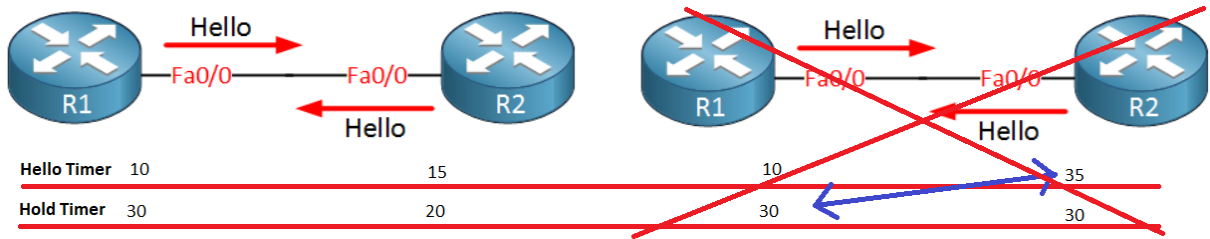


EIGRP - 3

Failure Detection and Timers

EIGRP protokolünde routerlar aralarında varsayılanda her 5 saniyede bir Hello paketi yollayarak ayakta olduklarını bildirir. 15 saniye boyunca Hello paketi gönderilmezse routerlar arası komşuluk koparılır. Bu süreler isteğe port bazında yeniden ayarlanabiliyor. **Diğer yönlendirme protokollerinden farklı olarak bu sürelerin karşılıklı portlar arasında aynı olması şartı aranmıyor (OSPF protokolünde aynı olmadığı takdirde komşuluk kurulmuyordu).** EIGRP protokolünde timer süreleri üzerinde düzenleme yapılırken dikkat edilesi gereken noktalardan birisi de Hello paketlerinin gönderildiği süre karşı routerun Hold Time süresinden daha kısa olmalıdır.



Timer sürelerini düzenlemek için Classic Mode EIGRP konfigürasyonunda ilgili portuna altına girildikten sonra “**ip hello-interval eigrp <AS Number> <Hello Time>**” ve “**ip Hold-time eigrp <AS Number> <Hello Time>**” komutlarıyla Hello Time ve Hold Time süreleri ayarlanabiliyor.

Named Mode EIGRP konfigürasyonu için EIGRP prosesi altında “**af-interface <Interface ID>**” komutuyla ilgili port konfigürasyon arayüzünün altına girilerek “**hello-interval <Hello Time>**” ve “**hold-time <Hold Time>**” komutuyla Hello Time ve Hold Time süreleri ayarlanabiliyor.

Convergence

Convergence, topolojide gerçekleşen bir değişimi topolojideki bütün routerların öğrenmesi için geçirilen süreye verilen isimdir. Alınan değişiklik bilgisine göre topolojideki bütün routerların rota bilgilerini yenide hesaplayıp yönlendirme tablosunu bu doğrultuda düzenlemiş haline ise buna Converged network deniliyor.

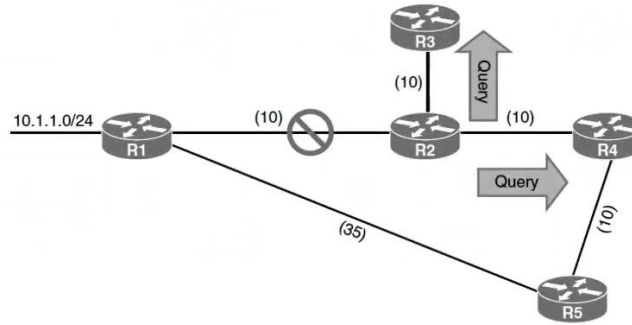
EIGRP protokolünde bir networke erişim için asıl hat olan Successor Route seçimi yapıldıktan sonra olası bir kesinti sonrasında hızlıca geçiş yapılabilecek alternatif yedek rotaları (Feasible Successor) da değerlendirip hazırda bekletiyordu. Bu hesaplamalar yapıldıktan sonra route **Passive mode’a** geçiş yaparak topolojide herhangi bir değişiklik meydana gelmediği sürece sorguda bulunmuyordu. Eğer ki hedef network için

kullanılabilecek rotalar arasından yedek hat olabilecek bir rota belirlenemediyse ve Successor Route seçilen bağlantı kesildiyse, bu durumda router tekrar **Active mode'a** geçiş yaparak hedef networke erişim için yeniden arayışa girecektir.

Router Active Mode'a geçiş yaptığında komşularına Query paketleri göndererek hedef networke erişim için alternatif bir rota tanımına sahip olup olmadığı sorgulanır (Rota hesaplama sürecinde Feasible Successor seçilme şartını karşılamayan rotalar mevcut olabilir. Bu rotalar değerlendirmeye alınacaktır). Aşağıdaki görsel üzerinden örnek vermek gerekirse;

- İlk aşamada R3 routerunun 10.1.1.0/24 networküne erişimi için R1 routeru üzerinden gidilen hat Successor router seçilecektir. R4 üzerinden gidilen hat Feasible Successor seçimi için gereken şartı sağlamadığından Feasible Successor seçilmeyecektir.
- Bu durumda R1-R2 arası bağlantı koparıldığında R2, 10.1.1.0/24 networküne yeniden erişebilmek için Active Mode'a geçerek komşusu olan R4 ve R3'e Query paketiyle 10.1.1.0/24 networküne erişim için alternatif bir rotaya sahip olup olmadığı sorulur. Bu durumda iki alternatif sonuç çıkabilir;
 - 1- Komşu routerlardan 10.1.1.0/24 networküne erişim için alternatif bir rota bilgisi bulunmayabilir. Bu **durumda komşu router 10.1.1.0/24 networküne erişimi olmadığını Reply paketi içerisinde Delay parametresini "Infinity" olacak şekilde gönderiyor.** Yani sonsuz gecikmeyle ulaşılabilir/erişimim yok demenin başka bir yolu.
 - 2- Aşağıdaki görsel üzerinden açıklamak gerekirse,
 - a- R2, R4'e 10.1.1.0/24 networküne erişim için alternatif bir rotaya sahip olup olmadığını sorgulamak için Query paketi gönderir (burada normalde R1-R2 arası bağlantı kesilmeden önce R4 de 10.1.1.0/24 networküne erişim için R2'yi kullanıyordu. Yani 10.1.1.0/24 networküne erişim için R2, R4'ün Successor Route'uydu).
 - b- R4, R2'den gelen bu sorguyla 10.1.1.0/24 networküne olan erişimin koptuğunu anlar ve R4'de R5'e Query paketiyle 10.1.1.0/24 networküne erişim için alternatif bir rotaya sahip olmadığını sorar (**Burada R4, R2 kesinti öncesinde Successor Route'u olduğu için 10.1.1.0/24 networkünden ötürü R2'ye tekrar Query paketi göndermiyor.**).
 - c- R5 routeru (R2-R3 arasında olduğu gibi burada da normalde R1-R2 arası bağlantı kesilmeden önce R5 de 10.1.1.0/24 networküne erişim için R3'ü kullanıyordu) da aynı şekilde Query paketiyle R1 routeruna 10.1.1.0/24 networküne erişim için alternatif bir rotaya sahip olmadığını sorar.

