

EIGRP 5

Throubleshooting EIGRP for IPv4 Neighbor Adjavencies

EIGRP protokolünde gerçekleştirilmesi gereken ilk adım routerlar arasında komşuluk kurulmasıdır. Bu süreç 224.0.0.10 Multicast adresi üzerinden gerçekleştirilir. Routerlar aralarına Hello paketleri göndererek komşuluk kurma sürecini başlatırlar. Bu Hello paketlerinin içerisinde çeşitli parametreler bulunduruluyor. Bu parametrelerden bazıları komşu router tarafından kabul edilmediği sürece routerlar arasında EIGRP komşuluğu kurulmayacaktır. Bu ve benzeri durumlarda EIGRP komşuluğunun kurulamaması durumunda karşılaşılabilecek çeşitli durumlara bakıldığında;

- **Interface is Down**, çoğu zaman varsayılanda L3 portlar kapalı durumdadır. EIGRP komşuluğunun kurulabilmesi için komşuluk kuracak portu Up durumda olması gerekir.
 - o “**sh ip int bri**” portların L3 durumu hakkında bilgi verir.
- **Mismatched AS Number**, komşuluk kuracak routerların AS numaraları aynı olması gerekir. Farklı AS içerisinde tanımlanması durumunda komşuluk kurulmayacaktır.
 - o “**sh ip protocols**”, cihaz üzerinde çalışan bütün dinamik yönlendirme protokolleri hakkında detaylı bilgi gösterir.
 - o “**sh run | sec eigrp**”, çalıştırılan konfigürasyon dosyasında tanımlı eigrp konfigürasyonunu gösterir.
 - o “**debug eigrp packets**” eigrp protokolüne yönelik Debug başlatılarak, paketler kullanıldıkça konsol satırında logların görünmesini sağlamak sağlanabilir. İsteğe bağlı olarak belirli türdeki paketlerin görüntülenmesi için filtre uygulanabiliyor. Eğer ki karşı router farklı AS'den Hello paketi gönderiyorsa Debug çıktısında sadece router üzerinden gönderilen Hello paketleri olduğu görülür (karşı routerdan Hello paketleri gelmez). **Debug ile ilgili süreç tamamlandıktan sonra “no debug eigrp packets”, “undebug all” veya “no debug all” komutlarından birisiyle Debug'ın kapatılması gerekiyor.**
- **Incorrect Network Statement**, EIGRP protokolünde network adreslerini anons edilebilmesi için tanımların manuel olarak yapılması gerekiyordu (networkler 3 farklı şekilde tanımlanabiliyordu). Yanlış yapılan network tanımı sonrasında ilgili portta EIGRP protokolü başlatılmaz, network bilgisi de anons edilmez (“network” komutunun iki asli amacında bahsedilmişti. Bunlar, networkü anons edilmesi ve bu networkün kullanıldığı portta EIGRP protokolünü başlatmasını sağlamaktır).
 - o “**sh eigrp interfaces**”, EIGRP protokolünün hangi portlarda başlatıldığını ve bu süreçle ilgili portlarına bağlı kaç komşu EIGRP routerun bulunduğu gösterilmesi gibi çeşitli istatistikler gösterilir.

