Yotsuba Network Design Brief

360CT - Advanced Network Management and Design

By
James Thomas - 9195071
Liam Smith - 8452270
Alexander Collins - 9442540

Contents

1. Introduction

2. Requirements and Assumptions

2.1 Expansion

Yotsuba Group is a company experiencing rapid growth, hence the need for their new office space. It is assumed that this rapid expansion is to be around 10-20 (May need to be more scaleable) new employees per year. Because of this, there is a strong requirement for scalability, so the network can cope with this growth and there are no detrimental effects on network performance. It should be kept in mind that the selection of devices and routing protocols should support this need for scalability.

2.2 Network Speeds and Bandwidth

Research showed that private internet for the greater Tokyo region had available speeds in the range of 10Mbps to 1Gbps. It is assumed that enterprise internet speeds will be within a similar range and that the Yotsuba Group will be purchasing at the top range. Therefor a 10Gbps connection will be used for the designs.

2.3 Employee breakdown

As no information on individual department employee count was provided it has been assumed based on departmental needs.

- Research and Technology - 50 employees
- Financial Planning - 20 employees
- Sales - 34 employees
- Material and Design - 50 employees
- Personnel - 10 employees
- Planning and Manufacturing - 60 employees
- Legal and Accounting - 10 employees
- Marketing - 20 employees
- IT - 16 employees
- Department Head and Assistants - 16 (8+8) employees

2.4 Cisco in Japan

The network will be using Cisco hardware, some of which will be transferred from the old building. Cisco press release demonstrates how the company plans to transition further into Japan through an agreement between the Japanese Government and Cisco on mass-scale digitalisation projects (Cisco, 2021a).

2.5 Physical Office Dimensions

For floors U1, U2, G, 1, 2, 3, 4, 5, 6: 30mx50m - 64, 7m2 pp Floor 7: 50mx20m - 16 Floor7 Balcony: 50mx10m
The space provided to each employee workstation area was calculated via an online tool (von Piekartz, 2019).

2.6 Underground Carpark

We are assuming that the two-floor underground car park does not currently have a good mobile signal and therefore, Wi-Fi APs could be implemented underground. This does depend on the budget of the organisation though because it is not necessarily something that is needed but would be helpful for employees who have parked underground as they can still make calls, send emails or do other work from their cars.

2.7 Previous Devices

Explain that old devices have been bough over, more detailed explaination in section 3.

2.8 Extra Devices

something something something

2.9 Previous Security Threats

The Yotsuba Group reported a number of security incidents in the last 6 months. These have been assumed below.

2.9.1 IP Theft

The company had some intellectual property stolen from a physical attack on the servers within the company premises, the attackers were not found or apprehended as the security was not to standard. This attack was made possible by a lack of physical security measures on there network infrastructure.

2.9.2 Internal Breach

30% of attacks come from employee's within the companies, some data was accessed by departments who has access to other parts of the organisation that they should not have had. A lack of access control was the cause of this attack.

2.9.3 Identity Theft

An external attack left the customer database held by the company open and accessible to the attackers, this in turn was used to ciphon their data and initiate fraud through loan applications under customer names.

3. Physical Network Design

3.1 Devices

3.1.1 Workstations

It is assumed that all workstations in use have been bought over from the old branch to reduce on cost. The only upgrade that would have to be made to each workstation is the installation of an SFP+ network adaptor. The recommended PCI expansion card is the *ASUS 10GbE SFP+ PCIe 3.0 Network Adapter*. This recommendation is due to high reviews and a reputable manufacturer.

3.1.2 Servers

Any servers needed in the network such as email, DNS or vpn will be generic Linux based draws stored in the server room. Inside the network these servers will be placed within the DMZ area.

3.1.3 Wireless Access Points (WAP)

The Cisco Catalyst 9136 WAP has been chosen for its ability to use WiFi 6, further future-proofing our network solution.

3.1.4 Media Converter

When applicable for use the TP-Link MC220L media converter will be used to allow for use of copper cabling. An example of this use case would be the connection from switch to WAP as the WAP does not have an SFP+ port.

3.1.5 Layer 3 Switch

3.1.5.1 Chassis - C4506-E

It has been assumed that this is a switch that has been bought over from the old building to save on costs. It is an older model that is no longer sold but is going to be supported by Cisco until 2025 (Cisco, 2019).

3.1.5.2 Line Card - WS-X4712-SFP+E5

This line card has been chosen because it can handle the speed of the network while being able to fit multiple in the chosen layer 3 chassis.

SKU	Ports	Speed	Connector
WS-X4712-SFP+E5	12	10GBASE-R	SFP+/SFP

3.1.6 Layer 2 Switch

3.1.6.1 Chassis - C9404R

This chassis has been chosen as it is the correct size needed to fit two supervisor cards and two line cards. This allows for the correct number of ports as well as additional for company expansion. Going any larger would not be beneficial and cost more.

3.1.6.2 Line Card - C9400-LC-48XS

This line card has been chosen for the access layer switch as we can fit two of them in the chosen chassis. This will provide enough ports to cover the existing devices on each floor as well as any new devices bought in due to expansion.

SKU	Ports	Connector	Speed	Total Needed
C9400-LC-48XS	48	SFP/SFP+	1/10Gbps	2

3.1.6.3 Supervisor Card - C9400-SUP-1XL-Y

Allows for 10Gbps on each port.

3.1.7 Router

Cisco 4000 Series Integrated Services Router

3.1.8 Firewall

Cisco Firepower 4125

3.2 Wiring

A full fiber solution will be employed for this network to account for future proofing and to reduce noise on the network.

