

PRACTICAL NO 5: Configuring IPv6 ACLs

Access Control Lists for IPv6 Traffic Filtering

The standard ACL functionality in IPv6 is similar to standard ACLs in IPv4. Access lists determine what traffic is blocked and what traffic is forwarded at device interfaces and allow filtering based on source and destination addresses, inbound and outbound to a specific interface. Each access list has an implicit deny statement at the end. IPv6 ACLs are defined and their deny and permit conditions are set using the **ipv6 access-list** command with the deny and **permit** keywords in global configuration mode.

IPv6 extended ACLs augments standard IPv6 ACL functionality to support traffic filtering based on IPv6 option headers and optional, upper-layer protocol type information for finer granularity of control (functionality similar to extended ACLs in IPv4).

IPv6 Packet Inspection

Access Class Filtering in IPv6

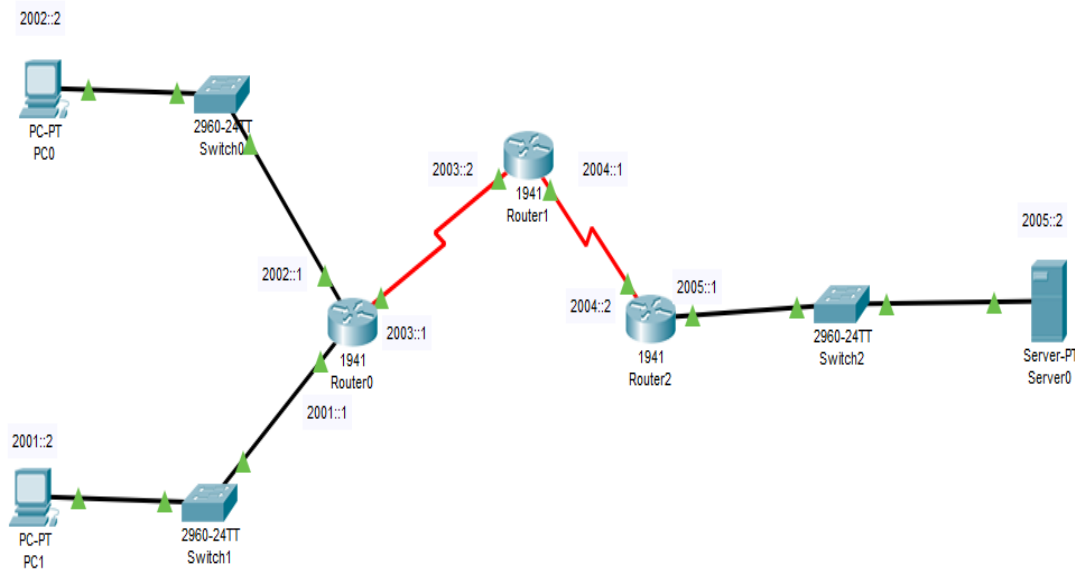
IPv6 Packet Inspection

The following header fields are used for IPv6 inspection: traffic class, flow label, payload length, next header, hop limit, and source or destination IP address. For further information on and descriptions of the IPv6 header fields, see RFC 2474.

