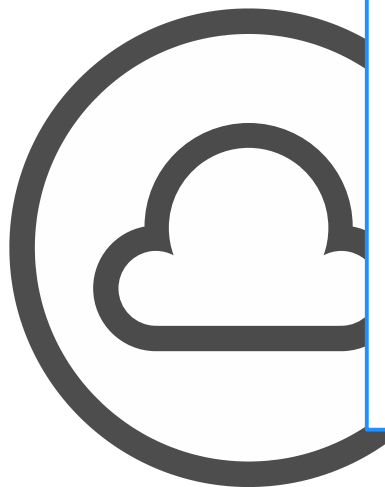# CCNA Day 51

Dynamic ARP Inspection

5.0 Security Fundamentals   15% ∧

5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
5.2 Describe security program elements (user awareness, training, and physical access control)
5.3 Configure device access control using local passwords
5.4 Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
5.5. Describe remote access and site-to-site VPNs
5.6 Configure and verify access control lists
5.7 Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
5.8 Differentiate authentication, authorization, and accounting concepts
5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)
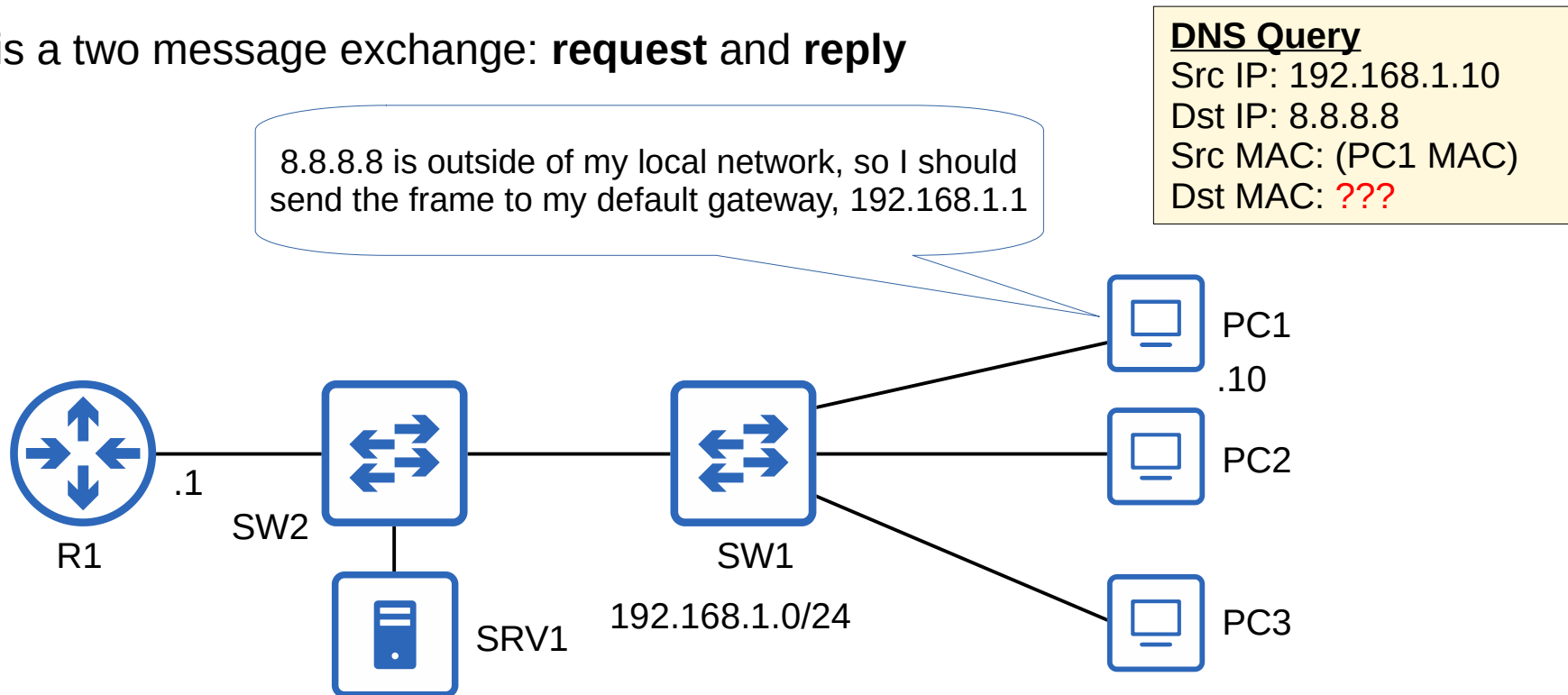5.10 Configure WLAN using WPA2 PSK using the GUI
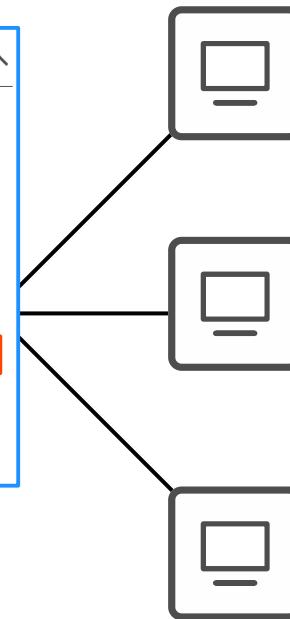
- What is Dynamic ARP Inspection?

- How does it work?

