Configure IPv6-based Access Control List (ACL) and Access Control Entry (ACE) on a Switch

Objective

An Access Control List (ACL) is a list of network traffic filters and correlated actions used to improve security. It blocks or allows users to access specific resources. An ACL contains the hosts that are permitted or denied access to the network device.

The typical ACL functionality in IPv6 is similar to ACLs in IPv4. ACLs determine which traffic to block and which traffic to forward at switch interfaces. ACLs allow filtering based upon source and destination addresses, inbound and outbound to specific interfaces. Each ACL has an implicit deny statement at the end. The rules for the ACLs are configured in the Access Control Entries (ACEs).

You should use access lists to provide a basic level of security for accessing your network. If you do not configure access lists on your network devices, all packets passing through the switch or router could be allowed onto all parts of your network.

This article provides instructions on how to configure IPv6-based ACL and ACE on a switch.

Applicable Devices

- Sx350 Series
- SG350X Series
- Sx500 Series
- Sx550X Series

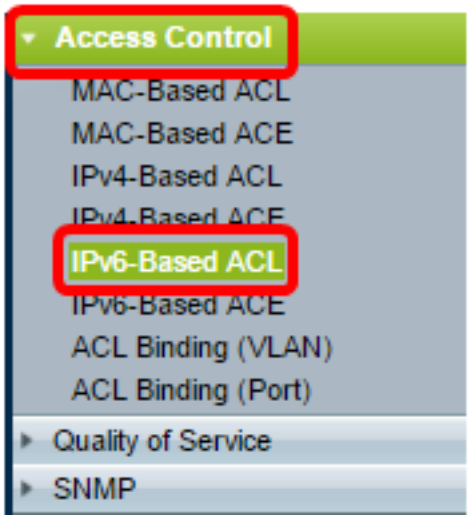
Software Version

- 1.4.5.02 – Sx500 Series
- 2.2.5.68 – Sx350 Series, SG350X Series, Sx550X Series

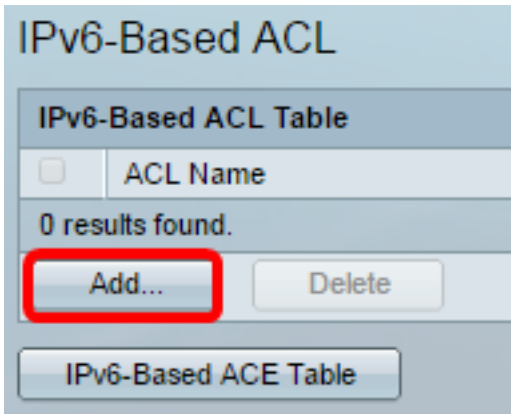
Configure IPv6-Based ACL and ACE

Configure IPv6-Based ACL

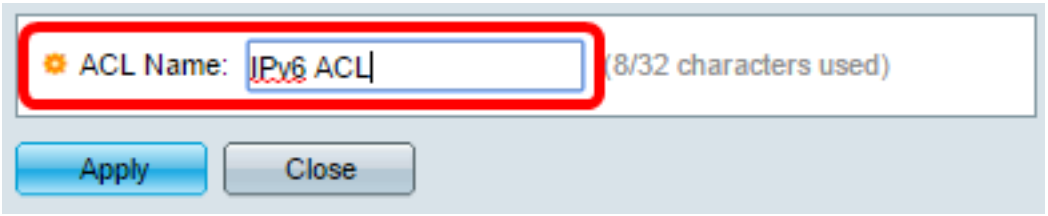
Step 1. Log in to the web-based utility then go to **Access Control > IPv6-Based ACL**.



Step 2. Click the **Add** button.

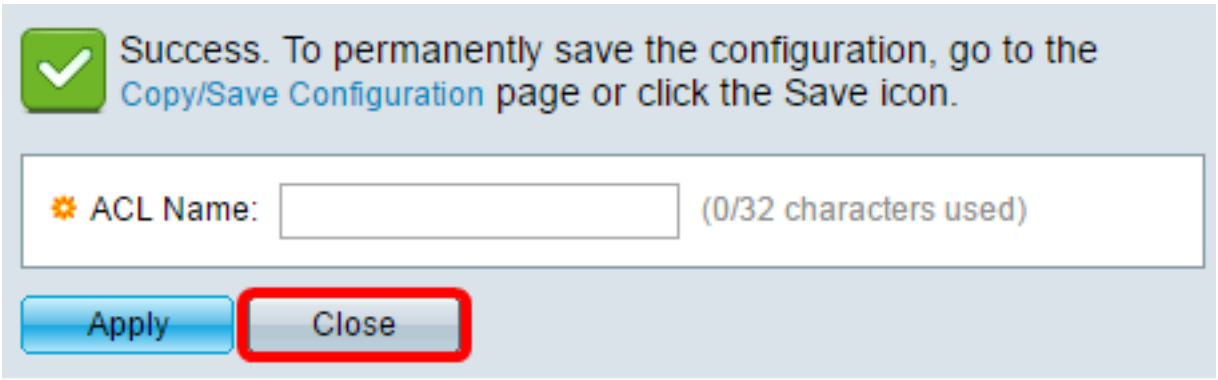


Step 3. Enter the name of the new ACL in the *ACL Name* field.



Note: In this example, IPv6 ACL is used.

Step 4. Click **Apply** then click **Close**.



Step 5. (Optional) Click **Save** to save settings in the startup configuration file.

You should now have configured an IPv6-based ACL on your switch.

