IN PARTNERSHIP WITH PLYMOUTH UNIVERSITY

Name: Gunathilaka	Group (G20)
Student Reference Number:	10898583

Module Code: PUSL2065	Module Name: Computer Networks
Coursework Title: Computer Networks Group Project	
Deadline Date:11/4/2023	Member of staff responsible for coursework: Mr Chamara Dissanayake
Program: BSc. (Hons) Computer Networks	

Please note that University Academic Regulations are available under Rules and Regulations on the University website www.plymouth.ac.uk/studenthandbook.

Group work: please list all names of all participants formally associated with this work and state whether the work was undertaken alone or as part of a team. Please note you may be required to identify individual responsibility for parts.

Gunathilaka -	10898583
Gangabadage L Mansith -	10899326
Guniyangodage Sandeepa -	10898684
Wanniachchige Fonseka -	10899263
Welikadage Botheju -	10900327
Ranasinghe Priyantha -	10899343

We confirm that we have read and understood the Plymouth University regulations relating to Assessment Offences and that we are aware of the possible penalties for any breach of these regulations. We confirm that this is the independent work of the group.

Signed on behalf of the group: Gunathilaka 10898583

Individual assignment: ***I confirm that I have read and understood the Plymouth University regulations relating to Assessment Offences and that I am aware of the possible penalties for any breach of these regulations. I confirm that this is my independent work.***

Signed:

Use of translation software: failure to declare that translation software or a similar writing aid has been used will be treated as an assessment offence.

I *have used/not used translation software.

If used, please state the name of the software…………………………………………………………………

Overall mark _____% **Assessors Initials ______** **Date_________**

*Please delete as appropriate

Contents

❖ Introduction

The National University of Information Technology (NUIT) emerges as a beacon of technological education in Sri Lanka. With its main campus established in Homagama and ambitious plans for regional campuses across the country, NUIT aims to empower students with the skills and knowledge to thrive in the digital age. A robust and secure network infrastructure is paramount to facilitating this vision. This report delves into the design of a network architecture that caters to NUIT's unique needs. It balances the university's aspirations for scalability, security, and manageability across its distributed campuses.

• The Challenge: Unifying a Network Across Regions

NUIT's network faces a unique challenge – bridging the physical distance between the main campus and regional locations. Ensuring seamless connectivity for staff, students, and guests across these dispersed sites requires a well-defined network architecture. This architecture must not only facilitate communication and resource access but also prioritize robust security measures to protect sensitive university data.

• Key Considerations for NUIT's Network

- **Segmentation:** Dividing the network into logical segments isolates traffic flows for different user groups (staff, students, guests) and departmental functions. This enhances security by preventing unauthorized access to critical resources and improves overall network performance by reducing congestion.
- **Scalability**: The network design must accommodate future growth as NUIT expands its regional presence. Scalability necessitates flexibility in addressing additional campuses and user demands without compromising network performance.
- **Security**: Cyber threats pose a significant risk to any university network. The design prioritizes security measures like firewalls, intrusion detection/prevention systems (IDS/IPS), and access control lists (ACLs) to safeguard sensitive information and university resources.
- **Manageability**: A centralized management system simplifies network administration and troubleshooting. This allows network administrators to monitor network health, identify and resolve issues efficiently, and ensure smooth network operation across all campuses.

- **The Road Ahead: A Comprehensive Network Design**

This report explores and presents a detailed network design tailored to NUIT's specific requirements. It outlines network segmentation strategies, proposes a hierarchical subnet structure for efficient address allocation, and dives into a sample IP addressing plan for a faculty within the main campus. Additionally, the report specifies the network components and technologies necessary for both the main university and regional campuses, including core and access layer networking devices, secure wireless connectivity, and a reliable connection method between campuses. Furthermore, the report delves into the implementation of a security and network management framework. This framework leverages a network management system (NMS) for centralized control, utilizes firewalls and IDS/IPS for security enforcement, and emphasizes the importance of access control lists and secure VPN connections between campuses. By following this comprehensive network design, NUIT can establish a secure, scalable, and efficiently managed network infrastructure that empowers its academic mission across all its campuses. This network will serve as the backbone for facilitating collaboration, innovation, and knowledge dissemination throughout Sri Lanka's educational landscape.

❖ Logical Design

Fig:1

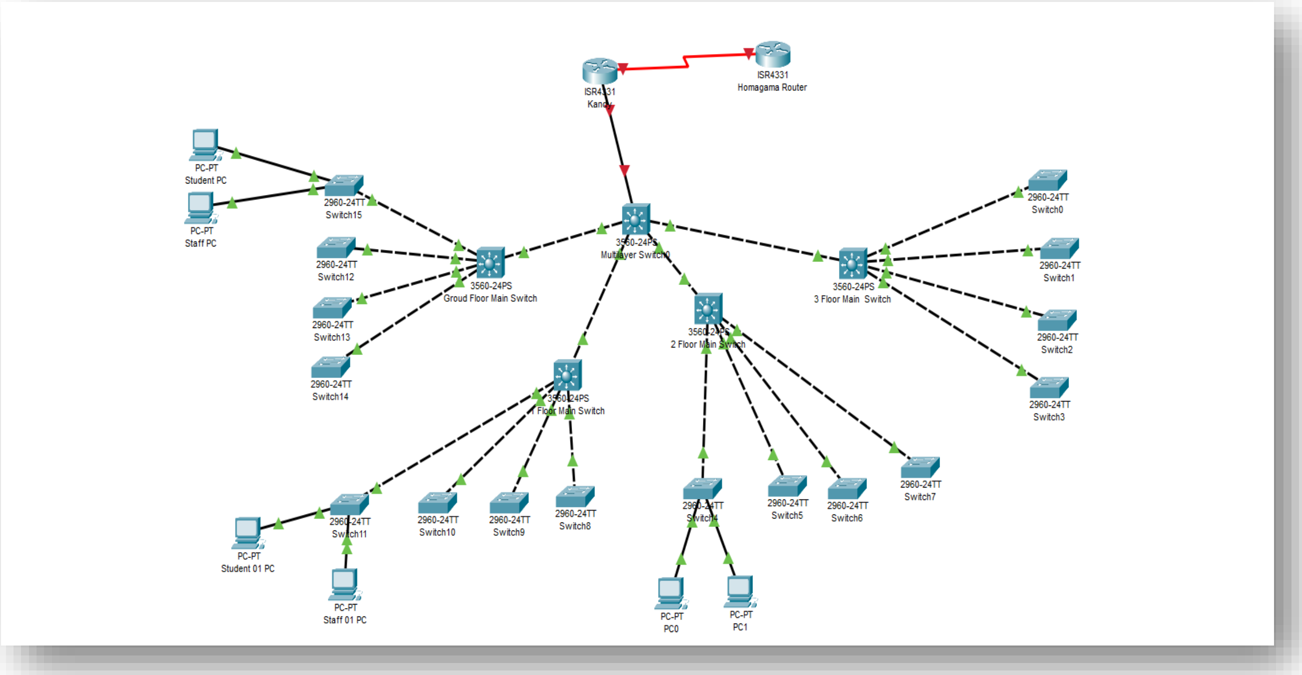


Fig:2

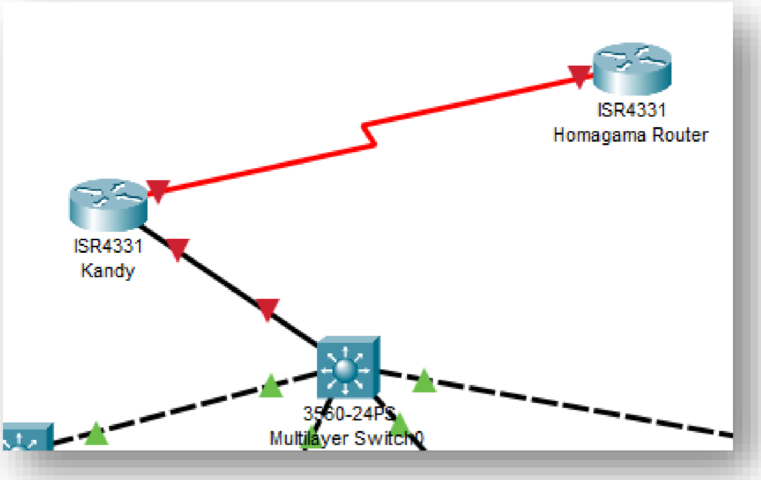
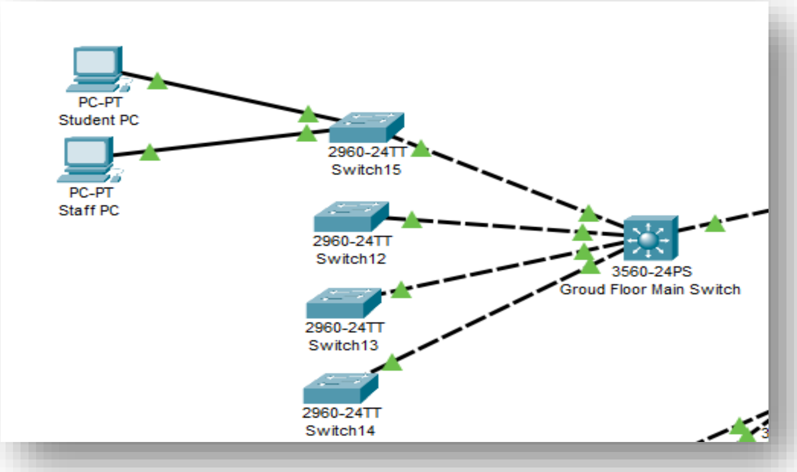


