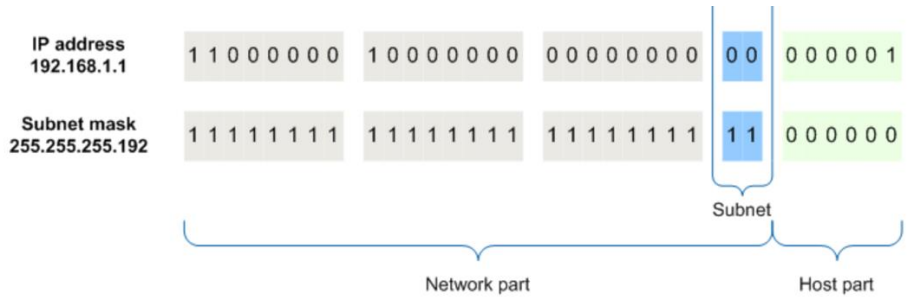
Routing Fundamentals - 1

ENARSI eğitimi, gelişmiş yönlendirme teknolojileri ve hizmetlerine ilişkin uygulama ve sorun giderme üzerine hazırlanan bir eğitim serisidir. Bu seri üzerine çalışmaya başlamadan önce bu yazıyla eğitim süresince ihtiyaç duyulacak temel bilgiler için genel bir tekrar olması amacıyla hazırlanmıştır.

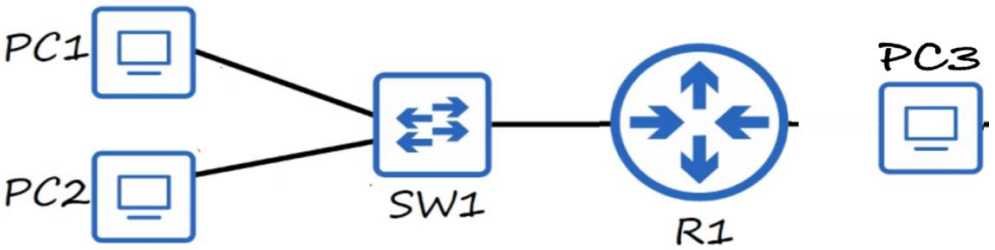
Network üzerinde iki cihazı aralarında haberleştirebilmek için sahip olmaları gereken 3 bilgi bulunuyor. Bunlar **ip adresi**, **Subnet maskesi** ve **Default Gateway** adresidir. Bu adreslerden ip adresi network üzerinde cihazı ayırt edebilmeyi sağlıyor.

Subnet maskesi, ip adresinin ne kadarlık kısmının network adresini temsil ettiğini tanımlayabilmek için kullanılıyor. Yani paketler henüz kaynak istemciden çıkarılmadan önce ilk olarak hedef adresin Subnet bilgileri kontrol edilerek hedef cihazın kaynak istemci ile aynı networkte olup olmadığı kontrol edilir. Hedef cihaz aynı network içerisindeyse ARP sorgusuyla hedef cihazın MAC adresini öğrenir ve paketi buna göre revize eder. Aynı network içerisinde değilse Default Gateway'in MAC adresi öğrenerek paketi buna göre revize eder.



Bu çalışma prensibine istinaden,
Soru: Aşağıdaki görselde bulunan cihazların ip yapılandırması aşağıdaki gibi yapıldığında PC1 ve PC2 farklı Subnet maskelerine sahip olmalarına rağmen aralarında iletişim kurabilir mi?

- 192.168.1.10/28 → PC1
  - IP : **11000000.10101000.00000001.0000**1010
  - SM : 11111111.11111111.11111111.11110000
- 192.168.1.20/26 → PC2
  - IP : **11000000.10101000.00000001.0001**0100
  - SM : 11111111.11111111.11111111.11000000
- 192.168.1.1/26 → R1



- Ek bir konfigürasyon yapılmadığı sürece evet kurabilir. Nasıl mı?

PC1, PC2'ye paket göndermek istediğinde kendi Subnet bilgisi ile hedef ip adresini eşleştirdiğinde (**yani /28 ile kontrol edecektir**) hedef ip adresinin farklı network üzerinde olduğunu değerlendirecek ve paketi Default Gateway'a gönderecektir. Default Gateway ise kendisine gelen paketin hedef ip adresini kontrol ettiğinde hedef networkün kendisine doğrudan bağlı networke ait olduğunu belirleyip (**burada Default Gateway adresi 192.168.1.1/26**) paketi PC2'ye yönlendirecektir (yani PC1, PC2'ye paketleri Default Gateway üzerinden gerçekleştirilecektir).
P2, PC1'e yanıt göndermek istediğinde ise hedef cihazın ip adresini kendi Subnet maskesi ile eşleştirecek ve hedef cihazın aynı network içerisinde olduğunu değerlendirip paketi doğrudan PC1'e gönderebilecektir.

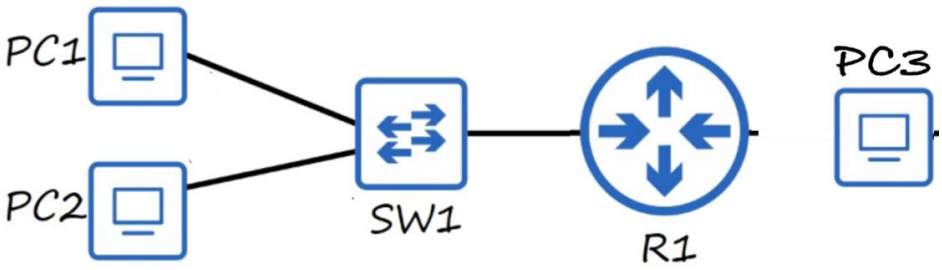
Benzer şekilde cihazlara aşağıdaki ip bilgileri verildiğinde;

- 192.168.1.74/26 → PC1
  - IP : **11000000.10101000.00000001.**01001010
  - SM : 11111111.11111111.11111111.11000000
  - DG : 192.168.1.1/26
- 192.168.1.20/26 → PC2
  - IP : **11000000.10101000.00000001.**00010100
  - SM : 11111111.11111111.11111111.11000000
  - DG : 192.168.1.1/26
- 192.168.1.1/26 → R1
  - IP : **11000000.10101000.00000001.**00000001
  - SM : 11111111.11111111.11111111.11000000

Şeklinde tanımlanması durumunda PC1, kendisine tanımlanan Default Gateway ile aynı netwokte olmadığı için ne Default Gateway ile ne de PC2 ile haberleşemeyecektir.

