Configure IPv4-Based Access Lists on the 200/300 Series Managed Switches

Objective

Access lists are rules you can apply to allow or deny specific traffic flow on your network, which adds more security and increases overall performance on your network.

The objective of this document is to show you how to configure IPv4-based access lists on the 200/300 Series Managed Switches.

Applicable Devices

- SF/SG 200 and SF/SG 300 Series Managed Switches

Software Version

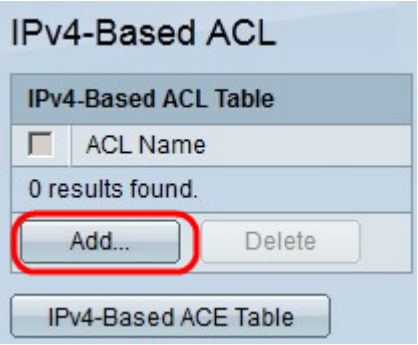
- 1.3.0.62

Configuration of IPv4-Based ACL and ACE

IPv4-Based ACLs

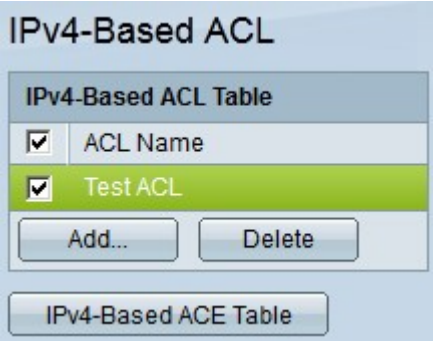
Step 1. Log in to the web configuration utility and choose **Access Control > IPv4-Based ACL**. The *IPv4-Based ACL* page opens.

Step 2. Click **Add** to add a new access list.



Step 3. In the *ACL Name* field, enter a name for the new access list.

Step 4. Click **Apply** to save the access list.



Step 5. (Optional) To delete an access list, check the check box of the access list you wish to delete, and click **Delete**.

