Student ID: 46392459
Student Name: Khalid Bakhshi

Question 1a:

Sydney CBD Office requires **2 Subnets:** Separating voice and security systems from office traffic improves quality of service and security. VoIP phones are time sensitive and requires low latency, low jitter and minimal packet loss [1]. Placing them in separate subnets allows for improved call quality and prevents dropped/delayed calls from occurring [1]. Furthermore, devices such as access card readers and VoIP phones sharing the same subnet as office PCS, increases the likelihood of being exposed to malware attacks if a workstation is compromised. Keromytis in 2010 drew VoIP security statistics showing that 58% of VoIP attack are on Denial of Service, while 20% are on hijacking [2]. This emphasises the importance of VoIP security measures.

- Subnet 1 for Access Card Reader and VoIP phones
- Subnet 2 for Office Workstations (Receptionist PCs, Sales PCs, Customer service PCs, and Printer)

Sydney CBD Data Centre requires **3 Subnets**: Compute and Storage should be separated for better dataflow/performance, and Tech PCs and phones should be grouped under a management subnet. Compute servers generate large volume of general use traffic, and storage servers can carry high bandwidth [3]. Mixing them on the same subnet can cause congestion and reduce performance.

- Subnet 3 for Compute Servers (1-10)
- Subnet 4 for Storage Servers (1-10)
- Subnet 5 for Technician PC1&PC2, VoIP Phone 3&4

Melbourne CBD Data Centre requires **3 Subnets**: Ensures clear separation between core services such as compute, storage, and support infrastructure. This allows for a more secure, manageable, and scalable network foundation [3]. Same justification as Sydney CBD Data Centre

- Subnet 6: Compute Servers (11-30)
- Subnet 7: Storage Servers (11-20)
- Subnet 8: Technician PCs (3&4), VoIP Phones (5&6), Access Card Reader

Overall, a total of **8 Subnets** is required for the existing topology.

Student ID: 46392459
Student Name: Khalid Bakhshi

Question 1b:

1. Before subnetting, existing netmask for Class C → 255.255.255.0. This gives the following address range for the network before subnetting: 223.0.104.0 → 223.0.107.255

2. Number of bits needed: 8 useable subnets are required. $2^3 = 8$ → 3 bits required.

3. Existing netmask is 255.255.252.0 (i.e. /22). New netmask will be /25 (22 + 3 = 25) → 255.255.255.10000000 → 255.255.255.128

4. 7 bits remaining for the host portion for the host portion of the address (all in the 4th octet): $2^7 = 128$ → 128 total addresses per subnet. 128 – 2 = 126 per subnet = Useable host addresses

5. The network address for the first subnet will be the same as the original network: 223.0.104.0

6. The broadcast address for the last subnet will be 223.0.107.255

7. Each successive subnet network address will simply be the subnet number (counting starts at zero) multiplied by 128 or 2^7:

0 * 128 = 0 → 223.0.104.0

1 * 128 = 128 → 223.0.104.128

2 * 128 = 256, → 223.0.105.0, etc

Subnet Number	Subnet ID binary Value	Hosts bits binary range	Last octet binary range	Last octet decimal range	IP range	Useable Y/N
0	000	0000000 - 1111111	00000000 - 01111111	0 – 127	223.0.104.0 – 223.0.104.127	Y
1	001	0000000 - 1111111	10000000 - 11111111	128 – 255	223.0.104.128 – 223.0.104.255	Y
2	010	0000000 - 1111111	00000000 - 01111111	0 – 127	223.0.105.0 – 223.0.105.127	Y
3	011	0000000 - 1111111	10000000 - 11111111	128 – 255	223.0.105.128 – 223.0.105.255	Y
4	100	0000000 - 1111111	00000000 - 01111111	0 – 127	223.0.106.0 – 223.0.106.127	Y
5	101	0000000 - 1111111	10000000 - 11111111	128 – 255	223.0.106.128 – 223.0.106.255	Y
6	110	0000000 - 1111111	00000000 - 01111111	0 - 127	223.0.107.0 – 223.0.107.127	Y
7	111	0000000 - 1111111	10000000 - 11111111	128 - 255	223.0.107.128 – 223.0.107.255	Y

