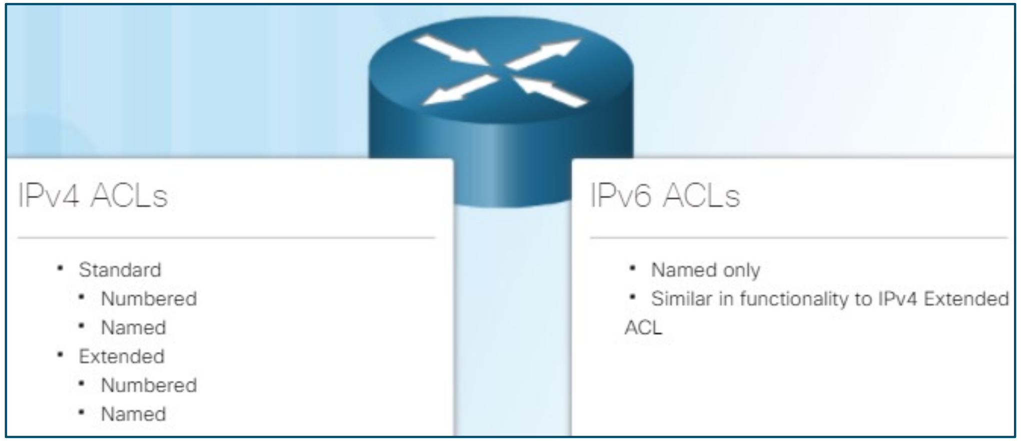
Access Control Lists IPv6

1. IPv6 ACLs Configuration

IPv6 ACL Creation

- IPv6 ACLs are similar to IPv4 ACLs in both operation and configuration.

In IPv4 there are two types of ACLs, standard and extended and both types of ACLs can be either numbered or named ACLs.



IPv4 ACLs

- Standard
  - Numbered
  - Named
- Extended
  - Numbered
  - Named

IPv6 ACLs

- Named only
- Similar in functionality to IPv4 Extended ACL

With IPv6, there is only one type of ACL, which is equivalent to an IPv4 **extended named ACL** and there are no numbered ACLs in IPv6.

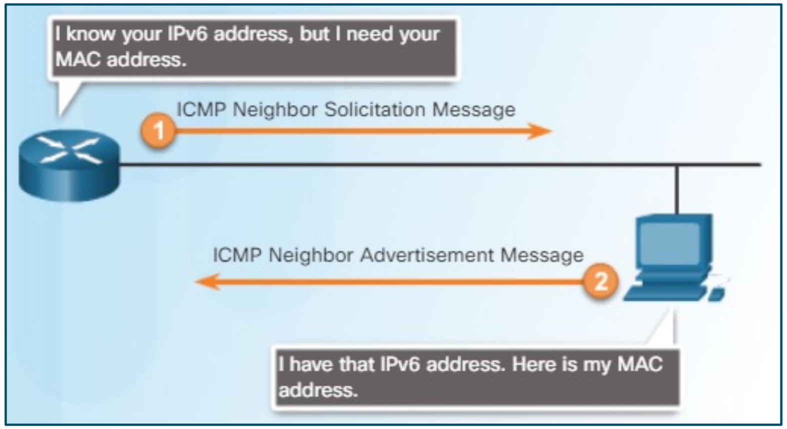
- **Note:**
  - An IPv4 ACL and an IPv6 ACL cannot share the same name.

IPv6 ACL Creation

- There are **three significant differences** between IPv4 and IPv6 ACLs:
  - The command used to apply an IPv6 ACL to an interface is **ipv6 traffic-filter** command.
  - IPv6 ACLs **do not use wildcard masks** but instead specifies the **prefix-length** to indicate how much of an IPv6 source or destination address should be matched.
  - Additional Default Statements:
    - IPv6 includes a **deny ipv6 any any** statement at the end (similar to IPv4 ACLs)
    - Two other **implicit statements** by default:

```
permit icmp any any nd-na
permit icmp any any nd-ns
```

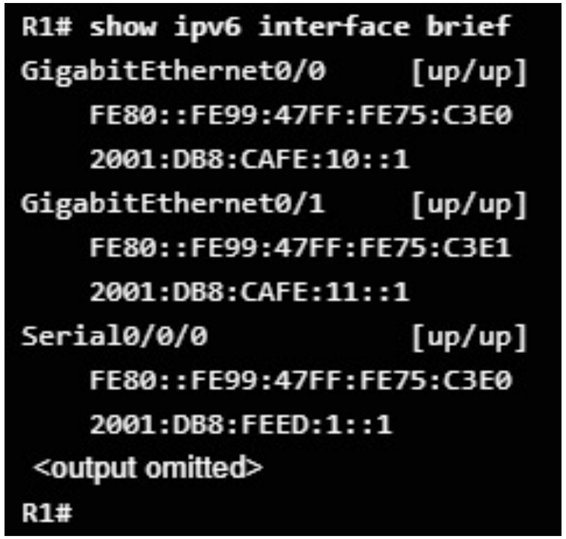
IPv6 uses ICMP Neighbor Discovery (ND) messages (Neighbor Solicitation (NS) and Neighbor Advertisement (NA) to accomplish what ARP does in IPv4.


I know your IPv6 address, but I need your MAC address.
1
ICMP Neighbor Solicitation Message
ICMP Neighbor Advertisement Message
2
I have that IPv6 address. Here is my MAC address.

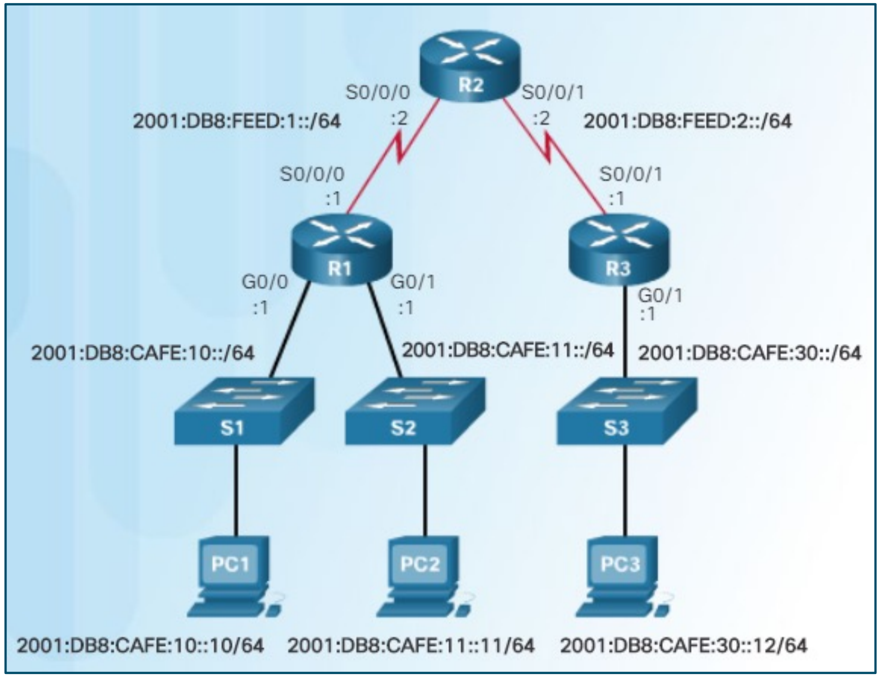
ND messages are encapsulated in IPv6 packets and thus using the Layer 3 service for neighbor discovery. Therefore, IPv6 ACLs need to implicitly permit ND packets to be sent and received on an interface. Specifically, both Neighbor Discovery - Neighbor Advertisement (nd-na) and Neighbor Discovery - Neighbor Solicitation (nd-ns) messages need to be permitted

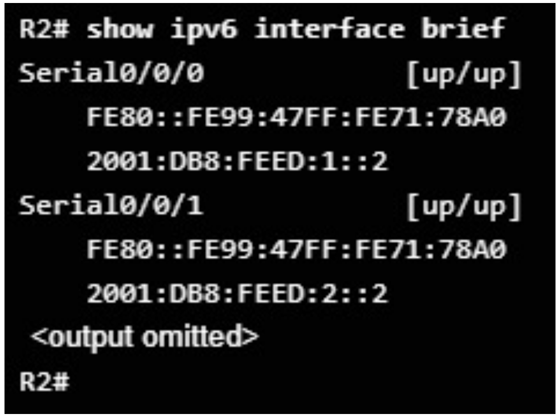
Configuring IPv6 ACLs

- The following is the **sample topology** that will be used to demonstrate IPv6 ACLs.
  - All interfaces are configured and active.

