SECURE INTER-VLAN IPv6 ROUTING: IMPLEMENTATION & EVALUATION

Zeeshan Ashraf [1] and Muhammad Yousaf [2]

[1] Department of CS & IT, University of Sargodha, Sub-Campus Mandi Bahauddin, Pakistan

[2] Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan

Corresponding Author Email: zeeshan.np@gmail.com

ABSTRACT: *Enterprise or campus networks are often large in size and are complex to manage. Network administrators need to frequently perform deliberate changes according to organizational needs. VLANs are broadly used in enterprise or campus networks to improve scalability, flexibility, ease of management and to reduce broadcasts. In inter-VLAN routing over geographically dispersed VLANs on a public network, data traffic faces many security challenges. This paper investigates ways to provide secure communication between VLANs by using multi-layer switch routing with IPv6. We used IPsec VPN to provide strong data security for geographically dispersed VLANs over a public network. This paper presents results of performance comparisons of inter-VLAN routing for IPv4 and IPv6 VLANs with transport and tunnel modes of IPsec VPNs. Results show that without IPsec, as compared to IPv6, IPv4 inter-VLAN routing performs better whereas with IPsec, IPv6 inter-VLAN routing performs better. Moreover, results show that IPsec transport mode has a slight advantage in terms of delay over the IPsec tunnel mode.*

Keywords: ACL, Inter-VLAN Routing, IPsec, IPv4, IPv6, VLAN, VPN

1. INTRODUCTION

Enterprise or campus networks span over the large geographical area in which many Ethernet switches and computers may be connected to each other as well as connected to the Internet. From the perspective of the larger network size these networks are complex to manage [1]. Today's Ethernet technology has become the industry standard for Local Area Network (LAN) due to its better speed, ease of use, and full duplex switched features. The capacity has grown gradually in Ethernet and is now available up to 1 Gbps for workstations and 10 Gbps are commonly available for servers [2]. On the other hand, Ethernet segments are also increasing in size and distance. Due to the large size of the segment and a single broadcast domain of Ethernet switched network, large volumes of broadcast traffic may cause traffic congestion.

In order to reduce the size of broadcast traffic over the network, frequent changes may be introduced, like changes in design and configuration, adding/removing hosts, revising the policies and administrative workloads; resultantly VLANs are used widely. In VLANs, the hosts are connected within their own broadcast domain and security policies. VLAN Trunking Protocol (VTP) decreases administrative overhead in a switched network [3]. Use of VLANs is ever increasing due to simplified network management, improved security, flexibility, and scalability requirements [4, 5].

Host in one VLAN cannot directly communicate with the host in another VLAN. For this purpose, inter-VLAN routing techniques are used. Inter-VLAN routing is the process of forwarding traffic from one VLAN to another VLAN by using a layer-3 device. Security is the main concern and at high risk for the geographically dispersed enterprise network segments connected over the public network [6].

Internet protocol (IPv4) was introduced in 1981. It is relatively easy for configuration and implementation. However, the exponential growth of the Internet in the whole world demands more IP address. Lack of address space and rapid enlargement of the routing table are the main problems of IPv4. To eliminate such deficiencies a new IPv6 protocol was developed by IETF in the 1990s [7]. In 1996, a special report by the American Registry for Internet Numbers (ARIN) told that all of the IPv4 class A addresses had been assigned, 62% of the class B addresses and 37% of the class C addresses had also been assigned. The IPv6 protocol introduces new features like routing speed, quality of service and security.

This study focuses on security perspective of VLANs and inter-VLAN routing with IPv6 protocol. Researchers anticipated various safety measures against some of the possible VLAN attacks like VLAN Hopping, Spanning Tree, and Private VLANs to secure layer-2 traffic within the network and the Virtual Private Network (VPN) to secure the layer-3 traffic outside the network. Few of the present security threats are the denial of service (DoS) attacks, spoofing attacks and network traffic interception [8]. We should prevent all these mentioned threats to adopt security mechanisms at the IP level or at least ease their influence. To achieve this goal, IPsec architecture protocol was introduced. Further, the paper presents the experimental performance comparisons of inter-VLAN L3 switch routing of IPv4 and IPv6 with and without IPsec VPNs in transport and tunnel modes.

The rest of this paper is organized as follows: Section II presents related work and compares this research work to existing studies. Section III contains a brief description of the VLAN. Section IV contains a brief description of the inter-VLAN routing solution that is central to this study. In section V, we describe the design for a secured inter-VLAN routing. In section VI, we present the experimental results. Finally, section VII concludes the paper.

2. RELATED WORK

Enterprise or campus networks usually are Ethernet based large and complex networks. Ethernet is known to be an insecure network. The closest related work to this paper is [2] in which the authors conducted an Ethernet LAN security survey and described the security challenges and their existing solutions. In recent years, researchers have studied VLAN usage and its importance in enterprise or campus networks using traffic data [4], [9] and presented known Ethernet related threats. In another study [5] which presents an application-oriented secure VLAN architecture design to increase the security level and scalability of the LAN in campus networks. The researchers designed an “S-VLAN” architecture which provides security to VLANs. This architectural design did not provide upper layer IP security services like data origin authentication and data integrity. This architecture did not protect against packet replay attack. In [10] the researchers show policy based VLAN design to increase the security of the LAN and to avoid the presence of hackers in the network.

