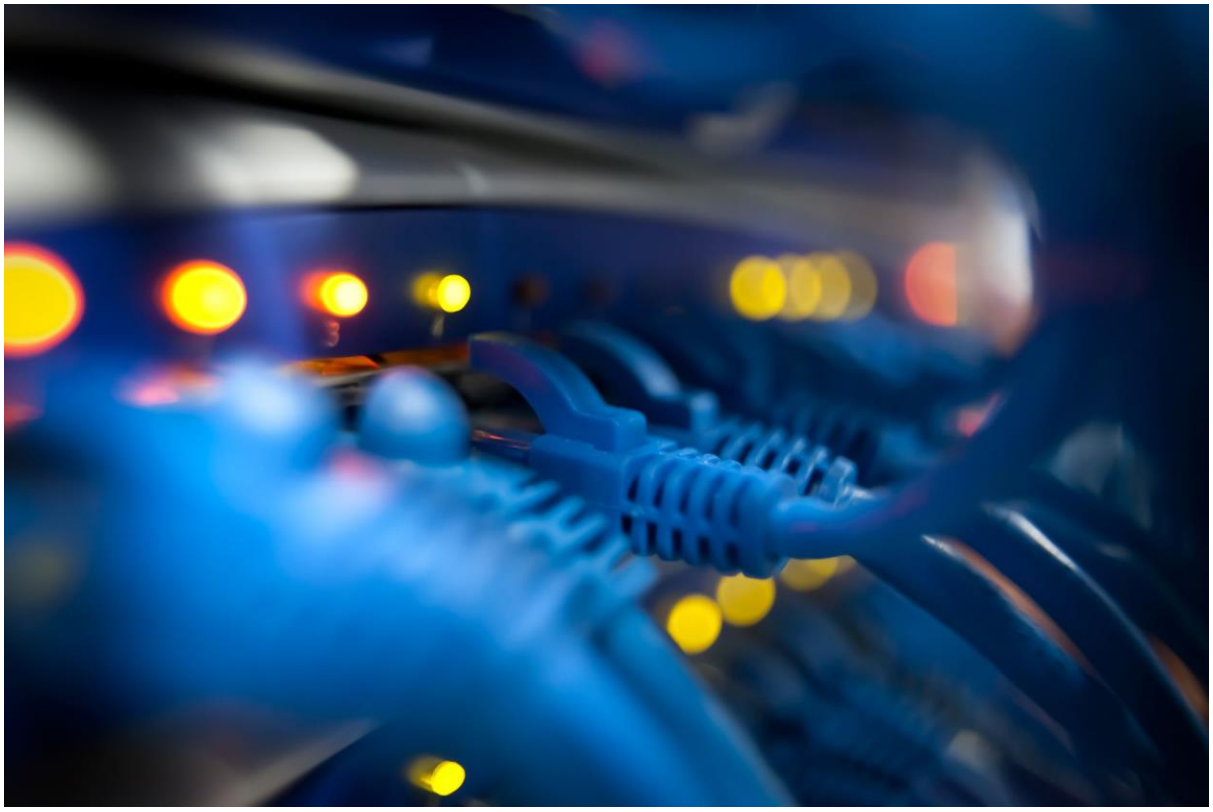


CASE STUDY REPORT

TNE20002 | NETWORK ROUTING PRINCIPLES

Contents

Case Study Group

Group: G02

Lab Class: Friday 8:30 ATC328

Class Tutor: Peter Granville

Group Members

Shaugato Paroi 103523487

Chaitanya Sood 103501933

Ashim Adhikari 104104333

Prabesh Bhattarai 104085535

Specification Information

Specification Number:	12.2
Class A Internal network address:	77.32.0.0/19
Class B NAT pool public address:	157.2.0.0/21
Class C ISP network connection address:	207.12.2.0/30
Class B ISP Internet Web Server address:	157.17.12.0/30
Wireless Deployment Site:	Perth
Management VLAN Number:	33
Percentage Growth (VLSM):	30

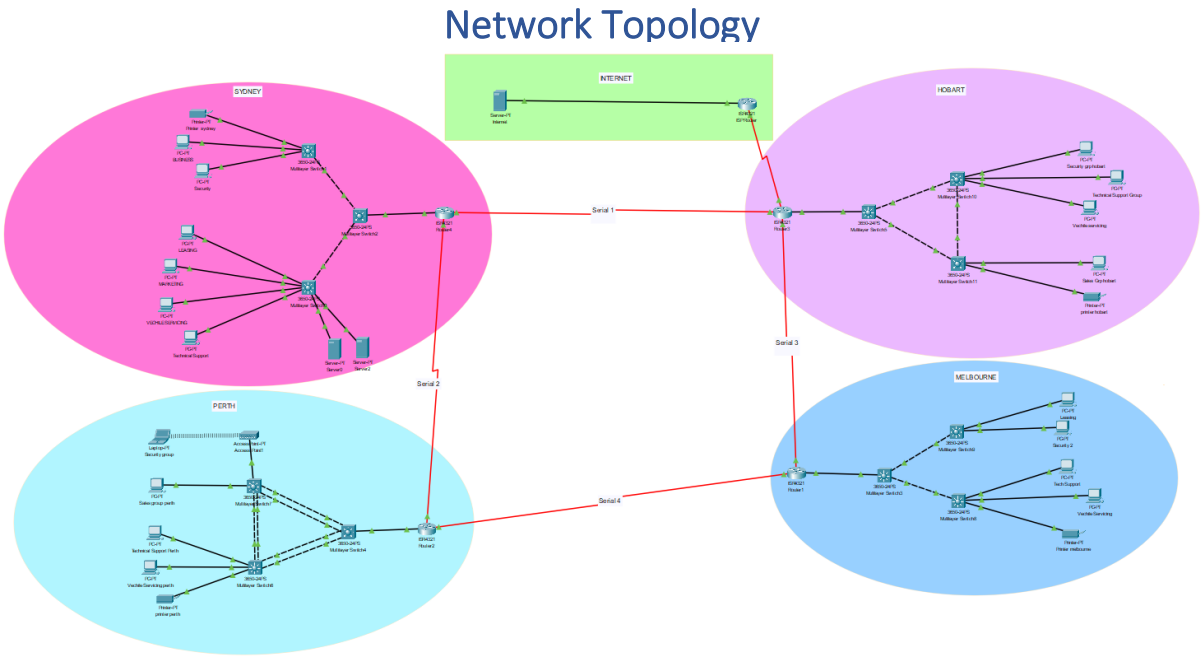


Figure 1 - Network Topology

Our network infrastructure spans four different sites: Sydney, Perth, Melbourne, and Hobart. Each site has a unique network topology, with the Hobart router as the gateway router. The internal routers of Sydney and Melbourne are directly connected to the Hobart gateway router. In contrast, the internal router of Perth is connected to the internal routers of Sydney and Perth. This connection enables Perth's internal router to access the gateway router indirectly.

Furthermore, the Hobart gateway router is connected to an ISP router, which provides access to the ISP server and the internet. This setup allows all devices across the four sites to connect to the ISP server and access the internet. Detailed topological descriptions of each area will be provided separately, outlining the specific network configurations at each location.

