Sri Lanka Institute of Information Technology

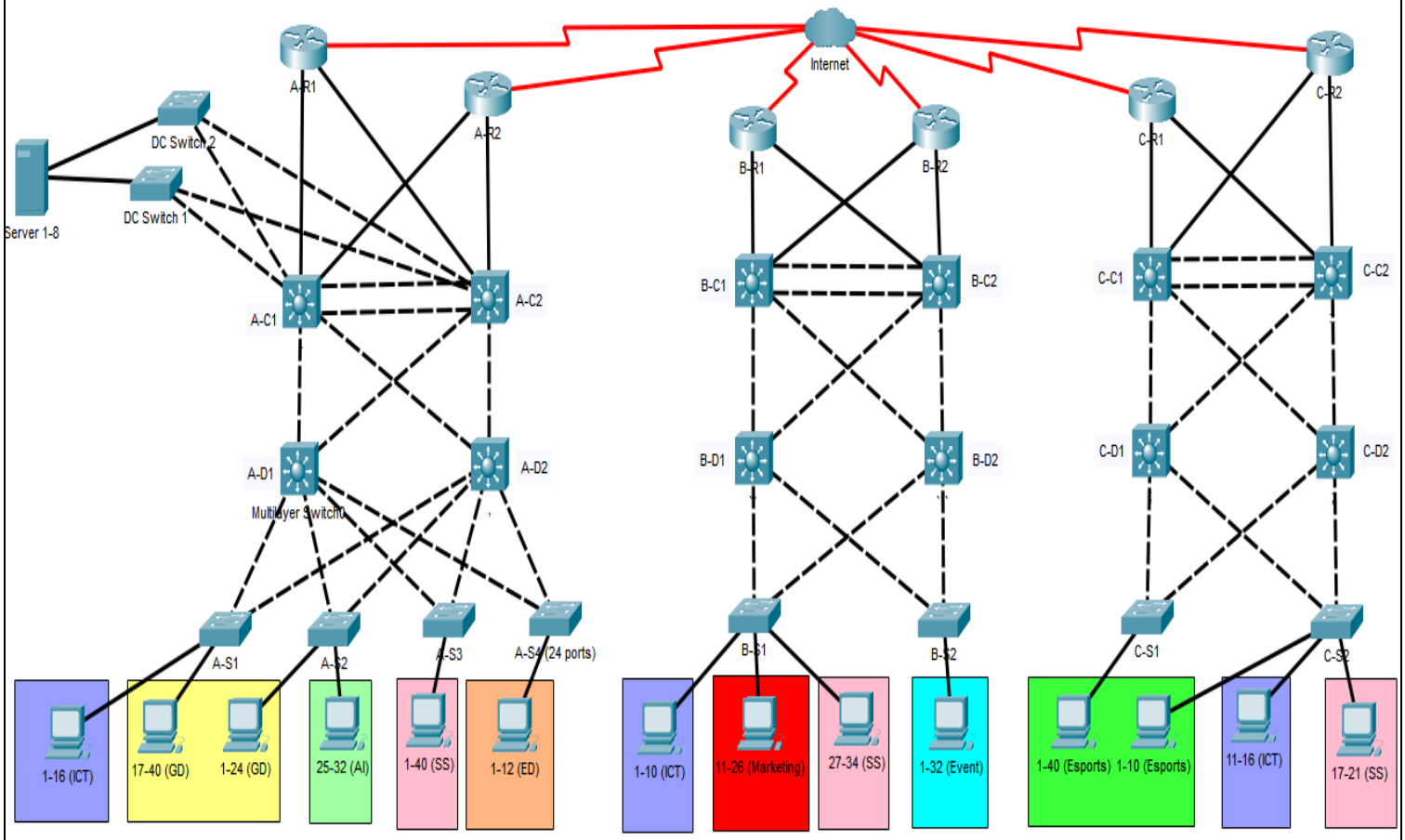
Network Design and Development

Advanced Networking Technologies – IE2052

B.Sc. (Hons) in Information Technology Specializing in Cyber Security

Group Members	
Student Name	**Registration Number**
Vijayanathan Rishan	IT20659462
Sivagnanamoorthy Pavithiran	IT20668822
Thisitha K.L. D	IT20618872

1. **Design a three-layer network topology according to the above given specifications. Requirements such as redundancy and port aggregation must be considered in the design**



2. Analyze the security requirements of such a network and ensure they are considered in the design

- **Port Security**

  Port Security use to secure the network from unauthorized devices forwarding packets. and it gives permission to a device to use that switch. When unknown devices connect to the switch, it marks it as a violation and disables network access to that port [1]. In our design we limit the number of MAC addresses for each port. Packets that have a matching MAC address only forwarded, and other packets are restricted.