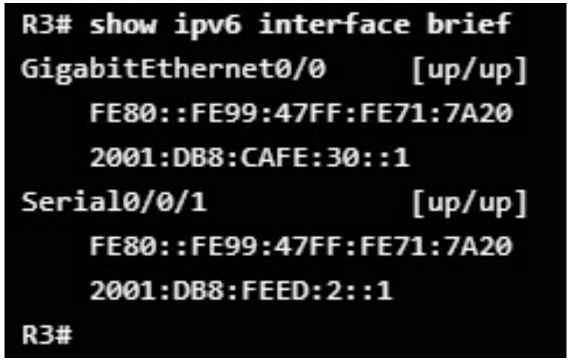


```
R1# show ipv6 interface brief
GigabitEthernet0/0       [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:CAFE:10::1
GigabitEthernet0/1       [up/up]
    FE80::FE99:47FF:FE75:C3E1
    2001:DB8:CAFE:11::1
Serial0/0/0              [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:FEED:1::1
 <output omitted>
R1#
```





```
R2# show ipv6 interface brief
Serial0/0/0              [up/up]
    FE80::FE99:47FF:FE71:78A0
    2001:DB8:FEED:1::2
Serial0/0/1              [up/up]
    FE80::FE99:47FF:FE71:78A0
    2001:DB8:FEED:2::2
 <output omitted>
R2#
```



```
R3# show ipv6 interface brief
GigabitEthernet0/0       [up/up]
    FE80::FE99:47FF:FE71:7A20
    2001:DB8:CAFE:30::1
Serial0/0/1              [up/up]
    FE80::FE99:47FF:FE71:7A20
    2001:DB8:FEED:2::1
R3#
```

IPv6 ACLs

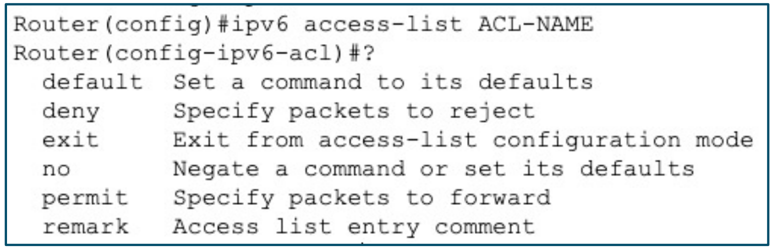
Configuring IPv6 ACLs

In IPv6 there are **only extended named ACLs** and the configuration is similar to IPv4 extended named ACLs.

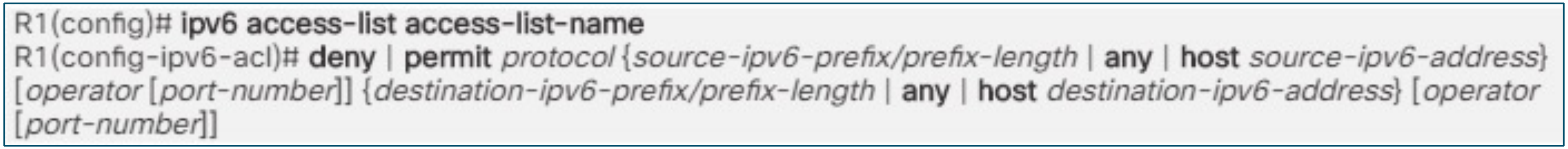
There are **two basic steps** to configure an IPv6 ACL:

1. From global configuration mode, use the **`ipv6 access-list`** *`name`* command to create an IPv6 ACL. IPv6 names are alphanumeric, case sensitive, and must be unique. Unlike IPv4, there is **no need for a standard or extended option**.

2. From the named ACL configuration mode, use **`permit`** or **`deny`** statements to specify one or more conditions to determine if a packet is forwarded or dropped.



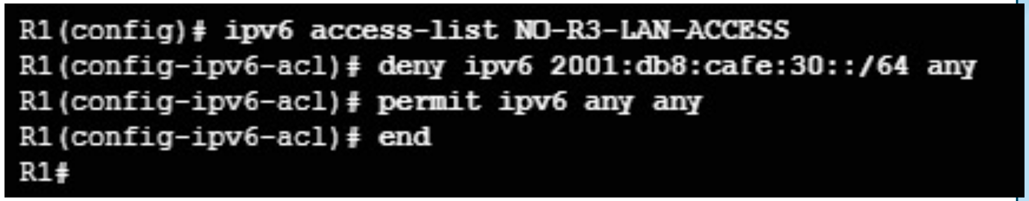
```
Router(config)#ipv6 access-list ACL-NAME
Router(config-ipv6-acl)#?
  default   Set a command to its defaults
  deny      Specify packets to reject
  exit      Exit from access-list configuration mode
  no        Negate a command or set its defaults
  permit    Specify packets to forward
  remark    Access list entry comment
```



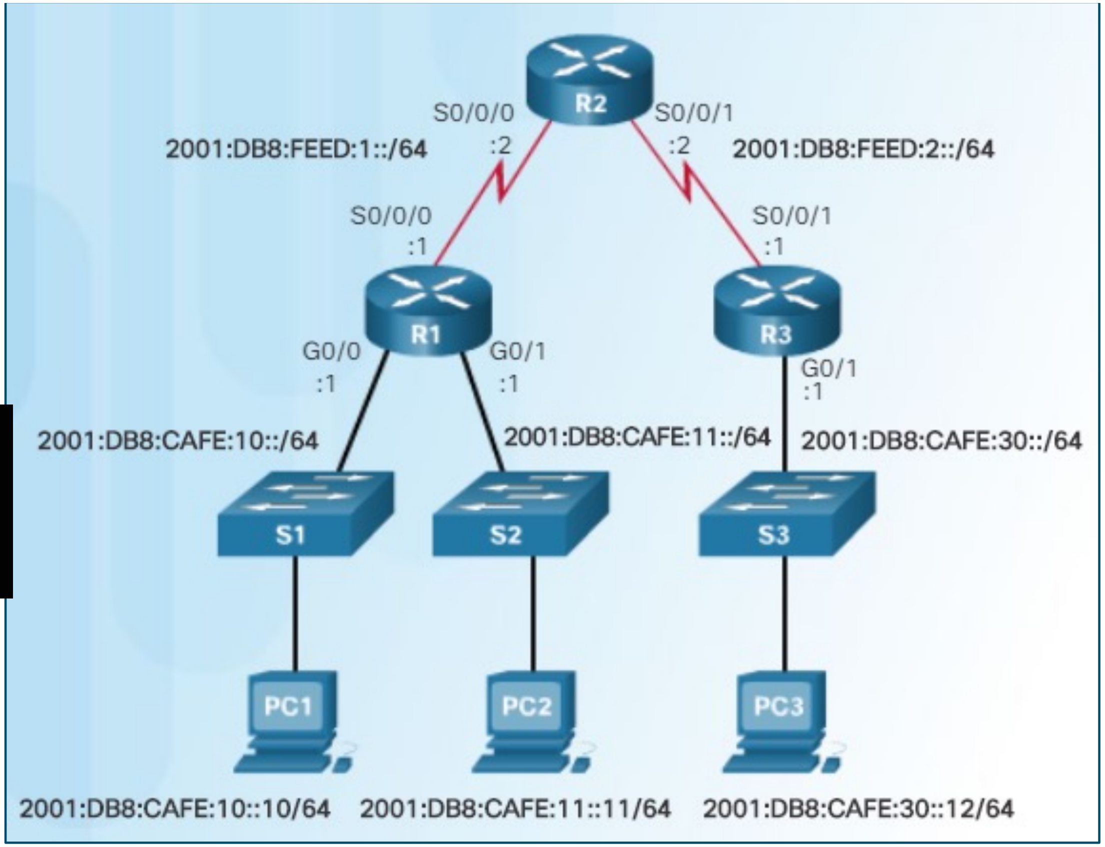
```
R1(config)# ipv6 access-list access-list-name
R1(config-ipv6-acl)# deny | permit protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address}
[operator [port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [operator
[port-number]]
```

IPv6 ACLs

Configuring IPv6 ACLs



```
R1(config)# ipv6 access-list NO-R3-LAN-ACCESS
R1(config-ipv6-acl)# deny ipv6 2001:db8:cafe:30::/64 any
R1(config-ipv6-acl)# permit ipv6 any any
R1(config-ipv6-acl)# end
R1#
```



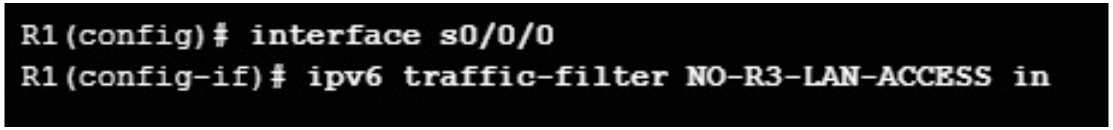
- In this example:
  - The 1st statement names the IPv6 ACL **NO-R3-LAN-ACCESS**.
  - The 2nd statement denies all IPv6 packets from the 2001:DB8:CAFE:30::/64 destined for any IPv6 network.
  - The 3rd statement allows all other IPv6 packets.