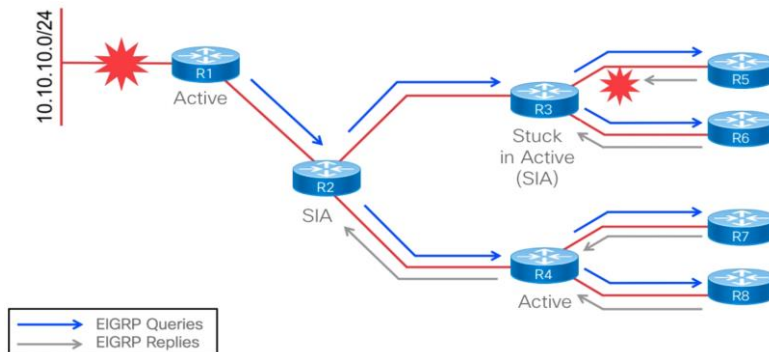
- d- Son durumda R1'den R5'e, R5'den R4'e ve R4'den R2'ye Reply paketiyle 10.1.1.0/24 networküne erişim için alternatif rota bilgisi olduğu parametreleriyle beraber paylaşılır. Bu doğrultuda hesaplamalar tekrar yapılarak tüm routerlar topoloji tablolarını ve yönlendirme tablolarını bu doğrultuda günceller.



NOT: Eğer ki R5 10.1.1.0/24 networküne R4, R2, R1 üzerinden değil de doğrudan R1 üzerinden gidiyor olsaydı (Yani R1-R5 arası bağlantının Metric değeri 35 değil de 25 olsaydı), R1-R2 arası bağlantı koptuğunda routerlar arasında gerçekleştirilen sorgu mekanizması R5'e geldiğinde R5, R1 routeru üzerinden 10.1.1.0/24 networküne erişimi olduğuna dair Reply paketi dönecekti (Yani R5, R1'e Query paketiyle 10.1.1.0/24 networküne erişimi olup olmadığını sormasına gerek kalmayacaktı).

Stuck in Active

Stuck in Active, eğer ki bir network için Feasible Successor bulunmuyorsa ve herhangi bir zamanda Successor Route üzerinde bir sorun yaşanmışsa (10.10.10.0/24 networküne erişim kesiliyor), router komşularına hedef networke ulaşmak için yönlendirme tablolarında herhangi bir rota tanımlı bulundurup bulundurmadığını Query paketi göndererek sorgular (Bu Query paketi aynı AS içerisinde bulunan bütün routerlara gönderiliyor). Bu sürede bütün routerlardan Reply paketi gönderilene kadar (bu networke erişmek için öğrenilen) hiçbir rota kullanılamıyor. **Query paketine AS bölgesi içerisindeki herhangi bir routerdan Reply yanıtı gelmezse maksimum 3 dk beklenir** (R5 Reply gönderemiyor). Eğer ki 3 dakika içinde herhangi bir routerdan Reply paketi gelmezse Routerun komşuluğu sıfırlanır (3 dakika sonunda R1 ile R2'in komşuluğu sıfırlanır).



Üzerinde hedef network için alternatif bir rota bulundurup bulundurmadığını sormak üzere gönderilen Query sorgusuna 3 dakika (180 saniye) içerisinde Reply paketi gönderilmezse mekanizmayı tetiklemek adına (gönderilen Query paketinin hedef router'a ulaşmamış olma ihtimaline karşın) bu sürenin yarısında (90. saniyesinde) SIA (Stuck in Active) Query paketi gönderilir. Bu süreçte de Reply paketi gönderilmezse komşuluk koparılıyor.

```
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

A 10.2.4.0/24, 0 successors, FD is 512640000, Q
  1 replies, active 00:00:01, query-origin: Local origin  *
    via 10.1.2.2 (Infinity/Infinity), Serial1
  1 replies, active 00:00:01, query-origin: Local origin
    via 10.1.3.2 (Infinity/Infinity), r, Serial3
Remaining replies:
  via 10.1.1.2, r, Serial0 DÖNÜŞ YAPILMAMIŞ
```

İsteğe bağlı olarak SIA Timer değeri değiştirilebiliyor. Bunun için Classic Mode konfigürasyonda EIGRP prosesi altında “**timers active-time <Minute>**” komutu kullanılırken, Named Mode konfigürasyonda “**topology base**” ve “**timers active-time <Minute>**” komutlarıyla düzenlenebiliyor (SIA Query süresi de burada verilen zamana göre).

```
R1(config)# router eigrp 100
R1(config-router)# timers active-time 2

R2(config)# router eigrp EIGRP-NAMED
R2(config-router)# address-family ipv4 unicast autonomous-system 100
R2(config-router-af)# topology base
R2(config-router-af-topology)# timers active-time 2
```

Stuck in Active durumuna önlem olarak iki seçenek uygulanabiliyor. Bunlar;

