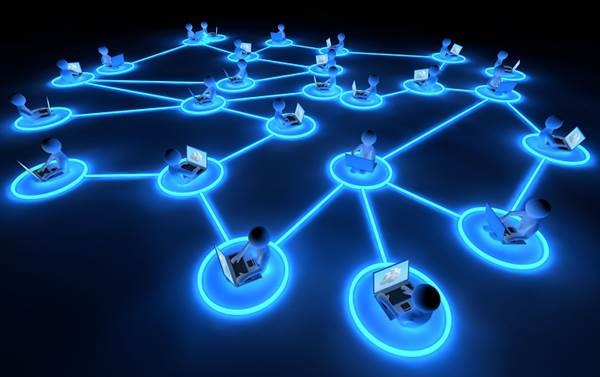
TCP/IP Networking concepts



H.D.C.S Munithunga

Student No : Sa23091184

Year 2 semester 1

DCCN Assignment part 1

Table of Contents

[1. Introduction 3](file:///C:\Users\Vinuya%20Ekanayake\Desktop\SLIITA\dccn\Tcp%20Assignment%201%20Report.docx#_Toc133852673)

[1.1. Security Capabilities 3](file:///C:\Users\Vinuya%20Ekanayake\Desktop\SLIITA\dccn\Tcp%20Assignment%201%20Report.docx#_Toc133852674)

1.2 Use of Load Balancing for efficient data transfer ………………………….3

[1.3. VPN Clients 4](file:///C:\Users\Vinuya%20Ekanayake\Desktop\SLIITA\dccn\Tcp%20Assignment%201%20Report.docx#_Toc133852675)

[1.4. Disaster Recovery Plans 4](file:///C:\Users\Vinuya%20Ekanayake\Desktop\SLIITA\dccn\Tcp%20Assignment%201%20Report.docx#_Toc133852676)

[2. Basic network Design 5](file:///C:\Users\Vinuya%20Ekanayake\Desktop\SLIITA\dccn\Tcp%20Assignment%201%20Report.docx#_Toc133852677)

[3. Network Plan 6](file:///C:\Users\Vinuya%20Ekanayake\Desktop\SLIITA\dccn\Tcp%20Assignment%201%20Report.docx#_Toc133852678)

[4. Devices to be Purchased 7](file:///C:\Users\Vinuya%20Ekanayake\Desktop\SLIITA\dccn\Tcp%20Assignment%201%20Report.docx#_Toc133852679)

[5. Methodology 8](file:///C:\Users\Vinuya%20Ekanayake\Desktop\SLIITA\dccn\Tcp%20Assignment%201%20Report.docx#_Toc133852680)

[6. Maintenance plan and Future Work 9](file:///C:\Users\Vinuya%20Ekanayake\Desktop\SLIITA\dccn\Tcp%20Assignment%201%20Report.docx#_Toc133852681)

[7. References 10](file:///C:\Users\Vinuya%20Ekanayake\Desktop\SLIITA\dccn\Tcp%20Assignment%201%20Report.docx#_Toc133852682)

1. Introduction

The objective of this report is to propose a network design for University of Peradeniya Expansion Plan. The network should meet the functional requirements specified in the project, which are to provide reliable and secure connectivity for the university workers and parents. This report includes a logical diagram of the proposed network, an IP addressing plan, a list of recommended devices to be purchased, a methodology to implement the network, and a maintenance plan.

1.1Security Capabilities

Here the Security capabilities refer to the various technologies ways to protect the network and its data from unauthorized accesses. These capabilities have range of tools to ensure the availability of resources.

1. 1.firewalls- used to check the network traffic, securing unauthorized access and attacks.
2. Virtual Private Network - provide a secure and encrypted connection on untrusted networks. Ensuring that data is protected when traveling between users and the internal network
3. Data Encryption- Data encryption protect data from unauthorized access and prevent interception. This is useful in public network. It is used to secure sensitive data in the network while stored in devices
4. Network segmentation is used in dividing a larger network into smaller network. It helps to improve security policies and reduces the attack by restricting communication in the network.
   1. Use of Load Balancing for efficient data transfer

Load balancing is a technique used to distribute incoming network traffic across different servers. It increases availability, and improve the performance of services. The main goal is to prevent any single server affecting by excessive traffic.

