ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

# Design and Implementation of a Network Security Model for Campus Network Using Various Securities

Varsha, Tomar Kuldeep

M.Tech Scholar, Department of Computer Science & Engineering, NGFCET, Palwal, India

Associate Professor, Department of Computer Science & Engineering, NGFCET, Palwal, India

**ABSTRACT:** This project is totally dedicated to the Network Engineer for new and smart learning of the Network Structure. In this concept it is possible for the networker to check the Network Structure of a company spread in the big campus area. The incoming & the outgoing traffic can be maintained along with some security concepts as well. In this logic we use the multiple Routing Protocols in different areas of the company. The practical shows us the proper movement of the packet from one part of the company to the other part of the company. Multiple Routing protocols have been used in all the departments and they can communicate with other different departments through the Redistribution among different Routing Protocols.

## I. INTRODUCTION

A campus network is a proprietary local area network (LAN) or set of interconnected LANs serving a corporation, government agency, university, or similar organization. In this context, a typical campus encompasses a set of buildings in close proximity[1]. Because their distribution are geographically distant, which can be a few kilometers or even hundreds of kilometers, and their scale are changing increasingly large. With the development of informatization construction in colleges and universities, campus network is becoming more and more popular. The campus network in teaching, scientific research, and campus administration has played a positive and significant role. In comparison with static routing, less administrative overhead is required in dynamic routing protocols. However, the expense of using dynamic routing protocols is dedicating part of a router's resources for protocol operation including CPU time and network link bandwidth. Besides, to meet the demands of changing network requirements dynamic routing protocols have evolved over several years. Though several organizations have shifted towards more recent routing protocols such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF), many of the earlier routing protocols, such as Routing Information Protocol (RIPv2), are still in use today[5].

### 1.1 Security in Campus Network

Campus Networks can be made secure by using some security mechanism. For providing better security to campus network we can use security mechanism like ARP inspection, DHCP snooping, Port Security, Private VLAN, Time based ACL's, authentication of routing protocol and firewalls. Every security mechanism has its own functionality and feature. Time based ACL's provides access to the network during certain time frame. Port security enables an administrator configure individual switch ports to allow only a specified number of source

1. Understand the business and organizational drivers. To know what to protect, you need to understand how revenue enters the business stream and what front-end components, such as point-of-sale terminals and back-end components, support the core functions of the enterprise. Then, identify which assets, data and personnel are critical to ensure continuity of the business.
2. Create the plan. You want to classify, isolate and protect the most important components. Group related items together, for example all your Windows servers, into one virtual LAN (VLAN). Other asset groups might include infrastructure (routers, switches, VPNs and VOIP) in one VLAN and security assets (IDS, firewalls, web filters and scanners) in another.

DOI: 10.15680/IJIRCCE.2017. 0506012

Financial or human resource servers typically need their own VLAN because of the confidential nature of the information they process and store. You want separate VLANs for groups of personnel as well, so Windows server administrators might be in one, while security administration are in another and executive management in a third. Data requiring special protection such as credit card
numbers that need to comply with PCI-DSS or patient information that is subject to HIPAA should be isolated from other data and put in their own VLANs.
3. Determine who can access what data. This boils down to business need: who needs to administer the routers or switches? Who needs access to the human resources or financial systems? How many folks should be able to remotely control the security cameras? Be ruthless. If there is no business need, there should be no access.
Organizations that operate entirely on a local or regional domestic level may even want to implement wholesale blocking of remote geographic regions at the IP layer. In general, adopt a default deny access posture for each VLAN. Your goal is to limit access to sensitive information to those who need it within the organization and to create roadblocks to stop or slow intruders, who may have broken through one layer of security, from doing further damage.
4. Implement segmentation. In a large organization, network segmentation is a significant, long-term project, but each step along the way increases security. Start somewhere, perhaps with the network administrators or Windows servers. In that instance, you could set up VLANs called network-admins (for their workstations) and network-devices (for routers and switches).
Log all traffic between segments to determine what is normal and needed for effective functioning.
Once you know what’s necessary, start blocking access to the VLANs from everywhere else, with the ultimate goal of default deny. Make sure you have the controls to enforce segmentation and to monitor whether later requested changes to access may compromise the segmentation. Continue the process through each group of assets, personnel and data.