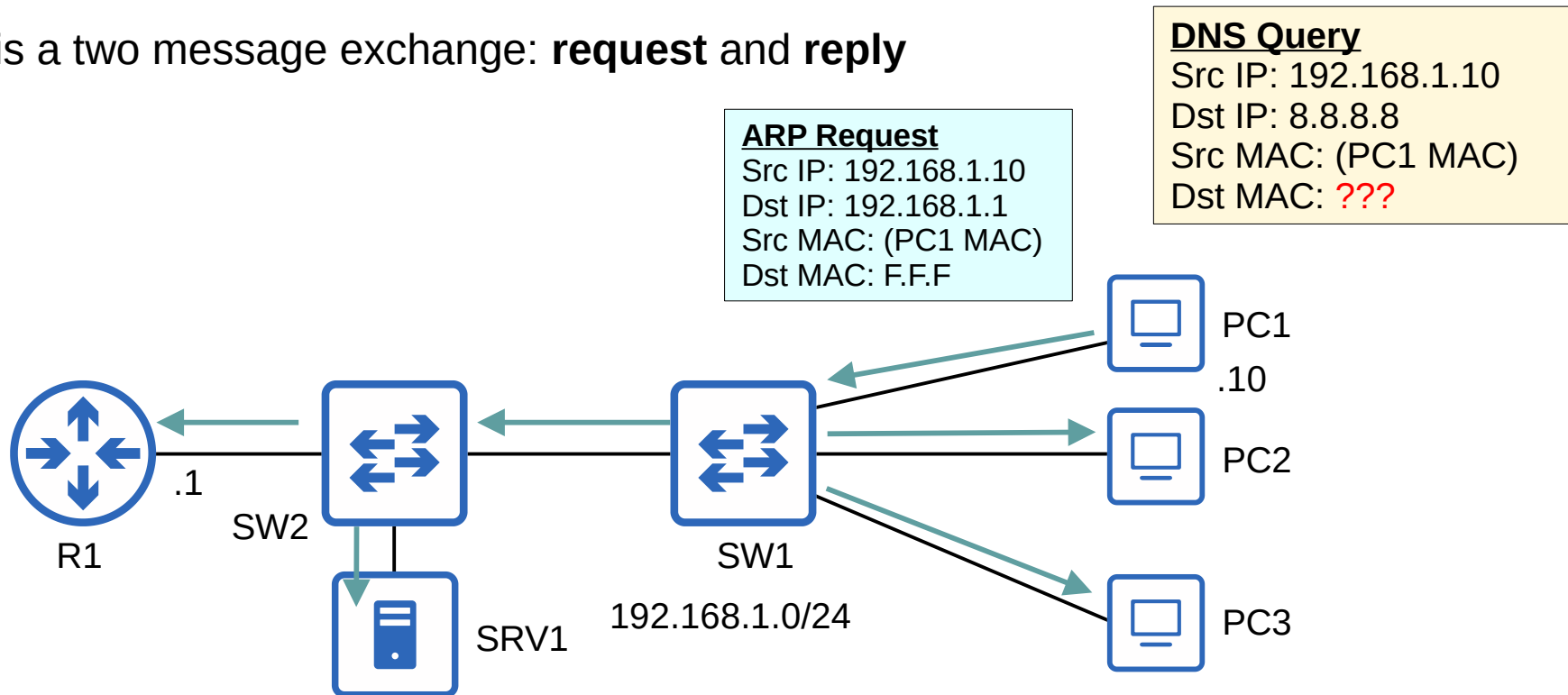- What attacks does it prevent?

- DAI configuration

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: **request** and **reply**

DNS Query
Src IP: 192.168.1.10
Dst IP: 8.8.8.8
Src MAC: (PC1 MAC)
Dst MAC: ???

8.8.8.8 is outside of my local network, so I should send the frame to my default gateway, 192.168.1.1

R1 .1

SW2

SRV1

SW1

192.168.1.0/24

PC1 .10

PC2

PC3

- 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: **request** and **reply**

DNS Query
Src IP: 192.168.1.10
Dst IP: 8.8.8.8
Src MAC: (PC1 MAC)
Dst MAC: ???

ARP Request
Src IP: 192.168.1.10
Dst IP: 192.168.1.1
Src MAC: (PC1 MAC)
Dst MAC: F.F.F

PC1
.10

PC2

PC3

.1
SW2

R1

SW1

SRV1

192.168.1.0/24

ARP Review

```
>  Frame 99: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
v  Ethernet II, Src: 0c:29:2f:90:91:00 (0c:29:2f:90:91:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
   >  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
   >  Source: 0c:29:2f:90:91:00 (0c:29:2f:90:91:00)
      Type: ARP (0x0806)
      Padding: 000000000000000000000000000000000000
v  Address Resolution Protocol (request)
      Hardware type: Ethernet (1)
      Protocol type: IPv4 (0x0800)
      Hardware size: 6
      Protocol size: 4
      Opcode: request (1)
      Sender MAC address: 0c:29:2f:90:91:00 (0c:29:2f:90:91:00)
      Sender IP address: 192.168.1.10
      Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
      Target IP address: 192.168.1.1
```

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.

