Ms.Thendral K, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Implementation of Vlan, Ospf and Inter-Vlan Routing for Seamless Connectivity

Ms.Thendral K, Kaviya Sri K, Padmapriya B, Parameshwari P, Rubashri M
[1]Electronics and Communication Engineering Paavai Engineering College
Tamil Nadu,India.

Abstract- In modern enterprise and campus networks, maintaining seamless connectivity, scalability, and performance is a major challenge when multiple departments share the same network segment. Such configurations often lead to excessive broadcast traffic, reduced efficiency, and security vulnerabilities. Additionally, static routing becomes inefficient and prone to configuration errors during network changes. This project focuses on implementing Virtual Local Area Networks (VLANs) and OSPF-based Inter-VLAN Routing on Juniper SRX300 devices to achieve optimized network segmentation and dynamic routing. VLANs are configured to logically separate departmental traffic, thereby reducing broadcast domains and enhancing network security. Inter-VLAN routing enables communication between different VLANs, ensuring seamless connectivity across departments. The Open Shortest Path First (OSPF) protocol is used to provide scalable and adaptive routing, allowing the network to automatically adjust to topology changes. The iPerf tool is utilized to analyze network performance parameters such as throughput, latency, and bandwidth utilization, validating the effectiveness of the proposed setup. Experimental results demonstrate improved network performance, reduced broadcast traffic, and enhanced routing efficiency, ensuring a secure, reliable, and high-performance network infrastructure.

Keywords: VLAN, Inter-VLAN Routing, OSPF, Network Segmentation.

I. INTRODUCTION

As modern campus and enterprise networks continue to expand, the need for faster, more secure, and scalable communication systems has become increasingly important. The rise in the number of connected devices has made traditional flat network structures inefficient, often leading to network congestion and increased security risks. In such scenarios, proper traffic management, reliable fault handling, and optimized routing play a key role in ensuring stable network performance.To address these challenges, technologies such as Virtual Local Area Networks (VLANs), and Open Shortest Path First (OSPF) routing can be combined to create an efficient and flexible network design. This project focuses on implementing these solutions using Juniper SRX300 devices, which function as both security gateways and Layer 3 routers.By using VLANs, the network is divided into separate segments, allowing better security and reducing unnecessary broadcast traffic.

Link aggregation is used to increase bandwidth and provide redundancy between network devices, improving overall reliability. Additionally, OSPF enables dynamic routing, allowing the network to quickly adapt to changes and maintain connectivity. Overall, this approach results in a secure, scalable, and high-performance network architecture that is well-suited for modern campus environments with growing user and application demands.

II. LITERATURE SURVEY

K. Swapna, B. Nandeeshwar, A. Aravind, and R. Bolimera present a practical approach to campus network design using Cisco Packet Tracer, which acts as a foundational model for implementing VLAN segmentation, link aggregation, and inter-VLAN routing in academic environments. Building on such simulation-based implementations, Ajiji, Cirella, Galas, and Jadah focus on VLANs from a security standpoint, highlighting their role in isolating traffic and reducing vulnerabilities.In terms of routing efficiency, T. Sachinidis, and C. S. Hilas analyze the differences between single-area and multi-area OSPF, emphasizing network convergence time as a key performance factor.

Supporting this, Jayanta Borthakur and his team compare both approaches in campus networks and

© 2026 Ms.Thendral K, This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

observe that single-area OSPF is simpler and effective for smaller networks, whereas multi-area OSPF becomes more suitable as the network expands. This is mainly because it minimizes routing overhead, reduces LSDB updates, and limits unnecessary processing on edge devices. They further suggest a gradual transition to multi-area OSPF as network complexity increases, providing practical configuration insights for both simulation tools and real-world deployments.Cao and Ai investigate the impact of Access Control List placement on network performance. Their findings indicate that placing ACLs at the access layer helps block unwanted traffic early but increases processing overhead on multiple devices.In contrast, centralized ACL implementation reduces processing load but may allow unnecessary traffic to traverse deeper into the network.