Student ID: 46392459
Student Name: Khalid Bakhshi

Question 1c:

Broadcast Domain 1 223.0.104.0/25	**Broadcast Domain 2** 223.0.104.128/25	**Broadcast Domain 3** 223.0.105.0/25	**Broadcast Domain 4** 223.0.105.128/25	**Broadcast Domain 5** 223.0.106.0/25	**Broadcast Domain 6** 223.0.106.128/25	**Broadcast Domain 7** 223.0.107.0/25	**Broadcast Domain 8**
Device Name	**Device Name**	**Device Name**	**Device Name**	**Device Name**	**Device Name**	**Device Name**	**Device Name**
Compute Server 1 – 10	Storage Server 1-10	Tech PC1-2	Receptionist PC1-2	Customer Service PC1-10	Compute Server 11-20	Compute Server 21 – 30	Storage Server 11-20
		IP Phone 3-4	Sales PC1-6				Tech PC3
			Admin PC1-2				Tech PC4
			Printer 1				IP Phone 5
			Access Card Reader 1				IP Phone 6
							Access Card Reader 2

Student ID: 46392459
Student Name: Khalid Bakhshi

Question 1d:

In a switched Ethernet network, each switch port functions as a separate collision domain, meaning devices connected to different ports can transmit data simultaneously without causing collisions [4]

Collision Domain	Device Name
1	Compute Server 1
2	Compute Server 2
3	Compute Server 3
4	Compute Server 4
5	Compute Server 5
6	Compute Server 6
7	Compute Server 7
8	Compute Server 8
9	Compute Server 9
10	Compute Server 10
11	Storage Server 1
12	Storage Server 2
13	Storage Server 3
14	Storage Server 4
15	Storage Server 5
16	Storage Server 6
17	Storage Server 7
18	Storage Server 8
19	Storage Server 9
20	Storage Server 10
21	Tech PC1
22	IP Phone 3
23	Tech PC2
24	IP Phone 4

Student ID: 46392459
Student Name: Khalid Bakhshi

Question 1e:

The current FLSM doesn't support the full expansion. Currently there are 8 subnets created by applying /25 mask to 223.0.104.0/22 and each subnet produces 126 useable host IPs. All 8 subnets are already allocated to the existing topology, 3 for Sydney CBD DC, 2 for Sydney CBD Office, and 3 for Melbourne CBD DC. Therefore, this expansion requires additional Subnets to support new devices at new locations.

The Perth CBD Data Centre contains 20 compute servers, 30 storage servers, and 2 technician PCs. 2-3 subnets for compute servers, storage servers, and the tech and IP phones (if its added) would be recommended. The Perth CBD Office contains 1 receptionist, 2 sales PCs, 6 customer service PCs, and 1 printer. This can fit 1 new subnet. Lastly, the existing DCs we are adding 10 compute servers to Sydney DC, 10 Storage Servers to Sydney DC, 10 compute Servers to Melbourne DC, and 10 storage servers to Melbourne DC. These expansion requirements to the existing DC would push the device count beyond 126 per subnet, especially in Melbourne where compute servers would now be 30+. Assigning 1 more additional subnet to both Syndey DC and Melbourne DC would be recommended.

Overall, there would be a total of 5 additional subnets needed for the expansion. However, a change to overcome this problem is to request a larger CIDR block from the ISP such as /21 or allocating a second /22 block for the Perth site. And, maintaining the current /25 subnetting scheme, would yield an additional 8 subnets to support the expansion requirements without disrupting the existing network structure.

Student ID: 46392459
Student Name: Khalid Bakhshi

Question 2a:

Encapsulation and Network Traversal:

1)) ARP Request of Admin PC2 to Default Gateway

Admin PC2 unaware of MAC address of Default Gateway (Router 1), therefore broadcasts an ARP request to obtain MAC address.

[Ethernet SRC: Admin PC2 (MAC), DST: FF: FF: FF: FF: FF: FF

[ARP Request: Who has Router 1 (IP)? Tell Admin PC2 (IP)]]

2)) ARP Replies of Router 1 to Admin PC2

Router 1 provides its MAC address.

