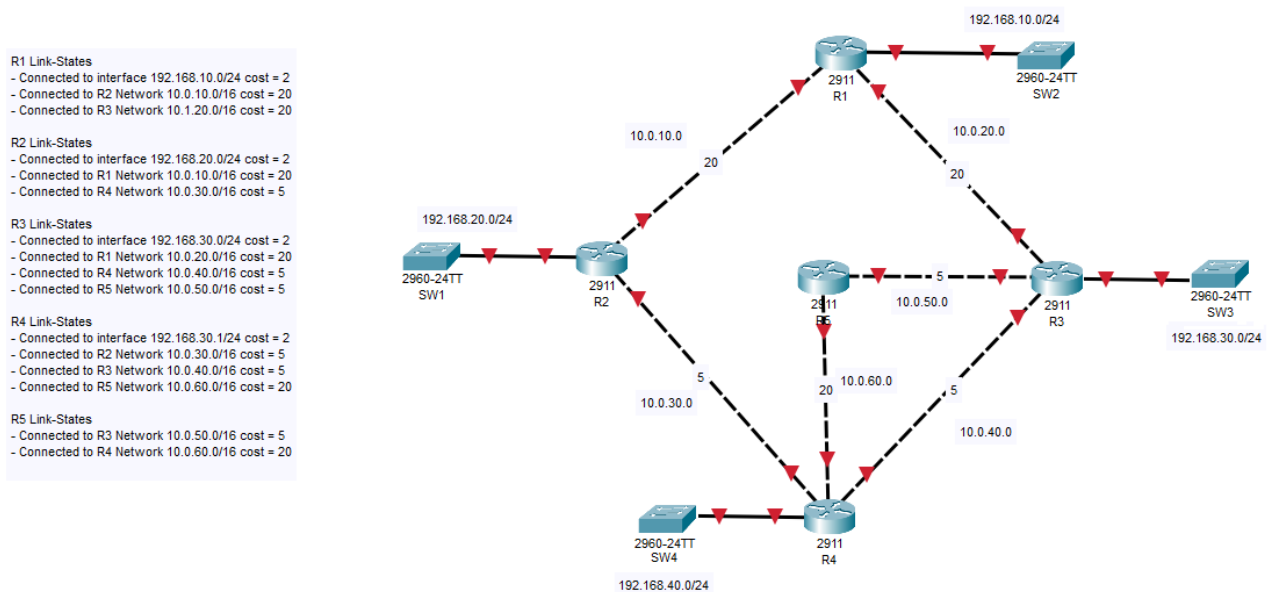


OSPFv2

OSPF (Open Shortest Path First), dinamik yönlendirme protokollerinden birisidir. Kurum içi networklerde en yaygın kullanılan dinamik yönlendirme protokollerindendir. Link State algoritmasını temel alarak çalışır.

Link State algoritmasıyla, router üzerindeki link bilgilerini komşu routerlarla paylaşırlar (Link bilgisi içerisinde routerun öğrendiği networklerin ip ve subnet bilgisi, Cost değeri, farklı router üzerinden öğrenilmiş ise bağlı olan routerun bilgisi ve kullanılan Ethernet teknolojisi bulunmaktadır). Bu sayede topolojideki her network bilgisi her routerla paylaşılmış olur. Bu link bilgileri, routerlarda **Link State Database (Topology Table)** adında bir veri tabanında tutulur. Convergence olmuş bir topolojide her routerun Topology Table tablosu aynı olmaktadır. Bu tabloda depolanan Link State bilgileri SPF (Shortest Path First) algoritması kullanılarak en iyi rota tespiti yapılır. Tespit edilen en iyi rotalar kullanılarak yönlendirme tablosu oluşturulur.