- **Mismatched K Values**, EIGRP protokolünde metrik hesabı K değerleri üzerinden yapılmaktadır. K değerleri sayesinde metrik değeri hesaplanırken hangi parametrelerin göz önünde bulundurulması gerektiği belirleniyordu (varsayılanda Band genişliği ve Delay parametrelerine bakılıyor). Varsayılanda gelen değişkenler dışında farklı parametrelerin de metrik hesabına dahil edilmesi için K değerleri devreye alınırsa, bu değişikliğin yapıldığı porta bağlı EIGRP routeurn portunda da uygulanması gerekiyor. Aksi takdirde K değerleri karşılıklı olarak uyuşmazsa komşuluk kurulmuyor (K değerleri Hello paketi içerisinde komşu routerla paylaşılıyor).
 - o “**sh ip protocols**”, cihaz üzerinde çalışan bütün dinamik yönlendirme protokolleri hakkında detaylı bilgi gösterir.
 - o “**sh run | sec eigrp**”, çalıştırılan konfigürasyon dosyasında tanımlı eigrp konfigürasyonunu gösterir.
- **Passive Interface**, EIGRP komşuluğu kurulması beklenmeyen portlarda (son kullanıcıya hizmet verilen portlar) EIGRP paketlerinin gönderilmemesi ve alınmaması için devreye alınan özelliktir (bu özellik, portlarda kimlik denetimi de açık değilse son kullanıcıların EIGRP protokolünü manipüle edememesi adına bir noktaya kadar güvenlik de sağlıyordu). Eğer ki routerun komşuluk kurulacak portu da Passive Interface olarak seçilmişse Hello paketleri gönderilmeyeceği için komşuluk kurulamayacaktır.
- **Different Subnets**, karşılıklı EIGRP çalışacak portlarda farklı networklere ait ip adresleri verilmişse bu durumda routerların bu portlar üzerinde komşuluk kurma şansı olmayacaktır.
- **Authentication**, router portları arasındaki iletişimin daha güvenli olması adına kimlik denetimi açılabilirdi. Kimlik denetiminde kullanılan Key tanımları router portlarında karşılıklı olarak aynı olmadığı takdirde routerlar arasında komşuluk kurulamayacaktır.
 - o “**sh key chain**”, router üzerinde bir anahtar zinciri oluşturulmuşsa bunu görüntülemek için kullanılıyor.
 - o “**sh ip eigrp interface detail <Interface ID>**” ilgili portta EIGRP protokolüne yönelik kullanılan özellikleri/konfigürasyonları ve istatistiklerinin detaylarını görüntülemek için kullanılıyor.
 - o “**sh run | sec eigrp**”, çalıştırılan konfigürasyon dosyasında tanımlı eigrp konfigürasyonunu gösterir.
- **ACLs**, routerlar üzerinde ACL tanımlarıyla filtre uygulanırken EIGRP protokolünde kullanılan paketler göz önünde bulundurulmamış olabilir. Bu durumda ACL’in uygulandığı portta EIGRP protokolü çalışmayabilir.
 - o “**sh ip interface <Interface ID>**”, EIGRP çalışan port altında ACL tanımı uygulanıp uygulanmadığı kontrol etmek için kullanılabilir.

- “**sh Access-list <ACL Nubmer | ACL Name>**”, port altında uygulanan bir ACL tanımı bulunuyorsa AC içerisinde tanımlı ACI’leri görüntülemek için kullanılmaktadır.
- ACL tanımlarında EIGRP protokolüne yönelik trafikleri temsil etmek Multicast IP adresini yazmak yerine doğrudan “**eigrp**” anahtar kelimesi kullanılabiliyor (aşağıdaki görselde EIGRP protokolüne yönelik trafikler hangi interface altında uygulanmışsa o portta bloklanacaktır). EIGRP protokolü, L3 başlığının arkasına gelen doğrudan bir 3. katman protokolüdür (dolayısıyla TCP veya UDP protokollerine bağlı çalışmamaktadır) (Farklı bir tanım şekli olarak EIGRP paketleri ip protokolü üzerinden hedef adresi 224.0.0.10 olan paketler için ACI yazılarak da ifade edilebilir).

```
R1# show access-lists 100
Extended IP access list 100
10 deny eigrp any any (62 matches)
20 permit ip any any
```

- **Timers**, EIGRP protokolünde timer tanımları absürt verilmediği sürece EIGRP protokolünde komşuluk kurulabiliyor. Dikkat edilmesi gereken noktalardan birisi de router portlarında karşılıklı olarak Hello Interval sürelerini Hold Interval sürelerinden yüksek tanımlanmış olmaması gerekiyor. Absürt tanıma örnek vermek gerekirse;
 - Eğer ki R1 portunda Hello interval 10, Hold Interval 30 verilmişken, R2 portunda Hello Interval 35, Hold Interval 105 gibi bir değer verilmişse, bu durumda routerlar arasında komşuluk kurulsada dahi her 30 saniyede bir komşuluk koparılıp yeniden kurulmaya çalışılacaktır.
 - “**sh ip eigrp interface detail <Interface ID>**” ilgili portta EIGRP protokolüne yönelik kullanılan özellikleri/konfigürasyonları ve istatistiklerinin detaylarını görüntülemek için kullanılıyor.