3.2.1 Multimode Fiber - OM4

The current network will be 10GBASE-SR, using OM4 fiber cables. Using OM4 fiber will give us options to expand to 40GBASE-SR or 100GBASE-SR in future also. As the solution planned for this building is mostly copperless, OM4 cables will run between all three layers of our network model. While the distance of 550m at 10Gbps for OM4 is overkill for a 7 story building, the allowance for higher distances at higher speeds (100m at 100Gbps) will be good for future-proofing our solution. The cost of fiber has been decreasing steadily over the past years, due to this there will not be much of a difference between the cost of copper and fiber ethernet solutions. The only additional cost over a copper solution will be the installation of fiber network adaptors in workstation PCs.

Designation	Distance (m)			
	1000BASE-SR	10GBASE-SR	40GBASE-SR	100GBASE-SR
OM1	300	33	N/A	N/A
OM2	600	82	N/A	N/A
OM3	1000	300	100	100
OM4	1100	550	150	150
OM5	1100	550	150	150

Table 3.1: *Table of distances for Multimode Fiber cables.*

3.2.2 Uninterruptible Power Supply

3.3 Device Placement

3.3.1 Patch Pannels

Patch pannels will be placed on each floor to house access section L2 switches. This allows for the creation of several points of failure, as opposed to a single point of failure of storing all switches in the server room.

