Configure IPv4-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 IPv4-based ACL is a list of source IPv4 addresses that use Layer 3 information to permit or deny access to traffic. IPv4 ACLs restrict IP-related traffic based on the configured IP filters. A filter contains the rules to match an IP packet, and if the packet matches, the rule also stipulates if the packet should be permitted or denied.

An Access Control Entry (ACE) contains the actual access rule criteria. Once the ACE is created, it is applied to an ACL.

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 IPv4-based ACL and ACE on your managed switch.

Applicable Devices

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

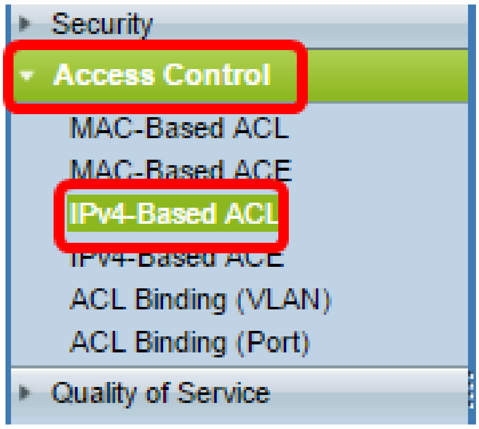
Software Version

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

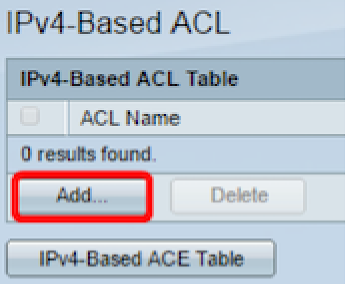
Configure IPv4-Based ACL and ACE

Configure IPv4-Based ACL

Step 1. Log in to the web-based utility then go to **Access Control > IPv4-Based ACL**.



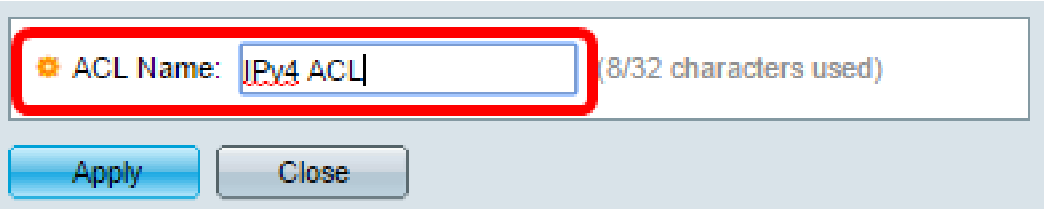
Step 2. Click the **Add** button.


IPv4-Based ACL

IPv4-Based ACL Table

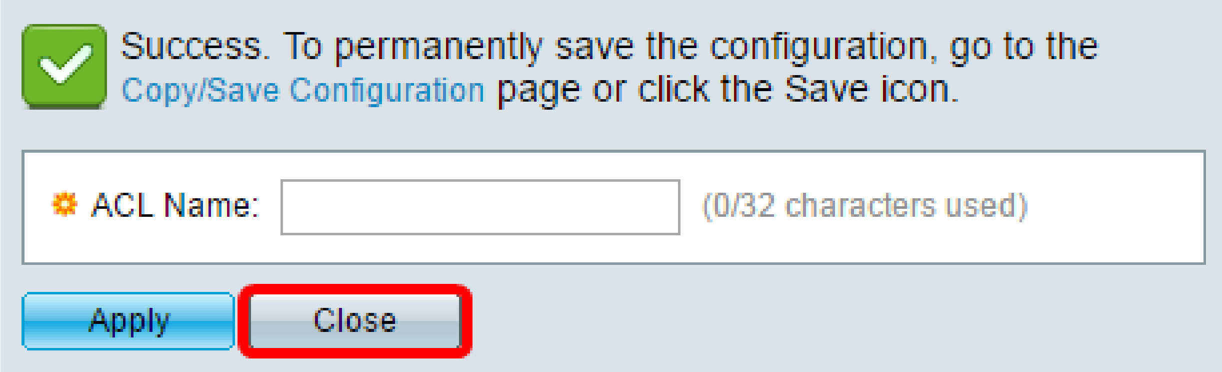
□	ACL Name
0 results found.	

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


ACL Name: IPv4 ACL (8/32 characters used)

