CCNA 200-301, Volume 2

Chapter 8

DHCP Snooping and ARP Inspection

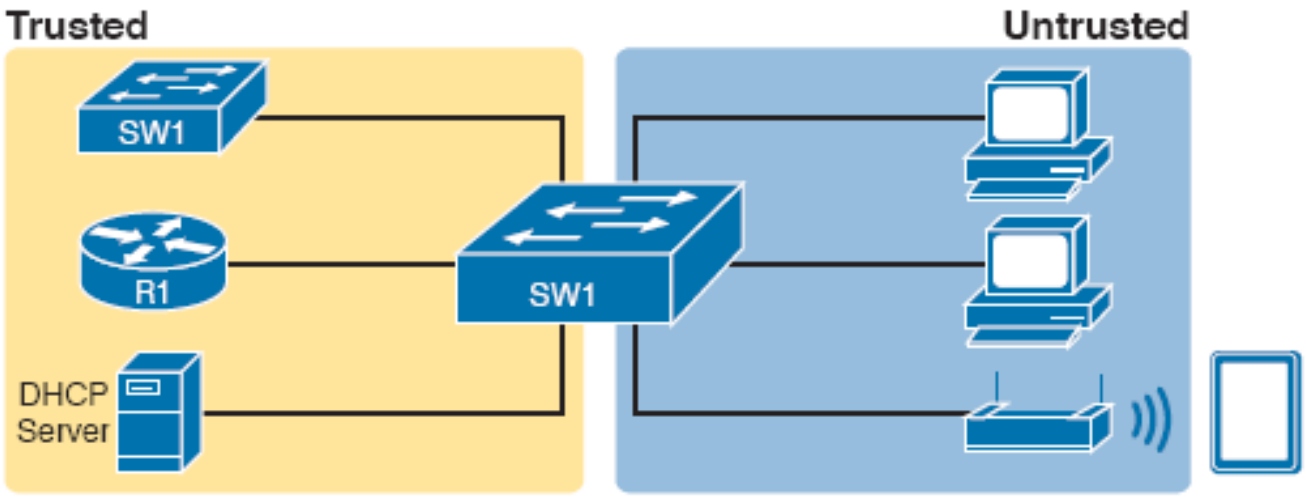
Objectives

- Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)

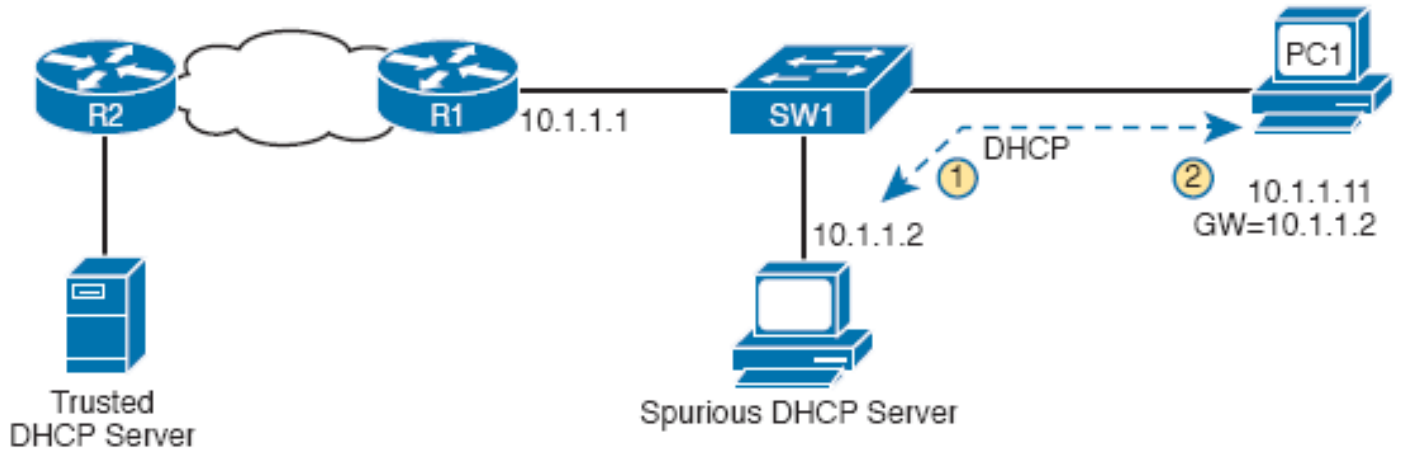
DHCP Snooping

- Acts like a firewall or an ACL in many ways
- Watches for incoming messages on either all ports or some ports
- Looks for DHCP messages and ignores all non-DHCP messages
- DHCP snooping logic: allow the message or discard the message
- Acts off the concept of trusted and untrusted ports for determining which DHCP messages are allowed

