|  |
| --- |
| .0  Introduction  In today's digital landscape, where data breaches and unauthorized access are significant concerns, organizations need robust security measures to protect their networks and sensitive information.  ACLs provide a vital layer of Defence by controlling and filtering network traffic, allowing only authorized traffic to pass through while blocking or restricting unauthorized access.  VPN a virtual private network (VPN) is a service that protects your online privacy and security by creating an encrypted tunnel between your device and the internet. This tunnel encrypts all of your data traffic, making it unreadable to anyone who tries to intercept it.  The project recognizes the importance of securing the network infrastructure and aims to design, configure, and implement ACLs across the network, and VPN creating an encrypted tunnel between your device and the internet. By doing so, the project will enforce specific security policies and requirements that align with the organization's overall security strategy. This will not only mitigate the risk of unauthorized access but also safeguard against potential malicious activities and data breaches.    Scope Of the Project    Overview  The project aims to implement Access Control Lists (ACLs) and Virtual Private Network (VPN) to enhance the security of a network infrastructure. ACLs provide a mechanism for controlling and filtering network traffic, allowing only authorized traffic to pass through while blocking or restricting unauthorized access. VPN provides with a secure connection for data transfer or communication. The scope of the project includes the design, configuration, and implementation of ACL and VPN across the network infrastructure. Objectives  * Assess Current Network Infrastructure: Conduct a thorough assessment of the existing network infrastructure to understand its topology, devices, and traffic patterns. * Define Security Requirements: Identify the specific security requirements and policies that need to be enforced using ACLs. * Design ACL Architecture: Develop a comprehensive ACL architecture that aligns with the security requirements and network topology, considering factors such as traffic flows, user roles, and service-level agreements. * Configure ACLs: Implement the designed ACL rules on network devices (routers, switches, etc.) to enforce the desired security policies. * Design VPN Architecture: Develop a comprehensive VPN architecture that aligns the security requirements. * Configure VPN: Implement the designed VPN on network devices where the configuration is required. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Here are some common scenarios where ACLs are deployed.   1. **Network Perimeter Security:**   VPNs can be a powerful tool for bolstering perimeter security, especially when used alongside other security measures.   1. **VLAN (Virtual Local Area Network) Segmentation:**   ACLs play a crucial role in network segmentation by controlling communication between different VLANs. Organizations can implement ACLs on switches or routers to restrict traffic flow between VLANs, ensuring that only authorized traffic is allowed while preventing unauthorized access or potential attacks.   1. **Remote Access Control:**   When providing remote access to internal resources, such as through VPN (Virtual Private Network) connections, ACLs can be used to define access rules for remote users. By implementing ACLs on VPN concentrators or firewalls, organizations can control which resources remote users can access and enforce granular access policies based on user roles or groups.   