



ACLs & Wildcard Masks

Use this when: you permit or deny traffic on a router or switch, or lock down who can SSH to it.

CCNA 200-301 · topic 5.6
Sheet v1.0 · Oct 2026

🔧 Wildcard masks and how an ACL decides

Wildcard = 255.255.255.255 minus the subnet mask

0 bit = must match

1 bit = ignore

One host	192.0.2.10 0.0.0.0	= host 192.0.2.10
/24	192.0.2.0 0.0.0.255	192.0.2.0 to .255
/26	192.0.2.64 0.0.0.63	192.0.2.64 to .127
Everything	0.0.0.0 255.255.255.255	= any

PER PACKET

- 1 Check lines top to bottom
- 2 First match wins; stop there
- 3 No match? Hidden **deny any** at the end

🔧 Standard vs extended

	STANDARD	EXTENDED
Numbers	1-99, 1300-1999	100-199, 2000-2699
Matches	Source IP only	Protocol, source, dest, ports
Place it	Near the destination	Near the source
Named	ip access-list standard extended NAME	

🔧 Rules of thumb

One per	Interface, direction, protocol
in / out	In = before routing; out = after
Order	Specific lines above general ones
Ports	eq gt lt neq range

🔧 Extended, named

```
ip access-list extended WEB-IN
remark HTTPS to the web server
10 permit tcp any host 192.0.2.10 eq 443
20 permit tcp 198.51.100.0 0.0.0.255 host 192.0.2.10 eq 22
30 deny ip any any log
interface g0/1
ip access-group WEB-IN in
```

Sequence numbers let you insert (**15 permit ...**) or delete (**no 20**).

🔧 Lock down SSH

```
access-list 10 permit host 198.51.100.5
line vty 0 15
access-class 10 in
transport input ssh
```

Only the admin PC can SSH in. On lines, use a numbered standard ACL with **access-class**, not **access-group**.

🔧 Check it

show access-lists	Lines and hit counts
show ip interface g0/1	Which ACL is applied, which way
show run section access-list	The config
clear access-list counters	Reset hit counts
deny ip any any log	See what the hidden deny drops

🔧 Don't lock yourself out

⚠️ **DANGER** A new ACL on your management path can cut you off. Permit your admin subnet first, and set **reload in 10** as a safety net.

⚠️ **CAUTION** An ACL with only **deny** lines blocks everything.

⚠️ **CAUTION** An outbound ACL does not filter traffic the router itself sends.



• /27 mask .224 = wildcard .31

• First match wins

• Hidden **deny any** at the end