Soru: Aşağıdaki görselde bulunan cihazların ip yapılandırması yukarıdaki gibi yapıldığında PC1 ve PC3 farklı network adreslerine sahip olmalarına rağmen aralarında iletişim kurabilir mi? Farklı bir örnek olarak;

- 192.168.1.10/16 → PC1
  - IP : **11000000.10101000.**00000001.00001010
  - SM : 11111111.11111111.11111111.11110000
- 192.168.1.1/26 → R1
- 192.168.1.20/24 → PC3
  - IP : **11000000.10101000.**00000001.00010100
  - SM : 11111111.11111111.11111111.00000000



- R1 routeru üzerinde **Proxy ARP özelliği devrede değilse** hayır iletişim kuramazlar. Neden mi?

PC1, PC2 ile haberleşecektir ama PC1, PC3'e paket göndermek istediğinde PC3'ün ip adresiyle kendi Subnet maskesini eşler ve aynı networke dahil olduğunu görüp paketi network içerisinde ip adresine sahip MAC adresini aramaya çalışır. (Oysa ki hedef farklı networktedir ama yanlış Subnet bilgisinden dolayı kaynak istemci hedefi aynı network içerisinde arar). Bu nedenle cihazlara ip bilgileri tanımlanırken Subnet maskelerine dikkat edilmelidir.

DHCPv4

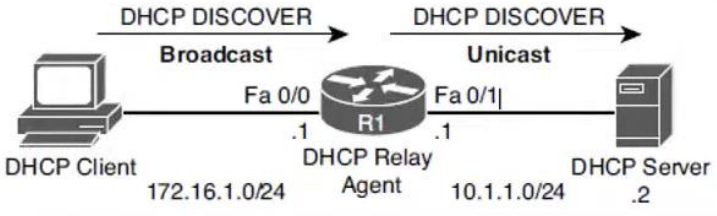
DHCP protokolü, istemcilerin otomatize ip bilgisi almasını sağlamak üzerine geliştirilen bir protokoldür. Uygulama katmanı protokolüdür. UDP 67. ve 68. Portları kullanır. Bu işlemi DORA kısaltmasıyla da tanımlayabileceğimiz dört adımda gerçekleştiriyor. Bu adımlarda gerçekleştirdiği işlemleri kısaca hatırlayacak olursak;

- **DHCP Discover**, network içerisinde DHCP sunucusu olup olmadığını tespit etmek için istemcinin ağa bıraktığı pakettir. Broadcast yayınla bırakılır (Hedef ip adres bilgisi dahil olduğu subnetin broadcast adresi, hedef MAC adresi ise FF:FF:FF olacaktır). Kaynak MAC adresi istekte bulunacak cihazın MAC adresi olurken bu aşamada henüz ip adresi olmadığı için 0.0.0.0 kaynak ip adresiyle yayın yapılır.
    - Bu durum farklı networklerde tanımlı DHCP sunucularından hizmet alındığı durumlarda Relay Agent özelliği kullanılıyor. **Routerlarda oluşturulan ACL tanımlamalarında kaynak ip adresi 0.0.0.0 olan paketler de göz önünde bulundurulmadığı taktirde istemcilerin farklı network üzerindeki DHCP sunucusundan ip bilgisi çekmesi engellenmiş olur.**
    - DHCP istemcisi sorguyu UDP 67 portuyla gerçekleştiriyor.
- **DHCP Offer**, DHCP sunucusunun istemciye ip bilgilerini sunduğu pakettir. Unicast yayın kullanılarak gerçekleştirilir (Broadcast yayınla gönderilmesi de sağlanabiliyor).
    - İstemci bu paketi aldığında kendisine sunulan ip bilgilerini kullanan bir başka istemci olup olmadığını kontrol edebilmek için ARP sorgusu yapar. ARP sorgusuna yanıt dönerse bu ip adresinin başka bir istemci tarafından kullanıldığını gösterir. Böyle bir durumda ip çakışması olduğu anlaşılır ve istemci bu ip bilgileri için DHCP Request paketi göndermiyor.
    - DHCP sunucusu istemciye yanıtını UDP 67 portuna gönderiyor.
- **DHCP Request**, istemcinin sunucuya kendisine sunduğu ip bilgilerini kullanmak istediğini göstermek için gönderdiği pakettir. Broadcast yayın kullanılarak gerçekleştirilir.
    - Bu paketin Broadcast yayınla gönderilmesinin nedeni ortamda birden fazla DHCP sunucusu bulunma ihtimalidir. Broadcast yayın sayesinde istemcinin ortamdaki DHCP sunucularından sunulan ip bilgilerinden hangisini kullanacağını belirtir.
- **DHCP ACK**, istemcinin istekte bulunduğu ip adresini kullanabileceğini gösteren pakettir. Unicast yayın kullanılarak gönderilir (Broadcast yayınla gönderilmesi de sağlanabiliyor).