## II. LITERATURE REVIEW

### 2.1 RELATED WORK

In the year 2013, Mohammed Nadir Bin Ali, Prof. Dr. M. Lutfar Rahman and Prof. Dr. Syed Akhter Hossain purposed "Network Architecture with Security mechanism for Campus Networks". The author mainly targeted towards campus networks which deliver required security. This is essential because, it prevents the institution from suffering any significant attacks associated with network. A university network has a number of uses such as teaching, learning, research, management, e-library, and connections with the external uses. Therefore, network architecture and its security are vital issues for any university. In this work, a network infrastructure is proposed on the basis of the practical and experimental requirements. The proposed network infrastructure is realizable with adaptable infrastructure.
In the year 2015, Yaxun Lan, Zhengshi Chen purposed “The OSPF security optimization mechanism for Campus Network” which aimed at the OSPF security problems existing in the large campus network, the paper research the OSPF security optimizing design from the accessibility of the non-backbone area route, OSPF external routing propagation control and routing spread control in OSPF area.

## III. PROPOSED WORK

Implementation of RIPv2, EIGRP and OSPF with better security mechanism in campus network. Security can be obtained by using security mechanism like Arp Inspection , VLAN , DHCP Snooping, Time Based ACL Authentication of RIPv2, Authentication of EIGRP, Authentication of OSPF and Port security. Specifically the aim of the research is:
 **Implementation and redistribution of OSPF, EIGRP, RIPV2 in Campus Network:**
Implemented RIPv2, OSPF and EIGRP in a Campus Network and to redistribute them which will enable campus network to have the features of more than one routing protocols. We have implemented OSPF in the core layer, EIGRP in the distributed layer and have used BGP for outside connectivity. OSPF provide full details about the network. EIGRP can be used for fast convergence in the distributed layer. **Providing Security to the Campus Network by implementing the following Security Mechanisms:**
*a) ARP Inspection*: It is a security feature that rejects invalid and malicious ARP packets. The feature prevents a class

of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors.
b) *DHCP snooping*: it is a layer 2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. The fundamental use case for DHCP snooping is to prevent unauthorized (rogue)DHCP servers offering IP addresses to DHCP clients.
*c) Authentication of RIPV2, EIGRP and OSPF*: This practice provide routers to only accept routing information from other routers that have been configured with the right password or authentication information. It prevent wrong information flow in the network by authenticating the packet.
d) *Port Security:* it is a layer two traffic control feature on Cisco Catalyst switches. It enables an administrator configure individual switch ports to allow only a specified number of source MAC addresses ingressing the port.
*e) Private VLAN:* they also known as port isolation, is a technique in computer networking where a VLAN contains switch ports that are restricted such that they can only communicate with a given "uplink". The restricted ports are called "private ports". It is the concept of master slave vlan.
f) *Firewalls:* A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

## IV. METHODOLOGY

The methodology to be used in carrying out this research work is exploratory research which involves the following steps:
a) Study of Campus Network: it involves study of the campus network characteristics and the technologies that can be deployed in the campus network.
b) Study of routing protocols (RIPv2, OSPF and EIGRP): in campus network interior gateway routing protocols are used such as RIPv2, OSPF and EIGRP. We need to study how to use them effectively for better performance and network optimization.
c) Study of network parameters and metrics: network parameters involves the bandwidth, response time, memory utilization, throughput. We need to study them to analyse the result.
d) Designing topology and implementation of routing protocols in GNS3 using ipv4.
e) Adding security mechanisms in Campus Network: security can be added to campus network using security mechanism like DHCP snooping, port security, ARP Inspection, Time base ACLs and other mechanism.
f) Observing the results: we need to analyse our results with the work done in the past and to improve them.

## V. DESIGN AND IMPLEMENTATION

### 5.1 Topology:

Topology selection criteria are:
1.Determining Network Requirements:Designing a network can be a challenging task. Your first step is to understand your networking requirements. The rest of this chapter explains how to determine these requirements.
Networking devices must reflect the goals, characteristics, and policies of the organizations in which they operate. Two primary goals drive networking design and implementation:
 Application availability—Networks carry application information between computers. If the applications are not available to network users, the network is not doing its job.
 Cost of ownership—Information system (IS) budgets today often run in the millions of dollars. As large organizations increasingly rely on electronic data for managing business activities, the associated costs of computing resources will continue to rise.
A well-designed network can help balance these objectives. When properly implemented, the network infrastructure can optimize application availability and allow the cost-effective use of existing network resources.
2.Considering the Design Problem for Optimizing Availability and Cost
In general, the network design problem consists of the following three general elements:
 Environmental givens—Environmental givens include the location of hosts, servers, terminals, and other end nodes; the projected traffic for the environment; and the projected costs for delivering different service levels.

