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

- Introduction
- Motivation
- Literature Survey
- Data Center Survey
- Problem statement
- Objectives
- Flowchart
- Methodology
- Network Topology
- Results & Analysis
- Conclusion
- Future Scope
- References

Introduction

The main goal of this project is to make secured campus network design to protect against common internal attacks such as ARP Spoofing, DHCP Snooping, VLAN Hopping, and DOS attacks. As Network security is a growing concern in today’s digital phenomenon it is imperative to have an system in place to protect the data and system from common attacks, approve or block unauthorized access and monitor traffic using network monitoring tool.

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
IEEE	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 which were quite expensive.	In the current network we have used bus topology as it is a cost effective

Literature Survey

Publisher	Year	Author	Title	Summary	Gaps Identified	Problems Solved
IEEE	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 area was not secured.	By making hierarchical network design, the network could resist most of network attacks and hence security was improved

Literature Survey

Publisher	Year	Author	Title	Summary	Gaps Identified	Problems Solved
IEEE	2013	M. N. B. Ali, M. L. Rahman and S. A. Hossain	Network architecture and security issues in campus networks	This paper represents the hireachical campus network design and dhcp snooping attack is discussed and mitigated	As several techniques for mitigating attacks are discussed but in this only dhcp attacks is mitigated	As per data center survey most common attacks are ARP Spoofing, DHCP Snooping, VLAN Hopping so we prevented these attacks

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

Literature Survey

Publisher	Year	Author	Title	Summary	Gaps Identified	Problems Solved
IEEE	2014	X. Li and T. Jiang	Design and Implementation of the Campus Network Monitoring System	This paper represents technical analysis of network monitoring as to ensure network stability and monitor the traffic in network	As there are various network parameters which are useful for network such as Bandwidth, Throughput, Jitter,	Using PRTG Network Monitoring we measured network parameters such as throughput, Bandwidth, Jitter, Port Range

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, Throughput, Jitter)
Fortigate Firewall is used to monitor network performance parameters	PRTG, Solar Winds Network monitoring tool will be used

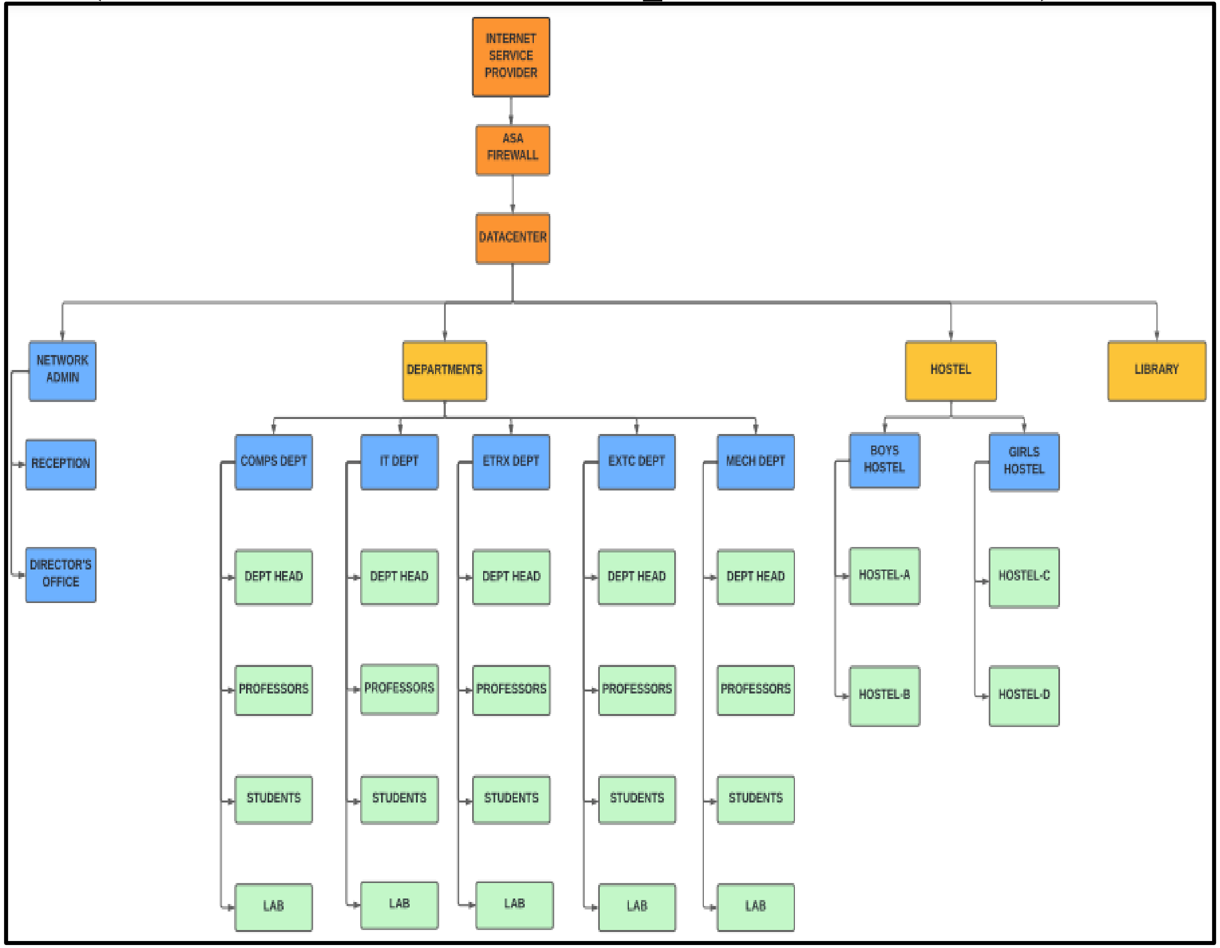
Problem Statement

To maintain campus integrity, the campus network needs to have secure network design to protect from different types of attacks.

Objectives

- To create design of Secured Campus Area Network.
- Creation of VLANs, OSPFs, ACLs for internal 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 (Overview of campus network)



Methodology

Step 1: Gathering Network Requirements (No. of networks, network devices, subnets)

Step 2: Subnetting (Addressing Tables)

Step 3: VLANs Configuration (For Departments & Hostels)

Step 4: InterVLAN Configuration (For Departments & Hostels)

Step 5: Routing Configuration

Step 6: ACLs Configuration

Step 7: Common Attacks prevented

Step 8: Network Performance Parameters Measured by integrating GNS3 with PRTG

Methodology

Step 1: Gathering Network Requirements

From Flowchart (Overview of campus network) we can see different sections created such as Data-center, Network-admins, Reception, Library, Departments

Methodology

Step 2: Subnetting (Addressing Tables)

Example of Addressing table of Data-center

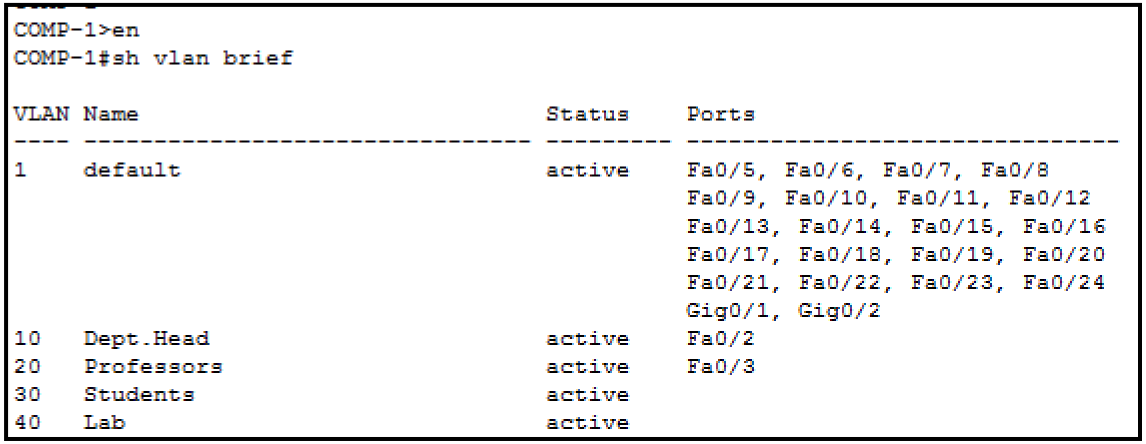
Hostname	IP address	Subnet Mask	Default gateway
Servers	82.0.0.2	255.0.0.0	82.0.0.1
Server-PC	82.0.0.3	255.0.0.0	82.0.0.1
ISP Router	82.10.0.1	255.0.0.0	82.10.0.1

In data-center there is one server which consists of 4 servers. i.e. DNS, HTTP, SMTP, FTP. It also has a PC to access the servers. All the data of the entire campus is stored in server room.