Fig:3



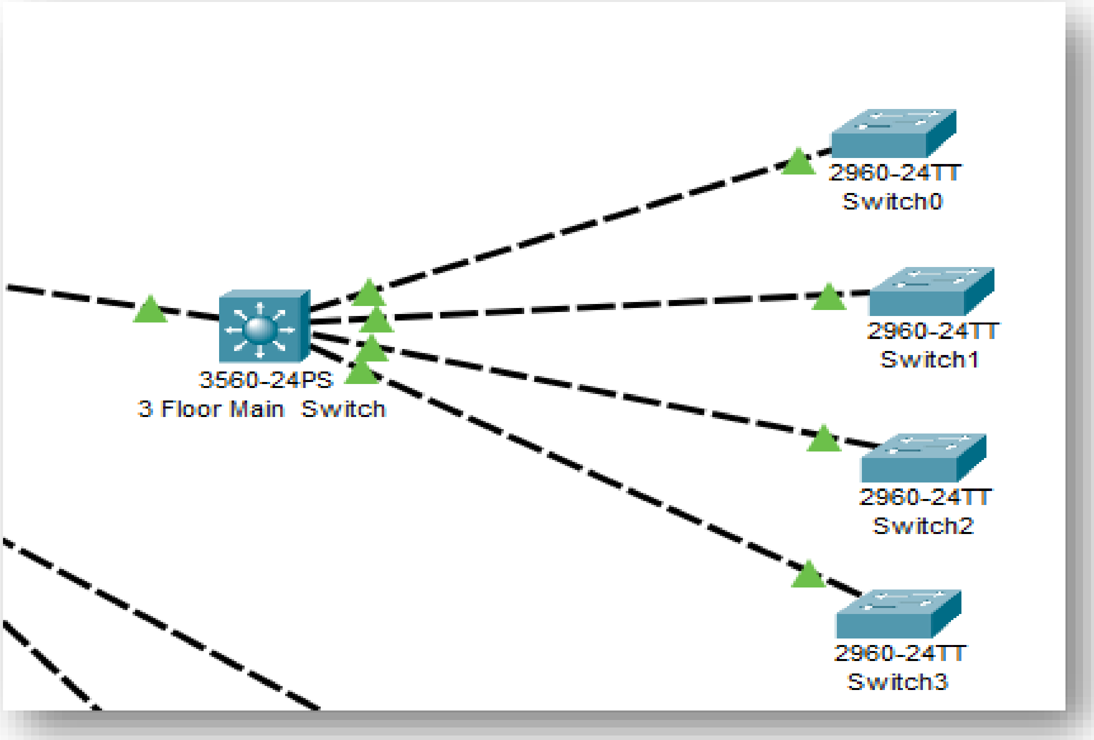


Fig:4

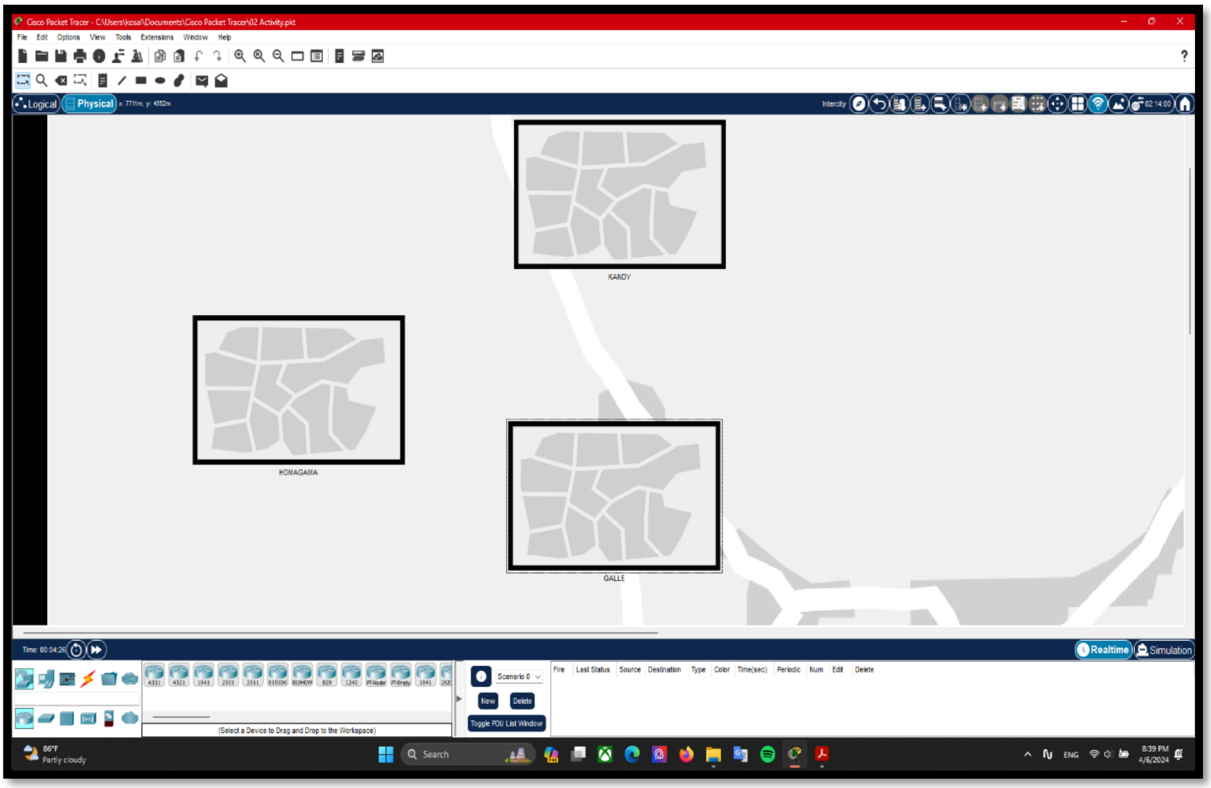

Cisco Packet Tracer - C:\Users\kosal\Documents\Cisco Packet Tracer\02 Activity.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
x: 7711m, y: 4552m
Intercity
02:14:00
KANDY
HOMAGAMA
GALLE
Time: 00:04:26
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
(Select a Device to Drag and Drop to the Workspace)
86°F
Partly cloudy
Search
ENG
8:39 PM
4/6/2024

