Security Features Overview

Security Features Overview

The switch supports a LAN base image or a LAN lite image with a reduced feature set, depending on switch hardware. The security features are as follows:

- FIPS Certification

  Cisco IOS XE Release 15.0(2)EX1 on the Catalyst 2960-X switch has been submitted for certification under FIPS 140-2 and Common Criteria compliance with the US Government, Security Requirements for Network Devices.

  FIPS 140-2 is a cryptographic-focused certification, required by many government and enterprise customers, which ensures the compliance of the encryption and decryption operations performed by the switch to the approved FIPS cryptographic strengths and management methods for safeguarding these operations.

- IPv6 First Hop Security—A suite of security features to be applied at the first hop switch to protect against vulnerabilities inherent in IPv6 networks. These include, Binding Integrity Guard (Binding Table), Router Advertisement Guard (RA Guard), DHCP Guard, IPv6 Neighbor Discovery Inspection (ND Guard).

- Web Authentication—Allows a supplicant (client) that does not support IEEE 802.1x functionality to be authenticated using a web browser.

  Note To use Web Authentication, the switch must be running the LAN Base image.

- Local Web Authentication Banner—A custom banner or an image file displayed at a web authentication login screen.

- IEEE 802.1x Authentication with ACLs and the RADIUS Filter-Id Attribute

  Note To use Web Authentication, the switch must be running the LAN Base image.

- Password-protected access (read-only and read-write access) to management interfaces (device manager, Network Assistant, and the CLI) for protection against unauthorized configuration changes
- Multilevel security for a choice of security level, notification, and resulting actions
- Static MAC addressing for ensuring security
- Protected port option for restricting the forwarding of traffic to designated ports on the same switch
- Port security option for limiting and identifying MAC addresses of the stations allowed to access the port
- VLAN aware port security option to shut down the VLAN on the port when a violation occurs,instead of shutting down the entire port.
- Port security aging to set the aging time for secure addresses on a port.
- Protocol storm protection to control the rate of incoming protocol traffic to a switch by dropping packets that exceed a specified ingress rate.
- BPDU guard for shutting down a Port Fast-configured port when an invalid configuration occurs.
- Standard and extended IP access control lists (ACLs) for defining inbound security policies on Layer 2 interfaces (port ACLs).
- Extended MAC access control lists for defining security policies in the inbound direction on Layer 2 interfaces.
- Source and destination MAC-based ACLs for filtering non-IP traffic.
- DHCP snooping to filter untrusted DHCP messages between untrusted hosts and DHCP servers.
- 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
- IEEE 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network. These 802.1x features are supported:
  - Multidomain authentication (MDA) to allow both a data device and a voice device, such as an IP phone (Cisco or non-Cisco), to independently authenticate on the same IEEE 802.1x-enabled switch port.

    Note To use MDA, the switch must be running the LAN Base image.

  - Dynamic voice virtual LAN (VLAN) for MDA to allow a dynamic voice VLAN on an MDA-enabled port.
  - VLAN assignment for restricting 802.1x-authenticated users to a specified VLAN.
  - Support for VLAN assignment on a port configured for multi-auth mode. The RADIUS server assigns a VLAN to the first host to authenticate on the port, and subsequent hosts use the same VLAN. Voice VLAN assignment is supported for one IP phone.

Note To use this feature, the switch must be running the LAN Base image.

- Port security for controlling access to 802.1x ports.
- Voice VLAN to permit a Cisco IP Phone to access the voice VLAN regardless of the authorized or unauthorized state of the port.
- IP phone detection enhancement to detect and recognize a Cisco IP phone.
- Guest VLAN to provide limited services to non-802.1x-compliant users.
- Restricted VLAN to provide limited services to users who are 802.1x compliant, but do not have the credentials to authenticate via the standard 802.1x processes.

Note To use authentication with restricted VLANs, the switch must be running the LAN Base image.

- 802.1x accounting to track network usage.
- 802.1x with wake-on-LAN to allow dormant PCs to be powered on based on the receipt of a specific Ethernet frame.
- 802.1x readiness check to determine the readiness of connected end hosts before configuring IEEE 802.1x on the switch.

Note To use 802.1x readiness check, the switch must be running the LAN Base image.

- Voice aware 802.1x security to apply traffic violation actions only on the VLAN on which a security violation occurs.

Note To use voice aware 802.1x authentication, the switch must be running the LAN Base image.

- MAC authentication bypass (MAB) to authorize clients based on the client MAC address.

Note To use MAC authentication bypass, the switch must be running the LAN Base image.

- Network Admission Control (NAC) Layer 2 802.1x validation of the antivirus condition or posture of endpoint systems or clients before granting the devices network access.

Note To use NAC, the switch must be running the LAN Base image.

- Network Edge Access Topology (NEAT) with 802.1X switch supplicant, host authorization with CISP, and auto enablement to authenticate a switch outside a wiring closet as a supplicant to another switch.
- IEEE 802.1x with open access to allow a host to access the network before being authenticated.
- IEEE 802.1x authentication with downloadable ACLs and redirect URLs to allow per-user ACL downloads from a Cisco Secure ACS server to an authenticated switch.
- Support for dynamic creation or attachment of an auth-default ACL on a port that has no configured static ACLs.

Note To use this feature, the switch must be running the LAN Base image.

- Flexible-authentication sequencing to configure the order of the authentication methods that a port tries when authenticating a new host.
- Multiple-user authentication to allow more than one host to authenticate on an 802.1x-enabled port.

- TACACS+, a proprietary feature for managing network security through a TACACS server for both IPv4 and IPv6.
- RADIUS for verifying the identity of, granting access to, and tracking the actions of remote users through authentication, authorization, and accounting (AAA) services for both IPv4 and IPv6.
- Enhancements to RADIUS, TACACS+, and SSH to function over IPv6.
- Secure Socket Layer (SSL) Version 3.0 support for the HTTP 1.1 server authentication, encryption, and message integrity and HTTP client authentication to allow secure HTTP communications (requires the cryptographic version of the software).
- IEEE 802.1x Authentication with ACLs and the RADIUS Filter-Id Attribute.
- Support for IP source guard on static hosts.
- RADIUS Change of Authorization (CoA) to change the attributes of a certain session after it is authenticated. When there is a change in policy for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server, such as Cisco Identity Services Engine, or Cisco Secure ACS to reinitialize authentication, and apply to the new policies.
- IEEE 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.
- Support for critical VLAN with multiple-host authentication so that when a port is configured for multi-auth, and an AAA server becomes unreachable, the port is placed in a critical VLAN in order to still permit access to critical resources.
- Support for Network Edge Access Topology (NEAT) to change the port host mode and to apply a standard port configuration on the authenticator switch port.
- VLAN-ID based MAC authentication to use the combined VLAN and MAC address information for user authentication to prevent network access from unauthorized VLANs.

- MAC move to allow hosts (including the hosts connected behind an IP phone) to move across ports within the same switch without any restrictions to enable mobility. With MAC move, the switch treats the reappearance of the same MAC address on another port in the same way as a completely new MAC address.
- Support for 3DES and AES with version 3 of the Simple Network Management Protocol (SNMPv3). This release adds support for the 168-bit Triple Data Encryption Standard (3DES) and the 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms to SNMPv3.
- Support for Cisco TrustSec SXP protocol.

Security Features Overview