International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 05 | May - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Implementing Vlan Technology to L2 and L3 Switches and Network Automation

Sindhu M K
II Semester MTech CNE, Department of Information Science and Engineering
BMS College of Engineering

Dr Radhika KR
Professor, CNE, Department of Information Science and Engineering
BMS College of Engineer Bangalore

Abstract - Number of conference rooms of Intel campus are noted and validated with the respective team. The rise in remote work has made video conferencing systems a necessary tool for many businesses. Microsoft Teams Room has all the necessary tools to hold productive meetings.
Automation of Access-list (ACL) viewing process has gained scope, since it is easier to access and make changes and less time consuming. ACL is a conventional set of rubrics defined for regulatory of the network traffic and reducing network outbreak. ACLs are used to riddle traffic based on the set of rules defined for the arriving or departing from the network.

I INTRODUCTION

To Provide Network Connectivity reference for Microsoft Team. This project is executed to provide next generation video conferencing solution. Objective of this project is subjected to provide backbone connectivity for MTR.

Number of conference rooms of Intel campus are noted and validated with the respective team. The rise in remote work has made video conferencing systems a necessary tool for many businesses. Microsoft Teams Room has all the necessary tools to hold productive meetings.

Access list is an established set of instructions well- defined for directive network traffic flow as in intending and implying the necessary and access grant authentic traffic should flow in the network.

ACL features:

The established set of instructions expressed are coordinated serial wise i.e., identical flinches with the initial line, then 2nd, then 3rd and so on.

The packets are coordinated only till it ties the rule. Once a rule is coordinated then no additional assessment takes place and that instruction will be performed.

There is an implied deny at the end of each ACL, i.e., if no disorder or rule matches then the packet will be rejected.

II. CHALLENGES

The major difficulty in order to implement this new network backbone to the existing network architecture is to per check for the availability of unused subnets in the network system. Analysis is made in order to understand how many of the subnets should be reserved to process this network implementation. Thorough background verification is done related to the presence of number of video conferencing rooms in the subjected campus. While implementing the configurations to get the Vlan backbone connectivity in the command prompt, a small mistake of syntax in the command can let the whole network system down.

III. State of work

"Design and Implementation of Application-based Secure VLAN" Minli Zhu, Mart Molle and Bala Brahmam.

Authors of this paper have expressed interest in explaining the application based secure Vlan with its pro and cons. Detailed description is also given about the prototype used for Implementation of S-based Vlan and its related application.

"Applied Study of Layer 3 Switching Configuration Based on VLAN Among Colleges' Library Network Systems" Zhang Yaojun, Liu Hao, Ren Feng

Authors of this paper have discussed about the problems of network security that may arise during the planning and implementation of Vlan among the colleges 'Library network system and importance of Vlan and its features with that they have proposed a solution to the network security issues.

"Multi-VLAN Design over IPSec VPN for Campus Network" Sasalak Tongkaw, Aumnat Tongkaw

Authors of this paper defines the VLAN strategy and implementation of multi-application amongst two campuses of Songkhla Rajabhat University. The study gives illustrations of three aids of multi-VLAN design, primary, it is a profitable way to deploy numerous types of applications, subsequent, it rises safety and security, and tertiary, it can also decrease the network administrators' supervision of upholding and managing the network as a whole.

IV. Table of work

Simple IP Subnet Vlan Implementation	Vlan Implementation is well expressed with simple terms and limitations of this Implementation are mentioned as well.
A Secure Vlan Construction Protocol in Wireless Ad Hoc Networks.	SVCP is proposed to enhance the performance in the area of Ad hoc Network.
Enhancement of Industrial Ethernet Performance Using Multicasting/VLAN techniques	Industrial Ethernet performance under different conditions is studied with a detailed format.
Design and Implementation of Application-based Secure VLAN	Security and access control list is majorly concentrated and possible new approaches are discussed and mentioned.
Applied Study of Layer 3 Switching Configuration Based on VLAN Among Colleges' Library Network Systems	Problems related to network security is discussed and analysis is made to give it a structure for a college 'Library Network system.
Finding efficient VLAN topology for better broadcast containment	Different set of Topologies of Vlans are mentioned and a detailed study is subjected to choose an efficient topology for a better usage.
Research on VLAN Technology in L3 Switch	Classification of L2 and L3 is predominantly mentioned and its functionality is described with its characteristics.