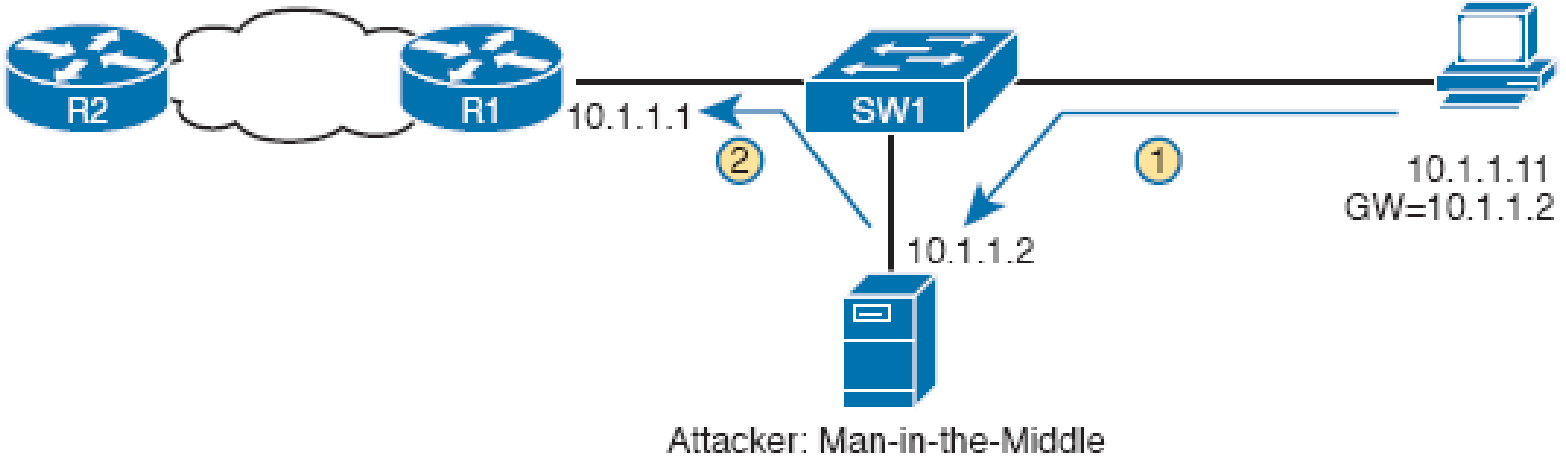
DHCP Snooping Basics: Client Ports are Untrusted



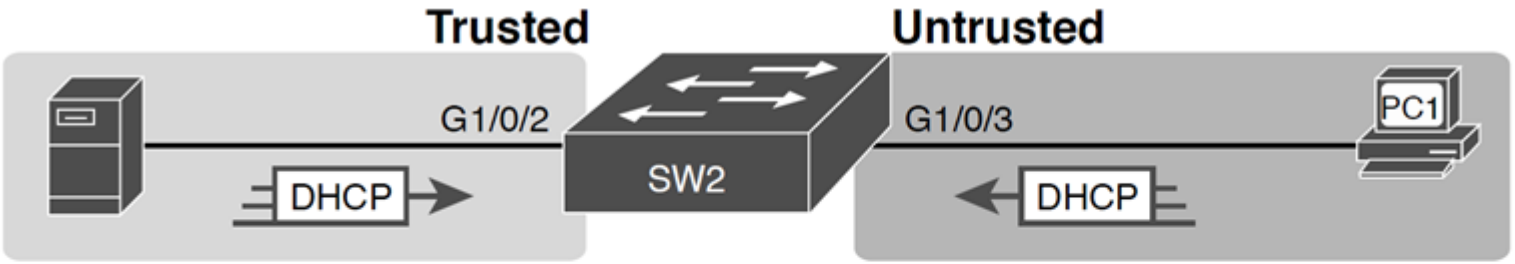
DHCP Attack Supplies Good IP Address but Wrong Default Gateway