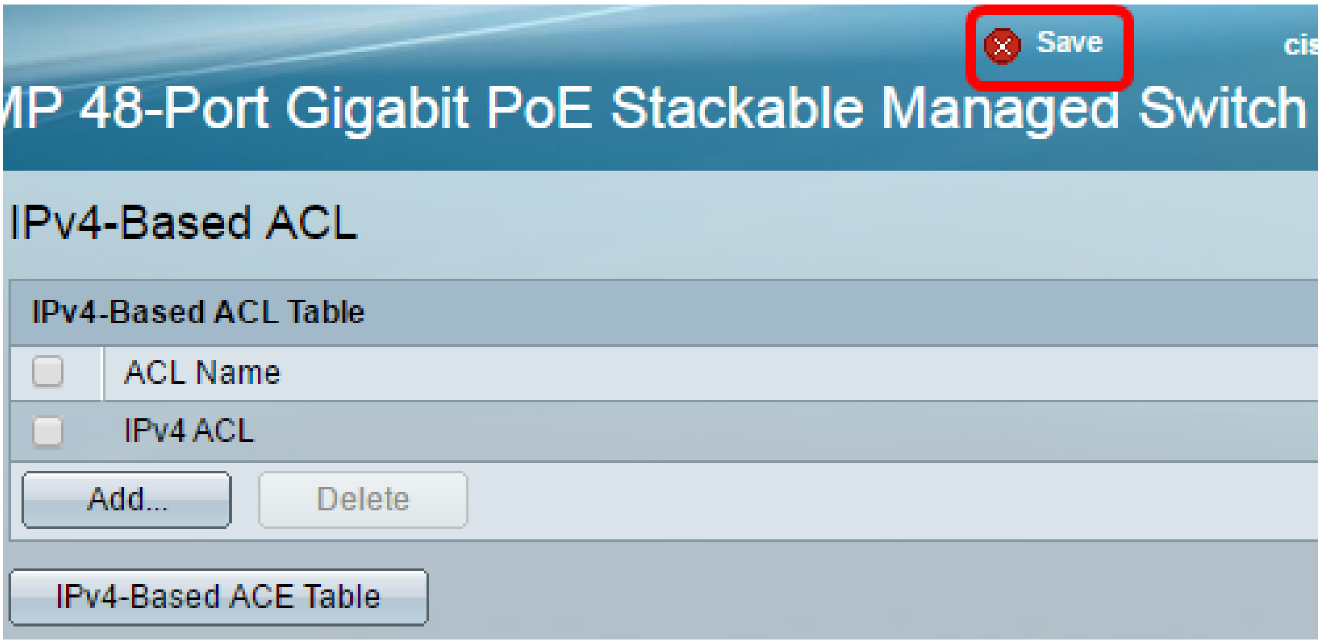
Note: In this example, IPv4 ACL is used.

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


Success. To permanently save the configuration, go to the Copy/Save Configuration page or click the Save icon.

ACL Name: (0/32 characters used)

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



You should now have configured an IPv4-based ACL on your switch.

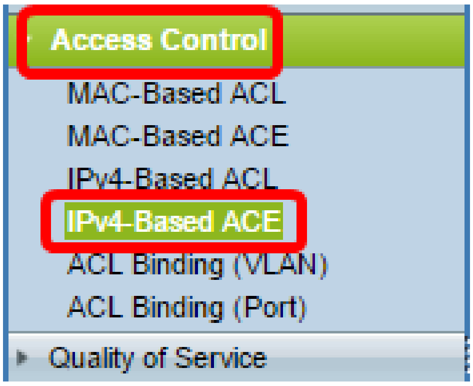
Configure IPv4-Based ACE

When a packet is received on a port, the switch processes the packet 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.

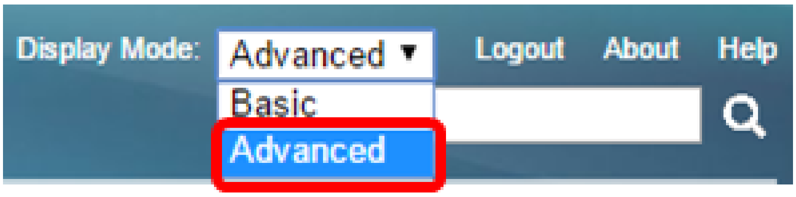
In this scenario, an ACE will be created to deny traffic that is sent from a specific user-defined source IPv4 address to any destination addresses.

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

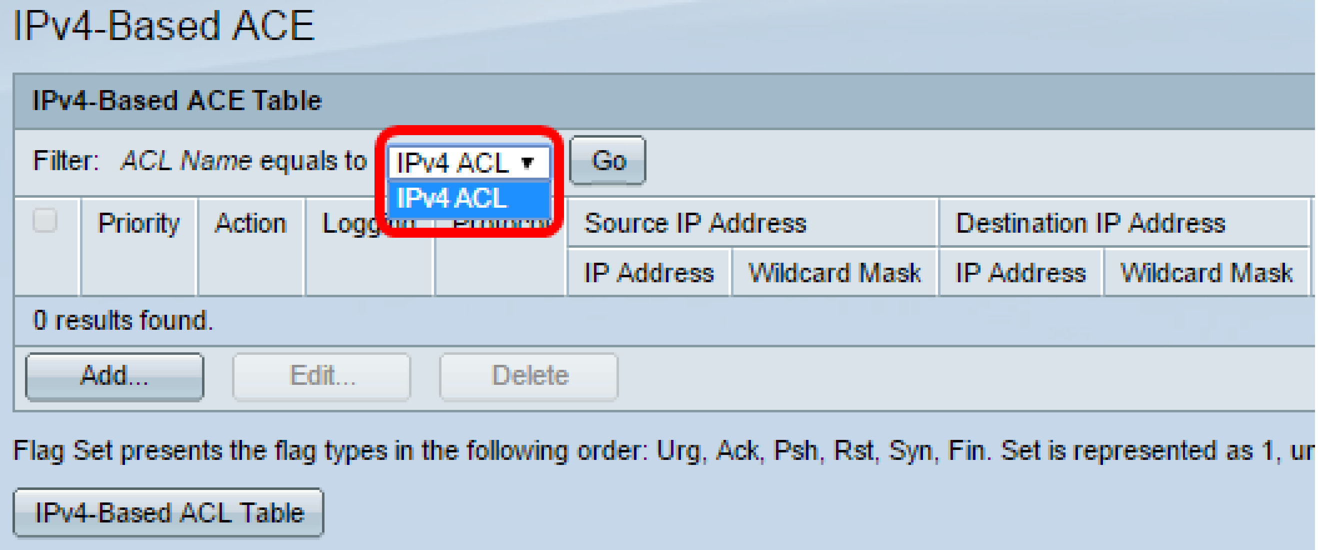
Step 1. On the web-based utility, go to **Access Control > IPv4-Based ACE**.