V. Proposed Work

Microsoft Teams Room Network Deployment

Pre-Implementation

For Video Conferencing Solution Cisco Telepresence Codec 100(STD-HD) was used.

The Cisco Telepresence portfolio creates an immersive, in-person understanding over the network- authorizing you to cooperate with others like never before. From side to side an authoritative amalgamation of technologies and policy that permits you and distant contributors to feel as if you are all in the similar chamber, the Cisco Telepresence portfolio has the impending attitude to provide boundless productivity assistances and renovate your business.

Implementation

To Implement the Microsoft Teams room to the conference rooms, with lot of pre-work and validation of ports and considering the requirement specified by the project owners list of rooms and number of ports are decided. Using Excel Sheets all necessary data is updated regarding Ip address for each network devices and scope is also subjected to the switches to create new Vlan and to add Vlan number for allowing the traffic through specified port cannel, and spanning tree is set to prioritize the traffic follow and the network is advertised under routing protocol. Router ACL (Access list) is added to allow the traffic into the device.

All the necessary implementation commands are listed and added according to the switches to create a level 2 Vlan implementation.

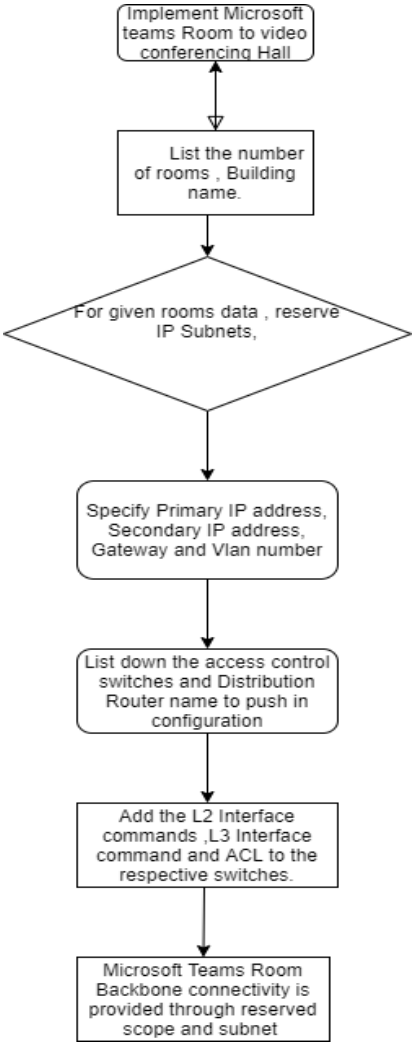


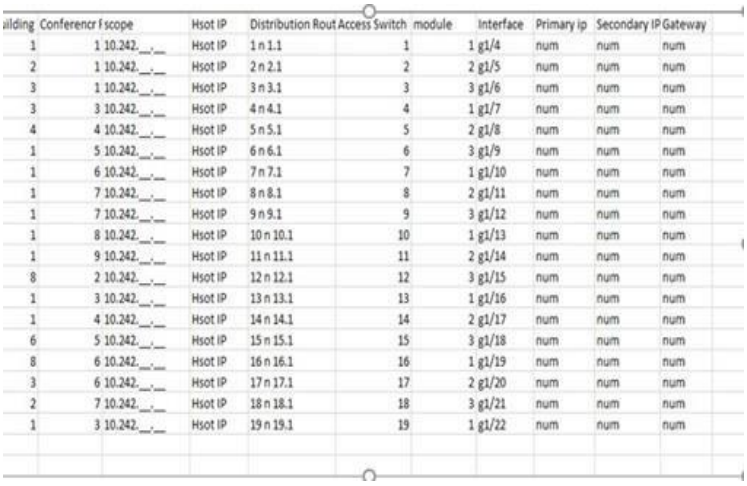
Fig 1: Flowchart of Implementation

Microsoft Teams is a determined chat-centered association platform comprehensive with document division, online conferences, and many more enormously useful structures for corporate communications. Having an outstanding team space is key to being able to make creative choices and interconnect with one another.

