

BGP – 1

BGP, internet üzerinde networklerin haberleşmesini sağlayan dinamik yönlendirme protokolü olarak tanımlanabilir.

Birçok dinamik yönlendirme protokolüne kıyasla BGP protokolü, daha yavaş çalışması (Nedeni, topolojide gerçekleşen her değişimin BGP protokolü kullanan her router'a tek tek anons ediliyor olması), daha yüksek donanımlı cihazlara ihtiyaç duyulması (İnternet üzerindeki bütün networklerin kaydını tutuyor) veya her zaman en iyi rotaya karar verememesi gibi durumlarla karşı karşıya kalırsa da BGP protokolüne ihtiyaç duyulan durumlar da bulunmaktadır.

BGP protokolünün kullanılmaması gereken durumlara bakıldığında;

- Tek bir network çıkışına sahip olduğunda,
 - o Veya internet çıkışı yedekli (birden fazla çıkışa sahip olması) ama hepsinin aynı ISP'ye bağlıysa kullanılmasına gerek yoktur.
- BGP protokolünü çalıştırabilecek gereksinimlere sahip cihazlara sahip olunmadığı durumlarda,
 - o Protokolün çalışabilmesi için yüksek işlem gücüne ve depolama alanına sahip olunması gerekiyor
- BGP protokolüne dair sınırlı bilgiye sahip olduğunda kullanılmaması gerekiyor.
- BGP protokolü hakkında yeterli bilgiye sahip olunmadığı durumda da kullanılmamalıdır. OSPF, EIGRP gibi protokollere kıyasla çok daha karmaşık bir işleyişe sahiptir.

BGP protokolüne ihtiyaç duyulan durumlara bakıldığında;

- Kurumda birden fazla ASN'e (aynı anda birden fazla ISP'den hizmet alınması) bağlı bir network kullanıldığı durumlarda
 - o Örnek olarak kurumun bir web sayfası varsa (Tek bir ip adresine sahip olacaktır) bu web sitesine erişim için domain kaydı tek bir ip adresine yapılacaktır. Bu ip adresinin aynı anda iki ISP üzerinden de yayınlanması sağlanabiliyor (Aynı zamanda ISP'lerden birinden bir problem olması durumunda web sayfasına diğer ISP üzerinden erişilebilecektir. Bu sayede yedeklilik de sağlanmış oluyor).
 - o Farklı ISP firmaları üzerinden tek bir ip adresi yayınlandığı durumda trafiklerin farklı ISP'ler üzerinden paylaştırılarak alınması sağlanacaktır (ISP1'den hizmet alan kullanıcılar ISP1 üzerinden, ISP2'den hizmet alan kullanıcılar ISP2 üzerinden gelecektir).
- Bir kaynağa erişim için paketlerin internet üzerinde farklı konumlarda bulunan routerlar üzerinden (farklı ISP'lere ait) yönlendirilmesi gibi çeşitli manipülasyonlara ihtiyaç duyulduğu durumlarda kullanılabilir.
 - o Örnek olarak, 4.5.6.0/24 networküne gelen isteklerin Türk ISP firmasından, 4.5.7.0/24 networküne gelen isteklerin İtalyan ISP firması üzerinden gelmesini sağlayabiliyor.

AS Numbers

AS (Autonomous System) Numbers, bir kurumun/kuruluşun sahip olduğu network yapısının kapsamını temsil etmek için kullanılan benzersiz bir numardır (bir kurumun yönetimi altında olan routerların bütünü temsil etmek için kullanılan sayısal değerdir). Tanımdan da anlaşılacağı gibi bu değer dünya genelinde benzersiz olmak zorundadır.

AS Number, ilk zamanlarında 2 bayt ($65535 - 2^{16}$) ile ifade edilirken, zaman içerisinde bu tanım aralığının yetersiz kaldığı öngörülerek bu değer günümüzde 4 bayta ($4,294,967,295 - 2^{32}$) çıkarılmıştır (her iki adres boyutu da aralarında komşuluk kurabiliyor).

