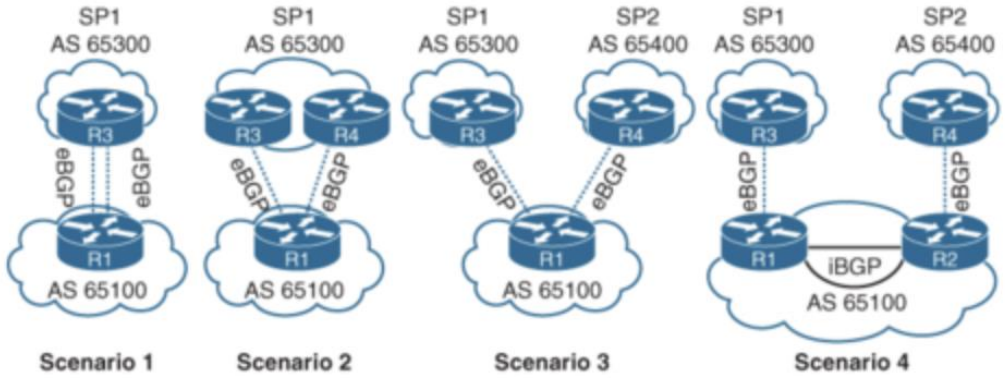
BGP – 4

Kurumların internet çıkışları için kullanabilecek birkaç alternatif seçenek bulunuyor. Bu seçeneklere bakıldığında kurum;

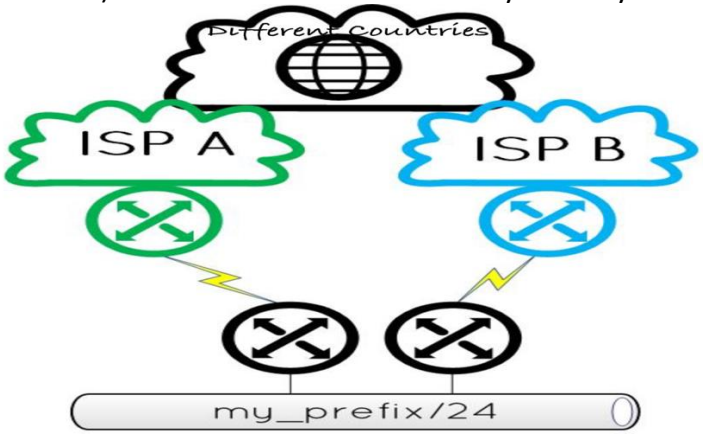
- Tek router üzerinden tek ISP'nin tek routerunu kullanarak internete çıkıyor olabilir (Cihaz ve ISP yedekliliği bulunmuyor. Senaryo-1).
- Tek router üzerinden aynı ISP'nin iki ayrı routerunu kullanarak internete çıkıyor olabilir (Sadece ISP tarafındaki routerlarda cihaz yedeklilik bulunuyor. Senaryo-2).
- Tek router üzerinden farklı ISP'lerin routerlarını kullanarak internete çıkıyor olabilir (Sadece ISP tarafında yedeklilik bulunuyor. Senaryo-3).
- İki router üzerinden farklı ISP'lerin routerlarını kullanarak internete çıkıyor olabilir (Hem ISP yedekliliği bulunuyor, hem de ISP ve kurum taraflarında cihaz yedekliliği sağlanıyor. Senaryo-4).



Bu seçenekler kurumların ihtiyaçlarına ve bütçelerine yönelik tercih edilmektedir.

