**DHCP SNOOPING**

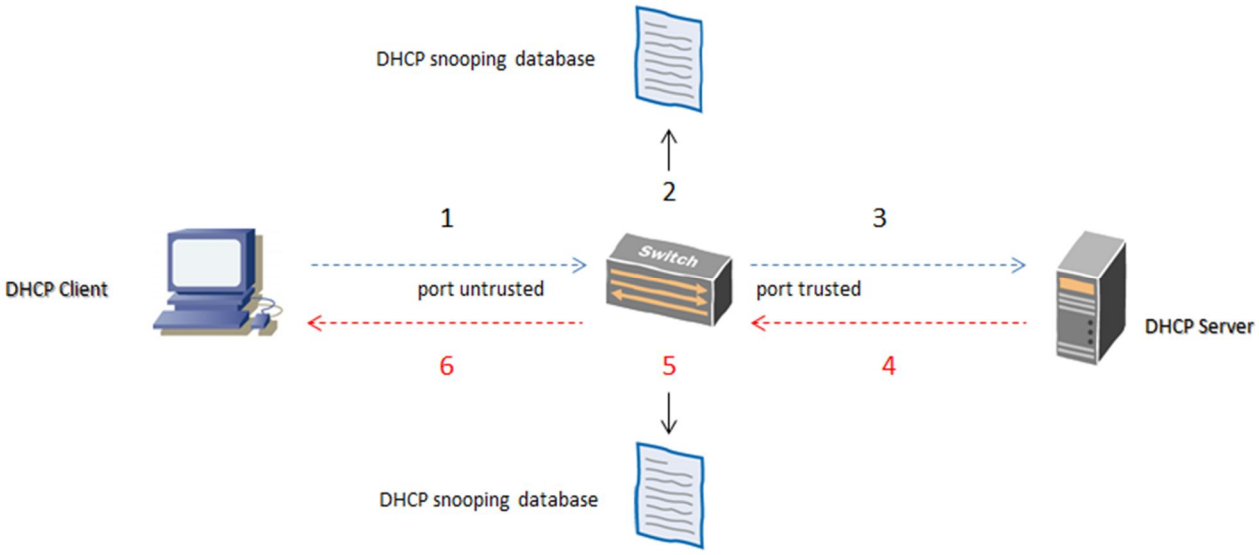
Il DHCP Snooping costruisce e mantiene un database a livello switch, che mappa l'IP address assegnato ad un dhcp client con il suo MAC address più la vlan associata; appena il dhcp client rilascia l'IP address "in affitto" (attraverso un DHCPRELEASE message), l'associazione mapping viene cancellata dal database.

DHCP Snooping protegge quindi gli switch layer 2 da eventuali vulnerabilità quali DoS attack from server dhcp malicius che in modo intenzionale risponde alle richieste DHCP REQUEST dei vari client della rete, attraverso l'ispezione dei pacchetti dhcp su porte di tipo untrusted.

N.B. le porte di tipo untrusted sono quelle configurate in mode access; trusted invece quelle configurate in mode trunk.

Message DHCP client server:


**DHCP SNOOPING PROCESS (OPTION 82)**



1. Il client dhcp invia una richiesta DHCP DISCOVER or DHCP REQUEST verso il server attraverso lo switch.

2. lo switch rileva il pacchetto dhcp request ed aggiorna il database snooping attraverso l'option 82 (dhcp relay agent) con il quale identifica la porta su cui è connesso il client e inserisce questa informazione nell'header del pacchetto di richiesta

3. lo switch trasmette questo pacchetto DHCP REQUEST or DHCP DISCOVER completo di location client "option 82" verso il server dhcp

4. il server dhcp legge l'option 82 aggiunto al pacchetto e lo impiega per rilasciare un IP address o un altro tipo di parametro al client; a questo punto trasmette un pacchetto di tipo DHCP OFFER, DHCP PACK or DHCP NAK verso il client attraverso lo switch con lo stesso option 82 contenuto nell'header.

5. lo switch rileva il pacchetto dhcp offer, pack or nak proveniente dal server e rimuove l'option 82 dall'header del pacchetto aggiornando il database snooping

6. lo switch a questo punto trasmette il pacchetto dhcp offer, pack or nak verso il client

DHCP option 82 si può configurare:

- per singola vlan oppure per tutte le vlan presenti nello switch
- per layer 3 interface (RVI routed vlan interface) quando lo switch ha funzione di relay agent.

