BGP-3

BGP Route Filtering and Manipulation

Her dinamik yönlendirme protokolünde olduğu gibi BGP protokolünde de filtreleme işlemi önemli konulardan birisidir. Filtreleme işlemi dört farklı şekilde gerçekleştirilebiliyor. Bunlar;

1- **Distribution List**, bir ACL tanımı yapılır (burada Extended ACL tanımıyla Subnet maskesi aralığının nasıl olacağı belirtiliyordu). Bu tanımlar BGP prosesi altında "**neighbor <IP Address> distribute-list <ACL Number/Name> (in | out)**" komutuyla hangi komşu BGP routerdan gelecek rota tanımlarından hangi rota bilgilerinin (ACL içerisinde tanımlanan) öğrenilmesi/öğrenilmemesi istendiği belirtiliyor. Eğer ki tanım "**in"** yönündeyse bu rotaların öğrenileceği yönde uygulandığı anlaşılır. Eğer ki tanım "**out**" yönündeyse bu ACL içerisindeki rota tanımlarının öğretilecek yönde uygulandığı anlaşılır.

```
R1
ip access-list extended ACL-ALLOW
 permit ip 192.168.0.0 0.0.255.255 host 255.255.255.255
 permit ip 100.64.0.0 0.0.255.0 host 255.255.255.128
!
router bgp 65100
 address-family ipv4
  neighbor 10.12.1.2 distribute-list ACL-ALLOW in
```

|→ ACL tanımının ilk satırında 192.168.X.X subnetiyle tam olarak eşleşen network bilgileri temsil edilmiş.

|→ ACL tanımının ikinci satırında 100.64.X.0 ip adreslerinin /24-/25 aralığındaki prefix değerleriyle eşleşen network bilgileri temsil edilmiş.

|→ Distribution List tanımına bakıldığında 10.12.1.2'den gelecek rota bilgilerinde sadece ACL ile belirlenen networklerin öğrenilmesi istendiği belirtilmiş. Sonuç olarak aşağıdaki gibi bir çıktı olacaktır (10.12.1.0/24 kendi üzerinde olduğu için filtrelenmez).

```
R1# show bgp ipv4 unicast | begin Network
     Network          Next Hop            Metric LocPrf Weight Path
*>   10.12.1.0/24     0.0.0.0                  0         32768 ?
*>   100.64.2.0/25    10.12.1.2               22             0 65200 ?
*>   100.64.3.0/25    10.12.1.2               22             0 65200 65300 300 ?
*>   192.168.1.1/32   0.0.0.0                  0         32768 ?
*>   192.168.2.2/32   10.12.1.2               22             0 65200 ?
*>   192.168.3.3/32   10.12.1.2             3333             0 65200 65300 ?
```

2- **Prefix List**, bir ACL tanımı içerisinde doğrudan veya Regex ifadeler kullanılarak belirli ip ve subnet tanımlarının oluşturularak filtreleme yapılmasına imkân tanıyan yöntemdir. Tanımının nasıl yapıldığı bir sonraki yazıda detaylıca açıklanmıştır. Prefix-List tanımı yapıldıktan sonra ilgili BGP prosesi altında "**neighbor <IP Address> prefix-list <Prefix List Name> (in | out)**" komutuyla komşu routerun ip adresi belirtilerek uygulanmaktadır.

```
R1(config)# ip prefix-list RFC1918 seq 5 permit 192.168.0.0/13 ge 32
R1(config)# ip prefix-list RFC1918 seq 10 deny 0.0.0.0/0 ge 32
R1(config)# ip prefix-list RFC1918 seq 15 permit 10.0.0.0/7 ge 8
R1(config)# ip prefix-list RFC1918 seq 20 permit 172.16.0.0/11 ge 12
R1(config)# ip prefix-list RFC1918 seq 25 permit 192.168.0.0/15 ge 16
```