1. **Data Centre Security:**   Within a data centre environment, ACLs are commonly used to control access to critical servers, databases, or storage systems. By configuring ACLs on switches or load balancers, organizations can restrict access to specific servers or services, limit administrative access to authorized personnel, and protect sensitive data from unauthorized access or potential attacks.   1. **Application Security:**   ACLs can be implemented at the application layer to control access to specific applications or services within the network. This can involve defining rules based on source IP addresses, user authentication, or specific application-level protocols. Application-level ACLs help protect critical applications from unauthorized access, reduce the attack surface, and ensure secure communication.   1. **Guest Network Management:**   ACLs are commonly used to manage guest networks, providing restricted access to visitors while protecting internal resources. By implementing ACLs on guest network gateways or access points, organizations can allow internet access for guests while limiting their ability to access internal systems or other guests' devices.   1. **Compliance and Regulatory Requirements:**   Many industries have compliance requirements that necessitate access control mechanisms. ACLs help meet these requirements by enforcing access restrictions, logging and monitoring access attempts, and ensuring compliance with regulations such as HIPAA, PCI DSS, or GDPR.  Requirement Specification  Hardware Requirement   |  |  |  |  | | --- | --- | --- | --- | | Sl. No. | Device | Component Name | Quantity | | 1 | Cisco Router | 2911 series | 10 | | 2 | Switch | 2960 | 10 | | 3 | Server | Server | 10 | | 4 | Access Point | Access-Point | 14 | | 5 | PC | PC | 08 | | 6 | Laptop | Laptop | 14 |   Security Requirement  This security requirement is the combination of design and security policies. A security requirement is a statement of needed security functionality that ensures one of many different security properties of software is being satisfied. Security requirements are derived from industry standards, applicable laws, and a history of past vulnerabilities.    Architectural Design  Building design  BUILDING - 1  FLOOR - 4 Project Team 1   |  |  |  |  |  | | --- | --- | --- | --- | --- | | Host | IP Address | VLAN | Server | Access Policy  (Server) | | Leader | 20.0.0.2 | V3 | Server 1 | Permit (Server 1) | | Member | 10.0.0.2 | V2 | Server 1 | Permit (Server 1) | | Member | 10.0.0.2 | V2 | Server 1 | Permit (Server 1) |   FLOOR - 3 Project Team 2   |  |  |  |  |  | | --- | --- | --- | --- | --- | | Host | IP Address | VLAN | Server | Access Policy  (Server) | | Leader | 50.0.0.2 | V3 | Server 2 | Permit (Server 2) | | Member | 40.0.0.2 | V2 | Server 2 | Permit (Server 2) | | Member | 40.0.0.3 | V2 | Server 2 | Permit (Server 2) |     FLOOR - 2 Project Team 3   |  |  |  |  |  | | --- | --- | --- | --- | --- | | Host | IP Address | VLAN | Server | Access Policy  (Server) | | Leader | 80.0.0.2 | V3 | Server 3 | Permit (Server 3) | | Member | 70.0.0.2 | V2 | Server 3 | Permit (Server 3) | | Member | 70.0.0.3 | V2 | Server 3 | Permit (Server 3) |   FLOOR - 1 Non-Technical Team 1   |  |  |  |  |  | | --- | --- | --- | --- | --- | | Host | IP Address | VLAN | Server | Access Policy  (Server) | | Admin | 100.0.0.2 | V2 | Admin | Permit (Admin Server) | | Reception | 110.0.0.2 | V3 | Reception | Permit (Reception Server) |     BUILDING – 2  FLOOR - 4 Project Team 4   |  |  |  |  |  | | --- | --- | --- | --- | --- | | Host | IP Address | VLAN | Server | Access Policy  (Server) | | Leader | 12.0.0.2 | V3 | Server 4 | Permit (Server 4) | | Member | 11.0.0.2 | V2 | Server 4 | Permit (Server 4) | | Member | 11.0.0.3 | V2 | Server 4 | Permit (Server 4) |   FLOOR - 3 Project Team 5   |  |  |  |  |  | | --- | --- | --- | --- | --- | | Host | IP Address | VLAN | Server | Access Policy  (Server) | | Leader | 15.0.0.2 | V3 | Server 5 | Permit (Server 5) | | Member | 14.0.0.2 | V2 | Server 5 | Permit (Server 5) | | Member | 14.0.0.3 | V2 | Server 5 | Permit (Server 5) |   FLOOR - 2 Project Team 6   |  |  |  |  |  | | --- | --- | --- | --- | --- | | Host | IP Address | VLAN | Server | Access Policy  (Server) | | Leader | 18.0.0.2 | V3 | Server 6 | Permit (Server 6) | | Member | 17.0.0.2 | V2 | Server 6 | Permit (Server 6) | | Member | 17.0.0.3 | V2 | Server 6 | Permit (Server 6) |   FLOOR - 1 Non-Technical Team 2   |  |  |  |  |  | | --- | --- | --- | --- | --- | | Host | IP Address | VLAN | Server | Access Policy  (Server) | | Account | 21.0.0.2 | V3 | Account Server | Permit (Account Server) | | Sales | 22.0.0.2 | V2 | Sales Server | Permit (Sales Server) |   Data Centre  Data Centre-1   |  |  |  | | --- | --- | --- | | Host | IP Address | VLAN | | Team1 Server | 24.0.0.2 | V2 | | Team2 Server | 25.0.0.2 | V3 | | Team3 Server | 26.0.0.2 | V4 | | Admin Server | 27.0.0.2 | V5 | | Reception Server | 28.0.0.2 | V6 |   Data Centre-2   |  |  |  | | --- | --- | --- | | Host | IP Address | VLAN | | Team4 Server | 29.0.0.2 | V2 | | Team5 Server | 31.0.0.2 | V3 | | Team6 Server | 32.0.0.2 | V4 | | Account Server | 33.0.0.2 | V5 | | Sales Server | 34.0.0.2 | V6 |     Complete Architectural  **Configuration:-** **Building- 01**  **Router-B1F4R1**  >en  #config t  #hostname ProjectTeam1  #int g0/0  #no ip address  #no shut  #int g0/0.2  #encapsulation dot1q 2  #ip address 10.0.0.1 255.0.0.0  #no shut  #int g0/0.3  # encapsulation dot1q 3  #ip address 20.0.0.1 255.0.0.0  #no shut  #int g0/1  #ip address 30.0.0.1 225.0.0.0  #no shut  #exit  #router ospf 1  #network 10.0.0.0 0.0.0.255 area 0  #network 20.0.0.0 0.0.0.255 area 0  #network 30.0.0.0 0.0.0.255 area 0  **Router-B1F3R2**  >en  #config t  #hostname ProjectTeam2  #int g0/0  #no ip address  #no shut  #int g0/0.2  #encapsulation dot1q 2  #ip address 40.0.0.1 255.0.0.0  #no shut  #int g0/0.3  # encapsulation dot1q 3  #ip address 50.0.0.1 255.0.0.0  #no shut  #int g0/1  #ip address 30.0.0.2 225.0.0.0  #no shut  #int g0/2  #ip address 60.0.0.1 225.0.0.0  #no shut  #exit  #router ospf 1  #network 30.0.0.0 0.0.0.255 area 0  #network 40.0.0.0 0.0.0.255 area 0  #network 50.0.0.0 0.0.0.255 area 0  #network 60.0.0.0 0.0.0.255 area 0  **Router-B1F2R3**  >en  #config t  #hostname ProjectTeam3  #int g0/0  #no ip address  #no shut  #int g0/0.2  #encapsulation dot1q 2  #ip address 70.0.0.1 255.0.0.0  #no shut  #int g0/0.3  # encapsulation dot1q 3  #ip address 80.0.0.1 255.0.0.0  #no shut  #int g0/1  #ip address 60.0.0.2 225.0.0.0  #no shut  #int g0/2  #ip address 90.0.0.1 225.0.0.0  #no shut  #exit  #router ospf 1  #network 60.0.0.0 0.0.0.255 area 0  #network 70.0.0.0 0.0.0.255 area 0  #network 80.0.0.0 0.0.0.255 area 0  #network 90.0.0.0 0.0.0.255 area 0  **Router-B1F1R4**  >en  #config t  #hostname Non-TechnicalTeam1  #int g0/0  #no ip address  #no shut  #int g0/0.2  #encapsulation dot1q 2  #ip address 100.0.0.1 255.0.0.0  #no shut  #int g0/0.3  # encapsulation dot1q 3  #ip address 110.0.0.1 255.0.0.0  #no shut  #int g0/1  #ip address 90.0.0.2 225.0.0.0  #no shut  #int g0/2  #ip address 23.0.0.1 225.0.0.0  #no shut  #exit  #router ospf 1  #network 