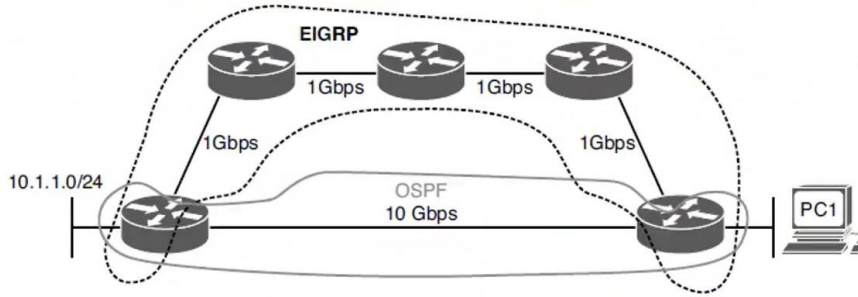
Throubleshootinh EIGRP for IPv4 Routes

EIGRP protokolünde komşuluk kurulduktan sonra hesaplanan rotalar üzerinde sorun giderme süreci başlıyor. Bu süreçte karşılaşılabilecek yaygın problemlere bakıldığında;

- **Bad or Missing Network Command**, network bilgisi eksik veya yanlış girilmiş olabilir. Bu durumda network bilgisi EIGRP protokolüyle anons edilmeyecektir.
- **Better Source of Information**, bilindiği üzere EIGRP protokolünde kullanılan 3 farklı AD değeri bulunuyor (5 -> Summarization, 90 -> EIGRP, 170 -> Redistribute) network bilgisi AD değeri daha düşük olacak şekilde EIGRP protokolü dışında

harici bir dinamik yönlendirme protokolüyle, doğrudan bağlı veya statik rota tanımıyla öğrenilmiş olabilir. Bu durumda aksi bir konfigürasyon yapılmadığı sürece ilgili networke erişim için EIGRP protokolüyle öğrenilen rota tercih edilmeyecektir. EIGRP protokolüyle öğrenilen rota “**Suboptimal Routing Occurs**” olarak bekletilecektir.

- “**sh ip route <IP Address> <Subnet Mask>**” ilgili network için tercih edilen rota bilgisini görüntülemeyi sağlıyor.
- **Aşağıdaki görselden de anlaşılacağı üzere her ne kadar OSPF protokolüyle öğrenilen rotanın bant genişliği daha yüksek olsa da EIGRP protokolünün AD değeri daha düşük olduğu için EIGRP protokolüyle öğrenilen rota tercih edilecektir. Bu gibi durumlara da en kaliteli hattın seçilmesi sürecine müdahale edilmesi gerekecektir.**