Unfortunate Result: DHCP Attack Leads to Man-in-the-Middle



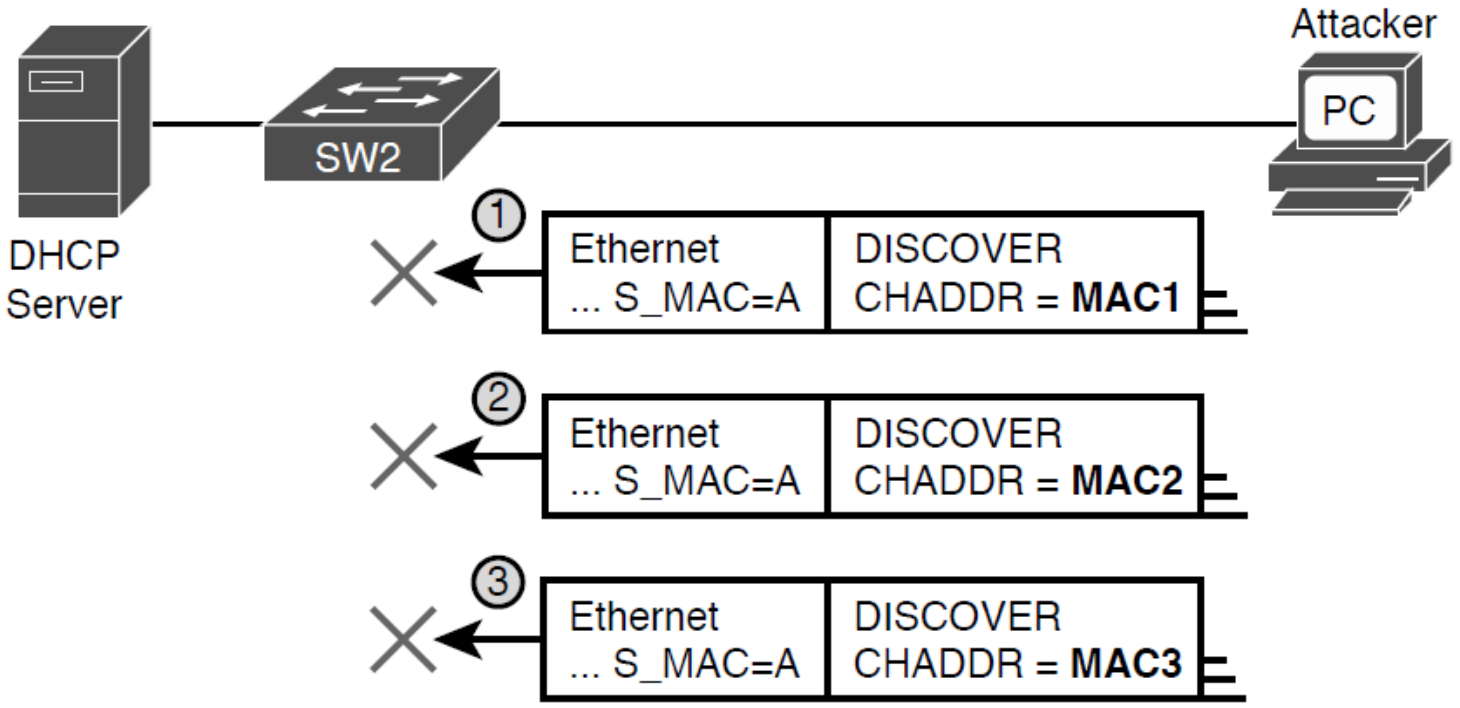
Summary of Rules for DHCP Snooping



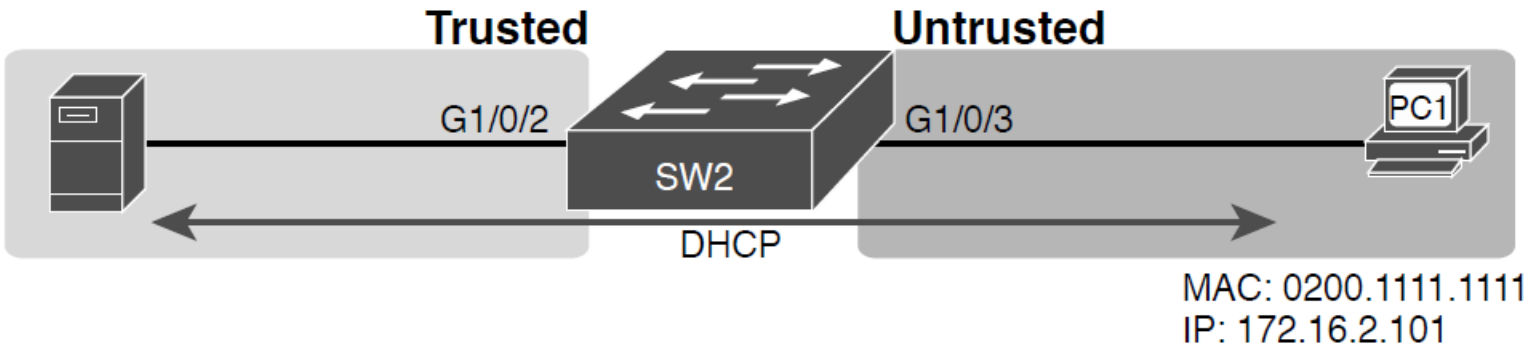
DHCP **All** Messages: **Approved!**

DHCP **Server** Messages: **Rejected!**
DHCP **Client** Messages:
A) Check DISCOVER MAC Addresses
B) Check RELEASE/DECLINE

DHCP Snooping Checks chaddr and Ethernet Source MAC



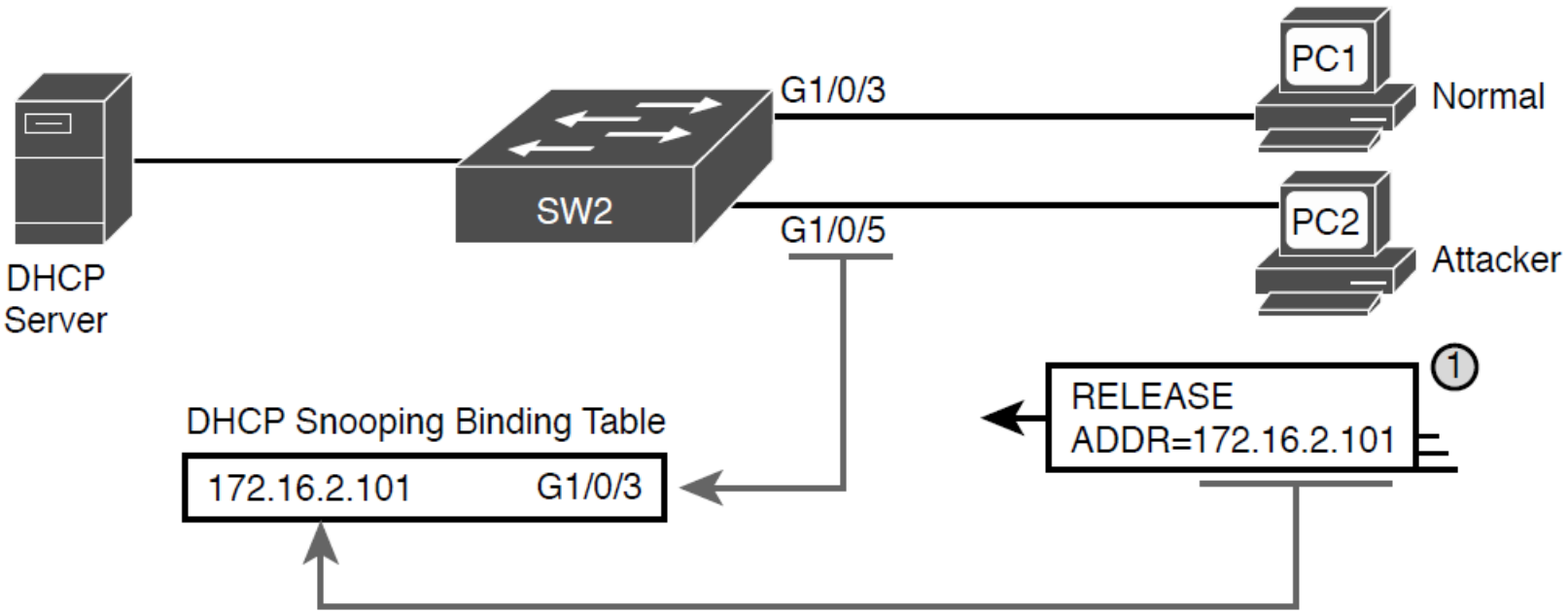
Legitimate DHCP Client with DHCP Binding Entry Built by DHCP Snooping



