PreviousDC Network Expansion: Subnetting, Security, and DNS Strategies

Prepared by: Abrar Walid Ahmed
April 13, 2025

Table of Contents

This report describes how to meet the network expansion requirements of PreviousDC, a cloud service provider, in subnetting, network traversal and security enhancements. The topology of the existing network is the Sydney CBD Office, the Sydney CBD Data Centre, and the Melbourne CBD Data Centre. A new Perth CBD Office and Data Centre has also been introduced along with upgrades to the existing data centres in the expansion plan. In particular, the Perth CBD Data Centre is composed of 20 computer servers (expandable to 30), 30 storage servers, and 2 technician PCs; the Perth CBD Office will support 10 hosts. The Sydney and Melbourne data centres

will also get 10 more computers and storage servers, raising the host requirements from 62 to 82.

The need for subnetting is proposed to accommodate this growth. My first attempt is to use a Fixed Length Subnet Masking (FLSM) with a /26 mask, which provides 16 subnets. This creates six of the subnets for the current topology and leaves 10 for expansion in the future. The expanded data centres, however, increase host demands beyond the capacity of the /26 and a suggestion is made for Variable Length Subnet Masking (VLSM). VLSM uses subnet sizes to suit the requirements of each location with respect to IP address utilization.

A ping request from the Sydney CBD Office to the Melbourne CBD Data Centre is analyzed to determine how the network would traverse. It is this exercise that describes the traffic flow, namely, encapsulation and decapsulation at each hop, ARP in resolving MAC addresses, and routing decisions. Having two WAN links (WAN1 and WAN2) available, the ping could favour WAN1 as per the routing configurations, which would be the most efficient and reliable connection.

The report also analyzes PreviousDC's potential to provide DNS services. This will need using authoritative DNS servers, complying with ICANN rules of domain registration, and having good security for preventing DNS threats.

1.1 Number of Subnets Required for Existing Topology

Sydney CBD Office, Sydney CBD DC, and Melbourne CBD DC make up DC's previous existing topology. Three LAN subnets are needed for each location to support its devices. Besides, there are WAN links among these sites: one from Sydney CBD Office to Sydney CBD DC and two from Sydney CBD DC to Melbourne CBD DC (WAN1, WAN2).
There is a subnet for each WAN link, which is a point-to-point connection, for proper routing and isolation, bringing us to three more subnets. Therefore, the total number of required subnets is six: three LAN subnets and three WAN counts (Sydney CBD Office LAN, Sydney CBD DC LAN, Melbourne CBD DC LAN, Sydney CBD Office to Sydney CBD DC, Sydney CBD DC to Melbourne CBD DC via WAN1, Sydney CBD DC to Melbourne CBD DC via WAN2). This explains the different network segments mentioned above and guarantees that each has its own IP range for communications and the management. This estimation can be made without Appendix A by using the described connectivity and device distribution, which can be considered as standard network design for such a topology.

1.2 Fixed Length Subnetting (FLSM) scheme

Their ISP has previously allocated DC the 223.0.104.0/22 network. When you get to a /22 network, you have 10 host bits (32 - 22 = 10), 2^{10} or 1024 addresses, and after reserving network and broadcast addresses, 1022 usable hosts. This block must be divided into equal sized subnets to be able to accommodate the six subnets identified in 1.1 for Fixed Length Subnet Masking (FLSM). There are 62 hosts in each of the data centres (Sydney CBD DC: 30 Compute Servers, 30 Storage Servers, 2 Technician PCs; Melbourne CBD DC: similar), so they have the largest subnet requirement. In order to create a subnet, you need atleast 64 addresses (62 + 2) for network and broadcast addresses. In this case the smallest subnet size that will support this is /26 ($2^6 = 64$ addresses, 62 usable) with a netmask of 255.255.255.192.