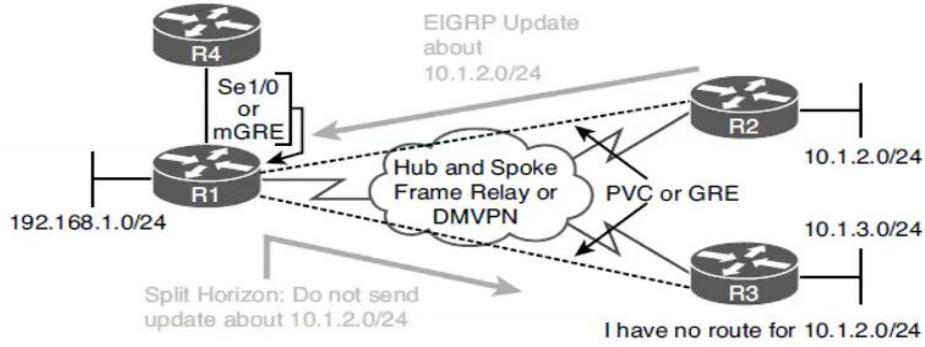


- **Route Filtering**, ilgili network için doğrudan bağlı olduğu router üzerinde veya networke erişim sürecinde üzerinden geçilmesi gereken routerların birisinde Route Filtering tanımı yapılmış olabilir. ACL tanımıyla hata yapılmış olabilir. Bu durumda ilgili networkün EIGRP protokolü üzerinden öğrenilmemesi veya anons edilmemesi engellenecektir (Distribution List'te kullanılan ACL tanımı doğru yazılmamış olabilir, Distribution List tanımı doğru yönde, doğru arayüze uygulanmamış olabilir, Offset List tanımı uygulanmış olabilir).
- “**sh ip protocols**”, cihaz üzerinde çalışan bütün dinamik yönlendirme protokolleri hakkında detaylı bilgi gösterir.
- “**sh run | sec router eigrp**”, çalıştırılan konfigürasyon dosyasında tanımlı eigrp konfigürasyonunu gösterir.
- “**sh Access-list <ACL Nubmer | ACL Name>**”, port altında uygulanan bir ACL tanımı bulunuyorsa AC içerisinde tanımlı ACI'leri görüntülemek için kullanılmaktadır.
- “**sh ip prefix list**”, “**sh route-map**” Prefix List ve Route Map tanımlarını gösterir.

```
R1# show run | section router eigrp
router eigrp 100
  distribute-list 10 in GigabitEthernet1/0
  network 10.1.1.1 0.0.0.0
  network 10.1.12.1 0.0.0.0
  passive-interface GigabitEthernet0/0
```

|→ Distribution List tanımından da anlaşılacağı üzere filtre tanımı sadece Gi 1/0 portuna uygulanmıştır.

- **EIGRP Stub Configuration**, ilgili networkün bulunduğu router üzerinde veya ilgili networke erişim sürecinde geçilen routerların birisinin üzerinde EIGRP Stub konfigürasyonu uygulanmış olabilir (SIA ihtimalini düşürmek için Stub konfigürasyonu yapılmak istenmiş olabilir). Bu durumda EIGRP Stub özelliği devreye alınan routerda EIGRP protokolüne üzerinde öğrenilen rotalar geçirilmeyeceği için ilgili networklere erişim kesilebilir.
 - **“sh ip neighbor detail”** komşu routerların EIGRP Stub süreçleri hakkında bilgileri görüntülemek için kullanılıyor.
- **Interface is Shut Down**, ilgili network için doğrudan bağlı olduğu router üzerinde veya networke erişim sürecinde üzerinden geçilmesi gereken routerların birisinin portu kapatılmış olabilir. Dolayısıyla ilgili networke erişim için alternatif bir rota bilgisi bulunmaması durumunda erişim kesilecektir.
 - **“sh ip int bri”** portların L3 durumu hakkında bilgi verir.
- **Split Horizon**, Distance Vector algoritmasını kullanan dinamik yönlendirme protokollerinde Loop oluşumunu önlemek için kullanılan özelliktir (tereciye tere satma !!!). Bir network bilgisini öğrendiği porttan tekrar anons edilmesinin önüne geçmek için kullanılıyordu (fiziksel port altında Sub-Interface tanımları varsa Split Horizon özelliğinden etkilenmez. Sub-Interface’ler arasında network bilgisi anons edilebilir). DMVPN veya Frame Relay (tek port üzerinde Sub-Interface tanımları oluşturularak bu durum atlatılabiliyordu) gibi tek port üzerinden birden fazla bağlantı sağlanıyor olabilir. Bu durumda Split Horizon özelliği de devredeyse (varsayılanda devrede gelmektedir) bu türden Hub-And-Spoke yapılarda EIGRP protokolüyle network bilgileri anons edilemeyecektir.
 - **“sh ip interface <Interface ID>”** ilgili port üzerine detaylı bilgi görüntülemek için kullanılıyor.
 - **“sh ip eigrp interface detail <Interface ID>”** EIGRP protokolüne yönelik portlar üzerinde detayları görüntülemek için kullanılır.
 - Router üzerinde Split Horizon özelliği **“no ip split-horizon”** komutuyla kapatıldığında RIP ve EIGRP protokolü için kapatılacaktır. **“no ip split-horizon eigrp”** komutuyla kapatıldığında sadece EIGRP protokolü için kapatılacaktır.