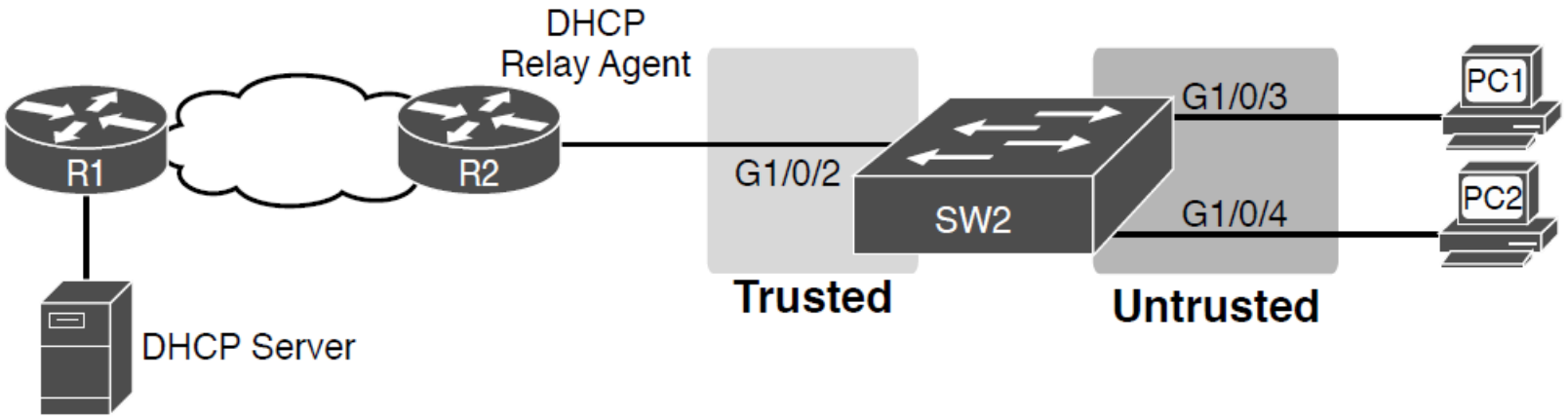
SW2 DHCP Snooping Binding Table

MAC	IP	VLAN	Interface
0200.1111.1111	172.16.2.101	11	G1/0/3

DHCP Snooping Defeats a DHCP RELEASE from Another Port



Sample Network Used in DHCP Snooping Configuration Examples



DHCP Snooping Configuration to Match Previous Graphic

```
ip dhcp snooping
ip dhcp snooping vlan 11
no ip dhcp snooping information option
!
interface GigabitEthernet1/0/2
 ip dhcp snooping trust
```

SW2 DHCP Snooping Status

```
SW2# show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
11
DHCP snooping is operational on following VLANs:
11
Smartlog is configured on following VLANs:
none
Smartlog is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is disabled
   circuit-id default format: vlan-mod-port
   remote-id: bcc4.938b.a180 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
GigabitEthernet1/0/2       yes        yes             unlimited
  Custom circuit-ids:
```

Configuring DHCP Snooping Message Rate Limits

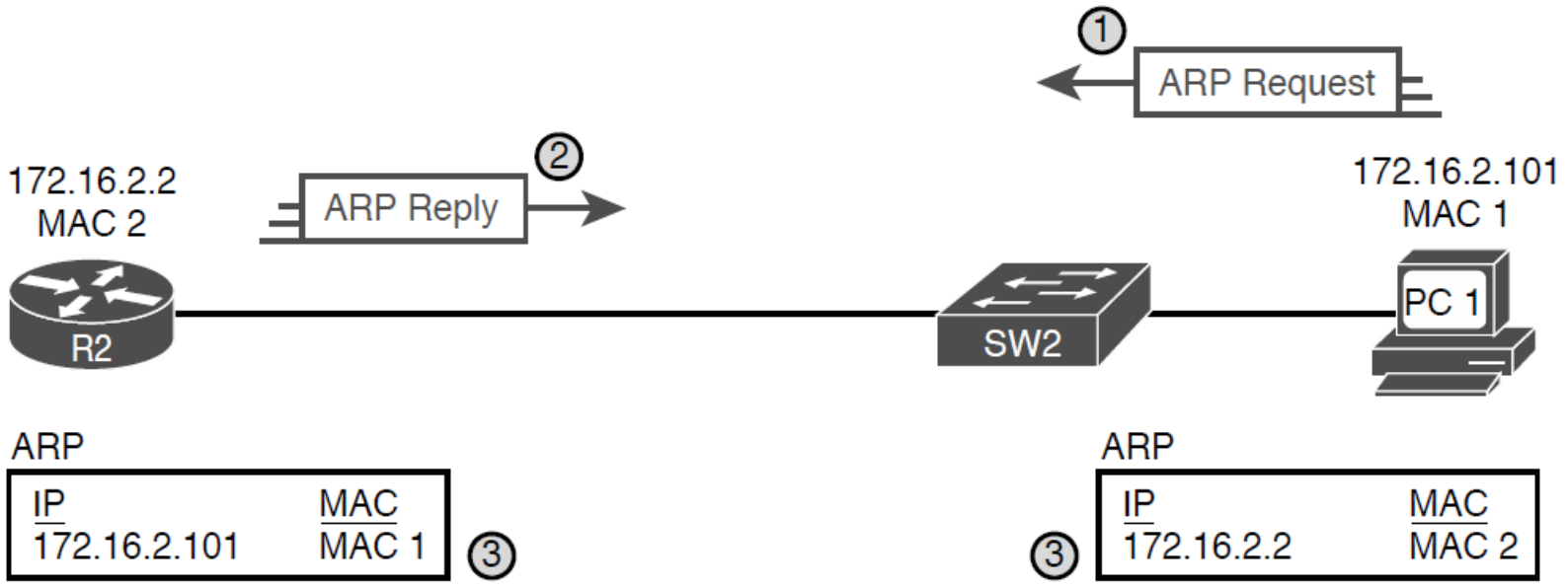
```
errdisable recovery cause dhcp-rate-limit
errdisable recovery interval 30
!
interface GigabitEthernet1/0/2
 ip dhcp snooping limit rate 10
!
interface GigabitEthernet1/0/3
 ip dhcp snooping limit rate 2
```

