Security

This chapter contains the following sections:

TACACS+

An organization can establish a Terminal Access Controller Access Control System (TACACS+) server to provide centralized security for all of its devices. In this way, authentication and authorization can be handled on a single server for all devices in the organization.

The switch can act as a TACACS+ client that uses the TACACS+ server for the following services:

- Authentication—Provides authentication of administrators logging onto the switch by using usernames and user-defined passwords.
- Authorization—Performed at login. After the authentication session is completed, an authorization session starts using the authenticated username. The TACACS+ server then checks user privileges.

The TACACS+ protocol ensures network integrity, through encrypted protocol exchanges between the device and the TACACS+ server

Some TACACS+ servers support a single connection that enables the device to receive all information in a single connection. If the TACACS+ server does not support this, the device reverts back to multiple connections.

Use the TACACS+ page to configure the TACACS+ servers and define the default parameters that are used for communicating with all TACACS+ servers. A user must be configured on the TACACS+ to have privilege level 15 to be granted permission to administer the switch.

To define default TACACS+ parameters and add a TACACS+ server:

Step 1 Click **Security** > **TACACS+**.

Step 2 Enter the default TACACS+ parameters if required. Values entered in the Default Parameters are applied to all servers. If a value is not entered for a specific server (in the Add TACACS+ Server page) the device uses the values in these fields.

- Timeout for Reply—Enter the amount of time in seconds that passes before the connection between the switch and the TACACS+ server times out. If a value is not entered for an individual server, the value is taken from this field.
- Key String—Enter the default key string in encrypted or plaintext form used for communicating with all TACACS+ servers. If you do not enter the default key string here, the key entered on the Add page must match the encryption key used by the TACACS+ server. If you enter the default key string here and a key string for an individual TACACS+ server, the key string configured for the individual TACACS+ server takes precedence.

Step 3 Click **Apply**. The TACACS+ default settings for the device are updated in the Running Configuration file.

Step 4 Enter the values in the fields for each TACACS+ server. To use the default values entered in the RADIUS page, select **Use Default**.

- Server Definition—Select whether to specify the TACACS+ server by IP address or name.
- IP Version—Select the version of the IP address of the TACACS+ server.
- Server IP Address/Name—Enter the TACACS+ server by IP address or name.
- Priority—Enter the priority of the server. The priority determines the order the device attempts to contact the servers to authenticate a user. The device starts with the highest priority TACACS+ server first. Zero is the highest priority
- Key String—Enter the default key string in encrypted or plaintext form used for communicating with all TACACS+ servers. If you do not enter the default key string here, the key entered on the Add page must match the encryption key used by the TACACS+ server. If you enter the default key string here and a key string for an individual TACACS+ server, the key string configured for the individual TACACS+ server takes precedence.

Step 5 Click **Apply**. The RADIUS server definition is added to the Running Configuration file of the device.

Step 6 To display sensitive data in plaintext form on the page, click Display Sensitive Data As Plaintext.

RADIUS Client

Remote Authorization Dial-In User Service (RADIUS) servers provide a centralized 802.1X or MAC-based network access control. The device can be configured to be a RADIUS client that can use a RADIUS server to provide centralized security, and as a RADIUS server. An organization can use the device as establish a Remote Authorization Dial-In User Service (RADIUS) server to provide centralized 802.1X or MAC-based network access control for all of its devices. In this way, authentication and authorization can be handled on a single server for all devices in the organization.

Use RADIUS in network environments that require access security. To set the RADIUS server parameters, follow these steps:

Step 1 Click **Security > RADIUS Client**.

Step 2 Enter the default RADIUS parameters if required. Values entered in the Default Parameters are applied to all servers. If a value is not entered for a specific server (in the Add RADIUS Server page) the device uses the values in these fields.

- Retries—Enter the number of transmitted requests that are sent to the RADIUS server before a failure is considered to have occurred.
- Timeout for Reply—Enter the number of seconds that the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server.
- Key String—Enter the default key string used for authenticating and encrypting between the device and the RADIUS server. This key must match the key configured on the RADIUS server. A key string is used to encrypt communications by using MD5. The key can be entered in Encrypted or Plaintext form. If you do not have an encrypted key string (from another device), enter the key string in plaintext mode and click Apply. The encrypted key string is generated and displayed.

Step 3 Click **Apply**. The RADIUS default settings for the device are updated in the Running Configuration file.

Step 4 To add a RADIUS server, click **Add**.

Step 5 Enter the values in the fields for each RADIUS server. To use the default values entered in the RADIUS page, select **Use Default**.

- Server Definition—Select whether to specify the RADIUS server by IP address or name.
- IP Version—Select the version of the IP address of the RADIUS server.
- Server IP Address/Name—Enter the RADIUS server by IP address or name.
- Priority—Enter the priority of the server. The priority determines the order the device attempts to contact the servers to authenticate a user. The device starts with the highest priority RADIUS server first. Zero is the highest priority.
- Key String—Enter the key string used for authenticating and encrypting communication between the device and the RADIUS server. This key must match the key configured on the RADIUS server. It can be entered in Encrypted or Plaintext format. If Use Default is selected, the device attempts to authenticate to the RADIUS server by using the default Key String.
- Timeout for Reply—Select User Defined and enter the number of seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server if the maximum number of retries made. If Use Default is selected, the device uses the default timeout value.
- Authentication Port—Enter the UDP port number of the RADIUS server port for authentication requests
- Retries—Select User Defined and enter the number of requests that are sent to the RADIUS server before a failure is considered to have occurred. If Use Default is selected, the device uses the default value for the number of retries.
- Usage Type—Enter the RADIUS server authentication type. The options are:
  - Login—RADIUS server is used for authenticating users that ask to administer the device.
  - 802.1x—RADIUS server is used for 802.1x authentication.
  - All—RADIUS server is used for authenticating user that ask to administer the device and for 802.1X authentication.

Step 6 Click **Apply**. The RADIUS server definition is added to the Running Configuration file of the device.

Step 7 To display sensitive data in plaintext form on the page, click **Display Sensitive Data As Plaintext**.

Management Access Method

This section describes access rules for various management methods.

Access profiles determine how to authenticate and authorize users accessing the device through various access methods. Access Profiles can limit management access from specific sources.

Only users who pass both the active access profile and the management access authentication methods are given management access to the device.

There can only be a single access profile active on the device at one time.

Access profiles consist of one or more rules. The rules are executed in order of their priority within the access profile (top to bottom).

Rules are composed of filters that include the following elements:

- Access Methods-Methods for accessing and managing the device:
  - Telnet
  - Secure Telnet (SSH)
  - Hypertext Transfer Protocol (HTTP)
  - Secure HTTP (HTTPS)
  - Simple Network Management Protocol (SNMP)
  - All of the above
- Action-Permit or deny access to an interface or source address.
- Interface-Which ports, LAGs, or VLANs are permitted to access or are denied access to the web-based configuration utility.
- Source IP Address-IP addresses or subnets. Access to management methods might differ among user groups. For example, one user group might be able to access the device module only by using an HTTPS session, while another user group might be able to access the device module by using both HTTPS and Telnet sessions.

