Friendly Limited's Network

Networking coursework

Trevor Wachaga
ID: 13058317
word count:1995

Introduction

For an organisation to be successful, it needs a strong network. Due to the performance issues faced in the old network, this new network design sets out to ensure high performance, scalability, and enhanced security across the network.

This report consists of a reflection of the old network and the requirements needed to make the new network achieve its goal. Following this, the design will be made, and the architecture and security of it will be described so it can be understood. Finally, there will be an addressing scheme to show how the network can be connected.

Reflection of Old Network (assumptions) and the New Requirements

The main issue was that the old network wasn't scalable and was vulnerable. The previous design was a fully centralised network model. This meant that there was a single point of failure, because if the hub failed – which it frequently did – the entirety of the network goes down. There were many collision and broadcast domain issues too.

The first year of the business had 50 employees, now it's year 5 and there are 400 employees. Based on a rate of expansion formula, 40% is the rate meaning that the new network needs to be scalable.

Furthermore, the research and development department have expanded the most since year 1, require the most space and resources, and frequently had performance issues as it delivered data very slowly.

There are some old components that can still be used. The servers, Wi-Fi access points, and the PCs are all high-performance so they can be utilised again. There are copper cables available too, but only used for end devices.

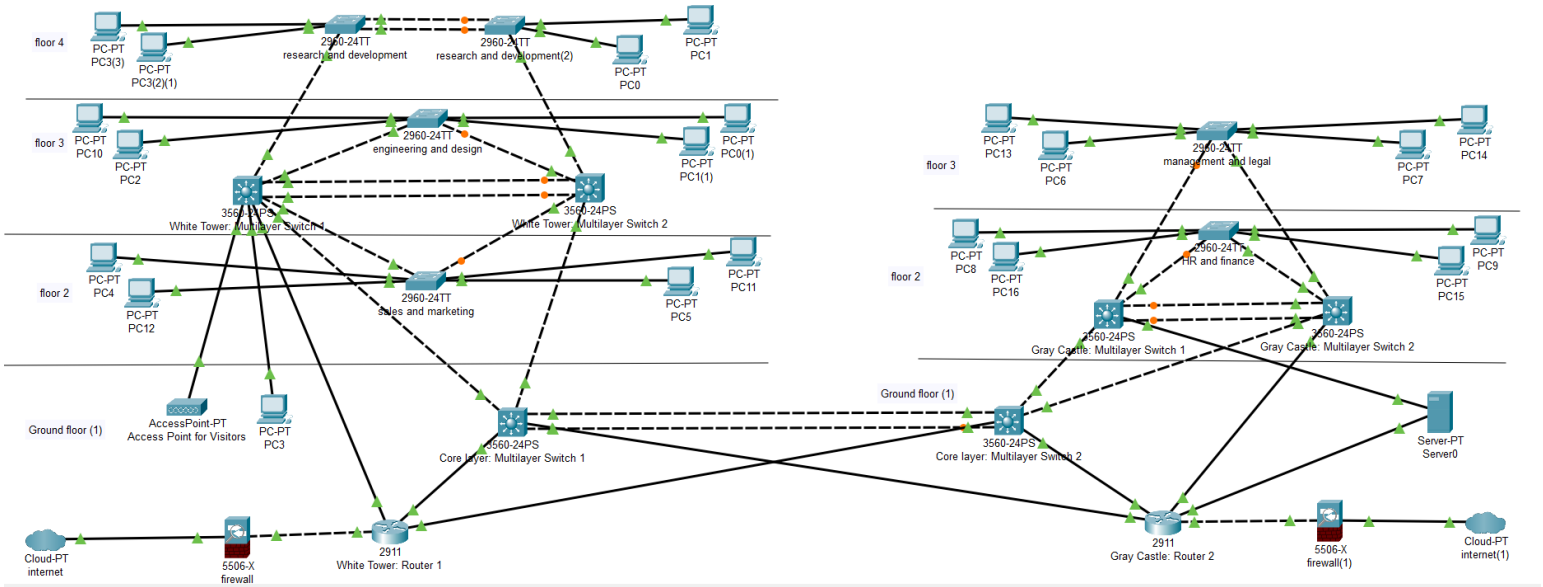
The departments within the same building and different floors must be able to communicate and send data to each other. Also, optimising the spaces in the building is vital so below is a table that shows the new arrangement of the departments.

