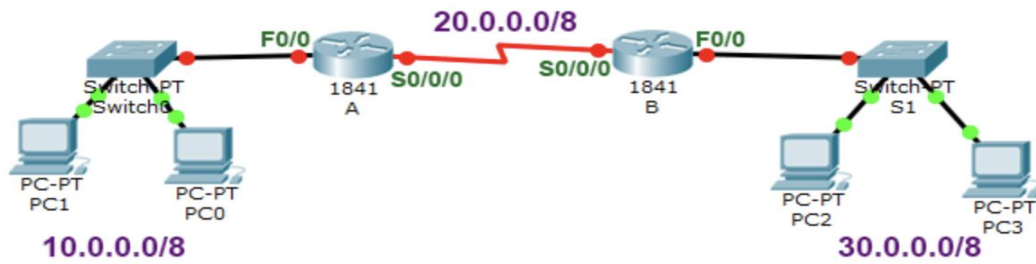


Routing Fundamentals - 2

Bir istemci farklı bir istemciye Ping atmak istediğinde öncelikle hedef istemcinin ip adresiyle kendi ip adresini karşılaştırarak hedefin aynı networkte olup olmadığına karar verir. Hedef aynı network içerisinde bulunuyorsa (ARP tablosunda hedef istemcinin MAC adresi yoksa) ARP sorgusu yaparak hedefin MAC adresini öğrenir ve paketi hedefe iletir. Eğer ki hedef farklı bir network üzerindeyse bu durumda Gateway adresinin MAC adresini öğrenmek üzere ARP sorgusu yapar ve hedefi Gateway adresine gönderir.

Paket routera ulaştığında öncelikle hedef ip adresinin yönlendirme tablosunda kayıtlı olup olmadığı kontrol edilir. İp adresi yönlendirme tablosunda bulunuyorsa yönlendireceği arayüzü belirler. Paketi yönlendireceği arayüzde L2'e kullanılan protokole göre işlem yapar (örnek olarak kullanacağı arayüzde L2'de Ethernet protokolü kullanılıyorsa ARP ile Next Hop ip adresinin MAC adresini öğrenir. **PPP/Serial bağlantı kullanılıyorsa herhangi bir L2 adres kullanılmadığı için buna gerek kalmaz**). Next Hop Mac adresi öğrenildikten sonra paketin TTL değerini 1 düşürür ve Header Checksum değerini yeniden hesaplar (TTL değeri değiştiği için Header Checksum değerini yeniden hesaplanması gerekiyor). Bu işlemlerin ardından paketi Next Hop ip adresine yönlendirir. Bu şekilde paket routerlar üzerinden hedef networke ulaştırılır.

Gateway üzerinde yönlendirme tablosu kullanılarak paket hedef networke yönlendirilir. Hedef networke ulaştırıldığında yeniden ARP sorgusu yapılarak paketin hangi istemciye iletileceği belirlenir ve paket hedef istemciye ulaştırılır. Bu süreç hedef istemci yanıtını gönderirken tekrar uygulanır (bu nedenle Ping paketlerinin ilki bu süreçte birçok kez yapılan ARP sorgularından kaynaklı olarak zaman aşımına uğrar. PC1->A, B->PC2, PC2->B, A->PC1 olmak üzere toplamda 4 tane ARP sorgusu yapılacaktır).



İki istemci arasındaki haberleşme süreci genel anlamda bu şekilde gerçekleşmektedir. Paket router üzerine geldiğinde router paketin hedef ip adresini yönlendirme tablosunda aramaya başlayacaktır. Yönlendirme tablosunda aynı ip adresine sahip birden fazla rota tanımı bulunduğu durumda kullanılacak rotaya karar verirken göz önünde bulunduracağı kriterler sırasıyla;

- Hedef ip adresiyle eşleşen en Max Match/Best Match Prefix Length uzunluğuna sahip rota tanımı
- En düşük AD değerine sahip rota tanımı (Kullanılan yönlendirme protokolünün kalitesini gösteriyor).
- En düşük Metrik değere sahip rota tanımı olacak şekilde paketin gönderileceği rotaya karar verecektir (Kullanılan yönlendirme protokolünde belirtilen rotaların maliyetini ifade ediyor).

- Metrik değeri dahi eşit olan rota tanımları arasında Load-Balance yapılarak paketler iletilecektir.