Step 1: To perform L2 and L3 implementation, there are few important steps to be followed.

Create a Ip planning list it should include all the necessary data such as:

- Building name
- Room number
- Vlan Number
- Distribution Router name
- Access Switch name
- Module number
- Interface
- Primary Ip
- Secondary Ip
- Gateway



ilding	Conferencr Fscope	Hsot IP	Distribution Rout	Access Switch	module	Interface	Primary ip	Secondary IP	Gateway
1	1 10.242.__.__	Hsot IP	1 n 1.1	1		1 g1/4	num	num	num
2	1 10.242.__.__	Hsot IP	2 n 2.1	2		2 g1/5	num	num	num
3	1 10.242.__.__	Hsot IP	3 n 3.1	3		3 g1/6	num	num	num
3	3 10.242.__.__	Hsot IP	4 n 4.1	4		1 g1/7	num	num	num
4	4 10.242.__.__	Hsot IP	5 n 5.1	5		2 g1/8	num	num	num
1	5 10.242.__.__	Hsot IP	6 n 6.1	6		3 g1/9	num	num	num
1	6 10.242.__.__	Hsot IP	7 n 7.1	7		1 g1/10	num	num	num
1	7 10.242.__.__	Hsot IP	8 n 8.1	8		2 g1/11	num	num	num
1	7 10.242.__.__	Hsot IP	9 n 9.1	9		3 g1/12	num	num	num
1	8 10.242.__.__	Hsot IP	10 n 10.1	10		1 g1/13	num	num	num
1	9 10.242.__.__	Hsot IP	11 n 11.1	11		2 g1/14	num	num	num
8	2 10.242.__.__	Hsot IP	12 n 12.1	12		3 g1/15	num	num	num
1	3 10.242.__.__	Hsot IP	13 n 13.1	13		1 g1/16	num	num	num
1	4 10.242.__.__	Hsot IP	14 n 14.1	14		2 g1/17	num	num	num
6	5 10.242.__.__	Hsot IP	15 n 15.1	15		3 g1/18	num	num	num
8	6 10.242.__.__	Hsot IP	16 n 16.1	16		1 g1/19	num	num	num
3	6 10.242.__.__	Hsot IP	17 n 17.1	17		2 g1/20	num	num	num
2	7 10.242.__.__	Hsot IP	18 n 18.1	18		3 g1/21	num	num	num
1	3 10.242.__.__	Hsot IP	19 n 19.1	19		1 g1/22	num	num	num

Fig 2: Ip planning File

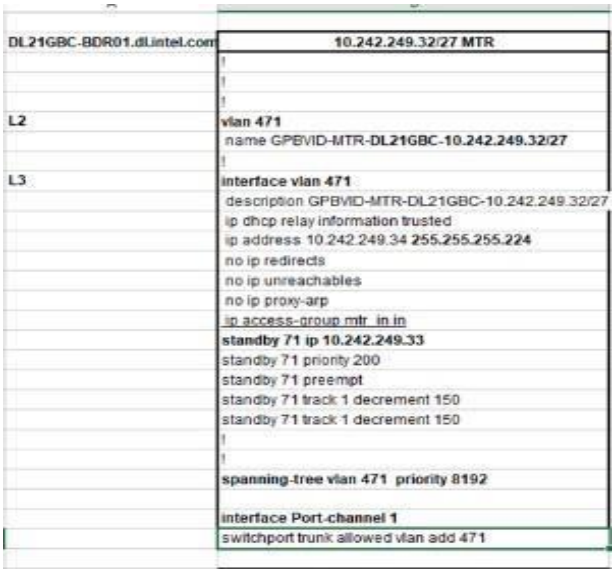
Once the IP planning list is ready, should per validate before performing the change and should execute all test cases accordingly to the change that is been implemented.
Backup should be taken to the Routers and switches before implementing or configuring new interfaces to the running network.

