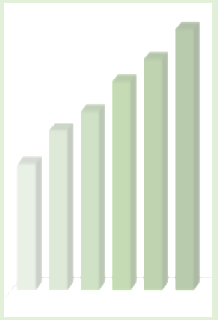
Presentation
On

ACL
(Access Control List)

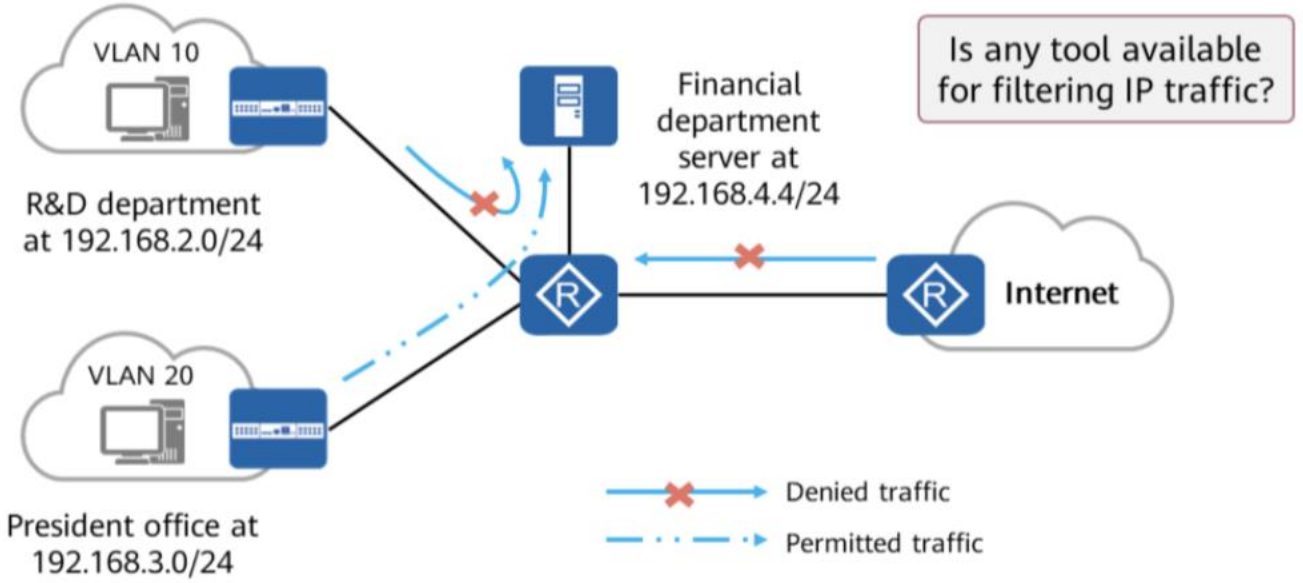


BdREN

Connect
Collaborate
Innovate

Venue: KUET

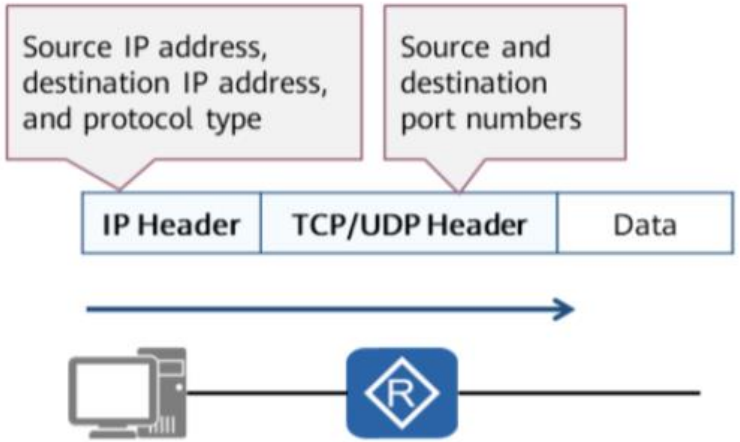
Background: A tool required to filter traffic



- To ensure financial data security, an enterprise prohibits the R&D department's access to the financial department server but allows the president office's access to the Financial department server.

ACL Overview

- An ACL is a set of sequential rules composed of permit or deny statement used to control network traffic.
- An ACL matches and distinguishes packets.
- It filters packets based on predefined conditions.
- Purpose: Enhance security and manage traffic efficiently.



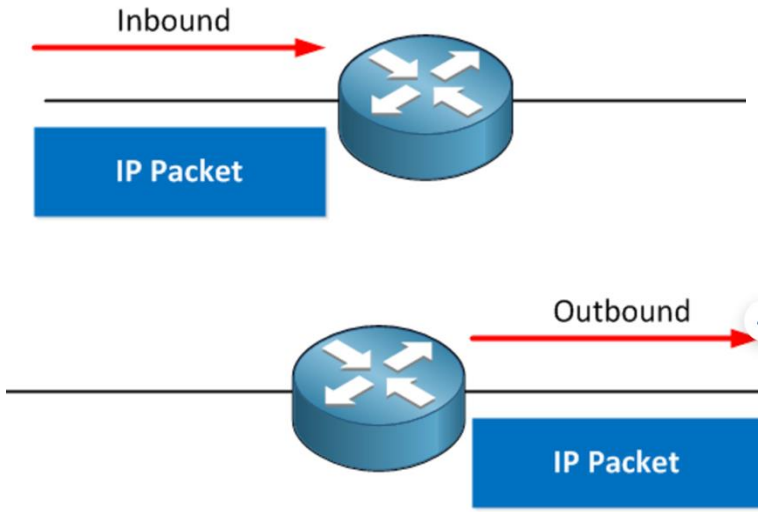
ACL Application

- Access-lists work on the network (layer 3) and the transport (layer 4) layer and can be used for two different things:

  - **Filtering:** Filtering permits or denies traffic reaching certain parts of our network.
  - **Classification:** Classification does not drop IP packets as filtering does, but we use it to "select" traffic.