- 1- **EIGRP Summarization**, yönlendirme tablosundaki satır sayısını küçültüp yönetimini kolaylaştırmak için kullanılan tekniktir. Aşağıdaki görsel üzerinden açıklamak gerekirse R2 routeruna bağlı bütün networklerin R4 routeruna doğru erişim sağlanabilmesi için R2 routerunda, R1 ve R3 üzerindeki networklerin her biri için ayrı ayrı tanım yapmak gerekir (bu durumda R4 routerunun yönlendirme tablosunda 5 satır oluşur). Bunun yerine R2 routeru üzerinde R4 routeruna bütün networkü özetleyecek 172.16.0.0/16 gibi tek bir satır rota bilgisi anons edilmesi yeterli olacaktır. Bu sayede R4 routeru 172.16.0.0/16 networkünün tamamının R2 üzerinde olduğunu gösteren tek bir satır rota bilgisine sahip olacaktır. Rota özetlemenin Stuck in Active problemine etkisine bakıldığında, R4 routeru sadece 172.16.0.0/16 networkünün tamamının R2'ye bağlı olduğunu bilir. R1 veya R3 routerlarındaki 172.16.X.X/XX networküne erişimin kesilmesinden R4 routeru etkilenmez çünkü R2 routeru R4 routeruna 172.16.0.0/16 networküne kendisi üzerinden gidilebileceğinin anons etmiştir. R4 routeru 172.16.X.X/XX networklerine dair detaylarını bilmez. Dolayısıyla R4 routeruna bağlı diğer EIGRP routerları da bu durumdan etkilenmeyecektir.

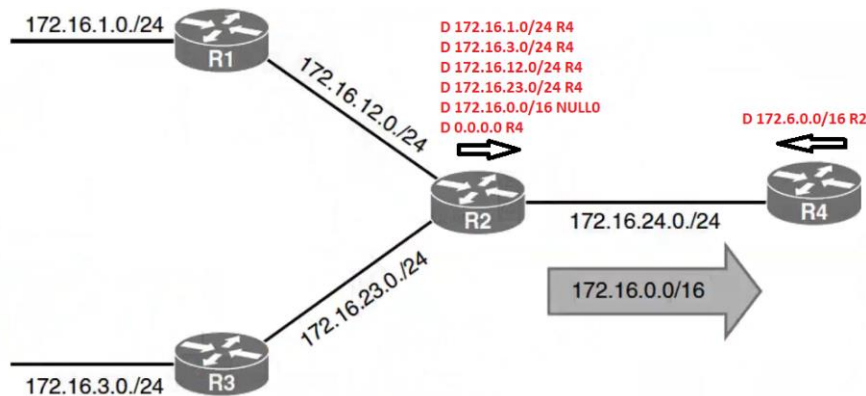
- a- Route Summarization, yönlendirme tablosundaki satırların sayısını azaltıp yönetimi kolaylaştırmakla beraber ACL tanımı gibi çözümlerde de kolaylık sağlıyor.
- 2- **EIGRP Stub**, konfigürasyonda tek çıkışlı routerlara “**eigrp stub**” komutu kullanılıyor. Bu sayede Query paketleri bu routerlara gönderilmiyor (R5, R6, R7, R8 gibi). Bu özellik sayesinde Stuck in Active olma ihtimali azaltılmış oluyor.

Some Summarization Problems

Summarization işleminin topolojiyi olumsuz etkileyen iki yanı bulunuyor. Olumsuz etkileyen ilk durum Loop riski oluşturmastır. Olumsuz etkileyen ikinci durum ise Summarization işlemi uygulandığında Summarization’a dahil olan bütün networkler tek bir satırla ifade ediliyor. Dolayısıyla bu kapsama dahil olan bütün networkler tek bir Administrative Distance ve Metrik değeriyle ifade ediliyor (Varsayılanda EIGRP’de özet anonsunda rotalar arasındaki en düşük metrik seçilir). Yani topolojide Summarization tanımına dahil edilen networklere gidilebilecek daha uygun bir rota bilgisi mevcut olsa dahi Summarization tanımının AD değeri 5 olduğundan daha performanslı rotalar tercih edilmeyecektir.

LOOP Reason

Summarization konfigürasyonunda Loop yapısının nasıl oluştuğu aşağıdaki görsel üzerinden açıklamak gerekirse, R2 routerunda 172.16.0.0/16 subnetine ait bütün networklerin kendisi üzerinde olduğunu belirtmek üzere R4 routeruna anons edecektir. Bu durumda R4 routeru, 172.16.0.0/16 networküne ait bütün paketleri R2 routeruna gönderecektir. R2 routeru üzerinde ise Default Route tanımı yapıldığında hedef adresi 172.16.50.0/24 gibi R2 üzerinde bulunmayan paketleri R4 routeruna gönderecektir. R4 routeru ise kendisine gönderilen 172.16.50.0/24 hedef ip adresine sahip paketi R2 üzerinde olduğunu öğrendiği için R2 routeruna gönderecektir. Bu durumda L3 Loop oluşacak ve paketler TTL değeri 0 olana kadar R2 ve R4 arasında yönlendirilip duracaktır. Bu durumun önüne geçilmek **özetleme yapılan her yerde mutlaka NULL0 arayüzüne yönlendirmek üzere Static Route tanımı eklenir**. EIGRP gibi bazı protokollerde Loop oluşumunu önlemek için bu tanım otomatik olarak ekleniyor.



Loop oluşumunu önlemek için oluşturulan NULL0 satırının çalışma şekline bakıldığında, R2 routerunun yönlendirme tablosunda 172.16.1.0/24, 172.16.3.0/24, 172.16.12.0/24 ve 172.16.23.0/24 için kayıtlar bulunacaktır. Bu tanımlara ek olarak **“ip route 17216.0.0 0.0.255.255 null0”** gibi bir komut kullanılarak yönlendirme tablosuna bir satır daha eklenecektir (EIGRP ve OSPF protokollerinde otomatik olarak ekleniyor. **Eklenen NULL0 rotasının Administrative Distance değeri 5 oluyor**). Bu durumda routera gelen paketler yönlendirilirken yönlendirme tablosundaki Best Matched Prefix Length değerine bakılarak belirleneceği için özetlenen ip aralığında bulunmayan (172.16.1.0/24, 172.16.3.0/24, 172.16.12.0/24 ve 172.16.23.0/24 dışında kalan 172.16.0.0/16 networkler) paketler bu satırla eşleşecek ve Drop edilecektir (172.16.0.0/16 satırıyla eşleşmeyen diğer paketler ise tanımlanmışsa Default Route satırıyla eşleşerek R4 routeruna gönderilecektir).

