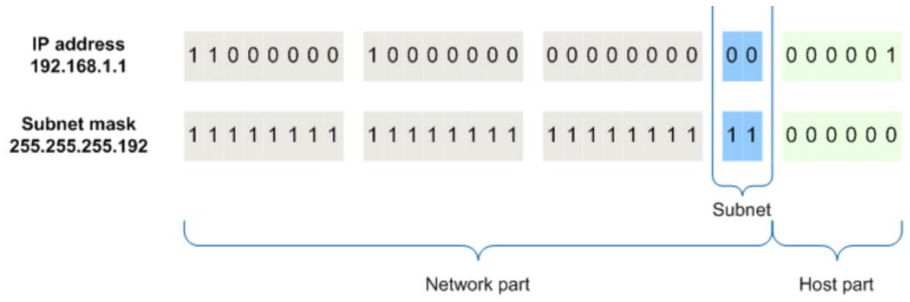
Routing Fundamentals - 1

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.

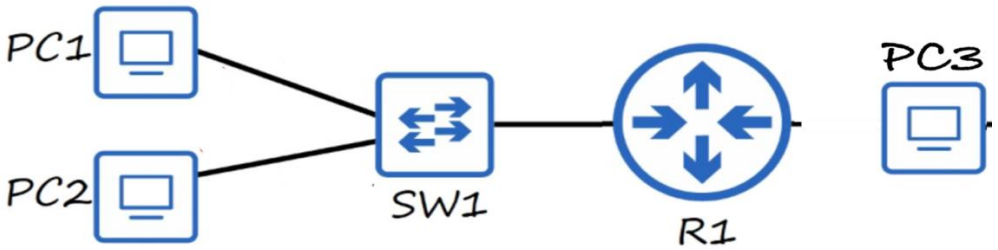
Network üzerinde iki cihazı aralarında haberleştirebilmek için sahip olmaları gereken 3 bilgi bulunuyor. Bunlar **ip adresi**, **Subnet maskesi** ve **Default Gateway** adresidir. Bu adreslerden ip adresi network üzerinde cihazı ayırt edebilmeyi sağlıyor.

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 iletişimleri 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.

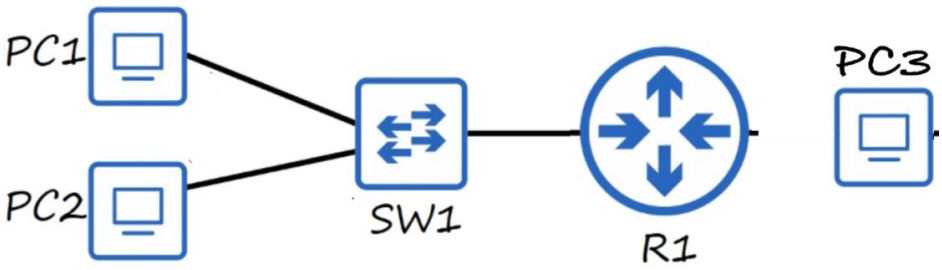
Benzer şekilde cihazlara ip bilgileri;

- 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, 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 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 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.

DHCP Relay Agent özelliği ile her ne kadar router 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 protokkollerin 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 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. Bu kontrolü istemciler gibi ARP sorgusu yaparak gerçekleştiremiyor çünkü çoğu zaman farklı network üzerinde tanımlı oluyor. ARP sorgusunda paketler Broadcast yayın kullanılarak networke bırakıldığı için paketler network dışına çıkarılamıyor**. Bu nedenle ip kontrolünü Ping paketleri kullanarak gerçekleştiriliyor** (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 alınmaıs/loglanması için "**ip dhcp conflict logging**" komutu kullanılıyor.
    - **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 sabitlenmesi de sağlanabiliyor.

```
ip dhcp pool static
 host 192.168.184.183 255.255.255.0
 hardware-address bce1.43d4.16b1
 default-router 192.168.183.1
 dns-server x.170.119.9 x.170.119.19 8.8.8.8 8.8.4.4
```

- 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.

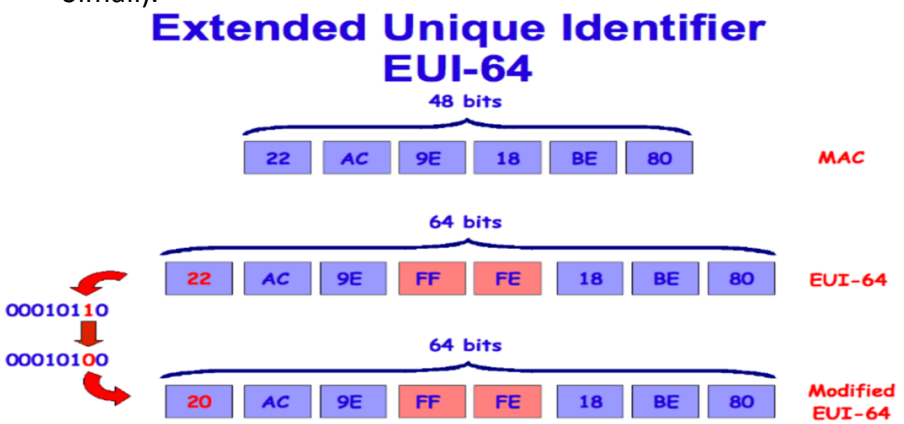
IPv6 Addressing

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. Bu adresi 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 adresi baştan 7. Bit değiştirilebiliyor – 0 ise 1, 1 ise 0 yapılabiliyor. Cisco cihazlarda 7. bit isteğe bağlı olarak değil de doğrudan değiştiriliyor). Bu yöntemde Link Local adres 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).



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. İstemci ise bu paketi alır ve içerisindeki ip bilgileri doğrultusunda kendi kendine ip adresi atar.
    a. RA paketi içerisinde sadece "A" biti 1 set edilerek belirtilir.
    b. Herhangi bir arayüze IPv6 adres atandıktan sonra varsayılanda gelen yöntemdir. İsteğe bağlı olarak port arayüzü altında "**ipv6 nd ra suppress all**" komutuyla kapatılabilir. Kapatıldığı takdirde network üzerinde başka bir router yoksa istemcilerin IPv6 adres bilgilerini alamayacağı göz önünde bulundurulmalıdır.
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**, 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.

Bitlerin anlamlarına bakıldığında A (The Address Autoconfiguration) = SLAAC kullan, O (The Other Configuration) = Diğer/eksik bilgileri DHCP'den öğren, M (Managed Address Configuration) = Bütün bilgiyi DHCP sunucusundan öğreneceğin gösteriyor.

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.

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.
- 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 tablosudevreye alınmalıdır.
- IPv6'da Multicast adresler FE02:: ile başlıyor.

Terminolojiler;

- **Span/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
- debug ip dhcp server packets
    - DHCP sürecini adım adım görüntülüyor.