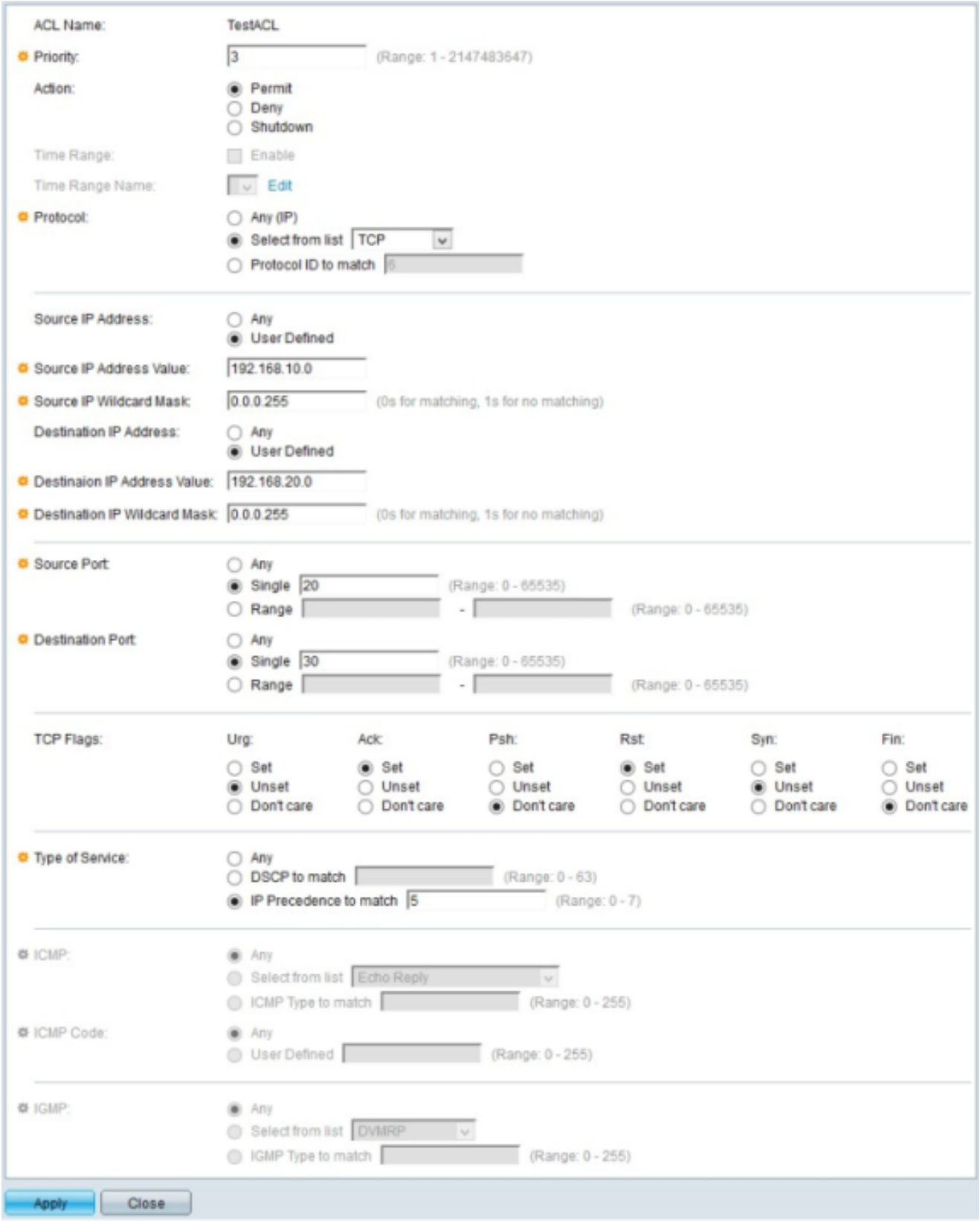
IPv4-Based ACEs

To manage an ACE to an ACL, the next steps need to be followed.

Step 1. Log in to the web configuration utility and choose **Access Control > IPv4-Based ACEs**. The *IPv4-Based ACE* page opens.

Step 2. In the *Filter: ACL Name equals to* drop-down list, choose the access list you wish to assign an access rule.

Step 3. Click **Add**. The *Add IP-Based ACE* window appears.



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

Step 5. In the *Action* field, click the radio button of the action you want this access rule to perform. The available options are:

- Permit — Forwards packets filtered by the current ACE.
- Deny — Drops packets that are filtered by the current ACE.

- Shutdown — Drops packets that are filtered by the current ACE and disables the port from where the packets were received.

Step 6. In the *Protocol* field, click the radio button of the Protocol you wish to add in the ACE. The ACE is configured for all routed network protocols in order to filter the packets as the packets pass through a router. The available options are:

- Any — Chooses any of the IPv4-Based ACE Protocols.
- Select from list — Choose the desired protocol from the drop-down list.
- Protocol ID to match — This option lets you enter the protocol ID you want to use.

Step 7. In the *Source IP Address* field, click one of the available options as the source IP address:

- Any — This option applies the access rule to any of the IP addresses available in a specific network segment.
- User Defined — This option lets you enter a specific IP address.
  - Source IP Address Value — In this field, enter the source IP address.
  - Source IP Wildcard Mask — In this field, enter the wildcard mask of the source IP address. The wild card mask lets you specify to which host of the source IP address this access list is applied.

Step 8. In the *Destination IP Address* field, click one of the available options as the destination IP address:

- Any — This option applies the access rule to any of the IP addresses available in a specific network segment.
- User Defined — This option lets you enter a specific IP address to apply the access rule:
  – Destination IP Address Value — In this field, enter the destination IP address.
  – Destination IP Wildcard Mask — In this field, enter the wildcard mask of the destination IP address. The wild card mask lets you specify which hosts of the destination IP address this access list is applied to.

Step 9. The *Source Port* field is enabled only when you choose TCP or UDP from Step 5. Click the radio button of one of the available options to choose the source port:

- Any — This option accepts any source port.
- Single — This option lets you enter a single source port value.
- Range — This option lets you enter a range of available source ports.

Step 10. The *Destination Port* field is enabled only when you choose TCP or UDP from Step 5. Click the radio button of one of the available options to choose the destination port:

- Any — This option accepts any destination port.
- Single — This option lets you enter a single destination port value.

- Range — This option lets you enter a range of available destination ports.

