Access Control List

ACL stands for Access Control List, a fundamental network security feature used to control the traffic flow within a network or between networks. ACLs are configured on routers, switches, and firewalls to filter packets based on specified criteria, such as source/destination IP addresses, protocols, port numbers, and other packet attributes. Here's an overview of ACLs:

Purpose of ACLs:

- **Control Access:** ACLs allow network administrators to permit or deny traffic based on defined rules, thereby controlling which packets are allowed to pass through network devices.
- **Enhance Security:** By filtering traffic, ACLs help mitigate security risks by blocking unauthorized access, preventing DoS (Denial of Service) attacks, and protecting against malicious activity.
- **Optimize Network Performance:** ACLs can be used to prioritize certain types of traffic (Quality of Service) or block unwanted traffic, improving network performance and resource utilization.

Types of ACLs:

1. **Standard ACLs:**

   - Filter traffic based solely on the source IP address.
   - Typically used for simple access control requirements.
   - Example: Blocking or permitting traffic from specific IP addresses.

2. **Extended ACLs:**

   - Filter traffic based on both source and destination IP addresses, protocols, port numbers, and other packet attributes.
   - Offer more granular control over traffic compared to standard ACLs.
   - Example: Allowing or denying specific types of traffic (e.g., HTTP, FTP, ICMP) between certain hosts or networks.

> It is applicable for router and firewall Applicable to layer 3 devices you can apply only one ACL on one interface.

ACL Configuration:

- ACLs are configured using a series of permit or deny statements, which define the criteria for filtering traffic.
- Each ACL statement includes one or more match conditions, such as source/destination IP addresses, protocols, and port numbers.
- ACLs are applied to specific interfaces (inbound or outbound) or VLANs on routers, switches, or firewalls.
- ACLs are processed sequentially, with each packet being evaluated against the ACL statements until a match is found. Once a match is found, the corresponding action (permit or deny) is applied, and further processing stops.

Best Practices:

- Use descriptive names for ACLs to easily identify their purpose and functionality.
- Implement the principle of least privilege, allowing only the necessary traffic and denying all other traffic by default.
- Regularly review and update ACL configurations to adapt to changes in network requirements and security threats.
- Test ACL configurations in a controlled environment before deploying them in production to ensure they function as intended.

```
A(config)# access-list 10 permit 172.16.10.2 0.0.0.0
A(config)# access-list 10 permit 172.16.10.3 0.0.0.0

A(config)# int g0/0
A(config-if)# ip access-group 15 in

A(config-if)# ip access-group <access list number> <in/out>
```

here in / out is to allow traffic or to deny traffic

IF you deny perticular host in network

```
A(config)# access-list 25 deny 172.16.10.2 0.0.0.0
A(config)# access-list 25 deny host 172.16.10.3
A(config)# access-list 25 permit 172.16.10.0 0.0.0.255

A(conifg)# int g0/0
A(conifig)# access-group 25 in
```

if you want to permit rest of all host

```
A(config-if)# access-group 25 any
```

> Access list should contains one permit statements.

syntax

```
A(config)# access-list <Number> <protocol> <source server ip> <wildcard mask>
<destination ip> <wildcard mask> eq <port on keyword>
```

here Number - 100-199 protocol - IP, ICMP, UDP, TCP

Golden Rule for ACL:

Rule 1

- There is implicit deny any at the end of every access list so,
  - access list should not carry all deny statement, it must have at least one permit statement.
  - whatever not matching with access list gets discarded.

Rule 2

- Specific statement should be applied at the top.

Rule 3

- Only one access list per interface per direction is allowed.

By using NACL (Named Access Control List):

A Named Access Control List (NACL) is a type of ACL configuration that allows administrators to assign a descriptive name to an ACL rule set, making it easier to identify and manage. Unlike numbered ACLs, where ACLs are identified by numeric IDs, named ACLs use user-defined names for identification. Here's an overview of Named ACLs:

Purpose of Named ACLs:

- **Improved Manageability:** Named ACLs use descriptive names, making it easier to understand and manage ACL configurations, especially in environments with multiple ACLs.
- **Ease of Modification:** Named ACLs allow administrators to modify ACL rules without needing to renumber ACL entries, reducing the risk of misconfiguration and simplifying maintenance.
- **Clarity and Documentation:** By providing meaningful names for ACLs, named ACLs enhance documentation and clarity, facilitating communication among network administrators and stakeholders.