R4 routerunun yönlendirme tablosunda ise R2 üzerinde bulunan her bir 172.16.X.X/24 networkü için ayrı ayrı satır bulundurmak yerine 172.16.0.0/16 olacak şekilde tek bir satır bulunacaktır.

NOT: IPv6 protokolünde de Summarization işlemi yapılmak isteniyorsa mutlaka NULL0 rotası mutlaka yazılmalıdır (EIGRP ve OSPF protokollerinde otomatik olarak ekleniyor).

Summarization işlemi port bazında yapılır. Router sadece Summarization yaptığı port üzerinden bağlı olduğu komşu EIGRP routera özetlenen rotalar için anons yapar. EIGRP protokolünde **Summarization yapmak için Border Routerun** (Classic Mode) ilgili portunun altında **“ip summary-address eigrp <AS Number> <Summary Ip Address>”** komutunun veya (Named Mode) **“af-interface <Interface ID>”** ve **“summary-address <Summary Ip Address>”** komutlarının kullanılması yeterlidir.

|→ Varsayılanda rotalar arasındaki en düşük Metrik değeriyle Summarization anonsu yapılır. Summarization içerisine halihazırda olan rotalardan daha düşük Metrik değerine sahip bir rota eklenmesi durumunda Summarization anonsunun da Metrik değeri güncellenir. İsteğe bağlı olarak EIGRP prosesi altında **“summary-metric <Summary Ip Adress> <Subnet Mask> distance <Metric>”** komutuyla anons edilecek metrik değeri özelleştirilebiliyor.

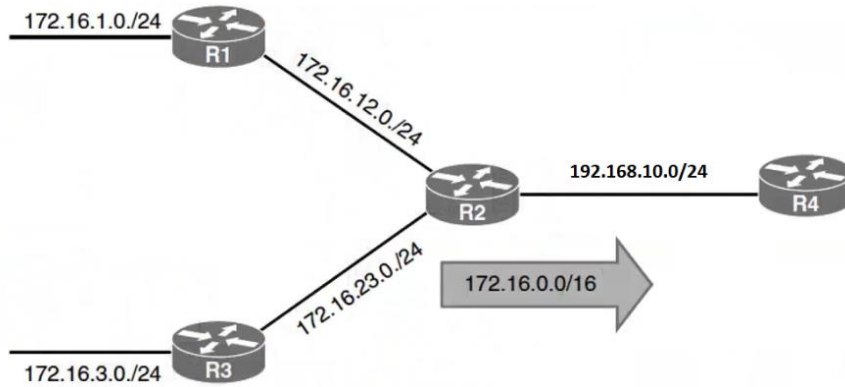
|→ Farklı olarak **“summary-metric <Summarization Ip Adress> <BW> <DLY> <RLY> <LD> <MTU>”** komutuyla Summarization tanımının metrik değerinin hesaplanabilmesi için parametrelerin karşı routera gönderilmesi de sağlanabiliyor.

```
router eigrp EIGRP-NAMED
address-family ipv4 unicast autonomous-system 100
af-interface GigabitEthernet0/4
ip summary-address eigrp 100 172.16.0.0/16 summary-address 172.16.0.0 255.255.0.0
```

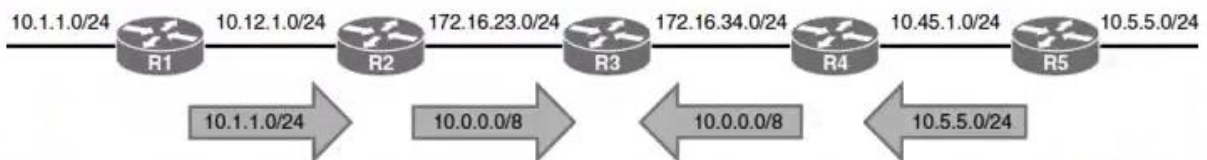
- Bir network bilgisinin Summarization tanını kapsamına girmesine rağmen ayrıca anons edilmesi gerektiği durumda **EIGRP Summarization Leak Map** tanımı kullanılabiliyor (detaylarına <https://networklessons.com/eigrp/eigrp-summary-leak-map> adresinden bakılabilir.).

Auto Summary

Classful adreslerin kullanıldığı zamanlarda her adres sınıfı Major Network olarak ifade ediliyordu. Auto Summary özelliği devrede olan routerlarda ise Major Network geçişlerinin olduğu router arayüzlerinde otomatik olarak Summarization yapılması sağlanıyordu. Aşağıdaki görsel üzerinden açıklamak gerekirse, R2 routerunun arkasındaki networkler 172.16.X.X/16 yani B sınıfı ip adresinden 192.168.10.0/24 yani C sınıfı networke geçiş yapıldığı anlaşıldıktan sonra R2 routerundan R4 routeruna otomatik olarak Summarization yapıp anons gönderecektir.



Auto Summary özelliği bazı routerlarda varsayılanda devrede gelebiliyor. Varsayılanda devrede gelmesi durumunda çeşitli sorunlara neden olabiliyor. Örnek olarak aşağıdaki görselde olduğu gibi R1 ve R2 routerunda bulunan 10.1.1.0/24 ve 10.12.1.0/24 networkleri A sınıfı adresler olduğu için R3 routeruna 10.0.0.0/8 olarak anons edilecektir. Benzer şekilde R5 ve R4 üzerindeki 10.54.1.0/24 ve 10.5.5.0/24 networkleri de A sınıfı adresler olduğu için R3 routeruna 10.0.0.0/8 olarak anons edilecektir. Dolayısıyla R3 routerunda 10.0.0.0/8 networküne ait iki farklı rota bilgisi gelecektir. Öğrenilen her iki rotanın da AD değerleri 5 olacağından Metrik değerleri de aynı anons edilirse R3 routeru 10.0.0.0/8 networküne gönderilecek paketleri R2 ve R4 arasında Load-Balance etmeye çalışacaktır. Dolayısıyla gönderilen paketlerin birisi R2 routeruna diğerini R4 routeruna gönderecektir. Bu gibi sorunlarla karşı karşıya kalmamak için routerlarda **Auto Summary özelliği varsayılanda açık gelmişse ve kullanılmayacaksa mutlaka kapatılması gerekmektedir.**



