

# Routerkonfiguration Access Control Lists (ACLs)

## 1) ACL erstellen (specific -> general)

### Nummerierte Standard-ACL (nahe am Ziel, Nummer: 1-99)

```
ROUTER(config)# access-list NUMBER permit|deny QUELL-IP
ROUTER(config)# access-list NUMBER permit|deny QUELL-IP
```

### Nummerierte Extended-ACL (nahe an Quelle, Nummer: 100-199)

```
ROUTER(config)# access-list NUMBER permit|deny ERWEITERTE KRITERIEN
ROUTER(config)# access-list NUMBER permit|deny ERWEITERTE KRITERIEN
```

### Named Standard-ACL (nahe am Ziel)

```
ROUTER(config)# ip access-list standard NAME
ROUTER(config-std-nacl)# permit|deny QUELL-IP
ROUTER(config-std-nacl)# permit|deny QUELL-IP
```

### Named Extended-ACL (nahe an Quelle)

```
ROUTER(config)# ip access-list extended NAME
ROUTER(config-ext-nacl)# permit|deny ERWEITERTE KRITERIEN
ROUTER(config-ext-nacl)# permit|deny ERWEITERTE KRITERIEN
```

ERWEITERTE KRITERIEN					
<b>ip</b>	QUELL-IP	ZIEL-IP			
<b>icmp</b>	QUELL-IP	ZIEL-IP	[ICMP-TYP]		
<b>tcp</b>	QUELL-IP	[QUELL-PORT]	ZIEL-IP	[ZIEL-PORT]	[established]
<b>udp</b>	QUELL-IP	[QUELL-PORT]	ZIEL-IP	[ZIEL-PORT]	

QUELL-IP, ZIEL-IP		
einzelne IP-Adresse	<b>host</b>	192.168.0.1
mehrere IP-Adressen	IP	192.168.0.1
	WILDCARD	0.0.0.255
alle IP-Adressen	<b>any</b>	0.0.0.0 255.255.255.255

ICMP-TYP
0 - 255
<b>echo</b>
<b>echo-reply</b>
<b>host-unreachable</b>
<b>net-unreachable</b>
<b>port-unreachable</b>
<b>protocol-unreachable</b>
<b>ttl-exceeded</b>
<b>unreachable</b>

QUELL-PORT, ZIEL-PORT	
	0 - 65535
	<b>ftp</b> (21)
	<b>pop3</b> (110)
	<b>smtp</b> (25)
	<b>telnet</b> (23)
	<b>www</b> (80)
<b>eq</b> (==)	
<b>gt</b> (>)	
<b>lt</b> (<)	
<b>neq</b> (!=)	
	<b>bootpc</b> (68)
	<b>bootps</b> (67)
	<b>domain</b> (53)
	<b>snmp</b> (161)
	<b>tftp</b> (69)
<b>range</b> 20 100	

## 2) ACL positionieren

```
ROUTER(config-if)# ip access-group NUMBER in|out
ROUTER(config-if)# ip access-group NAME in|out
```

## 3) Diagnose

```
ROUTER# show access-lists
ROUTER# show ip interface Serial 0
ROUTER# show running-config
```

# Telnetzugriff auf Router einschränken

## 1) Standard-ACL erstellen

```
ROUTER(config)# access-list NUMBER permit|deny QUELL-IP
```

## 2) ACL positionieren

```
ROUTER(config)# line vty 0 4
ROUTER(config-line)# password XXX
ROUTER(config-line)# login
ROUTER(config-line)# access-class NUMBER in
```