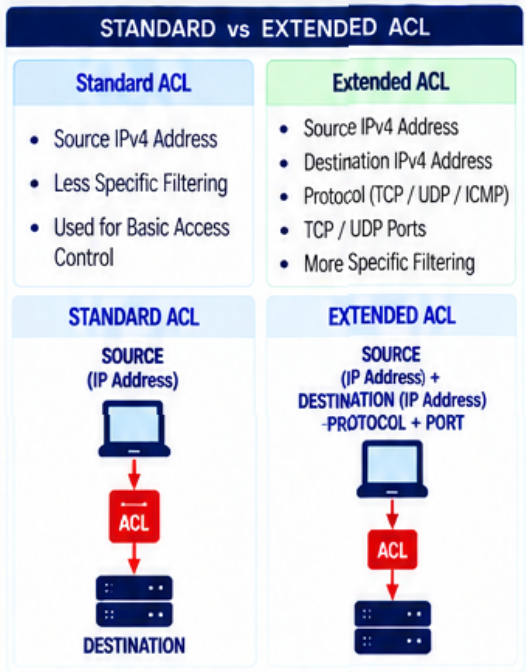
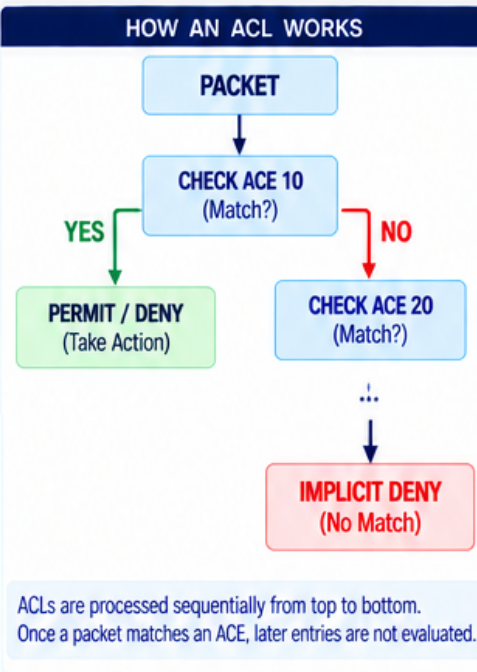


ACL QUICK FACTS	
Feature	Description
Full Name	Access Control List
Main Purpose	Permit / Deny Traffic
Rule	Access Control Entry (ACE)
Processing	Top → Bottom
Match Behavior	First Match Wins
Default End	Implicit Deny
Application	Interface + Direction

ACLs use ordered rules called Access Control Entries (ACEs) to classify and control traffic.



NUMBERED vs NAMED ACL

Numbered ACL	Named ACL
access-list 10 permit ...	ip access-list standard USERS permit ...

Common IPv4 ACL Number Ranges

ACL Type	Number Range
Standard	1 – 99
Extended	100 – 199
Expanded Standard	1300 – 1999
Expanded Extended	2000 – 2699

Named ACLs use descriptive names instead of ACL numbers.

WILDCARD MASKS

A wildcard mask determines which address bits must match.

