

# StoneOS ARP And MAC Address Defense

## 1. Introduction

The proliferation of switches is causing a flattening of the network topology for a number of customers. The general deployment scenarios use VLANs to segment networks and use Layer 3 switching to provide routing service between the VLANs. The increasing use of VLANs means that many stations across different locations in customer's premises can be part of a broadcasting network. In such a network, a Layer 2 attack that is not properly defended can cross many layer 2 devices and potentially bring down the network.

The two major kind of Layer 2 attacks are attacks on ARP protocol and on the MAC learning table (CAM table) of the switch.

StoneOS offers a variety of mechanisms that prevents these attacks:

- Authenticated ARP between client and gateway
- Static IP-MAC binding
- Static MAC-Port binding
- Enable/disable ARP learning
- Enable/disable MAC learning
- ARP spoofing detection
- IP per MAC limit
- Automatic Gratuitous ARP
- Automatic Gratuitous ARP for servers
- ARP reverse lookup
- Port isolation
- ARP inspection

## 2. ARP Spoofing

ARP is a network mechanism to translate IP into link layer addresses. On Ethernet, the link layer address is the MAC address.

Traditionally, the station that needs to find the MAC address of an IP sends out an ARP request. This is a broadcast message that is sent to all stations in the Ethernet domain. The station with the correct IP sends back an ARP response with its IP and MAC information. This is a unicast message.

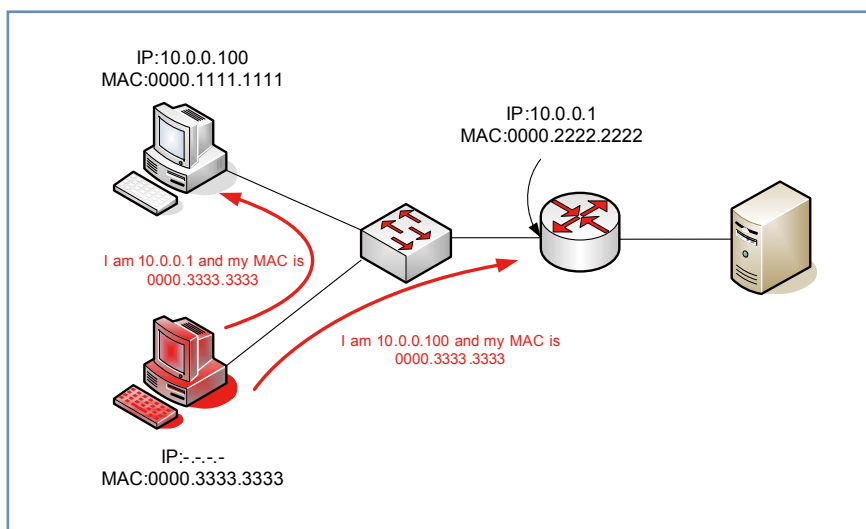
The originating station caches this entry for later use.

A station can also send out gratuitous ARP. It is used to detect conflict IP on a network and inform other stations of the IP address change.

Even though ARP protocol is request/response, a lot of the protocol implementation is stateless. That is, a station will accept an unsolicited ARP replies even without a ARP request being sent.

ARP spoofing (a.k.a ARP cache poisoning) utilizes the stateless nature of the ARP processing by sending unicast ARP replies to the victim station.