III. PROPOSED SYSTEM

The proposed system is designed to build a secure and well-structured network using a Juniper SRX300 firewall along with Juniper EX4100 and EX2300 switches. The main goal of this setup is to organize the network efficiently by dividing it into logical segments using Virtual Local Area Networks (VLANs), which helps in better traffic management and improved performance.In this implementation, VLAN 30 (named vlan-girls) is configured to separate a specific group of users from the rest of the network. This type of segmentation reduces unnecessary broadcast traffic and enhances overall network efficiency. The VLAN is created and managed on the EX4100 and EX2300 switches, which function as access-layer devices connecting end-user systems.

The Juniper SRX300 acts as the core device, handling both routing and security operations. It performs Layer 3 functions such as routing between networks, assigning IP addresses using DHCP, applying Network Address Translation (NAT), and enforcing security policies. To enable communication within VLAN 30, the VLAN is linked to the integrated routing interface (IRB), specifically irb.30, on the SRX300.Additionally, DHCP is configured on the SRX300 to automatically assign IP addresses to devices within VLAN 30, reducing the need for manual configuration. Security zones and firewall policies are also implemented to regulate traffic flow between internal and external networks, ensuring controlled and secure communication. Overall, this design provides a reliable, secure, and scalable network solution that is well-suited for both campus and enterprise environment.

A. VLAN Implementation

Virtual Local Area Networks (VLANs) are used to divide a single physical network into multiple logical segments, each acting as its own broadcast domain. This allows network administrators to organize devices more efficiently without the need for additional hardware. By using VLANs, devices can be grouped based on function or department rather than their physical location.In this project, VLAN 30, named vlan-girls, is implemented to isolate a specific group of users from the rest of the network. This separation helps improve security, reduce unnecessary traffic, and enhance overall network performance.

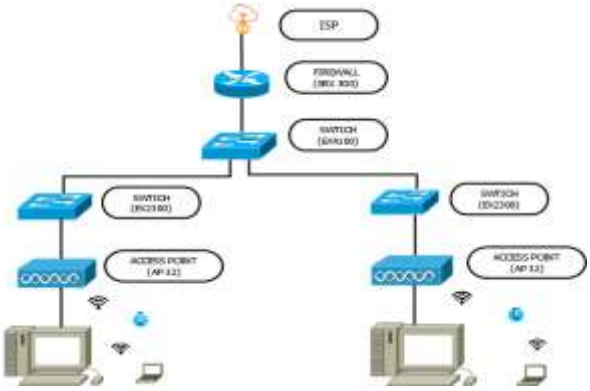

Figure 1.1 System Architecture

The VLAN is configured on Juniper EX4100 and EX2300 switches, where the ports connected to end-user devices are assigned to VLAN 30. These ports are set up as access ports, allowing devices within the same VLAN to communicate easily with each other.The switches then transmit VLAN traffic to the SRX300 firewall using trunk links, which carry data from multiple VLANs. This setup ensures that all devices in VLAN 30 stay within the same logical network while still enabling proper communication with the routing and security functions handled by the firewall.

```
mist@PIF_Juniper> show vlans vlan-girls

Routing instance        VLAN name             Tag          Interfaces
default-switch          vlan-girls            30
                                                           ge-0/0/1.0*
                                                           ge-0/0/4.0
```

Figure 1.2 VLAN Creation Verification

B. Routing Using IRB Interface in SRX300

Routing within the VLAN network is managed by the Juniper SRX300 firewall using an Integrated Routing and Bridging (IRB) interface. In this setup, the vlan-girls VLAN is linked to the logical interface irb.30 on the SRX300 device, which serves as the default gateway for all devices in VLAN 30.The IP address 10.10.30.1/24 is assigned to the irb.30 interface, allowing devices within the VLAN to communicate with other networks. Whenever a device in VLAN 30 needs to send data outside its local network, the traffic is directed to this gateway.The SRX300 receives the packet, examines it based on the routing table and configured security policies, and then forwards it to the appropriate destination. This process ensures smooth internal communication while also providing secure and controlled access to external networks.

```
mist@PIF_Juniper> show interfaces irb.30 terse
Interface               Admin Link Proto    Local                 Remote
irb.30                  up    up   inet     10.10.30.1/24
```

