

# Secure Unified Access with Cisco Catalyst 2960-X, 2960-XR, 2960-CX, and 3560-CX Series Switches

## Overview

The Cisco Catalyst® 2960-X, 2960-XR, 2960-CX and 3560-CX Series Switches are the industry's leading access switching platforms, enabling increased business productivity and agility with features designed to address enterprise networking megatrends, such as IPv6 transition, Bring Your Own Device (BYOD), and mobility. The Cisco Catalyst 2960-X, 2960-XR, 2960-CX, and 3560-CX provide security features to enable these transitions in the network in a secure and efficient manner.

Cisco Catalyst 2960-X, 2960-XR, 2960-CX, and 3560-CX Series Switches provide a rich and comprehensive set of security features designed to:

- Secure the network from traffic interception, spoofing, and denial-of-service (DoS) attacks
- Control access to resources in your network with access control lists (ACLs), including ACLs based on user and/or device type
- Secure network access based on user identity and user role
- Provision device-based policies through device profiling
- Protect confidentiality and Integrity of network traffic through encryption (hardware capability)
- Securely boot digitally signed Cisco IOS® Software images

As a part of Cisco Unified Access™ architecture, the Cisco Catalyst 2960-X, 2960-XR, 2960-CX, and 3560-CX Series Switches represent a network infrastructure that is capable of distributed policy classification and enforcement at the access layer with the policy definitions from the Cisco One Policy platform, the Cisco Identity Services Engine (ISE).

The Cisco Catalyst 2960-X, 2960-XR, 2960-CX and 3560-CX Series Switches help secure networks and provide secure access through the following primary feature categories:

- **IPv4 First Hop Security (FHS):** Cisco Catalyst switches offer Cisco Integrated Security Features (ISF), an industry-leading solution that provides superior Layer 2 threat defense capabilities for mitigating man-in-the-middle attacks (such as MAC, IP, and Address Resolution Protocol [ARP] spoofing). Delivering powerful, easy-to-use tools to effectively prevent the most common and potentially damaging Layer 2 security threats, Cisco ISF provides robust security throughout the network.
- **IPv6 FHS:** IPv6 FHS raises a number of FHS concerns that were not present in IPv4. Those concerns stem from the protocol's unique manner in which it performs router and neighbor discovery, address assignment, and address resolution using Neighbor Discovery Protocol (NDP). These mechanisms can allow an attacker to deploy attacks such as traffic interception, DoS, or man in the middle.

- 
- **Device profiling:** Trends such as bring-your-own-device (BYOD) programs require customers to have visibility into the various types of devices accessing the network and to be able to administer access control, segmentation policies, and quality-of-service (QoS) policies based on the type of device connected. Cisco Catalyst switches have built-in device-profiling capabilities to identify the type of device connected and apply policies based on device type.
  - **Identity-based networking:** Cisco supports a wide range of authentication options, including IEEE 802.1x for managed devices and users, web authentication for guests or non-802.1x users, and MAC authentication bypass for unmanaged or non-802.1x devices. The order and priority of authentication methods can be configured along with behavior after 802.1x or AAA server failures.
  - **Cisco TrustSec:** Cisco TrustSec® technology enables role-based policy definitions in a centralized policy engine (Cisco ISE) and the distributed enforcement of those policies in the network infrastructure independent of network architecture. This provides for the ability to define granular policies based on user role, device, location, posture, and so on while making policy definition and change management operationally efficient.
  - **Encrypting traffic:** Hardware capability to encrypt traffic using IEEE 802.1AE-based MACsec on the Cisco Catalyst 3560-CX Series Switches.

Let's take a look at the detailed descriptions of each one of these categories of features.

### IPv4 First Hop Security

IPv4 FHS, also known as Cisco ISF, delivers powerful, easy-to-use tools to effectively prevent the most common and potentially damaging Layer 2 security threats. Cisco ISF includes the following:

- **Port Security:** Prevents MAC-address-flooding attacks by limiting the MAC addresses of stations allowed access to the same physical port. Port Security limits the number of learned MAC addresses to deny MAC address flooding.
- **DHCP Snooping:** Prevents Dynamic Host Configuration Protocol (DHCP) server spoofing and man-in-the-middle attacks with the access switch acting much like a small security firewall between users and the legitimate DHCP server. Network attackers can no longer assign themselves as the default gateway or reroute and monitor traffic flow between the two endpoints.
- **Dynamic ARP Inspection:** Prevents Address Resolution Protocol (ARP) spoofing by helping to ensure that the access switch relays only valid ARP requests and responses. This capability prevents malicious hosts from invisibly eavesdropping on the conversation between the two endpoints to glean passwords or data or to listen to IP phone conversations.
- **IP Source Guard:** Prevents IP host spoofing from attackers and Internet worms assuming a valid user's IP address. IP Source Guard permits forwarding of only packets with valid source addresses.