Figure 1: ARP spoofing ▶



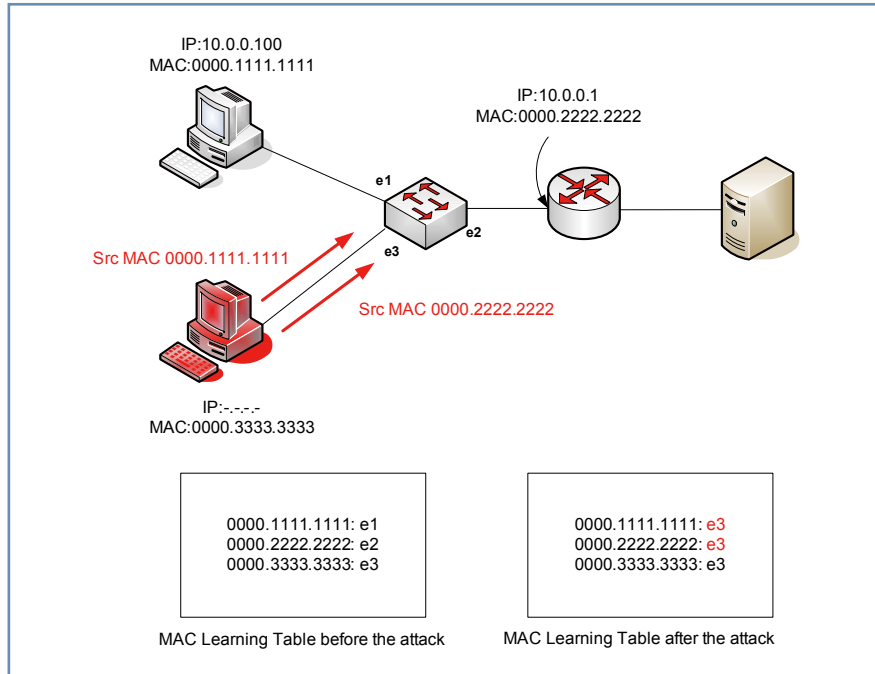
In the above diagram, the attacker can send ARP reply to both the victim station and the victim gateway. If the attack is successful, the 10.0.0.100 station will think that the attacker (3333.3333.3333) is the gateway, and the gateway will think the attacker has the IP 10.0.0.100 and will send all return traffic from the server to the victim station to the attacker.

Beside Deny-of-Service, ARP spoofing can achieve Man-In-the-Middle attacks which are very dangerous.

### 3. MAC Address/CAM Table Attacks

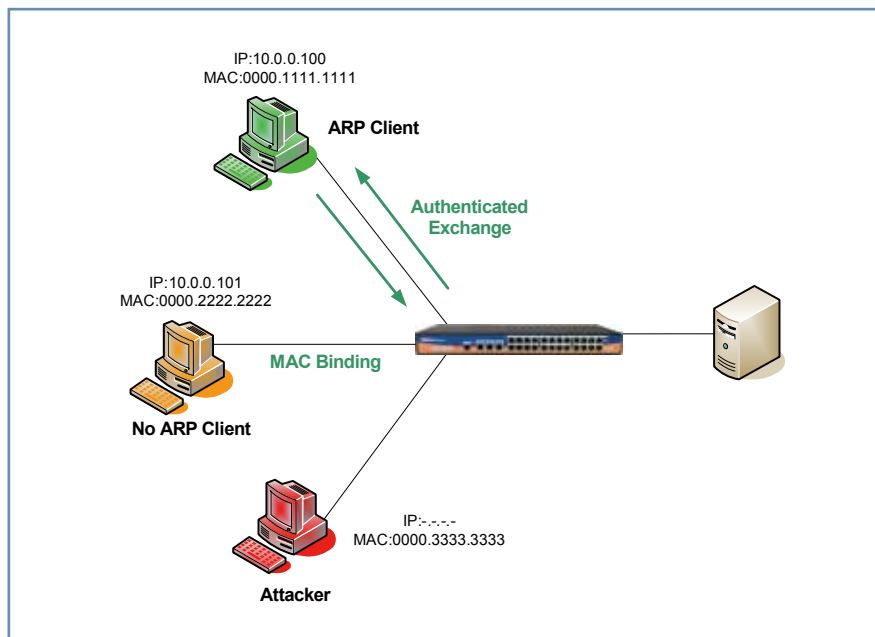
The basic functionality of a layer 2 switch is to learn the MACs of stations beyond each of its ports, and avoid unnecessary flooding of traffic to all the ports like a hub would do. This can be targeted by attacker to achieve traffic redirection and deny of service.

Figure 2: Layer 2 switch attack ▶



What is shown in Figure 2 is a surprisingly simple attack which a lot of the current network can not defend. The attacker first use ARP to scan the network to find out the IP and MAC of current stations. Then it simply sends out packets with forged source MACs to the switch. The switches MAC learning will be confused. If the attacker sends out these type of traffic at a high enough interval, it will overwhelm other legitimate traffic and subsequently the switch will forward all future traffic going to these MACs to the attacker. This in many cases will cause a Deny-of-Service in the network.

Figure 3: Hillstone integrated gateway combines functionality of firewall, switch and router ▶



## 4. StoneOS Solutions

A Hillstone appliance that integrates firewall, router and switch functionalities employs a rich set of methods in guarding against Layer 2 attacks.

