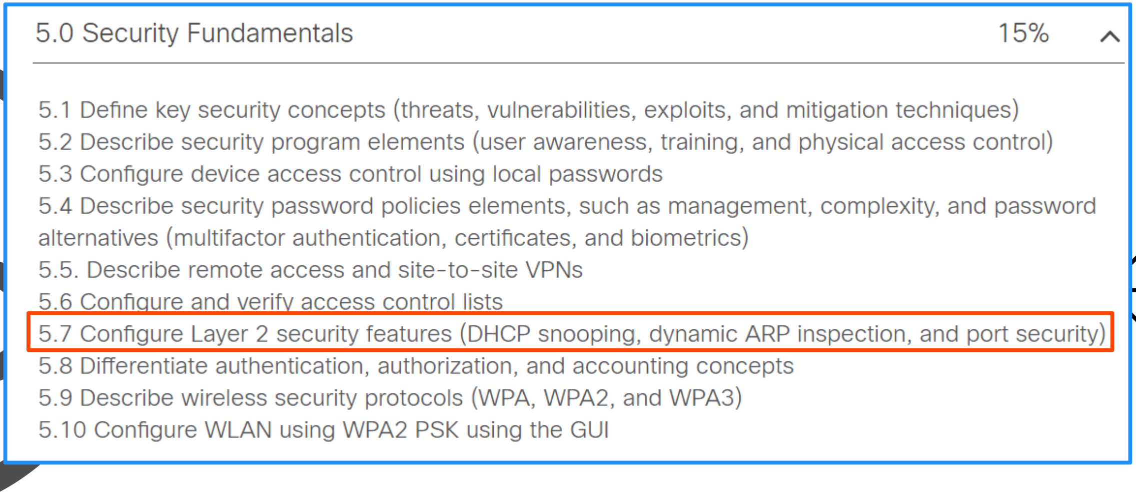
CCNA Day 50

DHCP Snooping



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

Things we'll cover

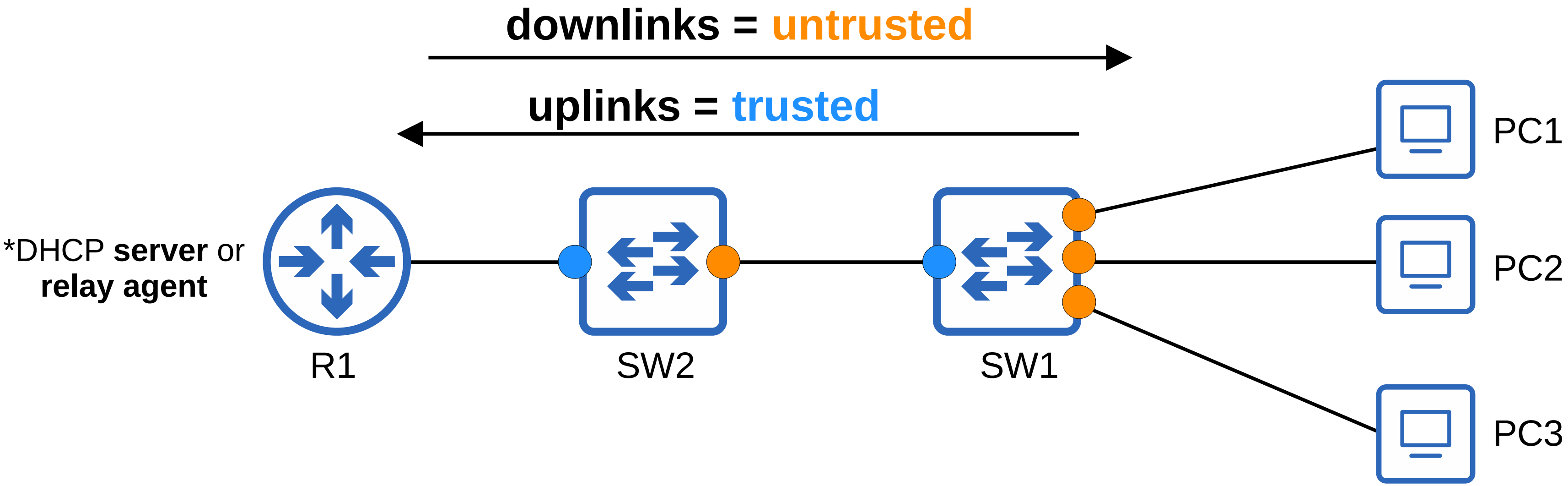
- What is DHCP Snooping?
- How does it work?
- What attacks does it prevent?
- DCHP Snooping configuration

DHCP Snooping

- DHCP snooping is a security feature of switches that is used to filter DHCP messages received on *untrusted* ports.

- DHCP snooping only filters DHCP messages. Non-DHCP messages aren't affected.

- All ports are *untrusted* by default.
  → Usually, **uplink** ports are configured as *trusted* ports, and **downlink** ports remain *untrusted.*

