SOMAIYA
VIDYAVIHAR UNIVERSITY
K J Somaiya College of Engineering

Somaiya
TRUST

Design and Implementation of End to End Secured Campus Area Network

By
Harsh Panchal – 1813033
Kaushal Patil – 1813038
Shubh Dedhia –1813040
Rohit Shah – 1813042

Project Guide
Dr. Kiran Ajetrao

Table of Contents

1. Introduction
2. Motivation
3. Literature Survey
4. Problem statement
5. Objectives
6. Flowchart
7. Network Topology
8. Data Center Survey
9. Methodology
10. Results & Analysis
11. Conclusion
12. Future work
13. References

Introduction

- Campus Area Network (CAN) is a group of interconnected Local Area Networks (LAN) within a limited geographical area like school campus, university campus, military bases, or organizational campuses and corporate buildings.
- Example of CAN : Let’s think about a university where university networks interconnect academic building, admission building, library, account section, examination section, placement section etc of an institution when connected with each other combine to form Campus Area Network (CAN).

Motivation

- The core motivation behind developing this project is to maximize security on campus in the era of ever increasing data and various threats and attacks associated to it.
- As college data is very crucial when it comes to any level of the campus network so to prevent any privacy breach of any entity a secured network is very much necessary.
- With the Pandemic, Things going virtual and studying/working from home has become the new normal, the security aspect must go hand in hand to ensure smooth functioning of life on virtual campus.

Literature Survey

Publisher	Year	Author	Title	Summary	Gaps Identified	Problem Solved
IJRTE	2019	Mugdha Sharma, Chirag Pupreja, Akash Arora	Design and Implementation of University Network	This paper presents the design of campus area network using Bus topology	There are various topologies for designing a network	In the current network we have used bus topology

Literature Survey

Publisher	Year	Author	Title	Summary	Gaps Identified	Problems Solved
IJETTCS	2014	S. Sudharsan, M. Naga Srinivas, G. Sai Shabareesh, P.Kiran Rao	Campus Network Security And Management	This paper presents the design of campus area network using star topology	Inter department Communication was not possible.	In the current network we have used VLANs for inter department communication using InterVLAN Routinng

Literature Survey

Publisher	Year	Author	Title	Summary	Gaps Identified	Problems Solved
IJPAM	2017	G.Michael	Design And Implementation Of A Secure Campus Network	This paper represented the current network security of the campus network, analyzes security threats to campus network and represented the ways to solve it.	There were various network attacks due to which campus network was not secured.	We prevented ARP Spoofing, DHCP Spoofing, VLAN Hopping to secure campus network

Literature Survey

Publisher	Year	Author	Title	Summary	Gaps Identified	Problems Solved
Researchgate	2011	Lalita Kumari, Swapan Debbarma, Radhey Shyam	Security Problems in Campus Network and Its Solutions	This paper represents the current security status of the campus network and to analyze security threats to campus network	As campus area network is vast and complex there are many network security issues which needs to be resolved	Using Firewall technology, VLAN, encryption technology we can improve security of network

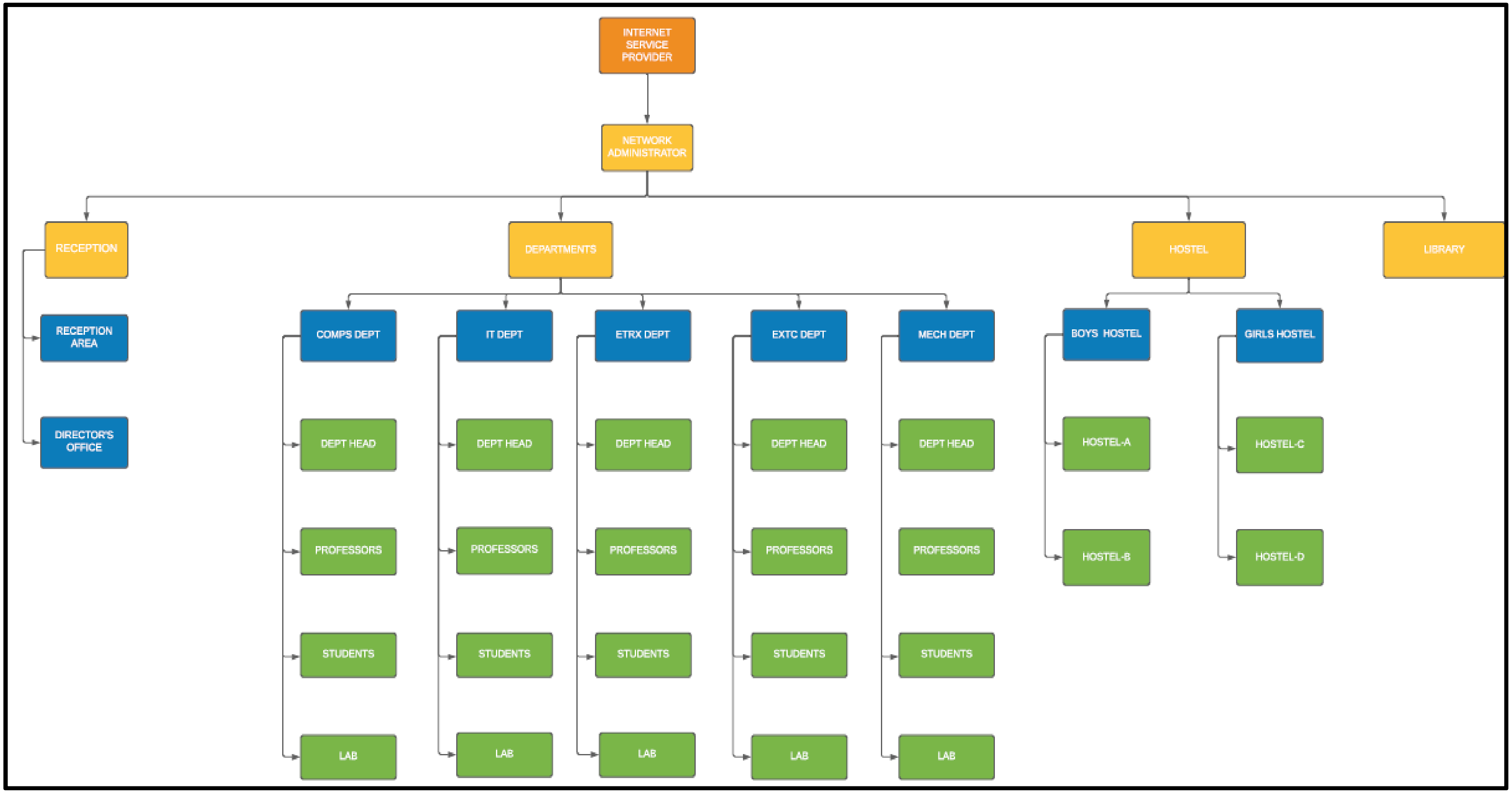
Problem Statement

To maintain data privacy and campus integrity the campus network needs to have secure network design to protect from different types of threats and attacks.

Objectives

- To create design of Secured Campus Area Network.
- Creation of VLANs, OSPFs, ACLs and implementing ASA firewall for internal and external security of network.
- For security of the network, we will identify the threats which are more likely to occur in a campus area network and prevent them.
- Measure network performance parameters of Campus Network