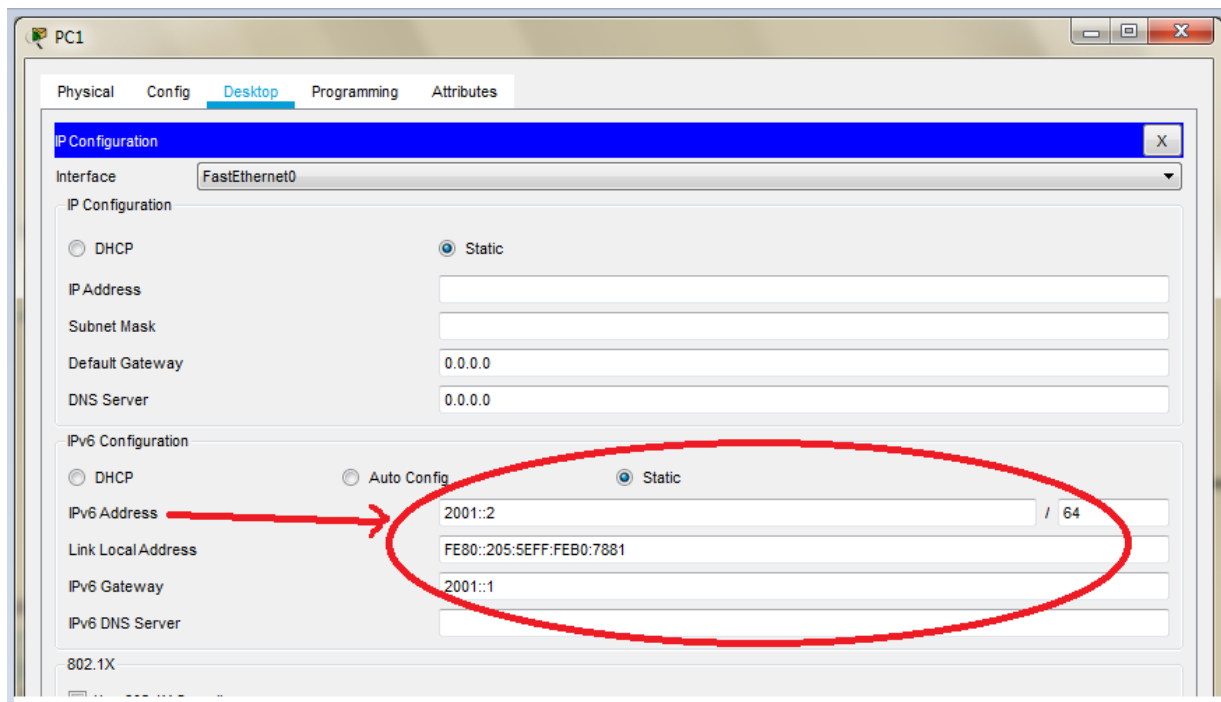
Access Class Filtering in IPv6

Filtering incoming and outgoing connections to and from the device based on an IPv6 ACL is performed using the **ipv6 access-class** command in line configuration mode. The **ipv6 access-class** command is similar to the **access-class** command, except the IPv6 ACLs are defined by a name. If the IPv6 ACL is applied to inbound traffic, the source address in the ACL is matched against the incoming connection source address and the destination address in the ACL is matched against the local device address on the interface. If the IPv6 ACL is applied to outbound traffic, the source address in the ACL is matched against the local device address on the interface and the destination address in the ACL is matched against the outgoing connection source address. We recommend that identical restrictions are set on all the virtual terminal lines because a user can attempt to connect to any of them.

We use the following topology



Configuring PC1



Configuring PC0

The screenshot shows the configuration window for PC0. The 'Desktop' tab is selected. The 'Interface' dropdown is set to 'FastEthernet0'. Under 'IP Configuration', the 'Static' radio button is selected. The 'IP Address' and 'Subnet Mask' fields are empty. The 'Default Gateway' is set to '0.0.0.0' and the 'DNS Server' is also set to '0.0.0.0'. Under 'IPv6 Configuration', the 'Static' radio button is selected. The 'IPv6 Address' is set to '2002::2' with a prefix length of '64'. The 'Link Local Address' is set to 'FE80::201:97FF:FEA4:DD7B'. The 'IPv6 Gateway' is set to '2002::1' and the 'IPv6 DNS Server' is empty. The '802.1X' section is visible at the bottom.

PC0

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IP Address:

Subnet Mask:

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address: 2002::2 / 64

Link Local Address: FE80::201:97FF:FEA4:DD7B

IPv6 Gateway: 2002::1

IPv6 DNS Server:

802.1X

Configuring Server0

The screenshot shows the configuration window for Server0. The 'Desktop' tab is selected. The 'Interface' dropdown is set to 'FastEthernet0'. Under 'IP Configuration', the 'Static' radio button is selected. The 'IP Address' and 'Subnet Mask' fields are empty. The 'Default Gateway' is set to '0.0.0.0' and the 'DNS Server' is also set to '0.0.0.0'. Under 'IPv6 Configuration', the 'Static' radio button is selected. The 'IPv6 Address' is set to '2005::2' with a prefix length of '64'. The 'Link Local Address' is set to 'FE80::20A:F3FF:FE03:E83D'. The 'IPv6 Gateway' is set to '2005::1' and the 'IPv6 DNS Server' is empty. The '802.1X' section is visible at the bottom.