S	Pro	Netowrk	[A.D / Metr]	Int
1	R	10.0.0.0/24	[120 / 3]	IntX1
2	D	10.0.0.0/16	[90 / 6000]	IntX2
3	S	10.0.0.0/8	[1 / 0]	IntX3
4	O	10.0.0.0/24	[110 / 600]	IntX4
5	O	10.0.0.0/24	[110 / 600]	IntX5
6	O	10.0.0.0/24	[110 / 700]	IntX6

Yukarıdaki tabloya istinaden 10.0.0.1 ip adresine paket gönderilmek isteniyorsa bu durumda uygulanacak karar mekanizmasında;

- En uygun Prefix Length değerine sahip olan 1,4,5 ve 6. Satır dışındaki satırlar elenecektir.
- Bu satırlar arasında AD değeri en düşük olanlar, yani 4,5 ve 6. satır dışındakiler elenecektir.
- Son adımda Metrik değeri düşük olan 4 ve 5. satırlar dışındaki satırlar elenecektir. Bu satırlar arasında da Load-Balance yapılarak paketler iletilmeye başlanacaktır.

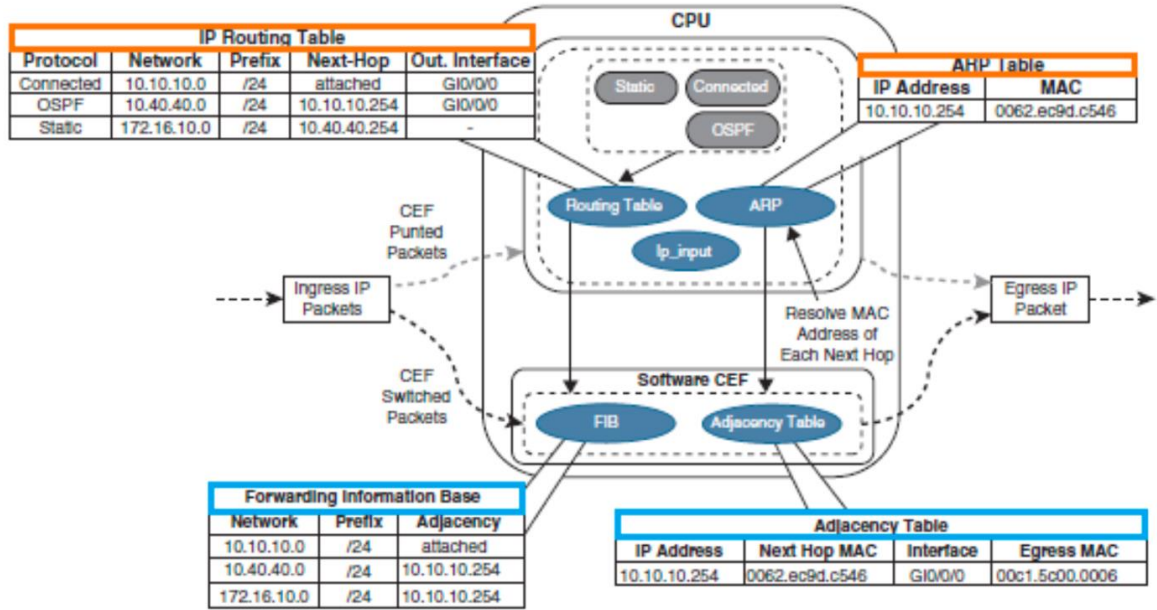
Farklı bir örnek olarak 10.0.1.1 adresine bir paket gönderilmek istendiğinde en uygun Prefix Length olan 2. satır üzerinden paketler gönderilmeye başlanacaktır.

CEF (Cisco Express Forwarding)

Yazının başında da bahsedildiği üzere **routerlar** kendilerine gönderilen paketler için pek çok işlem gerçekleştiriyor. Bu işlemleri (özellikle de bant genişliğini yüksek olması durumunda) normal bir CPU ve RAM donanımıyla gerçekleştirmek pek mümkün olmuyor. Çünkü bu işlemlerin yanında routerlar üzerinde devreye alınan SNMP, SSH, DHCP gibi özelliklerle beraber routerun asli görevi olan paket yönlendirme işlemine ayıracağı kaynak miktarı azalacaktır. Bu nedenle süreci daha etkin işletebilmek routerların yapısı Control Plane ve Data Plane olarak iki kısma ayrılıyor. Bu kısımlar (Detaylı bilgi için **CCNP - 01 - Packet Forwarding** notlarını inceleyebilirsiniz);