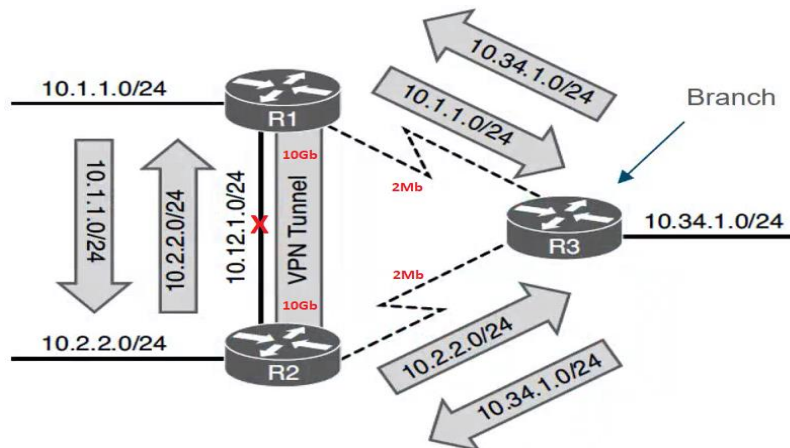
WAN Considerations

WAN Consideration çözümünü aşağıdaki topoloji üzerinden örnekendirerek açıklamak gerekirse, arasında yedeklenen R1 ve R2 üzerinde bulunan iki Data Center yapısı arasında 10Gbit VPN bağlantısı bulunmaktadır. R1 ve R2 routeru internete 2Mbit'lik bağlantılar üzerinden internete çıkmaktadır. Bu durumda;

- R1 ve R2 arasındaki VPN bağlantısı için kullanılan 10Gbit hatta bir kesinti olması durumunda R1 ve R2 EIGRP protokolüyle R3 üzerindeki 2Mbitlik hattın haberleşmeye devam etmek isteyecektir. Böyle bir durumda R3 routerunda R1 ve R2 arasında **Transit Area** olacaktır. Dolayısıyla R1 ve R2 routerları arasındaki haberleşme süreci 10Gbit hızdan 2Mbit hıza sahip bağlantı üzerinden sağlanmaya çalışıldığında R1 ve R2 routerunun internet için kullandığı 2Mbitlik hatlar satüre olur ve internete erişim sağlanamaz hale gelir (Bu nedenle, R1 ve R2 arasındaki VPN bağlantısının kurulduğu hatlarda bir kesinti meydana gelmesi durumunda Data Center'lerden birisinin devre dışı kalıp sadece tek bir DC'nin hizmet vermesi daha uygun olabilir).
- 1- Transit Area, iki bölgenin haberleşme sürecinde arada kalınması/ara cihaz olması anlamına gelmektedir.
- R3 routerunun 2Mbitlik bağlantısı üzerinden Transit Area olmaması için **EIGRP Stub** özelliği kullanılmalıdır.

EIGRP Stub

EIGRP Stub özelliği, tek çıkışı olan networke sahip routerlarda **varsayılanda** **sadece kendi üzerinde doğrudan bağlı bulunan rotaların ve Summarization ile öğrenilen rota bilgileri dışında hiçbir rota bilgisini öğretilmemesini** sağlayan özelliktir (Bu süreçte EIGRP ile anons edilen bütün rotaları öğrenmeye devam ediyor ama sadece öğretme sürecinde belirli rota bilgilerini öğretiyor). Bu özellik sayesinde, R3 routeru R1 ve R2'nin arkasındaki (10.1.1.0/24 ve 10.2.2.0/24 networkleri) networkleri öğrenecek ama bu rotaları R1 ve R2'ye öğretmeyecektir. Dolayısıyla R1 ve R2'nin arkasında haberleşme sürecini kendi üzerinden sağlanmasının önüne geçilerek Transit Area olmaktan kurtulacaktır.



- EIGRP Stub konfigürasyonu için EIGRP prosesi altında “**eigrp stub {connected | receive-only | redistributed | static | summary}**” komutunun kullanılması yeterli olacaktır. Komut yapısından da anlaşılacağı üzere rotaların öğrenilme şekline göre farklı rota bilgilerinin öğretilmesi de sağlanabiliyor. Varsayılanda sadece Directly Connected ve Summarization ile öğrenilen rotaların anons edilmesi sağlanıyor. Yukarıdaki topolojide ise bu komutun sadece R3 routerundaki EIGRP prosesi altında tanımlanması yeterli olacaktır.

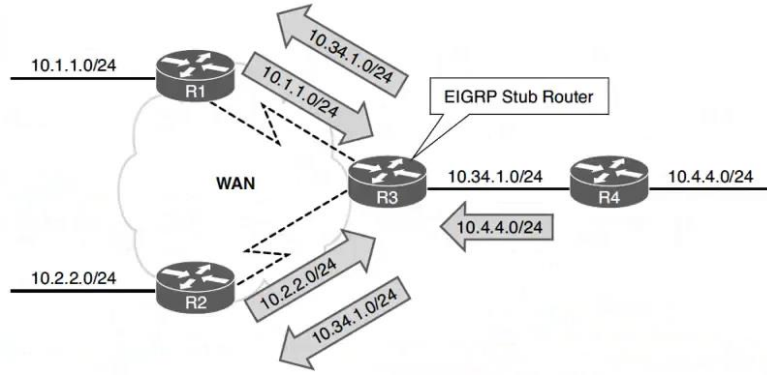
R3 (Classic Configuration)	R3 (Named Mode Configuration)
<pre>router eigrp 100 network 0.0.0.0 255.255.255.255 eigrp stub</pre>	<pre>router eigrp EIGRP-NAMED address-family ipv4 unicast autonomous-system 100 eigrp stub</pre>

- Eğer ki R3 routerunun da ucuna bir R4 routeru bağlanır ve R4 router üzerinden gelen (10.4.4.0/24) EIGRP anonslarının R1 ve R2 routerlarına öğretilmesi gerekebilir. R3 routeru üzerinde EIGRP Stub konfigürasyonu yapıldıktan sonra R4 üzerinden EIGRP protokolüyle öğreneceği networkleri R1 ve R2 ‘ye öğretmeyeceği gibi R1 ve R2’nin arkasında bulunan networkleri (10.1.1.0/24 ve 10.2.2.0/24 networkleri) de EIGRP protokolüyle R4 routeruna öğretmeyecektir. Bu gibi durumlar için EIGRP protokolünde **EIGRP Stub Site Feature** özelliği kullanılabiliyor.