Access Profile

The Access Profiles page displays the access profiles that are defined and enables selecting one access profile to be the active one.

When a user attempts to access the device through an access method, the device looks to see if the active access profile explicitly permits management access to the device through this method. If no match is found, access is denied.

When an attempt to access the device is in violation of the active access profile, the device generates a SYSLOG message to alert the system administrator of the attempt.

Use the Access Profiles page to create an access profile and to add its first rule. If the access profile only contains a single rule, you're finished. To add more rules to the profile, use the Profile Rules page.

Step 1 Click **Security** > **Mgmt Access Method** > **Access Profiles**.

This page displays all of the access profiles, active and inactive.

Step 2 To change the active access profile, select a profile from the Active Access Profile drop down menu and click **Apply**. This makes the chosen profile the active access profile.

Note A caution message displays if you selected any other access profile, warning you that, depending on the selected access profile, you might be disconnected from the web-based configuration utility.

Step 3 Click **OK** to select the active access profile or click **Cancel** to discontinue the action.

Step 4 Click **Add** to open the Add Access Profile page. The page allows you to configure a new profile and one rule.

Step 5 Enter the Access Profile Name. This name can contain up to 32 characters.

Step 6 Enter the parameters.

- Rule Priority—Enter the rule priority. When the packet is matched to a rule, user groups are either granted or denied access to the device. The rule priority is essential to matching packets to rules, as packets are matched on a first-match basis. The highest priority is '1'.
- Management Method—Select the management method for which the rule is defined. The options are:
  - All—Assigns all management methods to the rule
  - Telnet—Users requesting access to the device that meets the Telnet access profile criteria are permitted or denied access.
  - Secure Telnet (SSH)—Users requesting access to the device that meets the SSH access profile criteria, are permitted or denied access.
  - HTTP— Users requesting access to the device that meets the HTTP access profile criteria, are permitted or denied.
  - Secure HTTP (HTTPS)—Users requesting access to the device that meets the HTTPS access profile criteria, are permitted or denied.
  - SNMP—Users requesting access to the device that meets the SNMP access profile criteria are permitted or denied.
- Action—Select the action attached to the rule. The options are:
  - Permit—Permits access to the device if the user matches the settings in the profile.
  - Deny—Denies access to the device if the user matches the settings in the profile
- Applies to Interface—Select the interface attached to the rule. The options are:
  - All—Applies to all ports, VLANs, and LAGs
  - User Defined—Applies to selected interface.

- Interface—Enter the interface number if User Defined was selected.
- Applies to Source IP Address—Select the type of source IP address to which the access profile applies. The Source IP Address field is valid for a subnetwork. Select one of the following values:
  - All—Applies to all types of IP addresses
  - User Defined—Applies to only those types of IP addresses defined in the fields.
- IP Version—Enter the version of the source IP address: Version 6 or Version 4.
- IP Address—Enter the source IP address.
- Mask—Select the format for the subnet mask for the source IP address, and enter a value in one of the fields:
  - Network Mask—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
  - Prefix Length—Select the Prefix Length and enter the number of bits that comprise the source IP address prefix.

Step 7 Click **Apply**. The access profile is written to the Running Configuration file. You can now select this access profile as the active access profile.

Profile Rules

Access profiles can contain up to 255 rules to determine who is permitted to manage and access the device, and the access methods that may be used.

Each rule in an access profile contains an action and criteria (one or more parameters) to match. Each rule has a priority; rules with the lowest priority are checked first. If the incoming packet matches a rule, the action associated with the rule is performed. If no matching rule is found within the active access profile, the packet is dropped.

For example, you can limit access to the device from all IP addresses except IP addresses that are allocated to the IT management center. In this way, the device can still be managed and has gained another layer of security.

To add profile rules to an access profile, complete the following steps:

Step 1 Click **Security > Mgmt Access Method > Profile Rules**.

Step 2 Select the Filter field, and an access profile. Click **Go**.

The selected access profile appears in the Profile Rule Table.

Step 3 Click **Add** to add a rule.

Step 4 Enter the parameters.

- Access Profile Name—Select an access profile.
- Rule Priority—Enter the rule priority. When the packet is matched to a rule, user groups are either granted or denied access to the device. The rule priority is essential to matching packets to rules, as packets are matched on a first-fit basis.

- Management Method—Select the management method for which the rule is defined. The options are:
  - All—Assigns all management methods to the rule
  - Telnet—Users requesting access to the device that meets the Telnet access profile criteria are permitted or denied access.
  - Secure Telnet (SSH)—Users requesting access to the device that meets the Telnet access profile criteria, are permitted or denied access.
  - HTTP—Assigns HTTP access to the rule Users requesting access to the device that meets the HTTP access profile criteria, are permitted or denied.
  - Secure HTTP (HTTPS)—Users requesting access to the device that meets the HTTPS access profile criteria, are permitted or denied.
  - SNMP—Users requesting access to the device that meets the SNMP access profile criteria are permitted or denied.
- Action—Select one of the following options.
  - Permit—Allow device access to users coming from the interface and IP source defined in this rule.
  - Deny—Deny device access to users coming from the interface and IP source defined in this rule.
- Applies to Interface—Select the interface attached to the rule. The options are:
  - All—Applies to all ports, VLANs, and LAGs
  - User Defined—Applies only to the port, VLAN, or LAG selected.
- Interface—Enter the interface number if the User Defined option is selected for the field above.
- Applies to Source IP Address—Select the type of source IP address to which the access profile applies. The Source IP Address field is valid for a subnetwork. Select one of the following values:
  - All—Applies to all types of IP addresses
  - User Defined—Applies to only those types of IP addresses defined in the fields.
- IP Version—Select the supported IP version of the source address: IPv6 or IPv4.
- IP Address—Enter the source IP address.
- Mask—Select the format for the subnet mask for the source IP address, and enter a value in one of the fields:
  - Network Mask—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
  - Prefix Length—Select the Prefix Length and enter the number of bits that comprise the source IP address prefix.

Step 5 Click **Apply,** and the rule is added to the access profile.

Password Strength

The default username/password is **cisco/cisco**. The first time that you log in with the default username and password, you're required to enter a new password. Password complexity is enabled by default. If the password that you choose isn't complex enough, (**Password Complexity Settings** are enabled in the Password Strength page), you're prompted to create another password.

To define password complexity rules:

Step 1 Click **Security** > **Password Strength**.

Step 2 Enter the following parameters for passwords:

- Password Aging—If selected, the user is prompted to change the password when the Password Aging Time expires.
- Password Aging Time—Enter the number of days that can elapse before the user is prompted to change the password.

Step 3 The following parameters may be configured:

- Minimal Password Length—Enter the minimal number of characters required for passwords.
- Allowed Character Repetition—Enter the number of times that a character can be repeated.
- Minimal Number of Character Classes—Enter the number of character classes which must be present in a password. Character classes are lower case (1), upper case (2), digits (3), and symbols or special characters (4).

Step 4 Click **Apply**. The password settings are written to the Running Configuration file.