- **Firewall**

  In our network design we used firewall it can protect our computer and data by managing our network traffic [1]. It protects from outside cyber attackers from malicious or unnecessary network traffic. And it protects from malicious software accessing our network over the internet.

- **Disabling un used port**

  In this network design switch and router have some un used ports that can be vulnerable to unauthorized access [2]. so, by disabling those ports prevent unauthorized access and secure our network.

3. Create an appropriate IP addressing plan and document it.

Device	Interface	Address	Subnet Mask
A-R1	G/0/0	192.158.1.113	255.255.255.240
	G/0/1	192.158.1.114	255.255.255.240
A-R2	G/0/0	192.158.1.115	255.255.255.240
	G/0/1	192.158.1.116	255.255.255.240
B-R1	G/0/0	192.158.1.117	255.255.255.240
	G/0/1	192.158.1.118	255.255.255.240
B-R2	G/0/0	192.158.1.119	255.255.255.240
	G/0/1	192.158.1.120	255.255.255.240
C-R1	G/0/0	192.158.1.121	255.255.255.240
	G/0/1	192.158.1.122	255.255.255.240
C-R2	G/0/0	192.158.1.123	255.255.255.240
	G/0/1	192.158.1.124	255.255.255.240
PC A-S1 (1-16)	NIC	192.158.1.1- 192.158.1.16	255.255.255.192
PC A-S1 (17-40)	NIC	192.158.0.129- 192.158.0.152	255.255.255.192
PC A-S2 (1-24)	NIC	192.158.0.153- 192.158.0.176	255.255.255.192
PC A-S2 (25-32)	NIC	192.158.1.129- 192.158.1.136	255.255.255.240
PC A-S3 (1-40)	NIC	192.158.0.1- 192.158.0.40	255.255.255.192
PC A-S4 (1-12)	NIC	192.158.1.97- 192.158.1.108	255.255.255.240
PC B-S1 (1-10)	NIC	192.158.1.17- 192.158.1.26	255.255.255.192
PC B-S1 (11-26)	NIC	192.158.1.65- 192.158.1.80	255.255.255.224

PC B-S1 (27-34)	NIC	192.158.0.41- 192.158.0.48	255.255.255.192
PC B-S2 (1-32)	NIC	192.158.0.193- 192.158.0.224	255.255.255.192
PC C-S1 (1-40)	NIC	192.158.0.65- 192.158.0.104	255.255.255.192
PC C-S2 (1-10)	NIC	192.158.0.105- 192.158.0.114	255.255.255.192
PC C-S2 (11-16)	NIC	192.158.1.27- 192.158.1.32	255.255.255.192
PC C-S2 (17-21)	NIC	192.158.0.50- 192.158.0.54	255.255.255.192
Server (1-8)		192.158.1.145- 192.158.1.152	255.255.255.240
	VLAN 5 (Support Services)	192.158.0.0	255.255.255.192
	VLAN 10 (Esports)	192.158.0.64	255.255.255.192
	VLAN 20 (Games Design)	192.158.0.128	255.255.255.192
	VLAN 30 (Events)	192.158.0.192	255.255.255.192
	VLAN 40 (ICT)	192.158.1.0	255.255.255.192
	VLAN 50 (Marketing)	192.158.1.64	255.255.255.224
	VLAN 60 (Engine Development)	192.158.1.96	255.255.255.240
	VLAN 70 (AI)	192.158.1.128	255.255.255.240
	VLAN 80 (Server)	192.158.1.144	255.255.255.240

4. **The hardware devices that will be used to implement the network must be selected and justified.**

Selected Switches:

Access Layer

- Building A

Selected switches: Three 48 port Switches and one 24 port switch (A-S4)

Down link ports and speed: 40 and 20 ports with 1Gbps

Uplink ports and speed: 8 and 4 ports with 10Gbps

Available Host: 140

Required Host: 124 (except Data sever)

Extra Host: 16

- Building B

Selected switches: Two 48 port Switches

Down link ports and speed: 40 ports with 1Gbps

Uplink ports and speed: 8 ports with 10Gbps

Available Host: 80

Required Host: 66

Extra Host: 14

- Building C

Selected switches: Two 48 port Switches

Down link ports and speed: 40 ports with 1Gbps

Uplink ports and speed: 8 ports with 10Gbps

Available Host: 80

Required Host: 61

Extra Host: 19

They mention in the design required access layer speed must be allowed 1 Gbps so to full fill this requirement minimum we need 40 Gbps from uplink here we dived 8 uplinks into two parts and connect 4 ports to one distribution switch and another 4 ports to another distribution switch for redundancy. So, we select 10 Gbps uplink switch to get 40Gbps form 4 uplinks to full fill the

requirement. In building A, we used one 24 port switch to reduce the number of unusable ports. Son in our design every building has number of extra hosts that can be use full for future development.

