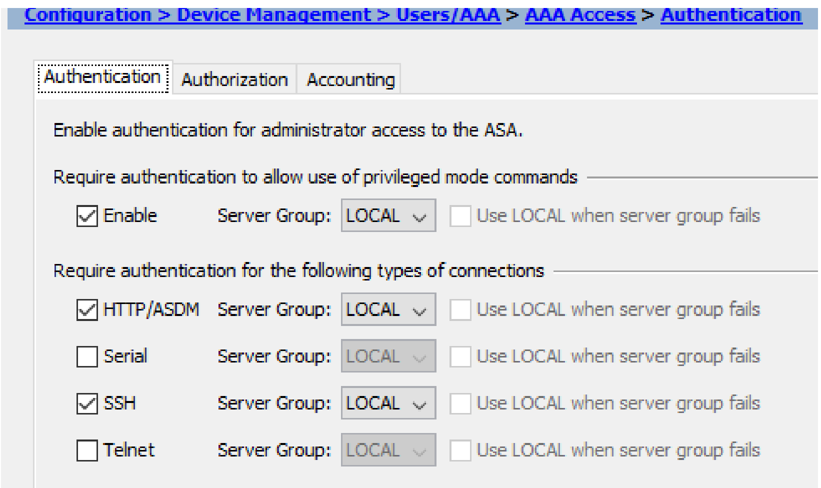
Then allow the network where the Client will be doing SSH to the ASA.

I used ASDM, and I have allowed connections for outside and inside the network. Because It is easier to use my pc than the virtual pc in gns3.

Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH

Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH.

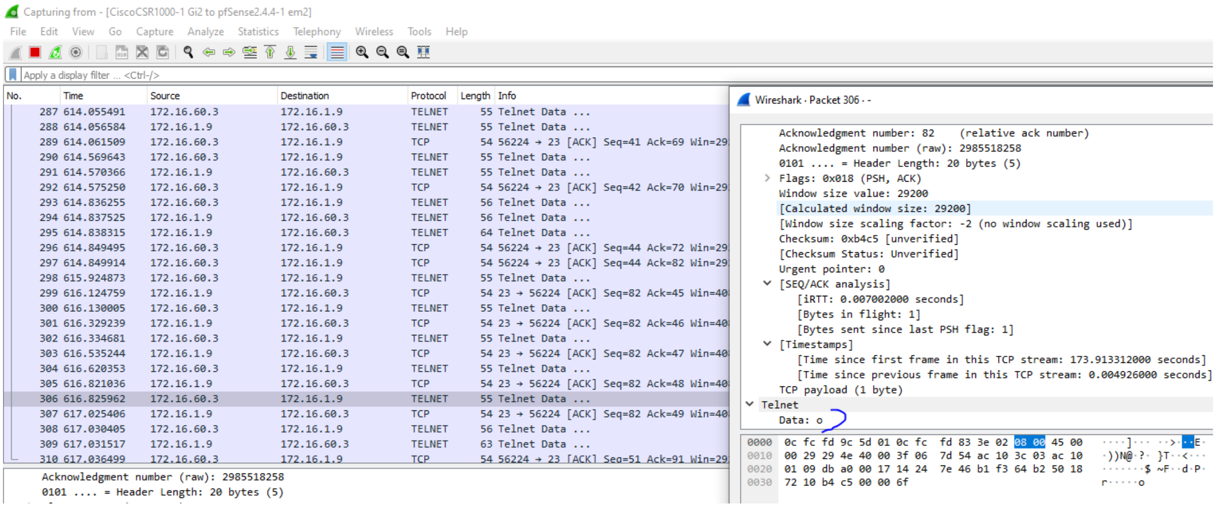
Type	Interface	IP Address	Mask/Prefix Length
ASDM/HTTPS	inside	192.168.2.0	255.255.255.252
SSH	inside	192.168.2.0	255.255.255.252
ASDM/HTTPS	outside	192.168.140.0	255.255.255.0
SSH	outside	192.168.140.0	255.255.255.0



Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock
enable_15	15	Full	N/A	N/A
cisco	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --

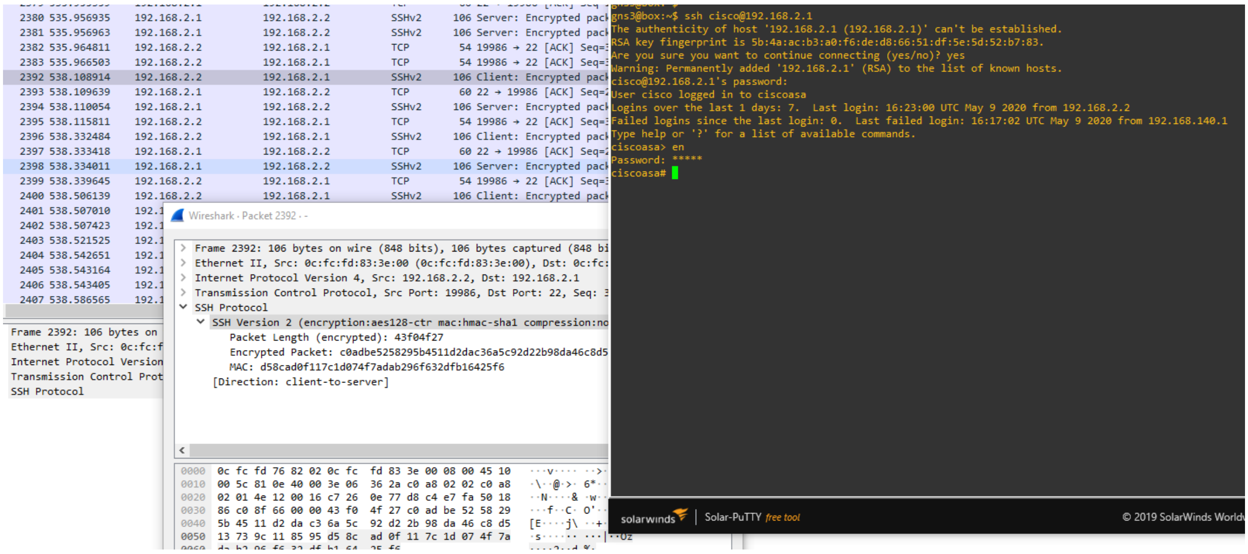
```
gns3@box:~$ ssh cisco@192.168.2.1
cisco@192.168.2.1's password:
User cisco logged in to ciscoasa
Logins over the last 1 days: 6.  Last login: 16:20:27 UTC May 9 2020 from 192.168.2.2
Failed logins since the last login: 0.  Last failed login: 16:17:02 UTC May 9 2020 from 192.168.140.1
Type help or '?' for a list of available commands.
ciscoasa> en
Password: *****
ciscoasa#
```

3.1.3 Packet capture between the Cisco router and PfSense:



The telnet protocol is not secure and doesn't encrypt the data and send it in plaintext. So, I was able to capture the data in plaintext, like the password for the Router. And it is easy to reconstruct the connection again using the info from the capture.