The following requirements are always enforced:

- New password is different from the current password
- New Password does not repeat or reverse the users name
- New Password does not repeat or reverse the manufacturers name

Management Access Authentication

You can assign authentication methods to the various management access methods, such as SSH, Telnet, HTTP, and HTTPS. The authentication can be performed locally or on a server.

If authorization is enabled, both the identity and read/write privileges of the user are verified. If authorization isn't enabled, only the identity of the user is verified.

The authorization/authentication method used is determined by the order that the authentication methods are selected. If the first authentication method isn't available, the next selected method is used. For example, if the selected authentication methods are RADIUS and Local, and all configured RADIUS servers are queried in priority order and don't reply, the user is authorized/authenticated locally.

If authorization is enabled, and an authentication method fails or the user has insufficient privilege level, the user is denied access to the device. In other words, if authentication fails for an authentication method, the

device stops the authentication attempt; it doesn't continue and doesn't attempt to use the next authentication method.

Similarly, if authorization isn't enabled, and authentication fails for a method, the device stops the authentication attempt.

To define authentication methods for an access method:

Step 1 Click **Security** > **Management Access Authentication**.

Step 2 Enter the Application (type) of the management access method.

Step 3 Select **Authorization** to enable both authentication and authorization of the user by the list of methods described below. If the field is not selected, only authentication is performed. If Authorization is enabled, the read/write privileges of users are checked. This privilege level is set in the User Accounts page.

Step 4 Use the arrows to move the authentication method between the Optional Methods column and the Selected Methods column. The first method selected is the first method that is used.

- RADIUS—User is authorized/authenticated on a RADIUS server. You must have configured one or more RADIUS servers. For the RADIUS server to grant access to the web-based configuration utility, the RADIUS server must return cisco-avpair = shell:priv-lvl=15.
- TACACS+—User authorized/authenticated on the TACACS+ server. You must have configured one or more TACACS+ servers.
- None—User is allowed to access the device without authorization/authentication.
- Local—Username and password are checked against the data stored on the local device. These username and password pairs are defined in the User Accounts page.

Note The Local or None authentication method must always be selected last. All authentication methods selected after Local or None are ignored.

Step 5 Click **Apply**. The selected authentication methods are associated with the access method.

TCP/UDP Services

The TCP/UDP Services page enables TCP or UDP-based services on the device, usually for security reasons.

The device offers the following TCP/UDP services:

- HTTP-Enabled by factory default
- HTTPS-Enabled by factory default
- SNMP-Disabled by factory default
- Telnet-Disabled by factory default
- SSH-Disabled by factory default

To configure TCP/UDP services, follow these steps:

Step 1 Click **Security** > **TCP/UDP Services**.

Step 2 Enable or disable the following TCP/UDP services on the displayed services.

- HTTP Service-Indicates whether the HTTP service is enabled or disabled.
- HTTPS Service-Indicates whether the HTTPS service is enabled or disabled.
- SNMP Service-Indicates whether the SNMP service is enabled or disabled.
- Telnet Service-Indicates whether the Telnet service is enabled or disabled.
- SSH Service-Indicates whether the SSH server service is enabled or disabled.

Step 3 Click **Apply**. The services are written to the Running Configuration file.

The TCP Service Table displays the following fields for each service:

- Service Name-Access method through which the device is offering the TCP service.
- Type-IP protocol the service uses.
- Local IP Address-Local IP address through which the device is offering the service.
- Local Port-Local TCP port through which the device is offering the service.
- Remote IP Address-IP address of the remote device that is requesting the service.
- Remote Port-TCP port of the remote device that is requesting the service.
- State-Status of the service.
  - ESTABLISHED—The socket has an established connection.
  - SYN_SENT—The socket is actively attempting to establish a connection.
  - SYN_RECV—A connection request has been received from the network.
  - FIN_WAIT1—The socket is closed, and the connection is shutting down.
  - FIN_WAIT2—The connection is closed, and the socket is waiting for a shutdown from the remote end.
  - TIME_WAIT—The socket is waiting after close to handle packets still in the network
  - CLOSED—The socket is not being used.
  - CLOSE_WAIT—The remote end has shut down, waiting for the socket to close.
  - LAST_ACK—The remote end has shut down, and the socket is closed. Waiting for acknowledgment
  - LISTEN—The socket is listening for incoming connections.
  - CLOSING—Both sockets are shut down but we still do not have all our data sent.
  - UNKNOWN—The state of the socket is unknown.

The UDP Service table displays the following information:

- Service Name-Access method through which the device is offering the UDP service.
- Type-IP protocol the service uses.

- Local IP Address-Local IP address through which the device is offering the service.
- Local Port-Local UDP port through which the device is offering the service.

Storm Control

When Broadcast, Multicast, or Unknown Unicast frames are received, they are duplicated, and a copy is sent to all possible egress ports. This means that in practice they are sent to all ports belonging to the relevant VLAN. In this way, one ingress frame is turned into many, creating the potential for a traffic storm.

Storm protection enables you to limit the number of frames entering the device and to define the types of frames that are counted towards this limit.

When the rate of Broadcast, Multicast, or Unknown Unicast frames is higher than the user-defined threshold, frames received beyond the threshold are discarded.

To define Storm Control, follow these steps:

Step 1 Click **Security** > **Storm Control**.

Step 2 Configure the following parameters.

- Frame Configuration—Select Included (including preamble and IFG 20Bytes) to count the Broadcast, unknown Multicast, or unknown Unicast frames, or select Excluded (excluding preamble and IFG 20Bytes) to not count the Broadcast, unknown Multicast, or unknown Unicast frames
- Storm Control Rate Threshold Mode—Select the mode of the rate threshold: Packets per second or Kbits/sec.

Step 3 Click **Apply**. The storm control parameters are defined, and the Running Configuration is updated

Step 4 Select a port and click **Edit.**

Step 5 Enter the parameters.

- Interface—Select the port for which storm control is enabled.
- Storm Control—Select to enable Storm Control on selected port.
- Unknown Unicast—Select to enable Storm Control for Unicast packets.
- Storm Control Rate Threshold—Enter the maximum rate at which unknown packets can be forwarded. This value can be entered By kbits/sec or By percentage of the total available bandwidth.
- Unknown Multicast—Select to enable Storm Control for Multicast packets.
- Storm Control Rate Threshold—Enter the maximum rate at which unknown packets can be forwarded. This value can be entered By kbits/sec or By percentage of the total available bandwidth.
- Broadcast—Select to enable Storm Control for Broadcast packets.
- Storm Control Rate Threshold—Enter the maximum rate at which unknown packets can be forwarded. This value can be entered By kbits/sec or By percentage of the total available bandwidth.
- Action—Select to shut down a port when a storm occurs on the port. If this isn’t selected extra traffic is discarded.

Step 6 Click **Apply**. Storm control is modified, and the Running Configuration file is updated.

Port Security

Note Port security cannot be enabled on ports on which 802.1X is enabled or on ports that defined as SPAN destination.

Network security can be increased by limiting access on a port to users with specific MAC addresses. The MAC addresses can be either dynamically learned or statically configured.