Confirming DHCP Snooping Rate Limits

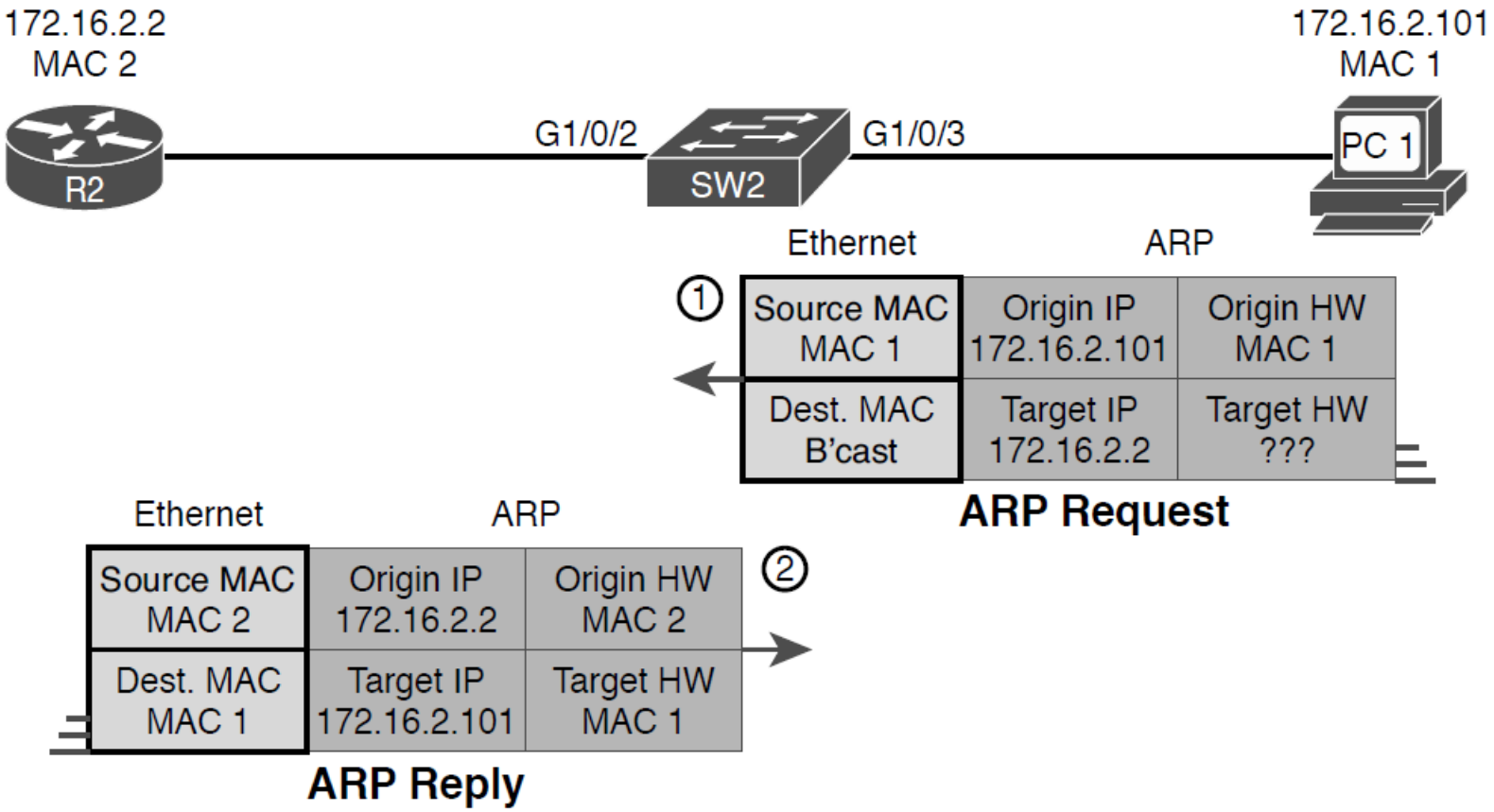
```
SW2# show ip dhcp snooping
! Lines omitted for brevity

Interface                    Trusted    Allow option    Rate limit (pps)
-----------------------      -------    ------------    ----------------
GigabitEthernet1/0/2         yes        yes             10
  Custom circuit-ids:
GigabitEthernet1/0/3         no         no              2
  Custom circuit-ids:
```

