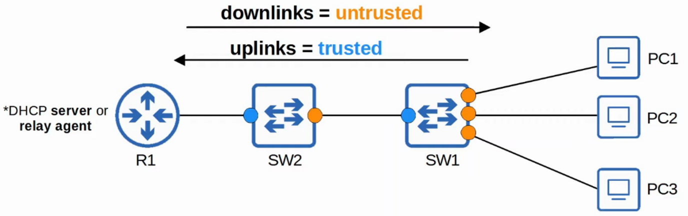
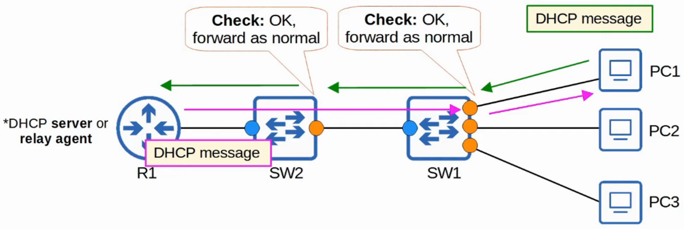
50. DHCP SNOOPING (LAYER 2)

WHAT IS 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 are not affected
- All PORTS are UNTRUSTED, by DEFAULT
  - Usually UPLINK PORTS are configured as TRUSTED PORTS, and DOWNLINK PORTS remain UNTRUSTED



image

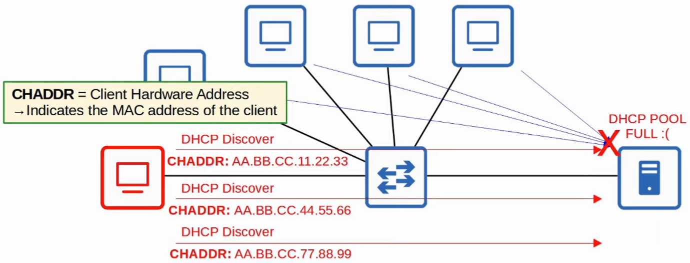

Check: OK, forward as normal
Check: OK, forward as normal
DHCP message
PC1
*DHCP server or relay agent
DHCP message
R1
SW2
SW1
PC2
PC3

image

ATTACKS ON DHCP

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 DoS to other DEVICES


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

image

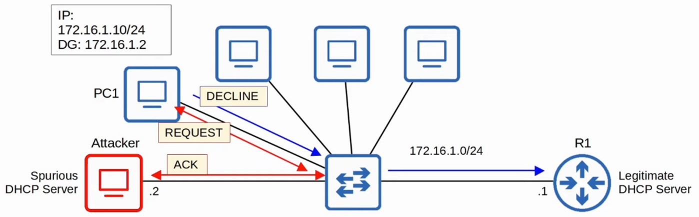
DHCP POISONING (Man-in-the-Middle)

- 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*

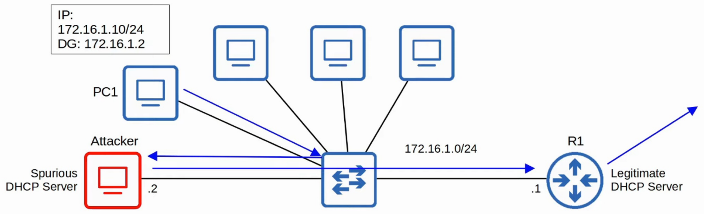
IP as a DEFAULT GATEWAY

** CLIENTS usually accept the first DHCP 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



image



image

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:

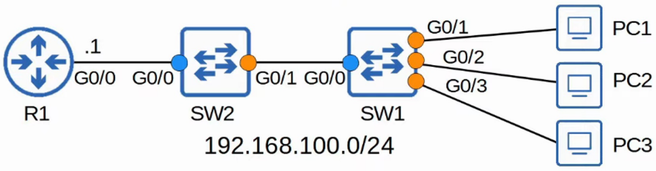
  - DISCOVER
  - REQUEST
  - RELEASE = Used to tell the SERVER that the CLIENT no longer needs its IP ADDRESS
  - DECLINE = Used to DECLINE the IP ADDRESS offered by a DHCP SERVER

HOW DOES IT WORK?

- 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 as 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*

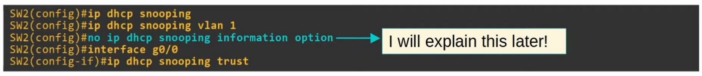
    - MATCH = FORWARD
    - MISMATCH = DISCARD
- When a CLIENT successfully leases an IP ADDRESS from a SERVER, create a new entry in the *DHCP SNOOPING BINDING TABLE*

DHCP SNOOPING CONFIGURATION



image

SWITCH 2's CONFIGURATION

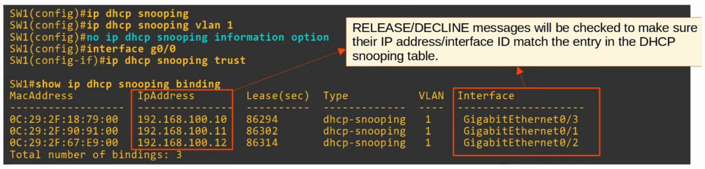


```
SW2(config)#ip dhcp snooping
SW2(config)#ip dhcp snooping vlan 1
SW2(config)#no ip dhcp snooping information option
SW2(config)#interface g0/0
SW2(config-if)#ip dhcp snooping trust
```

I will explain this later!