The number of subnets of /26 is simply $2^{(22-26)} = 2^4 = 16$ subnets, each containing a block size of 64 addresses (1024 addresses in /22, divided between 64 = 16). This is more than the required six, thus leaving room for future growth. The following are the FLSM scheme of the six subnets in the specified format:

- Sydney CBD Office LAN
- Network Address: 223.0.104.0
- Broadcast Address: 223.0.104.63
- Usable Hosts: 223.0.104.1 – 223.0.104.62
- Maximum Hosts Supported: 62
- Netmask: 255.255.255.192 (/26)
- Supports 2 Admin PCs and 1 Printer (3 hosts), well within capacity.
- Sydney CBD DC LAN
- Network Address: 223.0.104.64
- Broadcast Address: 223.0.104.127
- Usable Hosts: 223.0.104.65 – 223.0.104.126
- Maximum Hosts Supported: 62
- Netmask: 255.255.255.192 (/26)
- Supports 30 Compute Servers, 30 Storage Servers, 2 Technician PCs (62 hosts), fully utilized.
- Melbourne CBD DC LAN
- Network Address: 223.0.104.128
- Broadcast Address: 223.0.104.191
- Usable Hosts: 223.0.104.129 – 223.0.104.190
- Maximum Hosts Supported: 62
- Netmask: 255.255.255.192 (/26)
- Matches Sydney CBD DC's 62 hosts, fully utilized.
- WAN Link: Sydney CBD Office to Sydney CBD DC

- Network Address: 223.0.104.192
- Broadcast Address: 223.0.104.255
- Usable Hosts: 223.0.104.193 – 223.0.104.254
- Maximum Hosts Supported: 62
- Netmask: 255.255.255.192 (/26)
- Point-to-point link needs only 2 hosts (Router 3 and Router 1 interfaces); /26 is oversized but required by FLSM.
- WAN1: Sydney CBD DC to Melbourne CBD DC
- Network Address: 223.0.105.0
- Broadcast Address: 223.0.105.63
- Usable Hosts: 223.0.105.1 – 223.0.105.62
- Maximum Hosts Supported: 62
- Netmask: 255.255.255.192 (/26)
- Point-to-point link (Router 1 to Router 7); /26 is inefficient but consistent with FLSM.
- WAN2: Sydney CBD DC to Melbourne CBD DC
- Network Address: 223.0.105.64
- Broadcast Address: 223.0.105.127
- Usable Hosts: 223.0.105.65 – 223.0.105.126
- Maximum Hosts Supported: 62
- Netmask: 255.255.255.192 (/26)
- Second point-to-point link (Router 1 to Router 7); uses same /26 size.

1.3 Broadcast Domains

In the FLSM scheme each /26 subnet is a separate broadcast domain because broadcasts are confined to subnet boundaries in a routed network. Six broadcast domain and their devices are given below.

Broadcast Domain	Devices
Sydney CBD Office LAN (223.0.104.0/26)	Admin PC1, Admin PC2, Printer1, Router 3 (interface)
Sydney CBD DC LAN (223.0.104.64/26)	Compute Server 1–30, Storage Server 1–30, Tech PC1, Tech PC2, Router 1 (interface)
Melbourne CBD DC LAN (223.0.104.128/26)	Compute Server 1–30, Storage Server 1–30, Tech PC3, Tech PC4, Router 7 (interface)
WAN Office to Sydney DC (223.0.104.192/26)	Router 3 (interface), Router 1 (interface)
WAN1 Sydney DC to Melbourne DC (223.0.105.0/26)	Router 1 (interface), Router 7 (interface)
WAN2 Sydney DC to Melbourne DC (223.0.105.64/26)	Router 1 (interface), Router 7 (interface)

All devices connected to the LAN as well as the router interface become part of a single broadcast domain per subnet. The WAN links being point to point contain only two router interfaces. Without VLANs, switches (Switch 1, Switch 2) increase the broadcast domain for devices connected.

1.4 Collision Domains in Sydney CBD DC

A modern full duplex Ethernet network in the Sydney CBD DC has each switch port constituting a separate collision domain, with Switch 1 and Switch 2 connecting devices. When connected to individual switch ports, 62 end devices (30 Compute Servers, 30 Storage Servers, and 2 Technician PCs) each occupy its own collision domain. The interface connection to the switches on router 1 is not an end device and therefore not on this list. Here is a partial table (the full list has 62 rows):.

Collision Domain	Device
1	Compute Server 1
2	Compute Server 2
…	…
30	Compute Server 30
31	Storage Server 1
…	…
60	Storage Server 30
61	Tech PC1
62	Tech PC2

If full duplex operation eliminates collisions on switch to device links, each row represents a device in its own collision domain. The only 62 end devices are listed as inter switch or switch to router links are separate collision domains, but do not have end devices.

