IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 6, June 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306061|

Design and Implementation of Enterprise Network in Cisco Packet Tracer

V.Ellappan[1], D.Krishnakumar[2], D.Dhnanush[3], S.Jeeva[4], A.Abimani [5]

Professor, Department of ECE, Mahendra Institute of Technology, Tamil Nadu, India[1]

Final Year Students, Department of ECE, Mahendra Institute of Technology, Namakkal, Tamil Nadu, India[2,3,4,5]

ABSTRACT: The growth of the Internet proposes also leads to challenges for information security. Routing protocols used to distribute routing informations between routers and layer3 switches capable of routing. Routers are capable of finding least hop route according to the routing information and forward the data packet by the routing protocols. Without router protocol, the data packet is not forward to its destination or dropped by routers which does not having the destination network. So OSPF (Open Shortest Path First) routing protocol is implemented for providing scalability and availability of networks inside enterprises. This paper explains about the security of enterprise network using access control lists, enabling console password, enabling ssh in routers.

KEYWORDS: access control list, ssh, ospf , network, security.

I. INTRODUCTION

With the growing development of Internet technology, the amount of networks is getting huge and huge, and the topology of the networks is also raising in complex manner, and making the availability of Internet is necessary for network infrastructures. Routing protocol is the main keything of network infrastructure, this helps other routers to share information in their routing tables. Routers with routing capability that constructs routing tables by getting and reassembles this information to other routers to provide forwarding services. If there's no routing information, data packets face the threat of data notsufficiency or leads to packet failure. Therefore, routing protocol is the basis for transmitting data packets, playing a important role in network security. Open Shortest Path First (OSPF) routing protocol is a interior gateway protocol established for the development of the Internet. It having the distinctive qualities of particular parameters in link-state routing protocol for broadcasting routing information between routers in the same group of autonomous system. Routers with OSPF protocols broadcast its routing table to others and getting the routing information of the whole autonomous systems, thus understanding the entire autonomous network topologys and operate routers independently. Because OSPF having characteristics of scalability and fast transmitting, it become the widely implemented for interior gateway protocol. One of the best security practices for implementing remote access is Secure Shell (SSH). The Secure Shell (SSH) protocol a method for securely sending commands to a computer over an unsecured network. SSH uses cryptography to authenticate and encrypt connections between devices.

II. ENTERPRISE NETWORK USING CISCO PACKET TRACER

A. Description of our Enterprise Network

In our model, we have created 12 departments for our enterprise network. Each floor has 4 departments respectively. The first floor consists of Marketing, Management, Finance, Human Resource departments. The second floor consists of Java-developers, Python-developers, App-developers, Full Stack departments. The third floor consists of a Server room, Tech support, Legal, AI departments.

TABLE 1Department's network and subnet mask

Department	Network	Subnet Mask
Marketing	192.168.0.0	255.255.255.0
Management	192.168.1.0	255.255.255.0
Finance	192.168.3.0	255.255.255.0

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306061|

HR	192.168.4.0	255.255.255.0
Java-Dev	192.168.5.0	255.255.255.0
Python-Dev	192.168.6.0	255.255.255.0
App-Dev	192.168.7.0	255.255.255.0
Full Stack	192.168.8.0	255.255.255.0
Server room	192.168.2.0	255.255.255.0
Legal	192.168.9.0	255.255.255.0
Tech Support	192.168.10.0	255.255.255.0
AI	192.168.11.0	255.255.255.0

The networks used are class c private IP addresses with the subnet mask of /24. The single /24 network has 256 IP addresses, starting IP address is reserved for denoting the network and ending IP address is reserved for broadcast purpose. The remaining 254 IP addresses are used to connecting devices.

TABLE 2 : Department's Gateway and maximum number of users

Department	Gateway	Max Users
Marketing	192.168.0.1	254
Management	192.168.1.1	254
Finance	192.168.3.1	254
HR	192.168.4.1	254
Java-Dev	192.168.5.1	254
Python-Dev	192.168.6.1	254
App-Dev	192.168.7.1	254
Full Stack	192.168.8.1	254
Server room	192.168.2.1	254
Legal	192.168.9.1	254
Tech Support	192.168.10.1	254
AI	192.168.11.1	254

B. Device Specifications

For this enterprise network we have used 26 routers, 6 layer 3 switches, 12 layer 2 switches, 3 sniffers, 12 pc.

