**Abstract**

This documentation serves to provide an overview and analysis of the network topology task for the second assignment in this module. Contained within is a brief overview of the planning stage, detailed documentation on how the network was implemented, and finally a critical reflection on the method implemented.

Reece alqotaibi | 19063069

4WCM0019-0105-2020 - Platforms for Computing (COM)

Assignment 2: Network Documentation

2021

### Requirements and Planning

**Brief Analysis**

Based on the brief, it is clear to understand that we are to have at least six different subnets (172.16.20-25), with one for each department/room at the least. The brief also specifies the use of a /30 subnet which indicates that there are going to be two routers implemented in the network topology.

**IP Addressing**

Based on the requirements, the following IP scheme will be used as an overview:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Department/Device** | **Interface** | **Subnet** | **Mask** | **Default Gateway** | **DNS/DHCP** |
| Routers | Gig0/0 | 10.0.4.0 | 255.255.255.252 | N/A | N/A |
| Programmer PCs | Fa0 | 172.16.20.0 | 255.255.255.0 | 172.16.20.1 | 172.16.25.10 |
| Sales PCs | Fa0 | 172.16.21.0 | 255.255.255.0 | 172.16.21.1 | 172.16.25.10 |
| Tech Support PCs | Fa0 | 172.16.22.0 | 255.255.255.0 | 172.16.22.1 | 172.16.25.10 |
| Accounting PCs | Fa0 | 172.16.23.0 | 255.255.255.0 | 172.16.23.1 | 172.16.25.10 |
| Manager Laptops | Wi0 | 172.16.24.0 | 255.255.255.0 | 172.16.24.1 | 172.16.25.10 |
| Programmer PCs | Fa0 | 172.16.25.0 | 255.255.255.0 | 172.16.25.1 | 172.16.25.10 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| Router 1 | Gig0/0 | 10.0.4.1 | 255.255.255.252 | N/A |
| Gig1/0 | 172.16.20.1 | 255.255.255.0 | N/A |
| Gig2/0 | 172.16.22.1 | 255.255.255.0 | N/A |
| Gig3/0 | 172.16.23.1 | 255.255.255.0 | N/A |
| Gig4/0 | 172.16.24.1 | 255.255.255.0 | N/A |
| Router 2 | Gig0/0 | 10.0.4.2 | 255.255.255.252 | N/A |
| Gig1/0 | 172.16.21.1 | 255.255.255.0 | N/A |
| Gig2/0 | 172.16.25.1 | 255.255.255.0 | N/A |