Port security monitors received and learned packets. Access to locked ports is limited to users with specific MAC addresses.

Port Security has two modes:

- Classic Lock—All learned MAC addresses on the port are locked, and the port doesn't learn any new MAC addresses. The learned addresses aren't subject to aging or relearning.
- Limited Dynamic Lock—The device learns MAC addresses up to the configured limit of allowed addresses. After the limit is reached, the device doesn't learn additional addresses. In this mode, the addresses are subject to aging and relearning.

When a frame from a new MAC address is detected on a port where it's not authorized (the port is classically locked, and there's a new MAC address, or the port is dynamically locked, and the maximum number of allowed addresses has been exceeded), the protection mechanism is invoked, and one of the following actions can take place:

- Frame is discarded.
- Frame is forwarded.
- Frame is discarded and a SYSLOG message is generated.
- Port is shut down.

When the secure MAC address is seen on another port, the frame is forwarded, but the MAC address isn't learned on that port.

In addition to one of these actions, you can also generate traps, and limit their frequency and number to avoid overloading the devices.

To configure port security, complete the following:

Step 1 Click **Security** > **Port Security**.

Step 2 Select an interface to be modified, and click **Edit.**

Step 3 Enter the parameters.

- Interface—Select the interface name.
- Interface Status—Select to lock the port.

- Learning Mode—Select the type of port locking. To configure this field, the Interface Status must be unlocked. The Learning Mode field is enabled only if the Interface Status field is locked. To change the Learning Mode, the Lock Interface must be cleared. After the mode is changed, the Lock Interface can be reinstated. The options are:
  - Classic Lock—Locks the port immediately, regardless of the number of addresses that have already been learned.
  - Limited Dynamic Lock—Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both relearning and aging of MAC addresses are enabled.
- Max No. of Addresses Allowed—Enter the maximum number of MAC addresses that can be learned on the port if Limited Dynamic Lock learning mode is selected. The number 0 indicates that only static addresses are supported on the interface.
- Action on Violation—Select an action to be applied to packets arriving on a locked port. The options are:
  - Discard—Discards packets from any unlearned source
  - Forward—Forwards packets from an unknown source without learning the MAC address
  - Discard and Log—Discards packets from any unlearned source, shuts down the interface, logs the events, and sends traps to the specified trap receivers
  - Shutdown—Discards packets from any unlearned source, and shuts down the port The port remains shut down until reactivated, or until the device is rebooted.
- Trap Frequency—Enter minimum time (in seconds) that elapses between traps.

Step 4 Click **Apply**. Port security is modified, and the Running Configuration file is updated.

802.1X

802.1x authentication restricts unauthorized clients from connecting to a LAN through publicity-accessible ports. 802.1x authentication is a client-server model. In this model, network devices have the following specific roles.

- Client or supplicant
- Authenticator
- Authentication server

A network device can be either a client/supplicant, authenticator or both per port.

802.1X Properties

The Properties page is used to globally enable port/device authentication. For authentication to function, it must be activated both globally and individually on each port.

To define port-based authentication, follow these steps:

Step 1 Click **Security > 802.1X > Properties**.

Step 2 Enter the parameters.

- Port-Based Authentication—Enable or disable port-based authentication.
- Guest VLAN—Select to enable the use of a guest VLAN for unauthorized ports. If a guest VLAN is enabled, all unauthorized ports automatically join the VLAN selected in the Guest VLAN ID field. If a port is later authorized, it's removed from the guest VLAN.

  The guest VLAN can be defined as a layer 3 interface (assigned an IP address) like any other VLAN. However, device management isn't available via the guest VLAN IP address.
- Guest VLAN ID—Select the guest VLAN from the list of VLANs.

Step 3 Click **Apply**. The 802.1X properties are written to the Running Configuration file.

Port Authentication

The Port Authentication page enables configuration of parameters for each port. Since some of the configuration changes are only possible while the port is in Force Authorized state, such as host authentication, it's recommended that you change the port control to Force Authorized before making changes. When the configuration is complete, return the port control to its previous state.

Note A port with 802.1x defined on it can't become a member of a LAG. 802.1x and Port Security can't be enabled on same port at same time. If you enable port security on an interface, the Administrative Port Control can't be changed to Auto mode.

To define 802.1X authentication:

Step 1 Click **Security** > **802.1X** > **Port Authentication**.

This page displays authentication settings for all ports.

Step 2 Select a port and click **Edit.**

Step 3 Enter the parameters.

- Interface—Select a port.
- Administrative Port Control—Select the Administrative Port Authorization state. The options are:
  - Disable—Disable 802.1X
  - Force Unauthorized—Denies the interface access by moving the interface into the unauthorized state. The device doesn't provide authentication services to the client through the interface.
  - Auto—Enables port-based authentication and authorization on the device. The interface moves between an authorized or unauthorized state based on the authentication exchange between the device and the client.
  - Force Authorized—Authorizes the interface without authentication.

- RADIUS VLAN Assignment—Select to enable Dynamic VLAN assignment on the selected port. The options are:
  - Disable—Ignore the VLAN authorization result and keep original VLAN of host.
  - Reject—If get VLAN authorized information, just use it. However, if there is no VLAN authorized information, reject the host and make it unauthorized
  - Static—If get VLAN authorized information, just use it. If there is no VLAN authorized information, keep original VLAN of host

Note If there is VLAN authorized information from RADIUS, but the VLAN is not administrative created on DUT, the VLAN will be created automatically

Tip For the Dynamic VLAN Assignment feature to work, the switch requires the following VLAN attributes to be sent by the RADIUS server (as defined in RFC 3580):

- [64] Tunnel-Type = VLAN (type 13)
- [65] Tunnel-Medium-Type = 802 (type 6)
- [81] Tunnel-Private-Group-Id = VLAN ID

- Guest VLAN—Select to enable using a guest VLAN for unauthorized ports.
- Periodic Reauthentication—Select to enable port reauthentication attempts after the specified Reauthentication Period.
- Reauthentication Period—Enter the number of seconds after which the selected port is reauthenticated.
- Reauthenticate Now—Select to enable immediate port reauthentication.
- Authenticator State—Displays the defined port authorization state. The options are:
  - Initialize—In process of coming up.
  - Force-Authorized—Controlled port state is set to Force-Authorized (forward traffic).
  - Force-Unauthorized—Controlled port state is set to Force-Unauthorized (discard traffic).

    Note If the port isn't in Force-Authorized or Force-Unauthorized, it's in Auto Mode and the authenticator displays the state of the authentication in progress. After the port is authenticated, the state is shown as Authenticated.

- Max Hosts—Enter the maximum number of authorized hosts allowed on the interface.

  Select either Infinite for no limit, or User Defined to set a limit.

  Note Set this value to 1 to simulate single-host mode for web-based authentication in multi-sessions mode.

- Quiet Period—Enter the length of the quiet period.
- Resending EAP—Enter the number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request.
- Max EAP Requests—Enter the maximum number of EAP requests that will be sent. If a response isn't received after the defined period (supplicant timeout), the authentication process is restarted.
- Supplicant Timeout—Enter the number of seconds that lapses before EAP requests are resent to the supplicant.