### 4.1 Hillstone ARP Client

It turns out that even statically bound ARP entries on some Windows platform can be changed by ARP attack. StoneOS supports a proprietary protocol to authenticate ARP request and response. This is best used in a scenario where static binding is hard to do or not feasible.

The PC with Hillstone ARP client installed will perform authenticated ARP with the Hillstone device (See Figure 3). It ensures to the client that the device MAC is authentic and comes from a Hillstone device. The exchange uses Private Key Infrastructure (or PKI) to guarantee the authenticity of the ARP information. The protocol implements strong anti-forgery and anti-replay mechanisms to defend from various attacks on the system. Forgery of ARP packets or replay of device ARP packets will not be accepted by the system.

ARP client also monitors the PC for suspicious layer 2 behaviors and blocks an infected PC from ARP attack of other PCs and devices in its LAN segment.

Furthermore, StoneOS has the ability to detect whether a client has installed the ARP authentication tool and blocks the client's access to the internet until the client installs the tool. This helps administrators to enforce the deployment of the ARP defense policy. The protocol and tool were designed to achieve backward compatibility with the traditional ARP protocol. So there would be no interoperability problems with legacy devices/clients, if policy permits.

The ARP client needs zero configuration. Each PC only needs to execute the installation once and no further action needs to be taken afterwards.

### 4.2 Clientless ARP and Layer 2 Defense

- **Static IP-MAC binding:** Static IP-MAC binding is one of the most effective methods against ARP spoofing attacks. A statically bound IP-MAC entry can not be changed by ARP request and response. The disadvantage of this method is its high administrative cost. StoneOS alleviates this problem by implementing an easy-to-use scan-and-bind functionality, allowing the

administrator to first scan the stations in the network and perform static binding automatically. This feature can be used together with 'Enable/Disable ARP learning' to achieve the desired security level.

- Static MAC-Port binding: Just like Static IP-MAC bind, static MAC-Port binding can defend against MAC address table attacks described above. A switch will ignore MAC learnt if the MAC is already statically bound to a port. Any packet that is received with MAC-Port conflict with static binding will be dropped. This feature can be used together with 'Enable/Disable MAC learning' to achieve the desired security level. StoneOS makes static MAC-Port binding easy by integrating this feature inside the scan-and-bind functionality. The administrator can perform Static IP-MAC binding and static MAC-Port binding with one button click.

- Enable/disable ARP learning: Disable ARP learning means that asided from MACs that are statically bound to an IP, stations with other MACs can not be routed through the Hillstone device.

- Enable/disable MAC learning: Disable MAC learning means that aside from MACs that are statically bound to a port, stations with other MACs can not be switched by the Hillstone device.

- ARP spoofing detection: ARP spoofing appears as address conflict is reported by the Hillstone device when two MACs appear to claim the same IP.

2007-11-28 09:56:38	warn	NET: IP address 10.160.65.51 on 001c.5400.0900 conflicts with the interface ethernet0/0
2007-12-06 14:40:02	warn	FLOW: ARP spoof attack:alarm! MAC address 0013.c36b.0e80 and 0090.fb0a.2763 has same IP address 10.160.33.149 on interface ethernet0/1

- IP per MAC limit: StoneOS can limit the number of IPs that map to the same MAC. Set this number to 1 effectively limits the ARP spoofing and avoids the Man-in-the-Middle attack.

- Automatic Gratuitous ARP: StoneOS can send periodic gratuitous ARP to defend against attackers that masquerades as the Hillstone device.

- Automatic Gratuitous ARP for servers: StoneOS can also send gratuitous ARP on behalf of the servers to defend them against attackers that masquerades as the server.

- ARP reverse lookup: When receiving ARP request/response and

gratuitous ARP, we record the sender's MAC and send ARP request to the sender. Inspect the MAC in the response and match with the stored MAC.

- Port isolation: StoneOS offers this option as a protection that each port forms its own broadcasting domain. While it does not protect the downstream switches, it can protect L2 attacks from crossing from one branch of the domain to another.

- ARP inspection: On certain Hillstone platforms, ARP inspection is supported in Layer 2 and Mixed mode. All ARP packets that go through the device will be inspected against local static IP-MAC binding.

## 5. Conclusion

Hillstone's StoneOS is a professional security operating system that integrates security with traditional networking functionalities such as routing and switching. StoneOS introduces a comprehensive list of defenses that effectively prevents ARP and Layer 2 attacks. These defenses guard the ARP learning table and MAC learning table from hijacking by both internal and external threats.