* Load balancers provide traffic management that allow administrators to prioritize certain types of traffic. This implements in traffic policies use to improve performance and meet business requirements.
* load balancers can work to provide failover support to overcome fault tolerance

1.3. VPN Clients

Deployment of VPN Software will Install and configure VPN client on devices used by university staff, students, and other users.

Ensure compatibility on operating systems and devices to provide various user needs.

User Authentication can Implement string authentication mechanisms, such as passwords, two-factor authentication in order to verify user identities before getting VPN access to the network.

Encryption Protocols are used to produce strong encryption protocols, to provide a secure data transmission over VPN c and protect against stealing sensitive data by cyberattacks

Monitoring and Management will employ VPN tools to monitor client connections and produce security policies, such as access controls and session timeouts.

1.4Data Backup and Recovery Plan

A strong data backup and recovery plan is used for maintaining data integrity and availability and ensuring business continuity. The proposed plan includes:

The backup server is a dedicated server within the network architecture. It is in charge of creating and preserving copies of data from various systems and applications. Its primary responsibilities include creating backup copies of primary servers and storage devices on a regular basis known as Data Backup, offering methods for recovering accidentally deleted, corrupted data and organizing, indexing, and maintaining backups of data to guarantee simple retrieval and adherence to retention guidelines

Regular Backups are Scheduled periodic backups of all critical data, applications, and systems to secure storage locations, such as onsite servers or cloud repositories. Backups are Implement a combination of full, incremental, and differential backups to optimize storage space and recovery times.

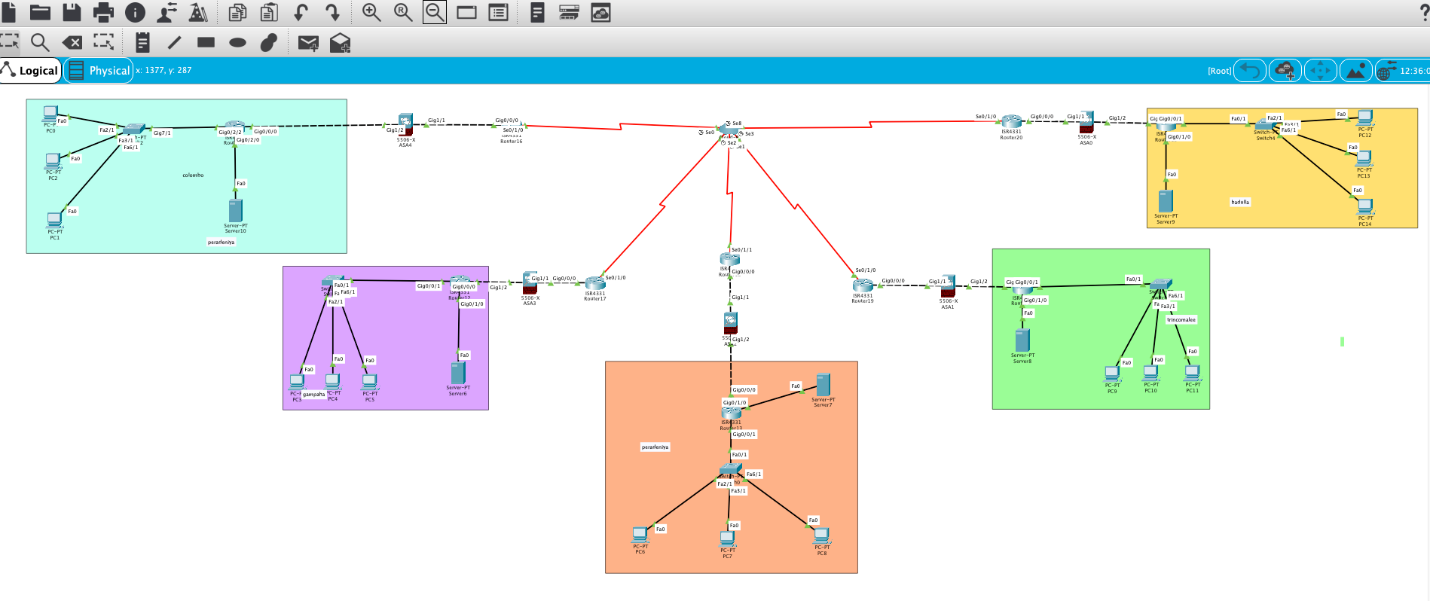
Offsite Storage Store backup copies in secure locations that are separated from primary data centers, to reduce risks associated with physical disasters