- **Control Plane**, CPU ve RAM donanımlarından oluşan bölümdür. Yönlendirme tablolarının oluşturulması, SSH, DHCP Server. ACL tanımları gibi yönetimsel süreçler burada gerçekleştirilir.
- **Data Plane**, paket yönlendirme/anahtarlama işlemine yönelik özel oluşturulan ASIC ve TCAM donanımlarından oluşan bölümdür. Control Plane üzerinde alınan kararlara istinaden (yönlendirme tablosu, ACL tanımları gibi) paketlerin yönlendirme/anahtarlama işlemi bu alanda gerçekleştirilir (Yani bir anlamda routerların asıl performansını belirleyen donanımların bulunduğu alandır).
 - o Control Plane’de yönlendirme tablosu oluşturulduktan sonra bu tablo RAM’dan TCAM üzerine kopyalanır. Bu sayede CPU ve RAM donanımlarının iş yükü azaltılarak, ASIC ve TCAM kullanılarak paket yönlendirme/anahtarlama işlemi yapılabilir (ASIC ve TCAM ‘in asli amacı paket anahtarlama olduğu için başka bir süreçte kullanılmaz. Dolayısıyla paket anahtarlama sürecinde performans kaybı yaşanmaz).

- Control Plane’de oluşturulan **yönlendirme tablosu** Data Plane’de **CEF FIB (Forwarding Information Base)** olarak kopyalanır.
- Control Plane’de oluşturulan **Layer 3-to-Layer 2 Mappings** tablosu Data Plane’de **CEF Adjacency Table** olarak kopyalanır.
 - L2’de Ethernet protokolü kullanılıyorsa Layer 3-to-Layer 2 Mapping olarak isimlendirilen tablo ARP tablosu oluyor. Cisco cihazlarda ARP tablosuna eklenen bir Ip-MAC bilgisi 4 saat boyunca silinmiyor (ARP tablosu switchlerdeki MAC adres tablosuyla karıştırılmamalıdır. MAC adres tablosu yani MAC-Port eşleniği 300 saniye sonunda trafik oluşturulmadığı takdirde siliniyordu).



Bu çalışma yapısı (yönetimsel kararların Control Plane tarafından verilmesi, paketlerin Data Plane üzerinden (ASIC ve TCAM kullanılarak) anahtarlanması) **CEF (Cisco Express Forwarding)** olarak bilinmektedir. Bu özellik Cisco cihazlarda varsayılanda açık gelmektedir. İsteğe bağlı olarak bu özellik “no ip cef” komutu kullanılarak kapatılabiliyor (kapatılması durumunda tüm süreç CPU ve RAM üzerinden gerçekleştirileceği için cihazın kapasitesinin büyük oranda düşecektir). Kurumsal yapılarda router seçilirken cihazların CPU ve RAM değerlerine bakmak yerine asıl anahtarlama işlemini yapan TCAM ve ASIC gibi donanımların paket anahtarlama kapasitelerine bakılır.

- CEF çözümünün ilk zamanlarda desteklemediği durumlar olmasından dolayı devre dışı bırakılabiliyormuş ama günümüze kadar yapılan geliştirmeler sayesinde artık devre dışı bırakmaya ihtiyaç duyulmuyor.
- Her markada muadili çözümler vardır. Sadece isim değişikliği görülüyor.
- Tanımlı ACL’ler dahi Data Plane’e kopyalanarak donanımsal yapılması sağlanabiliyor. Bu sayede performansa etkisi olmuyor.

Routerların Control Plane ve Data Plane olmak üzere iki kısımdan oluştuğu açıklanmıştır. Control Plane’de bulunan CPU ve RAM birimleri bilgisayarlarda da bulunmaktadır. Bunun üzerine **OpenFlow** adı verilen protokol kullanılarak Control Plane’in yapması gereken süreçlerin/hesaplamaların bir bilgisayar üzerinden gerçekleştirilerek routerların Data Plane’ine kopyalanması sağlanabiliyor (yani routerların yönetim süreci bir bilgisayar üzerinden kontrol edilebiliyor). Bu yönetim sürecini bilgisayar üzerinden sağlayabilmek için kullanılan yazılıma da **SDN (Software Define Network)** deniliyor.

