Wednesday, July 16, 2025 8:58 PM

🔐 What is ACL (Access Control List)?

ACL stands for **Access Control List** — it's a set of **rules** used on **routers or switches** (mostly Cisco devices) to **control network traffic** and improve **security**.

ACLs **filter traffic** based on:

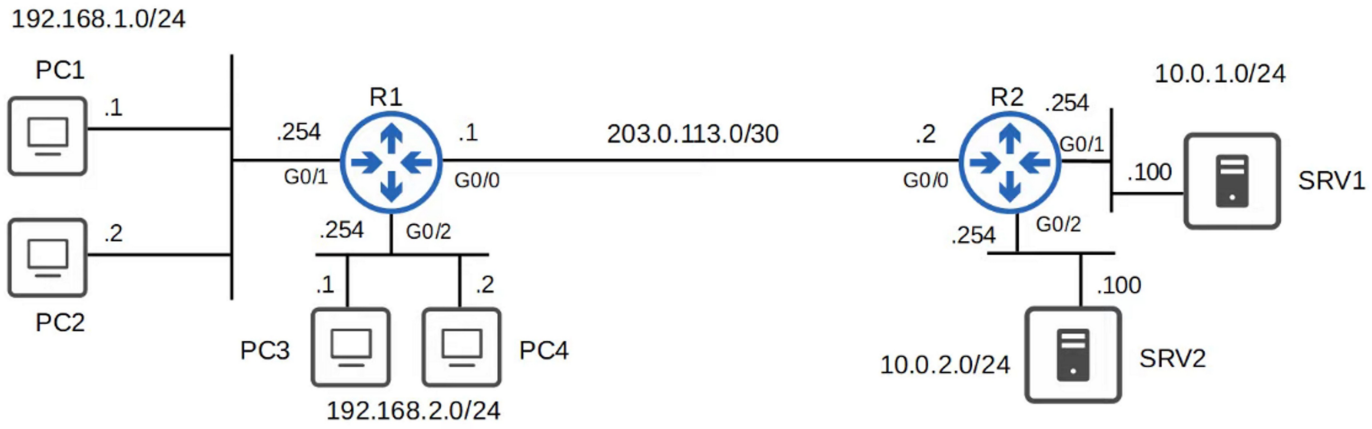
- IP addresses
- Protocols (TCP, UDP, ICMP, etc.)
- Port numbers
- Source/destination info

🧠 Why Use ACL?

ACLs decide:

- Which traffic is **allowed** or **denied**
- Who can **access what**
- Which ports and services are **restricted**

They're like **traffic police** for routers, controlling **who can enter or exit** the network.



📜 Where are ACLs Applied?

ACLs can be applied on:

- **Inbound** traffic: Before it enters an interface
- **Outbound** traffic: Before it leaves an interface

interface FastEthernet0/0
ip access-group 100 in

📚 Types of ACLs in Cisco

There are **two main types** of ACLs:

Type	Description	Filtering Capability
Standard ACL	Filters **only by source IP**	Basic

Extended ACL Filters by **source, destination, protocol, and port** Advanced

- Standard ACLs: Match based on **Source IP address** only
  - → Standard Numbered ACLs
  - → Standard Named ACLs

- Extended ACLs: Match based on **Source/Destination IP, Source/Destination port,** etc.
  - → Extended Numbered ACLs
  - → Extended Named ACLs

🔸 **1. Standard ACL**

✅ **What it does:**

- Filters traffic **based only on source IP address**
- Cannot filter by port or protocol

🔢 **Number Range:**

- 1 to 99 (or 1300–1999)

🔧 **Example:**

```
access-list 10 deny 192.168.1.5
access-list 10 permit any
interface fa0/0
ip access-group 10 in
```

🔍 Meaning: Block traffic from 192.168.1.5, allow everything else.

🔹 **2. Extended ACL**

✅ **What it does:**

- Filters traffic by:
  - **Source IP**
  - **Destination IP**
  - **Protocol** (TCP, UDP, ICMP)
  - **Port number** (e.g., 80 for HTTP, 23 for Telnet)

🔢 **Number Range:**

- 100 to 199 (or 2000–2699)

🔧 **Example:**

```
access-list 101 deny tcp 192.168.1.5 0.0.0.0 10.0.0.10 0.0.0.0 eq 80
```

access-list 101 permit ip any any
interface fa0/0
ip access-group 101 in
🔍 Meaning: Deny only HTTP (port 80) from 192.168.1.5 to 10.0.0.10. Allow all other traffic.

📂 Named ACLs (Optional Format)

You can name an ACL instead of using numbers:

🔧 **Example:**

ip access-list standard BLOCK_HOST
deny 192.168.1.5
permit any

📜 ACL Wildcard Masks

Used to match IP ranges (opposite of subnet masks):

Subnet Mask	Wildcard Mask
255.255.255.0	0.0.0.255
255.255.0.0	0.0.255.255

✅ Summary Table

Feature	Standard ACL	Extended ACL
Filters by	Source IP only	Source, Destination, Protocol, Port
Number Range	1–99	100–199
Control Level	Basic	Advanced
Placement Best	Near destination	Near source

```
R1(config)#access-list 1 deny 1.1.1.1 0.0.0.0
R1(config)#access-list 1 permit 0.0.0.0 255.255.255.255
R1(config)#access-list 1 remark ## BLOCK BOB FROM ACCOUNTING ##
R1(config)#
R1(config)#do show access-lists
Standard IP access list 1
    10 deny   1.1.1.1
    20 permit any
R1(config)#
R1(config)#do show ip access-lists
Standard IP access list 1
    10 deny   1.1.1.1
    20 permit any
R1(config)#
R1(config)#do show running-config | include access-list
access-list 1 deny   1.1.1.1
access-list 1 permit any
access-list 1 remark ## BLOCK BOB FROM ACCOUNTING ##
R1(config)#
```

Standard Numbered ACLs

```
R1(config)#access-list 1 permit 192.168.1.1
R1(config)#access-list 1 deny 192.168.1.0 0.0.0.255
R1(config)#access-list 1 permit any
R1(config)#
R1(config)#interface g0/2
R1(config-if)#ip access-group 1 out
R1(config-if)#
```

Requirements:
- PC1 can access 192.168.2.0/24.
- Other PCs in 192.168.1.0/24 can't access 192.168.2.0/24.