Fig:5

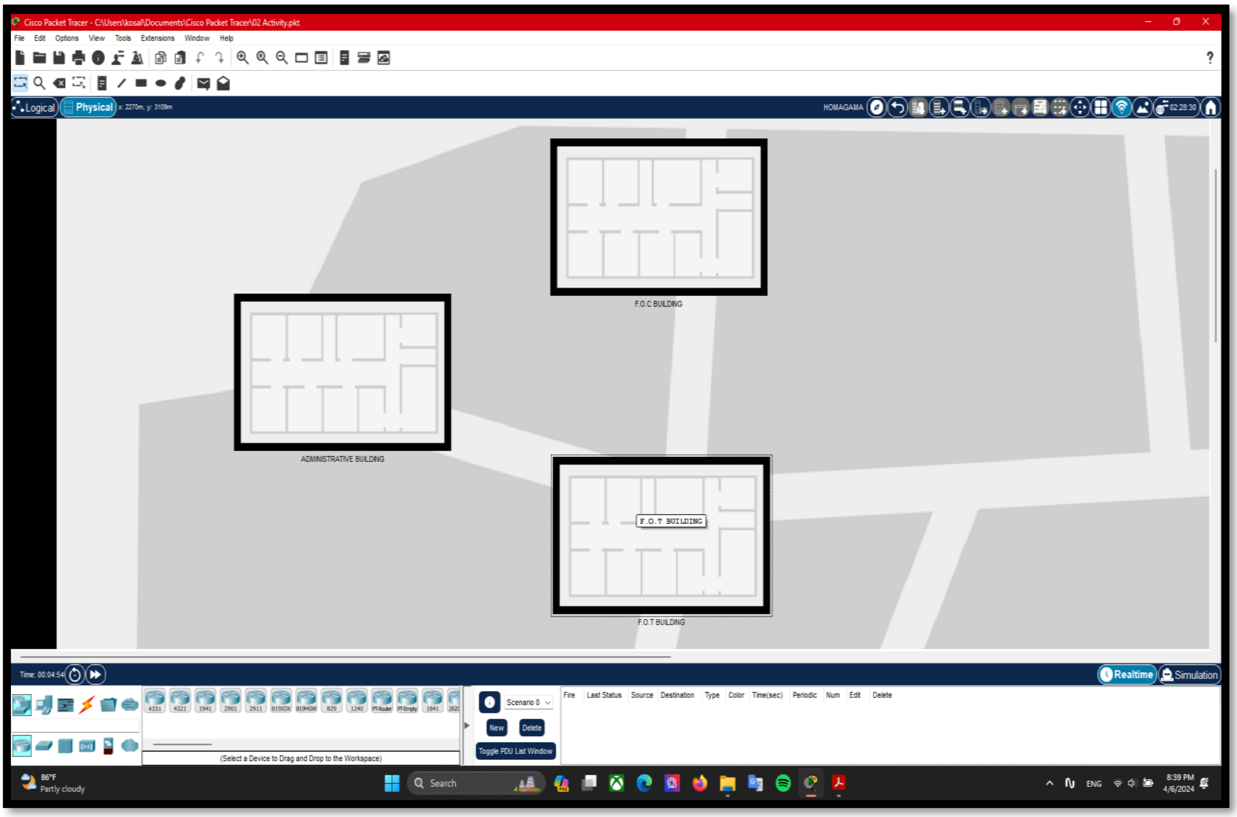

Cisco Packet Tracer - C:\Users\kosal\Documents\Cisco Packet Tracer\02 Activity.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
x: 2270m, y: 3109m
HOMAGAMA
02:28:30
F.O.C BUILDING
ADMINISTRATIVE BUILDING
F.O.T BUILDING
F.O.T BUILDING
Time: 00:04:54
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
(Select a Device to Drag and Drop to the Workspace)
86°F
Partly cloudy
Search
ENG
8:39 PM
4/6/2024

Fig: 6

❖ IP Addressing (Ipv4 & Ipv6)

• IPv4 Addressing the University Network.

This IPv4 address block provides 256 IP addresses in total. Now, let's subnet it to accommodate the required segments, so we are categorizing subnets into two main parts.

1). Main University Subnets

➢ Faculty of Technology: /26(Subnet Mask: 255,255,255,192)
Network address:192.248.40.0
Broadcast address:192.248.40.63
Usable Ip Range (192.248.40.1-192.248.40.62) (62 addresses)

192.248.40.1
192.248.40.2
192.248.40.3
192.248.40.4
192.248.40.5
192.248.40.6
192.248.40.7
192.248.40.8
192.248.40.9
192.248.40.10
192.248.40.11
192.248.40.12
192.248.40.13
192.248.40.14
192.248.40.15
192.248.40.16
192.248.40.17
192.248.40.18
192.248.40.19
192.248.40.20
192.248.40.21
192.248.40.22
192.248.40.23
192.248.40.24
192.248.40.25
192.248.40.26
192.248.40.27
192.248.40.28
192.248.40.29
192.248.40.30
192.248.40.31

192.248.40.32
192.248.40.33
192.248.40.34
192.248.40.35
192.248.40.36
192.248.40.37
192.248.40.38
192.248.40.39
192.248.40.40
192.248.40.41
192.248.40.42
192.248.40.43
192.248.40.44
192.248.40.45
192.248.40.46
192.248.40.47
192.248.40.48
192.248.40.49
192.248.40.50
192.248.40.51
192.248.40.52
192.248.40.53
192.248.40.54
192.248.40.55
192.248.40.56
192.248.40.57
192.248.40.58
192.248.40.59
192.248.40.60
192.248.40.61
192.248.40.62

- Faculty of computing:/26 (Subnet Mask:255.255.255.192)
  Network address:192.248.40.64
  Broadcast address:192.248.40.127
  Usable IP Range (192.248.40.65-192.248.40.126) (62 addresses)

  192.248.40.65
  192.248.40.66
  192.248.40.67
  192.248.40.68
  192.248.40.69
  192.248.40.70
  192.248.40.71
  192.248.40.72
  192.248.40.73
  192.248.40.74
  192.248.40.75
  192.248.40.76
  192.248.40.78
  192.248.40.79
  192.248.40.80
  192.248.40.81
  192.248.40.82
  192.248.40.83
  192.248.40.84
  192.248.40.85
  192.248.40.86
  192.248.40.87
  192.248.40.88
  192.248.40.89
  192.248.40.90
  192.248.40.91
  192.248.40.92
  192.248.40.93
  192.248.40.94
  192.248.40.95
  192.248.40.96
  192.248.40.97
  192.248.40.98
  192.248.40.99
  192.248.40.100
  192.248.40.101
  192.248.40.102
  192.248.40.103
  192.248.40.104
  192.248.40.105

192.248.40.106
192.248.40.107
192.248.40.108
192.248.40.109
192.248.40.110
192.248.40.111
192.248.40.112
192.248.40.113
192.248.40.114
192.248.40.115
192.248.40.116
192.248.40.117
192.248.40.118
192.248.40.119
192.248.40.120
192.248.40.121
192.248.40.122
192.248.40.123
192.248.40.124
192.248.40.125
192.248.40.126

- Administrative Building :/26(Subnet Mask :255.255.255.192)
  Network Address:192.248.40.128
  Broadcast Ip: 192.248.40.191
  Usable Ip Range:(192.248.40.129-192.248.40.190) (62 addresses)

  192.248.40.129
  192.248.40.130
  192.248.40.131
  192.248.40.132
  192.248.40.133
  192.248.40.134
  192.248.40.135
  192.248.40.136
  192.248.40.137
  192.248.40.138
  192.248.40.139
  192.248.40.140
  192.248.40.141
  192.248.40.142
  192.248.40.143
  192.248.40.144
  192.248.40.145
  192.248.40.146
  192.248.40.147
  192.248.40.148

192.248.40.149
192.248.40.150
192.248.40.151
192.248.40.152
192.248.40.153
192.248.40.154
192.248.40.155
192.248.40.156
192.248.40.157
192.248.40.158
192.248.40.159
192.248.40.160
192.248.40.161
192.248.40.162
192.248.40.163
192.248.40.164
192.248.40.165
192.248.40.166
192.248.40.167
192.248.40.168
192.248.40.169
192.248.40.170
192.248.40.171
192.248.40.172
192.248.40.173
192.248.40.174
192.248.40.175
192.248.40.176
192.248.40.177
192.248.40.178
192.248.40.179
192.248.40.180
192.248.40.181
192.248.40.182
192.248.40.183
192.248.40.184
192.248.40.185
192.248.40.186
192.248.40.187
192.248.40.188
192.248.40.189
192.248.40.190

- Student users:/26 (Subnet Mask: 255.255.255.192)
  Network Address: 192.248.40.192
  Broadcast Address: 192.248.40.255
  Usable Ip Range:(192.248.40.193-192.248.40.254) (62 addresses)

192.248.40.193
192.248.40.194
192.248.40.195
192.248.40.196
192.248.40.197
192.248.40.198
192.248.40.199
192.248.40.200
192.248.40.201
192.248.40.202
192.248.40.203
192.248.40.204
192.248.40.205
192.248.40.206
192.248.40.207
192.248.40.208
192.248.40.209
192.248.40.210
192.248.40.211
192.248.40.212
192.248.40.213
192.248.40.214
192.248.40.215
192.248.40.216
192.248.40.217
192.248.40.218
192.248.40.219
192.248.40.220
192.248.40.221
192.248.40.222
192.248.40.223
192.248.40.224
192.248.40.225
192.248.40.226
192.248.40.227
192.248.40.228
192.248.40.230
192.248.40.231
192.248.40.232
192.248.40.233
192.248.40.234
192.248.40.235
192.248.40.236
192.248.40.237
192.248.40.238
192.248.40.239
192.248.40.240