Routing Information Sources

Yönlendirme tabloları oluşturulurken tabloya eklenen rota bilgileri birkaç farklı şekilde elde edilebilir. Bunlar;

- **Directly Connect**, router arayüzüne doğrudan bağlı network adreslerinin yönlendirme tablosuna doğrudan dahil edilmesidir.
- **Static Route**, network yöneticisinin bir network adresini manuel/statik olarak tanımlayarak yönlendirme tablosuna dahil etmesidir.
- **Dynamic Route**, dinamik yönlendirme protokollerinin kullandığı veri yapıları (örnek olarak OSPF protokolünde Link-State Database verilebilir) üzerinde hesaplamalar yapılarak uygun rotaların yönlendirme tablolarına dahil edilmesidir.
- **Redistributed Route**, farklı dinamik yönlendirme protokolleri üzerinden öğrenilen rota bilgilerinin yönlendirme tablosuna dahil edilmesidir.

Öğrenilen rota bilgilerinin öğrenildiği kaynağa göre kalitesini belirlemek amacıyla **Administrative Distance** değeri kullanılıyor. Öğrenilen bir rota tanımının AD değerlerinin küçük olması öğrenilen rotanın kalitesinin yüksek olduğunu gösterir. AD değerlerine bakıldığında;

Route Source	Default Distance Values
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown*	255

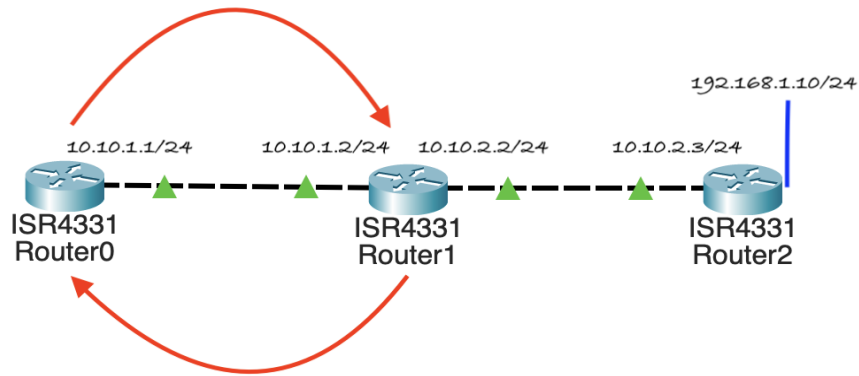
Normalde statik rota tanımlarında AD değeri 1'dir. Aynı rota için birden fazla statik rota tanımı yapıldığında ise varsayılanda AD değerleri aynı olacaktır. Burada aynı network için yapılan iki statik rota tanımını kıyaslayabilecek bir Metric değere sahip olunmadığı için (Dinamik yönlendirme protokollerinde Metric değerler göz önünde bulunduruluyordu) Load-Balance işlemi yapılacaktır.

- **Load-Balance** yapılacak statik rota tanımları arasında kullanılan bant genişlikleri eşit olmayabilir. Bu durumda bant genişliği düşük olan rota tanımı yüksek olan rota tanımını sekteye uğratacaktır (örnek olarak TCP kullanılan bir trafik akışında Session'ların tamamlanması için bant genişliği düşük olan rota tanımından gönderilen paketler beklenecektir). Bu nedenle statik rota tanımları arasında da önceliklendirme işlemi yapılması gerekecektir. Bu öncelik değeri statik rota tanımlarının AD değerleri üzerinde değişiklikler yapılarak gerçekleştiriliyor. Bu işleme **Floating Static Route** deniliyor. Bu sayede düşük bant genişliğine sahip rota tanımı yedek rota tanımı olarak bekletilmeye başlanıyor (aynı statik rota tanımları arasında öncelikli rota (AD değeri düşük olan) tanımında bir problem yaşanmadığı sürece öncelik değer düşük olan statik rota tanımı/yedek yönlendirme tablosuna eklenmez).

- **Floating Static Route** tanımı sadece statik rota tanımları arasında önceliklendirme işlemi için kullanılmıyor. Aynı zamanda Dinamik yönlendirme protokolleriyle hesaplanan rota tanımlarına müdahale edebilmek için de kullanılıyor. Dinamik yönlendirme protokolleri kullanılarak hesaplanan rota bilgilerinin AD değerlerinden daha düşük veya yüksek statik rota tanımları yapılarak yönlendirme tablolarına müdahale edilebiliyor.
- Statik rota tanımında AD değerini değiştirmek için “**ip route <Destination Network Address> <Destination Subnet Mask> <Next Hop Ip Address> <Administrative Distance Value>**” komutu kullanılıyor.