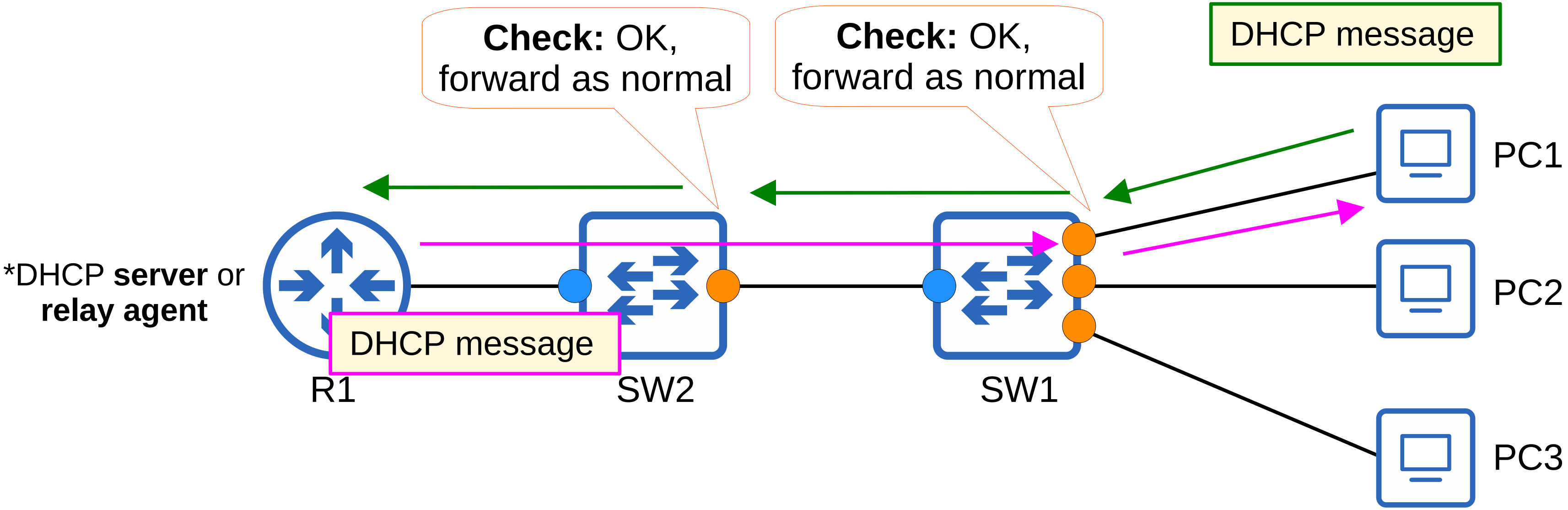

downlinks = untrusted
uplinks = trusted
*DHCP **server** or **relay agent**
R1
SW2
SW1
PC1
PC2
PC3

DHCP Snooping

- DHCP snooping is a security feature of switches that is used to filter DHCP messages received on *untrusted* ports.

- DHCP snooping only filters DHCP messages. Non-DHCP messages aren't affected.

- All ports are *untrusted* by default.
  → Usually, **uplink** ports are configured as *trusted* ports, and **downlink** ports remain *untrusted.*



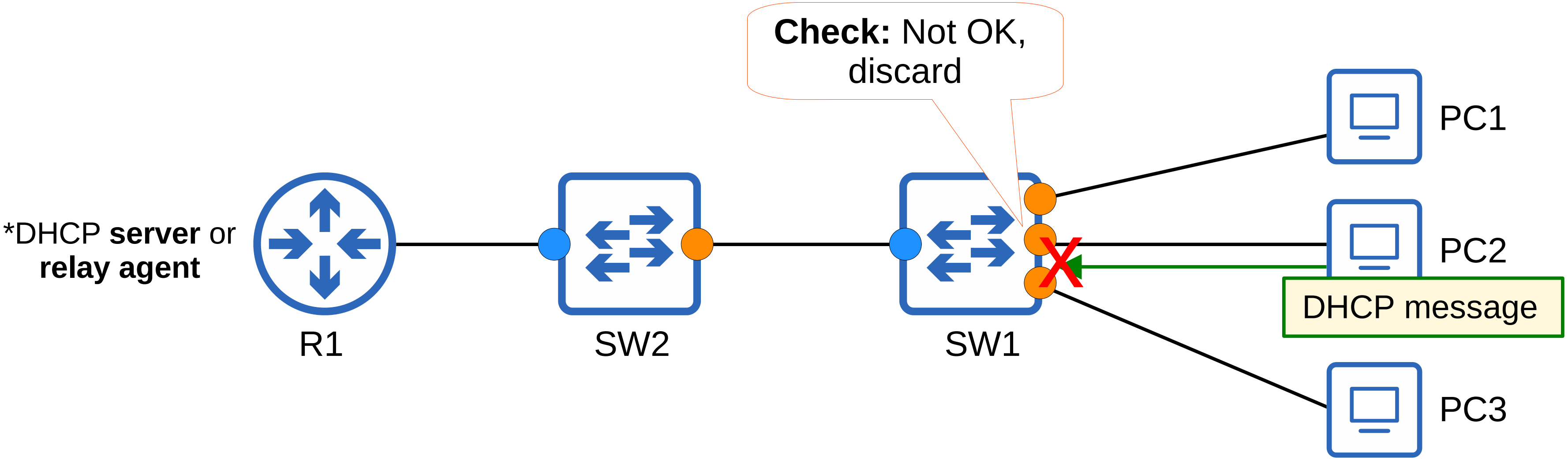
Check: OK, forward as normal
Check: OK, forward as normal
DHCP message
PC1
PC2
PC3
*DHCP **server** or **relay agent**
R1
SW2
SW1
DHCP message

DHCP Snooping

- DHCP snooping is a security feature of switches that is used to filter DHCP messages received on *untrusted* ports.

