Security features

Security features are a collection of integrated tools, protocols, and policies designed to safeguard network systems and data by mitigating threats, preventing unauthorized access, and ensuring data integrity.

Starting with Cisco NX-OS Release 10.6(1s), you can configure these security features on the Cisco N9324C-SE1U, Cisco N9348Y2C6D-SE1U switches.

- IP Access Control List (IP ACL)
- Dynamic Host Configuration Protocol (DHCP) relay
- Control Plane Policing (CoPP)
- Media Access Control Security (MACsec)

IP ACL

An IP ACL is an ordered set of rules that filters network traffic by specifying conditions based on IP packet information, such as source and destination IP addresses and protocol type, to determine whether a packet is permitted or denied.

For information on IP ACLs, see Configure IP ACLs.

DHCP relay

DHCP relay is a feature that enhances network control by centralizing IP address allocation, which enables consistent policy enforcement and aids in the prevention of rogue DHCP servers by forwarding client requests exclusively to trusted, remote servers.

For information on DHCP relay, see Configuring DHCP.

Control Plane Policing

CoPP is a security feature that protects a network device's control plane from Denial of Service (DoS) attacks by applying a policy map to limit the rate of traffic destined for the CPU, ensuring network stability and reachability.

A custom CoPP policy is an administrator-defined ruleset that tailors the protection of a device's control plane by classifying specific traffic types and applying unique rate limits to meet a network's particular security and operational requirements.

For information on CoPP, see Configure Control Plane Policing.

MACsec

MACsec is an IEEE 802.1AE security standard that provides confidentiality and data integrity for Ethernet links by encrypting traffic at Layer 2 on a hop-by-hop basis.

For information on MACsec, see Configure MACsec.

• Security feature guidelines, on page 2

Security feature guidelines

This section outlines feature support, guidelines, and limitations for security functionalities on Cisco N9324C-SE1U, Cisco N9348Y2C6D-SE1U switches.

Table 1: Supported features and releases

Features	Release
PACL	10.6(1s)
RACL on L3 interfaces, L3 Port-channel interfaces, subinterfaces, and SVI interfaces	10.6(1s)
PBR ACL	10.6(1s)
DHCP relay	10.6(1s)
Custom CoPP	10.6(1s)
MACsec	10.6(1s)

ACL limitations

- The **mac packet-classify** command is not supported.
- Each TCAM slice supports 7136 entries for RACL or PACL. The Cisco N9324C-SE1U, Cisco N9348Y2C6D-SE1U switches have two slices.

DHCP relay limitations

When a DHCP relay is configured on a switch and a RACL is also applied, the RACL will drop unicast DHCP relay traffic. This occurs because RACLs and other security policies have a higher priority in the processing order than control plane traffic, such as DHCP relay.

CoPP limitations

- Policer rates are specified in packets per second (PPS).
- Destination IP-based access-list matching is not supported in Custom CoPP.
- User-defined MAC access lists are not supported; only built-in MAC ACLs can be used.
- A maximum of 28 class maps can be configured under a Custom CoPP policy.

- Custom CoPP supports maximum 360 IPv4 (uni-dimensional) and 180 IPv6 (uni-dimensional) TCAM entries.
- The CoPP Consistency Checker is not supported for Custom CoPP.
- Zero Committed Information Rate (CIR) is not supported. If zero CIR is configured, the hardware sets it to the minimum possible value.

MACsec limitations

- On Cisco N9324C-SE1U switch, MACsec is supported on all 24 QSFP28 ports.
- On Cisco N9348Y2C6D-SE1U switch, MACsec is supported on all 48 SFP28, 6 QSFP-DD, and 2 QSP28 ports.
- The MACsec SecY statistics do not support any statistical information related to egress Secure Association (SA) counters. Egress statistical data always displays as zero.
- For EAPOL configuration, ensure the following requirements are met:
  - The EAPOL MAC address must be in the range 0180.C200.0000 to 0180.C200.00FF (the last byte can be from 0x00 to 0xFF) and the EtherType can be any value between 0x600 and 0xFFFF.
  - Any MAC address is allowed when the EtherType is set to the default value 0x888E.
  - The broadcast MAC address can be used with any EtherType value in the range 0x600 to 0xFFFF.