DHCP protokolü her ne kadar bu dört paket yapısıyla işliyor olsa da bu paketler dışında da paket yapıları bulunuyor. Bunlar;

- **DHCP DECLİNE**, DHCP sunucusunun istemciye sunduğu ip bilgileri istemci ARP sorgusu yaparak hali hazırda kullanılıp kullanılmadığını kontrol ediyordu. Bu kontrol sonucunda ip bilgilerinin farklı bir istemci tarafından kullanıldığı tespit edilirse, istemcinin sunucuya ip bilgilerini kabul etmediğini göstermek için kullandığı paket yapısıdır (Yani ip çakışması yaşandığı durumunda kullanılan pakettir).
- **DHCP NACK**, DHCP sunucusunun istemciye sunduğu ip bilgilerini sağlamaya devam edemeyeceğini göstermek için istemciye gönderdiği paket yapısıdır.
    - Bu duruma örnek olarak normalde sunucunun istemciye kiraladığı ip bilgilerinin sınırlı bir süresi vardır ve bu sürenin yarısına ulaşıldığında istemci DHCP REQUEST paketiyle sunucuya kendisine verilen ip bilgilerini kullanmaya devam etmek istediğini belirtir. Sunucu ip bilgilerinin kira süresini uzatamayacağı durumlarda istemciye DHCP DECLINE paketi gönderir.
- **DHCP RELEASE**, istemcinin hali hazırda kullandığı ip bilgilerini kira süresi dolmadan bırakacağı zamanlarda sunucuya gönderdiği pakettir.
    - Windows cihazlarda "**ipconfig /release**" komutuyla bu işlem gerçekleştirilebilir.
- **DHCP INFORM**, ip detaylarını sormak üzere istemciden DHCP sunucusuna gönderilen pakettir. DHCP istemcisi bir IP adresi aldıktan sonra, ağ geçidi adresi ve DNS sunucusu adresi gibi diğer ağ yapılandırma parametrelerini elde etmek için DHCP istemcisi tarafından gönderilir.
    - Özel router cihazlarının kullanıldığı zamanlarda bu router cihazların üzerinde PRI (Primary Rate Interface, bakır tellerden oluşan fiziksel bir ağa dayanan uçtan uca bir iletişim çözümüdür) oluyordu ve PRI üzerinden telefon hatlarıyla telefon şebekesinden DailyUp hizmeti verilebiliyordu. Bu süreçte router, bir DHCP sunucusundan ip bilgilerini alıp bu bilgiyi istemcilere dağıtırken kullandığı paket türüydü. Günümüzde pek kullanılmayan paket türlerinden birisidir.

Kurumlarda dinamik ip adresi alması istenen her network için tek bir DHCP servisi bir sunucu üzerinde ayağa kaldırılır. Bu sunucuya farklı netwoprklerden erişmek için ilgili networklere Gateway'lik yapan routerların arayüzünde DHCP Relay-Agent özelliği devreye alınır. Relay Agent özelliği ile DHCP hizmetine yönelik Broadcast yayınların router üzerinden Unicast yayına dönüştürülerek ilgili DHCP sunucusuna erişimi sağlanır. DHCP Relay-Agent özelliğini devreye almak için routerun hizmet verdiği networkün bağlı olduğu arayüzünde "**ip helper-address <DHCP Server Ip Address>**" komutuyla ilgili DHCP sunucusunun ip adresi girilir. Burada dikkat edilmesi gereken nokta router üzerinden girilecek DHCP sunucusunun ip adresine erişimi olmasıdır. Aksi takdirde router paketleri Drop edecektir.




```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface fa 0/0
R1(config-if)# ip helper-address 10.1.1.2
```

DHCP Relay Agent özelliği ile her ne kadar routerun kendisine Broadcast yayınla gelen DHCP Discover paketlerine vekillik yapıyor olsa da aynı zamanda Broadcast yayın kullanan farklı protokoller için de vekillik yapabiliyor ("**ip forward-protocol {udp [port] | any-local-broadcast | spanning-tree | turbo-flood}**" komutu kullanılıyor. Bu süreçte protokollerin kullanılan port numaraları baz alınıyor. Detaylı bilgi için https[:]//www.oreilly.com/library/view/cisco-ios-in/0596008694/re341.html). Bu protokollere bakıldığında;

- TFTP, DNS, ITS (Internet Time Service), NetBIOS Name server, NetBIOS Datagram server, BootP, TACACS

(Konfigürasyonlarını ve detaylarını CCNA - 2.07 - DHCPv4 ve CCNA - 2.08 - DHCPv6 – SLAAC notlarında bulabilirsin).

DHCP konusunda değinilmesi gereken bir başka konu ise **DHCP Option** kodlarıdır. Bu kodlar sayesinde DHCP istemcilere ip bilgisinin yanında herhangi bir TFTP, WAC gibi çeşitli network kaynaklarının adresleri de öğretilebiliyor. Option kodu üzerinden öğretilebilecek kaynak türlerine IANA'nin kendi sitesindenki listeden erişilebilir (https[:]//www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml).

DHCP Protokolünde Karşılaşılabilecek Problemler

- DHCP sunucusu farklı network üzerinde olduğu durumlarda DHCP Relay Agent özelliği routerun istekte bulunulan arayüzünde tanımlanan ip adresini paketin kaynak ip adresiyle değiştirerek DHCP sunucusuna gönderiyor. Bu sayede paket sunucuya ulaştığında hangi ip adresi havuzundan ip verileceğine karar veriliyor.
    - Router arayüzünde (Gateway adresi) Subnet veya ip bilgisi yanlış tanımlandığı taktirde istemciler DHCP sunucusundan yanlış ip bilgisi almasına veya ip bilgisi alamamasına neden olacaktır.
- DHCP sunucusunda tanımlanan ip aralığındaki bütün ip adreslerinin kiralanması/kullanılması durumunda da istemcilere ip bilgisi verilemeyecektir.
- DHCP sunucusunda yanlış ip adres aralığı tanımlanmış olabilir.
- DHCP sunucusunda tanımlı ip aralığında olan bir ip adresi statik olarak bir istemciye atanmış olabilir. Bu durumda ip çakışması olacaktır.
- DHCP sunucularının yedekli olduğu bir topolojide DHCP sunucusu ile yedek DHCP sunucusu arasındaki bağlantı kesilmiş olabilir. Bu durumda DHCP sunucusunun kiraladığı bir ip adresini bir başka DHCP sunucusu öğrenemeyeceği için aynı ip bilgisini bir başka istemciye verme riski vardır. Ip çakışması yaşanabilir.
    - DHCP sunucusunun istemciye ip bilgisi sunmadan önce ip çakışması olup olmayacağı kontrol ettirilebiliyor. DHCP sunucusu bu kontrolü istemciler gibi ARP sorgusu yaparak gerçekleştirebilir ama bunu DHCP istemcileriyle aynı network üzerinde olduğunda gerçekleştirebiliyor. DHCP sunucusu ile istemcisi ise çoğu zaman farklı network üzerinde bulunuyor. ARP sorgusunda paketler Broadcast yayın kullanılarak networke bırakıldığı için paketler network dışına çıkarılamıyor**.** Bu nedenle **"ip dhcp ping"** komutu kullanılarak ip kontrolünün Ping paketleriyle gerçekleştirilmesi sağlanabiliyor (Bu kontrol Cisco cihazlara özel değil. Windows veya Linux üzerinde çalışan bir DHCP sunucusuna da yaptırılabiliyor).