- **Private ASN** aralığı da bulunmaktadır. Bunlar;
 - o 2 bayt kullanımı için aralık; 64512-65535
 - o 4 bayt kullanımı için aralık; 4200000000 – 4294967294
- Kullanımına örnek olarak kurumlar anons yapmak istediklerinde Private ASN numarasıyla anonslarını ISP'ye gönderiyor. ISP ise kendisine gönderilen Private ASN numarasını kendi ASN numarasıyla değiştirip internete anons ediyor (Bir tür NAT işlemi gibi).
- EIGRP protokolündeki AS ile karşılaştırıldığında; EIGRP protokolünde AS umarası yönetici tarafından rastgele atanıyordu. BGP protokolünde ise (internet anons yapılabilmesi için) bu değer RIPE, APNIC, ARIN gibi **RIRs (Regional Internet Registries)** kurumlar tarafından veriliyor. AS Number alınarak kurumlar kendi ip hizmetlerini BGP protokolüyle anons edebiliyorlar.

Path Attributes

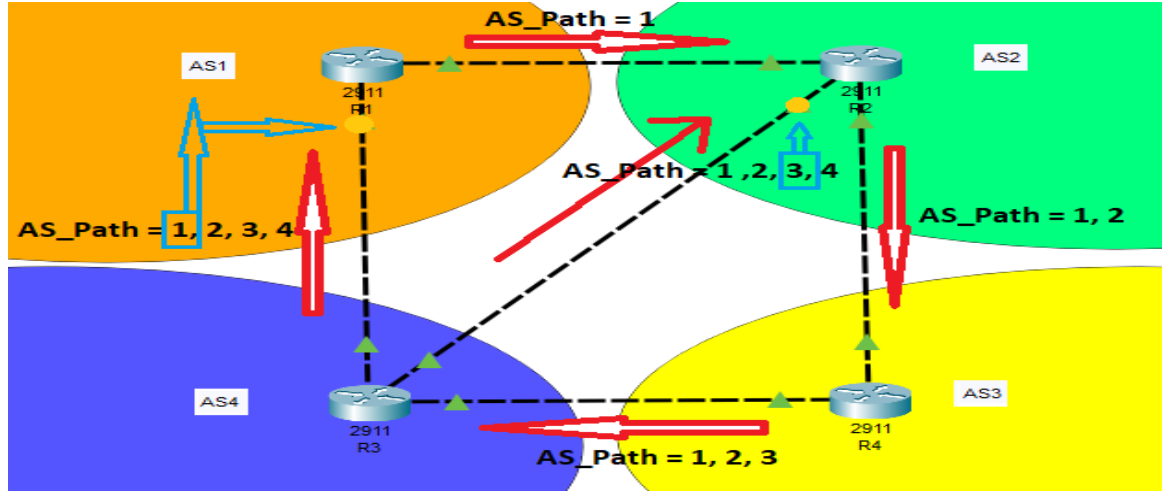
BGP protokolünde bilinen diğer dinamik yönlendirme protokollerinde olduğu gibi tek bir özellik değerlendirilerek rota seçimi yapılmaz. Rota seçimi için **Path Attributes** adı verilen parametreler kullanılır. Bu parametrelerin tamamını her routerun bilmesi gerekmiyor. Parametreler bu kapsamda dört kategoriye ayrılıyor. Bunlar;

- **Well-Known Mandatory**, BGP protokolü kullanan tüm routerlar tarafından kullanılması ve anonslarda bulundurulması zorunlu tutulan parametrelerdir (bu kategorideki bir değer bulunmaması durumunda komşuluk kesilir).
- **Well-Known Discretionary**, tüm BGP routerların bildiği ama anonslarda bulunması zorunlu olmayan parametrelerdir (Çeşitli durumlarda kullanılan değişkenlerdir).
- **Optional Transitive**, routerların bilmek zorunda olmadığı ama kendisine gönderildiğinde, kendisine bağlı routerlara anons etmesi istenen parametrelerdir.
- **Optional Non-Transitive**, routerların bilmek zorunda olmadığı ve anons edilmesi istenmeyen değişkenlerdir (routerlar tarafından bilinse de anons edilmesi istenmeyen değişkenlerdir).

