Port Security for EX Series Switches Overview

Ethernet LANs are vulnerable to attacks such as address spoofing (forging) and Layer 2 denial of service (DoS) on network devices. Port security features help protect the access ports on your switch against the losses of information and productivity that can result from such attacks.

Juniper Networks JUNOS Software on Juniper Networks EX Series Ethernet Switches provides features to help secure ports on the switch. The ports can be categorized as either trusted or untrusted. You apply policies appropriate to those categories to protect against various types of attacks.

Port security features can be turned on to obtain the most robust port security level. Basic port security features are enabled in the switch's default configuration. You can configure additional features with minimal configuration steps.

Port security features on EX Series switches are:

- DHCP snooping—Filters and blocks ingress DHCP server messages on untrusted ports; builds and maintains an IP-address/MAC-address binding database (called the DHCP snooping database). You enable this feature on VLANs.
- Dynamic ARP inspection (DAI)—Prevents ARP spoofing attacks. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made based on the results of those comparisons. You enable this feature on VLANs.
- MAC limiting—Protects against flooding of the Ethernet switching table (also known as the MAC forwarding table or Layer 2 forwarding table). You enable this feature on access interfaces (ports).
- MAC move limiting—Detects MAC movement and MAC spoofing on access ports. You enable this feature on VLANs.
- Trusted DHCP server—With a DHCP server on a trusted port, protects against rogue DHCP servers sending leases. You enable this feature on interfaces (ports). By default, access ports are untrusted and trunk ports are trusted. (Access ports are the switch ports that connect to Ethernet endpoints such as user PCs and laptops, servers, and printers. Trunk ports are the switch ports that connect to other Ethernet switches or to routers.)
- IP source guard—Mitigates the effects of IP address spoofing attacks on the Ethernet LAN. You enable this feature on VLANs. With IP source guard enabled, the source IP address in the packet sent from an untrusted access interface is validated against the source MAC address in the DHCP snooping database. The packet is allowed for further processing if the source IP address to source MAC address binding is valid; if the binding is not valid, the packet is discarded.
- DHCP option 82—Also known as the DHCP relay agent information option. Helps protect the EX Series switch against attacks such as spoofing of IP addresses and MAC addresses and DHCP IP address starvation. Option 82 provides information

about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.

- Unrestricted proxy ARP—For additional access port security on EX Series switches, you can choose to use unrestricted proxy Address Resolution Protocol (ARP). With unrestricted proxy ARP, hosts cannot communicate directly with one another. Instead all communications must go through the switch. If you enable proxy ARP on an EX Series switch, the mode is unrestricted by default (that is the only mode supported) and it applies globally to all interfaces on the switch. The switch responds to any ARP request on condition that the switch has an active route to the destination address.

Related Topics

- Security Features for EX Series Switches Overview
- Understanding DHCP Snooping for Port Security on EX Series Switches
- Understanding DAI for Port Security on EX Series Switches
- Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches
- Understanding IP Source Guard for Port Security on EX Series Switches
- Understanding DHCP Option 82 for Port Security on EX Series Switches
- Understanding How to Protect Access Ports on EX Series Switches from Common Attacks
- Understanding Proxy ARP for Port Security on EX Series Switches

---

Published: 2009-07-23