Atlantis Highlights in Computer Sciences, volume 4
Proceedings of the 3rd International Conference on Integrated Intelligent Computing
Communication & Security (ICIIC 2021)

Strategic Framework for Campus Network Environment Using Virtual Switching System

Jamuna C J[1,*] Ashok Kumar R[2] Santhosh Belvadi S[3]

[1,2] *Department of Information Science and Engineering, BMS College of Engineering, Bangalore, India*
[3] *Intel Technology India Pvt. Ltd., Bangalore, India*
[*]*Corresponding author. Email: jamunacj.scn19@bmsce.ac.in*

ABSTRACT
Due to modernization of technology, networking has been an important aspect of any campus environment. Apart from having a feasible architecture it is equally important to provide continuous connectivity with high flexibility for data transfer. Hence, the proposed framework for a campus network provides high availability and reliability in the real network infrastructure. In here, Virtual Switching System (VSS) is been implemented which is an exceptional functionality that serves as an efficient redundant protocol on both the distribution and campus core space. The proposed network is also supported with a dynamic routing protocol, Enhanced Interior Gateway Routing Protocol (EIGRP), that increases the throughput and provides security for the data traffic. Finally, the test results showed that VSS provides highly available redundant campus network environment when compared to Hot Standby Routing Protocol (HSRP).

Keywords: *Campus, Ether Channel, Gateway, High Availability, Load Balancing, Loop-Free, Network, Redundancy, Routing Protocol.*

1. INTRODUCTION

Way back in a decade, very few computer devices were used by the students to connect to the Internet in an educational institution [1]. But as and when the technology improved new learning methods were adopted for teaching the growing minds, which caused an increased usage in the number of systems. As per the study [2], on an average a student would utilize around five devices to get connectivity from the Internet to serve their daily purpose. In the modern learning system students/teachers could get access to the course materials, discussion boards, assignments, etc., by connecting to the college Learning Management System (LMS) through the Internet. Along with this, implementation of latest technology enabled through Internet of Things (IOT) requires uptime in the network without causing any failure [1]. Hence, this has made an educational environment develop an infrastructure and bought the importance of networking in the field. Until now the traditional campus network used Local Area Network (LAN), Wide Area Network (WAN), and other networking topology that supported different services with scalability, availability, etc. [5]. But some of the challenges such as - lower routing convergence rate, adopting extensive routing topology, using Spanning Tree Protocol (STP) to avoid loop-free topology, utilizing single active uplink in Virtual Local Area Network (VLAN) for load sharing in a redundant network caused unnecessary packet loss [8] and an inefficient infrastructure for the long run [11, 12].

To provide better stability and utilization, enhancements are made in the campus design that involves low installation and network cost for improving the Quality of Service (QoS) in an Information Technology (IT) enabled campus network [7]. The main aim of this paper is to provide non-stop connectivity for communication without any network down-time, using a simplified infrastructure that has redundant topology with high failover. This is made possible by implementing VSS in the distribution and core layer using the L3 switch that forms a 3-Tier architecture in a campus design. To support higher convergence Enhanced Interior Gateway Routing Protocol (EIGRP) routing is used to increase the throughput and manage the routing peers dynamically [9]. Even Multi-chassis Ether Channel (MCE) is incorporated to discard the dependency of STP protocol, thereby providing dual-link for load balancing the VLANs and supporting loop-free topology. The proposed architecture is used to increase the operational efficiency with minimum control protocols and provides higher bandwidth for data traffic in the campus network.

2. LITERATURE SURVEY

Designing a better infrastructure having different networks with varied applications is very essential in a campus network. Deling Ran, (2020) [3] proposed a radio and wireless coverage application, to analyse the distance between the bridge and each equipment in an indoor and outdoor areas. Here, the range of connectivity (35-110m) for 20-30 PC's was optimal and the application was able to identify the Access Points (AP's) to establish the wireless connectivity in a campus network. Different challenges were encountered to support multiple services that transfer the data over the internet. Ojugo and Eboka, (2020) [4] implemented the technology to overcome the challenges such as - jitter, latency and packet loss observed while streaming the data, voice, audio and video through the internet in a college campus network. They increased the bandwidth and speed that enhanced productivity, mobility, resilience and flexibility.