Methodology

Step 3: VLANs Configuration (For Departments & Hostel)

- Created 4 VLANs for each department
- VLAN 10 - Dept Head - 32.10.0.0, VLAN 20 - Professors - 32.20.0.0, VLAN 30 - Students - 32.30.0.0, VLAN 40 - Lab - 32.40.0.0
- Similarly 2 VLANs are created in each hostel i.e. VLAN 50 - Students and VLAN 60 - warden

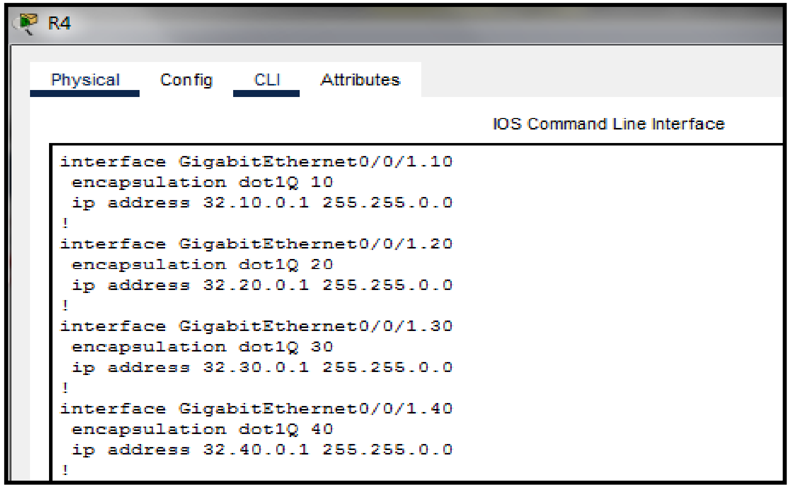


```
COMP-1>en
COMP-1#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   Dept.Head                        active    Fa0/2
20   Professors                       active    Fa0/3
30   Students                         active
40   Lab                              active
```

Methodology

Step 4: InterVLAN Configuration (For Departments & Hostel)

- Router-on-stick method is used for intervlan Routing.
- By this method dept. head, professors, students and lab can communicate with each other.
- Similarly in hostel, warden and students can communicate with each other

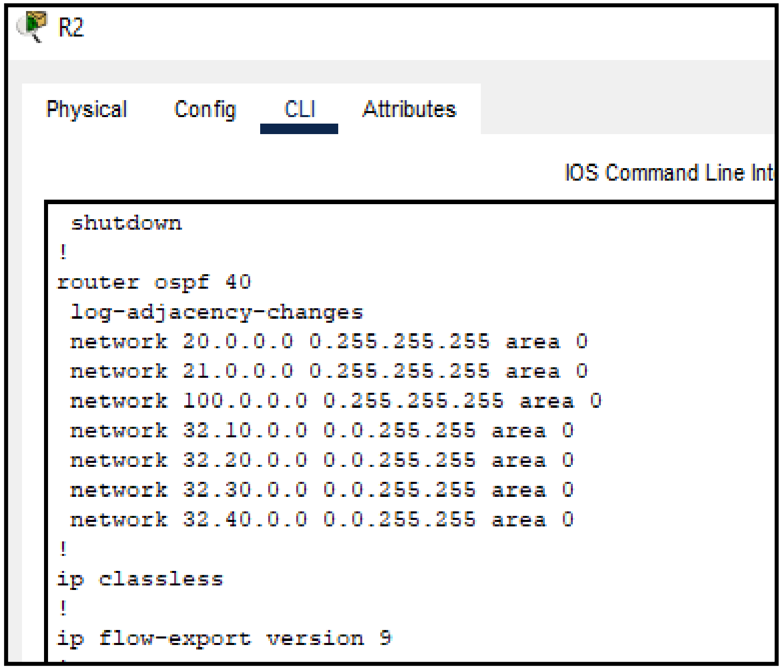


```
interface GigabitEthernet0/0/1.10
 encapsulation dot1Q 10
 ip address 32.10.0.1 255.255.0.0
!
interface GigabitEthernet0/0/1.20
 encapsulation dot1Q 20
 ip address 32.20.0.1 255.255.0.0
!
interface GigabitEthernet0/0/1.30
 encapsulation dot1Q 30
 ip address 32.30.0.1 255.255.0.0
!
interface GigabitEthernet0/0/1.40
 encapsulation dot1Q 40
 ip address 32.40.0.1 255.255.0.0
!
```

Methodology

Step 5: Routing Configuration

OSPF Routing Method is used on R1, R2 and R3 Routers to communicate between each other

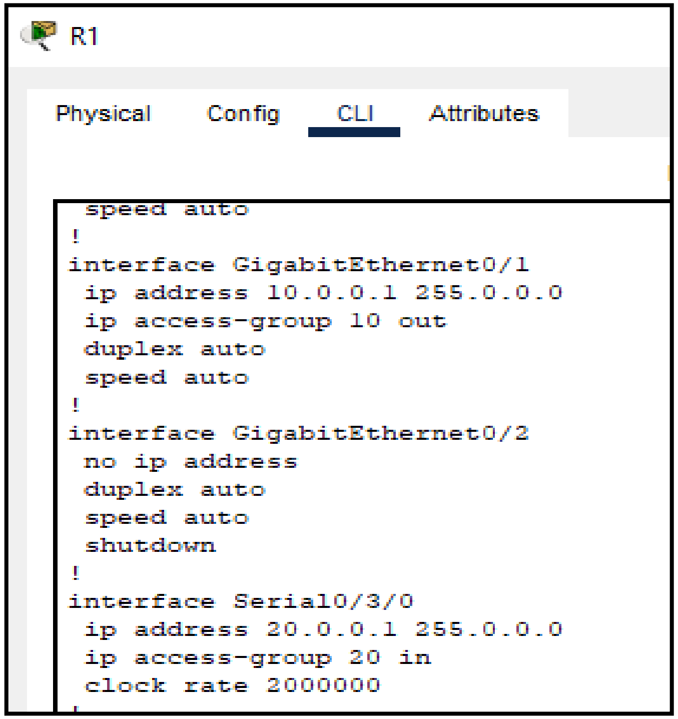


```
 shutdown
!
router ospf 40
 log-adjacency-changes
 network 20.0.0.0 0.255.255.255 area 0
 network 21.0.0.0 0.255.255.255 area 0
 network 100.0.0.0 0.255.255.255 area 0
 network 32.10.0.0 0.0.255.255 area 0
 network 32.20.0.0 0.0.255.255 area 0
 network 32.30.0.0 0.0.255.255 area 0
 network 32.40.0.0 0.0.255.255 area 0
!
ip classless
!
ip flow-export version 9
```

Methodology

Step 6: ACLs Configuration

ACLs are used to filter traffic based on the set of rules



```
 speed auto
!
interface GigabitEthernet0/1
 ip address 10.0.0.1 255.0.0.0
 ip access-group 10 out
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/3/0
 ip address 20.0.0.1 255.0.0.0
 ip access-group 20 in
 clock rate 2000000
```

