DHCP SNOOPING

Penulis : Muhammad Idham Hilman bin Adenam

Jawatan : Penolong Pegawai Teknologi Maklumat

Bahagian : Unit Rangkaian & Telekomunikasi

Apa itu DHCP

DHCP bermaksud *Dynamic Host Configuration Protocol*.

DHCP digunakan untuk mengawal konfigurasi rangkaian dari *client/host* melalui *server* . fungsi DHCP merupakan fungsi standard di sebahagian besar sistem operasi. DHCP merupakan kaedah yang baik untuk konfigurasi alamat IP secara automatik, berbanding menggunakan konfigurasi secara manual yang memakan masa untuk tetapan alamat IP pada host atau peranti rangkaian.

Terdapat beberapa proses kerja bagi DHCP iaitu :

1. DHCP DISCOVER

Ini adalah mesej DHCP yang menandakan interaksi awal DHCP antara pelanggan dan pelayan . Mesej ini dihantar oleh pelanggan (*host* atau peranti yang disambungkan ke rangkaian) yang bersambung ke subnet tempatan . Ia menghantar mesej yang menggunakan 255.255.255.255 sebagai alamat IP destinasi sementara sumber alamat IP adalah 0.0.0.0.

2. DHCP OFFER

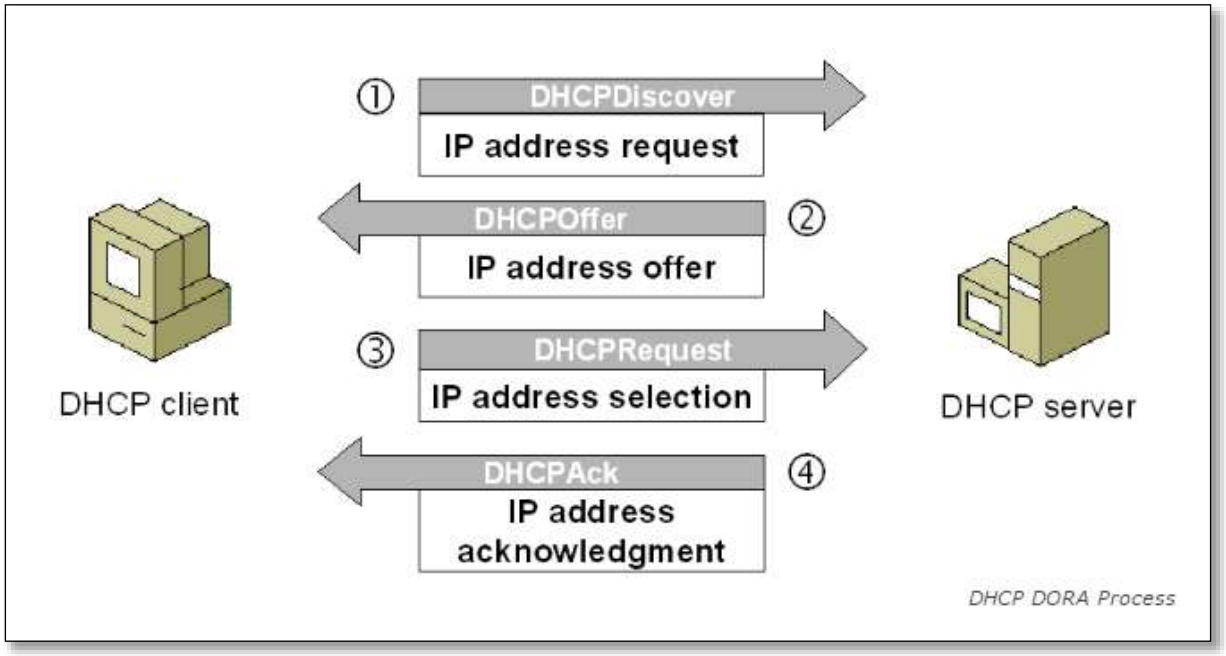
Ini adalah msesj DHCP yang dihantar bagi memberi respon dari DHCPDISCOVER oleh pelayan DHCP untuk pelanggan DHCP . Mesej ini mengandungi tetapan konfigurasi rangkaian untuk pelanggan yang menghantar mesej DHCPDISCOVER.