1.5 Support for Expansion Requirements

The expansion consists of Perth CBD DC (20 compute servers with 30 hosts capacity for compute; 30 storage servers; 2 technician PCs = 62 hosts initially; 62 hosts potentially), Perth CBD Office (10 hosts); and upgrades to Sydney and Melbourne DCs (adding 10 compute and 10 storage servers, hosts from 62 to 82). The current FLSM uses /26 subnets which support 62 hosts. For the current topology and initial Perth CBD DC, this is sufficient, but for the expanded Sydney and Melbourne DCs, it will not suffice as 82 hosts (84 addresses with network/broadcast) are needed. The requirement is for a /25 subnet (126 hosts), but a /22 network only provides 8 /25 subnets (2^3), i.e. 2 to the power of 3, which is not sufficient for the 6 already there and at least another 3 (Perth DC LAN, Perth Office LAN, and WAN link to Perth
DC) i.e. 9 in total.

The /26 size is limited, because it does not support 82 hosts, and switching /25 FLSM gives too small number of subnets. For DC LANs use VLSM address space with /25 (126 hosts), use /28 for Perth Office (14 hosts) and /30 for WAN links (2 hosts) to optimize the use of the /22 address space. As VLSM requires redesigning the FLSM, they do not append any new subnets to the FLSM.

2.1 Traffic Generated by a Ping Request

A ping from Admin PC2 (Sydney CBD Office, 223.0.104.0/26) to Compute Server 21 (Melbourne CBD DC, 223.0.104.128/26, e.g., 223.0.104.149) traverses' multiple subnets with empty ARP caches. Below is the traffic sequence:

1. [Ethernet SRC: Admin PC2 (MAC), DST: Broadcast [ARP Who has Router 3 IP?]] Admin PC2 ARPs for Router 3's MAC (default gateway) to send the ping.
2. [Ethernet SRC: Router 3 (MAC), DST: Admin PC2 (MAC) [ARP I am Router 3 IP, MAC: Router 3 (MAC)]]
   Router 3 replies with its MAC.
3. [Ethernet SRC: Admin PC2 (MAC), DST: Router 3 (MAC) [IP SRC: Admin PC2 IP, DST: 223.0.104.149 [ICMP Echo Request]]]
   Admin PC2 sends the ping to Router 3.
4. [Ethernet SRC: Router 3 (WAN MAC), DST: Broadcast [ARP Who has Router 1 IP (WAN link)?]]
   Router 3 ARPs for Router 1's MAC on the WAN link (223.0.104.192/26).
5. [Ethernet SRC: Router 1 (WAN MAC), DST: Router 3 (WAN MAC) [ARP I am Router 1 IP, MAC: Router 1 (WAN MAC)]]
   Router 1 replies.
6. [Ethernet SRC: Router 3 (WAN MAC), DST: Router 1 (WAN MAC) [IP SRC: Admin PC2 IP, DST: 223.0.104.149 [ICMP Echo Request]]]
   Router 3 forwards the ping to Router 1.
7. [Ethernet SRC: Router 1 (WAN1 MAC), DST: Broadcast [ARP Who has Router 7 IP (WAN1)?]]
   Router 1 ARPs for Router 7 via WAN1 (223.0.105.0/26).
8. [Ethernet SRC: Router 7 (WAN1 MAC), DST: Router 1 (WAN1 MAC) [ARP I am Router 7 IP, MAC: Router 7 (WAN1 MAC)]]
   Router 7 replies.
9. [Ethernet SRC: Router 1 (WAN1 MAC), DST: Router 7 (WAN1 MAC) [IP SRC: Admin PC2 IP, DST: 223.0.104.149 [ICMP Echo Request]]]
   Router 1 forwards the ping to Router 7.
10. [Ethernet SRC: Router 7 (LAN MAC), DST: Broadcast [ARP Who has 223.0.104.149?]] Router 7 ARPs for Compute Server 21's MAC on the LAN.
11. [Ethernet SRC: Compute Server 21 (MAC), DST: Router 7 (LAN MAC) [ARP I am 223.0.104.149, MAC: Compute Server 21 (MAC)]]
    Compute Server 21 replies.
12. [Ethernet SRC: Router 7 (LAN MAC), DST: Compute Server 21 (MAC) [IP SRC: Admin PC2 IP, DST: 223.0.104.149 [ICMP Echo Request]]]
    Router 7 delivers the ping to Compute Server 21.