192.248.40.241
192.248.40.242
192.248.40.243
192.248.40.244
192.248.40.245
192.248.40.246
192.248.40.247
192.248.40.248
192.248.40.249
192.248.40.250
192.248.40.251
192.248.40.252
192.248.40.253
192.248.40.254

- Staff users :/26 (Subnet mask :255.255.255.192)
  Network Address: 192.248.41.0
  Broadcast Address: 192.248.41.63
  Usable IP Range:(192.248.41.1-192.248.41.62) (62 addresses)

  192.248.41.1
  192.248.41.2
  192.248.41.3
  192.248.41.4
  192.248.41.5
  192.248.41.6
  192.248.41.7
  192.248.41.8
  192.248.41.9
  192.248.41.10
  192.248.41.11
  192.248.41.12
  192.248.41.13
  192.248.41.14
  192.248.41.15
  192.248.41.16
  192.248.41.17
  192.248.41.18
  192.248.41.19
  192.248.41.20
  192.248.41.21
  192.248.41.22
  192.248.41.23
  192.248.41.24
  192.248.41.25
  192.248.41.26
  192.248.41.27

192.248.41.28
192.248.41.29
192.248.41.30
192.248.41.31
192.248.41.32
192.248.41.33
192.248.41.34
192.248.41.35
192.248.41.36
192.248.41.37
192.248.41.38
192.248.41.39
192.248.41.40
192.248.41.41
192.248.41.42
192.248.41.43
192.248.41.44
192.248.41.45
192.248.41.46
192.248.41.47
192.248.41.48
192.248.41.49
192.248.41.50
192.248.41.51
192.248.41.52
192.248.41.53
192.248.41.54
192.248.41.55
192.248.41.56
192.248.41.57
192.248.41.58
192.248.41.59
192.248.41.60
192.248.41.61
192.248.41.62

- Guest Users:/26 (Subnet Mask: 255.255.255.192)
  Network Address: 192.248.41.64
  Broadcast Address: 192.248.41.127
  Usable Ip Range :(192.248.41.65-192.248.41.126) (62 addresses)

192.248.41.65
192.248.41.66
192.248.41.67

192.248.41.68
192.248.41.69
192.248.41.70
192.248.41.71
192.248.41.72
192.248.41.73
192.248.41.74
192.248.41.75
192.248.41.76
192.248.41.77
192.248.41.78
192.248.41.79
192.248.41.80
192.248.41.81
192.248.41.82
192.248.41.83
192.248.41.84
192.248.41.85
192.248.41.86
192.248.41.87
192.248.41.88
192.248.41.89
192.248.41.90
192.248.41.91
192.248.41.92
192.248.41.93
192.248.41.94
192.248.41.95
192.248.41.96
192.248.41.97
192.248.41.98
192.248.41.99
192.248.41.100
192.248.41.101
192.248.41.102
192.248.41.103
192.248.41.104
192.248.41.105
192.248.41.106
192.248.41.107
192.248.41.108
192.248.41.109
192.248.41.110
192.248.41.111
192.248.41.112
192.248.41.113
192.248.41.114

192.248.41.115
192.248.41.116
192.248.41.117
192.248.41.118
192.248.41.119
192.248.41.120
192.248.41.121
192.248.41.122
192.248.41.123
192.248.41.124
192.248.41.125
192.248.41.126

2). Regional Campus Subnets

- Kandy campus:/27 (Subnet Mask: 255.255.255.224)
  Network Address: 192.248.41.128
  Broadcast Address:192.248.41.159
  Usable Ip Range:(192.248.41.129-192.248.41.158) (30 addresses)

  192.248.41.129
  192.248.41.130
  192.248.41.131
  192.248.41.132
  192.248.41.133
  192.248.41.134
  192.248.41.135
  192.248.41.136
  192.248.41.137
  192.248.41.138
  192.248.41.139
  192.248.41.140
  192.248.41.141
  192.248.41.142
  192.248.41.143
  192.248.41.144
  192.248.41.145
  192.248.41.146
  192.248.41.147
  192.248.41.148
  192.248.41.149
  192.248.41.150
  192.248.41.151

192.248.41.152
192.248.41.153
192.248.41.154
192.248.41.155
192.248.41.156
192.248.41.157
192.248.41.158

- Galle campus:/27 (Subnet Mask:255.255.255.224)
  Network Address: 192.248.41.160
  Broadcast Address: 192.248.41.191
  Usable Ip Range:(30 addresses)

192.248.41.161
192.248.41.162
192.248.41.163
192.248.41.164
192.248.41.165
192.248.41.166
192.248.41.167
192.248.41.168
192.248.41.169
192.248.41.170
192.248.41.171
192.248.41.172
192.248.41.173
192.248.41.174
192.248.41.175
192.248.41.176
192.248.41.177
192.248.41.178
192.248.41.179
192.248.41.180
192.248.41.181
192.248.41.182
192.248.41.183
192.248.41.184
192.248.41.185
192.248.41.186
192.248.41.187
192.248.41.188
192.248.41.189
192.248.41.190

- ## IPv6 Addressing

In our meticulously planned IPv6 address block, **2003:DF0:100: :/48**, we've strategically allocated subnet addresses to cater to the diverse segments of the National University of Information Technology's (NUIT) network infrastructure. Adhering to the standard subnet size of /64, we've precisely delineated each segment with its unique network address within the broader address block, ensuring efficient network management and scalability.

At the heart of our network architecture lies the main university, where the Faculty of Technology, Faculty of Computing, and Administrative Building are housed. Each of these vital components possesses its distinct subnet address for streamlined administration and optimized performance. The Faculty of Technology operates within the subnet **2003:DF0:100: :/64**, fostering an environment conducive to technological exploration and innovation. Similarly, the Faculty of Computing operates within the subnet **2003:DF0:100:1: :/64**, facilitating cutting-edge research and development in computational sciences. Meanwhile, the Administrative Building, serving as the nerve centre of NUIT's administrative operations, operates within the subnet **2003:DF0:100:2: :/64**, ensuring seamless coordination and efficient management of university affairs.

Furthermore, we've allocated dedicated subnets for different user groups within the main university, underscoring our commitment to personalized network access and security. Students accessing NUIT's resources operate within the subnet **2003:DF0:100:3: :/64**, ensuring secure and tailored access to educational materials and collaborative platforms. Meanwhile, staff members, entrusted with the responsibility of nurturing academic excellence, operate within the subnet **2003:DF0:100:4: :/64**, enjoying privileged access to administrative tools and educational resources. Additionally, guests visiting our esteemed institution are provided with a separate subnet, **2003:DF0:100:5: :/64**, ensuring controlled and secure access to NUIT's network resources while maintaining the integrity of our infrastructure.

Expanding our network footprint beyond the confines of the main university, we've established regional campuses in Kandy and Galle, each with its subnet address to support localized network management and service provisioning. The Kandy Campus operates within the subnet **2003:DF0:100:6: :/64**, catering to the educational needs of students in the Central Province. Similarly, the Galle Campus operates within the subnet **2003:DF0:100:7: :/64**, extending NUIT's educational reach to the Southern Province.

This meticulous subnet allocation strategy not only ensures efficient utilization of IPv6 address space but also underscores our commitment to providing a robust, secure, and scalable network infrastructure to support NUIT's academic endeavours. By adhering to industry best practices and leveraging the inherent capabilities of IPv6, we are poised to meet the evolving demands of the digital age while empowering our students and staff with seamless access to educational resources and collaborative tools.

❖ Proposed Subnetting Structure

- **Main University Subnetting Strategy**

The main university comprises three primary buildings: the Faculty of Technology, the Faculty of Computing, and the Administrative Building. Each has distinct network requirements based on the user count and the nature of the network traffic expected.

Faculty of Technology Building:

- Given the high number of nodes (500) in computer laboratories, a subnet size that accommodates at least 510 devices is necessary to allow for network growth and additional network devices. Therefore, a /23 subnet (providing up to 510 usable IP addresses) is recommended, which could be 192.248.40.0/23. This range is more than sufficient for the current needs and short-term growth, ensuring that laboratory devices, faculty staff, and students have reliable network access.