3.3.2 Ground Floor

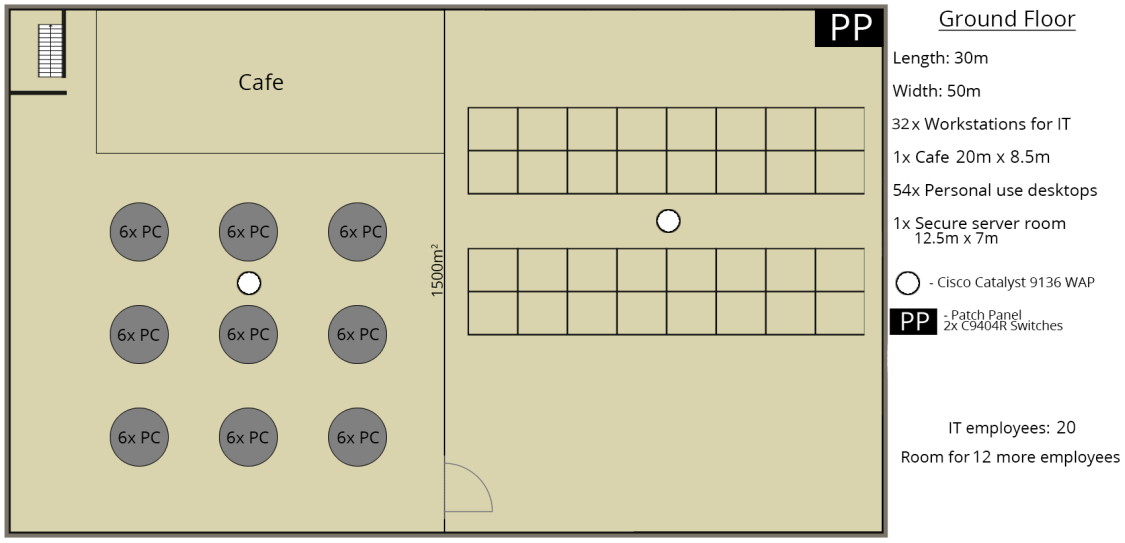

Figure 3.1: *Ground floor plan*

3.3.3 1st Floor

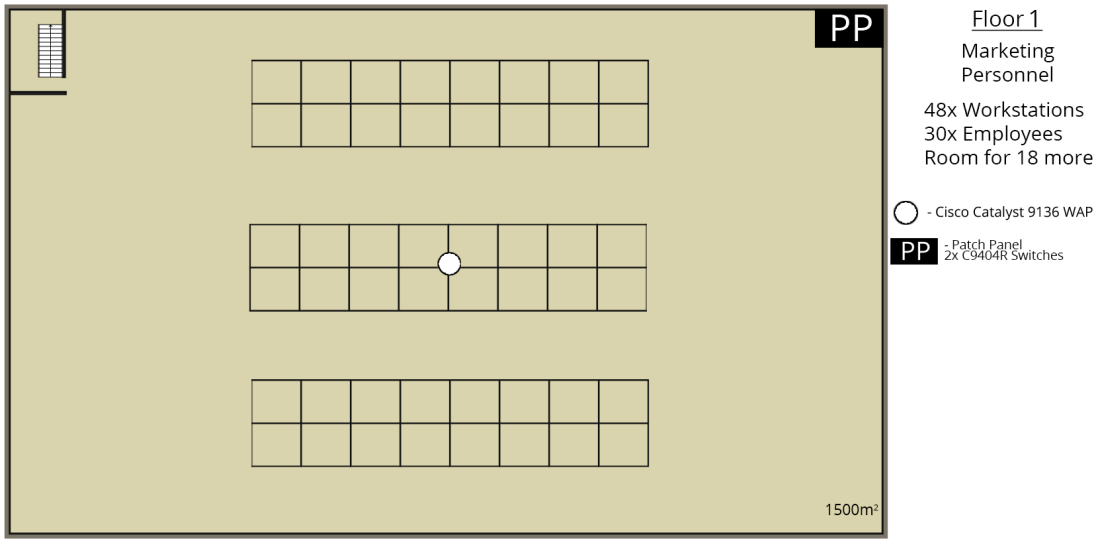

Figure 3.2: *1st floor plan*

3.3.4 2nd Floor

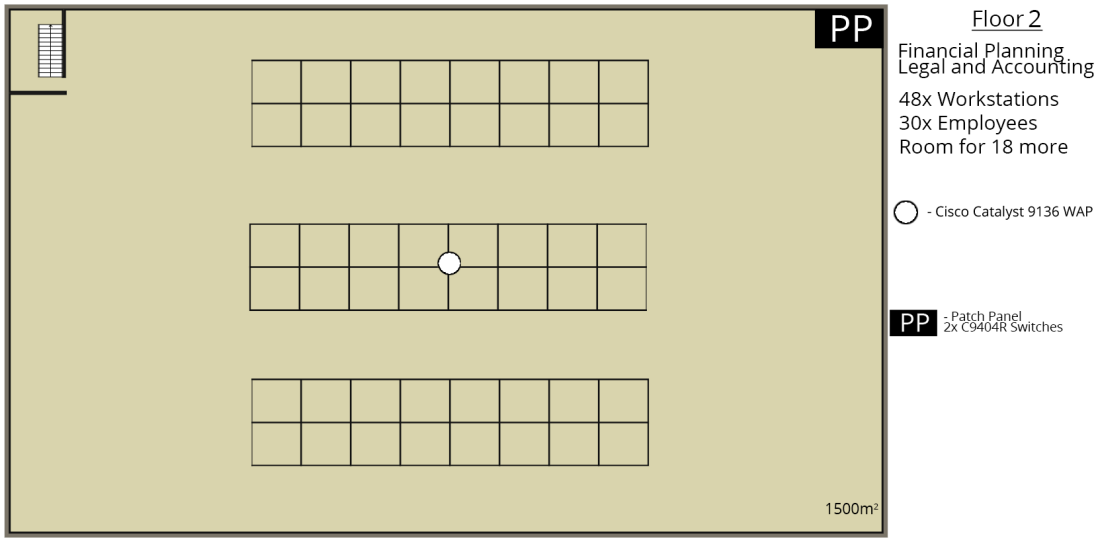

Figure 3.3: *2nd floor plan*

3.3.5 3rd Floor

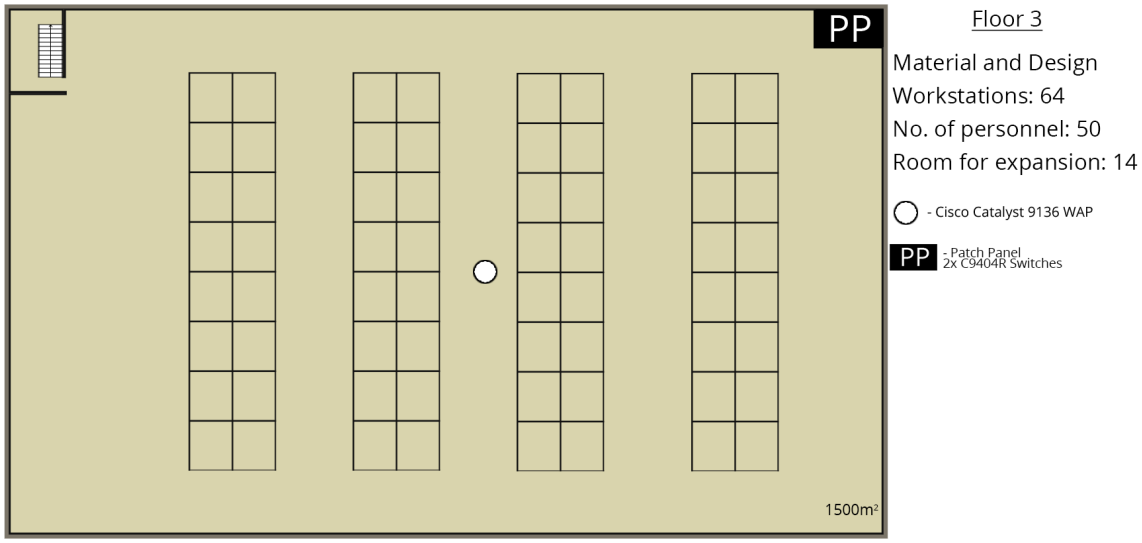

Figure 3.4: *3rd floor plan*

3.3.6 4th Floor

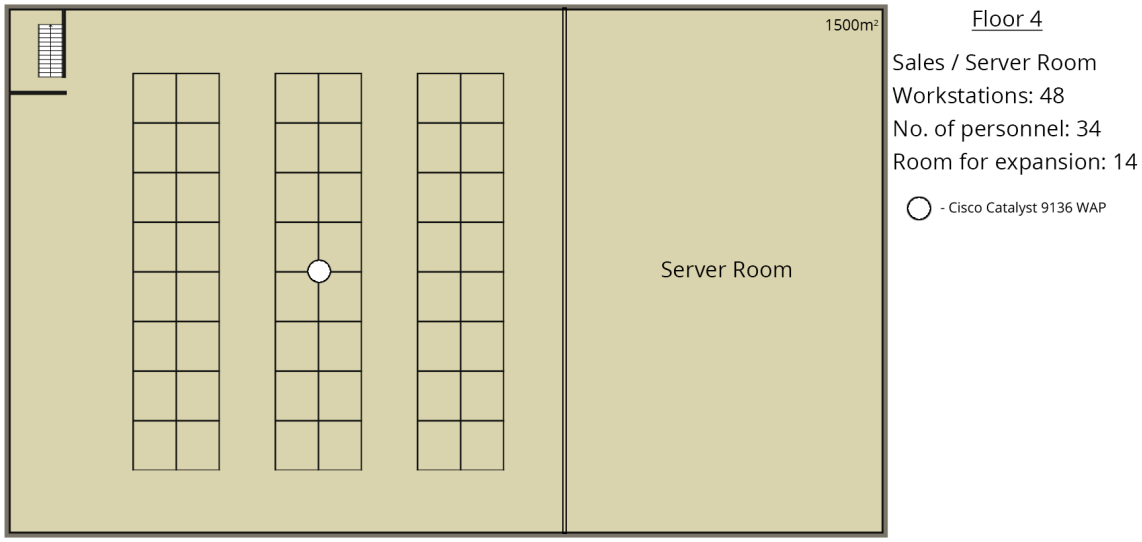

Figure 3.5: *4th floor plan*

Explain why server room here

3.3.7 5th Floor

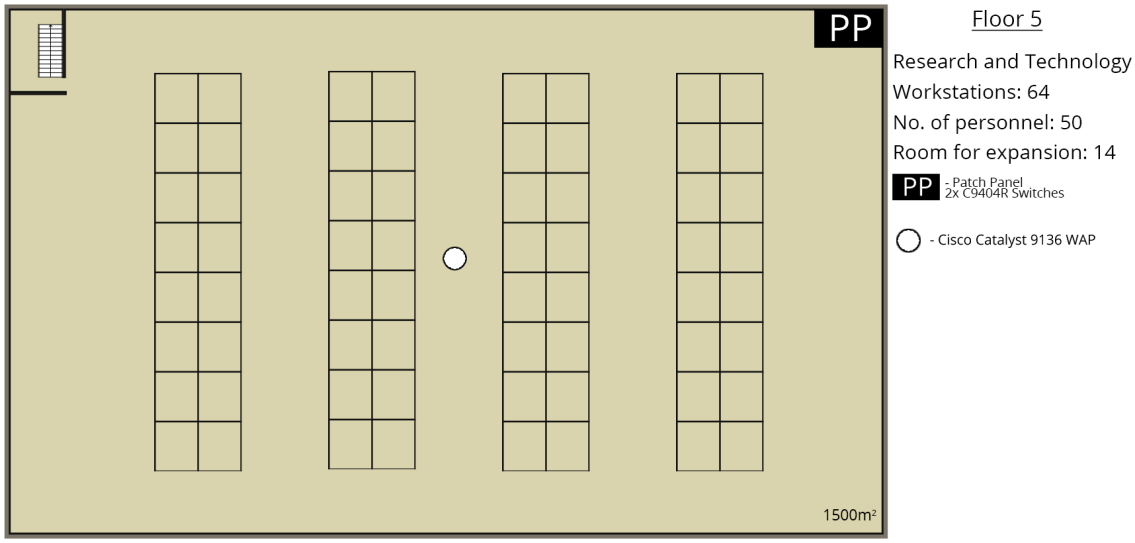

Figure 3.6: *5th floor plan*

3.3.8 6th Floor

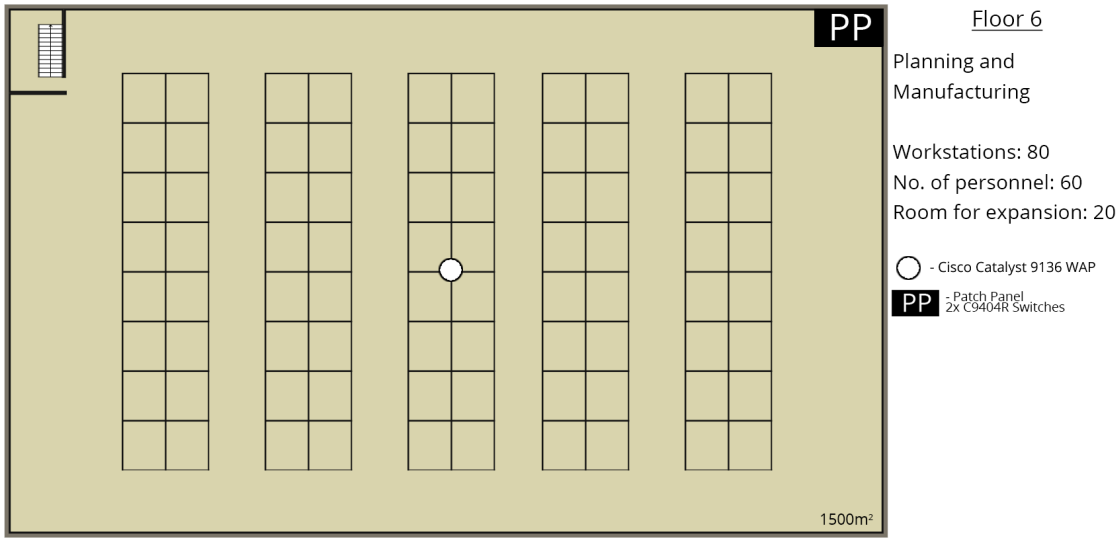

Figure 3.7: *6th floor plan*

3.3.9 7th Floor

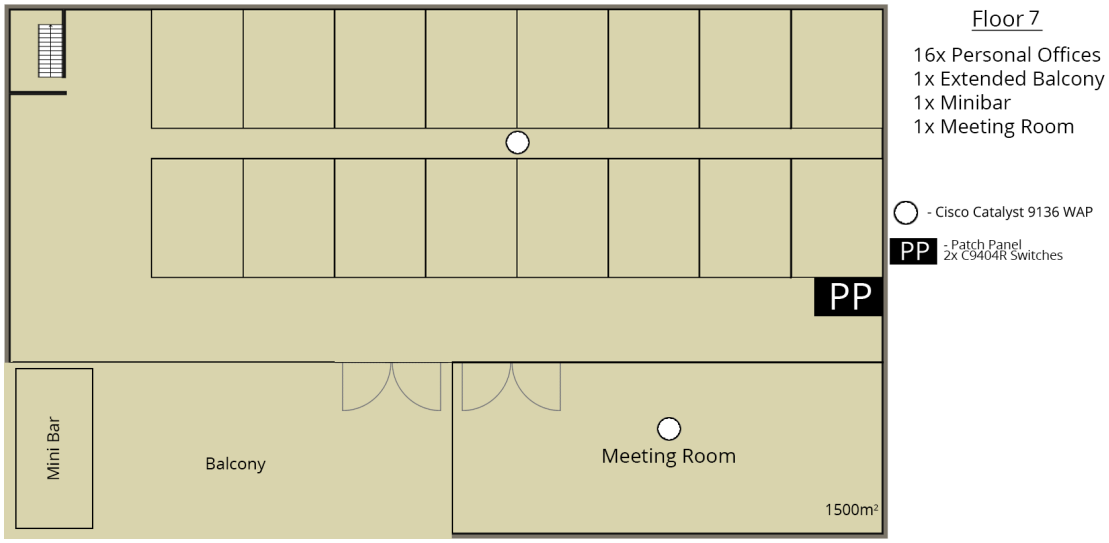

Figure 3.8: *7th floor plan*

3.3.10 Server Room

4. Logical Network Design