    - Cisco cihazlar üzerinde tanımlı DHCP sunucularında bu kontrolü devreye almak için "i**p dhcp ping"** komutu kullanılıyor. Bir ip çakışması tespit edildiğinde bunun kayıt altına alınması/loglanması için "**ip dhcp conflict logging**" komutu kullanılıyor. Ek olarak syslog sunucusunda da bir çakışma olması durumunda mail atılması sağlanarak ip çakışmasına neden olan kullanıcılardan haberdar olunması sağlanabiliyor.
    - **Conflict olarak tespit edilen ip adresleri, statik olarak kullanıldığı varsayılıyor ve kullanılır durumda görüldüğü için herhangi bir istemciye tekrar sunulmuyor**. Bu durum ip havuzunun küçülmesine neden oluyor. Bu ip adreslerinin tekrar kullanılabilmeleri için belirli aralıklarda "**clear ip dhcp conflict <Ip Address | *>"** komutuyla kullanılmayan ip adresleri kontrol edilerek listeden silinmesi veya listenin tamamının silinmesi gerekiyor.
    - İsteğe bağlı olarak DHCP sunucusunda belirli MAC adreslerine belirli ip adreslerinin **statik olarak** sabitlenmesi/Bind edilmesi de sağlanabiliyor. "**sh ip dhcp binding**" komutuyla da Bind edilen cihaz bilgileri görüntülenebiliyor.
    - Bir istemcinin Cisco router üzerinde açılan DHCP sunucusundan ip bilgisi alma süreci (sunucudan gönderilen-istemciden gelen paketler) "**debug ip dhcp server packet**" komutuyla takip edilebiliyor (Duruma göre DHCP sunucusunun bağlı olduğu port üzerinde SPAN/Mirrior/Monitor port özelliği kullanılarak Wireshark uygulamasında da ip alma süreci gözlemlenebilir).

- DHCP sunucusu bir network için tanımlı ip aralığından ip adreslerini kiraladıktan sonra tanımlı network adresi değiştirilmek istenebilir (sunucuda o network için farklı bir aralıktan ip adresinin dağıtılması istenebilir). Bu durumda ip adresi kiralamış istemciler kira süreleri bitene kadar yeni tanımlanan ip aralığından ip bilgileri alamayacaklardır. Networkteki bütün istemcilerin yeni aralıktan ip adresi alabilmeleri için;
    - Switch üzerinde "**reload**" komutuyla kapatılıp yeniden açılabilir. L1 Down olup yeniden Up konuma geleceği için istemciler yeni ip bilgisi almak isteyecek ve DHCP sunucusuna başvuracaktır.
    - İstemciler yeniden başlatılabilir.
    - İstemcilerin komut satırında "**ipconfig /release**" ve "**ipconfig /renew**" komutları çalıştırılabilir.
- DHCP sunucusunda yanlış ip bilgileri tanımlanması durumunda da istemciler ip bilgisi alamayacaktır.

IPv6 Addressing

CCNA notlarında da bahsedildiği gibi günümüzde IPv4 adresler tükendiği için artık CG NAT (Carrier-Grade NAT) gibi çözümler kullanılıyor. Bunun gibi çözümler kullanıcılara Private ip adresleri verip internete çıkışını baz alan çözümlerdir. Her ne kadar internete çıkışını sağlasa de beraberinde getirdiği dezavantajlar da bulunuyor.

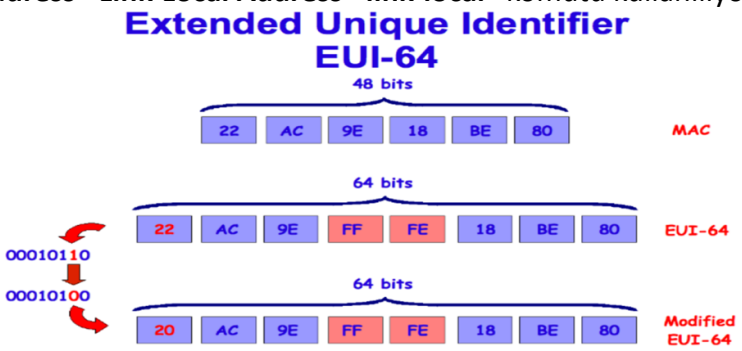
IPv4 adreslerden IPv6 adreslere geçiş sürecinde hem IPv4 hem de IPv6 adreslerin kullanıldığı Dual Stack adı verilen topolojiler kullanılıyordu. Eğer ki kaynak istemci de hedef istemci de Pv6 adrese sahip ise paketler IPv6 adresler kullanılarak gönderiliyor (sahip değilse IPv4 adresler kullanılıyor).