Methodology

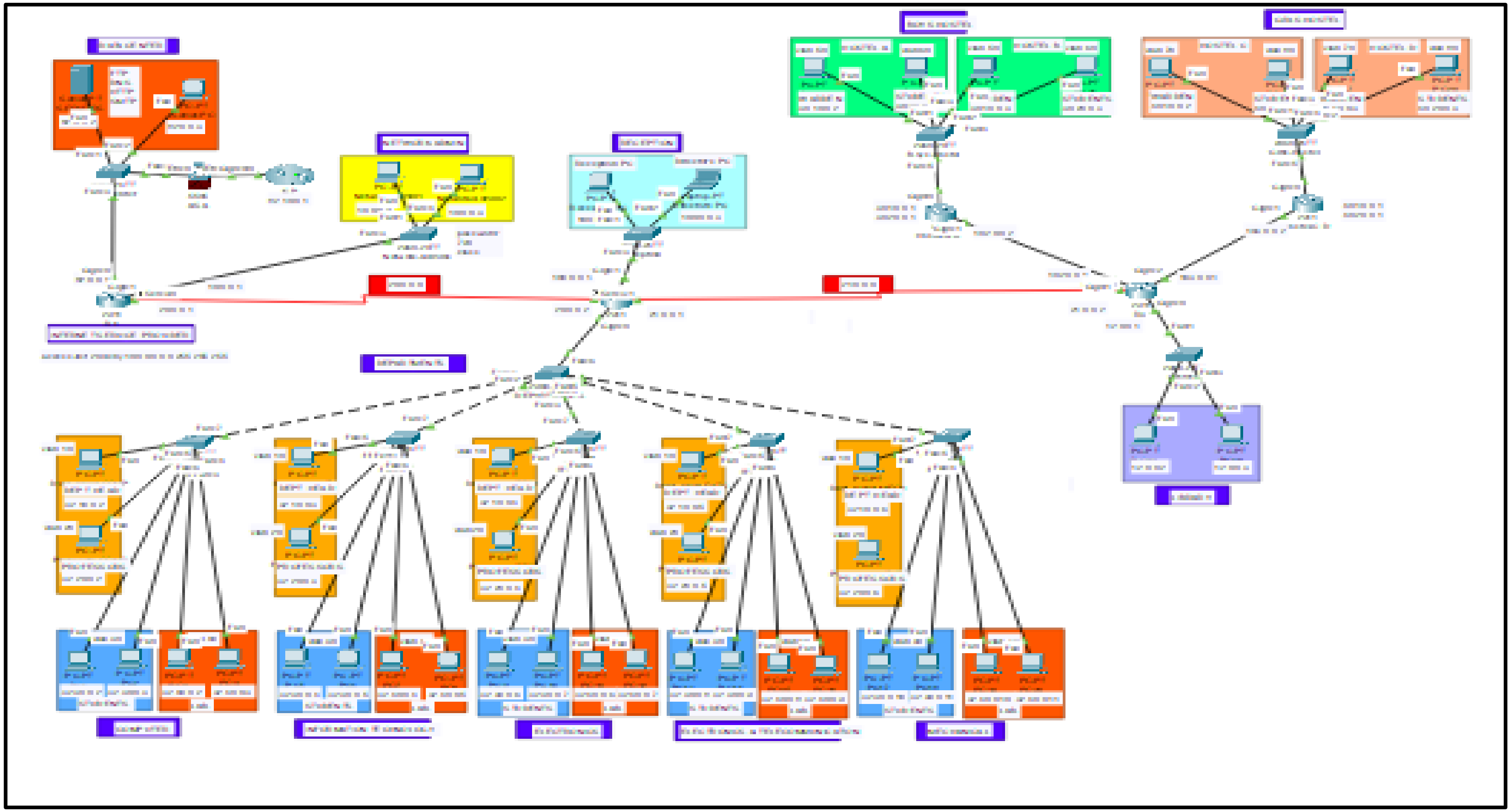
Step 7: Common Attacks prevented

1. DHCP Snooping
2. VLAN Hopping
3. ARP Spoofing (ARP Poisoning)

Step 8: Network Performance Parameters Measured by integrating GNS3 with PRTG

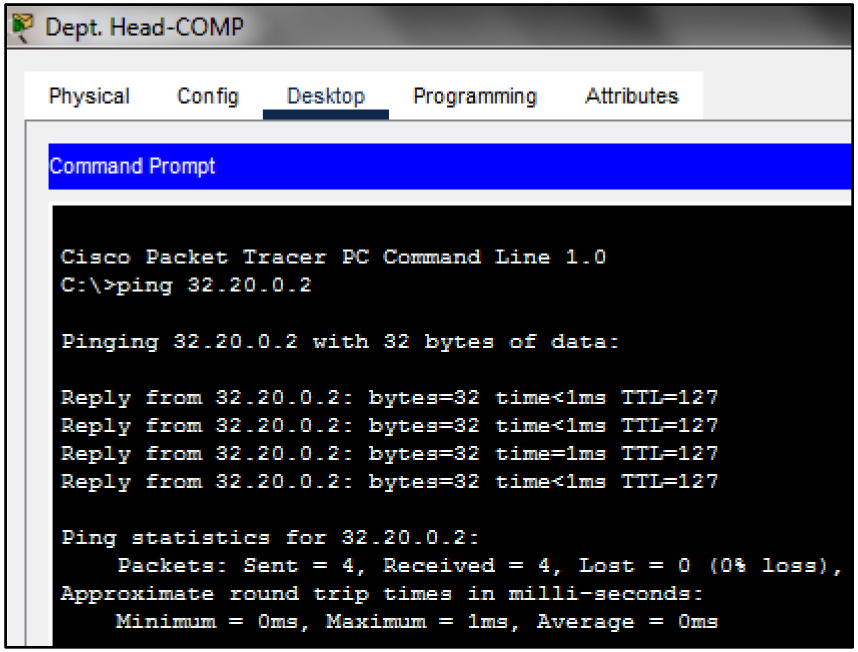
1. Ping
2. Throughput
3. Jitter
4. Port Range
5. Ping jitter