Flowchart

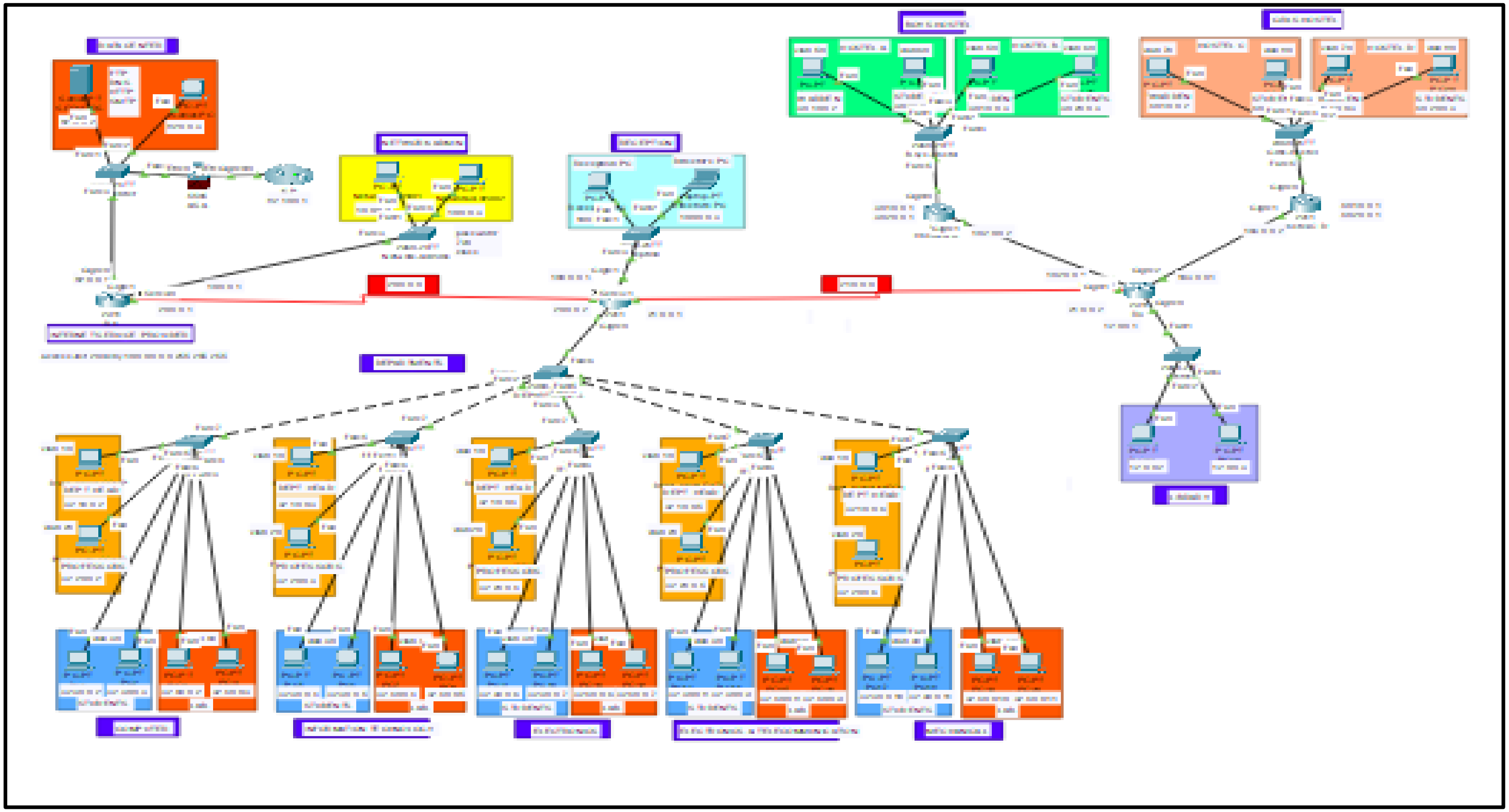


INTERNET SERVICE PROVIDER

NETWORK ADMINISTRATOR

- RECEPTION
  - RECEPTION AREA
  - DIRECTOR'S OFFICE
- DEPARTMENTS
  - COMPS DEPT
    - DEPT HEAD
    - PROFESSORS
    - STUDENTS
    - LAB
  - IT DEPT
    - DEPT HEAD
    - PROFESSORS
    - STUDENTS
    - LAB
  - ETRX DEPT
    - DEPT HEAD
    - PROFESSORS
    - STUDENTS
    - LAB
  - EXTC DEPT
    - DEPT HEAD
    - PROFESSORS
    - STUDENTS
    - LAB
  - MECH DEPT
    - DEPT HEAD
    - PROFESSORS
    - STUDENTS
    - LAB
- HOSTEL
  - BOYS HOSTEL
    - HOSTEL-A
    - HOSTEL-B
  - GIRLS HOSTEL
    - HOSTEL-C
    - HOSTEL-D
- LIBRARY

Network Topology



Data Center Survey

Existing College Network	Our College Network
Fortigate Firewall	ASA Firewall
Layer 2 Device – 2960 Switch (Cisco Nexus 9000)	Layer 2 Device – 2960 Switch
Core Switch (L3 Switch)	L3 Switch is not used
Router is not used	2911 Router
Bus Topology is used	Bus Topology is used
Static Routing is used	OSPF Routing is used
Intervlan Communication is blocked for segregation of college networks	Intervlan Communication is used
Network performance parameters (Bandwidth, Port Bandwidth, Latency)	Network performance parameters (Bandwidth, Port Bandwidth, Latency)
Fortigate Firewall is used to monitor network performance parameters	Nagios, Solar Winds Network monitoring tool will be used

Methodology

1) Virtual LANs (VLANs)

- Created vlans for Dept. Head, Professors, Students and lab for Each of the 5 Departments.
- Created vlans for Boys Hostel (Hostel-A,Hostel-B) and Girls Hostel (Hostel-C, Hostel-D).
- In Boys Hostel, anyone can communicate within Hostel-A,B
- In Girls Hostel, anyone can communicate within Hostel-C,D

2) InterVLAN Routing (Router on stick method)

- Inter VLAN routing is a process in which we make different virtual LANs communicate with each other irrespective of where the VLANs are present (on same switch or different switch).
- Inter Vlan Routing can be achieved through a layer-3 device i.e. Router or layer-3 Switch. When the Inter VLAN Routing is done through Router it is known as Router on a stick.

Methodology

3) Internal Security

1. ARP Spoofing (ARP Poisoning)

- It is used for resolving IP addresses to machine MAC addresses. All the devices which want to communicate in the network, broadcast ARP-queries in the system to find out the MAC addresses of other machines.
- ARP Spoofing constructs a huge number of forced ARP requests and replies packets to overload the switch. The intention of the attacker all the network packets and switch set in forwarding mode.

2. DHCP Snooping

- DHCP snooping is done on switches that connects end devices to prevent DHCP based attack. Basically DHCP snooping divides interfaces of switch into two parts
- Trusted Ports – All the ports which connects management controlled devices like switches, routers, servers etc are made trusted ports.
- Untrusted Ports – All the ports that connect end devices like PC, Laptops, Access points etc are made untrusted port.

Methodology

3. VLAN Hopping

- It is a method of attacking the network resources of the VLAN by sending packets to a port not usually accessible from an end system.
- In VLAN hopping, a threat actor must first breach at least one VLAN on the network. This enables cybercriminals to create a base of operations to attack other VLANs connected to the network.

Methodology

4) OSPF

- Open Shortest Path First (OSPF) is one of the Interior Gateway Protocol (IGP), which helps to find the best routing path between the source and the destination router using its own shortest path first (SPF) algorithm.
- It is a Link-state routing protocol that is used to distribute routing information about data packets within a large Autonomous System.

5) Access-List

- Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks.
- ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

There are 2 types:

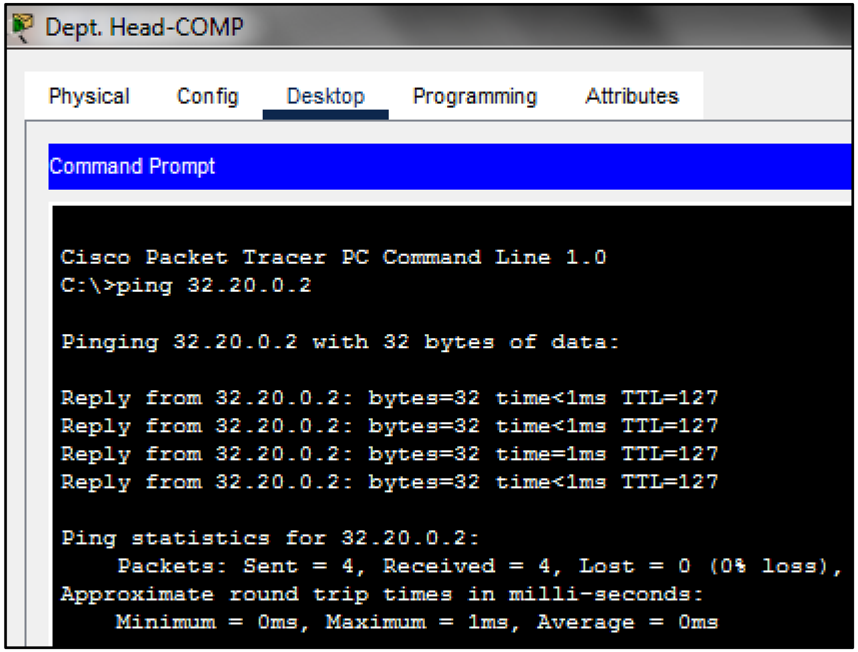
  - Standard Access-List
  - Extended Access-List

Network Performance Parameters

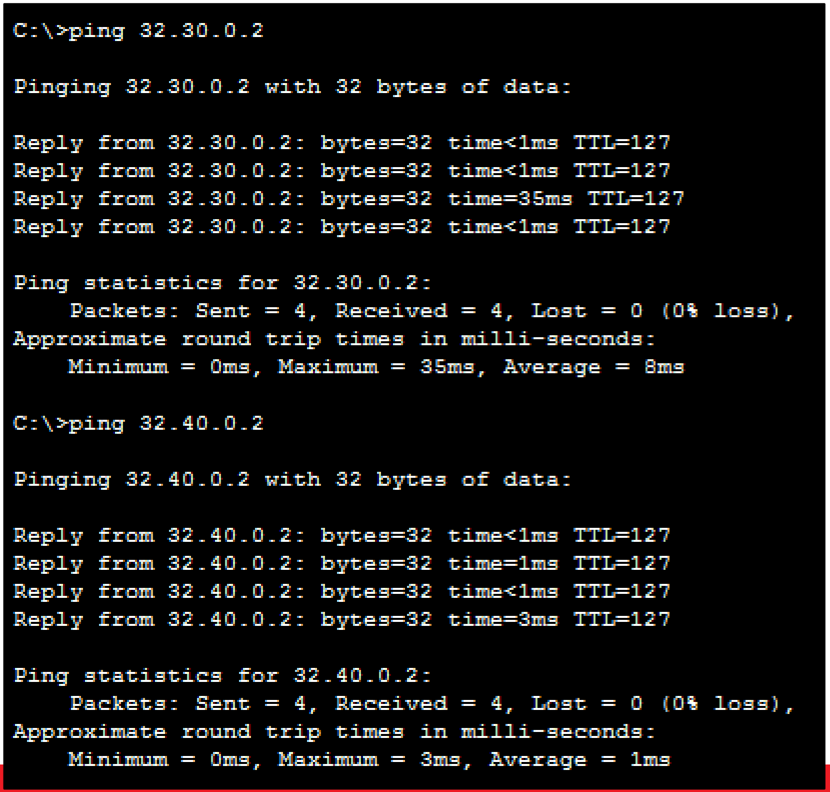
Existing College Network	Our College Network
Port Bandwidth	Bandwidth
Network Traffic	Network Traffic
Throughput	Throughput
---	Latency

