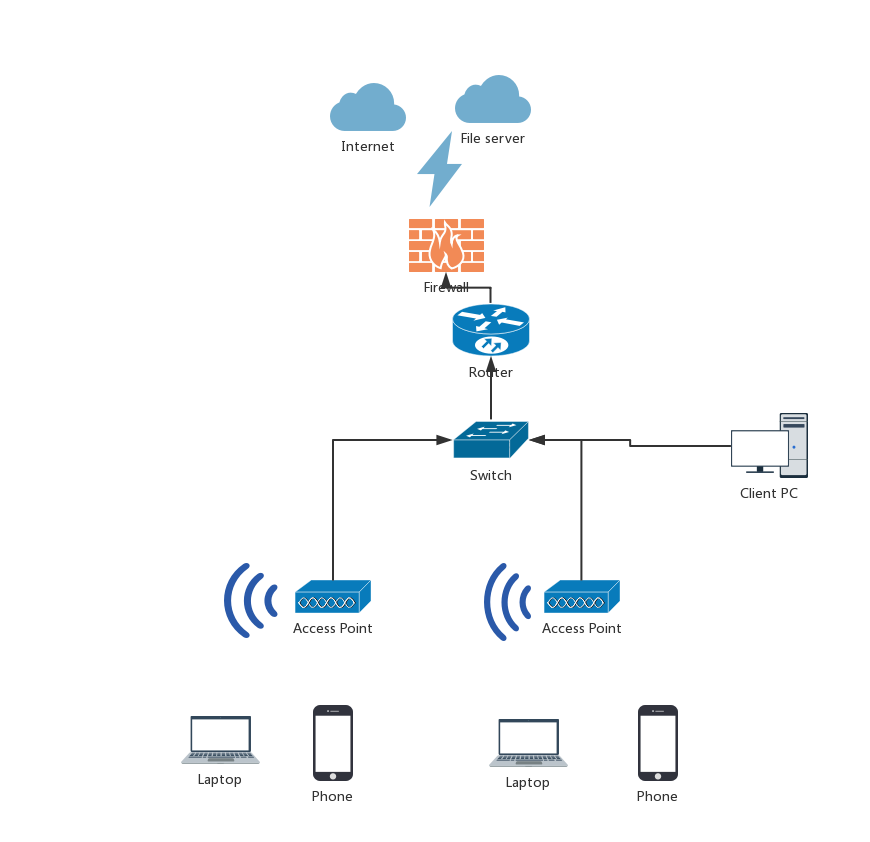
**Case study**

**1. Network upgrade proposal**

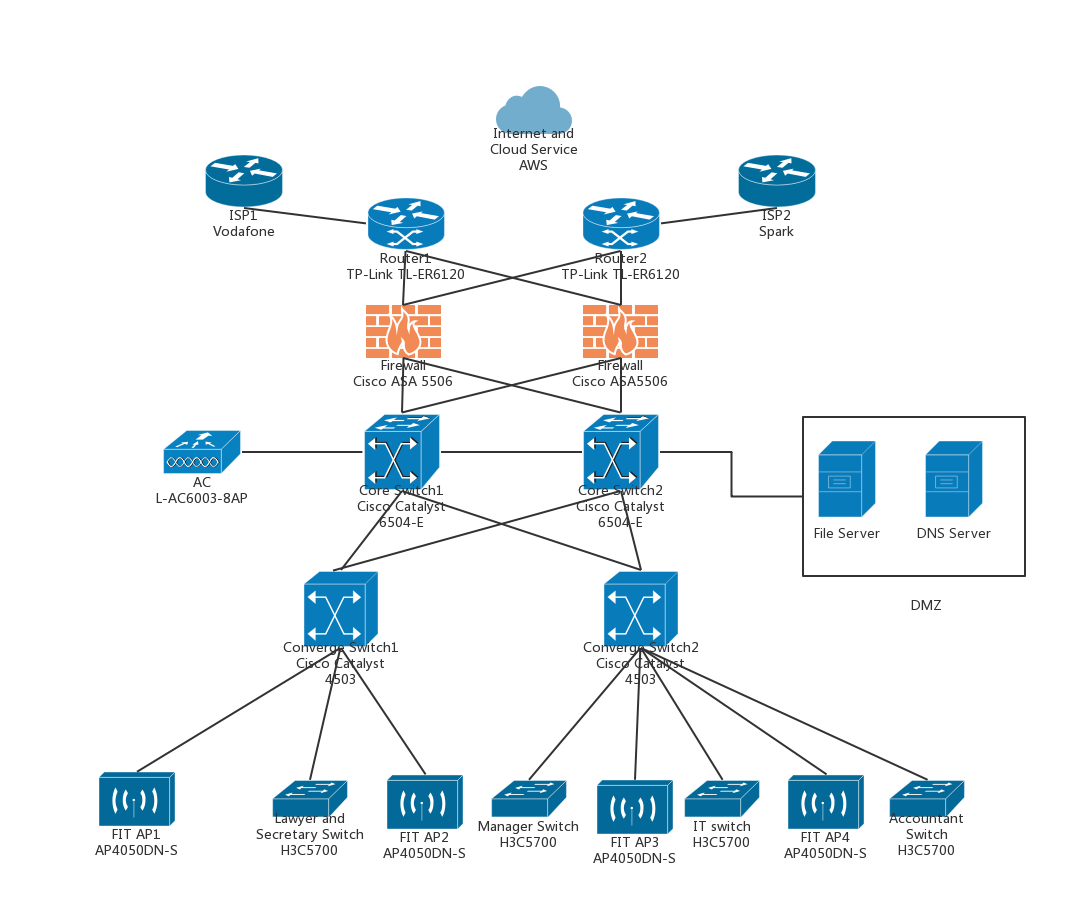
From the given scenario, the probable structure of the scenario company could be the following diagram.