	White Tower	**Gray Castle**
Floor 4	Research and development: 100	
Floor 3	Engineering: 70 Design: 30	Management: 25 Legal: 10
Floor 2	Sales: 60 Marketing: 50	Finance: 35 Hr: 20
Floor 1 (Ground floor)	Visitor's centre	IT facilities and Server room

Gray castle is "for authorised company personnel only", it makes sense to put departments that deal with the company's and employee's personal data, into Gray Castle.

To summarise, the new site requires a new network model that will be scalable, secure, and high performing.

Network Design



Three-Tier Hierarchical Model

As you can the proposed network design is a three-tier hierarchical network architecture, which is “the preferred approach to network design “ (CISCO, as cited in Omnisecu, n.d.). Furthermore, this model achieves scalability, high performance, and enhanced security. The new design consists of a core, distribution, and access layer, each serving their own purposes.

Core Layer

This is the backbone of the network, which transports data across the network as fast as possible. In the new design, the core layer consists of both routers and multilayer switches, all connected from different ISP’s.

- **Redundancy & Fault Tolerance**
  Having two routers connected to different ISPs provides redundancy, because if one fails, the network remains operational as there is an alternative path. This is vital as it means the network is always available, which wasn’t the case for the old system.
  Similarly, the multilayer switches are interconnected which creates redundancy as traffic can flow through alternative paths if one switch encounters failure.

  Since the old system suffered many faults, such as collision and broadcast domain issues, incorporating switches and routers eradicates this as switches separates the collision domains “so messages that come from devices connected to different ports never experience a collision” (GeeksforGeeks, 2017). Furthermore, routers can break broadcast domains too.

- **Load balancing:**
  Another reason for multiple layer 3 devices in the core layer for load balancing. Packets will be distributed more evenly by optimising bandwidth. This prevents a single device from overloading and causing network congestion.

As data needs to flow between two buildings and 9 departments, it makes sense to have a layer 3 devices as they have the capability to optimise resources and maximise throughput.

The switching method used is store and forward and although it introduces latency, the layer 3 switches ensure entire packets get to their destination at high speeds. Furthermore, the two multilayer switches will use their 10 Gigabit ports for the routers and for the connection between each other. To connect, fibre optic cables will be used as they provide “higher speeds and bandwidth…compared to…coaxial or even copper wires” (UK.rs-Online.com, 2023). Furthermore, the old system used copper cables, which contributed to the performance issues. Therefore, utilising fibre optic cables within the core layer will transport data more efficiently.

These switches also connect to the other multilayer switches in the distribution layer using the 1 Gigabit ports.

Distribution Layer

In this design, the four multilayer switches (2 interconnected in each building) route traffic to the different offices and rooms in each building.

In White Tower, the two multilayer switches route traffic to five departments: sales and marketing on floor 2, engineering and design on floor 3, and research and development on floor 4. In Gray Castle, the two multilayer switches route traffic to four departments: HR and finance on floor 2, and management and legal on floor 3. Each floor has a switch that is shared by departments and every department has a VLAN.

- VLANs:
  The reason VLANs will be used in the new design is to better utilise the ports as it’s better to allow “groups of ports to define logical devices” (Filippas, 2023). It ensures that scalability is always possible as redesigning the network is easier, furthermore as the company expanding, this is crucial.

  The departments require frequent communication so having a VLAN is very logical. Similarly, in Gray Castle the departments have common elements, e.g. management and legal both need to access sensitive data, and they also collaborate frequently on decisions about the company. Furthermore, this is why the departments are grouped as shown in the diagram.

- Redundancy:
  The two multilayer switches are interconnected so traffic still flows if one fails. Furthermore, they both have connections to the core layer so the network will always remain available if one switch stops working. Both switches are also connected to all the layer 2 switches.

Access Layer

This layer provides end devices to network connectivity. Each floor has their own switch connected to the distribution layer.

- Inter-VLAN
  As stated each floor has a switch that is shared by departments, and each department has their own VLAN. Furthermore, Inter-VLAN routing can “route, or send, traffic between VLANs” (Catchpoint, 2023), meaning that departments can communicate with each other.

  Additionally, this can only work if a layer 3 device routes the traffic, which is another reason why there is multilayer switch in the distribution layer. For example, once the inter-VLAN

configurations are made, the sales department (second floor) can send data to the engineering department (fourth floor).

