**Project**

Networking Engineering Applications - HIT274

Andrew Mu - S318846

**Background**

This background information will only briefly discuss about relevant concepts to this project. Networking has become one of the most crucial processes in the modern world of computer science. In simple terms, networking is a process used to connect two or more computers, creating a network, which enables us to share resources, communicate with each other and create many other benefits. The communication between devices often use common standards, namely protocols.

There are two prominent types of networks, one being local area network (LAN) which is a network covering a limited area and the other wide area network (WAN) which covers a larger distance. Networks can consist of many different devices and equipment, some of which are routers, switches, cables, and end devices.

As building networks can be unpredictable and technical, a useful technique being real-life simulations of networks are used. This technique helps us to help analyse many different factors that come into networks such as cost, interaction and so on. One method of how these simulations are modelled is through software, in this project Cisco Packet Tracer will be used.

**Aim**

To design and create a network utilising Internet Protocol version 4 (IPv4) for a large organisation with several hundreds of employees with many different departments such as human resources, finance, information technology and others. There are certain criteria set in place that the network must achieve, a few to name are wireless and wired connectivity, security, redundancies, and access to the internet.

**Design**

**Overall Layout**

The network topology is a simplified version and does not showcase the true values. For instance, there is only 4 switches per department and a few end devices connected such as computers, servers, and printers. However, in practice there would be hundreds of more end devices and hence more switches per department to support these devices.

There are in total five departments in the organisation:

* Operations
* Information Technology (IT)
* Finance
* Human Resources (HR)
* Marketing

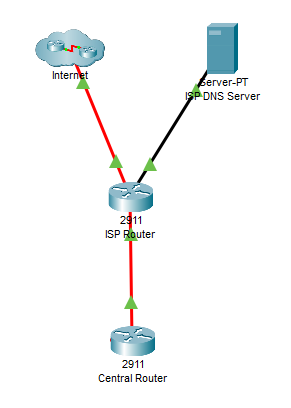
These departments are represented by subnet and their respective router. For each department there is a main switch connected to many sub-switches which enables multiple devices such as computers, servers, printers, etc. to be able to connect to the network through ethernet. Access points are installed in the departments allowing wireless connection as well. Rough estimate numbers of different device types that were considered per department when designing the network are as follows:

* Computers – Hundreds
* Routers - Unit
* Printers – Units
* Servers – Units
* Access Points – Units

One dissimilar router is the central router which connects to the internet service provider (ISP) router and other department networks hence granting internet and hence world wide web access for the whole organisation network.

**Internet Connection**

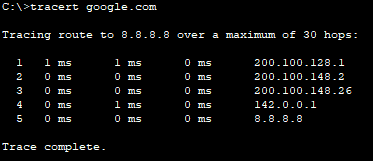
Internet connection for the organisation network is provided by an internet service provider. The method will involve connecting the central main router of the network to one of their routers. This connection towards the ISP router will allow the organisation network to connect to many different computers and other electronic devices, namely the internet. The internet provides access to email, fast communication between other internet users, and the world wide web (WWW). In addition, the ISP also provide a domain name system (DNS) server for the network which will resolve most domain names on the internet. This scenario is depicted by the image shown below.



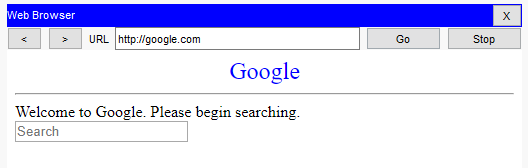
In the network topology, it shows that the ISP router is connected to a cloud which is the simulation of internet on a smaller scale. Seeing inside the cloud it reveals a vast network of many different connected routers and servers. The organisation network can connect to the world wide web, a collection of many different websites hosted by servers on the internet. An example of the organisation network utilising internet connection to access the world wide web is shown below.

**Example: Connection to Google Server/Website From IT Department**

**Trace Route to Google Server**



**Google Website Page**



**IP Addressing**

The network to be built is allocated an IPv4 address of 200.100.128.0/17 which is used for variable-length subnetting to create many different networks. The design allocates a subnet with a suitable amount of usable host IP addresses available for each department and each connection between two routers. Through consideration, the subnet mask of /22 is given to each department allowing 1022 usable host address per subnet while the mask of /30 is sufficient for the connection between two routers. The table below shows how the subnetting of the allocated IP address has been done.

