

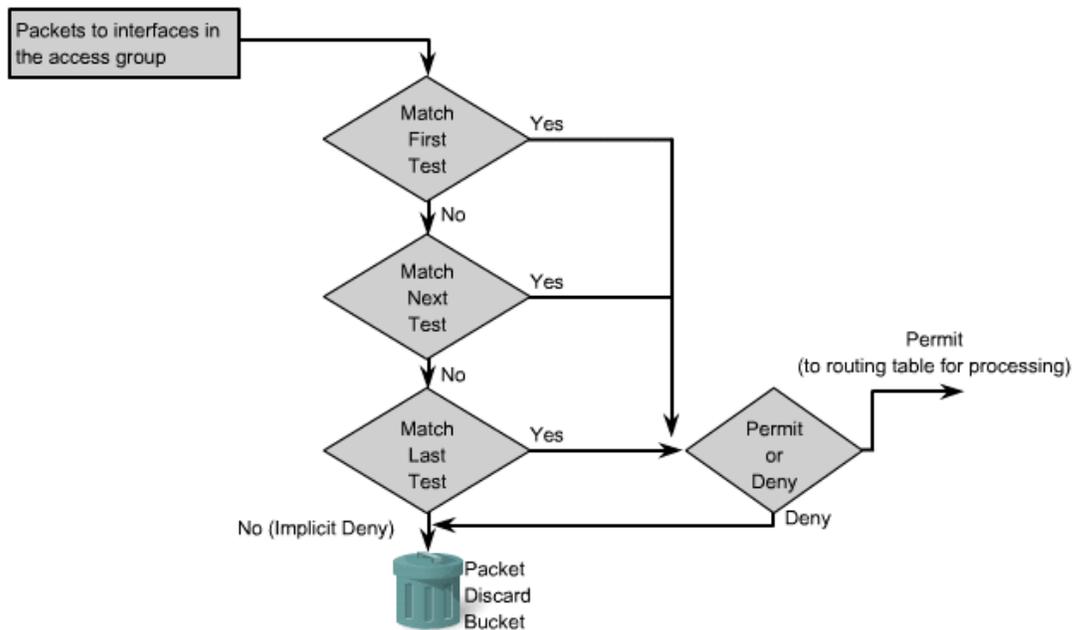
ACL Placement

Table of Contents

Inbound ACL Operation Flow.....	2
Outbound ACL Operation Flow.....	3
ACL Placement	5
Where to place a Standard ACL?	7
Where to place a Extended ACL?.....	8

Inbound ACL Operation Flow

Inbound ACL Operation Flow



© 2012 Cisco and/or its affiliates. All rights reserved.

20

**020 ACL Placement. Packet interfaces, right? Checks the first line, checks the second line, keeps going until it matches or hits the bit bucket. If it matches, then it goes to routing table for processing. So this is what? This is an inbound access list. Inbound access list goes through here first, and then get route processed. Why would that be true?

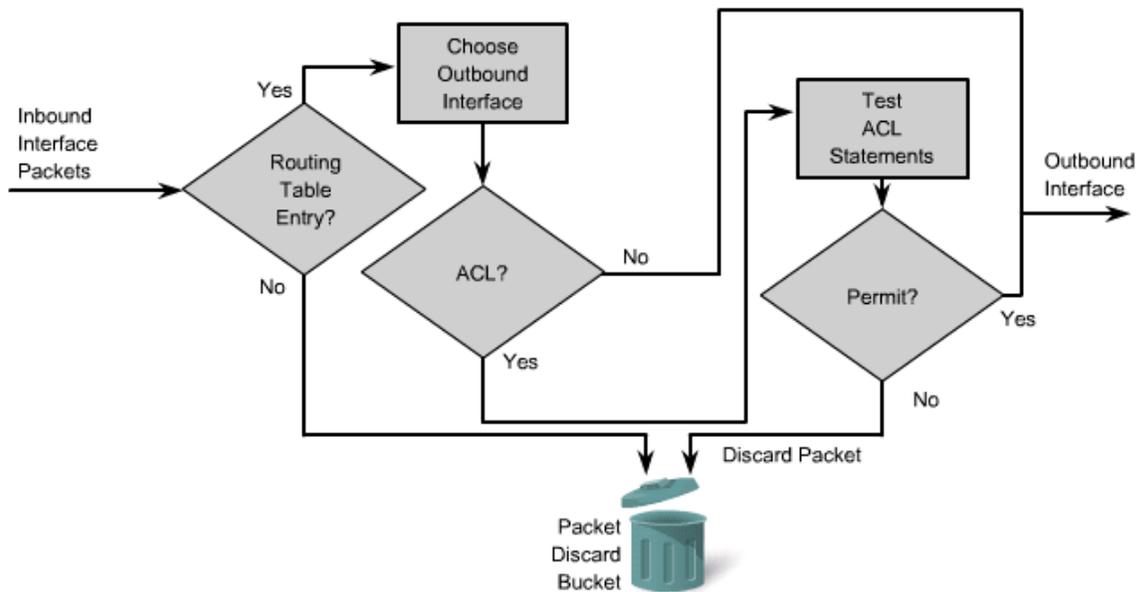
Student: Because the ACL is set up before goes into the buffer.