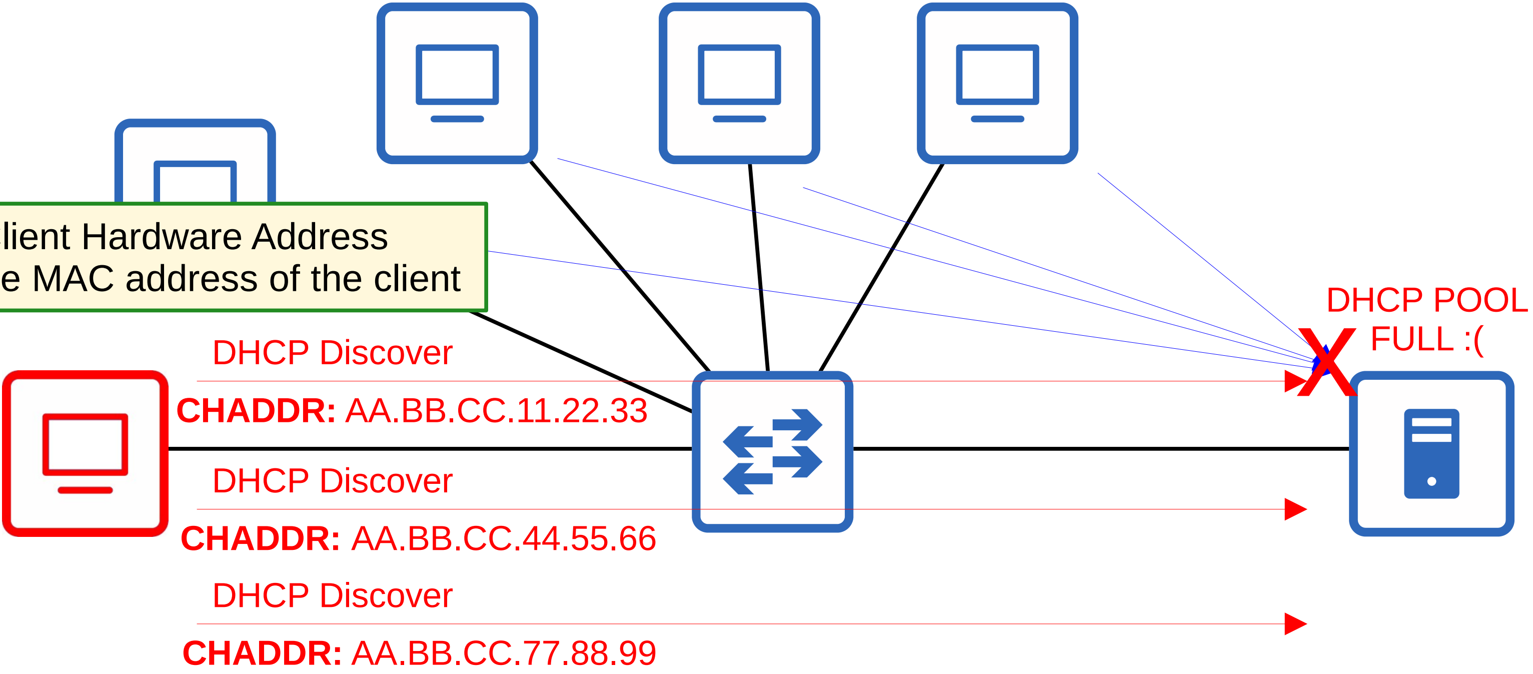
- DHCP snooping only filters DHCP messages. Non-DHCP messages aren't affected.

- All ports are *untrusted* by default.
  → Usually, **uplink** ports are configured as *trusted* ports, and **downlink** ports remain *untrusted.*


Check: Not OK, discard
PC1
PC2
DHCP message
PC3
*DHCP **server** or **relay agent**
R1
SW2
SW1

DHCP Starvation

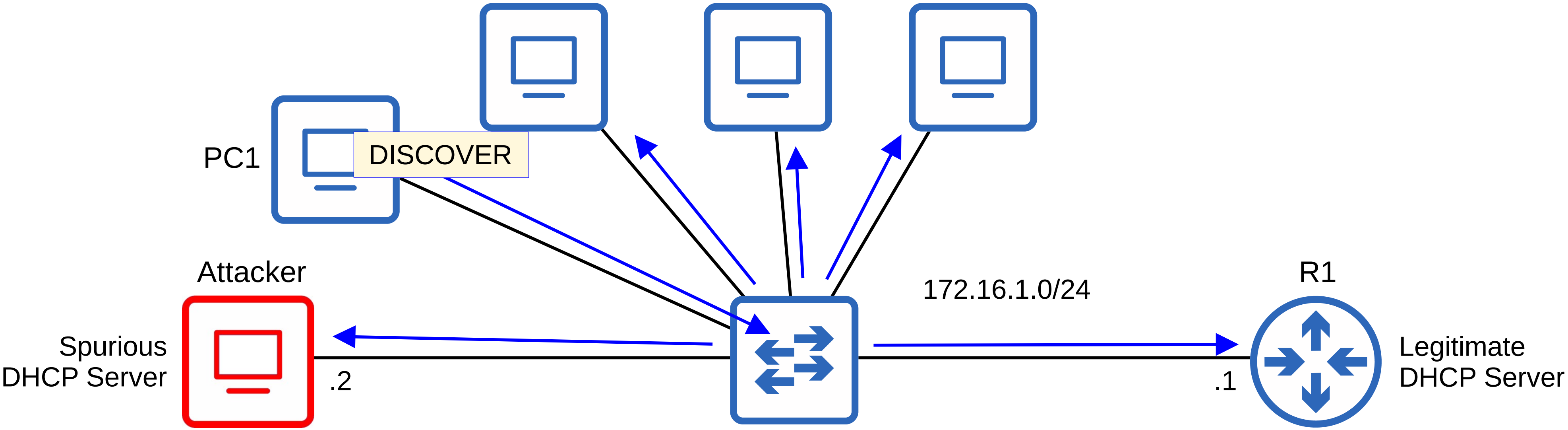
- An example of a DHCP-based attack is a **DHCP starvation** attack.
- An attacker uses spoofed MAC addresses to flood DHCP Discover messages.
- The target server's DHCP pool becomes full, resulting in a denial-of-service to other devices.