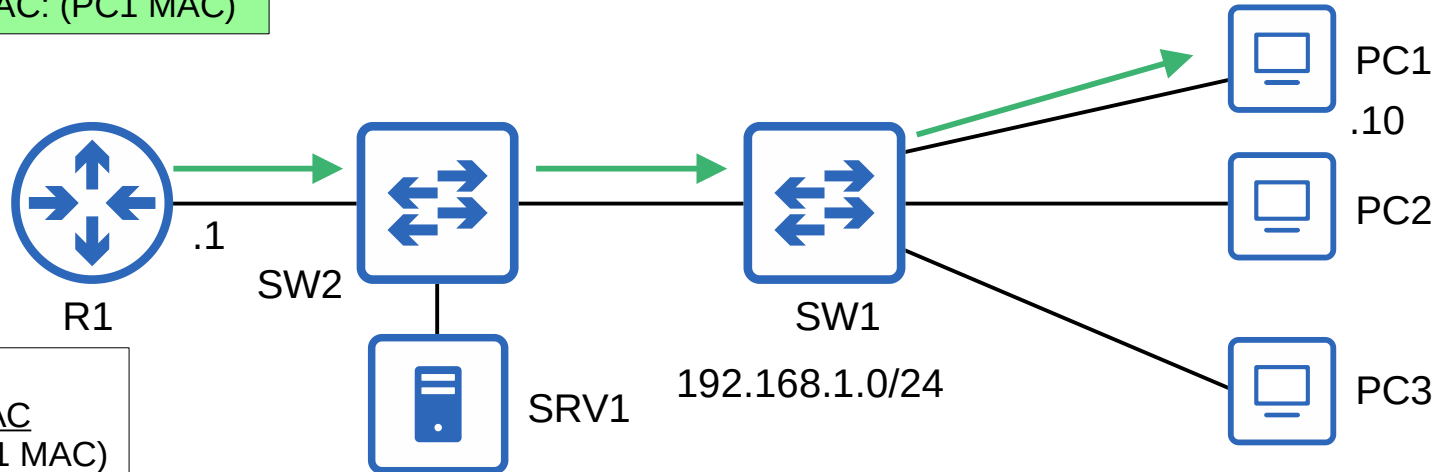- Typically it is a two message exchange: **request** and **reply**

DNS Query
Src IP: 192.168.1.10
Dst IP: 8.8.8.8
Src MAC: (PC1 MAC)
Dst MAC: ???

ARP Reply
Src IP: 192.168.1.1
Dst IP: 192.168.1.10
Src MAC: (R1 MAC)
Dst MAC: (PC1 MAC)

ARP Table:
IP   MAC
192.168.1.1   (R1 MAC)

ARP Table:
IP   MAC
192.168.1.10 (PC1 MAC)

R1   SW2   SRV1   SW1   192.168.1.0/24   PC1 .10   PC2   PC3

.1

ARP Review


```
> Frame 224: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
v 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: 000000000000000000000000000000000000
v 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
```
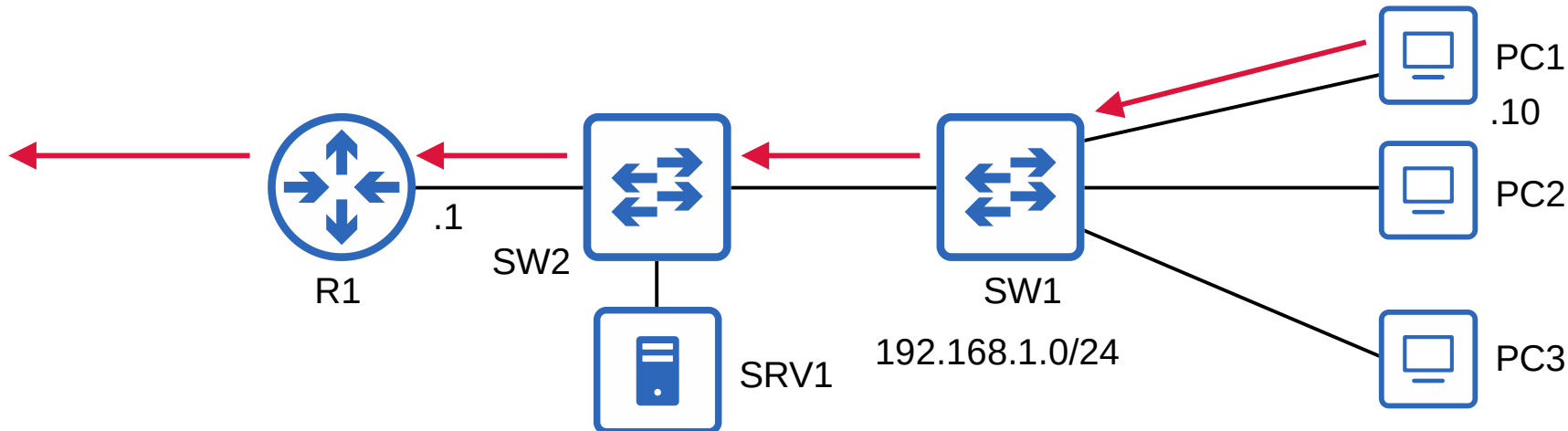
- ARP is used to learn the MAC address of another device with a known IP address.

- For example, a PC will use ARP to learn the MAC address of its default gateway to communicate with external networks.