Instructor: Correct. Because the point they make at that point is why execute this if you're not going to--

I'm sorry. Why execute the routing if you're going to drop the packet afterward? If you're going to drop it anyway, let's just drop it based on the ACL and never bother the route process. On the other side, if it's outbound, what happens?

Outbound ACL Operation Flow

Outbound ACL Operation Flow



© 2012 Cisco and/or its affiliates. All rights reserved.

21

**021 Student: Has to get routed first.

Instructor: Yep. And there the question's kind of two-prong. Half of that question is some of them aren't going to route, and if they don't route they get dropped by themselves so they don't have to be

evaluated. The other part of it is, what's the routing going to do? Until you route it, you don't know which interface it's going out. You know which one it came in on, but depending on the route it could go out any number of exit interfaces, correct? Because the ACLs are applied per interface, you can't screen it until after knowing which interface it's going out on. Yes?

Student: Can I assume it'll do any kind of NAT translations after the ACLs? So otherwise it's going to change the inbound or change the source board, if it's on the NAT table.

Instructor: It does. The access list first and then the NAT.

Student: Yeah.

Instructor: Because that way, the logic behind that is, that way no matter what interface you put it on, the source hasn't changed, so--

Student: Until the last possible second.

Instructor: Right. So the list is still accurate.

Student: And the next routing source will be that router.

Instructor: Correct. But your router doesn't see the next router, so it doesn't matter. It's the next router's problem to know what the address is coming in.

ACL Placement

- Standard ACL placement:
 - Standard ACLs are placed **as close to the destination as possible**.
 - Standard ACLs filter packets based on the source address only so placing these ACLs too close to the source can adversely affect packets by denying all traffic, including valid traffic.
- Extended ACL placement:
 - Extended ACLs are placed on routers **as close to the source as possible** that is being filtered.
 - Placing Extended ACLs too far from the source is inefficient use of network resources because packets can be sent a long way only to be dropped or denied.



© 2012 Cisco and/or its affiliates. All rights reserved.