Results & Analysis of Intervlan Communication

From Computer Department: Dept. Head can communicate with professors, students, lab of Computer Department and can also communicate with other department's Dept. head, professors, students and lab

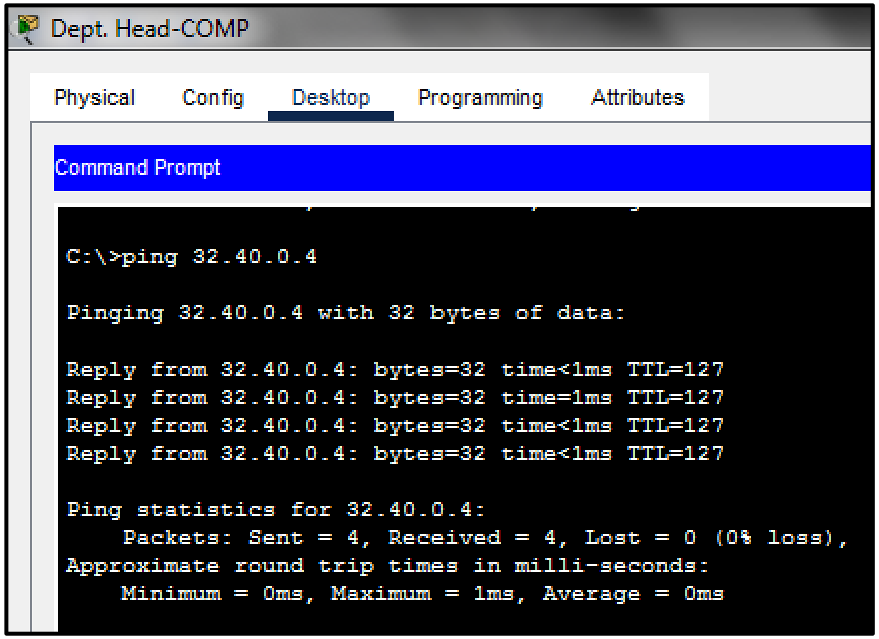


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 32.20.0.2

Pinging 32.20.0.2 with 32 bytes of data:

Reply from 32.20.0.2: bytes=32 time<1ms TTL=127
Reply from 32.20.0.2: bytes=32 time<1ms TTL=127
Reply from 32.20.0.2: bytes=32 time=1ms TTL=127
Reply from 32.20.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 32.20.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

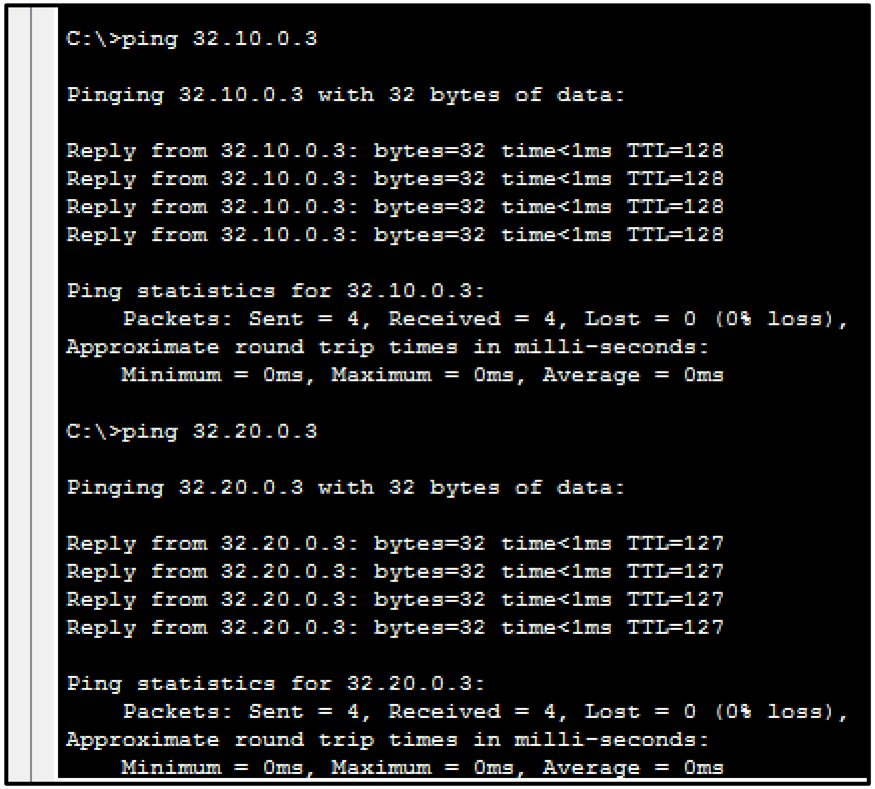


```
C:\>ping 32.30.0.2

Pinging 32.30.0.2 with 32 bytes of data:

Reply from 32.30.0.2: bytes=32 time<1ms TTL=127
Reply from 32.30.0.2: bytes=32 time<1ms TTL=127
Reply from 32.30.0.2: bytes=32 time=35ms TTL=127
Reply from 32.30.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 32.30.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 35ms, Average = 8ms

C:\>ping 32.40.0.2

Pinging 32.40.0.2 with 32 bytes of data:

Reply from 32.40.0.2: bytes=32 time<1ms TTL=127
Reply from 32.40.0.2: bytes=32 time=1ms TTL=127
Reply from 32.40.0.2: bytes=32 time<1ms TTL=127
Reply from 32.40.0.2: bytes=32 time=3ms TTL=127

Ping statistics for 32.40.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

Results & Analysis of Intervlan Communication

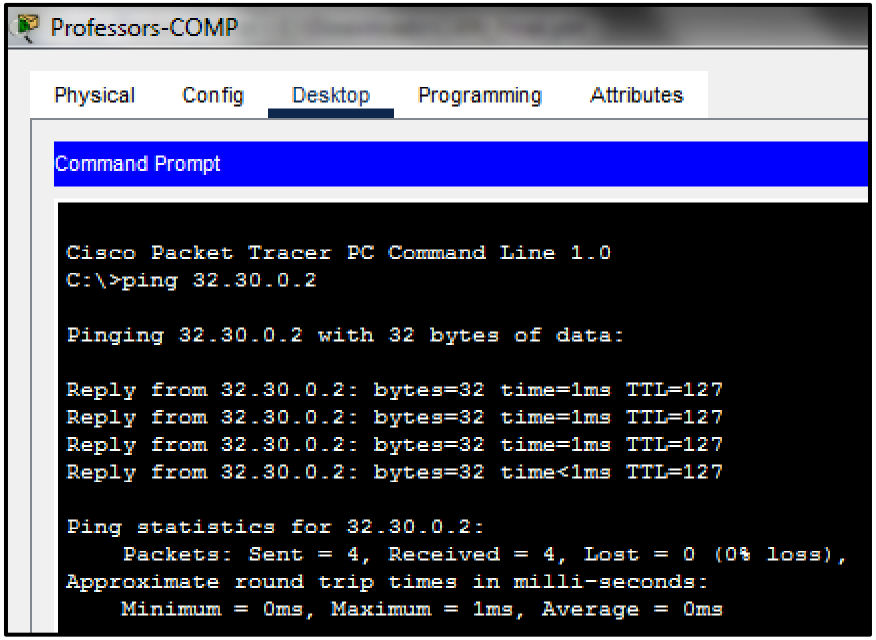


```
C:\>ping 32.40.0.4

Pinging 32.40.0.4 with 32 bytes of data:

Reply from 32.40.0.4: bytes=32 time<1ms TTL=127
Reply from 32.40.0.4: bytes=32 time=1ms TTL=127
Reply from 32.40.0.4: bytes=32 time<1ms TTL=127
Reply from 32.40.0.4: bytes=32 time<1ms TTL=127