For router, cisco 2911 Integrated Services Router is deployed. It offers high-speed ethernet connectivity with data rates of 10, 100, 1000 Mbits/s. It is equipped with three LAN/WAN ports. It also has four SFP (Scalable Form-Factor Pluggable) interfaces for WAN connection and two onboard digital signal processors.

For layer 3 switch, cisco catalyst 3650 is deployed. It offers high-speed ethernet connectivity with data rates of 10, 100, 1000 Mbits/s. It is equipped with 24 LAN ports. It also has four SFP (Scalable Form-Factor Pluggable) interfaces for LAN.

For layer 2 switch, cisco catalyst 2960 is deployed. It offers high-speed ethernet connectivity with data rates of 10, 100, 1000 Mbits/s. It is equipped with 24 LAN ports.

For sniffers and pc, the default model form cisco packet tracer is deployed.

III. EXPERIMENT

For designing and implementing the enterprise network, we have used cisco's packet tracer software. Which is a tool for designing and simulating switching, routing techniques.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306061|

For this model we have used a 3-tier architecture model. Tiers in this model are core layer, distribution layer, access layer.

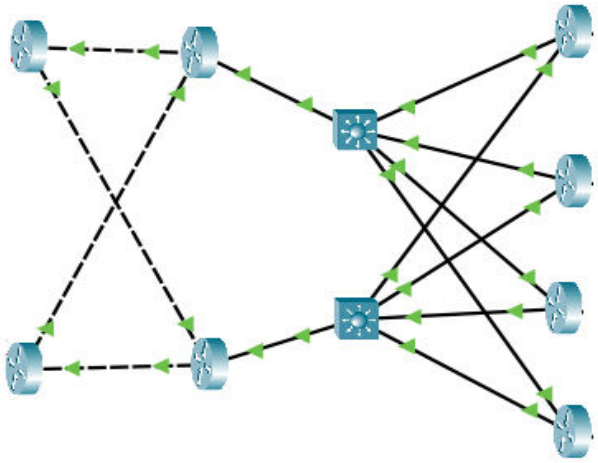


Figure 1Representation of 3-tier architecture

C. Design Scenario

By using star topology, we can increase network's reliability, performance and easy to manage all the connecting nodes. We have used different types of cable for connection. Copper straight-through cable is used to connecting layer 2 switches and pc. Copper cross-over cable is used to connecting routers to routers.