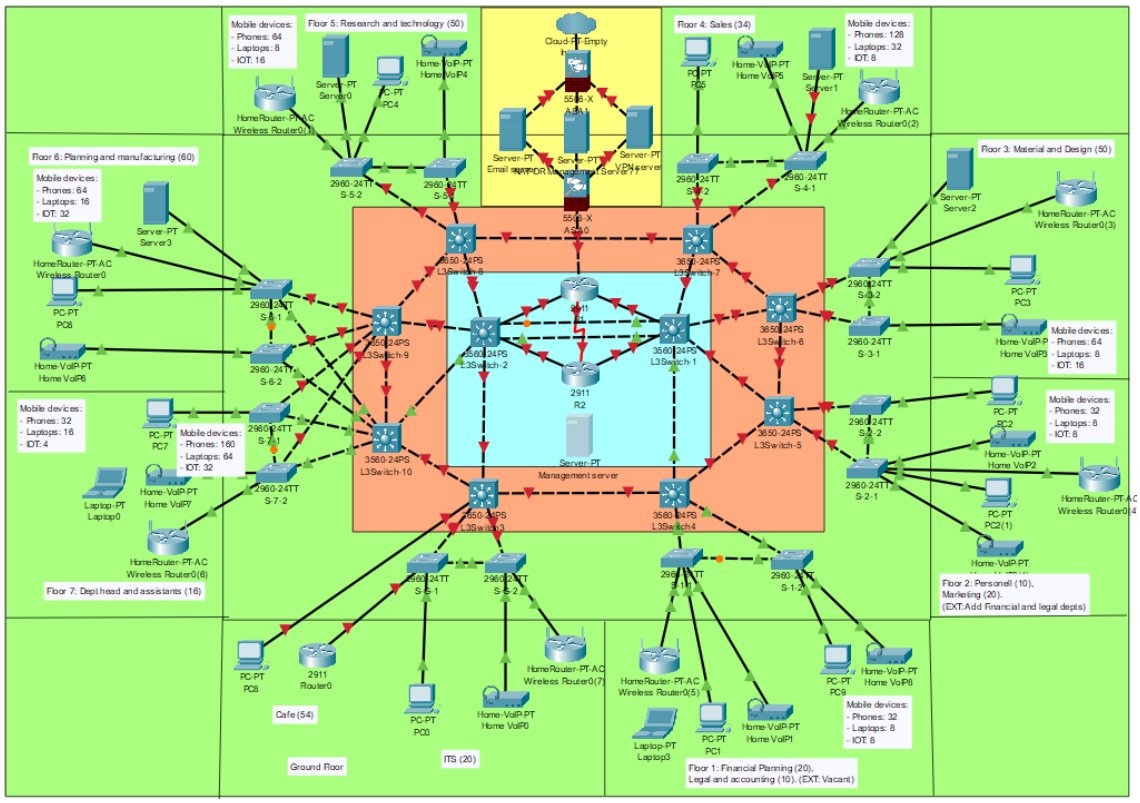

Figure 4.1: *A Network Design produced in PacketTracer.*

4.1 Justifications

The network diagram presented is a logical representation of the network being proposed. It is based on the assumptions of implementing the devices discussed earlier, as well as being secure and accessible for those who require it. See appendix section A for a guide to understanding the format.

4.1.1 Server connections

- Management server: This server will be established as a core device that will provide a platform for managing the entire network, this device is only accessible from within the network itself and is provided access control mechanisms via R2.

- Email and VPN servers: Located within the DMZ, these servers are highly secured due to their increased risk of being attacked by entities attempting to contact them. They provide services to those working away from the office and help to manage the communication in and out of the network.
- Department servers: The departments that have dedicated servers are connected to the same switches to make sure they are secure and accessible

4.1.2 Topology

This design incorporates a hybrid mix of topologies to achieve the aim of being robust and tolerant to different types of operational problems. The mesh/ring structure of the core and distribution layers allows alternative paths and load balancing between the backbone devices of the network. The fully meshed connections between distribution and core layer switches gives a similar function, however with more redundancies.