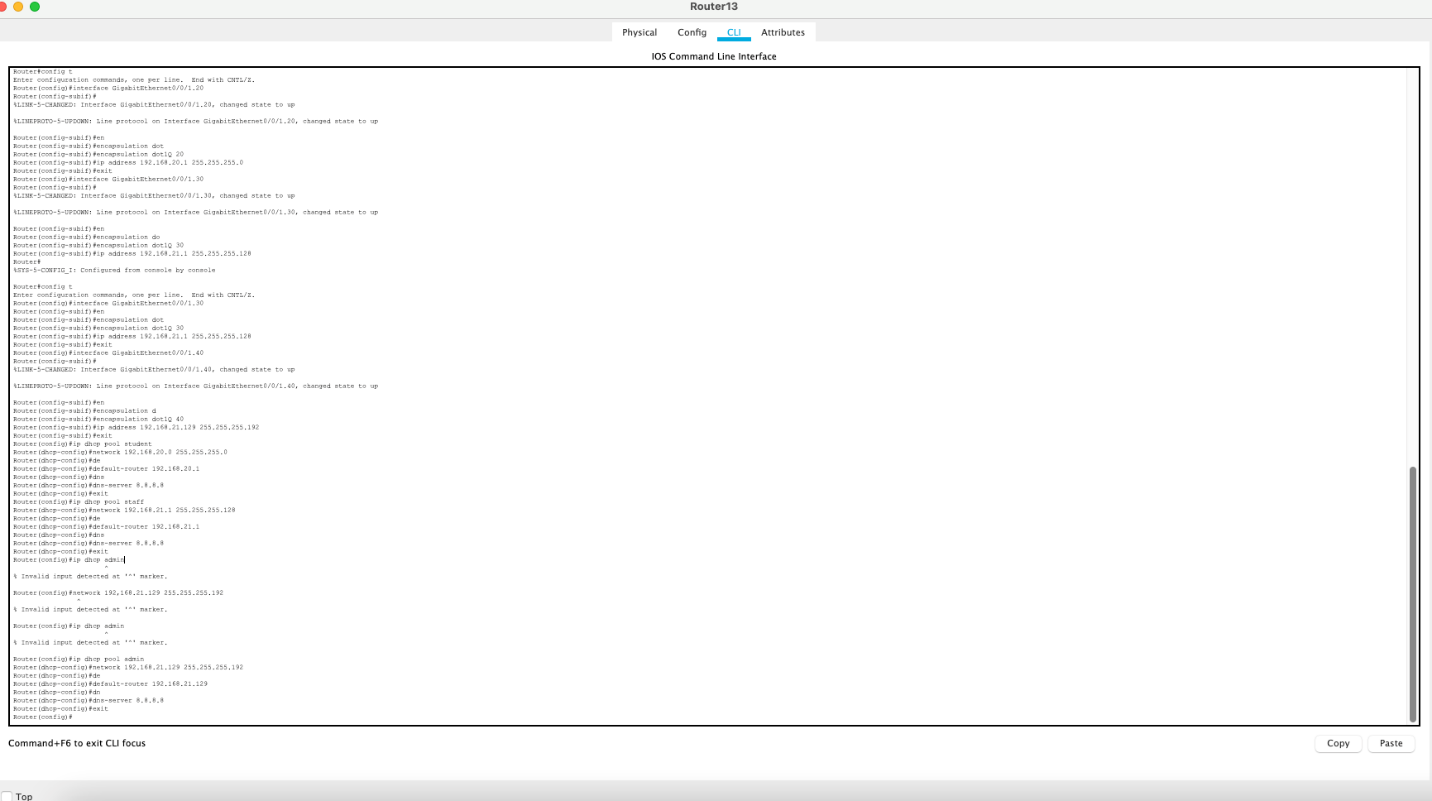
Disaster Recovery Plan is to Develop a disaster recovery plan giving a step-by-step procedure for data restoration in any catastrophic incident like hardware failures or natural disasters.

