DHCP

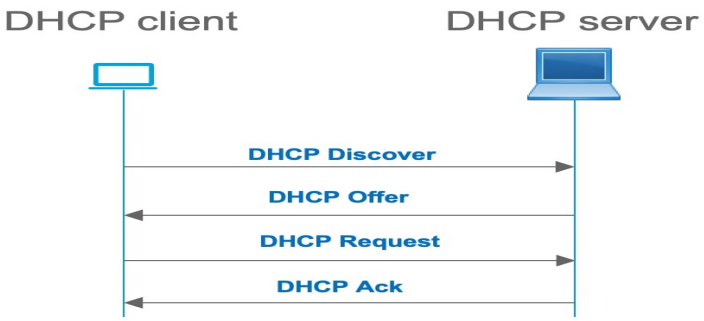
DHCP (Dynamic Host Configuration Protocol), networke bağlanan istemcilere ihtiyaç duyduğu ip bilgilerinin otamatik olarak verilmesini/kiralanmasını sağlayan protokoldür.

DHCP sunucusunda hizmet verilecek network için belirli bir ip aralığına/havuzu oluşturulur. Networke yeni bir istemci bağlandığında, istemciye DHCP sunucusunun ip havuzundan bir ip adresi ve network için tanımlanmış diğer bilgiler (Gateway, DNS...) kiralanır. Kira süresi bittiğinde ip adresi kullanılmaya devam edilmiyorsa farklı bir istemciye verilmek üzere tekrar ip havuzuna gönderilir.

DHCP konfigürasyonu, sunucularda, routerlarda, L3 switch veya yeni nesil L2 switchlerin üzerinde konfigüre edilebiliyor. SOHO (Small Office Home Ofice) gibi küçük networkler için kullanılabilir olsa da büyük ölçekli networklerde bu kullanım şekli tavsiye edilmiyor. Büyük ölçekli networkler için ayrıca bir sunucu üzerinde DHCP servisi ayağa kaldırılıyor.

DHCP Protokolü Çalışma Mekanizması (DORA)

- İlk olarak networke bağlanan istemci, networkte ip bilgilerini alabileceği bir DHCP sunucusu olup olmadığını öğrenebilmek için networke DHCP DISCOVER paketi gönderir.
  |→ Networkte konfigüre edilmiş bir DHCP sunucusu varsa bile bu sunucunun ip adresi (DHCP sunucusu farklı bir network üzerinden hizmet veriyor olabilir) veya MAC adresi bilinmediği için bu paket broadcast yayınla gönderiyor.
- Networkte konfigüre edilmiş bir DHCP sunucusu varsa networke bırakılan DHCP DISCOVER paketini alır ve ardından istemciye DHCP OFFER paketi gönderir. DHCP OFFER paketiyle istemciye bağlanmak istediği network için kullanabileceği ip bilgileri sunulur.
  |→ DHCP DISCOVER paketinde istemcinin MAC adresi bulunduğu için DHCP OFFER paketi istemciye Unicast yayınla gönderilebiliyor.
- İstemci DHCP OFFER paketiyle kendisine sunulan ip bilgilerini kabul ettiğini göstermek için (kendisine sunulan ip bilgilerini kullanmaya başlamadan önce) sunucuya DHCP REQUEST paketi gönderir.
  |→ DHCP REQUEST paketi, istemci henüz ip adresini kullanmaya başlmadığı için yine broadcast yayın kullanılarak sunucuya iletilir.
  |→ DHCP REQUEST paketi gönderilirken boradcast yayın yapılmasının bir diğer sebebi ise networkte konfigüre edilmiş birden fazla DHCP sunucusu olabilir. Bu durumda ilk adımda istemcinin gönderdiği DHCP DISCOVER paketi aynı anda iki sunucuya ulaşacaktır. Özetle istemciye birden fazla ip bilgisi sunulacaktır (DHCP DISCOVER paketlerini alan sunucular istemciye ip bilgileri sunmak isteyecektir). İstemici kendisine sunulan birden fazla ip bilgisinden birini kabul ederken (Bu genelde ilk DHCP OFFER paketi gönderen sunucunun sunduğu ip bilgileri olur) diğer sunucuların gönderdiği ip bilgilerini kabul etmediğini gösterir. Bu sayede diğer DHCP sunucuları sunduğu ip adres bilgilerini farklı bir istemciye sunmak üzere tekrar ip havuzuna bırakır.
- Son adımda ise DHCP sunucusu istemciye sunduğu ip bilgilerini kabul ettiğini onaylamak için DHCP ACK paketi gönderir. Bu adımdan sonra istemci kendisine kiralanan ip bilgilerini kira süresince kullanmaya başlar.



Sunucu istemciye kiraladığı ip adresininin kira süresi yarılandığı zaman istemci kendisine kiralanan ip bilgilerini kullanmaya devam edeceğini sunucuya DHCP REQUEST paketi göndererek bildirir. İstemcinin ip bilgilerini kullanmasında bi sorun yoksa DHCP sunucusu istemciye DHCP ACK paketi göndererek kira süresini uzatır.

|→ Eğer ki istemciye farklı ip adresi verilmek isteniyorsa bu durumda sunucu DHCP ACK paketi göndermez. İstemcinin kullandığı ip adresinin kira süresi dolduktan sonra DHCP sunucusuna tekrar ip isteği gönderir ve yeni ip adresini alır.