IPv6 adreslemede 3 farklı adres tipi bulunuyordu. Bunlar;

- GUA, internet üzerinde haberleşme yapılacağı zamanlarda kullanılan ip adresidir.
- LLA, aynı networkte bulunan istemcilerle iletişim kurabilmek için kullanılan adreslerdir. Cisco routerlarda ilgili arayüz altında "**ipv6 enable**" komutu kullanıldığında router kendi Link-Local adresini otomatik olarak hesaplamaktadır. Bu adres yapısının ilk 64 bitini network adresi oluştururken **kullanıcıyı temsil edecek (host) son 64 bitini istemciler kendiliğinden oluşturuyor** (FE80::). Bu adres tanımı iki farklı yöntemle oluşturulabiliyor. Bunlar;
    - **EUI64**, MAC adresini baz alarak ip adresinin host kısmını oluşturma yöntemidir. MAC adresinin ilk 6 hanesi IPv6 adresin ilk kısmını, MAC adresinin son 6 hanesi IPv6 adresin son kısmını oluştururken araya FF:FE tanımı ekleniyor (İsteğe bağlı olarak Link Local adresin host kısmını oluşturan son64 bitin baştan 7. Biti değiştirilebiliyor – 0 ise 1, 1 ise 0 yapılabiliyor. Cisco cihazlarda 7. bit isteğe bağlı olarak değil de doğrudan değiştiriliyor). Bu yöntemde her ne kadar network kısmını oluşturan ilk 64 biti değişmiyor olsa da Link Local adresin Host kısmını oluşturan son 64 biti MAC adresinde türetildiği için hangi networke bağlanırsa bağlansın **Link Local adresin Host kısmı değişmiyor**. Dolayısıyla takip edilebilir olduğu için günümüzde tercih edilen bir yöntem değildir.
        - Cisco routerlarda IPv6 Link Local adres tanımını EUI64 yöntemiyle oluşturabilmek için ilgili portun arayüzü altına giriş yapılarak "**ipv6 address <GUA>/<Prefix Length> eui-64**" komutunu kullanmak yeterli oluyor (Komutta GUA tanımında Prefix Length değeri /64 değilse doğal olarak Link Local adres tanımı için EUI64 yöntemi de kullanılamıyor – Yani EUI64 kullanabilmek için Network kısmı-> 64, Host kısmı-> 64 bit olmalı).

```
R2# config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# interface gigabitEthernet 0/0
R2(config-if)# ipv6 address 2001:db8:a:a::/64 eui-64
```

    - Router arayüzlerinde Link-Local adresi manuel olarak verebilmek için "**ipv6 address <Link-Local Address> link-local**" komutu kullanılıyor.



DHCPv6 sürecinde kullanılan 3 bit bulunuyor bu bitlerin anlamlarına bakıldığında;

- **A (The Address Autoconfiguration)** => SLAAC yönteminin kullanılacağını gösterir.
- **O (The Other Configuration)** => Diğer/eksik bilgileri DHCP'den öğrenileceğini gösterir.
- **M (Managed Address Configuration)** => Bütün bilgiyi DHCP sunucusundan öğreneceğin gösterir.

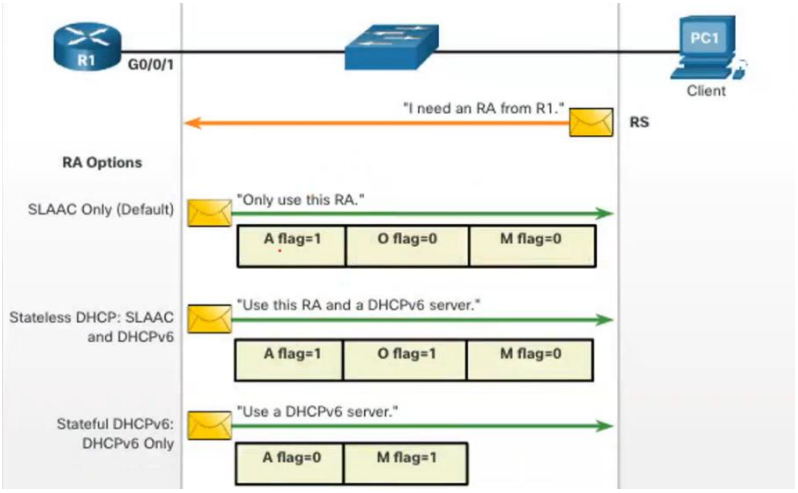
Network üzerinde istemcilere IPv6 adres dağıtmak için kullanılabilecek 3 yöntem bulunuyordu (**Unutulmaması gereken konulardan birisi de IPv6'da istemcilerin ip adresi alabilmesi için mutlaka en azından bir router bulunması gerektiğidir**. Bu süreçte RA, RS, NA ve NS paketleri kullanılır. Detaylı bilgi için CCNA - 2.08 - DHCPv6 – SLAAC notlarını inceleyebilirsin). Bunlar;

1- **SLAAC (Stateless Address Auto Configuration) Only**, networkte konfigüre edilmiş bir DHCP sunucusu olmadığı durumlarda, istemcinin ip bilgilerini router tarafından aldığı bilgiler doğrultusunda kendiliğinden belirlediği yöntemdir. Router belirli aralıklarla networke RA paketleri gönderir (bu paket içeriğinde router kendi ip adresini (Default Gateway), kullanılan network adresini (IPv6 adresin ilk 64 biti oluyor) ve Prefix değerlerini) istemciye bildiriyor). İstemci ise bu paketi alır ve içerisindeki ip bilgileri doğrultusunda IPv6 GUA adresin host kısmını oluşturan son 64 bitini kendisi oluşturur. Eksik olan DNS bilgisi gibi kısımlar da manuel girilmelidir. Bu yöntem router arayüzünde IPv6 devreye alındığında varsayılanda gelmektedir.
   a. IP takibi sağlanamadığı için kurumsal networklerde tercih edilmemektedir.
   b. RA paketi içerisinde sadece "A" biti 1 set edilerek belirtilir. Burada RA paketi Multicast yayınla networkteki herkese gönderilir. Paket içeriğinde hedef ip adresi olarak "**FF02::1**", hedef MAC adresi olarak "**33:33:00:00:00:01**" adreslerini kullanır.
   c. Herhangi bir arayüze IPv6 adres atandıktan sonra varsayılanda gelen yöntemdir. İsteğe bağlı olarak port arayüzü altında "**ipv6 nd ra suppress all**" komutuyla RA paketi göndermesi engellenebilir. Kapatıldığı takdirde network üzerinde başka bir router yoksa istemcilerin IPv6 adres bilgilerini alamayacağı göz önünde bulundurulmalıdır.
   d. Cisco router üzerinde herhangi bir arayüzün SLAAC yöntemiyle ip adresi alması istendiği durumda ilgili arayüz altında "**ipv6 address autoconfig**" komutunu kullanması yeterli olacaktır. (Network üzerinde birden fazla router olduğu zamanlarda bu özelliğin devre dışı bırakılması istenebilir).

```
R2# config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# interface gigabitEthernet 0/0
R2(config-if)# ipv6 address autoconfig
```