A review made by Swati *et al.* (2020) [5] showed that not only Layer 2 (L2) but, with the minimal usage of network devices one could implement a university system using Layer 3 (L3) switches. It even showed that better routing protocols like EIGRP could be used to enhance the security and thereby reduce the network cost. But in order to improve network stability and reliability, maintaining redundancy by providing the backup path between the routers and L3 switches are the key thing. Hariadi, (2021) [6] described the manual implementation of load balancing on VLAN's using HSRP groups. In the transition process, delay of about 6.35 seconds was observed during the failover and 6.58 seconds during recovery. But the delay in data transmission could be overcome by configuring highly available network that provides accurate QoS analysis by avoiding packet loss. Mahmud Mansour, (2020) [7] made a comparison analysis among the First Hop Redundancy Protocols (FHRP) that is, HSRP, Virtual Router Redundancy Protocol (VRRP) and Gateway Load Balancing Protocol (GLBP), to check the one having better proficiency. From the study it was analysed that, all of them were capable to transfer the traffic flow during network failover with minimum packet loss. But GLBP become an efficient and reliable protocol serving the purpose of redundancy during network failure. On the similar grounds Shahriar and Fan, (2020) [8] proposed a network topology using STP for VLAN's to reduce the data collision and enhance the recovery of links upon device failure. The results showed that, when compared to VRRP and GLBP, HSRP consumed less time with high packet transfer and low end-to-end delay for both defective and normal network environments. This is also best suited for infrastructure including complex VLAN's.

Apart from this, to have better flexibility in the network, implementation of dynamic routing protocols is necessary for increasing throughput, bandwidth, scalability that reduces the CPU utilization and convergence time. Okonkwo and Emmanuel, (2020) [9] made a comparative study between EIGRP and OSPF by implementing star and mesh network topology. The experiment showed that EIGRP gave higher performance for checking the link failure and adding new links as per the network requirement. Kouroush, et.al (2020) [10] presented a practical approach to check redundancy feature in the network that provides the continuous uptime. They implemented a simple workflow that enhanced the network quality in the modern digital company by monitoring the failures.

From the survey it was found that, even with the usage of all the above stated redundant protocols some amount of packet loss was observed in the traditional protocols. This causes interference in the network when the local host establishes communication but the remote host with some amount of disruption due to switch-over from the active to the standby router. To resolve this problem, a simple campus architecture that has VSS on both distribution and core layer to maintain the high availability in the network was proposed. Along with this the dynamic routing protocol, EIGRP was used which caused no change to the underlying information. The network uses distance vector algorithm technique to provide a loop-free topology in the network environment.

3. PROPOSED ARCHITECTURAL DESIGN FOR CAMPUS NETWORK

Building a stronger networking infrastructure is necessary to provide a modular and high-availability campus network. The proposed architectural layout in Figure 1 has three primary layers in a hierarchical campus design. This network forms a three-tier architecture by including Access Layer, Distribution Layer and Core Layer, where each of them are detailed below.

3.1. Access Layer

The Main Campus network has different building blocks that includes user's (Student/Teachers) accessing Internet for enhancing their knowledge using Personal Computers (PC's) or laptops or even mobile devices. The access layer includes L2 Switches (Switch connecting each lab/floor in a building) having ports to which the host is connect for accessing the network devices. An uplink is provided by aggregating the end user to the Distribution layer by providing different port security

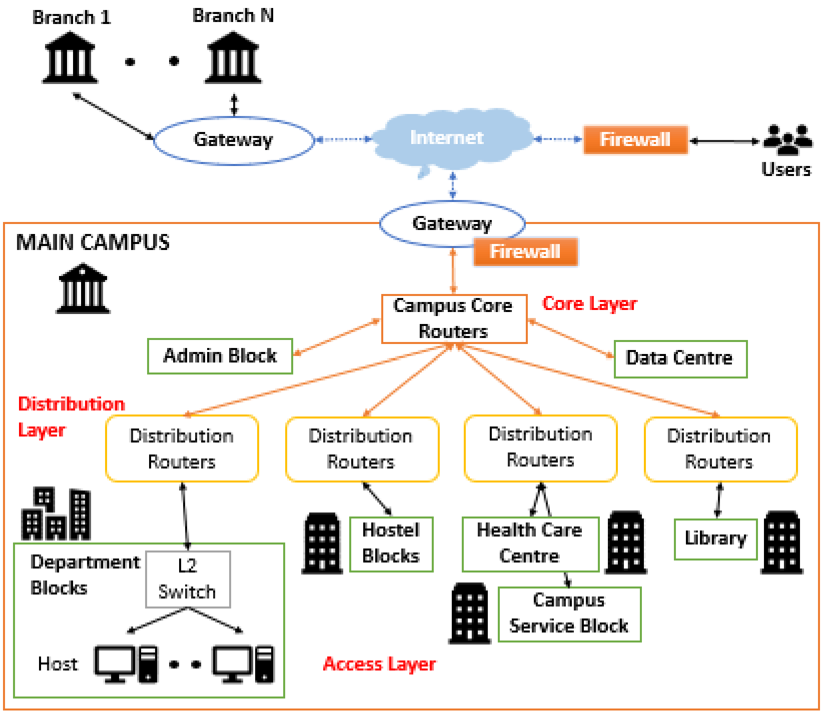

Figure 1 Proposed Architecture for Campus Network

such as – Dynamic Host Configuration Protocol (DHCP) snooping [10], Dynamic Address Resolution Protocol (DARP), IP source guard etc.

