CE155 Assignment 1 – Cisco CCNA1 Skills Test

Eliandro Goncalves
1504492

Subnet	Network address	Mask in dotted decimal form (e.g. 255.255.0.0)	Number of hosts, including PCs and router interfaces	Number of unused addresses
A	192.168.245.0	255.255.255.224	19	11
B	192.168.245.32	255.255.255.224	5	25
C	192.168.245.64	255.255.255.224	24	6
D	192.168.245.96	255.255.255.224	3	27
E	192.168.245.128	255.255.255.224	2	28

Table 1. Subnet details.

Device	Interface	IP address	Mask in dotted decimal form (e.g. 255.255.0.0 for /16)	Default Gateway
R1	Fa0/0	192.168.245.30	255.255.255.224	N/A
	Fa0/1	192.168.245.62	255.255.255.224	N/A
	S0/0	192.168.245.158	255.255.255.224	N/A
R2	Fa0/0	192.168.245.94	255.255.255.224	N/A
	Fa0/1	192.168.245.126	255.255.255.224	N/A
	S0/0	192.168.245.157	255.255.255.224	N/A
1st PC subnet A	NIC	192.168.245.1	255.255.255.224	192.168.245.30
Last PC subnet A	NIC	192.168.245.18	255.255.255.224	192.168.245.30
1st PC subnet B	NIC	192.168.245.33	255.255.255.224	192.168.245.62
Last PC subnet B	NIC	192.168.245.37	255.255.255.224	192.168.245.62
1st PC subnet C	NIC	192.168.245.65	255.255.255.224	192.168.245.94
Last PC subnet C	NIC	192.168.245.88	255.255.255.224	192.168.245.64
1st PC subnet D	NIC	192.168.245.97	255.255.255.224	192.168.245.126
Last PC subnet D	NIC	192.168.245.97	255.255.255.224	192.168.245.126
DNS server	NIC	192.168.245.97	255.255.255.224	192.168.245.126
Eagle server	NIC	192.168.245.98	255.255.255.224	192.168.245.126

Table 2. Addressing table.

2. Analysis of address space usagew

Subnet	Network address	Mask in dotted decimal form
A	192.168.245.0	255.255.255.224
B	192.168.245.32	255.255.255.224
C	192.168.245.64	255.255.255.224
D	192.168.245.96	255.255.255.224
E	192.168.245.128	255.255.255.224
F	192.168.245.160	255.255.255.224
G	192.168.245.192	255.255.255.224
H	192.168.245.224	255.255.255.224

Table 1. Subnet details.

With this particular range and mask I can have a total of 8 subnets which is 3 higher than the given problem which means 90 more hosts than the 150 possible ones, this is a small scalable network.

The address space I was allocated for the subnets was not efficient as most of the spaces in the subnet were empty, even if I tried to change the mask length but still keeping it fixed the lowest mask I could have is 27 which does not change anything which means I either have more free space when increasing the mask length, however the range I had could have been made more efficient if the mask length for every subnet was not fixed making the number of free hosts decrease.

Part 3

SSH

SSH is the abbreviation to Secure Shell Protocol.
SSH is a protocol that provides a way to establish a CLI session of a device remotely so that a secure remote login can occur, this protocol uses secure network services by providing a "strong" password authentication and it also encrypts data when transporting it, over the Transport layer. This all happens over an insecure layer [1].
This protocol consists of 3 major components: The Transport Layer Protocol the" SSH-TRANS", the User Authentication Protocol and the Connection Protocol. TCP/IP is the transport layer protocol usually used to transport the application protocol, this protocol uses port 22. [2]
SSH protocol works by a request being sent by the client once a secure transport Layer connection has been made, then a second request is sent once the user authentication is complete. The connection protocol creates channels that can transfer data in both directions simultaneously.

POP

POP is an abbreviation of Post Office Protocol and is in the application –layer..
The purpose of POP protocol is to acquire e-mail from a remote mailbox server through a host over TCP/IP.
The transport layer protocol used to transport the application protocol is TCP/IP, and uses ports 109(POP2), 110(POP3).
This protocol listens for a connection, when one is opened the server sends a message and waits for commands, when they are received the server acts on them and replies.[3]

4. References

[1] Ylonen & Lonvick, The Secure Shell (SSH) Protocol Architecture, IETF RFC 4251, January 2006, Available from: https://tools.ietf.org/rfc/rfc4251.txt
[2] Ylonen & Lonvick, The Secure Shell (SSH) Protocol Architecture, IETF RFC 4253, January 2006, Available from: https://tools.ietf.org/html/rfc4253#section-4.1
[3] Reynolds, POST OFFICE PROTOCOL, IETF RFC 918, October 1984, Available from: https://tools.ietf.org/rfc/rfc918.txt