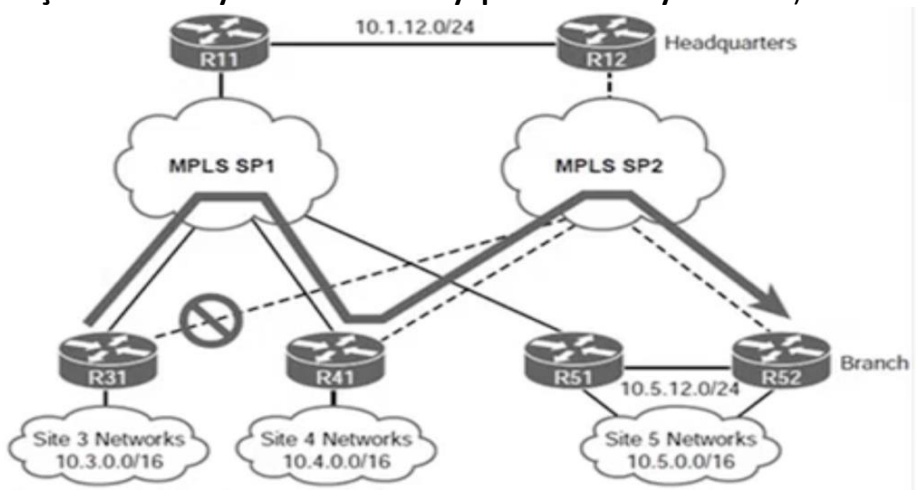
Internet Transit Routing

Kurumların internet çıkışı için kullanabileceği yöntemlerden Senaryo-3 ve Senaryo-4 üzerinde olduğu gibi birden fazla ISP'nin routeru aynı anda kullanılmak istendiğinde eğer ki önlem alınmazsa ISP'ler kendi trafiklerini kurum routeru üzerinden karşı ISP'ye taşıyabilir (Normalde ISP'ler arasında anlaşma bulunmuyorsa, ISP firmalarının trafikleri farklı ülkeler üzerinden birbirine aktarılıyor). Bu duruma **Internet Transit Routing** deniliyor (Kurum routeru **Transit Area** oluyor. Böyle bir durumda ISP, hedef ISP'ye daha kısa bir rota olduğunu görüp bütün trafiği kurum üzerinden hedef ISP'ye taşımaya başlayabilir. Dolayısıyla kurumun bant genişliği işgal edilecektir). Normalde ISP'ler önlemini alıyor ama yine de bilinçli olunmalıdır).

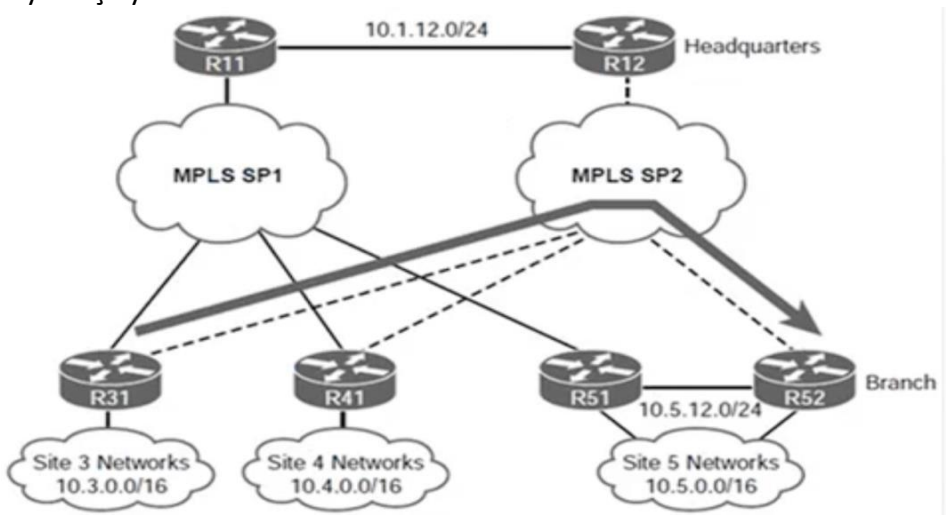


Branch Transit Routing

Kurumun şubeleri ve merkezi arasında birden fazla ISP üzerinden MPLS altyapısıyla bağlantı sağlanıyor olabilir (Kurum içinde BGP kullanılıyor – IBGP/IGP). Bu durumda şubelerin haberleşme sürecinde hangi ISP üzerindeki MPLS altyapısını öncelikli olarak tercih etmesi gerektiğinin ayrıca belirlenmesi gerekiyor. Aksi takdirde şubelerin trafikleri hedef şubelere veya merkeze ulaşabilmek için trafiğini farklı şubeler üzerinden geçirmesine neden olabilir. Böyle bir durumda hem gereksiz yere farklı şubelerin bant genişliği tüketilmiş olacak hem de şubelerin tercih ettiği ISP'nin MPLS yapısı farklı olması durumunda trafiklerin gönderildiği rotalardan değil de farklı rotalar üzerinden dönmesine neden olabilir (MPLS SP1'den R41'e , R41 üzerinden MPLS SP2'ye gönderilerek hedefe routera ulaşması gibi. Bu istenmeyen bir durumdur. Her ne kadar MPLS hatlarında olmasa da farklı ISP'ler arasında gecikme süreleri arasındaki fark çok yüksek olabilir. **Bu durumda paketlerin gönderildiği ve dönerken tercih ettiği rotalar arasında gecikme süreleri çok yüksek olabilir. Bu nedenle Upload işleminin de Download işleminin de aynı ISP üzerinden yapılmasında fayda vardır**).