SYDNEY TOPOLOGY

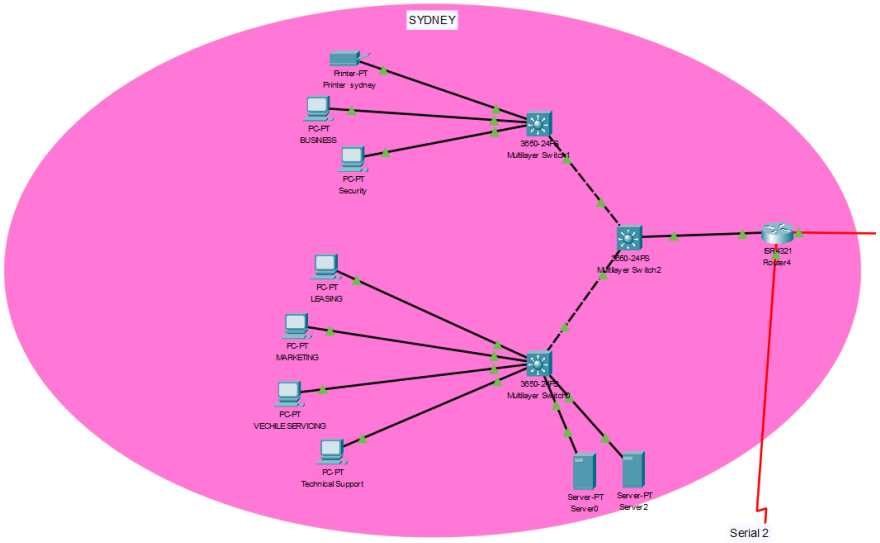


Figure 2- Sydney Topology

The network topology in Sydney maximizes switch and router usage for efficient communication across VLANs on every floor. Access layer switches are installed on each floor and connected to a distribution layer switch connected to a router. The VLANs were configured on each access layer switch to connect PCs to the designated VLAN. We also have two server farms, which are connected to one of the access layer switches as well. This hierarchical structure optimizes network traffic management.

PERTH TOPOLOGY

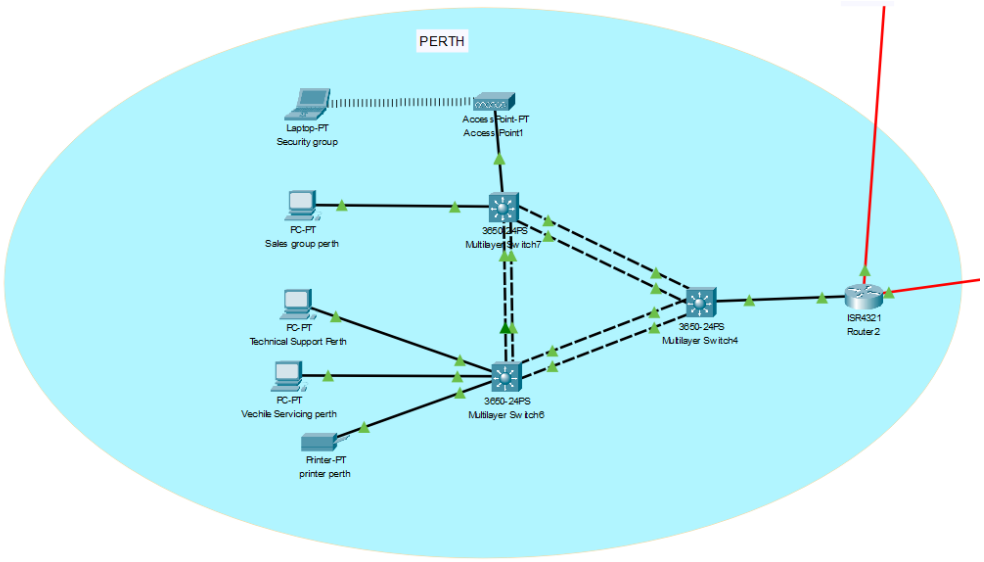
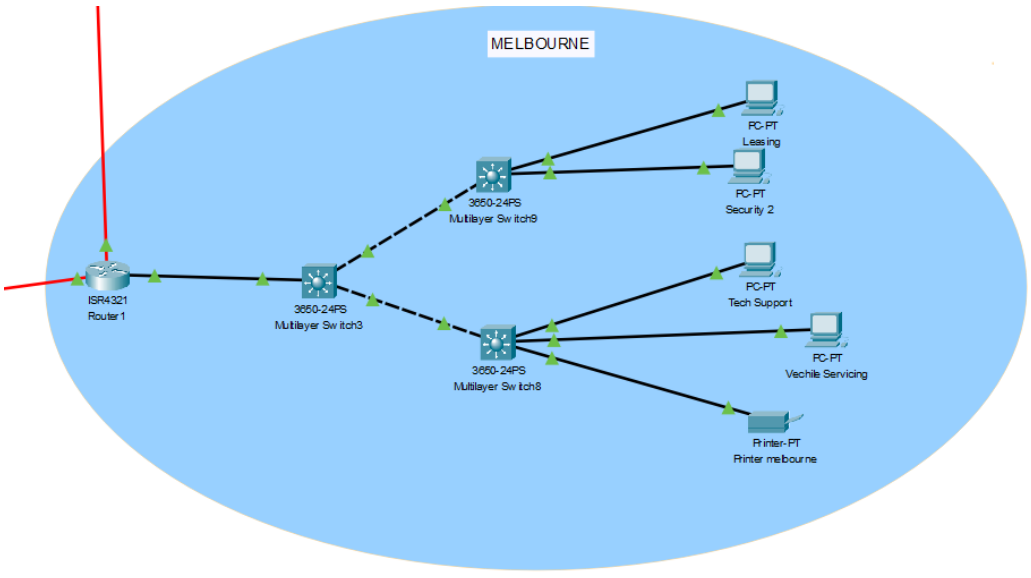


Figure 3-Perth Topology

Perth's network topology consists of a wireless access point connected to an access layer switch. The network also has two access layer switches and one distribution layer switch connected to the router. To improve network performance, we created an EtherChannel bundling to combine the three switches. VLANs were implemented based on the network requirements for the access layer switches. Additionally, a PC was connected to the specified VLANs to segregate network traffic and testing purposes. This configuration optimizes network performance, improves security, and simplifies network management.

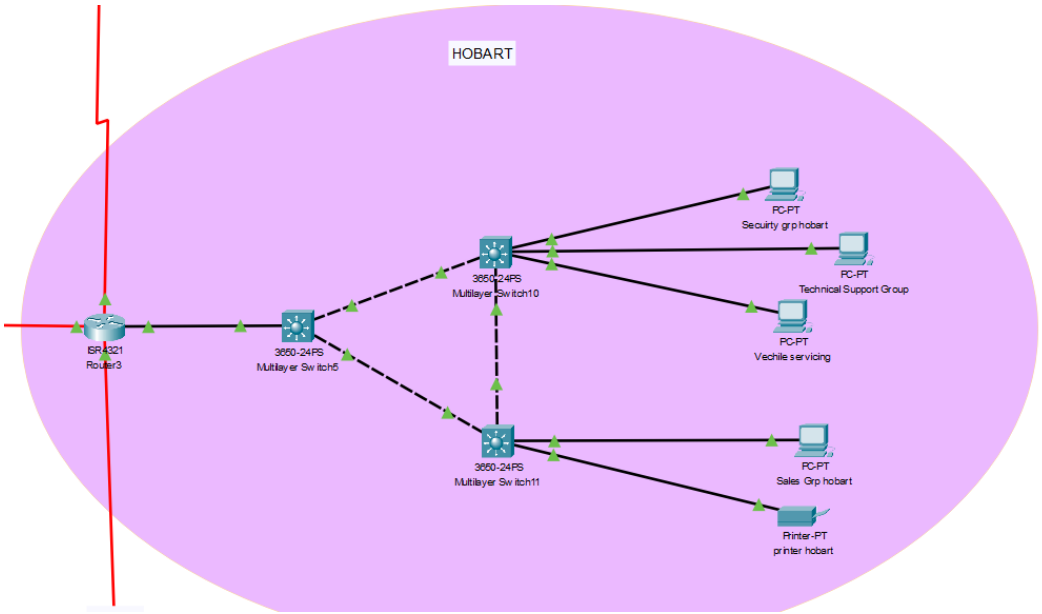
MELBOURNE TOPOLOGY



In Melbourne, the network setup consists of two access layer switches and one distribution layer switch. The access layer switches are linked to the distribution layer switch connected to the router. We set up VLANs on the access layer switches to meet the network requirements, and a PC was connected to a specific VLAN for testing purposes.