IPv6 ACLs

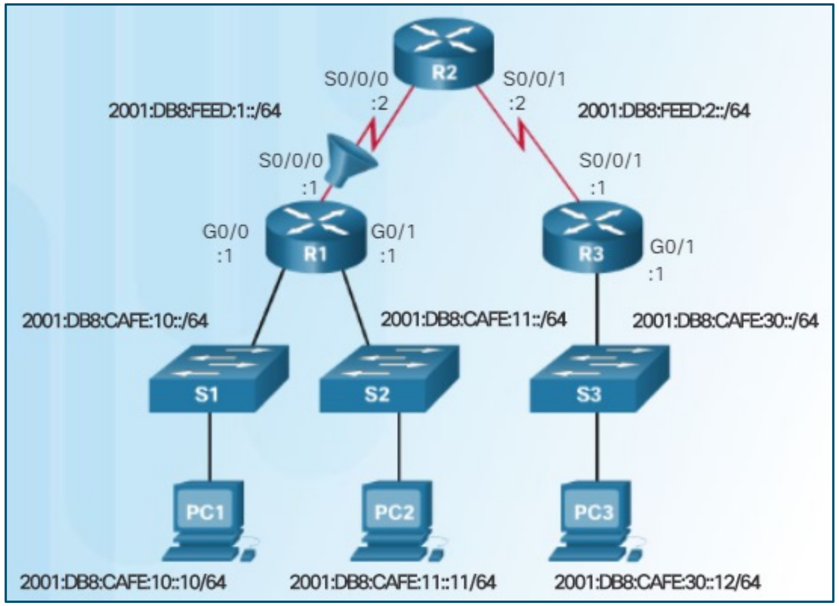
Configuring IPv6 ACLs

- After an IPv6 ACL is configured, it is linked to an interface using the following interface command:
  - **ipv6 traffic-filter** *access-list-name* {**in** | **out**}

  The command applies the NO-R3-LAN-ACCESS IPv6 ACL inbound to the S0/0/0 interface of R1.



```
R1(config)# interface s0/0/0
R1(config-if)# ipv6 traffic-filter NO-R3-LAN-ACCESS in
```



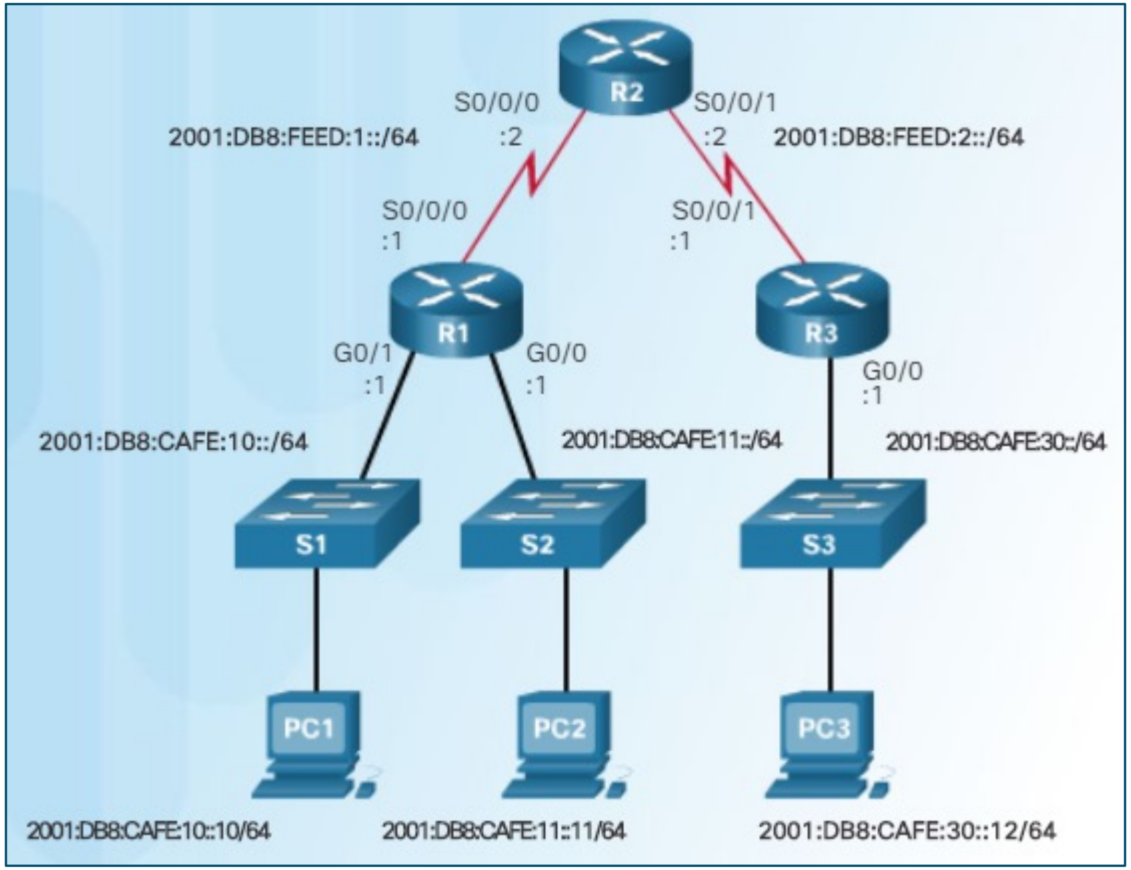
- To **remove** an IPv6 ACL, enter the **no ipv6 traffic-filter** command on the interface, and then enter the global **no ipv6 access-list** command to remove the access list.

- Note that IPv4 and IPv6 both use the **access-class** command to **apply an access list to VTY ports**.