Bu gibi problemlerle karşı karşıya kalmamak adına şubelerin öncelikli olarak tercih etmesi gereken ISP'nin MPLS altyapısı ayrıca belirtilmelidir. Öncelikli tercih dilen ISP'nin MPLS altyapısında problem yaşanması durumunda bütün şubelerin diğer ISP'nin MPLS altyapısını kullanmaya başlayacaktır.



Conditional Matching

IGP protokollerinde rota filtreleme işlemlerini yapabilmek için **Prefix List** veya **ACL** tanımları kullanılıyordu. BGP protokolünde de filtreleme işlemi yapabilmek için bu yöntemler kullanılıyor. IGP protokollerinden farklı olarak BGP (EGP) protokolünde ACL'ler kullanılarak filitreleme işlemleri yapılmak istendiğinde ACL tanım formatı değişiklik gösteriyor. Bu değişikliklere bakıldığında;

- **Standard ACLs**, sadece kaynak ip adreslerine bakılarak filtreleme yapan kural listesidir. Routing protokollerinde (IGP veya EGP protokollerinde değişiklik göstermiyor) kullanıldığında da bu şekilde çalışmaktadır. Örneklerine bakıldığında;
  - "**permit any**" -> tüm networklere izin verir.
  - "**Permit <IP Address> <Wild Card Mask>"** -> sadece belirtilen aralığa izin verir.
  - "P**ermit host <IP Address>"** -> Sadece belirtilen IP'ye izin verir.

- **Extended ACLs**, kayna ve hedef ip adreslerinin yanında port bilgilerine bakılarak filtreleme yapan kural listesidir. **Burada dikkat edilmesi gereken noktalardan birisi de Extended ACL tanımı IGP (RIP, EIGRP, OSPF, IS-IS) protokollerinde kullanıldığında tanım formatında bir değişiklik olmazken, BGP protokolünde kullanılmak üzere tanımlandığında tanım formatı değişiklik göstermektedir.**
  IGP protokollerinde kullanıldığında;
  - "**Permit any any**" -> Tüm networklere izin verir.
  - "**Permit ip host <IP Adress> host <Subnet Mask>"** -> sadece belirtilen network aralığına izin verir.
  - "**Permit host <IP Address>**" sadece belirtilen ip adresine izin verir.

ACE Entry	Networks
permit ip any any	Permits all networks
permit ip host 172.16.0.0 host 255.240.0.0	Permits all networks in the 172.16.0.0/12 range
permit ip host 172.16.0.0 host 255.255.0.0	Permits all networks in the 172.16.0.0/16 range
permit host 192.168.1.1	Permits only the 192.168.1.1/32 network

  BGP protokolünde kullanıldığında;
  - "**Permit <Src IP Address> <Wildcard Mask of Src IP Address> <Subnet Mask> <Wildcard Mask of Subnet Mask>"** -> IP adresinden sonraki Wildcard maskesi ip adresinin tam olarak eşleşmesi gerektiğini temsil etmek için tanımlanmıştır. Subnet maskesinden sonraki Wildcard maskesi Subnet maskesiyle (/24) tam olarak eşleşmesi gerektiğini temsil etmek için tanımlanmıştır.