3.1.4 Packet capture between the Cisco router and PfSense:



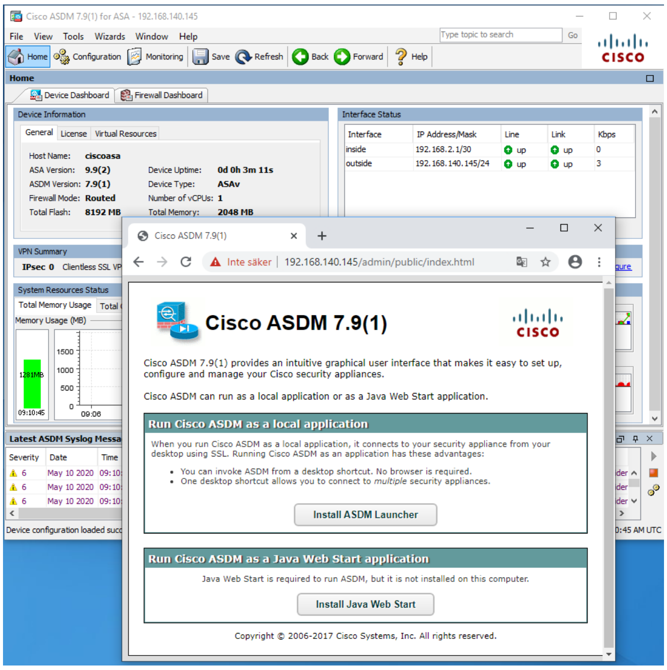
The data was encrypted in the capture. SSH protocol uses public-key to encrypt data when sending it. Therefore, we couldn't reconstruct the connection from the capture info.

And that's why it is recommended to use SSH instead of telnet for security purposes.

3.1.5 Web-based management for both Cisco:

Cisco ASA:

To use ASDM, we need to upload the ASDM image to cisco flash. Create a user account with admin permission and allow traffic to access ASDM. We can connect to the ASA throw webpage using interface IP on HTTPS. Then we can download ASDM to manage the ASA in GUI.



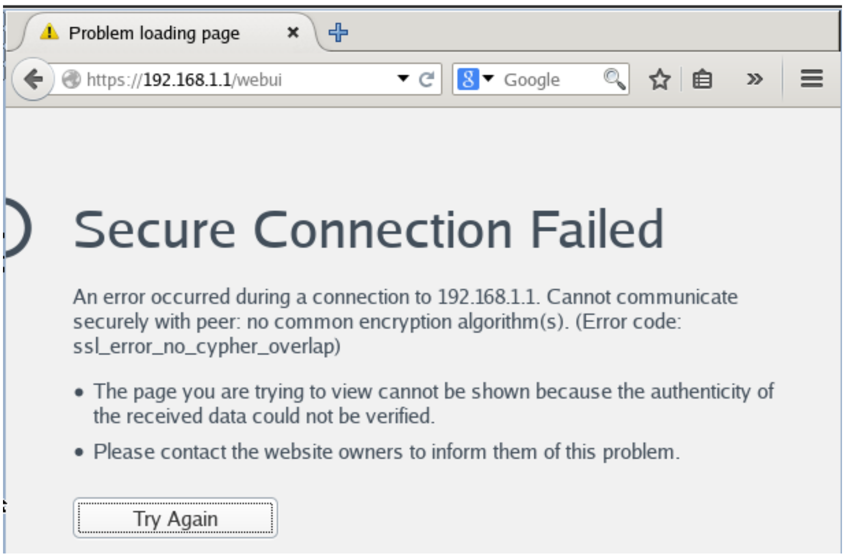
Cisco CSR router:

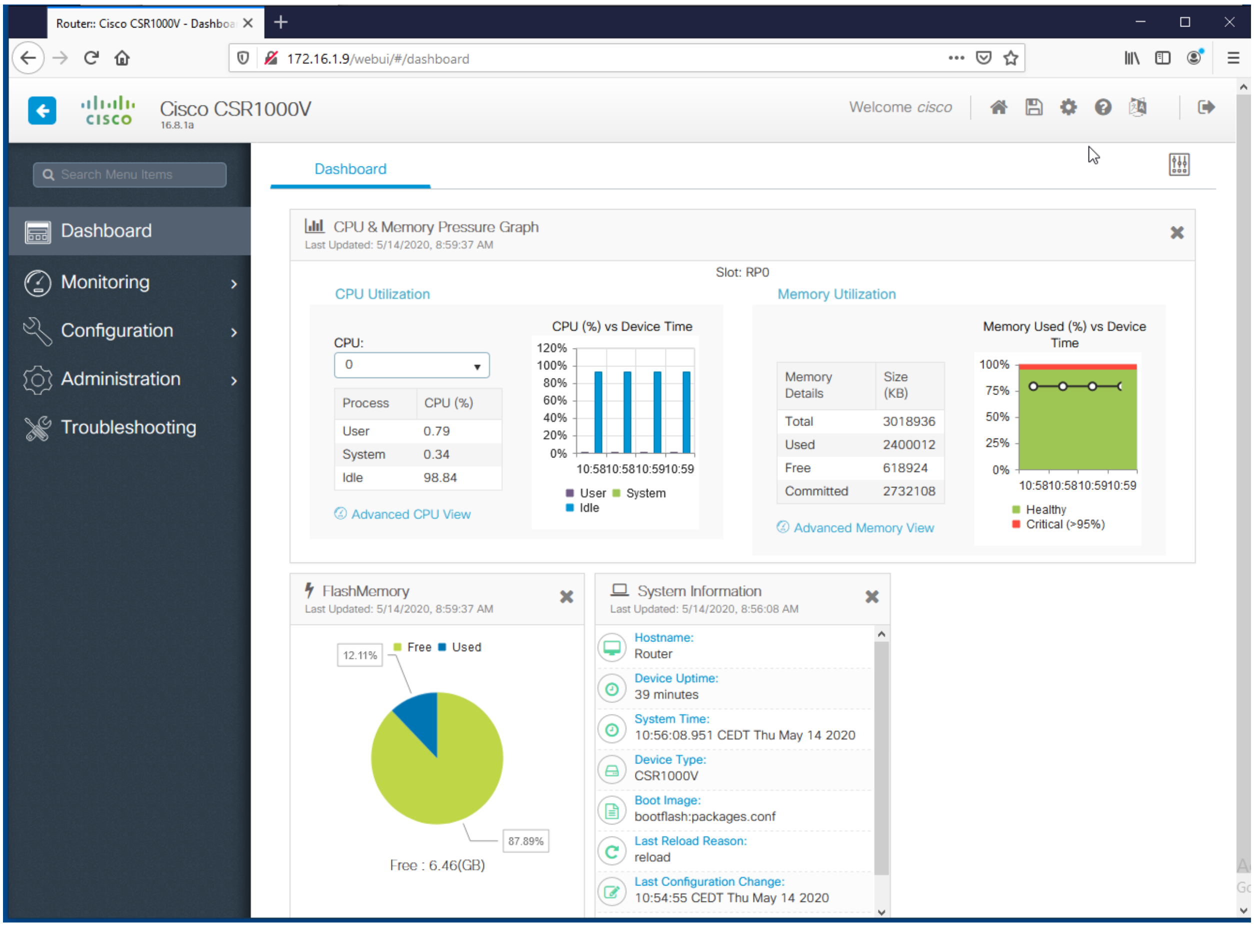
I had added a user account with admin privilege.

```
Router(config)#username cisco privilege 15  password cisco
```

Then I connect from a pc connected to the pfSense router :

I have tried many times, but I could not find any good solution. Maybe if we got a newer version can fix the problem. I have disabled HTTPS, and it works fine then. I can connect to using an IP interface on the Cisco router.





Router:: Cisco CSR1000V - Dashboa
172.16.1.9/webui/#/dashboard
Cisco CSR1000V
16.8.1a
Welcome cisco
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Dashboard
CPU & Memory Pressure Graph
Last Updated: 5/14/2020, 8:59:37 AM
Slot: RP0
CPU Utilization
CPU:
0
Process
CPU (%)
User
0.79
System
0.34
Idle
98.84
CPU (%) vs Device Time
Advanced CPU View
Memory Utilization
Memory Used (%) vs Device Time
Memory Details
Size (KB)
Total
3018936
Used
2400012
Free
618924
Committed
2732108
Healthy
Critical (>95%)
Advanced Memory View
FlashMemory
Last Updated: 5/14/2020, 8:59:37 AM
Free
Used
12.11%
87.89%
Free : 6.46(GB)
System Information
Last Updated: 5/14/2020, 8:56:08 AM
Hostname:
Router
Device Uptime:
39 minutes
System Time:
10:56:08.951 CEDT Thu May 14 2020
Device Type:
CSR1000V
Boot Image:
bootflash:packages.conf
Last Reload Reason:
reload
Last Configuration Change:
10:54:55 CEDT Thu May 14 2020

3.2 Network Management System (NMS)

NTP Network Time Protocol:

I have configured the PfSense to act as an NTP server and uses the pool form ntp.org to synchronize its clock. And the NTP server in PfSense will listen to all interfaces to respond to client requests. I have included the status of NTP below from the PfSense router.