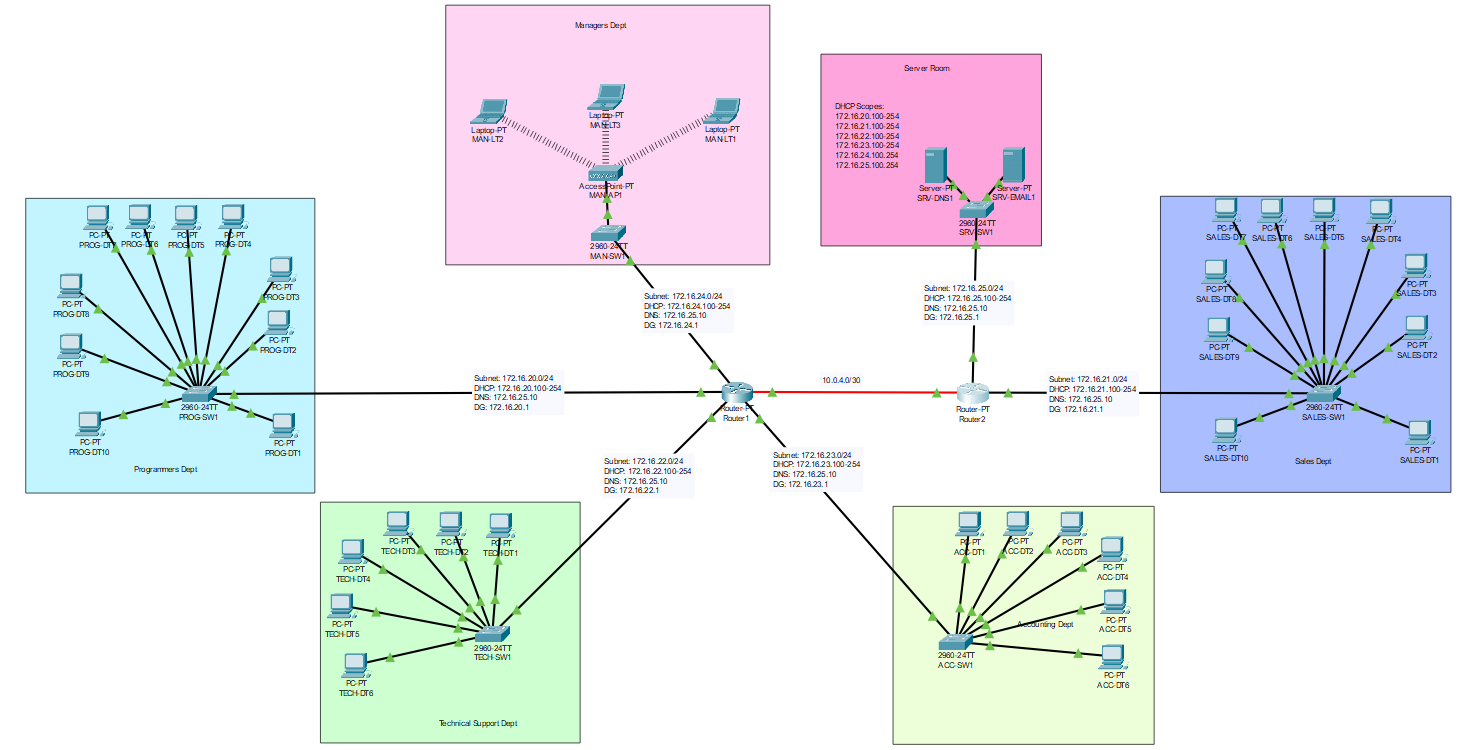
**Plan**

Based on the above criteria I knew most of the devices I was going to use, lending on experience from my profession to accomplish the task. Essentially, I was going to implement two physical Local Area Networks for Andromeda.

My plan was to implement the networks independently, and then provide routing between them so that traffic can pass between the two LANs.

### Implementation

The result of the implementation is the following:



Using the criteria and plan I started building the network model by placing the management devices I needed into the Packet Tracer. These devices were: Router1, Router2, along with switches for Programming, Sales, Tech Support, Accounting, Managers, and finally Servers. This gave me a total of two routers and six switches.

**Router 1**

By default, they came with 100Mbps interfaces, but for theoretical speed I powered off the router and gave it one Gigabit Fibre port, and four Gigabit Ethernet ports. I then configured each interface as required, assigning each interface a static IP address, depicted in the IP addressing scheme.

**Router 2**

The second router was also part of the /30 subnet. With there only being one usable host left, it was clear the two routers were destined to be in this subnet. I configured this, again according to the IP addressing scheme.

I connected a fibre cable from each fibre port on the respective router to each other to give them establish a link.

I entered the CLI, enabled EXEC, then ensure they were both connected by sending an ICMP request from one to the other.

**Switches**

For each switch that I had placed in the network topology I manually went into the CLI and assigned each device a static IP address on the native VLAN (VLAN 1). This is a best practice approach to ensure that the devices always have the same IP address, even after shutdowns and reboots. For example, on switch PROG-SW1, I gave this the IP Address 172.16.20.2, as this was the second management device for this network (the first being the default gateway/router). I then entered the CLI and gave the switch the respective default gateway. ‘IP default-gateway 172.16.20.1’. Finally, I performed another connectivity test by again sending ICMP requests from the switch to the gateway. All came back successful. At this point I was aware that there would be no routing between the switches but something I would address later.

**Servers**

I placed two servers in their respective subnet and proceeded to configure each as required.

The DNS/DHCP server was first and I started with DNS by configuring a static IP address which would be outside of the DHCP scope set up later. I then enabled the DNS service. I added a static A record for the email server, with the idea in mind that when it was created, I would likely need to reference this for the SMTP and IMAP/POP, depending on the protocols available when I got to it.

DHCP was set up by enabling the service, and then adding DHCP scopes for each of the subnets that are in the network topology (excluding the management subnet, as this only has two usable hosts – both of which are in use).