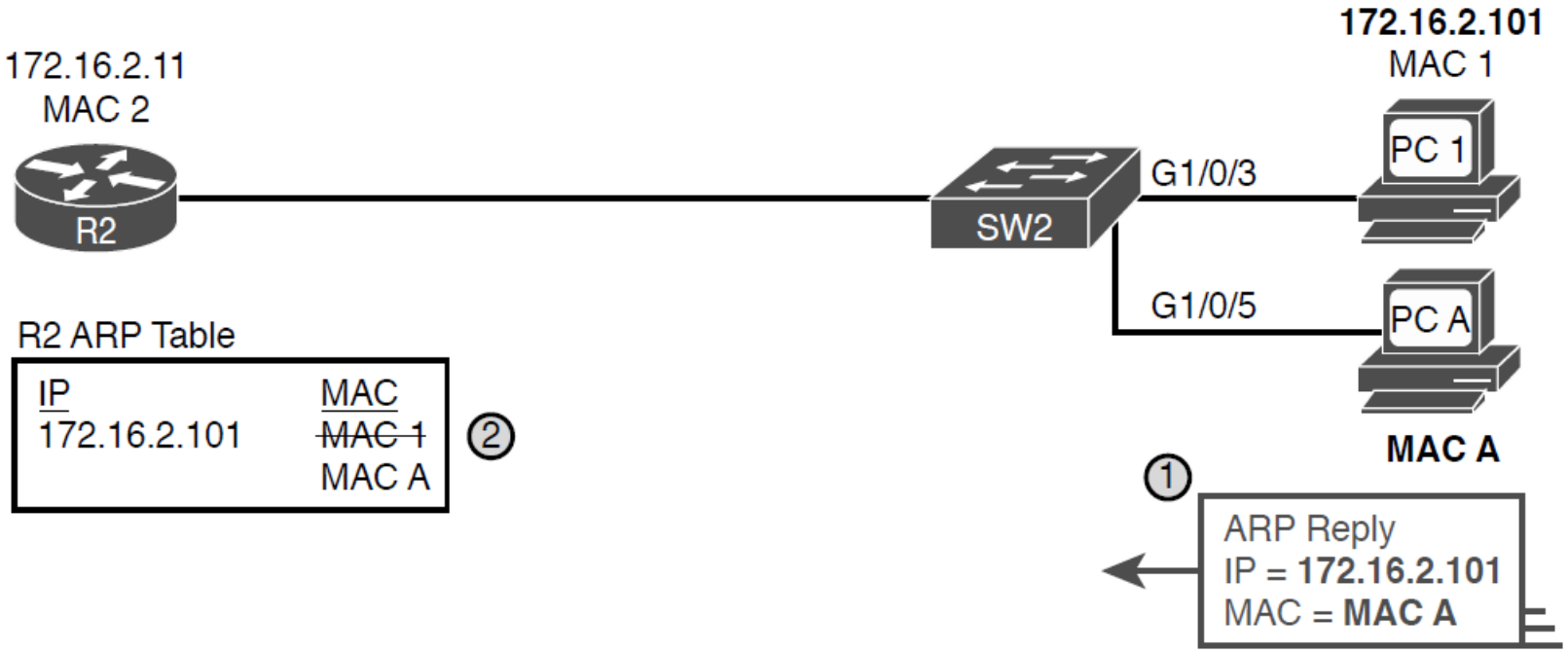
Legitimate ARP Tables After PC1 DHCP and ARP with Router R2



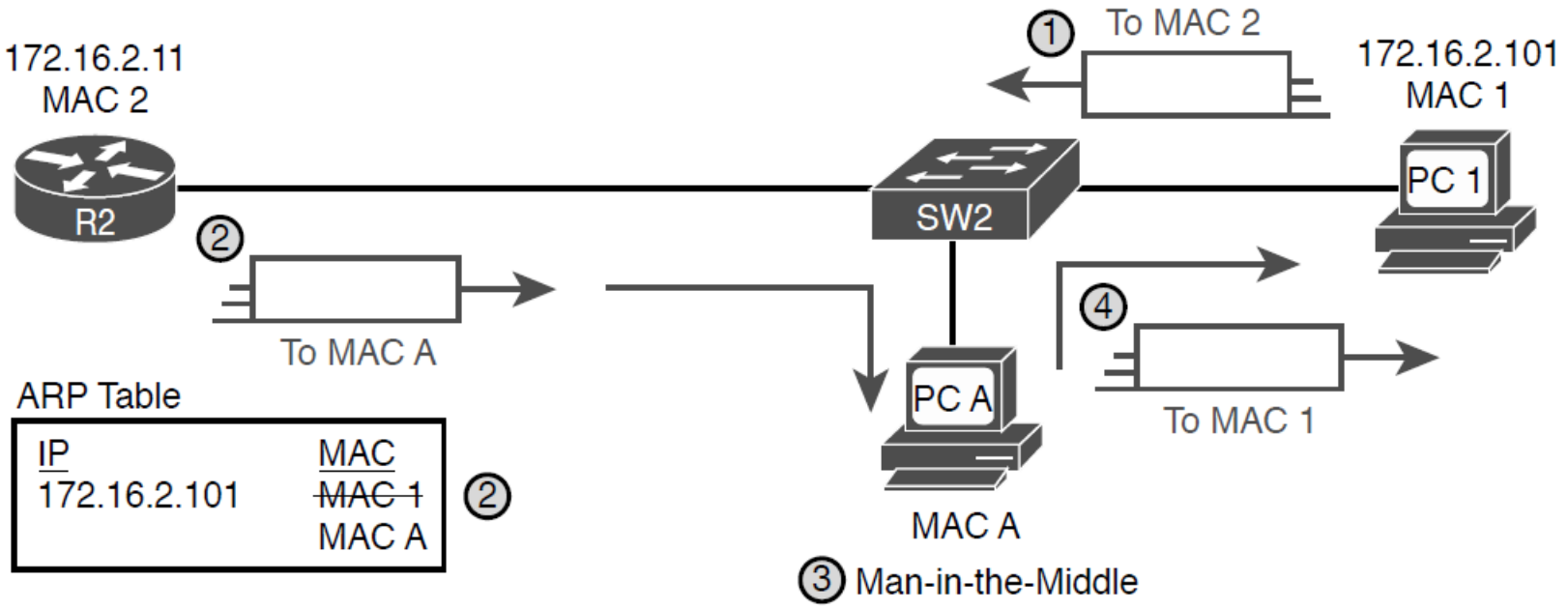
A Detailed Look at ARP Request and Reply



