NETWORK SWITCHING FEATURES

ARP INSPECTION

Document ID: SW-ARP-001
Revision ID: 01 | Revision Date: 29-08-2024

Table of Contents

Glossary

The following terms are frequently used in this document.

Term	Definition
ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
DAI	Dynamic ARP Inspection
VLAN	Virtual Local Area Network
IP	Internet Protocol
MAC	Media Access Control
DOS	Denial Of Service
NIC	Network Interface Card
OSI	Open Systems Interconnection
MITM	Man-In-The-Middle

Functional Description

Address Resolution Protocol (ARP) is a fundamental protocol in network communication that bridges the gap between logical (IP) and physical (MAC) addresses. When a device needs to send data to another device on the same network, it initially only knows the destination's IP address. ARP is responsible for determining the corresponding MAC address, which is essential for frame encapsulation and transmission.

IP address: A 32-bit logical address assigned to a device for network identification.

MAC address: A 48-bit physical address unique to each network interface card (NIC).

ARP operates at Layer 2 (Data Link layer) of the OSI model, where data frames are prepared for transmission. It maintains a cache of IP-to-MAC address mappings to improve efficiency. When a device needs to send a packet to a destination IP address, it first checks its ARP cache. If the MAC address is found, it directly encapsulates the packet in a frame with the destination MAC

address. If not, it broadcasts an ARP request to discover the MAC address. The destination device responds with an ARP reply, and the sender updates its ARP cache.

