Volume: 15 Issue: 06 Pages: 6211 – 6217 (2024) ISSN: 0975-0290

Campus Network Design for Information Technology Faculty

Abdulhadi Hasan Alarbad
Department of Computer Networks, Misurata University, Libya
Email: m0918l038@it.misuratau.edu.1y
Anas Mohammed Alsharif
Department of Computer Networks, Misurata University, Libya
Email: m0918l0l0@it.misuratau.edu.ly
Salem Omar Sati
Department of Computer Networks, Misurata University, Libya
Email: salem.sati@it.misuratau.edu.ly

----------ABSTRACT----------

The impact of network services failures can have a significant effect on the functionality of education. The construction of a campus network has played a crucial role in advancing educational systems and creating optimal learning environments. Therefore, it is essential to ensure a high level of network availability to guarantee timely access to resources. This research paper introduces a campus network design which incorporates a hierarchical structure with dual single-homed internet access to enhance reliability. Emphasizing the importance of reliability and security, the paper applies the CISCO methodology to address the specific challenges of campus network design using the GNS3 simulator. The resulting topology ensures robust security, scalability, and high availability through the implementation of redundancy mechanisms and the dynamic operation of DHCP, HSRP, and STP protocols.

Keywords - **Campus Network, Campus Design Models, Campus Redundancy, Campus Three Layers, GNS3 Simulator, Campus Performance.**

Date of Submission: April 11, 2024 Date of Acceptance: April 28, 2024

I. INTRODUCTION

The well-designed campus network [1], [2] provides high-speed and reliable connectivity throughout the university. Where students can access online resources, research mate1ials, and e-learning platforms [3] effortlessly. it offers improved communication: which facilitate efficient communication between students, faculty, and administrative staff. Instant messaging, email services, and VoIP (Voice over Internet Protocol) [4] enable real-time communication, allowing students to connect with teachers, peers, and support services easily. Campus network also provides access to online learning resources such as digital libra1ies, Cloud computing [16], research databases, and e-books. These resources enhancing the learning experience and promoting self-paced learning. Campus networks incorporate security measures such as firewalls, intrusion detection systems, and access control mechanisms. This ensures the protection of sensitive data and personal information, creating a secure digital environment for students and faculty. The campus networks simplifies administrative processes by enabling online registration, automated grading systems, and digital document management. A robust campus network infrastructure supports the Internet of Things (IoT) devices [5], smart classrooms, and virtual reality simulations. This prepares students for the demands of the digital era. Therefore, designing a campus network is a complex task that requires careful planning and consideration of various factors of the paper should explain the nature of the problem, previous work, purpose, and the contribution of the paper. The contents of each section may be provided to understand easily about the paper.

II. RELATED WORK

This section highlights various papers that address different aspects of campus network design and security. In the paper referenced as [7], proposed techniques are discussed to overcome challenges and enhance the security of the campus network. The design emphasizes reliable connectivity, support for advanced applications, and efficient communication and collaboration among students. Another research paper referenced as [8] proposes a security system structure with longitudinal anti-attack capability and diversified defense mechanisms. The behavior of traffic and the implementation of Quality of Service (QoS) policies in campus networks are explored in the paper cited as [9]. The study focuses on understanding and managing the traffic patterns in these networks. The analysis of network management issues and characteristics specific to campus networks is presented in the paper cited as [10]. The paper provides insights into the current state of network management in campus environments. In the paper referenced as [1], a dual-stack IPv4/IPv6 network scheme based on the OSPF protocol is designed and proposed. The goal is to analyze and investigate existing IPv6 transition schemes for campus networks. Addressing the specific scenario of schools with high real-time access control requirements, the paper cited as [11] proposes a novel cloud-edge collaborative face recognition access control method. This method aims to enhance access control systems in such environments. Finally, two papers, referenced as [12] and [13], suggest solutions for campus networks and propose efficient designs for such interconnected networks.

Volume: 15 Issue: 06 Pages: 6211 – 6217 (2024) ISSN: 0975-0290

III. CAMPUS NETWORK DESIGN METHODOLOGY

The Cisco PPDIOO methodology consist of (Prepare, Plan, Design, Implement, Operate, and Optimize) methodology. The PPDIOO methodology provides a framework for ensuring a well-designed and efficient network infrastructure. This is an explanation of each phase of PPDIOO in the context of campus network design:

A. Prepare Phase

During the prepare phase of campus network design there are several sub-stages or activities that can be considered. These activities related to identifying the specific needs of different departments or student groups, such as data transfer rates, application requirements, security considerations, and scalability. Furthermore, this stage has developing a campus design plan which creates a detailed outlines the timeline, milestones, resource allocation, and responsibilities for each phase of the next design and implementation process.