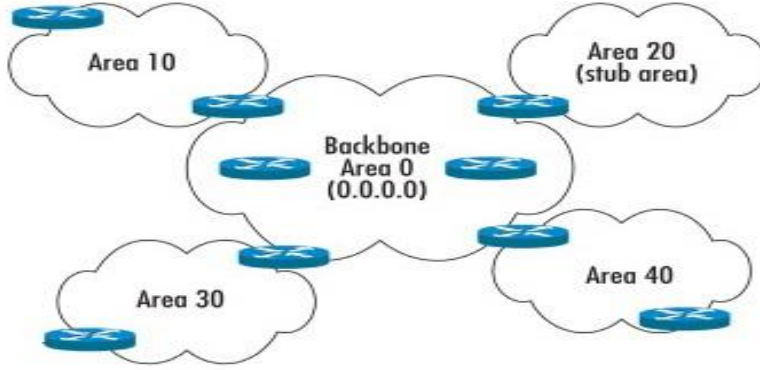


Routerlar aralarında Link bilgilerini paylaşmadan önce komşuluk kurulması gerekiyor. Kurulan komşuluklar routerlarda **Adjacency Database (Neighbor Table)** adında bir veri tabanında tutuluyor. Komşuluk kurulduktan sonra routerlar aralarında varsayılanda 10 saniye olan Hello interval süresi aralığında birbirlerine Hello paketleri gönderirler. Eğer ki varsayılanda 40 saniye olan Dead Interval süresince komşu routerdan Hello paketi alınmazsa router Neighbor Table tablosunda routerun komşuluk bilgisini kaldırır. Komşuluğunu bitirdiği için aynı zamanda bu komşuluktan öğrendiği Link State bilgilerini de yönlendirme tablosundan kaldırır.

Özet Olarak;

- Komşuluk kurulumu
- Link State bilgileri paylaşılır
- Link State Database oluşturulur
- SFP algoritmasıyla en iyi rota seçimi yapılır
- Yönlendirme tablosu oluşturulur

OSPF'in daha büyük topolojilerde kullanılabilmesi için hiyerarşik bir yapı oluşturuluyor. Bunun için topolojiler belirli sayıda router ile sınırlandırılmaktadır ve adına Single Area OSPF denilmektedir. Single Area OSPF'lerin aralarında haberleştirilmesine ise Multi Area OSPF denilmektedir. Bu durum LAN-WAN ilişkisine benzetilebilir. Sadece Single Area OSPF'leri aralarında haberleştirebilmek için kullanılan Area'ya **BackBone Area (Area 0)** denilmektedir.



SORU : Neden Single Area OSPF'de kullanılabilecek router sayısı sınırlandırılmıştır?

- Topolojide network sayısı yükseldikçe Link State Database'indeki satır sayısı artmaktadır. Bu durum Link State Database'in boyutunun büyümesine ve her network için ayrıca çalıştırılan SFP algoritmasının da performansının düşmesine neden olmaktadır.
- Topolojiye her yeni network eklendiğinde (Topolojide bir değişim meydana geldiğinde) Link State Database yeniden oluşturuluyor ve yeniden SFP algoritması çalışarak yeniden en iyi rotalar tekrar tekrar hesaplanıyor. Single Area OSPF ise sınırlı sayıda router içerdiği için topolojiye bir network eklendiğinde bundan daha az sayıda router etkiliyor. Yani routerlarda çok daha hızlı hesalama yapılması ve daha az kaynak tüketmesi sağlanıyor. Aynı zamanda networkte değişimlerin daha az gerçekleşmesi de sağlanıyor.

OSPF Protokolünde Kullanılan Paketler

- **Hello**, routerlar aralarında bilgi paylaşmadan önce komşuluk kurmaları için kullanılıyor. Komşuluk kurulduktan sonra da routerlar aralarında Hello paketleriyle ayakta olduklarını birbirlerine bildiriyor.

8	8	8	8
Version	Type = 1	Packet Length	
Router ID			
Area ID			
Checksum		AuType	
Authentication			
Authentication			
Network Mask			
Hello Interval		Options	Router Priority
Router Dead Interval			
Designated Router			
Backup Designated Router			
Neighbor			
⋮			
Neighbor			

| → Buradaki Type alanı paketin tipini (Hello, DBD, LSR,LSU,LSAck) belirtmektedir. Kalan kısımlar ise adından anlaşılmaktadır.

| → Hello paketi içerisindeki parametreler uyuşmadığı durumlarda routerlar arasında komşuluk kurulmuyor. Nedir bu parametreler?