Loop Prevention

BGP protokolünde Loop oluşumunu önlemek için anons içerisine **AS_Path** adı verilen bir parametre kullanılmaktadır. AS_Path parametresi sayesinde anons paketleri, geçtiği her routerun ASN değerini kaydediyor. Bu sayede anons paketi bir ASN'e ikinci kez yönlendirildiğinde, paketin AS_Path değişkenine bakılarak daha önce bu AS'e geldiği anlaşılır ve paket bu AS içerisinde drop edilir. Bu sayede BGP protokolünde Loop oluşumu engellenir (Loop-Free).

| → Bu yapı daha iyi rota seçimi için de kullanılabilir. RIP protokolünün işleyişine benzer şekilde hedefe ulaşmak için kullanılan rotalar arasından daha az AS üzerinden geçilen ulaşılan rota en iyi rota olarak seçilebiliyor (Bu kriter rota seçimi sürecinde bakılan kriterlerden sadece biridir).



| → AS_Path değeri BGP protokolü için çok önemlidir. AS_Path değeri kullanılarak manipülasyonlar yapılabiliyor (bir ISP firmasının bütün trafiği engellenebiliyor) veya daha kaliteli rota seçimi için kullanılabilir.

Address Families

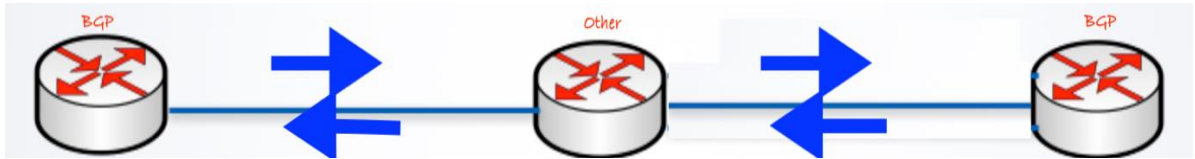
BGP protokolü ilk çıktığında BGPv4 olarak biliniyordu (Sadece IPv4 desteklemektedir). BGPv4 sürümü, IPv6 desteklemediği için BGPv4 sürümü üzerinde geliştirmeler yapıldı. **Bu geliştirmeler içerisinde SAFI (Subsequence Address-Family Identifier / yayın yapılan paketin yayın tipini belirtilerek anons yapılmasını sağlayan özelliktir (Unicast, Multicast)) ve kullanılan ip protokolü (IPv4, IPv6) de belirtilmeye başlandı.** Bu geliştirmeler sonrasında BGPv4+ adını aldı. Her iki protokolü (BGPv4 ve BGPv4+) destekleyen versiyona MBGP/ MP-BGP (Multi Protocol BGP) deniliyor.

- BGP protokolünde her bir protokol için ve bu protokollerin alt sınıfları için ayrı ayrı veritabanları oluşturuluyor (Unicast-IPv4, Unicast-IPv6, Multicast-IPv4, Multicast-IPv6 gibi).
 - o IPv4 ve IPv6'nın yanı sıra MPLS protokolü de kullanılıyorsa, BGP ile MPLS yapıldığında **VPNv4** veya **VPNv6** olacak şekilde iki farklı bir adresleme kullanılıyor (MPLS protokolünde de BGP protokolü kullanılıyordu). BMPLS ile ilgili bu detaylar da BGP protokolüyle öğretilebiliyor.
- BGPv4+ protokolünde komşu routerlar arasında bir Update/anons yollandığında (networkler üzerinde bir değişiklik meydana geldiğinde) anons içerisinde hedef networke ulaşmak için kullanılacak PATH Attribute değerleriyle beraber **NLRI** (Network Layer Reachability Information) adı verilen ek bir alan öğretiliyordu. MBGP/MP-BGP versiyonunda ise bu bilgi **MP_REACH_NLRI** alanıyla bildiriliyor.
 - o **NLRI**, komşu BGP routerlar arasında hedef network bilgisini öğretmek için kullanılan alandır (MP-BGP -> MP_REACH_NLRI).
 - o **Withdraw**, bir network erişiminin kesildiğini komşu BGP routera (Update paketi içerisinde) bildirmek için kullanılan alandır (MP-BGP -> MP_UNREACH_NLRI).