 Performance constraints—Performance constraints consist of network reliability, traffic throughput, and host/client computer speeds (for example, network interface cards and hard drive access speeds).
 Networking variables—Networking variables include the network topology, line capacities, and packet-flow assignments.
The goal is to minimize cost based on these elements while delivering service that does not compromise established availability requirements. You face two primary concerns: availability and cost. These issues are essentially at odds. Any increase in availability must generally be reflected as an increase in cost. As a result, you must weigh the relative importance of resource availability and overall cost carefully.
3.In general, users primarily want application availability in their networks. The chief components of application availability are response time, throughput, and reliability:
 Response time is the time between entry of a command or keystroke and the host system's execution of the command or delivery of a response. User satisfaction about response time is generally considered to be a monotonic function up to some limit, at which point user satisfaction falls off to nearly zero.

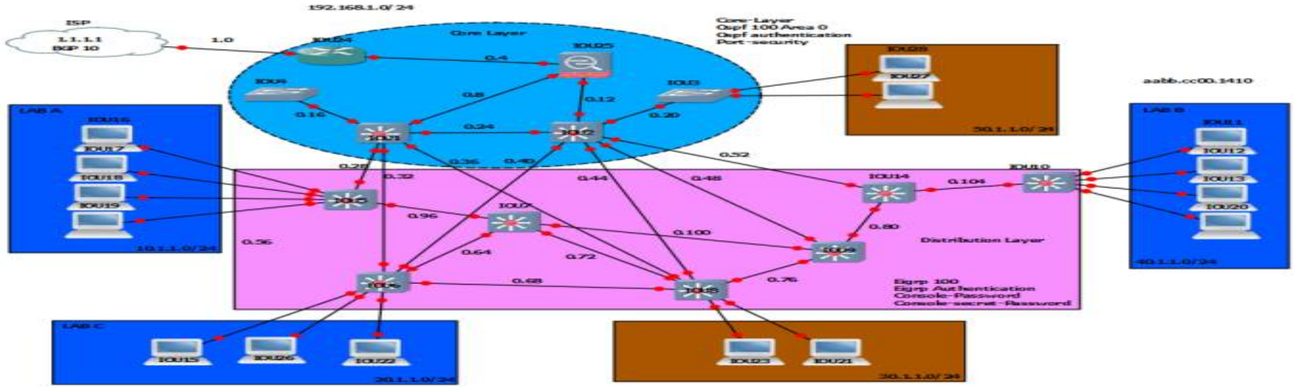


Figure 5.1: Campus network topology

**Key Features of Topology**

- Topology follows Cisco three-layered Hierarchical model.
- Security is provided in routing by authentication and device level security is provided.
- Monitoring tool like solar wind are used in core layer.
- Core Layer
- OSPF authentication and port security.
- EIGRP authentication to allow use of message digest with key based authentication for packet authentication
- DHCP Snooping to prevent fake DHCP from getting details of hosts.
- Use of port security in protected mode to prevent MAC address spoofing without turning off the port.

### 5.2 DHCP Snooping

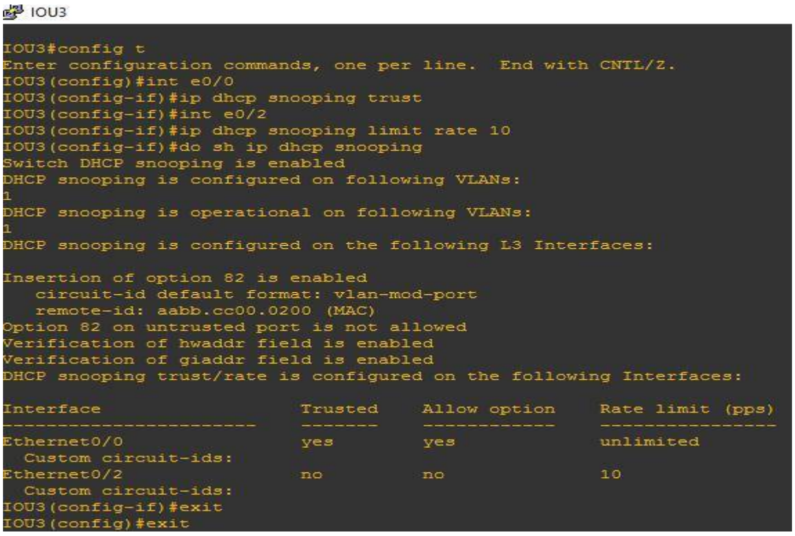
Command used for DHCP snooping are:

```
ip dhcp pool 10
network 10.1.1.0 255.255.255.0
default-router 10.1.1.100
```

