

51. DYNAMIC ARP INSPECTION

WHAT IS DYNAMIC ARP INSPECTION (DAI) ?

ARP REVIEW

- ARP is used to learn the MAC ADDRESS of another DEVICE with a known IP ADDRESS
 - For example, a PC will use ARP to learn the MAC ADDRESS of its DEFAULT GATEWAY to communicate with external NETWORKS
- Typically, it is a TWO MESSAGE EXCHANGE : ARP REQUEST and ARP REPLY

GRATUITOUS ARP

- A GRATUITOUS ARP MESSAGE is an ARP REPLY that is sent without receiving an ARP REQUEST
- It is SENT to the BROADCAST MAC ADDRESS
- It allows other DEVICES to learn the MAC ADDRESS of the sending DEVICE without having to send ARP REQUESTS.
- Some DEVICES automatically send GARP MESSAGES when an INTERFACE is enabled, IP ADDRESS is changed, MAC address is changed, etc.

DYNAMIC ARP INSPECTION

- DAI is a SECURITY FEATURE of SWITCHES that is used to filter ARP MESSAGES received on *UNTRUSTED PORTS*
- DAI only filters ARP MESSAGES. Non-ARP MESSAGES are NOT affected
- All PORTS are *UNTRUSTED*, by DEFAULT
 - Typically, all PORTS connected to other NETWORK DEVICES (SWITCHES, ROUTERS) should be configured as TRUSTED, while INTERFACES connected to END HOSTS should remain UNTRUSTED

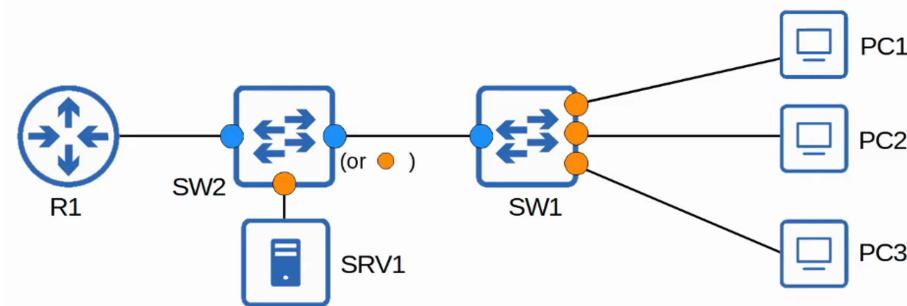


Figure 1: image

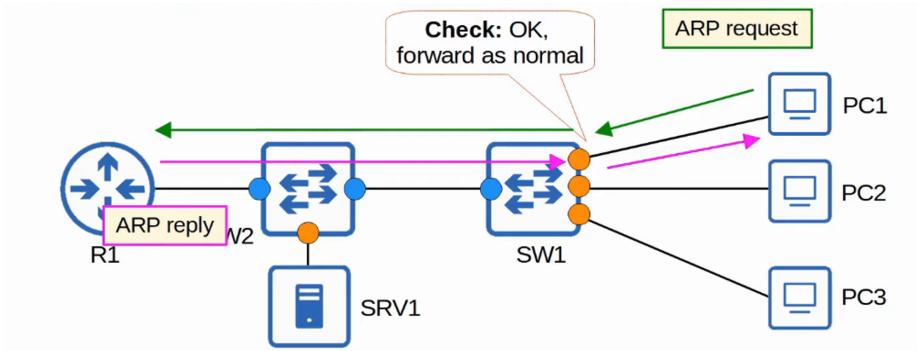


Figure 2: image

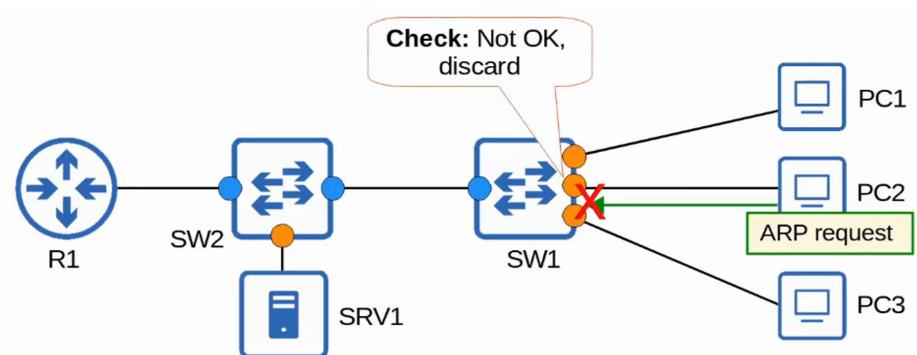


Figure 3: image

ARP POISONING (MAN IN THE MIDDLE)