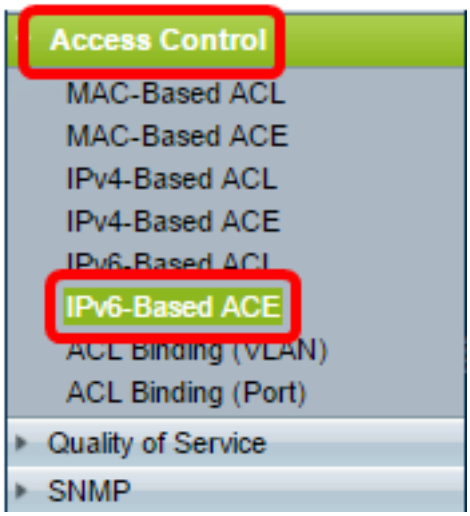
Configure IPv6-Based ACE

When a packet is received on a port, the switch processes the frame through the first ACL. If the packet matches an ACE filter of the first ACL, the ACE action takes place. If the packet matches none of the ACE filters, the next ACL is processed. If no match is found to any ACE in all relevant ACLs, the packet is dropped by default.

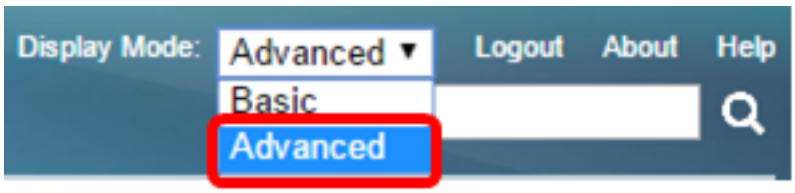
In this scenario, an ACE will be created to deny traffic that is sent from a specific user-defined source IPv6 address to any destination addresses.

Note: This default action can be avoided by the creation of a low priority ACE that permits all traffic.

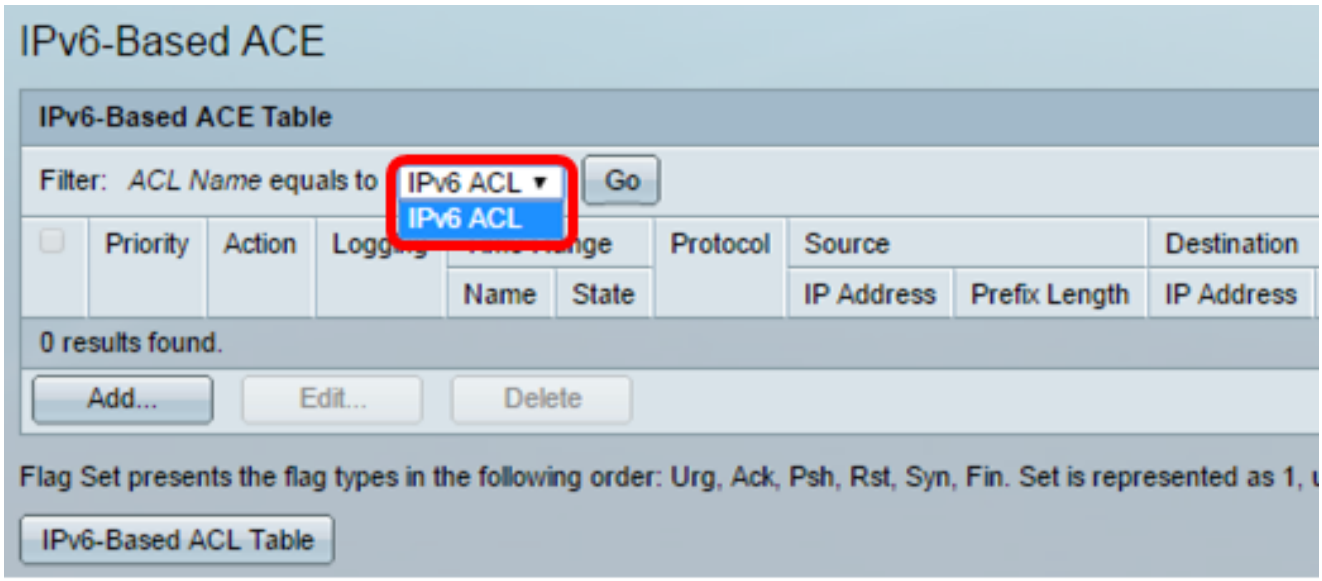
Step 1. On the web-based utility, go to **Access Control > IPv6-Based ACE**.



Important: If you have an Sx350, SG350X, Sx550X switch, change to Advanced mode by choosing **Advanced** from the Display Mode drop-down list in the upper-right corner of the page.