3.2. Distribution Layer

In order to provide high availability in a campus network each block is managed by the distribution routers that are redundant in nature. Multiple switches present in an access layer of each block are connected to the routers in the distribution layer through boundary control. With this, by resolving the network issues the routers form redistribution points for routing protocols that stores the routing summary. They even support policy-based connectivity, load balancing, QoS etc., in a campus network [13].

3.3. Core Layer

The backbone of any campus network is the core layer, which aggregates different distribution routers providing optimal transportation and high-performance routing. The admin and the data centre block are connected directly to the core router for managing the entire campus network. High level of redundancy is maintained for adopting quickly to the network changes as it interacts with the outer network. It has scalable protocol which supports smooth recovery by providing an alternative path during any network failure and load balances low level devices [14].

The detailed technical design of the campus network is as shown in Figure 2 and is illustrated as follow. Multiple hosts from different departments are connected to the respective L2 switches through Ethernet cable. To maintain load balancing in a campus network, VLANs are configured on the switches to which the host are connected. Different switches from a single building connects to one set of distribution routers (L3 Switches) through dual connection. Similar connection would follow for all the other blocks such as, hostel, health care, library and campus service [22-25].

To increase the bandwidth and maintain load balancing Multi-chassis EtherChannel (MEC) technique is incorporated on the dual connection. This provides a single logical gateway connection to the distribution routers with a loop-free topology having, high flexibility and availability in the campus network. The distribution routers are a combination of two physical chassis (L3 Switch) configured with VSS, forming a single logical system for the low-level switches. This is essential and is used to maintain redundancy in a campus network that supports Non-Stop Forwarding (NSF) and Stateful Switch Over (SSO). In order to auto-synchronize the configuration between two chassis, a Virtual Switch Link (VSL) having control-plane and data-plane interface is configured that provides a physical channel capacity ranging more than 20Gig. The L3 Switches provide fast path recovery for packet transfer using dynamic routing protocol such as EIGRP. They even isolate the core routers from the switches avoiding network shutdown, if network impact is encountered in the access layer.

In order to avoid the complexity of cabling present in the 2-Tier architecture, all the distribution routers contained in different blocks are connected to a single set of core routers. In here, the VSS configured provides high-speed network connectivity and maintains redundancy. The core routers are connected directly to the administrative and datacentre block having different servers such as, File Transfer Protocol (FTP), Mail, Web, Authentication and Database Servers, that provides services and manages network connectivity for the entire campus network. They even include the workstation along with the campus security system that plays a major role in managing the entire campus framework. Here, a high level of network security is maintained with the help of firewall that monitors and controls the inward and outward flow of the network traffic. Finally, the network gateway acts as an interface to establish a connection from the campus core network to the outside world (Internet). It also converts the information/data from one protocol to the other for establishing an easy communication.

Apart from this the same architecture could be implemented on multiple branches (Branch 1 to N as shown in Figure 1) to provide efficient communication. Here, the main campus connecting multiple branches communicates through the Internet via a gateway as shown in Figure 2. Even a user can communicate to the campus network from a remote location via Internet. Hence, this shows that the proposed architecture helps in managing the campus network with high availability having no impact on the network due to failures [26-28].