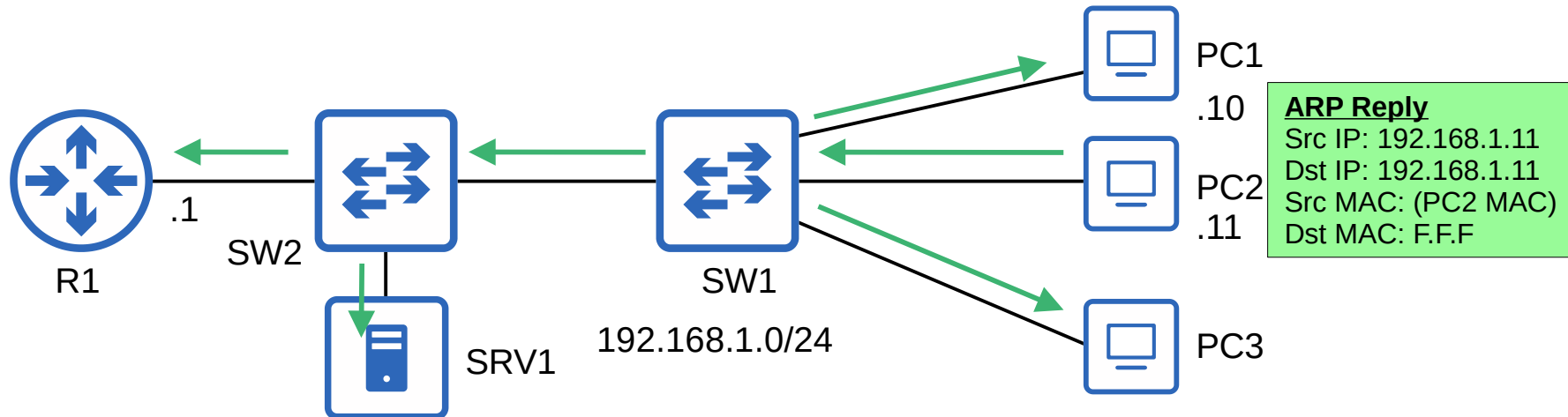- Typically it is a two message exchange: **request** and **reply**

DNS Query
Src IP: 192.168.1.10
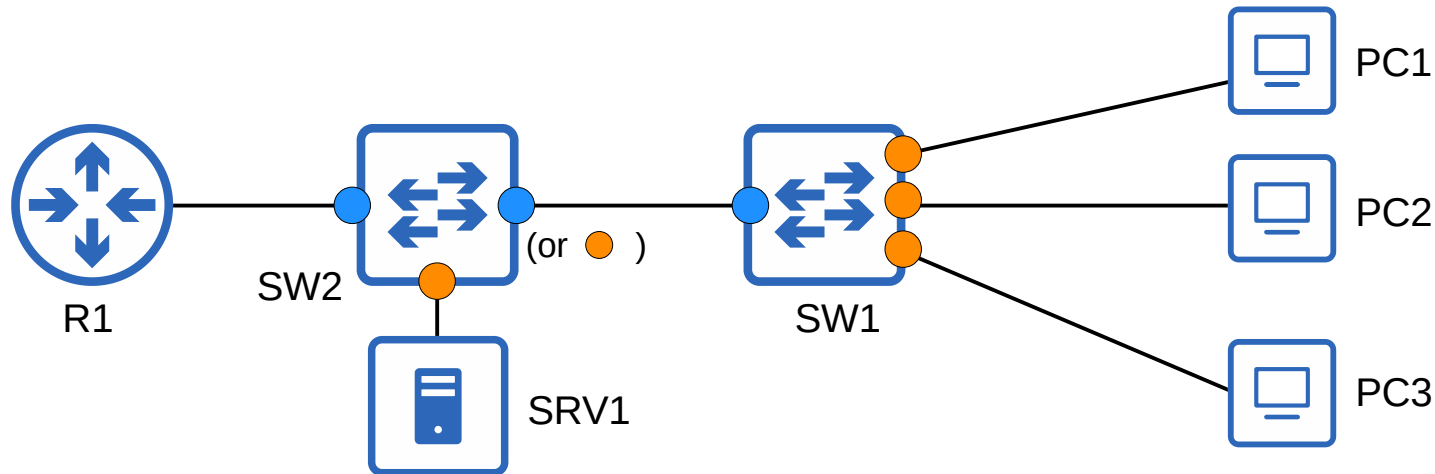Dst IP: 8.8.8.8
Src MAC: (PC1 MAC)
Dst MAC: (R1 MAC)