3. DHCP REQUEST

Mesej ini dihantar bagi memberi respon kepada DHCPOFFER menunjukkan bahawa pelanggan telah menerima konfigurasi rangkaian yang dihantar melalui mesej DHCPOFFER dari pelayan.

4. DHCP ACK

Mesej ini dihantar oleh pelayan DHCP bagi memberi respon DHCPREQUEST diterima daripada pelanggan . Mesej ini menandakan proses akhir yang bermula dengan DHCPDISCOVER . Mesej DHCPACK hanyalah pengesahan oleh pelayan DHCP yang mengesahkan bahawa pelanggan DHCP untuk mula menggunakan konfigurasi rangkaian yang diterima dari pelayan DHCP sebelumnya.

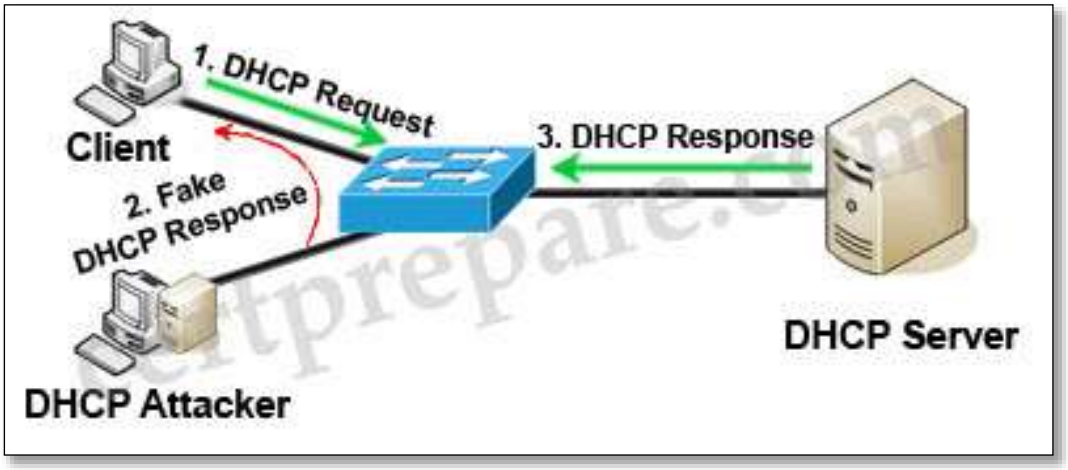


Proses DHCP

Apa itu DHCP SNOOPING

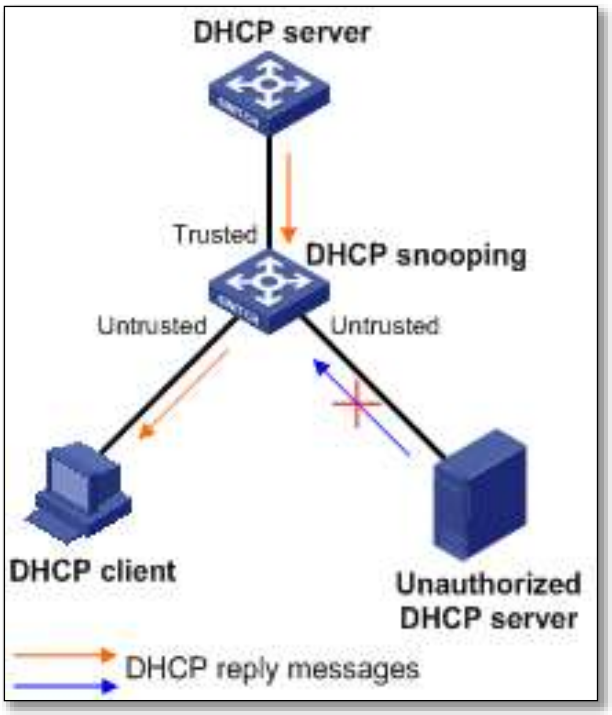
DHCP snooping adalah fungsi yang menentukan peranti tertentu yang dapat bertindak balas terhadap permintaan DHCP . DHCP snooping boleh digunakan untuk mencegah mesej DHCP yang tidak sah, yang mengandungi maklumat seperti data berkaitan alamat IP yang disediakan untuk peranti rangkaian.

