CCNA 200-301
DYNAMIC ARP INSPECTION (DAI)

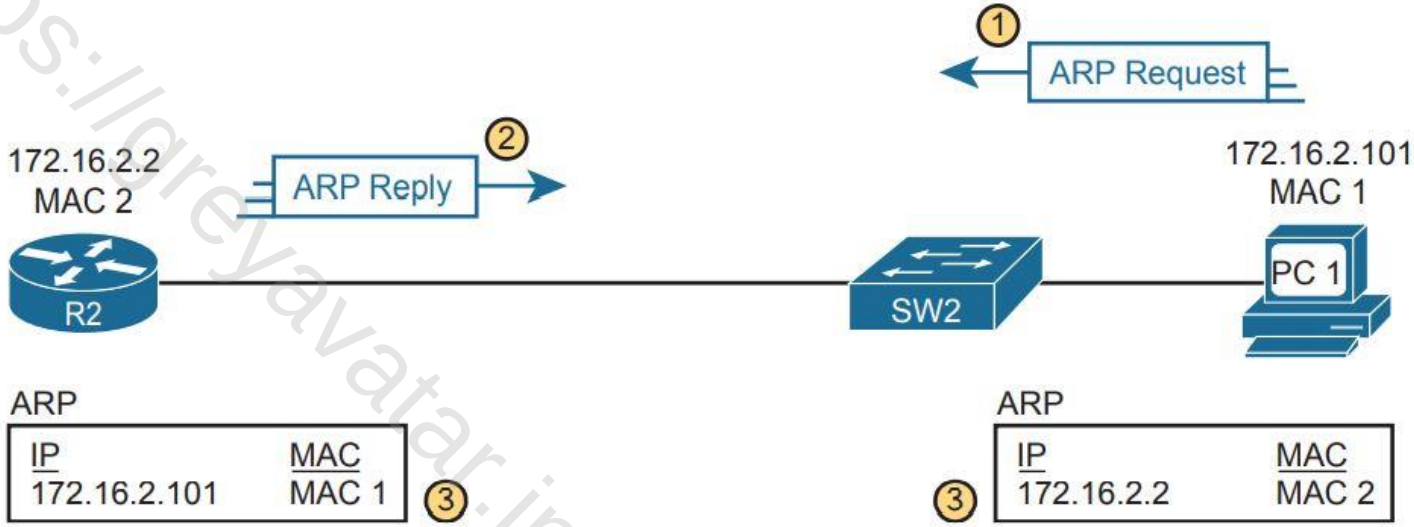
INTRODUZIONE

DAI PRINCIPIO DI FUNZIONAMENTO

- DAI è una funzionalità che permette di esaminare i messaggi ARP in ingresso provenienti dalle porte non sicure e di filtrarli se si ipotizza siano parte di un attacco.
- I messaggi ARP vengono confrontati con due sorgenti:
  - La DHCP Snooping binding table
  - E le liste ACL configurate allo scopo di filtrare i messaggi ARP

FLUSSO MESSAGGI ARP

1. PC1 invia una richiesta ARP per apprendere l'indirizzo fisico MAC sapendo l'indirizzo IP del router
2. Ruter R2 risponde con un messaggio ARP reply
3. PC1 e R2 aggiornano la tabella ARP con I rispettivi IP e MAC dell'interlocutore.