Figure 1.3 IRB Interface Verification

C. Security Integration

Security plays a vital role in the overall network design. In this setup, the Juniper SRX300 firewall is used to safeguard the internal network by providing strong and reliable security features that prevent unauthorized access.To achieve this, the network is divided into different security zones based on trust levels. These policies determine whether traffic should be allowed or blocked by evaluating factors such as source and destination IP addresses, as well as the type of application being used.

```
mist@PIF_Juniper> show configuration security zones security-zone untrust
screen untrust-screen;
interfaces {
    ge-0/0/0.0 {
        host-inbound-traffic {
            system-services {
                dhcp;
                tftp;
                https;
                ssh;
            }
        }
    }
}
```

Figure 1.4 Untrust Zone Interface Verification

D. IP Addressing and Network Design

A well-planned IP addressing scheme is used in this network design to make configuration and management easier. In this setup, VLAN 30 (vlan-girls) is assigned the subnet 10.10.30.0/24, which clearly defines the range of IP addresses for devices within that network segment.The Juniper SRX300 firewall acts as the gateway for this VLAN, with the IP address 10.10.30.1 configured on the irb.30 interface. This allows devices in the VLAN to communicate with other networks through the firewall.To simplify device configuration, a DHCP pool is created on the SRX300. This DHCP server automatically assigns IP addresses to connected devices within the range 10.10.30.10 to 10.10.30.50.By using dynamic IP allocation, the need for manual configuration on each device is removed, reducing errors and improving overall efficiency in network management.

```
mist@PIF_Juniper> ...s address-assignment pool vlan-girls_POOL
family inet {
    network 10.10.30.0/24;
    range DHCP_RANGE {
        low 10.10.30.10;
        high 10.10.30.50;
    }
    dhcp-attributes {
        name-server {
            192.0.0.254;
            8.8.8.8;
        }
        router {
            10.10.30.1;
        }
    }
}
```

Figure 1.5 DHCP Pool Verification

E. Simulation Environment

The network setup was implemented and tested in a simulated environment to closely mimic real-world enterprise networking conditions. This simulation includes a Juniper SRX300 firewall along with Juniper EX4100 and EX2300 switches, all configured with the required VLAN and routing settings.The environment enables thorough testing of key functionalities such as VLAN segmentation, dynamic IP address allocation through DHCP, and communication between client devices and the SRX300 gateway.To ensure everything was working as expected, various verification commands were used.

IV. SYSTEM DESIGN AND IMPLEMENTATION

The network architecture is designed using a hierarchical model that consists of three main layers: Core, Distribution, and Access. In this setup, the Juniper SRX300 serves as the central device responsible for both routing and security, enabling communication between VLANs while also enforcing network policies.To improve network organization, separate VLANs are created for different departments. This helps in isolating broadcast traffic and provides better control over how data flows within the network. Trunk ports are configured between switches using IEEE 802.1Q encapsulation, allowing multiple VLANs to be carried over a single physical link.Additionally, this design supports redundancy by providing alternative paths in case of link failure, and it helps distribute traffic efficiently across multiple connections, ensuring better performance and reliability.

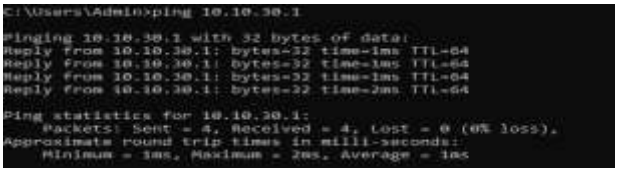

Figure 1.6 Internet Connectivity via NA

V. PORT MIRRORING IMPLEMENTATION

Port mirroring was set up on the access switch to observe network traffic without affecting normal operations. In this configuration, both incoming (ingress) and outgoing (egress) traffic from the source interface ge-0/0/6.0 was duplicated and sent to a monitoring interface, ge-0/0/8.0, for analysis.A separate monitoring system was used to capture this mirrored traffic with the help of a packet analysis tool. The captured data included protocols such as ARP, DHCP, DNS, and TCP handshake packets, which confirmed that both Layer 2 and Layer 3 communications were functioning correctly within the network.Since this method works passively, it allows detailed traffic analysis without introducing delays or impacting overall network performance.