Ping statistics for 32.40.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

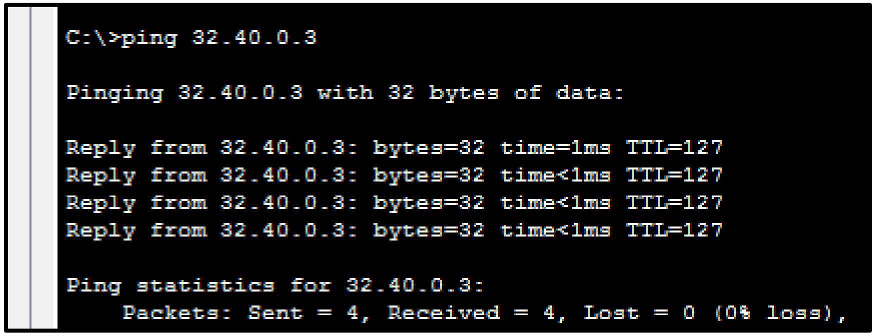


```
C:\>ping 32.10.0.3

Pinging 32.10.0.3 with 32 bytes of data:

Reply from 32.10.0.3: bytes=32 time<1ms TTL=128
Reply from 32.10.0.3: bytes=32 time<1ms TTL=128
Reply from 32.10.0.3: bytes=32 time<1ms TTL=128
Reply from 32.10.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 32.10.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 32.20.0.3

Pinging 32.20.0.3 with 32 bytes of data:

Reply from 32.20.0.3: bytes=32 time<1ms TTL=127
Reply from 32.20.0.3: bytes=32 time<1ms TTL=127
Reply from 32.20.0.3: bytes=32 time<1ms TTL=127
Reply from 32.20.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 32.20.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Results & Analysis of Intervlan Communication



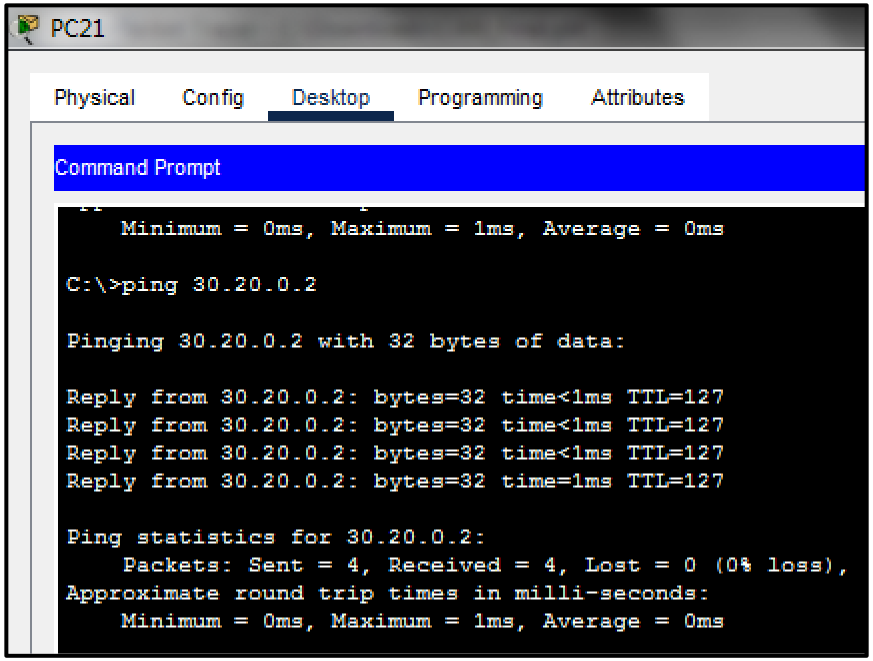
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 32.30.0.2

Pinging 32.30.0.2 with 32 bytes of data:

Reply from 32.30.0.2: bytes=32 time=1ms TTL=127
Reply from 32.30.0.2: bytes=32 time=1ms TTL=127
Reply from 32.30.0.2: bytes=32 time=1ms TTL=127
Reply from 32.30.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 32.30.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



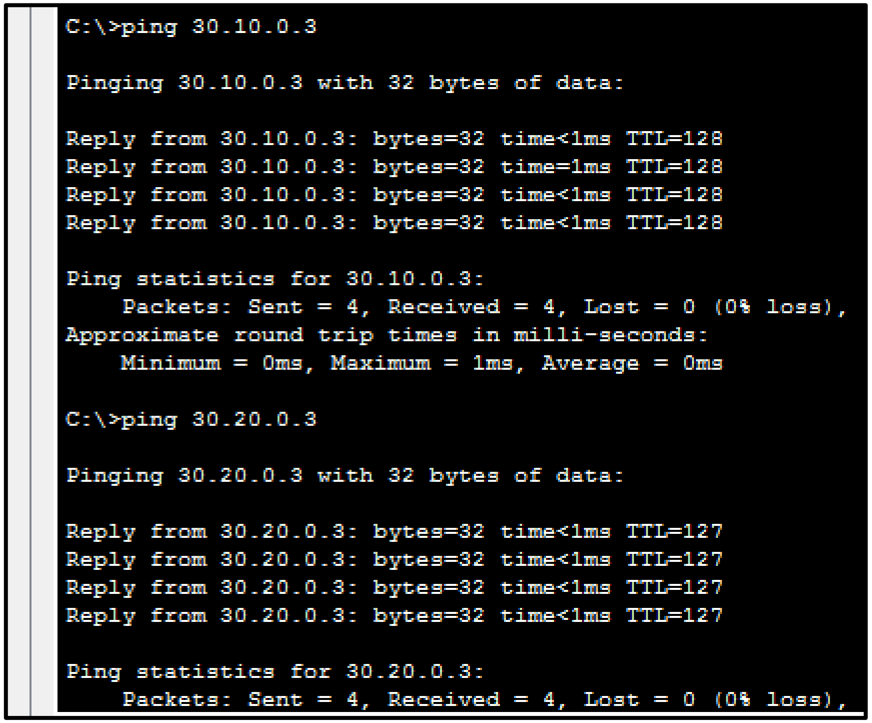
```
C:\>ping 32.40.0.3

Pinging 32.40.0.3 with 32 bytes of data:

Reply from 32.40.0.3: bytes=32 time=1ms TTL=127
Reply from 32.40.0.3: bytes=32 time<1ms TTL=127
Reply from 32.40.0.3: bytes=32 time<1ms TTL=127
Reply from 32.40.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 32.40.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Results & Analysis of Intervlan Communication

From Hostel-A: Warden from Hostel-A can communicate with students of Hostel-A and also warden, students of Hostel-B

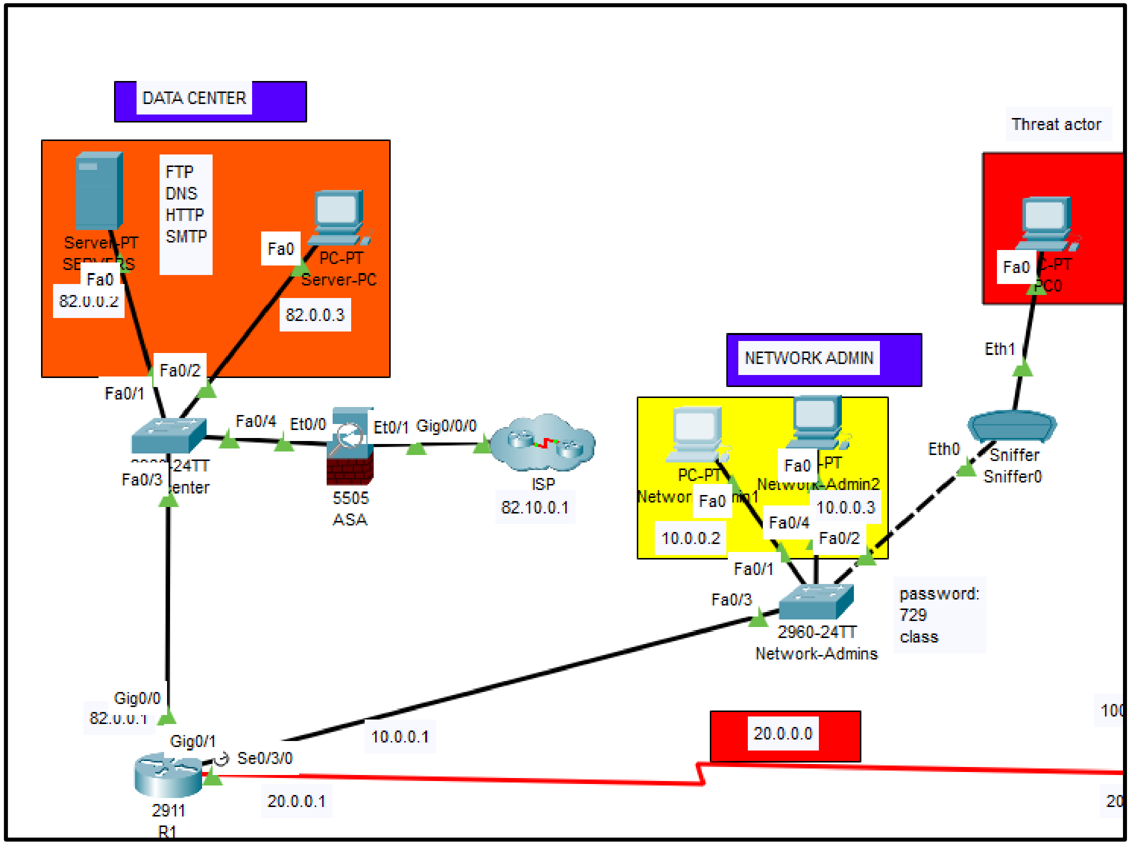


```
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 30.20.0.2

Pinging 30.20.0.2 with 32 bytes of data:

Reply from 30.20.0.2: bytes=32 time<1ms TTL=127
Reply from 30.20.0.2: bytes=32 time<1ms TTL=127
Reply from 30.20.0.2: bytes=32 time<1ms TTL=127
Reply from 30.20.0.2: bytes=32 time=1ms TTL=127

Ping statistics for 30.20.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



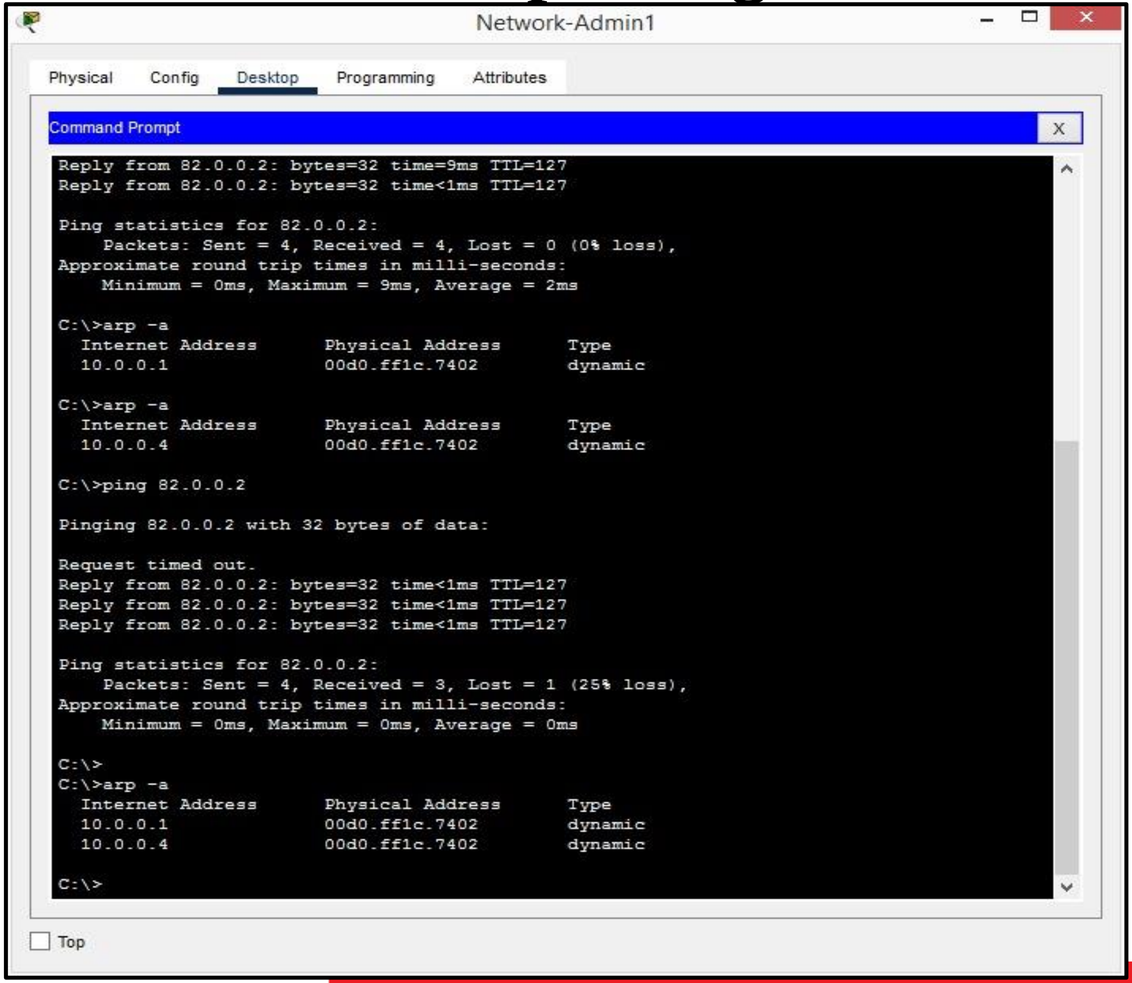
```
C:\>ping 30.10.0.3