Status / NTP

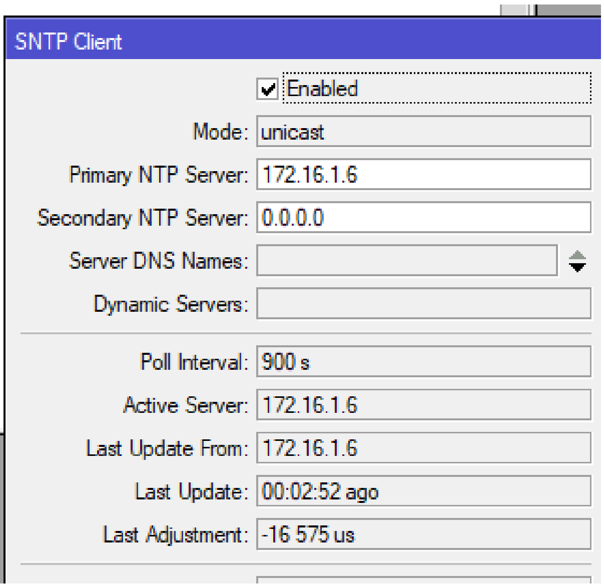
Network Time Protocol Status

Status	Server	Ref ID	Stratum	Type	When	Poll	Reach	Delay	Offset	Jitter
Pool Placeholder	0.pool.ntp.org	.POOL.	16	p	-	64	0	0.000	+0.000	0.008
Pool Placeholder	1.pool.ntp.org	.POOL.	16	p	-	64	0	0.000	+0.000	0.008
Pool Placeholder	2.pool.ntp.org	.POOL.	16	p	-	64	0	0.000	+0.000	0.008
Pool Placeholder	3.pool.ntp.org	.POOL.	16	p	-	64	0	0.000	+0.000	0.008
Selected	95.216.136.148	195.210.189.106	2	u	2	64	377	15.473	-58.060	66.832
Candidate	62.241.198.253	194.100.2.198	2	u	8	64	177	17.291	-100.25	45.951
Candidate	62.241.198.251	193.66.253.102	2	u	14	64	177	16.929	-99.635	46.018
Candidate	162.159.200.123	10.128.8.4	3	u	28	64	377	8.964	-109.69	52.032
Candidate	193.182.111.141	192.36.143.150	2	u	34	64	355	9.954	-89.352	40.690
Candidate	193.182.111.142	194.58.202.20	2	u	37	64	377	10.733	-96.920	50.045
Candidate	91.209.0.17	232.6.188.111	2	u	31	64	357	12.655	-0.038	100.692
Active Peer	192.36.143.130	.PPS.	1	u	34	64	357	9.159	-90.664	52.786
Candidate	79.136.85.193	194.58.204.148	2	u	97	64	376	16.827	-22.772	93.793
Candidate	193.182.111.13	192.36.143.153	2	u	34	64	377	10.165	-109.50	51.019
Candidate	212.181.170.177	194.58.202.20	2	u	96	64	376	13.753	-105.17	63.967

I have configured Mikrotik router, Cisco CSR, And Cisco ASA as the three NTP clients, and I have a screenshot showing that listed below.