B. Plan Phase

Planning phase has several sub-stages or activities that can be considered. One of them is network requirements gathering This activity involves understanding the expected network capacity, desired performance, security requirements, scalability. It also considers network topology design. It also related to IP addressing and subnetting, quality of service (QoS). Furthermore, it related to the redundancy and high availability. Finally it deals with the network management design which means the develop of the network monitoring, configuration, and troubleshooting of the campus network.

C. Design Phase

The activity of the design phase includes the logical network design. This activity focusing on the network architecture and addressing scheme. It also deals with the network device selection based on the requirements and objectives of the campus network. It also related to the security design using a comprehensive security framework for the campus net- work. This framework considers firewall rules, intrusion detection/prevention systems, and secure remote access mechanisms. Where Quality of Service (QoS) design related to determining bandwidth allocation, traffic shaping, and prioritization rules based on application requirements and campus performance objectives. Moreover, This stage considers protocols such as Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) for loop prevention and link redundancy.

D. Implementation Phase

Implementation phase has several sub-stages or activities that can be considered. These include physical infrastructure setup. This stage includes mounting network devices, running cables, connecting and labeling ports, and ensuring proper power and cooling arrangements. It also related to the configuration and initialization. This involves setting up IP addresses, VLANs, routing protocols, QoS policies, security settings It also deploy network services such as DHCP, DNS, NTP and configuring firewalls, access control lists (ACLs), VPNs (Virtual Private Networks).

E. Operation Phase

Operation phase of campus network design includes network monitoring and management. The activity such as implement network monitoring tools such as SNMP (Simple Network Management Protocol) to continuously monitor the performance, availability, and security of the campus network. capacity planning by monitor network usage and plan for future capacity needs. Analyze network traffic trends, Performance reporting to track the campus's performance, availability, and security metrics.

F. Optimization Phase

Optimization phase of campus network design includes performance assessment of the current campus performance to detect required improvement. Evaluate factors such as network latency, throughput, packet loss, and application performance. It includes traffic analysis and capacity planning based on the traffic analysis and future growth. Where routing protocol optimization by evaluates the efficiency and stability of routing protocols used in the campus network. These routing performance metrics such as convergence time, load balancing, and route summarization. Furthermore, network device firmware and software updates impact on campus performance. There- fore, scheduled software and platfo1ms update should be considered.

IV. DESIGN FUNDAMENTALS OF CAMPUS NETWORK

The campus is the networking infrastructure that provides access to services and resources for students. The campus network uses a hierarchical design model to break the design up into modular groups or layers. Breaking the design up into layers allows each layer to implement specific functions, which simplifies the design and management of the network. Modularity in network design allows to create elements that can be replicated throughout the network. Replication provides an easy way to scale the network. Hierarchical design helps constrain operational changes to a subset of the network, which makes it easy to manage as well as improve resiliency. The hierarchical design includes the following three layers:

A. Access layer:

The access layer serves as the point of connection for end devices within the campus network. One important function of the access layer is to provide high-bandwidth connectivity for devices. This is particularly important in a campus environment where students engage in tasks that require substantial network resources. Therefore, the access layer must be capable of supporting high-bandwidth traffic efficiently. Furthermore, the access layer should be designed to accommodate multiple logical networks. This capability offers several advantages, including improved performance, simplified network management, and enhanced security. By segmenting the network into logical networks at the access layer, administrators can optimize performance, streamline network administration, and enforce security policies effectively. When designing the access layer, several features should be taken into consideration to ensure its effectiveness. These features may include:

1) Resiliency and security services
2) Advanced technology capabilities

Volume: 15 Issue: 06 Pages: 6211 – 6217 (2024) ISSN: 0975-0290

3) Multigigabit Ethernet (mGig) and Power over Ethernet
4) Oversubscription ratios
5) Increasing uplink speeds
6) Uplink queuing management

B. Distribution layer

The distribution layer facilitates end-to-end connectivity within the network, whether between different access layer devices or from an access layer device to the WAN or internet. In a three-tier campus network design, it is recommended to have a dedicated distribution layer that is separate from the access layer devices. This separation ensures that network services are efficiently provided without being shared with the connectivity functions of the access layer. Additionally, when connecting multiple distribution layers together, it is advisable to consider using a core layer for distribution connectivity. There are several factors that drive the design of a campus network with multiple distribution layer modules. These fac- tors may include:
1) The number of ports and the bandwidth capacity of the distribution layer platform di1·ectly impact network performance and throughput.
2) Network resilience is a crucial consideration. When all campus and network-based services rely on a single platform.
3) Change control and frequency also play a role in re-silience. When all campus network services are consolidated on a single distribution layer.