Network Topology

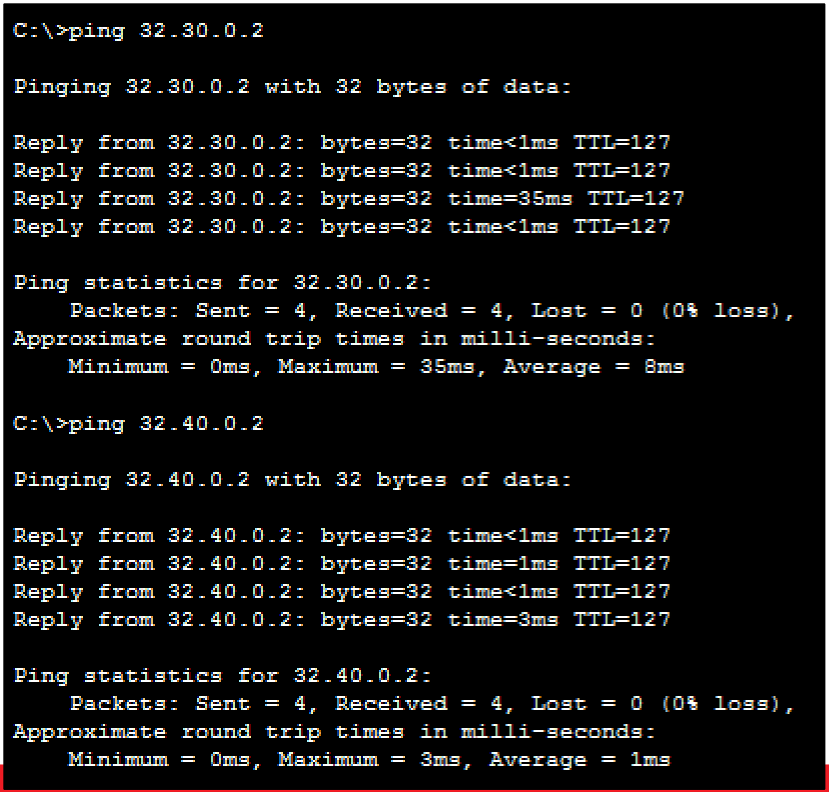


Results & Analysis of InterVLAN Communication

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

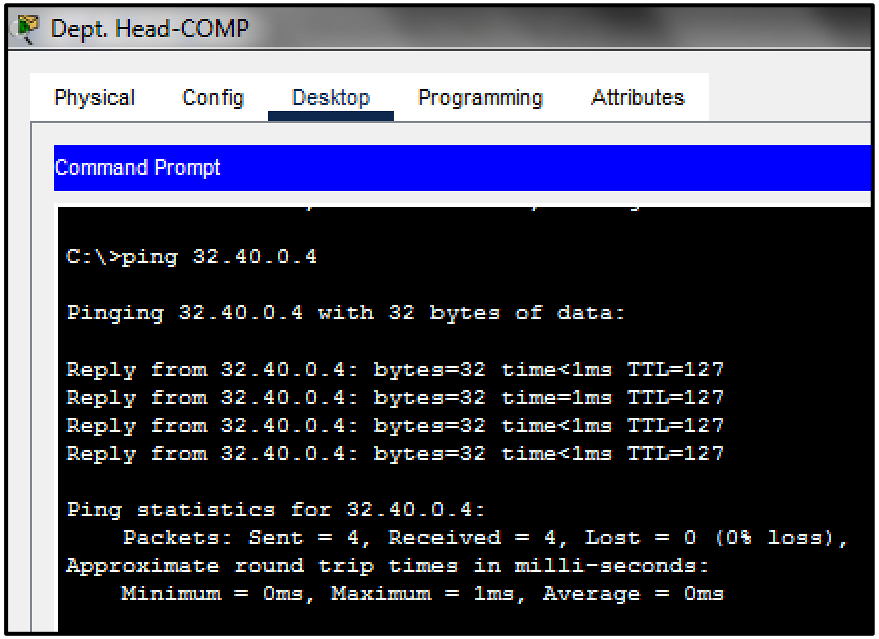


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 32.20.0.2

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
```

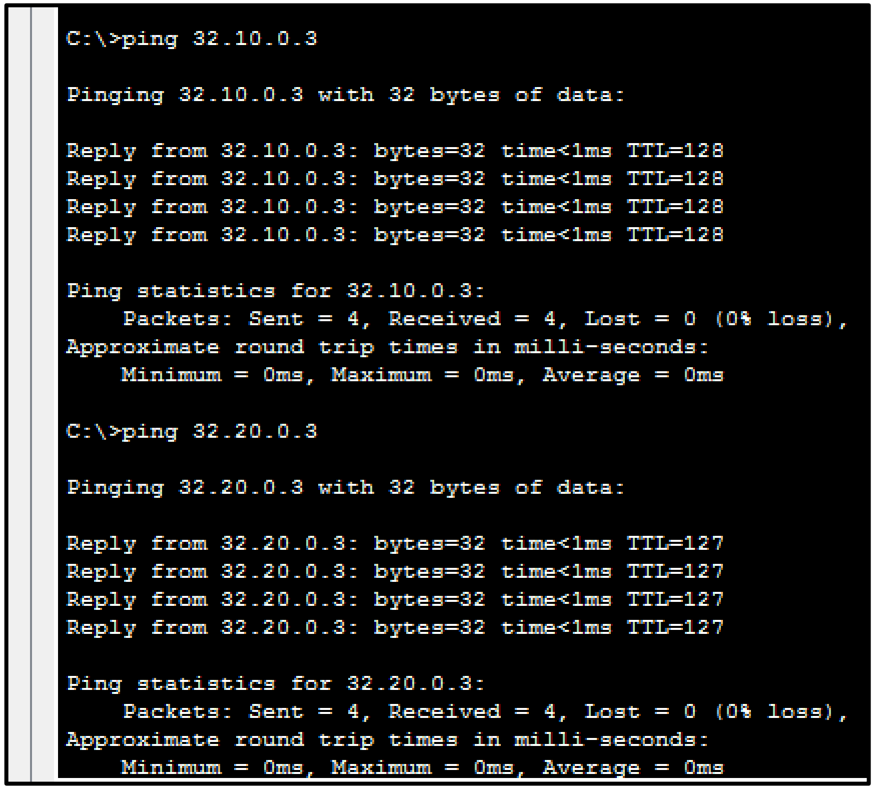


```
C:\>ping 32.30.0.2

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

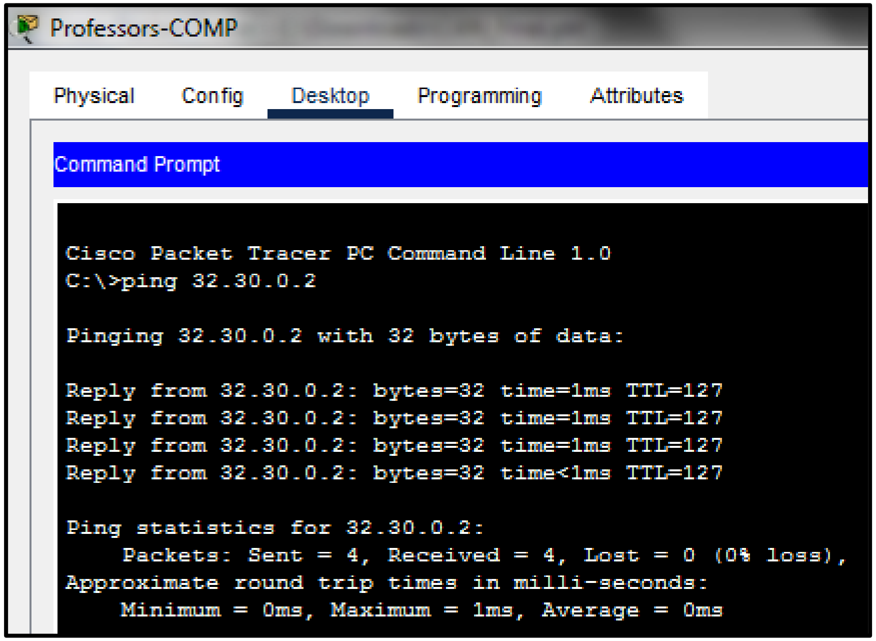


```
C:\>ping 32.40.0.4

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
```

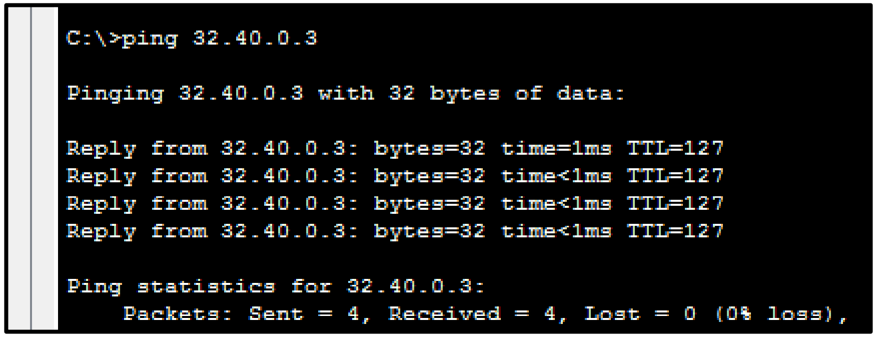


```
C:\>ping 32.10.0.3

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



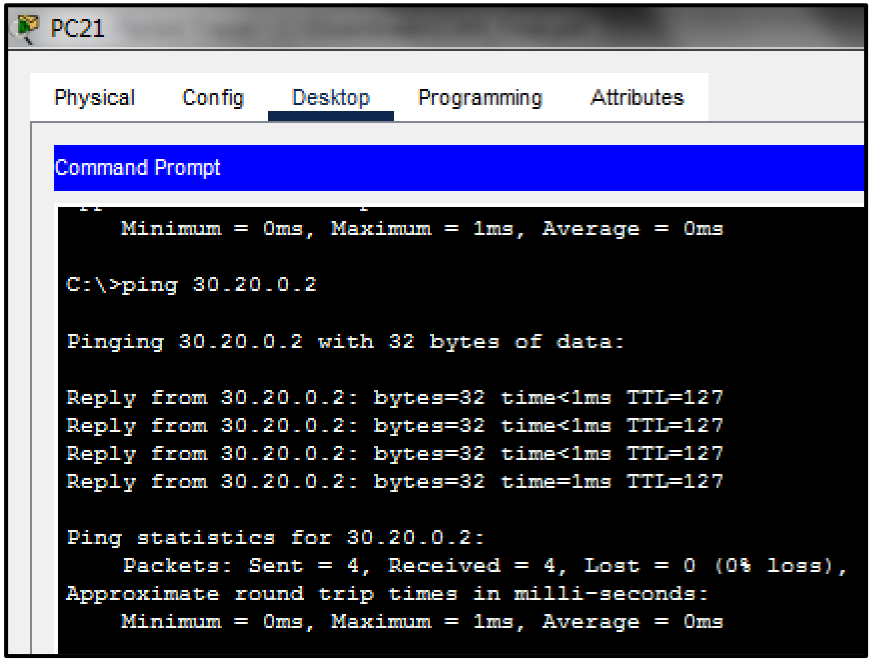
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 32.30.0.2

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
```



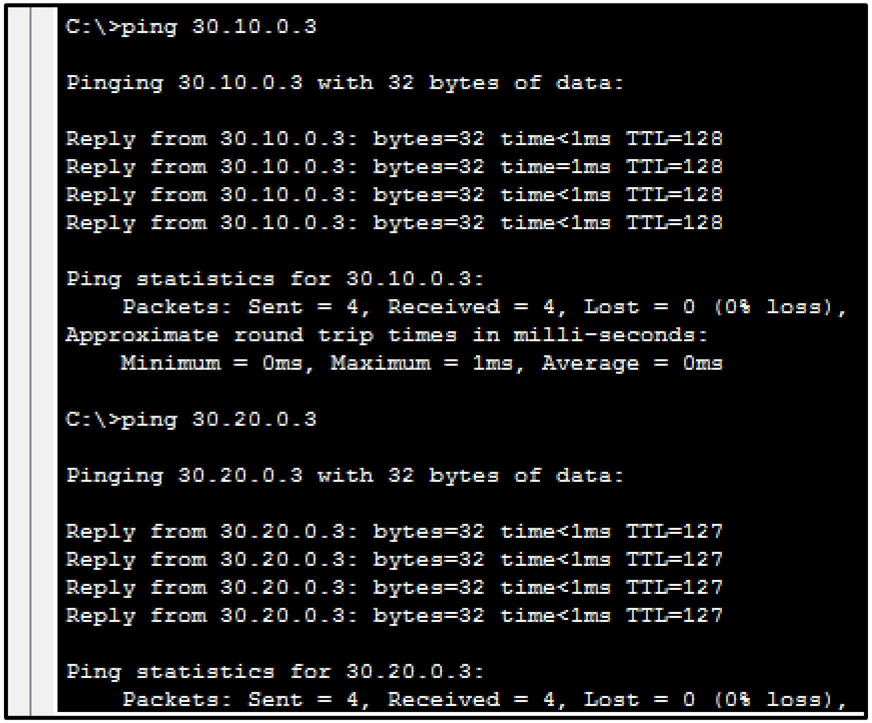
```
C:\>ping 32.40.0.3

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

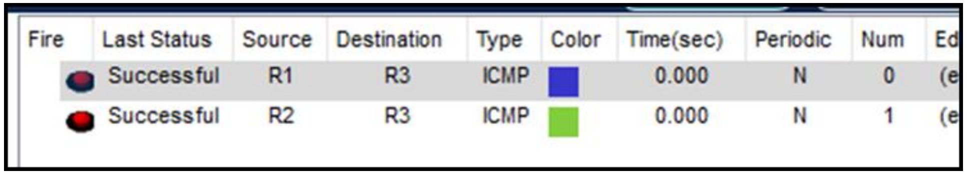


