

DHCP Snooping ve Option 82(information option)

```
Option: (t=12,l=15) Host Name = "b1db-a7f07bd1
Option: (t=60,l=8) vendor class identifier = "
Option: (t=55,l=11) Parameter Request List
Option: (t=43,l=2) Vendor-Specific Information
Option: (t=82,l=18) Agent Information Option
Option: (82) Agent Information option
Length: 18
Value: 0106000400010102020800060025B46D9200
Agent Circuit ID: 000400010102
Agent Remote ID: 00060025B46D9200
End Option
```

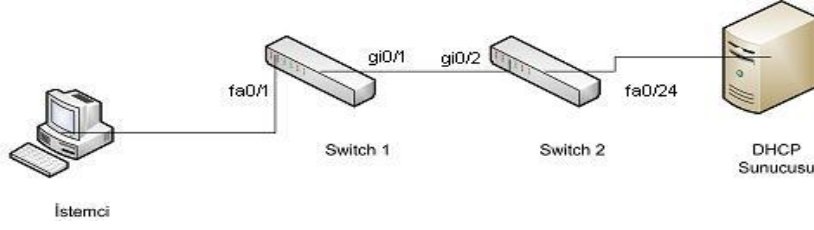
İlk bakışta bir switch'te DHCP Snooping'i devreye almak 2 satır global configuration mode komutu bir de uplink'e ya da DHCP sunucunuzun bulunduğu port'a trust yazmakla bitiyor gibi gözüküyor. Fakat DHCP Snooping devreye alındığında varsayılanda switch tarafından option 82(information option) bilgisinin istemci kaynaklı DHCP paketlerine eklenmesi de devreye alınmış olunuyor. Çok yararlı ve kullanışlı olabilecek bu özellik ilk etapta DHCP snooping'i devreye aldım ama istemciler neden IP alamıyorlar sorusunun cevabıdır çoğu zaman. **Yazının başında, eğer option 82 bilgisini kullanan bir DHCP sunucunuz yoksa, aşağıdaki komutla option 82 bilgisinin eklenmesi özelliğini kapatmanızı şiddetle tavsiye ettiğim belirtmek isterim.** Daha sonrasında ise option 82'nin detaylarını ve bu bilgiyi kullanarak ne gibi faydalar sağlanacağını açıklayacağım. Sonraki bir yazımda ise option 82 destekleyen bir sunucu kurulumunu anlatıp option 82 özelliğini switchlerinizde tekrar aktive etmeniz yönünde sizi ikna etmeye çalışacağım :)

Switch(config)#*no ip dhcp snooping information option*

DHCP Snooping hakkında bilgi sahibi olan herkes untrusted portlardan gelen DHCP OFFER, DHCPACK, DHCPNAK ya da DHCPLEASEQUERY gibi DHCP sunucu paketlerinin drop edildiğini bilir. Buna ek olarak DHCP snooping aktif olan bir switchin DHCP paketlerini drop ettiği diğer durumlar ise;

- Untrusted portlardan gelen source MAC adresi ve DHCP paketinin içerisinde bulunan client hardware address bilgisinin uyuşmaması.
- DHCP Snooping Binding tablosunda bulunan bir MAC adresini içeren DHCPRELEASE ya da DHCPDECLINE broadcast mesajının Binding tablosundakinden farklı bir porttan gelmesi.
- Bir DHCP relay agent tarafından içerdiği Relay-agent IP address bilgisi 0.0.0.0'dan farklı ya da option 82 bilgisi içeren bir DHCP paketinin iletilmesi.

İlk iki durum daha çok atak olarak nitelendireceğimiz durumlar olsa da son durum birden fazla switch içeren topolojilerde karşılanacak bir durumdur. Aşağıdaki gibi istemcilerin bağlı olduğu switchlerde DHCP snooping aktif ise istemcilerin göndereceği her DHCP mesajına switch tarafından option 82 bilgisi eklenecektir. Switch ise trusted portlara bu mesajı iletacaktır. Bu noktada dökümanlarda açıkça belirtilmese de testlerin bize gösterdiği üzere switch'in istemcilerden gelen DHCP paketlerini broadcast tipinde olmalarına rağmen sadece trusted portlara ilettiklerine de değinmek isterim. DHCP sunucumuz diğer bir switch üzerinde olduğundan uplink bağlantımızı sağlayan interface'imizde *ip dhcp snooping trust* komutunu girmiş olmamız gerekiyor.



İstemcinin DHCPDISCOVER paketini alan Switch1 option82 bilgisini DHCP paketine ekleyecek ve Switch1’de gi0/1 trusted port olarak tanımlandığından istemcinin DHCPDISCOVER paketini gi0/1’inden Switch2’ye gönderecek. DHCP Snooping aktif olan Switch2 ise varsayılan ayarlar ile kendisine gelen paket option 82 bilgisi içerdiğinden paketi drop edecek ve DHCP sunucusuna istekler hiçbir zaman ulaşamayacak ve Switch2’de aşağıdaki gibi bir log oluşacak.

```

Feb 1 20:36:52: %DHCP_SNOOPING-5-DHCP_SNOOPING_NONZERO_GIADDR: DHCP_SNOOPING drop message
type: DHCPRELEASE, MAC sa: 000e.7bca.10de
Feb 1 20:37:57: %DHCP_SNOOPING-5-DHCP_SNOOPING_NONZERO_GIADDR: DHCP_SNOOPING drop message
type: DHCPDISCOVER, MAC sa: 000e.7bca.10de
Feb 1 20:43:53: %DHCP_SNOOPING-5-DHCP_SNOOPING_NONZERO_GIADDR: DHCP_SNOOPING drop message
type: DHCPDISCOVER, MAC sa: 000e.7bca.10de
Feb 1 20:44:24: %DHCP_SNOOPING-5-DHCP_SNOOPING_NONZERO_GIADDR: DHCP_SNOOPING drop message
type: DHCPDISCOVER, MAC sa: 000e.7bca.10de
  
```

Çözümlerden bir tanesi Switch2’de gi0/2’sini trusted port olarak atamaktır. Fakat trusted port olarak atanan bir interface’e gelen paketler DHCP Snooping binding tablosuna eklenmez ya da bir incelemeye tabi tutulmaz. Bu da istenmeyen bir durum olabilir.

Diğer bir çözüm untrusted portlardan gelen option 82 bilgilerine izin vermek. Bunu yapmak için global configuration mode’da ***ip dhcp snooping information option allow-untrusted*** komutu girilmelidir. DHCP Snooping’in kullanıldığı networklerde bir çok kenar switch’e bağlantı sağlayan aggregation switch’lerde girilmesi gereken bir komuttur. Ayrıca bu komut Catalyst 2960 switch’lerde interface configuration mode’da da girilebiliyor.

Switch2(config)#***ip dhcp snooping information option allow-untrusted***

Devamında option 82 detayları ve sunucu tarafıyla sizinle olmak dileğiyle hoşçakalın.

Sımmaz KETENCİ