Statik rota tanımı yapılırken dikkatli olunmadığı takdirde Loop oluşumuna neden olunabilir. Örnek olarak Router1 üzerinden 192.168.1.10 adresine gidebilmek için bir rota tanımı yapılırken “**ip route 192.168.1.10 255.255.255.0 10.10.2.3**” tanımı yerine “**ip route 192.168.1.10 255.255.255.0 10.10.1.1**” tanımı yapılırsa paketler Router0’a gönderilecektir. Router0 üzerinden de 192.168.1.10 adresine ulaşmak için “**ip route 192.168.1.10 255.255.255.0 10.10.1.2**” tanımı bulunuyorsa paketler Router1 ve Router0 arasında Loop oluşturacaktır (paketlerin TTL değeri 0 olana kadar). Bu durumda Router0 ve Router1 arasındaki bağlantının bant genişliği de Loop nedeniyle meşgul edilecektir/dolduracaktır (kesintiye neden olacaktır). **Dolayısıyla Router0, Router1 üzerinden erişim sağladığı diğer networklere de erişimini kaybedecektir.**

- Loop oluşumunda paketler belirli routerların üzerinden tekrar tekrar geçeceği için böyle bir durum **Traceroute** komutuyla tespit edilebilmektedir.



Recursive LookUp

CEF kullanmayan routerlar kendilerine gönderilen paketleri yönlendirebilmek için öncelikle hedef network adresinin yönlendirme tablosunda olup olmadığını kontrol eder. Yönlendirme tablosunda hedef network için adres kaydıyla birlikte paketin gönderileceği Next Hop ip adres bilgisi bulunur (ilk sorgu süreci). Next Hop Ip adres bilgisi paketin hangi arayüzden gönderileceğini belirlemek için yeterli değildir. Bu nedenle ikinci kez/tekrar yönlendirme tablosuna bakılarak paketin hangi arayüz üzerinden gönderileceği/Exit Interface bilgisi belirlenir (ikinci sorgu süreci). Bu şekilde yönlendirme tablosunun iki kez kontrol edilmesine **Recursive LookUp** deniliyor.

- **CEF çözümünde bu bilgiler Data Plane üzerinde tek bir satırda eşleşmiş şekilde depolandığı için Recursive LookUp yapılmasına gerek kalmıyor.**

- Alternatif olarak Recursive LookUp yapılmasının önüne geçebilmek için statik rota tanımlarında “**ip route <Destination Network Address> <Destination Subnet Mask> <Exit Interface Id> <Next Hop Ip Address> <Administrative Distance Value>**” şeklinde Exit Interface bilgisi de verilebiliyor. Bu tanım şekline **Fully Qualified IPv4 Static Route** deniliyor.
 - o L2’de PPP gibi Multi Access olmayan bir protokol kullanılıyorsa “**ip route <Destination Network Address> <Destination Subnet Mask> <Exit Interface Id> <Administrative Distance Value>**” şeklinde sadece Exit Interface tanımının yapılması yeterli oluyor. Buna **Directly Connected Static Route** deniliyor. Eklenen rota tanımı yönlendirme tablosuna Directly Connected olarak kaydediliyor (AD değeri 1 olarak kalmaya devam ediyor. Tanımda sadece Exit Interface bilgisi verildiği için bu şekilde kaydediliyor).
 - o L2’de Ethernet protokolü gibi Multi Access bir protokol kullanılıyorsa statik rota tanımında **sadece Exit Interface bilgisinin** verilmesi yeterli olmuyor. Sadece Exit Interface tanımı yapıldığında paketin gönderileceği arayüzde Next Hop Ip adres bilgisi bilinmediği için ARP sorgusu yapılamayacaktır. Dolayısıyla Next Hop Ip bilgisinin MAC adresi öğrenilemeyeceği için paket yönlendirilemeyecektir (**Proxy ARP** özelliği devrede değilse).

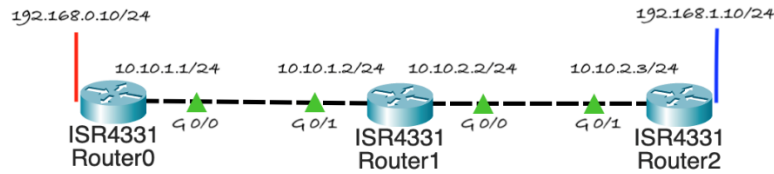
Proxy ARP

Statik rota tanımında normal şartlar altında Next Hop Ip adresi yerine Exit Interface tanımı yapıldığında komşu routerun ip adresi bilinmediği için ARP sorgusuyla hedef cihazın MAC adresinin öğrenilemediğinden bahsedilmişti. Statik rota tanımında Exit Interface tanımı yapıldığında Next Hop Ip adresi yerine **hedef network bilgisi yönlendirme tablosunda Directly Connected olarak kaydediliyor**. Bu durumda hedef networke iletilmek üzere paket gönderildiğinde router komşu routerun ip adresi bilinmediği ama yönlendireceği paketin hedef network adresi Directly Connected olarak görüldüğü için Exit Interface üzerinden hedef ip adresi için broadcast yayınla ARP sorgusu başlatacaktır.