Inter-Router Communication

BGP protokolünde, OSPF protokolünde olduğu gibi komşu routerları ve topolojideki networklerin keşfedilmesi için routerlar arasında belirli periyotlarda “Hello” paketleri gönderilmez (komşu routerlar keşfedilmez). BGP routerların aralarında Unicast haberleşme yapıyor. Bu nedenle BGP routerlar aralarında komşuluk kurulabilmesi için mutlaka komşu BGP routerun ip adresinin belirtilmesi gerekiyor.

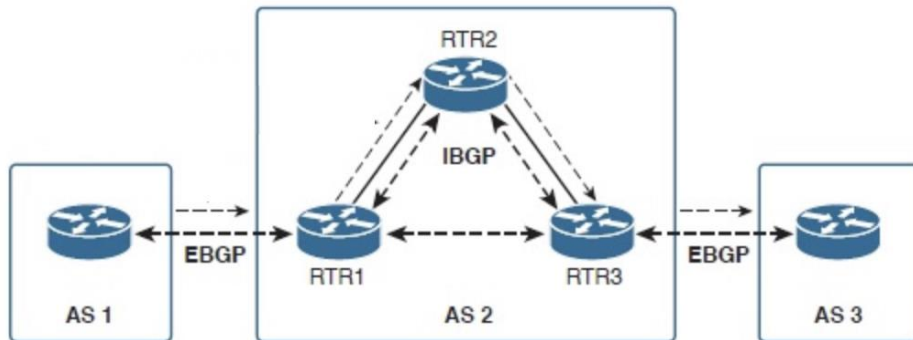
- Burada Unicast haberleşme yapılmasının olumlu yönlerinden birisi de BGP komşuluğu kurulacak routerların birbirine doğrudan bağlı olmasının şart olmamasıdır (Arada bulunan routerun komşu BGP routerlar arasındaki trafiği yönlendirebilmesi için BGP komşuluğu kuran routerların networklerini öğrenmiş olması gerekiyor). Aralarında BGP çalışmayan herhangi bir router konumlandırılrsa dahi paketler Unicast gönderildiği için BGP komşuluğu sorunsuzca kurulacaktır (OSPF ve EIGRP gibi protokoller Multicast yayın kullandığı için bu durum sağlanamıyor). Ek olarak komşuluk kurulacak BGP routerun kaç hop uzakta olduğunun da ayrıca belirtilmesi gerekiyor
 - o Bu gibi durumlarda aradaki routerun MTU (Maximum Transfer Unit – bir paketin olabileceği en yüksek boyutu temsil ediyor. Bu değer arayüzler üzerinde kısılmış veya yükseltilmiş olabilir) değeri de farklı ayarlanmış olabiliyor. Bu durumda BGP routerlar arasında komşuluk kurulamayacaktır. MTU değerinin farklı olduğu durumlarda paketlerin geçmediği arka planda MTU Discovery adı verilen özellik ile bu durum tespit edilecek ve yanıt olarak ICMP hatası gönderilecektir.



- BGP protokolü **TCP 179**. Portu kullanır. TCP protokolü güvenilir olduğu için ayrıca bir kontrol mekanizmasına ihtiyaç duyulmamıştır (ACL yazılırken TCP 179. portuna gelen trafikler göz ardı edilmemelidir).
- Komşuluk kuran BGP router çiftine **BGP Peers** veya **BGP Neighbor** deniliyor.

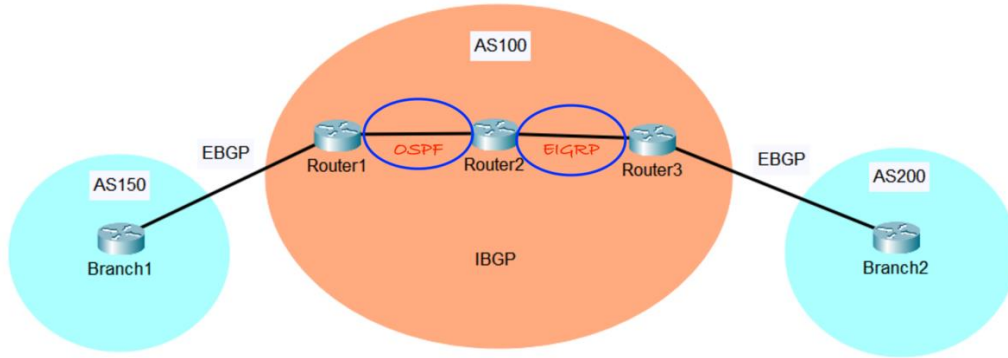
BGP Session Types

BGP protokolü kurum içinde kullanılan (IGP) ve kurumlar arasında kullanılan (EBGP) BGP protokolleri olmak üzere iki gruba ayrılmaktadır.

