Achievable

CCNA DUMP SHEET

Access control lists

Standard vs extended

	Standard	Extended
Matches	Source IP only	Source and destination IP, protocol, TCP/UDP ports
Numbers	1-99, 1300-1999	100-199, 2000-2699
Place	Closest to the destination	Closest to the source
Why	It sees only the source	Saves bandwidth

How a router reads an ACL

- **Top-down:** first match wins, then the router stops checking
- **Implicit deny:** hidden last line of every ACL, denies all IP
- **To pass the rest:** `permit any` or `permit ip any any`
- **Order:** specific entries first, catch-alls last
- **New entry:** added at the bottom. New number, new ACL

Wildcard masks

- **Bits:** 0 must match exactly, 1 is ignored
- **Find it:** 255.255.255.255 minus the subnet mask

Subnet mask	Wildcard	Matches
255.255.255.252	0.0.0.3	192.168.1.0 to .3
255.255.255.248	0.0.0.7	192.168.1.8 to .15
255.255.255.192	0.0.0.63	192.168.1.64 to .127
255.255.255.0	0.0.0.255	192.168.1.0 to .255
255.255.252.0	0.0.3.255	192.168.0.0 to 192.168.3.255
255.255.0.0	0.0.255.255	10.1.0.0 to 10.1.255.255

- `host 192.168.1.100` is `192.168.1.100 0.0.0.0`
- `any` is `0.0.0.0 255.255.255.255`
- **Standard ACL, mask left off:** 0.0.0.0 is assumed

Extended ACL: only SMTP from 192.168.1.2 to the mail server

`R1(config)# access-list 100 permit tcp host 192.168.1.2 host 172.16.1.100 eq 25`	Every field must match. Specific first
`R1(config)# access-list 100 deny ip 192.168.1.0 0.0.0.255 host 172.16.1.100`	The rest of the LAN to the server
`R1(config)# access-list 100 permit ip any any`	Negates the implicit deny
`R1(config)# interface g0/0`	The router port nearest the source
`R1(config-if)# ip access-group 100 in`	Checked as packets enter

- **Port:** `eq` after the address it belongs to. Blank means any
- **Source port:** usually blank, since clients pick it at random
- **Protocol:** `ip` is all, with no ports. Also `tcp`, `udp`, `icmp`
- **Aliases:** `www` is 80, `telnet` is 23. Config shows 25 as `smtp`

Standard ACL: deny one LAN, pass the rest

```
R2(config)# access-list 1 deny 192.168.1.0 0.0.0.255
R2(config)# access-list 1 permit any
R2(config)# interface g0/0
R2(config-if)# ip access-group 1 out
```

The same ACL, named

```
R2(config)# ip access-list standard BLOCK_192
R2(config-std-nacl)# deny 192.168.1.0 0.0.0.255
R2(config-std-nacl)# permit any
R2(config-std-nacl)# interface g0/0
R2(config-if)# ip access-group BLOCK_192 out
```

- **Extended:** `ip access-list extended PERMIT_WEB`

Applying an ACL

- **Direction:** `in` as packets enter, `out` before they leave
- **One ACL per interface, per direction:** a second replaces it
- **Trap:** `ip access-group` applies, `ip access-list` creates

Editing with sequence numbers

```
R2(config)# ip access-list standard BLOCK_192
R2(config-std-nacl)# 5 permit host 192.168.1.100
```

- **Numbering:** IOS counts by 10, so 5 lands above 10
- **Already applied:** nothing to reapply after an edit
- **Delete a line:** `no 10` in the same mode
- **Numbered ACL:** same, under `ip access-list standard 1`
- **Trap:** `no access-list 1 deny ...` deletes the whole ACL

Verify

Command	What it does
`show access-lists`	Entries, numbers, hit counts
`show ip interface g0/0`	Inbound and outgoing ACLs
`show running-config`	`ip access-group` on the interface