4.1.3 External facing router

R1 is the router that is closest to the internet, it is behind the firewalls and connected to all components of the network via multiple links. It is heavily secured and monitored.

4.1.4 Wireless access points

Each department has their own WAP and block of IP addresses in order to divide the network for security purposes.

4.1.5 Private addressing scheme and implementation

To provide the most addresses for the network we are using NAT/PAT, this private addressing allows us to be wasteful, and we have addressed the network accordingly. Each subnet has 254 addresses which is more than enough to consider expansion.

5. Addressing Scheme

5.1 Scheme

Floor	Section	Address
G	IT	10.0.1.0
	Cafe	10.0.2.0
	Wireless	10.0.3.0
	Phones	10.0.4.0
1	Financial Planning	10.1.1.0
	Legal & Accounting	10.1.2.0
	Wireless	10.1.3.0
	Phones	10.1.4.0
2	Personnel	10.2.1.0
	Marketing	10.2.2.0
	Wireless	10.2.3.0
	Phones	10.2.4.0
3	Material & Design	10.3.1.0
	Wireless	10.3.2.0
	Phones	10.3.3.0
4	Sales	10.4.1.0
	Wireless	10.4.2.0
	Phones	10.4.3.0
5	Research & Tech	10.5.1.0
	Wireless	10.5.2.0
	Phones	10.5.3.0
6	Planning & Manufacturing	10.6.1.0
	Wireless	10.6.2.0
	Phones	10.6.3.0
7	Dept Heads & Assistants	10.7.1.0
	Wireless	10.7.2.0
	Phones	10.7.3.0
B1	Wireless	10.8.1.0

5.2 Justifications

6. Policies

6.1 Work issued hardware

- Cannot be left unattended.
- Should donly be used for work purposes.
- Every quater all work issued hardware should be handed back for security inspections, security updates and inspection.
- Software used while connected or virtually connected to the company network should conform to an allowed list of softwares.

6.2 backups

- all server infrastructure should be backed up on a regular basis (Quaterly?)
-

6.3 New Infrastructure

- Any new server infrastructure should be installed inside the network DMZ

6.4 Employee onboarding/offboarding

- An introductory course for new employees on best practicies in regards to network and general online saftey.
- Offboarding session where all company issued hardware should be returned, logged and stored.
- Any offbaording employee should have their company ID and accounts frozen and then deleted after a certain period (2 months).

6.5 Personal Devices

- personal devices should be ensured to have a sufficient level of anti-virus
- Software used while connected or virtually connected to the company network should conform to an allowed list of softwares.

6.6 Remote Working

- VPN access

6.7 Access Control

- Only authorised employees should have physical access to network infrastructure.
- All critical network infrastructure should be secured behind access card controlled locks.
- All shared file servers should have access control

7. Security

7.1 Overview

As Yotsuba Group is a large manufacturing company leading the market in Asia, their assets and infrastructure are a prime target for cyber-attacks. The manufacturing industry is reported as the 2nd most targeted industry by cyber attackers, primarily due to COVID-19 (Miller, 2021) so ensuring that Yotsuba Group can cope with these threats is crucial.

7.2 Identifying Network Security Threats

7.2.1 MAC Spoofing

MAC spoofing is a common layer 2 attack that forges a suspicious MAC address as a legitimate one. Due to this, a suspicious device can then bypass security controls to access the network (Upadhyay, 2020). ARP Cache Poisoning: Similarly, common layer 3 attacks include ARP cache poisoning. This attack takes advantage of the insecure nature of the ARP protocol and potentially leads to man-in-the-middle attacks. Since the ARP protocol doesn't verify identities, it can be easy for an attacker to trick a legitimate host into thinking its legitimate itself. Therefore, if an ARP poisoning attack is successful, the attacker can view all traffic sent between two hosts (Grimmick, 2021) check.

7.2.2 Static VLAN Security

Insecurities of static VLAN switches could lead to an attacker being able to connect to a VLAN by simply connecting their device to a switch. If successful, an attacker would be able to communicate to other devices in the VLAN as well as accessing potentially sensitive data.

7.3 Mitigation

7.3.1 Device Security

At the very least, YG should implement a strong password policy and multi-factor authentication. This is basic level security but prevents even the simplest of attacks. Unnecessary services and applications should also be disabled on devices that do not need them to protect the network from vulnerabilities in certain applications. For

example, employees in the manufacturing department will not need access to finance applications, so segregating them makes the network more robust.

7.3.2 Port Security

Sticky MAC addressing. A switch will learn a MAC address that corresponds to a specific port. In sticky learning, this is remembered even after a reboot. Introducing sticky MAC address learning means a device that is not recognised will not be allowed into the network.

7.3.3 ACLs and Firewalls

Thorough Access Control Lists should be created to control network traffic. Having ACLs limits the lateral movement an attacker can make within a network by permitting or denying traffic from one host or group to another. Similarly, we have placed a firewall between the internet and internal network. The firewall protects the network by filtering incoming packets and decides whether to drop the packet based off a predefined set of rules (Cisco, 2021b).

7.3.4 Static ARP Tables

Manually configuring ARP tables means that MAC addresses can be statically mapped to their corresponding IP address. Doing this is a highly effective method to prevent ARP poisoning attacks, although requires a lot of time to complete (Grimmick, 2021).

