Rev. 20180926.151011

(ICND1) 26(C). ACL T-Shooting
(ICND2) 17(C). ACL T-Shooting

ccnacookbook.com

ACL BEST PRACTICES

Put more specific lines (exceptions to broader rules) earlier in an ACL, since IOS will act on the first match it sees.

Before modifying an ACL, remove it from any interfaces ("access-group" command). Routers are a dynamic environment and will process packets based on a partial config. On current versions, IOS won't filter any packets if you blow away an ACL while it's still invoked on an interface. In old versions, it would still enforce the implicit "deny all," effectively killing the interface.

ACL TROUBLESHOOTING

ACLs complicate everyday troubleshooting simply by their presence. The most important thing to remember is that an extended ACL will almost certainly treat pings differently than data because they are different protocols and require separate (additional) lines in the ACL.

Some problems you might see on an exam:

Problem / Symptom	Diagnosis
Wrong order on ACL statements	
Source & Destination addresses reversed	
Source & Destination ports reversed	
Extended Syntax (need TCP or UDP to check ports)	
Trying to use TCP, or UDP to control pings (they use the ICMP protocol)	
Packets being silently killed by the implicit "deny any" at the end of the ACL. This could kill a routing protocol's relationship with its neighbors.	Put an explicit "deny any" at end so the counters will show that it's being triggered
Location—standard ACLs too close to the source can cast a "shadow" over legitimate recipients.	

Finding Interfaces with ACLs & Direction

```
R> show ip interface fa0/0
```

Displays outgoing and inbound ACLs on an interface

```
R# show run | begin interface
```

Look for "access-group" on interfaces

Finding ACL Definitions & Hit Counters—check if the line you want is incrementing. If not, maybe an earlier line is denying (and incrementing).

```
R# show [ip] access-lists [ <name> | <number> ]
```

Look for the match counters

```
R# show run | begin access-list
```

Bonus: Clearing Hit Counters—You can reset the hit counters (the "match" numbers in parentheses) for a single ACL or all ACLs. Unfortunately, there is no way to clear only one line of one ACL without editing the ACL to remove that line and then put it back in.

```
R# clear [ip] access-list counters [ <name> | <number> ]
```

Curiously, "access-list" is singular in this command and plural in the "show" command

If you omit the "ip" keyword, this command can also clear IPv6 or other kinds of access-list

Determining Address Range matched by ACL Statement—If the ACL is on the router, the address is the low end of the range (IOS automatically normalizes the address to make this true). Find the high end of the range by adding the wildcard to it.

Remember (this is the third mention in two chapters) that routing protocol update messages can be killed by an inbound ACL even thought the outbound updates are unaffected because their source is internal to the router, making them immune to outbound ACLs. Making you a neighbor to another router and them not on your neighbor list. Maybe the updates are just passing though, having come in an interface that didn't have an inbound ACL blocking them. This is especially insidious because of the implicit "deny all" at the end of each ACL. If you didn't explicitly allow routing updates (or allow all) on an input, you actually just mangled your routing protocol in a way that's hard to track down.

```
permit udp any any eq 520
```

RIP v2

```
permit eigrp any any
permit ospf any any
```

Serial Point-to-Point Pings—if you ping the address of your own serial interface, the ping will actually go out the interface (because routers are optimized for routing, not considering whether an internally-generated packet is actually for themselves). The router at the other end will correctly interpret the destination address with its routing table and send the packet back again. The same thing happens again in reverse for the ping response. The round-trip time shown will actually be double the true round-trip time.

Ethernet Self-Pings—these don't actually go out the interface, but the inbound ACL on that interface is still applied, so it must allow ICMP. Of course, the interface must be up/up, also.