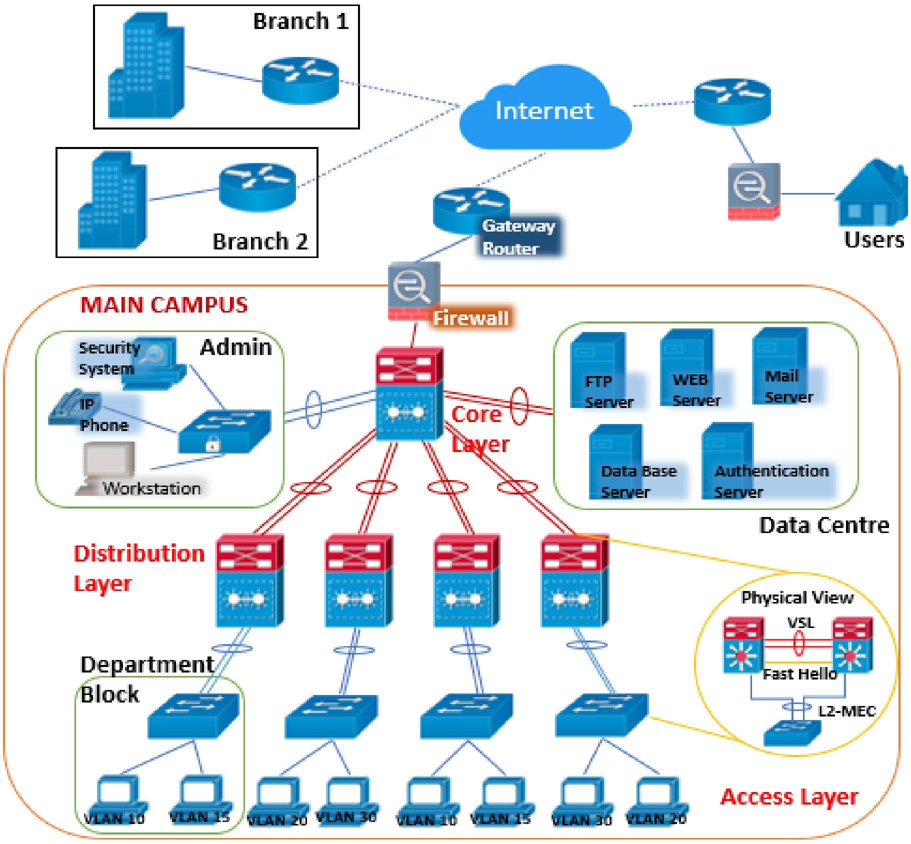

Figure 2 Technical design of a Campus Network

4. IMPLEMENTATION OF HSRP AND VSS FRAMEWORK

4.3 Traditional HSRP Framework

To achieve the best results among all the redundant protocols and to show high availability provided in a campus network, both HSRP and VSS was implemented. Here HSRP was implemented using the Cisco Packet Tracer and VSS implementation was conducted in a live experimental environment using Catalyst 6K routers in the distribution layer and L2 switches in the access layer.

Figure 3 show the experimental setup of HSRP in a campus network. PC0 (Host with IP 192.168.1.10/24) is connected to the LAN Switch (L2 Switch) through Ethernet cable. An Address Resolution Protocol (ARP) is used to broadcast the packet to all the network devices for discovering the MAC address of the remote host. This switch is connected to two distribution routers (L3 switch) through the dual link and has VLAN configured for having intercommunication among different LAN networks (different departments). Here two routers are considered i.e., active (high priority 200) and standby (low/default priority 100) that are configured with HSRP for maintaining network redundance in the distribution layer. The L3 switches of an individual block are assigned with a group ID, representing that the entities belong to the same HSRP group. In order to maintain the network redundancy same virtual gateway IP 192.168.1.1/24 (include same virtual MAC address) is created on both the L3 switches, where the host uses this to transfer the packet through the gateway to remote PC (PC1). EIGRP is used as a dynamic routing protocol for easy packet transfer between the host and the remote PC. To have a loop-free topology and to avoid unnecessary packet loss in the access layer, STP is used to select the single path that has the shortest distance for transferring the data traffic to the remote host. The distribution router is then connected to the gateway router (L3 switch) which in turn connects to the outer network (Internet) having remote host connected through outer switch (L2 Switch).[15-18]

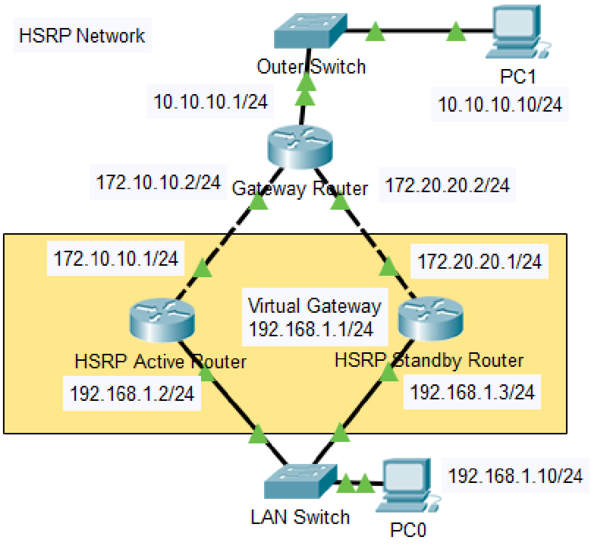

Figure 3 Implementation of HSRP framework

4.4 VSS Implementation in a Campus Framework

The implementation of VSS for a campus network and the experimental design is as shown in Figure 4. Even in here the LAN switch (having VLAN configured) is connected to the distribution routers, a combination of active and the standby routers (L3 switches). The devices are configured with VSS having a VSL for extending the CPU communication and internal chassis fabric with the standby L3 switch. This makes them logically look as a single network entity from the control and management perspective to the connecting host (PC0 with IP 192.168.1.10/24). Along with this the use of Fast Hello mechanism frequently monitors the switch status by exchanging fast hello heartbeat messages along with the switch state. A loop-free topology with link aggregation is created using MEC that handles convergence and shares the load traffic among the two switches. A single logical IP 192.168.1.1/24 is configured (include same MAC address) between the two L3 switches for easy packet transfer. The distribution router is then connected to the gateway router (L3 switch) which further links with the L2 switch and the remote host. Note that, since the implementation has a network with access switch connecting the distribution router which is configured with VSS, L2-MEC is used. But, to have the connectivity from distribution to core (where both layers configured with VSS), L3-MEC should be used.[19-21]