Important: To fully utilize the available features and functions of the 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**.



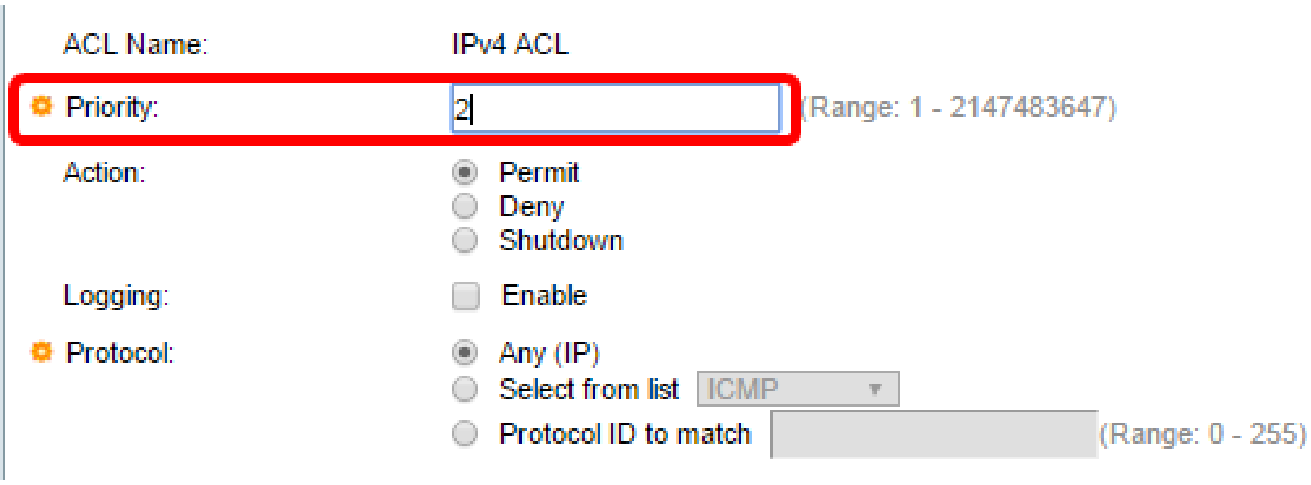
Flag Set presents the flag types in the following order: Urg, Ack, Psh, Rst, Syn, Fin. Set is represented as 1, ur

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.



ACL Name: IPv4 ACL

Priority: 2 (Range: 1 - 2147483647)

Action: ● Permit ○ Deny ○ Shutdown

Logging: □ Enable

Protocol: ● Any (IP) ○ Select from list ICMP ▾ ○ Protocol ID to match (Range: 0 - 255)

Note: In this example, 2 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.

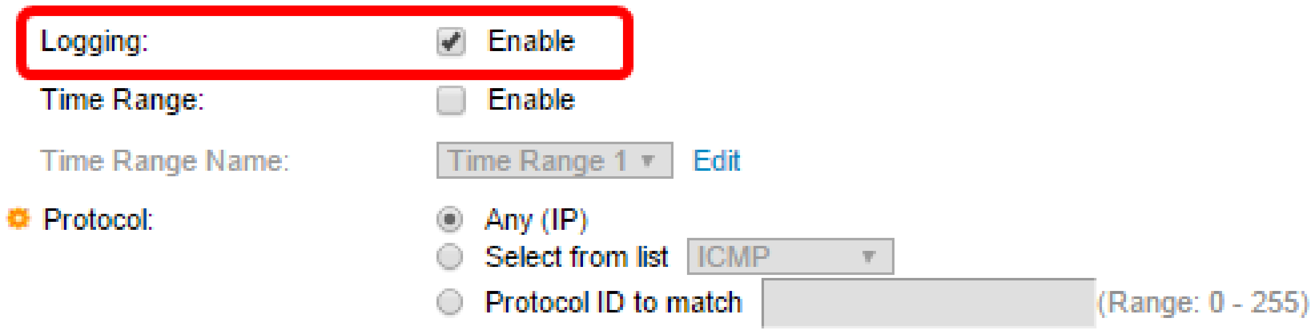
Note: In this example, Permit is chosen.

- 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.

Note: Disabled ports can be reactivated on the Port Settings page.

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



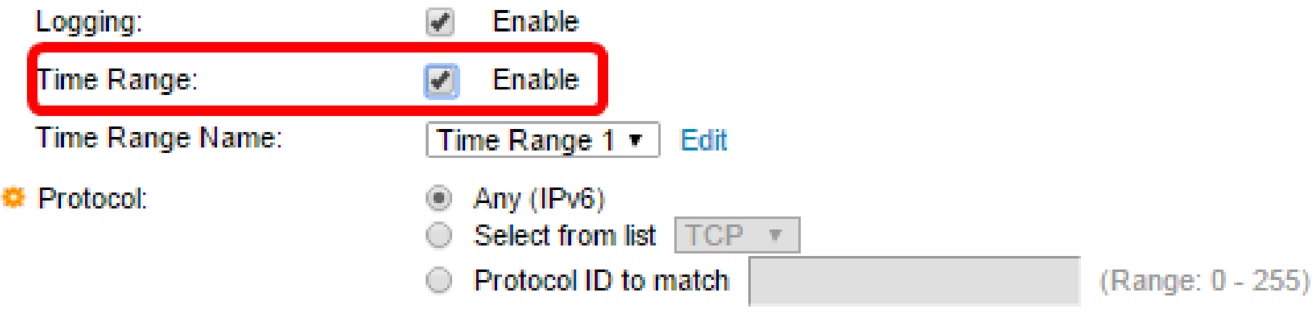
Logging: ☑ Enable

Time Range: □ Enable

Time Range Name: Time Range 1 ▾ Edit

Protocol: ● Any (IP)
○ Select from list ICMP ▾
○ Protocol ID to match (Range: 0 - 255)

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.