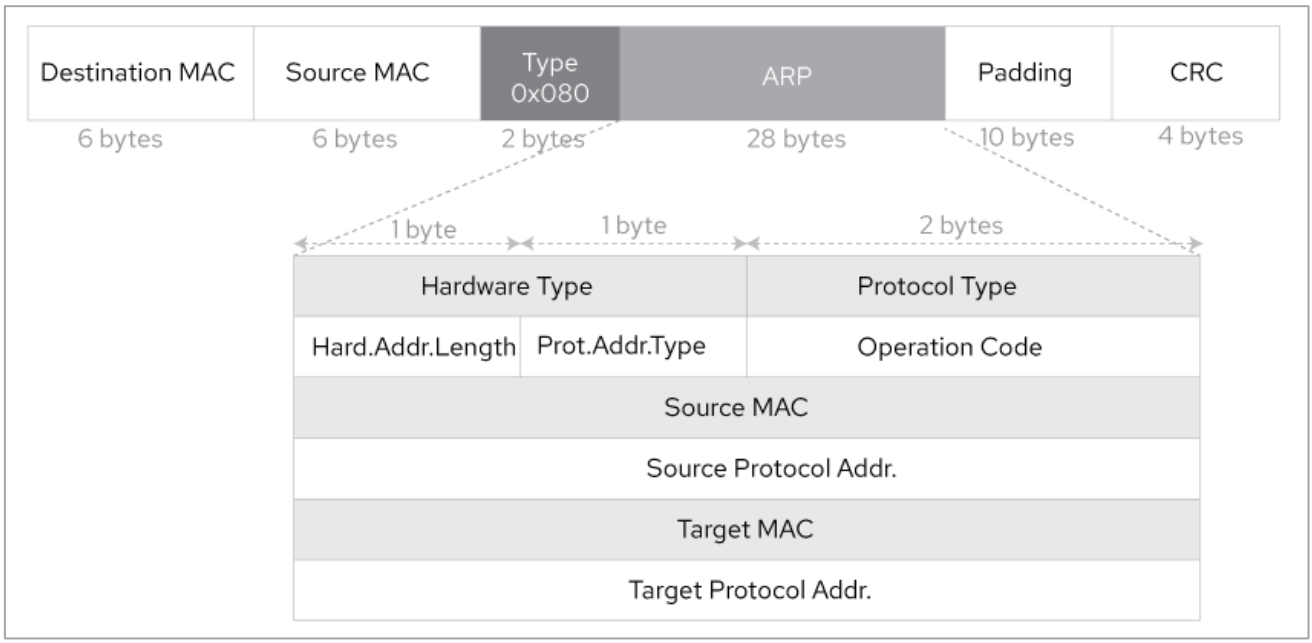

Fig.1

- **Hardware type**—Hardware address type. The value 1 represents Ethernet.
- **Protocol type**—Type of the protocol address to be mapped. The hexadecimal value 0x0800 represents IP.
- **Hardware address length and protocol address length**—Length, in bytes, of a hardware address and a protocol address. For an Ethernet address, the value of the hardware address length field is 6. For an IPv4 address, the value of the protocol address length field is 4.
- **OP**—Operation code, which describes the type of ARP message. The value 1 represents an ARP request, and the value 2 represents an ARP reply.
- **Sender hardware address**—Hardware address of the device sending the message.
- **Sender protocol address**—Protocol address of the device sending the message.
- **Target hardware address**—Hardware address of the device to which the message is being sent.
- **Target protocol address**—Protocol address of the device to which the message is being sent.

The Threat of ARP Poisoning

ARP, while essential, is vulnerable to attacks. **ARP poisoning** occurs when a malicious actor broadcasts forged ARP replies, claiming to be the default gateway or another device on the network. This misleads other devices into updating their ARP cache with incorrect MAC addresses. As a result, the attacker can intercept and potentially modify traffic intended for other hosts.

Consequences of ARP poisoning include:

- **Man-in-the-middle attacks:** The attacker can eavesdrop on network traffic, steal sensitive information, and inject malicious content.
- **Denial of Service (DoS):** By flooding the network with forged ARP replies, the attacker can disrupt normal network operations.
- **Session hijacking:** The attacker can take control of established network sessions.

To protect against ARP poisoning, network devices employ **Dynamic ARP Inspection (DAI)**.

Dynamic ARP inspection is a security feature that validates ARP packets in a network. Dynamic ARP inspection determines the validity of packets by performing an IP-to-MAC address binding inspection stored in a trusted database, (the DHCP snooping binding database) before forwarding the packet to the appropriate destination. Dynamic ARP inspection will drop all ARP packets with invalid IP-to-MAC address bindings that fail the inspection. The DHCP snooping binding database is built when the DHCP snooping feature is enabled on the VLANs and on the switch.

Below diagram shows an example of an attacker attempting to spoof and hijack traffic for an important address (a default gateway in this example) by broadcasting to all hosts spoofing the MAC address of the router (using a gratuitous ARP). This will poison ARP cache entries (create an invalid ARP entry) on Host A and Host B, resulting in data being redirected to the wrong destination. Because of the poisoned entries, when Host A sends data destined for the router, it is incorrectly sent to the attacker instead. Dynamic ARP inspection locks down the IP-MAC mapping for hosts so that the attacking ARP is denied and logged.