### IPv6 First Hop Security

Security has become one of the most popular subjects of IPv6 discussions. IPv6 FHS is a suite of features designed specifically to harden IPv6 link operation, as well as help with scale in large Layer 2 domains. The first hop for an end host is very often a Layer 2 switch. The first hop switch is strategically located to learn about all its neighbors, and hence the switch can easily either allow or deny certain types of traffic, end-node roles, and claims. It inspects the Neighbor Discovery Protocol (NDP) traffic, provides information about Layer 2 and Layer 3 binding, and monitors the use of the NDP by host to spot potentially abnormal behaviors.

---

Ultimately, the switch can block undesired traffic such as rogue Router Advertisement, rogue DHCP server advertisement, and data traffic coming from undesired IP addresses or prefixes.

The core IPv6FHS features available on Cisco Catalyst 2960-X, 2960-XR, 2960-Cisco, and 3560-CX Series Switches are:

- **RA Guard:** Blocks unauthorized Router Advertisements.
- **DHCP Guard:** Blocks unauthorized DHCP servers.
- **IPv6 Snooping:** Analyzes control and data switch traffic, detects IP address, and stores and updates them in a binding table.
- **Source Guard:** Blocks any data traffic from an unknown source (supported on the Catalyst 3560-CX Series Switches only).

### Device Profiling

Cisco Catalyst 2960-X, 2960-XR, 2960-Cisco, and 3560-CX switches support Device Sensor functionality built into Cisco IOS Software. Device Sensor captures protocol packets such as Cisco Discovery Protocol, Link Layer Discovery Protocol (LLDP), DHCP, H.323, and multicast Domain Name System (mDNS), as well as MAC Organizationally Unique Identifier (OUI) information from the end hosts and classifies the device based on a device database that is built into Cisco IOS Software. Device Sensor functionality is also supported in conjunction with the Cisco ISE. In Device Sensor functionality, the switch profiles the end host by capturing the protocol information and sending the protocol attribute information to Cisco ISE using Remote Authentication Dial-In User Service (RADIUS). This enables devices to be centrally classified and monitored in Cisco ISE in a scalable manner. Authorization policies, such as VLAN assignment or discretionary access control lists (DACLS) based on device type, can be defined in Cisco ISE. Also, Cisco IOS Auto SmartPort macros that configure additional configurations to the port can be triggered according to the device type that is determined through Device Sensor. These Auto SmartPort macros can also be pushed to the switch port from Cisco ISE.

### Identity-Based Networking

Cisco Identity-Based Networking Services (IBNS) enable enterprise policy enforcement of all users and hosts, whether managed or unmanaged. The solution promotes authentication to access the network. This authentication also serves as the basis for differentiating users and/or hosts, providing varying levels of access to networked resources based on corporate access policy. Cisco IBNS on Cisco Catalyst switches provides a very rich feature set of IEEE 802.1X and associated functionality designed to reduce the operational overhead associated with deploying 802.1X, while providing the flexibility to implement authentication and authorization policies required to maintain secure access. These new capabilities include:

- Flexible authentication that supports multiple authentication mechanisms, including 802.1X, MAC authentication bypass, and web authentication, using a single, consistent configuration
- Guest access capabilities integrated with Cisco ISE
- Open mode that enables a user-friendly environment for 802.1X operations
- Integration of device-profiling technology and guest access handling with Cisco switching to significantly improve security while reducing deployment and operational challenges
- Comprehensive policy management capabilities such as RADIUS change of authorization and downloadable access control lists (ACLs)
- End-to-end system troubleshooting, monitoring, and reporting capabilities