C. Core layer

The large campus environment requires multiple distribution layer switches. One reason for this is that when access layer switches are located in multiple geographically dispersed buildings. As campus grows beyond three distribution layers in a single location, University should use a core layer to optimize the design. Another reason to use multiple distribution layer switches is when the number of access layer switches connecting to a single distribution layer exceeds the performance goals of the campus network designer. In environments where multiple distribution layer switches exist in close proximity and where fiber optics provide the ability for high bandwidth inter connectivity. The core layer of the campus is a c1itical part of the scalable campus and, by design, is one of the simplest. The distribution layer provides the fault and control domains, and the core should guarantee connectivity between them. Connectivity to and from the core is Layer three only, which drives increased resiliency and stability.

V. DESIGN OPTIONS OF CAMPUS WIRED NETWORK

When the network has a single switch in a campus up to a full three-tier campus network, the reliability of the network is increasingly important, because network downtime likely affects a greater student population with a larger work-place significance. Campus network design includes additional resiliency options, such as redundant links, switches. The p1imary function of the distribution layer is to aggregate access layer switches in a campus. The distribution layer provides a boundary between the Layer two domain of the access layer and the Layer three domain that provides a path to the internet. This boundary provides two key functions for the campus network. On the Layer two side, the distribution layer creates a boundary for spanning tree protocol (STP), limiting propagation of Layer two faults. On the Layer three side, the distribution layer provides a logical point to summarize IP routing information when it enters the network. The summarization reduces IP route tables for easier troubleshooting and reduces protocol overhead for faster recovery from failures. The following is a summary of some of design and operational concerns with the traditional multilayer campus design, driving alternative approaches such as Spanning-tree protocol looping prevention and FHRP configuration.

TABLE I
GNS3 EMULATOR SETTINGS

No	SeLLings	Value(s)
	Simulator and Tools	GNS3 (2.2.42) VMware workstation player (17.0.2) Cisco 10S Software, IOSv Software Version 15.6(2)T
2	Campus Model Type	3 Tier Campus LAN Topology
3	VLANs	I 0,20.30 and 40
4	Protocols	HSRP, LACP, RPVST PAT and DHCP
5	Security	Switchport Port-Security
6	Routing Protocols	iBGP,eBGP and OSPF
7	ISP Connection Type	Dual Single Homed
8	IP	Version 4
9	Layers	BackkBonc = Core Aggregation = Distribution Access
lO	Autonomous System Number	GPTC ASN = 21003 IT Faculty ASN = 3277:,2

VI. DESIGN FUNDAMENTALS OF CAMPUS SECURITY

The campus network design should consider the security. These are a few fundamental tools to help with basic network security, These tools such as DHCP Snooping. DHCP Snoop-ing is a tool used to combat rogue DHCP servers. The other tool is Dynamic ARP Inspection. This ARP attack related to man-in-the middle attacks. Dynamic ARP Inspection (DAI) is a tool that can be used to mitigate this attack. DAI uses the DHCP snooping database for IP to MAC address bindings. DAI then intercepts all ARP packets and drops any packet where the IP to MAC address binding is not valid. Regarding STP there is protection tool called BPDU Guard. BPDU guard is a protocol designed to solve STP problems.

VII. SIMULATION AND RESULTS

The campus network design for the information technology faculty was developed following the guidelines provided by CISCO in their design guide [14] and utilizing the PPDIOO methodology. The design employed a three-tier model, as depicted in Fig 1, and listed in table 1, which primitizes redundancy, security, and scalability to enhance internet and

connectivity performance.

