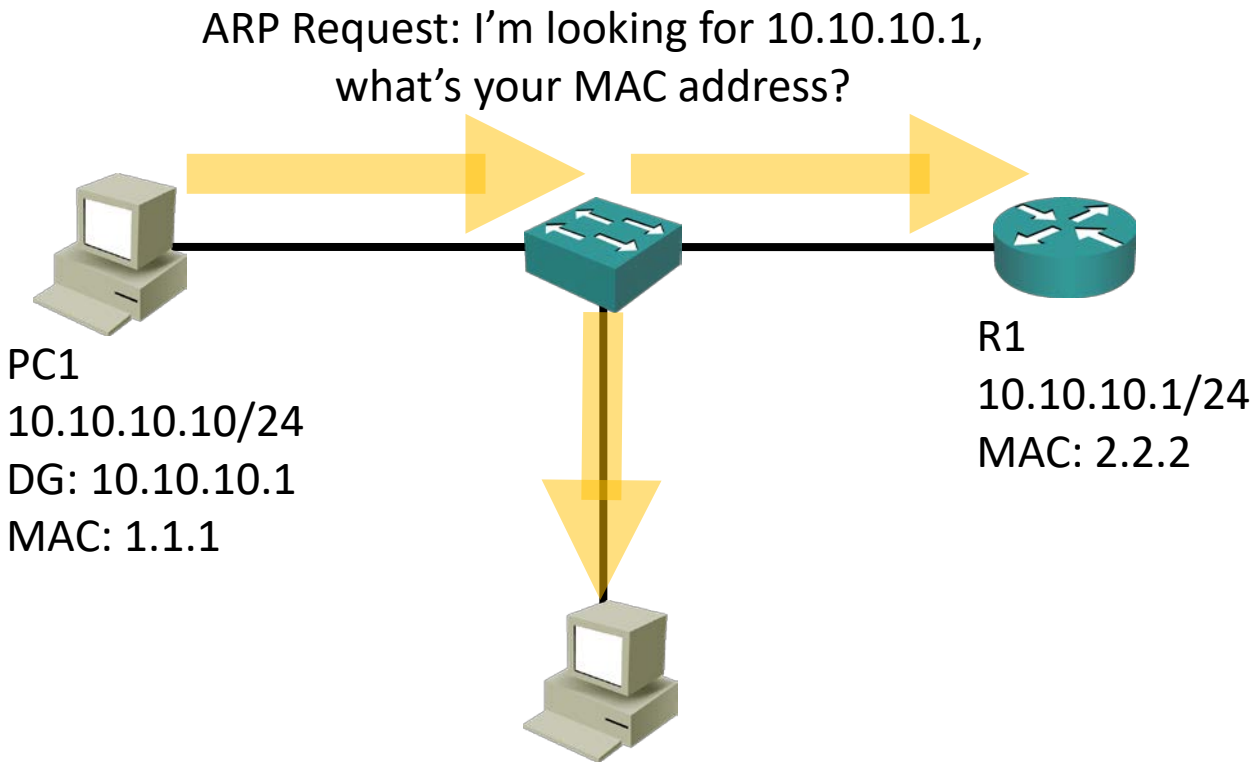
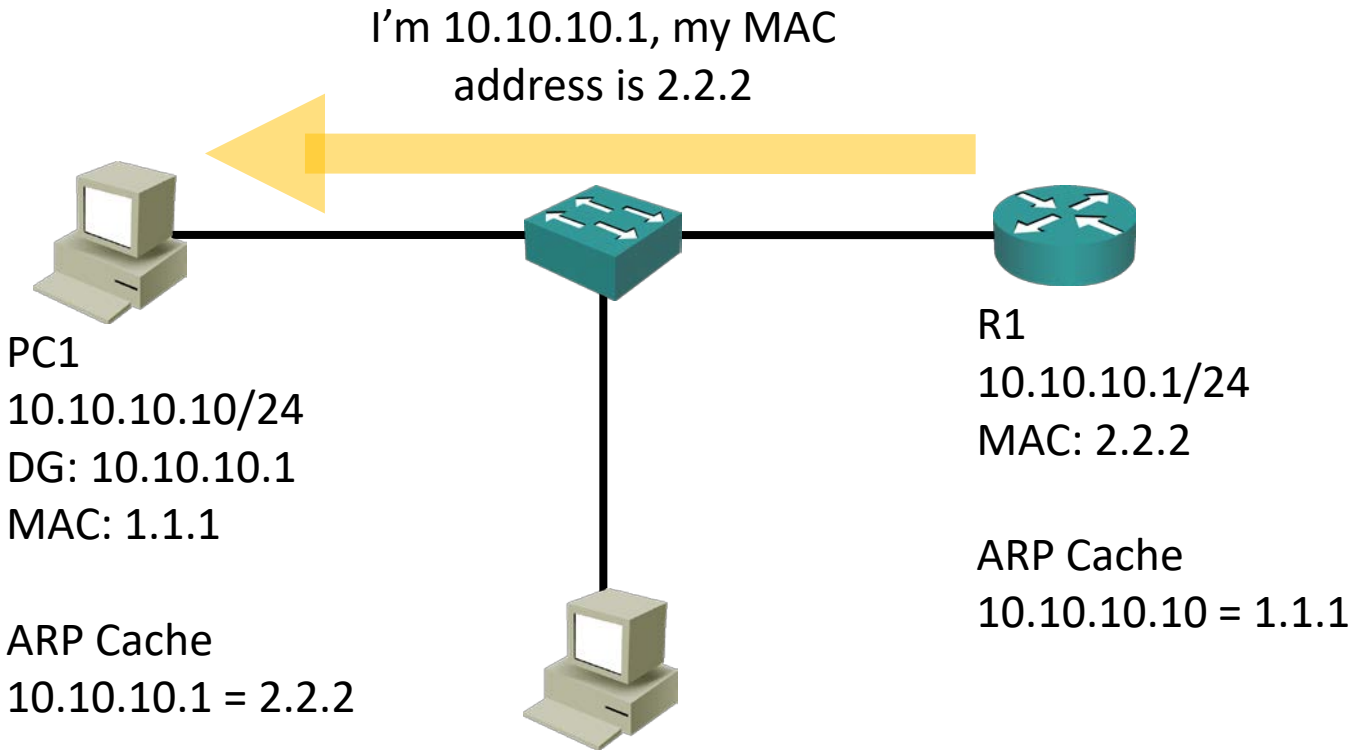