IPv6 ACLs

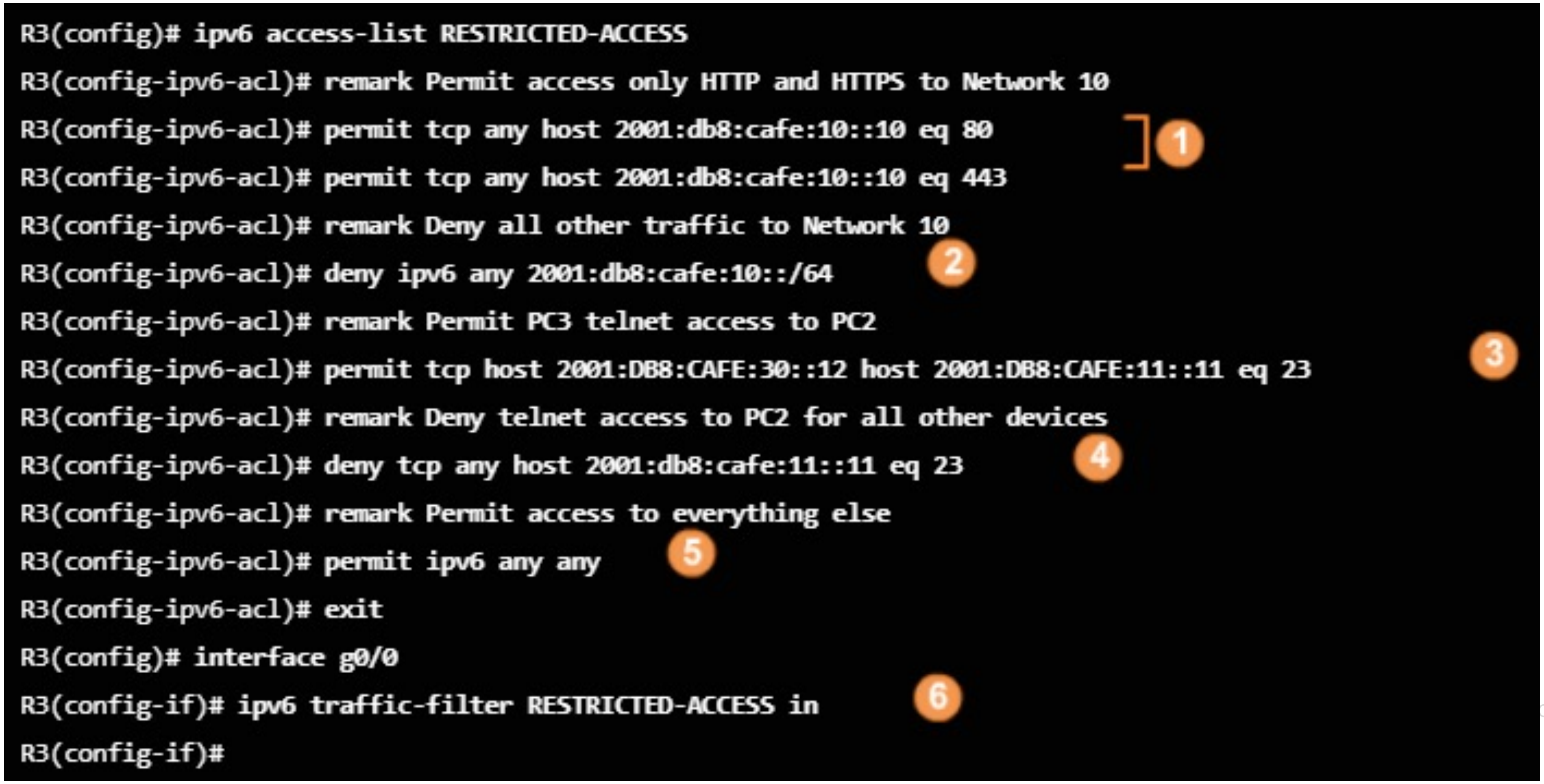
Configuring IPv6 ACLs

- In this example, an IPv6 ACL permits R3 LAN users **limited access** to the LANs on R1.



Configuring IPv6 ACLs

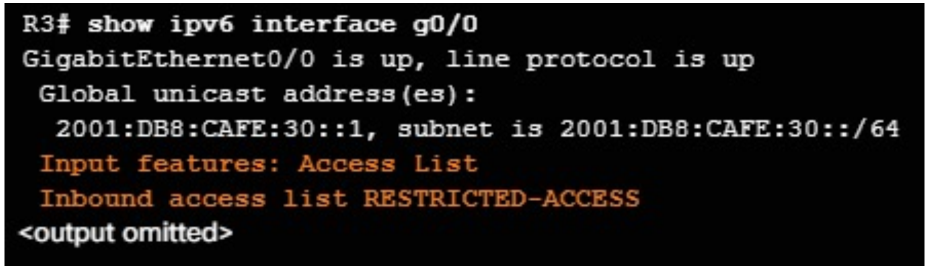
1. These ACEs allow access from any device to the web server on PC1 (2001:DB8:CAFE:10::10).
2. All other devices are denied access to the 2001:DB8:CAFE:10::/64 network.
3. PC3 (2001:DB8:CAFE:30::12) is permitted Telnet access to PC2 (2001:DB8:CAFE:11::11).
4. All others are denied Telnet access to PC2.
5. All other IPv6 traffic is permitted to all other destinations.
6. The IPv6 access list is applied inbound on G0/0 so only the 2001:DB8:CAFE:30::/64 network is affected.



```
R3(config)# ipv6 access-list RESTRICTED-ACCESS
R3(config-ipv6-acl)# remark Permit access only HTTP and HTTPS to Network 10
R3(config-ipv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 80
R3(config-ipv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 443
R3(config-ipv6-acl)# remark Deny all other traffic to Network 10
R3(config-ipv6-acl)# deny ipv6 any 2001:db8:cafe:10::/64
R3(config-ipv6-acl)# remark Permit PC3 telnet access to PC2
R3(config-ipv6-acl)# permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11 eq 23
R3(config-ipv6-acl)# remark Deny telnet access to PC2 for all other devices
R3(config-ipv6-acl)# deny tcp any host 2001:db8:cafe:11::11 eq 23
R3(config-ipv6-acl)# remark Permit access to everything else
R3(config-ipv6-acl)# permit ipv6 any any
R3(config-ipv6-acl)# exit
R3(config)# interface g0/0
R3(config-if)# ipv6 traffic-filter RESTRICTED-ACCESS in
R3(config-if)#
```

Configuring IPv6 ACLs

- The commands used to verify an IPv6 access list are similar to those used for IPv4 ACLs.
- Use the **show ipv6 interface** command to see which ACL and direction is configured on an interface.

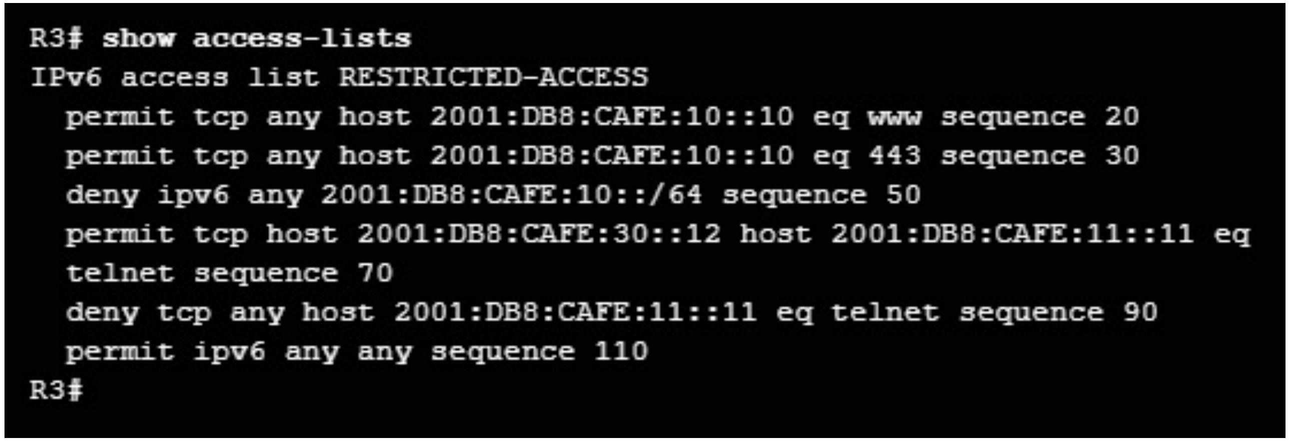


```
R3# show ipv6 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
 Global unicast address(es):
  2001:DB8:CAFE:30::1, subnet is 2001:DB8:CAFE:30::/64
 Input features: Access List
 Inbound access list RESTRICTED-ACCESS
<output omitted>
```

IPv6 ACLs

Configuring IPv6 ACLs

- Use the **show access-lists** command displays all configured IPv4 and IPv6 access lists
  - Notice that IPv6 ACL **sequence numbers** are displayed **at the end of the ACE**.
  - Although the statements appear in the order they were entered, they are **not always incremented by 10**. This is because the remark statements that were entered use a sequence number but are not displayed in the output of the **show access-lists** command.
  - Similar to extended ACLs for IPv4, **IPv6 access lists are displayed and processed in the order the statements are entered**.