[Ethernet SRC: Router 1 (MAC), DST: Admin PC2 (MAC)

[ARP Reply: Router 1 (IP) is at Router 1 (MAC)]]

3)) ICMP Echo Request Packet of Admin PC2 to Compute Server 21

Admin PC2 knows where to send the packet, so it sends the ICMP Echo Request to Compute Server 21 through its gateway Router 1.

[Ethernet SRC: Admin PC2 (MAC), DST: Router 1 (MAC)

[IP SRC: Admin PC2 (IP), DST: Compute Server 21 (IP)

[ICMP Type: 8 (Echo Request)]]]

4)) Router 1 forwards to WAN and needs MAC of Router 2

Router 1 doesn't know its MAC but needs to forward to Router 2 (first WAN router). It sends an ARP request on WAN link.

[Ethernet SRC: Router 1 (MAC), DST: FF: FF: FF: FF: FF: FF

[ARP Request: Who has Router 2 (IP)? Tell Router 1 (IP)]]

5)) ARP Reply of Router 2 to Router 1

[Ethernet SRC: Router 2 (MAC), DST: Router 1 (MAC)

[ARP Reply: Router 2 (IP) is at Router 2 (MAC)]]

6)) Packet forwarded to Router 2

[Ethernet SRC: Router 1 (MAC), DST: Router 2 (MAC)

[IP SRC: Admin PC2 (IP), DST: Compute Server 21 (IP)

[ICMP Type: 8 (Echo Request)]]]

7)) Router 2 → Router 3 → Router 4 → Router 7, the steps are repeated across the WAN

[Ethernet SRC: Router 2 (MAC), DST: Router 3 (MAC)

[IP SRC: Admin PC2 (IP), DST: Compute Server 21 (IP)

Student ID: 46392459
Student Name: Khalid Bakhshi

[ICMP Type: 8 (Echo Request)]]]

8)) ARP Request of Router 7 to Compute Server 21

Router 7 doesn't know Compute Servers MAC, but needs to deliver

[Ethernet SRC: Router 7 (MAC), DST: FF:FF:FF:FF:FF:FF

[ARP Request: Who has Compute Server 21 (IP)? Tell Router 7 (IP)]]

9)) ARP reply of Compute Server 21 to Router 7

[Ethernet SRC: Compute Server 21 (MAC), DST: Router 7 (MAC)

[ARP Reply: Compute Server 21 (IP) is at Compute Server 21 (MAC)]]

10)) Final ICMP Echo Request

[Ethernet SRC: Router 7 (MAC), DST: Compute Server 21 (MAC)

[IP SRC: Admin PC2 (IP), DST: Compute Server 21 (IP)

[ICMP Type: 8 (Echo Request)]]]

Question 2B:

The ping request takes the path determined by the routing table on Router 1 and will favour the path with the least administrative distance and cost/metrics, which is most likely WAN1. Firstly, routing protocols decide the path due to Routers like Router 1 using protocols (OSPF, EIGRPM BGP, or static routes) to determine which path to use when there are multiple routes to the same destination [5] Secondly, metrics and costs determine preference because of routing tables evaluating administrative distance, and the number of metrics such as hop count, bandwidth, and delay [6]. Thus, the route with the lowest cost and lowest administrative distance is preferred. For example, if the route to Compute Server 21 (Melbourne DC) via WAN1 has a lower hop count, lower latency, and higher bandwidth, then WAN1 will be selected as the primary route [6]. However, WAN2 will only be used if WAN1 is down, and WAN2 is manually configured to be preferred. Administrative distance is a value that indicates how trustworthy the source of the route is [6]. A lower AD means that it is more preferred. Overall, the ping request will follow the best path in Router 1s routing table.