R1 .1

SW2

SRV1

SW1

192.168.1.0/24

PC1
.10

PC2

PC3

- 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.
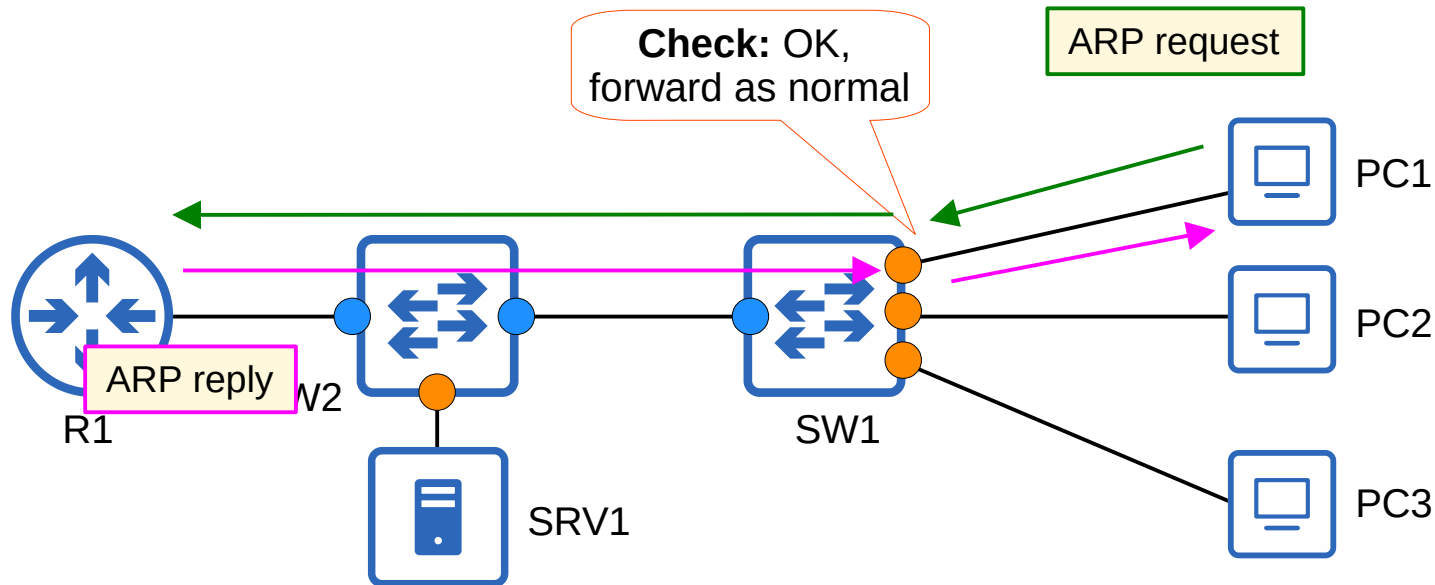

R1
.1
SW2
SRV1
SW1
192.168.1.0/24
PC1
.10
PC2
.11
PC3

ARP Reply
Src IP: 192.168.1.11
Dst IP: 192.168.1.11
Src MAC: (PC2 MAC)
Dst MAC: F.F.F

- 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 aren't 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**.
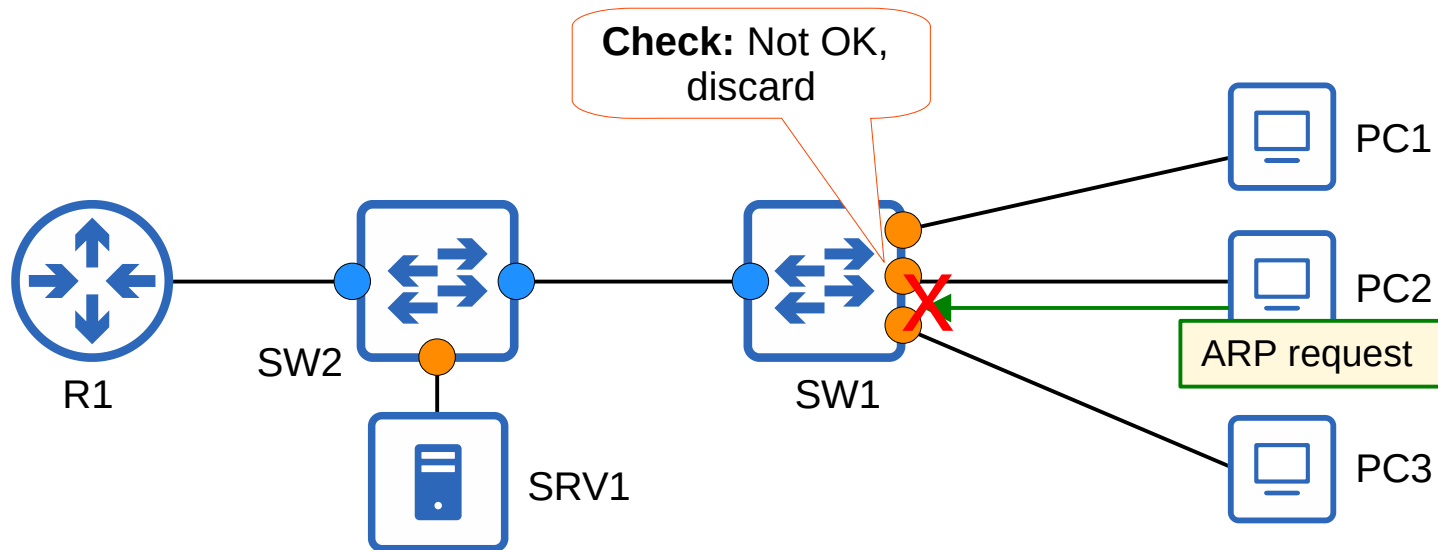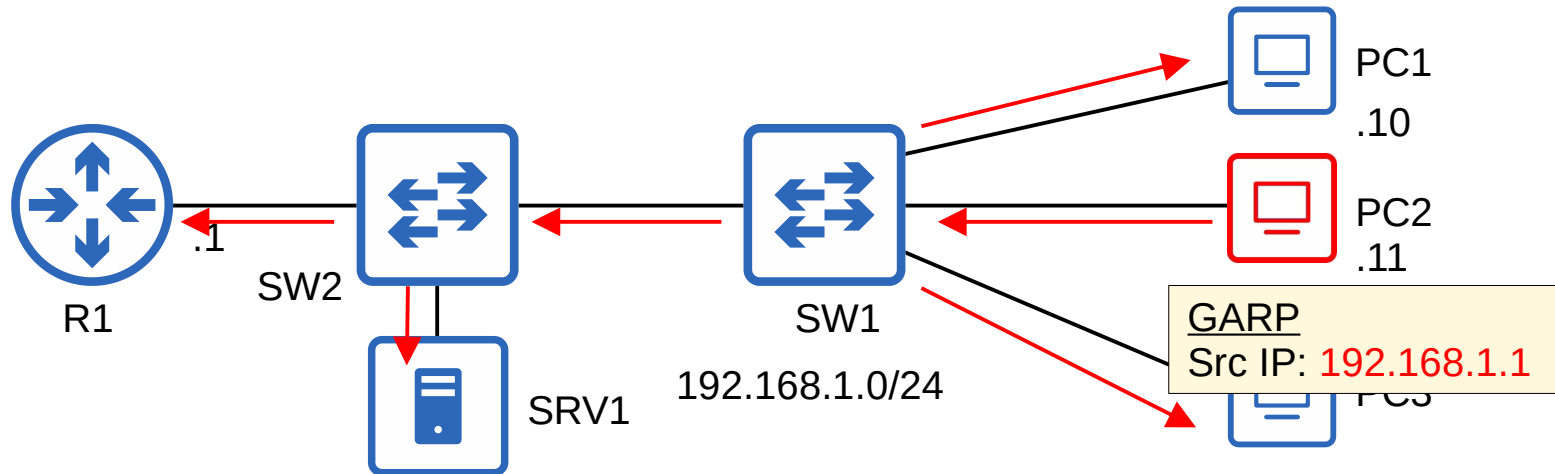
- DAI is a security feature of switches that is used to filter ARP messages received on *untrusted* ports.