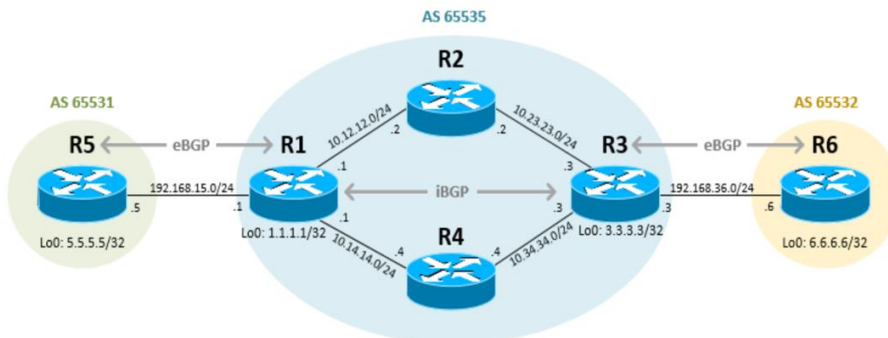


Internal BGP (IBGP/IGP), kurum içinde (Aynı AS içindeki) kullanılan BGP protokolüne denilmektedir. BGP protokolü kurum içerisinde yapıldığında AD (Administrative Distance) değeri 200 olmaktadır. Bunun nedeni konunun başında da açıkladığı üzere BGP protokolünde Loop Free tasarım AS_Path değerleri üzerinden gerçekleştiriliyordu. Kurum içerisinde tek bir AS değeri olduğu için Loop Free bir tasarım sağlanamıyor. Loop oluşma ihtimalinden kaynaklı olarak Internal BGP'de AD değeri 200 olmaktadır.

- Normalde External BGP üzerinden öğrenilen network tanımları Redistribute edilerek IGP içerisinde kullanılan OSPF veya EIGRP protokolü üzerinden tekrar EBGp protokolüne aktarılabilir. Bu süreçte dikkat edilmesi gereken noktalardan birisi BGP protokolü çok büyük yönlendirme tablolarına sahiptir. Bu durumda öğrenilen network miktarı OSPF veya EIGRP protokollerinin çatlamasına neden olabilir. Bu nedenle böyle bir tasarım oluşturabilmek için EBGp protokolünden OSPF veya EIGRP protokollerine Redistribute edilecek network tanımlarının sadeleştirilmesi/filtrelemesi gerekiyor.
 - o Bu şekilde bir AS içerisinde OSPF veya EIGRP gibi protokolleri kullanıldığında BGP protokolünün sağladığı Path Attribute değerleri etkili bir şekilde kullanılmıyor (OSPF veya EIGRP protokollerinin çalışma mekanizmalarından kaynaklı). Bu nedenle AS içerisinde de IGP kullanılması öneriliyor.

