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

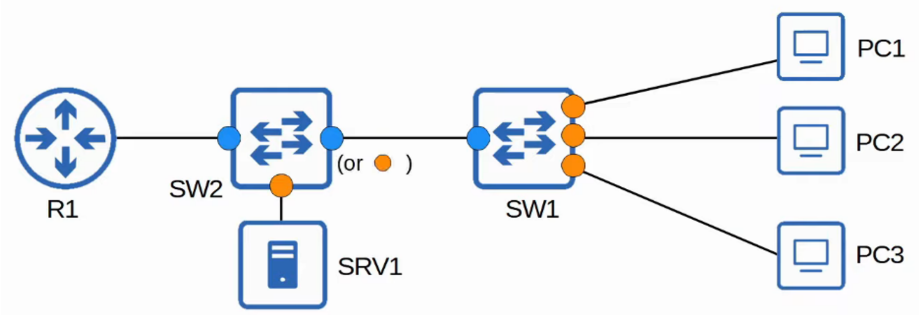

Figure 1: image

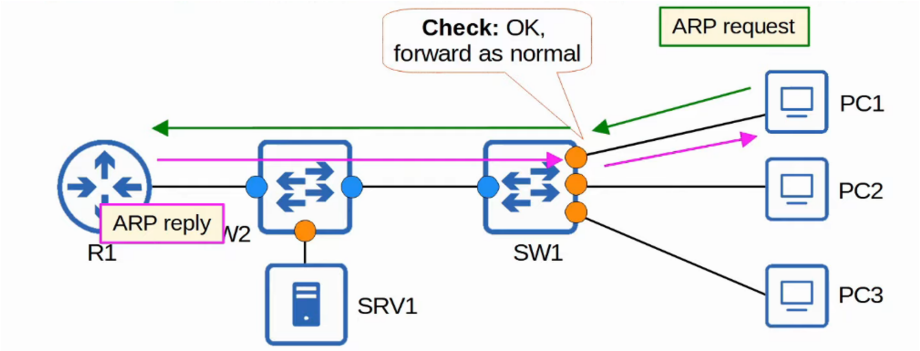

Figure 2: image

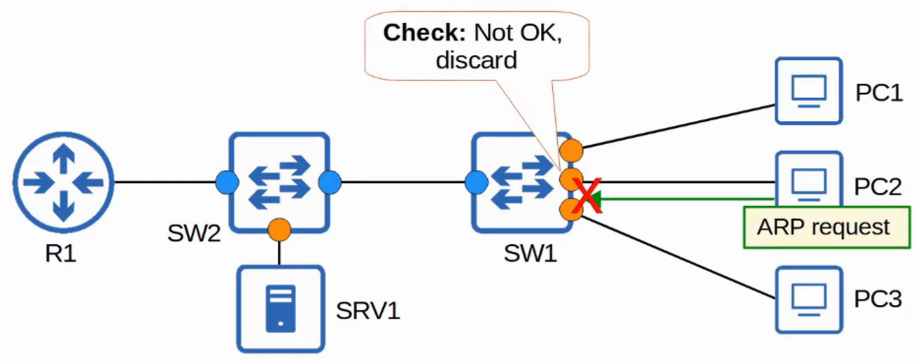

Figure 3: image

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

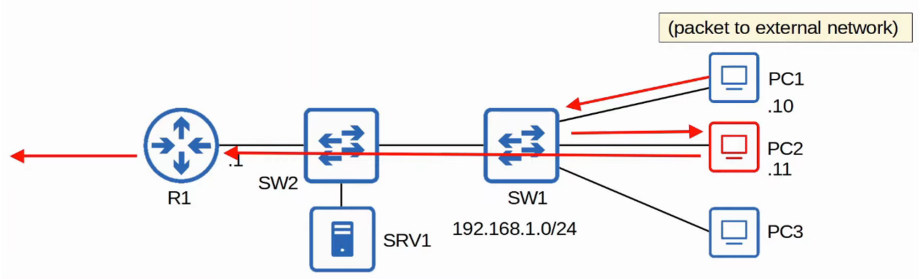

Figure 4: image

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 OVER-LOAD the SWITCH CPU with ARP MESSAGES

