Overview

This document describes how to configure security features on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches.

The switch provides security for the subscriber, the switch, and the network.

Subscriber Security

- By default, local switching is disabled among subscriber ports to ensure that subscribers are isolated.
- DHCP snooping to filter untrusted DHCP messages between untrusted hosts and DHCP servers.
- DHCP Snooping Statistics **show** and **clear** commands to display and remove DHCP snooping statistics in summary or detail form.
- IP source guard to restrict traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings.
- Dynamic ARP inspection to prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN.

Related Topics

- Chapter 5, "Configuring DHCP Features and IP Source Guard"
- Chapter 6, "Configuring Dynamic ARP Inspection"

Switch Security

Note The Kerberos feature listed in this section is only available on the cryptographic version of the switch software.

- TACACS+, a proprietary feature for managing network security through a TACACS server.
- RADIUS for verifying the identity of, granting access to, and tracking the actions of remote users through authentication, authorization, and accounting (AAA) services.
- Kerberos security system to authenticate requests for network resources by using a trusted third party (requires the cryptographic version of the switch software).

- Password-protected access (read-only and read-write access) to management interfaces for protection against unauthorized configuration changes.
- Configuration file security so that only authenticated and authorized users have access to the configuration file, preventing users from accessing the configuration file by using the password recovery process.
- Multilevel security for a choice of security level, notification, and resulting actions.
- Port security option for limiting and identifying MAC addresses of the stations allowed to access the port.
- Port security aging to set the aging time for secure addresses on a port.
- LLDP (Link Layer Discovery Protocol) and LLDP-MED (Media Extensions)—Adds support for 802.1AB link layer discovery protocol for interoperability in multi-vendor networks. Switches exchange speed, duplex, and power settings with end devices such as IP Phones.
- UNI and ENI default port state is disabled.
- Automatic control-plane protection to protect the CPU from accidental or malicious overload due to Layer 2 control traffic on UNIs or ENIs.
- Configurable control plane security that provides service providers with the flexibility to drop customers control-plane traffic on a per-port, per-protocol basis. Allows configuring of ENI protocol control packets for CDP, STP, LLDP, LACP, or PAgP.

Related Topics

- Chapter 2, “Configuring Switch-Based Authentication”
- Chapter 3, “Configuring IEEE 802.1x Port-Based Authentication”
- Chapter 9, “Configuring Control-Plane Security”

Network Security

- 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network. These features are supported:
  - VLAN assignment for restricting 802.1x-authenticated users to a specified VLAN.
  - Port security for controlling access to 802.1x ports.
  - 802.1x accounting to track network usage.
  - 802.1x readiness check to determine the readiness of connected end hosts before configuring 802.1x on the switch.
  - Network Edge Access Topology (NEAT) with 802.1x switch supplicant, host authorization with Client Information Signalling Protocol (CISP), and auto enablement to authenticate a switch outside a wiring closet as a supplicant to another switch.
- Support for IP source guard on static hosts.
- 802.1x User Distribution to allow deployments with multiple VLANs (for a group of users) to improve scalability of the network by load balancing users across different VLANs. Authorized users are assigned to the least populated VLAN in the group, assigned by RADIUS server.

- Static MAC addressing for ensuring security.
- Web authentication proxy, to authenticate end users on host systems that do not run the IEEE 802.1x supplicant.
- Standard and extended IP access control lists (ACLs) for defining security policies in both directions on routed interfaces (router ACLs) and VLANs and inbound on Layer 2 interfaces (port ACLs).
- Extended MAC access control lists for defining security policies in the inbound direction on Layer 2 interfaces.
- VLAN ACLs (VLAN maps) for providing intra-VLAN security by filtering traffic based on information in the MAC, IP, and TCP/UDP headers.
- Source and destination MAC-based ACLs for filtering non-IP traffic.
- IPv6 ACLs to be applied to interfaces to filter IPv6 traffic.

Related Topics

- Chapter 2, “Configuring Switch-Based Authentication”
- Chapter 3, “Configuring IEEE 802.1x Port-Based Authentication”
- Chapter 4, “Configuring Web-Based Authentication”
- Chapter 7, “Configuring Network Security with ACLs”
- Chapter 8, “Configuring IPv6 ACLs”