Since there is no direct link between the two access layer switches, Spanning Tree Protocol (STP) is not required. This network arrangement ensures excellent performance, enhances security, and simplifies network administration.

HOBART TOPOLOGY



Hobart's network topology features two interconnected access layer switches and one distribution layer switch. Both access layer switches are linked, while the distribution layer switch is connected to both access layer switches and the router (We also defined this as a gateway router). This configuration introduces a redundant link, necessitating STP (Spanning Tree Protocol) to prevent broadcast storms and ensure network stability.

Moreover, VLANs have been implemented in each access layer switch to segregate network traffic and enhance security. A PC has been connected to the designated VLAN, effectively isolating its traffic within the specified network segment. The network achieves improved redundancy, optimized performance, and enhanced manageability by employing STP and VLANs.

.

IP VLSM Design

In the case study, the team was instructed to subnet the provided internal network to accommodate Best Motors Ltd.'s expanding needs. Best Motors Ltd. leases, buys, sells, and repairs vehicles, trucks, and buses. The company has offices in Melbourne, Sydney, Hobart, and Perth, with its Head Office in Sydney.

We used Variable Length Subnet Masking (VLSM) to subnet the provided network, dividing it into smaller subnets of various sizes, each with its subnet mask. VLSM allowed us to use the IP addresses that were available effectively. The company provided the team with a Class A internal network

address, and by using VLSM, we allocated IP addresses to all the 1312 hosts in total. We divided the major network into subnets based on each site's requirements. [Table A: VLSM Design]

Sydney		
Vlan	Numbers of host	Number of Host After Growth
Leasing Group	125	163
Marketing Group	180	234
Business Group	200	260
Security Group	5	7
Technical Support Group	5	7
Vehicle Service group	5	7
Server Farm_1	10	13
Server Farm_2	10	13
Management	15	20
Printer	1	2
Melbourne		
Leasing Group	80	104
Security Group	5	7
Technical Support Group	5	7
Vehicle_Servicing Group	5	7
Management	15	20
Printer	1	2
Perth		
Sales Group	140	182
Security Group	5	7
Technical Support Group	5	7
Vehicle Servicing Group	5	7
Management	15	20
Printer	1	2
Hobert		
Sales Group	125	163
Security group	5	7
Technical Support Group	5	7
Vehicle Servicing Group	5	7
Management	15	20
Printer	1	2

The above table shows that an extra 30% of space was allocated to every subnet to support potential growth over the next five years. Hence, the total number of hosts required was the number of hosts after adding in the 30% extra space.

We also used 2 Server VLANs for the Server Farm at the Sydney Site. We also included these in the IP address space in our VLSM and allocated 20 hosts for the management VLANs and two hosts for the printer VLANs at every location.

For Example, Sydney Leasing Group required 125 hosts + 30% Extra Space = 163 Hosts.

Hence, the IP address for future use will be 77.32.4.164 – 77.32.4.254.

Routing Protocols

Routers use protocols or rules known as network routing protocols to identify the best route for delivering network traffic. These protocols help routers to build and maintain routing tables which contain information about available network paths and their associated metrics and costs. There are various routing protocols, such as RIP, EIGRP and OSPF. We used OSPF as the routing protocol in our network implementation.

Open Shortest Path First (OSPF) is a link-state routing protocol, which means that routers exchange information about the state of their links with neighbouring routers. The bandwidth on all internal router serial links has been set to 256, and all the VLAN sub-interfaces have been designated as passive interfaces not to send any unnecessary updates to the VLANs.

The link between the Sydney and Hobart Routers has the OSPF MD5 authentication, which utilizes the MD5 algorithm to create a unique hash value based on the content and password of each OSPF packet. This hash value is included in the packet and sent to the receiving end, which computes its value. The packet is not changed if the calculated and received hash values are the same, ensuring message integrity. This method enhances security and maintains data integrity.

A default route has been configured from Hobart Router to the ISP Router, which means that when a router cannot find any other suitable route in its routing table to forward an incoming packet, it resorts to the default route. As a result, any packet that arrives at the router without a corresponding entry in the routing table will not be discarded but forwarded to ISP.

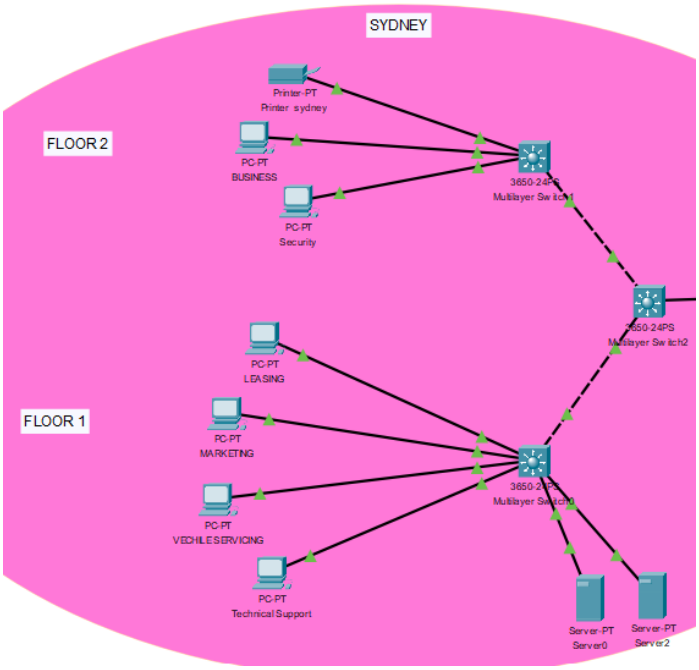
More information on routers can be found in [Table C: Router Details]

Switches: VLANs, STP, EtherChannel

VLANs

The team implemented Virtual Area Networks (VLANs) in every location to segment the network into smaller networks for each group in all the sites, allowing devices to be grouped based on the group they belong to. Also, implementing VLANs helps reduce security risks as each group operates as an independent broadcast domain. VLAN 33 was assigned as the management VLAN at every location. All unallocated switch ports were administratively shut down to follow good practices.

SYDNEY VLANs



In Sydney, we made the VLANs as per requirements. As you can see, the VLANs on the top switch, floor two, were named starting with 1X.

```
11   Business                         active    Gig1/0/2
12   Printer                          active    Gig1/0/1
13   Security                         active    Gig1/0/3
33   Management                       active
```

VLANs on the bottom switch which is floor 1 were named starting with 2X.

```
21   Leasing                          active    Gig1/0/24
22   Marketing                        active    Gig1/0/23
23   VechileServicing                 active    Gig1/0/22
24   TechnicalSupport                 active    Gig1/0/21
25   Server0                          active    Gig1/0/20
26   Server2                          active    Gig1/0/19
33   Management                       active
```

PERTH VLANs

In Perth, all the VLANs were named starting with 4X.

```
33   Management                       active
41   Sales                            active
42   Security                         active
43   TechnicalSupport                 active
44   Vehicle                          active
45   Printer                          active
```

MELBOURNE VLANs

In Melbourne, all the VLANs were named starting with 5X.

```
33   Management                       active
51   Leasing                          active
52   Security                         active
53   VechileServicing                 active
54   Printer                          active
55   Tech_Support                     active
```

Additionally, the access switch ports of the Melbourne site have been configured with port security, which helps prevent unauthorized devices from connecting to the network. The violation protection was used, meaning the switch will drop any packet from an unknown MAC address. Mac-address sticky ensures that the MAC addresses are learnt dynamically from the connected devices.