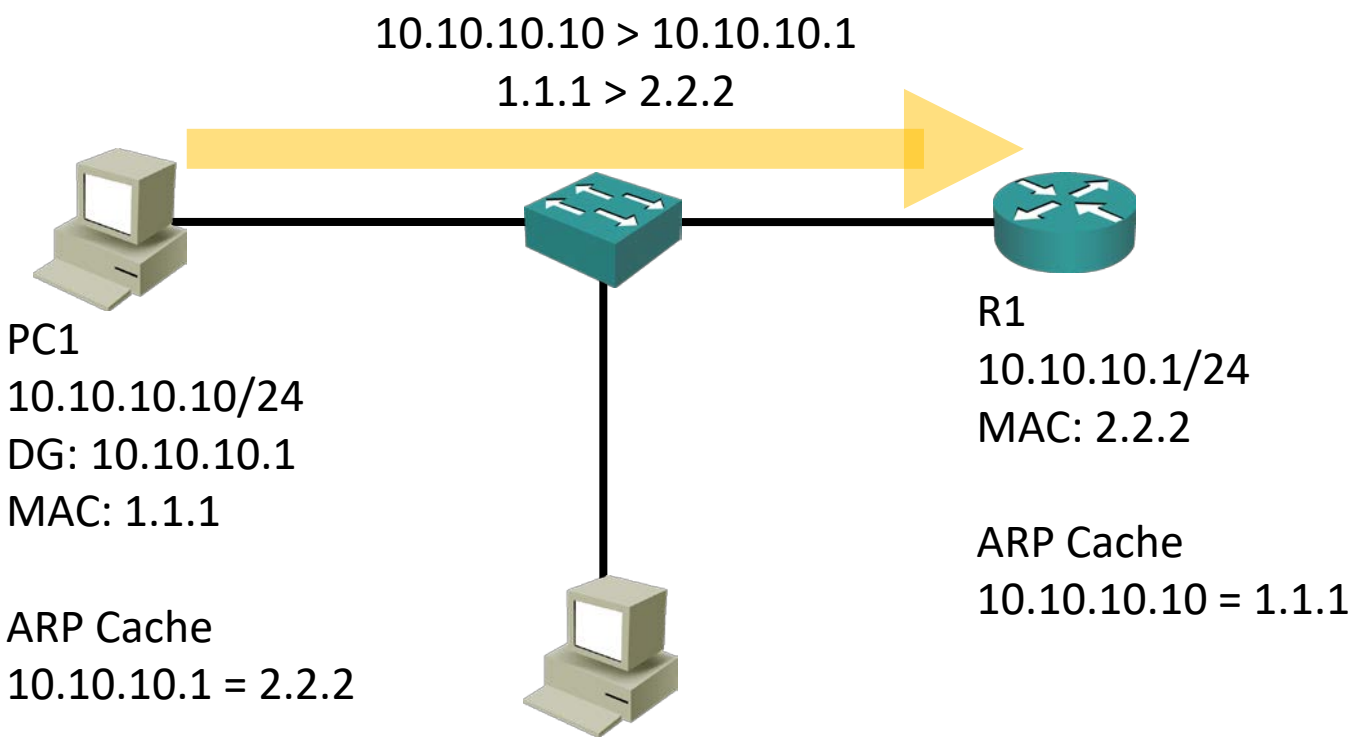
ARP Address Resolution Protocol