Pinging 30.10.0.3 with 32 bytes of data:

Reply from 30.10.0.3: bytes=32 time<1ms TTL=128
Reply from 30.10.0.3: bytes=32 time=1ms TTL=128
Reply from 30.10.0.3: bytes=32 time<1ms TTL=128
Reply from 30.10.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 30.10.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 30.20.0.3

Pinging 30.20.0.3 with 32 bytes of data:

Reply from 30.20.0.3: bytes=32 time<1ms TTL=127
Reply from 30.20.0.3: bytes=32 time<1ms TTL=127
Reply from 30.20.0.3: bytes=32 time<1ms TTL=127
Reply from 30.20.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 30.20.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Results & Analysis of ARP Spoofing



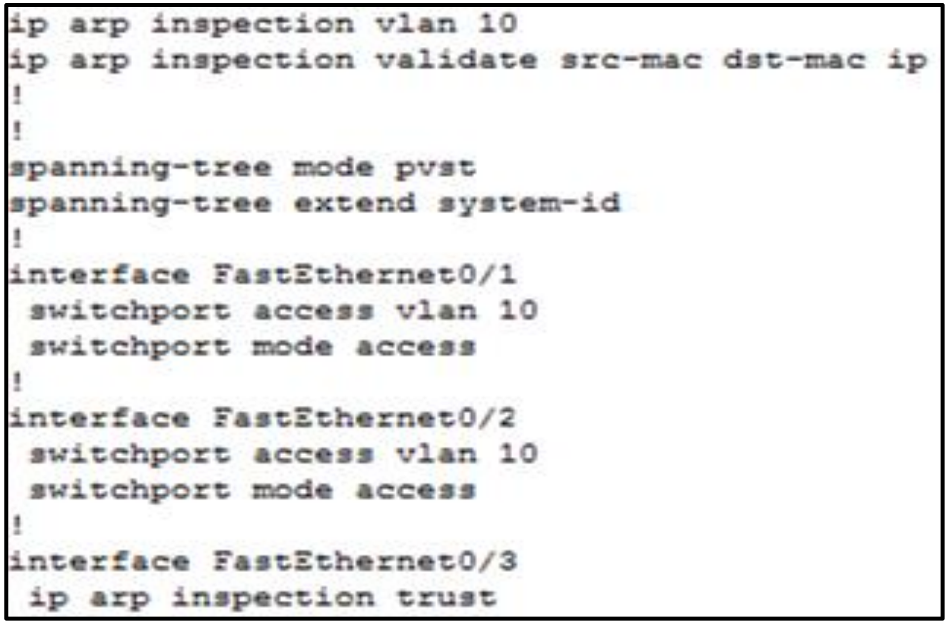
- The threat actor tries to snoop the information exchanged between the network admins and the datacenter.
- The Threat actor is the man in the middle because it has acquired the mac address of the default gateway so ARP spoofing is also called Man in the middle attack

Result of ARP Spoofing Attack



```
Reply from 82.0.0.2: bytes=32 time=9ms TTL=127
Reply from 82.0.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 82.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 2ms

C:\>arp -a
  Internet Address      Physical Address      Type
  10.0.0.1              00d0.ff1c.7402        dynamic

C:\>arp -a
  Internet Address      Physical Address      Type
  10.0.0.4              00d0.ff1c.7402        dynamic

C:\>ping 82.0.0.2

Pinging 82.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 82.0.0.2: bytes=32 time<1ms TTL=127
Reply from 82.0.0.2: bytes=32 time<1ms TTL=127
Reply from 82.0.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 82.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
C:\>arp -a
  Internet Address      Physical Address      Type
  10.0.0.1              00d0.ff1c.7402        dynamic
  10.0.0.4              00d0.ff1c.7402        dynamic

C:\>
```

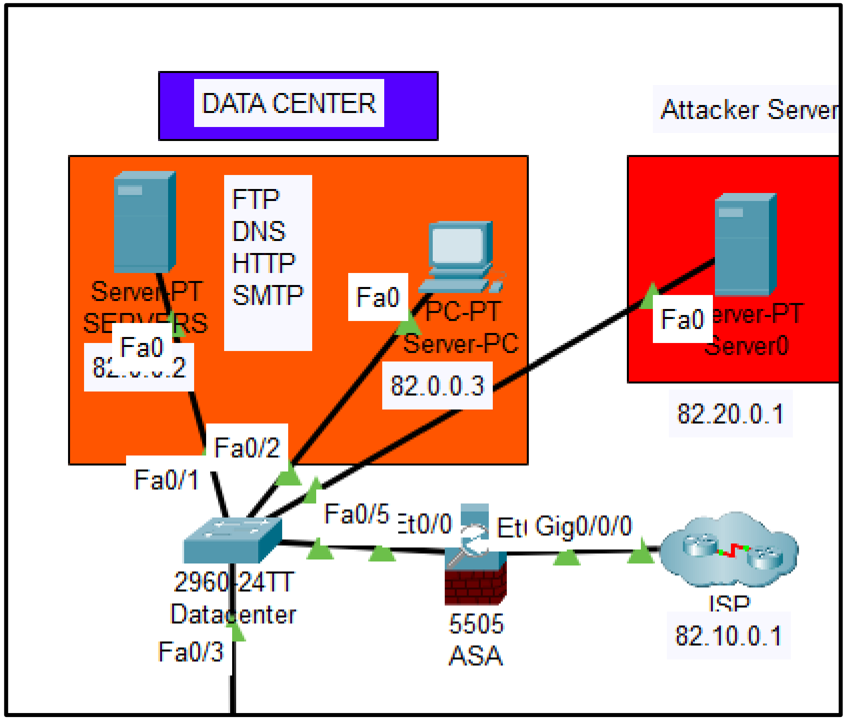
Results & Analysis of Protection against ARP spoofing



```
ip arp inspection vlan 10
ip arp inspection validate src-mac dst-mac ip
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 ip arp inspection trust
```