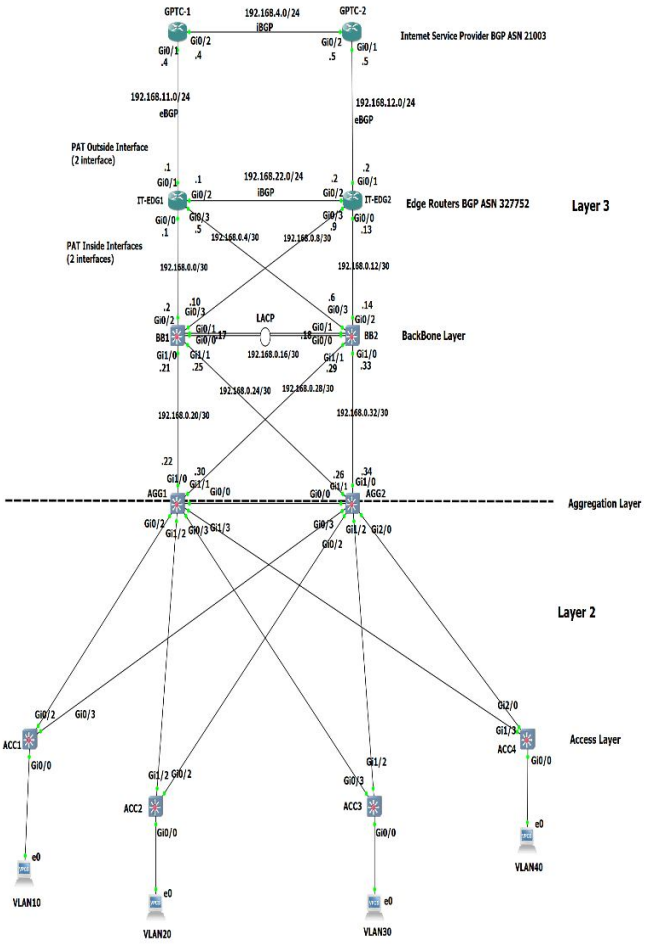

Fig. l. Designed Campus Network Topology

```
GPTC-1#sh ip bgp
BGP table version is 8, local router ID is 192.168.11.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 r>i 0.0.0.0          192.168.4.5              0    100      0 i
 r                    0.0.0.0                                0 i
 * i 192.168.4.0      192.168.4.5              0    100      0 i
 *>                   0.0.0.0                  0         32768 i
 *   192.168.11.0     192.168.11.1             0             0 327752 i
 *>                   0.0.0.0                  0         32768 i
 *>i 192.168.12.0     192.168.4.5              0    100      0 i
 * i 192.168.22.0     192.168.12.2             0    100      0 327752 i
 *>                   192.168.11.1             0             0 327752 i
GPTC-1#sh ip bgp summary
BGP router identifier 192.168.11.4, local AS number 21003
BGP table version is 8, main routing table version 8
5 network entries using 720 bytes of memory
9 path entries using 720 bytes of memory
5/3 BGP path/bestpath attribute entries using 760 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2224 total bytes of memory
BGP activity 5/0 prefixes, 10/1 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.4.5     4        21003     115     114        8    0    0 01:39:12        4
192.168.11.1    4       327752     105     112        8    0    0 01:35:22        2
GPTC-1#
```

Fig. 2. GPTC ISP Configuration

```
IT-EDG1#sh ip bgp
BGP table version is 6, local router ID is 192.168.22.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 * i 0.0.0.0          192.168.22.2             0     50      0 21003 i
 *>                   192.168.11.4                  100      0 21003 i
 *>  192.168.4.0      192.168.11.4             0    100      0 21003 i
 *   192.168.11.0     192.168.11.4             0    100      0 21003 i
 *>                   0.0.0.0                  0         32768 i
 *>  192.168.12.0     192.168.11.4                  100      0 21003 i
 *>  192.168.22.0     0.0.0.0                  0         32768 i
IT-EDG1#sh ip bgp summary
BGP router identifier 192.168.22.1, local AS number 327752
BGP table version is 6, main routing table version 6
5 network entries using 720 bytes of memory
7 path entries using 560 bytes of memory
6/3 BGP path/bestpath attribute entries using 912 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2216 total bytes of memory
BGP activity 5/0 prefixes, 8/1 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.11.4    4        21003     114     107        6    0    0 01:34:39        4
192.168.22.2    4       327752      27      28        6    0    0 00:19:26        1
IT-EDG1#
IT-EDG1#
```

Fig.3 IT Faculty Edge Router Configuration

To eliminate loops at both the second and third layers, three-layer switches and routers were configured. IP version 4 was utilized for IP addressing within the design. For internet connectivity, the model incorporated dual single-homed setups to ensure backup availability. Scalability was addressed through the use of core or backbone switches that can be extended using modular or stack-wise switches. This topology's interconnected switches were designed to mitigate the risks of point failures. Finally, the proposed campus network design was simulated using Graphic Network Simulator version three (GNS3) [15]. The laboratory environment for the simulated campus topology was configured according to the settings outlined in Table I.