DYNAMIC ARP INSPECTION CONFIGURATION

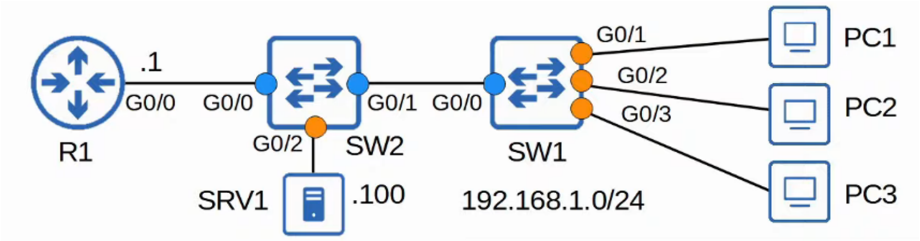

Figure 6: image

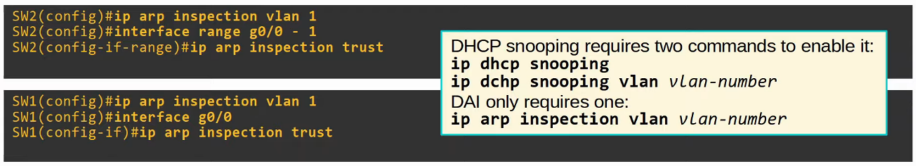

Figure 7: image

Command : `show ip arp inspection interfaces`

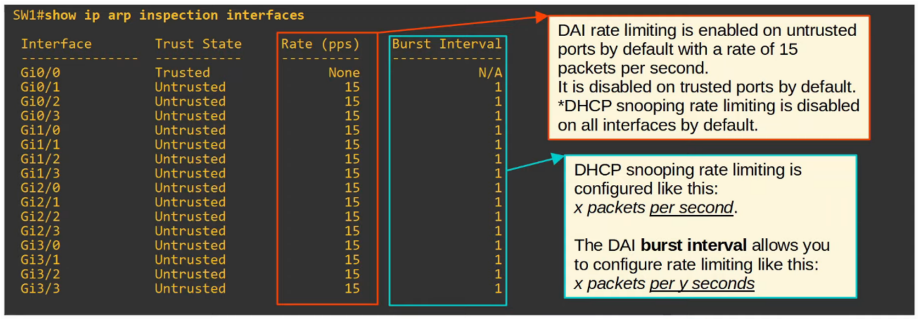

Figure 8: image

DAI RATE LIMITING

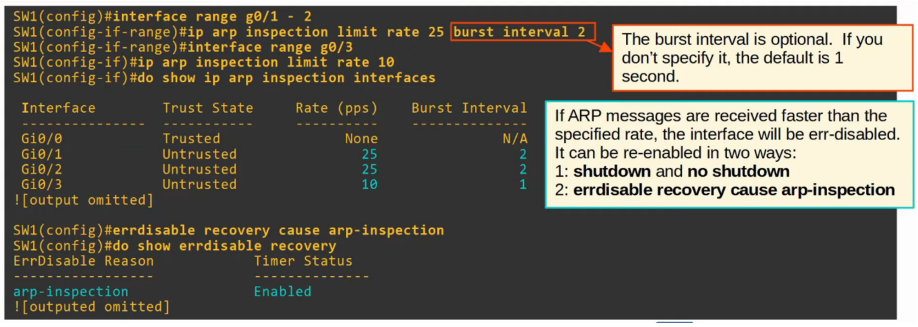

Figure 9: image

DAI OPTIONAL CHECKS

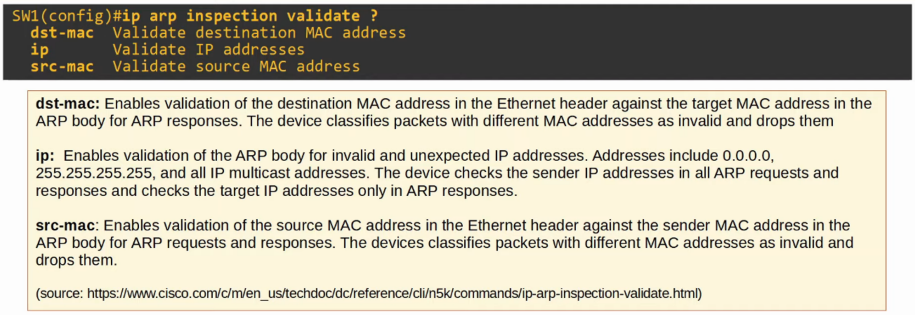

Figure 10: image