HOBART VLANs

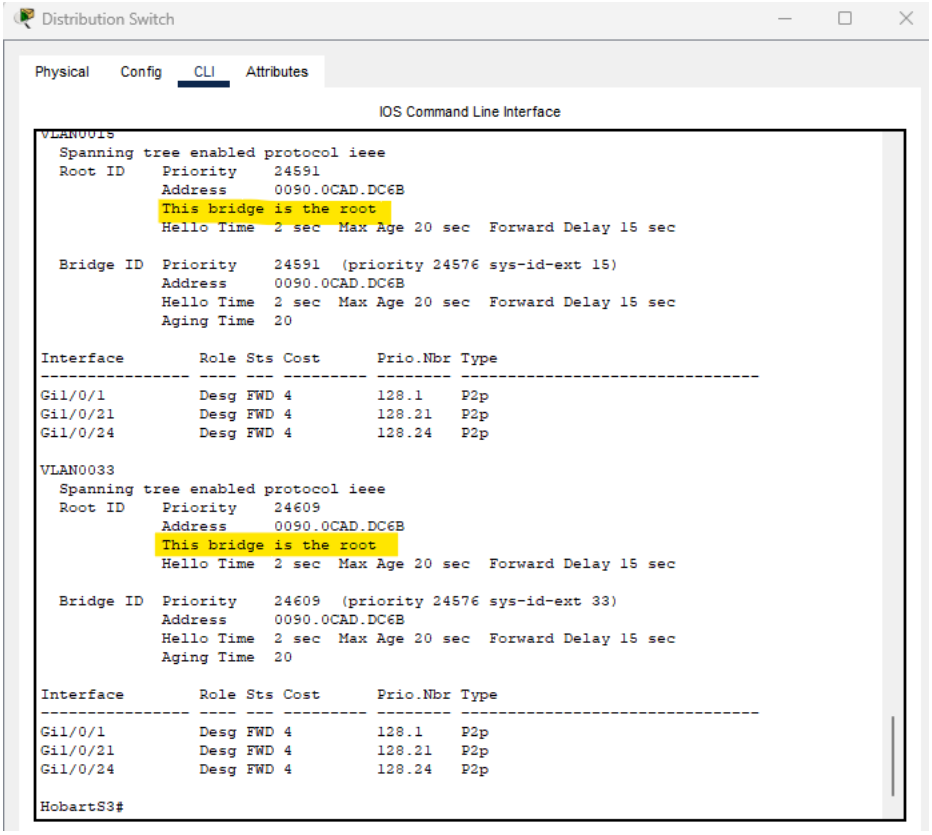
In Hobart, all the VLANs were named starting with 1X.

```
11   Security                         active
12   Technical_Support                active
13   Vehicle_Servicing                active
14   Sales_Group                      active
15   Printer                          active
33   Management                       active
```

For more information [Table B: Switch Details]

STP

Spanning tree Protocol (STP) is a Layer 2 protocol that is used to prevent Layer 2 loops caused by redundant links between the switches. The looping of frames can cause problems such as MAC table instability, broadcast storm and multiple Frame transmissions. We configured STP in the Hobart site and made the Distribution switch the root bridge as per the requirements. The switch directly connected to the router is called the distribution switch (HobartS3); the others are the access layer switches (HobartS1 and HobartS2).



EtherChannel

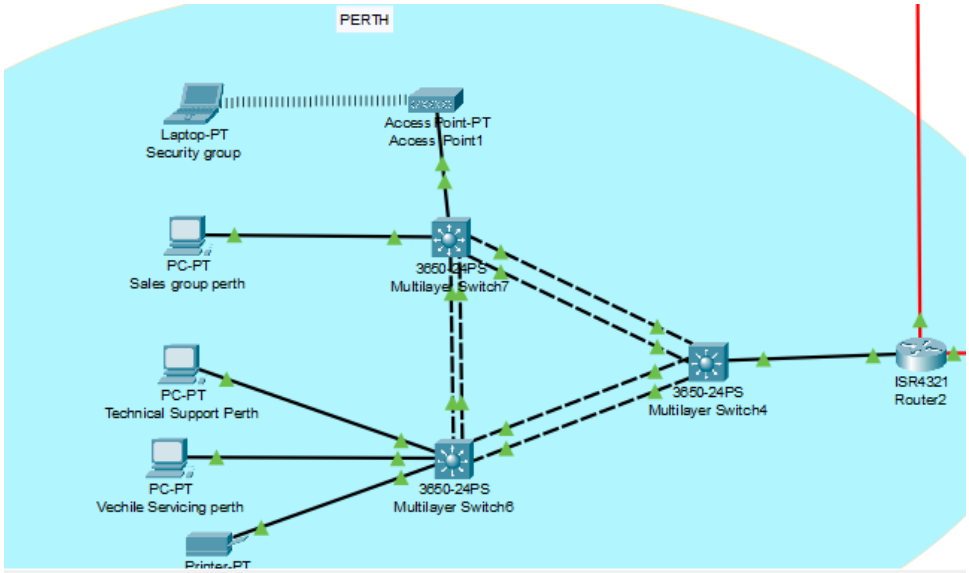
EtherChannel is a protocol used for Link Aggregation, a technology that combines multiple physical Ethernet links into a single logical link. It provides increased bandwidth, improved fault tolerance and enhanced load-balancing capabilities. It is generally used to aggregate various parallel links into a single logical link. Using EtherChannel has excellent advantages in a network:

1. Increased bandwidth – It aggregates multiple physical links into a single logical link, allowing higher data transfer rates and improving network performance.

2. Improved fault tolerance- EtherChannel provides adequate network reliability by providing redundant links.

3. Scalability: EtherChannel allows for easy scalability. As the administrator can add future links to the network, this protocol ensures that the network can adapt quickly to the growing requirements.

We have implemented LACP (Link Aggregation Control Protocol) in this network prototype. It is a standardized protocol defined by IEEE 802.3ad standard, which means multiple vendors support it. This protocol is implemented in Perth Site between the two access layer switches by bundling the two physical links into a single logical link between each end.



Here, on viewing the EtherChannel summary on PerthS1, we can identify the ports Gig1/0/1(P) and Gig1/0/5(P) have been bundled together with the other end having Gig1/0/2(P) and Gig (1/0/4) (P) with LACP protocol.

```
PerthS1#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-------------------------

1      Pol(SU)           LACP   Gig1/0/1(P) Gig1/0/2(P)
2      Po2(SU)           LACP   Gig1/0/3(P) Gig1/0/4(P)
```

Wireless LANs and Site Layout for the specified site

Wireless LANs

In the given scenario, Perth has been allocated as Wireless Deployment Site. We have implemented a wireless access point in the site, which is addressed in Table F. The Security group of the Perth Site have access to the network through the wireless connection between them and the access point. We have assigned a VLAN to the access point and configured it as inter-vlan routing to communicate within the network. The security group laptop is acting as a prototype in the topology to test the connection between them and the internal network of the Perth site.

The SSID of the access point is 'Hello', and the password given is '12345678'.