A- Internet Connectivity at ISP

In the proposed model, this particular segment is connected to the internet through a dual single-homed setup, ensuring high availability of internet access. The chosen Internet Service Provider (ISP) for providing internet services is the General Posts and Telecommunications Company (GPTS) with an ASN (Autonomous System Number) of 21003, as depicted in Fig 2. The ISP's IP address is assigned as 192.168.4.0/24. The ISP is connected as dual single-homed through two networks, namely 192.168.11.0/24 and 192.168.12.0/24. The routing protocol used for this connection is exterior (Border Gateway Protocol) (eBGP), which is a path vector routing protocol. eBGP is responsible for establishing the connection between the ISP and the IT faculty's ASN, which is 327752. Interior BGP (iBGP) is utilized to allow communication between the two BGP routers, acting as speakers. The default routes of both GPTS routers are directed to the Null0 inte1faces. The edge routers are configured with a prefix-list to match only the default route. This prefix-list is used in conjunction with a couple of route-maps. One of these route-maps sets the local preference for routes received from eBGP neighbors, which helps prevent the creation of routing table

Volume: 15 Issue: 06 Pages: 6211 – 6217 (2024) ISSN: 0975-0290

loops. The other route-map sets the local preference for the default route learned via iBGP within the 327752 domain.

```
Gateway of last resort is 192.168.0.9 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 192.168.0.9, 00:20:38, GigabitEthernet0/3
                [110/1] via 192.168.0.1, 01:13:34, GigabitEthernet0/2
      192.168.0.0/24 is variably subnetted, 14 subnets, 2 masks
C        192.168.0.0/30 is directly connected, GigabitEthernet0/2
L        192.168.0.2/32 is directly connected, GigabitEthernet0/2
O        192.168.0.4/30 [110/2] via 192.168.0.18, 00:04:42, Port-channel1
                        [110/2] via 192.168.0.1, 01:13:34, GigabitEthernet0/2
C        192.168.0.8/30 is directly connected, GigabitEthernet0/3
L        192.168.0.10/32 is directly connected, GigabitEthernet0/3
O        192.168.0.12/30 [110/2] via 192.168.0.18, 00:04:42, Port-channel1
                         [110/2] via 192.168.0.9, 00:20:38, GigabitEthernet0/3
C        192.168.0.16/30 is directly connected, Port-channel1
L        192.168.0.17/32 is directly connected, Port-channel1
C        192.168.0.20/30 is directly connected, GigabitEthernet1/0
L        192.168.0.21/32 is directly connected, GigabitEthernet1/0
C        192.168.0.24/30 is directly connected, GigabitEthernet1/1
L        192.168.0.25/32 is directly connected, GigabitEthernet1/1
O        192.168.0.28/30
           [110/2] via 192.168.0.22, 00:46:33, GigabitEthernet1/0
           [110/2] via 192.168.0.18, 00:04:42, Port-channel1
O        192.168.0.32/30
           [110/2] via 192.168.0.26, 00:41:19, GigabitEthernet1/1
           [110/2] via 192.168.0.18, 00:04:42, Port-channel1
O     192.168.10.0/24 [110/2] via 192.168.0.26, 00:41:19, GigabitEthernet1/1
                      [110/2] via 192.168.0.22, 00:46:07, GigabitEthernet1/0
O     192.168.20.0/24 [110/2] via 192.168.0.26, 00:41:19, GigabitEthernet1/1
                      [110/2] via 192.168.0.22, 00:46:07, GigabitEthernet1/0
O     192.168.30.0/24 [110/2] via 192.168.0.26, 00:41:09, GigabitEthernet1/1
                      [110/2] via 192.168.0.22, 00:46:07, GigabitEthernet1/0
O     192.168.40.0/24 [110/2] via 192.168.0.26, 00:41:19, GigabitEthernet1/1
                      [110/2] via 192.168.0.22, 00:46:07, GigabitEthernet1/0
BB1#
```

Fig. 4. BackBone Switch Configuration

B- It Faculty Edge Routers

The edge routers within the information technology faculty serve as a boundary between the ISP with ASN 327752 and the IT faculty with the same ASN of 327752. As illustrated in Fig 3, these routers establish an eBGP connection between the IT ASN and the ISP ASN. Additionally, they exchange iBGP information locally within the IT ASN domain. The network connecting the ISP and the IT faculty utilizes the IP address range of 192.168.11.0/24, while an alternate path is established through the network of 192.168.12.0/24. Within the IT faculty, iBGP communication takes place between the two edge routers, utilizing the network 192.168.22.0/24.