Diagram 1

****

* 1. **Analysis of given scenario**
     1. In the given scenario company, there is only one server to store all the documents. There is not enough for a medium-sized company to have only one file server because this type of networking doesn’t has the ability to recover from disasters, for example, when the file server broke down, all the documents will be lost.
     2. In the given scenario company, the staff can’t use their own device to do their work, thus it is not very convenient for them and it is reducing the efficiency of work.
     3. In the given scenario company, they use wireless LAN to access the file server which not very stable and reliable because the wireless LAN based on wireless router which is easily destroyed and the level of security is relatively low.
     4. In the given scenario company, there are often connectivity issues. Since this company uses wireless LAN, I assume the structure of this company’s network has one layer and the access point of wireless LAN is FAT Access Point. FAT Access Point has a lot of merits but it can’t cover a large area so it always bringing connectivity issues. A FAT Access Point is more suitable for a family instead of a company.
     5. In the given scenario company, the staff use gmail to send and receive work emails which is a big issue to a lawyer company. Lawyer company requires confidentiality while gmail is a third party platform service which makes it easily hackered.
  2. **Proposed upgrade solution**

Diagram 2(2019)

****

Device

Routers: TP-Link TL-ER6120

Core switches: Cisco Catalyst 6504-E

Distribution switches: Cisco Catalyst 4503

Access switches: H3C 5700

AP: AP4050DN-S

AC:L-AC6003-8AP

Firewall: Cisco ASA 5506

* + 1. **VLAN**

The network topology designed in this paper basically guarantees the reliability, scalability, manageability and security of the network. This network is standard three-layer network which contains core layer, distribution layer and access layer. At the same time, the core layer uses hot backup to ensure stability of the network. This network shown as diagram 2.

As the diagram shows, two high-bandwidth Gigabit switches work as the hub of this network and connect to the firewall to ensure the security of the network.

The distribution layer contains two switches that support Layer 3 switching technology and VLAN in order to reduce the load of devices on the core layer.

Switches on the access layer don not support Layer 3 technology and VLAN. Deploying access switches in different departments, and then using VLAN technology to isolate data of different departments in the scope of their own broadcast domain through Layer 2. At the same time, configuring access control at each gateway to strengthen the security. For example, prohibiting networking between departments to prevent attack in one of the departments contaminating other departments.

For servers with large traffic and frequent access in the network, for example, file server and DNS server, using MSTP+VRRP technology to connect to switch on distribution layer to provide high redundancy of devices and balance load.

This network has two channels for data flow and connect two ISPs, Vodafone and Spark. Any device in each channel is broken, the data flow will not be impacted.(2019)

* + 1. **WLAN**

Considering the connectivity issues of the given scenario, the upgrade network uses FIT AP instead of the previous wireless LAN strategy. Different from FAT AP, FIT AP separate its function into two parts, one is Access Point, another one is Access Controller. Access Controller is used to control users’ access and users’ data encryption. Access Point is used to amplified signal to ensure a large range covering wireless signal.