- Aşağıdaki görselin ikinci örneği (permit ip 10.0.0.0 0.0.**255**.0 255.255.255.0 0.0.0.0) üzerinden açıklamak gerekirse; ip adresinin 3. Oktet değerinin değişiklik gösterebileceği (10.0.X.0), Subnet maskesi kısmında ise birebir eşleşmesi gerektiğini ifade etmektedir. Buna istinaden örnek vermek gerekirse;
  - 10.0.1.0/24, 10.0.2.0/24, 10.0.10.0/24 adresleri verilebilir.
- Aşağıdaki görselin üçüncü örneğine (permit ip 172.16.0.0 0.0.255.255 255.255.255.0 0.0.0.255) bakıldığında ip kısmı için ilk iki oktet'in (172.16.X.X) eşleşmesi gerektiği, Subnet maskesinin de ilk üç oktet'in eşleşmesi gerektiği (/24-/32 arası verilebilir) ifade edilmiş. Buna istinaden örnek vermek gerekirse;
  - 172.16.1.1/24, 172.16.1.1/28, 172.16.100.1/32, 172.16.11.1/26 adresleri verilebilir.
- Aşağıdaki görselin son örneğinde 172.16.X.X adresinin /25 - /32 arasında Subnet maskesi alabileceği ifade edilmektedir.

Extended ACL	Matches These Networks
permit ip 10.0.0.0 0.0.0.0 255.255.0.0 0.0.0.0	Permits only the 10.0.0.0/16 network
permit ip 10.0.0.0 0.0.255.0 255.255.255.0 0.0.0.0	Permits any 10.0.x.0 network with a /24 prefix length
permit ip 172.16.0.0 0.0.255.255 255.255.255.0 0.0.0.255	Permits any 172.16.x.x network with a /24 to /32 prefix length
permit ip 172.16.0.0 0.0.255.255 255.255.255.128 0.0.0.127	Permits any 172.16.x.x network with a /25 to /32 prefix length

Olağan dışı bir durum olmadığı durumda genelde filtreleme işlemleri için **Prefix List** metodu tercih ediliyor. Olağan dışı bir tanıma örnek ip adresindeki ara Oktet (10.0.X.0 veya 10.X.X.1 gibi tanımları) kısımlarında değerlerin değişkenik gösterebileceği ifade edilmesi gerekebilir. Bu durumda Extended ACL metodunun kullanılması gerekecektir.

Prefix List

Routing protokollerinde filtreleme işlemi için genelde tercih edilen metottur. Prefix List tanımı oluşturma formatını örnekler üzerinden açıklamak gerekirse;

- Tek bir subnet değeri için filtreleme işlemi yapılabilir.
  - "**ip prefix-list TEST seq 5 deny 196.200.220.291/26**" -> sadece burada belirtilen subnetin anons edilmesini veya kendi üzerine kayıt etmesi/öğrenmesi engellenir.
- Bir network içerisindeki bazı Subnet bilgileri için filtreleme işlemleri yapılabilir. Bu tanımlara örnek olarak;
  - "**ip prefix-list TEST seq 5 permit 196.0.0.0/8 le 24**" -> 196.0.0.0/8 ila 196.0.0.0/24 aralığındaki network adreslerine izin verir (Equals or Less Than).
  - "**ip prefix-list TEST seq 10 deny 196.200.220.0/24 ge 25**" -> 196.200.220.0**/25** ila 196.200.220.0**/32** aralığındaki network adreslerine izin verir (Equals or Greater Than).

    - “**ip prefix-list TEST seq 15 permit 196.0.0.0/8 ge 16 le 24**” -> bu tanımda hem alt sınır hem de üst sınır belirtildiği için 196.0.0.0/8 networkünde bulunan 196.0.0.0/16 ila 196.0.0.0/24 arasındaki subnetlere izin verir.
        - Burada dikkatini çekmesi gereken kısım “le” veya “ge” parametreleriyle belirtilen subnet aralıkları komut başında belirtilen Subnet’in kapsadığı aralıklardadır (196.0.0.0/8 için /16 - /24 aralığı filtrelendi).
    - “**ip prefix-list TEST seq 20 permit 0.0.0.0/0 le 32**” -> Tüm networkleri izin verir (Implicit Deny satırını boşa düşürmek için kullanılabiliyor). Bu tanımın sonunda bulunan “le 32” kısmı eklenmezse sadece varsayılan rota tanımına izin ver demek oluyor (**yani bir aralık (tüm ip adresleri) belirtilmemiş oluyor**). Bu nedenle Prefix List tanımlarında dikkat edilmesi gereken konulardan birisidir.
- Tanımlanan Prefix List tanımına bir sıra numarası belirtilmediği takdirde tanımlanan ilk Prefix List tanımı için sıra numarası 5’ten başlatılıyor. Eğer ki aynı isimle yeni tanımlar yapılmaya devam edilirse her bir tanım için sıra numarası 5’er arttırılarak verilmeye devam edilir.
- ACL tanımında olduğu gibi kurallar üst satırlardan aşağı satırlara doğru kontrol ediliyor. Yani daha özel kurallar düşük sıra numaralarıyla tanımlanırken daha genel kurallar daha yüksek sıra numaralarıyla tanımlanmalıdır.
- En alt kısımda varsayılanda **IMPLICIT DENY** satırı bulunduğu unutulmamalıdır.

```
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
```