```
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

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
```



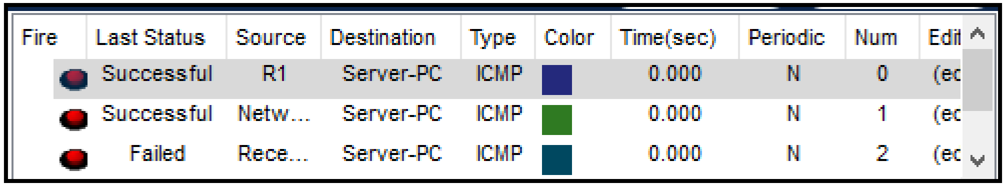
```
C:\>ping 30.10.0.3

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 OSPF & Access-Lists



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Ed
●	Successful	R1	R3	ICMP	🟦	0.000	N	0	(e
●	Successful	R2	R3	ICMP	🟩	0.000	N	1	(e

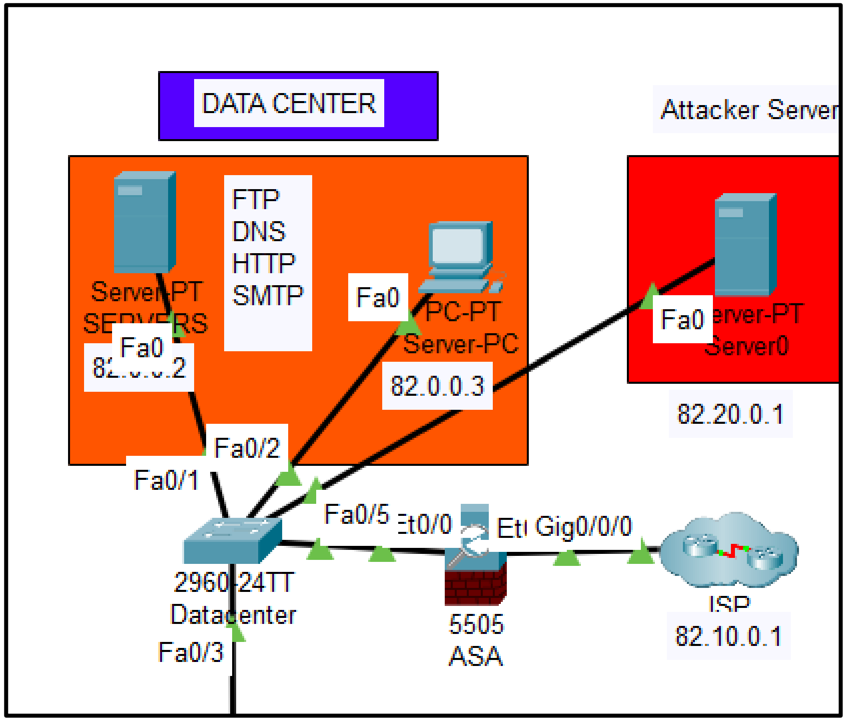
Router 1, Router 2 and Router 3 can communicate with each other as we configured ospf on these routers



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
●	Successful	R1	Server-PC	ICMP	🟦	0.000	N	0	(ec
●	Successful	Netw...	Server-PC	ICMP	🟩	0.000	N	1	(ec
●	Failed	Rece...	Server-PC	ICMP	🟦	0.000	N	2	(ec

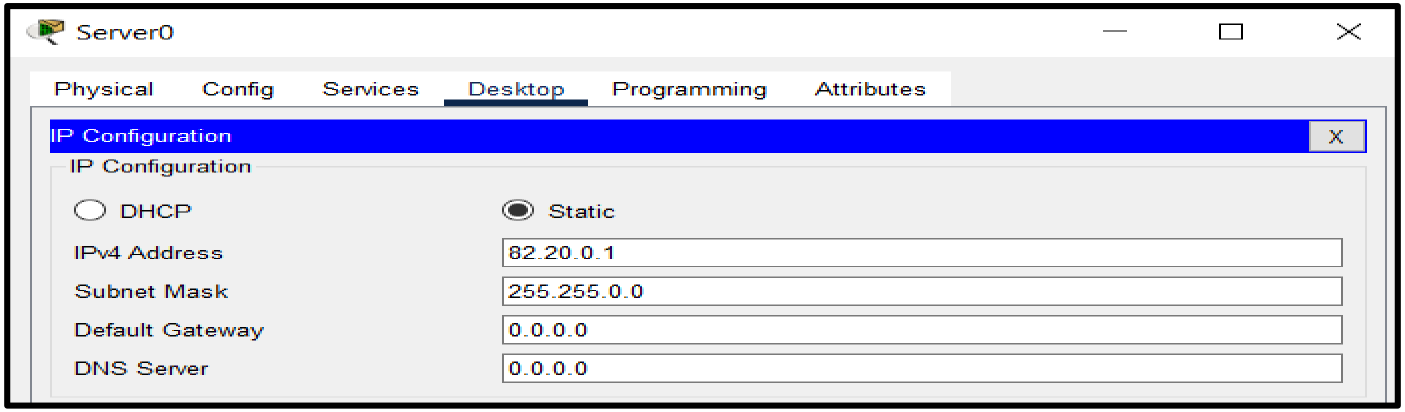
As network admin has only access to data-center they can communicate with each other but rest of end devices can’t communicate with data center