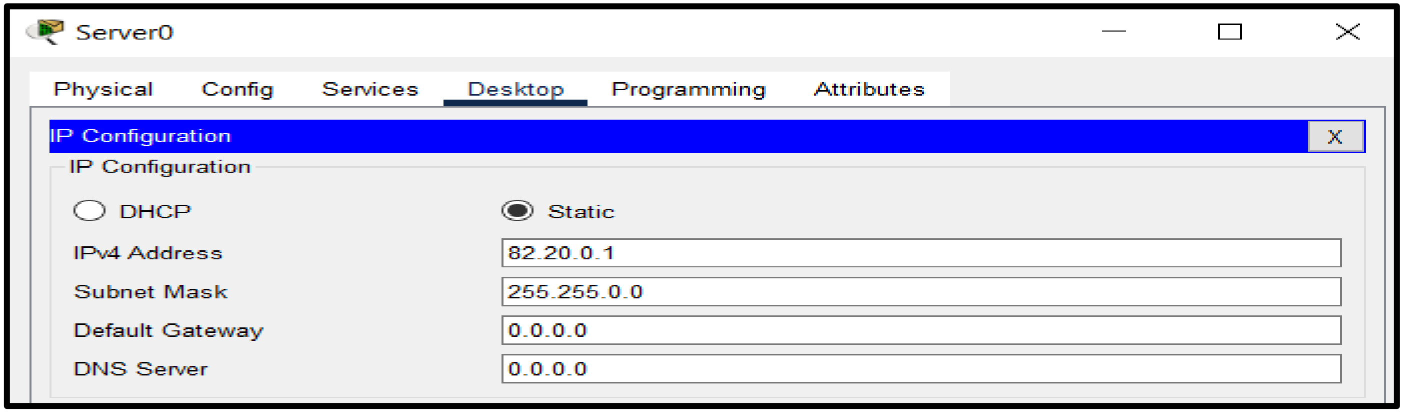
- Fast ethernet port 0/3 is a trusted port. Traffic from that port will have authorization
- VLAN 10 has also undergone dynamic arp inspection VLAN
- Similarly the source and destination mac address are inspected

Results & Analysis of DHCP Snoofing



- The threat Server tries to snoop the information exchanged between the datacenter by creating DHCP Serverpool

Results & Analysis of DHCP Snoofing



IP Configuration

IP Configuration

○ DHCP ● Static

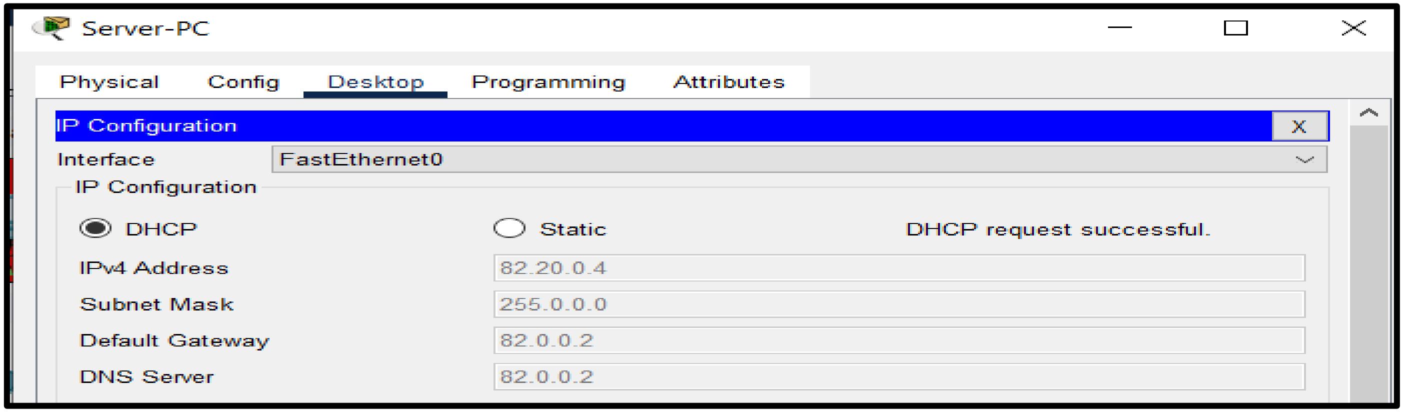
IPv4 Address: 82.20.0.1

Subnet Mask: 255.255.0.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

This is Threat Server's IP Address



IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 82.20.0.4

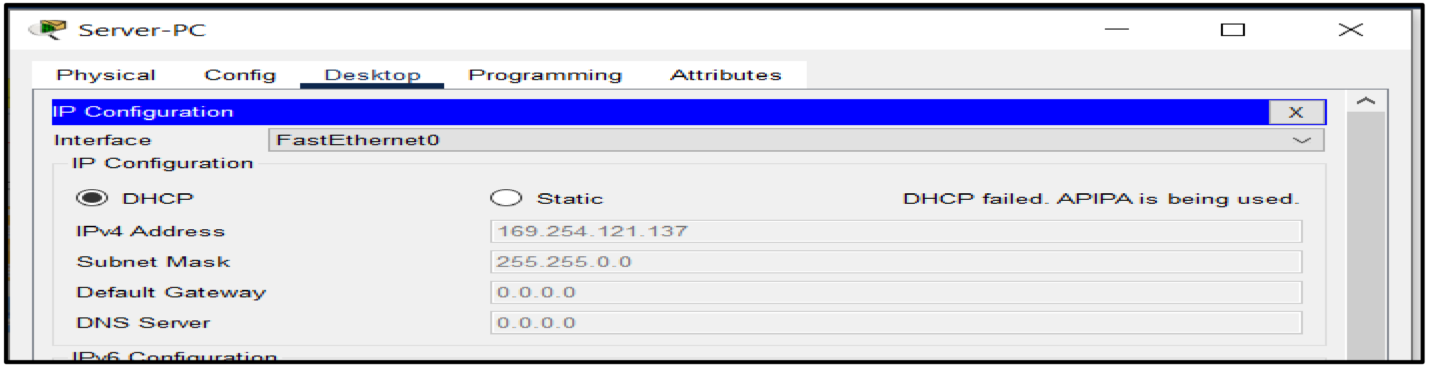
Subnet Mask: 255.0.0.0

Default Gateway: 82.0.0.2

DNS Server: 82.0.0.2

Our PC has dynamically accessed Threat Server IP Address

Results & Analysis of Protection against DHCP Snooping



Server-PC

Physical | Config | Desktop | Programming | Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP failed. APIPA is being used.

IPv4 Address: 169.254.121.137

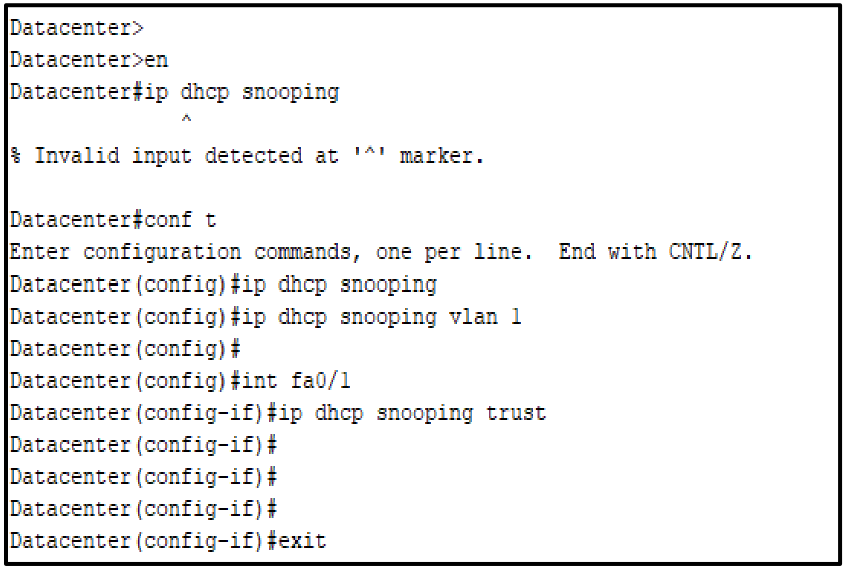
Subnet Mask: 255.255.0.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

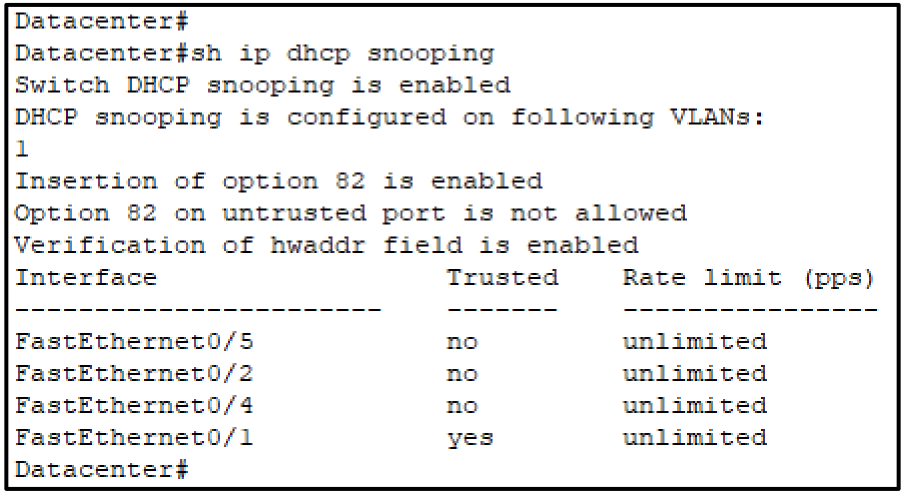
From this image we can see attack is prevented as our pc is unable access ip address



```
Datacenter>
Datacenter>en
Datacenter#ip dhcp snooping
              ^
% Invalid input detected at '^' marker.

Datacenter#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Datacenter(config)#ip dhcp snooping
Datacenter(config)#ip dhcp snooping vlan 1
Datacenter(config)#
Datacenter(config)#int fa0/1
Datacenter(config-if)#ip dhcp snooping trust
Datacenter(config-if)#
Datacenter(config-if)#
Datacenter(config-if)#
Datacenter(config-if)#exit
```