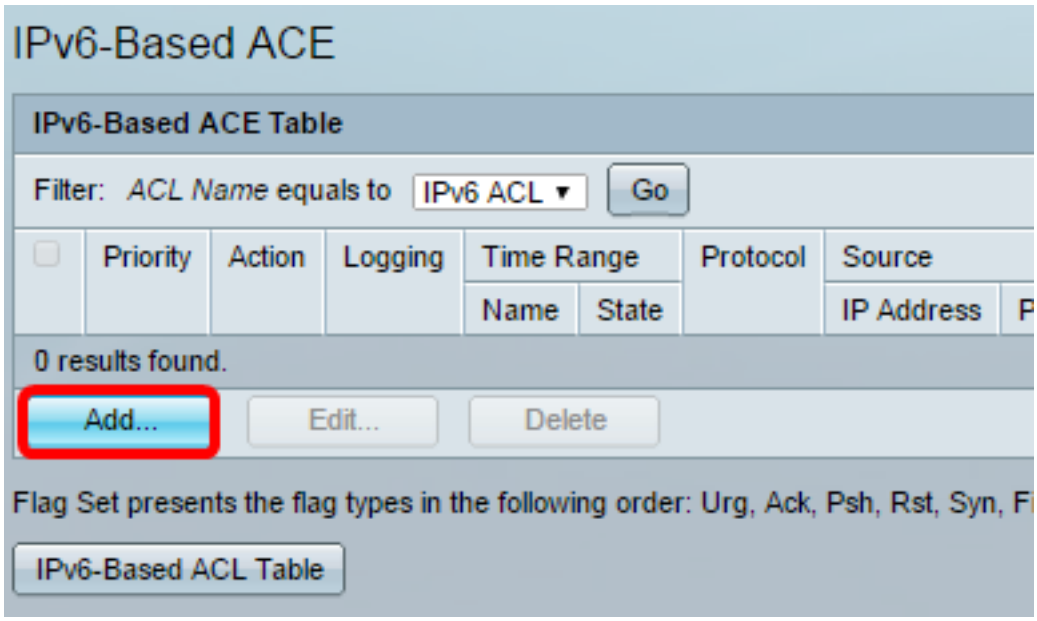


Step 2. Choose an ACL from the ACL Name drop-down list then click **Go**.



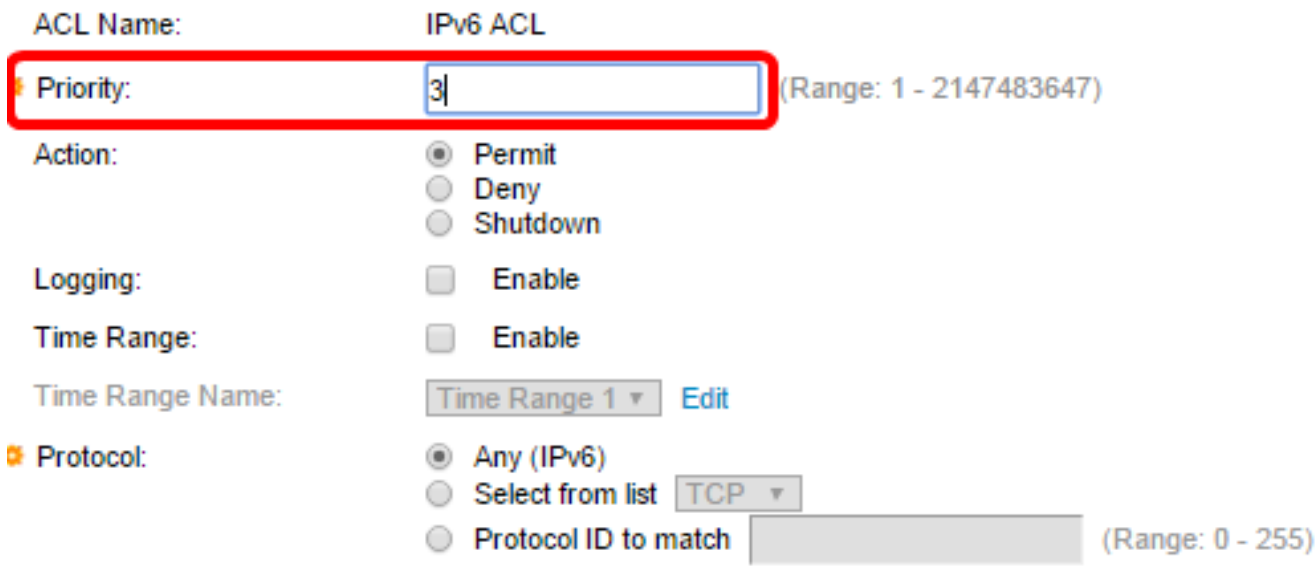
Note: The ACEs that are already configured for the ACL will be displayed in the table.

Step 3. Click the **Add** button to add a new rule to the ACL.



Note: The *ACL Name* field displays the name of the ACL.

Step 4. Enter the priority value for the ACE in the *Priority* field. ACEs with a higher priority value are processed first. The value 1 is the highest priority. It has a range of 1 to 2147483647.



Note: In this example, 3 is used.

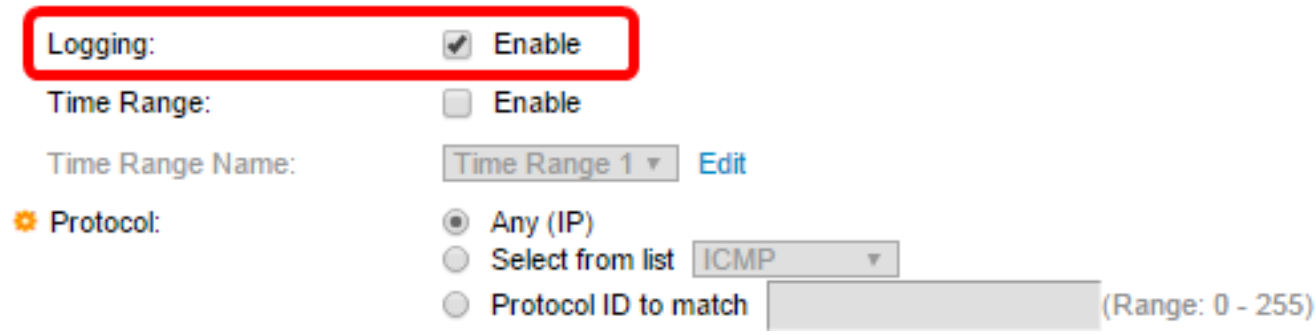
Step 5. Click the radio button that corresponds to the desired action that is taken when a frame meets the required criteria of the ACE.

Note: In this example, Permit is chosen.