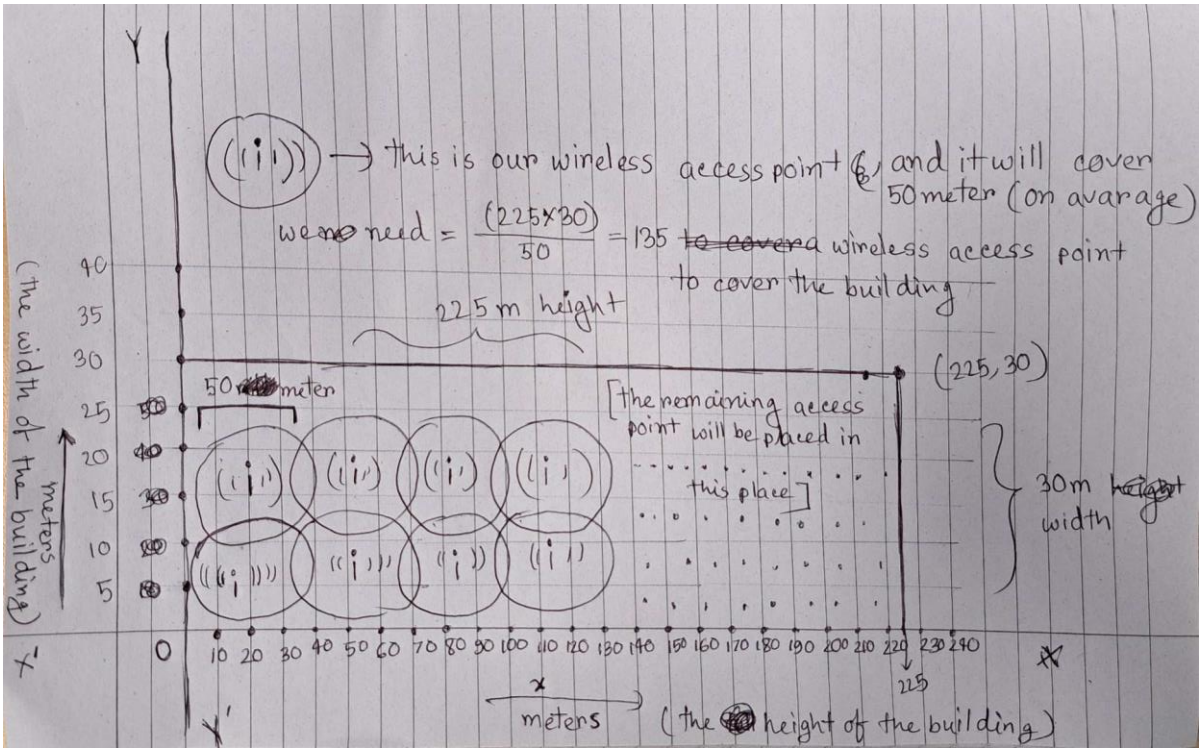
Site Layout for the specified site

The building floor size of the Perth site is 225 meters*30 meters, and the whole site area is 2000*2000 meters. To cover the wireless connectivity within the building, we need almost 135 access points. While in the future, if there is an expansion over the site to cover the end of the Perth Site, we need around 80,000 access points to cover the area with efficient wireless connectivity.

Note: Here, an access point coverage area is taken as 50 meters. The area coverage may face some hindrance by the number of users or any other circumstances.

No of access points required in the building = (225*30)/50= 135 access points

No of access points required across the site = (2000*2000)/50= 80,000 access points



DHCP

We configure DHCP in our internal router of Melbourne.

```
!
ip dhcp pool poolVLAN52
 network 77.32.7.48 255.255.255.240
 default-router 77.32.7.49
ip dhcp pool poolVLAN53
 network 77.32.7.176 255.255.255.240
 default-router 77.32.7.177
ip dhcp pool poolVLAN54
 network 77.32.7.228 255.255.255.252
 default-router 77.32.7.229
ip dhcp pool poolVLAN55
 network 77.32.7.112 255.255.255.240
 default-router 77.32.7.113
ip dhcp pool poolVLAN51
 network 77.32.6.0 255.255.255.128
 default-router 77.32.6.1
!
```

The commands above are configuring DHCP pools for different VLANs in Melbourne. DHCP stands for Dynamic Host Configuration Protocol, a standardized network protocol used to automatically assign IP addresses and other network configuration parameters to devices on a network.

The first line of each command creates a DHCP pool for a specific VLAN (Virtual Local Area Network). For example, the first command creates a pool for VLAN 52 named "poolVLAN52".

The "network" command specifies the IP address range for which the DHCP pool will be responsible. In each command, the second parameter specifies the subnet mask for the network. For instance, the second command sets the network range for VLAN 53 to 77.32.7.176/28.

The "default-router" command sets the default gateway (router) that the DHCP clients will use. In each command, the IP address specified after "default-router" is the default gateway for that specific VLAN.

These commands allow for the automatic assignment of IP addresses and default gateways for devices connected to each VLAN in the network.

The benefits of using DHCP

- Efficient IP Address Management
- Centralized Network administrations
- Scalability
- Flexibility
- Security

NAT:

Creating nat pool:

```
!NAT POOLFOR VLAN 11 Sydney
ip nat pool POOLVLAN11SYDNEY 157.2.0.1 157.2.1.10 netmask 255.255.248.0
!
!NAT POOLFOR VLAN 12 Sydney(PRINTER)
ip nat pool POOLVLAN12SYDNEY 157.2.1.11 157.2.1.14 netmask 255.255.248.0
!
!NAT POOLFOR VLAN 13 Sydney
ip nat pool POOLVLAN13SYDNEY 157.2.1.15 157.2.1.23 netmask 255.255.248.0
!
```

Creating access Control List for each vlan:

```
ip access-list extended ACLVLANSYDNEY11
permit ip 77.32.0.0 0.0.1.255 any
ip access-list extended ACLVLANSYDNEY12
permit ip 77.32.7.236 0.0.0.3 any
ip access-list extended ACLVLANSYDNEY13
permit ip 77.32.7.64 0.0.0.15 any
ip access-list extended ACLVLANSYDNEY21
permit ip 77.32.4.0 0.0.0.255 any
```

Establish Dynamic Source Translation by Binding the pool to the access control list

```
ip nat inside source list ACLVLANSYDNEY11 pool POOLVLAN11SYDNEY
ip nat inside source list ACLVLANSYDNEY12 pool POOLVLAN12SYDNEY
ip nat inside source list ACLVLANSYDNEY13 pool POOLVLAN13SYDNEY
ip nat inside source list ACLVLANSYDNEY21 pool POOLVLAN21SYDNEY
ip nat inside source list ACLVLANSYDNEY22 pool POOLVLAN22SYDNEY
ip nat inside source list ACLVLANSYDNEY23 pool POOLVLAN23SYDNEY
```

configuring inside and outside

```
int s0/1/0
ip nat inside
int s0/1/1
ip nat inside
int s0/2/1
ip nat inside
int g0/0/1
```

Command Breakdown:

- We have defined multiple NAT pools for different VLANs and locations. Each pool specifies a range of IP addresses that can be used for translation. For example, We have defined pools

for VLANs 11, 12, 13, and so on in different locations like Sydney, Hobart, Melbourne, and Perth. Each pool has a specified range of IP addresses and a corresponding subnet mask.

- Each NAT pool is assigned a unique name and associated with a specific VLAN on the network device. For example, "ip nat pool POOLVLAN11SYDNEY 157.2.0.1 157.2.1.10 netmask 255.255.248.0" defines a NAT pool named "POOLVLAN11SYDNEY" for VLAN 11 in Sydney, with a range of public IP addresses from 157.2.0.1 to 157.2.1.10 and a subnet mask of 255.255.248.0.
- Access Control Lists (ACLs): We have defined ACLs to control which traffic is subject to NAT. The ACLs specify source IP address ranges that are permitted for translation. Each VLAN or location has its ACL that allows traffic from specific source IP ranges to be translated. These ACLs are referenced in your NAT configuration to determine which traffic should undergo NAT.
- The range of IP addresses within each NAT pool is used to translate private IP addresses within the corresponding VLAN. For example, hosts in VLAN 11 in Sydney with private IP addresses in the range of 77.32.0.0/23 will be translated to a public IP address from the "POOLVLAN11SYDNEY" NAT pool when accessing the Internet.
- The subnet mask for each NAT pool determines the size of the IP address range and the number of hosts that can be translated using that pool.
- We have configured NAT inside and outside interfaces. The inside interfaces are where the traffic originates, and the outside interface faces the external network or the Internet.