Faculty of Computing Building:

- Similarly, this building hosts 500 nodes in its laboratories. Allocating a /23 subnet here as well, such as 192.248.42.0/23, ensures ample address space for all computing devices, faculty, and potential expansions.

Administrative Building:

- This segment involves not just staff devices but also critical network infrastructure and servers. Considering the diverse roles and the critical nature of devices in this building, a /24 subnet might suffice initially, offering up to 254 usable IP addresses. This is allocated as 192.248.44.0/24.

- **Regional Campus Subnetting Strategy**

Each regional campus, such as those in Kandy and Galle, is smaller but still requires careful planning to ensure network efficiency and future scalability.

Campus-Wide Subnet Allocation: For simplicity and efficient address management, each regional campus can be assigned a /22 subnet, which can then be subdivided into smaller subnets for different departments or needs. For instance, the Kandy campus could be allocated 192.248.46.0/22, and the Galle campus could receive 192.248.50.0/22. These blocks provide flexibility for detailed segmentation within the campuses.

- **IPv6 Allocation Strategy**

With the expansive address space offered by IPv6, the university has the opportunity to implement a more hierarchical and structured addressing scheme that can accommodate future growth indefinitely.

Main University and Regional Campuses: Each main segment (e.g., Technology Faculty, Computing Faculty, Administrative Building) can be allocated a /56 subnet, allowing for extensive subdivision within each segment.
For instance:

- Faculty of Technology: 2003:DF0:100: A000: :/56
- Faculty of Computing: 2003:DF0:100: B000: :/56
- Administrative Building: 2003:DF0:100:C000: :/56

For the regional campuses, a similar approach allows each to have a designated /48 subnet, ensuring that they have ample space for detailed internal segmentation based on future needs.
For example:

- Kandy Campus: 2003:DF0:100: D000: :/48
- Galle Campus: 2003:DF0:100: E000: :/48

- **Detailed Considerations**

This structured approach to subnetting ensures that each part of the university’s network is allocated enough address space to support current devices and future growth. Subnetting not only segments the network logically but also enhances security by isolating traffic within these segments. Proper VLAN configuration will complement this subnetting strategy, improving network management and efficiency. For security, assigning different subnets to different user groups (staff, students, guests) within these broader segments allows for more granular access control and monitoring. Implementing VLANs aligned with subnetting enhances security and traffic management, allowing policies to be applied more uniformly and effectively across the network.

❖ Justification of proposed technologies

- **Network Requirements: -**

- Connect Three Campus (Homagama, Kandy, Galle)
- Allow staff and students to have access to the internet and educational resources.
- Divide the network into secure segments (Staff, Student, Guest)
- Centrally manage the network from Homagama
- scalable to allow for future growth.

- **Network Design Suggestion:**

- **This design makes use of a three-layered hierarchical network structure: -**

- Core Layer: Provides redundant, high-bandwidth links between the three campuses.
- Distribution Layer: traffic across each campus to reach access layer devices.
- Access Layer: joins hardware to the network (For Computer, etc...)

1. **Core Layer**

- ➢ Devices- Two redundant, highly available high-performance routers
- ➢ Connection Technology - Fibre optic cables (1 Gbps or more): Take future growth requirements into account.

2. **Distribution Layer**

- **Homagama Campus**
- ➢ Devices- Layer 3 switches (one per building)
- ➢ Connection Technology - Fibre optic cable (1 Gbps) to switches at the access and core layers.
- **Kandy & Galle Campuses**
- ➢ Devices- Layer 3 switches
- ➢ Connection Technology - 100 Mbps leased lines; upgrade to fibre as needed.

3. **Access Layer**

- ➢ Devices- Managed Layer 2 switches on every floor and building
- ➢ Connection Technology- Cat6 Ethernet cables are used in wired networks.
- ➢ Wireless Access Point- thoughtfully placed to offer campus-wide Wi-Fi coverage.

- **Network Segmentation**

- ➢ Firewalls- To manage traffic flow between VLANs and the internet, implement firewalls at the core layer.
- ➢ Access Control Links- Install firewalls at the core layer to control traffic flow between VLANs and the internet.

- **Centralized Management**

Network Management System- Monitor and control network devices from the main campus by using NMS.

- **Security Considerations**

- Strong Authentication- For wired networks use a comparable protocol; for wireless networks, use WPA2/WPA3.
- Intrusion Detection/Prevention System (IDS/IPS)- To identify and stop malicious activities, install an IDS/IPS at the core layer.
- Regular Security Audit- Conduct security audits regularly to find and fix issues.

- **Scalability**

- As the university grows, the design may be simply scaled by adding more distribution layer switches, access layer devices, and core routers.
- When necessary, it is possible to upgrade the regional campuses' leased lines to fibre optic connections.

- **Financial Considerations**

- The fibre optic backbone and redundancy in the core layer will result in a larger initial investment.
- Nonetheless, the initial expense is surpassed by the long-term advantages of management, scalability, and dependability.

- **Additional Considerations**

- To guarantee network availability during power outages, install a reliable power backup system.
- Plan for cable management that will make maintenance and access simple.

❖ Network Segmentation.

In addition to the proposed segmentation strategies and implementation technologies for NUIT, several other factors and considerations are vital for ensuring the success and effectiveness of the network infrastructure:

1. Compliance Requirements: NUIT must adhere to various regulatory and compliance standards, particularly concerning data protection and privacy. Segmentation helps in enforcing compliance by isolating sensitive data and limiting access to authorized users only. This is particularly crucial in educational institutions where student and faculty data privacy is paramount.

2. Redundancy and High Availability: Implementing redundancy measures within each segment and across the network infrastructure is essential to ensure uninterrupted service availability. Redundant links, failover mechanisms, and backup systems should be considered to mitigate the risk of network downtime. This is especially important for NUIT's mission-critical services such as online learning platforms and research databases.

3. Integration with Identity and Access Management (IAM) Systems: Integration with IAM systems allows NUIT to enforce granular access controls based on user roles, privileges, and authentication factors. This ensures that only authorized users can access specific network resources within their respective segments, enhancing overall security posture.

4. Monitoring and Logging: Robust monitoring and logging mechanisms should be in place to track network activity, detect anomalies, and facilitate forensic analysis in the event of security incidents. Centralized logging solutions and intrusion detection/prevention systems (IDS/IPS) can provide real-time visibility into network traffic and aid in identifying and mitigating potential threats.

5. Education and Awareness: Educating network users about the importance of network security and segmentation is critical for maintaining a secure computing environment. NUIT should conduct regular training sessions, and awareness campaigns, and provide clear guidelines on acceptable use policies to prevent security breaches resulting from user negligence or ignorance.

6. Disaster Recovery and Business Continuity: NUIT should develop comprehensive disaster recovery and business continuity plans to mitigate the impact of network disruptions or security incidents. This includes regular backups of critical data, offsite storage solutions, and predefined procedures for restoring network services in the event of a catastrophic event.

7. Regular Security Audits and Penetration Testing: Conducting regular security audits and penetration testing exercises helps identify vulnerabilities and weaknesses in the network infrastructure. NUIT should engage third-party security firms to perform thorough assessments and recommend remediation measures to strengthen the overall security posture.

8. Adoption of Emerging Technologies: Keeping abreast of emerging technologies and trends in network security is essential for NUIT to stay ahead of evolving threats. This includes exploring technologies such as software-defined networking (SDN), network virtualization, and artificial intelligence/machine learning-based security solutions to augment existing segmentation strategies and enhance overall resilience.

By considering these additional factors and adopting a holistic approach to network segmentation and security, NUIT can build a robust and future-proof infrastructure that supports its mission of fostering innovation and education in Sri Lanka's technology landscape.

Recommendations

1. Network Segmentation and Subnet Structure

Use VLANs for Segmentation: Implement VLANs to segregate traffic between different user groups and departments. This ensures enhanced security and better network performance by reducing broadcast domains.

Efficient IP Allocation: For subnetting, consider the anticipated growth in student and staff numbers. Use a hierarchical addressing scheme that allows for expansion without renumbering. For IPv4, consider using variable-length subnet masking (VLSM) to conserve addresses. For IPv6, leverage its abundant address space to simplify your design while planning for future growth.

2. IP Address Distribution Plan

Dynamic and Static Addressing: Allocate static IP addresses for critical infrastructure (servers, network printers, etc.) and dynamic addresses (via DHCP) for student and staff devices. This approach simplifies management and accommodates the fluctuating number of devices.

IPv6 Implementation: Emphasize the adoption of IPv6, considering its increasing importance and the benefits it offers in terms of address space and autoconfiguration capabilities. Plan for dual-stack implementation to ensure compatibility and seamless transition from IPv4.