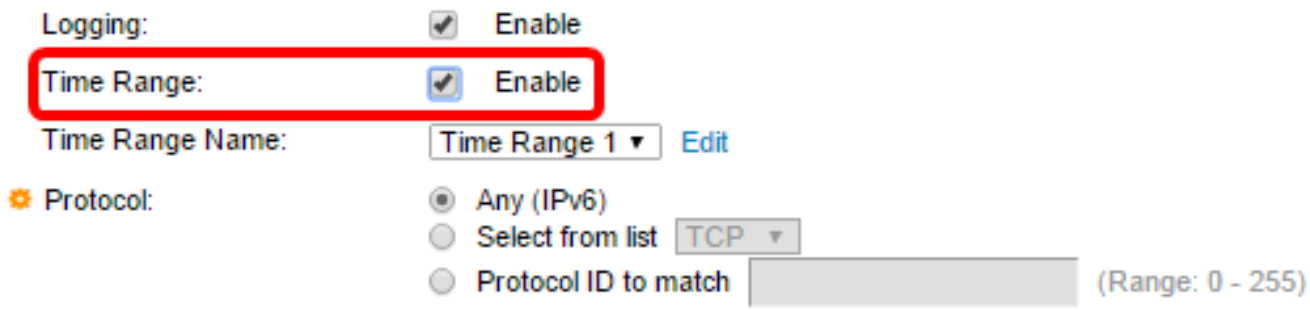
- Permit — The switch forwards packets that meet the required criteria of the ACE.
- Deny — The switch drops packets that meet the required criteria of the ACE.

Shutdown — The switch drops packets that do not meet the required criteria of the ACE and disables the port where the packets were received. Disabled ports can be reactivated on the Port Settings page.

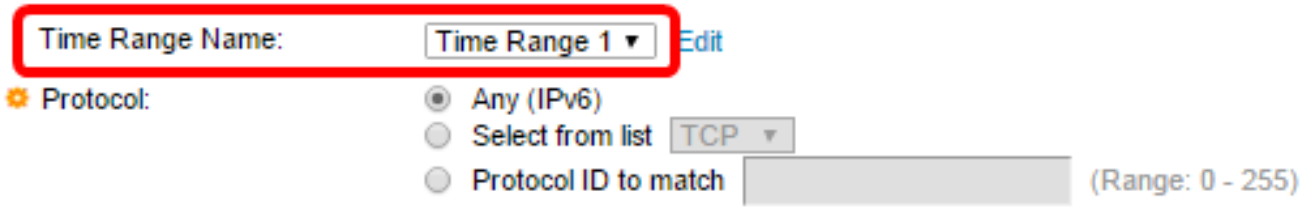
Step 6. (Optional) Check the **Enable** Logging check box to enable logging ACL flows that match the ACL rule.



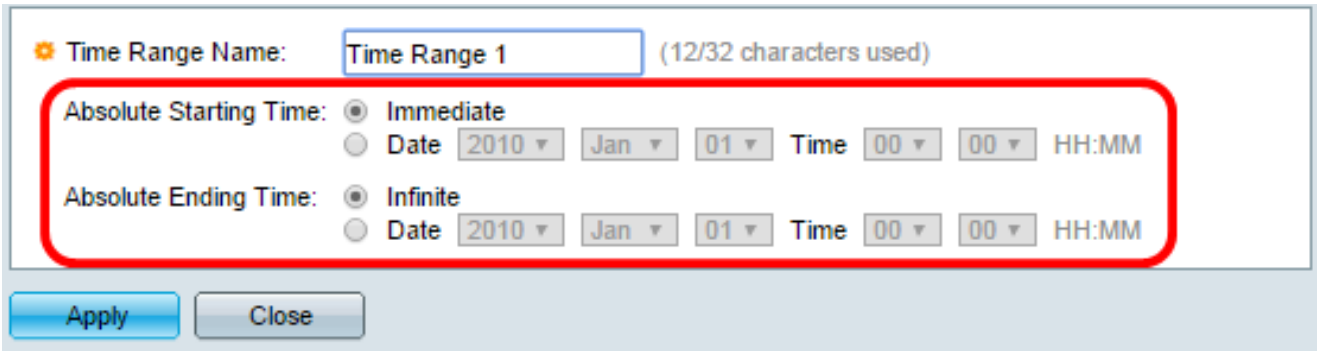
Step 7. (Optional) Check the **Enable** Time Range check box to allow a time range to be configured to the ACE. Time ranges are used to limit the amount of time an ACE is in effect. If this is left disabled, the ACE works at any time.



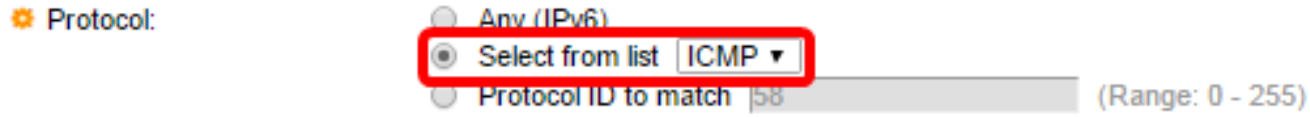
Step 8. (Optional) From the Time Range Name drop-down list, choose a time range to apply to the ACE.



Note: You can click **Edit** to navigate and create a time range on the Time Range page.



Step 9. Choose a protocol type in the Protocol area. The ACE will be created based on a specific protocol or protocol ID.