Komşu router kaynak routerdan gönderilen paketi aldığı anda hedef network bilgisinin kendi yönlendirme tablosunda tanımlı olup olmadığını kontrol eder. Eğer ki ARP sorgusunda kullanılan hedef ip adresine erişebiliyorsa (yönlendirme tablosunda ilgili network için tanım bulunuyorsa) ARP sorgusu başlatan kaynak routerla kendi MAC adresini öğretmek hedef ip adresine kendisi üzerinden (Burada Proxy görevi görüyor) erişebilmesini sağlar (**Özetle routerun ARP sorgusu başlatan cihazın Default Gateway adresini bilmediğini düşünerek vekillik yaptığı durumudur**). Bu özelliğe **Proxy ARP** denilmektedir. Proxy ARP özelliğini aşağıdaki örnek üzerinden açıklamak gerekirse;

- 192.168.0.10 adresinden 192.168.1.10 adresine erişebilmek için Router0 üzerinde “**ip route 192.168.1.0 255.255.255.0 gig 0/0**” şeklinde bir statik rota tanımı yapılmıştır. Bu durumda 192.168.1.0/24 networkü Router0’ın yönlendirme tablosuna Directly Connected olarak kaydedilecektir.
- Router0, Router1’in G0/1 arayüzündeki ip adresini (Next Hop Ip adresini) bilmediği için ARP sorgusu yapamayacaktır. **Bunun yerine Router0 üzerinde 192.168.1.0/24 networkü G 0/0 arayüzüne Directly Connected olarak görüneceği için G 0/0 arayüzünden 192.168.1.10 ip adresi için ARP sorgusu (broadcast yayınla yapıyordu) başlatacaktır.**

- Router1, Router0'ın 192.168.1.0 networkü için başlattığı ARP sorgusunu aldığıında yönlendirme tablosunu kontrol ederek 192.168.1.0/24 networküne erişimi olup olmadığını kontrol eder. Erişimi olması durumunda (Static Route tanımı yapılmışsa) Router0'ın 192.168.1.0/24 networküne kendisi üzerinden erişebileceğini görüp Router0'a kendi G 0/1 arayüzündeki MAC adresini öğretir.
- Bu sayede 192.168.0.0/24 - 192.168.1.0/24 networkleri haberleştirilebilir (Router0'ın ARP tablosunda hedef ip adresine ulaşmak için gönderilecek arayüz bilgisi ve hedef MAC adresi görüntülenebilir).



| → Cisco routerlarda Proxy ARP özelliği varsayılanda açık gelebiliyor. İsteğe bağlı olarak Global konfigürasyon modunda **“no ip proxy-arp”** komutuyla devre dışı bırakılabilir.

| → Proxy ARP özelliği devrede olmaması durumunda statik rota tanımlarında sadece Exit Interface belirtilirse hedefe erişim sağlanamayacaktır. Bu nedenle Ethernet protokolü gibi Multi Access protokol kullanılan bağlantılarda sadece Exit Interface bilgisi kullanılarak statik rota tanımları yapılmamalıdır.

| → Proxy ARP özelliği çok eski cihazları desteklemek için varsayılanda devrede geliyor. Günümüzde yeni model switchlerde varsayılanda devrede gelmeyebilir.

| → Cisco cihazlarda herhangi bir portun altında Proxy ARP özelliğini açmak için ilgili portun arayüzü altına girilerek **“ip proxy-arp”** komutu kullanılabilir.

Proxy ARP özelliği, DHCP protokolünün olmadığı zamanlarda istemcilere (**Dummy Terminal**) sadece ip adresi öğretilabiliyordu. İstemciler gateway ve subnet gibi bilgilere sahip olmadığı için farklı bir networke erişmek istediğinde bulundukları network üzerinde hedef ip adresine ulaşabilmek için bir ARP sorgusu başlatır. ARP paketlerini alan ve hedef networke erişimi olduğunu gören routerlar ARP sorgusunu başlatan istemcilerin gateway adresine sahip olmadığını düşünerek hedef networklere erişebilmeleri için Proxy hizmeti yapılması için kullanılmaktaymış.