EIGRP Stub Site Feature

EIGRP Stub Site Feature özelliği ile routerların belirli portlardan EIGRP protokolü ile öğrendiği rota bilgilerinin anons edilmemesi sağlanabiliyor. EIGRP Stub Site özelliğiyle, bir routerunun EIGRP protokolü üzerinden öğrendiği rotaları anons etmemesi gereken routerların bağlı olduğu portlar **WAN-Interface** olarak tanımlanıyor. Bu tanım sonrasında WAN-Interface olarak belirlenen portlar dışındaki portlara bağlı routerlardan EIGRP protokolü üzerinden gelen rota bilgileri anons edilmesi sağlanırken, WAN-Interface olarak belirlenen portlardan öğrenilen rota bilgileri yeniden anons edilmesinin önüne geçiliyor. EIGRP Stub Site özelliği aşağıdaki topoloji üzerinden açıklanmaya çalışıldığında, R3 routeru R4 routerundan EIGRP protokolü ile öğreneceği 10.4.4.0/24 networkünü R1 ve R2’ye de öğretmesi gerekmektedir. Bunun için;

- R3 routerunun R1 ve R2 arasında Transit Area olmaması gerekiyor. R3 üzerinde EIGRP Stub özelliği devreye alınırsa bu durumda R4 üzerinden öğrendiği rota bilgilerini de R1 ve R2 routerlarına anons edemeyecektir. Bu nedenle EIGRP Stub özelliği kullanılamıyor.
- R3 routerunda R1 ve R2 routerlarının bağlı olduğu portlar WAN-Interface olarak ayarladıktan sonra R1 ve R2 routerları üzerinden öğrendiği networkleri yeniden EIGRP protokolüyle anons etmezken, R4 routerundan EIGRP protokolü ile öğreneceği rotaları anons etmeye devam edecektir. Bu sayede R1 ve R2 routerları EIGRP protokolü üzerinden 10.4.4.0/24 networkünü öğrenebilecektir.



EIGRP Stub Site özelliği sadece Named Mode EIGRP konfigürasyonunda kullanılabiliyor. Konfigürasyonuna bakıldığında;

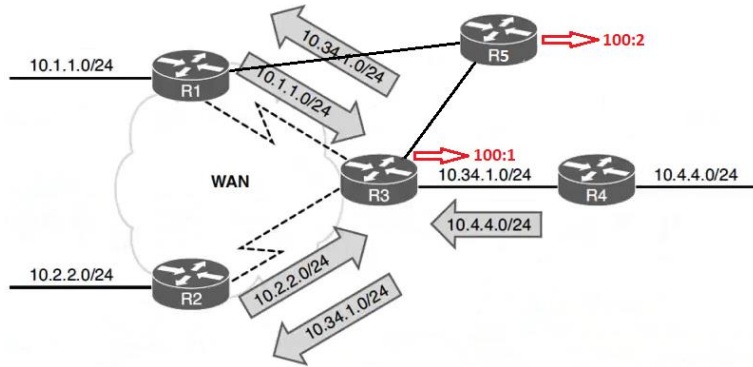
- EIGRP protokolüyle anons edilmeyecek portlar WAN-Interface olarak işaretlenmelidir. Bu işlem için “**af-interface <Interface ID>**” ve “**stub-interface wen-interface**” komutlarıyla ilgili port arayüzlerinin altında WAN-Interface tanımları yapılmalıdır.
- Son adımda EIGRP prosesi altında “**eigrp stub-site <AS Number>:<Identifier>**” komutuyla EIGRP Stun-Site özelliğinin çalışacağı AS numarası ve ID değeri belirtilmelidir.

```
R3
router eigrp EIGRP-NAMED
address-family ipv4 unicast autonomous-system 100
  af-interface Serial1/0
    stub-site wan-interface
  exit-af-interface
!
  af-interface Serial1/1
    stub-site wan-interface
  exit-af-interface
  eigrp stub-site 100:1
exit-address-family
```

EIGRP Stub Site konfigürasyonunda kullanılan **ID** tanımının kullanım amacına bakıldığında, topoloji üzerinde EIGRP Stub Site konfigürasyonu yapılan routerun anons edilmemesi gereken network bilgilerini başka bir bağlantısı üzerinden/portuna bağlı router üzerinden öğrenip anons edebilme ihtimali bulunuyor. Bunun önüne geçebilmek için anons edilmemesi gereken network bilgilerini öğrenme ihtimali bulunan routerlar arasında fiziksel veya sanal bir bağlantı olsa dahi EIGRP Stub Site konfigürasyonunda ID değerleri farklı verilerek bu routerlar ile arasında izolasyon sağlanıyor. Aşağıdaki görsel üzerinden açıklamak gerekirse;

- R5 routerunun R1 ve R3 routerlarına da bağlantısı bulunmaktadır. Böyle bir durumda R5 routeru R1 routerunun arkasındaki networkü öğrenip EIGRP protokolüyle R3 routeruna da anons etmek isteyecektir. R3 routeru R1 routerunun arkasındaki networkü öğrenip anons ederse R2 routeru trafiğini R3 üzerinden R1’e göndermek isteyecektir. R3 routeru Transit Area olacaktır.

