SECURE NETWORK TOPOLOGY

Functional Specification

Student: Aaron Morrissey
Student ID: C00239014
Supervisor: James Egan

Contents

Abstract

It has come to the attention of staff members working at ABC Hospital group that their supposed network is seen as lacking in a number of areas and has resulted in them voicing their irritation, thus, as a consultant network engineer it is my duty to do in-depth research on various beneficial technologies and apply them to a simulated virtual network, mirroring that of the hospitals, in order to test and provide solutions to combat this issue so that users and company personnel might experience a higher quality of service.

The purpose of this report is to summarize and highlight the functionality of a distributed network after improvements have been implemented based on my research and testing. Within this report aspects such as core features will be discussed as well as who exactly will have access to what features and why they access to them compared to non-sanctioned users. There is also the question of how these implementations compare to existing instances of organisational networks and whether they are more beneficial and, if so, how to gauge their performance.

Introduction

Currently, the ABC hospital network is comprised of four main sites located in Belfast, Carlow, Cork, and Dublin, that's issue is that its limited capabilities are starting to become more noticeable. With more devices being assimilated into the network and users such as staff and patients adding to the vast amounts of network traffic, this results in the hospitals already weak LAN and WAN infrastructure becoming even more fragile giving rise to negative effects in regard to:

- Connection speed
- Management and Control
- Redundancy and Cost
- Network Security and Reliability

Given the situation, it is my responsible as the consultant network engineer, it should be of the upmost importance to approach this issue by asking myself the question "How might we be able to reconstruct this network to such a degree that it's standards aren't just only on-par with how a modern-day network should act and behave" but also "How might we strive to make its overall performance that of one which exceeds what has been seen to date?".

Deliverable's

Given the current state at which the network currently resides, the desired characteristics we wish for it to incorporate, and exhibit include:

- A high standard of security that does not impede or limit the operational capabilities of other technologies.
- Fast, reliable, and encrypted communications between distributed sites.
- High functioning maintenance and control systems to be monitored and managed from a remote site.
- Incorporate the necessary technologies to achieve the most cost-effective result.

Functionality

Core

It should be noted that even though the ideal outcome for this project would be to achieve an overall quality of industry level network standards, at the end of the day the core functionality of any network is to be simply able to provide end to end IP communications and letting devices recognize and converse with each other regardless of distance.

Secondary Core

Second to communication, other core functions required by the network include:

1. A high level of security to be achieved by adding a multitude of safeguards to ensure that data in any form is protected and safe against any individual who would try to attain it through unauthorized or malicious methods.

    - Allow or deny access to configurations and services based on whether a user or group can authenticate through either correct credential's, privilege level or team/role-based position within the company.
    - Distinguish between whether a packet was sent from a trusted source or spoofed address.
    - Allow for private and secure communication between devices across the network.
    - Multiple Firewalls

2. It's overall reliability to continually function without device or path failure through the aid of various redundant disaster recovery methods and alternative sources of supply.

    - Point in the direction of the best possible path when transmitting data.
    - Provide alternative communication pathways and backup servers in the event of extended maintenance or network failure.

3. Optimal performance of communication by significantly increasing the rate and quality at which it is able to transmit and receive data from one device to another.

    - Accommodate high quality, low jitter for communications such VoIP and video services.
    - Separate traffic based on packet importance, e.g. reserve fastest path for real-time service's such as VoIP through the use of MPLS.