- Server Timeout—Enter the number of seconds that lapses before the device resends a request to the authentication server.

Step 4 Click **Apply**. The port settings are written to the Running Configuration file.

Host and Session Authentication

The Host and Session Authentication page enables defining the mode in which 802.1X operates on the port and the action to perform if a violation has been detected.

To define 802.1X advanced settings for ports, complete the following steps:

Step 1 Click **Security** > **802.1X Authentication** > **Host and Session Authentication**.

The authentication parameters are described for all ports. All fields except the following are described in the Edit page.

- Number of Violations—Displays the number of packets that arrive on the interface in single-host mode, from a host whose MAC address isn't the supplicant MAC address.

Step 2 Select a port, and click **Edit.**

Step 3 Enter the parameters.

- Interface—Enter a port number for which host authentication is enabled.
- Host Authentication—Select from one of the following modes.
  - Single Host—A port is authorized if there is an authorized client. Only one host can be authorized on a port.
  - Multiple Host (802.1x)—A port is authorized if there is if there is at least one authorized client.
  - Multiple Sessions—Unlike the single-host and multi-host modes, a port in the multi-session mode does not have an authentication status. This status is assigned to each client connected to the port.

  Single Host Violation Settings—Can only be chosen if host authentication is Single Host.
- Action on Violation—Select the action to be applied to packets arriving in Single Session/Single Host mode, from a host whose MAC address isn't the supplicant MAC address. The options are:
  - Protect (Discard)—Discards the packets.
  - Restrict (Forward)—Forwards the packets.
  - Shutdown—Discards the packets and shuts down the port. The ports remain shut down until reactivated, or until the device is rebooted.
- Traps—Select to enable traps.
- Trap Frequency—Defines how often traps are sent to the host. This field can be defined only if multiple hosts are disabled.

Step 4 Click **Apply**. The settings are written to the Running Configuration file.

Authenticated Hosts

To view details about authenticated users, click. **Security** > **802.1X Authentication** > **Authenticated Hosts**.

This page displays the following fields:

- User Name—Supplicant names that authenticated on each port.
- Port—Number of the port
- Session Time (DD:HH:MM:SS)—Amount of time that the supplicant was authenticated and authorized access at the port.
- Authentication Method — Method by which the last session was authenticated
- MAC Address—Displays the supplicant MAC address.

Denial of Service

A Denial of Service (DoS) attack is a hacker attempt to make a device unavailable to its users.

DoS attacks saturate the device with external communication requests, so that it cannot respond to legitimate traffic. These attacks usually lead to a device CPU overload.

One method of resisting DoS attacks employed by the device is the use of Secure Core Technology (SCT), which is enabled by default and cannot be disabled. The Cisco device is an advanced device that handles management traffic, protocol traffic and snooping traffic, in addition to end-user (TCP) traffic. SCT ensures that the device receives and processes management and protocol traffic, no matter how much total traffic is received. This is done by rate-limiting TCP traffic to the CPU.

Security Suite Settings

Note Before activating DoS Prevention, you must unbind all Access Control Lists (ACLs) or advanced QoS policies that are bound to a port. ACL and advanced QoS policies aren't active when a port has DoS Protection enabled on it.

To configure DoS Prevention global settings and monitor SCT:

Step 1 Click **Security** > **Denial of Service Prevention** > **Security Suite Settings**.

CPU Protection Mechanism: Enabled indicates that SCT is enabled.

Step 2 Click **Details** to view CPU resource utilization information.

Step 3 Click **Edit** beside TCP SYN Protection to set the feature.

Step 4 In the **Denial of Service Protection** area, enable one or more of the following DoS protection options and specify the threshold if necessary:

- DA Equals SA
- ICMP Frag Packets

- ICMP Ping Maximum Length
- IPv6 Minimum Frag Length
- Land
- Null Scan
- POD
- Smurf Netmask
- TCP Source Port Less 1024
- TCP Blat
- TCP Frag-Off Minimum check
- TCP Herder Minimum Length
- UDP Blat
- XMA

Step 5 Click **Apply**. The Denial of Service prevention Security Suite settings are written to the Running Configuration file.

Interface Settings

Use the Interface Settings to enable DoS protection and IP gratuitous ARP protection on specific ports. The DoS protection feature enabled in security suite will take effect on DoS protection enabled ports.

To enable DoS protection and IP gratuitous ARP protection on a port:

Step 1 Click **Security > Denial of Service Prevention > Interface Settings**.

The Interface Settings Table displays the following information:

- Interface—Shows the port ID
- Denial of Service Protection—Shows whether the DoS Protection feature is enabled or disabled on the port.
- IP Gratuitous ARPs Protection—Check Enable to enable the IP gratuitous ARP protection feature on the port, or uncheck to disable this feature on the port.

Step 2 To edit the DoS settings for a port, select the desired port, and click **Edit**.

Step 3 Enter the following information:

- Interface—Select the port to be configured.
- Denial of Service Protection—Check **Enable** to enable the DoS Protection feature on the port, or uncheck to disable this feature on the port.
- IP Gratuitous ARPs Protection—Check **Enable** to enable the IP gratuitous ARP protection feature on the port, or uncheck to disable this feature on the port.

Step 4 Click **Apply**. The DoS protection and IP gratuitous ARP protection are enabled or disabled on the port, and the Running Configuration is updated.

SYN Protection

The network ports might be used by hackers to attack the device in a SYN attack, which consumes TCP resources (buffers) and CPU power.

Since the CPU is protected using SCT, TCP traffic to the CPU is limited. However, if one or more ports are attacked with a high rate of SYN packets, the CPU receives only the attacker packets, thus creating Denial-of-Service.

When using the SYN protection feature, the CPU counts the SYN packets ingressing from each network port to the CPU per second.

To configure SYN protection, follow these steps:

Step 1 Click **Security** > **Denial of Service Prevention** > **SYN Protection**.

Step 2 Enter the parameters.

- Block SYN-RST Packets-Select to enable the feature. All TCP packets with both SYN and RST flags are dropped on all ports.
- Block SYN-FIN Packets-Select to enable the feature. All TCP packets with both SYN and FIN flags are dropped on all ports.
- SYN Protection Mode-Select between three modes:
  - Disable-The feature is disabled on a specific interface.
  - Report-Generates a SYSLOG message. The status of the port is changed to Attacked when the threshold is passed
  - Block and Report-When a TCP SYN attack is identified, TCP SYN packets destined for the system are dropped and the status of the port is changed to Blocked.
- SYN Protection Threshold-Number of SYN packets per second before SYN packets will be blocked (deny SYN with MAC-to-me rule will be applied on the port).
- SYN Protection Period-Time in seconds before unblocking the SYN packets (the deny SYN with MAC-to-me rule is unbound from the port).

Step 3 Click **Apply**. SYN protection is defined, and the Running Configuration file is updated.

The SYN Protection Interface Table displays the following fields for every port or LAG (as requested by the user).