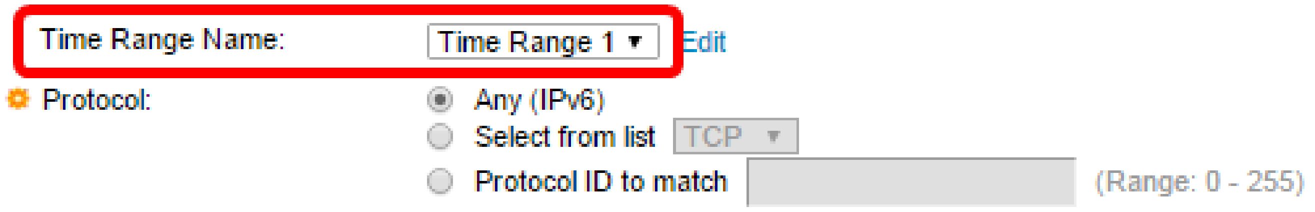
Logging: ☑ Enable

Time Range: ☑ Enable

Time Range Name: Time Range 1 ▾ Edit

Protocol: ● Any (IPv6)
○ Select from list TCP ▾
○ Protocol ID to match (Range: 0 - 255)

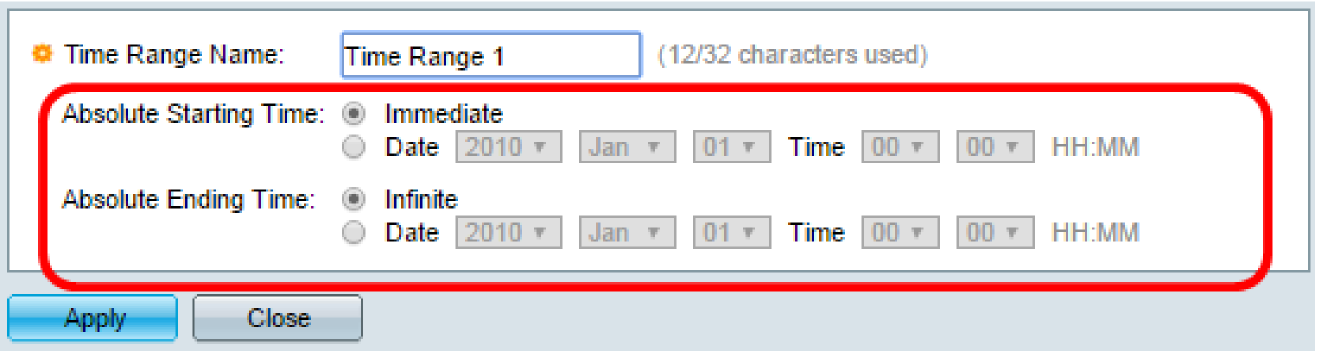
Step 8. (Optional) From the Time Range Name drop-down list, choose a time range to apply to the ACE.



Time Range Name: Time Range 1 ▾ Edit

Protocol: ● Any (IPv6)
○ Select from list TCP ▾
○ Protocol ID to match (Range: 0 - 255)

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

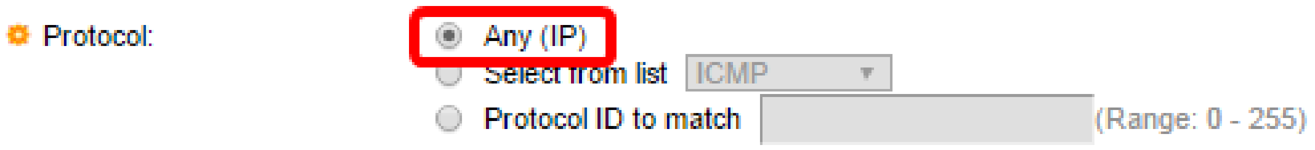


Time Range Name: Time Range 1 (12/32 characters used)

Absolute Starting Time: ● Immediate
○ Date 2010 ▾ Jan ▾ 01 ▾ Time 00 ▾ 00 ▾ HH:MM