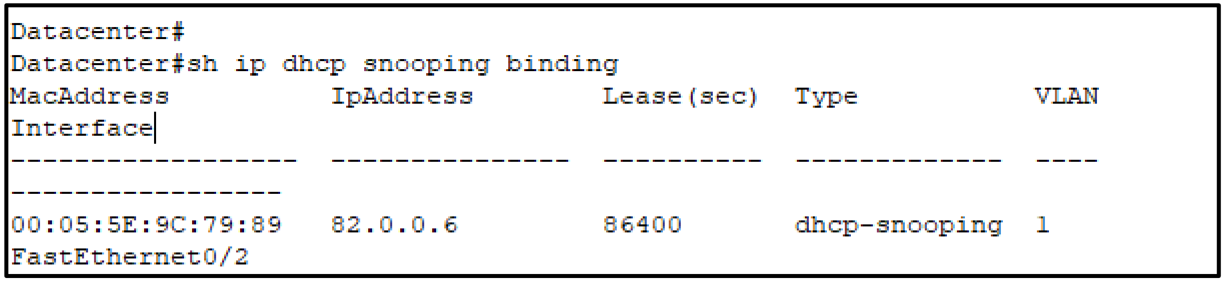
By using these commands we can prevent DHCP Snooping attack

Results & Analysis of Protection against DHCP Snooping



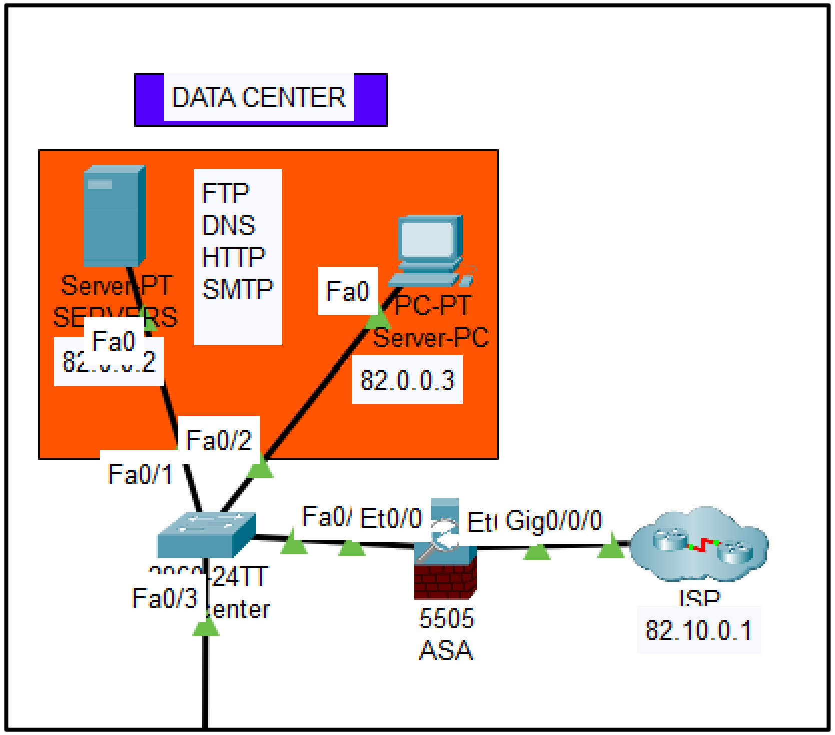
```
Datacenter#
Datacenter#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/5            no         unlimited
FastEthernet0/2            no         unlimited
FastEthernet0/4            no         unlimited
FastEthernet0/1            yes        unlimited
Datacenter#
```

- Fast ethernet 0/1 is set as trusted port and traffic from that port will have authorization
- From binding table we can see ip address of our PC



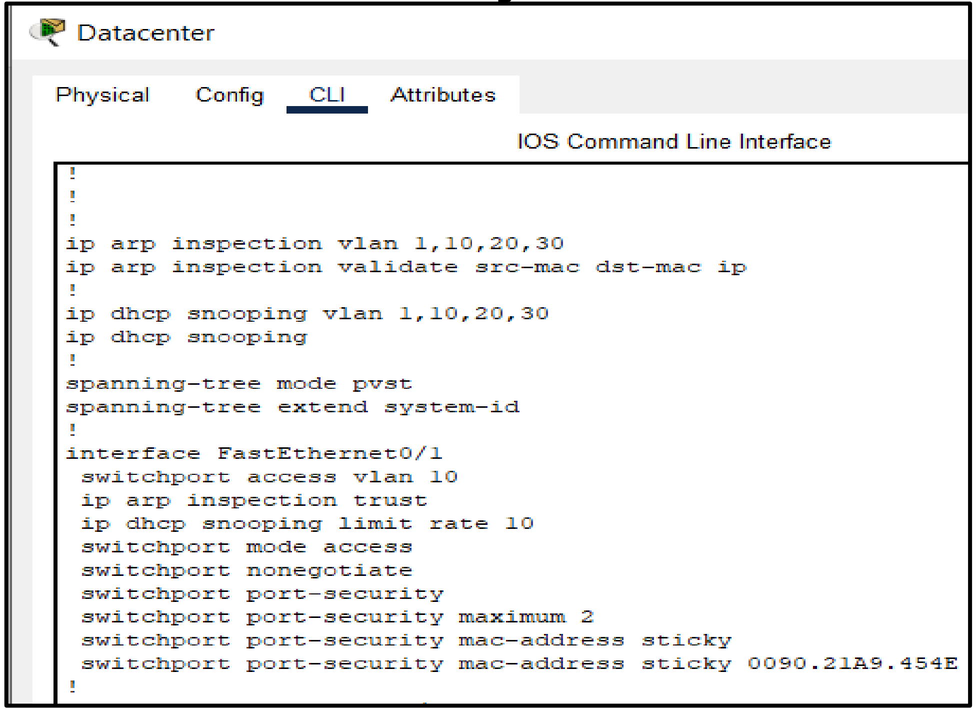
```
Datacenter#
Datacenter#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN
Interface
------------------  ---------------  ----------  -------------  ----
------------------
00:05:5E:9C:79:89   82.0.0.6         86400       dhcp-snooping  1
FastEthernet0/2
```

Results & Analysis of VLAN Hopping



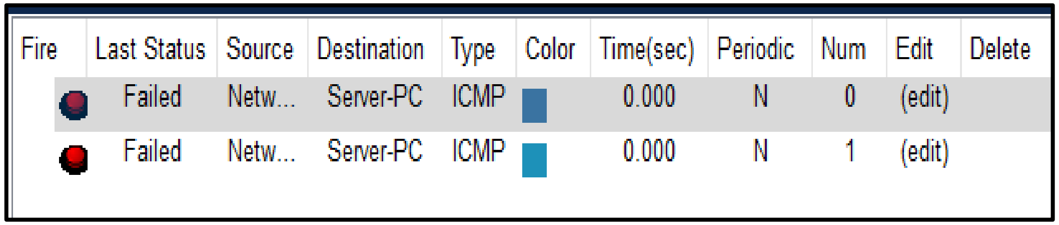
- We created 3 vlans vlan 10 for Servers, vlan 20 for data center and vlan 30 for unused ports
- We used switchport nonegotiate command to disable dtp server

Results & Analysis of VLAN Hopping



```
!
!
!
ip arp inspection vlan 1,10,20,30
ip arp inspection validate src-mac dst-mac ip
!
ip dhcp snooping vlan 1,10,20,30
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
 ip arp inspection trust
 ip dhcp snooping limit rate 10
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0090.21A9.454E
!
```

