Guidelines for ACL Creation

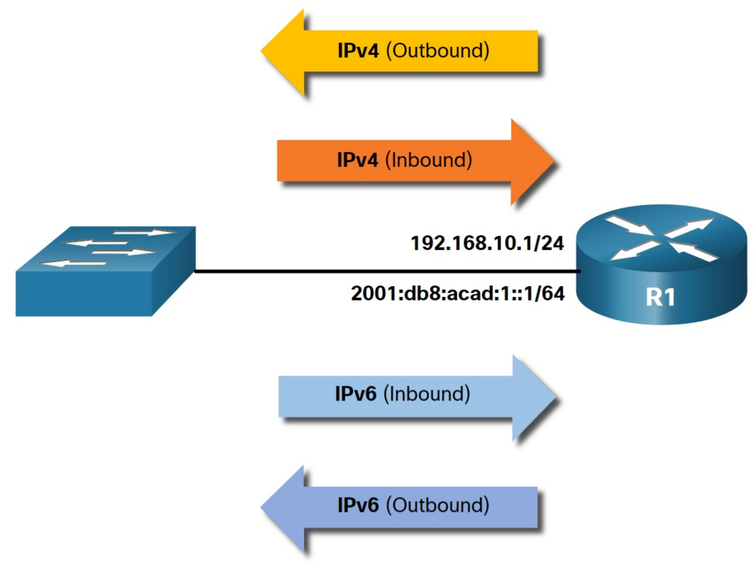
4.3.1

Limited Number of ACLs per Interface

In a previous topic, you learned about how wildcard masks are used in ACLs. This topic will focus on the guidelines for ACL creation. There is a limit on the number of ACLs that can be applied on a router interface. For example, a dual-stacked (i.e., IPv4 and IPv6) router interface can have up to four ACLs applied, as shown in the figure.

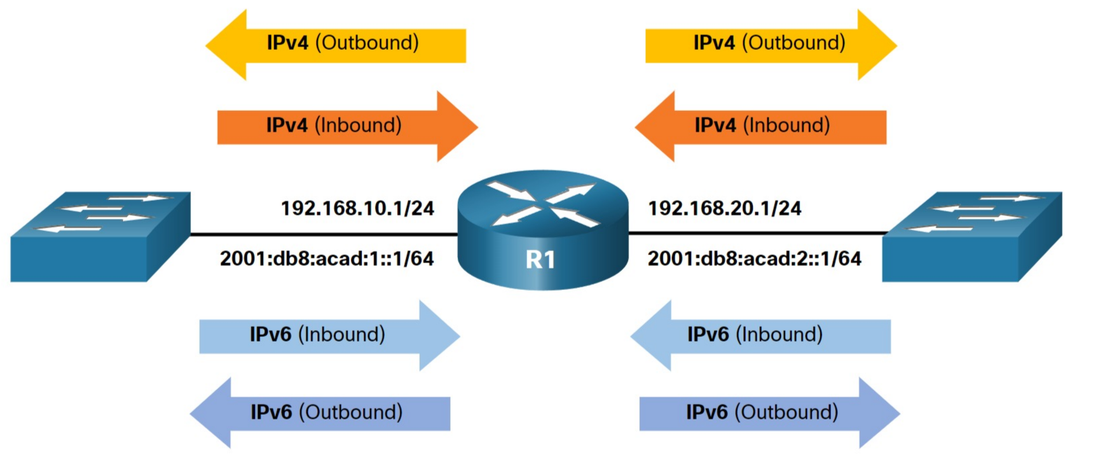
Specifically, a router interface can have:

- one outbound IPv4 ACL
- one inbound IPv4 ACL
- one inbound IPv6 ACL
- one outbound IPv6 ACL



Assume R1 has two dual-stacked interfaces that require inbound and outbound IPv4 and IPv6 ACLs applied. As shown in the figure, R1 could have up to 8 ACLs configured and applied to interfaces. Each interface would have four ACLs; two ACLs for IPv4 and two ACLs for IPv6. For each protocol, one ACL is for inbound traffic and one for outbound traffic.

Note: ACLs do not have to be configured in both directions. The number of ACLs and their direction applied to the interface will depend on the security policy of the organization.



4.3.2

ACL Best Practices

Using ACLs requires attention to detail and great care. Mistakes can be costly in terms of downtime, troubleshooting efforts, and poor network service. Basic planning is required before configuring an ACL.

The table presents guidelines that form the basis of an ACL best practices list.

Guideline	Benefit
Base ACLs on the organizational security policies.	This will ensure you implement organizational security guidelines.
Write out what you want the ACL to do.	This will help you avoid inadvertently creating potential access problems.
Use a text editor to create, edit, and save all of your ACLs.	This will help you create a library of reusable ACLs.
Document the ACLs using the **remark** command.	This will help you (and others) understand the purpose of an ACE.
Test the ACLs on a development network before implementing them on a production network.	This will help you avoid costly errors.

4.3.3

Check Your Understanding - Guidelines for ACL Creation

Check your understanding of ACL creation by choosing the BEST answer to the following questions.

1. How many total ACLs (both IPv4 and IPv6) can be configured on an interface?

- 0
- 1
- 2
- 4
- 8

2. Which of the following is an ACL best practice?

- Always test ACLs on a production network.
- Create your ACLs on a production router.
- Document the ACLs using the **description** ACL command.
- Write the ACL before configuring it on a router.

Check

Show Me

Reset