8. Monitoring and Maintenance

8.1 Overview

The network performance and maintenance strategy will focus on maintaining specific network performance goals. Ongoing evaluation of this strategy should be performed routinely, to ensure that it helps achieve the objectives outlined below:

- Minimising network downtime
- Providing sufficient bandwidth
- Minimising latency
- Proactively identifying security or network issues
- Troubleshooting issues as quickly as possible

8.2 Network Monitoring and Maintenance

The tool of choice to help achieve this will be the Intermapper Network Monitoring Software developed by HelpSystems, which provides mapping, monitoring and alerting solutions (Helpsystems, 2022). It is an SNMPv3 enabled software, allowing for enhanced security and performance of monitoring network devices. Some key features include:

- Automatic network mapping - colour-coded statuses on network devices provide the IT team with a visual indication of how the network is performing.
- Proactive network monitoring - SNMP protocol allows for continuous status updates for all devices, servers and applications.
- Remote network monitoring - geographically scattered devices and offices can be monitored, allowing for problems to be diagnosed and addressed remotely.
- Network traffic analysis - provides insight into bandwidth usage, traffic statistics and suspicious spikes or dips.
- Network automation - reduces manual network activities by executing pre-defined responses to alerts.

Other solutions on the market included software such as the Solarwinds Network Performance Monitor (Solarwinds, 2022) and Datadog Network Peformance Monitoring (Datadog, 2022). Although they are more popular, two of the main factors in choosing Intermapper was due to its remote network monitoring and network automation features. As Yotsuba Group expands rapidly, there will be more instances of devices being spread across a larger geographical area. Intermapper bridges the gap so that those devices can still be monitored, but also issues on these devices can be resolved with a degree of automation. The pricing of Intermapper also helps with the upscaling of Yotsuba Group in line with expansion, with prices varying depending on the number of devices that need to be monitored. Intermapper also comes with a risk-free 30-day trial so if for whatever reason it does not meet the requirements of the network, another provider can be sourced.

9. Disaster Plan

9.1 Outline and Scope

This disaster management and contingency plan aims to identify risks and provide methods of mitigation. Certain network issues can be treated with automation via the setup of executables using the Intermapper network management software. If manual intervention is required, the plan employs a systematic approach, which allows problems to be treated in a sufficient timeframe, but with enough knowledge so that it can be understood and corrected properly. We have been proactive with our network design, employing the Cisco 3-layer hierarchical model to prevent issues and help with troubleshooting. Our design makes it easier to isolate a section of the network where an issue may be found, makes scaling easier and ensures we have redundancy within the network.

9.2 Risks and Mitigation

Risk	Potential Consequences	Mitigation
Natural Disaster i.e., flooding, earthquake, tsunami	Destruction of the building or critical IT infrastructure. Loss of critical personal and manufacturing data.	Seek cloud-based computing solutions for storage of critical data in geographical locations where natural disasters are less frequent.
Fire	Destruction or damage to critical IT infrastructure. Damage to company reputation	Conduct regular fire assessments, ensuring sockets are PAT tested and fire extinguishers are readily available.
Power Cut	Disrupt operations and potential loss of data.	Utilise the space in the underground car park for a temporary backup power supply. Ensure this power supply can handle normal business operations.
Network Issues	Loss of communications and disruption of operations.	Ensure adequate levels of redundancy are implemented into the network. Isolate network where the issue is and ensure there is enough backup equipment available to create a simple network should critical operations be required.
Theft	Loss of infrastructure or crucial data. Damage to reputation.	Ensure IT team performs regular checks on IT devices along with trackers and encrypted hardware.
Software Issues	Disruption of operations. Loss of access to data.	Perform backups regularly before updating software. If the latest versions of software cause issues, the IT team should roll back to the previous version if there is no significant vulnerability risk.
Hardware Issues	Disruption of operations. Loss of access to data.	Planned resolution methods for each network device, whether it is router, switch or computer. Isolate network where hardware issue is if needed and perform regular backups to prevent loss of data.
Employee Lost Device	Possible loss of data and/or exposure of sensitive company data.	Ensure password policies are enforced on employee devices, with multi-factor authentication and encrypted hard drives.

Table 9.1: *Risks and mitigations*

9.3 Risk Assessment Matrix

The Risk Assessment Matrix provides visual indication of how likely a risk is to occur, as well as its impact on Yotsuba Group in such an event. Mitigation methods described in Table 9.1 will help overcome and reduce the consequences of these risks.

		Impact				
		Neglible (1)	Low (2)	Moderate (3)	Significant (4)	Catastrophic (5)
Likelihood	Improbable (1)					
	Remote (2)		Power Cut	Employee Lost Device	Network Outage	Fire
	Occasional (3)			Theft		
	Probable (4)		Software Issues		Natural Disaster	
	Frequent (5)		Hardware Issues			

Figure 9.1: *Risk assessment matrix for Yotsuba Group*

10. Additional Problems

10.1 Renting One Floor Out

The second floor will combine four different departments to allow for space in the first floor. The new layout can be seen in figure 10.1.