DHCP POOL FULL :(
DHCP Discover
CHADDR: AA.BB.CC.11.22.33
DHCP Discover
CHADDR: AA.BB.CC.44.55.66
DHCP Discover
CHADDR: AA.BB.CC.77.88.99

CHADDR = Client Hardware Address
→ Indicates the MAC address of the client

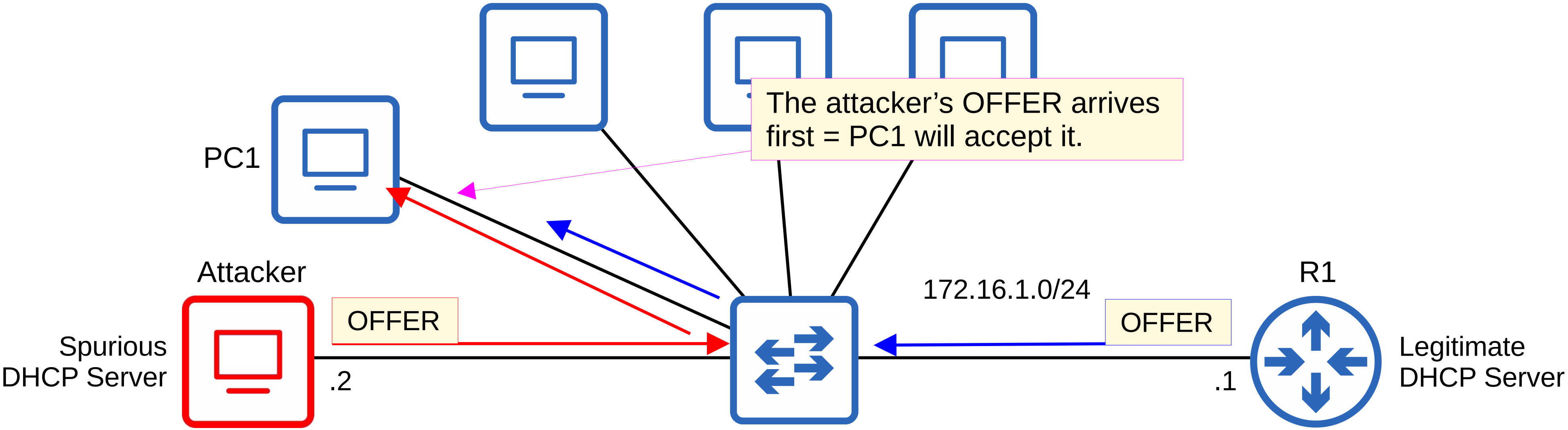
DHCP Poisoning (Man-in-the-Middle)

- Similar to ARP Poisoning, DHCP Poisoning can be used to perform a Man-in-the-Middle attack.
- A *spurious DHCP server* replies to clients' DHCP Discover messages and assigns them IP addresses, but makes the clients use the spurious server's IP as the default gateway.
  *Clients usually accept the first Offer message they receive.
- This will cause the client to send traffic to the attacker instead of the legitimate default gateway.
- The attacker can then examine/modify the traffic before forwarding it to the legitimate default gateway.



DHCP Poisoning (Man-in-the-Middle)

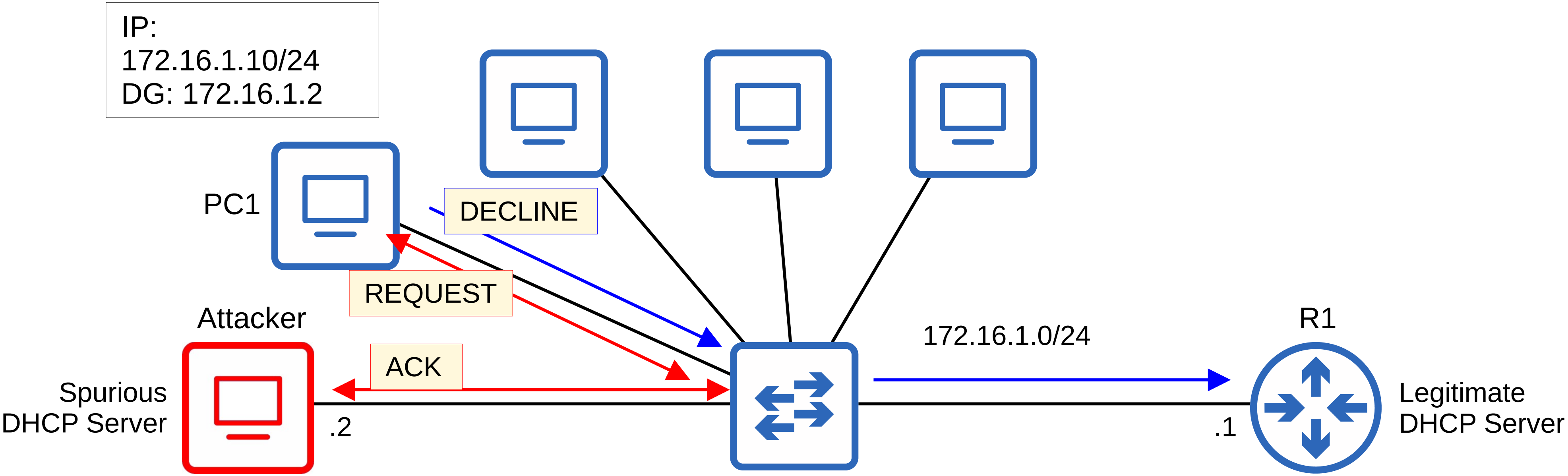
- Similar to ARP Poisoning, DHCP Poisoning can be used to perform a Man-in-the-Middle attack.
- A spurious DHCP server replies to clients' DHCP Discover messages and assigns them IP addresses, but makes the client use the spurious server's IP as the default gateway.
  *Clients usually accept the first OFFER message they receive.
- This will cause the client to send traffic to the attacker instead of the legitimate default gateway.
- The attacker can then examine/modify the traffic before forwarding it to the legitimate default gateway.