- Current Status-Interface status. The possible values are:
  - Normal-No attack was identified on this interface.
  - Blocked-Traffic isn’t forwarded on this interface.
  - Attacked-Attack was identified on this interface.

- Last Attack-Date of last SYN-FIN or SYN-RST attack identified by the system and the system action.

DHCP Snooping

DHCP Snooping provides network security by filtering untrusted DHCP messages and by building and by maintaining a DHCP Snooping binding database (table). DHCP Snooping acts as a firewall between untrusted hosts and DHCP servers. DHCP Snooping differentiates between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

DHCP Snooping Properties

Use the Properties page to enable DHCP Snooping on the switch and define general DHCP Snooping parameters. To define general DHCP Snooping properties:

Step 1 Click **Security > DHCP Snooping > Properties**.

Step 2 Enter the following information:

- DHCP Snooping Status—Check **Enable** to enable DHCP Snooping on the switch, or uncheck to disable this feature. By default, DHCP Snooping is disabled.
- DHCP Packet Validation—Check **Enable** to enable verifying (on an untrusted port) that the source MAC address of the Layer 2 header matches the client hardware address as appears in the DHCP Header (part of the payload), uncheck to disable this feature. By default, it is disabled.
- Option 82 Status—Check **Enable** to enable global Option 82 insert on the switch, or uncheck to disable this feature.
- Remote ID—If Option 82 is enabled, select User Defined to manually enter the format remote ID, or select Use Default to use the default value.
- Backup Database Type—Set the type of backup DHCP Snooping database agent. The options are:
  - None—Disables DHCP Snooping database agent.
  - Flash—Saves DHCP Snooping binding database in the switch NVRAM.
  - TFTP—Saves DHCP Snooping binding database on a TFTP server.
- File Name—When TFTP is selected, enter the file name of the DHCP Snooping settings that will be written to the TFTP server.
- Server IP Address—When TFTP is selected, enter the IP address or host name of the remote TFTP server.
- Write Delay—Enter the duration in seconds for which the transfer should be delayed after the DHCP Snooping binding database changes. The default is 300 seconds. The range is from 15 to 86400 seconds.
- Timeout—Enter the value in seconds when to stop the database transfer process after the DHCP Snooping binding database changes. The default is 300 seconds. The range is from 0 to 86400. Use 0 to define an Infinite duration

Step 3 Click **Apply**. The DHCP Snooping properties are defined, and the Running Configuration is updated.

DHCP Snooping VLAN Settings

Use the VLAN Settings page to enable DHCP Snooping on VLANs. To enable DHCP Snooping on a VLAN, ensure that DHCP Snooping is globally enabled on the switch.

To define DHCP Snooping on VLANs, complete the following steps:

Step 1 Click **Security** > **DHCP Snooping** > **VLAN Settings**.

Step 2 Select the VLANs from the Available VLANs column and add them to the Enabled VLANs column.

Step 3 Click **Apply**. DHCP Snooping is enabled on the selected VLANs, the Running Configuration is updated

DHCP Snooping Interface Settings

Use the Interface Settings page to define the DHCP Snooping trusted interfaces. The switch transfers all DHCP requests to trusted interfaces. To define DHCP Snooping trusted interfaces:

Step 1 Click **Security** > **DHCP Snooping** > **Interface Settings**.

Step 2 Select the interface type (Port or LAG), and click **Go**.

Step 3 Select an interface and click **Edit**.

Step 4 Enter the following information:

- Trusted Interface—Select to trust or not trust the selected interface.

Note Configure the ports that are connected to a DHCP server or to other switches or routers as trusted ports. Configure the ports that are connected to DHCP clients as untrusted ports.

- Rate Limit (pps)—Check to limit the rate on the interface. If rate limit is enabled, enter the maximum number of rate that can be allowed on the interface.

Step 5 Click **Apply**. The DHCP Snooping trusted interface settings are defined, and the Running Configuration is updated.

Binding Database

Use the Binding Database page to query the DHCP Snooping binding database. To query addresses that are bound to the DHCP Snooping database:

Step 1 Click **Security** > **DHCP Snooping** > **Binding Database**.

Step 2 Define any of the following fields as a query filter:

- VLAN ID—Indicates the VLANs recorded in the DHCP database.

- MAC Address—Indicates the MAC addresses recorded in the DHCP database.
- IP Address—Indicates the IP addresses recorded in the DHCP database.
- Interface—Contains the interface by which the DHCP database can be queried.

Step 3 Click **Go**. These appear in the Binding Database table:

- VLAN ID—VLAN ID to which the IP address is attached in the DHCP Snooping Database.
- MAC Address—MAC address found during the query.
- IP Address—IP address found during the query.
- Interface—Interface connected to the address found during the query.
- Type—IP address binding type. The possible values are:
  - Static—Indicates the IP address is static.
  - Dynamic—Indicates the IP address is defined as a dynamic address in the DHCP database.
- Lease Time—The amount of time that the DHCP Snooping entry is active.

Addresses whose lease times are expired are deleted from the database.

DHCP Snooping Statistics

To view DHCP Snooping statistics:

Step 1 Click **Security > DHCP Snooping > Statistics**.

Step 2 Select the interface type (Port or LAG), click **Go**.

The following DHCP Snooping statistical information is displayed:

- Port—Port identifier or LAG identifier.
- Forward—Total number of forwarded packets.
- Chaddr Check Dropped—Total number of packets that are dropped by Chaddr check.
- Untrust Port Dropped—Total number of packets that are dropped by untrusted ports.
- Untrust Port with Option 82 Dropped—Total number of packets that are dropped by untrusted ports that enable Option 82.
- Invalid Drop—Total number of packets that are dropped due to invalid.

Step 3 Click **Refresh** to refresh the data in the table, or click Clear to clear all data in the table.

Option82 Port Settings

Use the Option82 Port Settings page to accept DHCP packets with Option 82 information that are received on the untrusted interfaces. To define the action for packets received on an untrusted interface, complete the following:

Step 1 Click **Security > DHCP Snooping > Option82 Port Settings**.

Step 2 Select the interface type (Port or LAG), click **Go**.

Step 3 Select an interface and click **Edit**.

Step 4 Enter the following information:

- Interface—Select the port or LAG to be defined.
- Allow Untrusted—Select one of the following actions when the untrusted port receives DHCP packets:
  - Keep—Keeps DHCP packets with Option 82 information.
  - Drop—Drops DHCP packets with Option 82 information.
  - Replace—Replaces DHCP packets with Option 82 information.

Step 5 Click **Apply**. The Running Configuration is updated.

Option82 Port CID Settings

Use the Option82 Port CID Settings page to configure the Option 82 circuit-ID sub-option. To configure the Option 82 circuit-ID sub-option, complete the following:

Step 1 Click **Security > DHCP Snooping > Option82 Port CID Settings.**

Step 2 Click **Add**.