C- IT Faculty Backbone or Core Layer Three Switches

The backbone layer three switches in the network are configured to function as routers by enabling IP routing and removing the layer two switch configuration. The specific configuration for the backbone layer three routing can be observed in Fig 4. To ensure redundancy between the edge routers of the IT faculty and the backbone or core switches, there are two links for each path in the network topology. The first two links utilize the networks 192.168.0.0/30 and 192.168.0.4/30, while the second edge router is connected to the backbone layer three switches through the networks 192.168.0.8/30 and 192.168.0.12/30. In order to enhance pe1formance and bandwidth, an Ethernet channel using the LACP (Link Aggregation Control Protocol) protocol is established between the two backbone switches, utilizing the network 192.168.0.16/30. Additionally, a port overloading NAT (Network Address Translation) configuration, specifically PAT (Port Address Translation), is implemented between the backbone or core layer and the IT edge routers domain, as depicted in Fig 6. Within the backbone domain, the OSPF (Open Shortest Path First) link state routing algorithm is configured and the routes are redistributed using the path vector of BGP.

```
Gateway of last resort is 192.168.0.29 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 192.168.0.29, 00:20:06, GigabitEthernet1/1
                [110/1] via 192.168.0.21, 00:20:06, GigabitEthernet1/0
      192.168.0.0/24 is variably subnetted, 11 subnets, 2 masks
O        192.168.0.0/30 [110/2] via 192.168.0.21, 00:42:20, GigabitEthernet1/0
O        192.168.0.4/30 [110/2] via 192.168.0.29, 00:42:20, GigabitEthernet1/1
O        192.168.0.8/30 [110/2] via 192.168.0.21, 00:23:22, GigabitEthernet1/0
O        192.168.0.12/30
           [110/2] via 192.168.0.29, 00:23:22, GigabitEthernet1/1
O        192.168.0.16/30
           [110/2] via 192.168.0.29, 00:42:20, GigabitEthernet1/1
           [110/2] via 192.168.0.21, 00:08:08, GigabitEthernet1/0
C        192.168.0.20/30 is directly connected, GigabitEthernet1/0
L        192.168.0.22/32 is directly connected, GigabitEthernet1/0
O        192.168.0.24/30 [110/2] via 192.168.30.3, 00:37:38, Vlan30
                         [110/2] via 192.168.20.3, 00:37:38, Vlan20
                         [110/2] via 192.168.10.3, 00:37:38, Vlan10
                         [110/2] via 192.168.0.21, 00:42:20, GigabitEthernet1/0
C        192.168.0.28/30 is directly connected, GigabitEthernet1/1
L        192.168.0.30/32 is directly connected, GigabitEthernet1/1
O        192.168.0.32/30 [110/2] via 192.168.30.3, 00:37:38, Vlan30
                         [110/2] via 192.168.20.3, 00:37:38, Vlan20
                         [110/2] via 192.168.10.3, 00:37:38, Vlan10
                         [110/2] via 192.168.0.29, 00:42:20, GigabitEthernet1/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, Vlan10
L        192.168.10.2/32 is directly connected, Vlan10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, Vlan20
L        192.168.20.2/32 is directly connected, Vlan20
      192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.30.0/24 is directly connected, Vlan30
L        192.168.30.2/32 is directly connected, Vlan30
      192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.40.0/24 is directly connected, Vlan40
L        192.168.40.2/32 is directly connected, Vlan40
AGG1#
```

Fig. 5. Aggregation Switch Configuration

```
AGG1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        10   120 P Active  local           192.168.10.3    192.168.10.1
Vl20        20   120 P Active  local           192.168.20.3    192.168.20.1
Vl30        30   100   Standby 192.168.30.3    local           192.168.30.1
Vl40        40   100   Standby 192.168.40.3    local           192.168.40.1
AGG1#
```

```
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
1      Po1(RU)         LACP      Gi0/0(P)    Gi0/1(P)

BB1#
```

Fig. 6. LACP and HSRP Protocols Configuration

D- IT Faculty Aggregation or Distribution Layer Three Switches

To enhance performance and bandwidth, an Ethernet channel utilizing the LACP (Link Aggregation Control Protocol) protocol is established between the two backbone switches. This Ethernet channel is configured as a layer three aggregation channel and utilizes the IP addresses 192.168.0.17/30 and 192.168.0.18/30 within the network 192.168.0.16/30. The purpose of this configuration is to increase performance and bandwidth within the network. For redundancy between the aggregation (distribution) and backbone (core) switches, there are two links for each path in the network topology. The first two links utilize the networks 192.168.0.20/30 and 192.168.0.24/30, while the second edge router is connected to the backbone layer three switches through the networks 192.168.0.28/30 and 192.168.0.32/30. These configurations can be observed in Fig l and the aggregation switch configuration in Fig 5. Furthermore, trunking is established between the two aggregation switches to further increase bandwidth

Volume: 15 Issue: 06 Pages: 6211 – 6217 (2024) ISSN: 0975-0290

and improve the overall pe1formance of the network topology.