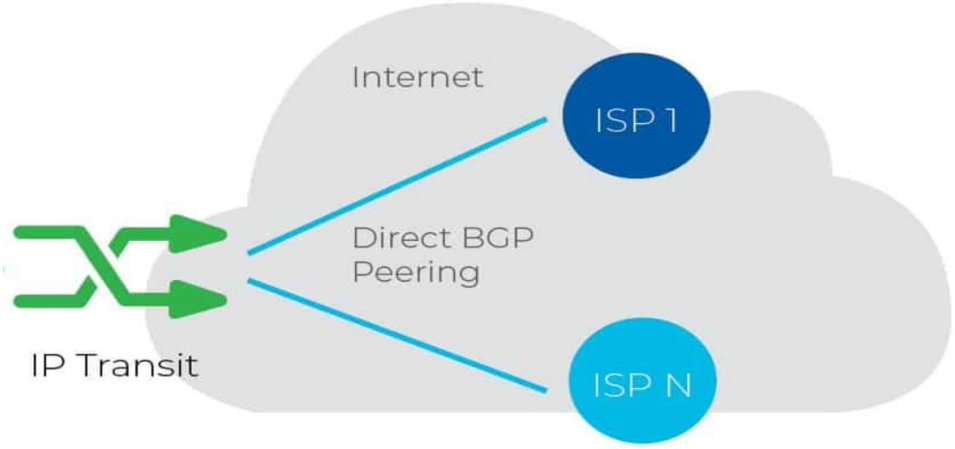
3- **AS Path ACL/Filtering**, diğer 3 fltreleme yönteminden farklı olarak burada rota bilgilerine bakılmaksızın sadece AS değerleri baz alınarak filtreleme yapılmasına imkân veren yöntemdir. Bu sayede birkaç satır tanımla bir ISP'nin veya ülkenin bütün trafiği filtrelenebiliyor.

AS Path Filter tanımı için "**ip as-path Access-list <Sequence Number> (permit | deny) <AS Paths>**" komutuyla Regex kullanılarak bir tanım oluşturulur. Bu tanım BGP prosesinin altında "**neighbor <Neighbor BGP Router IP Address> filter-list <AS Path Filter Sequence Number> (in | out)**" komutuyla komşu BGP router üzerinden gelecek AS değerleri filtreleniyor.

```
ip as-path access-list 1 deny _4$
ip as-path access-list 1 permit .*

router bgp 3
 neighbor 10.2.2.2 remote-as 1
```

ISP yedekliliği için iki farklı ISP hattı kullanıldığında Kurumun BGP routeru bir ISP'den öğrendiği AS değerlerini diğer ISP'ye öğretecektir. Dolayısıyla ISP routerlarına AS değerlerini kendi üzerinden öğrettiği için ISP trafiklerini kedi üzerinden ISP'ler arasında taşıyacaktır. Bu durumda kurum routeruna **Transit Area** denilir. Bir sonraki yazıda detaylı olarak açıklanacaktır.



Bu noktada kurum routerunun Transit Area olmaması için ISP routerlarına sadece kurum networkündeki networkleri öğretmesi için filter tanımı yapılması gerekiyor. BGP routerunda sadece kurum networklerini anons edilmesi için "**ip as-path acess-list <Sequence Number> permit ^$**" tanımı gerekiyor. Bu tanım BGP prosesi altında "**neighbor <Neighbor BGP Router IP Address> filter-list <AS Path Filter Sequence Number> out**" komutlarıyla komşu BGP routerlara doğru uygulandığında ISP'ler üzerinden gelecek AS değerleri öğrenilirken bu AS değerleri Implicit Deny satırıyla eşleşeceği için ISP routerlarına anons edilmeyecektir (Yani sadece Origini kendi olan rotalar anons edilecektir).

```
R1(config)#ip as-path access-list 1 permit ^$

R1(config-router)#neighbor 192.168.12.2 filter-list 1 out
R1(config-router)#neighbor 192.168.13.3 filter-list 1 out
```

4- **Route Maps**, BGP protokolünde rota tanımlarını filtrelemek için kullanılan yöntemlerden birisidir. Diğer 3 filtreleme yönteminden farklı olarak Route Map tanımları rotaların Attribute değerleri üzerinde değişiklikler yapılabilmesine de imkân veriyor. Bu sayede rotalar üzerinde manipülasyonlar yapılabiliyor.