DOI: 10.15680/IJIRCCE.2017. 0506012

```
exit

ip dhcp pool 20
network 20.1.1.0
255.255.255.0 default-
router 20.1.1.100 dns-
server 20.1.1.1
exit

ip dhcp pool 30
network 30.1.1.0
255.255.255.0 default-
router 30.1.1.100 dns-
server 30.1.1.1
exit

ip dhcp snooping
ip dhcp snooping
vlan 1 int f0/5
ip dhcp snooping
trust exit
int eo/o
ip
address
dhcp
no sh
exit
To check DHCP snooping
 sh ip dhcp pool
sh ip dhcp binding
sh ip dhcp snooping
```

dns-server 10.1.1.1

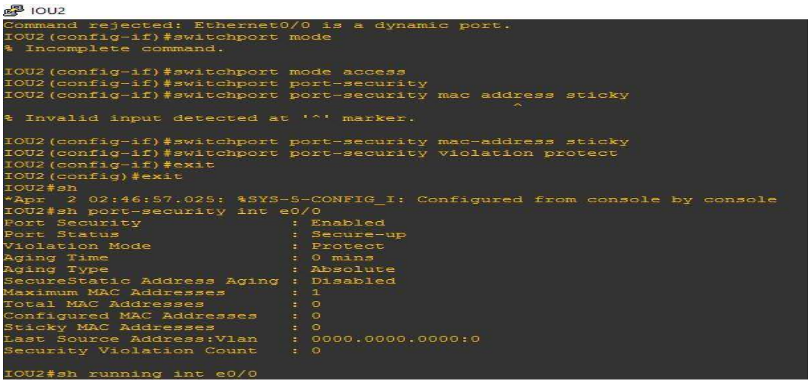


```
IOU3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
IOU3(config)#int e0/0
IOU3(config-if)#ip dhcp snooping trust
IOU3(config-if)#int e0/2
IOU3(config-if)#ip dhcp snooping limit rate 10
IOU3(config-if)#do sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
DHCP snooping is operational on following VLANs:
1
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: aabb.cc00.0200 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
Ethernet0/0                yes        yes             unlimited
  Custom circuit-ids:
Ethernet0/2                no         no              10
  Custom circuit-ids:
IOU3(config-if)#exit
IOU3(config)#exit
```

Figure 5.2: Console for DHCP Snooping

### 5.3 Port Security

```
 interface FastEthernet0/13
  switchport access vlan 10
 switchport mode access
switchport voice vlan 20
 switchport port-security

  switchport port-security
  violation protected
  switchport port-security
  mac-address sticky
  end
```



```
Command rejected: Ethernet0/0 is a dynamic port.
IOU2(config-if)#switchport mode
% Incomplete command.

IOU2(config-if)#switchport mode access
IOU2(config-if)#switchport port-security
IOU2(config-if)#switchport port-security mac address sticky
                                                  ^
% Invalid input detected at '^' marker.

IOU2(config-if)#switchport port-security mac-address sticky
IOU2(config-if)#switchport port-security violation protect
IOU2(config-if)#exit
IOU2(config)#exit
IOU2#sh
*Apr  2 02:46:57.025: %SYS-5-CONFIG_I: Configured from console by console
IOU2#sh port-security int e0/0
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

IOU2#sh running int e0/0
```