Student ID: 46392459
Student Name: Khalid Bakhshi

Question 3a:

In addition to subnetting, Virtual Local Area Networks (VLANs) are a widely used method for isolating network traffic. It operates at Layer 2 of the OSI model and allows administrators to segment devices into separate broadcast domains, even if they share the same physical switch [7]. Each VLAN is identified by a Unique ID and uses IEEE 802.1G tagging on its switches to distinguish traffic [8]. The 802.1Q standard is managed by the Institute of Electrical and Electronics Engineers (IEEE), a leading organization in networking standards [8]. IEEE develops many of the protocols that support modern enterprise networks. The traffic between VLANs is blocked by default and requires routing through a Layer 3 device like a router or Layer 3 switch [9].

Subnetting organizes devices based on IP addressing, VLANs segment traffic by switch port [9]. While subnetting segregate traffic based on IP ranges, VLANs offer more control by segmenting traffic based on switch port configuration. This allows for more precise control, making it easier to separate departments, traffic types, or devices roles without needing to alter the physical infrastructure [10]. VLANS also minimize the broadcast traffic and enhance security by preventing unauthorized access to isolated segments [10].

To deploy VLANS in the existing PreviousDC network topology, the unmanaged switches would need to be replaced with managed switches. The device groups would be assigned specific VLAN IDs, and inter-VLAN routing would be established using a router or a Later 3 switch. This setup allows for scalable, adaptable network segmentation and offers improved administrative control as the network/infrastructure expands.

Student ID: 46392459
Student Name: Khalid Bakhshi

Question 3b:

Customers handling sensitive or confidential information need a secure and dependable method to access PreviousDCs cloud infrastructure. To meet this need, a combination of tools and technologies can be used to protect the confidentiality, integrity, and availability of data. Whether it's being transmitted across networks or stored within the cloud. This not only helps protect daily operations but also ensures compliance with industry standards and builds trust with clients and stakeholders.

The most frequent approach to secure data transmission involves VPNS (Virtual Private Networks). A VPN creates an encryption tunnel between cloud services in PreviousDC and the customer's device or their internal network through IPsec or SSL protocols [11]. VPNS enable secure remote access and branch connection for users accessing the internet from public networks.

Furthermore, the customers who require robust security and superior performance can establish their connection through dedicated private links including MPLS circuits. The physical connection between customer networks and PreviousDC data centres eliminates public internet paths while simultaneously delivering enhanced network speed at cybersecurity protection standards. MPLS networks allows for quality-of-service guarantee which is essential for businesses handling sensitive information. They include no exposure to DDoS attacks or man-in-the-middle-threats and contain dedicated links to ensure reduced jitter and packet loss which is vital for applications such as VoIP phones, video conferencing, and database replication [12].

Next, all cloud services need to enable TLS/SSL encryption for the purpose of safeguarding transmitted information. Data encryption is achieved through secure web portals and APIs that perform HTTPS encryption to protect information from online interception [13]. MFA (Multi-Factor Authentication) must be used for cloud portal and VPN access to employ extra user verification by validating with temporary codes [14].

In addition, RBAC (Role Based Access Control operates within the cloud setting to ensure users obtain access to only necessary systems and data connected to their specific roles [15]. The principle of least privilege is enforced while internal threats decrease through this method. The storage of cloud data should be protected through rest encryption standards that utilize robust AES-256 encryption to ensure maximum protection in case storage systems are breached [16].

Finally, (CASBs) Cloud Access Security Brokers can be used to provide visibility and policy enforcement between the customer and cloud services [17]. This allows customers to apply DLP (data loss prevention, audit logging, and compliance rules across all cloud applications that is hosted by PreviousDC.

Overall, through the combination of these technologies' VPNs, Private links, encryption, MFA, RBAC, and CASBs. PreviousDC can deliver secure, scalable, and industry standard access to its cloud services for customers that have sensitive data.

Student ID: 46392459
Student Name: Khalid Bakhshi

Question 3c:

The DNS (Domain Name System) operates as the central component for internet functionality due to it serving as a directory to transform domain names into IP addresses [18]. As a directory service DNS translates DNS domain names which are readable addresses into machine friendly IP addresses required for server identification and communication [18]. Operations between users, websites and cloud services would require memorization of IP addresses if DNS did not exist.