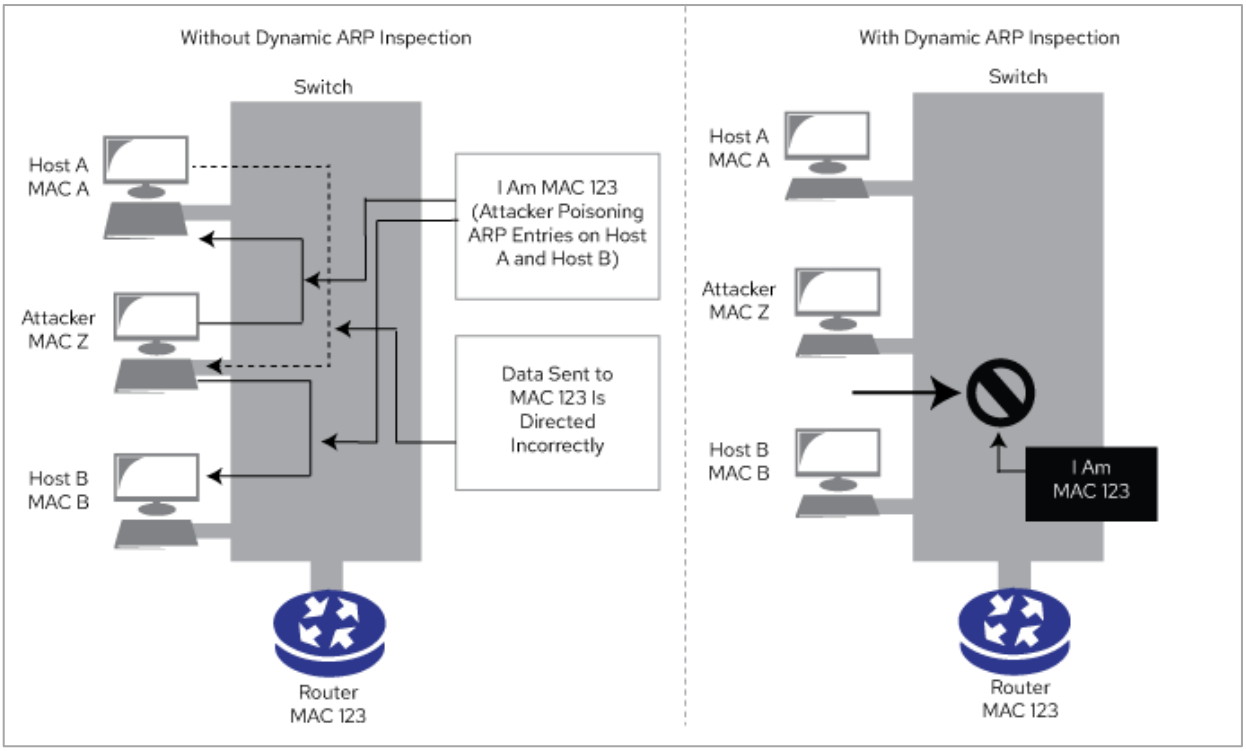

Fig. 2

The dynamic ARP Inspection (DAI) feature safeguards the network from many of the commonly known man-in-the-middle (MITM) type attacks. Dynamic ARP Inspection ensures that only valid ARP requests and responses are forwarded.

Below diagram shows an example of the DAI feature in action and shows how the intruder is blocked on the untrusted port when it is trying to poison ARP entries.

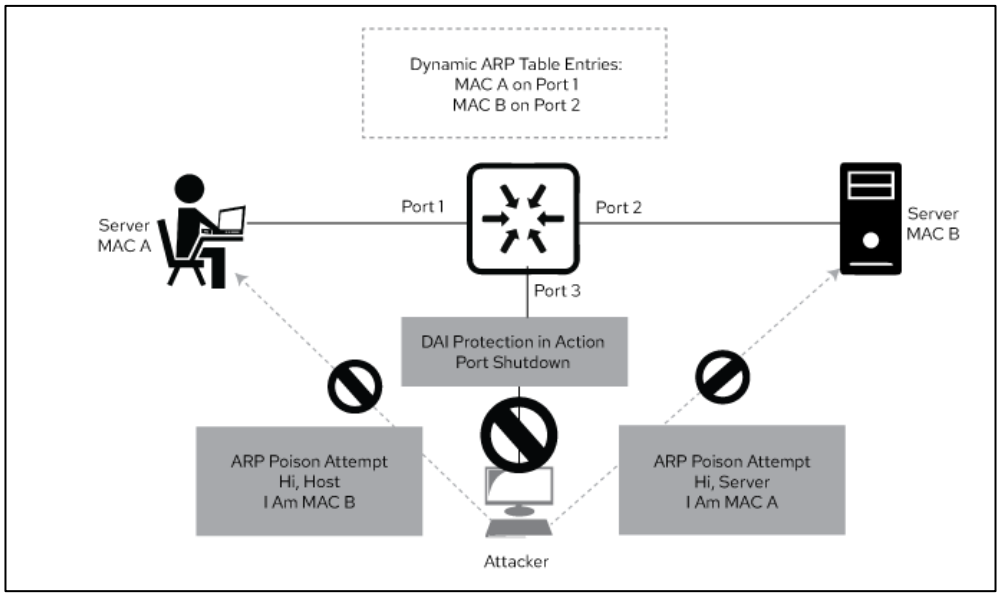

Fig. 3

- The attacker on Port 3 sends an **ARP Poison Attempt** to the host on Port 1, pretending to be MAC B (the server on Port 2).

- Simultaneously, the attacker sends another **ARP Poison Attempt** to the server on Port 2, pretending to be MAC A (the host on Port 1).

DAI Protection Mechanism:

- **DAI in Action**: The switch, using DAI, inspects the ARP packets. Since the ARP messages from the attacker do not match the information in the dynamic ARP table (MAC A on Port 1 and MAC B on Port 2), the switch detects the spoofing attempt.

