Monday, July 21, 2025 7:32 PM

🔐 What is Extended ACL? (Access Control List)

An **Extended ACL** (Access Control List) is a set of rules used on routers (mostly Cisco) to **control traffic more precisely** — not just by **IP address**, but also by **protocol**, **port number**, and **source/destination**.
It gives **more control and security** than a standard ACL.

📌 Extended ACL Key Features:

Feature	Description
✅ Filters by	**Source IP, Destination IP, Protocol, Port**
📍 Applied	**Near the source** (to save bandwidth)
📁 Number range	**100–199** (or **2000–2699** for expanded range)
📊 More detailed	Can allow/deny based on TCP, UDP, ICMP, etc.

🧠 Why Use Extended ACL?

If you want to block:

- A specific **IP** accessing a **web server**
- A **host** using a specific **protocol (like FTP or Telnet)**
- **Only HTTP (port 80)** traffic from a source to destination

... then you use an **Extended ACL**.

📦 Extended ACL Format:

access-list <number> <permit|deny> <protocol> <source> <wildcard> <destination> <wildcard> [eq <port_number>]

🧪 Example 1: Block HTTP from a specific IP

Task: Block 192.168.1.5 from accessing 10.0.0.10 on port 80 (HTTP)

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

👉 Explanation:

- 101: Extended ACL number
- deny tcp: Block TCP protocol
- 192.168.1.5: Source IP
- 10.0.0.10: Destination IP

- eq 80: Matches HTTP (port 80)

🧪 Example 2: Allow only FTP from 192.168.1.0/24 to 10.0.0.0/24

```
access-list 110 permit tcp 192.168.1.0 0.0.0.255 10.0.0.0 0.0.0.255 eq 21
access-list 110 deny ip any any
```

✅ Apply the ACL to an Interface

```
interface FastEthernet0/0
ip access-group 101 in
```

- in: Apply to incoming traffic
- out: Apply to outgoing traffic

🔄 Wildcard Mask Reminder

Subnet Mask	Wildcard Mask
255.255.255.0	0.0.0.255
255.0.0.0	0.255.255.255

✅ Summary

Type	Extended ACL
Filters on	IP, protocol, port
Example	Deny Telnet, allow HTTP
Range	100–199
Placement	Close to source
Flexibility	High

```
R1(config)#ip access-list extended EXAMPLE
R1(config-ext-nacl)#deny ?
  <0-255>        An IP protocol number
  ahp            Authentication Header Protocol
  eigrp          Cisco's EIGRP routing protocol
  esp            Encapsulation Security Payload
  gre            Cisco's GRE tunneling
  icmp           Internet Control Message Protocol
  igmp           Internet Gateway Message Protocol
  ip             Any Internet Protocol
  ipinip         IP in IP tunneling
  nos            KA9Q NOS compatible IP over IP tunneling
  object-group   Service object group
  ospf           OSPF routing protocol
  pcp            Payload Compression Protocol
  pim            Protocol Independent Multicast
  sctp           Stream Control Transmission Protocol
  tcp            Transmission Control Protocol
  udp            User Datagram Protocol
```

1: ICMP
6: TCP
17: UDP
88: EIGRP
89: OSPF

```
R1(config-ext-nacl)#deny tcp ?
  A.B.C.D        Source address
  any            Any source host
  host           A single source host
  object-group   Source network object group

R1(config-ext-nacl)#deny tcp any ?
  A.B.C.D        Destination address
  any            Any destination host
  eq             Match only packets on a given port number
  gt             Match only packets with a greater port number
  host           A single destination host
  lt             Match only packets with a lower port number
  neq            Match only packets not on a given port number
  object-group   Destination network object group
  range          Match only packets in the range of port numbers

R1(config-ext-nacl)#deny tcp any 10.0.0.0 ?
  A.B.C.D  Destination wildcard bits

R1(config-ext-nacl)#deny tcp any 10.0.0.0 0.0.0.255
R1(config-ext-nacl)#
```

In extended ACLs, to specify a /32 source or destination you have to use the **host** option or specify the wildcard mask.
You can't just write the address without either of those.

```
R1(config-ext-nacl)#deny tcp src-ip  eq   src-port-num   dest-ip  eq   dst-port-num
                                     gt                           gt
                                     lt                           lt
                                     neq                          neq
                                     range                        range
```

- **eq 80** = equal to port 80
- **gt 80** = greater than 80 (81 and greater)
- **lt 80** = less than 80 (79 and less)
- **neq 80** = NOT 80
- **range 80 100** = from port 80 to port 100

TCP
- FTP data (20)
- FTP control (21)
- SSH (22)
- Telnet (23)
- SMTP (25)
- HTTP (80)
- POP3 (110)
- HTTPS (443)

UDP
- DHCP server (67)
- DHCP client (68)
- TFTP (69)
- SNMP agent (161)
- SNMP manager (162)
- Syslog (514)

TCP & UDP
- DNS (53)