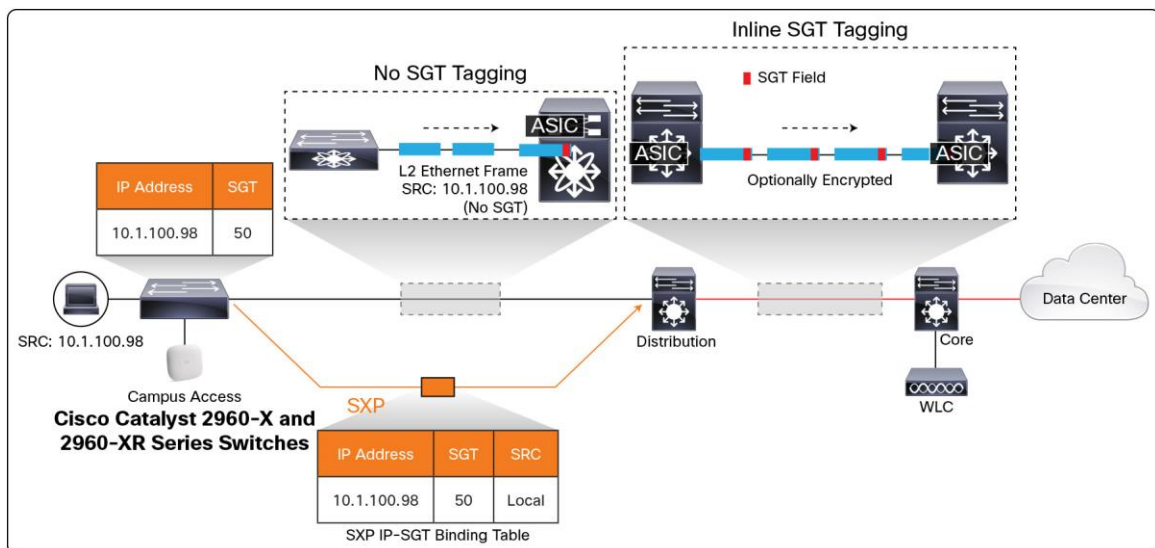
## Cisco TrustSec

Cisco TrustSec technology simplifies network security by defining security and access control permissions in terms of roles or security group tags rather than IP-based ACLs. The traffic from the end host is tagged with the identity information of the end host through a Cisco Security Group Tag (SGT). As the traffic flows through the network, the identity context of the traffic is carried throughout the network with the Cisco SGT tag, and appropriate security permissions can be applied to the traffic based on the Cisco SGT tag. These policies, called Security Group Access Control Lists (SGACLs), are based on identity information of the traffic derived from the Cisco SGT tag.

The Cisco Catalyst 3650-CX switch supports tagging packets with SGT. By using the SGT Exchange Protocol (SXP), Cisco Catalyst 2960-X, 2960-XR, 2960-Cisco, and 3560-CX switches can pass IP-address-to-SGT mappings to a Cisco TrustSec peer device that has hardware capable of using Cisco TrustSec technology.

The Cisco Catalyst 2960-X, 2960-XR, 2960-Cisco, and 3560-CX in the access layer perform 802.1X, MAB, and web-based authentication of the end host to determine the appropriate SGTs for ingress packets. The access layer switch learns the IP addresses of the source devices using IP device tracking and (optionally) DHCP snooping, and then uses SXP to pass the IP addresses of the source devices along with their SGTs to the distribution switches. Distribution switches with hardware capable of using Cisco TrustSec technology can use this IP-to-SGT mapping information to tag packets appropriately and to enforce SGACL policies (see Figure 1).

**Figure 1.** SXP Protocol to Propagate SGT Information



---

## For More Information

### IPv4 First Hop Security

[http://www.cisco.com/web/strategy/docs/gov/turniton\\_cisf.pdf](http://www.cisco.com/web/strategy/docs/gov/turniton_cisf.pdf)

### IPv6 First Hop Security

[http://www.cisco.com/web/about/security/intelligence/ipv6\\_first\\_hop.html](http://www.cisco.com/web/about/security/intelligence/ipv6_first_hop.html)

[http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/whitepaper\\_c11-602135.html](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/whitepaper_c11-602135.html)

[http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first\\_hop\\_security.html](http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html)

### Device Sensor

[http://www.cisco.com/en/US/docs/ios-xml/ios/sec\\_usr\\_aaa/configuration/15-1sg/sec-dev-sensor.html](http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_aaa/configuration/15-1sg/sec-dev-sensor.html)

### AutoSmartPorts

[http://www.cisco.com/en/US/docs/switches/lan/auto\\_smartports/15.0\\_1\\_se/configuration/guide/asp\\_cg.html](http://www.cisco.com/en/US/docs/switches/lan/auto_smartports/15.0_1_se/configuration/guide/asp_cg.html)

### Identity-Based Networking

[http://www.cisco.com/en/US/products/ps6638/products\\_ios\\_protocol\\_group\\_home.html](http://www.cisco.com/en/US/products/ps6638/products_ios_protocol_group_home.html)

<http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-overview.html>

### Cisco TrustSec Solutions

[http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/arch\\_over.html](http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/arch_over.html)

[http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing\\_DesignZone\\_TrustSec.html](http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html)



---

Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

Asia Pacific Headquarters  
Cisco Systems (USA) Pte. Ltd.  
Singapore

Europe Headquarters  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)