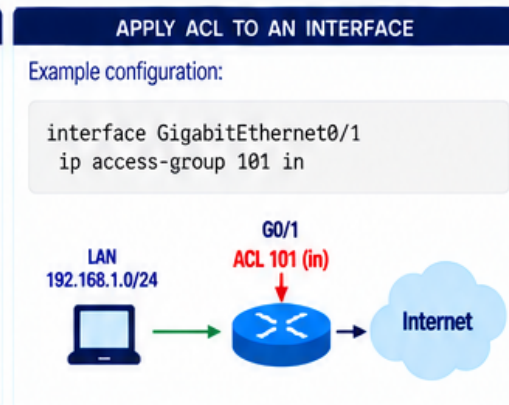
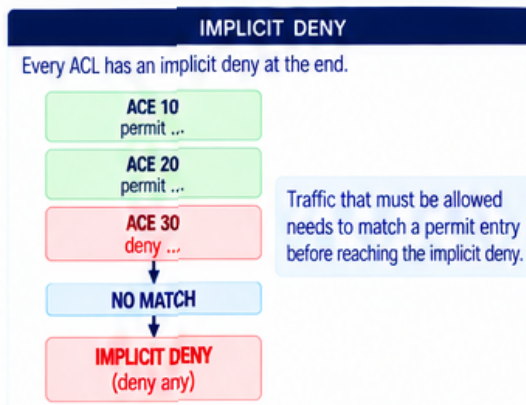
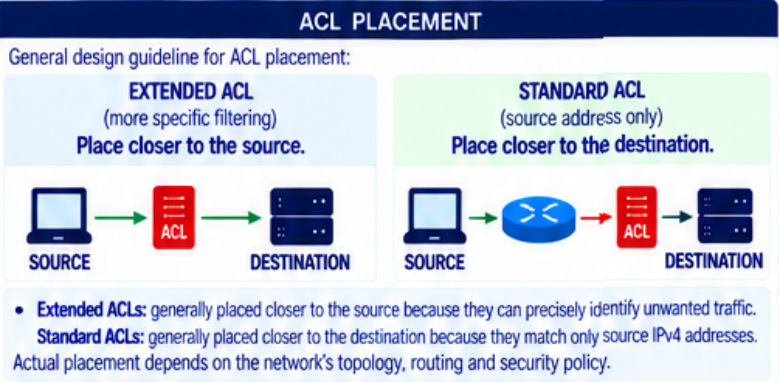
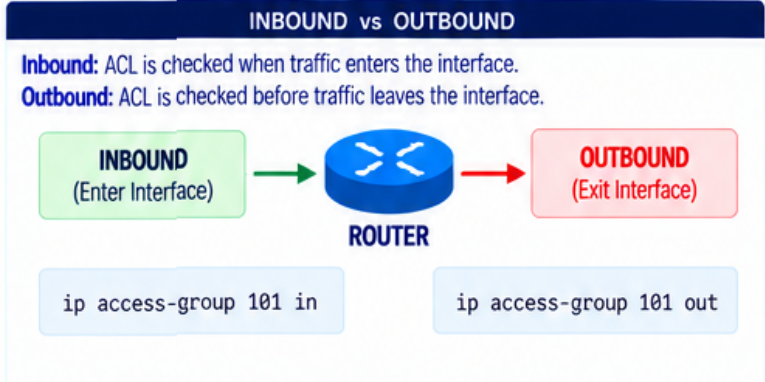
Prefix	Wildcard Mask	Example
/24	0.0.0.255	192.168.10.0
/25	0.0.0.127	0.0.0.255
/26	0.0.0.63	
/27	0.0.0.31	
/30	0.0.0.3	192.168.10.0/24

USEFUL ACL KEYWORDS

Keyword	Meaning
permit	Allow Matching Traffic
deny	Block Matching Traffic
host	One Specific Host
any	Any IPv4 Address
eq	Match Port (e.g. eq 80)
tcp	TCP
udp	UDP
icmp	ICMP

Example

host 10.1.1.1 is equivalent to 10.1.1.1 0.0.0.0



ACL VERIFICATION

Useful Cisco IOS commands:

```
show access-lists
show ip access-lists
show ip interface GigabitEthernet0/1
```

Check the following:

- ACL entries (Permit / Deny)
- Match counters (hit counts)
- Interface and direction (in / out)
- Correct logic and order
- Traffic is allowed / blocking as expected

PERMIT ONE HOST

Goal: Allow only host 192.168.1.10 to access the network.



Any other host

ACL Command:

```
access-list 10 permit host 192.168.1.10
```

All other source addresses are implicitly denied.

PERMIT ONE NETWORK

Goal: Allow network 192.168.10.0/24 to access the destination.