2.2 Path Selection Between WAN1 and WAN2

At Router 1 in the Sydney CBD Data Centre the packet has to make a critical decision, in this case the packet has to choose between two available paths towards its destination which is Compute Server 21 in the Melbourne CBD Data Centre, either WAN1 (223.0.105.0/26) or WAN2 (223.0.105.64/26). This is up to Router 1's routing configuration, controlling how Router 7 in the Melbourne CBD Data Centre is reached. For example, in a typical enterprise network like PreviousDC's, an Open Shortest

Path First (OSPF) dynamic routing protocol is probably used to determine this. OSPF assigns a cost to each link and calculates the best path according to these costs, which is usually expressed as bandwidth, latency, or hop count. For instance, if WAN1 has a higher bandwidth or lower latency compared to WAN2, OSPF will assign it less cost and hence WAN1 will be the preferred route for the ping packet.

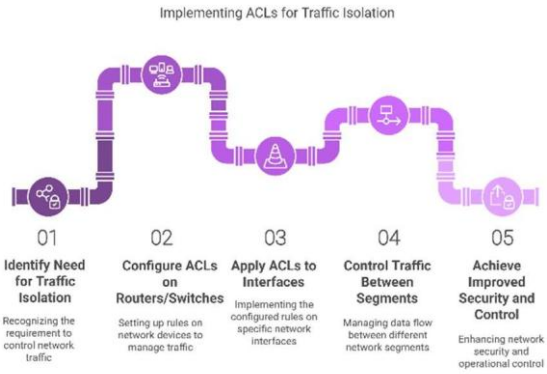
But if both the WAN1 and WAN2 have the same characteristics (same bandwidth, same latency and same hop count), OSPF would compute the cost of both paths similar. In such a case, Router 1 may perform load balancing, so that it can spread traffic over both links, some of the packets can go over WAN1 and some over WAN2 to use the network effectively. Alternatively, Router 1 could have a tiebreaker mechanism for picking one path every time, for example, preferring the link with lower network address (WAN1: 223.0.105.0 vs. WAN2: 223.0.105.64), or it might follow the order of entries in its routing table, and typically fall back to the first configured path, that may be WAN1.

Alternatively, PreviousDC's network administrators may have configured static routes on Router 1 to explicitly point traffic towards Melbourne CBD DC via WAN1 to have control and predictability. It also implies a redundancy design where the WAN1 link is assigned as the primary path and WAN2 is set to failover when the link fails. Without any details about link metrics, routing policies or failure states WAN1 is assumed to be the primary path as it has lower network address and standard practice for redundant network design. Therefore, the ping is likely to traverse WAN1 to reach its destination unless there is a policy or failure to change the preference to WAN2.

Signs of redundancy to make sure that the topology is reliable can be seen by the design, which has two WAN links. In such setups, WAN1 is usually designated as the primary link and WAN2 is used as the backup in case of failure. On normal operating conditions, therefore, Router 1 would probably select WAN1 to send the ping request so that it reaches the Melbourne CBD DC efficiently. Nevertheless, should WAN1's outage be detected by OSPF through its link state advertisements, Router 1 would failover to WAN2 and reroute the traffic to maintain connectivity. Since there are no specific metrics or configuration details, WAN1 is the most likely primary path per the conventional approach for redundant network designs [1].

3.1 Technology for Traffic Isolation

This method of isolating network traffic beyond subnetting is robust and is implemented at Layer 3 or 4 using Access Control Lists (ACLs) [1]. Rules configured on routers or switches in order to allow or disallow certain traffic based on IP addresses, protocols or port numbers are called ACLs. ACLs can limit communication between network segments or users in PreviousDC's topology, thus improving security and control. For instance, an ACL on Router 1 in the Sydney CBD Data Centre can prevent traffic destined for the Sydney CBD Office subnet (223.0.104.0/26) to Sydney CBD Data Centre subnet (223.0.104.128/26), so that only authorized data flows are from one site to the other. The isolation mechanism is to apply traffic policies: an ACL may allow or deny each protocol (for example, port 80 for HTTP traffic, port 21 for FTP), or range of IPs specifically. To implement ACLs, routers or Layer 3 switches that can process these rules are needed, such as Router 1, Router 3, and Router 7 in PreviousDC's configuration. The configuration is to define ACL rules and apply to the interfaces. There is no physical topology changes involved. This technique offers fine grained control and effectively separates traffic, but leaving the network flexible and usable.