Server0

Physical Config Services **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IP Address:

Subnet Mask:

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address: 2005::2 / 64

Link Local Address: FE80::20A:F3FF:FE03:E83D

IPv6 Gateway: 2005::1

IPv6 DNS Server:

802.1X

For setting the ipv6 addresses we need to use the CLI mode for each Router as follows

Configuring Router0

```
Router>
Router>enable
Router#
Router#configure terminal
Router(config)#ipv6 unicast-routing

Router(config)#interface GigabitEthernet0/0
Router(config-if)#ipv6 address 2002::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#

Router(config)#interface GigabitEthernet0/1
Router(config-if)#ipv6 address 2001::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#

Router(config)#interface Serial0/1/0
Router(config-if)#ipv6 address 2003::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Configuring Router1

```
Router>enable
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#

Router(config)#interface Serial0/1/0
Router(config-if)#ipv6 address 2003::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#exit
Router(config)#
```

```
Router(config)#interface Serial0/1/1
Router(config-if)#ipv6 address 2004::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

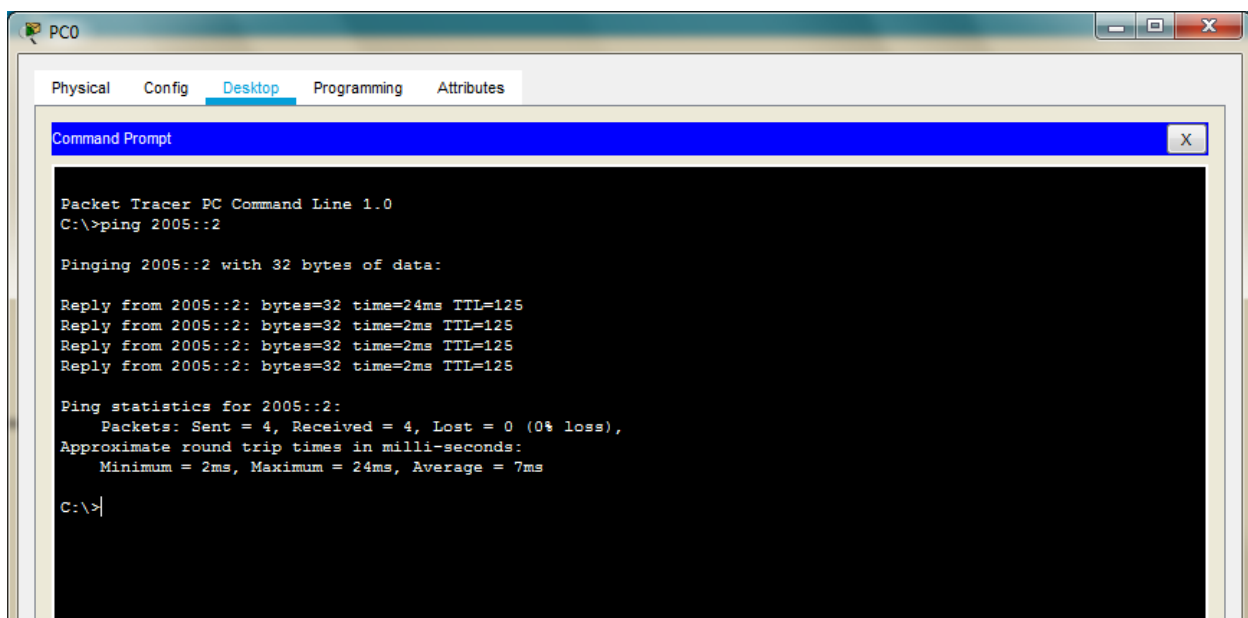
Configuring Router2

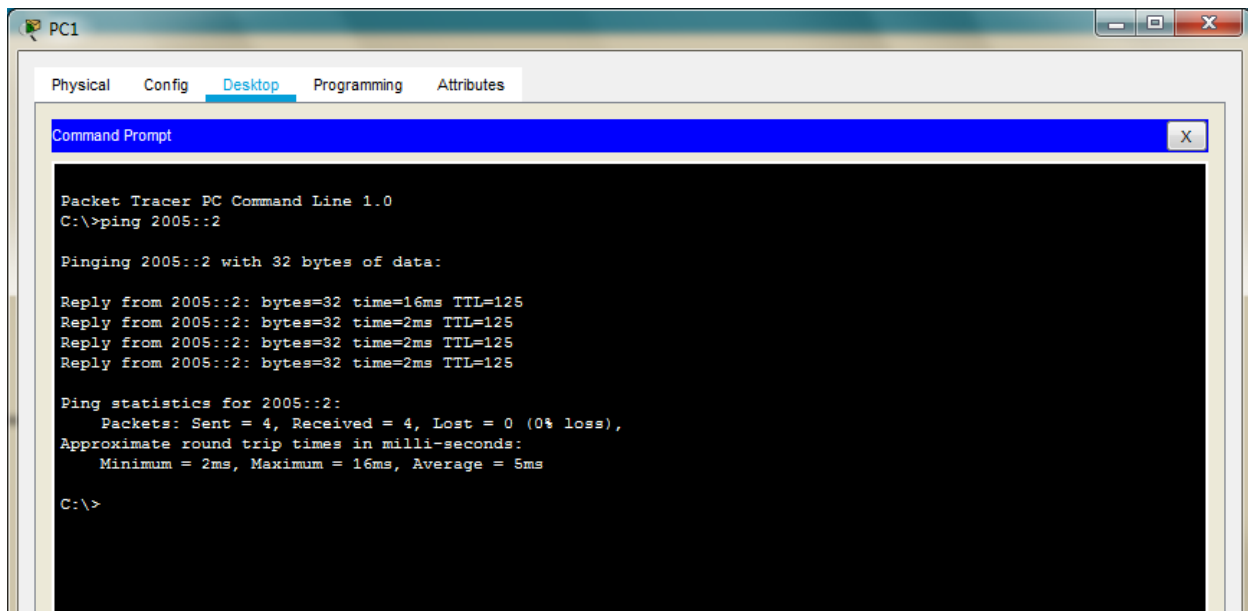
```
Router>enable
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#
```

```
Router(config)#interface Serial0/1/1
Router(config-if)#ipv6 address 2004::2/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
```

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ipv6 address 2005::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Check the connectivity by pinging from PCs to Server





And we see that the connectivity is established

We configure the ACL and apply it to the Router1 with the following conditions

- 1) No HTTP or HTTPS allowed on server by any host
- 2) No www service accessible on the server by any host
- 3) Only ipv6 packets allowed towards the server