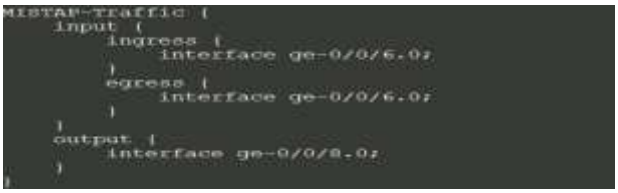

Figure 1.7 Port mirroring

VI. OSPF CONFIGURATION

The Open Shortest Path First (OSPF) protocol was configured on the SRX device to support dynamic routing within the network. This was done using the command set protocols ospf area 0.0.0.0 interface ge-0/0/0.0, which assigns the interface to Area 0, also known as the backbone area in OSPF.To verify the configuration, the command show configuration protocols ospf was used. The output confirms that the interface ge-0/0/0.0 is properly associated with Area 0.0.0.0. At the same time, interfaces such as irb.0, irb.30, and irb.40 are configured as passive interfaces.This setup ensures that OSPF routing is active where needed, while preventing unnecessary neighbor relationships on VLAN interfaces. As a result, the network avoids excess OSPF traffic and operates more efficiently.

Figure 1.8 OSPF Router ID Verification

In this project, the Raspberry Pi is used as a neighboring device to implement the Open Shortest Path First (OSPF) protocol, allowing smooth and efficient communication between different network segments. By installing FRRouting (FRR), the Raspberry Pi works like a router, where it exchanges Hello packets with other devices, establishes neighbor connections, and shares network information. Based on this information, it understands the overall network structure and selects the best path for data transmission, updating its routing table automatically. Even though it cannot match the performance of high-end routers, it serves as an affordable and flexible solution for

implementing dynamic routing in academic projects and small network setups.

Figure 1.9 OSPF Neighbor

VII. RESULTS AND DISCUSSION

The The network setup was simulated and tested using Juniper SRX300 configurations to evaluate its performance. Initially, baseline measurements were recorded using a flat network without VLANs or OSPF. After implementing VLAN segmentation and dynamic routing with OSPF, a noticeable improvement in network performance was observed.The results showed a significant reduction in broadcast traffic and overall latency. Throughput improved considerably, mainly due to better traffic distribution across aggregated links. During simulated link failure scenarios, OSPF demonstrated fast convergence, ensuring continuous communication between VLANs without major disruptions.Performance testing using iPerf indicated an average throughput increase of around 40%, along with a latency reduction of approximately 25% compared to the baseline setup.

These outcomes confirm that the proposed design effectively enhances bandwidth utilization while also improving network reliability and fault tolerance.In addition, VLAN-based segmentation strengthened data security by limiting unauthorized access between different departments. The security policies configured on the Juniper SRX300 further improved packet filtering and routing efficiency. Overall, the network design achieves a strong balance between performance.

VIII. CONCLUSION

This paper presented the design and implementation of a secure and scalable campus network using VLAN, Link Aggregation, and OSPF-based Inter-VLAN Routing on Juniper SRX300 devices. The approach successfully addressed network challenges such as congestion, limited scalability, and security vulnerabilities. Through effective segmentation, dynamic routing, and link redundancy, the system achieved significant This work presented the design and implementation of a secure and scalable campus network using VLANs, link aggregation, and OSPF-based inter-VLAN routing on Juniper SRX300 devices.

The proposed approach effectively addressed common network issues such as congestion, scalability limitations, and security risks. The results obtained through iPerf testing further confirmed the reliability and efficiency of the overall configuration.For future enhancements, the network can be extended to support advanced features such as IPv6 integration, Quality of Service (QoS) for traffic prioritization, and network monitoring using protocols like SNMP or NetFlow. These additions would further improve performance management, visibility, and scalability in more complex environments.

Figure 1.10 Iperf Verification

REFERENCE

1. K. Swapna, B. Gagan, A. Aravind and R. Bolimera.(2025), "Campus Network Design Using Cisco Packet Tracer," in Proc. 2025 10th Int. Conf. on Signal Processing and Communication (ICSC), Feb. 20, 2025,. DOI: 10.1109/ICSC64553.2025.10968176.