2- **SLAAC with DHCP,** istemci networke bağlandığında routerun gönderdiği RA mesajıyla kendisine ip adresi, subnet maskesi ve Default Gateway bilgilerini atıyor. Eksik olan bilgileri (DNS bilgisi gibi) ise DHCP sunucusundan alınacağını gösteriyor. Yani istemci kendi kendine ip bilgilerini atadıktan sonra DNS bilgisi için DHCP sunucusu arıyor ve networkte tanımlı sunucu varsa DNS bilgilerini de alıyor.
   a. RA paketi içerisinde "A" ve "O" bitleri 1 set edilerek belirtilir.

3- **Only DHCP (Statefull)**, istemcinin networke bağlandığında ip bilgilerini bir DHCP sunucusundan aldığı yöntemdir. İstemci ve sunucu arasındaki iletişim adımları IPv4'teki adımlarla aynıdır. IPv4'ten farklı olarak IPv6'da broadcast yayın olmadığı için networke bağlanan istemci DHCP sunucularına erişebilmek için DHCP sunucularına atanmış özel bir Multicast adres kullanıyorlar (ff02::1:2). Bu adrese paket gönderdiğinde networkteki tüm DHCP sunucularına bu paket iletilmiş oluyor.
   a. RA paketi içerisinde sadece "M" biti 1 set edilerek belirtilir.



RA paketi sorguda bulunulmasa dahi belirli sıklıklarda Multicast yayınla networkteki herkese yollanıyor (**FF02::1 adresiyle – 33:33:00:00:00:01 MAC adresiyle**). Yani bir anlamda Pv6'da ip bilgisi alma sürecini router başlatıyor diyebiliriz.

- Routerun herhangi bir arayüzlerine IPv6 adres tanımı yapıldıktan sonra veya Global konfigürasyon modunda "**ipv6 enable**" komutu (routerun Link Local adresini oluşturması sağlanıyor) kullanıldıktan sonra arayüz üzerinden RA paketleri yayınlanmaya başlanıyor (Networke RA paketlerinin gönderilmesi için ek bir konfigürasyona ihtiyaç duyulmuyor).

DHCPv6 Protokolünde Kullanılan Paket Tipleri

DHCPv6 protokolünde temelde kullanılan 4 paket yapısı bulunuyor. Bu paketler genel anlamda DHCPv4 protokolünde kullanılan paketlere benzer şekildedir. İstemci networkünde bulunan routerdan ip bilgilerini DHCP üzerinden alacağını öğrendikten sonra (**SARR**);

- **SOLICIT**, networkte bir DHCPv6 sunucusu olup olmadığını sorgulamak için istemci tarafından gönderilen pakettir. Bu paket **FF:02::1:2 Multicast** adres kullanılarak gönderiliyor (Bu Multicast adres DHCPv6 protokolü için revize edilmiştir).
    - Burada Multicast kullanılması DHCPv4'de kullanılan Broadcast yayın üzerinden DHCP sunucularına yönelik oluşturulabilen saldırı vektörlerinin önüne geçilebilmesini sağlıyor.
- **ADVERTİSE**, DHCPv6 sunucunun istemciye ip bilgilerini sunmak için kullandığı pakettir.
- **REQUEST**, İstemcinin kendisine sunulan ip bilgilerini kabul ettiğini DHCPv6 sunucusuna bildirmek için kullandığı pakettir.
- **REPLY**, DHCPv6 sunucunun istemciye sunduğu ip bilgisini kullanmaya başlayabileceğini bildirmek için kullandığı pakettir.

Bu paketler dışında DHCPv6 sürecinde kullanılan birçok paket yapısı daha var. Bunlar;

- **CONFIRM**, istemcinin bağlantısı git-gel yaptığında, bağlantı gitmeden önce kullandığı ip bilgilerini kullanmaya devam edip edemeyeceğini DHCPv6 sunucusuna sormak için kullandığı paket yapısıdır.
- **RENEW**, istemcinin kendisine kiralanan ip bilgisinin kira süresini uzatmak için DHCPv6 sunucusuna gönderdiği pakettir.
- **REBIND**, istemci ip bilgisi aldığı DHCPv6 sunucusuna RENEW paketi gönderdikten sonra dönüş alamadığı takdirde (DHCPv6 sunucusunun artık hizmet vermediğini anlar)

kendisine verilen ip bilgisini kullanmaya devam edip edemeyeceğini sormak üzere network üzerinde aktif farklı bir DHCPv6 sunucusu olup olmadığını sorgulamak için kullandığı pakettir.