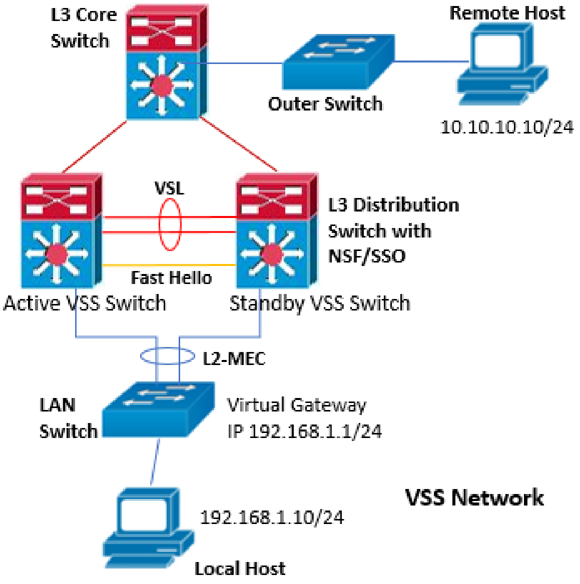

Figure 4 Implementation of VSS framework

5. RESULTS AND DISCUSSIONS

Different test cases were simulated on both HSRP and VSS design to check the connectivity loss in the network. This is analysed by observing the ping loss for each test case and the test results found during the experiment is as illustrated below.

5.1. Analysing the problems present in traditional architecture with respect to HSRP

When ping packets were sent from PC1 to PC0, the host first connected with the remote host by sending the Internet Control Message Protocol (ICMP) packets to the virtual gateway IP through the LAN switch. Before this, an ARP identified, to which device the packets have to be transferred. After this is completed, it become the responsibility of the active HSRP router to transfer the packet to the gateway router using EIGRP. Even STP protocol eliminated looping of packets within the same network. Once the packet reached the outer network, it became the responsibility of the outer switch to transfer the ICMP packet by discovering the remote host through ARP. Finally, the ping packets were sent to PC0.

Some of the possible test cases conducted during the flow of an HSRP design is as follows.

Test Case #1: When Active/Standby HSRP router fails

If the Active router fails as shown in Figure 5, there won't be any exchange of "HELLO" packets (sent every 3 seconds) between the active and the standby router which sets the hold timer in the standby router. When the waiting period exceeds beyond 10 seconds the standby router takes up the active job of packet transfer. Here, the priority of the active router is removed due to router failure and standby router's priority becomes the highest in the HSRP group [9]. During this switch over, nearly 2-3 packet loss was observed. Similarly, if the standby router fails when active is working as shown in Figure 5, it won't create any impact on the network.

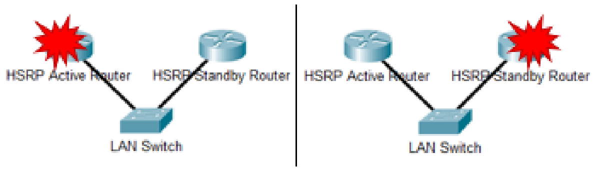

Figure 5 Representation of Active/Standby HSRP Switch failure

Test Case #2: When the link between access to distribution fails and comes-up

Due to wear and tear, if the physical link between the L2 and active HSRP router fails as shown in Figure 6, around 2-3 packet loss was observed. Due to pre-emption, the standby takes up the active role by reducing the priority of the active router. The path through which the packet needs to be transferred is redirected from the standby router, thereby establishing a best communication to the remote device. If the link comes-up as a process of manual replacement, around 5-6 packet loss was found between the communication. This is because the active router now tries to take up the responsibility of packet transfer by setting the pre-emption to low. Now that the active router attains the highest priority, all the packets again start to transfer from the active router.

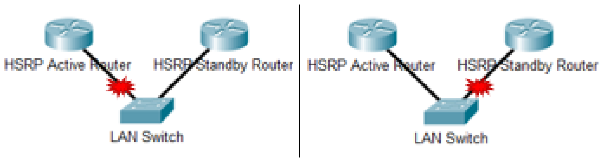

Figure 6 Representation of Single/Multiple link failure

Test Case #3: When switch attain dual active state and during forced switch over

This is a very rare scenario, where both the active and standby router attains the active state as shown in Figure 7. This would happen due to many reasons, especially when priorities aren't set properly, or due to the lag in switch over of the standby router from active to standby state (when active comes up), etc. In such situation it can cause 3-4 packet loss until the standby figures out the "HELLO" packet sent by active router is having the highest priority. Along with this, if any forced shut down was done for the active router due to maintenance, around 2-3 packet loss was observed in the communication.