Floor 1 have the departments of Marketing, Management, Finance, HR

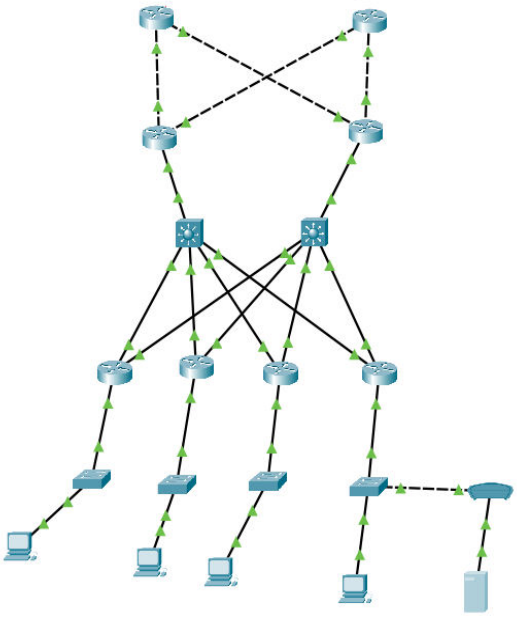


Figure 2Representation of floor 1 design

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306061|

Floor 2 have the departments of Java, Python, App, Full Stack developers

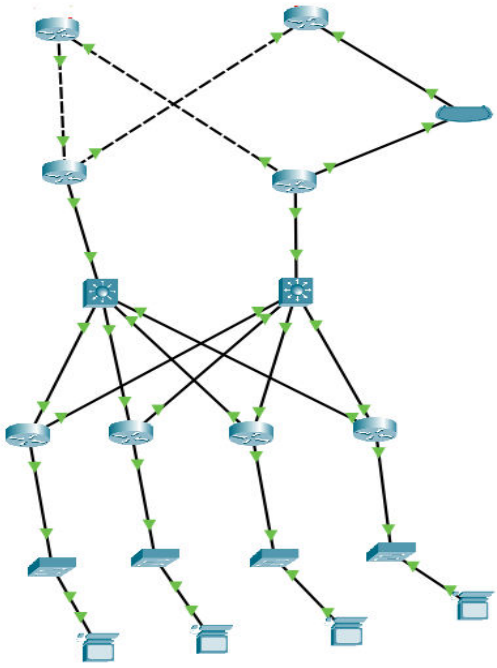


Figure 3 Representation of floor 2 design

Floor 3 have departments of Server room, Tech support, Legal, AI

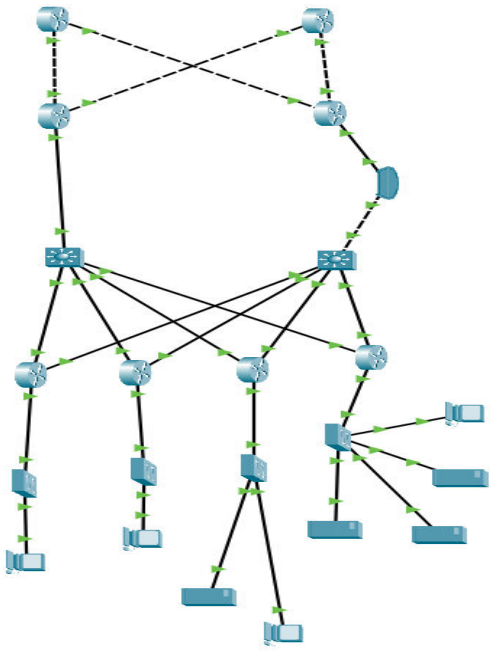


Figure 4Representation of floor 3 design

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306061|

D. Router Switch configuration

For increasing the security features in routers, we have enabled enable password as ccna for all the routers and switches. And turned on the password encryption

Syntax for configuring enable password:

Enable password <password>

Service password-encryption

E. SSH Configuration

SSH gives encrypted connection for remote access. We have configured SSH in all the routers with a unique loopback address with the subnet of 255.255.255.255. Transport input ssh is for allowing SSH traffic only.

Syntax for ssh configuration:

Hostname <hostname>

Ip domain-name <domain.name>

Crypto key generate rsa general-keys modulus <key_length>

Line vty 0 4

Login local

Transport input ssh

Username <username> password <password>

F. Configuring OSPF

For configuring the routing protocol, we are using OSPF (Open Short Path First) routing. It gathers available link state information from available routers and constructs topology map according to the network information.

Syntax for OSPF configuration:

Router ospf <process_id>

Router-id <router_id>

Network <network_address> <wildcard_mask> area <area_number>

G. Console Configuration

Without using ssh for configuration, we need console cable for configuring the network devices. Incase console password is not set, anyone with console cable can be able to configure network devices. To prevent this practice, we are enabling the password for console ports in network devices.

Syntax for configuring console password:

Line con 0

Login local

Username <username> password <password>

H. Access control list Configuration

By implementing an access control list, we can permit or deny IP addresses based on access control rules.

Syntax for access control list:

Ip access-list <standard>/<extended> <group_id>

<permit>/<deny> <IP_address> <wildcard_mask>

Interface <interface_name_where_the_network _is_present>

Ip access-group <group_id> <in>/<out>

IV. RESULT

I. Checking console password

Here we are going to check the console password for the console port.

```
User Access Verification

Username:
```

Figure 5Ask for username

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306061|

When the user gives the correct username and password, it prompts to user exec mode

```
User Access Verification

Username: router
Password:

6.6.6.6>
```

Figure 6 After entering valid credentials

When the user enters invalid credentials, it asks again

```
User Access Verification

Username: router
Password:
% Login invalid

Username:
```

Figure 7When user enters invalid credentials

J. Checking enable password

When user wants to move for privileged exec mode, user needs to enable the network devices by typing enable command. By enabling the enable password, when the user gives enable command it asks password.

```
6.6.6.6>en
Password:
```

Figure 8Asks for enable password

```
6.6.6.6>en
Password:
6.6.6.6#
```

Figure 9User exec changed to privileged exec mode

K. Checking access control lists

Here we configured the access control list for the Finance department. The employees of Management and Server room are only able to ping finance department.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

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

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure 10Ping from Marketing department

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306061|

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.2: bytes=32 time<1ms TTL=126
Reply from 192.168.3.2: bytes=32 time<1ms TTL=126
Reply from 192.168.3.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure 11Ping from Management department

L. Checking SSH

For checking SSH, login at a different router or pc

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 1.1.1.1

Password:



