

ACL CheatSheet – Kompakt

Standard und Extended Access Control Lists | CISCO Router

Übersicht

Merkmal	Standard	Extended
Nummernbereich	1-99, 1300-1399	100-199, 2000-2699
Filter	Quell-IP	Quelle, Ziel, Protokoll, Port
Position	Entfernt oder Interface-nah	Quelle-nah

Standard ACL (Numbered)

Syntax

```
access-list <nummer> [permit | deny] <quell-ip> [wildcard-maske]
```

Beispiel

```
access-list 10 permit 192.168.1.0 0.0.0.255
access-list 10 deny any
```

Interface-Anwendung

```
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip access-group 10 in
```

Extended ACL (Numbered)

Syntax

```
access-list <nummer> [permit | deny] <protokoll> <quelle> <quelle-wc>
<ziel> <ziel-wc> [operatoren]
```

Beispiel

```
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 443
access-list 100 deny ip any any
```

Interface-Anwendung

```
Router(config)# interface Serial 0/0
Router(config-if)# ip access-group 100 out
```

Standard Named ACL

Syntax

```
Router(config)# ip access-list standard <name>
Router(config-std-nacl)# [permit | deny] <quell-ip> [wildcard-maske]
Router(config-std-nacl)# exit
```

Beispiel

```
Router(config)# ip access-list standard ALLOW_ADMIN
Router(config-std-nacl)# permit host 192.168.1.1
Router(config-std-nacl)# deny any
Router(config-std-nacl)# exit
Router(config)# interface FastEthernet 0/1
Router(config-if)# ip access-group ALLOW_ADMIN in
```

Extended Named ACL

Syntax

```
Router(config)# ip access-list extended <name>
Router(config-ext-nacl)# [permit | deny] <protokoll> <quelle> <quelle-wc>
<ziel> <ziel-wc> [operatoren]
Router(config-ext-nacl)# exit
```

Beispiel

```
Router(config)# ip access-list extended WEB_TRAFFIC
Router(config-ext-nacl)# permit tcp any 10.0.0.0 0.0.0.255 eq 80
Router(config-ext-nacl)# permit tcp any 10.0.0.0 0.0.0.255 eq 443
Router(config-ext-nacl)# deny ip any any
Router(config-ext-nacl)# exit
```

Wildcard Masking

Grundprinzip: 0 = Bit vergleichen | 1 = Bit ignorieren

Wildcard	Bedeutung
0.0.0.0	Genau diese IP (host)
0.0.0.255	/24 Subnetz
0.0.255.255	/16 Subnetz
255.255.255.255	Alle (any)

Protokolle & Ports

Protokolle

- `ip` – Alle IP-Protokolle
- `tcp` – Transmission Control Protocol
- `udp` – User Datagram Protocol
- `icmp` – Internet Control Message Protocol

Häufige Ports

Service	Port	Service	Port
HTTP	80	DNS	53
HTTPS	443	DHCP	67,68
SSH	22	NTP	123
Telnet	23	SNMP	161,162
SMTP	25		

Operatoren & Schlüsselwörter

Operator	Bedeutung	Beispiel
<code>eq</code>	equal (gleich)	<code>eq 80</code>
<code>neq</code>	not equal	<code>neq 22</code>
<code>gt</code>	greater than	<code>gt 1023</code>
<code>lt</code>	less than	<code>lt 1024</code>
<code>range</code>	Bereich	<code>range 1000 2000</code>
<code>established</code>	Rückantworten	Stateful filtering
<code>host</code>	Einzelne IP	<code>host 192.168.1.1</code>
<code>any</code>	Alle Adressen	Wildcard 255.255.255.255

Verwaltung & Debugging

ACLs anzeigen

```
Router# show access-lists
Router# show access-lists 100
Router# show ip access-lists
```

ACLs löschen

```
Router(config)# no access-list 100
Router(config)# ip access-list extended WEB_TRAFFIC
Router(config-ext-nacl)# no 5
```

Interface-Anwendung prüfen

```
Router# show ip interface <interface> | include access list
```

Wichtige Regeln

- **First-Match-Prinzip:** Erste zutreffende Regel wird angewendet
- **Implizites Deny:** Ohne explizite Erlaubnis = verweigert
- **Spezifisch vor Allgemein:** Spezifische Regeln vorne positionieren
- **Inbound vs. Outbound:** Richtige Richtung beachten (in/out)
- **Wildcard invers:** Wildcard ≠ Subnetzmaske (invertiert!)