Results & Analysis of DHCP Snooping



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

Results of DHCP Snooping attack

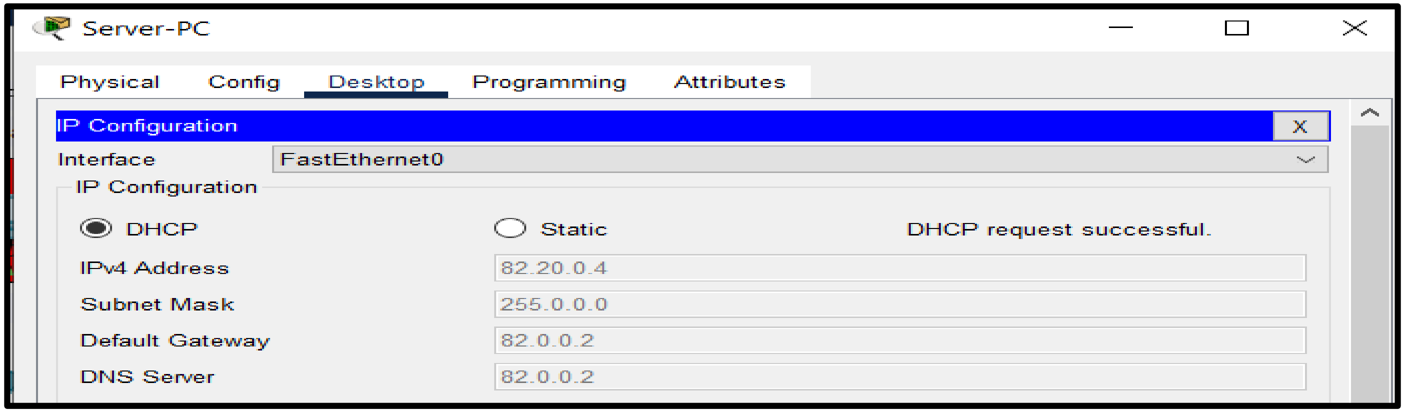


IP Configuration

○ 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



Interface FastEthernet0

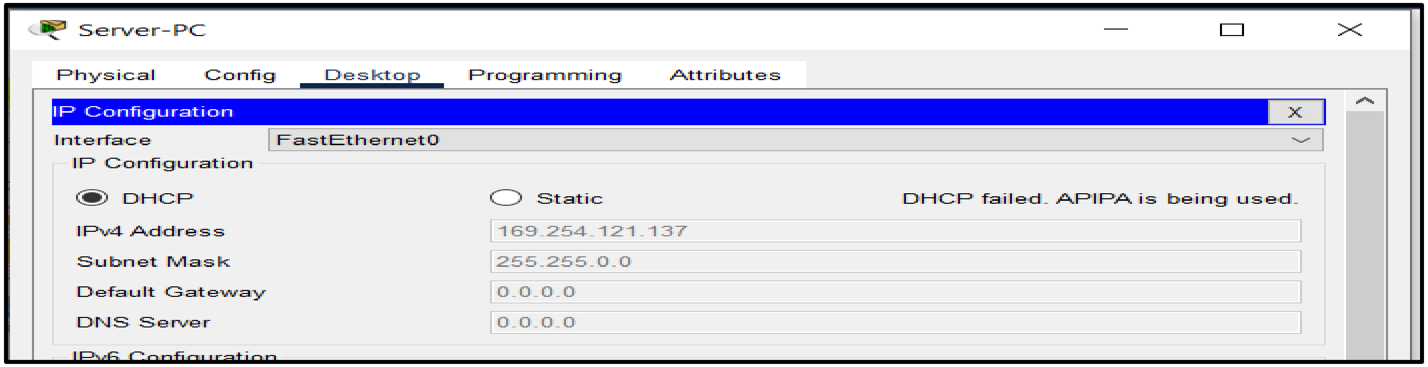
IP Configuration

● 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



Interface: FastEthernet0

IP Configuration

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

IPv4 Address: 169.254.121.137

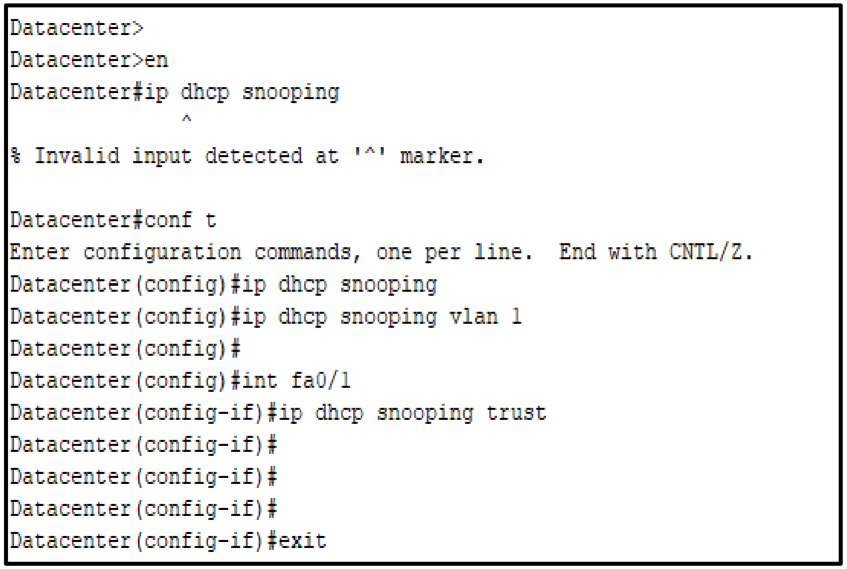
Subnet Mask: 255.255.0.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

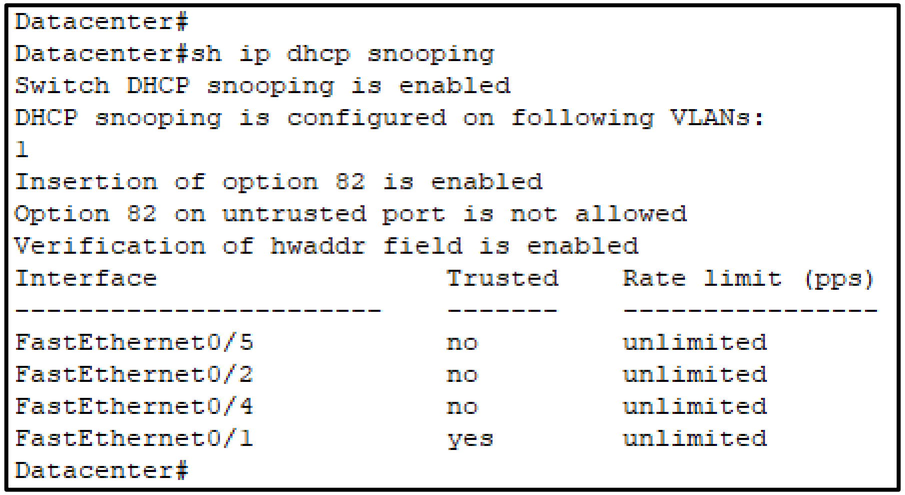
From this image we can see attack is prevented as our pc is unable access ip address



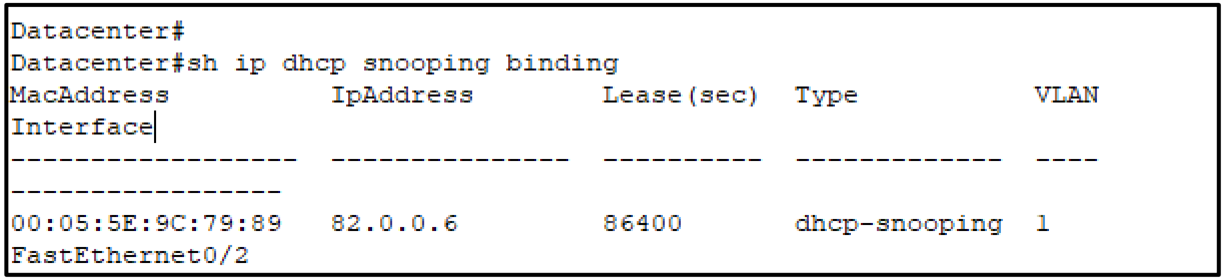
```
Datacenter>
Datacenter>en
Datacenter#ip dhcp snooping
              ^
% Invalid input detected at '^' marker.

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



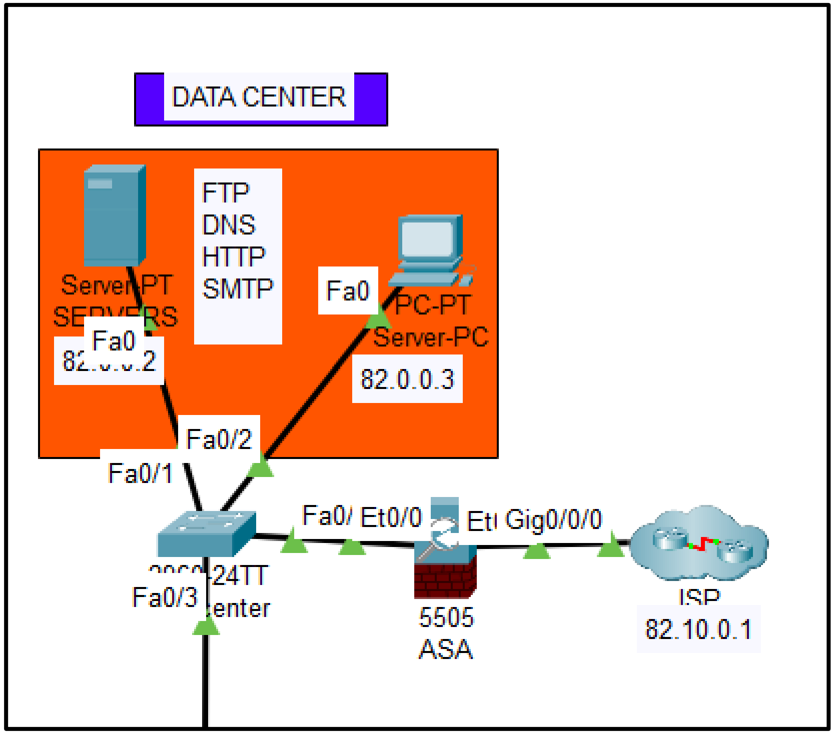
```
Datacenter#
Datacenter#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)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



```
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
```

