Days 34, 35: Access Control Lists

CCNA 200-301 Study Guide: Mastering Access Control Lists (ACLs)

1.0 Introduction: The Role of ACLs

In network engineering, an Access Control List (ACL) acts as a security bouncer. It inspects every packet attempting to cross a router interface and decides to Permit or Deny it based on specific rules.

Beyond security, ACLs are also used to "match" or classify traffic for:

- NAT (Network Address Translation)
- QoS (Quality of Service)
- Demand Dial Routing

2.0 The Core Principles of ACL Processing

ACL logic is strict and predictable. Routers follow three fundamental rules when evaluating a packet against a list:

1. Sequential Order (Top-Down): The router starts at the first line and moves down.
2. First Match Execution: As soon as a match is found, the action (Permit/Deny) is taken, and processing stops. The router does not check subsequent lines.
3. The Implicit Deny: Every ACL ends with an invisible, unwritten deny any any. If a packet doesn't match any of your permit rules, it is dropped.

Instructor's Note: Because of the implicit deny, every functional ACL must contain at least one permit statement, or it will block 100% of traffic.

Application Rules

- One ACL per interface, per protocol, per direction.
- An interface can have one inbound IPv4 ACL and one outbound IPv4 ACL.

3.0 Standard vs. Extended ACLs

Feature	Standard ACL	Extended ACL
Criteria	Source IP Address only.	Source/Dest IP, Protocol, and Ports.
Number Range	1–99 and 1300–1999	100–199 and 2000–2699
Granularity	Low (Sledgehammer)	High (Scalpel)
Placement	Closest to the Destination	Closest to the Source

The Placement Logic

- Standard (Sledgehammer): Since it only checks the source, placing it near the source might block the user from reaching everything. Place it near the destination to be specific.
- Extended (Scalpel): Since it knows exactly where the packet is going and what port it's using, place it near the source to drop unwanted traffic early and save bandwidth.

4.0 Wildcard Masks and Syntax

4.1 Wildcard Mask Logic

Wildcard masks are the inverse of subnet masks.

- 0 bit: Match Exactly.
- 1 bit: Ignore ("Don't Care").

Keywords:

- host: Equivalent to wildcard 0.0.0.0 (matches one IP).
- any: Equivalent to wildcard 255.255.255.255 (matches everything).

4.2 Configuration Syntax

Standard ACL:

access-list 10 permit 192.168.1.0 0.0.0.255

Extended ACL:

access-list 101 permit tcp 10.1.1.0 0.0.0.255 any eq 80

Pro Tip: The established keyword in Extended ACLs allows return traffic for already active TCP sessions but blocks new connections initiated from the outside.

5.0 Essential Protocol and Port Reference

Service	Protocol	Port	Transport
ICMP	1	N/A	IP
TCP	6	N/A	IP
UDP	17	N/A	IP
SSH	N/A	22	TCP
Telnet	N/A	23	TCP
DNS	N/A	53	TCP/UDP
HTTP	N/A	80	TCP
HTTPS	N/A	443	TCP
TFTP	N/A	69	UDP

6.0 ACL Management and Verification

6.1 Editing with Sequence Numbers

Modern IOS allows you to edit specific lines without deleting the whole list:

1. ip access-list extended 101
2. no 20 (Deletes line 20)
3. 25 permit udp any any eq 53 (Inserts new rule at line 25)

Resequencing: ip access-list resequence 101 10 10 (Starts at 10, increments by 10).

6.2 Verification Commands

- show access-lists: The most important command. Shows the rules and the "hit counts" (how many times a rule was matched).
- show ip interface <id>: Confirms if an ACL is applied and in which direction (In/Out).

7.0 Key Takeaways Summary

1. Top-Down Logic: Once a match is made, the router stops looking.
2. Implicit Deny: If you don't permit it, it's denied by default.
3. Standard: Match Source IP; place near Destination.
4. Extended: Match Source, Dest, Protocol, Port; place near Source.
5. Troubleshooting: Use show access-lists to check hit counts and verify your logic is actually catching traffic.

Revision #1
Created 2026-03-14 19:33:20 UTC by Tony Utter
Updated 2026-03-14 19:33:36 UTC by Tony Utter