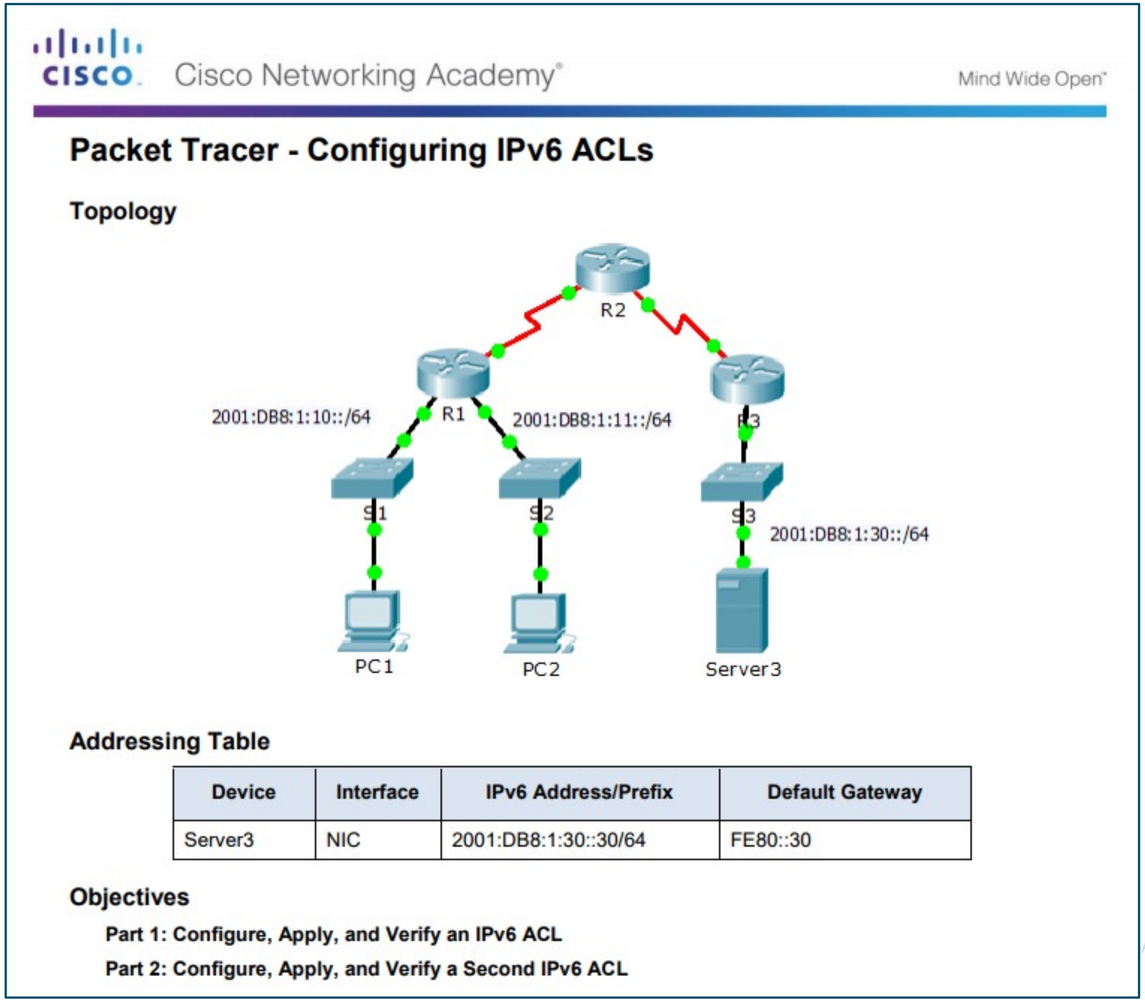


```
R3# show access-lists
IPv6 access list RESTRICTED-ACCESS
  permit tcp any host 2001:DB8:CAFE:10::10 eq www sequence 20
  permit tcp any host 2001:DB8:CAFE:10::10 eq 443 sequence 30
  deny ipv6 any 2001:DB8:CAFE:10::/64 sequence 50
  permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11 eq
  telnet sequence 70
  deny tcp any host 2001:DB8:CAFE:11::11 eq telnet sequence 90
  permit ipv6 any any sequence 110
R3#
```

- The **show running-config** command displays all of the ACEs and remark statements.

IPv6 ACLs

Configuring IPv6 ACLs



Cisco Networking Academy®

Mind Wide Open™

Packet Tracer - Configuring IPv6 ACLs

Topology

R2
R1
R3
2001:DB8:1:10::/64
2001:DB8:1:11::/64
2001:DB8:1:30::/64
S1
S2
S3
PC1
PC2
Server3

Addressing Table

Device	Interface	IPv6 Address/Prefix	Default Gateway
Server3	NIC	2001:DB8:1:30::30/64	FE80::30

Objectives

Part 1: Configure, Apply, and Verify an IPv6 ACL

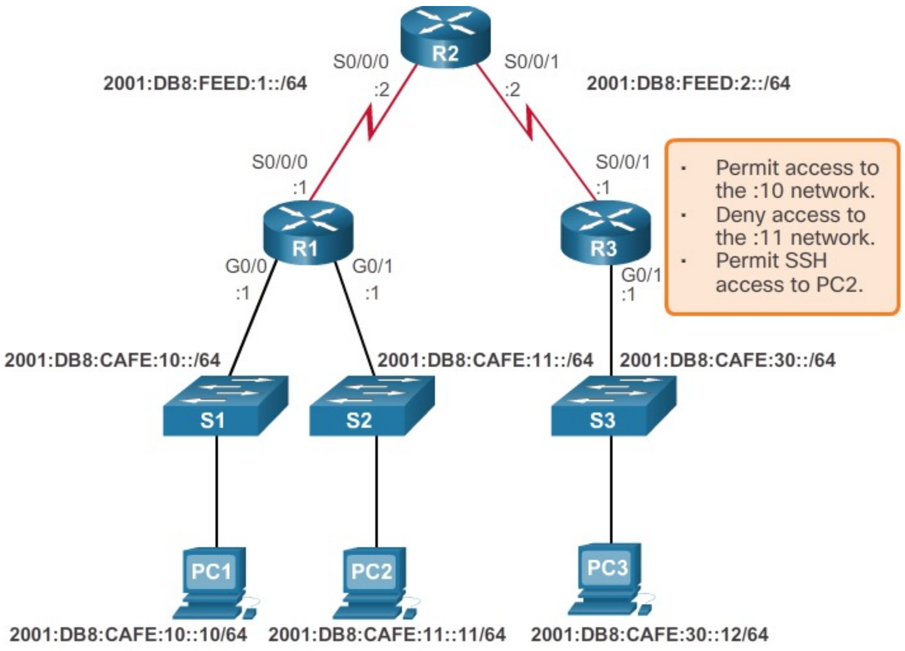
Part 2: Configure, Apply, and Verify a Second IPv6 ACL

2 Troubleshoot IPv6 ACLs

Common ACL Errors

Example 1: Troubleshooting IPv6 ACLs

- R3 is configured with IPv6 ACL RESTRICTED-ACCESS that should enforce the following policy for the R3 LAN:



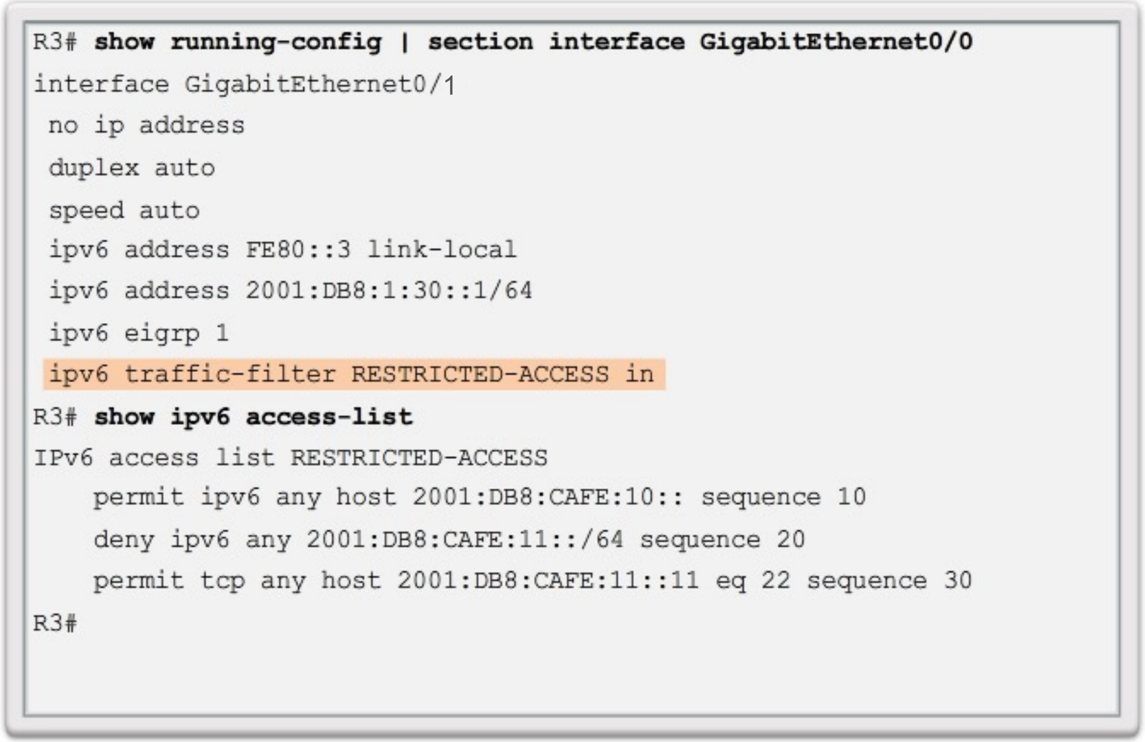
- Permit access to the :10 network.
- Deny access to the :11 network.
- Permit SSH access to PC2.