ARP Inspection in QN switches

Commands Outline

Use the ip arp inspection Global Configuration mode command globally to enable Address Resolution Protocol (ARP) inspection. Use the no form of this command to disable ARP inspection.

```
switch(config)# ip arp inspection
```

Use the ip arp inspection vlan Global Configuration mode command to enable ARP inspection on a VLAN, based on the DHCP Snooping database. Use the no form of this command to disable ARP inspection on a VLAN.

```
switch(config)# ip arp inspection vlan <Specify vlan Num>
```

Use the ip arp inspection trust Interface Configuration (Ethernet, Port-channel) mode command to configure an interface trust state that determines if incoming Address Resolution Protocol (ARP) packets are inspected. Use the no form of this command to restore the default configuration.

```
switch(config)# interface <interface Num>
switch(config-if) # ip arp inspection trust
```

Use the show ip arp inspection EXEC mode command to display the ARP inspection configuration for all interfaces or for a specific interface.

```
switch# show ip arp inspection
IP ARP inspection is Enabled
IP ARP inspection is configured on following VLANs: 1
Verification of packet header is Enabled
IP ARP inspection logging interval is: 222 seconds
Interface Trusted
```

```
..... .....
te1/0/ 1 Yes
te1/0/ 2 Yes
```

Dynamic ARP inspection

Dynamic ARP Inspection (DAI) works by inspecting ARP packets on the network. It typically uses information from the DHCP snooping database on the switch to validate the ARP packets. The DHCP snooping database keeps track of the IP addresses and MAC addresses of devices that have obtained IP addresses from a DHCP server.

DAI compares the MAC address and IP address information in the ARP packets with the information in the DHCP snooping database. If there is a mismatch, DAI drops the ARP packet, preventing the attacker from spoofing the IP address.

Static ARP Inspection

In static ARP inspection, you have to bind an IP address with its MAC address manually. A user can add a static ARP entry in the ARP table to bind the MAC address and IP address. The switch then checks the entry in the ARP table and drops the ARP packet if it doesn't match, preventing the attacker from spoofing the IP address.

Configuration Steps

Scenario 1

Let's consider that we are applying ARP inspection on a switch to prevent users from using static IP addresses and ensure that every user obtains an IP address from a legitimate DHCP server.

As shown in Fig. 4, we will enforce users to use only DHCP-assigned IP addresses, and for that, we will configure Dynamic ARP Inspection (DAI).