Figure 5.4:Console for Port Security

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

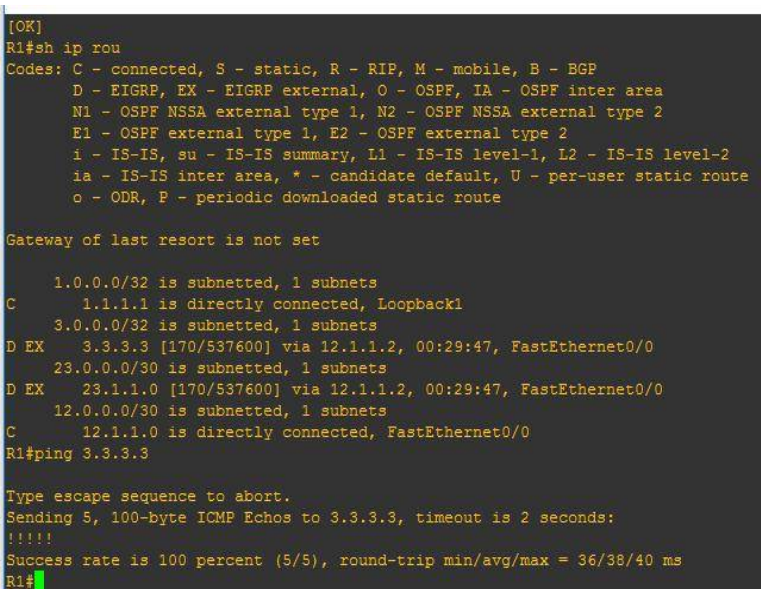
Vol. 5, Issue 6, June 2017

### 5.4 Redistribution of EIGRP and OSPF:

At block A:

router ospf 1

```
redistribute eigrp 100 subnets
net 192.168.12.6 0.0.0.0 area 0 net
3.3.3.1 0.0.0.0 area 0
net 3.3.3.2 0.0.0.0 area 0
router eigrp 100
redistribute ospf 1 metric 10000 1000 255 1 1500 net
192.168.12.57 0.0.0.0
net 192.168.12.9 0.0.0.0 no
auto-summary

At block B:
router ospf 1
redistribute eigrp 100 subnets net
192.168.12.25 0.0.0.0 area 0 net
4.4.4.1 0.0.0.0 area 0
net 4.4.4.2 0.0.0.0 area 0
router eigrp 100
redistribute ospf 1 metric 10000 1000 255 1 1500 net
192.168.12.69 0.0.0.0
net 192.168.12.62 0.0.0.0 net
192.168.12.10 0.0.0.0 net
192.168.12.13 0.0.0.0 no
auto-summary

At Block C
router ospf 1
redistribute eigrp 100 subnets net
192.168.12.34 0.0.0.0 area 0 net
192.168.12.46 0.0.0.0 area 0 net
5.5.5.1 0.0.0.0 area 0
net 5.5.5.2 0.0.0.0 area 0 exit
router eigrp 100
 redistribute ospf 1 metric 10000 1000 255 1
 1500 net 192.168.12.58 0.0.0.0
 net    192.168.12.61
 0.0.0.0              net
 192.168.12.65 0.0.0.0
 no auto-summary
 exit

 At block
 D router
 ospf 1
 redistribute eigrp 100 subnets
 net  192.168.12.38  0.0.0.0
 area  0  net  192.168.12.50
 0.0.0.0  area  0  net  6.6.6.1
 0.0.0.0 area 0
 net  6.6.6.2  0.0.0.0
 area  0  router  eigrp
 100
 redistribute ospf 1 metric 10000 1000 255 1
 1500 net 192.168.12.66 0.0.0.0
 net    192.168.12.70
 0.0.0.0              net
 192.168.12.73 0.0.0.0
 no auto-summary
 exit

 At block
 E router
 ospf 1
 redistribute eigrp 100 subnets
 net  192.168.12.21  0.0.0.0
```



```
[OK]
R1#sh ip rou
Codes: 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

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback1
     3.0.0.0/32 is subnetted, 1 subnets
D EX    3.3.3.3 [170/537600] via 12.1.1.2, 00:29:47, FastEthernet0/0
     23.0.0.0/30 is subnetted, 1 subnets
D EX    23.1.1.0 [170/537600] via 12.1.1.2, 00:29:47, FastEthernet0/0
     12.0.0.0/30 is subnetted, 1 subnets
C       12.1.1.0 is directly connected, FastEthernet0/0
R1#ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/38/40 ms
R1#
```