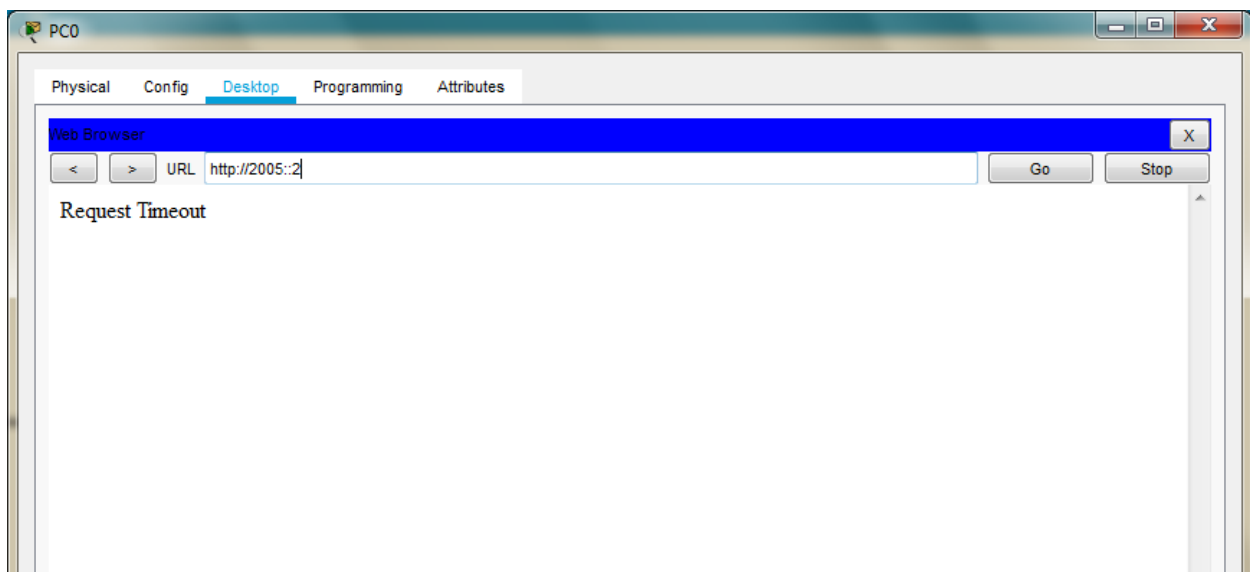
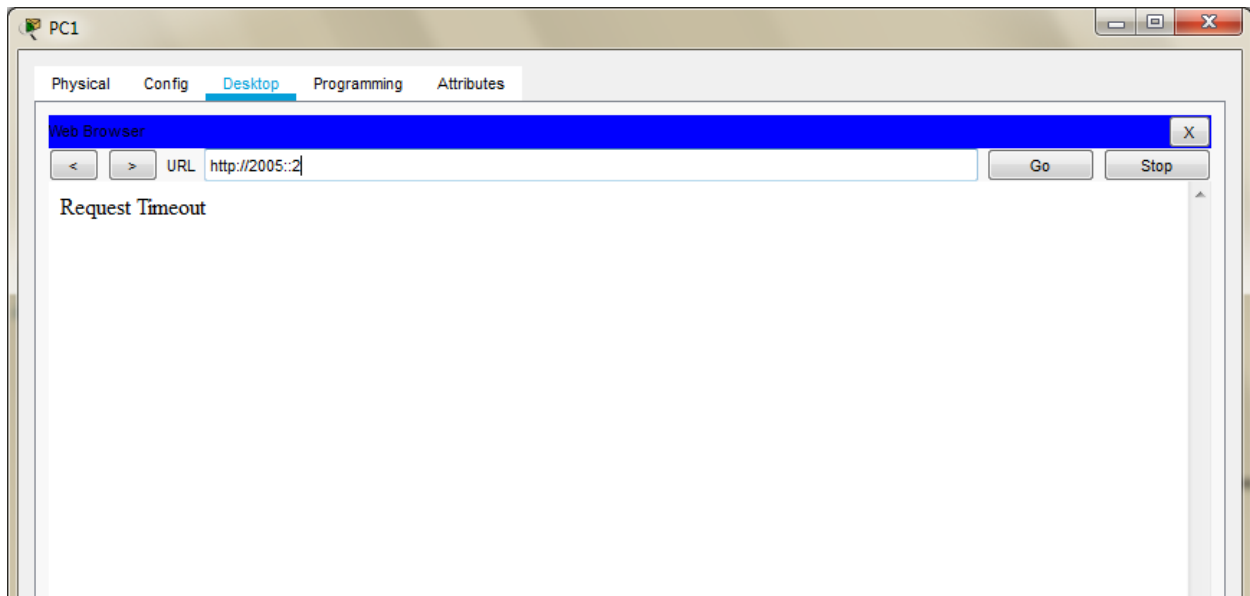
We enter the following commands in the CLI mode of the Router1 and apply it at the proper interface

```
Router>
Router>enable
Router#configure terminal
Router(config)#ipv6 access-list smile
Router(config-ipv6-acl)#deny tcp any host 2005::2 eq www