Likewise, in Gray Castle, each department can communicate with every other department in the building. Furthermore, communication between departments is a requirement, which is the main why I have the switches on each floor connected to the multilayer switch, as without it, Inter-VLAN (communication between departments) would not work.

- Intra-VLAN
  On each floor there are different offices for departments. Furthermore, implementing intra-VLAN means that devices part of a VLAN can communicate without going through a router. For instance, all devices in the design department can communicate among themselves without having to worry about traffic being router outside the design department's VLAN to reach a design department device. Furthermore, this reduces unnecessary traffic.

- EtherChannel
  Research and Development department suffered from performance issues in the old network. Furthermore, as a precaution an EtherChannel is used as the "the logical link provides increased bandwidth and redundancy, as well as improved load balancing" (GeeksforGeeks, 2018). There will be load balancing as they have the biggest department and share the most resources. As well as providing redundancy, the links are also faster meaning that the company don't need to worry about performance issues anymore.

Security Aspects and Measures

Before reaching the router, there is a firewall present as it can control and monitor traffic. They can filter out traffic that looks suspicious and they are the main reason why threats will be lessened in this network. The reason for its placement is a security measure because it stops threats from reaching the internal network and as there are two (one for each building), there is extra safety.

Access Control Lists (ACLs):

Throughout the network there will be many ACLs primarily within the switches.

- **Internet Traffic**: Multilayer switch in White Tower's distribution layer will have a rule stating that visitors can connect to the network, but only for the internet and not other network areas. This lessens the chance of attacks happening. The visitor's centre will have workstations and certain websites and services will be blocked.
- **VLANs**: communication between departments is controlled. Rules deciding to allow or deny communication will be constantly switching. It can't be kept on 'allow' for the whole time as that is a security concern because if an attacker ever gets a hold of a device in one department, it can attack the whole network. Furthermore, only under the company's circumstances can different VLANs can communicate.
- **Port Securit**y: since switches are capable of learning mac addresses of their ports, it means that unregistered devices won't be able to connect to them. This increases security as it stops unauthorised devices, which are potentially dangerous, from accessing the network.

VLANs: (configurations)

- **Intra-VLAN**: VLANs will be configured so it ensures a department's traffic doesn't flow outside of their VLAN just to communicate with a device within their network. Furthermore,

this is a security measure as it enables isolation and control, and if a security breach ever occurs, it stays within the VLAN.
Another configuration will be set so that certain users have more access to information or resources. This is a security measure as some admin users in each department need higher privileges compared to the rest of the staff. If less

More additions to network:

- For the routers, Open Shortest Path First protocol will be used as it is “more suitable for serving large, heterogeneous internetworks”. Furthermore, the network is mid-sized right now, but as it is expanding it will get bigger meaning OSPF configuration will be used.

- All the layer 3 devices in the network will incorporate SNMP which is “used to monitor and manage network devices connected over an IP”. If an error ever occurs then it’s extremely easy to check where it’s coming from. Since it’s a big network across two buildings, this protocol helps to point the error out.

- Dual power supplies will be used for the switches. Each one can work on their one just in case one fails. They will also be configured for load balancing, especially when expansion of the company happens.