IPv4 adresler için kullanılan prefix list tanım şekli IPv6 için de geçerlidir.

Regex Expressions (Regex)

Regular Expression, bir örüntüyü/diziyi tarif etmek için kullanılan kurallar bütünüdür. Pek çok alanda kullanılabildiği gibi BGP tanımı yaparken de kullanılıyor. Çeşitli alanlarda kullanılmasına karşın tanımlarda kullanılan semboller farklılık gösterebiliyor. Tanım için kullanılan karakterlerin/sembollerin anlamlarına bakıldığında;

^	Matches beginning of string
$	Matches end of string
_	Matches any delimiter (beginning, end, white space, tab, comma)
.	Matches any single character
[ ]	Matches any single character in the range (example [1-9] matches any single digit)
( )	Used to group smaller regular expressions into larger expressions
\	Remove the special meaning by preceding each character with a backslash
*	Matches zero or more atoms (preceding single character or group)
?	Matches zero or one atom
+	Matches one or more atoms
|	Logical OR

BGP protokolünde AS_PATH parametresi geçilen her bir AS'i kayıt altına almak için kullanılıyordu. Bu sayede paketlerin geçtiği her bir AS değeri kayıt altına alınıyordu.

AS_PATH parametresi üzerinde çeşitli filtreleme işlemlerinin yapılarak belirli AS'ler üzerinden gelen networklerin öğrenilmesi engellenebiliyor. Bu sayede belirli ülkelerden gelen bütün trafiklerin erişimleri birkaç satırla kesilebiliyor. Bu gibi pek çok işlem gerçekleştirilebiliyor. Bu filtreleme işlemlerine örnek olarak;

^$	paths in local AS
.*	paths
300	paths including 300
^300	paths announced from AS300 directly
^300$	paths in AS300
^300_	equal to regexp ^300
_300$	paths originated from AS300
_300_	equal to regexp 300
^(300_)*$	^$, ^300$, ^300 300$, ^300 300 300$, ...

1 →AS_PATH parametresinde herhangi bir AS numarası olmaması durumunu temsil ediyor. Bir başka açıklama olarak AS içerisindeki trafiği temsil etmek için kullanılıyor.
2 →
3 → Sadece AS 300 temsil ediliyor.
4 → AS_PATH parametresinin sadece AS 300 içermesi gerektiği ifade edilmiş (AS 300 ile başlaması ve AS 300 iler sonlanması gerekiyor. Arasında herhangi bir AS bulunmamalıdır).
5 →AS_PATH parametresinin AS 300'den başlayarak gelmesi gerektiği temsil edilmiş. AS 300'den çıktıktan sonra hangi AS'ler üzerinden geçtiğinin önemsiz olduğu belirtilmiş.
6 → AS_PATH parametresi
7→ AS_PATH parametresinin en son AS 300'den geçerek gelmesi gerektiğini temsil ediyor. "$" sembolüyle son geçilebilecek AS tanımının AS 300 olması gerektiği ifade edilmiş (Burada her yeni AS değeri AS_PATH parametresinde öne eklenerek devam edildiği unutulmamalıdır).

a- 234 – 4123 - 5234 - 300

8→ AS_PATH parametresinin başında veya sonunda ne olduğu fark etmeksizin AS 300'den geçen paketlerin tamamını temsil ediyor.

Route Maps

Route Map tanımları routing üzerinde özel manipülasyonlar ve filtreleme işlemleri yapmak için kullanılan özel bir konfigürasyon tekniğidir. BGP dışındaki dinamik yönlendirme protokollerinde çoğu zaman filtreleme işlemlerinde kullanılsa da BGP protokolünde routing işleminde metrik değerleri üzerinde değişiklikler yapmak için kullanılan konfigürasyon tekniğidir.