- Her routerun Router ID değeri benzersiz olmalı.
- Her iki router da aynı Area içinde bulunmalı (Area ID aynı olmalı).
- Arayüzlerde karşılıklı olarak MTUs boyutlarının aynı olması gerekiyor.
- Authentication bilgileri aynı olmak zorunda.
- Subnet bilgileri aynı olmak zorunda.
- Hello Interval ve Dead Interval süreleri aynı olmak zorunda.
- Her iki routerda da network tipleri aynı olmalı (Ethernet, PPP, ...)
- Area Type kısmında ek tanımlamalar/konfigürasyonlar yapıldıysa bunun da aynı olması gerekiyor (NSSA, Stub Area ...).

- **DBD (Database Description)**, routerun Link State veritabanının özetini içeren pakettir. Bu paket routerlar aralarında komşuluk kurulacağı zaman komşu routerun kendisinde bulunmayan link bilgilerini tespit edebilmesi için kullanılır.
- **LSR (Link-State Request)**, router kendisinde eksik olan link bilgilerini komşu routerlardan istemek için kullandığı pakettir.
- **LSU (Link-State Update)**, router komşu routerdan gönderilen LSR paketine karşılık eksik Link bilgilerini komşu routerlara iletmek için kullandığı pakettir.

| → LSU-LSA paketlerinin alt tipleri de bulunmaktadır. Daha çok Multi Area OSPF’de kullanıldığı için CCNP konusu (**Detaylar için CCNP - 06 – OSPF notlarını inceleyebilirsiniz**).

- LSA Type 1: OSPF Router LSA
- LSA Type 2: OSPF Network LSA
- LSA Type 3: OSPF Summary LSA
- LSA Type 4: OSPF ASBR Summary LSA
- LSA Type 5: OSPF ASBR External LSA
- LSA Type 6: OSPF Group Membership LSA
- LSA Type 7: OSPF Not So Stubby Area (NSSA) External LSA
- LSA Type 8: OSPF External Attributes LSA (OSPFv2) / Link Local LSA (OSPFv3)
- LSA Type 9: OSPF Link Scope Opaque (OSPFv2) / Intra Area Prefix LSA (OSPFv3)
- LSA Type 10: OSPF Area Scope Opaque LSA
- LSA Type 11: OSPF AS (Autonomous System) Scope Opaque LSA

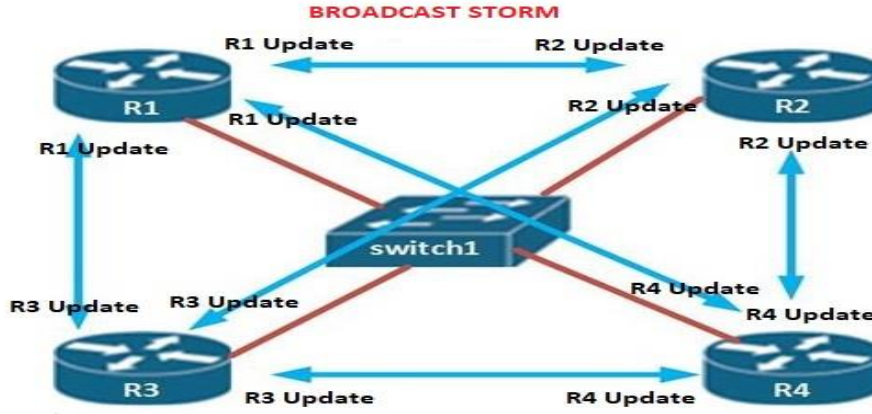


- **LSAck (Link-State Acknowledgement)**, Hello paketi dışında diğer 3 paketin komşu router'a sorunsuz ulaştığını belirtmek için kullanılır.