- R3 routerunun Transit Area olmaması için R3 ile R5 routeru arasında bağlantı olmasına rağmen **R3 routerunun ID değeri 1, R5 routerunun ID değeri 2** seçilmesi durumunda R3 ile R5 arasında izolasyon sağlanacaktır. Dolayısıyla R3 routeru R1'in arkasındaki networkü R5 üzerinden öğrenip R2 ve R4'e anons etmesinin önüne geçilmiş olunacaktır (ID değeri farklı verilen routerlar birbirinden izole oluyor).
- Birbirine fiziksel veya sanal olarak doğrudan bağlı olmayan routerlar arasında ID değerinin bir önemi yoktur. Böyle bir durumla karşılaşılmadığı sürece routerlarda ID değeri 1 verilip geçilebilir.



EIGRP Stub konfigürasyonu aynı zamanda SIA durumunu azaltmak için kullanılan özelliklerden birisidir (bir diğeri de Summarization yapmaktır). EIGRP Stub konfigürasyonu ile routerların arkasında anons yapmasını gerektirecek bir network bilgisinin olmadığı belirtiliyor. Örnek olarak, R1 üzerindeki bir networke erişim kesildiğinde R1 routeru erişimi kesilen network için R3 routeuruna alternatif bir rotaya sahip olup olmadığını öğrenmek için Query paketi göndermiyor çünkü R3 routeru Stub olarak konfigüre edilmiş (EIGRP protokolüyle öğrendiği networkleri anons etmiyor). Bu sayede SIA durumunda kalma ihtimali azalmış oluyor (R1 routerunda “**show ip eigrp neighbors detail <Interface ID>**” komutuyla EIGRP Stub olarak ayarlanmış routera bağlı port detayları görüntülenmek istendiğinde Query paketlerinin baskılandığı görülebilir).

IP Bandwidth Percent

İp telefon gibi Real Time haberleşme sağlanan topolojilerde bu tür trafıklere öncelik verilmesi elzemdir. EIGRP protokolünde ise trafik türü ayırt edilmeksizin portların tamamı kullanılabilir. Dolayısıyla paketler bant genişliğini kullanırken Real Time çalışan cihazların bu durumdan en az şekilde etkilenmelerini sağlayabilmek için **IP Bandwidth Percent** özelliği kullanılabilir. IP Bandwidth Percent özelliği ile EIGRP protokolünde bir portun toplam bant genişliğinin hangi AS'in ne kadarlık oranda kullanabileceğinin belirlenebilmesini sağlayan özelliktir. Bu özellik varsayılanda devrede geliyor ve EIGRP protokolü ilgili portun %50'sini kullanabilir (Her port üzerinde hangi AS için % kaç kullanılabileceği ayrıca tanımlanabilir).

IP Bandwidth Percent konfigürasyonu için ilgili port altında “**ip bandwidth percent eigrp <AS Number> <Percent>**” komutunun kullanılması yeterlidir.

R1 (Classic Configuration)	R1 (Named Mode Configuration)
interface GigabitEthernet0/0	router eigrp EIGRP-NAMED
ip address 10.34.1.4 255.255.255.0	address-family ipv4 unicast autonomous-system 100
ip bandwidth-percent eigrp 100 25	af-interface GigabitEthernet0/0
	bandwidth-percent 25

Default Route Propagation

Diğer dinamik yönlendirme protokolünden farklı olarak EIGRP protokolü üzerinden Default Static rota bilgisinin öğretmek üzere kullanılan bir komut bulunmuyor. Bunun yerine **Default Route olarak paketlerin gönderilmesi istenen Router üzerinde**, Default Route tanımı (0.0.0.0/0) Static olarak tanımlandıktan sonra “**redistribute static**” komutuyla Static olarak öğrenilen network bilgisinin EIGRP protokolüne dahil edilip anons edilmesi sağlanıyor. **Bu teknikle Default Route bilgisi öğretilmek istendiğinde ilgili router üzerindeki tüm statik rotalar EIGRP protokolüyle anons etmeye başlayacaktır. Filter tanımlarıyla bütün statik rotaların öğretilmesinin de önüne geçilebiliyor** (<https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/200279-Configure-Default-route-in-EIGRP.html>).

Default Route tanımını EIGRP protokolü üzerinden anons edilmesini sağlamak için kullanılan ikinci bir **teknik ise Default Route olarak paketlerin gönderilmesi istenen router üzerinde EIGRP Summarization adres olarak 0.0.0.0/0 networkünü EIGRP protokolüyle öğretilmesi sağlanabilir**. Aşağıda IPv4 ve IPv6 için örnekler verilmiştir ama IPv4 için de aynı şekilde uygulanabilir.

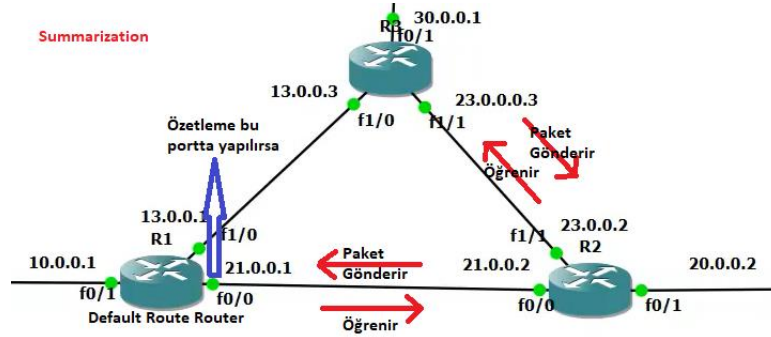
```
interface FastEthernet0/0
ip address 21.0.0.1 255.255.255.0
ip summary-address eigrp 10 0.0.0.0 0.0.0.0
duplex auto
speed auto
end
```

R2 (Classic Configuration)	R2 (Named Mode Configuration)
interface GigabitEthernet0/1	router eigrp CISCO
ipv6 eigrp 100	address-family ipv6 unicast autonomous-system 100
ipv6 summary-address eigrp 100 ::/0	af-interface GigabitEthernet0/1
	summary-address ::/0