Route Map tanımının nasıl yazıldığı bir sonraki bölümde detaylı bir şekilde açıklanmaya çalışılmıştır. Birkaç örnek vermek gerekirse;

```
ip prefix-list FIRST-RFC1918 permit  192.168.0.0/15 ge 16
ip as-path access-list 1 permit _65200$
ip prefix-list SECOND-CGNAT permit 100.64.0.0/10 ge 11
!
route-map AS65200IN deny 10
 description Deny any RFC1918 networks via Prefix List Matching
 match ip address prefix-list FIRST-RFC1918
!
route-map AS65200IN permit 20
 description Change local preference for AS65200 originate route in 100.64.x.x/10
 match ip address prefix-list SECOND-CGNAT
 match as-path 1
 set local-preference 222
!
route-map AS65200IN permit 30
 description Change the weight for AS65200 originate routes
 match as-path 1
 set weight 65200
!
route-map AS65200IN permit 40
 description Permit all other routes un-modified
!
router bgp 65100
 address-family ipv4 unicast
  neighbor 10.12.1.1 route-map AS65200IN in
```

|→ ilk Route Map tanımında RFC1918 isimli Prefix List tanımıyla eşleşen (Prefix List tanımındaki Permit edilen adresler için uygulanacaktır) rota tanımlarının **engellenmesi** sağlanmış (192.168.0.0/15-16 arasındaki networkler).
|→ İkinci Route Map tanımında SECON-CONAT isimli Prefix List tanımıyla eşleşen ve AS-Path değeri 1 olan rota tanımlarında **Local-Prefence değerinin 222 olarak set** edilmesi sağlanmış.
|→ Üçüncü Route Map tanımında AS-Path değeri 1 olan rota tanımlarının **Weight değerinin 56200 olarak set** edilmesi sağlanmış (ikinci satırsa AS-Path değeri ve Prefix List değeri eşleşmesi durumunda çalışacaktır. Yani Prefix List değeri eşleşmediği takdirde aşağıdaki satırlarla eşleşip eşleşmediği kontrol edilmeye devam edilecektir).

|→ Son Route Map tanımında ise **Implicit Deny satırını boşa düşürmek için tüm rota bilgilerine izin verilmiştir.** Bu satır tanımlanmadığı takdirde burada tanımlanmayan bütün rota tanımları Deny edilecektir.

BGP Prosesini Sıfırlamak/Temizlemek

BGP protokolü Timer değerleri yüksek olduğu tanımlanan değişikliklerin uygulanması zaman alabiliyor (Dolayısıyla yavaş çalıştığı söylenebilir). Bu nedenle BGP protokolü üzerinde yapılan bir tanımlamanın yanlış olup olmadığı konusunda tereddütler oluşabiliyor. Bu durumda da "**clear ip bgp (<Ip Address> | <Peer Group Name> | *) [soft {in | out}]**" komutuyla BGP prosesi sıfırlanarak bütün sürecin yeniden başlatılması sağlanabiliyor.

BGP prosesinin sıfırlanması demek BGP protokolü üzerinden öğrenilen bütün komşulukların ve rota bilgilerinin silinerek BGP protokolünün yeniden başlatılması demektir. Bu işlem sonrasında BGP protokolünün yeniden oturması (rotaların öğrenilmesi, hesaplamaların yapılması) uzun sürecektir. Aynı zamanda bu süreçte BGP protokolüyle birbirine bğlanan bütün routerlar bu güncellemeyi alacak, dolayısıyla etkilenecektir.
|→ Belirli aralıklarla BGP tablosu sıfırlanan (BGP prosesini sıfırlayan)/bağlantısı gidip-gelen routerların anonsu belirli bir süreliğine engellenmesi için ISP tarafında tanımlar yapılabiliyor. Örnek olarak 30 dakika içerisinde 5 defa BGP tablosu sıfırlanan routerun 30 dakika boyunca anons yapılması engellenebiliyor.
|→ Hali hazırda olan komşuluklar kopmadan BGP prosesini sıfırlamak için "**soft**" anahtar kelimesi kullanılıyor (BGP tablosu tek yönlü düzeltiliyor). Bu anahtar kelime kullanılarak BGP komşuları bağlantıyı yeniden başlatırken, rotaların yeniden hesaplanmasını sağlar. Özetle, "**clear bgp * soft {in | out}**" komutuyla Router komşuluklarını koparmadan komşu BGP routerun BGP tablosunu göndermesini talep ediyor.

|→ Özetle "in" anahtar kelimesi kullanılarak BGP prosesi sıfırlandıysa, router komşu/Peer BGP routerdan tekrar BGP tablosunu kendisine göndermesini ister. Bu doğrultuda routerda sadece giriş yönünde/gelen rotalar için filtre yazılmışsa, komut uygulandıktan sonra komşu/Peer BGP routerdan yeniden anonslar tekrar geleceği için giriş yönündeki filtreler yeniden çalışmış olur. Dolayısıyla sadece in yönünde uygulana filtreler doğrultusunda BGP tablosu güncellenmiş/değiştirilmiş oluyor.