- DAI only filters ARP messages. Non-ARP messages aren't 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**.
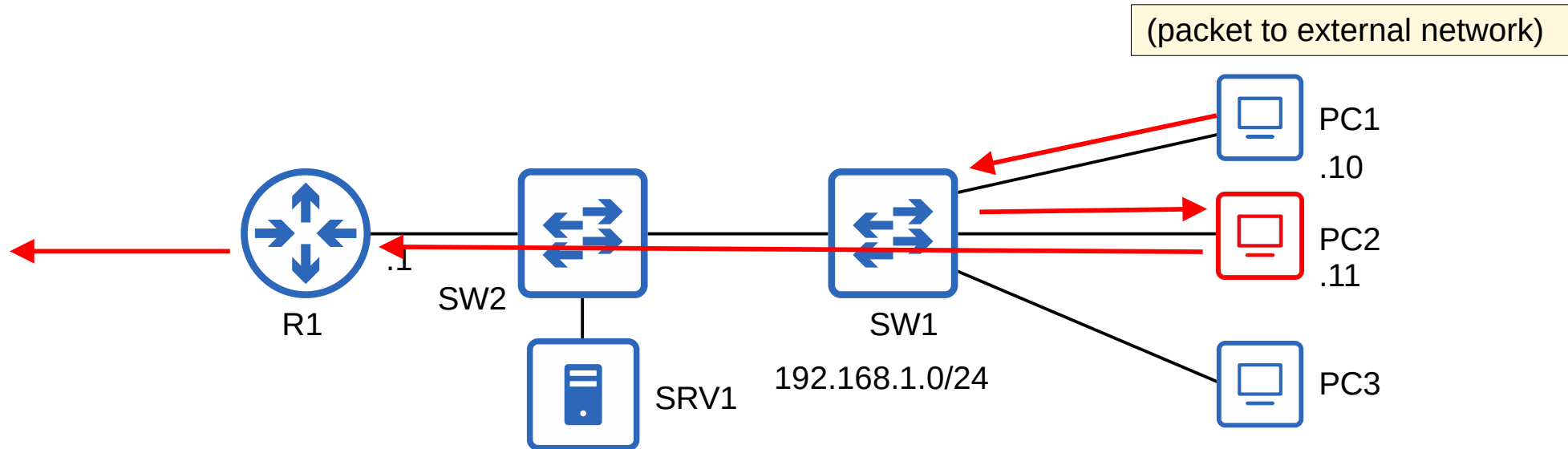

Check: OK, forward as normal

ARP request

PC1

ARP reply

R1

W2

SRV1

SW1

PC2

PC3

- 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 aren't 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**.

- Similar to DHCP poisoning, ARP poisoning involves an attacker manipulating targets' 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.

PC1
.10

PC2
.11

R1

SW2

.1

SRV1

SW1

192.168.1.0/24

GARP
Src IP: 192.168.1.1

PC3

- Similar to DHCP poisoning, ARP poisoning involves an attacker manipulating targets' 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.

(packet to external network)