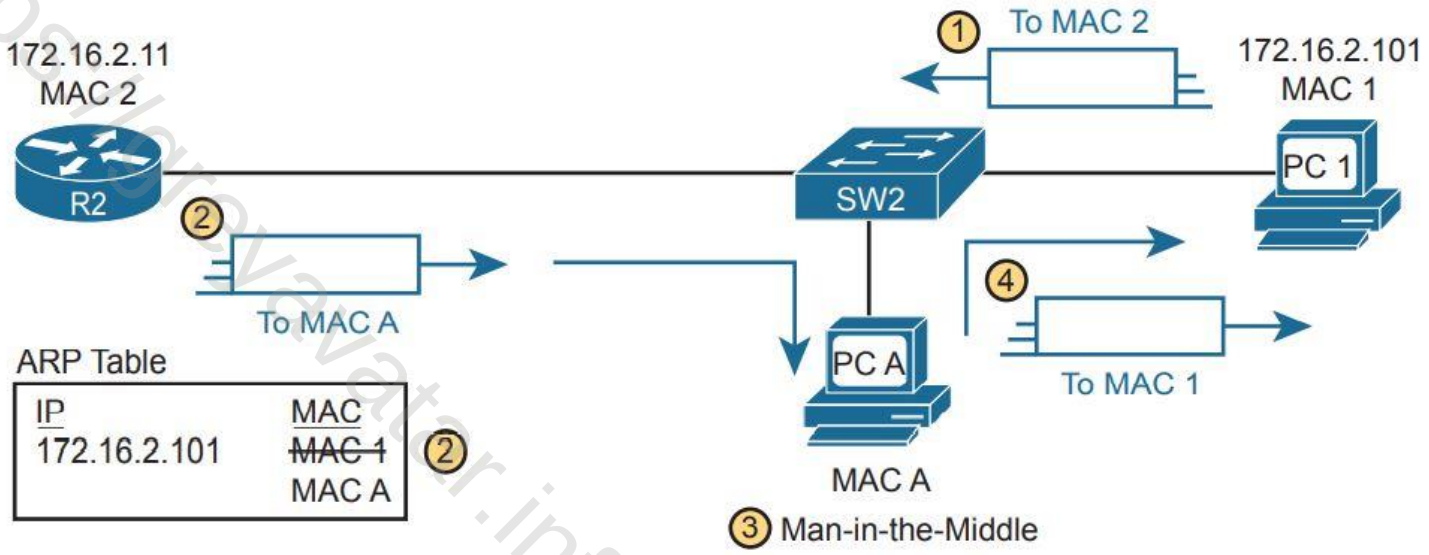


GRATUITOUS ARP AS AN ATTACK VECTOR

- Per ragioni legittime un Host potrebbe comunicare, senza una richiesta, ai dispositivi nella rete il suo MAC, ad esempio se questo è cambiato nel tempo.
- Messaggi GRATUITOUS ARP:
  - È una risposta ARP (ARP Reply)
  - Inviata senza aver ricevuto una richiesta ARP
  - Inviata tramite broadcast MAC in modo che tutti gli Host della rete lo ricevano

