Project 7 – Hospital Network Design

Introduction

Melbourne Health Services is a well-established health provider in Australia, which offers health solutions and services to its clients. The institution **operates in two locations** within the same city, having the **hospital headquarters (HQ) 20 km away from the branch hospital**. Each location is also expected to have a Guest/Waiting area – GWA for patients or visitors.
Therefore, they have **the following departments** within its main headquarters:

- Medical Lead Operation & Consultancy Service – **MLOCS**
- Medical Emergency & Reporting – **MER**
- Medical Records Management – **MRM**
- Informational Technology – **IT**
- Customer Service – **CS**
- Guest/Waiting area – **GWA**

The branch Hospital was designed to share the workloads with the headquarters; hence it contains the following departments:

- Nurses & Surgery Operations – **NSO**
- Hospital Labs – **HL**
- Human Resource – **HR**
- Marketing – **MK**
- Finance – **FIN**
- Guest/Waiting area – **GWA**

So far, the network was using third-party services to maintain its IT services. The senior management has decided to own their **network infrastructure including LAN, WAN and a Server-Side site** that is expected to be **located separately at the headquarters and is connected to the HQ Route**r with an access switch. **The server-side site will host the DHCP server, DNS Server, Web Server, and Email Server.**
The network is expected to be cost-effective and observes the information security rule of the CIA (**Confidentiality, Integrity, and Availability**). The network is expected to have a **hierarchical model** with two already purchased **Core Routers (one at HQ and one Branch) each connecting to two subscribed ISPs.** Due to security requirements, it has been decided that all the departments will be on a separate network segment within the same LAN.
You will perform an appropriate robust network design model to meet the given requirements. You will also **implement ACLs and VPN**s to enable secure communication considering security and network performance factors paramount to safeguarding Confidentiality, Integrity and Availability of data and communication. The network security policy will comprehensively dictate the user's access to each site using ACLs.

Network Design & Implementation requirements.

1. Use **hierarchical model** providing redundancy in the network. The routers from both HQ and Branch must be connected through **serial interfaces.**
2. For cost-effectiveness, **each site** is expected to have **one core router**, **two L3 switches and several access switches** connecting each department.
3. Each department must have its own VLAN.
4. **Every department in HQ is estimated to have around 60 users, while in Branch is estimated to have around 30 users**. With the corresponding wireless network.
5. Use the network **192.168.100.0 as base for all network departments**.
6. The company has the following **pool of Public IP addresses**: **195.136.17.0/30, 195.136.17.4/30, 195.136.17.8/30, and 195.136.17.12/30** connected to the two ISPs.
7. Configure the basics for each device: Hostnames, console password, enable password, banner msgs, and disable IP domain lookup.
8. Allow communication among all departments through **inter-VLAN routing**.
9. The **L3 Switches are expected to carry out both routing and switching functionalities** and thus will be assigned IP addresses.
10. **All devices** in the network **must obtain IP addresses automatically** from the dedicated DHCP server located in the server room (SR).
11. Only **devices in the server room must have Static IP addresses**.
12. Use **OSPF as the routing protocol** to advertise routers both on the routers and L3 Switches.
13. Configure **default static routing to enable Routers and L3 Switches to forward any traffic that doesn't match with routing table entries**. Use next-hoop IP addresses.
14. Configure **SSH in all Routers & L3 Switches for remote login**.
15. Configure **port-security** for the server site department switch **to allow only one device to connect to a switch port**, use **sticky method** to obtain mac-address and violation mode shutdown.
16. Configure **Extended ACLs and site-to-site VPN (IPSec VPN)** to create a tunnel and encrypt Communication **between HQ and the Branch network**.
17. Configure **PAT to use the respective outbound router interface** IPV4 address and implement all the necessary ACLs rule.
18. Test Communication: ensure everything configured is working well.

ADDRESSING

Networks Address Allocation

Initial Conditions

- 192.168.100.0 as base network
- 60 users per VLAN in HQ Network
- 30 users per VLAN in Branch Network
- Server-Side Site Department only needs 4 addresses