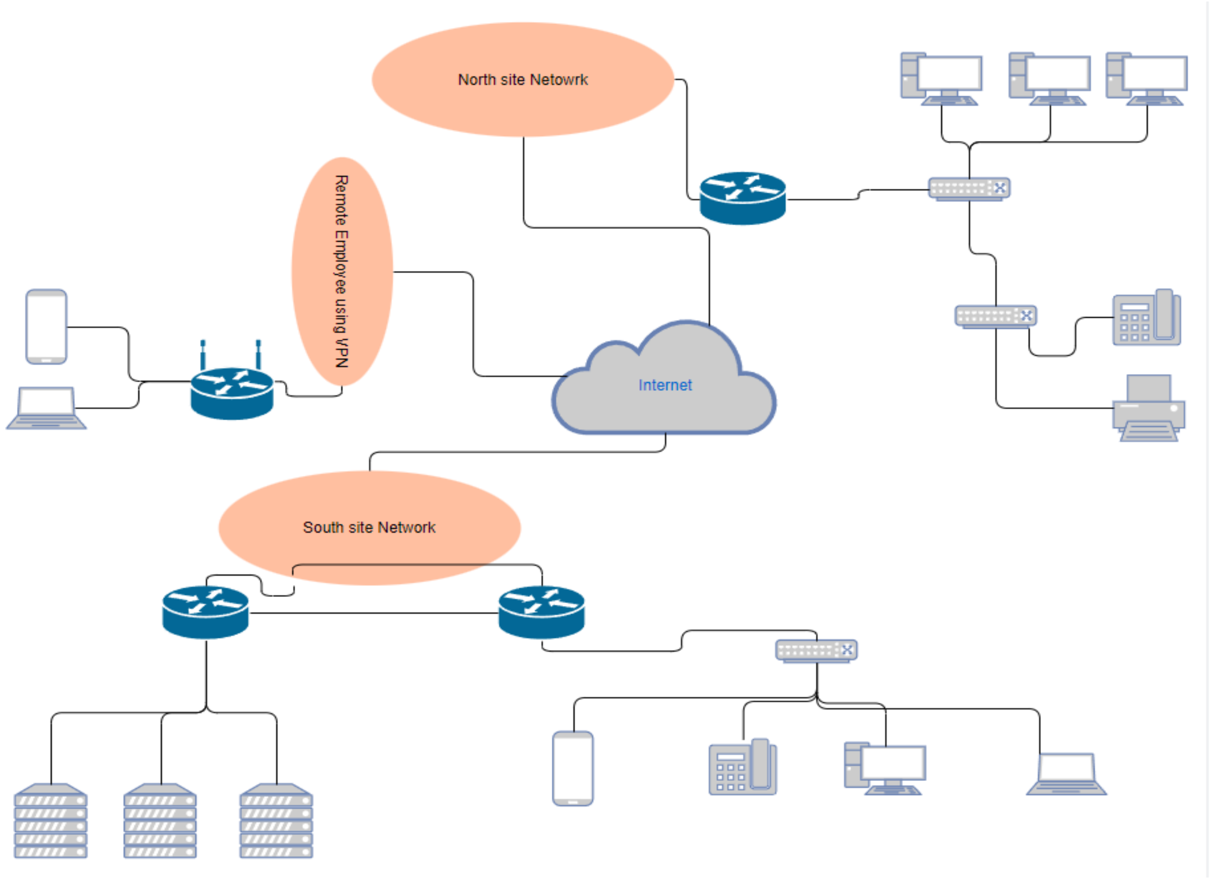
4. Efficient control over the network with the ability to monitor and manage traffic and devices through various methods.

    - Manage devices through automated configuration changes.
    - Use MPLS to place traffic into classes for efficient management e.g. real time = VoIP, best effort = Internet and email etc
    - Acknowledge device status.
    - Detection of errors, anomalies and attacks that have occurred.
    - The logging of events such as errors, auditing and configuring of devices.

Target Audience type

Large Enterprise's

Under normal circumstances the above core features would apply to any business that is serious about its performance and network integrity, however, in this specific case the protocols and technologies that I wish to incorporate such as MPLS are more suited to larger organisations consisting of branches that are geographically spread-out across a region, workplaces that host an exorbitant number of devices and machinery that results in vast quantities of network traffic. A vague example of a such a network would look something like:



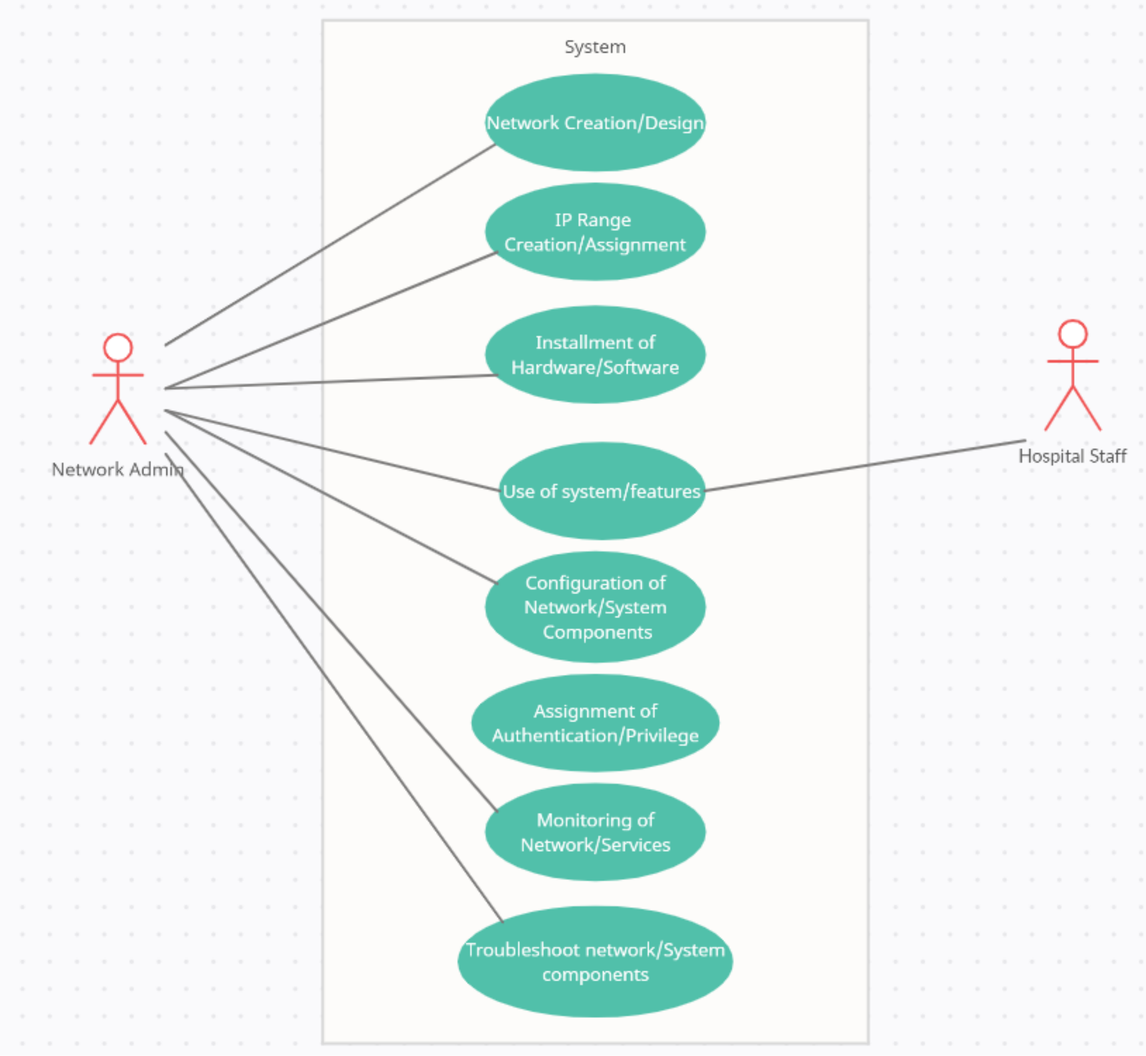
Network Users

Hospital Staff

The majority of the user base belongs to the hospital staff, these individuals have standard mid-level access to the network whose duties and responsibilities grant them the authority to access and use the system for the purpose's of updating patient files, forwarding requested information to other colleague's or sites as well as communicating with them via the company's private email and VoIP services etc.

Administrators & Moderators

It is the administrators and Moderators that have been appointed high privilege level's allowing them to interact with system in a much more influential way. As well as possessing the capabilities of the hospital staff, they have the authority to incite changes and make modifications such as installing and configuring hardware or software, redesigning network layout and IP addressing, reconfigurations of routing protocols and authentication keys, access to device logs and their activities, granting privilege levels to users and groups, permitting or denying types of traffic or IP addresses, normally through ACL's, etc.