Another very close related work to this paper is [11]. In this study, the researchers have presented many different types of layer-2 attacks and described techniques to mitigate these type of attacks. In addition, our focus in this paper is not only on the secure LAN but also on secure inter-VLAN. In [12], the researchers show the possibility of applying systematic top-down approaches to VLAN design and later they focus on algorithms for characterizing VLAN design changes in the operational network.

Another paper [13] showed how to design, deploy and implement inter-VLAN layer-2 and layer-3 Multiprotocol Label Switching (MPLS) VPN. MPLS layer-3 VPNs offer extremely scalable VPN architecture. The main disadvantage of MPLS VPN is that it does not provide the strong authentication and encryption. Another disadvantage of MPLS layer-3 VPN is that the customer does not have complete control of their WAN IP routing. In contrast, the focus of this paper is on traditional IP routing with IPv6 addresses scheme. We also present a performance evaluation comparison of inter-VLAN routing with security. We used IPsec VPN between different VLANs to protect layer-3 traffic by hackers. It provides the strong authentication and encryption. It also provides data confidentiality services. The advantage of IPsec is its transparency to applications. In all related works, the researchers provided different solutions about VLAN design in LAN and inter-VLAN routing in WAN based on IPv4 addressing. In contrast, this study focuses on IPv6 due to its ever increasing deployment as next generation IP routing. We used layer-3 switches in topology instead of routers for IP routing between different VLANs.

In [14], the researchers calculated the performance of different brand of switches. They measured Round Trip Time (RTT), throughput and fairness of PC-based switches and compare their performance by using different inter-VLAN routing architectures. In addition, we measure and compare the performance of inter-VLAN routing with and without security perspective by using IPv6.

3. VIRTUAL LOCAL AREA NETWORK

In a LAN, the hosts are connected to each other with switches. Users belonging to different departments are connected through the switch. The switch has one broadcast domain by default. It is not possible to divide the switch into parts physically; however we can logically divide the switch into segments. Each logical segment behaves like a separate physical switch. This method splits a single broadcast domain into multiple broadcast domains. This technique increases the efficiency as well as provide security [1, 2]. Every segment becomes a separate network for each department. As a result, flooded broadcast information can be reduced but not eliminated. These Virtual LANs can span across multiple switches with trunk links. Trunks transfer traffic for various VLANs. Trunks use special encapsulation to discriminate among different VLANs except native VLAN. There are two types of encapsulation mentioned below.

3.1 Inter-Switch Link (ISL)

ISL is a CISCO proprietary VLAN tagging method as shown in Fig. 1. In ISL, when a switch receives an Ethernet frame from a host, it encapsulates the frame before forwarding through trunk link, with another 26-byte ISL header which contains VLAN information. ISL header consists of VLAN ID, name and its priority. It is used to determine to which VLAN the Ethernet frame belongs.

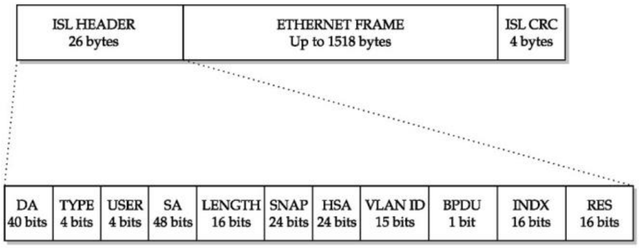

Fig. 1: Cisco ISL encapsulated Ethernet frame

3.2 IEEE 802.1Q

This tagging method is standardized by IEEE as shown in Fig. 2. In this method, a 4-bytes field called tag is inserted into a frame to identify the VLAN. If we are making a trunk link between a CISCO switch and a different brand of the switch then we have to use standard 802.1q tagging between them. This tagging method is also used in CISCO switches.

The basic function of these tagging methods is to provide the inter-switch VLAN communication. In our simulated topology, we used 802.1q tagging method.

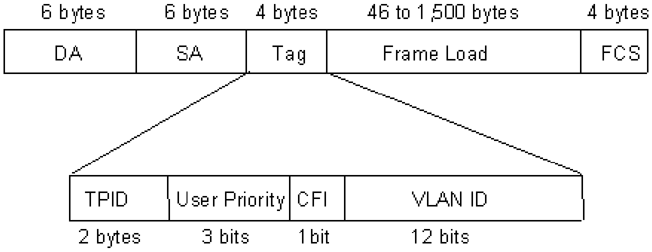

Fig. 2: IEEE 802.1q-tagged Ethernet frame

4. INTER-VLAN ROUTING

VLANs classify different users and their traffic from each other by placing them into different VLANs. Every VLAN has a single broadcast domain. A large network is divided into smaller segments also called IP sub-nets. A host can communicate with other host existing in the same sub-net but it can't communicate directly with another host which is located in a different sub-net. Now the question is how does traffic pass between two different VLANs? The answer is: it is feasible to engage a layer-3 device into sub-nets to route the traffic among multiple VLANs. There are many solutions to perform inter-VLAN routing. In modern LAN networks, three inter-VLAN routing architectures are used [14]. These are given below:

- Router-on-a-stick
- Router-on-a-stick using trunks
- Layer-3 switch routing

The router-on-a-stick architecture is the most basic method of inter-VLAN routing. In this method, a router's interface is connected physically to each VLAN. It is simple to understand because both layer-2 and layer-3 functions are physically separated.