BGP Load-Sharing

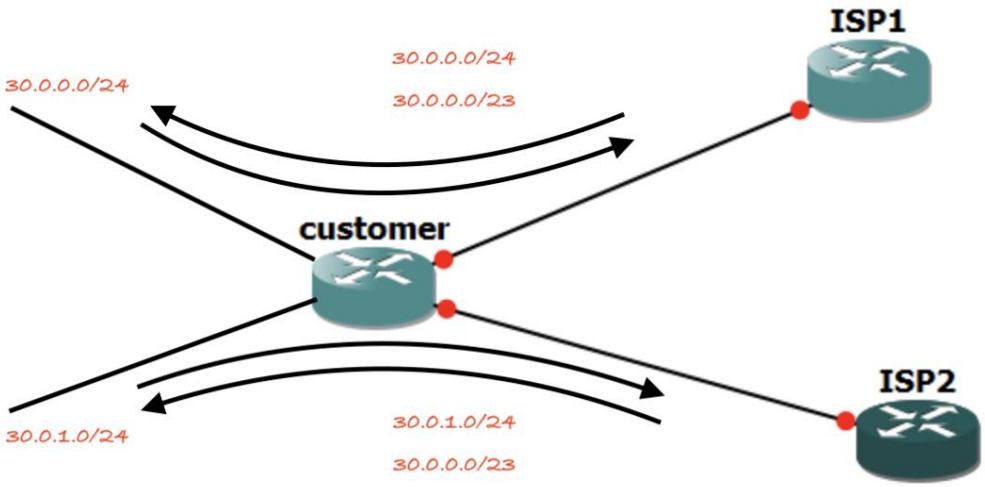
IGP protokollerinde bant genişliği gibi belirli bir kriterler doğrultusunda bu kararlar verildiği için en iyi hatlar doğrudan seçiliyor. Referans alınan rotalar aynı olduğu için Download işlemleri de Upload işlemleri de aynı hat üzerinden gerçekleşir. BGP protokolünde Path Selection kriterlerinin fazla olmasından dolayı Download ve Upload işlemleri farklı rotalar üzerinden gerçekleştirilebilir. Dolayısıyla BGP protokolünde Upload ve Download işlemleri iki farklı süreç olarak karşımıza çıkıyor.

Normal şartlarda çift ISP hattı kullanılan networklerde BGP protokolü doğası gereği yük paylaşımı yapmaktadır. BGP protokolü bu işlemi temelde rota belirleme sürecinde

kullandığı Path Selection parametreleri doğrultusunda gerçekleştiriyor. Dolayısıyla BGP protokolü için tanım yapıldığında aslında bir noktaya kadar ISP yedekliliğinin yanında Load-Sharing de sağlamış oluyor.

ISP yedekli bir yapıda Load-Sharing sağlayabilmek için BGP routerun iç bacağında iki farklı Subnet kullanılarak farklı ISP routerlar üzerinden internete çıkması sağlanabiliyor. Örnek olarak aşağıdaki örnekte olduğu gibi BGP routerun iç bacağında 30.0.0.0/24 ve 30.0.1.0/24 olacak şekilde iki farklı subnet tanımı kullanılarak 30.0.1.0/24 networkünün ISP 1 üzerinden, 30.0.1.0/24 networkünün ISP 2 üzerinden anons edilerek internete çıkması sağlanabiliyor