HQ Hospital Network				
Department	**Network**	**Mask**	**Host Range**	**Broadcast**
MLOCS	192.168.100.0	255.255.255.192 /26	100.1 – 100.62	192.168.100.63
MER	192.168.100.64	255.255.255.192 /26	100.65 – 100.126	192.168.100.127
MRM	192.168.100.128	255.255.255.192 /26	100.129 – 100.190	192.168.100.191
IT	192.168.100.192	255.255.255.192 /26	100.193 – 100.254	192.168.100.255
CS	192.168.101.0	255.255.255.192 /26	101.1 – 101.62	192.168.101.63
GWA-1	192.168.101.64	255.255.255.192 /26	101.65 – 101.126	192.168.101.127
Branch Hospital Network				
NSO	192.168.101.128	255.255.255.224 /27	101.129 – 101-158	192.168.101.159
HL	192.168.101.160	255.255.255.224 /27	101.161 – 101.190	192.168.101.191
HR	192.168.101.192	255.255.255.224 /27	101.193 – 101.222	192.168.101.223
MK	192.168.101.224	255.255.255.224 /27	101.225 – 101.254	192.168.101.255
FIN	192.168.102.0	255.255.255.224 /27	102.1 – 102.30	192.168.102.31
GWA-2	192.168.102.32	255.255.255.224 /27	102.33 – 102.62	192.168.102.63
Server-Side Site Network				
SSS	192.168.102.64	255.255.255.240 /28	102.64 – 102.78	192.168.102.79

Point-to-Point Links

Networks L3-Switches - Routers	
Link	**Network**
HQ-Router – HQ-L3-SW1	192.168.102.80 /30
HQ-Router – HQ-L3-SW2	192.168.102.84 /30
Branch-Router – Branch-L3-SW1	192.168.102.88 /30
Branch-Router – Branch L3-SW2	192.168.102.92 /30
HQ-Router – Branch-Router	192.168.102.96 /30

Networks Routers – ISP Routers	
Pool of public addresses	195.136.17.0 /30
	195.136.17.4 /30
	195.136.17.8 /30
	195.136.17.12 /30

Ports Address Allocation

Device	Interface	IP Address	Subnet Mask	Default GW
HQ-Multilayer-1	Gig 0/1	192.168.102.81	255.255.255.252	
HQ-Multilayer-2	Gig 0/1	192.168.102.85	255.255.255.252	
Branch-Multilayer-1	Gig 1/0/1	192.168.102.93	255.255.255.252	
Branch-Multilayer-2	Gig 1/0/1	192.168.102.97	255.255.255.252	
HQ Router	Gig 0/0	192.168.102.82	255.255.255.240	
	Gig 0/1	192.168.102.86	255.255.255.252	
	Gig 0/2	192.168.102.65	255.255.255.252	
	Se 0/0/0	195.136.17.1	255.255.255.252	
	Se 0/0/1	195.136.17.5	255.255.255.252	
	Se 0/1/0	192.168.102.89	255.255.255.252	
Branch Router	Gig 0/0	192.168.102.94	255.255.255.252	
	Gig 0/1	192.168.102.98	255.255.255.252	
	Se 0/0/0	195.136.17.13	255.255.255.252	
	Se 0/0/1	195.136.17.9	255.255.255.252	
	Se 0/1/0	192.168.102.90	255.255.255.252	
ISP-1	Se 0/0/0	195.136.17.2	255.255.255.252	
	Se 0/0/1	195.136.17.10	255.255.255.252	
ISP-2	Se 0/0/0	195.136.17.14	255.255.255.252	
	Se 0/0/1	195.136.17.6	255.255.255.252	
DHCP Server	Fa0	192.168.102.67	255.255.255.240	192.168.102.65
DNS Server	Fa0	192.168.102.68	255.255.255.240	192.168.102.65
Email Server	Fa0	192.168.102.69	255.255.255.240	192.168.102.65
Web Server	Fa0	192.168.102.70	255.255.255.240	192.168.102.65

DHCP Server Pools

HQ Network				
Department	**Defaul Gateway**	**Start IP Addresss**	**Subnet Mask**	**Number of Devices**
MLOCS Pool	192.168.100.1	192.168.100.5	255.255.255.192 /26	58
MER Pool	192.168.100.65	192.168.100.70		58
MRM Pool	192.168.100.129	192.168.100.134		58
IT Pool	192.168.100.193	192.168.100.197		58
CS Pool	192.168.101.1	192.168.101.5		58
GWA-1 Pool	192.168.101.65	192.168.101.68		58
Branch Network				
NSO Pool	192.168.101.129	192.168.101.134	255.255.255.224 /27	26
HL Pool	192.168.101.161	192.168.101.163		26
HR Pool	192.168.101.193	192.168.101.195		26
MK Pool	192.168.101.224	192.168.101.226		26
FIN Pool	192.168.102.1	192.168.102.3		26
GWA-2	192.168.102.33	192.168.102.35		26