In router-on-a-stick using trunks architecture, instead of multiple physical interfaces, a single trunk interface is connected to multiple VLAN by using tagging techniques such as ISL or 802.1q. Sub-interfaces of that physical interface are used to attach the router to each VLAN. IP addresses are assigned to sub-interfaces as a default gateway.

In layer-3 switch routing architecture, layer-2 and layer-3 functions are combined into a single device. Such devices are called multi-layer switches. In this method, Switch Virtual Interfaces (SVIs) are created to connect each VLAN. IP addresses are assigned to SVIs. Routing table and MAC table exist in the same device, so the performance must increase. This solution is more feasible as others.

In our simple simulated design as shown in Fig. 3, we used IPv6 address architecture [15] with layer-3 switch routing method because it is an advance inter-VLAN routing technique in comparison to all others. Major issues with the traditional inter-VLAN routing (Router on a stick) method are speed and cost. If megabit or gigabit routing speed is required between VLANs, then we need an expensive and high-performance router to perform inter-VLAN routing [14]. Layer-2 and layer-3 functions are performed on two different devices so it may cause the bottleneck.

In multi-layer switches, an advance layer-3 switching technology Cisco Express Forwarding (CEF) is used. It optimizes the performance and scalability in the large-scale network [16]. In a multi-layer switch, there is no physical interface for VLAN. SVIs are used to forward IP routing traffic between VLANs. The mapping between VLANs and SVIs is one-to-one. It means that only single VLAN mapped to single SVI [14]. In multi-layer switches, by default, all ports are in layer-2 working mode and IP routing is disabled. To enable any port into layer-3 working mode; just change its mode by using command "no switch port" in interface mode. Now that port becomes a routing port. Now assign IP address to that routed port. Before assigning an IPv6 address to an interface, IPv6 routing should be enabled.

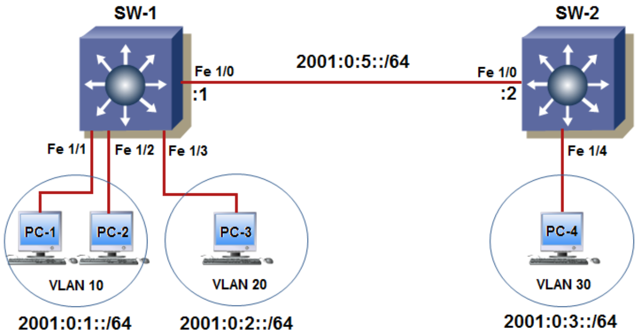

Fig. 3: L3 IPv6 Switching Routing

In our simulation topology, we used two multi-layer switches (SW-1 and SW-2) for the experiment. These switches provide layer-2 & layer-3 functionality as well as many other services like inter-VLAN routing, VLAN trunking, QoS, and security etc. Three PCs are connected to SW-1 and one PC is connected to SW-2 as shown in Fig. 3. There are two VLANs (VLAN-10 & VLAN-20) on SW-1 and one VLAN (VLAN-30) is on SW-2. PC-1 and PC-2 are placed in same VLAN-10 and PC-3 is placed in VLAN-20 while PC-4 is in VLAN-30. We created SVIs per VLAN on both switches for inter-VLAN routing. One routing port on both switches is required. Assigned IPv6 addresses are given in Table 1 to each one. IPv6 addresses of SVIs are in default gateway column. Routes must be there in the routing table of each layer-3 device before forwarding. Routing table should be complete either static or dynamic method before routing [17]. In this work, we used static entries.

TABLE I: IPv6 Address Allocated to Devices

Devices	*IPv6 Address*	*Default Gateway*
PC-1	2001:0:1::1/64	2001:0:1::100/64
PC-2	2001:0:1::2/64	2001:0:1::100/64
PC-3	2001:0:2::1/64	2001:0:2::100/64
PC-4	2001:0:3::1/64	2001:0:3::100/64
SW-1	2001:0:5::1/64	*
SW-2	2001:0:5::2/64	*

5. SECURE INTER-VLAN IPv6 ROUTING

Inter-VLAN routing is the process in which more than one VLAN can communicate with each other by using a layer-3 device. When more than one VLAN communicate to each other, then a lot of security threats arise inside and outside the network. Switches and routers provide a secure communication between VLANs. In our paper, we projected secure methods for IPv6 routing between VLANs.

5.1 Access Control

Access control is the ability to limit and control the access to the network. An unauthorized person may access your network in order to perform any wrong activity. We can protect our network from hackers by controlling access to the network.

5.1.1. Physical Security

Network devices can be placed in locked cabinet [2]. Only the authorized person is allowed to access all these network equipment in the data center.