ACL Command:

```
access-list 10 permit 192.168.10.0
0.0.0.255
```

PERMIT HTTPS TO A SERVER

Goal: Allow users from 192.168.1.0/24 to access HTTPS server 10.0.0.20.



ACL Command:

```
access-list 101 permit tcp
192.168.1.0 0.0.0.255
host 10.0.0.20 eq 443
```

PERMIT SSH TO A ROUTER

Goal: Allow only admin PC 192.168.1.50 to SSH to router 10.0.0.1.



ACL Command:

```
access-list 101 permit tcp
host 192.168.1.50
host 10.0.0.1 eq 22
```

PERMIT DNS QUERIES

Goal: Allow DNS queries from 192.168.10.0/24 to DNS server 10.0.0.53.



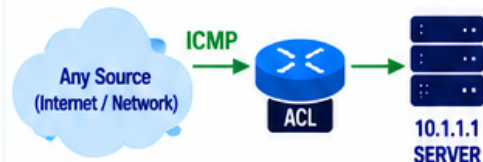
ACL Command:

```
access-list 101 permit udp
192.168.10.0 0.0.0.255
host 10.0.0.53 eq 53
```

This example permits UDP/53; DNS can also use TCP/53 in situations where TCP is required.

PERMIT ICMP TO A HOST

Goal: Allow ICMP traffic to server 10.1.1.1.

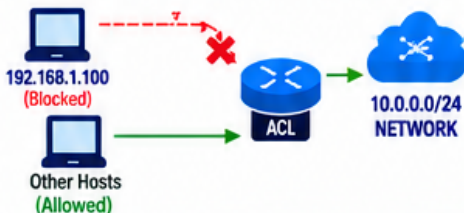


ACL Command:

```
access-list 101 permit icmp
any host 10.1.1.1
```

BLOCK ONE HOST

Goal: Block host 192.168.1.100, but allow other IPv4 sources to access the network.



ACL Command:

```
access-list 10 deny host 192.168.1.100
access-list 10 permit any
```

Order is critical because ACL processing stops at the first match.

BLOCK TELNET, PERMIT OTHER IP TRAFFIC

Goal: Block Telnet (TCP 23) from 192.168.1.0/24 to server 10.0.0.10, while permitting other IPv4 traffic.



ACL Command:

```
access-list 101 deny tcp
192.168.1.0 0.0.0.255 host 10.0.0.10 eq 23
access-list 101 permit ip any any
```

This final permit is necessary here because otherwise remaining traffic would hit the implicit deny.

ALLOW WEB, BLOCK EVERYTHING ELSE

Goal: Server 10.0.0.20 should receive only HTTP (80) and HTTPS (443) from any IPv4 source.



ACL Command:

```
access-list 101 permit tcp any host 10.0.0.20 eq 80
access-list 101 permit tcp any host 10.0.0.20 eq 443
```

All other unmatched traffic is denied by the implicit deny.

ACL PLACEMENT (REVIEW)

EXTENDED ACL

(match source, destination, protocol, port)
Place closer to the source.



- Extended ACLs: generally placed closer to the source because they can precisely identify unwanted traffic.
- Standard ACLs: generally placed closer to the destination because they match only source IPv4 addresses.
- Actual placement depends on the network's topology, routing and security policy.

STANDARD ACL

(match source address only)
Place closer to the destination.



IMPLICIT DENY (REVIEW)



Every ACL has an implicit deny at the end. Traffic that must be allowed needs to match a permit entry before reaching the implicit deny.

ACL TROUBLESHOOTING

- PACKET NOT WORKING?**
- CHECK ACL ORDER
 - CHECK SOURCE / DESTINATION
 - CHECK WILDCARD
 - CHECK PROTOCOL / PORT
 - CHECK INTERFACE
 - CHECK IN / OUT
 - CHECK COUNTERS

Useful commands:

```
show ip access-lists
show access-lists
show ip interface
```

Always verify and test ACL configurations in a lab environment before applying them to a production network.