- Burada unutulmamalıdır ki bu şekilde dahi tam olarak bir Load-Sharing sağlanmış olmuyor. Sonuç olarak trafik bu subneti kullanan kullanıcı yoğunluğuna göre değişiklik gösterecektir.
- Buraya kadar ki uygulanan kısımla aslında ISP yedekliliği sağlanmıyor (ISP 1 hattı kesilirse 30.0.0.0/24 networkü ISP 2'den anons edilemediği için internet bağlantısı kesilecektir).
- ISP yedeğini sağlamak için her iki ISP hattı için de **Summary Route** tanımı yapılıyor (30.0.0.0/23 – 2 C CLASS sınıf birleştirilmiş oluyor). Bu sayede ISP'lerden birisinin bağlantısı kesildiğinde (Örneğin ISP 1) üzerinden anons edilen subnet tanımı diğer ISP üzerinden (ISP2) Summary Route tanımı içerisinde anons edildiği için ilgili subnet (30.0.0.0/24) kalan tek ISP (ISP 2) üzerinden internete çıkmaya başlayacaktır.
    - ÖZETLEME YAPILIRKEN UNUTULMAMASI GEREKEN NOKTALARDAN BİRİSİ DE ÖZET TANIMDA BULUNAN AMA KARŞIĞILI OLMAYAN ROTALARIN DROP EDİLMESİ İÇİN SUMMARY ROUTE TANIMINI "**NULL0**" ARAYÜZÜNE YÖNLENDİRMEK ÜZERE İKİNCİ BİR ROTA TANIMI YAPILMASI GEREKTİĞİDİR. Aksi takdirde iBGP protokolü üzerinde bulunmayan bir rota tanımını anons etmeyecektir.
- Burada yapılan sadece Kurumun Download (ISP'den gelen) yönündeki trafiği için Load-Sharing sağlanacaktır. Unutulmamalıdır ki kurumun kullandığı subnetlerden trafik oluşturulduğunda bu trafiğin hangi ISP hattından gönderileceğine dair bir tanımlama yapılmamıştır. Dolayısıyla Upload yönünde de Load Sharing sağlayabilmek için farklı tekniklerin uygulanması gerekmektedir.



- Kurum networkünün Upload yönündeki trafik üzerinde Load-Sharing yapabilmek için **PBR (Policy Based Routing)** tanımları kullanılabilmektedir. PBR tanımı yönlendirme sürecinde kullanılan yönlendirme mekanizmasının dışına çıkılarak paketlerin neye göre yönlendirileceğini belirlemek için kullanılmaktadır.
    - Kurumun Upload yönündeki trafiği üzerinde Load-Sharing yapabilmek için gelen paketlerin kaynak ip adreslerinin baz alınarak trafiği yönlendirilmesi sağlanıyor. Yukarıdaki topoloji üzerinden açıklamak gerekirse; kaynak ip adresi 30.0.0.0/24 networkünden geliyorsa ISP1'in bulunduğu hatta yönlendirilmesi, 30.0.1.0/24 networkünden geliyorsa ISP2'in bulunduğu hatta yönlendirilmesi için tanım yapılıyor (benzer şekilde trafiklerin port bazında hangi ISP'ye yönlendirileceğine dair tanımlamalar da yapılabiliyor).

Accumulated IGP and BGP

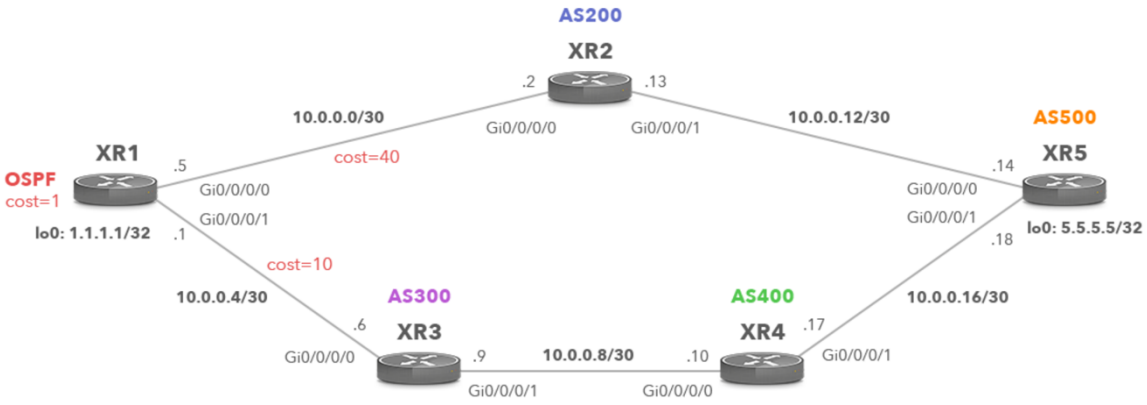
BGP protokolündeki Path Attribute değerleri göz önünde bulundurulduğunda aslında BGP protokolünün bant genişliğini pek de göz önünde bulundurmadan sağlıklı olan ilk rotayı belirleyerek trafikleri yönlendirdiği görülebiliyor. Bu durumda BGP protokolünde rota belirleme sürecinde bant genişliğinin de göz önünde bulundurarak karar verebilmesi gerektiği durumlarda kullanılmak üzere **Accumulated IGP and BGP** çözümü geliştirilmiştir.