5.1.2. Authentication

Authentication service is concerned with assuring that the communication is authentic. Whenever a person tries to access the network either in local or remote, the authentication service is a demand to identify your credential by providing information in the form of username and password. Two authentication protocols are used. One is Password Authentication Protocol (PAP) and second is Challenge Handshake Authentication Protocol (CHAP). CHAP is more secure than PAP. The authentication process can be performed by locally or remotely. Remote Authentication Dial-In User Service (RADIUS) server is usually used for remote authentication [18].

5.1.3. Firewall

Firewall is the most important security mechanism in the network that manages access between two networks. The goal is to control network traffic [19]. It filters all the traffic entering or leaving the network using the predefined set of filtering rules. It blocks unauthorized traffic according to a set of rules. Usually, it is placed between the local network and the Internet. It is available in software as well as in hardware form.

5.1.4. Access Control List

Network devices such as routers or switches can also be used as IOS based firewall with the help of Access Control List (ACL). ACLs are used to control traffic filtering. It allows trusted traffic and blocks all other traffic on a device interface based on source and destination MAC or IP addresses. The functionality of standard and extended ACL in IPv6 is the same to ACL in IPv4 [20]. IPv6 ACLs are set by using the "ipv6 access-list list-name" commands to deny or permit keywords in global configuration mode. Researchers are preferred extended ACLs to filter the traffic between different VLANs.

5.1.5. Port Security

In Ethernet LAN, cables are deployed in different positions to access the network by users. A user adds a small switch or hub as an extension and plugin multiple nodes and avail services to all of the connected devices with that hub. The network administrator can limit access of the user by controlling port in a switch. He just enters the MAC address with the port number in MAC table to control the access of multiple devices on a single port. Now if the user changes device, the port goes down in a block state.

5.2 VLAN Security

VLANs are used to divide the physical network into multiple logical networks. This approach increases the efficiency by limiting the size of the broadcast domain. But it also increases the security threats. In this section, we describe some possible attacks in VLANs and their solutions.

5.2.1. VLAN Hopping Attack

In VLAN hopping attack, the attacker avoids the layer-3 device during communication between multiple VLANs. The mugger sends a frame with MAC address of router's LAN port and IP address of a host in another VLAN by taking benefit of inaccurately configured trunk port. New switches prevent the basic VLAN hopping attacks [11]. The attackers send double encapsulated VLAN hopping attacks. To mitigate this type of attack, network administrators use a dedicated VLAN ID for all trunk ports and disable auto-trunking.

5.2.2. Spanning Tree Protocol

Spanning Tree Protocol (STP) is used to provide loop-free redundant switched network. It is a standard of IEEE 802.1D. In STP, one switch is elected as Root Bridge with the smallest bridge ID [2]. During the election process, switches broadcast messages are called Bridge Protocol Data Unit (BPDU). It takes around 30-50 seconds to the transaction with a failure or changes root bridge. The attacker sends BPDUs to force these changes. Two methods are available to mitigate this type of attack: Root guard and BPDU guard. Root guard feature protects the root if any other switch advertises with a better bridge ID. BPDU guard feature protects the integrity of switch ports that have PortFast enabled.

5.2.3. Private VLANs (PVLANs)

Generally, traffic is allowed to move unrestrictedly with a VLAN. PVLANs are used to create separate networks within a VLAN [21]. We use PVLAN when a host needs not to communicate to another host in the same VLAN but needs to communicate with the same router. The attacker sends a frame with a rogue MAC address but with the IP address of the target. VLAN ACL (VACL) is used to mitigate this type of attack. VACL is used to filter the packets between a source and destination in a VLAN if both connect to the local switch.

5.3 IPv6 Security

In enterprise networks, the island of Ethernet switches is connected to each other with IP backbone routers. IPv6 protocol is stronger than IPv4 protocol in terms of some security threats but some security threats might also affect an IPv6 network. An attack that affects IPv6 network is a sniffing attack. If one host wants to connect to another host over the network, it might be risky with insecure communication. Data confidentiality and data integrity could be compromised due to insecure communication. In sniffing attack, an attacker can easily capture confidential data that is transmitted in a plain text. To provide a secure communication, we projected VPN. VPN is a logical secure connection created over the public network (Internet). There are many flavors of security protocols available in modern technology.

Secure Socket Layer (SSL) protocol operates at the transport layer and Secure Hyper Text Transfer Protocol (HTTPS) operates at the application layer. If there is encryption at upper layer then some information at lower layer leaves unencrypted. For example, if encryption is performed at the application layer, an unauthorized intruder can easily gather information about computer system at lower layer [8]. That’s why the intention is to implement security mechanism at a lower layer (network layer). Some goals should be achieved in order to claim that security mechanisms are implemented satisfactorily. These goals are authentication, confidentiality and integrity of transmitted data. To achieve these goals, security architecture also known as IPsec is used in both IPv4 and IPv6. It provides multiple secure connections over the internetwork without using a leased line [22]. It enhanced security services for data by using different encryption techniques.