- Similar to DHCP POISONING, ARP POISONING involved an ATTACKER manipulating TARGET'S ARP TABLES so TRAFFIC is sent to the ATTACKER
- To do this, the ATTACKER can send GRATUITOUS ARP MESSAGES using another DEVICE'S IP ADDRESS
- Other DEVICES in the NETWORK will receive the GARP and update their ARP TABLES, causing them to send TRAFFIC to the ATTACKER instead of the legitimate DESTINATION

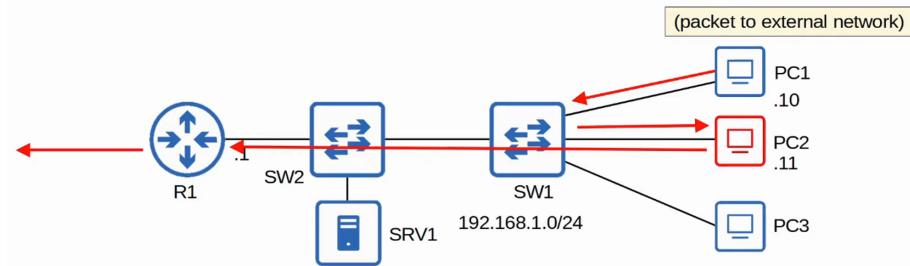


Figure 4: image

DYNAMIC ARP INSPECTION OPERATIONS

- DAI inspects the SENDER MAC and SENDER IP fields of ARP MESSAGES received on UNTRUSTED PORTS and checks that there is a matching entry in the DHCP SNOOPING BINDING TABLE
 - If there is a MATCH, the ARP MESSAGE is FORWARDED
 - If there is NO MATCH, the ARP MESSAGE is DISCARDED

```
SW1#show ip dhcp snooping binding
MacAddress          IpAddress      Lease(sec) Type        VLAN Interface
-----  -----
0C:29:2F:18:79:00  192.168.100.10  86294    dhcp-snooping 1  GigabitEthernet0/3
0C:29:2F:90:91:00  192.168.100.11  86302    dhcp-snooping 1  GigabitEthernet0/1
0C:29:2F:67:E9:00  192.168.100.12  86314    dhcp-snooping 1  GigabitEthernet0/2
Total number of bindings: 3
```

Figure 5: image

- DAI doesn't inspect messages received on TRUSTED PORTS. They are FORWARDED as normal.
- ARP ACLs can be manually configured to map IP ADDRESSES / MAC ADDRESSES for DAI to check
 - Useful for HOSTS that don't use DHCP
- DAI can be configured to perform more in-depth checks also - but these are optional

- Like DHCP SNOOPING, DAI also supports RATE-LIMITING to prevent ATTACKERS from overwhelming the SWITCH with ARP MESSAGES
 - DHCP SNOOPING and DAI both require work from the SWITCH'S CPU
 - Even if the ATTACKER'S messages are BLOCKED, they can OVERLOAD the SWITCH CPU with ARP MESSAGES

DYNAMIC ARP INSPECTION CONFIGURATION

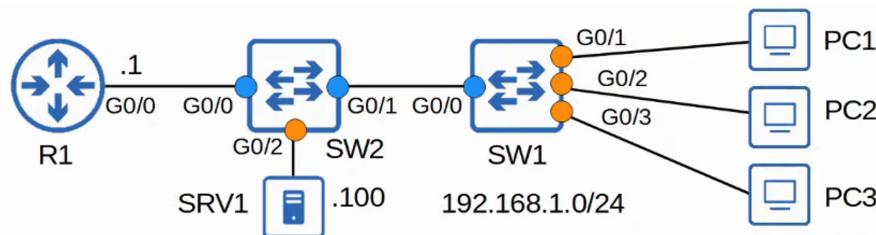


Figure 6: image

```
SW2(config)#ip arp inspection vlan 1
SW2(config)#interface range g0/0 - 1
SW2(config-if-range)#ip arp inspection trust

SW1(config)#ip arp inspection vlan 1
SW1(config)#interface g0/0
SW1(config-if)#ip arp inspection trust
```

DHCP snooping requires two commands to enable it:
`ip dhcp snooping`
`ip dhcp snooping vlan vlan-number`