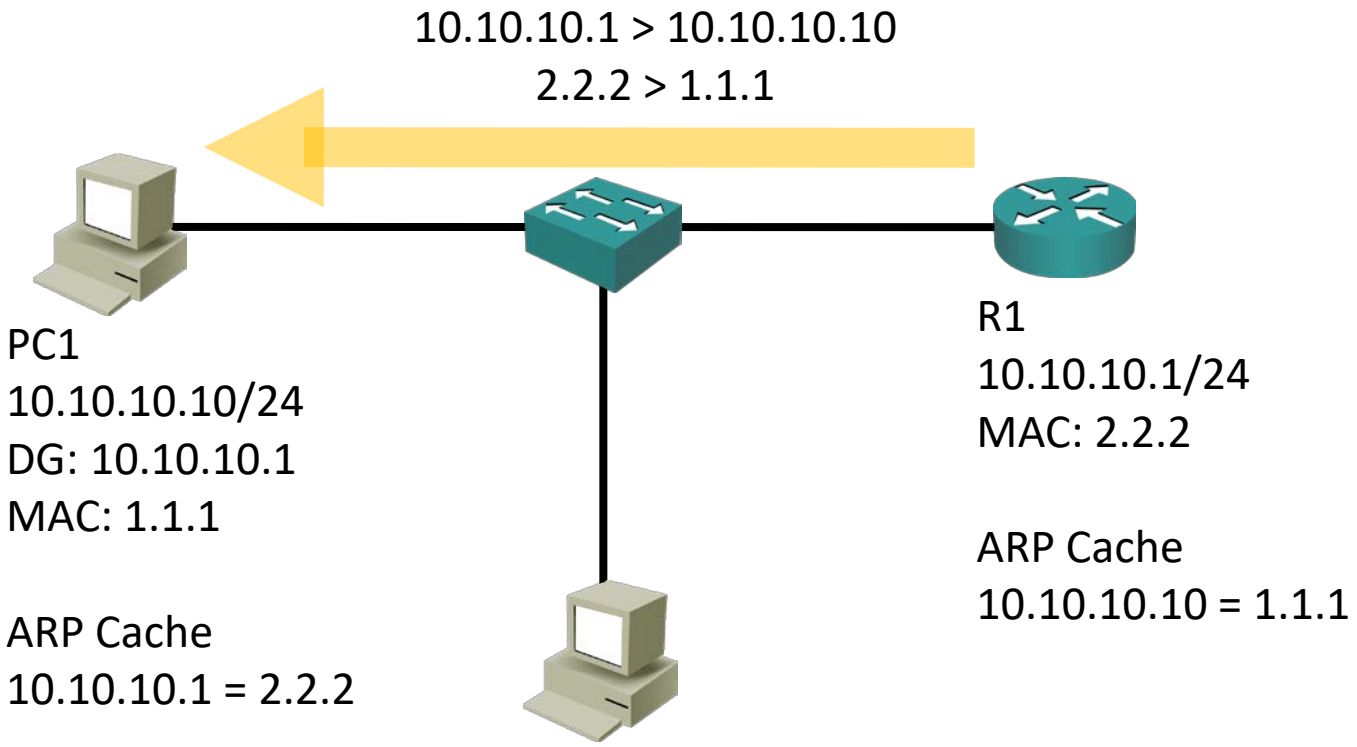
ARP Address Resolution Protocol



ARP Address Resolution Protocol

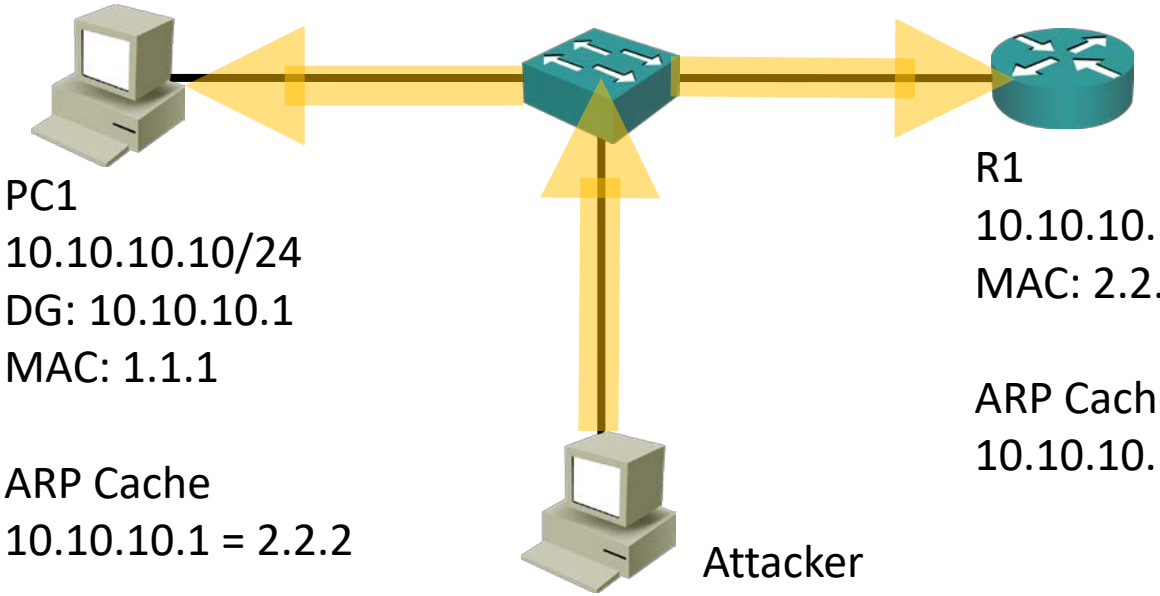


ARP Address Resolution Protocol



Man in the Middle ARP Spoofing

Gratuitous ARP: 'I am 10.10.10.1, my MAC address is 3.3.3'