Step 2: Generate a configuration file

Generating a configuration file is very important and should be done prior to perform any change and should be validated twice and should have accurate data and command in this type.

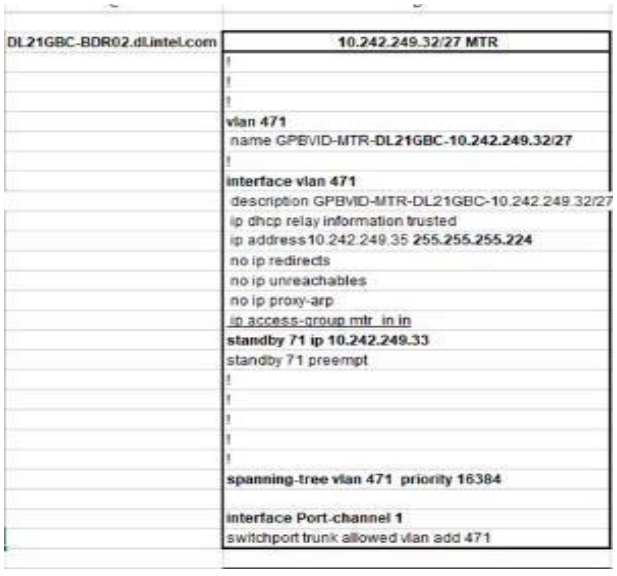
Content of the file:

L2 interface commands L3 interface commands Router ACL.



DL21GBC-BDR01.dl.intel.com	10.242.249.32/27 MTR
	!
	!
	!
L2	**vlan 471**
	name GPBVID-MTR-**DL21GBC-10.242.249.32/27**
	!
L3	**interface vlan 471**
	description GPBVID-MTR-DL21GBC-10.242.249.32/27
	ip dhcp relay information trusted
	ip address 10.242.249.34 **255.255.255.224**
	no ip redirects
	no ip unreachables
	no ip proxy-arp
	ip access-group mtr_in in
	standby 71 ip 10.242.249.33
	standby 71 priority 200
	standby 71 preempt
	standby 71 track 1 decrement 150
	standby 71 track 1 decrement 150
	!
	!
	spanning-tree vlan 471 priority 8192
	interface Port-channel 1
	switchport trunk allowed vlan add 471

Fig 3: Configuration File 1



DL21GBC-BDR02.dl.intel.com	10.242.249.32/27 MTR
	!
	!
	!
	vlan 471
	name GPBVID-MTR-**DL21GBC-10.242.249.32/27**
	!
	interface vlan 471
	description GPBVID-MTR-DL21GBC-10.242.249.32/27
	ip dhcp relay information trusted
	ip address10.242.249.35 **255.255.255.224**
	no ip redirects
	no ip unreachables
	no ip proxy-arp
	ip access-group mtr_in in
	standby 71 ip 10.242.249.33
	standby 71 preempt
	!
	!
	!
	!
	!
	spanning-tree vlan 471 priority 16384
	interface Port-channel 1
	switchport trunk allowed vlan add 471

Fig 4: Configuration File 2

Retrieving Access List of network devices through Automation

Implementation

To Improve network performance and to Provides security as administrator can configure the access list according to the needs and deny the unwanted packets from entering the network. ACL will also Provide control over the traffic as it can permit or deny according to the need of network. They also work on a set of rules that define how to forward or block a packet at the router's interface.