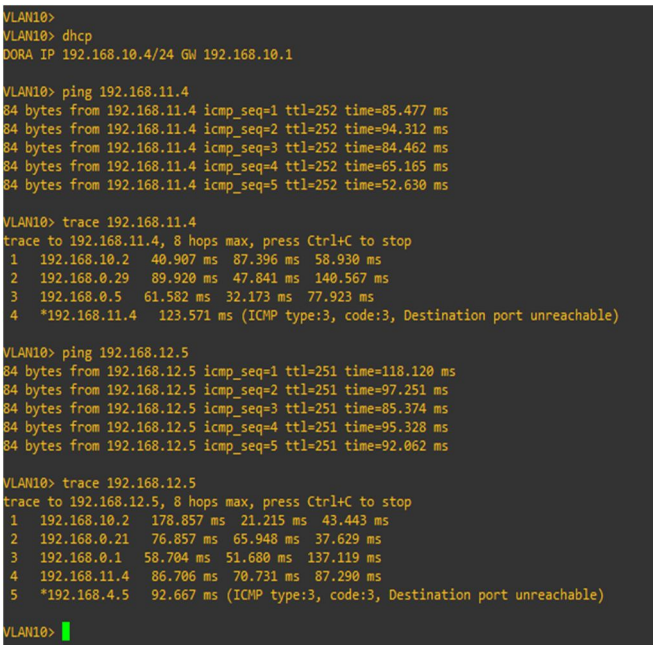

Fig. 7. Testing Topology Connectivity

E- It Faculty Access Layer Three Switches

The access switches have been configured with security commands to address various port security issues, including STP (Spanning Tree Protocol), ARP (Address Resolution Protocol), and STP security configurations. Additionally, VLANs 10, 20, 30, and 40 have been implemented to provide logical separation as a security measure and facilitate network traffic management. To prevent layer two loops, the RPVST (Rapid Per-VLAN Spanning Tree) protocol should be configured.

F- Connectivity Test from VLANs to Internet

After completing the configuration of the three-tier model depicted in Fig 1, the next step is to monitor the services. This includes accessing the internet using the PAT configuration. Additionally, dynamic IP addresses can be obtained from the DHCP server located at the Backbone layer. It is important to check the connectivity using the "ping" command in the te1minal. Furthermore, the trace command can be deployed to verify the path between a single VLAN and the internet, or even between different VLAN s, as illustrated in Fig 7.

VIII. CONCLUSION AND FUTURE WORK

This research paper proposes a scalable and secure campus network scenario based on the CISCO PPDIOO methodology, with a focus on enhancing security and availability, particularly on campuses. The designed network follows a three-tier model and is simulated using GNS3, a network simulation software.

The paper presents a topology that includes core, distribution, and access layers, along with dual single-homed internet connectivity to ensure redundancy. The deployment of protocols such as HSRP and STP further enhances network resilience. AdditionalLy, the paper discusses the implementation of access layer security measures. As suggestions for future work, the authors propose studying virtualization utilizing VxLAN (Virtual Extensible LAN) technology and exploring the design of wireless campus networks.

REFERENCES

[1]. S. Jing, L. Guo, Q. Wang, E. Li, C. Zhao, and B. Xiao, "Research and deployment of ipv4/ipv6 dual stack network in large-scale campus network," in 2021 IEEE Conference on Telecommunications, Optics and Computer Science (TOC.S), 2021, pp. 128-132.

[2]. T. Shanmugam and B. Malarkodi, "Analysis of campus network man- agement challenges and solutions," in 2019 TEQIP Ill Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW), 2019, pp. 312-316.

[3]. I. 0. Yablochnikova, K. A. Makhiboroda, S. L. Yablochnikov, V. B.Dzobelova, and T. A. Doguchaeva, "Modeling of e-learning processes," in 2023 Intelligent Technologies and Electronic Devices in Vehicle and Road Transport Complex (TJRVED), 2023, pp. 1-6.

[4]. X. Wei, Y. Bouslimani, and K. Sella!, "Voip based solution for the use over a campus environment," in 2012 25th IEEE Canadian C01iference on Electrical and Computer Engineering (CCECE), 2012, pp. 1-5.