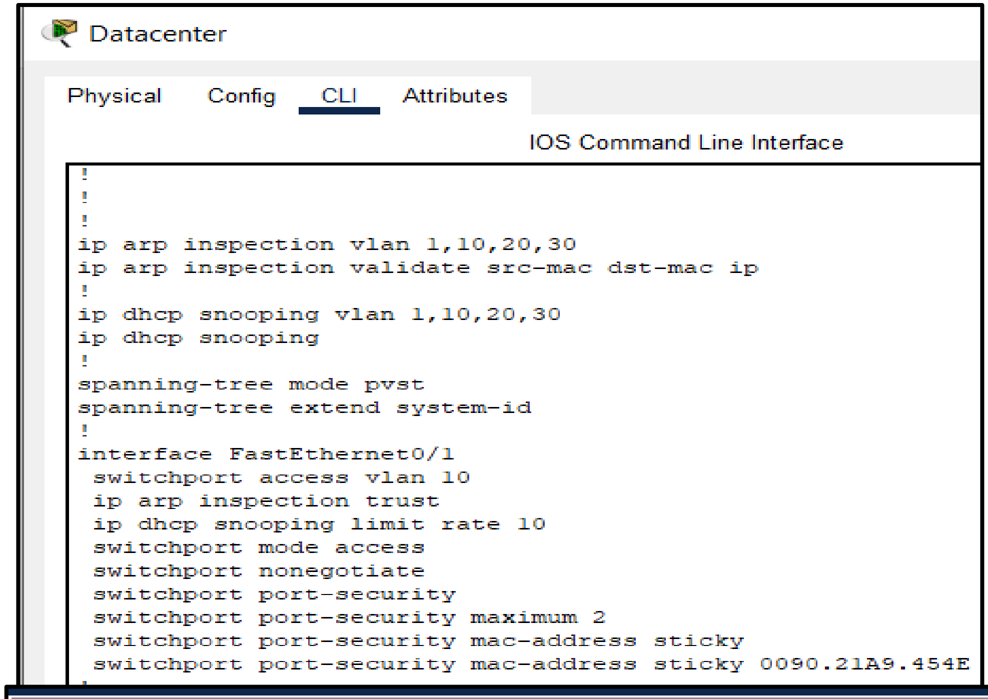
- Fast ethernet 0/1 is set as trusted port and traffic from that port will have authorization
- From binding table we can see ip address of our PC

Results & Analysis of VLAN Hopping



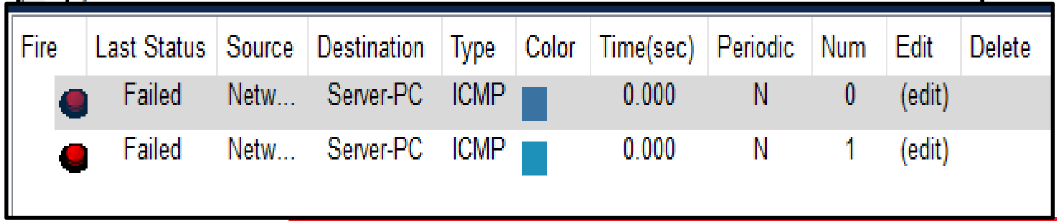
- We created 3 vlans vlan 10 for Servers, vlan 20 for data center and vlan 30 for unused ports
- We used switchport nonegotiate command to disable dtp server

Results & Analysis of Protection against 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
```

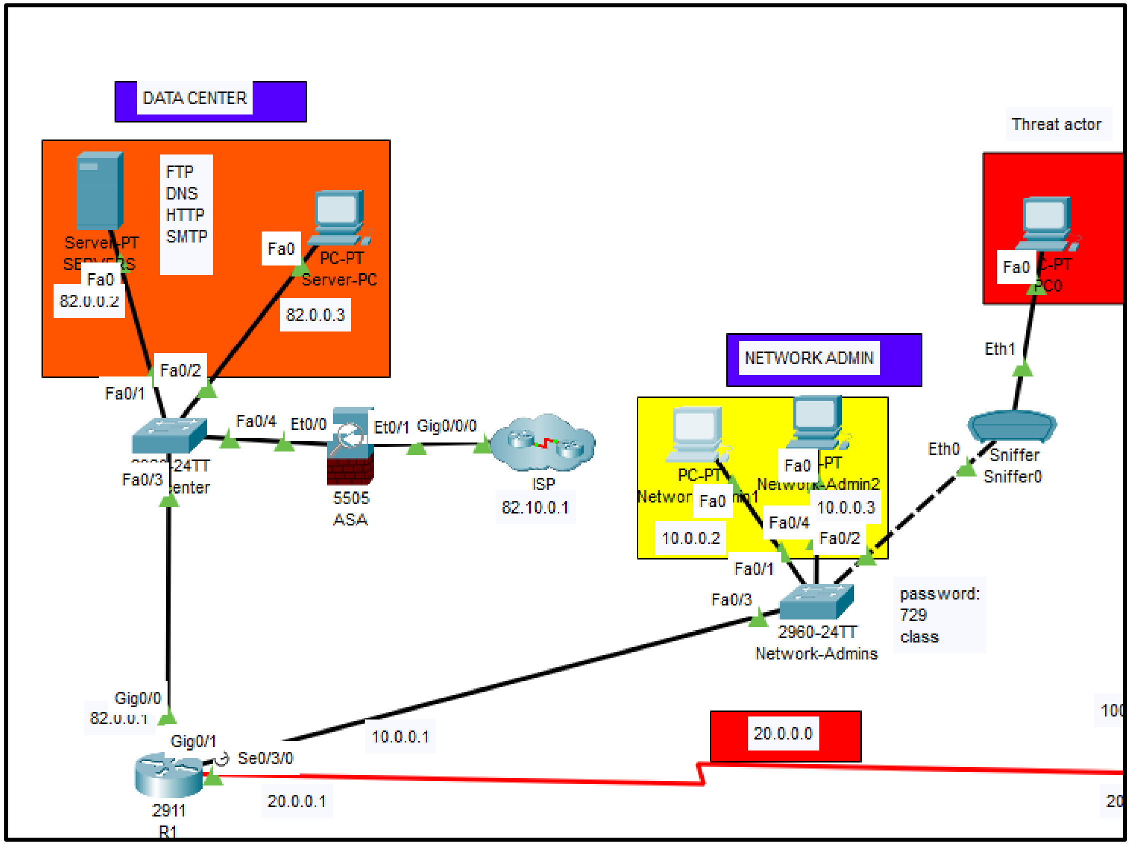
By using these commands we can prevent VLAN Hopping attack



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)	

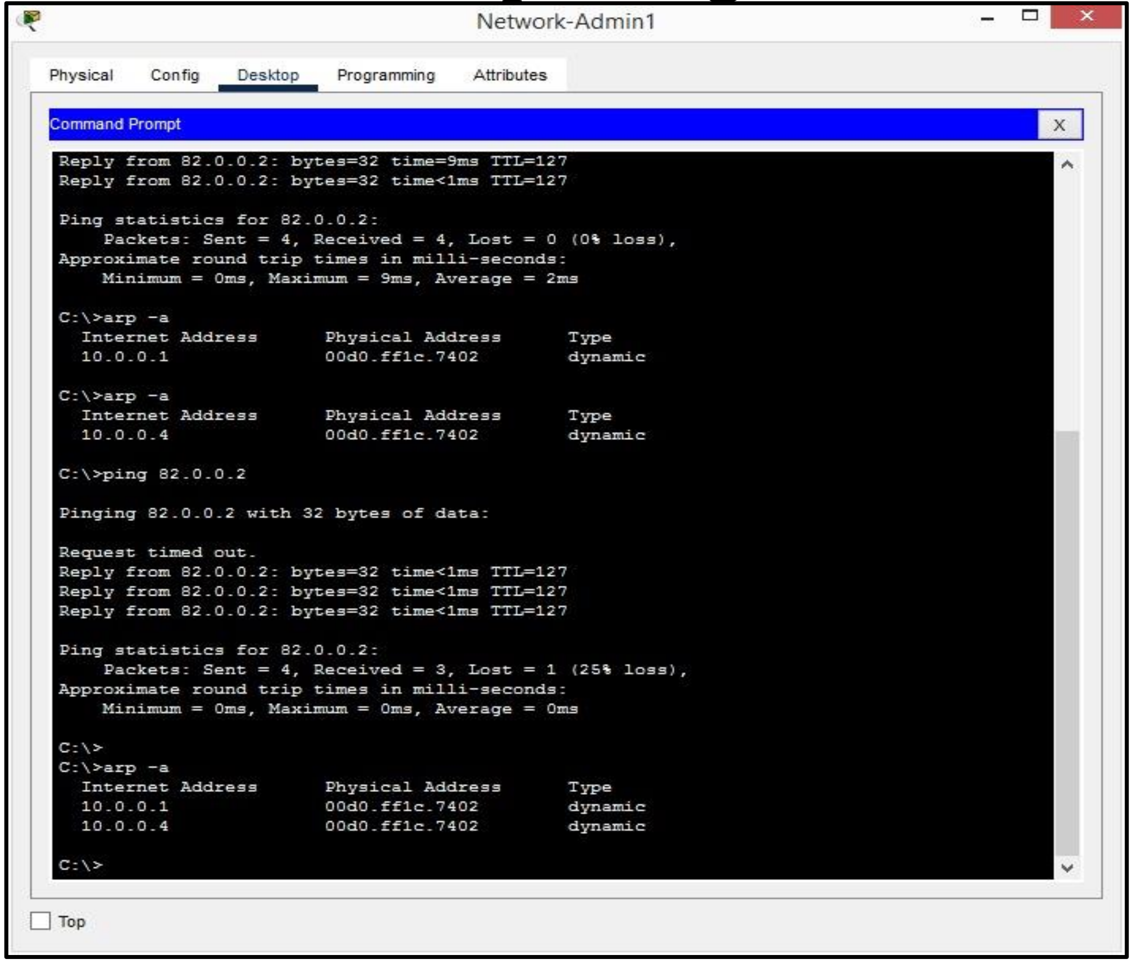
We can see traffic from outside network is unable to communicate with Datacenter

Results & Analysis of ARP Spoofing



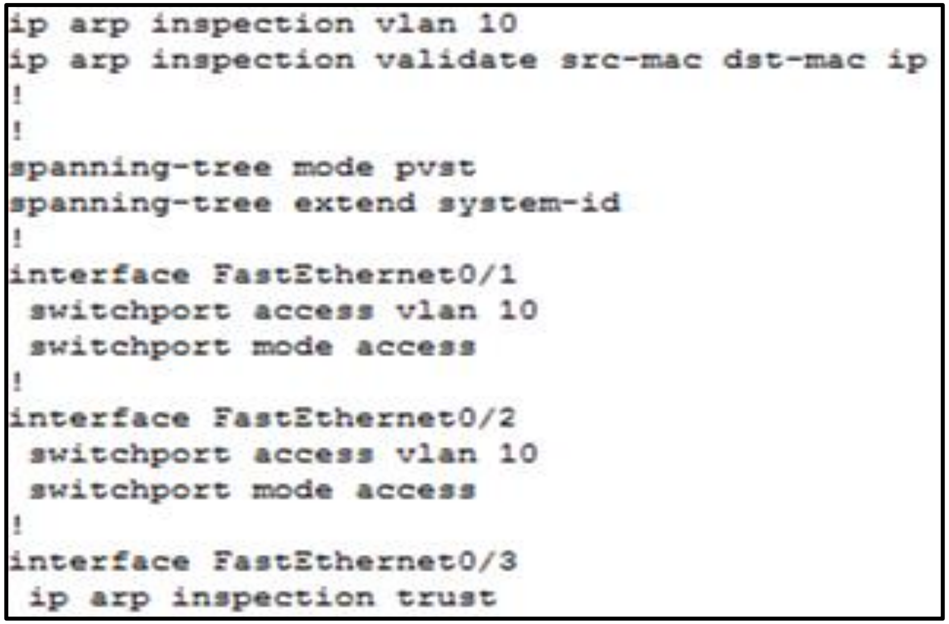
The threat actor tries to snoop the information exchanged between the network admins and the datacenter.

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:\>
```