To make the ACL automated, the details which user has to give, such as Username to access the ACL and the password for the username basically taking credential as input to the code. The details about the device name and the IP address of the device, as in taking the inputs to understand which device's ACL wants to be accessed. The code also Fetches ACL details such as the name of the ACL or its ID.

.

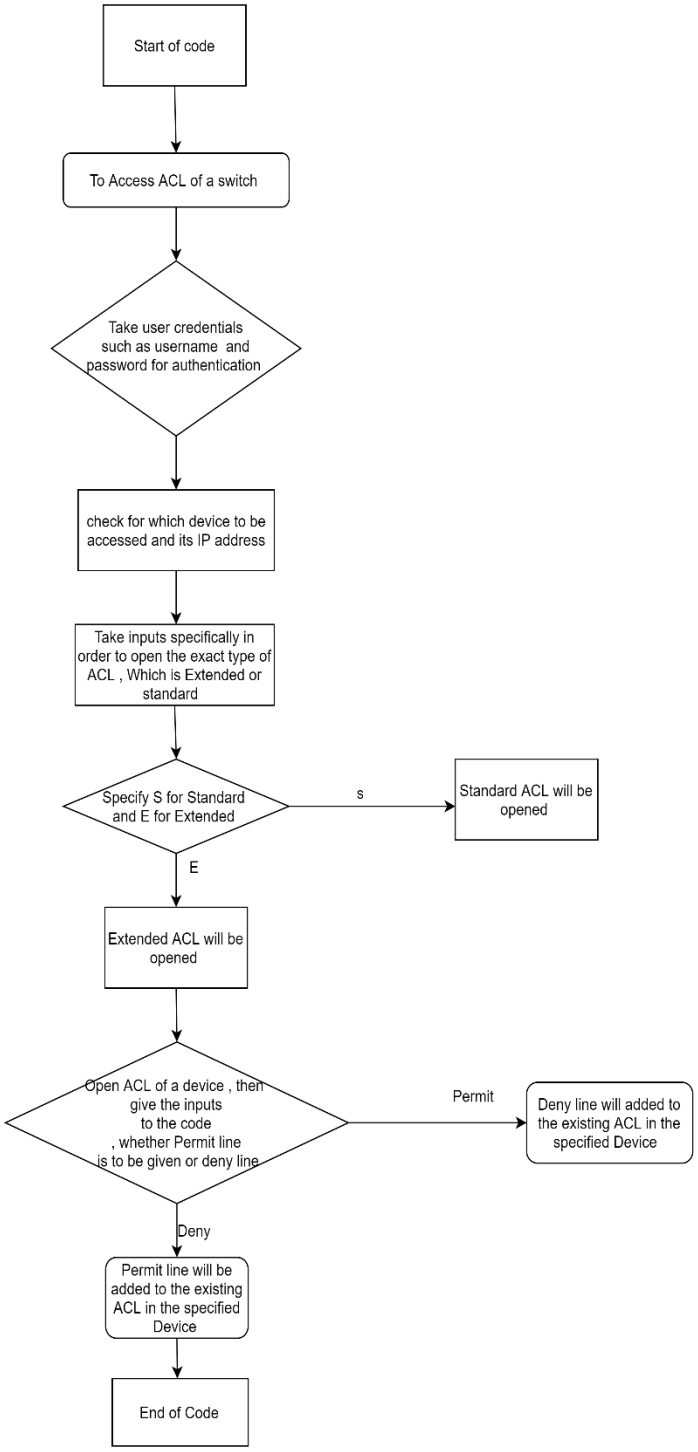


Fig 5: Flowchart of Implementation

ACL code will learn from the user accessing the code to fetch the ACL in two different format such as Standard ACL and Extended ACL, which will be given by the user as input to the code. The main functionality of this code is to add ACL Permit or deny lines into the existing ACL code of the subjected device.

```
---
- name: prompt
  hosts: localhost
  gather_facts: false
  vars_prompt:

    - name: username
      prompt: "What is your username?"
      private: no

    - name: password
      prompt: "What is your password?"
      private: yes

    - name: device_name
      prompt: "What is your Device name/IP Address?"
      private: no

  tasks:
    - name: Add host
      add_host:
        name: "{{device_name}}"
        ansible_ssh_user: "{{ username }}"
        ansible_ssh_pass: "{{ password }}"
        ansible_become_pass: "{{ password }}"
        ansible_connection: network_cli
        ansible_network_os: ios
        ansible_become: yes
        ansible_become_method: enable
        become_user: admin
        group: added_hosts

- hosts: added_hosts
  gather_facts: false
  vars_prompt:

    - name: acl_name
      prompt: "give the acl you want to add permit line in"
      private: no
      register: acl_name

    - name: acl_line
      prompt: "Give the line to add in ACL except initial permit"
      private: no
      register: acl_line

    - name: acl_type
      prompt: "Enter 'S' for standard and 'E' for extended ACL"
      private: no
      register: acl_type

  tasks:

    - name: gather device configuration details
      ios_command:
        commands: "sh ip access-list {{acl_name}}"
      register: display
    - debug:
        msg: "{{ display.stdout_lines }}"

    - name: Add ACL permit lines
      ios_config:
        lines:
          - ip access-list standard {{acl_name}}
          - permit {{acl_line}}
        parents: ip access-list standard {{acl_name}}
```

VI. Results