DHCP snooping berfungsi apabila port yang disambungkan kepada host atau sambungan ke pelayan DHCP dikonfigurasi. Port tersebut dikenali sebagai dipercayai (Trusted) dan tidak dipercayai (Untrusted) . Port dipercayai dapat memberi semua jenis mesej DHCP manakala port tidak dipercaya hanya dapat membuat permintaan DHCP saja (DHCP DISCOVER) . Konfigurasi ini melindungi rangkaian dari diserang oleh peranti yang bertindak sebagai pelayan DHCP palsu. Port dipercayai boleh terdiri daripada host pelayan DHCP atau boleh menjadi sambungan uplink ke pelayan DHCP . Jika peranti luar pada port yang tidak dipercayai cuba untuk menghantar pakej respon DHCP ke rangkaian, port tersebut akan dimatikan.



Pelbagai pelayan DHCP

Tanpa DHCP snooping , pelanggan dhcp boleh menerima Alamat IP dari pelayan DHCP yang asli atau pelayan DHCP yang palsu. Jika pelayan DHCP palsu memberi respon terlebih dahulu, pelanggan DHCP akan mendapat alamat IP yang tidak sah dan tidak akan dapat mengakses internet / intranet.



Port dipercayai (Trusted) dan tidak dipercayai (Untrusted)

Dengan DHCP snooping , port akan dikenal pasti sebagai dipercayai dan tidak dipercayai . Port dipercayai akan mendapat semua trafik mesej DHCP , termasuk tawaran DHCP dan pengesahan DHCP, dan port tidak dipercayai hanya boleh meminta DHCP saja.

Jika peranti palsu pada port yang tidak dipercayai cuba untuk menghantar pakej ke rangkaian menawarkan DHCP , maka port tersebut akan dimatikan .
DHCP snooping adalah fungsi keselamatan yang bertindak seperti firewall antara host tidak dipercayai dan host yang dipercayai. Ciri-ciri DHCP snooping melakukan tugasan berikut :

• mengesahkan mesej DHCP yang diterima dari sumber yang tidak dipercayai dan menapis mesej yang tidak sah.
• Mengawal trafik DHCP dari sumber yang dipercayai dan tidak dipercayai .
• Membangun dan memelihara pangkalan data DHCP snooping yang mengandungi maklumat tentang host tidak dipercayai dengan alamat IP yang diberi.
• Memanfaatkan pangkalan data DHCP snooping untuk mengesahkan permintaan seterusnya dari host yang tidak dipercayai.

DHCP snooping diaktifkan pada port secara per - VLAN . Secara default , fungsi ini dimatikan pada semua port dan VLAN . Fungsi ini boleh diaktifkan pada VLAN tunggal atau pelbagai VLAN .

Contoh konfigurasi DHCP snooping pada layer 2 switch :

```
Switch# configure terminal [memasuki mode konfigurasi]
Switch(config)# ip dhcp snooping [mengaktifkan fungsi dhcp snooping]
Switch(config)# ip dhcp snooping vlan 18 [mengaktifkan fungsi dhcp snooping pada vlan tertentu]
Switch(config)# interface gigabitEthernet 0/47 [memasuki port yang disambungkan ke pelayan DHCP]
Switch(config-if)# ip dhcp snooping trust [menjadikan port sebagai port dipercayai]
Switch(config-if)#end
Switch# write
```