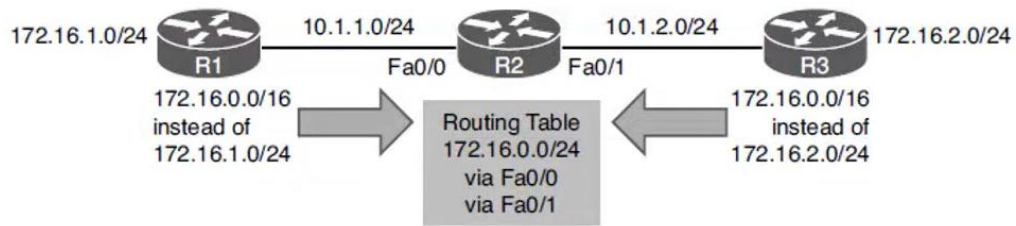


Throubleshooting Miscellaneous EIGRP for IPv4 Issues

- EIGRP protokolünde kullanılacak rota seçimi yapılırken alternatif rota bilgileri de göz önünde bulundurularak aktif seçilen rota üzerinde bir sorun olması durumunda doğrudan en hızlı şekilde yedek rotaya geçiş yapılabilmesi için alternatif rotalar da göz önünde bulundurularak uygunluğu kontrol ediliyordu. Bu doğrultuda kullanılacak rota belirlenirken aynı zamanda uygun olan alternatif rotalar da Feasible Successor/yedek rota olarak belirleniyordu. Bu rotalar **Pre-Calculates Paths** olarak da biliniyor. Yedek rota seçim sürecinde dair kontroller için aşağıdaki komutlar kullanılabilir.
 - o “**sh ip eigrp topology**” EIGRP protokolü üzerinden öğrenilen rotaların Feasible Distance ve Reported Distance değerlerini, ilgili network için Feasible Successor seçilip seçilmediği gibi parametrelerini görüntülemek için kullanılıyor (Successor Route seçilen rotanın Reported Distance değeri ile alternatif olan rotaların Feasible Distance değeri karşılaştırılarak Feasible Successor seçilip seçilmeyeceğine karar veriliyordu). Ek olarak bu komut kullanılarak Redistributed edilmiş rotalara dair bilgiler de görüntülenebiliyor.
 - o “**sh ip eigrp topology all-links**”, Feasible Successor seçilen, seçilmeyen **EIGRP protokolü ile öğrenilen bütün rota bilgilerini** görüntülemek için kullanılıyor (alternatif rota olup Feasible Successor seçilmeyen alternatif rota bilgilerini de listeliyor).
- EIGRP Auto Summarization, EIGRP protokolü üzerinden öğrenilen Major rota bilgilerinde ilgili routerun arkasında belirli sınıfa ait ip bloğuna dair birden fazla rota bilgisi bulunması durumunda, ip sınıfının değişiklik gösterdiği noktaya kadarki network bilgilerinin değişiklik gösterilen ilgili routerun portunda otomatik olarak özetlenmesini sağlayan özellikti. Geçmiş notlarda da bahsedildiği üzere bu durum topolojilerde kullanılan ip atamalarının düzenli yapılmaması durumunda çeşitli bağlantı sorunlara neden olabiliyordu. Auto Summarization özelliği varsayılanda IOS Version 15’ten sonra kapalı geliyor (bu durum cihazlarda kullanılan işletim sistemine göre değişiklik gösterebiliyor). Açık gelmesi

durumuna karşın kontrol edilip kapatılması, özetleme yapılması gerektiği durumda bu işlemin manuel yapılması daha sağlıklı olacaktır. Bu süreçte kontrol edilebilecek birkaç doneye bakıldığında;