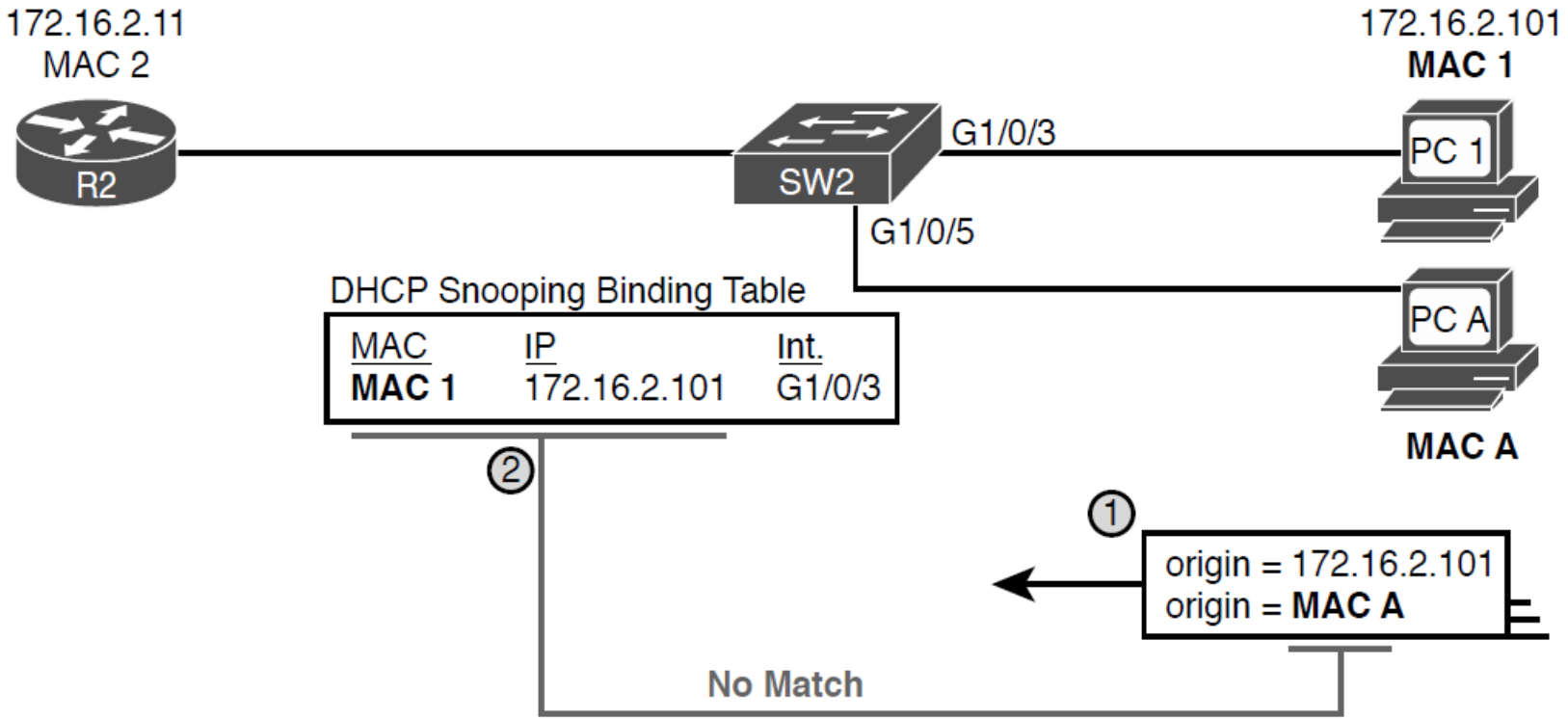
Nefarious Use of ARP Reply Causes Incorrect ARP Data on R2



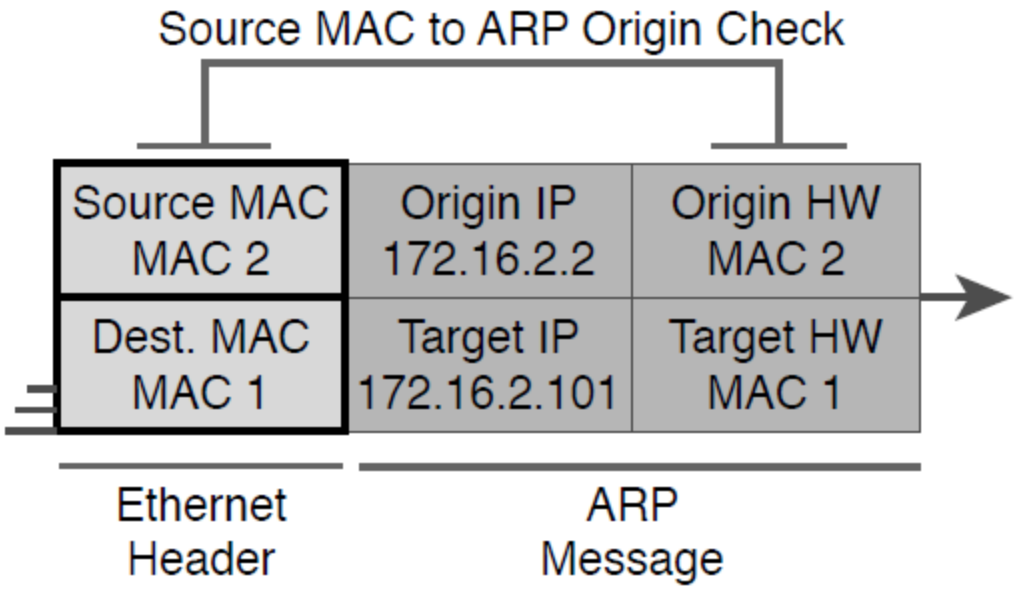
Man-in-the-Middle Attack Resulting from Gratuitous ARP