2. Ajiji, Y. M., Cirella, G., F. J., & Jadah, H. M. (2021),Network Performance Through Virtual Local Area Network (VLAN) Implementation & Enforcement on Network Security For Enterprise.International Journal of Advanced Networking and Applications, 12(06), 4750–4762.DOI: 10.35444/Ijana.2021.12604.
3. T. Sachinidis, A. C. Politis, C. S. Hilas.(2023),To Split or Not to Split? A Simulation Study on The Network Convergence Duration of Multi-Area OSPF International Conference on Telecommunications and Signal Processing DOI:10.1109/TSP.2023.00042(2023).
4. Jayanta Borthakur, et al.(2022) "A Comparison Study of Single-Area OSPF Network to Multiple-Area OSPF Implementation in Campus Area Network. "Proceedings of the 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, DOI: 10.1109/ICCCI50826.2021.9402693 .
5. Yuanqing Cao, Lisina Ai.(2022) "Experimental Simulation and Comparative Analysis of an Access Control List at Different Deployment Locations. "Proceedings of the 2022 International Conference on Computing, Communications, and Networking (ICCCN), 2022 DOI: 10.1109/ICCCN.2022.00042.
6. O. S. AlJamal, M. Aljamal, A. Alsarhan and A. Elrashidi,(2024) "Design and Simulation of a Network Infrastructure for a Multi-Branch Organization Using Cisco Packet Tracer," in Proc. 25th Int. Arab Conf. on Information Technology (ACIT), 2024, DOI: 10.1109/ACIT62805.2024.10876911.
7. A. Hirsi, L. Audah, A. M. Omar, and M. J. Abdiaziz,(2024) "Design and Simulation of a Secured Enterprise Network Architecture for All Departments at East Africa University (EAU), Somalia," in Proc. 2024 4th Int. Conf. on Science and Information Technology in Smart Administration (ICSINTESA), Balikpapan, Nov. 2024, pp. 552–559, DOI: 10.1109/ICSINTESA62455.2024.10747898.
8. Vivek Kumar, M., Praveena, G., Pavithra, C., & Deepalakshmi, S. (2025), Next-Generation Enterprise Networking for Enhanced Security, Reliability, and performance optimization. DOI:10.1109/RFCMO60235.2025.1235116.
9. M. Vivek Kumar, V. Soundharya, and M. Thirisankari,(2025) "Secure Healthcare Network Using VLAN, OSPF, IPsec VPN and ACL," in Proc. 2025 10th Int. Conf. on Signal Processing and Communication (ICSC), 2025, DOI: 10.1109/ICSC64553.2025.10968176.
10. V. Jadhav, T. Kajale, J. Suyad, and N. K. Mishra,(2025), "Design and Implementation of a Scalable Network Topology for Smart Megamall," 2025 International Conference on Energy, Power and Environment (ICEPE), Pune, India, 2025, DOI: 10.1109/ICEPE65965.2025.11139593.
11. K. V., S. V. Nayak, S. G. A., and S. M., (2025), "Design and Simulation of a VLAN-Based Hierarchical Enterprise Network with MSTP and Inter-VLAN Routing," in Proc. 2025 9th Int. Conf. on Computational System and Information Technology for Sustainable Solutions (CSITSS), Nov. 2025. DOI: 10.1109/CSITSS67709.2025.11294144.
12. J. Tao, R. Yuan,and Q. Xia, (2021), "Research and Implementation of a Network Based on SDN and Multi-Area OSPF Protocol," in Proc. 2021 IEEE 9th International Conference on Information, Communication and Networks (ICICN), Nov. 2021. DOI: 10.1109/ICICN52636.2021.9673836.
13. D. Davronbekov and B. Khasanov, (2022), "Use of Modern Routing Methods in Data Transmission Networks," in Proc. International Conference on Information Technology and Communications, 2022. DOI: 10.1007/978-3-031-27199-1_29.
14. M. Fahmi and M. Muladi, (2021), "IPv6 vs IPv4 Performance Simulation and Analysis using Dynamic Routing OSPF," in Proc. 2021 International Conference on Computer Engineering and Network, 2021. DOI: 10.1109/CoNMedia46929.2019.8981798.
15. A. Bhola, A. Jain and B. D. Lakshmi, (2022), "A Wide Area Network Design and Architecture using Cisco Packet Tracer," in Proc. 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), 2022. DOI: 10.1109/IC3I56241.2022.10073328.