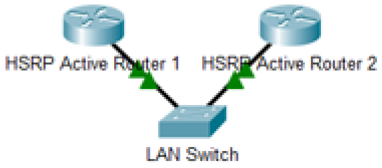

Figure 7 Representation of Dual Active state of Switches

5.2. Solutions proposed for a reliable campus network using VSS

Similar workflow steps as in HSRP would follow until the devices are identified when pinged. Here, PC0 connects to PC1 via the logical IP 192.168.1.1/24 where the data traffic is transferred to the gateway router by load balancing within the two-physical chassis (L3 switches). Because of VSL, automatic configuration sync happens between the active and hot-standby chassis. It even reduces making the manual configuration on the chassis compared to HSRP. Further, adopting MEC topology creates a sense of illusion that the host is communicating to a single device with SSO and NSF for packet transfer. This would reduce looping without any requirement to configure STP separately. Here the data packets transfer from both the routers, as the data-plane for both chassis remains active. But the control packets are sent from a single chassis, as the control-plan for the superior (active) device is set as active. This reduces the CPU utilization and minimizes the time taken for establishing communication with the remote host. Here, high availability in the network is achieved and provides efficient bandwidth for data transfer. Finally, the packets are sent to the outer network, where the outer switch transfer the ICMP packets to remote host through ARP discovery.

During the work flow of a VSS design few test cases were conducted, which are as follows.

Test Case #1: When Active/Standby VSS switch fails

Upon failure of the active switch as shown in Figure 8, the standby switch transit to the active role by performing SSO. All the modules are removed by triggering the Online Insertion and Removal (OIR) event which eliminates the interfaces from the data-path and transfers the traffic through the new switch. A minimal disruption in the traffic was observed for a sub second which causes one or no ping packet loss. This is due to the transition time taken by the standby switch to become active and also for modifying the path among the neighbour devices to the newly active device. Another scenario observed here (Figure 8) is when the standby switch fails. It is resolved by removing the modules connected to the switch by triggering OIR from the active switch. Here only the data-plane of the standby switch is affected leaving the active switch beside and is overcome by transferring all the packets to the active switch. No major impact is observed on the control-plane and hence provides high availability with no packet loss during transmission.

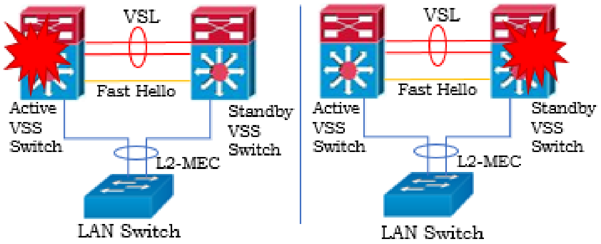

Figure 8 Representation of Active/Standby VSS Switch failure

Test Case #2: When the single/multiple links within MEC fails

When a single/multi-link in an MEC fails as shown in Figure 9, the control protocol like-PAgP, LACP, or even Link-Down event is used to recognise the link failure. Once a link failure is detected by the L2 switch, it changes the load-balancing algorithm to send the packets through the other active MEC links. If the data traffic is flowing through the failed link, there will be a single packet loss as the L2 switch takes time to redirect to the other path. In a single-link failure, no impacts are observed as the data traffic flows through other links that are active. Similarly, when multiple links in MEC fails as shown in Figure 9, the MEC link is converted into standard ether channel link. In the single homed port, whenever the traffic has to reach the L2 switch it is set through the VSL to the standby switch through which it reaches the low-level device. Even the control protocols are originated from the active switch but are sent out through the standby switch. During any link failure for detection and reprogramming the path with the system, a single packet loss is observed in the network.

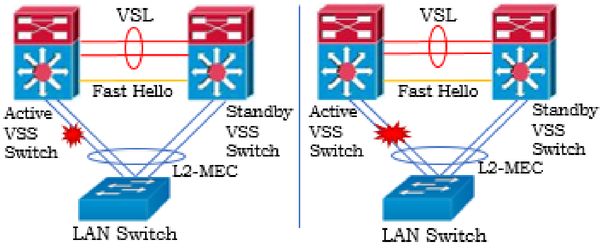

Figure 9 Representation of Single/Multiple MEC link failure

Test Case #3: When VSL single/dual link fails

The single/multi-link VSL failure is detected (Figure 10) by the active switch that sends the Link-Down event or periodic VSLP messages across the VSL link to check its status. In a single link, the data traffic that does not use VSL, tends to work properly with no effect. A single packet loss is observed if the traffic flows through failed VSL link. Whereas, when both the VSL links fail as shown in Figure 10, it creates a dual-active switch and the similar configurations on them could cause adverse effect on network traffic causing 100% ping packet loss. To overcome this situation, Fast Hello mechanism is used that frequently exchanges fast hello heartbeat messages between the two switches. When the switch fails to detect these messages, the active switch detects the dual condition and brings down the interface and management interface by entering into recovery mode. Through this the system recovers automatically and the VSL sends a Link-Up event to the active switch thereby initializing both active and standby router providing high availability with no packet loss.