Overall, the NAT configuration is used to provide Internet access to hosts within the network by translating their private IP addresses to public IP addresses. The NAT pools defined in the configuration enable this translation to occur in a controlled and organized manner, with each pool associated with a specific VLAN on the network device.

We didn’t use NAT / PAT overload method. Because we want to ensure the following:

We didn’t use NAT / PAT overload method. Because we want to ensure the following:

- Simplicity: Our implementation of NAT is simpler and easier to understand than the one outlined in the specs.
- Flexibility: Your implementation is more flexible as it can be easily scaled and modified.
- Security: Using one-to-one NAT, we have a more secure implementation as each server in the Server Farm has its unique public IP address. This reduces the risk of a single point of failure or a security breach affecting all servers.
- Debugging: Our implementation is easier to troubleshoot and debug in case of any issues.

Security and Access Control Policies

Security:

As per the requirements we implemented several security measurements in our Network Topology implementations.

Configuring SSH in Sydney:

SSH stands for Secure Shell, which is a network protocol used to establish a secure and encrypted connection between two networked devices. SSH provides a secure channel over an unsecured network by encrypting the traffic between the two devices and providing authentication mechanisms to ensure the devices are whom they claim to be.

We configure SSH for every switch in Sydney as per instructions. So, from the device, we can get access to the switches via *ssh -l casestudy <ip address's switch>*

The benefits of using SSH over Telnet are numerous. Telnet is an older protocol that provides no encryption or security mechanisms, which means that any data transmitted between the two devices is sent in clear text and can be intercepted by anyone with access to the network. SSH, on the other hand, encrypts all traffic between the two devices, providing a much higher level of security.

SSH configuration on Sydney distribution switch

```
Sydney_Switch_Distribution#sh access-lists
Standard IP access list ACLSSH
    10 permit 77.32.7.144 0.0.0.15
    20 deny any

Sydney_Switch_Distribution#
Sydney_Switch_Distribution#
```

SSH configuration on Sydney Floor 2 switch

```
Sydney_Switch_F2#sh access-lists
Standard IP access list ACLSSH
    10 permit 77.32.7.144 0.0.0.15
    20 deny any

Sydney_Switch_F2#
```

SSH configuration on Sydney Floor 1 switch

```
Sydney_Switch_F1#sh acc
Sydney_Switch_F1#sh access-lists
Standard IP access list ACLSSH
    10 permit 77.32.7.144 0.0.0.15
    20 deny any
```

Configuring Port-Security:

We configured port security for the Access Layer switch in Melbourne. To configure port security, we first enable the feature on the switch and then specify the number of allowed MAC addresses for each port.

The benefits of port security include increased network security by preventing unauthorized devices from accessing the network. It also helps prevent network attacks such as MAC spoofing, where attackers try to impersonate authorized devices by changing their MAC addresses.

Configuring CHAP and PPP:

We configure CHAP and PPP authentication between the Gateway router in Hobert and ISP router. CHAP (Challenge Handshake Authentication Protocol) and PAP (Password Authentication Protocol) are two authentication protocols used in Point-to-Point (PPP) communication to authenticate users or devices before establishing a connection. Configuring CHAP and PAP authentication ensures that only authenticated devices can establish a connection, preventing unauthorized access to the network. Additionally, CHAP is considered more secure than PAP as it uses a one-way hash function to encrypt the password during authentication, whereas PAP sends the password in clear text.

Access Control Policies (ACLs)

Access control lists are a feature used to filter and control traffic flow based on the rules applied. The router evaluates all network packets that pass through the interface as they move through it to see if they may be forwarded. There are a series of commands to filter packets.

In this project, we have configured ACLs to control and filter network traffics according to the requirements of the company Best Motors Ltd. The company had some criteria for IP traffic flow with its network and internet. As this was just a prototype network design, we implemented ACLs only at the Sydney site. The ACLs we configured are described briefly in the paragraph below.

We have designed to build 2 Server Farms in Sydney named Server0 and Server2. We have kept server0 in VLAN 25 and Server2 in VLAN 26. We have configured ACLs SydneyRouter so that server 0 is accessed by the Business, Printer, Security, Leasing, Marketing, and Vehicle Servicing groups. At the same time, the Security and Technical hosts can access both servers. We allowed server0 and server2 to be accessed by the security people and technicians because they need both servers for the maintenance and updating system.

As per the ACLs guide of the company, all the VLANs are permitted to the internet HTTP and ICMP we have not denied to the internet. But we denied and allowed ip traffic within the VLAN. We denied PC in Marketing hosts accessing Leasing hosts, but Marketing permits ping reply to the leasing. Furthermore, PC hosts on Vehicle Serving cannot access other VLAN hosts in Sydney, but we have permitted access from other hosts to the vehicle servicing VLAN. In addition, the Technical Support group cannot be accessed by any of the Pcs in any hosts in Sydney.

ACLs configuration on Sydney Router

```
SydneyRouter#sh ac
SydneyRouter#sh access-lists
Extended IP access list BUSINESS
    10 permit icmp 77.32.0.0 0.0.1.255 77.32.7.144 0.0.0.15 echo-reply
    20 deny ip 77.32.0.0 0.0.1.255 77.32.7.144 0.0.0.15
    30 deny ip 77.32.0.0 0.0.1.255 77.32.7.16 0.0.0.15
    40 permit ip any any
Extended IP access list PRINTER
    10 permit icmp 77.32.7.236 0.0.0.3 77.32.7.144 0.0.0.15 echo-reply
    20 deny ip 77.32.7.236 0.0.0.3 77.32.7.144 0.0.0.15
    30 deny ip 77.32.7.236 0.0.0.3 77.32.7.16 0.0.0.15
    40 permit ip any any
Extended IP access list Leasing
    10 permit icmp 77.32.4.0 0.0.0.255 77.32.7.144 0.0.0.15 echo-reply
    20 deny ip 77.32.4.0 0.0.0.255 77.32.7.144 0.0.0.15
    30 deny ip 77.32.4.0 0.0.0.255 77.32.7.16 0.0.0.15
    40 permit ip any any
Extended IP access list MARKETING
    10 permit icmp 77.32.2.0 0.0.0.255 77.32.7.144 0.0.0.15 echo-reply
    20 deny ip 77.32.2.0 0.0.0.255 77.32.7.144 0.0.0.15
    30 permit icmp 77.32.2.0 0.0.0.255 77.32.4.0 0.0.0.255 echo-reply
    40 deny ip 77.32.2.0 0.0.0.255 77.32.4.0 0.0.0.255
    50 deny ip 77.32.2.0 0.0.0.255 77.32.7.16 0.0.0.15
    60 permit ip any any
Extended IP access list SECURITY
    10 permit icmp 77.32.7.64 0.0.0.15 77.32.7.144 0.0.0.15 echo-reply
    20 deny ip 77.32.7.64 0.0.0.15 77.32.7.144 0.0.0.15
    30 permit ip any any
Extended IP access list VECHICLE
    10 permit icmp 77.32.7.208 0.0.0.15 77.32.0.0 0.0.1.255 echo-reply
    20 deny ip 77.32.7.208 0.0.0.15 77.32.0.0 0.0.1.255
    30 permit icmp 77.32.7.208 0.0.0.15 77.32.7.236 0.0.0.3 echo-reply
    40 deny ip 77.32.7.208 0.0.0.15 77.32.7.236 0.0.0.3
    50 permit icmp 77.32.7.208 0.0.0.15 77.32.7.64 0.0.0.15 echo-reply
    60 deny ip 77.32.7.208 0.0.0.15 77.32.7.64 0.0.0.15
    70 permit icmp 77.32.7.208 0.0.0.15 77.32.4.0 0.0.0.255 echo-reply
    80 deny ip 77.32.7.208 0.0.0.15 77.32.4.0 0.0.0.255
    90 permit icmp 77.32.7.208 0.0.0.15 77.32.2.0 0.0.0.255 echo-reply
    100 deny ip 77.32.7.208 0.0.0.15 77.32.2.0 0.0.0.255
    110 permit icmp 77.32.7.208 0.0.0.15 77.32.7.144 0.0.0.15 echo-reply (4 match(es))
    120 deny ip 77.32.7.208 0.0.0.15 77.32.7.144 0.0.0.15 (4 match(es))
    130 permit icmp 77.32.7.208 0.0.0.15 77.32.7.16 0.0.0.15 echo-reply (3 match(es))
    140 deny ip 77.32.7.208 0.0.0.15 77.32.7.16 0.0.0.15 (8 match(es))
    150 permit ip any any (8 match(es))
```

We have tested ACLs in Sydney site and it is perfectly working. There is the record of ACLs testing in the table below:

System Testing and Verification Strategy:

To test if the network is working correctly, we experimented with several commands and applied strategies for overcoming faults or bugs in the network.