The attacker's OFFER arrives first = PC1 will accept it.

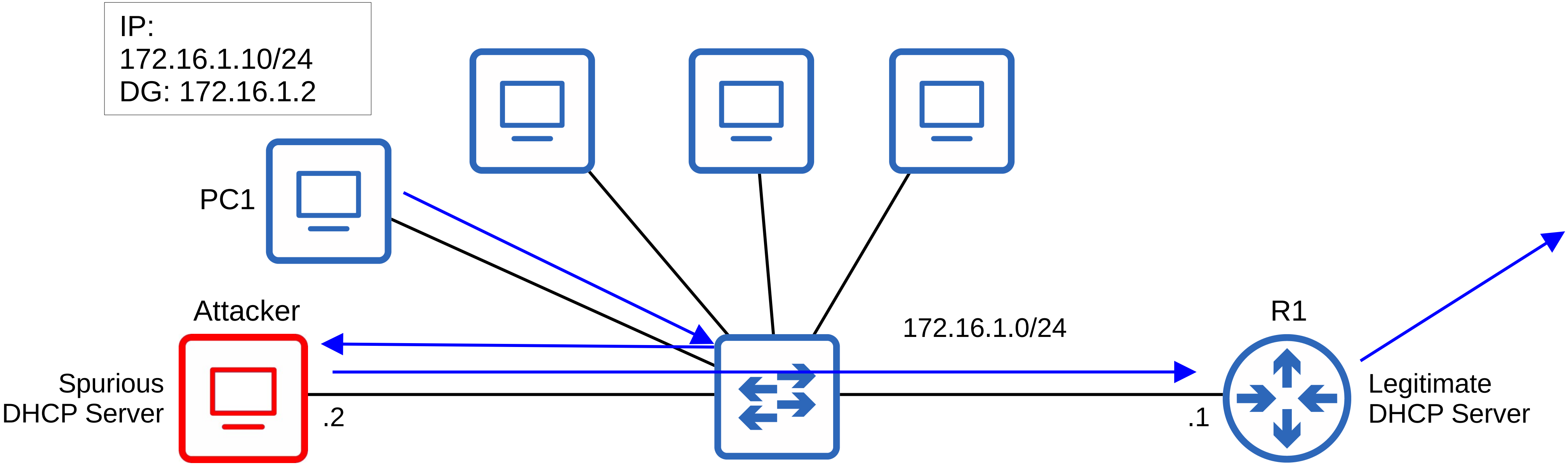
DHCP Poisoning (Man-in-the-Middle)

- Similar to ARP Poisoning, DHCP Poisoning can be used to perform a Man-in-the-Middle attack.
- A spurious DHCP server replies to clients' DHCP Discover messages and assigns them IP addresses, but makes the client use the spurious server's IP as the default gateway.
  *Clients usually accept the first OFFER message they receive.
- This will cause the client to send traffic to the attacker instead of the legitimate default gateway.
- The attacker can then examine/modify the traffic before forwarding it to the legitimate default gateway.



DHCP Poisoning (Man-in-the-Middle)

- Similar to ARP Poisoning, DHCP Poisoning can be used to perform a Man-in-the-Middle attack.
- A spurious DHCP server replies to clients' DHCP Discover messages and assigns them IP addresses, but makes the client use the spurious server's IP as the default gateway.
  *Clients usually accept the first OFFER message they receive.
- This will cause the client to send traffic to the attacker instead of the legitimate default gateway.
- The attacker can then examine/modify the traffic before forwarding it to the legitimate default gateway.



DHCP Messages

- When DHCP Snooping filters messages, it differentiates between **DHCP Server** messages and **DHCP Client** messages

- Messages sent by **DHCP Servers**:
  → OFFER
  → ACK
  → NAK = Opposite of ACK, used to decline a client’s REQUEST

- Messages sent by **DHCP Clients:**
  → DISCOVER
  → REQUEST
  → RELEASE = Used to tell the server that the client no longer needs its IP address
  → DECLINE = Used to decline the IP address offered by a DHCP server

DHCP Snooping Operations

- If a DHCP message is received on a **trusted port**, forward it as normal without inspection.

- If a DHCP message is received on an **untrusted port**, inspect it and act as follows:
  → If it is a **DHCP Server** message, discard it.

  → If it is a **DHCP Client** message, perform the following checks:

  DISCOVER/REQUEST messages: Check if the frame's source MAC address and the DHCP message's CHADDR fields match. Match = forward, mismatch = discard

  RELEASE/DECLINE messages: Check if the packet's source IP address and the receiving interface match the entry in the *DHCP Snooping Binding Table*. Match = forward, mismatch = discard

- When a client successfully leases an IP address from a server, create a new entry in the *DHCP Snooping Binding Table*.

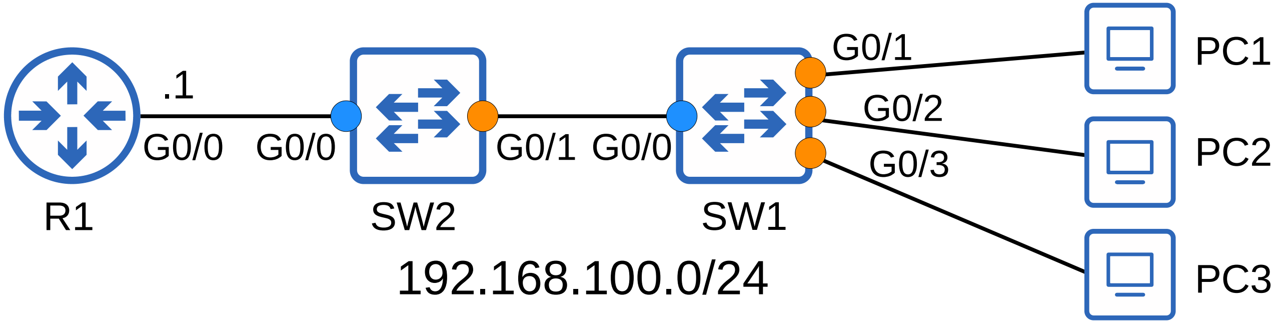
DHCP Snooping

```
SW2(config)#ip dhcp snooping
SW2(config)#ip dhcp snooping vlan 1
SW2(config)#no ip dhcp snooping information option
SW2(config)#interface g0/0
SW2(config-if)#ip dhcp snooping trust
```