Router(config-ipv6-acl)#deny tcp any host 2005::2 eq 443
Router(config-ipv6-acl)#permit ipv6 any any
Router(config-ipv6-acl)#
Router(config-ipv6-acl)#exit

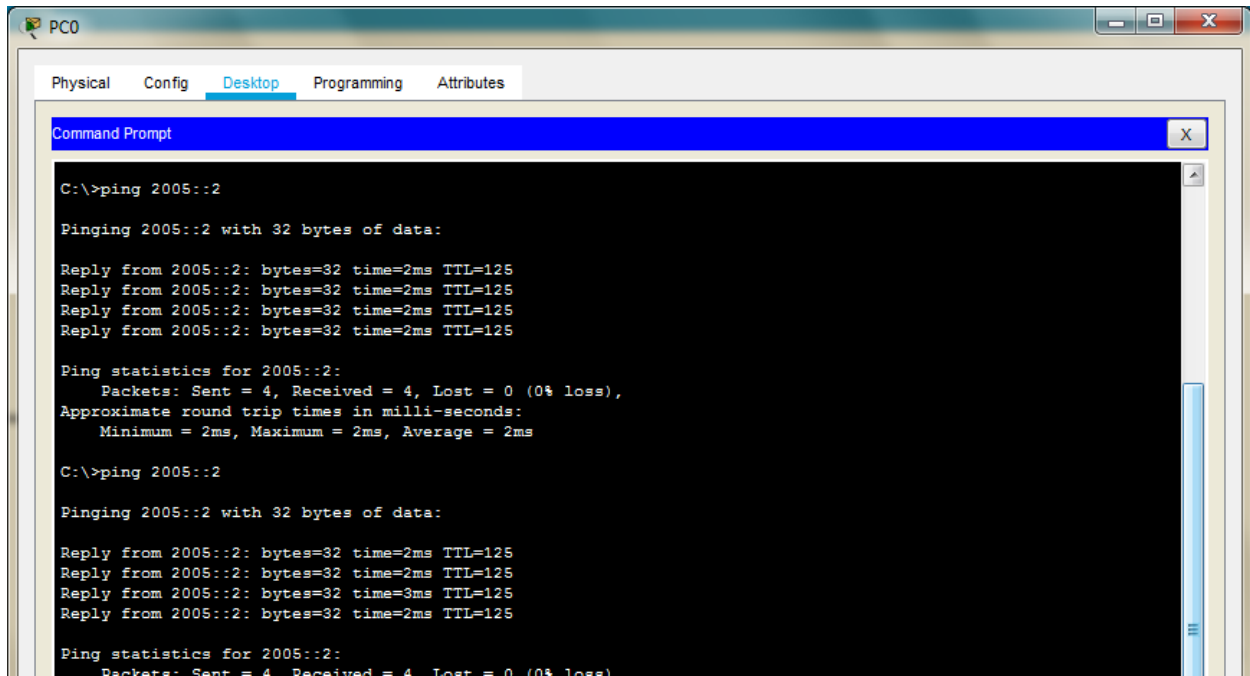
Router(config)#
Router(config)#interface Serial0/1/1
Router(config-if)#ipv6 traffic-filter smile in
```

```
Router(config-if)#exit  
Router(config)#
```