DAI only requires one:
`ip arp inspection vlan vlan-number`

Figure 7: image

Command : `show ip arp inspection interfaces`

Interface	Trust State	Rate (pps)	Burst Interval
Gio/0	Trusted	None	N/A
Gio/1	Untrusted	15	1
Gio/2	Untrusted	15	1
Gio/3	Untrusted	15	1
Gi1/0	Untrusted	15	1
Gi1/1	Untrusted	15	1
Gi1/2	Untrusted	15	1
Gi1/3	Untrusted	15	1
Gi2/0	Untrusted	15	1
Gi2/1	Untrusted	15	1
Gi2/2	Untrusted	15	1
Gi2/3	Untrusted	15	1
Gi3/0	Untrusted	15	1
Gi3/1	Untrusted	15	1
Gi3/2	Untrusted	15	1
Gi3/3	Untrusted	15	1

Figure 8: image

DAI RATE LIMITING

```

SW1(config)#interface range g0/1 - 2
SW1(config-if-range)#ip arp inspection limit rate 25 burst interval 2
SW1(config-if-range)#interface range g0/3
SW1(config-if)#ip arp inspection limit rate 10
SW1(config-if)#do show ip arp inspection interfaces
! [output omitted]

Interface      Trust State     Rate (pps)    Burst Interval
-----          -----          -----          -----
Gi0/0           Trusted        None          N/A
Gi0/1           Untrusted      25            2
Gi0/2           Untrusted      25            2
Gi0/3           Untrusted      10            1
! [output omitted]

SW1(config)#errdisable recovery cause arp-inspection
SW1(config)#do show errdisable recovery
ErrDisable Reason          Timer Status
-----                      -----
arp-inspection             Enabled
! [output omitted]

```

The burst interval is optional. If you don't specify it, the default is 1 second.

If ARP messages are received faster than the specified rate, the interface will be err-disabled. It can be re-enabled in two ways:
1: shutdown and no shutdown
2: errdisable recovery cause arp-inspection

Figure 9: image

DAI OPTIONAL CHECKS

```

SW1(config)#ip arp inspection validate ?
dst-mac Validate destination MAC address
ip      Validate IP addresses
src-mac Validate source MAC address

```

dst-mac: Enables validation of the destination MAC address in the Ethernet header against the target MAC address in the ARP body for ARP responses. The device classifies packets with different MAC addresses as invalid and drops them

ip: Enables validation of the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. The device checks the sender IP addresses in all ARP requests and responses and checks the target IP addresses only in ARP responses.

src-mac: Enables validation of the source MAC address in the Ethernet header against the sender MAC address in the ARP body for ARP requests and responses. The device classifies packets with different MAC addresses as invalid and drops them.

(source: https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/n5k/commands/ip-arp-inspection-validate.html)

Figure 10: image

ARP ACLs (Beyond Scope of CCNA)

CREATE AN ARP ACL FOR SRV1

AFTER APPLYING IT TO SWITCH 2, SRV1 is able to send ARP REQUEST to R1

Command: `show ip arp inspection`

Shows a summary of the DAI configuration and statistics

COMMAND REVIEW

```

SW1(config)#ip arp inspection validate ?
dst-mac Validate destination MAC address
ip Validate IP addresses
src-mac Validate source MAC address

> Frame 224: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
  ▾ Ethernet II, Src: 0c:29:2f:43:b5:00 (0c:29:2f:43:b5:00), Dst: 0c:29:2f:90:91:00 (0c:29:2f:90:91:00)
    > Destination: 0c:29:2f:90:91:00 (0c:29:2f:90:91:00)
    > Source: 0c:29:2f:43:b5:00 (0c:29:2f:43:b5:00)
      Type: ARP (0x0806)
      Padding: 00000000000000000000000000000000
      ▾ Address Resolution Protocol (reply)
        Hardware type: Ethernet (1)
        Protocol type: IPv4 (0x0800)
        Hardware size: 6
        Protocol size: 4
        Opcode: reply (2)
        Sender MAC address: 0c:29:2f:43:b5:00 (0c:29:2f:43:b5:00)
        Sender IP address: 192.168.1.1
        Target MAC address: 0c:29:2f:90:91:00 (0c:29:2f:90:91:00)
        Target IP address: 192.168.1.10

```

These checks are done in addition to the standard DAI check (sender MAC/IP). If configured, an ARP message must pass **all** of the checks to be considered valid.