- **RELEASE**, istemcinin kendisine verilen ip bilgilerinin kira süresi dolmadan kullanmayı bırakacağını DHCPv6 sunucusuna bildirmek için kullandığı pakettir.
- **DECLINE**, DHCPv6 sunucunun istemciye sunacağı ip adres bilgilerini farklı bir istemci kullanıyorsa, istemcinin DHCPv6 sunucusuna bu ip adresini kullanamayacağını bildirmek için kullandığı pakettir (İhtimali düşük de olsa ip çakışması durumu).
- **RECONFIGURE**, network bilgilerinde değişiklikler meydana geldiğinde DHCPv6 sunucunun istemcilere bu değişiklikleri bildirmek için kullandığı pakettir.
    - Güvenlik zafiyeti oluşturabilir mi? Saldırgan RECONFIGURE paketleriyle istemcilerin ip bilgileri üzerinde değişiklikler yaptırıp trafik akışını değiştirebilir mi?
- **INFORMATIN-REQUEST**, SLAAC with DHCP yönteminde olduğu gibi istemcinin ip bilgisi dışında diğer bilgileri DHCPv6 sunucusundan istemek için kullandığı pakettir.
- **RELAY-FORW** - **RELAY-REPL**, network içerisindeki istemcileri farklı bir networkteki merkezi bir DHCPv6 sunucudan ip bilgisi alması gerektiği durumlarda (routerlar Proxy görevi görüyordu) routerun merkezi DHCPv6 sunucusundan ip bilgisi talep etmek ve DHCPv6 sunucusunun routerun gönderdiği Relay Agent paketlerine yanıt verirken kullandığı paketlerdir.
    - Relay Agent konfigürasyonu için ilgili arayüz altında "**ipv6 dhcp relay destination <DHCPv6 IPv6 Ip Address>**" komutuyla merkezi DHCPv6 sunucunun ip adresini tanımlamak yeterli oluyor.

DHCPv6

Her ne kadar kullanılması önerilmese de IPv4'te olduğu gibi IPv6 için de router üzerinde Statefull ve Stateless olmak üzere iki farklı şekilde DHCPv6 konfigürasyonu yapılabiliyor. Stateless konfigürasyonu için;

- İlk olarak routerun IPv6 yönlendirmesini aktive edebilmek için "**ipv6 unicast-routing**" komutunun kullanılması gerekiyor.
- IPv4 DHCP konfigürasyonunda olduğu gibi IPv6 DHCP konfiürasyonunda da öncelikle Global konfigürasyon modunda "**ipv6 dhcp pool <Pool Name>**" komutuyla bir ip havuzu oluşturuluyor.
- Bu kısımdan sonra oluşturulan DHCP havuzunu devreye alabilmek için sunucunun kullanılacağı arayüze girilerek "**ipv6 dhcp server <Pool Name>**" komutu kullanılıyor. Bu sayede DHCP sunucusu arayüze atanan ip bilgilerini RA paketi içerisinde göndererek ip bilgisi almak isteyen istemcilere gönderebiliyor.
- İsteğe bağlı olarak "**ipv6 nd other-config-flag**" komutuyla istemcilerin DNS bilgilerini DHCP sunucusundan alabilmesi de sağlanabiliyor (İsteğe bağlı olarak istemcilere DNS bilgilerini DHCP sunucusundan aldırmak yerine "**ipv6 dhcp pool <Pool Name>**" arayüzüne girilerek "**dns-server <DNS Server Ip Address>**" komutuyla DNS bilgileri manuel olarak tanımımlanabiliyor. Bu sayede DNS bilgisi de router üzerinden verilebiliyor).
- Konfigürasyon sonunda routerun arayüzüne atanan ip adresi göz önünde bulundurularak istemci kendi ip adresini kendisi belirleyecektir.

```
R1(config)#interface gi 0/0/0
R1(config-if)#ipv6 address 2001:db8:ac10:fe01::/64
R1(config-if)#no sh

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

R1(config-if)#exit
R1(config)#ipv6 dhcp pool ITNetwork
R1(config-dhcpv6)#exit
R1(config)#interface gi 0/0/0
R1(config-if)#ipv6 dhcp server ITNetwork
R1(config-if)#ipv6 nd other-config-flag
R1(config-if)#exit
```

Statefull Konfigürasyonu için;

- İlk olarak routerun IPv6 yönlendirmesini aktive edebilmek için "**ipv6 unicast-routing**" komutu kullanılması gerekiyor.
- IPv4'te de olduğu gibi DHCP konfiürasyonuna da "**ipv6 dhcp pool <Pool Name>**" komutuyla bir ip havuzu oluşturularak başlanıyor.
- Ip havuzu oluşturulduktan sonra "**address prefix <Ip Address/Prefix> lifetime <Preferred Time> <Valid Time>**" komutuyla IPv6 adresi ve prefix uzunluğuyla beraber ip adresinin istemciye ne kadar süreyle kiralanacağını gösteren **Preferred Time** ve **Valid Time** değerleri tanımlanıyor.
- Normalde DHCP sunucusunda tanımlanan DNS bilgisi alınıyor ama isteğe bağlı olarak DNS bilgisi router üzerinden verilmek isteniyorsa "**dns-server <DNS Server Ip Address>**" komutuyla istemcilere gönderilecek DNS bilgisi de tanımlanabiliyor.
- Bu adımlardan sonra DHCP havuzunu devreye alabilmek için routerun ilgili arayüzüne girilerek "**ipv6 dhcp server <Pool Name>**" komutuyla oluşturulan DHCP havuzunun ismini buraya tanımlıyoruz.
- Tanımlama sonrasında istemcilere gönderilen RA paketi içerisinde M flag bitinin 1 gitmesini sağlamak için "**ipv6 nd managed-config-flag**" komutu kullanılıyor. Bu konfigürasyon sonunda router istemcilere ip bilgisi dağıtmaya başlayacaktır.

```
R1(config)#interface gi 0/0/1
R1(config-if)#ipv6 address 2001:db8:ac10:fe02::/64
R1(config-if)#no sh

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
exit
R1(config)#ipv6 dhcp pool HRNetwork
R1(config-dhcpv6)#address prefix 2001:db8:ac10:fe02::/64 lifetime 172800 86400
R1(config-dhcpv6)#dns-server 2001:4800:acad::1234
R1(config-dhcpv6)#exit
R1(config)#interface gi0/0/1
R1(config-if)#ipv6 dhcp server HRNetwork
R1(config-if)#ipv6 nd managed-config-flag
R1(config-if)#exit
R1(config)#
```

Statefull DHCPv6 konfigürasyonu router üzerinde yapıldığında, istemciler ip adresini nasıl alacağını routera sorup öğreniyor. Router ip bilgisini DHCP sunucusundan alacağını bildirdikten sonra istemci yeniden routera gelip ip bilgilerini alıyor.