BGP protokolü IGP protokollerinin (EIGRP, OSPF…) metrik değerlerini göz önünde bulundurarak rota seçimi yapması sağlanabiliyor (bu özellik aynı AS içerisindeki routerlar arasında olabildiği gibi AS'ler arasında karar verme mekanizmasında da uygulanabiliyor). Accumulated IGP and BGP kavramı ise IGP protokollerinin metrik değerleriyle BGP protokollerinin bütünleştirilmesi sonucu ortaya çıkmıştır.

- AS'ler arasında OSPF, EIGRP gibi IGP protokollerinin anonsları yapılmaz çünkü BGP Internet ortamında kullanılan Standart protokoldür. IGP protokolleri AS'ler arası kullanılmak istendiğinde AS'ler arasında farklı IGP protokolleri kullanılacaktır. Bu durum protokoller arasında rota aktarım sürecinde sorunlara neden olacaktır.

Accumulated IGP and BGP özelliği, varsayılanda devrede gelmemektedir. Bu özellik devreye alındığında ilgili metrik değerleri BGP protokolündeki anons paketlerinin içerisine Attribute olarak yerleştiriliyor ve komşu AS routerlara dahi anons ediliyor. Bu sayede BGP routerlar arasında IGP protokollerinin metrik değerlerinin göz önünde bulundurulması sağlanarak karar verilmesi sağlanabiliyor. Accumulated IGP and BGP özelliği devreye alındığında BGP protokolündeki karar verme mekanizması aşağıdaki gibi olmaktadır;

1- **Weigth**.
2- **Local Preferences**
3- **Local Originated**
4- **Accumulated Interior Gateway Protocol (AIGP)**
5- **ShortestAS_Path**
6- **Origin Type**
7- **MED (Multi-Exit Discriminator) Attribute**

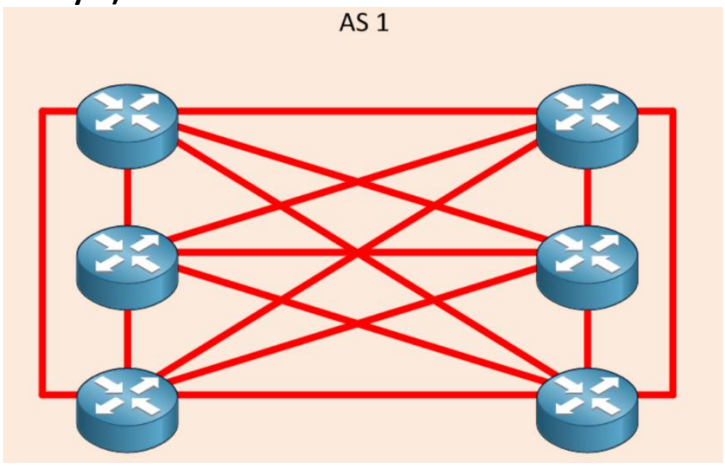


Accumulated IGP and BGP yapısı her ne kadar internet ortamında kullanılmasa da büyük kurumlarda veya bir ISP firmasının içerisinde BGP protokolü kullanılıyorsa ve BGP protokolünde kullanılan karar mekanizmasına IGP protokollerinde kullanılan Metric değerinin de eklenerek rota seçiminde değerlendirilmesi istendiği durumlarda Accumulated IGP and BGP özelliği kullanılabiliyor.

BGP protokolünün karar mekanizması olarak IGP protokollerine kıyasla daha yavaş ama daha kontrollüdür.

