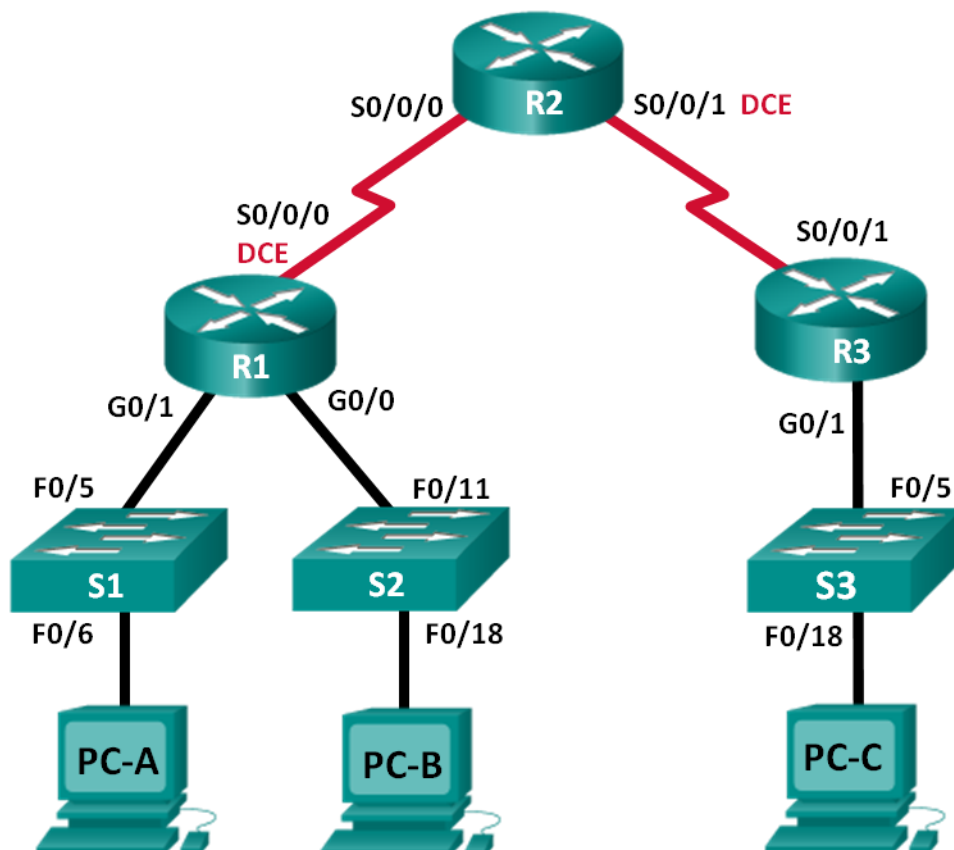


Lab – Configuring and Verifying IPv6 ACLs

Topology



Addressing Table

Device	Interface	IP Address	Default Gateway
R1	G0/0	2001:DB8:ACAD:B::1/64	N/A
	G0/1	2001:DB8:ACAD:A::1/64	N/A
	S0/0/0 (DCE)	2001:DB8:AAAA:1::1/64	N/A
R2	S0/0/0	2001:DB8:AAAA:1::2/64	N/A
	S0/0/1 (DCE)	2001:DB8:AAAA:2::2/64	N/A
R3	G0/1	2001:DB8:CAFE:C::1/64	N/A
	S0/0/1	2001:DB8:AAAA:2::1/64	N/A
S1	VLAN1	2001:DB8:ACAD:A::A/64	N/A
S2	VLAN1	2001:DB8:ACAD:B::A/64	N/A
S3	VLAN1	2001:DB8:CAFE:C::A/64	N/A
PC-A	NIC	2001:DB8:ACAD:A::3/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::3/64	FE80::1
PC-C	NIC	2001:DB8:CAFE:C::3/64	FE80::1

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Devices and Verify Connectivity

Part 3: Configure and Verify IPv6 ACLs

Part 4: Edit IPv6 ACLs

Background / Scenario

You can filter IPv6 traffic by creating IPv6 access control lists (ACLs) and applying them to interfaces similarly to the way that you create IPv4 named ACLs. IPv6 ACL types are extended and named. Standard and numbered ACLs are no longer used with IPv6. To apply an IPv6 ACL to a vty interface, you use the new **ipv6 access-class** command. The **ipv6 traffic-filter** command is still used to apply an IPv6 ACL to interfaces.