Addressing Scheme

Device (connection from)	**VLAN**	**IP Address**	**Subnet Mask**	**Host Range**	**Subnet**
Router 1 (From ISP)	N/A	192.168.1.1	255.255.255.252	N/A	N/A
Multilayer switch 1 (in core layer, from Router 1)	N/A	192.168.1.2	255.255.255.252	N/A	N/A
Multilayer switch 2 (in core layer, from Router 1)	N/A	192.168.1.3	255.255.255.252	N/A	N/A
Router 2 (From ISP)	N/A	192.168.1.5	255.255.255.252	N/A	N/A
Multilayer switch 1 (in core layer, from Router 2)	N/A	192.168.1.6	255.255.255.252	N/A	N/A
Multilayer switch 2 (in core layer, from Router 2)	N/A	192.168.1.7	255.255.255.252	N/A	N/A
White Tower Multilayer switch 1 (From core layer multilayer switch 1)	N/A	192.168.1.10	255.255.255.252	N/A	N/A
White Tower Multilayer switch 2 (From core layer multilayer switch 1)	N/A	192.168.1.14	255.255.255.252	N/A	N/A
White Tower Multilayer switch 1 (From router 1)	N/A	192.168.1.11	255.255.255.252	N/A	N/A
White Tower Multilayer switch 2 (From router 1)	N/A	192.168.1.12	255.255.255.252	N/A	N/A
White Tower **Access Layer Switch 1 SALES department**	10	192.168.10.0	255.255.255.0	192.168.10.1 - 192.168.10.254	192.168.10.0/24
White Tower **Access Layer Switch 1 MARKETING department**	20	192.168.20.0	255.255.255.0	192.168.20.1 - 192.168.20.254	192.168.20.0/24
White Tower **Access Layer Switch 2 ENGINEERING department**	30	192.168.30.0	255.255.255.0	192.168.30.1 - 192.168.30.254	192.168.30.0/24
White Tower **Access Layer Switch 2 DESIGN department**	40	192.168.40.0	255.255.255.0	192.168.40.1 - 192.168.40.254	192.168.40.0/24
White Tower **Access Layer Switch 3 RESEARCH & DEVELOPMENT department**	50	192.168.50.0	255.255.255.0	192.168.50.1 - 192.168.50.254	192.168.50.0/24
Gray Castle Multilayer switch 1 (From core layer multilayer switch 2)	N/A	192.168.1.18	255.255.255.252	N/A	N/A
Gray Castle Multilayer switch 2 (From core layer multilayer switch 2	N/A	192.168.1.22	255.255.255.252	N/A	N/A
Gray Castle Multilayer switch 1 (From router 2)	N/A	192.168.1.19	255.255.255.252	N/A	N/A
Gray Castle Multilayer	N/A	192.168.1.20	255.255.255.252	N/A	N/A

switch 2 (From router 2)					
Gray Castle **Access Layer Switch 1** **HR department**	60	192.168.60.0	255.255.255.0	192.168.60.1 - 192.168.60.254	192.168.60.0/24
Gray Castle **Access Layer Switch 1** **FINANCE department**	70	192.168.70.0	255.255.255.0	192.168.70.1 - 192.168.70.254	192.168.70.0/24
Gray Castle **Access Layer Switch 2** **MANAGEMENT department**	80	192.168.80.0	255.255.255.0	192.168.80.1 - 192.168.80.254	192.168.80.0/24
Gray Castle **Access Layer Switch 2** **LEGAL department**	90	192.168.90.0	255.255.255.0	192.168.90.1 - 192.168.90.254	192.168.90.0/24

To accommodate the design, above shows the addressing scheme used. I have gone with using Ipv4, due to its simplicity. Even though it's an old address scheme, it still useful.

Due to how familiar it is, it makes it easy to understand and implement. Furthermore, it's compatible with a large number of devices and software. Moreover, if there are any issues, it's easy to find a solution as there are more resources to learn from compared to Ipv6

The choice to use separate subnets for each department is due to having VLANs, but also because it enhances security. Features, such as ACLs and rules, can be implemented better in the subnets. Additionally, as the company is expanding, the network needs to be scalable. Furthermore, this addressing scheme accommodates for expansion and if changes are necessary, they can be easily implemented. Also, using a subnet mask of 255.255.255.0 for each department allows for 254 useable hosts, meaning it's more than enough to deal with each department.

References

Catchpoint. (2023). *Inter-VLAN Routing: Configuration Examples*. https://www.catchpoint.com/network-admin-guide/inter-vlan-routing

ComputerNetworkingNotes. (2021, May 4). *Access, Distribution, and Core Layers Explained*. https://www.computernetworkingnotes.com/ccna-study-guide/access-distribution-and-core-layers-explained.html

Filippas, John. (2023, September 20). Switches [PowerPoint slides]. Aula. https://files.coventry.aula.education/6d98ab6392c1ae5cec2f58e885a78be4l1.0_switches.pdf

GeeksforGeeks. (2018, May 3). *EtherChannel in Computer Network*. https://www.geeksforgeeks.org/etherchannel-in-computer-network/

Omnisecu. (n.d.). *Cisco Three Layer / Three-tier Hierarchical Network Model*. Omnisecu.com. https://www.omnisecu.com/cisco-certified-network-associate-ccna/three-tier-hierarchical-network-model.php

UK.rs-Online.com. (2023, January 30). *A Complete Guide to Fibre Optic Cables*. https://uk.rs-online.com/web/content/discovery/ideas-and-advice/fibre-optic-cables-guide