For security, there are seven types of authentication, the most suitable one here is 802.1X access authentication because this company uses 802.11n wireless LAN.

* + 1. **Cloud service**
       1. BYOD

Renting AWS EMM product. AWS EMM product contains Mobile Device Management, Mobile Application management, Mobile Policy Management, ID Management. AWS EMM covers nearly all the solutions needed for BYOD. Mobile Device Management is used for ensure the security for device loss. If the mobile device is lost, stolen, or out of compliance, MDM can clean up the data and applications protected by the mobile device. MAM provides batch-based automated control of policy-based mobile application distribution, access, configuration, updates, and deletions to achieve better user satisfaction and significantly reduce IT service costs. The purpose of MPM is to protect confidential business information from providing access availability and experience while the mobile environment is not being compromised. IDM provides a unique enterprise ID management and authentication service for employees using mobile devices, and is open to third-party mobile application developers through APIs for unified authorization and verification.

* + - 1. AWS Backup

Renting AWS Backup service

* + - 1. Office 365

Renting Office 365 service for email.

* + 1. **SCCM**

Using SCCM to configure Windows10 for each client pc. (Technologies, 2019)

* 1. **Justification of proposed solution**
     1. **VLAN**

Local area network topology

Common LAN topologies can be divided into: bus type, ring type, star type, tree type and point-to-point type.

Bus LAN -All computers and devices are connected in series to a single linear cable called a trunk or sometimes called a backbone.

Ring LAN-In this topology, all computers and devices are connected to cable that forms a closed loop.

Star LAN-All computers and devices are connected to a centrally located hub or switch.

Tree LAN-Combination of bus LAN and star LAN.("Types of Network Topology in Computer Networks | Studytonight", 2019)

Point-to-Point LAN-Each node is connected into a network structure.

In this paper, the network is tree LAN. Considering the given scenario is a lawyer company which requires high stability and security of network, tree LAN is the most suitable one. Compared with other topologies, tree LAN is easy expanded, easy isolated from malfunction and it has high reliability.

Although it rely more on the root node, once the root node fails, the whole network will not work, the redundancy design of this network will avoid this problem efficiently.

VLAN structure

In this paper, the network is designed to be a three layers network, the merit of three layers structure is evident that it is easy to replace the original hierarchical implementation with a new one. For example, performance optimization of sql does not affect the code structure of other layers.

Compared with one layer or two layer structure, three layer structure is more stable and safe. Considering this is a lawyer company and requires high level of security, three layer structure is more suitable than the others.

* + 1. **Wireless LAN**

Access authentication

Access authentication is used to control the users access to the wifi to ensure the security of the company. There are four types of access authentication, they are open, WEP, WPA, 802.1x. Since newly NICs and routers use IEEE 802.11n and WEP encryption or WPA-PSK/WPA2-PSK encryption will decrease transmission rate to 11g level, so it is better to choose 802.1x authentication.

* + 1. **BYOD**

There are a lot of strategies for BYOD, the following diagram shows the comparation of different products for BYOD.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | AWS EMM | Mobile Ark | NQSky | ZIYA | XenMobile | SaaS360 | AirWatch |
| MDM | √ | √ | √ | √ | √ | √ | √ |
| MAM | √ | √ | √ | √ | √ | √ | √ |
| MCM | √ | √ | √ | √ | √ | √ | √ |
| MPM | √ | √ |  | √ | √ | √ | √ |
| IDM | √ | √ | √ | √ | √ | √ | √ |
| Self-service | √ | √ |  | √ | √ | √ | √ |
| Mobile gate | √ |  | MEAP | √ | √ |  | √ |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | AWS EMM | Mobile Ark | NQSky | ZIYA | XenMobile | SaaS360 | AirWatch |
| File Sharing | √ | √ | √ | √ | √ | √ | √ |
| Work Communication | √ |  |  |  |  |  |  |
| Backlog | √ |  |  |  | √ |  |  |
| Address book | √ |  |  |  | √ |  |  |
| Email |  |  | √ |  | √ | √ | √ |
| Task management |  |  |  |  | √ | √ | √ |

Compared with other strategies, AWS EMM has relatively more function than the others and the price of AWS EMM is acceptable for a medium company. Therefore, I choose AWS EMM. ("AWS Marketplace: Centrify Endpoint Services - Enterprise Mobility Management (EMM)", 2019)

* + 1. **Storage**

There are three common strategies for storage, they are NAS, SAN and cloud platform storage. SAN is a network storage strategy, requiring more equipment and staff to maintain. ("What's the Difference Between SAN and NAS Storage?", 2019) Considering the IT department has only two people and the amount of data is not large, therefore, SAN is not suitable for this company. Cloud platform storage has the problem of security, even its private cloud storage is safe, the high price of private cloud storage is not suitable for a medium company. However, using cloud platform for backup is also a good choice. Considering all the reasons above, using NAS for the physical network and backup on cloud platform.