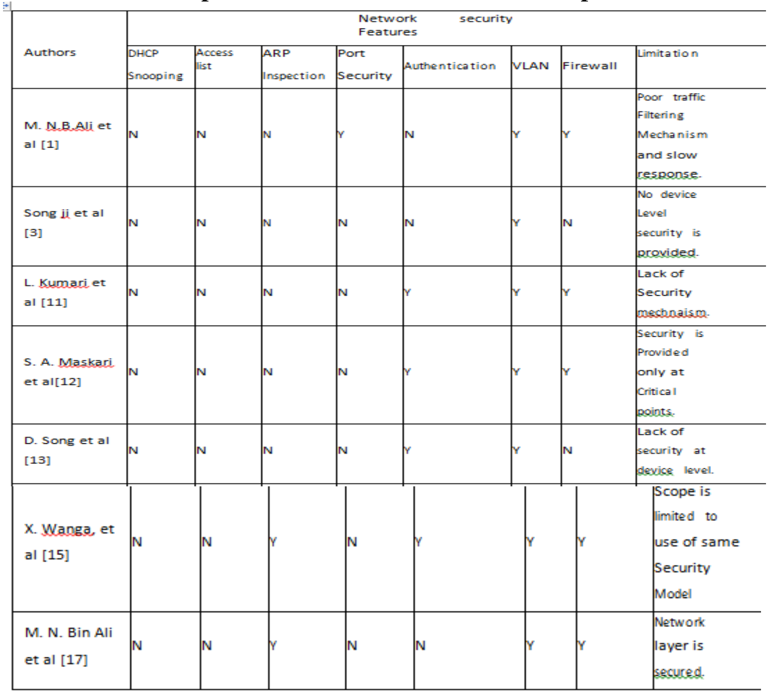
## VI. RESULTS

Analysis of result is done in this section we have analyzed the results with the previous work. We can compared network security features with the previous work. We analyzed the network performance in terms of response time, memory utilization, packet loss and CPU utilization.

DOI: 10.15680/IJIRCCE.2017. 0506012

### 6.1 Comparison of network security features with previous work

Table 6.1: Comparison of network features with previous work

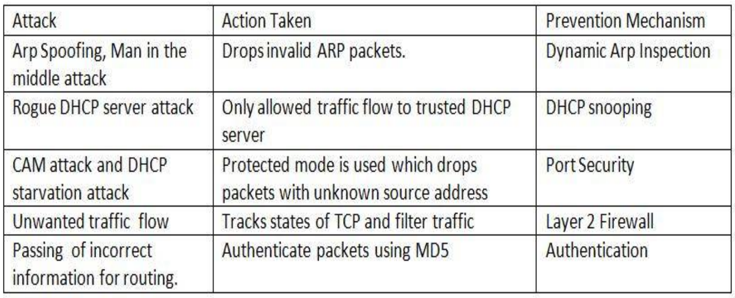


| Authors | Network security Features | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | DHCP Snooping | Access list | ARP Inspection | Port Security | Authentication | VLAN | Firewall | Limitation |
| M. N.B.Ali et al [1] | N | N | N | Y | N | Y | Y | Poor traffic Filtering Mechanism and slow response. |
| Song ji et al [3] | N | N | N | N | N | Y | N | No device Level security is provided. |
| L. Kumari et al [11] | N | N | N | N | Y | Y | Y | Lack of Security mechnaism. |
| S. A. Maskari et al[12] | N | N | N | N | Y | Y | Y | Security is Provided only at Critical points. |
| D. Song et al [13] | N | N | N | N | Y | Y | N | Lack of security at device level. |
| X. Wanga, et al [15] | N | N | Y | N | Y | Y | Y | Scope is limited to use of same Security Model |
| M. N. Bin Ali et al [17] | N | N | Y | N | N | Y | Y | Network layer is secured. |

Here, we would know that what kind  of securities are applied in the topology and wwhat are proposing.

### 6.2 Prevention mechanism from different attacks

Table 6.2: Prevention from different attack



| Attack | Action Taken | Prevention Mechanism |
|---|---|---|
| Arp Spoofing, Man in the middle attack | Drops invalid ARP packets. | Dynamic Arp Inspection |
| Rogue DHCP server attack | Only allowed traffic flow to trusted DHCP server | DHCP snooping |
| CAM attack and DHCP starvation attack | Protected mode is used which drops packets with unknown source address | Port Security |
| Unwanted traffic flow | Tracks states of TCP and filter traffic | Layer 2 Firewall |
| Passing of incorrect information for routing. | Authenticate packets using MD5 | Authentication |

According to Table 6.2

1. We are averting man in the middle attack by dropping invalid/unwanted ARP packets using “Dynamic ARP Inspection.”
2. Rough DHCP server attack is getting prohibited by only allowing traffic flow to trusted DHCP server using “DHCP snooping.”
3. CAM and DHCP starvation attack is getting prevented by dropping packets with unknown source addresses using “Port Security.”
4. Unwanted traffic flow is getting prevented by tracking states of TCP and filter traffic using “Layer 2 Firewall.”
5. Passing of incorrect information for routing is prevented by MD5 using “Authentication.”