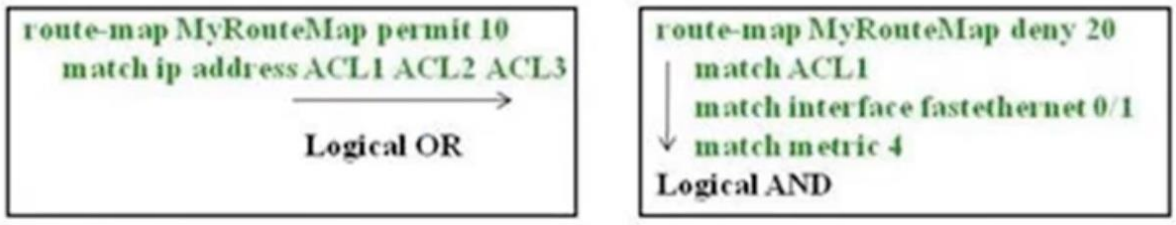
- Route Map'ler ACL'lere benzer şekilde yazılmaktadır. Bir Route Map tanımı yapılırken ilk olarak "**route-map <Route Map Name> (deny | permit) <Sequence Number>**" komutuyla tanımlanacak satırın hangi kural tanımının hangi satırında oluşturulacağı belirtilmelidir. Burada sonraki satırlarda belirtilecek ACL tanımlarının engellenip/engellenmeyeceği (engellenmeyecek ise Metric değerinin nasıl değiştirileceği) belirtiliyor.
    - Route Map tanımında deny tanımı yapılmışsa bu durumda eşleşen rotalar anons edilmeyecektir.
    - Route Map tanımı "**route-map <Route Map Name>**" şeklinde yapılırsa Sequence Number değeri otomatik olarak 10'ar 10'ar arttırılıyor. ACL tanımlarına benzer şekilde oluşturulan kurallar yukarıdan aşağıya doğru kontrol edilir. Yani kurallar özelden gelene doğru yazılmalıdır.
    - ACL tanımlarında olduğu gibi Route Map tanımında da en alt satırda Implicit Deny satırı bulunuyor. Özetle, hiçbir satırla eşleşmeyen tüm route tanımları Ipmlicit Deny satırına tabi tutulur (Bu satırla eşleşen networkler öğretilmez).
    - Implicit Deny satırını boşa çıkarmak için "**route-map <Route Map Name> permit <Sequence Number>**" komutuyla bir Route Map tanımı yapılması yeterli olacaktır. Bu durumda herhangi bir ACL veya Prefix List tanımı belirtilmediği için "Any" (tüm rotalar) olarak algılanacaktır. Bu satır altında herhangi bir Metric değer belirtilmediği durumda da bütün rotalar kendi Metric değerleriyle anons edilmeye başlayacaktır.
- Tanımlanacak satırın hangi kural tanımına dahil edileceği belirtildikten sonra "**match ip address <ACL Name/Number | Prefix List>"** komutuyla koşul/hangi durumlarda Match edeceğini belirleyecek olan ACL veya Prefix List tanımı belirtilmelidir.
    - Route Map tanımı altında eşleşecek rota tanımları için ayrıca Match ifadesi yazılmadığı takdirde bütün rotalarla eşleşecektir.
- Son adımda "**set metric <Metric>**" komutuyla ilgili ACL/Prefix List ile eşleşeceği durumda değişmesi istenen Attribute değeri belirtilmelidir.
    - Route Map tanımı altında "**set metric <Metric>**" tanımı yapılmadığı takdirde ilgili rotalar kendi Metric değerleriyle anons edilir.