- However, after configuring the ACL, PC3 cannot reach the 10 network or the 11 network, and it cannot SSH into the host at 2001:DB8:CAFE:11::11.

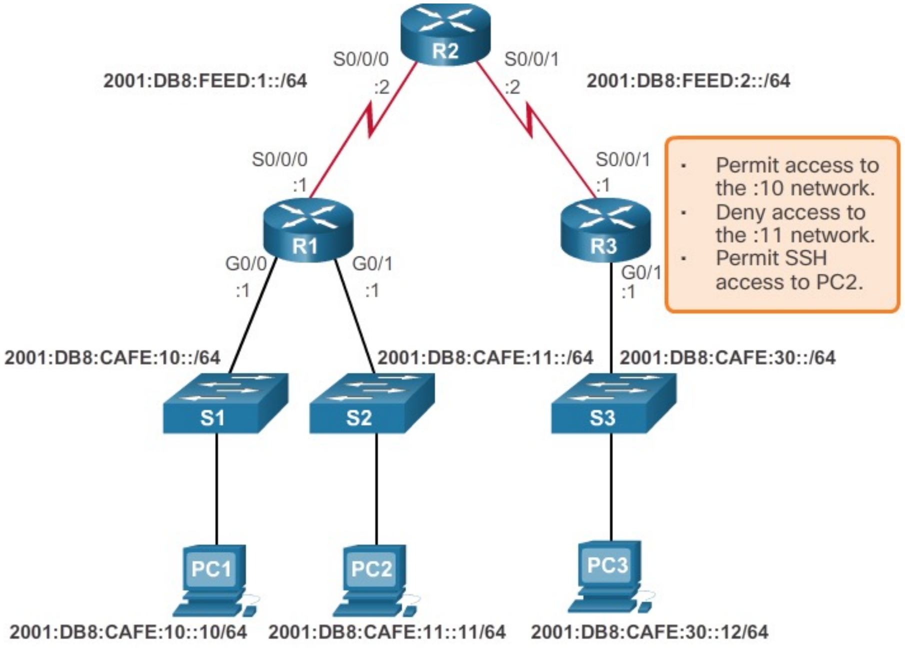
Common ACL Errors

Example 1: Troubleshooting IPv6 ACLs (cont.)

Verify the IPv6 ACL Configuration and Application



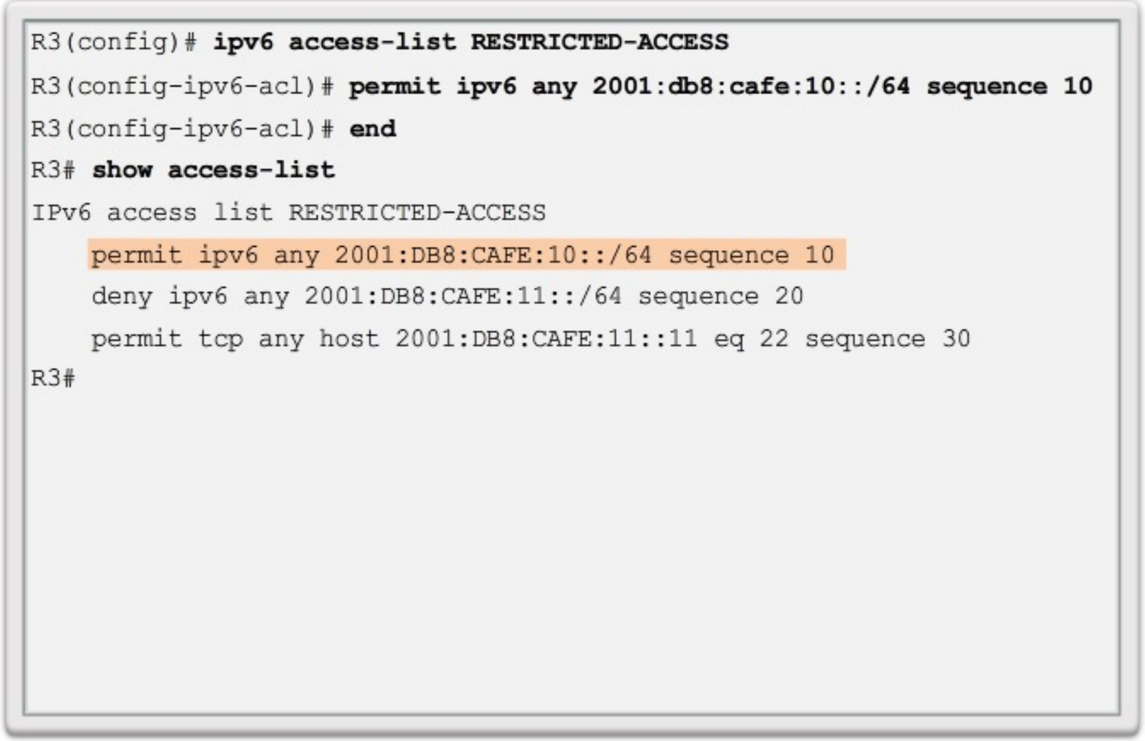
```
R3# show running-config | section interface GigabitEthernet0/0
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::3 link-local
 ipv6 address 2001:DB8:1:30::1/64
 ipv6 eigrp 1
 ipv6 traffic-filter RESTRICTED-ACCESS in
R3# show ipv6 access-list
IPv6 access list RESTRICTED-ACCESS
    permit ipv6 any host 2001:DB8:CAFE:10:: sequence 10
    deny ipv6 any 2001:DB8:CAFE:11::/64 sequence 20
    permit tcp any host 2001:DB8:CAFE:11::11 eq 22 sequence 30
R3#
```



- Permit access to the :10 network.
- Deny access to the :11 network.
- Permit SSH access to PC2.

Common ACL Errors

Example 1: Troubleshooting IPv6 ACLs (cont.)