100.0.0.0 0.0.0.255 area 0  #network 110.0.0.0 0.0.0.255 area 0  #network 90.0.0.0 0.0.0.255 area 0  #network 23.0.0.0 0.0.0.255 area 0  #access-list 130 permit icmp 10.0.0.0 0.0.0.255 24.0.0.0 0.0.0.255  #access-list 130 permit icmp 20.0.0.0 0.0.0.255 24.0.0.0 0.0.0.255  #access-list 130 permit icmp 40.0.0.0 0.0.0.255 25.0.0.0 0.0.0.255  #access-list 130 permit icmp 50.0.0.0 0.0.0.255 25.0.0.0 0.0.0.255  #access-list 130 permit icmp 70.0.0.0 0.0.0.255 26.0.0.0 0.0.0.255  #access-list 130 permit icmp 80.0.0.0 0.0.0.255 26.0.0.0 0.0.0.255  #access-list 130 permit icmp 100.0.0.0 0.0.0.255 27.0.0.0 0.0.0.255  #access-list 130 permit icmp 110.0.0.0 0.0.0.255 28.0.0.0 0.0.0.255  #int g0/2  #ip access-group 130 out  #exit  **Switch- B1F4S1**  >en  #config t  #hostname B1F4S1  #vtp domain abc  #vlan 2  #name TeamMember  #vlan 3  #name TeamLead  #exit  #int f0/1  #switchport mode access  #switchport access vlan 2  #int f0/2  #switchport mode access  #switchport access vlan 2  #int f0/3  #switchport mode access  #switchport access vlan 3  #int g0/1  #switchport mode trunk  **Switch- B1F3S2**  >en  #config t  #hostname B2F3S2  #vtp domain abc  #vlan 2  #name TeamMember  #vlan 3  #name TeamLead  #exit  #int f0/1  #switchport mode access  #switchport access vlan 2  #int f0/2  #switchport mode access  #switchport access vlan 2  #int f0/3  #switchport mode access  #switchport access vlan 3  #int g0/1  #switchport mode trunk  **Switch- B1F2S3**  >en  #config t  #hostname B1F2S3  #vtp domain abc  #vlan 2  #name TeamMember  #vlan 3  #name TeamLead  #exit  #int f0/1  #switchport mode access  #switchport access vlan 2  #int f0/2  #switchport mode access  #switchport access vlan 2  #int f0/3  #switchport mode access  #switchport access vlan 3  #int g0/1  #switchport mode trunk  **Switch- B1F1S4**  >en  #config t  #hostname B1F1S4  #vtp domain abc  #vlan 2  #name Admin  #vlan 3  #name Reception  #exit  #int f0/1  #switchport mode access  #switchport access vlan 2  #int f0/2  #switchport mode access  #switchport access vlan 3  #int g0/1  #switchport mode trunk |
| **Configuration:- Building- 02**  **Router-B2F4R1**  >en  #config t  #hostname ProjectTeam4  #int g0/0  #no ip address  #no shut  #int g0/0.2  #encapsulation dot1q 2  #ip address 11.0.0.1 255.0.0.0  #no shut  #int g0/0.3  # encapsulation dot1q 3  #ip address 12.0.0.1 255.0.0.0  #no shut  #int g0/1  #ip address 13.0.0.1 225.0.0.0  #no shut  #exit  #router ospf 1  #network 11.0.0.0 0.0.0.255 area 0  #network 12.0.0.0 0.0.0.255 area 0  #network 13.0.0.0 0.0.0.255 area 0  **Router-B2F3R2**  >en  #config t  #hostname ProjectTeam5  #int g0/0  #no ip address  #no shut  #int g0/0.2  #encapsulation dot1q 2  #ip address 14.0.0.1 255.0.0.0  #no shut  #int g0/0.3  # encapsulation dot1q 3  #ip address 15.0.0.1 255.0.0.0  #no shut  #int g0/1  #ip address 13.0.0.2 225.0.0.0  #no shut  #int g0/2  #ip address 16.0.0.1 225.0.0.0  #no shut  #exit  #router ospf 1  #network 13.0.0.0 0.0.0.255 area 0  #network 14.0.0.0 0.0.0.255 area 0  #network 15.0.0.0 0.0.0.255 area 0  #network 16.0.0.0 0.0.0.255 area 0  **Router-B2F2R3**  >en  #config t  #hostname ProjectTeam6  #int g0/0  #no ip address  #no shut  #int g0/0.2  #encapsulation dot1q 2  #ip address 17.0.0.1 255.0.0.0  #no shut  #int g0/0.3  # encapsulation dot1q 3  #ip address 18.0.0.1 255.0.0.0  #no shut  #int g0/1  #ip address 16.0.0.2 225.0.0.0  #no shut  #int g0/2  #ip address 19.0.0.1 225.0.0.0  #no shut  #exit  #router ospf 1  #network 16.0.0.0 0.0.0.255 area 0  #network 17.0.0.0 0.0.0.255 area 0  #network 18.0.0.0 0.0.0.255 area 0  #network 19.0.0.0 0.0.0.255 area 0  **Router-B2F1R4**  >en  #config t  #hostname Non-TechnicalTeam2  #int g0/0  #no ip address  #no shut  #int g0/0.2  #encapsulation dot1q 2  #ip address 21.0.0.1 255.0.0.0  #no shut  #int g0/0.3  # encapsulation dot1q 3  #ip address 22.0.0.1 255.0.0.0  #no shut  #int g0/1  #ip address 19.0.0.2 225.0.0.0  #no shut  #int g0/2  #ip address 35.0.0.1 225.0.0.0  #no shut  #exit  #router ospf 1  #network 19.0.0.0 0 0.0.255 area 0  #network 21.0.0.0 0.0.0.255 area 0  #network 22.0.0.0 0.0.0.255 area 0  #network 35.0.0.0 0.0.0.255 area 0  #exit  #access-list 150 permit icmp 11.0.0.0 0.0.0.255 29.0.0.0 0.0.0.255  #access-list 150 permit icmp 12.0.0.0 0.0.0.255 29.0.0.0 0.0.0.255  #access-list 150 permit icmp 14.0.0.0 0.0.0.255 31.0.0.0 0.0.0.255  #access-list 150 permit icmp 15.0.0.0 0.0.0.255 31.0.0.0 0.0.0.255  #access-list 150 permit icmp 17.0.0.0 0.0.0.255 32.0.0.0 0.0.0.255  #access-list 150 permit icmp 18.0.0.0 0.0.0.255 32.0.0.0 0.0.0.255  #access-list 150 permit icmp 21.0.0.0 0.0.0.255 33.0.0.0 0.0.0.255  #access-list 150 permit icmp 22.0.0.0 0.0.0.255 34.0.0.0 0.0.0.255  #int g0/2  #ip access-group 150 out  #exit  **Switch- B2F4S1**  >en  #config t  #hostname B2F4S1  #vtp domain efg  #vlan 2  #name TeamMember  #vlan 3  #name TeamLead  #exit  #int f0/1  #switchport mode access  #switchport access vlan 2  #int f0/2  #switchport mode access  #switchport access vlan 2  #int f0/3  #switchport mode access  #switchport access vlan 3  #int g0/1  #switchport mode trunk  **Switch- B2F3S2**  >en  #config t  #hostname B2F3S2  #vtp domain efg  #vlan 2  #name TeamMember  #vlan 3  #name TeamLead  #exit  #int f0/1  #switchport mode access  #switchport access vlan 2  #int f0/2  #switchport mode access  #switchport access vlan 2  #int f0/3  #switchport mode access  #switchport access vlan 3  #int g0/1  #switchport mode trunk  **Switch- B2F2S3**  >en  #config t  #hostname B2F2S3  #vtp domain efg  #vlan 2  #name TeamMember  #vlan 3  #name TeamLead  #exit  #int f0/1  #switchport mode access  #switchport access vlan 2  #int f0/2  #switchport mode access  #switchport access vlan 2  #int f0/3  #switchport mode access  #switchport access vlan 3  #int g0/1  #switchport mode trunk  **Switch- B2F1S4**  >en  #config t  #hostname B1F1S4  #vtp domain efg  #vlan 2  #name Account  #vlan 3  #name Sales  #exit  #int f0/1  #switchport mode access  #switchport access vlan 2  #int f0/2  #switchport mode access  #switchport access vlan 3  #int g0/1  #switchport mode trunk |
| **Configuration:- Data Centre**  **Router-DCR1**  >en  #config t  #hostname DCR1  #int g0/0  #no ip address  #no shut  #int g0/0.2  #encapsulation dot1q 2  #ip address 24.0.0.1 255.0.0.0  #no shut  #int g0/0.3  #encapsulation dot1q 3  #ip address 25.0.0.1 255.0.0.0  #no shut  #int g0/0.4  #encapsulation dot1q 4  #ip address 26.0.0.1 255.0.0.0  #int g0/0.5  #encapsulation dot1q 5  #ip address 27.0.0.1 255.0.0.0  #int g0/0.6  #encapsulation dot1q 6  #ip address 28.0.0.1 225.0.0.0  #no shut  #int g0/1  #ip address 23.0.0.2 255.0.0.0  #no shut  #int g0/2  #ip address 36.0.0.1 255.0.0.0  #no shut  #exit  #router ospf 1  #network 24.0.0.0 0.0.0.255 area 0  #network 25.0.0.0 0.0.0.255 area 0  #network 26.0.0.0 0.0.0.255 area 0  #network 27.0.0.0 0.0.0.255 area 0  #network 28.0.0.0 0.0.0.255 area 0  #network 23.0.0.0 0.0.0.255 area 0  #network 36.0.0.0 0.0.0.255 area 0  #exit  **Router-DCR2**  >en  #config t  #hostname DCR2  #int g0/0  #no ip address  #no shut  #int g0/0.2  #encapsulation dot1q 2  #ip address 29.0.0.1 255.0.0.0  #no shut  #int g0/0.3  #encapsulation dot1q 3  #ip address 31.0.0.1 255.0.0.0  #no shut  #int g0/0.4  #encapsulation