



Why Should I Care About Security?

With the rise of network problems caused by any user having access to any Ethernet port and potentially hacking into the systems, open campus networks cannot guarantee network security. The Cisco® Catalyst® 4500 Series classic and E-Series supervisor engines offer powerful techniques to effectively prevent untraceable man-in-the-middle attacks, control-plane resource exhaustion, IP spoofing, and flooding attacks without any change to the end user or host configurations. The new Cisco Catalyst 4500 Series Supervisor Engine 6-E helps ensure complete LAN access protection enabled by the new CenterFlex technology.

Common Security Threats

Unfortunately the skill level required to launch security attacks is minimal because of readily available, menu-driven hacker tools available on the Internet.

Table 1 summarizes the general switch security features and mitigation techniques for the most common and potentially damaging attacks.

Table 1. Security Features and Mitigation Techniques

Feature	Mitigation Technique
Port Security	Prevents MAC flooding attacks
DHCP Option 82 and DHCP Snooping	Secures DHCP transactions
Dynamic ARP Inspection (DAI)	Prevents man-in-the-middle attacks
IP Source Guard	Prevents IP spoofing
IEEE 802.1x Enhancements	Implements authentication and guest virtual LAN (VLAN) concept
Layer 2–4 Access Control Lists (ACLs) Including Port-Based ACL (PACL)	In isolated networks, limits IP addresses per customers on a port
Unicast Reverse Path Forwarding (uRPF)	Mitigates the denial-of-service attacks in a hacker attempt to spoof IP addresses to get access to a host

Note: It is important to understand that use of authentication and security features such as IEEE 802.1x and ACLs, while an integral part of an organization's threat-defense policies, cannot prevent security attacks. An authenticated user might have malicious intention and can easily implement all of these attacks.

Innovative Security Features on the Cisco Catalyst 4500 E-Series

The integrated security features on the Cisco Catalyst 4500 classic and E-Series supervisor engines can help prevent common security threats. Following is a summary of each threat and the security feature to prevent the attacks.

MAC Address Flooding Attacks

The switch has a bound memory space for the number of MAC addresses that can be learned in its forwarding table. Attacks that attempt to flood or overflow this table exploit the inherent MAC address learning capability and forwarding behavior of switches. The attacks exploit this natural hardware restriction by flooding the switch with unknown MAC addresses, which the switch will then learn. However, after the Layer 2 forwarding table limit is exceeded, packets are flooded to all ports in a VLAN, enabling a hacker to eavesdrop (or "sniff") network connections over a switched network while disrupting network performance.

MAC Address Flooding Attack Mitigation: Port Security

The Port Security feature can be used to limit and identify the MAC addresses of the stations that are allowed access to the same physical port. When a switch assigns MAC addresses to a secure port statically or dynamically, the port does not forward packets with source addresses outside the group of defined addresses. Limiting the number of allowable MAC addresses on a switch port using Port Security effectively shuts down a MAC address flooding attack.

DHCP Server Spoofing and "Man-in-the-Middle" Attacks

A rogue DHCP server is typically used by network attackers who give out IP host addresses and assign themselves as the default gateway, making it possible to reroute normal traffic flow between two endpoints, seeing all of the traffic between the two endpoints, hence the term "man-in-the-middle" attack.

DHCP Server Spoofing and "Man-in-the-Middle" Attack Mitigation: DHCP Snooping

A patented Cisco feature known as DHCP Snooping can be easily enabled on all Layer 2 ports. This 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 can act like a small security firewall between users and the legitimate DHCP server.

ARP-Based Man-in-the-Middle Attacks

ARP, in its most basic function, is used to allow two stations to communicate on a LAN segment. An attacker can send an ARP packet with a spoofed source address, causing the default gateway or another host to learn about it and store it in its ARP table. ARP will then create an entry in the targeted host for this malicious host without performing any type of authentication or filtering, making the network vulnerable. The malicious host can now eavesdrop on the conversation between the two endpoints without either endpoint being aware. The attacker can then collect passwords and data or listen to IP phone conversations.

ARP-Based Man-in-the-Middle Attack Mitigation: Dynamic ARP Inspection

This attack can be easily prevented through another patented Cisco security feature, Dynamic ARP Inspection (DAI), which 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.

IP Host Spoofing Attacks

An IP address-spoofing attacker can impersonate a valid address either by manually changing an address or by running a program designed to perform address spoofing. Internet worms can also use spoofing techniques to disguise their origins.

IP Host Spoofing Attack Mitigation: IP Source Guard

Using the IP Source Guard feature, an attacker cannot launch an attack by assuming a valid user's IP address. This feature will only permit forwarding of packets that have valid source addresses.

What Security Enhancements Does CenterFlex Technology Enable on the Cisco Catalyst 4500 Series Supervisor Engine 6-E?

Unicast Reverse Path Forwarding

With the addition of new Supervisor Engine 6-E, the uRPF filtering mechanism is enabled in hardware. It is supported in both IPv4 and IPv6; uRPF is used to prevent IP address spoofing. It examines each packet received as input on an interface, and blocks inbound source IP addresses that do not have a route in the routing table pointing back at the same interface on which the packet arrived.

Why Cisco Catalyst Integrated Security Features?

The Cisco Catalyst 4500 E-Series and classic supervisor engines have ample dedicated hardware resources to implement security features and offer a rich set of industry-leading, integrated security features to

proactively lock down your critical network infrastructure. Figure 1 graphically summarizes the security features.

Figure 1. Cisco Catalyst Integrated Security Features

For additional information, visit:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/index.htm>