In this lab, you will apply IPv6 filtering rules and then verify that they are restricting access as expected. You will also edit an IPv6 ACL and clear the match counters.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

The **default bias** template used by the Switch Database Manager (SDM) does not provide IPv6 address capabilities. Verify that SDM is using either the **dual-ipv4-and-ipv6** template or the **lanbase-routing** template. The new template will be used after reboot even if the configuration is not saved.

```
S1# show sdm prefer
```

Use the following commands to assign the **dual-ipv4-and-ipv6** template as the default SDM template.

```
S1# configure terminal
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Set Up the Topology and Initialize Devices

In Part 1, you set up the network topology and clear any configurations if necessary.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the routers and switches.

Part 2: Configure Devices and Verify Connectivity

In Part 2, you configure basic settings on the routers, switches and PCs. Refer to the Topology and Addressing Table at the beginning of this lab for device names and address information.

Step 1: Configure IPv6 addresses on all PCs.

Configure IPv6 global unicast addresses according to the Addressing Table. Use the link-local address of **FE80::1** for the default-gateway on all PCs.

Step 2: Configure the switches.

- Disable DNS lookup.
- Assign the hostname.
- Assign a domain-name of **ccna-lab.com**.
- Encrypt plain text passwords.
- Create a MOTD banner warning users that unauthorized access is prohibited.
- Create a local user database with a username of **admin** and password as **classadm**.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- Enable login on the VTY lines using the local database.
- Generate a crypto rsa key for ssh using a modulus size of 1024 bits.
- Change the transport input VTY lines to all for SSH and Telnet only.
- Assign an IPv6 address to VLAN 1 according to the Addressing Table.

- m. Administratively disable all inactive interfaces.

Step 3: Configure basic settings on all routers.

- a. Disable DNS lookup.
- b. Assign the hostname.
- c. Assign a domain-name of **ccna-lab.com**.
- d. Encrypt plain text passwords.
- e. Create a MOTD banner warning users that unauthorized access is prohibited.
- f. Create a local user database with a username of **admin** and password as **classadm**.
- g. Assign **class** as the privileged EXEC encrypted password.
- h. Assign **cisco** as the console password and enable login.
- i. Enable login on the VTY lines using the local database.
- j. Generate a crypto rsa key for ssh using a modulus size of 1024 bits.
- k. Change the transport input VTY lines to all for SSH and Telnet only.

Step 4: Configure IPv6 settings on R1.

- a. Configure the IPv6 unicast address on interface G0/0, G0/1, and S0/0/0.
- b. Configure the IPv6 link-local address on interface G0/0, G0/1, and S0/0/0. Use **FE80::1** for the link-local address on all three interfaces.
- c. Set the clock rate on S0/0/0 to 128000.
- d. Enable the interfaces.
- e. Enable IPv6 unicast routing.
- f. Configure an IPv6 default route to use interface S0/0/0.

```
R1(config)# ipv6 route ::/0 s0/0/0
```

Step 5: Configure IPv6 settings on R2.

- a. Configure the IPv6 unicast address on interface S0/0/0 and S0/0/1.
- b. Configure the IPv6 link-local address on interface S0/0/0 and S0/0/1. Use **FE80::2** for the link-local address on both interfaces.
- c. Set the clock rate on S0/0/1 to 128000.
- d. Enable the interfaces.
- e. Enable IPv6 unicast routing.
- f. Configure static IPv6 routes for traffic handling of R1 and R3 LAN subnets.