* + 1. **Firewall**

Hardware firewall and software firewall

Software firewall only has the function of packet filtering, however, hardware software has other functions such as content filtering, intrusion detection and intrusion prevention. For a lawyer company, packet filtering is not enough for the lawyers have to keep frequency contact with there clients and the content of their business is extremely confidential. In addition, the firewall is placed between router and the core switches, once the network is intruded, the whole network is also intruded. Therefore, hardware firewall is more suitable than software firewall here. (Hodge, 2019)

* + 1. **E-mail**

Configuring private mail server is one of the choices for company, however, it is very complicated to do it. The necessary components of a mail server include mail delivery agent, mail distribution agent, IMAP/POP3 server and firewall. The cost of configuring a mail server is expensive and the maintain of mail server is also complicated. Considering there are only two people in IT department, I choose third-party email service.

Gmail, Zoho, FastMail, Gandi and Microsoft office 365 are third party email service provider. Compared with the others, office 365 provide not only email service but also other necessary service such as Word, PowerPoint and Excel. The price of office 365 is acceptable. ("Microsoft - Official Home Page", 2019)

* 1. **Costing**

Equipment

Routers: $364.95x2=$729.9 (TP-Link TL-ER6120)

Core switches: $2070x2=$4140 (Cisco Catalyst 6504-E)

Distribution switches: $559x2=$1118 (Cisco Catalyst 4503)

Access switches: $336.89x4=$1347.56 (H3C 5700)

AP: $77.07x4= $308.27 (AP4050DN-S)

AC: $150.39 (L-AC6003-8AP)

Firewall: $793.95x2=$1587.9 (Cisco ASA 5506)

Online service

Office 365: $32392.1/year

AWS EMM: $13019.93/year

AWS Backup: $0.09/GB (Hot) $0.02/GB(Cold) (1T)

Labour

Five people work eight hours per day and five days per week. Time of this project is four weeks. Calculating $20 per hour, totally it is $16000.

Total cost is: $70904.05

* 1. **Work scope**

Deliverables

Configuring network layout and implementing network on a simulation software, for example, GNS3.

Integrated wiring related work is tested and documents are generated.

The network access and disaster recovery are completed through experiments or software simulations, which meets the requirements of the company.

Corresponding network security solutions are developed.

Web server and DNS server are configured.

Current documents of the company are well managed.

Online service is configured.

Staff

This project needs five people.

One is responsible for project management.

One is responsible for purchasing equipment and online service.

One is responsible for configuring hardware.

One is responsible for configuring software.

One is responsible for testing the implementation of the network.

* 1. **Planned schedule**

The project time will be four weeks. The methodology of implementing this project will be Agile. Time table of this project as following:

First week: Accomplish the evaluation of the previous network and make upgrade proposal. Confirm project executing and management plan.

Second week: Accomplish the purchasing of equipment and online service. Complete the configuration of hardware.

Third week: Accomplish the testing of the network and the configuration of software on bottom devices.

Forth week: Accomplish network testing and deliverables.

Stages

Check if all equipment and accessories are not broken.

Place all the equipment to the right area and then debugging the network devices.

Network device boot.

Network device log in.

Upper layer service configuration and testing.

Routing configuration and testing.

Interface configuration and link test.

Basic information configuration.

Save and backup configuration files.

Configuring WiFi security access.

Configuring domain controller and create Active Directory domain.

Configuring MAM,MDM,MPM,IDM.

Configuring office 365 on client pc.

* 1. **Assumptions**

Assumption1: The structure of previous network is one or two layers.

Assumption2: The previous wireless LAN uses FAT AP.

Assumption3: The previous wireless LAN has no access authentication.

Assumption4: The company has an Active Directory domain.

* 1. **Risks**

Physical and protocol port down: The fault may occur due to the inappropriate plug of the physical port, the network cable broken and power off of the device.