PC1
10.10.10.10/24
DG: 10.10.10.1
MAC: 1.1.1

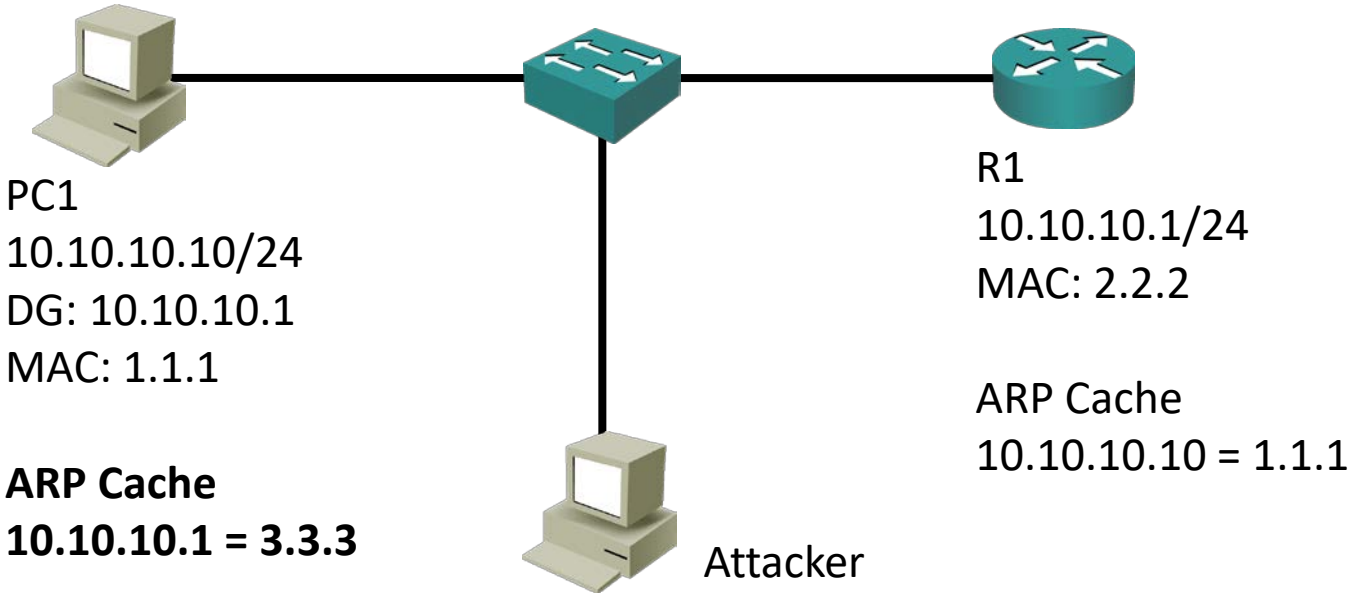
ARP Cache
10.10.10.1 = 2.2.2

R1
10.10.10.1/24
MAC: 2.2.2

ARP Cache
10.10.10.10 = 1.1.1

Attacker
10.10.10.100/24
MAC: 3.3.3

Man in the Middle ARP Spoofing



PC1
10.10.10.10/24
DG: 10.10.10.1
MAC: 1.1.1

ARP Cache
10.10.10.1 = 3.3.3

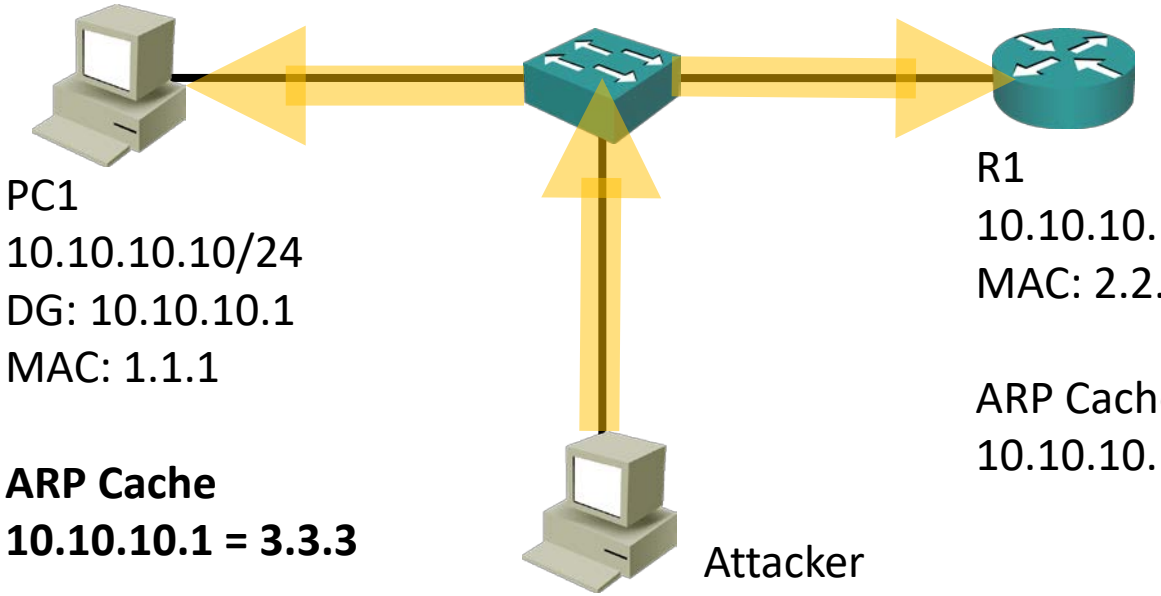
R1
10.10.10.1/24
MAC: 2.2.2

ARP Cache
10.10.10.10 = 1.1.1

Attacker
10.10.10.100/24
MAC: 3.3.3

Man in the Middle ARP Spoofing

Gratuitous ARP: 'I am 10.10.10.10, my MAC address is 3.3.3'