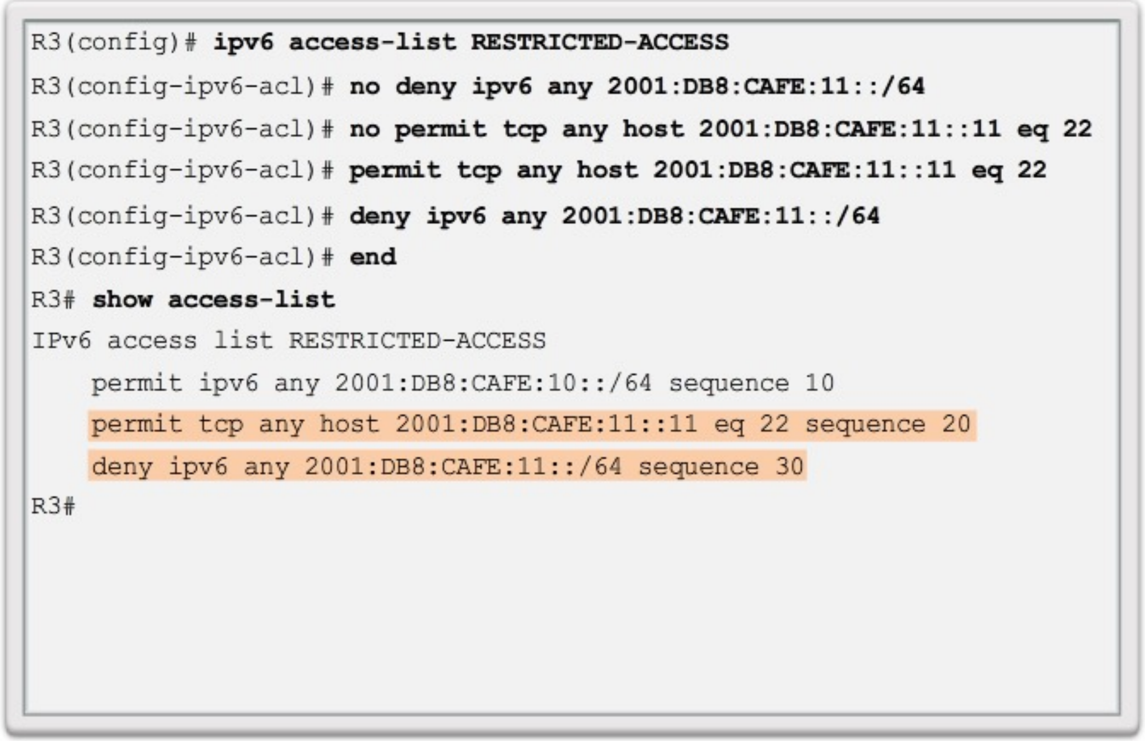
```
R3(config)# ipv6 access-list RESTRICTED-ACCESS
R3(config-ipv6-acl)# permit ipv6 any 2001:db8:cafe:10::/64 sequence 10
R3(config-ipv6-acl)# end
R3# show access-list
IPv6 access list RESTRICTED-ACCESS
    permit ipv6 any 2001:DB8:CAFE:10::/64 sequence 10
    deny ipv6 any 2001:DB8:CAFE:11::/64 sequence 20
    permit tcp any host 2001:DB8:CAFE:11::11 eq 22 sequence 30
R3#
```

First of all, you have to remove the existing statement:
no permit ipv6 …

Common ACL Errors

Example 1: Troubleshooting IPv6 ACLs (cont.)

Replace the IPv6 ACL Host Statement

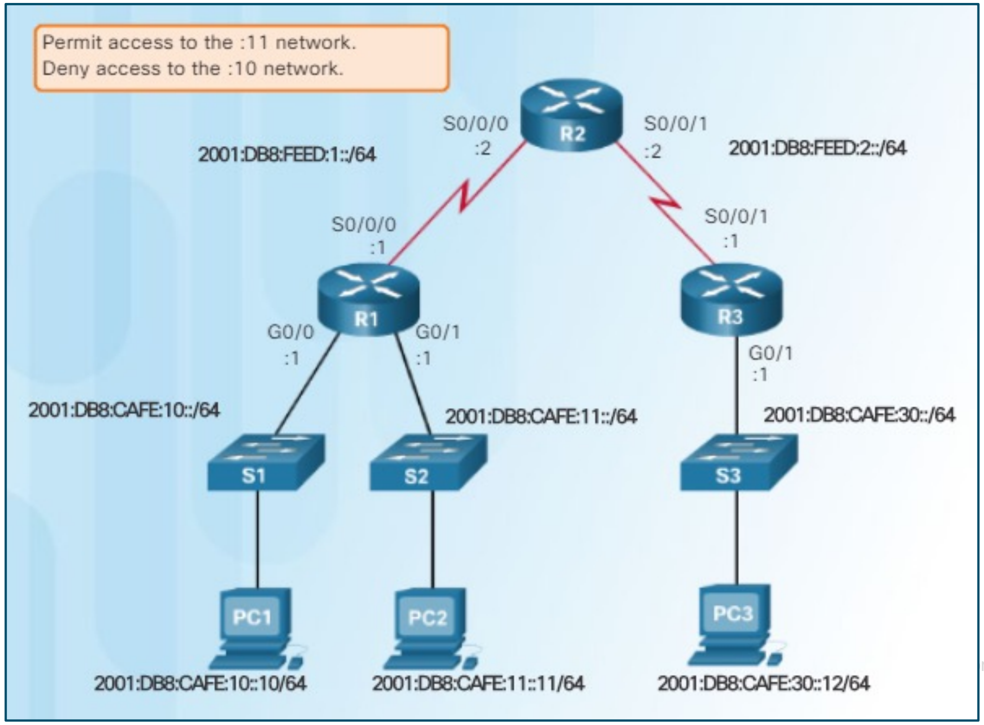


```
R3(config)# ipv6 access-list RESTRICTED-ACCESS
R3(config-ipv6-acl)# no deny ipv6 any 2001:DB8:CAFE:11::/64
R3(config-ipv6-acl)# no permit tcp any host 2001:DB8:CAFE:11::11 eq 22
R3(config-ipv6-acl)# permit tcp any host 2001:DB8:CAFE:11::11 eq 22
R3(config-ipv6-acl)# deny ipv6 any 2001:DB8:CAFE:11::/64
R3(config-ipv6-acl)# end
R3# show access-list
IPv6 access list RESTRICTED-ACCESS
    permit ipv6 any 2001:DB8:CAFE:10::/64 sequence 10
    permit tcp any host 2001:DB8:CAFE:11::11 eq 22 sequence 20
    deny ipv6 any 2001:DB8:CAFE:11::/64 sequence 30
R3#
```

Troubleshoot ACLs

Common ACLs Errors

- In example 2, R1 is configured with an IPv6 ACL named DENY-ACCESS.
  - The DENY-ACCESS ACL is supposed to permit access to the :11 network from the :30 network while denying access to the :10 network.
  - However, after applying the ACL to the interface the :10 network is still reachable from the :30 network.

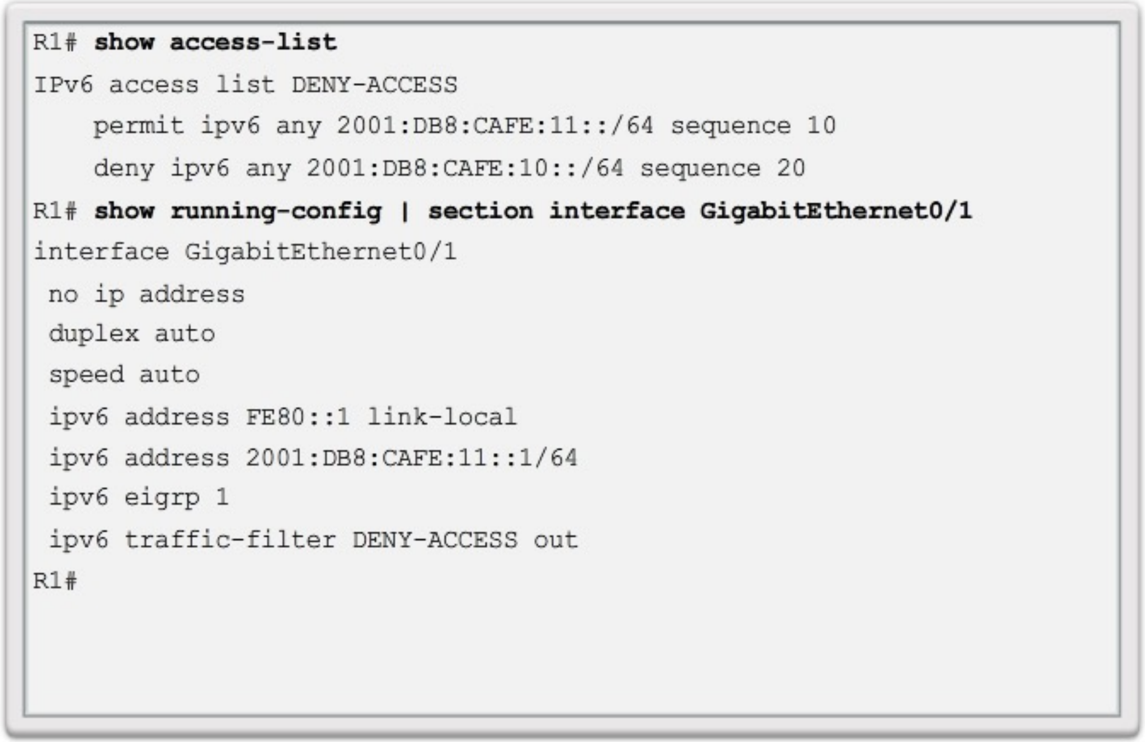


Permit access to the :11 network.
Deny access to the :10 network.