I will explain this later!

```
SW1(config)#ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 1
SW1(config)#no ip dhcp snooping information option
SW1(config)#interface g0/0
SW1(config-if)#ip dhcp snooping trust

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
```

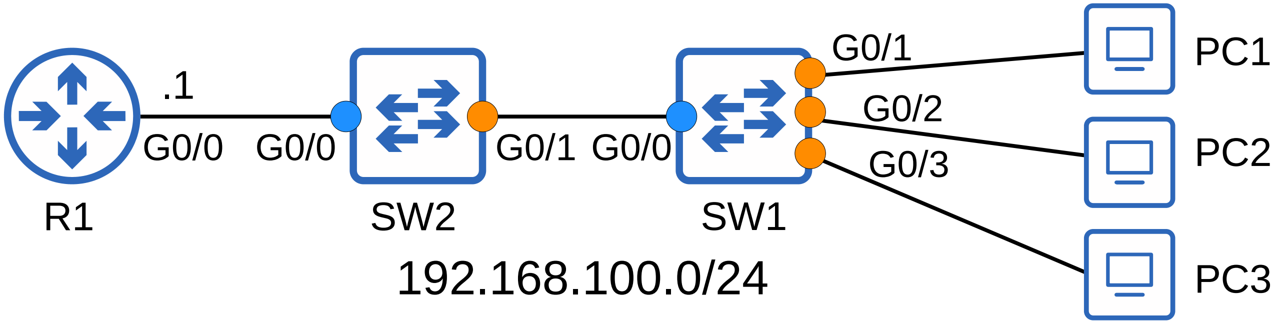
RELEASE/DECLINE messages will be checked to make sure their IP address/interface ID match the entry in the DHCP snooping table.