- Auto Summarization açık kalmış olabilir.
- Manuel Summarization yapılmış ama doğru port altında yapılmamış olabilir.
- Doğru AS değerine özetleme yapılmamış olabilir.
- Doğru network bilgileri için Summatization yapılmamış olabilir.
 - “sh ip protocols”, cihaz üzerinde çalışan bütün dinamik yönlendirme protokolleri hakkında detaylı bilgi gösterir (Auto Summarization durumu ve manuel Summarization yapıp yapılmadığı görüntülenebiliyor).



|-> R1 de R3 de 172.16.0.0/16 networkünün üzerinde olduğunu Auto Summarization özelliğiyle R2 routeruna anons edecektir. R2 her iki routerun da birbirine bağlı olduğunu düşünerek trafiği R1 ve R3 arasında Load-Balance etmeye çalışacaktır. Dolayısıyla paketlerin birisi hedefe ulaşırken diğeri ulaşmayacaktır.

- Summarization sürecinde Loop oluşumunu engellemek için Null0 arayüzüne doğru rota tanımı yapılması gerektiği unutulmamalıdır. EIGRP ve OSPF protokollerinde bu tanım otomatik olarak gelmektedir.
- Metrik değerleri eşit olan rotalar arasında Load-Balance yapılabiliyordu. Bu durum varsayılanda aynı networke giden 4 rota bulunuyorsa, bu rotalar arasında Load-Balancing yapılabiliyordu (Metrik değeri eşit 5 rota bulunsa dahi 5. Rota Load-Balancing sürecine dahil edilmiyordu). İsteğe bağlı olarak “” komutuyla da 4’den fazla rota arasında da Load-Balancing yapılabilmesi sağlanabiliyordu.
- EIGRP protokolünde diğer yönlendirme protokollerinden farklı olarak Metrik değerleri eşit olmayan rotalar arasında da “**Variance**” adı verilen değer kullanılarak Metrik değerleri arasında belirli bir katsayıya kadar rotalar arasında Load-Balancing işlemi yapılması sağlanabiliyordu.
- **Bir network adresi için alternatif hatlar olsa dahi bu hatlar Feasible Successor seçilmemiş ise alternatif rotalar Variance değeriyle belirtilen katsayıyı sağlansa dahi Load-Balancing işlemine dahil edilmez (Feasible Successor seçilme şartı Loop oluşmadığını garanti etmek için kullanılıyordu. Bu şartı sağlamayan alternatif rotalar Loop riski oluşturacağı için Load-Balancing sürecine dahil edilmiyor).**

Notlar

- Cihaz üzerinde varsayılanda loglar Console ekranına düşmez. Logların konsol ekranına düşmesi için “**terminal monitor**” komutunun kullanılması gerekiyor. Sorun giderme sürecinde veya konfigürasyon yapılırken uygulanan tanımların sonucunda cihaz üzerinde bir değişiklik meydana geldiğinde, bu değişikliğin konsol ekranına log düşürmesi sağlanır.
 - Çok daha öncesinde yaşanan bir problemin kayıtlarını görüntülemek için “**sh logging**” komutu kullanılabilir.
- **Debug komutları routerlarda dikkatli kullanılması gereken komutlardan birisidir. Cihazı çatlatabilir.**
 - Açılan tüm Debug’ları kapatmak için “**no debug all**” veya “**undebug all**” komutlarıyla kullanılabilir.

Terminolojiler

- **Discontiguous Network**, bir Major networkten başka bir Major networke geçiş yapılan duruma verilen isimdir.