Absolute Ending Time: ● Infinite
○ Date 2010 ▾ Jan ▾ 01 ▾ Time 00 ▾ 00 ▾ HH:MM

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



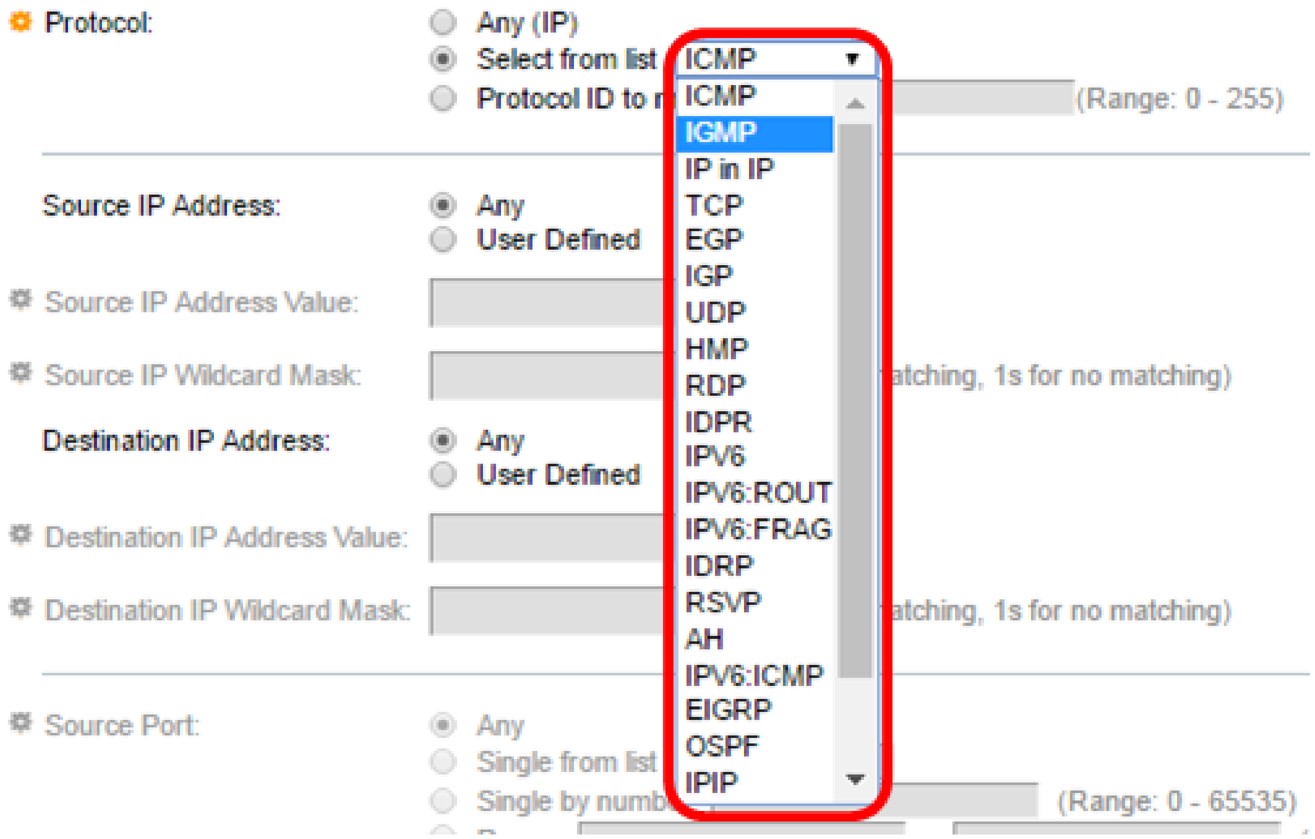
Protocol: ● Any (IP)
○ Select from list ICMP
○ Protocol ID to match (Range: 0 - 255)

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, Any (IP) is chosen.

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



Protocol: ○ Any (IP)
● Select from list ICMP
○ Protocol ID to match (Range: 0 - 255)

Source IP Address: ● Any ○ User Defined

Source IP Address Value:

Source IP Wildcard Mask: (0s for matching, 1s for no matching)

Destination IP Address: ● Any ○ User Defined

Destination IP Address Value:

Destination IP Wildcard Mask: (0s for matching, 1s for no matching)

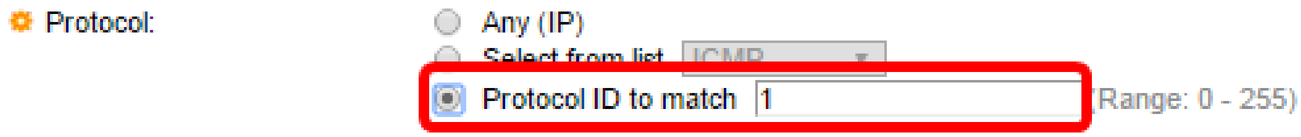
Source Port: ● Any ○ Single from list ○ Single by number (Range: 0 - 65535)

The options are:

- ICMP — Internet Control Message Protocol
- IP in IP — IP in IP encapsulation
- TCP — Transmission Control Protocol
- EGP — Exterior Gateway Protocol
- IGP — Interior Gateway Protocol
- UDP — User Datagram Protocol
- HMP — Host Mapping Protocol
- RDP — Reliable Datagram Protocol

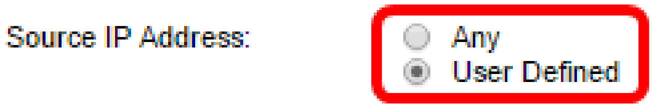
- IDPR — Interdomain Policy Routing
- IPV6 — IPv6 over IPv4 tunneling
- IPV6:ROUT — Matches packets belonging to the IPv6 over IPv4 route through a gateway
- IPV6:FRAG — Matches packets belonging to the IPv6 over IPv4 Fragment Header
- IDRP — IS-IS Interdomain Routing Protocol
- RSVP — ReSerVation Protocol
- AH — Authentication Header
- IPV6:ICMP — ICMP for IPv6
- EIGRP — Enhanced Interior Gateway Routing Protocol
- OSPF — Open Shortest Path First
- IPIP — IP in IP
- PIM — Protocol Independent Multicast
- L2TP — Layer 2 Tunneling Protocol

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



Protocol: ○ Any (IP)
○ Select from list ICMP
● Protocol ID to match 1 (Range: 0 - 255)

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



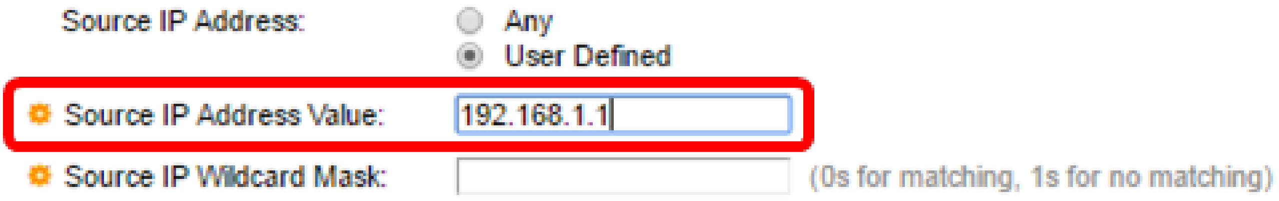
Source IP Address: ○ Any
● User Defined

The options are:

- Any — All source IPv4 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 Wildcard Mask* fields. Wildcard masks are used to define a range of IP addresses.