Conduct regular tests of the disaster recovery plan to make sure its effectiveness

Regularly verification is needed backup integrity and consistency to ensure data recoverability and compliance with regulatory requirements. Perform tests that will restore backup data to validate the restoration process

1. Basic network Design





1. Network Plan

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Host | Subnet | Increment | Network  Address | First Usable Address | Last Usable | Broadcast  Address | Ip Wastage |
| 350 | 255.255.255.0 | 2 | 192.168.70.0 | 192.168.70.1 | 192.168.70.254 | 192.168.71.255 | 164 |
| 150 | 255.255.254.0 | 1 | 192.168.2.0 | 192.168.2.1 | 192.168.2.254 | 192.168.2.255 | 104 |
| 80 | 255.255.255.128 | 128 | 192.168.3.0 | 192.168.3.1 | 192.168.3.126 | 192.168.3.128 | 64 |
| 100 | 255.255.255.128 | 128 | 192.168.3.129 | 192.168.3.130 | 192.168.3.254 | 192.168.3.255 | 24 |
| 40 | 255.255.255.224 | 64 | 192.168.4.0 | 192.168.4.1 | 192.168.4.62 | 192.168.4.63 | 22 |

4.Devices to be Purchased

A black computer tower with open doors

Description automatically generated

Samsung backup server 20 TB - $1025

24 port Gigabit switch (TP-Link TL-SG3428) with 4 SFP slots

A close-up of a switch

Description automatically generated

24 port Cisco switch (TP-Link TL-SG3428) with 4 SFP slots

Cost ; $220



he Gigabit wireless router

Cost ; $120



Network Tool Kit Box

Cost ; $100

5.Methodology

The suggested network architecture will be put into effect using a methodical process . Below shows the steps that will make up the methodology:

Analysis Phase is to Understand the current network setup and need for the University of Peradeniya Expansion Plan.

It evaluates the existing infrastructure and determine IP addresses need. Here we are to identify security and disaster recovery requirements needed.

Design Phase is to create a detailed plan a new network for the analysis.

Here we select hardware and software needed and design network layout.

Develop IP addressing scheme to the network. Check for the security measures.

And mention the disaster recovery strategies.

Implementation Phase is to put the newly designed network plan into action.

First the Install and configure network devices switches, routers and firewalls

Use the cloud infrastructure. Test network functionality and security. Educate the staff about the new network. Document the network configuration

By following these steps, we ensure a transformation to the new network design for the university of Peradeniya’s connectivity and security needs

6.Maintenance plan and Future Work

Maintenance Plan

Regular Updates are needed to keep the operating systems and network devices to protect and improve performance and security.

Can ensure antivirus and anti-malware software through regular updates to protect against evolving threats.

Network Monitoring is a Continuous monitor of the network looking for errors and performance issues

Provide regular training and programs in order to teach the users about security practices, like data protection. This will encourage users to report any security concerns or suspicious activities in the network.

Data and system are Regularly backup and store them securely. Test backups are used to improve integrity and reliability of data recovery processes.

Disaster Recovery Plan is used to ensure business continuity in the network failures or disasters.

Future Improvements:

Threat Detection Systems are used to affect an advanced detections in the systems by AI to identify and provide security to cyber threats more effectively.

Scalability Plan will be Developed to accommodate future growth in the number of users, devices, and data traffic. Use Data Loss Prevention methods to protect data from unauthorized access. User Experience Improvement will use more user-friendly security methods and minimizing disruption to user activities during security processes.

VPNs may integrate to endpoint security solutions to impose security policies and perform continuous monitoring on the endpoint devices for threats and attacks.