IPsec is an open standard framework developed by the IETF. It operates at network (Internet) layer. It provides data confidentiality, data integrity and data origin authentication services [23]. In addition, it provides packet counter mechanism. This mechanism protects against packet replay attack. When data is sent with IPsec, it could reach the destination without modifying and spoofing.

IPsec VPN is classified into two different modes. It could be configured as transport mode or as tunnel mode. By default, it is in transport mode. In our simulation design, IPsec tunnel with IPv6 is used between two different VLAN for secure remote communication.

5.3.1. Transport Mode

Transport mode provides End-to-End communication. It encrypts only the payload. It provides protection only to IP payload through Authentication Header (AH) or Encapsulation Security Payload (ESP) headers as shown in Fig. 4. AH provides authentication, integrity and anti-replay protection for the entire packet but it does not provide confidentiality. It means data is not encrypted and easily readable while ESP provides confidentiality as well as authentication, integrity and anti-replay [22]. Typically IP payloads are TCP or UDP segments or an ICMP message [23].

5.3.2. Tunnel Mode

Tunnel mode encrypts the IP header and payload. It provides protection to entire IP packet by treating it as an AH or ESP payload. In this mode, an entire IP packet is encapsulated with an AH or ESP header plus a new IP header attached to it as shown in Fig. 5. The IP addresses of the new IP header are the tunnel endpoints and the IP addresses of the encapsulated IP header are the source and destination addresses [24].

The main advantage of using IPsec VPN is its transparency to applications. It operates at layer-3 of OSI reference model, therefore, it has no impact on the higher layer.

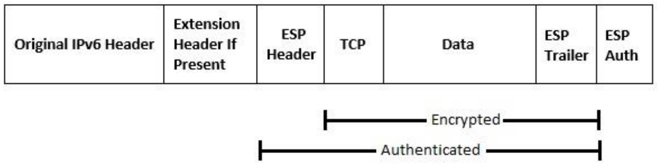

Fig. 4: Transport Mode

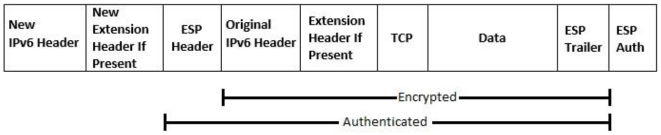

Fig. 5: Tunnel Mode

5.3.3. Intrusion Prevention System (IPS)

IPv6 is introduced with new features. It faces new security challenges. Reconnaissance attack is one of the most precarious attacks in IPv6. In this attack, the intruder gathers important data about network devices that can be misused for further attacks. To mitigate this type of attack, the network administrator uses Intrusion Prevention System (IPS). An IPS has the capability not only to detect but to prevent misuse and unauthorized access to network resources [25].

6. EXPERIMENTS AND RESULTS

We used IPsec tunnel with IPv6 addresses in our simulation design as shown in Fig. 6. The IPsec virtual tunnel interface is created by using “interface tunnel int-number” command. The

IPv6 addresses of the tunnel are “2012::1/64” on SW-1 and “2012::2/64” on SW-2. These IPv6 addresses are used as a new IPv6 header with secure encapsulated payload. Security policies should be matched on both sides.

In this section, the results obtained by round-trip delay (RTD) through our simulation experiments are displayed below. The “ping” command is used to calculate the packet round-trip delay (or round-trip time, RTT). RTD is the time required for the packet to travel from a specific source to a specific destination plus the time required for acknowledge to travel back. Researchers performed experiments for an inter-VLAN communication on same and different multi-layer switches by using IPv4 and IPv6 addressing with and without security overhead. And compare these results obtained by IPv4/IPv6 addresses. Normally IPv6 traffic is growing at the same rate as the IPv4 [26].