PC1
.10

R1 .1

SW2

SW1

192.168.1.0/24

SRV1

PC2
.11

PC3

- DAI inspects the <u>sender MAC</u> and <u>sender IP</u> fields of ARP messages received on **untrusted** ports and checks that there is a matching entry in the <u>DHCP snooping binding table</u>.
  - → If there is a matching entry, the ARP message is forwarded normally.
  - → If there isn't a matching entry, 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
```

- 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.

DAI Configuration

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

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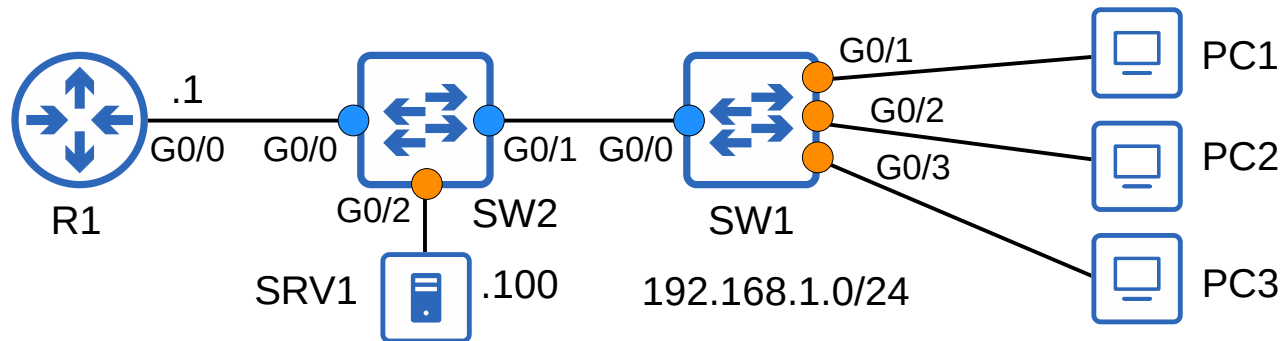
show ip arp inspection interfaces

```
SW1#show ip arp inspection interfaces

Interface         Trust State      Rate (pps)      Burst Interval
---------------   -----------      ----------      --------------
Gi0/0             Trusted                None                 N/A
Gi0/1             Untrusted                15                   1
Gi0/2             Untrusted                15                   1
Gi0/3             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
```

DAI rate limiting is enabled on untrusted ports by default with a rate of 15 packets per second.
It is disabled on trusted ports by default.
*DHCP snooping rate limiting is disabled on all interfaces by default.

DHCP snooping rate limiting is configured like this:
x packets _per second_.

The DAI **burst interval** allows you to configure rate limiting like this:
x packets _per y seconds_

R1 — G0/0 — .1 — G0/0 — SW2 — G0/1 — G0/0 — SW1 — G0/1 — PC1
SW2 — G0/2 — SRV1 — .100
SW1 — G0/2 — PC2
SW1 — G0/3 — PC3
192.168.1.0/24
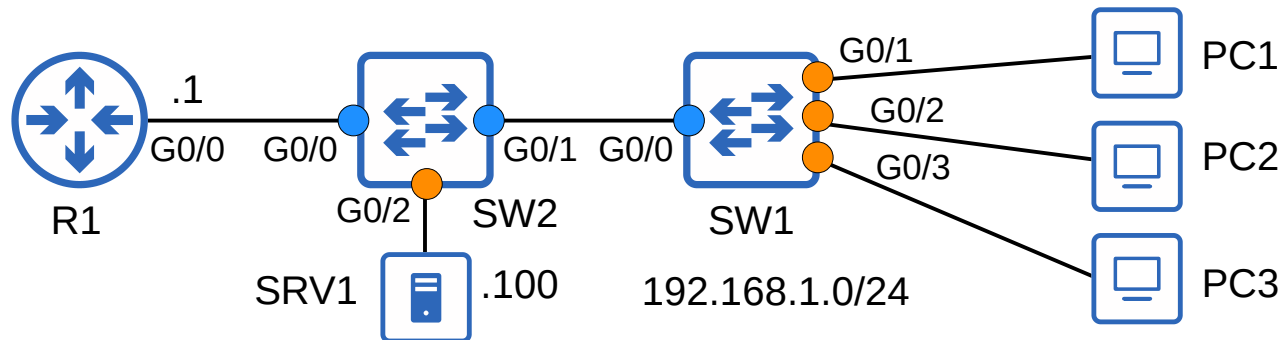
```
SW1(config)#interface range g0/1 - 2
SW1(config-if-range)#ip arp inspection limit rate 25 burst interval 2
SW1(config-if-range)#interface range g0/3
SW1(config-if)#ip arp inspection limit rate 10
SW1(config-if)#do show ip arp inspection interfaces

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
![outputed omitted]
```
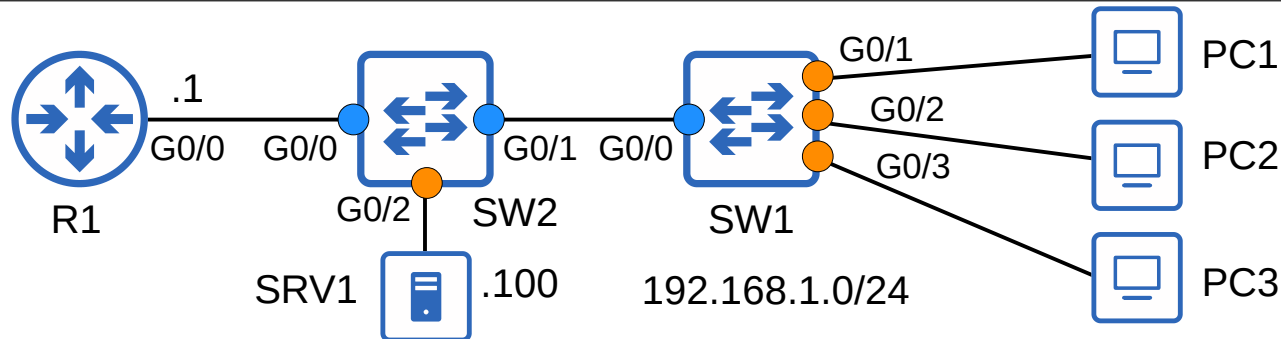
The burst interval is optional. If you don't specify it, the default is 1 second.

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**

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 devices 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)
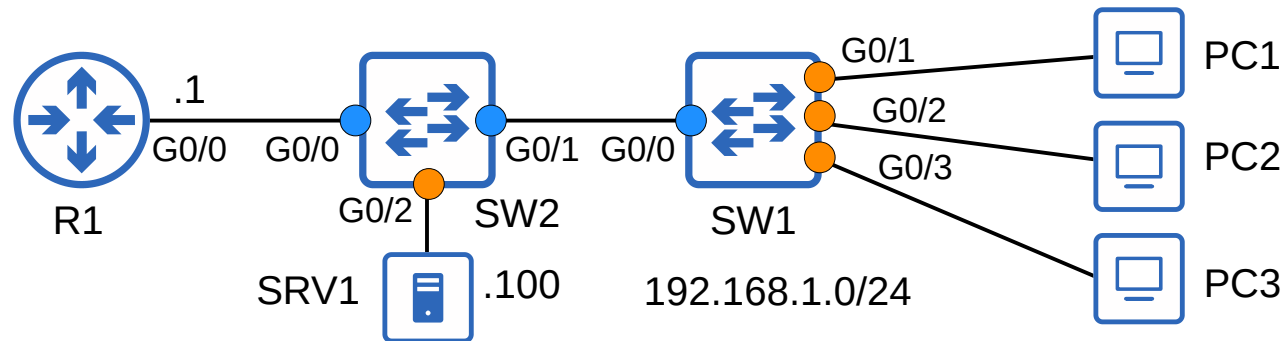
DAI Optional Checks

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

