Turn It On

Power Up

Turn on all these features to leverage the full value of Cisco routers and switches.

- Protective QoS Features
  - Control Plane Policing (CoPP)
  - Network-Based Application Recognition (NBAR)
- VRF-Lite/Multi-VRF CE
- Advanced VPN Services:
  - Dynamic Multipoint VPN (DMVPN)
  - Group Encrypted Transport (GET VPN)
- **Catalyst Integrated Security Features (CISF)**
- Spanning-Tree Protocol (STP) Toolkit
- Encapsulated Remote Switched Port Analyzer (ERSPAN)
- Dynamic Intelligent Routing Solutions
  - IP Service-Level Agreement (IPSLA)
  - Optimized Edge Routing (OER)
  - Embedded Event Manager (EEM)

Contact your Cisco Systems Engineer for more information and assistance in turning on the full functionality of your Cisco routers and switches.

To learn about enabling additional Cisco features, visit **www.cisco.com/go/turniton.**

To help you get the most functionality, value and ROI from your Cisco routers and switches, we want to ensure you're aware of the many powerful features residing within. Our Turn it On program is designed to empower Federal agencies like yours to take full advantage of Cisco's powerful core networking solutions to maximize your productivity, efficiency and technology investment.

Catalyst Integrated Security Features (CISF)

Layer 2 switched environments can prove easy targets for security attacks. These attacks exploit normal protocol processing such as a switches' ability to learn MAC addresses, end-station Media Access Control (MAC) address resolution through Address Resolution Protocol (ARP) or Dynamic Host Configuration Protocol (DHCP) IP address assignments. And because any user can gain access to any Ethernet port and potentially hack into the network using readily available, menu-driven hacker tools available on the Internet, open campus networks cannot guarantee network security.

The rich set of industry-leading integrated security features on Cisco Catalyst Switches (CISF) proactively protect your critical network infrastructure. Delivering powerful, easy-to-use tools to effectively prevent the most common—and potentially damaging—Layer 2 security threats, CISF provides robust security throughout the network. And these powerful features already reside on your Cisco Catalyst switches. All you have to do is turn them on.

Strong protection against common attacks

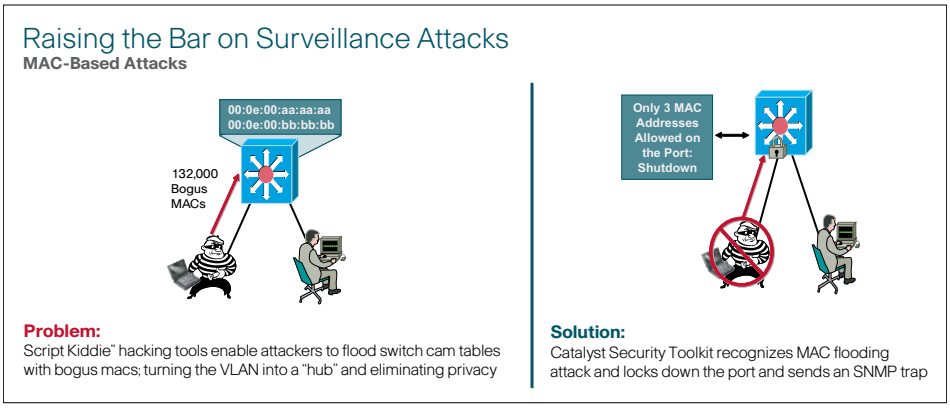
CISF works on switchports to intelligently guard against today's most prevalent and potentially crippling attacks.

CISF 1: Port Security

Function: Shuts down MAC address-flooding attacks

How it Works: Limits and identifies the MAC addresses of stations allowed access to the same physical port. When a switch is either configured for static MAC addresses or dynamically learns them, Port Security limits the number of learned MAC addresses to deny MAC address-flooding.

Raising the Bar on Surveillance Attacks – MAC-Based Attacks

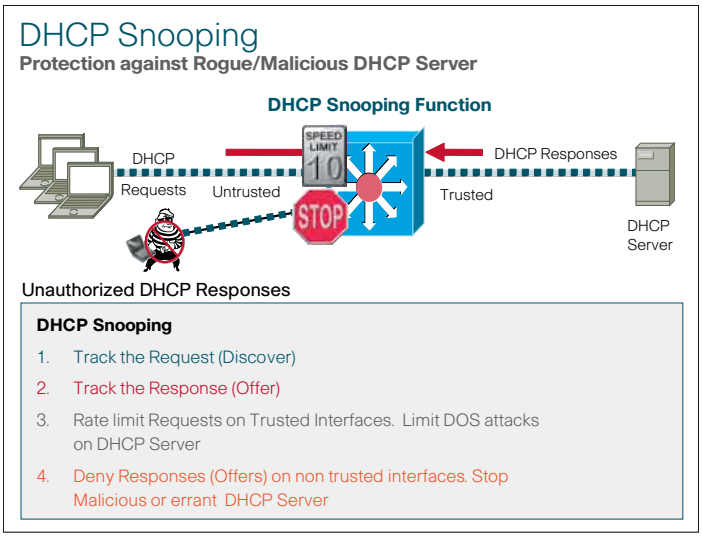


CISF 2: DHCP Snooping

Function: Prevents against server spoofing and "man in the middle" attacks

How it Works: Easily enabled on all Layer 2 ports, Cisco's patented DHCP Snooping feature defines trusted ports for legitimate DHCP servers that can send DHCP requests and offers. By intercepting all DHCP messages within the VLAN, the switch acts 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.