Common ACL Errors

Example 2: Troubleshooting IPv6 ACLs (cont.)

Verify the IPv6 ACL Configuration and Application



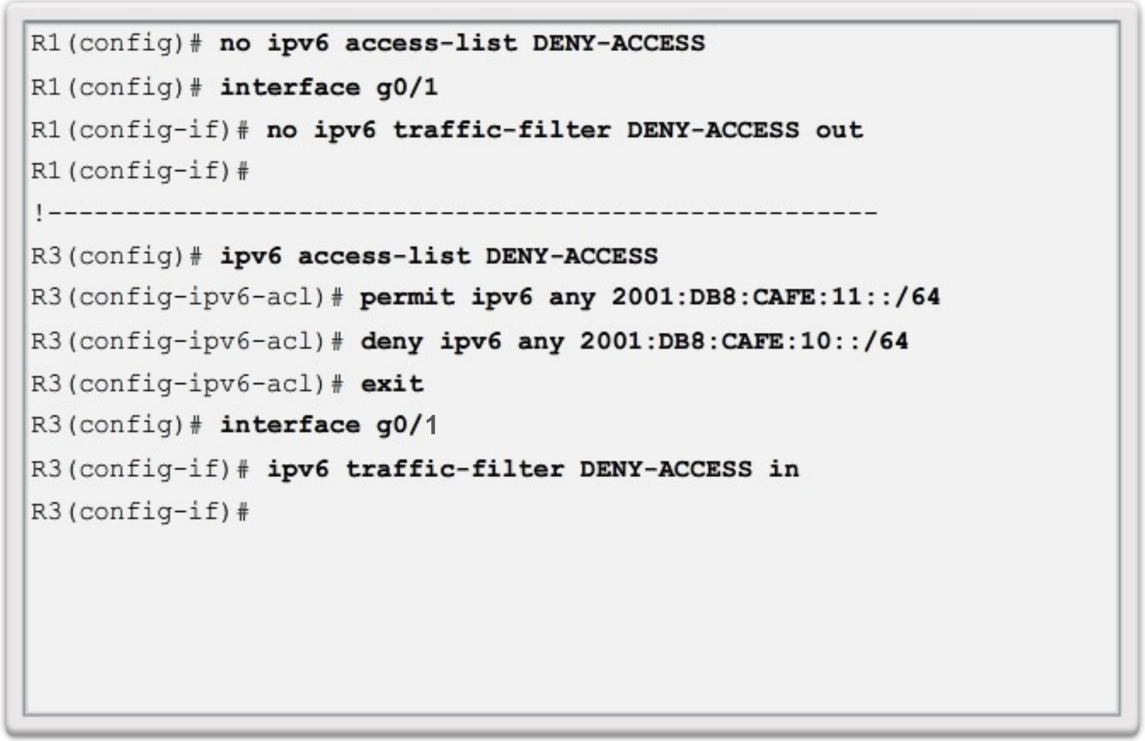
```
R1# show access-list
IPv6 access list DENY-ACCESS
    permit ipv6 any 2001:DB8:CAFE:11::/64 sequence 10
    deny ipv6 any 2001:DB8:CAFE:10::/64 sequence 20
R1# show running-config | section interface GigabitEthernet0/1
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:CAFE:11::1/64
 ipv6 eigrp 1
 ipv6 traffic-filter DENY-ACCESS out
R1#
```

The problem is with the location of the ACL and should be applied closest to the source of the traffic.

Common ACL Errors

Troubleshooting IPv6 ACLs- Example 3 (cont.)

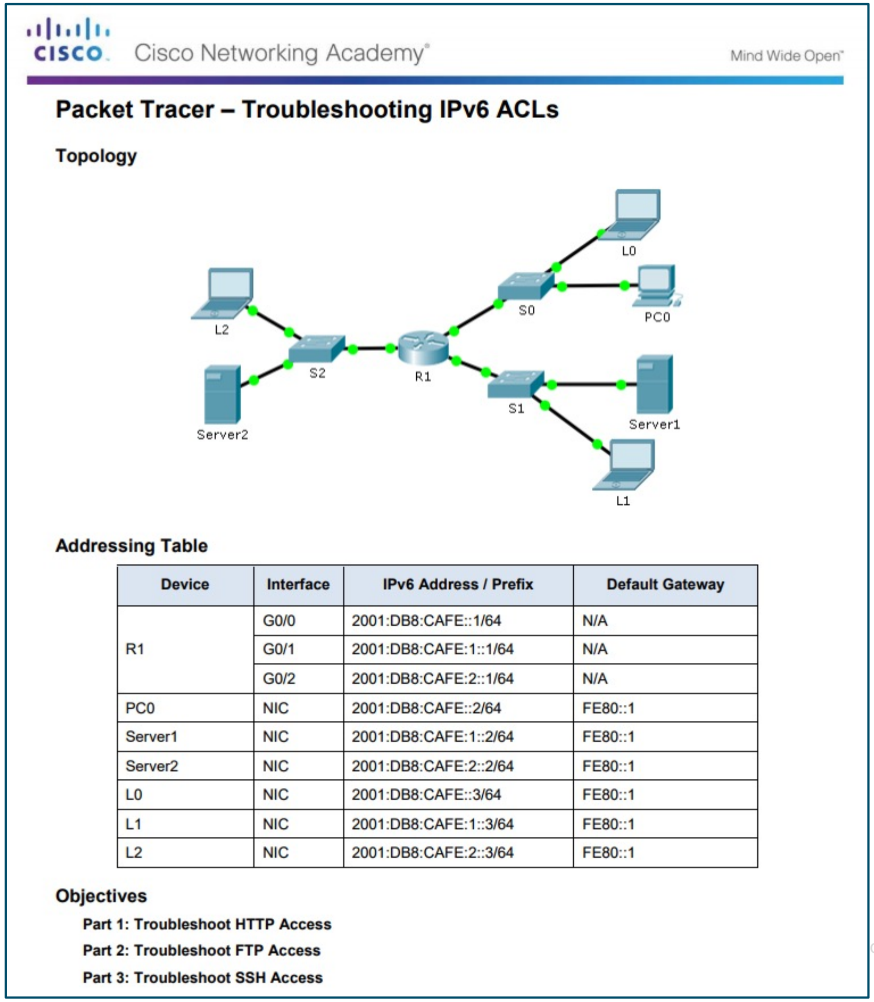
Remove ACL on R1, then Configure and Apply ACL on R3



```
R1(config)# no ipv6 access-list DENY-ACCESS
R1(config)# interface g0/1
R1(config-if)# no ipv6 traffic-filter DENY-ACCESS out
R1(config-if)#
!-----------------------------------------------------
R3(config)# ipv6 access-list DENY-ACCESS
R3(config-ipv6-acl)# permit ipv6 any 2001:DB8:CAFE:11::/64
R3(config-ipv6-acl)# deny ipv6 any 2001:DB8:CAFE:10::/64
R3(config-ipv6-acl)# exit
R3(config)# interface g0/1
R3(config-if)# ipv6 traffic-filter DENY-ACCESS in
R3(config-if)#
```

Troubleshoot ACLs

Common ACLs Errors



Cisco Networking Academy®

Mind Wide Open™

Packet Tracer – Troubleshooting IPv6 ACLs

Topology

L0
S0
PC0
L2
S2
R1
S1
Server1
Server2
L1

Addressing Table

Device	Interface	IPv6 Address / Prefix	Default Gateway
R1	G0/0	2001:DB8:CAFE::1/64	N/A
	G0/1	2001:DB8:CAFE:1::1/64	N/A
	G0/2	2001:DB8:CAFE:2::1/64	N/A
PC0	NIC	2001:DB8:CAFE::2/64	FE80::1
Server1	NIC	2001:DB8:CAFE:1::2/64	FE80::1
Server2	NIC	2001:DB8:CAFE:2::2/64	FE80::1
L0	NIC	2001:DB8:CAFE::3/64	FE80::1
L1	NIC	2001:DB8:CAFE:1::3/64	FE80::1
L2	NIC	2001:DB8:CAFE:2::3/64	FE80::1

Objectives

Part 1: Troubleshoot HTTP Access

Part 2: Troubleshoot FTP Access

Part 3: Troubleshoot SSH Access