Key Characteristics of Named ACLs:

1. **User-Defined Names:**

   - Named ACLs are identified by user-defined names rather than numeric IDs.
   - Names must adhere to specific naming conventions, such as using alphanumeric characters and underscores, and avoiding spaces and special characters.

2. **Flexible Syntax:**

   - Named ACLs support both standard and extended ACL configurations, offering flexibility in defining access control rules.
   - ACL statements within a named ACL follow the same syntax as numbered ACLs, consisting of permit or deny statements with match conditions.

3. **Application to Interfaces or VLANs:**

   - Like numbered ACLs, named ACLs can be applied to specific interfaces (inbound or outbound) or VLANs on routers, switches, or firewalls.
   - The application process remains the same, regardless of whether the ACL is named or numbered.

Advantages of Named ACLs:

- **Simplicity and Readability:** Named ACLs provide descriptive names that reflect their purpose, making them easier to understand and interpret compared to numeric IDs.
- **Scalability:** Named ACLs are scalable and well-suited for environments with numerous ACLs, as they can be organized and managed more efficiently.
- **Ease of Troubleshooting:** With meaningful names, troubleshooting ACL-related issues becomes more straightforward, as administrators can quickly identify the ACLs involved.

commands:

```
A(conif)# ip access-list extended blocktelnet
A(config-ext-nacl)# permit tcp host 172.16.10.0 0.0.0.255 host 172.16.20.2 eq 23
A(config-ext-nacl)# deny tcp host 172.16.10.0 0.0.0.255 host 172.16.20.2 eq 23
A(config-ext-nacl)# permit ip any any

A(conifg)# int g0/0
A(conifg-if)# ip access-group blocktelnet ip
```

WAN Technologies:

In Wide Area Networks (WANs), various types of connections are used to establish communication between geographically dispersed locations. Three common types of connections in WANs are dedicated lines, circuit-switched lines, and packet-switched lines. Here's an overview of each:

1. **Dedicated Line:**

   - **Description:** Dedicated lines, also known as leased lines, provide a continuous, dedicated connection between two points in a network.
   - **Characteristics:**
     - **Permanent Connection:** The connection is established and remains active 24/7, regardless of whether data is being transmitted.
     - **Fixed Bandwidth:** The bandwidth of the dedicated line is predetermined and dedicated exclusively to the connected sites.
   - **Applications:**
     - Ideal for organizations requiring constant and reliable connectivity between remote locations, such as banks, multinational corporations, and data centers.
     - Used for critical applications that demand high reliability and low latency, such as real-time data transfer and voice/video conferencing.

2. **Circuit-Switched Line:**

   - **Description:** Circuit-switched lines establish a temporary, dedicated connection between two points only when data needs to be transmitted.
   - **Characteristics:**
     - **On-Demand Connection:** The connection is established dynamically when needed and terminated after data transmission is complete.
     - **Variable Bandwidth:** Bandwidth is allocated dynamically based on the data transfer requirements at the time.
   - **Applications:**

    - Historically used for traditional telephone systems and dial-up internet connections.
    - Less common in modern WANs due to the prevalence of more efficient and cost-effective technologies, such as packet switching.

3. **Packet-Switched Line:**

    - **Description:** Packet-switched lines transmit data in discrete packets over shared network infrastructure.
    - **Characteristics:**
        - **Packet-Based Transmission:** Data is segmented into packets, which are individually routed across the network to their destination.
        - **Shared Bandwidth:** Bandwidth is shared among multiple users, allowing for efficient utilization of network resources.
    - **Technologies:**
        - **Frame Relay:** Provides virtual circuits for data transmission, offering predictable performance and cost-effective connectivity.
        - **Asynchronous Transfer Mode (ATM):** Uses fixed-size cells for data transmission, suitable for both voice and data applications.
        - **Internet Protocol (IP):** The foundation of the modern internet, routing packets based on IP addresses using technologies like MPLS (Multiprotocol Label Switching).