Table 1 Test Results showing ping loss for both HSRP and VSS

PC0 to PC1 ping testing	**Ping Loss in HSRP**	**Ping Loss in VSS**
Active Switch fails	2 or 3 ping losses	0 or 1 ping loss
Standby Switch fails	0 ping loss	0 ping loss
Access switch link failed	2 or 3 ping losses	0 or 1 ping loss
Access switch link comes up	5 or 6 ping losses	0 or 1 ping loss
Single VSL link failed	NA	0 ping loss
Both VSL link failed	NA	1 ping loss
VSL and Fast Hello link fails	NA	100% ping loss
Reverting from Dual Active state	3 or 4 ping losses	NA
Forced switch-over of the Active Switch	2 or 3 ping losses	1 ping loss

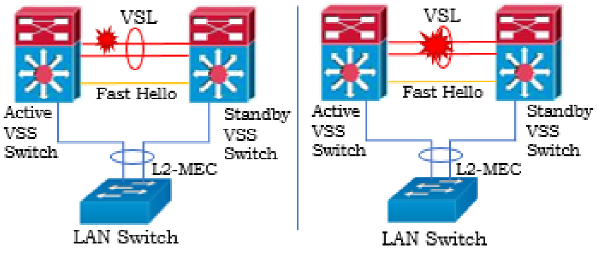

Figure 10 Representation of Single/Dual VSL link failure

The comparison table shows the test results of packet loss for different scenarios and are populated as shown in Table 1 for both HSRP and VSS network design in a campus network.

6. CONCLUSIONS

High availability campus network is designed using VSS that provides NSF and SSO for loss-free packet transfer. Single logical switch is created for different blocks in a campus network that reduces the complexity and simplifies the network infrastructure hiding the physical entity in both the distribution and core layer. The system is flexible because it reduces manual intervention by having easy configuration steps that takes less time for installation. Due to the incorporation of MEC technique between the access and the distribution layer the throughput and bandwidth of the system is increased. A dynamic routing protocol, EIGRP is incorporated for an autonomous system (campus network) to automatically route the packets by authenticating and for taking suitable decisions that enhances the network security. Finally, when compare with the test results of HSRP (or any traditional technology), the proposed system incorporated with VSS provides maximum efficiency in a campus network with high QoS even for different applications. Due to software failures or under unavoidable circumstance one could observe the failure of the entire network. This is a common scenario in most of the framework, but could be overcome by including necessary application toolset that brings the network back easily. The proposed architecture could be implemented on largest campus environment, where network criticality is at its high importance. In future the architecture could be adopted for the banking sector, military application, or even for corporate organizations by incorporating suitable software technologies in them.

REFERENCES

[1] Jess Scherman, How to Mitigate Network Outages on Your College Campus, in: Collegies Education, 2019.

[2] The Refuel Agency's 2018 College Explorer Market Research Study, in: College Explorer Series, 2018.

[3] Deling Ran, Design and Planning of University Campus Network, in: Journal of Physics: Conference Series, 022109, *vol.* 1533, 2020. DOI: https://doi.org/10.1088/1742-6596/1533/2/022109

[4] A.A. Ojugo, A.O. Eboka, Mitigating Technical Challenges via Redesigning Campus Network for Greater Efficiency, Scalability and Robustness: A Logical View, in: International Journal of Modern Education and Computer Science (IJMECS), vol. 12, No. 6, 2020, pp. 29-45. DOI: https://doi.org/10.5815/ijmecs.2020.06.03

[5] Swati Pawar, D. Vivek, Ugale, Ankita Nirmal, Pallavi Badgujar, Swapnali Borade, A Review On: Network Design for College Campus, in: International Journal of Research and Analytical Reviews, vol. 7, 2020, issue 1, pp. 284-288.

[6] F. Hariadi, Manual Load Balancing on Redundancy Link Using Multi-Group Hot Standby Router Protocol, in: Journal of Informatics and Information Systems Engineering, vol. 7, 2021, No. 1. DOI: https://doi.org/10.28932/jutisi.v7i1.3403

[7] Mahmud Mansour, Performance Evaluation of First Hop Redundancy Protocols, in: Procedia Computer Science, vol. 177, 2020, pp. 330-337. DOI: https://doi.org/10.1016/j.procs.2020.10.044

[8] F. Shahriar and J. Fan, Performance Analysis of FHRP in a VLAN Network with STP, in: 2020 IEEE 3rd International Conference on Electronics Technology (ICET), 2020, pp. 814-818. DOI: https://doi.org/10.1109/ICET49382.2020.9119624

[9] Okonkwo, IJ and Emmanuel, ID 2020, 'Comparative study of EIGRP and OSPF protocols based on network convergence, in: International Journal of Advanced Computer Science and Applications, vol. 11, No. 6, pp. 39-45. DOI: https://doi.org/10.14569/IJACSA.2020.0110605

[10] R. Phillips, K. Jenab, & S.Moslehpour, A practical approach to monitoring network redundancy, in: International Journal of Data and Network Science, vol. 4, No. 2, 2020, pp. 255-262. DOI: http://doi.org/10.5267/j.ijdns.2019.9.004

[11] Maged Sheghdara, Jameleddine Hassine, Automatic retrieval and analysis of high availability scenarios from system execution traces: A case study on hot standby router protocol, in: Journal of Systems and Software, vol.161, 2020. DOI: https://doi.org/10.1016/j.jss.2019.110490