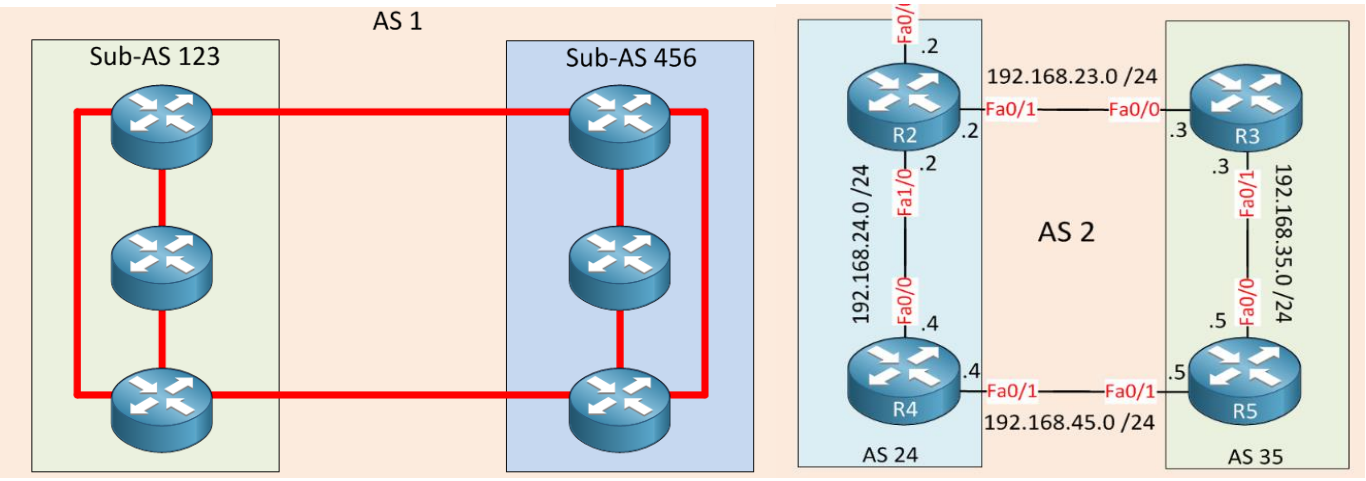
Techniques for Reduce Connection Count in IBGP

Normal şartlarda IBGP protokolünde paketler sadece 1 hop uzağa gönderilebiliyordu (**Aynı AS içerisinde Loop oluşup oluşmadığı anlaşılamadığı için routerlar sadece 1 hop uzağa paket gönderilebiliyordu. Dolayısıyla IBGP kullanılan topolojilerde Full Mesh bir yapı kurulamak zorundaydı).**



BGP Confederation

IBGP protokolünde Mesh yapı oluşturmaya gerek kalmadan Peer BGP routerların tamamının haberleşebilmesini sağlamak için **BGP Confederation** çözümü geliştirilmiştir. **BGP Confederation** çözümü, IBGP çalışan topolojide alt AS (Sub AS) tanımları oluşturarak topolojinin bir kısmının EBGP temelinde çalışmasını sağlayıp ihtiyaç duyulacak fiziksel bağlantı sayısını düşürmeyi amaçlamaktadır.




```
R4(config)#router bgp 24
R4(config-router)#bgp confederation identifier 2
R4(config-router)#bgp confederation peers 35
R4(config-router)#neighbor 2.2.2.2 remote-as 24
R4(config-router)#neighbor 2.2.2.2 update-source loopback 0
R4(config-router)#neighbor 5.5.5.5 remote-as 35
R4(config-router)#neighbor 5.5.5.5 update-source loopback 0
R4(config-router)#neighbor 5.5.5.5 ebgp-multihop 2
```

```
R3(config)#router bgp 35
R3(config-router)#bgp confederation identifier 2
R3(config-router)#bgp confederation peers 24
R3(config-router)#neighbor 2.2.2.2 remote-as 24
R3(config-router)#neighbor 2.2.2.2 update-source loopback 0
R3(config-router)#neighbor 2.2.2.2 ebgp-multihop 2
R3(config-router)#neighbor 5.5.5.5 remote-as 35
R3(config-router)#neighbor 5.5.5.5 update-source loopback 0
```

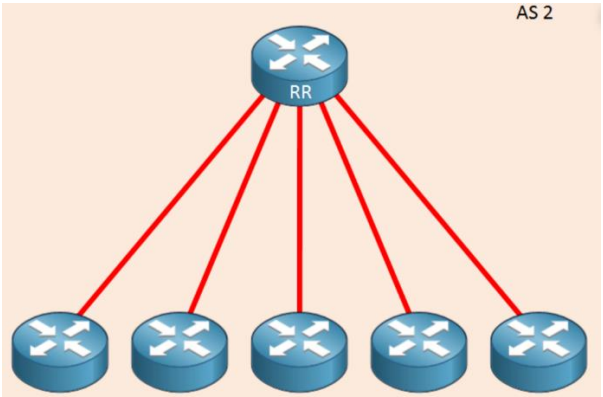
```
R2(config)#router bgp 24
R2(config-router)#bgp confederation identifier 2
R2(config-router)#bgp confederation peers 35
R2(config-router)#neighbor 4.4.4.4 remote-as 24
R2(config-router)#neighbor 4.4.4.4 update-source loopback 0
R2(config-router)#neighbor 3.3.3.3 remote-as 35
R2(config-router)#neighbor 3.3.3.3 update-source loopback 0
R2(config-router)#neighbor 3.3.3.3 ebgp-multihop 2
```

```
R5(config)#router bgp 35
R5(config-router)#bgp confederation identifier 2
R5(config-router)#bgp confederation peers 24
R5(config-router)#neighbor 4.4.4.4 remote-as 24
R5(config-router)#neighbor 4.4.4.4 update-source loopback 0
R5(config-router)#neighbor 4.4.4.4 ebgp-multihop 2
R5(config-router)#neighbor 3.3.3.3 remote-as 35
R5(config-router)#neighbor 3.3.3.3 update-source loopback 0
```