In a switch:

Show ip interface brief: it shows the status of the interface.

Show VLAN brief: the VLANs and access ports configured to the particular VLAN.

Show interface trunk: shows the trunking port which is used for travelling traffic of different VLANs

Show etherchannel summary: shows configured EtherChannel interface, the protocol used LACP or PAgp.

While coming to the router, it's a bit complex because several things are configured, like Acls, routing protocols, DHCP pool, NAT pool, the IP address of serial links and sub-interface, etc.

Show ip interface brief: shows the IP address and status of the interface and sub-interface.

Show IP route: shows the routing table of the router, including network prefixes, subnet mask, next-hop address, and interface information.

Show ip ospf neighbour: this command shows the ip address, interface, and adjacency state.

Show ip access lists: Shows the ACLs configured and their name, types and configured rules. If the acls are not working, we can refer to this command to analyse our problem.

Show ip dhcp pool: shows the pool of addresses divided into several VLANs.

Show ip nat statistics: it displays related to nat translation and counters, including nat pool; if there is a problem with the translation, we can find it by this command.

Debug ip nat and show ip nat translations: this command verifies the private to public address translation. It is done in the gateway router where the nat pool is configured

Sh ip dhcp binding: this command displays which host is assigned with which IP address from the DHCP pool.

Ping <ip address>: this command ensures if that one end of the host can communicate with another host.

Appendices – Tables A to G

Table A: VLSM Design

Number of host addresses required	Subnet Network Address	Subnet Mask	Subnet Prefix	Max Number of Host Possible	Address Space Future Use Y/N	VLAN Name	Site Location
260	77.32.0.0	255.255.254.0	/23	510	Yes	Business-11	Sydney
2	77.32.7.236	255.255.255.252	/30	2	Yes	Printer-12	Sydney
7	77.32.7.64	255.255.255.240	/28	14	yes	Security-13	Sydney
163	77.32.4.0	255.255.255.0	/24	254	Yes	Leasing-21	Sydney
234	77.32.2.0	255.255.255.0	/24	254	Yes	Leasing-21	Sydney
7	77.32.7.208	255.255.255.240	/28	14	Yes	VehicleServicing-22	Sydney
7	77.32.7.144	255.255.255.240	/28	14	Yes	Technical_Support-24	Sydney
13	77.32.7.0	255.255.255.240	/28	14	Yes	Server0-25	Sydney
13	77.32.7.16	255.255.255.240	/28	14	Yes	Server-2	Sydney
20	77.32.6.224	255.255.255.224	/27	30	Yes	Management-33	Sydney
20	77.32.6.192	255.255.255.192	/27	30	Yes	Management-33	Perth
182	77.32.3.0	255.255.255.0	/24	254	Yes	Sales-41	Perth
7	77.32.7.80	255.255.255.240	/28	14	Yes	Security-42	Perth
7	77.32.7.128	255.255.255.240	/28	14	Yes	TechnicalSupport-43	Perth
7	77.32.7.192	255.255.255.240	/28	14	Yes	Vehicle-44	Perth
2	77.32.7.232	255.255.255.252	/30	2	Yes	Printer-45	Perth
20	77.32.6.160	255.255.255.224	/27	30	Yes	Management-33	Melbourne
104	77.32.6.0	255.255.255.128	/25	126	Yes	Leasing-33	Melbourne
7	77.32.7.48	255.255.255.240	/28	14	Yes	Security-52	Melbourne
7	77.32.7.176	255.255.255.240	/28	14	Yes	VehicleServicing-53	Melbourne
2	77.32.7.228	255.255.255.252	/30	2	Yes	Printer-54	Melbourne
7	77.32.7.112	255.255.255.240	/28	14	Yes	Tech_Support-55	Melbourne
7	77.32.7.32	255.255.255.240	/28	14	Yes	Security-11	Hobart
7	77.32.7.96	255.255.255.240	/28	14	Yes	Technical_Support-12	Hobart

7	77.32.7.160	255.255.255.240	/28	14	Yes	Vehicle Servicing	Hobart
163	77.32.5.0	255.255.255.0	/24	254	Yes	Sales_Group-14	Hobart
2	77.32.7.224	255.255.255.252	/30	2	Yes	Printer-15	Hobert
20	77.32.6.128	255.255.255.224	/27	30	Yes	Management-33	Hobert

Table B: Switch Details

Name	Model	# of Ports	Location	Management VLAN IP Address	Default Gateway IP Address	Management VLAN
Sydney_Switch_F2	3650_24PS	24	SYDNEY	77.32.6.227	77.32.6.225	33
Sydney_Switch_Distribution	3650_24PS	24	SYDNEY	77.32.6.226	77.32.6.225	33
Sydney_Switch_F1	3650_24PS	24	SYDNEY	77.32.6.228	77.32.6.225	33
PerthS1	3650_24PS	24	PERTH	77.32.6.195	77.32.6.193	33
PerthS3	3650_24PS	24	PERTH	77.32.6.194	77.32.6.193	33
PerthS2	3650_24PS2	24	PERTH	77.32.6.196	77.32.6.193	33
MelbourneS3	3650_24PS	24	Melbourne	77.32.6.162	77.32.6.161	33
MelbourneS2	3650_24PS	24	Melbourne	77.32.6.164	77.32.6.161	33
MelbourneS1	3650_24PS	24	Melbourne	77.32.6.163	77.32.6.161	33
HobartS3	3650_24PS	24	Hobart	77.32.6.130	77.32.6.129	33
HobartS2	3650_24PS	24	Hobart	77.32.6.131	77.32.6.129	33

HobartS1	3650_24PS	24	Hobart	77.32.6.132	77.32.6.129	33

Table C: Router Details

1.1. Site: Sydney Router Name: SydneyRouter

Interface/Sub Interface Type/ Number	Description and Purpose	Network/VLAN Name	Network Address	Interface IP address	Subnet Mask/ value
interface GigabitEthernet0/0/1	creating sub interface for Sydney				
interface GigabitEthernet0/0/1.11	creting sub interface for Vlan 11 - Business	Business	77.32.0.0	77.32.0.1	/23
interface GigabitEthernet0/0/1.12	creting sub interface for Vlan 12 - Printer	Printer	77.32.7.236	77.32.7.237	/30
interface GigabitEthernet0/0/1.13	creting sub interface for Vlan 13 - Security	Security	77.32.7.64	77.32.7.65	/28
interface GigabitEthernet0/0/1.21	sub interface for Leasing on Floor 1	Leasing	77.32.4.0	77.32.4.1	/24
interface GigabitEthernet0/0/1.22	sub interface for Marketing on Floor 1	Marketing	77.32.2.0	77.32.2.1	/24
interface GigabitEthernet0/0/1.23	sub interface for VehicleServicing on Floor 1	VechileServicing	77.32.7.209	77.32.7.209	/28
interface GigabitEthernet0/0/1.24	sub interface for TechnicalSupport on Floor 1	TechnicalSupport	77.32.7.144	77.32.7.145	/28

interface GigabitEthernet0/0/1.25	sub-interface vlan 25 Server0 for other vlans in sydney	Server0	77.32.7.0	77.32.7.1	/28
interface GigabitEthernet0/0/1.26	ub-interface vlan 26 Server2 for security and Techinical Support group	Server2	77.32.7.16	77.32.7.17	/28
interface GigabitEthernet0/0/1.33	sub interface for Management vlan 33	Management	77.32.6.224	77.32.6.225	/27
interface Serial0/1/0	serial to hobart		77.32.7.240	77.32.7.241	/30
interface Serial0/1/1	serial to Perth		77.32.7.244	77.32.7.246	/30