To help with less administrative work, dynamic host control protocol (DHCP) has been configured into networks. The first 24 available host IP addresses are reserved for devices that are suited to have a static IP address, these devices include routers, servers, and printers. On the other hand, using the allocated DHCP server for the specific department, end devices such as computers, laptops and smart devices can obtain a dynamic IP address.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subnet | Network Address | Prefix | Host IP Address Range | Broadcast Address |
| IT | 200.100.128.0 | /22 | 200.100.128.1 – 200.100.131.254 | 200.100.131.255 |
| Operations | 200.100.132.0 | /22 | 200.100.132.1 – 200.100.135.254 | 200.100.135.255 |
| Finance | 200.100.136.0 | /22 | 200.100.136.1 – 200.100.139.254 | 200.100.139.255 |
| HR | 200.100.140.0 | /22 | 200.100.140.1 – 200.100.143.254 | 200.100.143.255 |
| Marketing | 200.100.144.0 | /22 | 200.100.144.1 – 200.100.147.254 | 200.100.147.255 |
| Central – IT | 200.100.148.0 | /30 | 200.100.148.1 – 200.100.148.2 | 200.100.148.3 |
| Operations – Central | 200.100.148.4 | /30 | 200.100.148.5 – 200.100.148.6 | 200.100.148.7 |
| Operations – Finance | 200.100.148.8 | /30 | 200.100.148.9 – 200.100.148.10 | 200.100.148.11 |
| Finance – HR | 200.100.148.12 | /30 | 200.100.148.13 – 200.100.148.14 | 200.100.148.15 |
| HR – Marketing | 200.100.148.16 | /30 | 200.100.148.17 – 200.100.148.18 | 200.100.148.19 |
| Marketing – IT | 200.100.148.20 | /30 | 200.100.148.21 – 200.100.148.22 | 200.100.148.23 |
| Central – ISP | 200.100.148.24 | /30 | 200.100.148.25 – 200.100.148.26 | 200.100.148.27 |
| ISP – DNS | 200.100.148.28 | /30 | 200.100.148.29 – 200.100.148.30 | 200.100.148.31 |

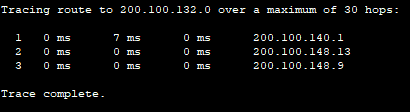
**Redundancies**

There are redundancies in place and appropriate design of the network to handle network or device failures. The design of the network entails that each department has one router for itself, this allows in the case of a department router failure there should be no down time for the other departments. In addition, each department has a main switch and sub switches connected to it.

All the main routers and their respective network have an optimal route to allow communication with other routers and their networks, in the scenario that any of the router or network fail there is an alternate route to still allow different networks to communicate with each other. For instance, HR network has an optimal route to Operations network. However, in the case that route fails, possibly due to the Finance network being down, there is still an alternative route. A trace route shown below is done to better illustrate and understand this concept.

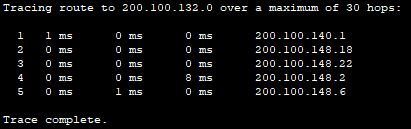
**Example 1:** **Trace Route from HR to Operations (Normal Route)**

**HR 🡪 Finance 🡪 Operations**



**Example 2: Trace Route from HR to Operations (Alternate Route)**

**HR 🡪 Marketing 🡪 IT 🡪 Central 🡪 Operations**



**Routing**

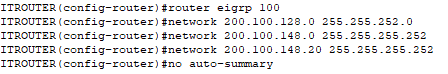
The network topology incorporates the use of dynamic routing as it has some key advantages over static routing most notably less administrative work of having to configure the routes on each router in the network, requiring only having to advertise the networks directly connected on a router. Another advantage of dynamic is that routers advertise to each other of failed routes to a network and alternative routes can be chosen instead to the specific network.

Dynamic routes are learned through routing protocols, for this network there were two main choices being either enhanced interior gateway routing protocol (EIGRP) or open shortest path first (OSPF). Both have their advantages and disadvantages, however, EIGRP was chosen as it is made and supported by Cisco which is the predominantly the brand of all devices. This protocol by default uses bandwidth and delay to calculate metrics and hence determine the best paths (successors) and backup paths (feasible successors).