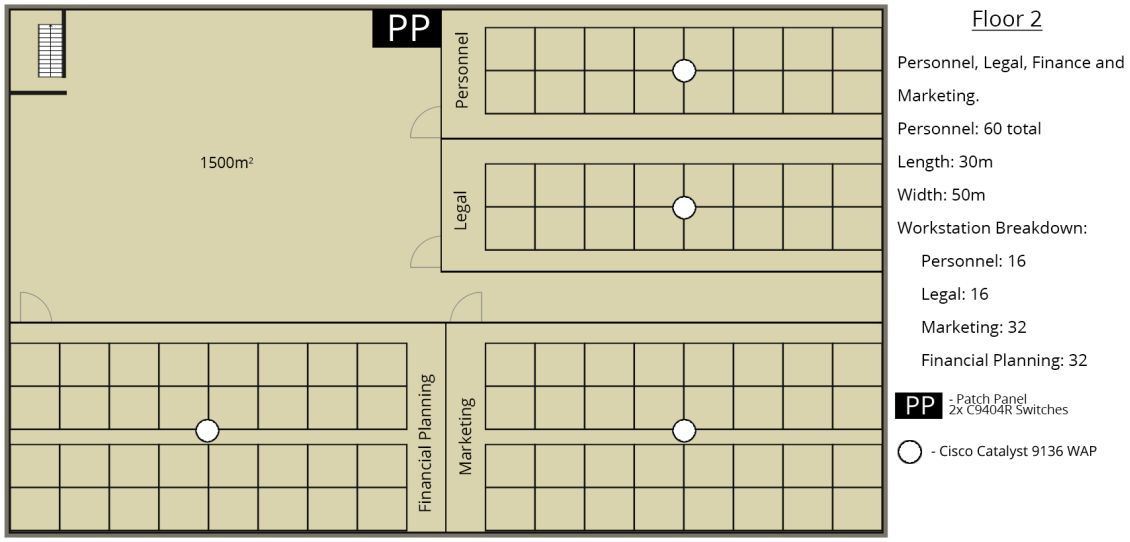

Figure 10.1: *2nd floor plan combining 4 different departments*

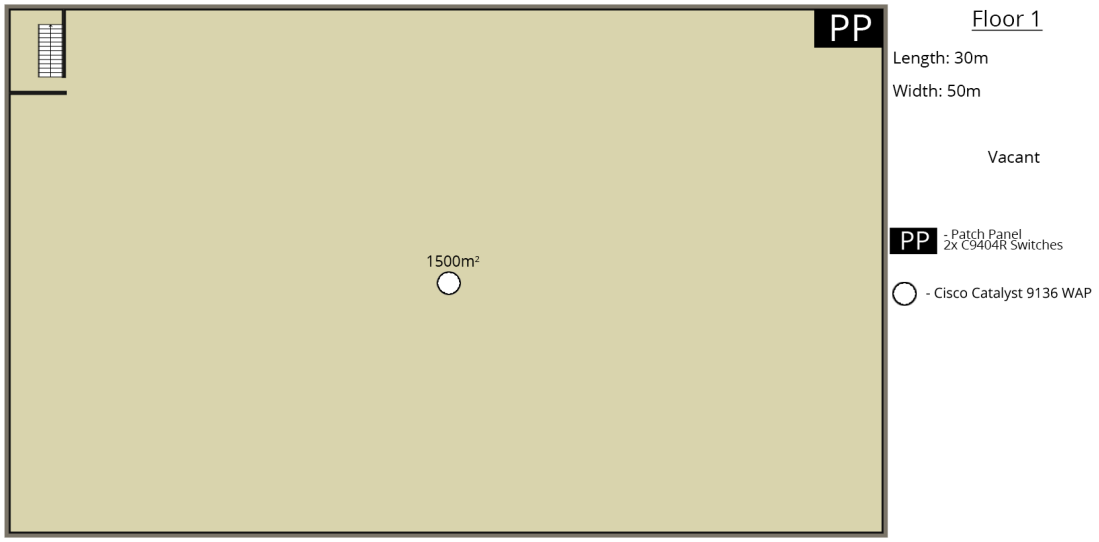

Figure 10.2: *1st floor vacant plan*

10.2 Splitting Between Two Buildings

Running Single mode fiber between buildings?

References

Cisco. (2019). End-of-sale and end-of-life announcement for the cisco catalyst c4500e series. https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-series-switches/eos-eol-notice-c51-743088.html

Cisco. (2021a). Cisco launches digitization program in japan to support inclusive pandemic recovery. https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2021/m02/cisco-launches-digitization-program-in-japan-to-support-inclusive-pandemic-recovery.html

Cisco. (2021b). What is a firewall? https://www.cisco.com/c/en_uk/products/security/firewalls/what-is-a-firewall.html

Datadog. (2022). Network performance monitoring. https://www.datadoghq.com/product/network-monitoring/network-performance-monitoring/

Grimmick, R. (2021). Arp poisoning: What it is & how to prevent arp spoofing attacks. https://www.varonis.com/blog/arp-poisoning

Helpsystems. (2022). Intermapper — network monitoring software. https://www.helpsystems.com/products/network-monitoring-software

Miller, J. (2021). Top 7 cyber threats for manufacturing companies. *BitLyft*. https://www.bitlyft.com/resources/cyber-threats-manufacturing-companies

Solarwinds. (2022). Network performance monitor - onsite & remote monitoring. https://www.solarwinds.com/network-performance-monitor

Upadhyay, I. (2020). Mac spoofing attack: All you need to know in 6 important points. https://www.jigsawacademy.com/blogs/cyber-security/mac-spoofing-attack/

von Piekartz, M. (2019). How many square meters of office space do you need per person. https://skepp.com/en/blog/office-tips/this-is-how-many-square-meters-of-office-space-you-need-per-person#calculator

Appendices

A. Cisco Hierarchical Model

This design uses the layered Core, Distribution, Access model approach to demonstrate the network structure. Each layer is represented by a different colour (Green = Access, Orange = Distribution, Blue = Core, and the Yellow = DMZ), and the tags on each section show the number of devices, name of the department, number of employees in each department and their floor numbers.

B. Demilitarized Zone (DMZ)

The DMZ presented keeps the external facing servers between two firewalls, giving them security but also easy access to the internet without going through the internal network.