PC1
10.10.10.10/24
DG: 10.10.10.1
MAC: 1.1.1

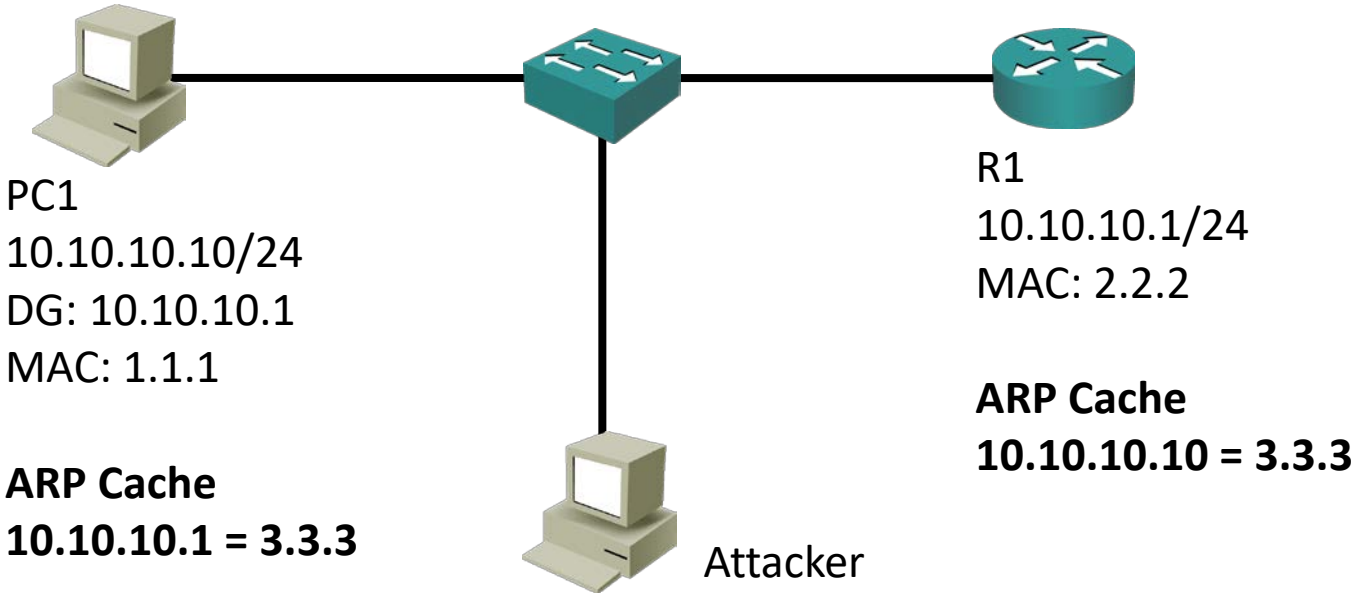
ARP Cache
10.10.10.1 = 3.3.3

R1
10.10.10.1/24
MAC: 2.2.2

ARP Cache
10.10.10.10 = 1.1.1

Attacker
10.10.10.100/24
MAC: 3.3.3

Man in the Middle ARP Spoofing



PC1
10.10.10.10/24
DG: 10.10.10.1
MAC: 1.1.1

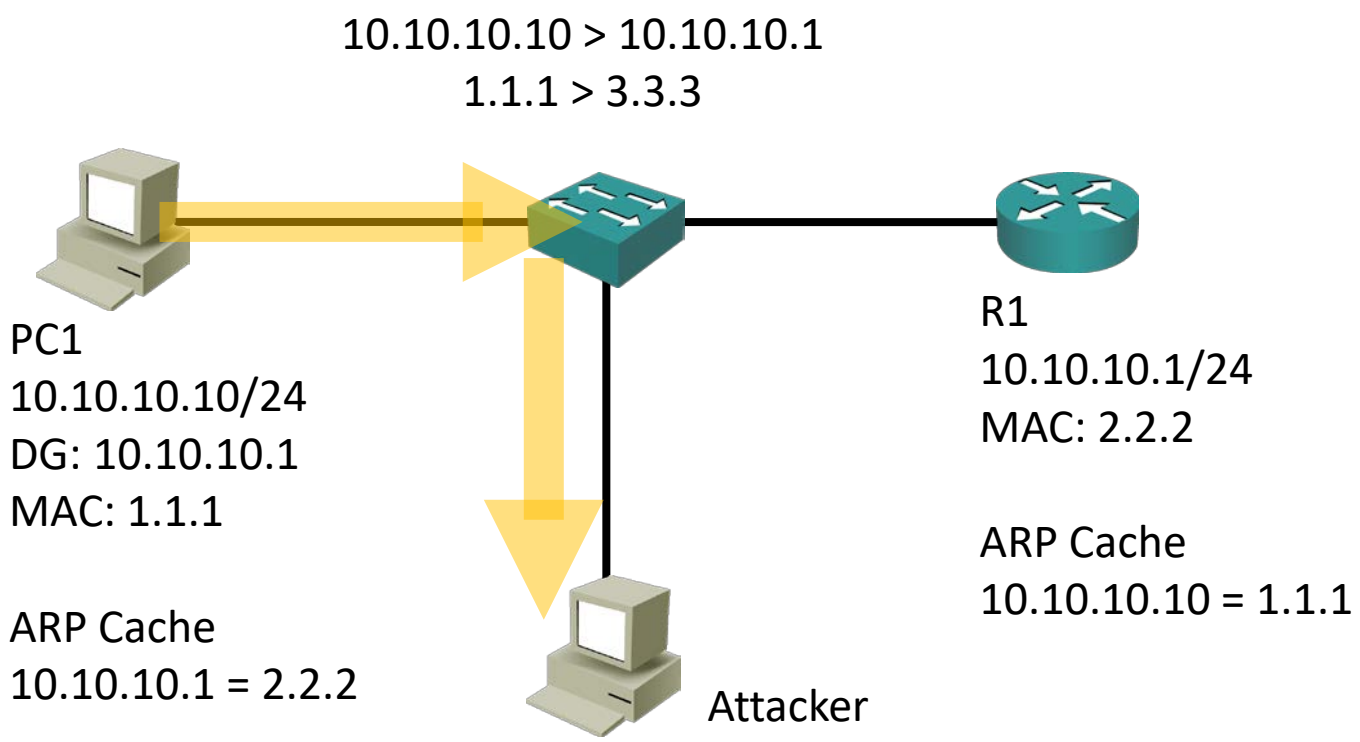
ARP Cache
10.10.10.1 = 3.3.3

R1
10.10.10.1/24