### 6.3 Performance in terms of response time, packet loss, CPU load and memory utilization

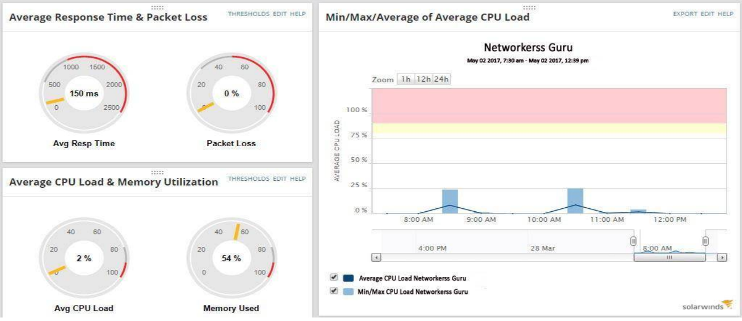


Figure 6.1: Network performance

Here, we are able to get to know network performance i.e. Average response time, packet loss and CPU load (at Min, Max, Average) while using software (GNS3).

## VII. CONCLUSION AND FUTURE SCOPE

There is a lack of security mechanism which makes the campus network vulnerable to different kinds of threats and attacks. For providing better security to campus network we can use security mechanism like ARP inspection, DHCP snooping, Port Security, Private VLAN, Time based ACL's and firewalls. Every security mechanism has its own functionality and feature. The study shows that how routing protocols like OSPF authenticates itself and how other routing protocol authenticate themselves and can be distinguished in a network. The study shows performance of network when we selected interior gateway dynamic routing protocols such as RIPv2, EIGRP and OSPF. Some redistribution issues can be seen in the network. The performance of Route redistribution technology between diverse routing protocols has significant importance. Route redistribution is certainly easily realized and cost effective technique. Through using it we can also settle Tactical Internet Communication. Comparative analysis among several routing protocol shows that the EIGRP protocol is better than the OSPF and RIPv2 routing protocol. But sometime EIGRP is held back by its proprietary features and costs. OSPF is better than other in large networks where its hierarchical nature increases scalability. And RIPv2 is useful in local and small area network.

### 7.1 Advantages

□ Designed campus network follows cisco standard three layer architecture.
□ prevention from ARP attack, rogue DHCP, DDOS , man in the middle attack and starvation atttack.
□ Good response time.
□ No packet Loss.
□ Traffic filtering mechanism is optimized.
□ Latencies are reduced.

### 7.2 Limitations

□ Memory requirement are high.
□ Use of expensive layer 3 switches.

### 7.3 Future Scope

The memory utilization of the network is quite high because of the different technology used which is one of the limitation of proposed work it can be improved in future.