3.2 Securing Customer Connections

Customers relying on PreviousDC's cloud services need to be protected from those who would seek to compromise customer connections, especially as many of them manage sensitive data; therefore, fortifying this strategy with protection mechanisms is essential. One of the main approaches is to use the Software Defined Wide Area Networking (SD-WAN) with embedded security features. SD-WAN allows the traffic to be routed across multiple paths (internet, private links) and embeds encryption and segmentation to build secure overlays between customer sites and PreviousDC's data centres in Sydney, Melbourne and Perth [2]. This guarantees that the data remains encrypted in transit, with policies that separate the customers' traffic from others to make the solution scalable for fears like healthcare or finance, which need strong protection. This can be another layer of security, which is added through Zero Trust Architecture (ZTA). ZTA works on the philosophy of 'never trust, always verify' that means continuously authenticating and authorizing every user and device trying to access PreviousDC services [3]. With identity aware proxies, PreviousDC can enforce tight access controls by authenticating the users through single sign on (SSO) and devices posture check before allowing users to access the resources so even if credentials are stolen, the risk is minimized. It is especially efficient for remote users accessing cloud services from across the board. To provide secure data in transit, PreviousDC can use Transport Layer Security (TLS) 1.3 for all communications, including web interactions and API calls, encrypted with the most recent

standards, cutting vulnerabilities to interception. At the data center level, Web Application Firewalls (WAFs) can be deployed to protect against application layer attacks like SQL injection to protect customer data in the process of interacting with cloud applications. Moreover, PreviousDC should integrate Data Loss Prevention (DLP) systems along with it to monitor and prevent sensitive data from being exfiltrated like credit card numbers or personal health information while following regulations like HIPAA or PCIDSS [4]. On the storage servers for PreviousDC's data at rest, you can access hardware-based encryption modules that support the FIPS 140-2 standard, ensuring data is safe even if physical access is gained. SD-WAN can run on existing routers such as Router 1 and Router 7; ZTA can leverage identity management systems, and WAFs can be added to data center gateways; all in all, these solutions fit seamlessly into PreviousDC's infrastructure to protect customer data, ensure compliance, and allow access only to those authorized to use it.

3.3 DNS

The internet navigation system is the Domain Name System (DNS) that translates the user-friendly domain names such as previousdc.com to IP addresses that devices use to connect. This translation allows users to access websites and services effortlessly without having to remember numerical addresses. The way DNS works is that there is a global hierarchy of servers, so a user's query begins with a 'recursive resolver,' which talks to root servers, top level domain (TLD) servers (.com, for example), then authoritative name servers that hold the domain's IP record and returns the result to the user. For PreviousDC to provide DNS services (registration and resolution) there are external requirements. PreviousDC must either become ICANN accredited and follow strict rules on how domains are priced, transferred and in dispute resolution or partner with an existing ICANN accredited registrar to do this for them. To achieve resolution, PreviousDC requires its authoritative DNS server to provide high uptime and redundancy so that queries are handled reliably. Compliance with regulations such as GDPR is crucial to preserve user privacy, and DNS Security Extensions (DNSSEC) needs to be set up to avoid attacks such as cache poisoning for the integrity and trust of the DNS service to be maintained.

References

[1] Y. Kannan, "Access control list (ACL) Compliance Verification and Alarm Systems: Strengthening Network Security," Available at SSRN 4705934. 2024 Mar 10.

[2] J. Wang, M. Bewong, L. Zheng, "SD-WAN: Hybrid edge cloud network between multi-site SDDC," Computer Networks, vol. 6, issue C, 2024 Aug 1.

[3] C. Sample, C. Shelton, SM. Loo, C. Justice, L. Hornung, I. Poynter, "ZTA: Never Trust, Always Verify," In ECCWS European Conference on Cyber Warfare. 2022 June.

[4] J. Seaman, "PCI DSS: An integrated data security standard guide," Apress; 2020 May 1.