Routerkonfiguration Access Control Lists (ACLs)

1) ACL erstellen (specific -> general)

Nummerierte Standard-ACL (nahe am Ziel, Nummer: 1-99, 1300-1999)

```
ROUTER(config)# access-list  NUMMER  remark  KOMMENTAR ZUM ABSCHNITT
ROUTER(config)# access-list  NUMMER  permit|deny  QUELL-IP
ROUTER(config)# access-list  NUMMER  permit|deny  QUELL-IP
```

Nummerierte Extended-ACL (nahe an Quelle, Nummer: 100-199, 2000-2699)

```
ROUTER(config)# access-list  NUMMER  remark  KOMMENTAR ZUM ABSCHNITT
ROUTER(config)# access-list  NUMMER  permit|deny  ERWEITERTE KRITERIEN
ROUTER(config)# access-list  NUMMER  permit|deny  ERWEITERTE KRITERIEN
```

Named Standard-ACL (nahe am Ziel)

```
ROUTER(config)# ip access-list standard  NAME
ROUTER(config-std-nacl)# remark  KOMMENTAR ZUM ABSCHNITT
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)# remark  KOMMENTAR ZUM ABSCHNITT
ROUTER(config-ext-nacl)# permit|deny  ERWEITERTE KRITERIEN
ROUTER(config-ext-nacl)# permit|deny  ERWEITERTE KRITERIEN
```

IPv6-ACL

```
ROUTER(config)# ipv6 access-list  NAME
ROUTER(config-ipv6-acl)# remark  KOMMENTAR ZUM ABSCHNITT
ROUTER(config-ipv6-acl)# permit|deny  ERWEITERTE KRITERIEN
ROUTER(config-ipv6-acl)# permit|deny  ERWEITERTE KRITERIEN
```

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

ERWEITERTE KRITERIEN					
ip	QUELL-IP	ZIEL-IP			
ipv6	QUELL-IP	ZIEL-IP			
icmp	QUELL-IP	ZIEL-IP	[ICMP-TYP]		
tcp	QUELL-IP	[QUELL-PORT]	ZIEL-IP	[ZIEL-PORT]	[**established**]
udp	QUELL-IP	[QUELL-PORT]	ZIEL-IP	[ZIEL-PORT]	

QUELL-IP, ZIEL-IP	
einzelne IP-Adresse	**host** 192.168.0.1 **host** 3000::1
mehrere IP-Adressen	IP WILDCARD 192.168.0.1 0.0.0.255 IPv6/SM 3000::1/64
alle IP-Adressen	**any**

ICMP-TYP	
ICMP	**ICMPv6**
0 - 255	
echo	**echo-request**
echo-reply	**echo-reply**
host-unreachable	**destination-unreachable**
net-unreachable	
port-unreachable	**port-unreachable**
protocol-unreachable	
ttl-exceeded	**time-exceeded**
unreachable	**unreachable**
	nd-ns
	nd-na

2) ACL positionieren

```
ROUTER(config-if)# ip access-group NUMMER in|out
ROUTER(config-if)# ip access-group NAME in|out
ROUTER(config-if)# ipv6 traffic-filter NAME in|out
```

3) Diagnose

```
ROUTER# show access-lists
ROUTER# clear access-list counters
ROUTER# show ipv6 access-list
ROUTER# show ip interface Serial 0
ROUTER# show running-config
```

Telnet- bzw. SSH-Zugriff auf Router einschränken

1) Standard-ACL bzw. IPv6-ACL erstellen

```
ROUTER(config)# ip access-list standard  NAME4
ROUTER(config-std-nacl)# permit|deny  QUELL-IP
ROUTER(config-std-nacl)# permit|deny  QUELL-IP

ROUTER(config)# ipv6 access-list  NAME6
ROUTER(config-ipv6-acl)# permit|deny  ipv6  QUELL-IP   any
ROUTER(config-ipv6-acl)# permit|deny  ipv6  QUELL-IP   any
```

2) ACL positionieren

```
ROUTER(config)# line vty 0 4
ROUTER(config-line)# password XXX
ROUTER(config-line)# login
ROUTER(config-line)# access-class NAME4 in
ROUTER(config-line)# ipv6 access-class NAME6 in
```