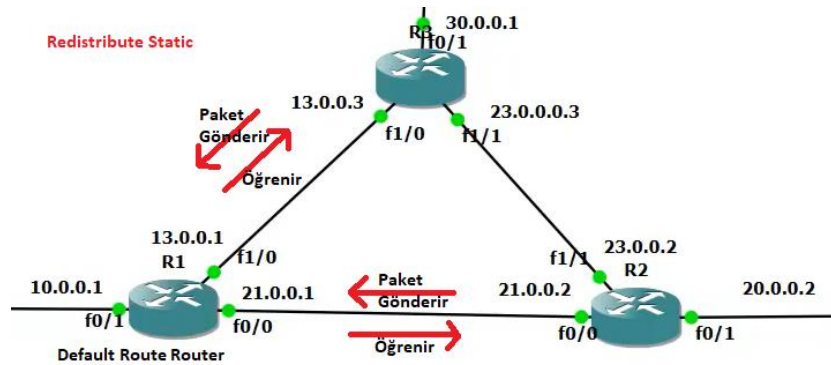
Redistribute Static ile EIGRP Summarization yöntemleriyle Default Route tanımının EIGRP protokolüyle anons edilmesi arasındaki fark ise EIGRP

Summarization işlemi port bazında yapılıyordu. Dolayısıyla EIGRP Summarization ile Default Route bilgisi öğretilmek istendiğinde topolojideki bütün routerlar Default Route tanımını ilgili routerun EIGRP Summarization yapılan tek bir portu üzerinden öğrenecektir. Bütün paketlerini de bu port üzerinden gönderecektir.

|→ Alternatif olarak EIGRP Summarization tanımı routerun tek bir portuna değil de bütün portlarına uygulanabilir. Bu durumda Redistribution Static yönteminde olduğu gibi bütün portlarından Default Route anonsunu EIGRP Summarization ile yapacaktır. Dolayısıyla tek porta bağlı kalınmayacaktır.



Redistribute Static yöntemiyle Default Route bilgisi öğretildiği takdirde router EIGRP çalışan bütün portlarından anons geçeceği için ilgili routerun EIGRP protokolü çalışan bütün portlarından paket almaya başlayacaktır.



NOT: Unutulmamalıdır ki, EIGRP Summarization ile Default Route bilgisi öğretilmek istendiğinde topolojideki EIGRP protokolü çalışan routerlara her bir network bilgisi ayrı ayrı öğretilmeden doğrudan Default Static Route tanımı öğretilecektir. Çünkü Default Static Route tanımı bütün networkleri kapsamaktadır. Yukarıdaki görsel üzerinden örnek vermek gerekirse R1 routerunun f0/0 ve f1/0 portlarında “**ip summary-address eigrp <AS Number> 0.0.0.0 0.0.0.0**” komutuyla EIGRP Summarization tanımı yapıldığında R2 ve R3 routerlarının yönlendirme tablosunda sadece doğrudan bağlı networkler için rota bilgisi bulunacaktır (Yani 10.0.0.1 networkünü R2 ve R3 ayrıca öğrenmeyecektir. EIGRP Summarization tanımı (0.0.0.0/0) 10.0.0.1 networkünü de kapsamaktadır. Bu nedenle ayrıca anons edilmez).

Notlar

- EIGRP protokolünde tanım şekline göre kullanılan 3 farklı Administrative Distance değeri bulunuyor. Bu tanımlara bakıldığında;

- 5, Summarization yapılan route üzerinde eklenen NULL0 rotasının AD değeridir.
- 90, EIGRP protokolü üzerinden öğrenilen rotalar için kullanılan AD değeridir.
- 170, Redistribution üzerinden öğrenilen rota bilgilerine verilen Administrative Distance değeridir.
- Eğer ki Default Route (0.0.0.0/0) tanımı EIGRP protokolü üzerinden öğretilmek isteniyorsa ve **Default Route Gateway (hedef network adresi bilinmeyen paketlerin yönlendirileceği) olacak router üzerindeki network bilgileri kolaylık olması açısından bütün portların anons edilebilmesi için “network 0.0.0.0”** komutuyla öğretilmişse, bu durumda her ne kadar **“ip route 0.0.0.0 0.0.0.0 <Next Hop Router>”** komutuyla default static route tanımı yapılmış olsa dahi Redistribute ile öğrendiği networke öncelik vermek yerine ,0.0.0.0/0 networkünü kendi üzerindeki bir network gibi öğretecektir (EIGRP prosesi altında **“network 0.0.0.0”** komutuyla tanımlanmış olduğu için). Dolayısıyla rota tanımının başında **D*EX** sembolüyle ifade edilip AD değeri 170 olması gerekirken **D** sembolüyle ifade edilip AD değeri 90 olacaktır.
 - Bu durumun düzeltilmesi için ilgili EIGRP prosesi altında **“no network 0.0.0.0”** komutu kullanıldıktan sonra her bir network teker teker **“network”** komutuyla tanımlanmalıdır.

```
D* 0.0.0.0/0 [90/30720] via 21.0.0.1, 00:02:41, FastEthernet0/0
    10.0.0.0/24 is subnetted, 1 subnets
D    10.0.0.0 [90/30720] via 21.0.0.1, 00:04:54, FastEthernet0/0
    13.0.0.0/24 is subnetted, 1 subnets
D    13.0.0.0 [90/30720] via 23.0.0.3, 00:04:54, FastEthernet1/1
    [90/30720] via 21.0.0.1, 00:04:54, FastEthernet0/0
    20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    20.0.0.0/24 is directly connected, FastEthernet0/1
L    20.0.0.2/32 is directly connected, FastEthernet0/1
```

```
D*EX 0.0.0.0/0 [170/30720] via 21.0.0.1, 00:00:03, FastEthernet0/0
    10.0.0.0/24 is subnetted, 1 subnets
D    10.0.0.0 [90/30720] via 21.0.0.1, 00:00:24, FastEthernet0/0
    13.0.0.0/24 is subnetted, 1 subnets
D    13.0.0.0 [90/30720] via 23.0.0.3, 00:00:24, FastEthernet1/1
    [90/30720] via 21.0.0.1, 00:00:24, FastEthernet0/0
    20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    20.0.0.0/24 is directly connected, FastEthernet0/1
L    20.0.0.2/32 is directly connected, FastEthernet0/1
```

Kontrol Komutları

- Show ip eigrp topology active
- Show ip eigrp topology <Network Address>/<Prefix Length>
- Show ip eigrp neighbors detail <Interface ID>
- Show ip eigrp interface detail