Distribution Layer

Selected switches: Two 24 port Switches for each building

Down link ports and speed: 16 ports with 10Gbps

Uplink ports and speed: 8 ports 40Gbps

To reduce broadcast traffic volumes, ease the configuration process for VLAN and to simplify the security management layer 3 switches are selected to distribution layer.

Core Layer

Selected switches: Two 24 port Switches for each building

Down link ports and speed: 12 ports with 40Gbps

Uplink ports and speed: 12 ports with 100Gbps

In core layer more uplink ports needed because of the redundancy implementation. So, we selected 24 ports layer 3 switches with 40Gbps downlink/ 100 Gbps uplink speeds.

In core layer and distribution layer we used two layer 3 switches in each building for redundancy. And uplinks are connected using port aggregation.

Data server

Selected switches: Two 24 port Switches for each building

Down link ports and speed: 16 ports with 10Gbps

Uplink ports and speed: 8 ports with 40Gbps

Data centers were connected indirectly to the core switches to provide high-speed packet switching and redundancy. We used separate two switches between the data center servers and core switches because of the number of uplink ports in core switch in not enough to connect all the data center links at once. So, we used two 24 ports layer-2 switches with 10Gbps downlink/40Gbps uplink

Selected Router:

Two routers were implemented in each building to interconnect with other buildings. And router is mandatory for inter VLAN routing for forwarding network traffic from one VLAN to another. And we selected a router that comes with built-in firewall and VPN for security. Instead of using separate firewall and VPN tunnel.

5. Identify 3 layer 2 technologies you will implement in the designed network. Evaluate and justify why the selected technology is suitable for the design proposed by you

- **Spanning Tree Protocol (STP)**

The Spanning Tree Protocol is a network protocol that prevents looping when devices share data via redundant channels in a Local Area Network [3]. To provide redundancy, we used two distribution switches for each building in our network design. Redundancy can protect against disaster but it can also cause switch looping. As a result, the Spanning Tree protocol keeps track of all network connections, discovers redundant connections, and disables ports that could cause looping.

- **VLAN**

VLAN stands for Virtual Local Area Network, and it's a network segmentation mechanism that's not based on physical location. One or more local area networks combine to form these. It allows many networks' devices to be combined into a single logical network [4]. Instead of using separate switches for each department, we used VLAN technology to split users into their own networks by isolating a specific number of ports from a switch and grouping them together.

- **MAC ACL**

All networked devices have a MAC (media access control) address. it used to identify those hardware devices uniquely. MAC access control list (ACL) technology use to permit or deny Wi-Fi access to individual devices based on their MAC addresses [5]. In our design we use this technology to maintain strict network security which allow only devices with known MAC addresses to connect.

6. **Identify 3 layer 3 technologies you will implement in the designed network. Evaluate and justify why the selected technology is suitable for the design proposed by you.**

- **IP ACL**

IP Access Control Lists (ACL) are used to filter packets and manage their flow via a network. It protects the network by limiting traffic access, restricting user and device access, and preventing traffic from exiting the network [5]. we use IP Access Control Lists technology to prevent spoofing and denial-of-service attacks, and allow dynamic, temporary user-access through a firewall.

- **OSPF technology**

Open Shortest Path First (OSPF) is a router technology that finds the best path for packets passing over a network [6]. We used this technology in our design to find out the best path to avoid latency and increase forwarding rate because there are multiple paths have a particular packet transfer.

- **Inter VLAN Routing**

Using a router to forwarding network traffic from one VLAN to another VLAN is a process of inter VLAN routing [7]. This Inter VLAN routing technology used in our design to communicate between two or more completely different VLAN in the same switch or other with the help of Router.

References

[1] "www.n-able.com," [Online]. Available: https://www.n-able.com/features/secure-network-design.

[2] J. McPhillips, "help.coalitioninc.com," 21 May 2022. [Online]. Available: https://help.coalitioninc.com/en/articles/3740263-closing-unused-network-ports.

[3] L. Williams, "www.guru99.com," 30 April 2022. [Online]. Available: https://www.guru99.com/stp-spanning-tree-protocol-examples.html.

[4] E. Harmoush, "www.practicalnetworking.net," 17 May 2022. [Online]. Available: https://www.practicalnetworking.net/stand-alone/vlans/.

[5] "kb.netgear.com," 28 November 2016. [Online]. Available: https://kb.netgear.com/21709/What-are-MAC-Access-Control-Lists-ACLs-and-how-do-they-work-with-my-managed-switch.

[6] nilenduapocalypse and Pushpender007, "www.geeksforgeeks.org," 12 October 2021. [Online]. Available: https://www.geeksforgeeks.org/open-shortest-path-first-ospf-protocol-states/.

[7] A. Dennis, "www.section.io," 21 March 2021. [Online]. Available: https://www.section.io/engineering-education/inter-vlan-routing/#:~:text=Inter%2DVLAN%20routing%20refers%20to,since%20they%20are%20logical%20connections..