IPv6'da DHCP Relay Agent konfigürasyonu için IPv4'te olduğu gibi farklı networkten DHCPv6 hizmeti almak isteyen arayüze giriş yapılarak "**ipv6 dhcp relay destination <Ip Address/Prefix>**" komutuyla hedef DHCPv6 sunucunun ip adresi ve bulunduğu arayüz tanımlanıyor.

```
R1(config)#interface gi 0/0/1
R1(config-if)#ipv6 dhcp relay destination 2001:db8:1234::2/64 G0/0/0
R1(config-if)#exit
```

NOTLAR

- Subnet hesaplamalarında kaç cihaza ip verileceğini hesaplamak için 256 değerinden subnet maskesinin değeri çıkarılarak bulunabilir. Örnek olarak;
    - /26 Prefix Length değeri için 255.255.255.192 tanımı kullanılır. 256-192=64 ip adresi kullanılabileceğini gösterir (Broadcast ve network adresi bu aralıkta çıkarıldığında ortaya 64-2=62 adet kullanılabilir ip adresi çıkıyor).
- Her ne kadar routerlar paketi işlemeyecek de olsa network içerisinde broadcast yapılan paketleri alıp değerlendirir.
- Normalde tüm Cisco marka switchlerde DHCP hizmeti varsayılanda devrede geliyor. Bu hizmet çeşitli durumlarda devre dışı bırakılmak istendiğinde global konfigürasyon modunda "**no service dhcp**" komutuyla devre dışı bırakılabiliyor.
    - DHCP hizmeti doğru çalışmadığı zamanlarda "**no service dhcp**" komutuyla devre dışı bırakılıp "**service dhcp**" komutuyla tekrar devreye alınabilir.
- DHCP sunucusu varsayılanda istemcilere önerdiği ip bilgilerinin networkte kullanılıp kullanılmadığını kontrol etmez. İstemciler DHCP sunucusunun kendisine önerdiği ip adresini (DHCP OFFER) kabul etmeden önce networkte ARP sorgusuyla kontrol eder. Eğer ki kendisine önerilen ip adresini farklı bir istemci kullanıyorsa DHCP NACK paketi göndererek reddeder. Bu süreçte istemciye önerilecek ip adresinin DHCP sunucusundan çıkmadan önce kontrol ettirilmesi sağlanabilir. Bunun için Cisco routerlarda "**ip dhcp ping**" komutu kullanılarak ip adresi istemciye sunulmadan önce kullanımda olup olmadığı kontrol ettirilebiliyor.
    - Ip çakışması tespit edildiğinde bunun Syslog üzerinde kayıt altına alınabilmesi/loglanması için "**ip dhcp conflict logging**" komutu kullanılabiliyor.
    - DHCP hizmeti verilen (router üzerinde) network routera doğrudan bağlıysa bu durumda varsayılanda ARP sorgusu yaparak ip adresinin kullanımda olup olmadığını kontrol ediyor.
- DNS sorgusu da broadcast yayınla yapılabiliyor
- BootP protokolü DHCP protokolünden önceki zamanlarda istemcilerin ip bilgisi almak için kullanılandıkları protokoldür.
- ISP routerları gibi WAN ağlarında router arayüzlerinin DHCP sunucusundan ip adresi alabilmesi için ilgili arayüze giriş yapıp "**ip address dhcp**" komutu kullanılıyordu. Burada bağlantı PPP ise broadcast yayın olmadığı için "**ip address negotiated**" komtu kullanılıyor.

```
R1# configure terminal
R1(config)# int fa 0/1
R1(config-if)# ip address dhcp
```

- Backup of DHCP Server Architectures,
- Varsayılanda Cisco cihazlarda IPv6 routing özelliği devre dışı gelebiliyor ("**sh protocols**" komutuyla kontrol edilebiliyor). Bu nedenle router üzerinde IPv6 adreslerin kullanılması planlanıyorsa "**ipv6 unicast-routing**" komutuyla IPv6 adresler için yönlendirme tablosu devreye alınmalıdır.
- IPv6'da Multicast adresler FE02:: ile başlıyor.

Terminolojiler;

- **Span/Mirrior/Monitor Port**, cihaz üzerindeki herhangi bir porttan geçen trafiğin bir kopyasının gönderildiği portlara deniliyor. Trafiği izlemek ve yedeklemek için kullanılan portlara verilen isim olarak da tanımlanabilir. Konfigürasyonuna bakıldığında;
    - Cihaz üzerinde global konfigürasyon modundan "**monitor session <Session Number> source interface <Source Interface Id>**" komutuyla trafiği kopyalanmak istenen port tanımı yapılıyor. Ardından "**monitor session <Session Number> destination interface <Destination Interface Id>**" komutuyla da hedef yani trafiğin kopyasının gönderileceği port tanımı yapılıyor.
- Proxy ARP,

Kontrol Komutları;

- sh ip dhcp conflict
- sh protocols
- sh ipv6 interface <Interface ID>
- debug ip dhcp server packets
    - DHCP sürecini adım adım görüntülüyor.

Yapılabilecek Uygulama Fikirleri

- Farklı protokollerin (DHCP dışında) Broadcas paketleri için relay agent özelliğiyle trafiğinin taşınma süreci test edilebilir.
- Yedek DHCP Server konfigürasyonu
    - Fail-Over Method
    - Load-Balance Method
- DHCPv6 LAN protokolü üzerine güvenlik zafiyetleri