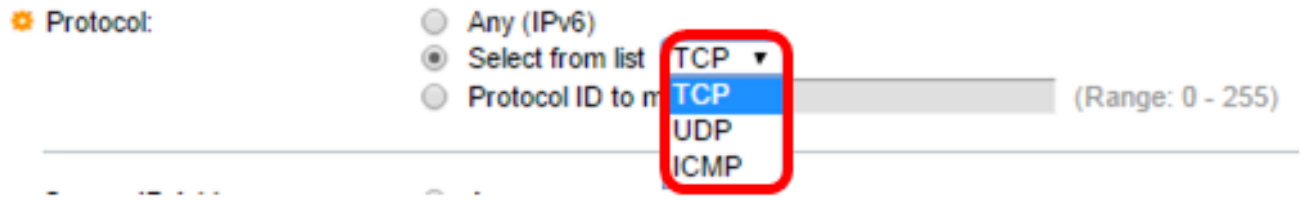


The options are:

- Any (IP) — This option will configure the ACE to accept all IP protocols.
- Select from list — This option will allow you to choose a protocol from a drop-down list. If you prefer this option, skip to Step 10.
- Protocol ID to match — This option will allow you to enter a protocol ID. If you prefer this option, skip to Step 11.

Note: In this example, Select from list is chosen.

Step 10. (Optional) If you chose Select from list in Step 9, choose a protocol from the drop-down list.

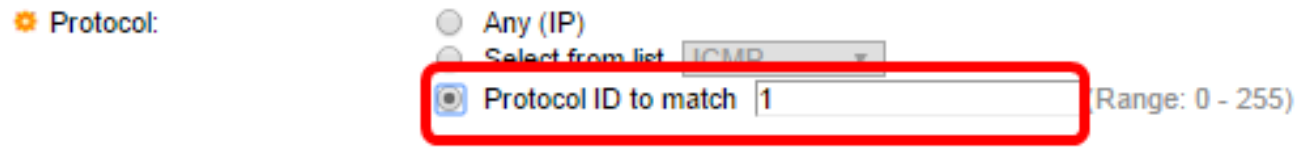


The options are:

- TCP — Transmission Control Protocol (TCP) enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees that packets are transmitted and received in the order they were sent.
- UDP — User Datagram Protocol (UDP) transmits packets but does not guarantee their delivery.
- ICMP — Matches packets to the Internet Control Message Protocol (ICMP).

Note: In this example, TCP is used.

Step 11. (Optional) If you chose Protocol ID to match in Step 9, enter the protocol ID in the *Protocol ID to match* field.



Note: In this example, 1 is used.

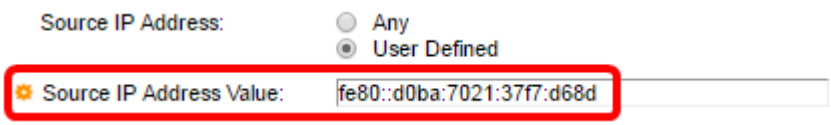
Step 12. Click the radio button that corresponds to the desired criteria of the ACE in the Source IP Address area.

The options are:

- Any — All source IPv6 addresses apply to the ACE.
- User Defined — Enter an IP address and IP wildcard mask that are to be applied to the ACE in the *Source IP Address Value* and *Source IP Prefix Length* fields.

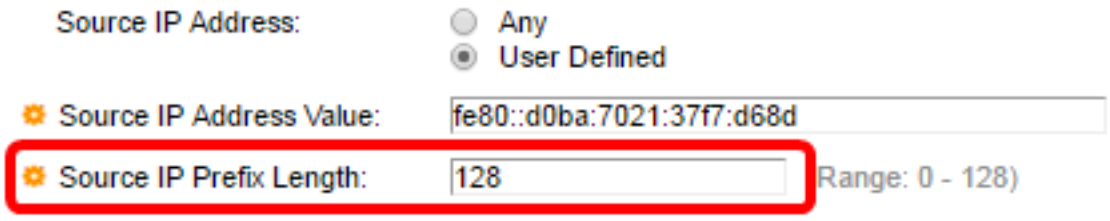
Note: In this example, User Defined is chosen. If you chose Any, skip to Step 15.

Step 13. Enter the source IP address in the *Source IP Address Value* field.



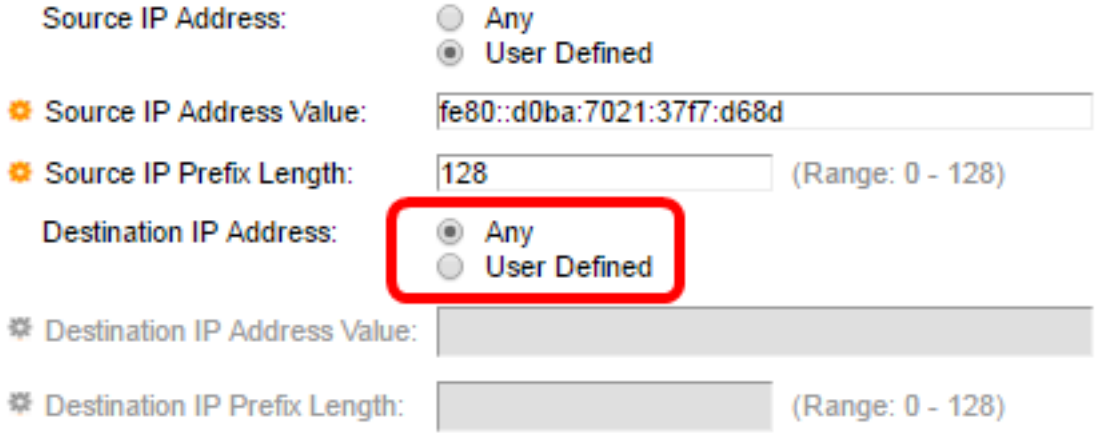
Note: In this example, fe80::d0ba:7021:37f7:d68d is used.

Step 14. Enter the source IP prefix length in the *Source IP Prefix Length* field.



Note: In this example, 128 is used.

Step 15. Click the radio button that corresponds to the desired criteria of the ACE in the DestinationIP Address area.