IPv6 Static Route

IPv6 protokolü için de Statik Route süreci IPv4 protokolüne benzer şekilde işlemektedir. Farklı olarak hedef ip adresi için GUA adres bilgisi kullanılırken Next Hop ip adres bilgisi iki farklı şekilde tanımlanabilmektedir. Bunlar;

- GUA adres kullanılması durumunda Next Hop ip adresi belirli bir networke dahil görüleceği için gönderilmesi gereken Interface anlaşılacaktır. Dolayısıyla Exit Interface bilgisine ihtiyaç duyulmadan paketler yönlendirilebilecektir.

- **Bir sonraki routerun Link-Local adresi tanımlanacaksa Exit Interface bilgisi de girilmek zorundadır.** Nedeni Link-Local adresler Private Ip'lerdir ve router üzerindeki her arayüzde aynı network aralığına sahiptir. Router paketleri hedef networklere yönlendirilirken hangi Interface'deki Link-Local ip adresini kullanarak göndereceğini bilmesi için Static Route tanımlarında Exit Interface bilgisinin de girilmesi gerekiyor (Örnek olarak "**ipv6 route 2001:DAB:0:2::/64 gig 0/0 FE80::2 5**" verilebilir "**ipv6 route <Dst GUA IPv6 Addr> (<Exit Int> <Next Hop Link-Local>) | (<GUA IPv6 Addr> <AD>)**").
 - o Bu durumda isteğe bağlı olarak bir routerun birden fazla arayüzüne aynı Link-Local ip adresi tanımlanabilir. Router'un her bir arayüzü kendi içerisinde ayrı bir network olacağı için herhangi bir ip çakışması yaşanmayacaktır (**Link-Local adreslere sahip paketler farklı networklere aktarılmazlar. Unutulmamalıdır ki Link-Local adresler sadece LAN içerisinde kullanılırlar**).
 - o IPv4'de yapıldığı gibi Static Route tanımında sadece hedef ip adresi ve Exit Interface bilgisi belirtilirse (Next Hop Link-Local adresi olmadan) bu durumda aynı şekilde yönlendirme tablosuna Static Route bilgisi eklenir ve Exit Interface olarak belirtilen arayüzden **NDP** sorgusu yapılır. Buradaki network içerisinde hedef ip adresi için ilgili cihazın MAC adresi bulunmuyorsa dönüş yapılamayacağı için paket Drop edilir (Adından da anlaşılacağı üzere Proxy **ARP** özelliği sadece IPv4 için geçerlidir).

Pv4 protokolünde hedefin MAC adresini öğrenebilmek için ARP protokolü (broadcast) kullanılıyordu. IPv6 protokolünde ise ARP protokolü yerine **NDP (Neighbor Discover Protocol)** protokolü kullanılıyor (IPv6 protokolünde broadcast yayın olmadığı için NDP protokolü Multicast yayınla gerçekleştiriliyor).

Notlar

- ARP tablosuyla MAC Address tablosu karıştırılmamalıdır.
 - o **ARP tablosunda** Ip-MAC adres eşlemesi tutulmaktadır.
 - o **MAC Address tablosunda** MAC-Port bilgisi tutulmaktadır.
- ARP tablosunu temizlemek için "**clear arp-cache**" komutu kullanılıyor.
- Router arayüzlerinde Link-Local adresi manuel olarak verebilmek için "**ipv6 address <Link-Local Address> link-local**" komutu kullanılıyor.
- IPv6 protokolünün kullanılabilmesi için hizmet alınan ISP'den IPv6 protokolünün devreye alınması talep edilmelidir.

Terminolojiler

- HDLC,
- PPP, kısaltmasından da anlaşılacağı üzere sadece bir noktadan bir noktaya erişim için kullanılan protokoldür.
- Multihop Frame Relay
 - o DLCI,
 - o <https://www.sysnettechsolutions.com/frame-relay-nedir/>
 - o <https://emre-ozel-2245.medium.com/frame-relay-4702cb423e35>
 - o <https://bidb.itu.edu.tr/sevir-defteri/blog/2013/09/07/frame-relay>