Implementation of the EIGRP in the routers only requires a few commands in config enable mode of the CLI. These commands include a common Autonomous System number between the routers, the networks that are directly connected to the specific router and a way to stop the summarisation of network addresses. An example of the process and results are shown in the screenshots.

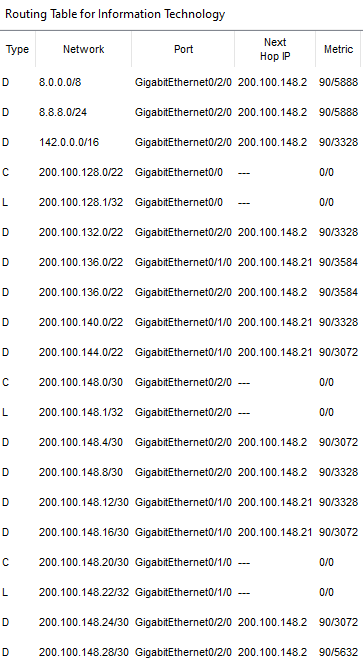
**Example: Implementation of EIGRP on IT Router**

**Enabling EIGRP / Config of Router**





**Routing Table**



**Wireless**

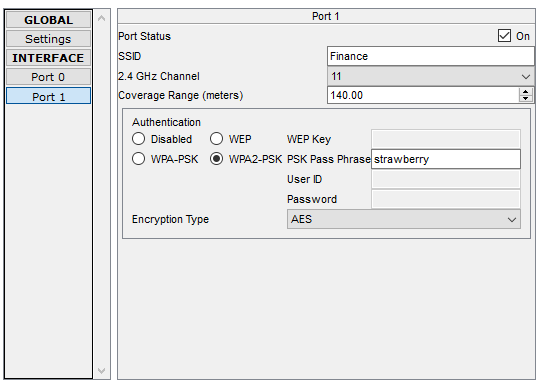
The use of wireless routers were considered, however, ultimately they are not used in the design as it is not needed. Instead, three access points per department are used to deploy wireless connectivity. There are a few reasons behind this decision, one being most of the functionalities of the wireless routers are already delegated elsewhere. Internet access is taken care of by the routers and ISP, DHCP is done by the respective DHCP server in the department and ethernet is provided by the switches which connect to the routers.

The only function needed is the actual wireless connectivity to the networks for wireless devices, which are taken care of by the access points connected to department sub switches. Another reason is that wireless routers are limited especially in terms of coverage, whereas access points offer more flexibility, scalability, and control.

The access points have been configured to prevent the overlapping of channels as this would cause interference. In 2.4GHz the recommended channels are 1, 6 and 11 to prevent overlapping. The design of the network incorporates that three access points are connected to every department. This will provide wireless connectivity coverage for the whole department, as well as provide a high strength and link speed wireless connection for devices.

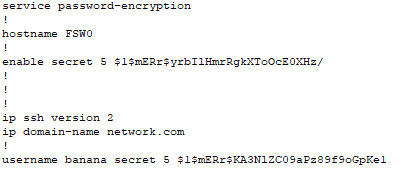
**Security**

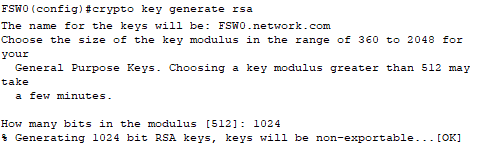
There are many different methods to implement in a network which could help improve the security of the network and lower the risk and effect of a security breach. Subnetting the departments into their own separate network makes it more secure as in the scenario a network department is compromised the other network departments will not be.

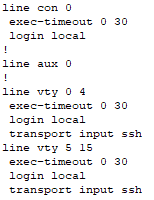
All the access points have been configured to require the correct password input to be able to connect to them. In addition, there is encryption for the wireless connectivity to prevent data that is transmitted between the rest of the network and wireless devices, from being compromised. The method of protection being used by all access points is WPA2-PSK which utilities encryption type AES. An example screenshot of the security configuration of an access point is shown below.

All switches and routers in the network have been configured to ensure security is maintained. This is done by entering config mode of switches and making the appropriate changes. All passwords are encrypted. The switches and routers require a valid username and matching password to access them through either console or secure remote connection (SSH). There is a password needed to enter the enable mode and any unused ports have been turned off. In addition, there is an inactive session timeout set to 30 seconds. An example of these security precautions are demonstrated below.