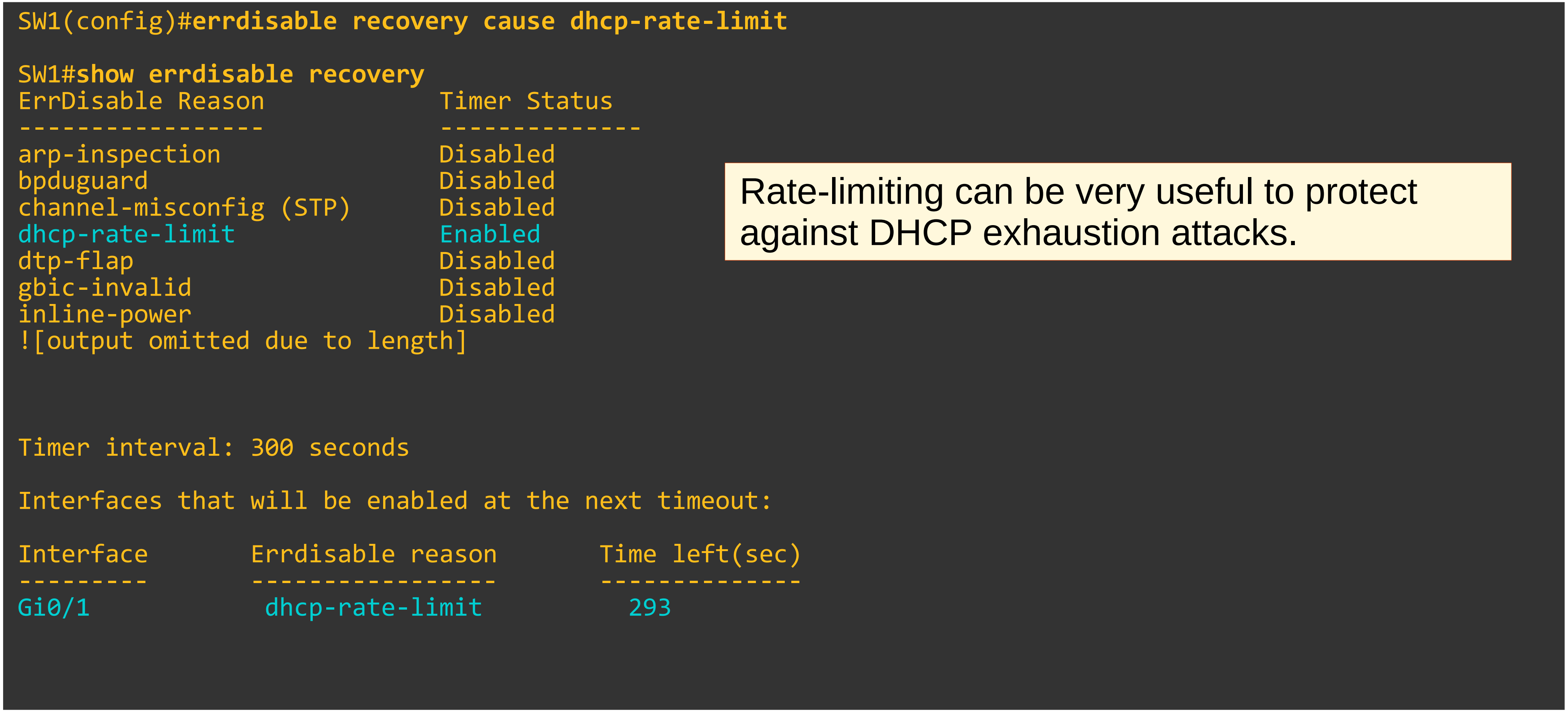
DHCP Snooping Rate-Limiting

- DHCP snooping can limit the rate at which DHCP messages are allowed to enter an interface.
- If the rate of DHCP messages crosses the configured limit, the interace is err-disabled.
- Like with Port Security, the interface can be manually re-enabled, or automatically re-enabled with errdisable recovery.

```
SW1(config)#interface range g0/1 - 3
SW1(config-if-range)#ip dhcp snooping limit rate 1

*Jun  5 13:15:14.180: %DHCP_SNOOPING-4-DHCP_SNOOPING_ERRDISABLE_WARNING: DHCP Snooping received 1 DHCP packets on
interface Gi0/1
*Jun  5 13:15:14.181: %DHCP_SNOOPING-4-DHCP_SNOOPING_RATE_LIMIT_EXCEEDED: The interface Gi0/1 is receiving more
than the threshold set
*Jun  5 13:15:14.182: %PM-4-ERR_DISABLE: dhcp-rate-limit error detected on Gi0/1, putting Gi0/1 in err-disable
state
*Jun  5 13:15:15.185: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
*Jun  5 13:15:16.190: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
```



DHCP Snooping Rate-Limiting



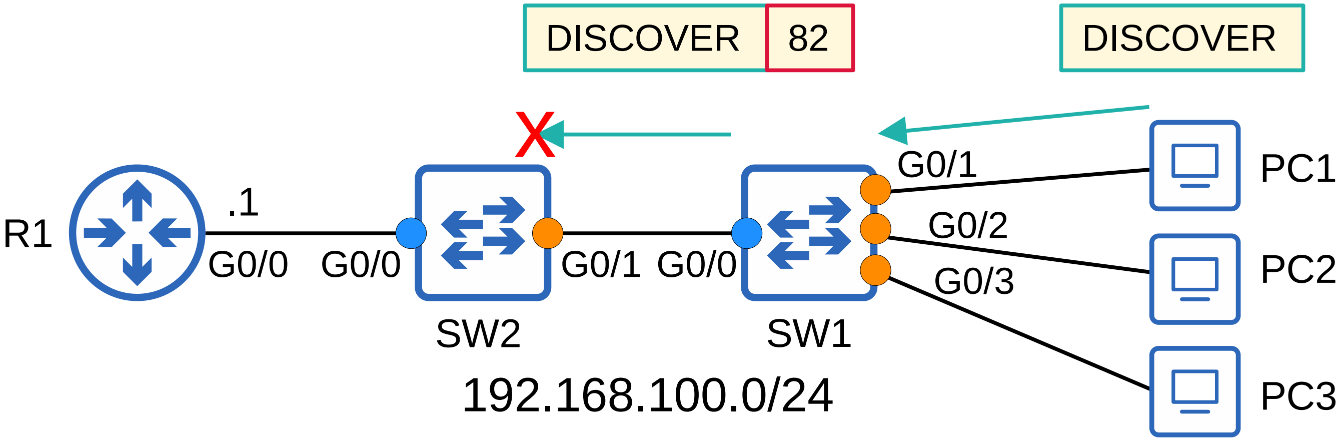
```
SW1(config)#errdisable recovery cause dhcp-rate-limit

SW1#show errdisable recovery
ErrDisable Reason             Timer Status
-----------------             --------------
arp-inspection                Disabled
bpduguard                     Disabled
channel-misconfig (STP)       Disabled
dhcp-rate-limit               Enabled
dtp-flap                      Disabled
gbic-invalid                  Disabled
inline-power                  Disabled
![output omitted due to length]



Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

Interface       Errdisable reason       Time left(sec)
---------       -----------------       --------------
Gi0/1            dhcp-rate-limit          293
```

Rate-limiting can be very useful to protect against DHCP exhaustion attacks.

DHCP Option 82 (Information Option)

- Option 82, also known as the ‘DHCP relay agent information option’ is one of many DHCP options.
- It provides additional information about which DHCP relay agent received the client’s message, on which interface, in which VLAN, etc.
- DHCP relay agents can add Option 82 to messages they forward to the remote DHCP server.
- With DHCP snooping enabled, by default Cisco switches will add Option 82 to DHCP messages they receive from clients, even if the switch isn’t acting as a DHCP relay agent.
- By default, Cisco switches will drop DHCP messages with Option 82 that are received on an untrusted port.

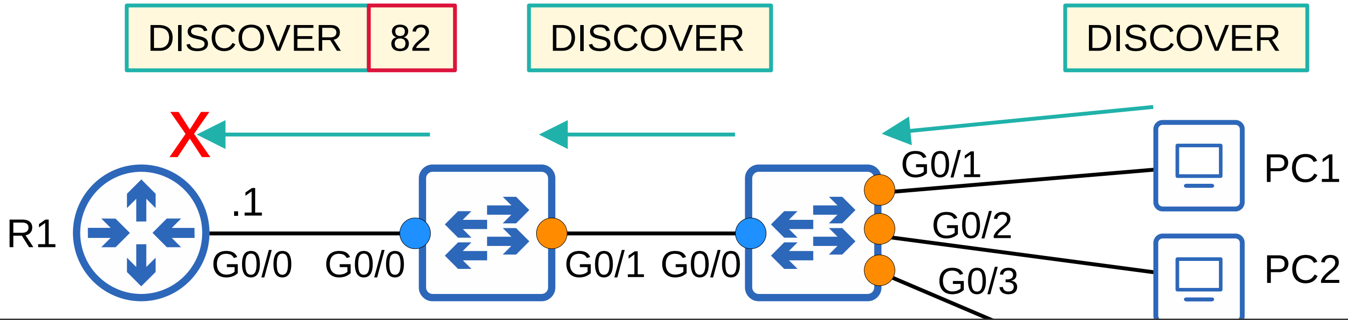
```
SW2#
*Jun  6 01:36:15.298: %DHCP_SNOOPING-5-DHCP_SNOOPING_NONZERO_GIADDR: DHCP_SNOOPING drop message with non-
zero giaddr or option82 value on untrusted port, message type: DHCPDISCOVER, MAC sa: 0c29.2f67.e900
```