3. Detailed Network Design

Core and Edge Layers: Clearly distinguish between the core network infrastructure, which should be highly reliable and capable of fast data transfer, and the edge layers, where security devices like firewalls and IDS/IPS are placed.

Wireless Access: Given the high reliance on wireless access for students and staff, ensure robust wireless network design, incorporating WPA3 encryption and sufficient coverage to avoid dead zones.

4. Security and Network Management Plan

Layered Security Approach: Implement a defence-in-depth strategy. This should include not just firewalls and IDS/IPS systems but also endpoint protection, secure access protocols (like SSH instead of Telnet), and regular vulnerability assessments.

Regular Updates and Patch Management: Establish a routine for updating all network devices and systems to protect against known vulnerabilities.

Training and Awareness: Develop a cybersecurity awareness program for all network users, focusing on phishing, password policies, and safe internet practices.

5. Justifications and Recommendations

Cost-Benefit Analysis: For each proposed technology or design choice, include a cost-benefit analysis. This demonstrates not only financial prudence but also an understanding of the value added by each component of your design.

Futureproofing: Recommend strategies for scalable network design to accommodate the anticipated expansion of the university and the integration of new technologies.

- ## Implementation Of the Sample Faculty Networks.

1. Network Topology Design

Layered Approach: Adopt a three-tier architecture consisting of the core layer, distribution layer, and access layer. The core layer provides a high-speed backbone and connects to the university's main network resources. The distribution layer controls access and routing between subnets, while the access layer connects end devices and local networks to the distribution layer.

Redundancy: Implement redundancy at the core and distribution layers to ensure network availability. This can be achieved through dual routing/switching hardware and using protocols like Spanning Tree Protocol (STP) to prevent loops.

2. Addressing Scheme

IPv4 and IPv6 Planning: Allocate a subnet from the given IP blocks to the faculty network. Use a /24 subnet for IPv4 for simplicity, providing up to 254 usable addresses per subnet. For IPv6, a /64 subnet is standard for local networks, offering a vast number of addresses.

Static and Dynamic Allocation: Assign static IP addresses to critical infrastructure (servers, network printers, access points) and use DHCP for dynamic addressing of end-user devices like computers and mobile devices.

3. Security Measures

Firewall Configuration: Place a firewall at the network's edge to control traffic between the faculty network and the rest of the university's network as well as the internet. Configure rules to allow necessary traffic while blocking known malicious sources.

Network Access Control (NAC): Implement NAC to ensure that only authorized devices can connect to the network. This could involve authentication against a directory service before network access is granted.

Intrusion Detection System (IDS): Deploy an IDS to monitor network traffic for signs of unusual activity or known attack patterns, alerting administrators to potential security issues.

4. Network Services

Wireless Network: Provide WPA2/WPA3 secured wireless access for students and staff. Consider implementing separate SSIDs for faculty, students, and guests, each with appropriate access restrictions.

VPN Access: Offer VPN services for secure remote access to the faculty network, ensuring that remote teaching and access to resources are as secure as on-campus.

Network Segmentation: Use VLANs to segment the network further, for example, separating administrative staff, faculty, and lab networks to limit broadcast traffic and enhance security.

5. Implementation with Network Simulator

Cisco Packet Tracer: Utilize the Cisco Packet Tracer to model the network. Start by placing routers and switches to reflect your core, distribution, and access layers. Add servers, computers, and other peripherals as needed to represent the faculty's infrastructure.

Configuration: Configure devices within your Packet Tracer model with appropriate IP addressing, VLANs, and security settings (firewall rules, NAC policies). Simulate traffic to test connectivity and security posture.

Documentation: Document your network design within Packet Tracer, including a description of each device's role, IP addressing, and any specific configurations applied. This documentation is crucial for understanding the network setup and for troubleshooting.

❖ Security and Network Management Plan for NUIT

- Security Design

1. Défense Depth: NUIT's security strategy embraces the "defence in depth" philosophy, which involves layering various defensive mechanisms to protect data and infrastructure. This multi-faceted approach ensures that even if one layer is breached, additional layers of defence continue to safeguard the university's digital assets.

2. Perimeter Security: Central to NUIT's perimeter defence are firewalls and Intrusion Detection/Prevention Systems (IDS/IPS). These critical components serve as the first line of defence against external threats.

Firewalls are deployed at strategic points to inspect incoming and outgoing network traffic, enforcing security policies that block unauthorized access while allowing legitimate communication to flow freely.

IDS/IPS systems extend beyond simple traffic filtering. These systems actively monitor for signs of malicious activity and, unlike traditional firewalls, can take pre-emptive actions to stop attacks in their tracks.

3. Internal Network Security: To bolster internal defences, NUIT implements network segmentation and stringent access control mechanisms.

Network Segmentation divides the network into distinct zones, such as academic departments, administrative offices, and student residences. This not only optimizes network performance but also minimizes the potential impact of security breaches by isolating them to specific segments.

Access Control Lists (ACLs) are meticulously configured on network devices to ensure that only authorized individuals can access sensitive areas of the network, providing a solid layer of security against internal threats.

4. Endpoint Security: Recognizing the importance of securing individual devices, NUIT deploys advanced antivirus and anti-malware solutions across all endpoints. This ensures comprehensive protection against a wide array of threats, from ransomware to spyware.

5. Wireless Security: With the ubiquity of wireless devices on campus, securing wireless networks is paramount. NUIT utilizes the latest encryption standards to safeguard wireless communication.

Implementing WPA2/WPA3 Encryption guarantees that all wireless traffic is encrypted, significantly reducing the risk of interception by unauthorized parties.

A dedicated Guest Network offers internet access to visitors while isolating them from the main network, ensuring that sensitive university resources remain protected.

- User Authentication and Authorization:

Multi-factor authentication (MFA) introduces an additional layer of security, requiring users to provide two or more verification factors to access sensitive systems, dramatically reducing the risk of unauthorized access.

Role-Based Access Control (RBAC) ensures that users are granted access only to resources necessary for their roles, minimizing potential internal threats and data breaches.

- **Network Management**

Central to NUIT's strategy is a Centralized Network Management System (NMS), enabling efficient oversight and management of the university's vast network infrastructure. The NMS offers real-time insights into network health, facilitating prompt identification and resolution of issues before they escalate into significant problems. Through Network Monitoring, NUIT keeps a vigilant eye on bandwidth utilization, device health, and error rates, ensuring the network remains robust and reliable.

Configuration Management plays a critical role in maintaining network integrity. By centralizing control, NUIT ensures consistent configurations across devices, reducing errors and simplifying network administration.

Log Management is essential for security and operational transparency. By aggregating logs in a central repository, NUIT can swiftly respond to security incidents and troubleshoot issues, enhancing overall network resilience.

The implementation of a Security Information and Event Management (SIEM) system marks a significant step forward in NUIT's security posture. This system aggregates and analyzes logs from various sources, enabling a unified response to security threats.

- **Single Point of Contact (PoC) for Security and Network Operations**

NUIT's innovative approach integrates the Security Operations Center (SOC) and Network Operations Centre (NOC) into a unified operational framework. This harmonization not only streamlines processes but also fosters a culture of collaboration and information sharing.

The SOC is tasked with the continuous monitoring of security events, ensuring rapid detection, investigation, and mitigation of potential threats. This proactive stance is crucial in maintaining the confidentiality, integrity, and availability of university data.