```
R2(config)# ipv6 route 2001:db8:acad::/48 s0/0/0
```

```
R2(config)# ipv6 route 2001:db8:cafe:c::/64 s0/0/1
```

Step 6: Configure IPv6 settings on R3.

- a. Configure the IPv6 unicast address on interface G0/1 and S0/0/1.
- b. Configure the IPv6 link-local address on interface G0/1 and S0/0/1. Use **FE80::1** for the link-local address on both interfaces.
- c. Enable the interfaces.

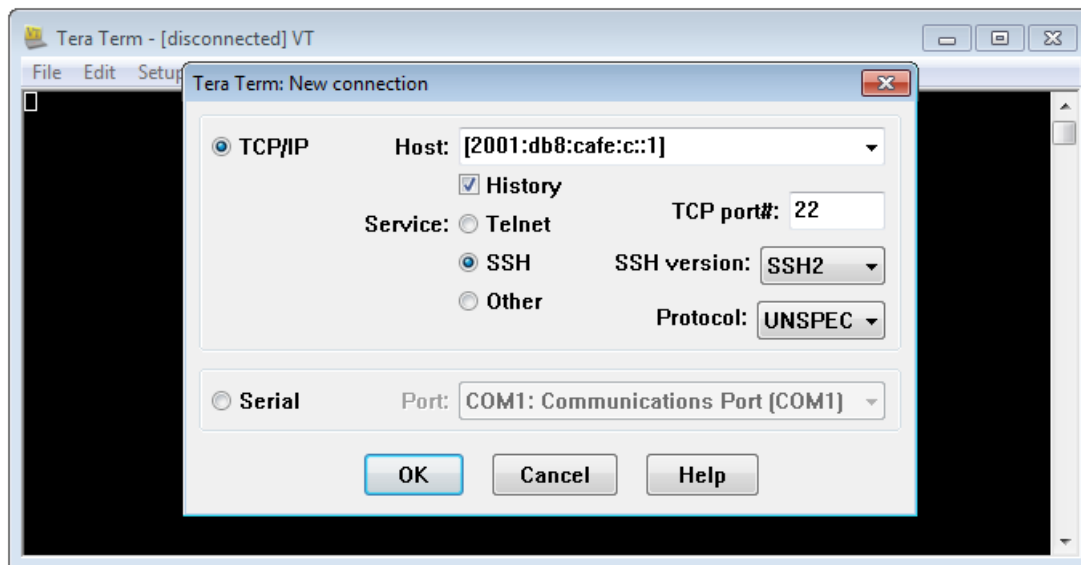
- d. Enable IPv6 unicast routing.
- e. Configure an IPv6 default route to use interface S0/0/1.