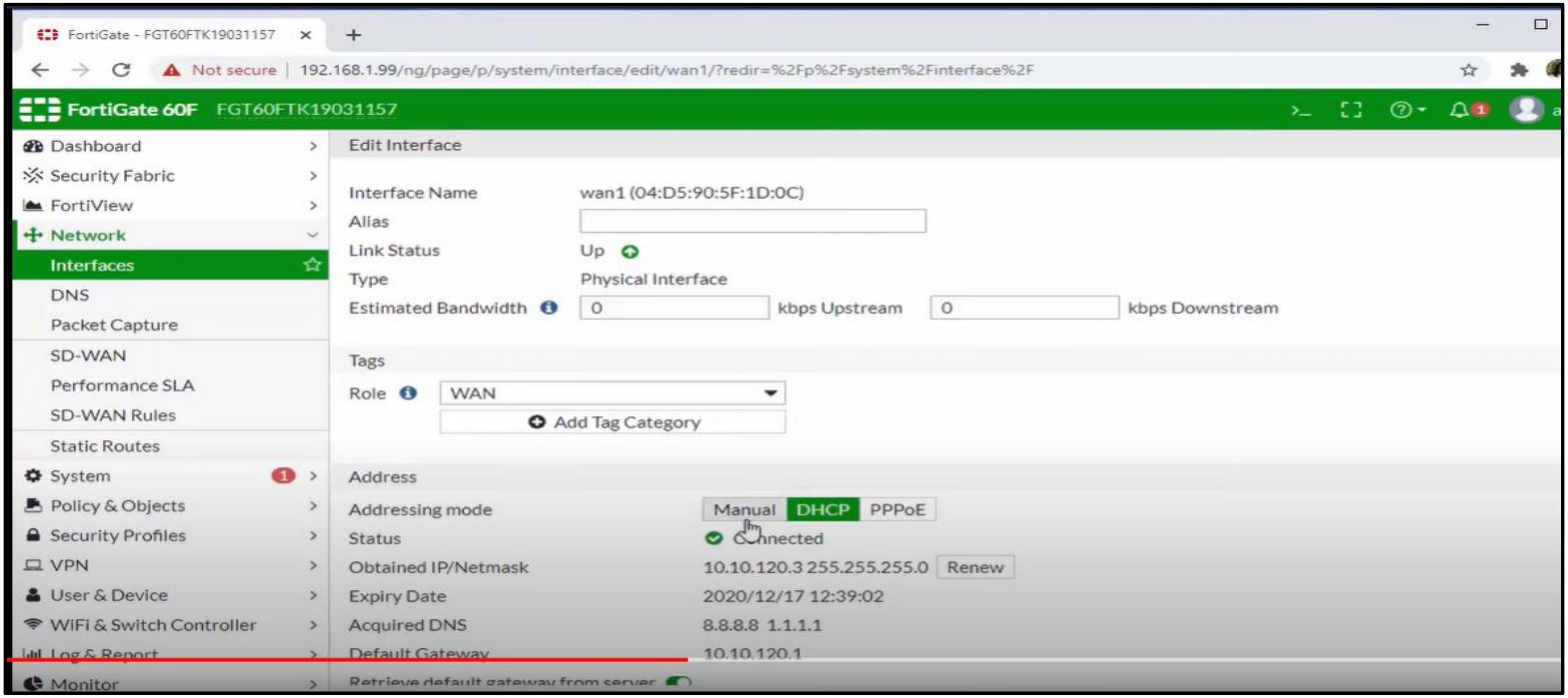
By using these commands we can prevent VLAN Hopping attack



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Failed	Netw...	Server-PC	ICMP	🟦	0.000	N	0	(edit)	
●	Failed	Netw...	Server-PC	ICMP	🟦	0.000	N	1	(edit)	

We can see traffic from outside network is unable to communicate with Datacenter

Results of Network Performance Parameters on Fortigate Firewall



Edit Interface

Interface Name wan1 (04:D5:90:5F:1D:0C)

Alias

Link Status Up

Type Physical Interface

Estimated Bandwidth 0 kbps Upstream 0 kbps Downstream

Tags

Role WAN

Address

Addressing mode Manual **DHCP** PPPoE

Status Connected

Obtained IP/Netmask 10.10.120.3 255.255.255.0

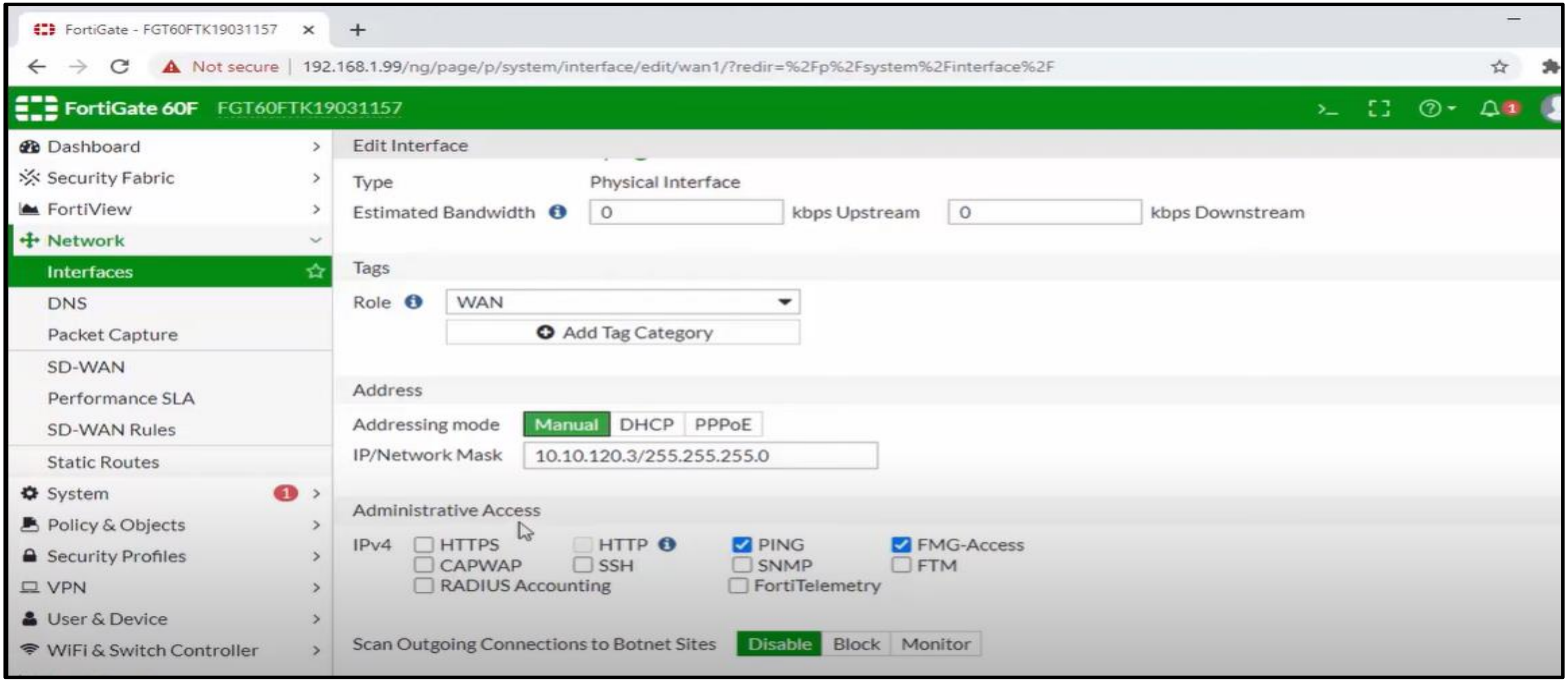
Expiry Date 2020/12/17 12:39:02

Acquired DNS 8.8.8.8 1.1.1.1

Default Gateway 10.10.120.1

Retrieve default gateway from server

Results of Network Performance Parameters on Fortigate Firewall



192.168.1.99/ng/page/p/system/interface/edit/wan1/?redir=%2Fp%2Fsystem%2Finterface%2F

FGT60FTK19031157

Edit Interface

Type: Physical Interface

Estimated Bandwidth: 0 kbps Upstream, 0 kbps Downstream

Tags

Role: WAN

Add Tag Category

Address

Addressing mode: [✓ Manual] DHCP PPPoE

IP/Network Mask: 10.10.120.3/255.255.255.0

Administrative Access

IPv4: □ HTTPS □ HTTP ☑ PING ☑ FMG-Access □ CAPWAP □ SSH □ SNMP □ FTM □ RADIUS Accounting □ FortiTelemetry

Scan Outgoing Connections to Botnet Sites: [✓ Disable] Block Monitor

Conclusion

- We created design of Campus Area Network using Cisco Packet Tracer.
- We learned and implemented VLANS for segregation (Dept. Head, Professors, Students & Labs), InterVlan Routing (Router on Stick Method) for interVlan communication between different departments, OSPF Routing Protocol for finding best routing path , Access-Control Lists to permit & deny traffic.
- We learned about different servers such as (DNS, HTTP, SMTP, FTP, DHCP) and added these multiple services in one server.
- We have done data center survey to know about existing college network for comparative analysis with our design of campus network.
- We learned and prevented common attacks that are possible in campus network such as (ARP Spoofing, DHCP Snooping, VLAN Hopping).

Future Work

- Working on Network Performance Parameters
- Working on ASA firewall using GNS3
- Validation of Small network using Hardware Setup.

References

1. Mugdha Sharma, Chirag Pupreja, Akash Arora “Design and Implementation of University Network” July 2019 International Journal of Recent Technology and Engineering (IJRTE)

2. S. Sudharsan, M. Naga Srinivas, G. Sai Shabareesh, P.Kiran Rao “Campus Network Security and Management” November-December 2014 International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)

3. Lalita Kumari Radhey Shyam Swapan Debbarma “Security Problems in Campus Problems and its solutions” January 2011 ResearchGate

4. G.Michael “Design and Implementation of a Secure Campus Network” 2017 2017 International Journal of Pure and Applied Mathematics(IJPAM)

5. Mohammed Nadir Bin Ali Prof. Dr. M. Lutfar Rahman Prof. Dr. Syed Akhter Hossain “Network Architecture and Security Issues in Campus” 2013 Networks Institute of Electrical and Electronics Engineers(IEEE)

References

6. Md. Nadir Bin Ali "Design and Implementation of a Secure Campus Network" July 2015 ResearchGate

7. Zaka Ullah Muhammad Zulkifl Hasan "Implementation Challenges in Campus Network Security" November 2017

8. Khaing Khaing Wai,Thuzar Khin ,Khin Thet Mar "Design and Simulation of Campus Area Network using Cisco Packet Tracer" 2019 International Journal of New Technologies in Science and Engineering

9. Joysankar Bhattacharjee "Design and Implementation of a Cost-effective and Secured Private Area Network for smooth as well as hassle-free Computing in the University Campus" Jan - Feb 2016 IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)

10. Thin Naing , Aung Nway "Design and Implementation of a Secure Network Connection of the University" IJARIIE-ISSN(O)
11. https://www.youtube.com/watch?v=wd2foo3_EBM&t=136s

THANK YOU