Physical port up but protocol port down: The fault may be caused by the inconsistency of the encapsulation protocols on both ends, the incorrect configuration of the IP address of the port, and the incorrect configuration of the IP configuration of the routing protocol.

Port both up but unable to ping: This type of fault may occur because the IP addresses of the two ends are not on the same segment, or the routing protocol is incorrectly configured.

Broadcast storm may occur.

1. **Disaster recovery plan**
   1. **Incident indicators**
      1. **Earthquakes**

As is known to all, New Zealand is a country with frequent earthquakes so it is possible for the hardware of network broken down after an earthquake and it is easy to detect it.

* + 1. **Device broken**

Networking hardware may be broken after long time work. This often manifests as the following:

Usually crashes of switches and routers.

Pinging gateway successfully but can not connect the internet.

The speed of connecting to the internet is pretty slow and usually drop.

* + 1. **Inappropriate operation**

Inappropriate operation is based on staff behaviors, for example, downloading harmful documents from the Internet. Those harmful documents may contain virus which may cause network paralysis of the whole company. This often shows as the following:

Abnormal network traffic

Computer system running extremely slow and more pop-up ads.

Frequent blue screen, program crashes.

Abnormal files and registry, mouse and keyboard do not work.

* + 1. **Outside attack**

There are a lot of attack from extranet which may cause the loss of documents or information leakage. The best way to detect attack is to check the Firewall list if it has strange IP address.

* 1. **Roles roster**

Set up several groups, including management group, technology recovery group, application recovery group, administration recovery group, business recovery group. At the same time, inviting equipment and online service provider staff to help disaster recovery.

* 1. **Containment strategies**

In the first type of incident, checking the damage of disaster and contacting equipment and online service provider to help reconstruct the network. At the same time, using the backup file to recover business.

In the second type of incident, finding out where the broken device is and starting alternate channel.

In the third type of incident, finding out which client pc infected and isolate infected client pc instantly.

In the forth type of incident, finding out which port is attacked and check firewall list if there is strange IP address.(Hanna,2019)

* 1. **Damage assessment procedures**

First, having a general evaluation of the situation: what happened, what assets are impacted and how about the damage, giving a general evaluation of potential escalate.

* 1. **External parties**

It is necessary to inform the partner of situation of happened disasters. Since the lawyer company’s partner including the government

* 1. **Technologies required for DR**

EMC,SRDF Remote data backup system, Veritas offsite backup disaster recovery solution.

Cloud platform backup, for example, AWS.

* 1. **Time considerations**

According to the seven levels disaster recovery, time for MTO, RTO, and RPO is different. In this scenario, the disaster recovery is level 3.

MTD: less than 24 hours

RTO: less than 24 hours

RPO: less than 24 hours

1. **Business continuity plan**
   1. **Site description**

A cold site is not enough for this company and a hot site is not necessary because of its high cost. A warm site is configured with hardware needed and documents. The documents stored in warm site are not latest but also necessary for continue the business. Therefore, a warm site is suitable for this company.

**References**

(2019). Retrieved 27 October 2019, from <https://yourbusiness.azcentral.com/list-steps-design-implement-new-network-small-manufacturing-company-22713.html>

Hanna, T. (2019). The 7 Levels of Disaster Recovery. Retrieved 27 October 2019, from <https://solutionsreview.com/backup-disaster-recovery/the-7-levels-of-disaster-recovery/>

Types of Network Topology in Computer Networks | Studytonight. (2019). Retrieved 27 October 2019, from <https://www.studytonight.com/computer-networks/network-topology-types>

Microsoft - Official Home Page. (2019). Retrieved 27 October 2019, from <https://www.microsoft.com/en-nz/>

AWS Marketplace: Centrify Endpoint Services - Enterprise Mobility Management (EMM). (2019). Retrieved 27 October 2019, from <https://aws.amazon.com/marketplace/pp/B07DPPVN7V>

What's the Difference Between SAN and NAS Storage?. (2019). Retrieved 27 October 2019, from <https://www.lifewire.com/san-vs-nas-818005>

Technologies, M. (2019). SCCM Tutorial For Beginners | Step By Step Guide To Learn Microsoft SCCM. Retrieved 27 October 2019, from <https://mindmajix.com/sccm-tutorial>

Hodge, S. (2019). The best enterprise level firewalls: Rating 10 top products. Retrieved 27 October 2019, from <https://www.networkworld.com/article/3313344/the-best-enterprise-level-firewalls-rating-10-top-products.html>