```
R3(config)# ipv6 route ::/0 s0/0/1
```

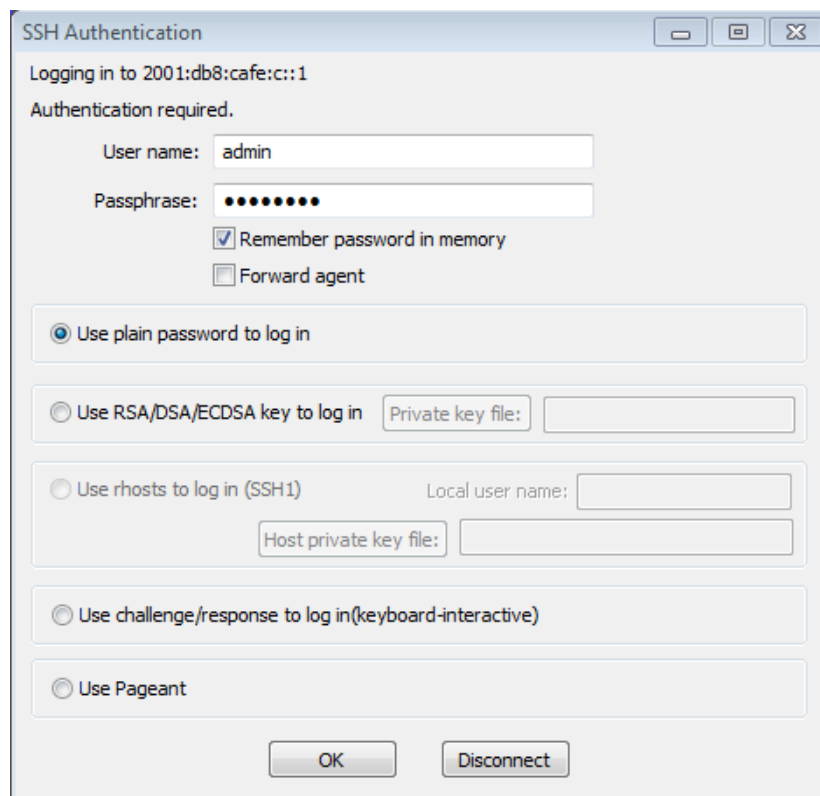
Step 7: Verify connectivity.

- a. Each PC should be able to ping the other PCs in the topology.
- b. Telnet to R1 from all PCs in the Topology.
- c. SSH to R1 from all PCs in the Topology.
- d. Telnet to S1 from all PCs in the Topology.
- e. SSH to S1 from all PCs in the Topology.
- f. Troubleshoot connectivity issues now because the ACLs that you create in Part 3 of this lab will restrict access to some areas of the network.

Note: Tera Term requires the target IPv6 address to be enclosed in brackets. Enter the IPv6 address as shown, click **OK** and then click **Continue** to accept the security warning and connect to the router.



Input the user credentials configured (username **admin** and password **classadm**) and select the **Use plain password to log in** in the SSH Authentication dialogue box. Click **OK** to continue.



Part 3: Configure and Verify IPv6 ACLs

Step 1: Configure and verify VTY restrictions on R1.

- a. Create an ACL to only allow hosts from the 2001:db8:acad:a::/64 network to telnet to R1. All hosts should only be able to ssh to R1.

```
R1(config)# ipv6 access-list RESTRICT-VTY
R1(config-ipv6-acl)# permit tcp 2001:db8:acad:a::/64 any eq 23
R1(config-ipv6-acl)# permit tcp any any eq 22
```

- b. Apply the RESTRICT-VTY ACL to R1's VTY lines.

```
R1(config-ipv6-acl)# line vty 0 4
R1(config-line)# ipv6 access-class RESTRICT-VTY in
R1(config-line)# end
R1#
```

- c. Show the new ACL.

```
R1# show access-lists
IPv6 access list RESTRICT-VTY
    permit tcp 2001:DB8:ACAD:A::/64 any sequence 10
    permit tcp any any eq 22 sequence 20
```

- d. Verify that the RESTRICT-VTY ACL is only allowing Telnet traffic from the 2001:db8:acad:a::/64 network.

How does the RESTRICT-VTY ACL only allow hosts from the 2001:db8:acad:a::/64 network to telnet to R1?

What does the second permit statement in the RESTRICT-VTY ACL do?

Step 2: Restrict Telnet access to the 2001:db8:acad:a::/64 network.

- a. Create an ACL called RESTRICTED-LAN that will block Telnet access to the 2001:db8:acad:a::/64 network.

```
R1(config)# ipv6 access-list RESTRICTED-LAN
R1(config-ipv6-acl)# remark Block Telnet from outside
R1(config-ipv6-acl)# deny tcp any 2001:db8:acad:a::/64 eq telnet
R1(config-ipv6-acl)# permit ipv6 any any
```

- b. Apply the RESTRICTED-LAN ACL to interface G0/1 for all outbound traffic.