DHCP Snooping Protection against Rogue/Malicious DHCP Server



CISF 3: Dynamic ARP Inspection

Function: Adds security to ARP using DHCP snooping table

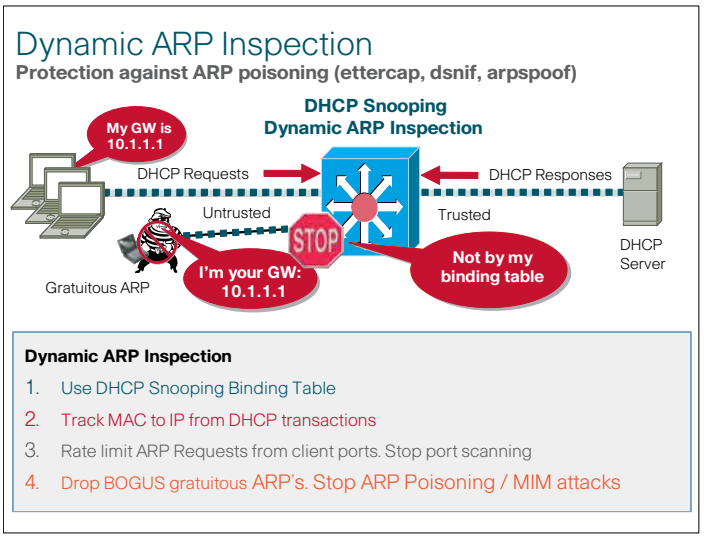
How it Works: Cisco's patented Dynamic ARP Inspection (DAI) feature helps ensure that the access switch relays only "valid" ARP requests and responses. DAI intercepts every ARP packet on the switch, and verifies the ARP information before updating the switch ARP cache or forwarding packets to the appropriate destination. This prevents malicious hosts from invisibly eavesdropping on the conversation between the two endpoints to glean passwords, data or listen to IP phone conversations.

Make the switch to security

Cisco's Integrated Security Features are available in varying capacities on these Catalyst switches, as well as on some End-of-Sale (EoS) switches.

- 3560/3560-E
- 3750/3750-E
- 4500
- 6500

Dynamic ARP Inspection Protection against Recognizance/ ARP Scan's

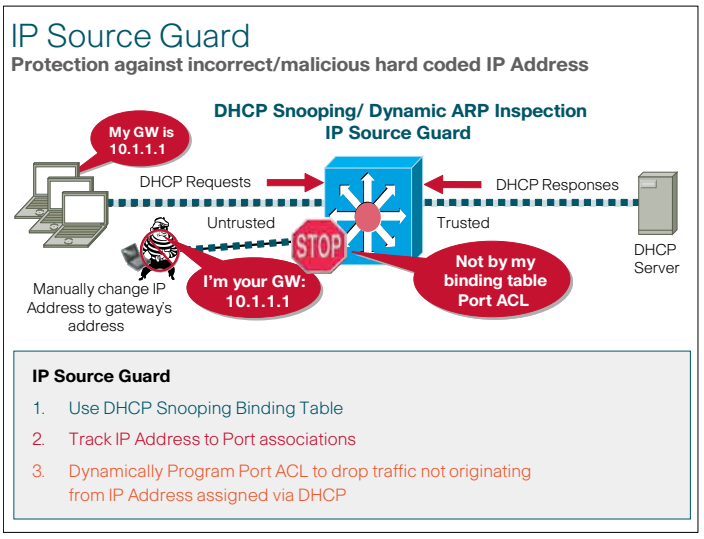


CISF 4: IP Source Guard

Function: Prevents IP host spoofing

How it works: Prevents attackers and Internet worms from launching attacks by assuming a valid user's IP address. IP Source Guard only permits forwarding of packets with valid source addresses.

IP Source Guard Protection against incorrect/malicious hard coded IP Address



Notes

- The 4 items that make up CISF's are available in different fashions on different switches. In fact some of the features are available on EoS switches as well.
- Everything here is inline with a secure port. With a dynamically learned mac address we can limit the number of learned mac addresses in order to deny mac address-flooding.

Contact your Cisco Systems Engineer for more information and assistance in turning on the full functionality of your Cisco routers and switches. To learn about enabling additional Cisco features, visit **www.cisco.com/go/turniton**.