Gli switch Juniper EX implementano l'option 82 con quattro sotto-opzioni configurabili:

- *circuit-id:* identifica l'interfaccia o la vlan o entrambe, dal quale la richiesta del client è stata ricevuta (es. circuit-id = ge-0/0/2:vlan20); se la richiesta è ricevuta da una interfaccia layer 3, il circuit-id specifica solo il nome dell'interfaccia.

- *prefix:* in modo opzionale si può aggiungere al circuit-id un nome che può essere ad esempio l'hostname dello switch (es. prefix = EXJ-switch1:ge-0/0/2:vlan10)

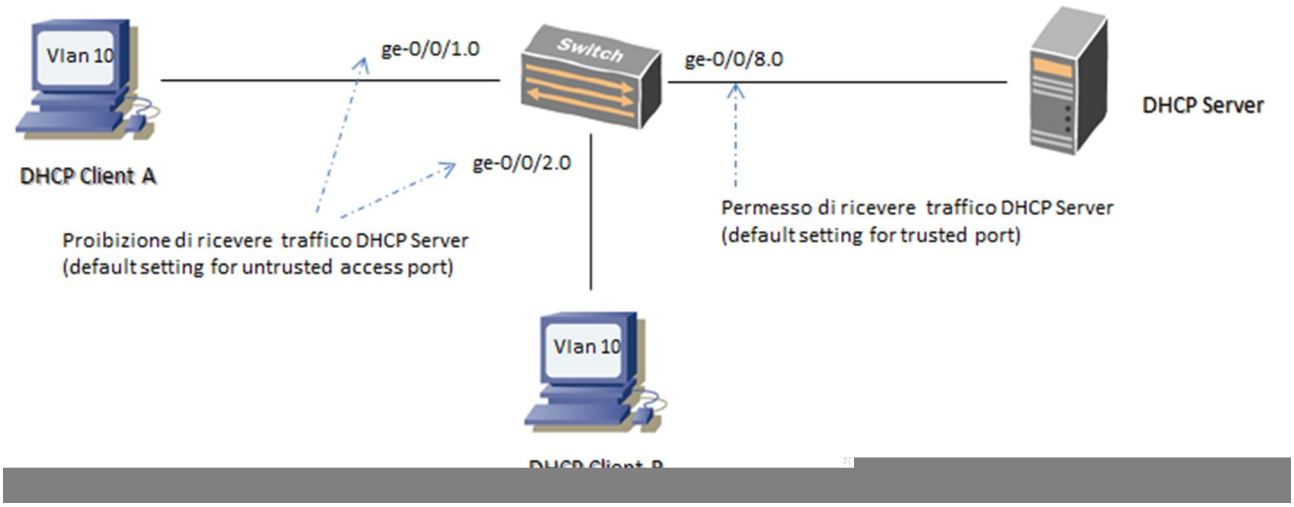
- *remote-id:* di default il remote-id identifica il MAC address dello switch; si può specificare in configurazione comunque qualsiasi cosa come ad esempio l'hostname dello switch, la description della interfaccia o altro.

- *vendor-id:* identifica il costruttore dell'host (di default questa sotto-opzione è Juniper)

**NOTA BENE**

Quando si abilita l'option 82, bisogna assicurarsi che il Server DHCP sia configurato per accettare questa opzione; se non dovesse essere cosi, lo switch non vedendosi tornare indietro il pacchetto completo di option 82 non trasmette il pacchetto di risposta del server al client, risultando un DHCP Failure.

**DHCP SNOOPING CONFIGURATION**




```
edit ethernet-switching-option secure access-port
!
set interface ge-0/0/1.0 no-dhcp-trusted
set interface ge-0/0/2.0 no-dhcp-trusted
!
set interface ge-0/0/8.0 dhcp-trusted
!
Set vlan v10 examine-dhcp      # enables DHCP snooping su base vlan
```

**DHCP Snooping Database:**

E' costruito, una volta abilitato il DHCP snooping, con le seguenti associazioni:

mapping IP address con la coppia VLAN-MAC address