System
Network Creation/Design
IP Range Creation/Assignment
Installment of Hardware/Software
Use of system/features
Configuration of Network/System Components
Assignment of Authentication/Privilege
Monitoring of Network/Services
Troubleshoot network/System components
Network Admin
Hospital Staff

Sample Use Cases

Case 1 (Simple connection between devices)

Primary Actor:

Hospital Staff member

Preconditions:

- Machines for topology have been acquired.
- Correct cabling of devices.
- IP addresses and default gateway applied to devices.
  - If the device that the user wishes to commune with is part of a remote site, implement correct routing protocols.

Scenario:

- The user will launch the command terminal on their PC.

- User will issue the ping command to test if connectivity between the two devices is active.

Expected Outcome:

Ping command was successful, and connectivity was established.

Case 2 (Updating Routing Table)

Primary Actor:

Network Administrator

Preconditions:

- Case 1 requirements should be implemented.
- Passwords and privilege levels configured to access device configuration.
- Routers should be configured with Neighbour Authentication.

Scenario:

- Administrator enters password to access configuration mode on a router
- Administrator decides to then update the contents of the routing table.
- Packets, along with an authentication key, will be sent to the other routers in the network to update their routing tables in the form of a message digest.

Expected Outcome:

The receiving routers update their routing tables by using their own key to authenticate the update packets source.

Case 3 (Test redundancy and recovery)

Primary Actor:

Network Administrator

Preconditions:

- Case 1
- Case 2
- Traffic Generator
- Monitoring software

Scenario:

- Administrator continuously sends traffic across network to a specific device.
- Monitoring software is watching the flow and quality of traffic.
- Administrator deliberately disables several interfaces on devices leading to the receiving device to test for redundancy and recovery speed.

Expected Outcome:

The routing tables within the network are automatically updated so that the traffic if diverted to the next best possible path to its destination while the monitoring software records the reconvergence time showing that traffic is once again reaching its destination.

Case 4 (Voice communication)

Primary Actor:

Hospital Staff

Preconditions:

- Case 1
- Case 2
- Case 3
- Configured:
    - VoIP
    - MPLS

Scenario:

- A hospital staff member wishes to communicate with a colleague working at a different site.
- They input the number associated with their colleague's company device into their own.

Expected Outcome:

The neighbouring device can receive the high quality, low jitter call and both staff members are able to commune with one-another.

FURPS

Functionality

The network must be configured in such a way that it is able to correctly distribute and direct the correct types of traffic to their destinations in a secure and efficient manner that does not limit or interfere with other services as well as providing access to high level operations only to those who are authenticated.

Usability

Staff members of the company should find that the network no longer lacks connection speed, that its features are accessible and user friendly and that's its authentication process is easy yet efficient for those wishing to update files and logs.

Reliability

The network must retain the ability to provide a thought-out and cost-efficient disaster recovery plan through means of backup equipment and multiple pathing choices should one be seen as down by means of Vlans, MPLS and MST's.

Performance

The performance of services should be displaying peak optimal standards in regards to efficiency, processing speed, throughput etc. These standards should be noticed when a employee initiates a call to another hospital site with VoIP showing high quality picture and low jitter.

Supportability

The network should have the ability to support the daily workload and traffic associated with large, distributed organisations without it limiting performance.

Project Plan

Plan #	Tasks	Due Date	Result
1	Independent Research	27/11/2021	Research Manual
2	Internal/External testing of routing protocols	27/11/2021	Optimal routing choices for network implementation.
3	First Presentation	16/12/2021	Explain and elaborate about my project to my supervisors.
4	Layout Design research	17/12/2021	Idea of what the network might look like.
5	Independent research on how the network will function	17/12/2021	Functional Specification Manual
Christmas Holiday			

6	First site configurations/Features implemented	28/01/2022	User features a site are operational.
7	Deployment of first site.	28/01/2022	First Hospital site fully implemented and functioning.
8	Second Presentation	28/01/2022	Explain and elaborate about my project to my supervisors.
9	Test features functionality between two sites.	05/02/2022	User features on separate sites are operational
10	Final Report	29/04/2022	Final Report completed and submitted to supervisor.
11	Finished Product	29/04/2022	Final product completed and submitted to supervisors.
12	Project Demo	29/04/2022	Demo the workings of the project to supervisors.