**Advanced Diploma of Information Technology**

**ICTNWK541 Assessment**

**Assessment Task 2: Project Portfolio**

**Manuel Sergio Perez Espitia**

**March 20th 2025, Melbourne, Victoria, Australia**

**ABC Enterprises WAN Expansion**



ABC Enterprises is a growing company with headquarters in Melbourne and two branch offices in Sydney and Brisbane. The company currently operates with an outdated network infrastructure that lacks secure, reliable WAN connectivity between sites. The IT department has been tasked with designing, implementing, and securing a new WAN infrastructure that ensures:

* Secure VPN connectivity between all sites.
* Optimised bandwidth usage with reliable routing protocols.
* Proper IPv6 deployment for future scalability.
* Enhanced security mechanisms including firewall rules and access control lists (ACLs).
* Troubleshooting and monitoring tools to detect and rectify network issues efficiently.

As part of the project, you will act as a network engineer responsible for implementing the required WAN connectivity for ABC Enterprises.

# Simulation Software & Tools:

Software installed to develop this protect.

* Cisco Packet Tracer 8.2.2
* Ubuntu 24.04 LTS
* Wireshark 4.2.2

# Network Design Review & Planning

## Network Details

### Topology and type

* Sydney Branch: LAN - Dual-Star
* Brisbane Branch: LAN - Star

### Network Nodes

|  |  |  |
| --- | --- | --- |
| **Type** | **Quantity** | **Location** |
| PC | n | Sydney |
| Laptop | n | Sydney |
| Smartphone | n | Sydney |
| Tablet | n | Sydney |
| Printer | 1 | Sydney |
| Switch | 4 | Sydney |
| Switch Multi-layer | 2 | Sydney |
| W Access Point | 2 | Sydney |
| Router | 2 | Sydney |
| Laptop | n | Brisbane |
| Smartphone | n | Brisbane |
| Tablet | n | Brisbane |
| Switch | 2 | Brisbane |
| W Access Point | 2 | Brisbane |
| Router | 1 | Brisbane |
| Cloud Cluster | 1 | ABC Enterprises |

## Legal And Security Protocol

## Installation Plan

# WAN Configuration

## General Implementations

1. Rename all devices:   
   sw (switches), rt (souters), ap (Wireless Access Points), ss ( Servers)
2. Install 2 servers to: DHCP, DNS and (1) its own switch
3. Connect server’s switch and both switch multi-layer
4. Implement Secure Access by SSH
5. Implement Additional Protocols: DHCPv6, IPv6
6. Implement Additional Protocols: LACP
7. Implement Additional Protocols: HSRPv2 IPv6

## Implement Firewalls

## WAN Protocols: PPP, VPN Site-To-Site, ADSL

## Additional Protocols: DHCPv6, IPV6

### Router 1

Firstly, IPv6 will be enable and then DHCPv6 will be set up

enable

configure terminal

hostname rt1

ipv6 unicast-routing

interface gigabitEthernet 0/0

ipv6 address 2000::2/64

no shutdown

ipv6 dhcp pool STATEFUL\_POOL

domain-name milestones.com

dns-server 2000::10

prefix-delegation pool STATEFUL\_POOL

exit

interface gigabitEthernet 0/0

ipv6 dhcp server STATEFUL\_POOL

ipv6 nd managed-config-flag

exit

exit

exit

## Implement Additional Protocols: LACP

Implementation of Link Aggregation Control Protocol (LACP) on links:

* swm1 gigabitEthernet 1/0/22 – swm2 gigabitEthernet 1/0/22
* swm1 gigabitEthernet 1/0/23 – swm2 gigabitEthernet 1/0/23
* swm1 gigabitEthernet 1/0/24 – swm2 gigabitEthernet 1/0/24

The LACP link will be the **channel-group** number **1** on both switches.

### Switch Main 1 (swm1)

enable

configure terminal

interface range gigabitEthernet 1/0/22, gigabitEthernet 1/0/23, gigabitEthernet 1/0/24

channel-group 1 mode active

exit

interface Port-channel 1

switchport mode trunk

exit

do wr

exit

exit

enable

configure terminal

interface gigabitEthernet 1/0/1

switchport

no shutdown

Exit

Do wr

exit

### Switch Main 2 (swm2)

enable

configure terminal

interface range gigabitEthernet 1/0/22, gigabitEthernet 1/0/23, gigabitEthernet 1/0/24

channel-group 1 mode passive

exit

interface Port-channel 1

switchport mode trunk

exit

do wr

exit

exit

enable

configure terminal

interface gigabitEthernet 1/0/1

switchport

no shutdown

Exit

Do wr

exit

## Implement Additional Protocols: HSRPv2 IPv6

* HSRP IPv6 Address: 2000::1/64
* R1 gigabitEthernet 0/0 : 2000::2 (primary router)
* R2 gigabitEthernet 0/0 : 2000::3 (secondary router)

### Router 1 (rt1)

enable

configure terminal

interface gigabitEthernet 0/0

ipv6 address 2000::2/64

standby version 2

standby 1 ipv6 autoconfig

standby 1 priority 120

no shutdown

Exit

Do wr

exit

exit

## Implement Network Topology

# Network Security Implementation

## Apply Access Control Lists (ACLS)

## Secure Access By SSH

### Switch 1

enable

configure terminal

service password-encryption

username administrator password cisco

ip domain-name netacad.pka

hostname sw1

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

line vty 0 15

transport input ssh

login local

exit

do wr

#### test: ssh -l admin <ip\_switch>

### Switch 2

enable

configure terminal

service password-encryption

username administrator password cisco

ip domain-name netacad.pka

hostname sw2

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

line vty 0 15

transport input ssh

login local

exit

do wr

exit

exit

#### test: ssh -l admin <ip\_switch>

### Switch 3

enable

configure terminal

service password-encryption

username administrator password cisco

ip domain-name netacad.pka

hostname sw3

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

line vty 0 15

transport input ssh

login local

exit

do wr

exit

exit

#### test: ssh -l admin <ip\_switch>

### Switch 4

enable

configure terminal

service password-encryption

username administrator password cisco

ip domain-name netacad.pka

hostname sw4

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

line vty 0 15

transport input ssh

login local

exit

do wr

exit

exit

#### test: ssh -l admin <ip\_switch>

### Switch 5

enable

configure terminal

service password-encryption

username administrator password cisco

ip domain-name netacad.pka

hostname sw5

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

line vty 0 15

transport input ssh

login local

exit

do wr

exit

exit

#### test: ssh -l admin <ip\_switch>

### Multi-layer Switch 1

Before configure, install AC-POWER-SUPPLY module.

enable

configure terminal

service password-encryption

username administrator password cisco

ip domain-name netacad.pka

hostname swm1

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

line vty 0 15

transport input ssh

login local

exit

do wr

exit

exit

#### test: ssh -l admin <ip\_switch>

### Multi-layer Switch 2

Before configure, install AC-POWER-SUPPLY module.

enable

configure terminal

service password-encryption

username administrator password cisco

ip domain-name netacad.pka

hostname swm2

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

line vty 0 15

transport input ssh

login local

exit

do wr

exit

exit

#### test: ssh -l admin <ip\_switch>

# Troubleshooting & Testing:

## Testing WAN Connectivity

# Bibliography