Line Termination Equipment (LTE)

Line Termination Equipment (LTE) refers to devices or systems that facilitate the connection between customer premises equipment (CPE) and the wide area network (WAN). LTE plays a crucial role in establishing and maintaining connectivity over various types of WAN technologies. Here's an overview of LTE:

Functionality:

1. **Interface Management:**

    - LTE manages the interface between the customer's network and the WAN infrastructure.
    - It ensures compatibility between different network protocols and standards used by the CPE and the WAN.

2. **Signal Conversion:**

    - LTE may perform signal conversion tasks, translating signals from one format to another as required by the WAN technology.
    - For example, LTE may convert digital signals from the customer's network into analog signals suitable for transmission over analog lines.

3. **Signal Amplification and Conditioning:**

    - LTE may amplify signals to ensure proper transmission over long distances or through challenging environments.
    - It may also condition signals to improve signal quality and reduce noise interference.

4. **Protocol Conversion:**

    - LTE may convert between different communication protocols used by the CPE and the WAN.

- For example, LTE may convert Ethernet frames into the appropriate protocol for transmission over a leased line or a packet-switched network.

5. **Error Handling and Correction:**

   - LTE may perform error detection and correction functions to ensure data integrity during transmission.
   - It may retransmit corrupted or lost data packets to ensure reliable communication between the CPE and the WAN.

6. **Security Features:**

   - LTE may incorporate security features such as encryption and authentication to protect data transmitted over the WAN.
   - It may implement VPN (Virtual Private Network) technologies to establish secure communication channels between remote locations and corporate networks.

Types of Line Termination Equipment:

1. **Modems:**

   - Modems are devices that modulate digital data into analog signals for transmission over analog lines (e.g., dial-up modems) or demodulate analog signals into digital data (e.g., DSL modems).

2. **CSU/DSU (Channel Service Unit/Data Service Unit):**

   - CSU/DSU devices are used to connect customer equipment to digital leased lines or T1/E1 circuits.
   - They perform signal conditioning, line monitoring, and clocking functions to ensure reliable communication over digital lines.

3. **Routers:**

   - Routers often serve as LTE, especially in packet-switched networks like the Internet.
   - They perform a wide range of functions, including protocol conversion, packet forwarding, and security enforcement.

4. **Network Interface Cards (NICs):**

   - NICs installed in servers or workstations may also serve as LTE, providing the interface between the device and the WAN.

> CPE- Customer Premices Equipment POP- Point of Presence Demark- Demarkation

High-Level Data Link Control (HDLC):

High-Level Data Link Control (HDLC) is a bit-oriented synchronous data link layer protocol used for communication over point-to-point and multipoint links. It provides a reliable and efficient method for transmitting data between network devices, especially in synchronous serial communication environments. Here's an overview of HDLC:

Frame Structure:

- HDLC frames consist of a header, data payload, and trailer.
- The header includes flags for frame delineation, control fields for addressing and control information, and error detection mechanisms.
- The data payload carries the actual data to be transmitted.
- The trailer contains error checking information, such as a Frame Check Sequence (FCS), for data integrity verification.

> Default framing techinque on CISCO router WAN interface it work only on synchronious links Its vendor specifice so both router should purchase from same vendor.

Network IP IPX AT

```
                        IPCP        IPICP       ATCP
```

```
                        [           NCP            ]
```

DataLink [LCP] (Line Control Protocol) --> Multilink --> Compression -> Stacker - compress dictionary send through WAN another router decompress it.

```
                                                            -> Predictor
                                                              - router (IOS)
                                                              - It is very fast,
less
                                                              compression.

                                                            -> Error Detection
Mechanism
                                                              - quality and magic
number.

                                                            -> Authentication
                                                            - 1. PAP
                                                                (Password
Authentication
                                                                Protocol)
                                                                - Two way(it sent
username
                                                                and password)
                                                                - Plain text once
                                                            - 2. CHAP
                                                                (Challange
Handshake
                                                                Authentication
Protocol)
```

```
                                                                - Encrypted,
Periodic
```

--- [HDLC]

Authentication Command (PAP and CHAP)

```
A(config)# int S0
A(config -if)# encap ppp
A(config-if)# ppp authentication chap pap
A(config-if)# exit
```

```
A(config)# username B password cisco
```

syntax

```
A(config)# username <hostname of remote router> password < Passowrd It should be same for both router>
```