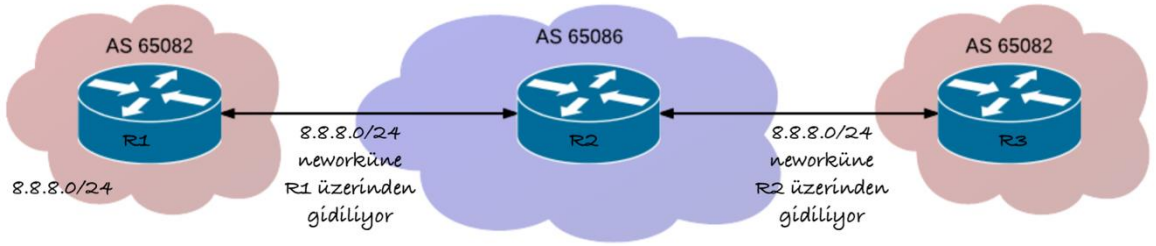


- **ALTIN KURAL** – EBGp router üzerinden öğrenilen bir network bilgisi bir IGP routera öğretilir ama bir IGP router üzerinden öğrenile network bilgisi başka bir IGP routera öğretilmiyor. Bu nedenle AS içerisindeki routerların (IGP routerların) tamamının **Full Mesh** yapıda bağlanması gerekiyor. Bu durumu aşağıdaki görsel üzerinde açıklanmak gerekirse; R5 (EBGP) üzerinden gelen network güncellemelerini alabilmek için IGP içerisindeki bütün routerlar R1'e doğrudan bağlanıyor. Benzer şekilde R6 (EBGP) üzerinden gelecek network bilgilerini alabilmek için IGP içindeki bütün routerlar R3'e bağlanıyor.
 - o Bunun nedeni, IGP içerisinde AS_PATH değerinin kullanılmadığı/aynı olduğu için Loop oluşumunu önlemek üzerine alınan bir önlemdir. Buna istinaden IGP protokolünde anons paketlerinin sadece 1 hop kadar uzağa iletilebildiği söylenebilir.



External BGP (EBGP), farklı kurumlar arasında (farklı AS'lere sahip) kullanılan BGP protokolüne denilmektedir. Loop Free bir tasarım sağlandığı için AD değeri 20'dir.

- Misyonu internet ortamını sağlamaktır.
- Aralarında BGP çalışmayan routerlar bulunsada dahi komşuluk kurulacak EBGP routerlar arasında karşılıklı olarak ip adresleri ve kaç hop uzata oldu belirtildiği takdirde eBGP komşuluğu kurulabiliyor.
 - o Kaç hop uzakta olduğu belirtilmediği takdirde varsayılanda 1 hop uzaklığa kadar komşuluk kurulabiliyor. Bu özellik aslında bir anlamda dünyanın herhangi bir yerindeki EBGP routerun komşuluk kurmasına karşı koruma da sağlıyor.
- Her EBGP anonsunda Next Hop ip adresi revize edilerek komşu EBGP router'a iletilir. Aşağıdaki görsel üzerinden açıklamak gerekirse; ilk olarak R1, R2 routeruna bir network adresi öğretirken, öğrettiği networke kendi ip adresi üzerinden erişilebileceğini öğretir. R2 bu network bilgisini EBGP komşusu olan R3 routeruna öğretirken, öğrettiği networke kendi ip adresi üzerinde ulaşabileceğini öğretir.
 - o IGP'de network öğretilirken bu şekilde Next Hop adres tanımları revize edilmiyor.



- EBGP protokolünde paketler her AS geçişinde, geçtiği AS değerini AS_Path değerine ekleyerek devam ediyor.

Özetle IGP,

- Full Mesh yapıda olması gerekiyor.
- IGP routerlar arasında komşuluk kurabilmesi için doğrudan bağlı olmaları gerekmiyor.
- Yeni bir network öğretilirken router Next Hop ip adresi olarak kendi ip adresini göstermiyor (EBGP'den öğrenildiği gibi anons ediliyor).
- Administrative Distance değeri 20'dir.
- İki EBGP router arasında komşuluk oturmadığı takdirde bir sonraki deneme hemen ardından (0 saniye sonra) gerçekleşecektir.

Özetle EBGP,

- Farklı AS'lerin aralarında anlaşmak için kullanılan BGP protokolüdür.
- Her EBGP router network yeni bir network öğretirken Next Hop adresi olarak kendisini gösteriyor.
- Varsayılanda TTL değeri 1 geliyor. Komşu EBGP routerun durumuna göre bu değer set edilebiliyor.
 - o Komşuluk kurmak için kaynak ip adresi olarak arayüz ip adresi yerine Loopback ip adresi verilebiliyor. Bu durumda TTL değeri bir kez daha azalacaktır. Bunun için TTL değeri 2 set edilmelidir.
- Administrative Distance değeri 20'dir.

- İki EBGp router arasında network bilgilerini aktarmak için OSPF veya EIGRP gibi (Redistribute edilerek) protokoller kullanılmalıdır.
- İki EBGp router arasında komşuluk oturmadığı takdirde bir sonraki deneme 30 saniye sonra gerçekleşecektir.