Route Reflector

Route Reflector, IBGP protokolünde Mesh yapıyı sağlamak için ihtiyaç duyulan bağlantı sayısını düşürmek için geliştirilen çözümlerden bir diğeridir. **Route Reflector** çözümü, OSPF protokolündeki DR router gibi tek bir vekil router (Route Reflector) seçilerek bütün Peer BGP routerların tek bir Peer BGP routerdan öğretilmesi sağlanabiliyor.

- Route Reflector seçilen router üzerinde bir sorun oluşması durumunda IBGP protokolünün sağlıklı çalışmaya devam edebilmesi için de Route Reflector seçilen routerun yedeklenmesi gerekiyor. Aksi takdirde IBGP protokolü çalışmayacaktır.
- Cluster ID değeri belirlenir. BGP Routerlar Peer BGP route bilgilerini sadece Domain içerisindeki Route Reflector seçilen routerdan alır.



Notlar

- Eğer ki bir network routerun kendi üzerindeyse BGP tablosunda o rotanın AS PATH değeri boş görünecektir.

```
R1# show bgp ipv4 unicast | begin Network
     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.3.3.0/24      10.12.1.2                33             0 65200 65300 3003 ?
 *   10.12.1.0/24     10.12.1.2                22             0 65200 ?
 *>                   0.0.0.0                   0         32768 ?
 *>  10.23.1.0/24     10.12.1.2               333             0 65200 ?
 *>  100.64.2.0/25    10.12.1.2                22             0 65200 ?
 *>  100.64.2.192/26  10.12.1.2                22             0 65200 ?
 *>  100.64.3.0/25    10.12.1.2                22             0 65200 65300 300 ?
 *>  192.168.1.1/32   0.0.0.0                   0         32768 ?
 *>  192.168.2.2/32   10.12.1.2                22             0 65200 ?
 *>  192.168.3.3/32   10.12.1.2              3333             0 65200 65300 ?
```

- Gecikme sürelerinin farklı olmasından dolayı Jitter oluşabileceği için genelde rotalar arasında Load-Balance yapılması istenmez. Bunun yerine Load-Sharing yapılması istenir. Yönlendirme protokollerinde Load-Balancing ile Load-Shaering arasındaki farkla bakıldığında;
    - **Load-Balancing**, trafiğin tamamını ayırt etmeksizin rotalar arasında eşit şekilde dağıtmak için kullanılmaktadır. Bu durumda bir uygulama trafiğinin iki paketi de farklı rotalar kullanılarak iletilecektir. Dolayısıyla paketlerin hedefe ulaşması farklı sıralarda ve farklı zamanlarda gerçekleşebilir.
    - **Load-Sharing**, trafiği duruma göre rotalar arasında paylaştırılması için kullanılmaktadır. Örnek olarak A uygulamasının tüm trafiğinin X rotasından, B uygulamasının tüm trafiğinin Y rotasından gitmesi verilebilir. Bu sayede uygulama paketleri gönderilirken farklı zamanlarda ve sırada hedefe ulaşmamış olur.
- **BGP Communities** ayrıca araştırılması gerekiyor (https[:]//www.noction.com/blog/understanding-bgp-communities).

Terminolojiler

- **BGP Multihoming**, Kurumların birden fazla ISP üzerinden internete çıkışına sahip olmasına deniliyor.

Kaynaklar

- https[:]//networklessons.com/bgp/bgp-confederation-explained
- https[:]//www.noction.com/blog/accumulated-igp-and-bgp