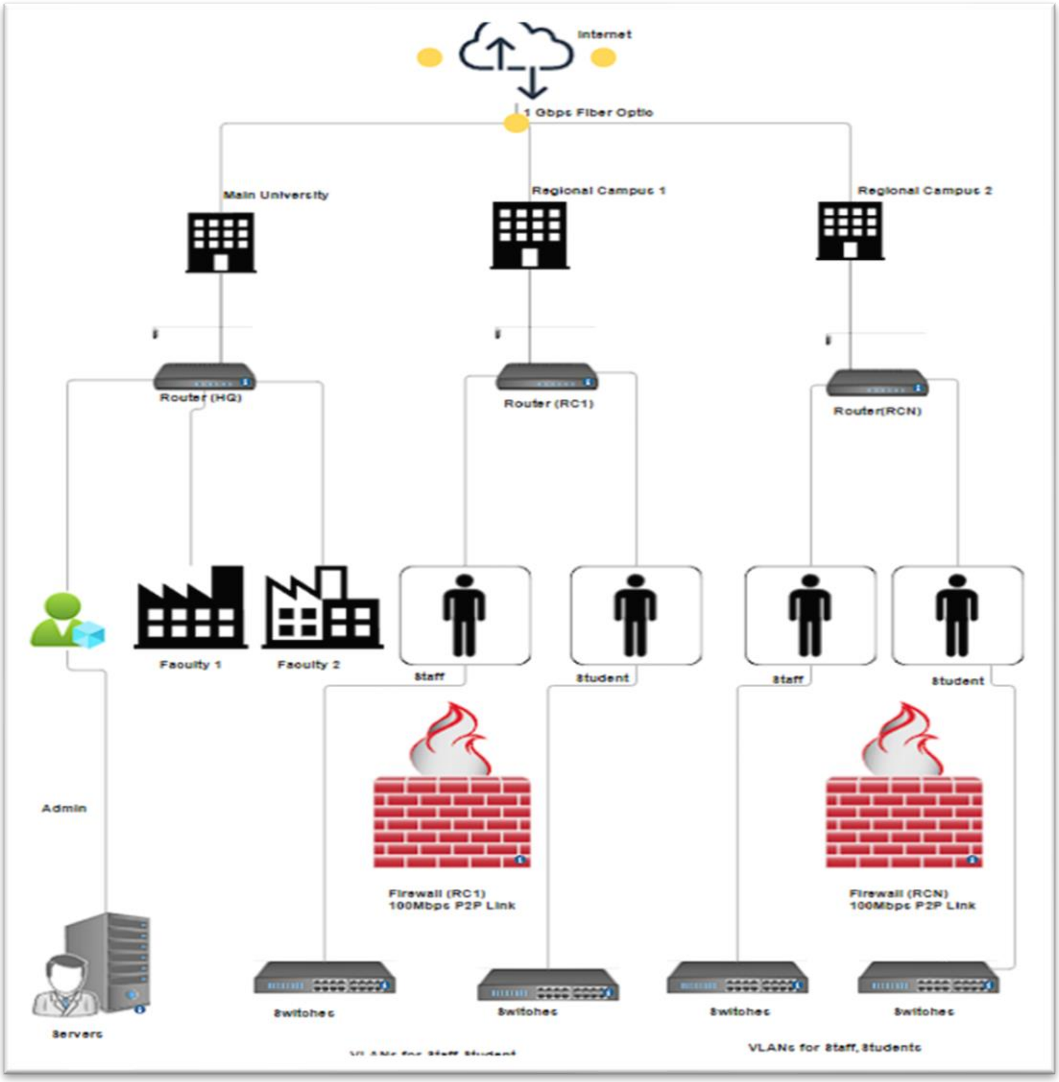
The NOC, on the other hand, focuses on ensuring optimal network performance and reliability. From monitoring to maintenance, the NOC plays a pivotal role in ensuring that NUIT's digital infrastructure supports the university's academic and administrative functions without interruption.

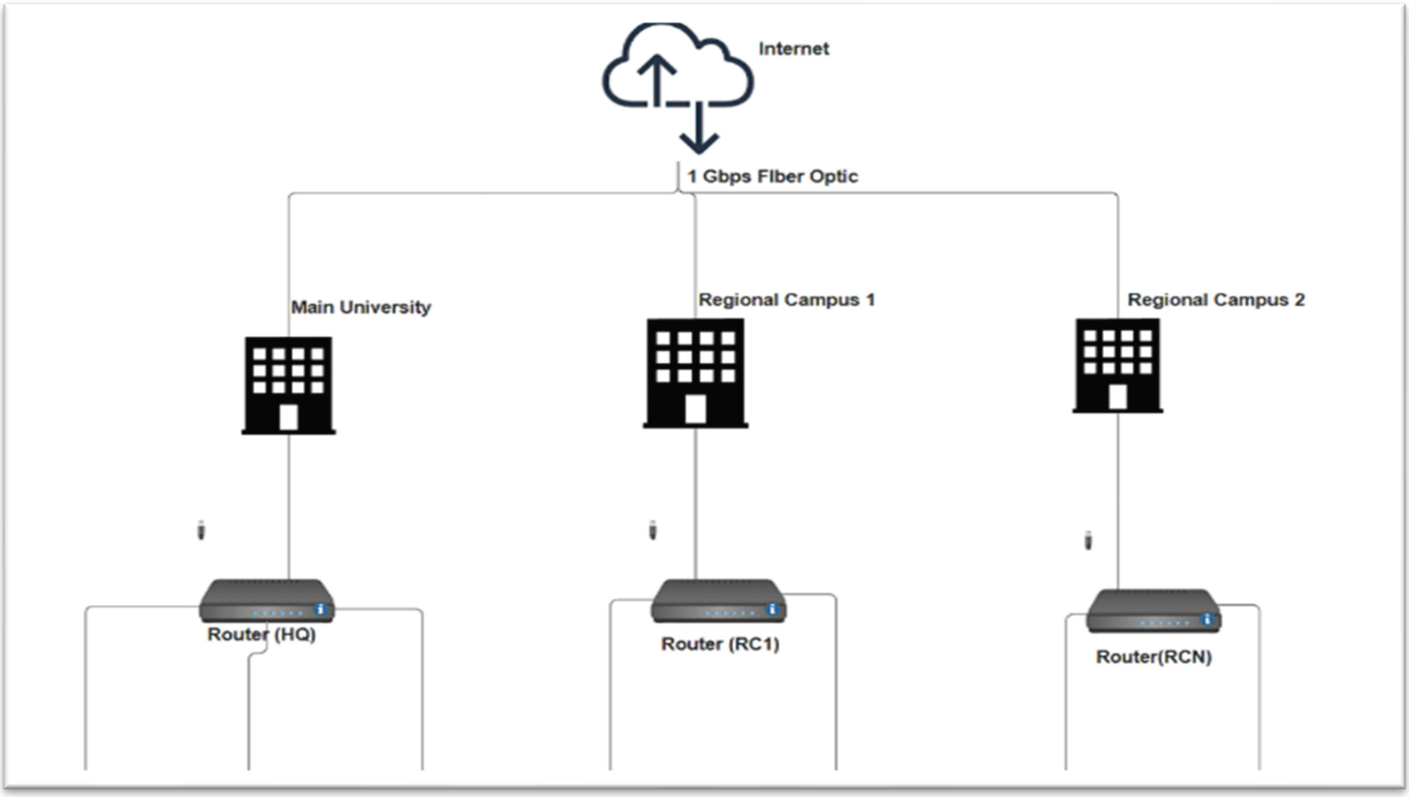
Integration between the SOC and NOC is not just strategic but essential for a cohesive response to incidents that may impact both security and network performance. This unified approach ensures that NUIT can swiftly address issues, minimizing potential disruptions.