We verify the configuration by first accessing the www service from the browser of both PCs and get failure



Next we verify whether the ipv6 protocol works by pinging server from any of the PC (it must be successful)



The screenshot shows a network simulation window for PC0. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows two successful ping operations to the IPv6 address 2005::2. Each operation consists of four replies, each with 32 bytes of data, a time of 2ms or 3ms, and a TTL of 125. The ping statistics for both operations show 4 packets sent, 4 received, and 0% loss.

```
C:\>ping 2005::2

Pinging 2005::2 with 32 bytes of data:

Reply from 2005::2: bytes=32 time=2ms TTL=125
Reply from 2005::2: bytes=32 time=2ms TTL=125
Reply from 2005::2: bytes=32 time=2ms TTL=125
Reply from 2005::2: bytes=32 time=2ms TTL=125

Ping statistics for 2005::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\>ping 2005::2

Pinging 2005::2 with 32 bytes of data:

Reply from 2005::2: bytes=32 time=2ms TTL=125
Reply from 2005::2: bytes=32 time=2ms TTL=125
Reply from 2005::2: bytes=32 time=3ms TTL=125
Reply from 2005::2: bytes=32 time=2ms TTL=125

Ping statistics for 2005::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Hence the given ACLs have been applied and verified on host running on ipv6 protocol