image

SWITCH 1's CONFIGURATION



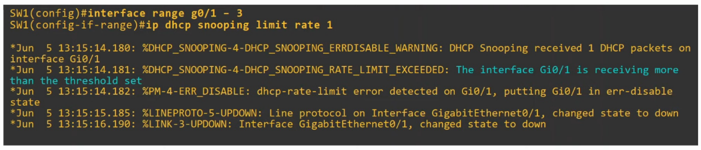
```
SW1(config)#ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 1
SW1(config)#no ip dhcp snooping information option
SW1(config)#interface g0/0
SW1(config-if)#ip dhcp snooping trust

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.

image

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 INTERFACE is `err-disabled`
- Like with PORT SECURITY, the interface can be manually re-enabled, or automatically re-enabled with `errdisable recovery`

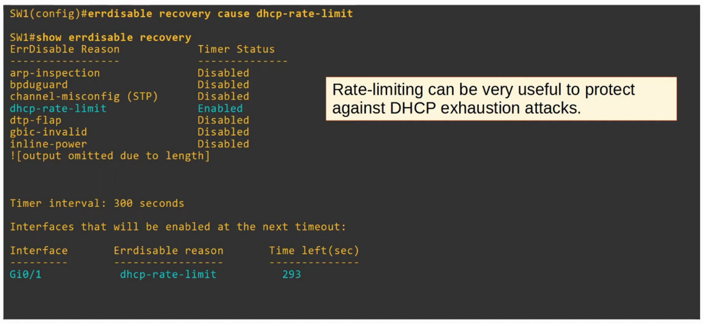


```
SW1(config)#interface range g0/1 - 3
SW1(config-if-range)#ip dhcp snooping limit rate 1

*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
```

image

- You wouldn't set the limit rate to 1 since it's so low, it would shut the port immediately but this shows how RATE-LIMITING works

`errdisable recovery cause dhcp-rate-limit`



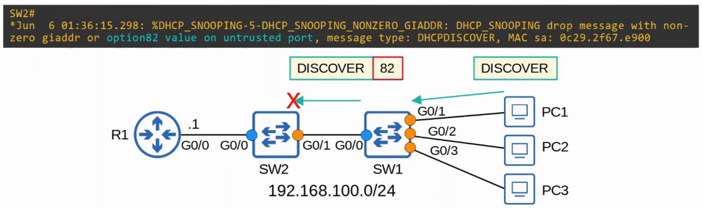
```
SW1(config)#errdisable recovery cause dhcp-rate-limit

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.

image

DHCP OPTION 82 (INFORMATION OPTION)

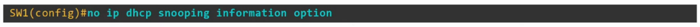
- OPTION 82, also known as a ‘DHCP RELAY AGENT INFOMRATION OPTION’ is one of MANY DHCP OPTIONS
- It provides additional information about which DHCP RELAY AGENT received the CLIENT’S message, on which INTERFACE, in which VLAN, etc.
- DHCP RELAY AGENTS can add OPTION 82 to message they forward to the 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
```

image

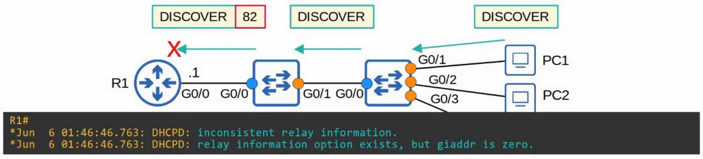
THIS command disables OPTION 82 for SW1 but NOT SW2



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

image

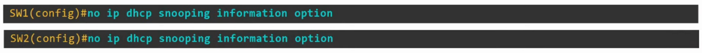
TRAFFIC gets passed to R1 and is DROPPED because of “inconsistent relay information” (packet contains OPTION 82 but wasn’t dropped by SW2)



```
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.
```

image

By ENABLING OPTION 82 on both SWITCHES…

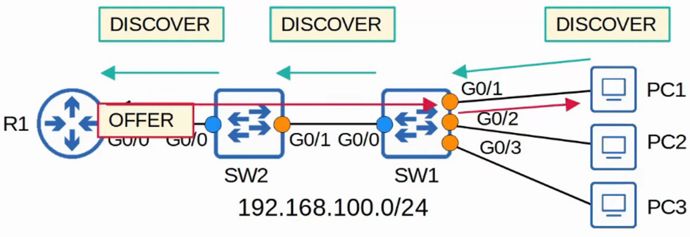


```
SW1(config)#no ip dhcp snooping information option
```

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

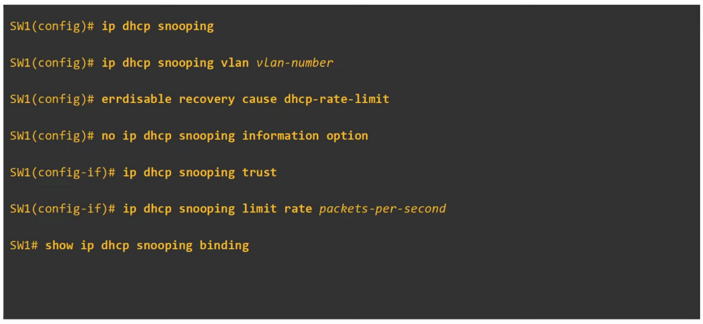
image

PC1’s DHCP DISCOVER message gets passed, through SW1 and SW2, to R1. R1 responds with an DHCP OFFER message, as normal



image

COMMAND SUMMARY



```
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
```

image