[12] M. Aldaoud, D. Al-Abri, A. Al Maashri et al., DHCP attacking tools: an analysis, in: Journal Computer Virology and Hacking Techniques, vol. 17, 2021, pp. 119–129. DOI: https://doi.org/10.1007/s11416-020-00374-8

[13] J. Xue, Y. Wu, J. Tao and Y. Zhang, Research on Campus Network Based on QoS Technology, in: 2020 IEEE 3rd International Conference on

Information Communication and Signal Processing (ICICSP), 2020, pp. 418-423. DOI: https://doi.org/10.1109/ICICSP50920.2020.9232073

[14] Ali Kharrazi, Yadong Yu, Arun Jacob, Nemi Vora, Brian D. Fath, Redundancy, Diversity, and Modularity in Network Resilience: Applications for International Trade and Implications for Public Policy, in: Current Research in Environmental Sustainability, vol. 2, 2020. DOI: https://doi.org/10.1016/j.crsust.2020.06.001

[15] Arun, M., E. Baraneetharan, A. Kanchana, and S. Prabu. "Detection and monitoring of the asymptotic COVID-19 patients using IoT devices and sensors." International Journal of Pervasive Computing and Communications (2020

[16] Kumar, M. Keerthi, B. D. Parameshachari, S. Prabu, and Silvia liberata Ullo. "Comparative Analysis to Identify Efficient Technique for Interfacing BCI System." In IOP Conference Series: Materials Science and Engineering, vol. 925, no. 1, p. 012062. IOP Publishing, 2020.

[17] Nguyen, Tu N., Bing-Hong Liu, Nam P. Nguyen, and Jung-Te Chou. "Cyber security of smart grid: attacks and defenses." In ICC 2020-2020 IEEE International Conference on Communications (ICC), pp. 1-6. IEEE, 2020.

[18] Naeem, Muhammad Ali, Tu N. Nguyen, Rashid Ali, Korhan Cengiz, Yahui Meng, and Tahir Khurshaid. "Hybrid Cache Management in IoT-based Named Data Networking." IEEE Internet of Things Journal (2021).

[19] Do, Dinh-Thuan, Tu Anh Le, Tu N. Nguyen, Xingwang Li, and Khaled M. Rabie. "Joint impacts of imperfect CSI and imperfect SIC in cognitive radio-assisted NOMA-V2X communications." IEEE Access 8 (2020): 128629-128645.

[20] Subramani, Prabu, K. Srinivas, R. Sujatha, and B. D. Parameshachari. "Prediction of muscular paralysis disease based on hybrid feature extraction with machine learning technique for COVID-19 and post-COVID-19 patients." Personal and Ubiquitous Computing (2021): 1-14.

[21] Rajendrakumar, Shiny, and V. K. Parvati. "Automation of irrigation system through embedded computing technology." In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, pp. 289-293. 2019.

[22] Puttamadappa, C., and B. D. Parameshachari. "Demand side management of small scale loads in a smart grid using glow-worm swarm optimization technique." Microprocessors and Microsystems 71 (2019): 102886.

[23] K. Yu, Z. Guo, Y. Shen, W. Wang, J. C. Lin, T. Sato, “Secure Artificial Intelligence of Things for Implicit Group Recommendations”, IEEE Internet of Things Journal, 2021, doi: 10.1109/JIOT.2021.3079574.

[24] H. Li, K. Yu, B. Liu, C. Feng, Z. Qin and G. Srivastava, "An Efficient Ciphertext-Policy Weighted Attribute-Based Encryption for the Internet of Health Things," IEEE Journal of Biomedical and Health Informatics, 2021, doi: 10.1109/JBHI.2021.3075995.

[25] L. Zhen, A. K. Bashir, K. Yu, Y. D. Al-Otaibi, C. H. Foh, and P. Xiao, “Energy-Efficient Random Access for LEO Satellite-Assisted 6G Internet of Remote Things”, IEEE Internet of Things Journal, doi: 10.1109/JIOT.2020.3030856.

[26] L. Tan, K. Yu, A. K. Bashir, X. Cheng, F. Ming, L. Zhao, X. Zhou, “Towards Real-time and Efficient Cardiovascular Monitoring for COVID-19 Patients by 5G-Enabled Wearable Medical Devices: A Deep Learning Approach”, Neural Computing and Applications, 2021, https://doi.org/10.1007/s00521-021-06219-9

[27] Z. Guo, A. K. Bashir, K. Yu, J. C. Lin, Y. Shen, “Graph Embedding-based Intelligent Industrial Decision for Complex Sewage Treatment Processes”, International Journal of Intelligent Systems，2021, doi: 10.1002/int.22540.

[28] K. Yu, L. Tan, M. Aloqaily, H. Yang, and Y. Jararweh, “Blockchain-Enhanced Data Sharing with Traceable and Direct Revocation in IIoT”, IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2021.3049141.