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.



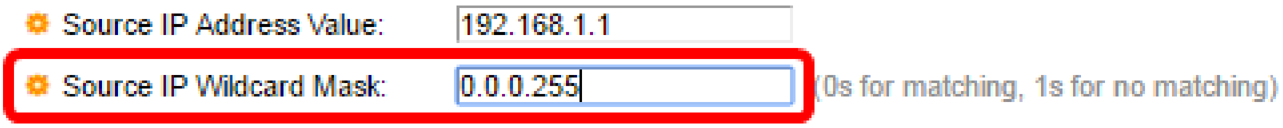
Source IP Address: ○ Any
● User Defined

Source IP Address Value: 192.168.1.1

Source IP Wildcard Mask: (0s for matching, 1s for no matching)

Note: In this example, 192.168.1.1 is used.

Step 14. Enter the source wildcard mask in the *Source IP Wildcard Mask* field.

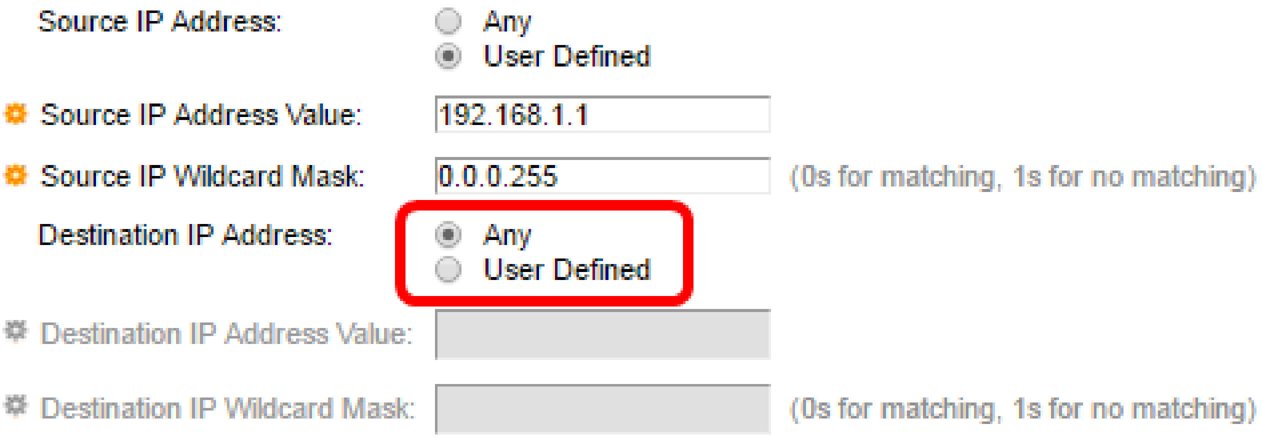


Source IP Address Value: 192.168.1.1

Source IP Wildcard Mask: 0.0.0.255 (0s for matching, 1s for no matching)

Note: In this example, 0.0.0.255 is used.

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



Source IP Address: ○ Any ● User Defined

Source IP Address Value: 192.168.1.1

Source IP Wildcard Mask: 0.0.0.255 (0s for matching, 1s for no matching)

Destination IP Address: ● Any ○ User Defined

Destination IP Address Value:

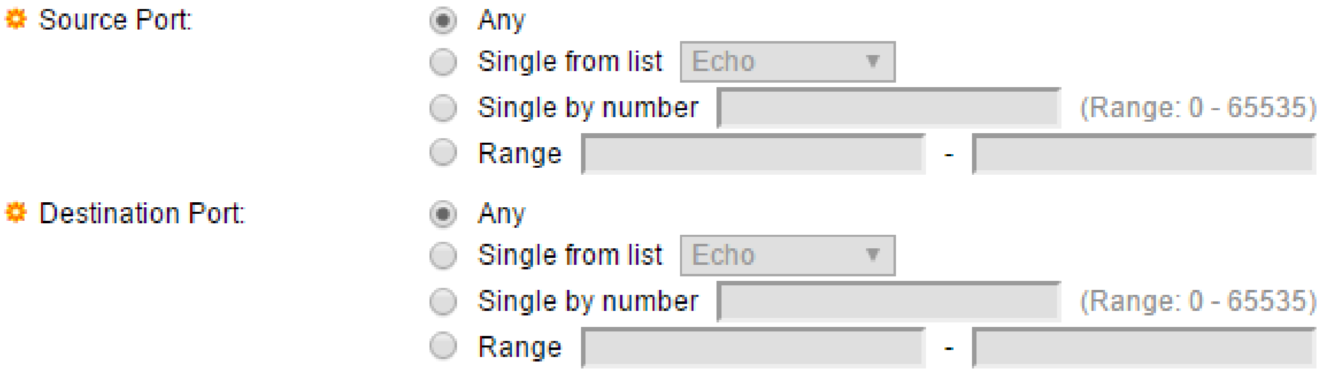
Destination IP Wildcard Mask: (0s for matching, 1s for no matching)

The options are:

- Any — All destination IPv4 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 IP Wildcard Mask* fields. Wildcard masks are used to define a range of IP addresses.