1.1.1.1>
```

Figure 12 Login 1.1.1.1 router from server room pc

M. Checking OSPF routes

For checking OSPF routes, give the command show ip ospf database

```
1.1.1.13#sh ip ospf database
           OSPF Router with ID (1.1.1.13) (Process ID 1)

               Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link cou
1.1.1.10        1.1.1.10        1503        0x8000000a 0x0001d3 9
9.9.9.9         9.9.9.9         1503        0x8000000a 0x003f4e 9
1.1.1.12        1.1.1.12        1469        0x80000008 0x002120 5
1.1.1.4         1.1.1.4         1468        0x80000008 0x00e1f5 4
1.1.1.2         1.1.1.2         1468        0x80000008 0x0001b9 5
8.8.8.8         8.8.8.8         1468        0x8000000a 0x005ed3 7
1.1.1.3         1.1.1.3         1468        0x8000000a 0x000a07 7
1.1.1.5         1.1.1.5         1468        0x80000008 0x00c2dd 4
1.1.1.11        1.1.1.11        1468        0x80000008 0x00b1ba 5
1.1.1.14        1.1.1.14        1468        0x80000008 0x006ed2 4
5.5.5.5         5.5.5.5         1467        0x80000008 0x002db9 4
1.1.1.9         1.1.1.9         1471        0x80000007 0x003fd3 4
3.3.3.3         3.3.3.3         1466        0x80000007 0x00982d 4
1.1.1.7         1.1.1.7         1464        0x80000009 0x007f9c 4
1.1.1.6         1.1.1.6         1464        0x80000007 0x001c08 4
1.1.1.15        1.1.1.15        1464        0x80000007 0x000a5a 4
4.4.4.4         4.4.4.4         1463        0x80000009 0x0011a3 4
1.1.1.16        1.1.1.16        1463        0x80000007 0x0080d7 4
1.1.1.1         1.1.1.1         1463        0x80000007 0x004b98 4
1.1.1.8         1.1.1.8         1463        0x80000009 0x0054be 4
6.6.6.6         6.6.6.6         1463        0x80000008 0x00d717 4
2.2.2.2         2.2.2.2         1463        0x8000000b 0x00864a 4
7.7.7.7         7.7.7.7         1463        0x80000008 0x0012db 5
1.1.1.18        1.1.1.18        1459        0x80000007 0x004ffc 4
```

Figure 12Router link states

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306061|

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
172.16.0.74	1.1.1.14	1474	0x80000001	0x009f71
172.16.0.33	7.7.7.7	1474	0x80000001	0x006ae3
172.16.0.9	1.1.1.5	1474	0x80000001	0x00f575
172.16.0.45	8.8.8.8	1473	0x80000001	0x008153
172.16.0.5	1.1.1.4	1473	0x80000001	0x00046e
172.16.0.37	7.7.7.7	1473	0x80000002	0x009d4c
172.16.0.70	1.1.1.14	1469	0x80000002	0x007073
172.16.0.78	1.1.1.13	1469	0x80000001	0x009d6e
172.16.0.2	1.1.1.4	1468	0x80000002	0x001a5b
172.16.0.42	8.8.8.8	1468	0x80000002	0x008b4f
172.16.0.66	1.1.1.13	1468	0x80000002	0x000e0a
172.16.0.14	1.1.1.5	1468	0x80000002	0x00c79c
10.20.1.4	1.1.1.9	1464	0x80000006	0x00bdaa
10.10.1.4	1.1.1.9	1463	0x80000008	0x003041
10.60.1.5	1.1.1.18	1459	0x80000008	0x00f70f
10.30.1.1	6.6.6.6	1464	0x80000004	0x001435
10.50.1.5	1.1.1.18	1449	0x8000000a	0x006aa5
10.40.1.1	5.5.5.5	1449	0x80000004	0x00d670

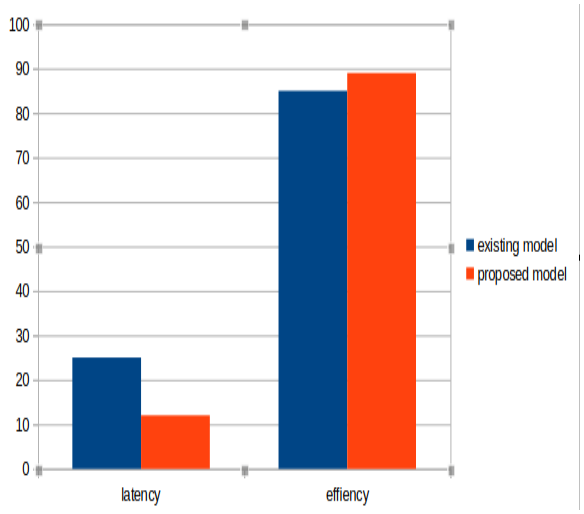
Figure 13 Net link states

N. Comparing Existed model vs proposed model

TABLE 3Comparing two models

	Existing model	Proposed model
Ssh	No	Yes
Latency	High	Low
Latency (ms)	25 ms	12 ms
Effiency (%)	85%	89%
Protocol	Ospf	Ospf
Architecture	star	Hybrid with 3-tier
Access control	No	Yes

GRAPH: 1COMPARISON OF LATENCY EFFIENCY OF EXISTING MODEL VS PROPOSED MODEL



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306061|

V. CONCLUSION