DHCP Konfigürasyonu

- Bir router üzerinde bir DHCP sunucusu konfigüre edebilmek için öncelikle global konfigürsayon modunda "**ip dhcp pool <Pool Name>**" komutuyla bir havuz oluşturulup isimlendirilmesi gerekiyor.
- Havuz oluşturulduktan sonra "**network <İp Address> <Subnet Mask>**" komutuyla hizmet verilecek network tanımlanıyor. Konfigürasyon bu komut sonrasında tanımlı ip aralığının başından başlayarak (kendi ip adresi dışında) sırasıyla ip adresi vermeye başlar.
  |→ Kurumlarda statik ip alması gereken cihazlar için global konfigürasyon modunda " **ip dhcp excluded-address <First Ip Address> < End Ip Address >**" komutuyla bir ip aralığı belirtilerek belirli aralığın havuz dışında tutabilmesi sağlanıyor.
  |→ Burada dikkat edilmesi gereken nokta routerda network adresi tanımlandıktan sonra router DHCP hizmeti vermeye başlayacaktır. **Bu süre içerisinde ip adresi alan istemcilere henüz gateway ve DNS gibi bilgiler tanımlı olmadığı için bu adresler verilemeyecektir.** İstemci ip adresi olduğu için de tekrar DHCP sunucusuna istekte bulunmayacaktır. Bunun için konfigürasyonda ilk olarak DNS ve gateway adresleri tanımlanabilir. Bu durumda en son network tanımı yapılacağı için istemciye bütün ip bilgileri gönderilecektir.
  - İkinci bir çözüm olarak DHCP konfigürasyonu tamamlandıktan sonra sadece ip bilgisi alan istemcilerin CMD ekranında "**ipconfig /release**" ve "**ipconfig /renew**" komutları çalıştırılarak yeniden ip bilgisi alması sağlanabilir.
- "**default-router <Ip Address>**" komutuyla istemcilere verilecek default gateway adresi tanımlanyor.
- "**dns-server <DNS Addresses>**" komutuyla DNS bilgisi tanımlanıyor. Her ne kadar PacketTracert desteklemese de burada aralarına virgül koyularak birden fazla DNS bilgisi tanımlanabiliyor.

```
R1(config)#ip dhcp pool ITNetwork
R1(dhcp-config)#dns-server 8.8.8.8
R1(dhcp-config)#default-router 192.168.1.1
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.50
```

- "**lease <Day> <Hour> <Minute>**" komutuyla ip adreslerinin istemcilere ne kadar süreyle kiralanacağı belirtilebiliyor.
- "**option <Option Code>**" komutuyla istemcilere öğretilmek üzere farklı ip bilgileri tanımlanabiliyor. Bu özellik sayesinde istemcilerden belirli bir option code geldiğinde sunucuda tanımlı Option Code karşılık gelen ip adresi istemciye gönderilebiliyor. Yani istemcilere farklı ip bilgileri öğretebilmesini sağlayan özelliktir.
  |→ Örnek olarak Cisco için option 150/ IEEE için option 66 -> Ip telefon yapılandırmalarını bir TFTP sunucusundan indirebilmeleri için TFTP sunucusunun ip adresini öğrettiği adrestir.

```
R1(dhcp-config)#option ?
  <0-254>  DHCP option code
R1(dhcp-config)#
```

DHCP Relay Agent

Kurumlarda her network için ayrı ayrı DHCP sunucusu oluşturmak yerine merkezi bir DHCP sunucusu oluşturarak bütün networklerin bu sunucudan hizmet alması istenir. DHCP protokolünde ise istemci ve sunucu arasında gerçekleştirilen iletişim sürecinde broadcast paketleri kullanılıyor. Routerlar ise broadcast paketlerini geçirmedikleri için farklı networkler tek bir merkezi DHCP sunucusundan hizmet alamıyor. Bu durumda devreye DHCP Relay Agent özelliği giriyor. DHCP Relay Agent, networke bir DHCP paketi bırakıldığında bunu DHCP sunucusunun olduğu networke Unicast olarak gönderilmesini sağlayan özelliktir (Özetle Ip adresi almak isteyen istemci ile DHCP sunucusu arasındaki iletişim sürecinde aracı rolü oynuyor).

DHCP Relay Agent konfigürasyonu için routerda DHCP sunucusundan hizmet alması isteyen araüze giriş yapılarak "**ip helper-address <Ip Address of DHCP Server>**" komutuyla DHCP sunucusunun ip adresi tanımlanıyor. Bu tanımlama sonrasında routertun bu arayüzüne bağlı networkte bir DHCP paketi bırakıldığında router bu paketi DHCP sunucusunun olduğu ip adresine yönlendiriyor.

```
R1(config)#interface gigabitEthernet 0/0/0
R1(config-if)#ip helper-address 192.168.10.100
R1(config-if)#exit
```

DHCP Relay Agent özelliği sadece DHCP sunucusu için değil broadcast kullanan NTP, TACACS, TFTP, DNS gibi çeşitli protokollerin paketlerini yönlendirmek için de kullanılabiliyor.