Figure 11: image

```

SW1(config)#ip arp inspection validate dst-mac
SW1(config)#ip arp inspection validate ip
SW1(config)#ip arp inspection validate src-mac

SW1(config)#do show running-config | include validate
ip arp inspection validate src-mac

SW1(config)#ip arp inspection validate ip src-mac dst-mac

SW1(config)#do show running-config | include validate
ip arp inspection validate src-mac dst-mac ip

```

You must enter all of the validation checks you want in a single command.
 *You can specify one, two, or all three.
 *The order isn't significant.

Figure 12: image

```

SW2#show ip dhcp snooping binding
-----+-----+-----+-----+-----+-----+
MacAddress      IPAddress      Lease(sec)   Type       VLAN  Interface
-----+-----+-----+-----+-----+-----+
0C:29:2F:18:79:00  192.168.1.12  79226      dhcp-snooping  1    GigabitEthernet0/1
0C:29:2F:90:91:00  192.168.1.10  79188      dhcp-snooping  1    GigabitEthernet0/1
0C:29:2F:67:E9:00  192.168.1.11  79210      dhcp-snooping  1    GigabitEthernet0/1
-----+-----+-----+-----+-----+-----+
Total number of bindings: 3

!SRV1 has a static IP address of 192.168.1.100, so it does not have an entry in SW2's DHCP
!snooping binding table.

*Jun 19 05:56:15.538: %SW DAI-4-DHCP_SNOOPING DENY: 1 Invalid ARPs (Req) on G10/2, vlan 1.
([0c29.2f1e.7700/192.168.1.100/0000.0000.0000/192.168.1.1/05:56:14 UTC Sat Jun 19 2021])

SW2(config)#arp access-list ARP-ACL-1
SW2(config-arp-nacl)#permit ip host 192.168.1.100 mac host 0c29.2f1e.7700
SW2(config)#ip arp inspection filter ARP-ACL-1 vlan 1

```

Figure 13: image

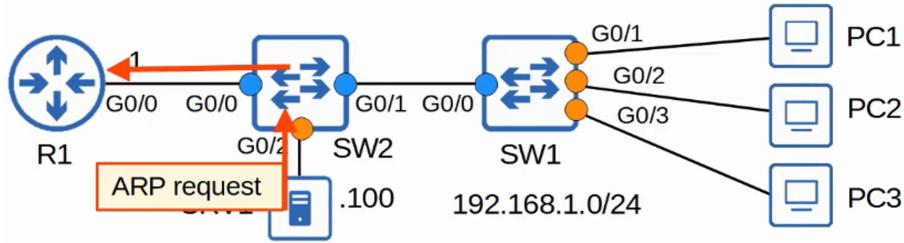


Figure 14: image

```
SW2#show ip arp inspection
Source Mac Validation : Enabled
Destination Mac Validation : Enabled
IP Address Validation : Enabled
Vlan Configuration Operation ACL Match Static ACL
--- -----
 1 Enabled Active ARP-ACL-1 No
Vlan ACL Logging DHCP Logging Probe Logging
--- -----
 1 Deny Deny Off
Vlan Forwarded Dropped DHCP Drops ACL Drops
--- -----
 1 56 4 4 0
Vlan DHCP Permits ACL Permits Probe Permits Source MAC Failures
--- -----
 1 0 1 0 0
Vlan Dest MAC Failures IP Validation Failures Invalid Protocol Data
--- -----
Vlan Dest MAC Failures IP Validation Failures Invalid Protocol Data
--- -----
 1 0 0 0 0
```

- If static ACL is set to yes, the implicit deny at the end of the ARP ACL will take effect.
- This will cause all ARP messages not permitted by the ARP ACL to be denied.
- In effect, this means that only the ARP ACL will be checked, the DHCP snooping table will not be checked.

Figure 15: image

```
SW1(config)# ip arp inspection vlan vlan-number
SW1(config)# errdisable recovery cause arp-inspection
SW1(config)# ip arp inspection validate (src-mac | dst-mac | ip)
SW1(config-if)# ip arp inspection trust
SW1(config-if)# ip arp inspection limit rate packets [burst interval seconds]

SW1(config)# arp access-list name
SW1(config-arp-nacl)# permit ip host ip-address mac host mac-address
SW1(config)# ip arp inspection filter arp-acl-name vlan vlan-number

SW1# show ip arp inspection
SW1# show ip arp inspection interfaces
```

Figure 16: image