## REFERENCES

[1] Mohammed Nadir Bin Ali, Prof. Dr. M. Lutfar Rahman and Prof. Dr. Syed Akhter Hossain, "Network Architecture and Security Issues in Campus Networks", Daffodil International University Dhaka, Bangladesh, 2013.
[2]Yaxun Lan, Zhengshi Chen, " The research on the OSPF security optimizing of Campus Network.", Guangzhou Vocational College of Science and technology, Guangzhou, China, 2015.
[3]Song ji, Ling Pang and WenYing, "Campus network security analysis and design of security system", China University of Geosciences Great Wall College BaoDing , China, 2015.
[4] Qiang Li, Tao Qin, Xiaohong Guan and Qinghua Zheng, "Empirical Analysis and Comparison of IPv4-IPv6 Traffic: A Case Study on the Campus Network", Xian Jiaotong University, Xian, China, 2012.
[5] Golap Kanti Dey, Md. Mobasher Ahmed and Kazi Tanveer Ahmeed, "Performance Analysis and Redistribution among RIPv2, EIGRP & OSPF Routing Protocol", University of Chittagong, Chittagong-433I , Bangladesh, 2015
[6] Abhishek Verma and Neha Bhardwaj, "A Review on Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) Routing Protocol", Gwalior,M.P, India, 2016.
[7] Eiji Oki, Yasunori Nakahodo, Takashi Naito and Satoru Okamoto, "Implementing Traffic Distribution Function of Smart OSPF in Software-Defined Networking", The University of Electro-Communications, Tokyo, Japan, 2015.
[8] Manoj Barnela, Akhil Kaushik, Satvika, " Performance Analysis of OSPF, RIP, IGRP and EIGRP Routing Protocols", TIT & S, Bhiwani, India, 2015
[9] Chandra Wijaya, "Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network", Parahyangan Catholic University Bandung, Indonesia, 2011.
[10] Megha Jayakumar N Ramya Shanthi Rekha, and Dr.B.Bharathi, "A Comparative study on RIP and OSPF protocols", Sathyabama University Chennai, India 2015.
[11]L. A. Maskari, Sanad Al; SAini, Dinesh Kumar; Raut, Swati Y; Hamdimani, "Secuirty and Vulnerability Issues in University Networks," Proc. World Congr. Eng., vol. I, pp. 1–5, 2011.
[12]D. Song and F. Ma, "Strategy and implementation of campus network security," 2012 Int. Conf. Syst. Informatics, ICSAI 2012, no. Icsai, pp. 1017–1019, 2012.
[13]Q. Zhao, Y. Mou, and S. H. Qin, "The design of security authentication system based on campus network," Proc. - Int. Conf. Electr. Control Eng. ICECE 2010, pp. 3070–3073, 2010.
[14]X. Wang and S. Zhang, "Research about optimization of campus network security system," Procedia Eng., vol. 15, pp. 1802–1806, 2011.
[15]G. Nakibl, "OSPF Vulnerability t o Persistent Poisoning Attacks : A Systematic Analysis", 2014.
[16]M. Nadir, B. Ali, M. E. Hossain, and M. Parvez, "Design and Implementation of a Secure Campus Network," Int. J. Emerg. Technol. Adv. Eng., vol. 5, no. 7, pp. 370–374, 2015.
[17]X. Li and T. Jiang, "Design and implementation of the campus network monitoring system," Proc. - 2014 IEEE Work. Electron. Comput. Appl. IWECA 2014, pp. 117–119, 2014.
[18]W. Zongjiang, "A New Type of Intelligent Network Security Model of the Campus Study",2011
[19]E. Kaffashi, A. M. Mousavi, H. R. Rahvard, S. H. Bojnordi, F. Khademsadegh, and S. Amirian, "A new attack on link-state database in open shortest path first routing protocol," vol. 3, pp. 39–45, 2015.
[20]S. Publisher, S. Arkadii, C. Vadym, and C. Vadym, "Improvement of EIGRP Protocol Routing Algorithm with the Consideration of Information Security Risk Parameters," vol. 3, no. 8, pp. 707–714, 2015.
[21]K. A. Al-Saud, H. Tahir, M. Saleh, and M. Saleh, "A performance comparison of MD5 authenticated routing traffic with EIGRP, RIPv2, and OSPF," Int. Arab J. Inf. Technol., vol.7, no. 4, pp. 380–387, 2010.
[22]M. Yang, Y. Wang, and H. Ding, "Design of Win Pcap Based ARP Spoofing Defense System," 2014 Fourth Int. Conf. Instrum. Meas. Comput. Commun. Control, pp. 221–225, 2014.
[23] R. O. Verma, "Effective Remote Management for Inter-VLAN Routing Networks," vol. 2013, no. Ratmig, 2013.
[24] D. Srinath, S. Panimalar, A. Jerrin Simla, and J. Deepa, "Detection and Prevention of ARP Spoofing using Centralized Server," vol. 113, no. 19, pp. 26–30, 2015.
[25] Abhishek Verma and Neha Bhardwaj, " A Review on Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) Routing Protocol ", 2013
[26] Hucaby, David. CCNP Routing And Switching SWITCH 300-115. 1st ed. Indianapolis: Cisco Press, 2015.
[27] Wallace, Kevin. CCNP Routing And Switching ROUTE 300-101 Offical Cert Guide. 1st ed. Indianapolis, IN: Pearson Education, 2015.
[28] Boger, Paul. CCNA Security. 1st ed. Indianapolis, IN: Cisco Press, 2015.
[29] "Free CCNA Tutorials. Study CCNA For Free!". Study-ccna.com. N.p., 2017. Web. 21 Mar. 2017.
[30] "Cite A Website - Cite This For Me". Networkstraining.com. N.p., 2017. Web. 21 Mar. 2017.