Step 3 Enter the following information:

- Interface—Select a port or a LAG.
- VLAN Status—Check Enable to use circuit ID on a specific VLAN, or uncheck to use circuit ID on all VLANs.
- VLAN ID—Select the VLAN ID.
- Circuit ID—Enter the circuit ID, using from 1 to 63 ASCII characters (no spaces). When the Option 82 feature is enabled, the default circuit-ID sub-option is the switch VLAN and port identifier, in the format of vlan-modport.

Step 4 Click **Apply**. The Running Configuration is updated.

IP Source Guard

IP Source Guard restricts the client IP traffic to those source IP addresses configured in the IP Source binding database. For example, IP Source Guard can help prevent traffic attacks caused when a host tries to use the IP address of its neighbor.

Interface Settings

Use the Interface Settings page to enable IP Source Guard on the interfaces. To enable IP Source Guard on an interface, complete the following steps:

Step 1 Click **Security** > **IP Source Guard** > **Interface Settings.**

Step 2 Select the interface type (Port or LAG), click **Go**.

Step 3 Select an interface, and click **Edit**.

Step 4 Enter the following information:

- Interface—Select a port or LAG.
- IP Source Guard—Check **Enable** to enable IP Source Guard on the interface, or uncheck to disable this feature on the interface.
- Verify Source—Select the type of source traffic to be verified. It can be IP or MAC and IP.
- Maximum Entry—Enter the maximum number of IP source binding rules. The range is 0 to 50, and 0 means no limit.

Step 5 Click **Apply**. The IP Source Guard Interface settings are defined, and the Running Configuration is updated.

IP Source Guard Binding Database

Use the Binding Database page to query and view information about inactive addresses recorded in the IP Source Guard database. To query the IP Source Guard database and/or define an IP source binding rule:

Step 1 Click **Security > IP Source Guard > Binding Database.**

Step 2 Define the preferred filter for searching the IP Source Guard database:

- VLAN ID—Queries the database by VLAN ID.
- MAC Address—Queries the database by MAC address.
- IP Address—Queries the database by IP address.
- Interface—Queries the database by Interface name.

Step 3 Click **Go**. These appear in the Binding Database table:

- VLAN ID—VLAN with which the IP address is associated.

- MAC Address—MAC address of the interface.
- IP Address—IP address of the interface.
- Interface—Interface name.
- Type—Type of the IP address. The possible values are:
  - Dynamic—Indicates the IP address is dynamically learned.
  - Static—Indicates the IP address is a static IP address.
- Lease Time—The amount of time that the IP address is active. IP addresses whose lease times are expired are deleted from the database.

Step 4 Click **Add** to add an IP source binding rule.

Step 5 Enter the following information:

- Interface—Select an interface.
- VLAN ID—Select a VLAN with which the address is associated.
- MAC Address—Enter the MAC address of the source traffic.
- IP Address—Enter the IP address of the source traffic.

Step 6 Click **Apply**. The IP source binding rule is defined, and the Running Configuration is updated.

ARP Inspection

Dynamic Address Resolution Protocol (ARP) is a TCP/IP protocol for translating IP addresses into MAC addresses.

ARP Cache Poisoning

A malicious user can attack hosts, switches, and routers connected to a Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet. This situation can happen because ARP allows a gratuitous reply from a host even if an ARP request was not received. After the attack, all traffic from the device under attack flows through the attacker's computer and then to the router, switch, or host.

How ARP Inspection Prevents Cache Poisoning

The ARP inspection feature relates to interfaces as either trusted or untrusted (see Security > ARP Inspection > Interface Settings page). Interfaces are classified by the user as follows:

- Trusted—Packets are not inspected.
- Untrusted—Packets are inspected as described below.

ARP inspection is performed only on untrusted interfaces. ARP packets that are received on the trusted interface are simply forwarded.

Upon packet arrival on untrusted interfaces the following logic is implemented:

- Search the ARP access control rules for the packet's IP/MAC addresses. If the IP address is found and the MAC address in the list matches the packet's MAC address, then the packet is valid
- If the packet's IP address was not found, and DHCP Snooping is enabled for the packet's VLAN, search the DHCP Snooping Binding database for the packet's <VLAN - IP address> pair. If the <VLAN - IP address> pair was found, and the MAC address and the interface in the database match the packet's MAC address and ingress interface, the packet is valid.
- If the packet's IP address was not found in the ARP access control rules or in the DHCP Snooping Binding database the packet is invalid and is dropped. A SYSLOG message is generated.
- If a packet is valid, it is forwarded and the ARP cache is updated.

If the ARP Packet Validation option is selected (on the Properties page), the following additional validation checks are performed:

- Source MAC Address—Compares the packet's source MAC address in the Ethernet header against the sender's MAC address in the ARP request. This check is performed on both ARP requests and responses.
- Destination MAC Address—Compares the packet's destination MAC address. This check is performed for ARP responses.
- IP Address—Compares the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP Multicast addresses.

Packets with invalid ARP Inspection bindings are logged and dropped.

Interaction Between ARP Inspection and DHCP Snooping

If DHCP Snooping is enabled, ARP Inspection uses the DHCP Snooping Binding database in addition to the ARP access control rules. If DHCP Snooping is not enabled, only the ARP access control rules are used.

Table 1: ARP Default

Option	Default State
Dynamic ARP Inspection	Disabled
ARP Packet Validation	Disabled
ARP Inspection Enabled on VLAN	Disabled
Log Buffer Interval	SYSLOG message generation for dropped packets is enabled at 10 seconds interval.

ARP Properties

Use the Properties page to enable dynamic ARP Inspection on the switch and set ARP packet validation parameters. To define ARP Inspection properties complete the following:

Step 1 Click **Security > ARP Inspection > Properties** .

Step 2 Enter the following information:

- ARP Inspection Status—Check **Enable** to enable ARP Inspection on the switch, or uncheck to disable this feature. By default, ARP Inspection is disabled.
- ARP Packet Validation—Defines the following ARP Inspection validation properties:
  - Source MAC Address—Check **Enable** to validate the source MAC addresses in ARP requests and replies.
  - Destination MAC Address—Check **Enable** to validate the destination MAC addresses in ARP replies.
  - IP Address—Check **Enable** to validate the IP addresses in ARP requests and replies.
  - Allow all-zeros IP—If IP address validation is enabled, check **Enable** to allow 0.0.0.0 the IP address.

Step 3 Click **Apply**. The ARP Inspection properties are defined, and the Running Configuration is updated.

ARP Inspection Interface Settings

Use the Interface Settings page to define trusted and untrusted interfaces. These settings are independent to the trusted interface settings defined for DHCP Snooping. ARP Inspection is enabled only on untrusted interfaces. To change the ARP trusted status of an interface:

Step 1 Click **Security > ARP Inspection > Interface Settings**.

Step 2 Select the interface type (Port or LAG), and click **Go**.

Step 3 Select an interface, and click **Edit**.

Step 4 Enter the following information:

- Interface—Select a port or LAG on which ARP Inspection trust mode can be enabled.
- Trusted Interface—Click Yes to enable ARP Inspection trust mode on the interface, or click No to disable ARP Inspection trust mode on the interface
  - If enabled, the port or LAG is a trusted interface, and ARP inspection is not performed on the ARP requests or replies sent to or from the interface.
  - If disabled, the port or LAG is not a trusted interface, and ARP inspection is performed on the ARP requests or replies sent to or from the interface. By default, it is disabled.
- Rate Limit (pps)—Enter the maximum rate that is allowed on the interface. The range is 1 to 50 pps and the default is 15.