DHCP Option 82 (Information Option)

- Option 82, also known as the ‘DHCP relay agent information option’ is one of many DHCP options.
- It provides additional information about which DHCP relay agent received the client’s message, on which interface, in which VLAN, etc.
- DHCP relay agents can add Option 82 to messages they forward to the remote DHCP server.
- With DHCP snooping enabled, by default Cisco switches will add Option 82 to DHCP messages they receive from clients, even if the switch isn’t acting as a DHCP relay agent.
- By default, Cisco switches will drop DHCP messages with Option 82 that are received on an untrusted port.

```
SW1(config)#no ip dhcp snooping information option
```



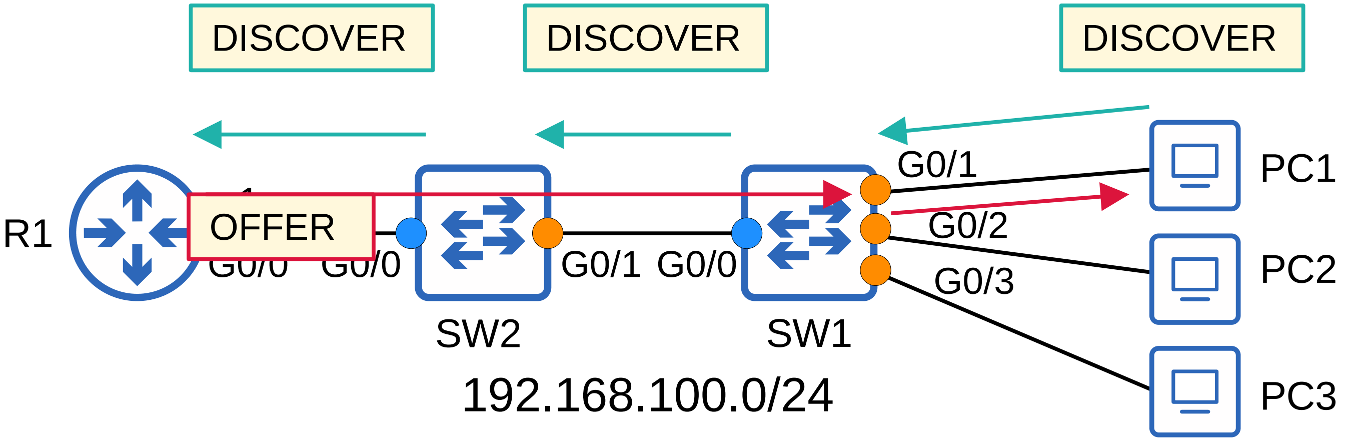
```
R1#
*Jun  6 01:46:46.763: DHCPD: inconsistent relay information.
*Jun  6 01:46:46.763: DHCPD: relay information option exists, but giaddr is zero.
```

DHCP Option 82 (Information Option)

- Option 82, also known as the ‘DHCP relay agent information option’ is one of many DHCP options.
- It provides additional information about which DHCP relay agent received the client’s message, on which interface, in which VLAN, etc.
- DHCP relay agents can add Option 82 to messages they forward to the remote DHCP server.
- With DHCP snooping enabled, by default Cisco switches will add Option 82 to DHCP messages they receive from clients, even if the switch isn’t acting as a DHCP relay agent.
- By default, Cisco switches will drop DHCP messages with Option 82 that are received on an untrusted port.

```
SW1(config)#no ip dhcp snooping information option
```

```
SW2(config)#no ip dhcp snooping information option
```



Command Review

```
SW1(config)# ip dhcp snooping

SW1(config)# ip dhcp snooping vlan vlan-number

SW1(config)# errdisable recovery cause dhcp-rate-limit

SW1(config)# no ip dhcp snooping information option

SW1(config-if)# ip dhcp snooping trust

SW1(config-if)# ip dhcp snooping limit rate packets-per-second

SW1# show ip dhcp snooping binding
```

Things we'll cover

- What is DHCP Snooping?
- How does it work?
- What attacks does it prevent?
- DCHP Snooping configuration

Quiz 1

Which of the following DHCP message types will always be discarded if received on a DHCP snooping untrusted interface? (select three)

a) DISCOVER

b) REQUEST

c) NAK

d) OFFER

e) DECLINE

f) RELEASE

g) ACK

Quiz 2

Which of the following is NOT stored in the DHCP snooping binding database?

a) IP address

b) Interface

c) VLAN

d) Default gateway

e) MAC address

```
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
```

Quiz 3

Which of the following are functions of DHCP snooping? (select two)

a) Limiting the rate of DCHP messages

b) Filtering DHCP messages on trusted ports

c) Filtering DHCP messages on untrusted ports

d) Filtering all DHCP messages

Quiz 4

When DHCP snooping inspects a DHCP DISCOVER message that arrives on an untrusted interface, what does it check? (select the two best answers)

a) Source MAC address

b) CHADDR

c) IP address

d) Interface

Quiz 5

DHCP snooping rate-limiting is configured on SW1’s G0/1 interface. What happens if DHCP messages are received on G0/1 at a rate faster than the configured limit?

a) The messages that cross the limit will be dropped

b) The interface will be disabled

c) All DHCP messages on the interface will be dropped

d) A warning syslog message will be displayed