DHCP Protokolüne Yönelik Saldırılar

- Rouge DHCP Attack, saldırganın networkte sahte bir DHCP sunucusu oluşturup istemcilere ip bilgileri dağıtmasıyla gerçekleştirilen bir saldırıdır. Saldırgan bu sayede istemcilere istediği gateway ve DNS bilgilerini verebiliyor. Burada gateway adresi kendi ip adresi verip istemcilerin internete çıkarken kendi bilgisayarı üzerinden geçmesini sağlayabilir. İnternet trafiğinin büyük bir kısmı şifreli olacağı için bir noktaya kadar sorun olmasa da sahte bir DNS sunucu adresi verip istemcileri istediği web sayfalarına çekebilir. Bu sayede istemcilere zararlı yazılımlar indirtebilir veya sahte web sayfaları hazırlayarak parolalarını ele geçirebilir.

- DHCP Starvation Attack, DHCP sunucularının ip havuzundaki ip adreslerinin tüketilmesine yönelik yapılan bir saldırıdır. Saldırgan networke hizmet veren DHCP sunucusuna farklı MAC adresleriyle DHCP DISCOVER paketleri göndererek yeni ip bilgisi talep eder. Bu durum DHCP sunucusunda istemcilere dağıtacak ip adresi kalmayıncaya kadar devam eder. DHCP sunucusunda dağıtacak ip adresi kalmadığında networke yeni bağlanan istemciler sunucudan ip bilgilerini alamayacaklardır. Dolayısıyla networke dahil olamazlar.

SORU : Birçok networke hizmet veren bir DHCP server kendisine DHCP Relay Agent özelliği kullanılarak bir paket gönderildiğinde hangi ip havuzundan ip adresi vereceğini nasıl anlıyor?

|→ DHCP Relay Agent özelliği ile bir paket gönderildiğinde, paketin kaynak ip adresi DHCP paketinin geldiği arayüzün ip adresi kullanılarak DHCP sunucusuna gönderiyor.Bu sayede paket DHCP sunucusuna ulaştığında hangi ip havuzundan ip adresi verileceği anlaşılıyor. DHCP sunucusundan cevap dönerken de paketin geldiği kaynak ip adresine bakılarak gönderildiği için paket ip isteğinde bulunan network arayüzüne gönderiliyor (VLAN'lar için uygulamasını Lab-2- dizini altında bulabilirsin).

NOT :

- Router veya swtich arayüzlerine de DHCP sunucularından "**ip address dhcp**" komutu kullanılarak ip adresleri aldırılabiliyor.
  |→ Routerlara DHCP sunucularında ip adresi aldırma durumu networklere gatewaylik yapan arayüzlerinde değil de ISP tarafında paket yönlendirme yapan routerlar için kullanılıyor.

```
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#ip address dhcp
R1(config-if)#no sh

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state
to up

R1(config-if)#exit
R1(config)#
```

```
SW1(config)#interface vlan 10
SW1(config-if)#ip address dhcp
SW1(config-if)#exit
SW1(config)#
```

- DHCP sunucusu kullanılarak bir domain-name, next-server, netbios-name-server gibi birçok adres bilgisi istemcilere öğretilebiliyor. Çok daha fazla özellik için https[:]//www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htdhcpsv.html adresine göz atabilirsin.
- İstemcilerin bağlı portlarda PortFast özelliği açılmadığında istemci ip adresi alamayabiliyor. Nedeni istemci porta bağlandığı zaman STP protokolü çalışacağı için 30 saniye bekletiliyordu. Bu süre içerisinde istemci networke paket bırakamadığı için DHCP sunucusuna erişip ip bilgileri alamıyor.
  |→ Çözüm olarak STP protokolü sonrasında istemcinin CLI ekranında "**ipconfig /renew**" komutları kullanılarak yeniden ip alması sağlanabilir.
- Cisco cihazlarda DHCP sunucusu varsayılanda açık geliyor. Bu "**no service dhcp**" komutuyla kapatılabiliyor.
- **İstemci sayısı yüksel olan topolojilerde router ve switch gibi cihazlar üzerinde DHCP servisi kurulması önerilmiyor. Nedeni DHCP sunucusu cihazlardaki ASIC donanımını kullandığı gibi CPU'da kullanıyorlar. CPU kullanmaları cihazları çatlatabiliyor.**

Terminolojiler :

- Netbios, network içerisinde bilgisayar ismi kullanılarak istemcilerin ip adreslerinin öğrenilmesini sağlayan bir hizmettir.
- APIPA, windows istemciler networke bağlandığında ip alacak bir DHCP sunucusu bulamadıklarında kendilerine 169.254 ile başlayan B sınıfı private bir adres atıyor. Bu sayede network içerisindeki Windows istemcilerle aralarına haberleşebilmeleri sağlanıyor.

Kontrol Komutları

- sh run
- sh ip dhcp binding
- sh ip dhcp server status