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 IPv4 address to any destination.

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



Source Port: ● Any ○ Single from list (Echo) ○ Single by number (Range: 0 - 65535) ○ Range -

Destination Port: ● Any ○ Single from list (Echo) ○ Single by number (Range: 0 - 65535) ○ Range -

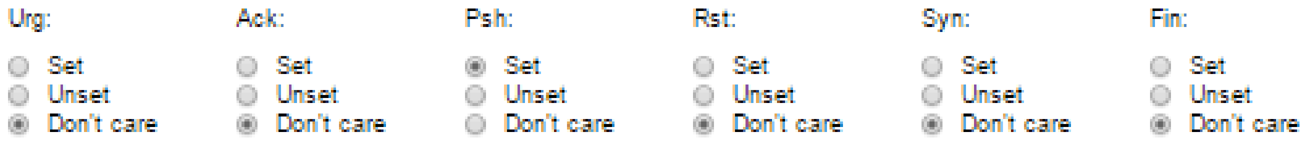
- Any — Match to all source ports.
- Single from list — You can choose a single TCP/UDP source port to which packets are matched. This field is active only if 800/6-TCP or 800/17-UDP is chosen in the Select from List drop-down menu.
- Single by number — You can choose a single TCP/UDP source port to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

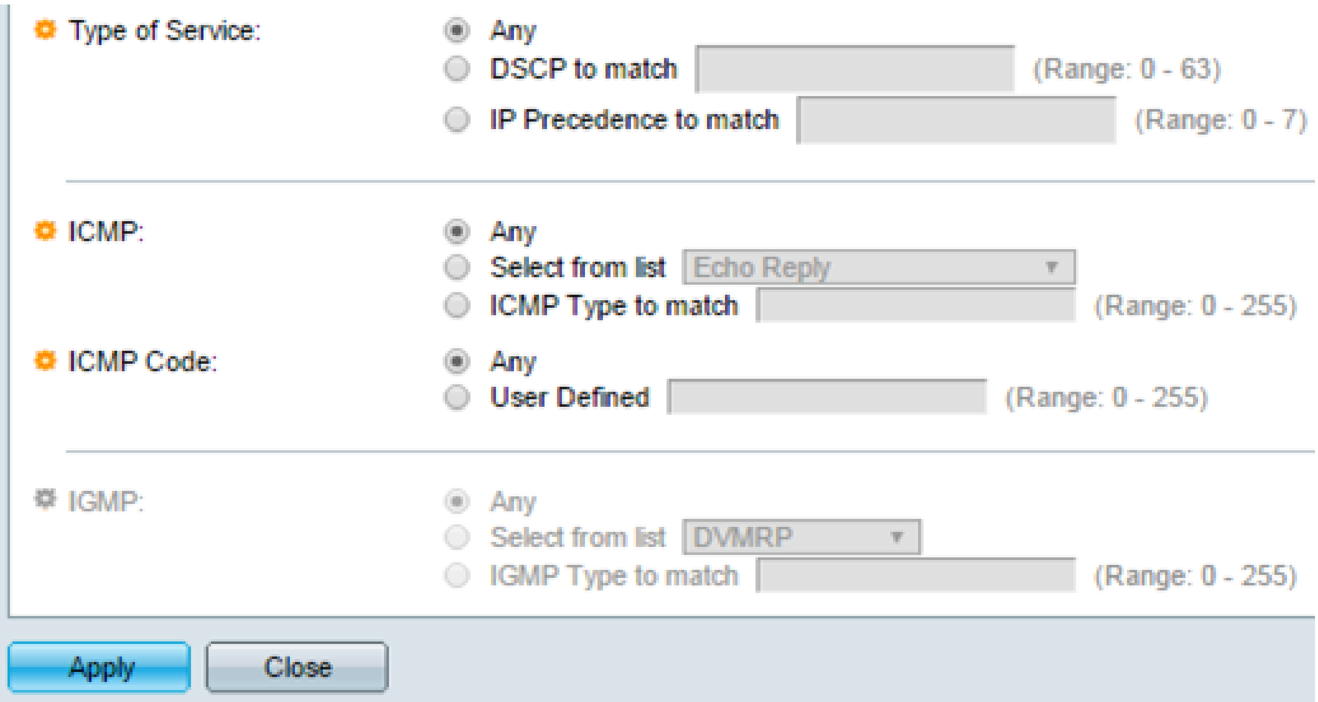


Urg:	Ack:	Psh:	Rst:	Syn:	Fin:
○ Set	○ Set	● Set	○ Set	○ Set	○ Set
○ Unset	○ Unset	○ Unset	○ Unset	○ Unset	○ Unset
● Don't care	● Don't care	○ Don't care	● Don't care	● Don't care	● Don't care

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.