Mikrotik sync its clock with pfSense:

```
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] > system ntp client print
              enabled: yes
          primary-ntp: 172.16.1.6
        secondary-ntp: 0.0.0.0
     server-dns-names:
                 mode: unicast
        poll-interval: 2m8s
        active-server: 172.16.1.6
     last-update-from: 172.16.1.6
   last-update-before: 35s220ms
      last-adjustment: 2ms923us
[admin@MikroTik] >
```



Cisco CSR syncs its clock with pfSense:

```
Router#sh clock detail
*16:05:31.869 UTC Mon May 11 2020
Time source is NTP
Router#sh ntp sta
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
ntp uptime is 126400 (1/100 of seconds), resolution is 4000
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 1.48 msec, peer dispersion is 0.00 msec
loopfilter state is 'FREQ' (Drift being measured), drift is 0.000000000 s/s
system poll interval is 64, never updated.
Router#sh ntp ass

  address         ref clock       st   when   poll reach  delay  offset   disp
 ~172.16.1.10     91.209.0.20      3    107     64     1  1.814  16.005 7937.9
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
Router#
```

Cisco ASA syncs its clock with pfSense:

```
ciscoasa# sh clock detail
18:20:12.678 CEDT Mon May 11 2020
Time source is NTP
UTC time is: 16:20:12 UTC Mon May 11 2020
Summer time starts 02:00:00 CEST Sun Mar 29 2020
Summer time ends 03:00:00 CEDT Sun Oct 25 2020
ciscoasa# sh ntp status
Clock is synchronized, stratum 5, reference is 192.168.2.2
nominal freq is 99.9984 Hz, actual freq is 99.9984 Hz, precision is 2**6
reference time is e263f9b9.c778fc6e (18:20:09.779 CEDT Mon May 11 2020)
clock offset is 19.9881 msec, root delay is 10.67 msec
root dispersion is 16193.01 msec, peer dispersion is 15890.63 msec
ciscoasa# sh ntp ass
ciscoasa# sh ntp associations
      address          ref clock     st  when  poll reach  delay  offset    disp
*~192.168.2.2      162.159.200.1     4    24    64    1      1.2    19.99  15890.
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
ciscoasa#
```

Network devices have an internal clock or use a Public Internet Time Server. The problem is that those methods lead to unsynchronized time between the network nodes and will be very difficult for system administrators to make a sequence of events if the devices not appropriately synchronized. So keeping accurate time for all nodes will help in the process of monitoring and analyzing the data throw the network.

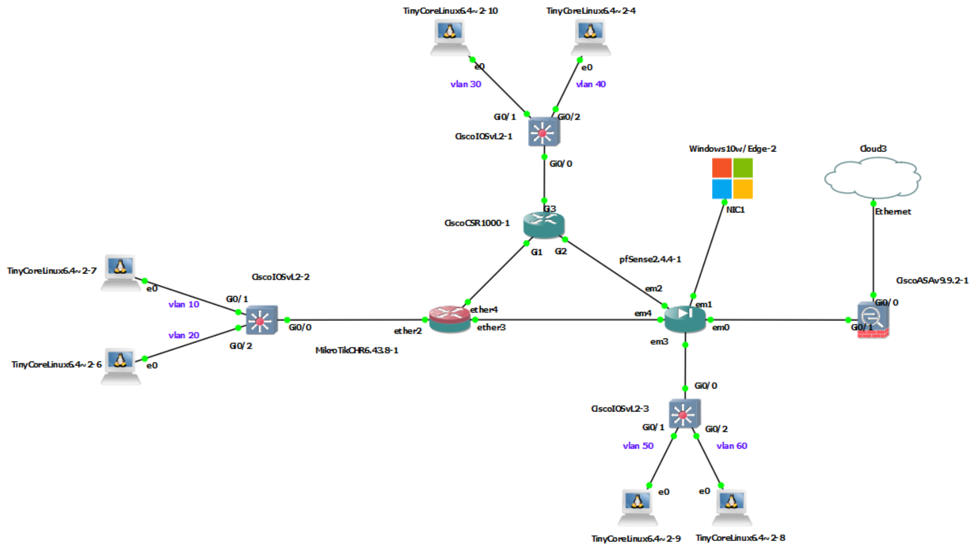
PRTG Network Management System:

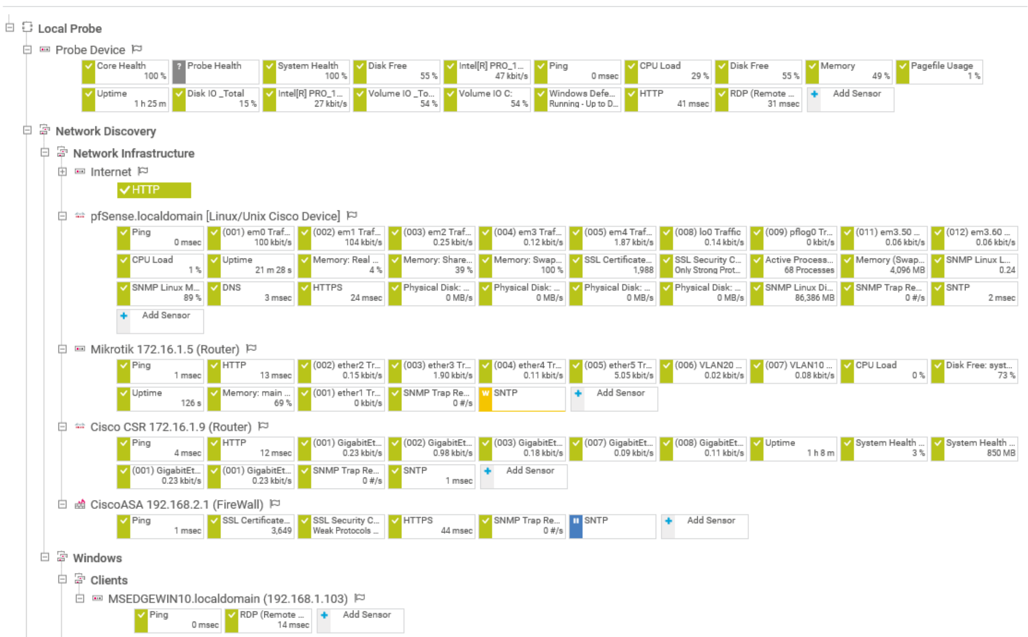
I have installed the management system on a Windows 10 Pc connected to the PfSense router and has IP from DHCP (192.168.1.103). I have discovered some devices, and I have added the rest.

I have Added some sensors like SNTP to monitor track network-wide time coherence

I have configured SNMP in all Router, and I have added SNMP traffic sensors to NMS, as in the screenshot below. And this allows me to collect more info from routers:

The NMS will help us to monitor the whole network devices as many sensors provide different information.





Conclusion

The assignment was a challenge and time-consuming. It takes too much time just to keep the topology alive in our devices. The topology had crashed many times, and I got no choice other than redoing it. Other than those problems that we faced, the assignment was exciting and had many new things to learn.

References

1.1.1
https://teachcomputerscience.com/simplex-half-duplex-full-duplex/
https://study-ccna.com/half-duplex-and-full-duplex/
https://en.wikipedia.org/wiki/Autonegotiation
https://www.techopedia.com/definition/25702/auto-negotiation

1.1.2
What is the difference between CAM and FIB table?
https://networkengineering.stackexchange.com/questions/48870/what-is-the-difference-between-cam-and-fib-table

2.3
About VLANs
https://networklessons.com/switching/intervlan-routing

How to set up NAT - Internet Sharing in Mikrotik Router OS

https://www.youtube.com/watch?v=vbpUqvblXmA

Cisco Router CSR| Configure to access the internet

https://www.youtube.com/watch?v=p3lOshakMss

Mikrotik Manual: Interface/VLAN

https://wiki.mikrotik.com/wiki/Manual:Interface/VLAN

Cisco VLAN Routing

https://www.ccnablog.com/inter-vlan-routing/

Setting up ASA and ASDM in GNS3

https://www.youtube.com/watch?v=_7uPz3G04Hk