Route Map tanımlarında rotaları temsil etmek için kullanılabilecek ifade çeşitlerine bakıldığında;

- AS Path → "**match as-path <ACL Number>**"
- ACL → "**match ip address <ACL Name | ACL Number>**"
- Prfix List → "**match ip address prefix-list <Prefix List>**"
- Local Prefence → "**match local-preference <Local Preference>**"
- Metric → "**match metric <Metric>**"
- Tag → "**match tag <Tag Value>**" üzerinden tanımlar yapılarak manipülasyon işlemleri yapılabiliyor.

```
route-map test permit 10
 match as-path 10 20 30
 continue 30
 exit
route-map test deny 20
 match community 30
 exit
route-map test permit 30
 match ip address prefix-list 1
 set metric 100
 exit
```

Route Map tanımlarında mantıksal “and” ve “or” işlemleri kullanılabiliyor. Bir Route Map tanımı altında alt alta birden fazla Match tanımı eklendiğinde bu mantıksal “and” işlemine karşılık gelecektir. Tek Match tanımı üzerinde birden fazla ACL/Prefix List tanımı yan yana eklendiğinde bu mantıksa “or” işlemine karşılık gelmektedir.



|→ İlk kısımda tanımlanan Route Map tanımında gelen rota bilgisi ACL1 veya ACL2 veya ACL3 ile eşleşmesi durumunda kendi Metric değeriyle anons edilirken ikinci kısımda tanımlanan Route Map tanımında ACL4 içerisinde belirtilmesi, F0/1 arayüzünden gelmesi ve Metric değeri 4 olması durumunda ilgili rotaların anons edilmemesi gerektiği ifade edilmiştir.
|→ Burada dikkat edilmesi gereken konulardan birisi de Route Map tanımlarına yeni bir Match tanımı eklenirken eski tanımların altına eklendiği unutulmamalıdır. Yani Match tanımları yapılırken günün sonunda Route Map tanımının istenildiği gibi olup olmadığı “**sh run**” komutuyla kontrol edilmelidir.

Route Map tanımıyla eşleşen rota bilgileri üzerinde “set” komutuyla değiştirilebilecek özelliklere bakıldığında;

- “**set as-path prepend <AS Number Pattern | Last AS 1-10>**” komutuyla AS path değeri üzerinde manipülasyonlar yaptırılabiliyor.
- “**set ip next-hop <Ip Address | Peer Address | Self>**” komutuyla Next-Hop adresi üzerinde manipülasyon işlemleri yaptırılabiliyor (Next-Hop manipülasyonu BGP protokolünde kullanılabildiği gibi Policy Base Routing‘de kullanılıyor).
- “**set local-preference <0-4294967295>**” komutuyla Local-Preferences değeri değiştirilebiliyor.
- “**set metric <+Value | -Value | Value>**” komutuyla Metric değerleri üzerinde değişiklikler yapılabiliyor.
- “**set origin <igp | incomplete>**” komutuyla Origin (komşu BGP routerdan öğrenilen rota bilgilerinin nasıl öğrenildiği) değiştirilebiliyor.
- “s**et tag <Tag Value>**” komutuyla rota bilgileri etiketlenebiliyor veya rotaların etiket bilgileri değiştirilebiliyor.
- “**set weight <0-65535>**” komutuyla rotaların Weight değerleri değiştirilebiliyor.

Normalde Route Map tanımları da ACL'ler gibi yukarıdan aşağı yönde kontrol edildiğinden bahsedilmişti. Bu şekilde normalde rota tanımının eşleştiği ilk Route Map satırı uygulanır ve diğer Route Map tanımlarına bakılmaz. Bir rota tanımının eşleştiği ilk Route Map tanımıyla eşleştikten sonra alt satırların da kontrol edilmesi istendiğinde, ilgili Route Map tanımı altında "**Continue**" anahtar kelimesi kullanılır. Bu kelime kullanıldığında ilgili rota tanımı için alt satırlardaki Route Map tanımları üzerinden kontrollere devam edilmesi sağlanıyor. Bu sayede rota tanımlarının birden fazla Attribute değeri üzerinde değişiklik yapılabilmesi gibi çeşitli işlemlerin yapılabilmesi sağlanır. İsteğe bağlı olarak "**continue <Route Map Sequence Number>**" komutuyla devam edilmesi istenen Route Map satırının sıra numarası da girilebiliyor.

Notlar:

- Prefix List ve Route Map tanımlarında bir Deny satırı tanımlandığında bu satır ilgili ACL'in Permit tanımlı satırıyla eşleştiğinde uygulanacağını gösterir. Yani Prefix List veya Route Map tanımına uygulanan ACL üzerinde eşleşen satırlar (Permit olan) Deny edilecektir.