When a user enters a domain into their browser, a DNS resolver queries various DNS servers in a hierarchical order to resolve the domain into an IP address. This resolution process involved recursive and authoritative name servers, with the final response providing the corresponding IP address to the client [19]. Once, resolved, the device can then establish a connection with the destination server.

PreviousDC needs to fulfill external regulatory and technical requirements before starting its DNS service offerings which include domain name registration and resolution. The company must gain accreditation from ICANN (Internet Corporation for Assigned Names and Numbers) through direct accreditation or by partnering with an already accredited ICANN registrar [20]. A DNS infrastructure must follow DNS protocol requirements specified in RFC 1034 [21] as well as RFC 1035 [22] while adding DNSSEC support to provide secure DNS functionalities. RFC 1034 defines the conceptual framework of the Domain Name System, including how domain names are structured and resolved [21]. RFC 1035 outlines the technical specifications such as message formats, query types, and resource records [22]. A DNS provider needs to focus on keeping operational services running continuously, safeguarding data precision and duplicate storage to build user confidence in the platform.

Student ID: 46392459
Student Name: Khalid Bakhshi

Bibliography:

[1] K. Salah, "On the deployment of VoIP in Ethernet networks: methodology and case study," Computer Communications, vol. 29, no. 8, pp. 1039–1054, May 2006, doi: 10.1016/j.comcom.2005.06.004. [Accessed 08/04/2025 1:30pm]

[2] G. Bella, P. Biondi, and S. Bognanni, "Multi-service threats: Attacking and protecting network printers and VoIP phones alike," *Internet of Things*, vol. 18, p. 100507, 2022, doi: 10.1016/j.iot.2022.100507. [Accessed 08/04/2025 1:50pm]

[3] S. N. Sisat, P. S. Bhopale, and V. K. Barbudhe, "IP Subnetting," *International Journal of Electronics, Communication and Soft Computing Science & Engineering (IJECSCSE)*, vol. 2, no. 5, pp. 5–9, 2012. [Accessed 07/04/2025 4:00pm]

[4] A. Quine, "Carrier Sense Multiple Access Collision Detect (CSMA/CD) Explained," ITPRC, Aug. 29, 2018. [Online]. Available: https://www.itprc.com/carrier-sense-multiple-access-collision-detect-csmacd-explained/. [Accessed: 08/04/2025 1:00pm].

[5] Juniper Networks, "Understanding BGP Path Selection," *Juniper Networks Documentation*, Apr. 14, 2025. [Online]. Available: https://www.juniper.net/documentation/us/en/software/junos/vpn-l2/bgp/topics/concept/routing-protocols-address-representation.html [Accessed: 12/04/2025 2:30pm]

[6] Study-CCNA.com, "Administrative distance & metric," *Study-CCNA.com*, [Online]. Available: https://study-ccna.com/administrative-distance-metric/. [Accessed: 12/04/2025 2:00pm].

[7] B. Liu, K. Wei, L. Zheng, and X. Li, "Design and study of network isolation between hosts in data centers based on Private VLANs," in Proc. 3rd Int. Conf. Cryptography, Network Security and Communication Technology, Jan. 2024, pp. 242–246. [Accessed: 13/04/2025 1:00pm]

[8] Cisco Systems, Inc., "Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation," *LAN Switching Configuration Guide, Cisco IOS XE Release 3S*, 2017. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/lanswitch/configuration/xe-3s/lanswitch-xe-3s-book/lnsw-conf-vlan-ieee.pdf. [Accessed: 13/04/2025 1:00pm]

[9] Cisco Networking Academy, "Inter-VLAN Routing using Layer 3 Switches (4.3)," in Switching, Routing, and Wireless Essentials Companion Guide (CCNAv7), Cisco Press, Jul. 29, 2020. [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=3089357&seqNum=6. [Accessed: 13/04/2025 1:20pm]

[10] Cisco Systems, Inc., "Configure Port to VLAN Interface Settings on a Switch through the CLI," *Cisco Support Documentation*, Feb. 15, 2020. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5653-configure-port-to-vlan-interface-settings-on-a-switch-throug.html. [Accessed: 13/04/25 1:40pm]