Vlan Backbone is successfully Implemented in 7 different Campus of Intel Technologies pvt, process of this implementation is executed around 72 Video Conferencing rooms in Intel campus , the Vlan backbone connection which is given to those room will get network connectivity through the network of Intel's network Infrastructure, thus Microsoft Teams Room became the new Video conferencing solution in those 72 video conferencing rooms,retrival of ACL automatically is also achieved by the code , which will allow the user to access the ACL of the mentioned device and to add a permit or deny line to the existing ACL of the device.

VII. Conclusion

Network Connectivity for a new device in 72 rooms effectively provided and Ip planning list which contained detailed execution requirement made the task flawless which also comprised of Subnets to be reserved , Primary IP , Secondary IP , Gateway and scope , these details lead to successfully generate a detailed configuration file , which was configured into the Distribution Router and Access switch through remote connection, thus providing the Vlan backbone to the Microsoft Teams Room to have a network connectivity.

Automating Retrival of ACL from a device is a program, where it can view and make changes to the ACL of the specified device, via taking user credentials and appropriate type of inputs regarding the type of ACL to be viewed and depending on that user will be able to add either permit or deny lines to the existing ACL of the device.

VIII. Future Work

Implementation of Microsoft Teams Room connectivity is made manually through remotely connecting to each of the devices , which are subjected for this implementation and it is configured in two levels that is via Distribution Router and Access switch to get the network connectivity to the new MTR installation , but process of execution could also be done through automation, a code can effectively run and implement the Vlan backbone simultaneously for the 72 rooms at a time and it could less time consuming.

```
  when: acl_type == "S"
  register: result

- name: Add ACL permit lines
  ios_config:
     lines:
       - ip access-list extended {{acl_name}}
       - permit {{acl_line}}
     parents: ip access-list extended {{acl_name}}
  when: acl_type == "E"

- name: Output Configuration
  ios_command:
    commands: "sho ip access-list {{acl_name}}"
  register: output
- debug:
   msg: "{{output.stdout_lines}}"
```

Fig 6: ACL Code

```
   40c-las01#
   40c-las01#              Sh ip access-list demo
Extended IP access list demo
    20 permit ip host 1.1.1.1 any
    30 permit ip any any
   40c-las01#
   40c-las01#
   40c-las01#
   40c-las01#
   40c-las01#
   40c-las01#
```