Step 5 Click **Apply**. The ARP Inspection trusted interfaces are defined, and the Running Configuration is updated.

ARP Inspection Statistics

The Statistics page displays the statistical information for ARP Inspection. To view ARP Inspection statistics:

Step 1 Click **Security > ARP Inspection > Statistics**.

- VLAN ID—Identifier of the VLAN.
- Forward—Total number of ARP packets forwarded by the VLAN.
- Source MAC Failures—Total number of ARP packets that include wrong source MAC addresses.
- Destination MAC Failures—Total number of ARP packets that include wrong destination MAC addresses.
- Source IP Address Validation Failures—Total number of ARP packets that the source IP address validation fails.
- Destination IP Address Validation Failures—Total number of ARP packets that the destination IP address validation fails.
- IP-MAC Mismatch Failures—Total number of ARP packets that the IP address does not match the MAC address.

Step 2 Click **Refresh** to refresh the data in the table, or click Clear to clear all ARP Inspection statistics.

ARP Inspection VLAN Settings

Use the VLAN Settings page to enable ARP Inspection on VLANs. In the Enabled VLAN table, users assign static ARP Inspection lists to enabled VLANs. When a packet passes through an untrusted interface that is enabled for ARP Inspection, the switch performs the following checks in order:

- Determines if the packet's IP address and MAC address exist in the static ARP Inspection list. If the addresses match, the packet passes through the interface.
- If the switch does not find a matching IP address, but DHCP Snooping is enabled on the VLAN, the switch checks the DHCP Snooping database for the IP address-VLAN match. If the entry exists in the DHCP Snooping database, the packet passes through the interface.
- If the packet's IP address is not listed in the ARP Inspection list or the DHCP Snooping database, the switch rejects the packet.

To define ARP Inspection on VLANs, complete the following steps:

Step 1 Click **Security > ARP Inspection > VLAN Settings**.

Step 2 Select the VLANs from the Available VLANs column and add them to the Enabled VLANs column.

Step 3 Click **Apply**. ARP Inspection settings are applied on the selected VLANs, and the Running Configuration is updated.

Certificate Settings

The Cisco Business Dashboard Agent (CBD) and Plug-n-Play (PNP) features require CA certificates to establish HTTPS communication with the CBD or PNP servers. The Certificate Settings feature allows these applications and device managers to do the following:

- Install trusted CA certificates and to remove certificates that are no longerwanted
- Statically add certificates to device configurationfile
- Manage a revocation list of untrustedcertificates

Note The validity of the certificates is based on the system clock. Use the default system clock or it does not provide proper validation. Therefore, make sure the system clock is based on device Real time clock (if supported) or was actively set since the last reboot (preferably via SNTP service). If the system clock is not based on RTC or was not set since last reboot validation of certificate will fail, even if the system clock is within the validity date of the certificate.

Dynamic Certificates

The embedded certificate is installed by default. The PNP applications can install dynamic trusted certificates to the device memory. The installed certificate must include the following attributes:

- Certificate name - A string that is used to identify the certificate
- Owner - The application name that installed the certificate (for example, PNP)
- The certificate itself in PEM format.

An application can also delete a specific or all dynamic certificates installed by that application.

Considerations

- Up to 512 dynamic certificates can be installed on the device.
- Dynamic certificates are removed when the device reboots.

Static Certificate

If an application wants to add a certificate that will not be deleted on reset, or if a user of the switch wants to add a certificate, they can add a static certificate. These certificates are saved in the device running configuration and can be copied to the startup configuration.

Adding a static certificate requires providing the following attributes:

- Certificate name - A string that is used to identify the certificate
- Owner - The application name that installed the certificate (for example, PNP)
- The certificate itself in PEM format.

Considerations

- Up to 128 static certificates can be installed on the device.
- It is possible for identical certificates to be added by different applications or users as long as the names used to identify them are different.

CA Certificate Setting

Users can access information on all installed certificates (dynamic and static). The following information is displayed per each certificate:

Step 1 Click **Security** > **Certificate Settings** > **CA Certificate Settings**.

Step 2 To import a new certificate, click **Add** and complete the following:

- Certificate Name—Enter the name of the certificate.
- Certificate Owner —Enter the owner of the certificate.
- Certificate—Paste the certificate in PEM format (including the begin and end marker lines).

Step 3 Click **Apply** to apply the new settings.

Step 4 To view the details of an existing certificate, select the certificate from the list and click **Details**. The following will be displayed:

Option	Description
Certificate Name	The name or unique identifier of the certificate.
Type	This can be signer, static or dynamic.
Owner	This can be signer, static, CBD or PNP
Version	The version of the certificate.
Serial Number	The serial number of the certificate.
Status	The status of the certificate.
Valid From	The date and time from which certificate is valid,
Valid To	The date and time until which the certificate is valid.
Issuer	The entity or CA that signed the certificate.
Subject	Distinguished name (DN) information for the certificate.
Public Key Type	The type of the public key.
Public Key Length	The length (in bits) of the public key.
Signature Algorithm	The cryptographic algorithm used by the CA to sign the certificate.
Certificate	The certificate details in PEM format.

Step 5 You can use the following filters to find a specific certificate.

- Type equals to—Check this box and select Signer, Static, or Dynamic from the drop-down list, to filter by these certificate types.
- Owner equals to—Paste the certificate in PEM format (including the begin and end marker lines).

Step 6 To remove one or more certificates select the certificate(s) and press **Delete**. Only Static certificates can be deleted.

CA Certificate Revocation List

If a certificate becomes untrusted for any reason, it can be added to the revocation list by the user or one of the applications. If a certificate is included in the revocation list, it is considered non-valid and the device will not allow it to be used. Adding a certificate to the revocation list will not remove the revoked certificate from the certificate database. It will only update its status to Not Valid (Revoked). When a certificate is removed from the revocation list, its status is automatically updated in the certificate database. There is no need to re-install it.

To add or remove a certificate to/from the revocation list, complete the following:

Step 1 Click **Security** > **Certificate Settings** > **CA Certificate Revocation List**.

Step 2 Click **Add** to open the Add Revoked Certificate dialog box

Step 3 Provide the following details:

- Issuer—The string identifying the issuer (for example: "C=US, O=MyTrustOrg, CN=MyCommonName") (1-160 chars).
- Serial Number—The serial number of the revoked certificate. This is a string of hexadecimal pairs (length 2-32).

Step 4 Click **Apply** to add the certificate.

Considerations

- Up to 512 certificates can be added to the revocation list.
- All certificates that match the entry in the revocation list are considered not valid (even if they are identified under different names in the certificate database).

Step 5 To delete an existing certificate, select the certificate from the Revoked CA Certificate Table and click **Delete**. Next, click **Apply** to apply the new settings.