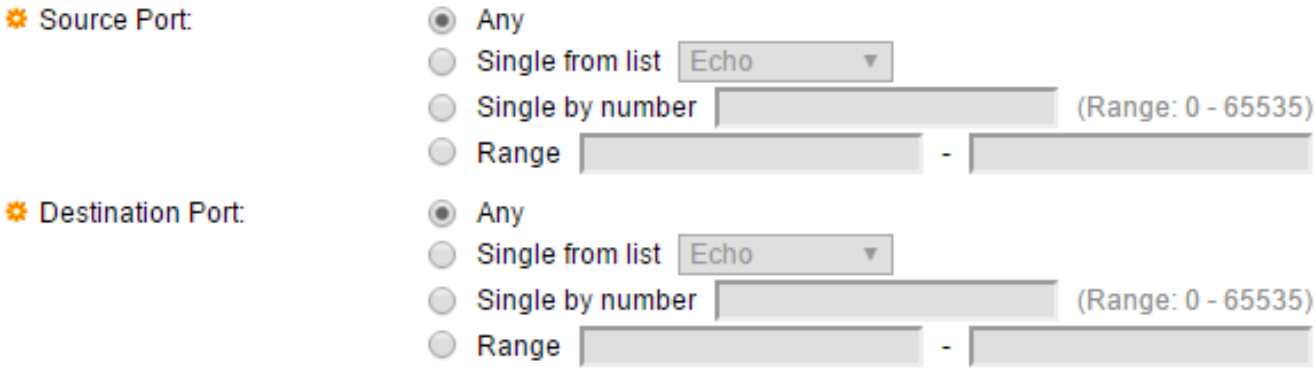


The options are:

- Any — All destination IPv6 addresses apply to the ACE.
- User Defined — Enter an IP address and IP wildcard mask that are to be applied to the ACE in the *Destination IP Address Value* and *Destination IPPrefix Length* fields.

Note: In this example, Any is chosen. Choosing this option means that the ACE to be created will permit the ACE traffic coming from the specified IPv6 address to any destination.

Step 16. (Optional) Click a radio button in theSource Port area. The default value is Any.



- Any — Match to all source ports.
- Single from list — You can choose a single TCP/UDP source port to which packets are matched. This field is active only if 800/6-TCP or 800/17-UDP is chosen in the Select from List drop-down menu.
- Single by number — You can choose a single TCP/UDP source port to which packets are matched. This field is active only if 800/6-TCP or 800/17-UDP is chosen in the Select from List drop-down menu.

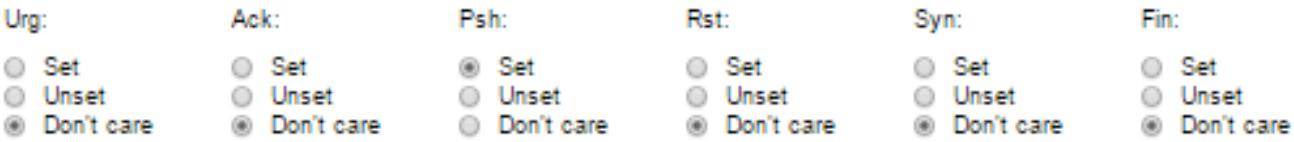
- Range — You can choose a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.

Step 17. (Optional) Click a radio button in theDestination Port area. The default value is Any.

- Any — Match to all source ports
- Single from list — You can choose a single TCP/UDP source port to which packets are matched. This field is active only if 800/6-TCP or 800/17-UDP is chosen in the Select from List drop-down menu.
- Single by number — You can choose a single TCP/UDP source port to which packets are matched. This field is active only if 800/6-TCP or 800/17-UDP is chosen in the Select from List drop-down menu.
- Range — You can choose a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.

Step 18. (Optional) In the TCP Flags area, choose one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security.

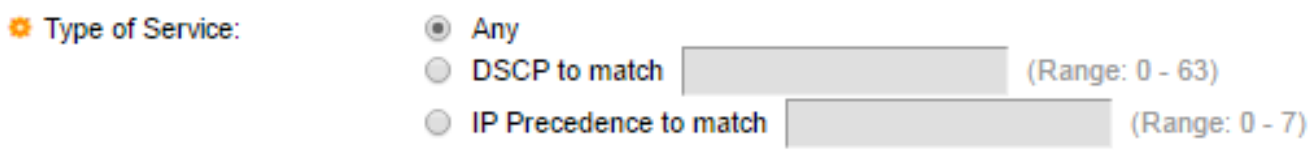
- Set — Match if the flag is set.
- Unset — Match if the flag is not set.
- Don’t care — Ignore the TCP flag.



The TCP flags are:

- Urg — This flag is used to identify incoming data as Urgent.
- Ack — This flag is used to acknowledge the successful receipt of packets.
- Psh — This flag is used to ensure that the data is given the priority (that it deserves) and is processed at the sending or receiving end.
- Rst — This flag is used when a segment arrives that is not intended for the current connection.
- Syn — This flag is used for TCP communications.
- Fin — This flag is used when the communication or data transfer is Finished.

Step 19. (Optional) Click the service type of the IP packet from the Type of Service area.



The options are:

- Any — It can be any type of service for traffic congestion.
- DSCP to Match — Differentiated Services Code Point is a mechanism for classifying and

managing network traffic. Six bits (0-63) is used to select the Per Hop Behavior a packet experiences at each node.