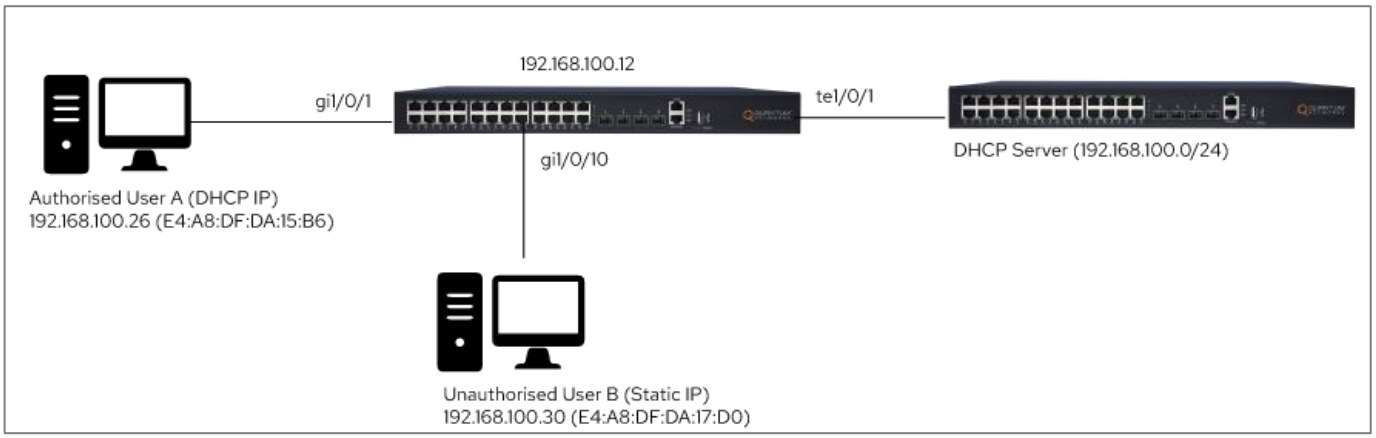

Fig. 4

First of all, we will enable IP DHCP snooping globally. Enabling **DHCP Snooping** on a network switch is necessary for **Dynamic ARP Inspection (DAI)** because DHCP Snooping builds and maintains a trusted database of IP-to-MAC address bindings. DAI uses this database to verify ARP packets against legitimate IP-MAC bindings, effectively preventing ARP spoofing attacks.

```
console(config)#ip dhcp snooping
```

To configure the switch to store DHCP snooping binding information. This helps to protect the network from DHCP spoofing attacks by maintaining a record of which IP addresses are assigned to which devices. The database allows the switch to enforce DHCP policies and validate DHCP messages more effectively.

```
console(config)#ip dhcp snooping database
<optional command>
```

To allow DHCP snooping information to be accepted from untrusted ports, which helps to preserve DHCP option data in scenarios where DHCP servers are connected to these ports.

```
console(config)#ip dhcp snooping information option allowed-untrusted
<optional command>
```

To configure a device, to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address.

```
console(config)#ip dhcp snooping verify
<optional command>
```

Enabling DHCP Snooping on a VLAN is crucial for ARP Inspection because DHCP Snooping monitors and records IP-to-MAC address bindings specifically within that VLAN. ARP Inspection relies on this binding information to accurately validate ARP packets within the same VLAN.

```
console(config)#ip dhcp snooping vlan 1
```

Navigate to the interface, to define dhcp snooping trust.

```
console(config)#interface ten1/0/1
```

Enable dhcp snooping trust, to ensure that legitimate DHCP servers and trusted devices can send DHCP offers and acknowledgments. Without setting specific interfaces as trusted, DHCP Snooping would block all DHCP traffic on those interfaces, potentially disrupting network services. By marking certain interfaces as trusted, ARP Inspection can correctly validate ARP packets and prevent spoofing while allowing legitimate DHCP communications to occur.

console(config-if)#ip dhcp snooping trust

Enable arp inspection trust, to allow legitimate ARP traffic to pass through without being blocked. Trusted interfaces are typically connected to devices or networks that are known to be secure, such as routers or other switches. By marking these interfaces as trusted, ARP Inspection can focus on inspecting and validating ARP traffic on untrusted interfaces, effectively preventing ARP spoofing while ensuring legitimate ARP communications are not disrupted.

console(config-if)#ip arp inspection trust

Now, exit the current interface configuration mode and return to the global configuration mode.

console(config-if)#exit

Enable arp inspection globally, because it activates the feature across the network device, allowing it to inspect ARP packets for potential spoofing. This global setting ensures that the device will check ARP packets against a trusted database or a security policy to prevent ARP spoofing attacks, which can compromise network integrity by redirecting or intercepting traffic.

console(config)#ip arp inspection

IP ARP Inspection List is a feature used in network security to protect against ARP (Address Resolution Protocol) spoofing attacks. ARP spoofing is a type of attack where an attacker sends falsified ARP messages on a network, allowing them to intercept, modify, or stop network traffic between devices.

console(config)#ip arp inspection list
<optional command>

To set the frequency at which ARP (Address Resolution Protocol) inspection logs are generated. These logs help in monitoring and troubleshooting ARP activities and issues, such as ARP spoofing attacks, by recording events at the specified interval. This command allows network administrators to control the amount of log data generated and manage the system's logging resources effectively.

console(config)#ip arp inspection logging interval <0-86400>/infinite
<optional command>

Arp inspection validate, to ensure ARP packets are checked for correct IP-to-MAC address mappings, preventing ARP spoofing and improving network security.

console(config)#ip arp inspection validate
<optional command>

Enable arp inspection on vlan, to prevent ARP spoofing attacks within that VLAN by ensuring ARP packets are validated against a trusted database, thus protecting network devices from malicious or incorrect ARP responses.

```
console(config)#ip arp inspection vlan 1
```

Scenario 2

Let's consider that we want to bind an IP address and MAC address to a port to ensure that no user with a different combination of MAC and IP addresses can gain access.