Fig 7: Before Execution of code

```
TASK [Add ACL permit lines] ************************
skipping: [       -las01.iind.     .com]

TASK [Add ACL permit lines] ************************
changed: [       las01.iind.     .com]

TASK [Output Configuration] ************************
ok: [       -las01.iind.     .com]

TASK [debug] ***************************************
ok: [       -las01.iind.     .com] => {
    "msg": [
        [
            "Extended IP access list demo",
            "    20 permit ip host 1.1.1.1 any",
            "    30 permit ip any any",
            "    40 permit ip 1.1.1.1 2.2.2.2 any"
        ]
    ]
}
```

Fig 8: Execution of code

```
      las01#
      las01#
     -las01#
    .-las01#Sh ip access-list demo
Extended IP access list demo
    20 permit ip host 1.1.1.1 any
    30 permit ip any any
    40 permit ip 1.1.1.1 2.2.2.2 any
     -las01#
     -las01#
     -las01#
     -las01#
```

Fig 9: After Execution of code

IX. References

[1] Zhang Yaojun, Liu Hao, Ren Feng, "Applied Study of Layer 3 Switching Configuration Based on VLAN Among Colleges' Library Network Systems", 978-1-4577-0860-2/11/$26.00 ©2011 IEEE.

[2] Marina Smith." Virtual Local Area Network [M]". Huang Xiwei, Wang Taoyi. Beijing: Tsinghua University press, 2003.

[3] Gan Shoufei, Zhou Guoxiang. Application Study of Institutes Library Network Based on VLAN Technology[J]. Journal of Suzhou University, 2008, 5

[4] Tang Lihua, Fang Luming. Research on the Application of Layer 3 switching and VLAN Technology in Campus Network [J]. Journal of Zhejiang A & F University,2002,19(1):86-89.

[5] Sasalak Tongkaw, Aumnat Tongkaw," Multi-VLAN Design over IPSec VPN for Campus Network" 2018 IEEE Conference on Wireless Sensors (ICWiSe)

[6] H. Nishino, Y. Nagatomo, T. Kagawa, and T. Haramaki, "A Mobile AR Assistant for Campus Area Network Management," in 2014 Eighth International Conference on Complex, Intelligent and Software Intensive Systems, Birmingham, UK, 2014, pp. 643–64

[7]] P. Titmus, "Securing IP telephony systems – best practices," Netw. Secur., vol. 2006, no. 9, pp. 11–13, Sep. 2006.

[8] Z. Fu et al., "IPSec/VPN Security Policy: Correctness, Conflict Detection, and Resolution," in Policies for Distributed Systems and Networks, 2001, pp. 39–56.

[9] Z. Ashraf and M. Yousaf, "SECURE INTER-VLAN IPv6 ROUTING: IMPLEMENTATION & EVALUATION," p. 8, 2016.

[10] D. A. J. AL-Khaffaf, "Improving LAN Performance Based on IEEE802.1Q VLAN Switching Techniques," J. Univ. Babylon, vol. 26, no. 1, pp. 286–297, 2018

[11] M. Yu, J. Rexford, X. Sun, S. Rao, and N. Feamster, "A survey of virtual LAN usage in campus networks," IEEE Commun. Mag., vol. 49, no. 7, pp. 98–103, Jul. 2011

[12] Giovanni and N. Surantha, "Design and Evaluation of Enterprise Network with Converged Services," Procedia Comput. Sci., vol. 135, pp. 526–533, Jan. 2018.

[13] S. Nichol, "VLANs usurped by virtual private networks," Comput. Secur., vol. 18, no. 4, p. 340, Jan. 1999.

[14] S. Somasundaram and M. Chandran, "A Simulation based study on Network Architecture Using Inter-VLAN Routing and Secure, Campus Area Network (CAN)," vol. 6, no. 3, pp. 111–121, Mar. 2018