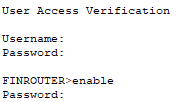
**Modifications of Console/VTY Lines, Enable Mode & SSH**



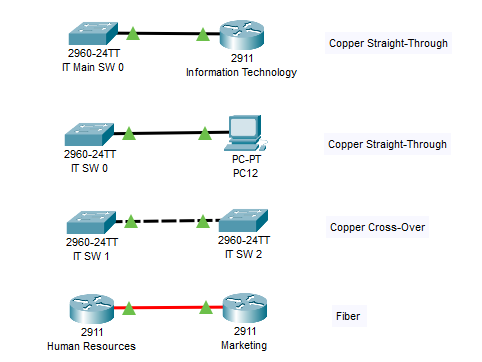


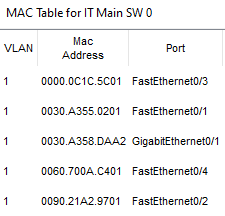


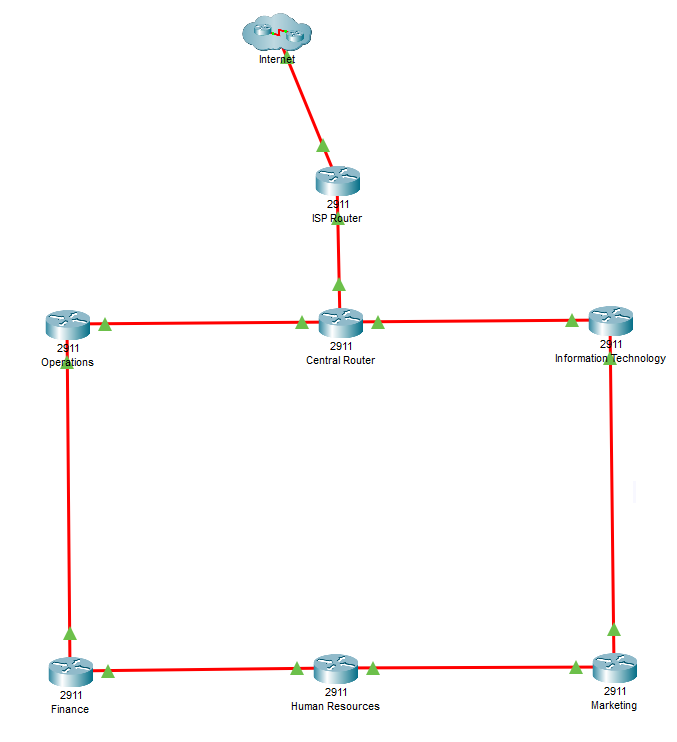
**Login and Enable Mode Prompt**



**Connectivity**

There are multiple various connections between devices in the network topology, however, each department do have very similar design to each other. Physical connections between dissimilar devices use copper straight through cables such as switch to end devices or router while alike devices such as switch-to-switch, use copper cross over cables. An exception is the router-to-router connection which uses fiber cables in this topology. Examples of these cable connections are shown below.

The first type of connections to look at are between the switches and devices. The switches are all connected enabling the switches themselves and end devices attached to them to communicate with each other. All these switches are layer 2 meaning that they communicate and reference each device through media access control (MAC) addresses. Departments can operate by themselves with just switches alone, however, to communicate with other networks including the other departments and accessing the internet, a layer 3 router is used. An example of the IT main switch MAC address table is shown below.

All the routers besides the ISP router have at least one direct connection to another department router, making all the routers and hence departments connected directly or via another router. The central router is connected to the ISP router which in turn is connected to the internet. Subsequently, as the departments (ultimately the whole organisation) are connected to the central router, they are also connected to the internet. A screenshot of the routers and connections are shown below.

**Conclusion**

The project created a simple and effective network for a large organisation with employees in different departments. The network has wired and wireless connectivity throughout the whole network enabling communication between the department subnets and internet. There is still further work that can be done on the topology to further improve the network. The redundancy can be enhanced by introducing more links, devices, and protocols such as fault-tolerant default gateway. The wireless connectivity can be improved by introducing 5 GHz connection. Other improvements can include implementing switch port security, VLANs, NAT and ACL to strengthen network efficiency and security.