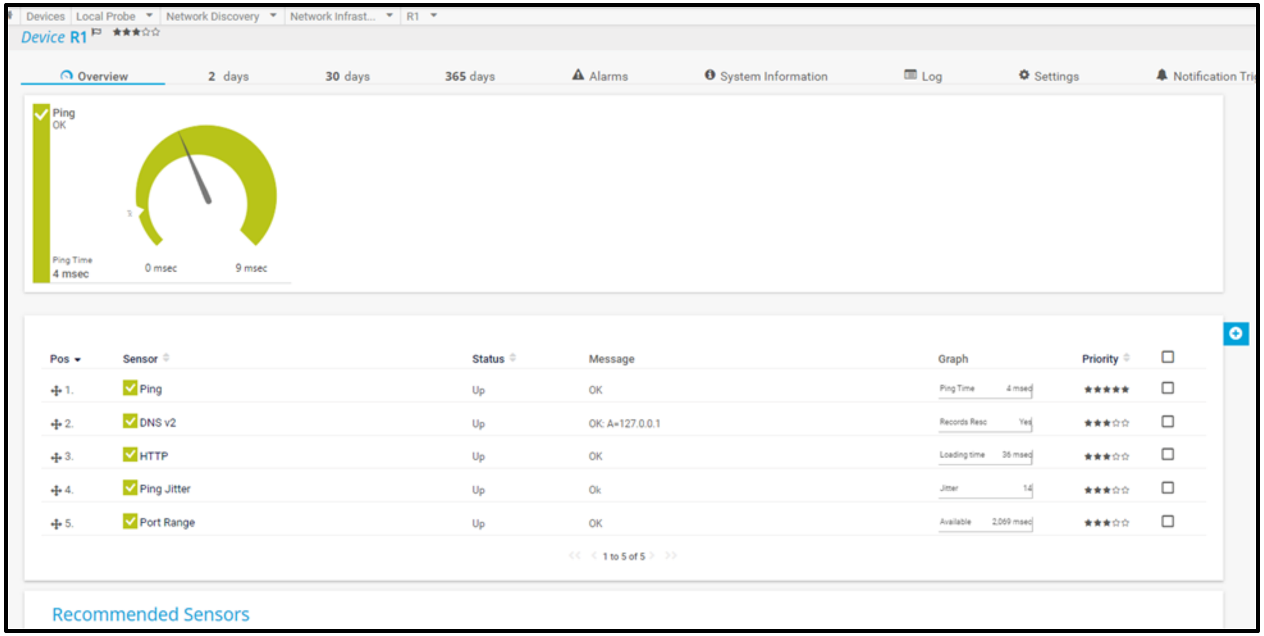
Results & Analysis of Protection against ARP spoofing



```
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 of Network Performance Parameters on PRTG



Pos	Sensor	Status	Message	Graph	Priority	□
1.	✓ Ping	Up	OK	Ping Time 4 msec	★★★★★	□
2.	✓ DNS v2	Up	OK: A=127.0.0.1	Records Resc Yes	★★★☆☆	□
3.	✓ HTTP	Up	OK	Loading time 36 msec	★★★☆☆	□
4.	✓ Ping Jitter	Up	Ok	Jitter 14	★★★☆☆	□
5.	✓ Port Range	Up	OK	Available 2,069 msec	★★★☆☆	□

1 to 5 of 5

These are network performance parameters showcased on PRTG Dashboard

Conclusion

- We created design of Campus Area Network using Cisco Packet Tracer.
- We learned and implemented VLANS, InterVLAN Routing (Router on Stick Method), OSPF Routing, Access-Control Lists.
- We learned about different servers such as (DNS, HTTP, SMTP, FTP, DHCP).
- We have done data center survey to do comparative analysis with our design of campus network.
- We learned and prevented common attacks such as (ARP Spoofing, DHCP Snooping, VLAN Hopping).
- We measured network performance parameters by integrating GNS3 with PRTG.

Future Scope

- Implementing Firewall to prevent external security attacks.
- In-depth working on network performance parameters.
- Managing network traffic to enhance network performance in our project.
- Also we can create intrusion detection system to protect the campus network.

References

1. Ali, Md. Nadir, “Design and Implementation of a Secure Campus Network”, Journal of Surface Engineered Materials and Advanced Technology, 2015
2. G.Michael, “Design and Implementation of a Secure Campus Network” 2017 International Journal of Pure and Applied Mathematics(IJPAM), Volume 116 No. 8 2017, 303-307
3. M. N. B. Ali, M. L. Rahman and S. A. Hossain, "Network architecture and security issues in campus networks," 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 2013, pp. 1-9, doi: 10.1109/ICCCNT.2013.6726595.
4. Kumari, Lalita & Debbarma, Swapan & Shyam, Radhey, “Security Problems in Campus Network and Its Solutions”, International Journal of Advanced Engineering & Applications (IJAEA), 2011, Volume-1. pp 98-101.
5. X. Li and T. Jiang, "Design and implementation of the campus network monitoring system," 2014 IEEE Workshop on Electronics, Computer and Applications, 2014, pp. 117-119, doi: 10.1109/IWECA.2014.6845571.

References

6. Bull, Ronny & Matthews, Jeanna & Trumbull, Kaitlin, “VLAN hopping, ARP poisoning and Man-In-The-Middle Attacks in Virtualized Environments”, 2016
7. H. Ning and X. Bing, "The research and analysis of security of campus network," 2011 6th IEEE Joint International Information Technology and Artificial Intelligence Conference, 2011, pp. 25-27, doi: 10.1109/ITAIC.2011.6030268.
8. Nuhu, Abdulhafiz, “Mitigating DHCP starvation attack using snooping technique” FUDMA Journal of Sciences, 2020, 4. 560.
9. Security Management Technology Based on Big Data," 2019 International Conference on Smart Grid and Electrical Automation (ICSGEA), 2019, pp. 571-575, doi: 10.1109/ICSGEA.2019.00133.
10. Doss, Srinath & S.Panimalar, S.Panimalar & Simla, A.Jerrin & J.Deepa, J.Deepa, (2015). “Detection and Prevention of ARP spoofing using Centralized Server”, International Journal of Computer Applications. 113. 26-30. 10.5120/19935-1931.

THANK YOU