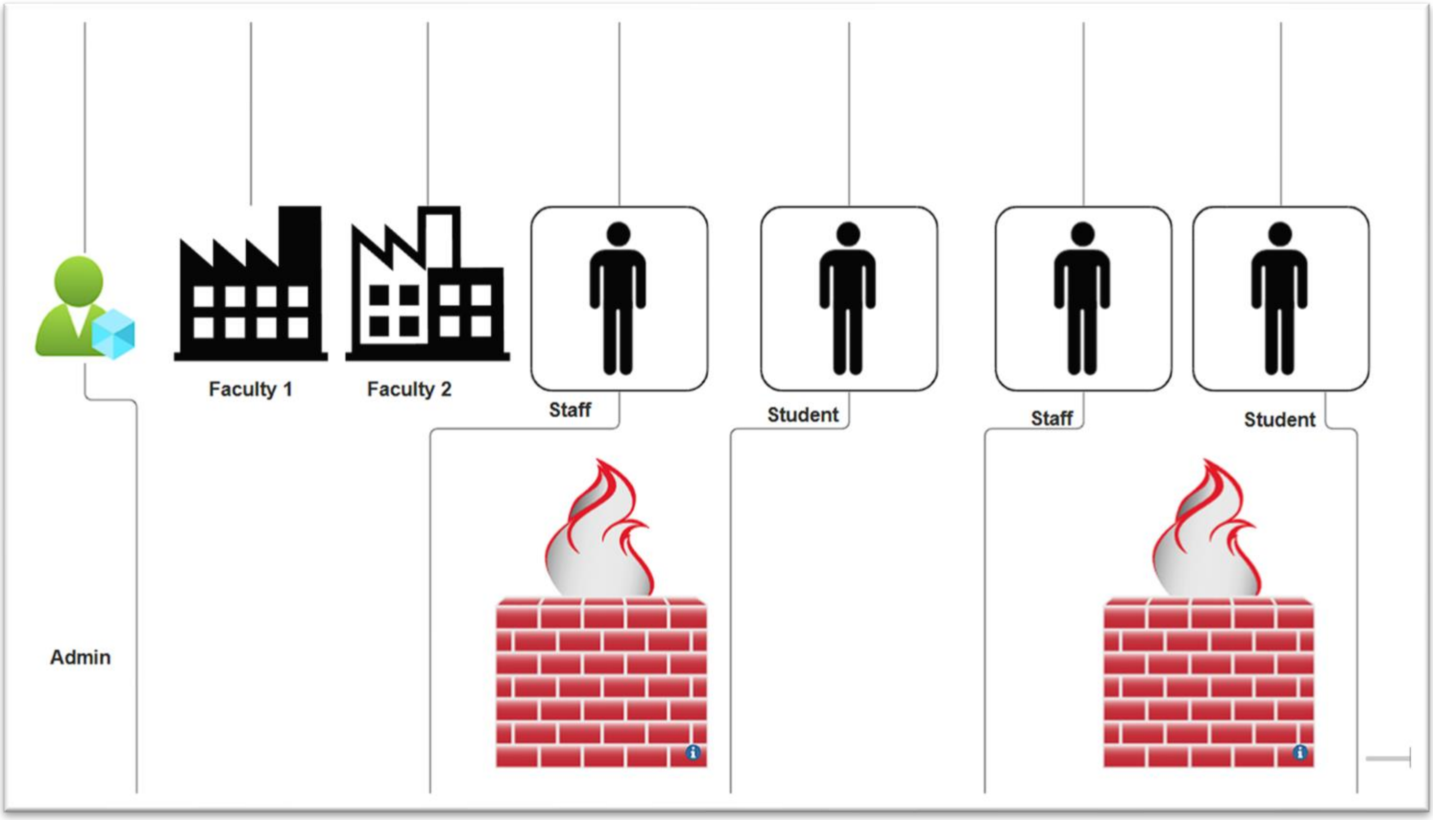
- **Benefits of a Single PoC:**

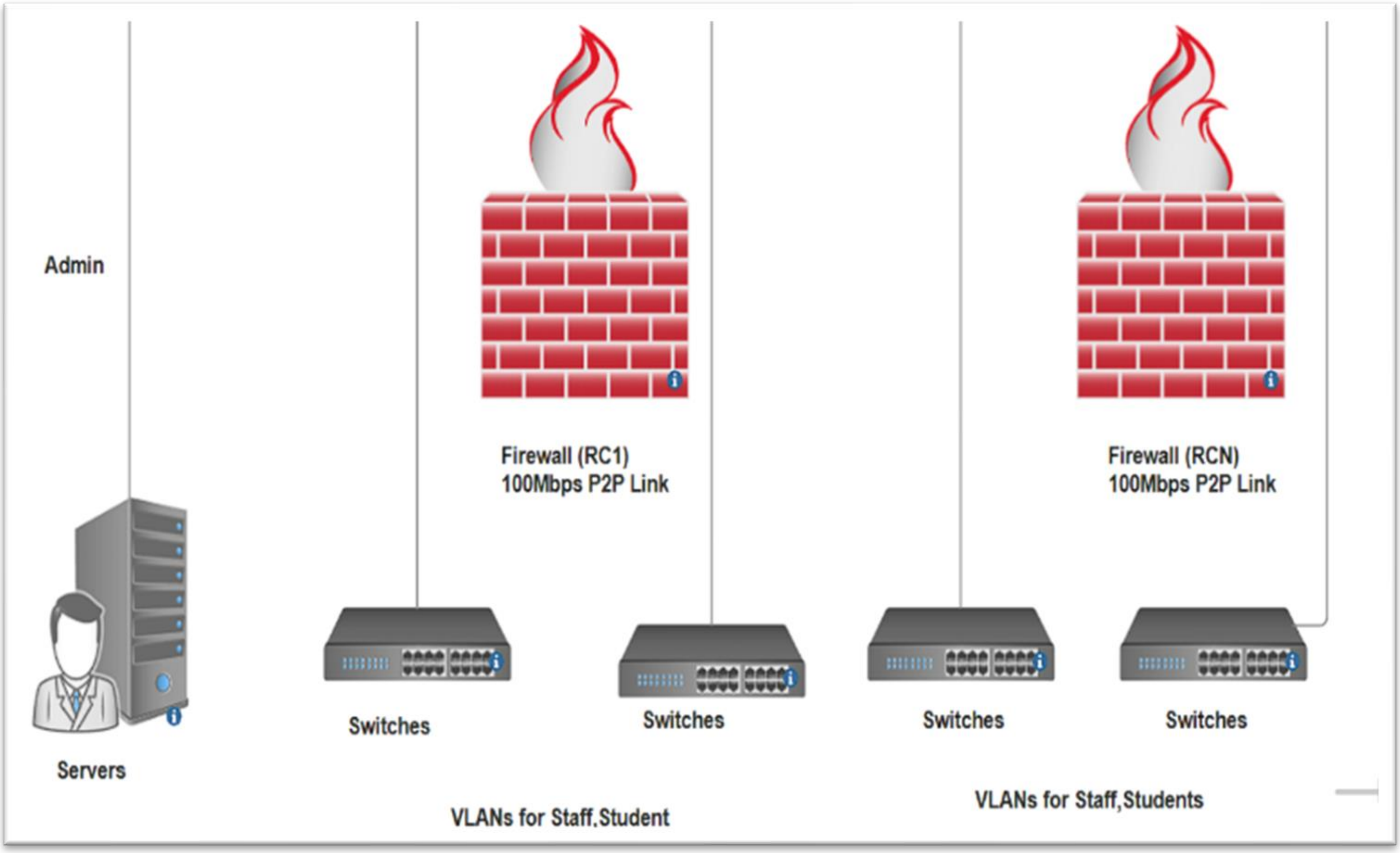
- Centralized Visibility into both network and security aspects allows NUIT to manage and protect its digital assets more effectively.
- Improved Efficiency is achieved by eliminating redundancies and fostering a streamlined operational model, enabling faster and more effective decision-making.
- Faster Response Times to both security incidents and network issues are facilitated by a unified command centre, enhancing NUIT's ability to protect and serve the university community.
- Standardized Practices ensure a consistent approach to network and security management across all campuses, fostering a secure and reliable digital environment for all members of the university.

❖ Network Design Diagram




Internet
1 Gbps Fiber Optic
Main University
Regional Campus 1
Regional Campus 2
Router (HQ)
Router (RC1)
Router(RCN)


Faculty 1
Faculty 2
Staff
Student
Staff
Student
Admin



- **Explanation:**

- The NUIT network is divided into three main segments: Main University, Regional Campus 1 (RC1), and Regional Campus N (RCN).
- The Main University has separate network segments for Faculty 1, Faculty 2, and Administration.
- Each Regional Campus has segments for Staff and Students.
- A central Router (HQ) at the Main University connects to the internet with a 1Gbps fibre optic link.
- Each Regional Campus Router (RC1, RCN) connects to the HQ Router using a dedicated 100Mbps P2P link.
- Firewalls are implemented at each Regional Campus for additional security.
- Switches connect devices within each network segment.
- VLANs (Virtual LANs) can be implemented within each segment to further isolate traffic (e.g., Staff and Students).
- Servers for virtual labs, learning management systems, and staff administration are located at the Main University.

❖ References

- Network segmentation - https://insights.sei.cmu.edu/blog/network-segmentation

concepts-and-practices/

- Network Simulator software – Cisco Packet Tracer

https://www.packettracernetwork.com/

- Network Security planning.

https://www.ibm.com/docs/en/power5?topic=communications-planning-network

security

- Network management best practices -

https://www.egr.msu.edu/~renjian/pubs/network-management.pdf

❖ Individual Contribution

Name	Pu Index no	Contribution
Gunathilaka	10898583	Logic diagram, Network design daigram
Guniyangodage Sandeepa	10898684	Justification of Proposed Technologies
Ganagabadage L Mansith	10899326	Logic design and IP approach, Recommendations
Wanniachchige Fonseka	10899263	Security & Network Management plan, Segmentation/IP addressing approach
Welikadage Botheju	10900327	Implementation of sample faculty networks
Ranasingha Priyantha	10899343	Security & Network Management plan, Segmentation/IP addressing approach