1.2. Site: Perth Router Name: PerthRouter

Interface/Sub Interface Type/ Number	Description and Purpose	Network/VLAN Name	Network Address	Interface IP address	Subnet Mask/ value
interface GigabitEthernet0/0/1	physical port to perth switches				
interface GigabitEthernet0/0/1.33	management vlan 33	Management	77.32.6.192	77.32.6.193	/27
interface GigabitEthernet0/0/1.41	sales vlan 41	Sales	77.32.3.0	77.32.3.1	/24
interface GigabitEthernet0/0/1.42	security vlan 42	Security	77.32.7.80	77.32.7.81	/28
interface GigabitEthernet0/0/1.43	Technical Support vlan 43	TechnicalSupport	77.32.7.128	77.32.7.129	/28

interface GigabitEthernet0/0/1.44	Vehicle Servicing VLAN 44	Vehicle	77.32.7.192	77.32.7.193	/28
interface GigabitEthernet0/0/1.45	Printer VLAN 45	Printer	77.32.7.232	77.32.7.233	/30
interface Serial0/1/0	serial interface from Perth to Melbourne		77.32.7.244	77.32.7.245	/30
interface Serial0/1/1	serial interface from perth to melbourne		77.32.7.252	77.32.7.254	/30

1.3. Site: Melbourne Router Name: MelbourneRouter

Interface/Sub Interface Type/ Number	Description and Purpose	Network/VLAN Name	Network Address	Interface IP address	Subnet Mask/ value
Interface GigabitEthernet0/0/1	Physical port to Melbourne switches				
interface GigabitEthernet0/0/1.33	vlan 33 Management	Management	77.32.6.160	77.32.6.161	/27
interface GigabitEthernet0/0/1.51	vlan 51 Leasing	Leasing	77.32.6.0	77.32.6.1	/25
interface GigabitEthernet0/0/1.52	vlan 52 Security	Security	77.32.7.48	77.32.7.49	/28
interface GigabitEthernet0/0/1.53	vlan 53 Vehicle Servicing	VechileServicing	77.32.7.176	77.32.7.177	/28
interface GigabitEthernet0/0/1.54	vlan 54 Printer	Printer	77.32.7.228	77.32.7.229	/30
interface GigabitEthernet0/0/1.55	vlan 55 TechnicalSupport	Tech_Support	77.32.7.112	77.32.7.113	/28

interface Serial0/1/0	serial link from Melbourne to Perth		77.32.7.252	77.32.7.253	/30
interface Serial0/1/1	serial link from Melbourne to Hobart		77.32.7.248	77.32.7.250	/30

1.4. Site: Hobart Router Name: HobartRouter

Interface/Sub Interface Type/ Number	Description and Purpose	Network/VLAN Name	Network Address	Interface IP address	Subnet Mask/ value
interface GigabitEthernet0/0/1	Physical port to Hobart switches				
interface GigabitEthernet0/0/1.11	creating sub innterface for Vlan 11 - Security Vlan	Security	77.32.7.32	77.32.7.33	/28
interface GigabitEthernet0/0/1.12	creating sub innterface for Vlan 12 - TechSupport Vlan	Technical_Support	77.32.7.96	77.32.7.97	/28
interface GigabitEthernet0/0/1.13	creating sub innterface for Vlan 13 - Vehicle Servicing Vlan	Vehicle_Servicing	77.32.7.160	77.32.7.161	/28
interface GigabitEthernet0/0/1.14	creating sub innterface for Vlan 14 - Sales Group Vlan	Sales_Group	77.32.5.0	77.32.5.1	/24
interface GigabitEthernet0/0/1.15	creating sub innterface for Vlan 15 - Printer Vlan	Printer	77.32.7.224	77.32.7.225	/30
interface GigabitEthernet0/0/1.33	creating sub innterface for Vlan 33 -	Management	77.32.6.128	77.32.6.129	/27

	Management Vlan				
interface Serial0/1/0	serial to sydney		77.32.7.240	77.32.7.242	/30
interface Serial0/1/1	serial to Melbourne		77.32.7.248	77.32.7.249	/30
interface Serial0/2/0	serial to isp		207.12.2.0	207.12.2.1	/30

1.5. Site: Internet Router Name: ISP

Interface/Sub Interface Type/ Number	Description and Purpose	Network/VLAN Name	Network Address	Interface IP address	Subnet Mask/ value
interface GigabitEthernet0/0/1	link to web server		157.17.12.0	157.17.12.1	/30
interface Serial0/1/0	serial to gateway		207.12.2.0	207.12.2.2	/30

Table D: Melbourne DHCP Server Pool IP Host Address

VLAN Name	IP Address Pool Range	Subnet Mask /value	Default Gateway IP Address
Security	77.32.7.48	/28	**77.32.77.49**
Vehicle Servicing	77.32.7.176	/28	**77.32.7.177**
Printer	77.32.7.228	/30	**77.32.7.228**
Tech Support	77.32.7.112	/28	**77.32.7.113**
Leasing	77.32.6.0	/25	**77.32.6.1**

Table E: Statically assigned IP Host Addresses

Server/Printer Name	In which VLAN	IP Address	Subnet Mask /Value	Default Gateway IP Address	Service/s Provided
Server0	Vlan-25	77.32.7.2	255.255.255.240	77.32.7.1	157.2.6.1
Server2	Vlan-26	77.32.7.188	255.255.255.240	77.32.7.17	157.2.7.1

Table F: Wireless Access Point Details

Name	Model	SSID	Channel
Wireless	Access Point	hello	2.4 GHZ=6

Table G: Record of ACL Testing (Sydney)

Source Host	Destination Host/Server	Protocol	Expected Result Permitted/Denied	Achieved Yes/No
Security and Technical group both can access	Server0 and Server2	ICMP	Permitted	Yes
Host on Business, Printer, Vehicle Servicing, Leasing and Marketing	Server0	ICMP	Permitted	Yes
Host on Business, Printer, Vehicle Servicing, Leasing and Marketing	server2	ICMP	Denied	Yes
All Vlans by default	Internet	HTTP	Permitted	Yes
Host on Marketing only	Leasing,	ICMP (echo-reply)	Permitted	Yes
Host on Marketing	Leasing,	ICMP	Denied	Yes
Host on Vehicle	Business, Printer, Security, Technical Support Leasing, and Marketing	ICMP (echo-reply)	Permitted	Yes
Host on Vehicle Servicing	Business, Printer, Security, Leasing, and Marketing	ICMP	Denied	Yes
Host on Business, Printer, Security, Vehicle Servicing Leasing, and Marketing	Technical Support	ICMP (echo-reply)	Permitted	Yes
Host on Business, Printer, Security, Vehicle Servicing, Leasing, and Marketing	Technical Support	ICMP	Denied	Yes

Host on Techinical support only	Sydney_Switch_F2 Sydney_Switch_F1 Sydney_Switch_Distribution	SSH	Permitted	Yes