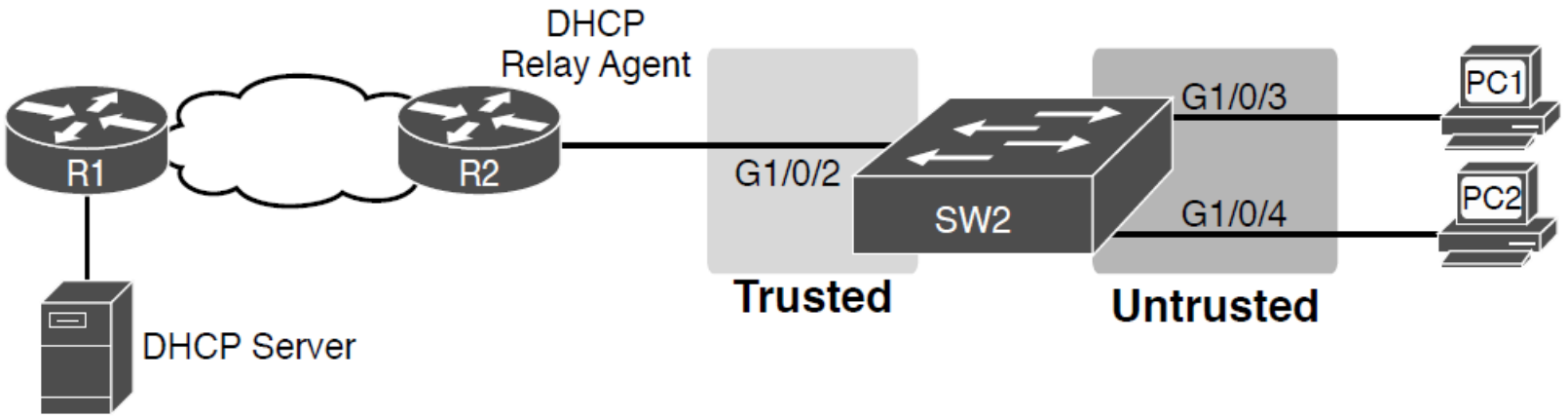
DAI Filtering ARP Based on DHCP Snooping Binding Table



DAI Filtering Checks for Source MAC Addresses



Sample Network Used in ARP Inspection Configuration Examples



IP ARP Inspection Configuration to Match Previous Graphic

```
ip arp inspection vlan 11
!
interface GigabitEthernet1/0/2
 ip arp inspection trust
```

IP DHCP Snooping Configuration Added to Support DAI

```
ip arp inspection vlan 11
ip dhcp snooping
ip dhcp snooping vlan 11
no ip dhcp snooping information option
!
interface GigabitEthernet1/0/2
 ip dhcp snooping trust
 ip arp inspection trust
```

SW2 IP ARP Inspection Status

```
SW2# show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
   11     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
   11     Deny             Deny              Off

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
   11             59              0              0              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
   11              7              0             49                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
   11                   0                        0                      0
SW2# show ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec) Type           VLAN  Interface
------------------  --------------  ---------- -------------  ----  --------------------
02:00:11:11:11:11   172.16.2.101    86110      dhcp-snooping    11  GigabitEthernet1/0/3
02:00:22:22:22:22   172.16.2.102    86399      dhcp-snooping    11  GigabitEthernet1/0/4
Total number of bindings: 2
```

Sample Results from an ARP Attack

```
Jul 25 14:28:20.763: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi1/0/4,
vlan 11.([0200.2222.2222/172.16.2.101/0000.0000.0000/172.16.2.1/09:28:20 EST Thu Jul
25 2019])

SW2# show ip arp inspection statistics

 Vlan      Forwarded         Dropped     DHCP Drops       ACL Drops
 ----      ---------         -------     ----------       ---------
   11             59              17             17               0

 Vlan   DHCP Permits     ACL Permits  Probe Permits    Source MAC Failures
 ----   ------------     -----------  -------------    -------------------
   11              7               0             49                      0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
   11                    0                        0                      0
```

Configuring ARP Inspection Message Rate Limits

```
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause arp-inspection
errdisable recovery interval 30
!
interface GigabitEthernet1/0/2
 ip dhcp snooping limit rate 10
 ip arp inspection limit rate 8
!
interface GigabitEthernet1/0/3
 ip dhcp snooping limit rate 2
 ip arp inspection limit rate 8 burst interval 4
```

Confirming ARP Inspection Rate Limits

```
SW2# show ip arp inspection interfaces
 Interface          Trust State     Rate (pps)     Burst Interval
 ---------------    -----------     ----------     --------------
 Gi1/0/1            Untrusted               15                  1
 Gi1/0/2            Trusted                  8                  1
 Gi1/0/3            Untrusted                8                  4
 Gi1/0/4            Untrusted               15                  1
! Lines omitted for brevity
```

Configuring Optional DAI Message Checks

```
SW2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

SW2(config)# ip arp inspection validate ?
  dst-mac  Validate destination MAC address
  ip       Validate IP addresses
  src-mac  Validate source MAC address

SW2(config)# ip arp inspection validate src-mac
SW2(config)# ^Z
SW2#
SW2# show ip arp inspection

Source Mac Validation      : Enabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
```