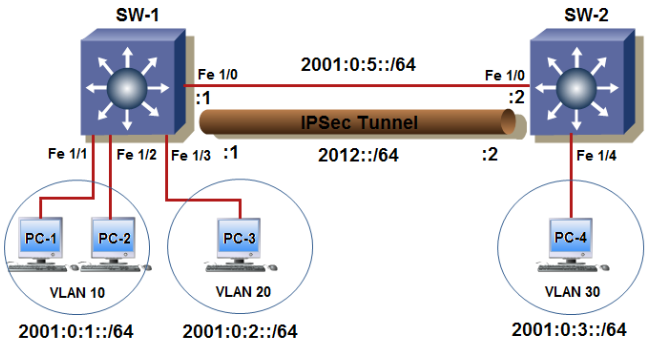

Fig. 6: L3 Secure IPv6 Switching Routing

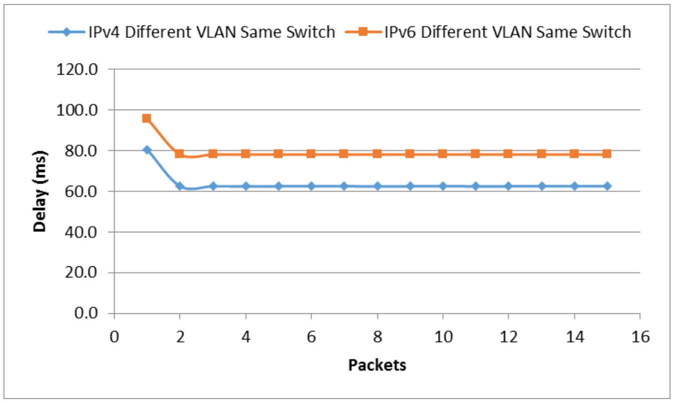

Fig.7: Packet Delay inter-VLAN routing with the Same Switch

Fig.7 shows the comparison of measured round-trip delay in an inter-VLAN routing between PC-1 and PC-3 on the same switch without security overhead for both IPv4/IPv6. In this comparison, IPv4 shows the lower RTD than IPv6 because IPv4 header size is 20 bytes while IPv6 header size is 40 bytes. First packet delay is high as compared to other packets because ICMP is a connection oriented protocol so, it takes a time to establish connection between source and destination.

In Fig.8, comparison of measured delay in an inter-VLAN routing between PC-1 and PC-4 connected with different switches without security overhead are shown. In this comparison, IPv4 shows again the lower RTD than IPv6.

Fig. 9 and 10, show the comparison of measured delay when ICMP traffic is sent from source host (PC-1) to destination host (PC-4) across the IPsec VPN with transport mode and tunnel mode for both IPv4/IPv6 addresses. IPv6 shows better performance than IPv4 with security overhead. However, the results of IPv6 with security overhead are approximately equal to the results without security overhead as shown in Fig. 8. But with IPv4 the results with security header are high as compared to results without security header as shown in Fig. 8. The packet delay for the first packet of IPv6 in these figures is much higher than with IPv4 because the size of security headers in IPv6 is also bigger than IPv4.

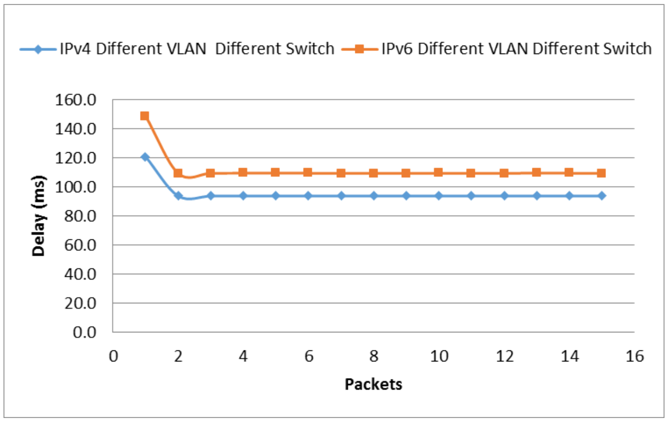

Fig. 8. Packet Delay inter-VLAN with Different Switches

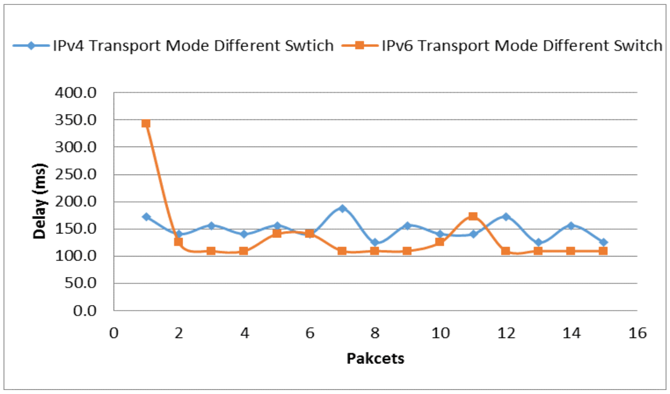

Fig. 9: Packet Delay inter-VLAN routing in transport mode

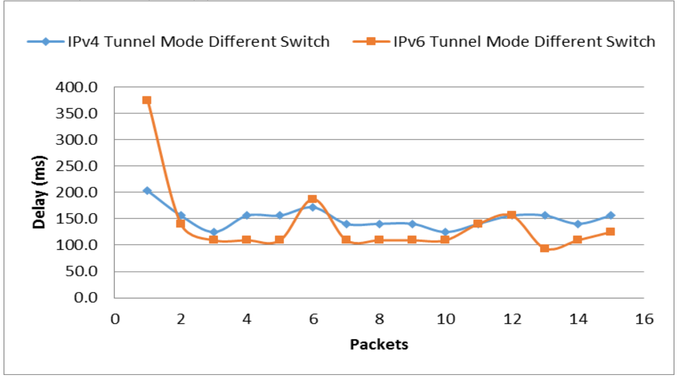

Fig. 10: Packet Delay inter-VLAN routing in tunnel mode

Finally, Fig. 11 shows the comparison of measured delay in a secure inter-VLAN IPv6 routing with transport mode and tunnel mode. There is a minor difference between two modes and it is negligible. Tunnel mode is more secure than transport mode. The results show that there is no more performance difference between IPsec tunnel mode and transport mode with IPv6.

