Core Switch ARP Prevention

Article Overview

Prevent ARP attacks on core switches using ARP inspection, rate limiting, dynamic ARP protection, and port security to maintain network stability and prevent spoofing.

ARP Flood and Broadcast Storm Prevention

To prevent ARP floods or broadcast storms, configure ARP rate limiting on the switch. This can be done based on source IP addresses, MAC addresses, or interfaces, limiting the number of ARP packets a device can send per second. For example, you can set a maximum rate of ARP packets per host or per interface to prevent a single device from overwhelming the network . Additionally, storm control can be enabled on Cisco switches to monitor and restrict broadcast traffic, including ARP packets .

ARP Spoofing Protection

ARP spoofing can redirect traffic to an attacker's device. To mitigate this, enable dynamic ARP protection or ARP inspection. These features validate ARP packets against a trusted database of IP-to-MAC bindings, often populated via DHCP snooping. Only ARP requests and replies with valid bindings are allowed; invalid packets are dropped . On Cisco devices, this can be implemented using IP Source Guard and ARP anti-spoofing commands, which discard unknown or malicious ARP packets .

Interface and VLAN-Based Controls

o Interface-based ARP entry limits: Restrict the number of ARP entries a port can learn dynamically to prevent a single interface from flooding the ARP table .
o VLAN segmentation: Place devices in separate VLANs and configure VLANIF interfaces with IP addresses to isolate ARP traffic and reduce broadcast domains .
o Trusted vs. untrusted ports: Mark uplinks to servers or routers as trusted and access ports as untrusted to ensure ARP inspection only applies to client devices .

Best Practices
o Enable DHCP snooping to maintain a reliable IP-to-MAC binding database.
o Regularly monitor ARP tables and network traffic to detect anomalies.
o Check for duplicate IP addresses, which can trigger ARP storms .
o Combine multiple protections: rate limiting, ARP inspection, port security, and VLAN segmentation for layered defense.
o Update switch firmware to ensure support for advanced ARP security features . By implementing these measures, core switches can effectively prevent ARP floods, spoofing, and broadcast storms, ensuring stable and secure network operations.

Dynamic ARP Inspection (DAI) prevents man-in-the-middle attacks and IP address spoofing by checking that packets from untrusted

Configure ARP rate limiting based on source MAC addresses and source IP addresses to prevent a large number of ARP packets

This example will instruct the administrator on how to configure the switch to protect the network from attackers using the same IP

Learn what Dynamic ARP Inspection (DAI) is, why it"s needed, how it protects the LAN from ARP spoofing, and how to configure and

On the VLAN interfaces of a routing switch, dynamic ARP protection ensures that only valid ARP requests and responses are

AnARPspoofingattackcanaffecthosts,switches,androutersconnectedtoyournetworkbyfloodingpackets

Introduction This document describes information to secure your Cisco IOS XE Software system devices, which increases the overall

We"ll illustrate their deployment in a large-scale network scenario involving approximately 100 switches (a mix of

Some users on my network using wifikill or netcut to prevent other users from accessing the internet [ISP"s router: public IP] - [

This document describes the information to help you secure your Cisco IOS® system devices, which increases the

When assessing the core switch connected to 13 edge switches and executing the "show

Hi I need to help with this attacks in my network, we work with virtualization and everyone copy the VMs, this

Home Support Technology White Papers ARP Attack Protection Technology White Paper-6W100

I also accidentally placed a duplicate IP on two devices on the same VLAN/subnet. Can duplicate IP cause an ARP

Core Switch ARP Prevention

As it is clear from the title, why do switches need ARP tables when the translation are done on the machines side?

ARP spoofing attacks and ARP cache poisoning can occur because ARP allows a reply from a host even if an ARP

Web: https://morwarreconst.co.za