- IP Precedence to match — IP precedence is a model of Type of Service (TOS) that the network uses to help provide the appropriate Quality of Service (QoS) commitments. This model uses the three most significant bits of the service type byte in the IP header, as described in RFC 791 and RFC 1349. The keyword with IP Preference values are the following:

  – 0 — for routine

  – 1 — for priority

  – 2 — for immediate

  – 3 — for flash

  – 4 — for flash-override

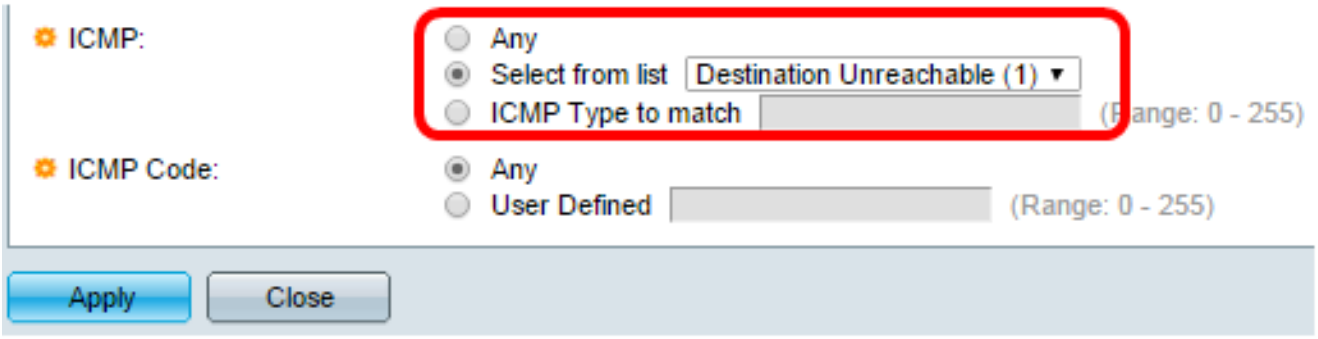
  – 5 — for critical

  – 6 — for internet

  – 7 — for network

Note: In this example, Any is chosen.

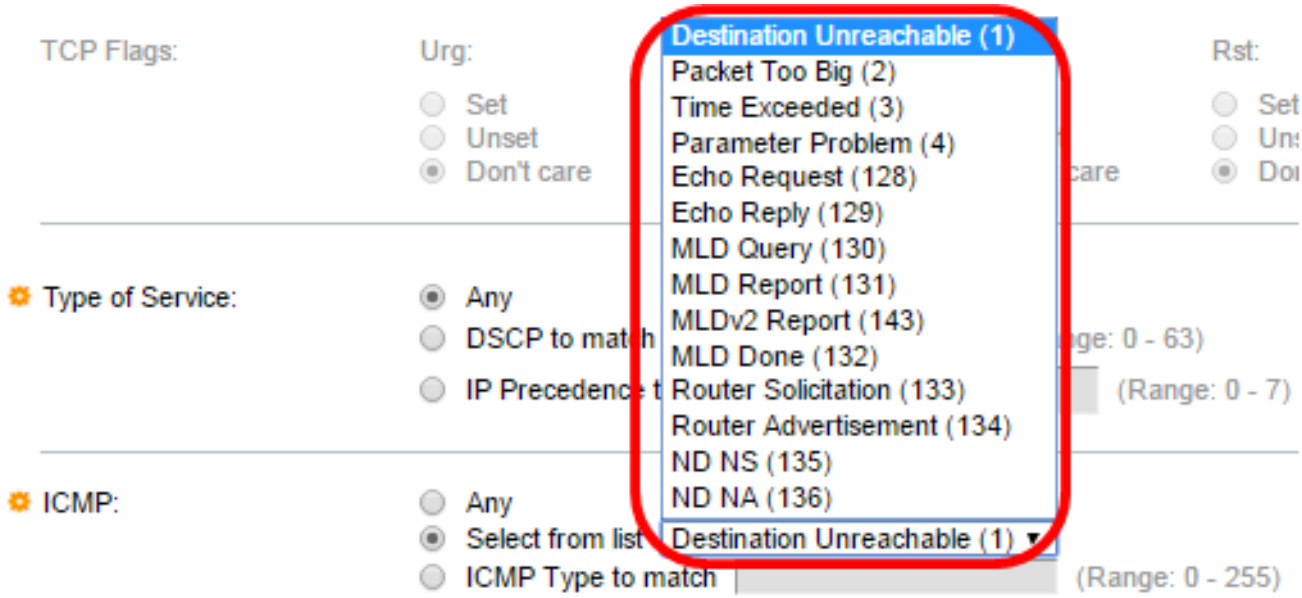
Step 20. (Optional) If the IP protocol of the ACL is ICMP, click the ICMP message type used for filtering purposes. Either choose the message type by name or enter the message type number:



- Any — All message types are accepted.
- Select from list — You can choose message type by name.
- ICMP Type to match — The number of message type to be used for filtering purposes.

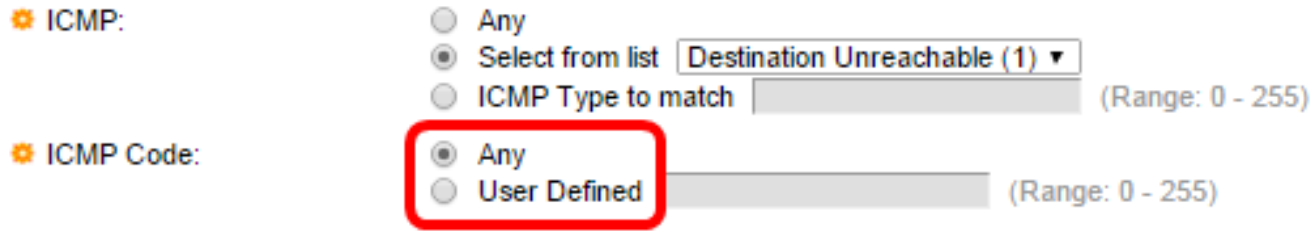
Note: In this example, Select from list is chosen.