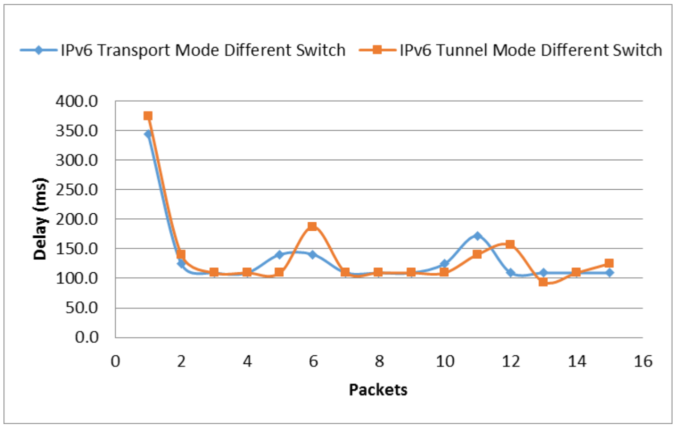

Fig. 11: Packet Delay Secure inter-VLAN IPv6 Routing

7. CONCLUSION

In this paper, we highlighted the security concerns and their solutions which arise due to inter-VLAN communication with IPv6 both locally and remotely. Solutions for secure inter-VLAN IPv6 communication are experimented using simulated network configuration. This study used IPsec VPN for secure inter-VLAN routing. Our results show that IPv6 routing is efficient with IPsec VPN and there is no extra overhead whether it is used in transport mode or tunnel mode. The results show that traditional IPv4 based inter-VLAN routing is more efficient as compared to IPv6 based inter-VLAN routing. Whereas, from the perspective of secure inter-VLAN routing with IPsec, IPv6 inter-VLAN routing performs better than the IPv4 inter-VLAN routing.

REFERENCES

[1] Y.-W. E. Sung, X. Sun, S. G. Rao, G. G. Xie, and D. A. Maltz, "Towards systematic design of enterprise networks," *Networking, IEEE/ACM Transactions on*, vol. 19, pp. 695-708, 2011.

[2] T. Kiravuo, M. Särelä, and J. Manner, "A Survey of Ethernet LAN Security," *IEEE Communications Surveys and Tutorials*, vol. 15, pp. 1477-1491, 2013.

[3] H. S. Johal, "Access List Based VLAN Map Architecture and Modified 802.1 q Frame Scheme for Addressing VTP Issues," in *Software Engineering Research, Management and Applications (SERA), 2010 Eighth ACIS International Conference on*, 2010, pp. 11-18.

[4] M. Yu, J. Rexford, X. Sun, S. Rao, and N. Feamster, "A survey of virtual lan usage in campus networks," *Communications Magazine, IEEE*, vol. 49, pp. 98-103, 2011.

[5] M. Zhu, M. Molle, and B. Brahmam, "Design and implementation of application-based secure VLAN," in *37th Annual IEEE Conference on Local Computer Networks*, 2004, pp. 407-408.

[6] R. O. Verma and S. Shriramwar, "Effective VTP Model for Enterprise VLAN Security," in *Communication Systems and Network Technologies (CSNT), 2013 International Conference on*, 2013, pp. 426-430.

[7] S. Deering and R. Hinden, "RFC 2460: internet protocol, version 6 (IPv6)," *Internet Engineering Task Force, RFC*, 1998.

[8] D. Žagar, K. Grgić, and S. Rimac-Drlje, "Security aspects in IPv6 networks–implementation and testing," *Computers & Electrical Engineering*, vol. 33, pp. 425-437, 2007.

[9] A. Mansy, M. B. Tariq, N. Feamster, and M. Ammar, "Measuring vlan-induced dependencies on a campus network," in *Proc. ACM SIGCOMM IMC*, 2009.

[10]M. Pokorný and P. Zach, "Design, implementation and security of a typical educational laboratory computer network," *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*, vol. 61, p. 119, 2013.

[11]H. Altunbasak, S. Krasser, H. L. Owen, J. Grimminger, H.-P. Huth, and J. Sokol, "Securing layer 2 in local area networks," in *Networking-ICN 2005*, ed: Springer, 2005, pp. 699-706.

[12]X. Sun, Y.-W. Sung, S. D. Krothapalli, and S. G. Rao, "A systematic approach for evolving VLAN designs," in *INFOCOM, 2010 Proceedings IEEE*, 2010, pp. 1-9

[13]T. Saad, B. Alawieh, and H. T. Mouftah, "InterVLAN VPNs over a high performance optical testbed," in *Testbeds and Research Infrastructures for the Development of Networks and Communities, 2005. Tridentcom 2005. First International Conference on*, 2005, pp. 221-229.

[14]F. Sans and E. Gamess, "Analytical Performance Evaluation of Different Switch Solutions," *Journal of Computer Networks and Communications*, vol. 2013, 2013.

[15]R. Hinden and S. Deering. *IP Version 6 Addressing Architecture*. CISCO Systems RFC 4291, February 2006.

[16]Cisco. (2014). *Cisco Express Forwarding Overview*. Available: www.cisco.com/c/en/us/td/docs/ios/12_2/switch/configuration/guide/fswtch_c/xcfcef.html

[17]Z. Ashraf, *IPv6 Routing: A practitioner approach*: Lambert Academic Publishing Germany, 2013.