I configured the following scopes:

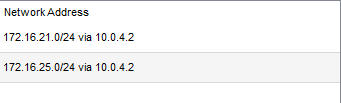
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Scope Name** | **Default Gateway** | **DNS Server** | **Pool Start IP Address** | **Subnet Mask** |
| serverPool | 172.16.25.1 | 172.16.25.10 | 172.16.25.100 | 255.255.255.0 |
| ProgPool | 172.16.20.1 | 172.16.25.10 | 172.16.20.100 | 255.255.255.0 |
| SalesPool | 172.16.21.1 | 172.16.25.10 | 172.16.21.100 | 255.255.255.0 |
| TechPool | 172.16.22.1 | 172.16.25.10 | 172.16.22.100 | 255.255.255.0 |
| AccountsPool | 172.16.23.1 | 172.16.25.10 | 172.16.23.100 | 255.255.255.0 |
| ManagerPool | 172.16.24.1 | 172.16.25.10 | 172.16.24.100 | 255.255.255.0 |

I was not sure if DHCP was enabled by default on the CISCO routers either, so I ran commands to disable in just in case: ‘no service dhcp’.

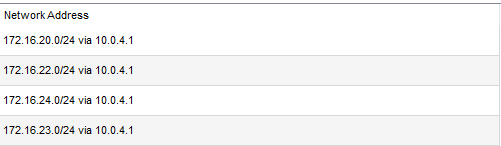
At this point I was presumptive that the only subnet that will receive DHCP leases is the subnet which the DHCP server is in, as there would be no helper rules defined in the router. For each interface with a 172.16.X.Y subnet, I added the following IP helper rule to redirect DHCP broadcast requests to the DHCP server in the server subnet: ‘ip helper-address 172.16.25.10’.

My final thought was that even with the DHCP helpers available, there would be no routing in place to route this traffic to the required switch. I remedied this by adding the following static routes to the route table.

**Router 1**

****

**Router 2**

****

The Email server was set up and configured by adding the domain andromedaprod.com and creating fictional users.

**Client Machines**

I decided, for demonstration purposes to include both wired and wireless clients in this topology. I decided that all the devices would be wired desktops, except the clients in the managers office, which would instead be laptops connecting to an access point in the room.

I dropped a total of 32 desktops into each of the departments/rooms that required them: ten for programmers; ten for sales; six for tech support and six for accounting.

I added an access point into the managers office, connected port 1 to the managers switch, then set up the wireless password. Finally, I added three laptops and gave them wireless cards.

With all the clients now in their respective pools, I set each machine network settings to DHCP. As expected, because of the static routing and the IP helpers I created, all the devices in each of the subnets received IP address leases from the DHCP server.

On a single machine in each subnet, I ran an ICMP test to the Email server using the DNS record I had set previously: ‘ping SRV-EMAIL1’. Out of the four requests sent, I received a 100% reply rate. This concluded a successful ping test.

Knowing that DNS was working as intended on the network I went about setting up the email accounts on each of the machines, for the users I had created. I then sent some test emails from various accounts, both to devices in the same local subnet, and separate ones.

Everything has been configured according to the specification set for the task, so I then went through the diagram and annotated it with the respective IP address information relative to each subnet.

### Reflection

To be perfectly honest, whilst the network is fully functional and working as required against the specification, it is not the way I would implement this if I had no limitations and constraints.

The first thing I would do is to strip out the second router. In an environment as small as this it is not really required. Instead, I would implement VLANs, which operate on layer 2 of the OSI model and allow network traffic to be segregated. This provides multiple benefits, and when using in conjunction with Inter-VLAN routing (Layer 3) allows for much more flexibility.

In its current state the security of the network is generally going to be quite vulnerable. The primary reason for this is that there is no firewall at any level. I would resolve this by adding a hardware firewall and implement access control lists, NAT policies, locking down ports, etc. I would also implement software firewalls on every machine, exposing only the inbound ports that are required: TCP/UDP 53 for DNS, TCP/UDP 1433 for SQL, for example.

To decrease network congestion, increasing speed in the process I would define access control lists for the VLANs also, and then apply Quality of Service to networked devices to prioritize higher priority traffic. Further to this, I would swap out all the network cards on the desktops and laptop, making them all Gigabit instead of FastEthernet. This would give a tenfold increase in available throughput for all the devices in the LAN.

Cost aside, I would implement failover pairs for the firewalls, routers, and switches. This provides redundancy if there is an issue with each, respectively. Additionally, I would provide more access points in the office, splitting out the corporate WiFi with guest WiFi, which users can connect their own devices to.