- **Layer 3-to-Layer 2 Mapping Table**, bu tanım ARP tablosu gibi L2 adreslerin L3 adreslerle eşleştirildiği tablolar için kullanılıyor. Tabi ki de bu tanım sadece ARP tablosu için geçerli değil. Frame Relay teknolojisinde kullanılan DLCI tablosu veya DMVPN (Dynamic Multipoint Virtual Private Network) teknolojisinde kullanılan tablosu gibi farklı çözümlerde de Layer 3-to-Layer 2 Mapping tablolar kullanılıyor.
- **Multipoint Frame Relay Network**, WAN üzerinde L2’de protokolü olarak kullanılan MultiAccess bir protokoldür. Ethernet protokolüne benzer şekilde çalışmaktadır (farklı L2 adresleme yapısı kullanır). Bu protokol için özel Frame Relay switch ve routerlar kullanılıyordu. Günümüzde aktif kullanılmamaktadır (zamanında almış ve altyapısını bozmak istemeyen firmalarda görülebiliyor).
- **MultiAccess Network**, bir kablodan çıkan bağlantı/veri birden fazla hedefe ulaşma şansına sahipse (yani PPP gibi gidebileceği tek nokta bulunmuyorsa) buna MultiAccess denir. Frame Relay ve Ethernet MultiAccess protokollerdir.
- **PBR (Policy Base Routing)**, her ne kadar yönlendirme tablosunda bir hedef network için bilinen rota tanımı bulunsa da paketlerin bu networke yönlendirilip yönlendirilmeyeceğinin kararının öncesinde belirlenmiş bir Politika kontrolü gerçekleştirilerek verildiği yapıdır. Fortigate, Palo Alto, Sophos gibi Firewall’lar bu doğrultuda çalışmaktadır.
 - Bu yapıya örnek olarak bir hedef networke ulaşmak için iki alternatif rotadan önceliği daha yüksek olan rotanın seçilmesi gerekirken Policy tanımıyla paketleri öncelik değeri daha düşük rota üzerinden gönderilmesi sağlanabiliyor.
- **Dummy Terminal**, hard disk donanımları olmayan (sadece RAM’leri var) sadece veri giriş çıkışı için kullanılan cihazlardır. Dolayısıyla herhangi bir veri işleme özelliği bulunmayan bilgisayar terminalidir (RARP protokolünü kullanıyorlar. Sadece ip adresini biliyorlar).

Kontrol Komutları

- Sh ip route <Ip Address>
 - Sh ip cef <Ip Address>
 - Data Plane’deki detaylarını görüntülemek için kullanılıyor
- Sh ip cef exact-route <Source Client Ip Address> <Destination Client Ip Address>
 - Kaynak ve hedef istemci arasında iletişim kurulabilmesi için CEF FIB tablosunda kayıt olup olmadığını kontrol etmek için kullanılıyor.
 - Yönlendirme tablosunda sadece hedef networklere ilişkin bilgiler tutulduğu için bu tür kaynak ip adresine yönelik sorgular yapılamaz.
- Sh ip arp
 - Data Plane’deki detaylarını görüntülemek için kullanılıyor
 - Router’a bağlı bütün networkler router üzerinden internete çıkacağı için networklerde bulunan her istemcinin ip ve MAC bilgisi router üzerinde mutlaka bulunur.
 - Bir anlamda router’a bağlı networklerin toplamda kaç istemciye sahip olduğu görüntülemek için de kullanılabilir.
 - Cisco cihazlarda ARP tablosuna eklenen bir Ip-MAC bilgisi 4 saat boyunca silinmiyor (ARP tablosu switchlerdeki MAC adres tablosuyla karıştırılmamalıdır).

MAC adres tablosu yani MAC-Port eşleniği 300 saniye sonunda trafik oluşturulmadığı takdirde siliniyordu).

- ARP tablosunu temizlemek için “**clear arp-cache**” veya “**clear ip arp <Ip Address>**” komutları kullanılabilir.
- Sh ip route {static | ospf | connected | bgp | <Ip Address> | ...}
- Sh ipv6 neighbors
- Sh adjacency detail

Yapılabilecek Uygulama Fikirleri

- SDN teknolojisi araştırılarak Eve-ng ortamında test edilebilir.
 - Python koduyla bu yapı üzerine uygulamalar yapılabilir.
- Router üzerindeki belirli süreçlerin otomatize kontrol edilebilmesi için bilgi çekilip kontrolünü sağlamak üzere scriptler yazılabilir.
 - https://web.itu.edu.tr/akingok/ulakcalistay09/Aranan_Kullanici_TespitiV11.pdf
 - <http://www.gokhanakin.net>
 - https://web.itu.edu.tr/akingok/ulakcalistay09/Aranan_Kullanici_TespitiV11Sunum.pdf
- L3 Loop uygulaması yapılabilir. Tracert çıktısı gözlemlenebilir.