

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