[11] N. Gautam, J. Mansuri, and P. Patel, "Comparative Study of Security Protocols in VPNs (IPSec and SSL)," *International Journal of Engineering Research & Technology (IJERT)*, vol. 13, no. 10, pp. 1–5, Oct. 2024. [Online]. Available: https://www.ijert.org/comparative-study-of-security-protocols-in-vpns-ipsec-and-ssl. [Accessed: 13/04/25 2:00pm]

[12] S. Smith, "Introduction to MPLS," presented at the 2003 Technical Symposium, Cisco Systems, Inc., 2003. [Online]. Available: https://www.cisco.com/c/dam/global/fr_ca/training-events/pdfs/Intro_to_mpls.pdf. [Accessed: 13/04/25 3:00pm]

[13] H. Krawczyk, "The order of encryption and authentication for protecting communications (or: How secure is SSL?)," in Proc. Annu. Int. Cryptology Conf. (CRYPTO 2001), Berlin, Germany: Springer, 2001, pp. 310–331. [Online]. Available: https://link.springer.com/chapter/10.1007/3-540-44647-8_19. [Accessed: 13/04/25 3:10pm]

[14] S. R. Gudimetla, "Multi-Factor Authentication for Cloud," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 6, no. 3, pp. 4341–4343, Mar. 2024. [Online]. Available: https://www.researchgate.net/publication/379820040_MULTI-FACTOR_AUTHENTICATION_FOR_CLOUD. [Accessed: 13/04/25 3:15pm].

[15] S. Harnal and R. K. Chauhan, "Efficient and Flexible Role-Based Access Control (EF-RBAC) Mechanism for Cloud," EAI Endorsed Transactions on Scalable Information Systems, vol. 7, no. 26, pp. 1–10, Nov. 2019. [Online]. Available: https://www.researchgate.net/publication/337354911_Efficient_and_Flexible_Role-Based_Access_Control_EFRBAC_Mechanism_for_Cloud. [Accessed: 13/04/25 3:40pm]

[16] M. P. Babitha and K. R. Babu, "Secure cloud storage using AES encryption," in *Proc. 2016 Int. Conf. Automatic Control and Dynamic Optimization Techniques (ICACDOT)*, Pune, India, Sep. 2016, pp. 859–864. doi: 10.1109/ICACDOT.2016.7877718. [Accessed: 14/04/25 1:00pm]

[17] S. George, F. Jolayemi, D. David, and G. Christopher, "Cloud Access Security Brokers (CASBs): Strengthening Cloud Security Posture," *ResearchGate*, Dec. 2023. [Online]. Available: https://www.researchgate.net/publication/386080443_Cloud_Access_Security_Brokers_CASBs_Strengthening_Cloud_Security_Posture. [Accessed: 14/04/25 1:30pm]

[18] A. Khormali, J. Park, H. Alasmary, A. Anwar, and D. Mohaisen, "Domain Name System Security and Privacy: A Contemporary Survey," arXiv preprint arXiv:2006.15277, Jun. 2020. [Online]. Available: https://arxiv.org/abs/2006.15277. [Accessed: 14/04/25 1:30pm]

[19] Y. Wang, M.-Z. Hu, B. Li, and B.-R. Yan, "Authoritative Server's Impact on Domain Name System's Performance and Security," in *Proc. Int. Conf. Intelligent Computing*, 2010, pp. 66–75. [Online]. Available: https://www.researchgate.net/publication/225587076_Authoritative_Server%27s_Impact_on_Domain_Name_System%27s_Performance_and_Security. [Accessed: 14/04/25 1:35pm]

[20] P. Mockapetris, "Domain names—concepts and facilities," *Request for Comments: 1034*, Internet Engineering Task Force (IETF), Nov. 1987. [Online]. [Available: 14/04/25 6:00pm] https://datatracker.ietf.org/doc/html/rfc1034

[21] P. Mockapetris, "Domain names—implementation and specification," Request for Comments: 1035, Internet Engineering Task Force (IETF), Nov. 1987. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc1035. [Available:14/04/25 6:00pm]