dot1q 4  #ip address 32.0.0.1 255.0.0.0  #int g0/0.5  #encapsulation dot1q 5  #ip address 33.0.0.1 255.0.0.0  #int g0/0.6  #encapsulation dot1q 6  #ip address 34.0.0.1 225.0.0.0  #no shut  #int g0/1  #ip address 35.0.0.2 255.0.0.0  #no shut  #int g0/2  #ip address 36.0.0.2 255.0.0.0  #no shut  #exit  #router ospf 1  #network 29.0.0.0 0.0.0.255 area 0  #network 31.0.0.0 0.0.0.255 area 0  #network 32.0.0.0 0.0.0.255 area 0  #network 33.0.0.0 0.0.0.255 area 0  #network 34.0.0.0 0.0.0.255 area 0  #network 35.0.0.0 0.0.0.255 area 0  #network 36.0.0.0 0.0.0.255 area 0  **Switch-DCS1**  >en  #config t  #hostname DCS1  #vtp domain abc  #vlan 2  #name Team1 Server  #vlan 3  #name Team2 Server  #vlan 4  #name Team3 Server  #vlan 5  #name Admin  #vlan 6  #name Reception  #exit  #int f0/1  #switchport mode access  #switchport access vlan 2  #int f0/2  #switchport mode access  #switchport access vlan 3  #int f0/3  #switchport mode access  #switchport access vlan 4  #int f0/4  #switchport mode access  #switchport access vlan 5  #int f0/5  #switchport mode access  #switchport access vlan 6  #int g0/1  #switchport mode trunk  **Switch-DCS2**  >en  #config t  #hostname DCS2  #vtp domain efg  #vlan 2  #name Team4 Server  #vlan 3  #name Team5 Server  #vlan 4  #name Team6 Server  #vlan 5  #name Account  #vlan 6  #name Sales  #exit  #int f0/1  #switchport mode access  #switchport access vlan 2  #int f0/2  #switchport mode access  #switchport access vlan 3  #int f0/3  #switchport mode access  #switchport access vlan 4  #int f0/4  #switchport mode access  #switchport access vlan 5  #int f0/5  #switchport mode access  #switchport access vlan 6  #int g0/1  #switchport mode trunk  Access Point Configuration  Building 1  Floor 4- Project Team 1    Floor 3- Project Team 2      Floor 2- Project Team 3      FLOOR - 1 Non-Technical Team 1    Building 2  Floor 4- Project Team 4    Floor 3- Project Team 5    Floor 2 - Project Team 6    FLOOR - 1 Non-Technical Team 2    Testing and Validation  Building 1- Project Team 1 to Team1 Server    Building 2 - Project Team 4 to Team4 Server    Non-Technical Team 1  Admin users to Admin Server    Reception users to Reception Server    Non-Technical Team 2  Account users to Accounts Server    Sales users to Sales Server    Conclusion  • The implementation of network design and ACLs has significantly improved network connectivity and security by mitigating vulnerabilities and enforcing access controls within the organization's network infrastructure. The project's findings and recommendations provide a excellent connectivity between networks and distribution of networks for different departments for ongoing security enhancements, ensuring the floor design, network design and security policies.  • Identification of design and policy: The project team conducted a thorough assessment of the network infrastructure, identifying required network design and connectivity. This allowed for targeted remediation efforts and the implementation of appropriate design and security controls.  • Implementation of Security Measures: The project implemented a range of security measure access control mechanisms. These measures provided layers of defense to safeguard the network against unauthorized access, data breaches, and malicious activities.  • Continuous Monitoring and Improvement: The project established a framework for continuous monitoring and improvement, including regular security assessments, vulnerability scanning, and patch management. This proactive approach ensures that the network security remains up to date and effective against emerging threats. |