Use Case:

- Matching IP traffic
- Used in a traffic filter
- Used in Network Address Translation (NAT)
- Used in a routing policy
- Used in a firewall policy
- Used in QoS.



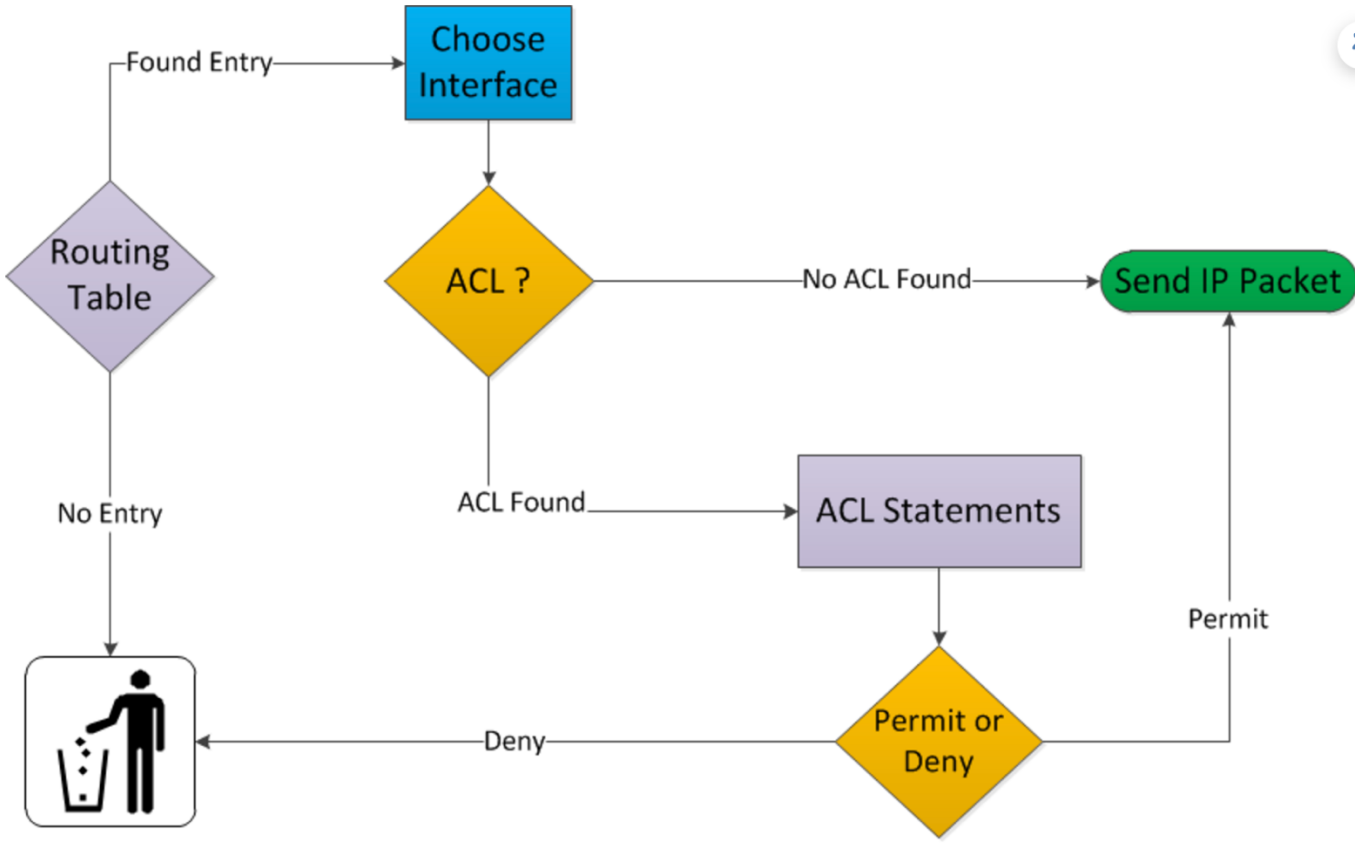
Types of ACL

- Standard ACL:
  - Filters traffic based on source IP address.
  - Can allow/block network, host, subnet.
  - All services are blocked.
  - Filtering is done based on only source IP address.
- Extended ACL:
  - Filters traffic based on source and destination IP, port, and protocol.
  - Can allow or block network, host, subnet or service.
  - Selected services can be blocked.
  - Filtering is done based on source IP, destination IP, Protocol, Port number.

Types of ACL

- Named ACL
  - Provides a user-friendly name for easier management.
- Numbered ACL
  - 1-99 for Standard ACL
  - 100-199 Extended ACL

ACL Working Process



Best Practices and Configuration Example

Connect
Collaborate
Innovate

Best Practices:

- Place standard ACLs close to the destination
- Place extended ACLs close to the source.
- Document ACL rules for easier management.
- Regularly review and update ACLs.

Configuration Example:

- Define the ACL:
  - access-list 10 permit 192.168.1.0 0.0.0.255
- Apply the ACL:
  - 'ip access-group 10 in' on an interface.
- Verify:
  - Use 'show access-lists' to check configurations.

THANK YOU

BdREN
Connect
Collaborate
Innovate