In the modern world, we require modern solutions for some problems as well as traditional solutions for some problems. Adding more layers of security is also a solution for some of the cyber-attacks. In this enterprise model, we have configured manual mode for giving IP address to prevent DHCP (Dynamic Host Configuration Protocol) spoofing attacks. And also disabled Telnet for remote access. Instead of Telnet, we have configured SSH for remote access. Access control lists are configured to some departments like Finance, HR, Legal etc... for providing excess security for confidential documents and files.

REFERENCES

1. D. Awduche, A. Chiu, A. Elwalid, I. Widjaja and X. Xiao, "Overview and Principles of Internet Traffic Engineering", Rfc-editor.org, 2002.[Online].Available:http://www.rfc-editor.org/info/rfc3272.[Accessed:23-March-2024].
2. Juniper Networks - LSA exists in the OSPF database, but not populated in the routing table - Knowledge Base", Kb.juniper.net, 2016. [Online].Available:http://kb.juniper.net/InfoCenter/index?page=content&id=KB13547.[Accessed: 11- Dec- 2023].
3. "Common Routing Problem with OSPF Forwarding Address", Cisco,2016.[Online].Available:http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13682-10.html. [Accessed: 11- Dec- 2023].
4. OpenFlow: Proactive vs Reactive", NetworkStatic | Brent Salisbury'sBlog, 2013. [Online]. Available: http://networkstatic.net/openflow-proactive-vs-reactive-flows/. [Accessed: 11- Dec- 2023].
5. Theofilos Sachinidis, Anastasios C. Politis, Constantinos S. Hilas, "To Split or not to Split? A Simulation Study on the Network Convergence Duration of Multi-Area OSPF", 2023 46th International Conference on Telecommunications and Signal Processing (TSP).
6. Jayanta Borthakur, "A comparison study of single area OSPF Network to multiple area OSPF Network implementation in a Campus area Network", 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT).
7. Jun Tao, Renbin Yuan, Qingqing Liu, Qinghuan Xia, "Research and Implementation of a Network Based on SDN and Multi Area OSPF Protocol", 2021 IEEE 9th International Conference on Information, Communication and Networks (ICICN)
8. Heru Nurwarsito, Achmad Rero Sindunata, "Optimization of Hello Interval in OSPF Routing Protocol Performance on Mesh Network Topology", 2020 10th Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS).
9. Asad Ali Khan, Muhammad Zafrullah, Majid Hussain, Ali Ahmad "Performance Analysis of OSPF and Hybrid Networks", 978-1-5386-1556-0/17/$31.00 ©2017 IEEE
10. D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S.Azodolmolky and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey", in Proceedings of the IEEE, vol. 103, no. 1, pp.14-76, Jan. 2015
11. E. C. G. Wille and M. M. Tenório, "Considering Packet Loss Probability in Fault-Tolerant OSPF Routing", IEEE LATIN AMERICA TRANSACTIONS, VOL. 12, NO. 2, MARCH 2014
12. Wei K, Shoushan L, Yang X. "Research and Analysis of the Security Mechanism on OSPF[J]", Sciencepaper Online, 2009.
13. M. Garetto, D. Towsley, "An efficient technique to analyze the impact of bursty TCP traffic in wide-area networks, Performance Evaluation", pp.181-202, Vol. 65, N. 2, 2008.
14. Di X, Jing Y, "A Kind of Low-cost and Reliable OSPF Authentication Mechanism[J]", Journal of Computer Applications, 2003.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details