MAC: 2.2.2

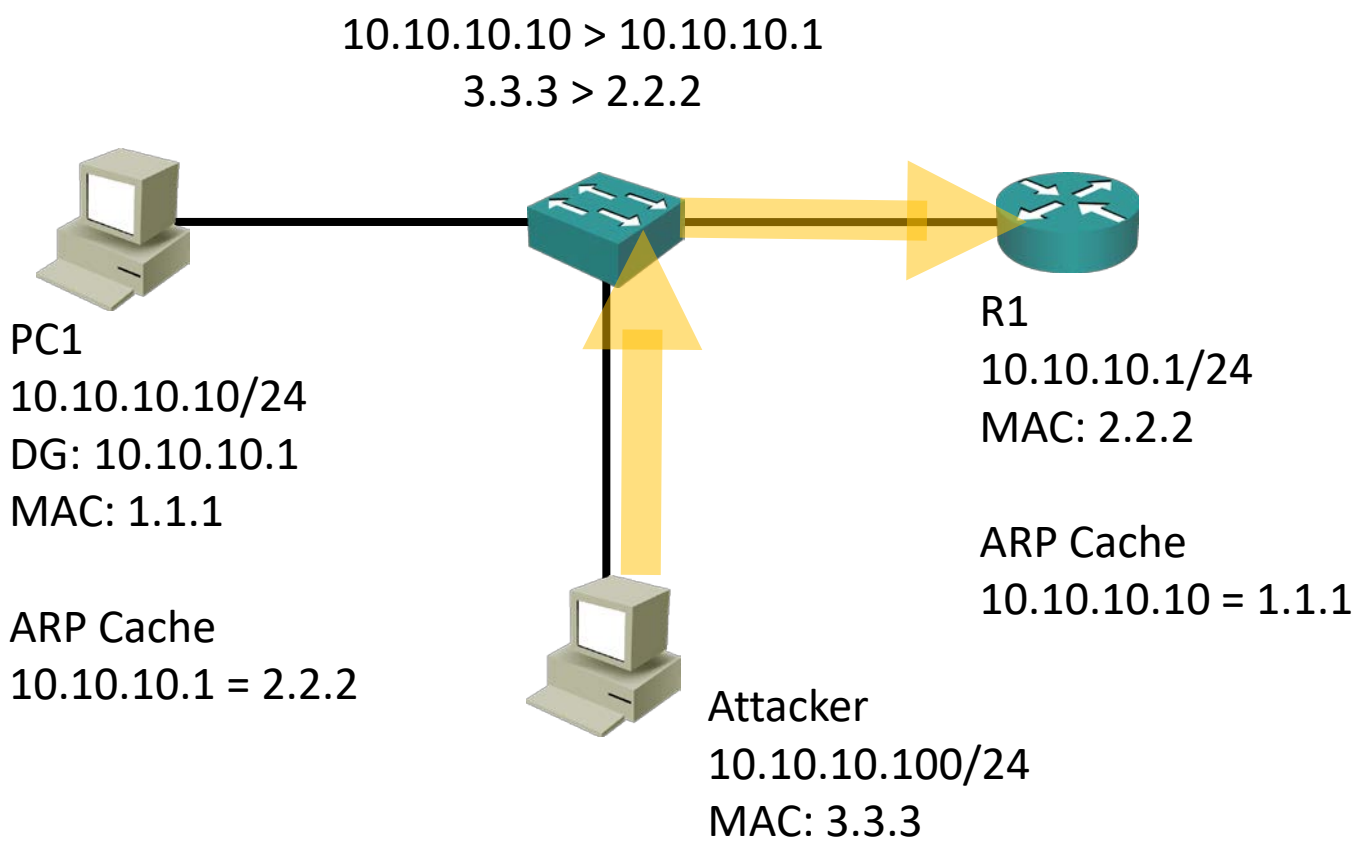
ARP Cache
10.10.10.10 = 3.3.3

Attacker
10.10.10.100/24
MAC: 3.3.3

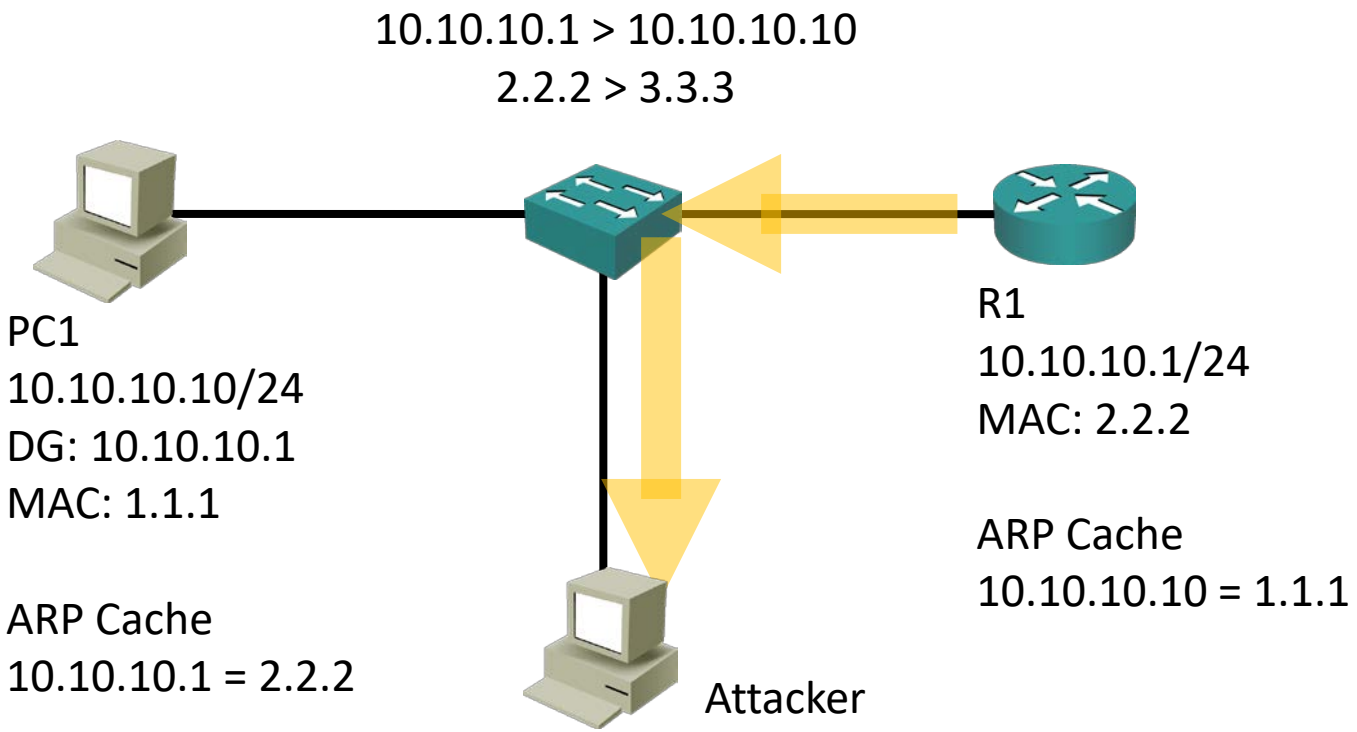
Man in the Middle ARP Spoofing



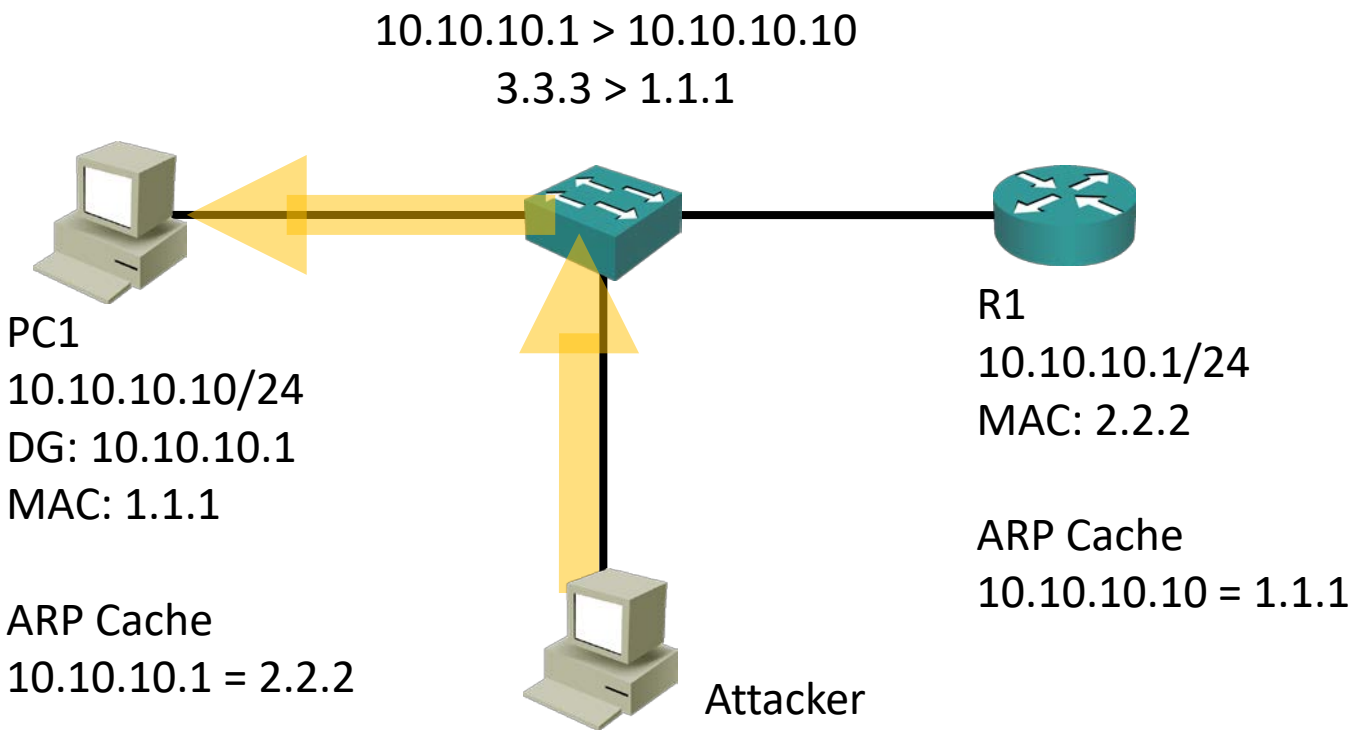
Man in the Middle ARP Spoofing



Man in the Middle ARP Spoofing



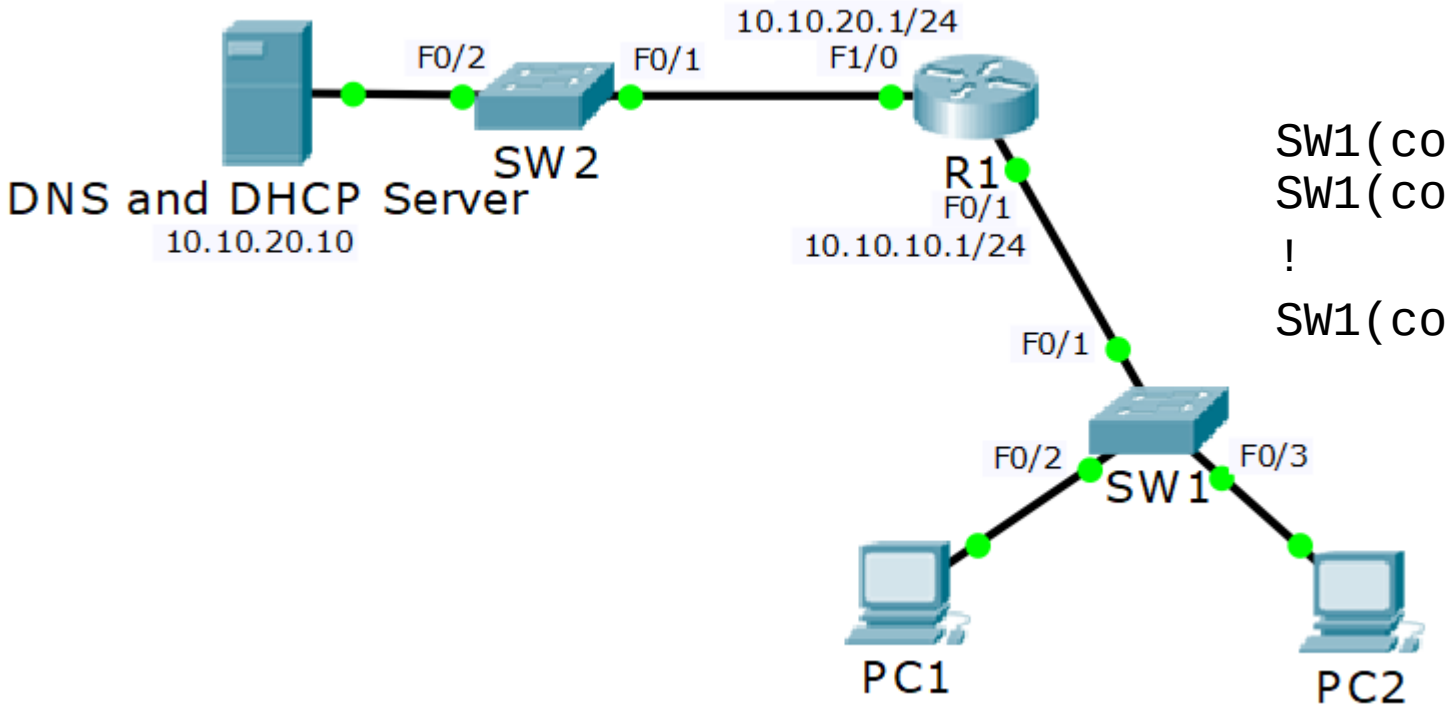
Man in the Middle ARP Spoofing



Dynamic ARP Inspection DAI

- When you enable DHCP snooping, the switch inspects the DHCP traffic and keeps track of which IP addresses were assigned to which MAC addresses
- For example, PC1 with MAC address 1.1.1 was assigned IP address 10.10.10
- If invalid ARP traffic tries to pass through the switch, for example 3.3.3 saying it is 10.10.10, the switch drops the traffic

DAI Configuration




```
SW1(config)#int f0/1
SW1(config-if)#ip arp inspection trust
!
SW1(config)#ip arp inspection vlan 10
```

DAI is not performed on trusted ports.

Enable this for non DHCP clients.

FLACKBOX
www.flackbox.com

Dynamic ARP Inspection DAI

- SBH-SW2(config)#int g1/0/23
  SBH-SW2(config-if)#ip arp inspection trust
- !
- SBH-SW2(config)#ip arp inspection vlan 12