[18]Y. Lu, X. Z. Chen, W. Wang, and Y. Yang, "Based on the RADIUS and AAA Authentication of the Campus Networks Security System Design and Implementation," *TELKOMNIKA Indonesian Journal of Electrical Engineering*, vol. 12, pp. 3040-3045, 2014.

[19] J. Garcia-Alfaro, F. Cuppens, N. Cuppens-Boulahia, S. Martinez, and J. Cabot, "Management of stateful firewall misconfiguration," Computers & Security, vol. 39, pp. 64-85, 2013.

[20]Cisco. (2014). *IPv6 Access Control Lists*. Available: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-3s/sec-data-acl-xe-3s-book/ip6-acls-xe.html

[21]W. Odom, J. Geier, and N. Mehta, *CCIE Routing and Switching Official Exam Certification Guide (Exam Certification Guide)*: Cisco Press, 2006.

[22] R. Kajal, D. Saini, and K. Grewal, "Virtual Private Network," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, 2012.

[23] Cisco. (2014). *Implementing IPsec in IPv6 Security*. Available: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ipv6-15-2mt-book/ip6-ipsec.html

[24] W. Stallings, *Network security essentials: applications and standards*: Pearson Education India, 2007.

[25] A. Patel, M. Taghavi, K. Bakhtiyari, and J. C. Júnior, "An intrusion detection and prevention system in cloud computing: A systematic review," Journal of Network and Computer Applications, vol. 36, pp. 25-41, 2013.

[26] E. Karpilovsky, A. Gerber, D. Pei, J. Rexford, and A. Shaikh, "Quantifying the extent of IPv6 deployment," in *Passive and Active Network Measurement*, ed: Springer, 2009, pp. 13-22.

APPENDIX: Configuration used in Experimentation

```
SW-1#vlan database
SW-1(vlan)#vlan 10 name VLAN-10
SW-1#configuration terminal
SW-1(config)#ipv6 unicast-routing
SW-1(config)#interface vlan 10
SW-1(config-if)#ipv6 address 2001:0:1::100/64
SW-1(config-if)#no shutdown
SW-1(config-if)#^Z
SW-1#show ipv6 interface brief
Vlan10                 [up/up]
   FE80::C000:12FF:FE6C:0
   2001:0:1::100
SW-1(config)#interface fastEthernet 1/0
SW-1(config-if)#no switchport
SW-1(config-if)#no shutdown
SW-1(config-if)#ipv6 address 2001:0:5::1/64
SW-1(config-if)#exit
SW-1(config)#ipv6 route 2001:0:3::/64 2001:0:5::2
SW-1#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      U - Per-user Static route
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2001:0:1::/64 [0/0]
    via ::, Vlan10
C   2001:0:2::/64 [0/0]
    via ::, Vlan20
S   2001:0:3::/64 [1/0]
    via 2001:0:5::2
C   2001:0:5::/64 [0/0]
    via ::, FastEthernet1/0
SW-1(config)#ipv6 access-list outbound
SW-1(config-ipv6-acl)#permit tcp 2001:0:3::/64 eq telnet any
SW-1(config)#crypto isakmp policy 10
SW-1(config-isakmp)#encryption aes 256
SW-1(config-isakmp)#hash sha256
SW-1(config-isakmp)#group 19
SW-1(config-isakmp)#authentication pre-share
SW-1(config-isakmp)#exit
SW-1(config)#crypto isakmp key 0 ipsecvpn address ipv6
2001:0:5::2/64
SW-1(config)#crypto isakmp peer address ipv6 2001:0:5::2
SW-1(config)#crypto ipsec transform-set ipv6_tset  esp-aes 256
esp-sha256-hmac
SW-1(config-crypto-trans)#mode tunnel
SW-1(config-crypto-trans)#exit
SW-1(config)#crypto ipsec profile myprofile
SW-1(ipsec-profile)#set transform-set ipv6_tset
SW-1(ipsec-profile)#exit
SW-1(config)#interface tunnel 1
SW-1(config)#ipv6 enable
SW-1(config-if)#ipv6 address 2012::1/64
SW-1(config-if)#tunnel source 2001:0:5::1
SW-1(config-if)#tunnel destination 2001:0:5::2
SW-1(config-if)#tunnel mode ipsec ipv6
SW-1(config-if)#tunnel protection ipsec profile myprofile
SW-1(config-if)#exit
SW-1(config)#exit
SW-1(config)#ipv6 route 2001:0:3::/64 2012::2
SW-1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state        conn-id slot status
IPv6 Crypto ISAKMP SA
 dst: 2001:0:5::2
 src: 2001:0:5::1
 state: QM_IDLE        conn-id:   1001 slot:    0 status: ACTIVE
SW-1-SW#ping 2001:0:3::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:0:3::1, timeout is 2
seconds:
!!!!!
SW-1#show crypto ipsec sa
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 2001:0:5::1
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (::/0/0/0)
   remote ident (addr/mask/prot/port): (::/0/0/0)
   current_peer 2001:0:5::2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20
    #pkts decaps: 19, #pkts decrypt: 19, #pkts verify: 19
    #pkts compressed: 0, #pkts decompressed: 0
```