22

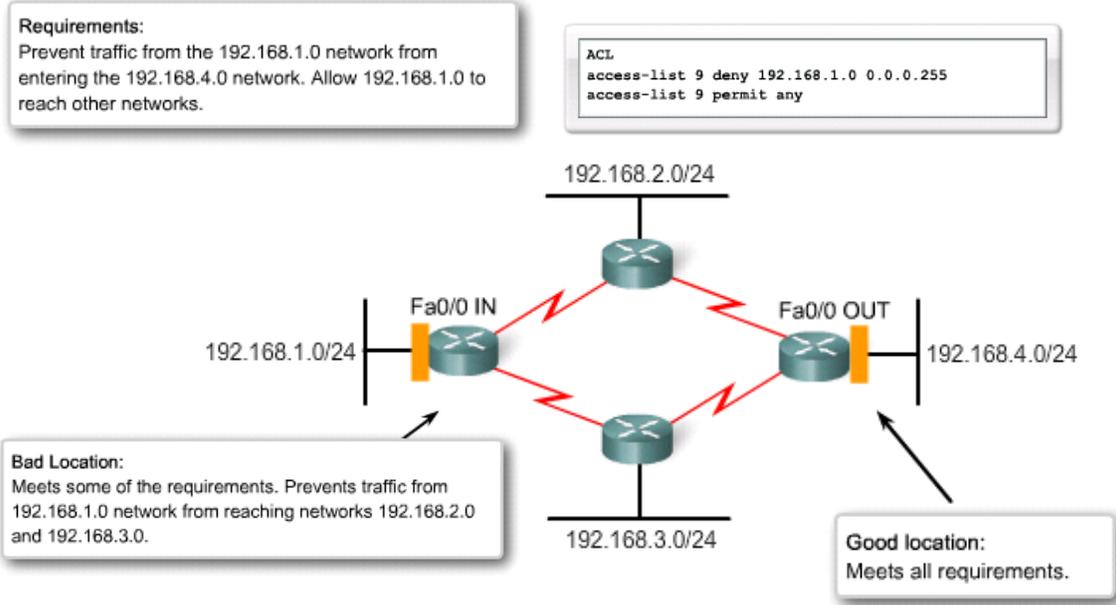
**022 Generally speaking, standard ACL's place is close to the destination as possible. What's the reason we talked about? If you put it close to the source, it's going to block everything. If it's a deny statement, in the example we used today, if I wanted to block it from going to the internet and I put it right next to the host, then it blocks it from doing anything. Can't even go on the router. So the way to allow it to talk to other machines locally but not hit the internet is to block it at the exit interface toward the internet.

Extended ACLs generally as close to the source as possible. And the idea

behind that one is because you can specify all the parameters for that packet, the source, the destination and all the ports, you know when it leaves if it's going to get blocked or not. So why take it through the routing process or other processes if you're going to drop it anyway? You don't have to worry about it putting an extended access list on and dropping all connectivity to the device because you're making a more granular definition of what you're going to keep and what you're going to drop. So you can put it as close to the device as possible and just drop it early in the process as you can.

Where to place a Standard ACL?

Where to place a Standard ACL?



© 2012 Cisco and/or its affiliates. All rights reserved.

23

**023 So here's the standard ACL.
Close to the edge, not close to the source. Because source is a bad location. It'll block 192.168.1.0 from going anywhere.

Where to place a Extended ACL?

Where to place a Extended ACL?

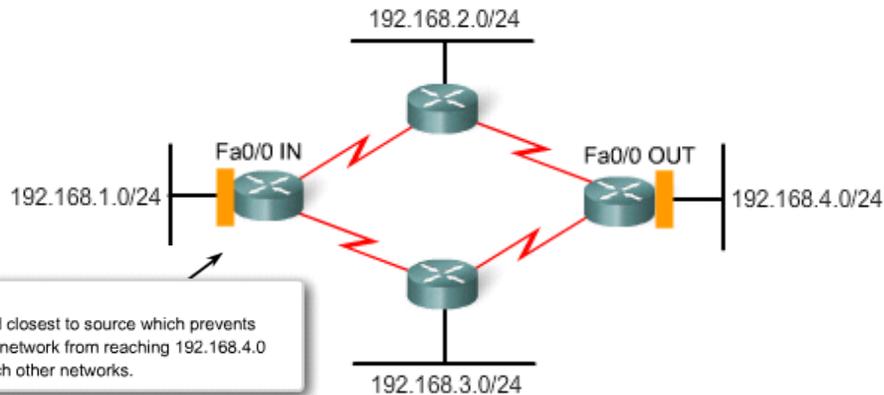
Requirements:

Use Extended ACL to prevent traffic from the 192.168.1.0 network from entering the 192.168.4.0 network but allow it to reach other networks.

```
ACL
access-list 109 deny ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
access-list 109 permit ip any any
```

Good location:

Extended ACL is placed closest to source which prevents traffic from 192.168.1.0 network from reaching 192.168.4.0 but also allows it to reach other networks.



© 2012 Cisco and/or its affiliates. All rights reserved.

24

**024 Extended ACL. Close to the source, because it's only going to block packets that meet all the requirements. So you don't have to wait until later to see where it's going to end up. You already know where it's going to end up. If it doesn't meet, then you should drop. And if you're going to drop it, why not drop it before it gets processed.