As shown in Fig. 1, we will bind the IP address and MAC address of User B to ensure that no other user can gain access to that VLAN. For this, we will configure Static ARP Inspection.

We will enable IP DHCP snooping globally. Enabling **DHCP Snooping** on a network switch is necessary for **Dynamic ARP Inspection (DAI)** because DHCP Snooping builds and maintains a trusted database of IP-to-MAC address bindings. DAI uses this database to verify ARP packets against legitimate IP-MAC bindings, effectively preventing ARP spoofing attacks.

```
console(config)#ip dhcp snooping
```

Enabling DHCP Snooping on a VLAN is crucial for ARP Inspection because DHCP Snooping monitors and records IP-to-MAC address bindings specifically within that VLAN. ARP Inspection relies on this binding information to accurately validate ARP packets within the same VLAN.

```
console(config)#ip dhcp snooping vlan 1
```

Navigate to the interface, for define dhcp snooping trust.

```
console(config)#interface ten1/0/1
```

Enable dhcp snooping trust, to ensure that legitimate DHCP servers and trusted devices can send DHCP offers and acknowledgments. Without setting specific interfaces as trusted, DHCP Snooping would block all DHCP traffic on those interfaces, potentially disrupting network services. By marking certain interfaces as trusted, ARP Inspection can correctly validate ARP packets and prevent spoofing while allowing legitimate DHCP communications to occur.

```
console(config-if)#ip dhcp snooping trust
```

Enable arp inspection trust, to allow legitimate ARP traffic to pass through without being blocked. Trusted interfaces are typically connected to devices or networks that are known to be secure, such as routers or other switches. By marking these interfaces as trusted, ARP Inspection

can focus on inspecting and validating ARP traffic on untrusted interfaces, effectively preventing ARP spoofing while ensuring legitimate ARP communications are not disrupted.

```
console(config-if)#ip arp inspection trust
```

Now, exit the current interface configuration mode and return to the global configuration mode.

```
console(config-if)#exit
```

Enable arp inspection globally, because it activates the feature across the network device, allowing it to inspect ARP packets for potential spoofing. This global setting ensures that the device will check ARP packets against a trusted database or a security policy to prevent ARP spoofing attacks, which can compromise network integrity by redirecting or intercepting traffic.

```
console(config)#ip arp inspection
```

Enable arp inspection on vlan, to prevent ARP spoofing attacks within that VLAN by ensuring ARP packets are validated against a trusted database, thus protecting network devices from malicious or incorrect ARP responses.

```
console(config)#ip arp inspection vlan 1
```

Now, exit the current interface configuration mode and return to the global configuration mode.

```
console(config)#exit
```

To manually bind MAC address and IP address on a particular interface to validate ARP packets.

```
console#ip dhcp snooping binding  e4:a8:df:da:17:d0 1 192.168.100.30 gig1/0/1
```

Verifying the configuration

```
console#show ip dhcp snooping binding
Total number of binding: 1

MAC Address        IP Address       Lease (sec)  Type       VLAN  Interface
-----------------  ---------------  -----------  ---------  ----  -----------
e4:a8:df:da:17:d0  192.168.100.30       -        snooping    1     gig1/0/10
```

Whenever an unauthorized user attempts to connect to a switch, we will receive the following log.

console(config)#24-Jul-2024 04:40:13 %ARPINSP-I-PCKTLOG: ARP packet dropped from port ten1/0/1 with VLAN tag 1 and reason: packet verification failed
SRC MAC E4:A8:DF:DA:17:D0 SRC IP 192.168.100.1 DST MAC 00:00:00:00:00:00 DST IP 192.168.100.30

Notes & Limitations

- **Default state of ARP Inspection:** ARP Inspection is disabled by default.
- **Untrusted port configuration:** If a port is configured as an untrusted port, it should also be configured as an untrusted port for DHCP Snooping, or the IP address and MAC address binding for this port should be configured statically. Otherwise, hosts attached to this port cannot respond to ARP requests.
- **Trusted interface behaviour:** The switch does not check ARP packets received on the trusted interface; it simply forwards the packets.