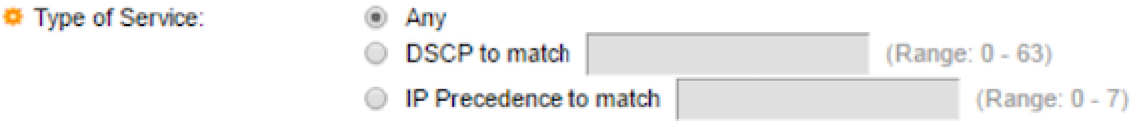
Type of Service: ● Any
○ DSCP to match (Range: 0 - 63)
○ IP Precedence to match (Range: 0 - 7)

ICMP: ● Any
○ Select from list Echo Reply
○ ICMP Type to match (Range: 0 - 255)

ICMP Code: ● Any
○ User Defined (Range: 0 - 255)

IGMP: ● Any
○ Select from list DVMRP
○ IGMP Type to match (Range: 0 - 255)

The options are:



Type of Service: ● Any
○ DSCP to match (Range: 0 - 63)
○ IP Precedence to match (Range: 0 - 7)

- Any — It can be any type of service for traffic congestion.
- DSCP to Match — DSCP 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 value 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

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 the message type by name.
- ICMP Type to match — The number of message type to be used for filtering purposes. It has a range of 0 to 255.

Step 21. (Optional) The ICMP messages can have a code field that indicates how to handle the message. Click one of the following options to configure whether to filter on this code:

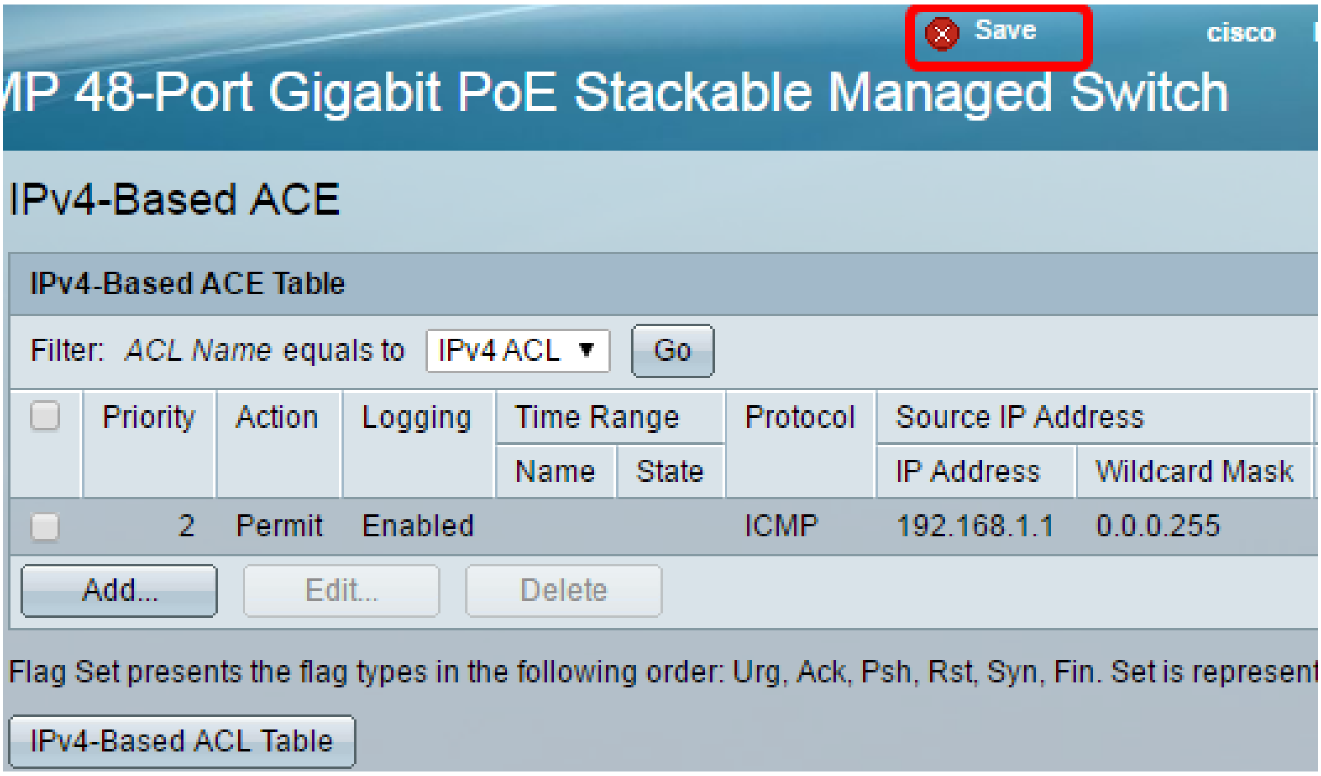
- Any — Accept all codes.
- User Defined — You can enter an ICMP code for filtering purposes. It has a range of 0 to 255.

Step 22. (Optional) If the ACL is based on IGMP, click the IGMP message type to be 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 any of the options from the drop-down list:
- DVMRP — Uses a reverse path flooding technique, sending a copy of a received packet out through each interface except the one at which the packet arrived.
- Host-Query — Periodically sends general host-query messages on each attached network for information.
- Host-Reply — It replies to the query.
- PIM — Protocol Independent Multicast (PIM) is used between the local and remote multicast routers to direct multicast traffic from the multicast server to many multicast clients.
- Trace — Provides information about joining and leaving the IGMP multicast groups.
- IGMP Type to match — The number of message type that is to be used for filtering purposes. It has a range of 0 to 255.

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.



IPv4-Based ACE

IPv4-Based ACE Table

Filter: *ACL Name* equals to IPv4 ACL ▼ Go

□	Priority	Action	Logging	Time Range		Protocol	Source IP Address	
				Name	State		IP Address	Wildcard Mask
□	2	Permit	Enabled			ICMP	192.168.1.1	0.0.0.255

Flag Set presents the flag types in the following order: Urg, Ack, Psh, Rst, Syn, Fin. Set is represent

You should now have configured an IPv4-based ACE on your switch.