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

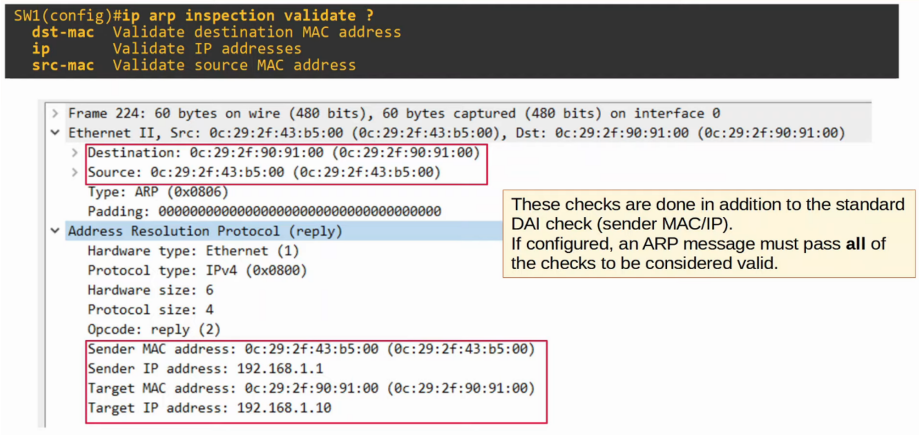

Figure 11: image

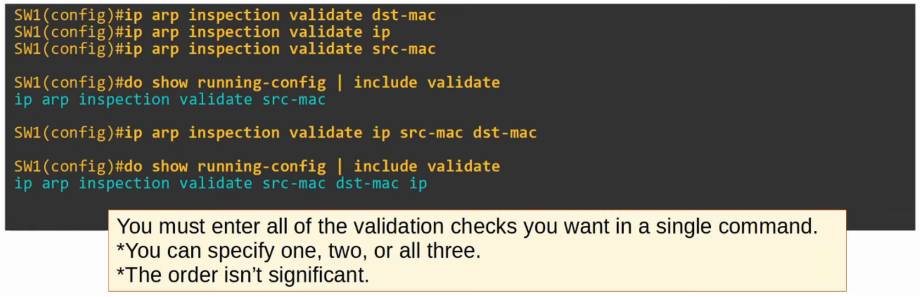

Figure 12: image

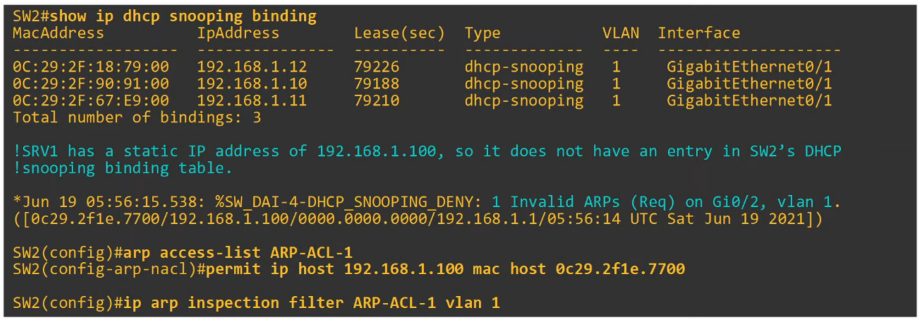

Figure 13: image

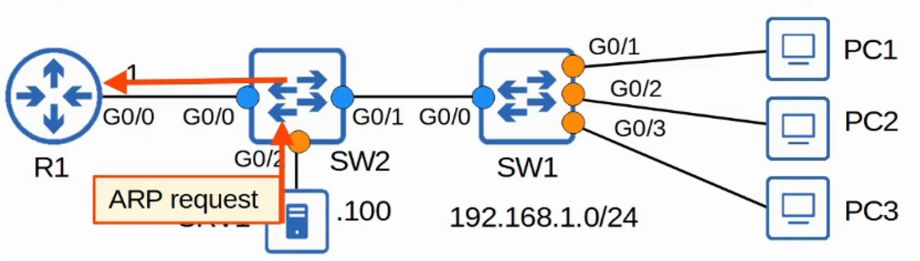

Figure 14: image

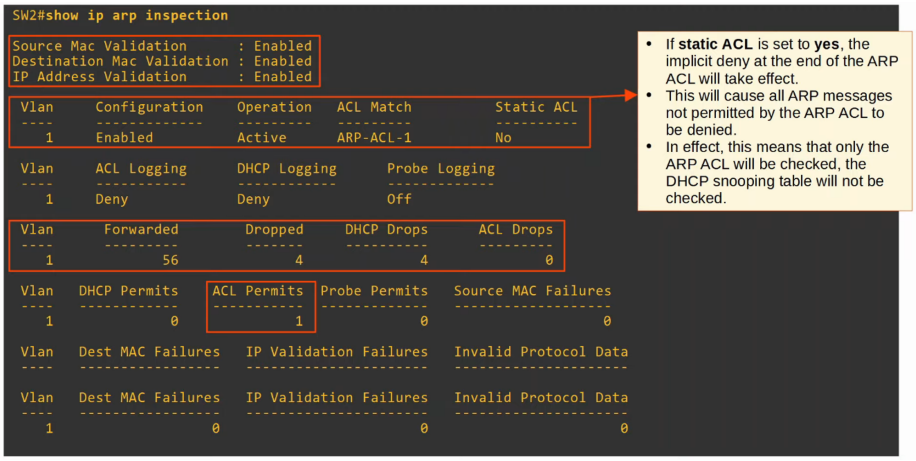

Figure 15: image

```
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