[5]. V. Subbarao, K. Srinivas, and R. Pavithr, "A survey on internet of things based smart, digital green and inteJJjgent campus," in 2019 4th International Coriference on Internet of Things: Smart Innovation and Usages (loT-S!U), 2019, pp. 1-6.

[6]. A. Elrashdi, S. Khiralla2, and S. Albaseer3, "Development ppdioo methodology to be compatible with technical projects for computer networks," 0 I 2018.

[7]. T. Shanmugam and B. Malarkodi, "Analysis of campus network man- agement challenges and solutions," in 2019 TEQJP Ill Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW), 2019, pp. 312-316.

[8]. J. Zhang, "Design of campus network security system based on network information security," in 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC), 2022, pp. 1194-1197.

[9]. R. G. Barba, M. Criollo, N. Aimacana, C. ManosaJvas, and C. Silva- Cardenas, "Qos policies to improve pe1formance in academic campus and sdn networks," in 2018 IEEE 10th Latin-American Cmiference on Communications (LATINCOM), 2018, pp. 1-6.

[10]. X. Wang, L. Wang, B. Yu, and G. Dong, "Studies on network management system framework of campus network," in 2010 2nd lntemational Asia Conference 011 biformatics in Control, Automation and Robotics (CAR 2010), vol. 2, 20IO, pp. 285-289.

[11]. S. Chen, F. Xue, Z. Huang, W. Chen, J. Ye, and G. Cai, "Design and implementation of a novel campus face recognition access control system based on cl0ud-edge c01lab0rati0n," in 2022 12th International Conference on Information Technology in Medicine and Education (JTME), 2022, pp. 671-675.

[12]. K. Crawley, Step 8: Build Redundancy and Resilience, 2022, pp. 155-172.

[13]. V. Morozov and 0. Tsesliv, "Investigating availability

Volume: 15 Issue: 06 Pages: 6211 – 6217 (2024) ISSN: 0975-0290

of cloud-deployed systems on redundancy, architecture, and recovery time," in 18th IEEE International Conference on Computer Science and Information Technologies, CSIT 2023, Lviv, Ukraine, October 19-21, 2023. IEEE, 2023, pp. l-4.

[14]. Campus LAN and Wireless LAN Solution Design Guide cisco.com," https://www.cisco.com/c/en/us/td/docs/solutions/CYD/Campus/cisco- campus-lan-wlan-design-guide.html, May 4, 2020, [Accessed 19-12-2023].

[15]. P. Gil, G. J. Garcia, A. D. Delgado, R. M. Medina, A. Calderon, and P. Marti, "Computer networks virtualization with GNS3: evaluating a solution to optimjze resources and achieve a distance learning," in IEEE Frontiers in Education Conference, FIE 2014, Proceedings, Madrid, Spain, October 22-25, 2014. IEEE Computer Society, 2014, pp. 1-4.

[16]. A. Y. Hamed, M. Kh. Elnahary, H. H. El-Sayed, " Task Scheduling Optimization in Cloud Computing by Coronavirus Herd Immunity Optimizer Algorithm," in The International Journal of Advanced Networking and Applications (IJANA), Volume 16, Issues 04, 2023, pp. 5686 - 5695 .

Authors Biography

Abdulhadi Alarbad: Mr. Alarbad is currently enrolled in the Department of Networks and Communications at Misurata University's Faculty of Information Technology, working towards obtaining his Bachelor's degree. His focus of study centers around enterprise network design and management. Currently, Mr. Alarbad is in the process of writing his BSc thesis and anticipates completing his degree by August 2024.

Anas Alsharif Alsharif is currently enrolled as a Bachelor's degree student in the Department of Networks and Communications at Misurata University's Faculty of Information Technology. His research interests primarily revolve around next-generation networks and data centers. At present, he is actively engaged in writing his BSc thesis. Additionally, he has set his sights on completing his BSc studies by August 2024.

Salem Sati: Dr. Sati holds a doctoral degree in computer science from HHU University in Dusseldorf, Germany, which was awarded in 2017. He also possesses a master's degree in computer engineering from the Higher Industrial Institute in Misurata, Libya, obtained in 2008. In addition, Dr. Sati completed his bachelor's degree in computer engineering at the Higher Industrial Institute in 1997. Dr. Sati has made significant contributions to various national conferences held in Libya, as well as international IEEE conferences across North America, Asia, and Europe, specifically in the field of computer networks. His research output includes numerous publications in IEEE conferences. Currently, Dr. Sati serves as an assistant professor at the Faculty of Information Technology in Misurata University..