Step 11. The *TCP flags* field are only enabled if you choose TCP from Step 5. Click one of the radio buttons for each flag in order to choose what state you want to trigger the access rule:

- Urg — This flag identifies incoming data as urgent.
- Ack — This flag is used to acknowledge receipt of packets successfully.
- Psh — This flag is used to ensure that the data is given the correct priority and is processed at the sending or receiving end.
- Rst — This flag is used when a connection receives a wrong segment.
- Syn — This flag is used for TCP communications.
- Fin — This flag is used when the communication or data transfer is finished.

Step 12. In the *Type of Service* field, click one of the available radio buttons to choose a type of service for the IP packet:

- Any — This option chooses any type of service.
- DSCP to match — Choose this option to implement Differentiated Service Code Point (DSCP) as a type of service. DSCP is a mechanism to classify and manage network traffic. Enter the DSCP value you wish to apply to the access rule.
- IP Precedence to match — This type of service is used by the current network to provide the correct QoS (Quality of Service). Enter the value you wish to apply to the access rule.

Step 13. The *ICMP (Internet Control Message Protocol)* field is enabled only when you choose ICMP in Step 5. ICMP is used to send error messages when a service is not available or to test the connectivity. Click one of the available radio buttons to filter ICMP message types:

- Any — It can be any of the error messages or query messages.
- Select from list — Choose any of the permitted control messages from the drop-down list.
- ICMP type to match — This option lets you enter the number of ICMP types you want to

filter.

Step 14. The *ICMP Code* field is enabled only when you choose ICMP from Step 5. ICMP codes are used to provide more specific information about the control messages. Click one of the available options:

- Any — It can be any value that matches the control message.
- User Defined — Enter the ICMP code you wish to filter.

Step 15. The *IGMP (Internet Group Management Protocol)* field is enabled only when you choose IGMP from Step 5. IGMP manages host membership in IP multicast groups on a network segment. Click one of the available radio buttons to filter IGMP message types:

- Any — This options accepts all the IGMP message types.
- Select from list — Choose one of the available options from the drop-down list to filter:

  – DVMRP — It uses a reverse path flooding technique, which sends a copy of a received packet out through each interface except the one at which the packet arrived.

  – Host-Query — It periodically sends general host-query messages on each attached network for information

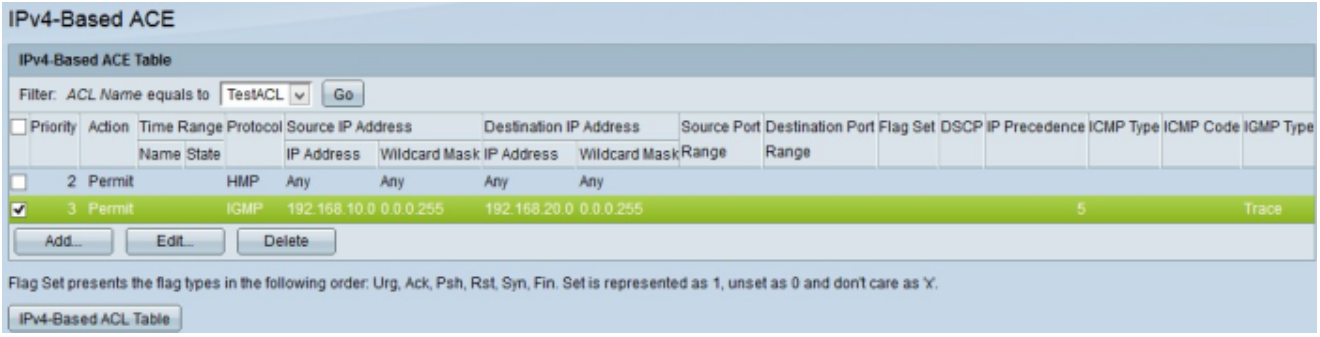
  – Host-Reply — It replies to the query .

  – PIM — It is used between the local and remote multicast routers to direct multicast traffic from the multicast server to many multicast clients.

  – Trace — It provides information to join and leave a IGMP multicast group.

- IGMP type of match — This option lets you enter the number of IGMP types you want to filter.

Step 16. Click **Apply** to save your configuration.



Step 17. (Optional) To edit a current access rule, check the check box of the access rule you wish to edit, and click **Edit**.

Step 18. (Optional) To delete a current access rule, check the check box of the access rule you wish to delete, and click **Delete**.