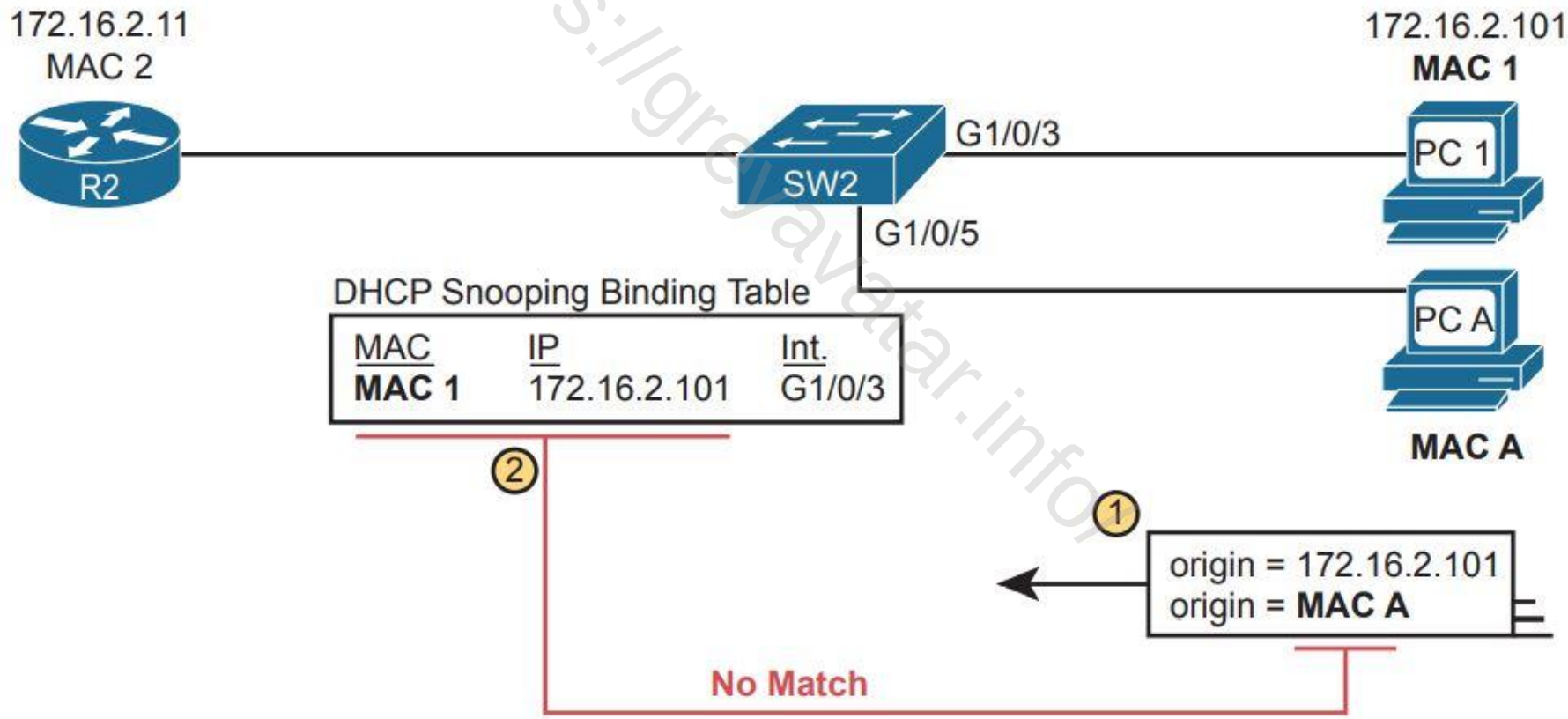
GRATUITOUS ARP AS AN ATTACK VECTOR

- A seguito di un messaggio ARP inviato maliziosamente da PCA il router R2 ha sostituito al MAC1 il MACA associato all'ip 172.16.2.101 del PC1.
- Le risposte ai messagi inviati dal PC1 verranno inviate al PCA, sarà poi il PCA ad inviarle al PC1 realizzando un attacco del tipo MAN IN THE MIDDLE



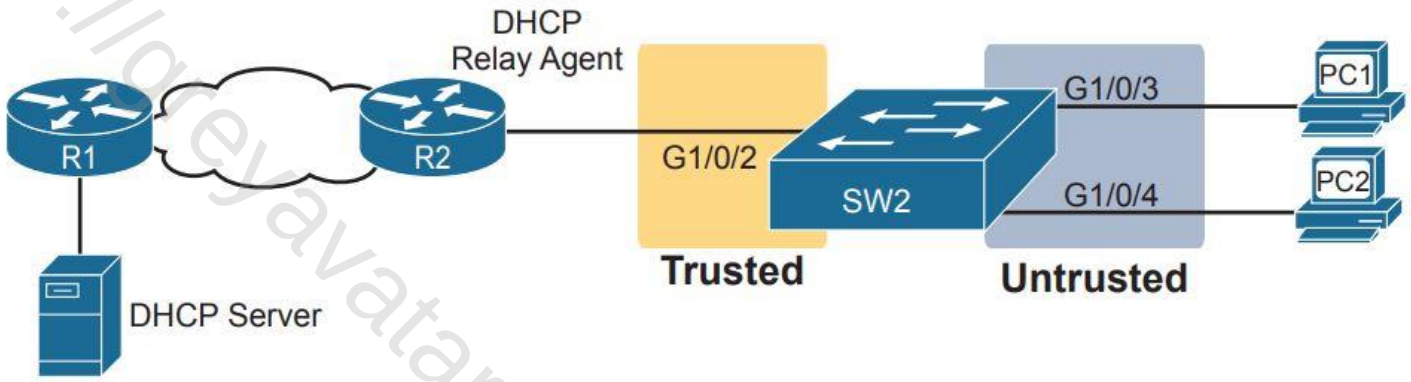
DAI

- Per evitare gli attacchi come precedentemente descritti lo switch confronterà i messaggi con la tabella DHCP Snooping Binding.
- I messaggi che risultano incoerenti con la tabella vengono scartati.



CONFIGURARE ARP INSPECTION SU SWITCH L2

- Decidere se fare affidamento su DHCP Snooping, liste ARP ACL o entrambi.
- Se si usa DHCP Snooping, configurare prima questo servizio e identificare le porte TRUSTED
- Scegliere le VLAN sulle quali abilitare DAI
- Rendere DAI Trusted sulle porte nelle Vlan che tipicamente sono le stesse scelte per il servizio DHCP Snooping



ESEMPIO DI CONFIGURAZIONE


```
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
```