Step 21. (Optional) If Select from list is chosen in Step 20, choose the control messages to filter from the possible options in the drop-down list:



- Destination Unreachable (1) — It is generated by the host or its gateway to inform the client that the destination is unreachable for some reason (Example: Network or Host unreachable error).
- Packet Too Big (2) — The size of the Datagram exceeds the given MTU.
- Time Exceeded (3) — It is generated by a gateway to inform the source of a discarded datagram due to the time to live field reaching zero.
- Parameter Problem (4) — It is generated as a response for any error not specifically covered by another ICMP message.
- Echo Request (128) — It is a ping, whose data is expected to be received back in an echo reply.
- Echo Reply (129) — It is generated in response to an echo request.
- MLD Query (130) — It is used to learn which multicast addresses have listeners on an attached link. Type 130 in decimal.
- MLD Report (131) — It is generated when IPv6 multicast address to which the message sender listens.
- MLD v2 Report (143) — It is same as MLD Report with version 2.
- MLD Done (132) — When the host leaves a group, it sends a multicast listener done message to multicast routers on the network.
- Router Solicitation (133) — It is a router discovery message. Hosts discover the addresses of their neighboring routers simply when they listen for advertisements. Default is 224.0.0.2 for multicast, otherwise it is 255.255.255.255.
- Router Advertisement (134) — The router periodically multicasts a Router Advertisement from each of its multicast interfaces, and announces the IP addresses of that interface.
- ND NS (135) — Messages are originated by nodes to request another node's link layer address and also for functions such as duplicate address detection and neighbor unreachability detection.
- ND NA (136) — Messages are sent in response to NS messages. If a node changes its link-layer address, it can send an unsolicited NA to advertise the new address.

Step 22. (Optional) The ICMP messages can have a code field that indicates how to handle the message. This is enabled if you choose the ICMP protocol in Step 10. Click one of the following options to configure whether to filter on this code:

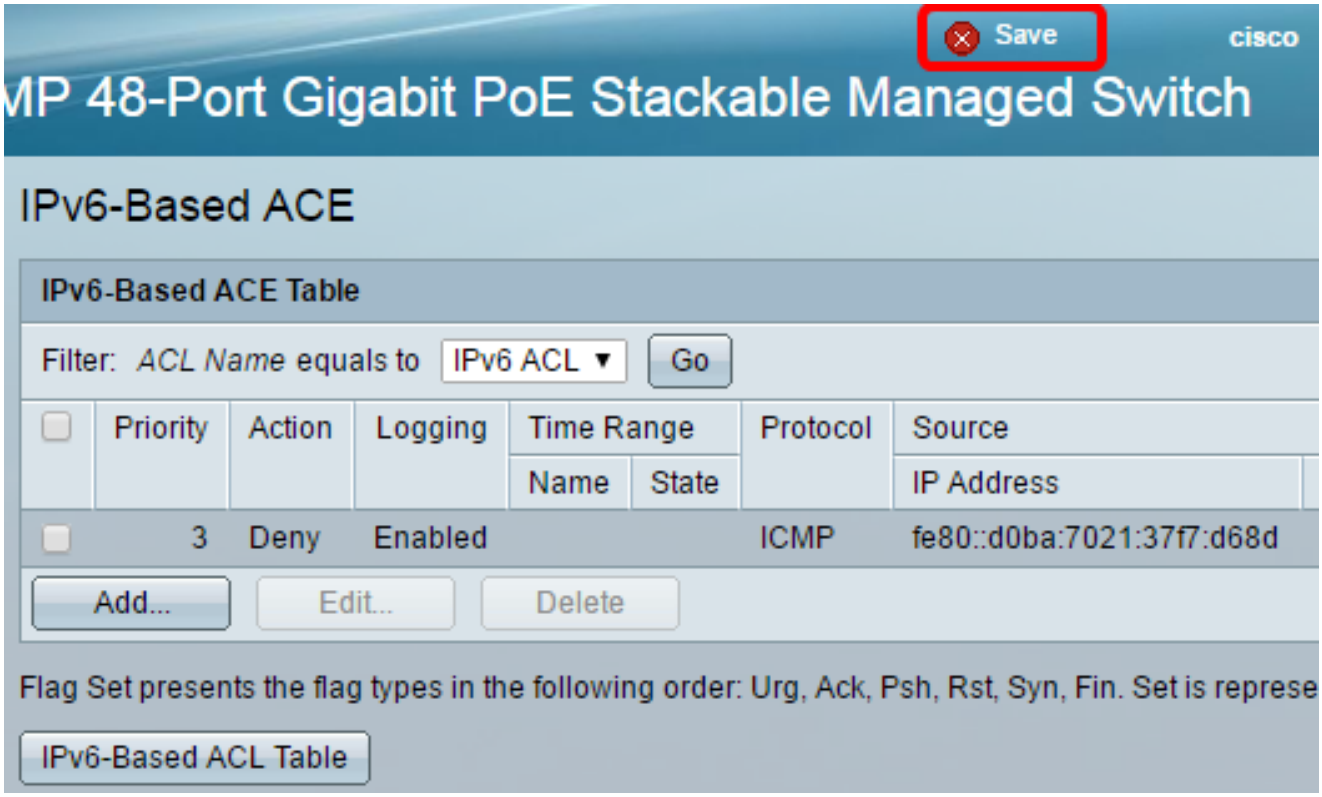


- Any — Accept all codes.
- User Defined — You can enter an ICMP code for filtering purposes.

Note: In this example, Any is chosen.

Step 23. Click **Apply** then click **Close**. The ACE is created and associated to the ACL name.

Step 24. Click **Save** to save settings to the startup configuration file.



You should now have configured an IPv6-based ACE on your switch.