```
R1(config-ipv6-acl)# int g0/1
R1(config-if)# ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

- c. Telnet to S1 from PC-B and PC-C to verify that Telnet has been restricted. SSH to S1 from PC-B to verify that it can still be reached using SSH. Troubleshoot if necessary.
- d. Use the **show ipv6 access-list** command to view the RESTRICTED-LAN ACL.

```
R1# show ipv6 access-lists RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
  deny tcp any 2001:DB8:ACAD:A::/64 eq telnet (6 matches) sequence 20
  permit ipv6 any any (45 matches) sequence 30
```

Notice that each statement identifies the number of hits or matches that have occurred since the ACL was applied to the interface.

- e. Use the **clear ipv6 access-list** to reset the match counters for the RESTRICTED-LAN ACL.

```
R1# clear ipv6 access-list RESTRICTED-LAN
```

- f. Redisplay the ACL with the **show access-lists** command to confirm that the counters were cleared.

```
R1# show access-lists RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
  deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
  permit ipv6 any any sequence 30
```

Part 4: Edit IPv6 ACLs

In Part 4, you will edit the RESTRICTED-LAN ACL that you created in Part 3. It is always a good idea to remove the ACL from the interface to which it is applied before editing it. After you complete your edits, then reapply the ACL to the interface.

Note: Many network administrators will make a copy of the ACL and edit the copy. When editing is complete, the administrator will remove the old ACL and apply the newly edited ACL to the interface. This method keeps the ACL in place until you are ready to apply the edited copy of the ACL.

Step 1: Remove the ACL from the interface.

```
R1(config)# int g0/1
R1(config-if)# no ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

Step 2: Use the show access-lists command to view the ACL.

```
R1# show access-lists
IPv6 access list RESTRICT-VTY
  permit tcp 2001:DB8:ACAD:A::/64 any (4 matches) sequence 10
  permit tcp any any eq 22 (6 matches) sequence 20
IPv6 access list RESTRICTED-LAN
  deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
  permit ipv6 any any (36 matches) sequence 30
```

Step 3: Insert a new ACL statement using sequence numbering.

```
R1(config)# ipv6 access-list RESTRICTED-LAN
R1(config-ipv6-acl)# permit tcp 2001:db8:acad:b::/64 host 2001:db8:acad:a::a
eq 23 sequence 15
```

What does this new permit statement do?

Step 4: Insert a new ACL statement at the end of the ACL.

```
R1(config-ipv6-acl)# permit tcp any host 2001:db8:acad:a::3 eq www
```

Note: This permit statement is only used to show how to add a statement to the end of an ACL. This ACL line would never be matched because the previous permit statement is matching on everything.

Step 5: Use the do show access-lists command to view the ACL change.

```
R1(config-ipv6-acl)# do show access-list
IPv6 access list RESTRICT-VTY
  permit tcp 2001:DB8:ACAD:A::/64 any (2 matches) sequence 10
  permit tcp any any eq 22 (6 matches) sequence 20
IPv6 access list RESTRICTED-LAN
  permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq telnet sequence 15
  deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
  permit ipv6 any any (124 matches) sequence 30
  permit tcp any host 2001:DB8:ACAD:A::3 eq www sequence 40
```

Note: The **do** command can be used to execute any privileged EXEC command while in global configuration mode or a submode.

Step 6: Delete an ACL statement.

Use the **no** command to delete the permit statement that you just added.

```
R1(config-ipv6-acl)# no permit tcp any host 2001:DB8:ACAD:A::3 eq www
```


Step 7: Use the `do show access-list RESTRICTED-LAN` command to view the ACL.

```
R1(config-ipv6-acl)# do show access-list RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
  permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq telnet sequence 15
  deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
  permit ipv6 any any (214 matches) sequence 30
```

Step 8: Re-apply the RESTRICTED-LAN ACL to the interface G0/1.

```
R1(config-ipv6-acl)# int g0/1
R1(config-if)# ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

Step 9: Test ACL changes.

Telnet to S1 from PC-B. Troubleshoot if necessary.

Reflection

1. What is causing the match count on the RESTRICTED-LAN `permit ipv6 any any` statement to continue to increase?
2. What command would you use to reset the counters for the ACL on the VTY lines?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
<p>Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.</p>				