```
> Frame 224: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
v 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: 000000000000000000000000000000000000
v 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.

```
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.

ARP ACLs

```
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 Gi0/2, 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
```

ARP ACLs

```
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 Gi0/2, 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
```

ARP ACLs

```
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
```

- 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.

```
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
```

JEREMY'S IT LAB

- What is Dynamic ARP Inspection?

- How does it work?

- What attacks does it prevent?

- DAI configuration

ExSim-Max™
PRACTICE EXAMS

You issue the **ip arp inspection vlan 1** command on SW1. Which of the following statements is true about SW1 after issuing the command?

a) All interfaces in VLAN 1 are untrusted

b) DAI isn't fully enabled until globally enabled with **ip arp inspection**

c) Only ARP messages from hosts with a static IP address will be permitted.

d) DHCP snooping is enabled.

The following commands are configured on SW1. Which of the following statements is true after the commands have been issued?

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

a) DAI validation is only enabled for IP addresses

b) DAI validation is only enabled for source MAC addresses

c) DAI validation is only enabled for destination MAC addresses

d) DAI validation is enabled for all three causes

Which of the following are true about DAI rate limiting? (select two)

a) It is enabled on trusted and untrusted ports by default.

b) It is enabled on untrusted ports by default.

c) It is enabled at a rate of 10 packets per second by default.

d) It is enabled at a rate of 15 packets per second by default.

DAI inspects the sender IP and MAC addresses to determine whether an ARP packet should be forwarded or dropped. Which of the following does it check the sender IP and MAC against? (select two)

a) MAC address table

b) DHCP snooping binding table

c) ARP table

d) ARP ACLs

Which of the following commands limit ARP messages to a maximum average of 15 per second? (select two)

a) **ip arp inspection limit rate 15**

b) **ip arp inspection limit rate 30 burst interval 3**

c) **ip arp inspection limit rate 45 burst interval 3**

d) **ip arp inspection limit rate 30 burst interval 1**

- Review flash cards
  (link in the description)

- Packet Tracer lab
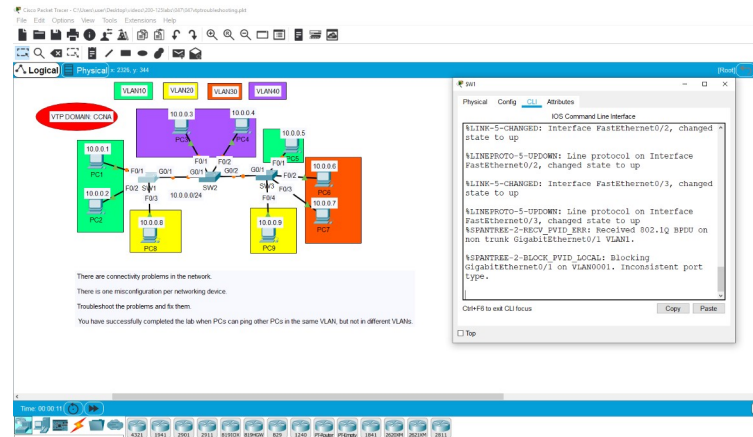
JCNP-Level Channel Members

tanvir Khan	Khoa Dang	Viktor Balogh	Donald Sabusap	john goff
Charlesetta Estelle	poopgirlSuates875...	Roger Bratseth	Gustavo BR	funnydart
Gerrard Baker	Tebogo Kgoloane	Suki Ghuman	Prakaash Rajan	velvijaykum
Tom Oakes	Anand Karandikar	Kenneth Williams	Nasir Chowdhury	Channel has been deleted
Samil Cañas	Павел М	Seamus Mooney	Erlison Santos	Boson Software
Scott Corbitt	Abraham Yeiah	Brandon Byers	Marko Barbaric	Devin Sukhu
Martin Keilaus	Serge Romeo Kwedi Ek...	Marcel Lord	Daming Li	Yonatan Makara
	Njoku Valentine	kone fine	Ed Velez	Vance Simmons

*as of June 19th, 2021