

# DHCP Snooping'i Standart Konfigürasyonunuza ekleyin!



Birkaç yıl öncesine kadar sadece 3 katman switchlerde sunulan birçok güvenlik teknolojileri artık birçok 2. katman cihazda da kullanılabilir durumda. Gelişen teknoloji ve firmalar arasındaki rekabet, mevcut cihazlarımızın sadece işletim sistemlerini güncelleyerek bu güvenlik teknolojilerinin kullanılabilmesine imkan tanıyor. Bu teknolojilerden bazıları DHCP Snooping, Source Guard ve Dynamic ARP Inspection. DHCP Snooping desteği Cisco Catalyst 2950 switch'lerde 12.1(22)EA1 ve sonrası IOS'lar, Catalyst 2960 switch'lerde ise 12.2(35)SE5 ve sonrası IOS'lar ile birlikte gelen bir özellik. Bu yazımda kendi yönettiğimiz network'teki cihazlarda kullanımını standart hale getirdiğimiz DHCP Snooping'in çalışma yapısının testi, doğrudan ve dolaylı yoldan sağladığı çözümler ile bu konudaki ilginç tecrübelerimizi paylaşacağım.

Snooping'in kelime anlamı "her şeye bununu sokmak", "gizlice bilgi toplamak" şeklinde belirtiliyor. DHCP Snooping ise isminden de tahmin edebileceği gibi DHCP paketlerinin incelenip filitrelenmesi ve buna göre DHCP Snooping Binding tablosunun oluşturulması prensibine dayalı çalışıyor. DHCP Snooping bir switch'te devreye alındığı zaman tüm portlarından switch'e giren paketler bu inceleme işlemine tabi kalıyor ve aksi belirtilmedikçe tüm portlar untrusted olarak kabul ediliyor. Portların trusted ve untrusted olması DHCP sunucularının istemcilere cevap niteliğinde gönderecekleri DHCP OFFER ve DHCPACK paketlerinin switch tarafından kabul edilip edilmeyeceği anlamına geliyor. Diğer bir deyişle herhangi bir port trusted olarak belirtilmemiş ise arka planda o port için aşağıdaki access-list "in" yönünde uygulanıyor diyebiliriz.

```
Switch(config)#access-list 101 deny udp any eq 67 any eq 68  
Switch(config)#access-list 101 permit any any
```

Eğer switch'iniz DHCP Snooping desteklemeyip 4. katman ACL'leri fiziksel interface'lere uygulamaya izin veriyorsa yukarıdaki ACL basit anlamda sahte DHCP sunucularını engellemeye yetecektir. Fakat günümüzde DHCP Snooping desteklemeyip 4. katman ACL destekleyen cihazla karşılaşmak çok zor :)Yine de DHCP Snooping'i devreye almadan sadece bir interface'e bağlı Sahte DHCP Sunucusuna erişim kısıtlaması getirmek isterseniz uygulayabileceğiniz bir yöntem. Daha önce karşılaştığımız trajikomik bir sahte DHCP sunucusu vakası ile ilgili Gökhan AKIN'ın yazısına <http://blog.csirt.ulakbim.gov.tr/?p=112> linkinden ulaşabilirsiniz.

DHCP Snooping sadece 4. katman başlığını değil paketlerin içeriğini de incelediğinden kaynak port UDP 67 ve hedef port UDP 68 bilgisini içeren tüm paketleri engellemiyor. Örneğin bir packet generator programı kullanarak kaynak port UDP 67, hedef port UDP 68 paketler yaratıp gönderdiğimizde DHCP Snooping untrusted portlarda bu paketleri engellemiyor.

DHCP Snooping temel işlevinin yanında **ip dhcp snooping limit rate** interface configuration mode komutu ile bir interface'in bir saniyede kabul edeceği DHCP paketlerini sınırlamaya imkan tanır. Varsayılanda untrusted portlarda bu özellik kapalıdır, trusted portlarda ise unlimited şeklinde görülür. Untrusted portlarda 100'den fazla verilmemesi önerilir. Bu özellik DHCP sunucularının DHCP pool'larındaki istemcilere atanacak adreslerin çok kısa bir sürede tüketilmesine karşı bir çözüm olarak geliştirilmiştir. Bu nedenle hedef port UDP 67 olup belirttiğiniz saniyedeki paket sayısının(pps) geçilmesi halinde port err-disabled konumuna getirerek DHCP sunucusunu korunur. Test ortamında laptopımızı bağladığımız switch portunda DHCP paketleri için pps değerini 100 olarak belirledik. Bunu bir packet generator programı ile hedef port UDP 67, farklı kaynak portlar ve farklı pps değerleri kullanarak içeriğinde DHCP mesajları bulunmayan paketler yaratarak test ettik. Saniyedeki paket sayısı sınırladığımız değer olan 100'e ulaştığı anda sağ alt köşede ağ kablosu takılı değil uyarısı bir anda beliriverdi.

Bu noktada **dhcp snooping limit rate** özelliğinin çoğunlukla tüm network'ü ya da belli bir bölgeyi felç edebilecek switching loop'larını engelleyebildiğini de tecrübe ettiğimizi paylaşmak isterim. Bazı bölgelerdeki uç noktalarda yönetilemeyen cihazlara sahipsiz saniyede binlerce paket sonsuz bir döngü içine girdiğinde merkez cihazlarda çalışan Spanning Tree'nin her zaman bir loop olduğunu algılaması mümkün olmayabiliyor. Bu noktada şansınız yaver gider ve bu binlerce paketin bir kısmı DHCP isteklerinden oluşuyorsa, portun neden err-disabled olduğuna baktığımızda beklenmedik bir gülümseme yüzünüzde beliriyor :) Spanning Tree'nin yapamadığını DHCP Snooping yaparak sizi olası büyük bir problemden kurtarıyor.

Aşağıdaki gibi 2950 switch'lerde dhcp snooping limit rate belirlenebilir. 2960 switch'lerde aynı komutlar işletildiğinde pps aralığı 1-2048 arasındadır. Ayrıca interface range komutu ile untrusted access portlara dhcp snooping limit rate tanımlanması faydalı olacaktır.

```
Switch(config)#int range fa0/1 - 23
Switch(config-if-range) #ip dhcp snooping limit rate ?
<1-4294967294> DHCP snooping rate limit
```

Toparlayacak olursak DHCP Snooping'i standart cihaz konfigürasyonunuza ekleyerek hem davetsiz DHCP sunucularını saf dışı bırakabilir, bir şekilde worm bulaşmış PC'lerin DHCP sunucunuzun DHCP pool'unun doldurulmasını engelleyebilir hatta başınıza büyük dert açacak switching loop'larını bile engelleyebilirsiniz. Sonraki yazımda DHCP Snooping'i devreye alırken dikkat edilmesi gereken hatta çoğu zaman neden çalışmıyor sorusunun cevabı olan option 82'nin (information option) detaylarını paylaşana kadar hoşça kalın...

Sınmaz KETENCİ