Broadcast Storm

Normalde Point-to-Point bağlantılarda routerlar komşuluk kurduktan sonra güncellemeleri doğrudan bağlı komşularına göndererek bildiriyor. Birden fazla router birbirine bir switch kullanılarak bağlandığında ise (buna **MultiAccess network** deniyor) ilk adımda güncellemeler bir router üzerinden switch'e bağlı bütün routerlara bildiriliyor ve switch'e bağlı bütün routerlar bu bilgiyi öğreniyor. Switch'e bağlı her router ise doğal olarak yeni öğrendiği network bilgisini komşularına bildirmek için bütün portlarından yeni öğrendiği network bilgisini gönderme eğiliminde bulunuyor. Bu işlemi switch'e bağlı her routerda tek tek gerçekleştiriyor. Bu durumda ise MultiAccess network içerisinde gereksiz yere çok fazla LSU paketi kullanılıyor. Bu olaya **Broadcast Storm** deniliyor.

Broadcast Storm olayının yaşanmaması için MultiAccess networklerde bütün güncellemeler tek bir router üzerinden bildirilir. Topolojiye yeni bir network eklendiğinde bu güncelleme MultiAccess network içerisinde tek bir routera bildirilir. Bu routera **DR** (Designated Router) router denilmektedir. Bu router ise öğrendiği network bilgisini sadece bir kere switch'e bağlı bütün routerlara gönderir. DR routerda bir sorun yaşandığında güncellemelerin aksamaması için bir de **BDR** (Backup Designated Router) router seçimi yapılır. DR routerda bir sorun yaşandığında devreye BDR router geçerek güncellemeler yine tek bir merkezden bütün routerlara dağıtılır. **DR ve BDR routerlar güncellemeleri networkte bulunan cihazlara iletmek için Multicast adresler kullanır (224.0.0.6 -> DR ve BDR güncelleme alır, 224.0.0.5 -> Güncellemeler basılır).**



OSPF Algoritmasının Çalışma Adımları

- **Down State**, OSPF protokolünün çalışmadığı durumdur.
- **Init State**, routerlar aksi bir konfigürasyon yapılmadıkça OSPF protokolü çalışmaya başladığında bütün portlarından Hello paketi gönderir. Bu adıma Init State denilmektedir.
- **Two-Way State**, portlarından Hello paketi gönderen iki routerun, aralarında Hello paketlerini alarak komşuluk kurmaya başladığı adımdır (Ayrıca bu adımda Ethernet kullanılıyorsa DR ve BDR seçimi yapılır, Ethernet değil de Point-to-Point bağlantı varsa bir sonraki adıma geçiliyor).
- **ExStart (Exchange Start) State**, komşuluk sürecinde her iki router da DBD (Database Description) paketleriyle tek seferde Link State veritabanlarının özetlerini birbirlerine göndermesi gerekiyor. Bu adımda DBD paketini ilk hangi routerun göndereceği belirleniyor (Yani değişime kimin başlayacağını kararı veriliyor. İlk DBD paketini Router Id değeri yüksek olan router gönderir).
- **Exchange State**, routerlar arasında DBD paketleri ile Link State veritabanlarının özetleri karşılıklı olarak paylaşıyor ve routerlar bu özet bilgileri kullanarak kendi Link State veritabanlarındaki eksik networkleri tespit ediyor.
- **Loading State**, routerlar Exchange State adımı tespit ettikleri eksik network bilgilerini LSR ve LSU paketleriyle birbirlerinden öğrenmeye başlıyorlar. Yani routerların kendilerindeki eksik link bilgilerini birbirlerinden öğrendiği adımdır.
- **Full State**, Son durumda her iki routerun da Link State veritabanları aynı oluyor ve routerlar aralarında komşuluk kurulmuş oluyor.

Komşuluk kurulduktan sonra DBD ve LSR paketleri bir daha kullanılmıyor. Routerlar aralarında belirli aralıklarla Hello paketleri göndererek birbirlerine ayakta olduklarını bildiriyorlar. Topolojiye yeni bir network eklendiğinde routerlar arasında LSU paketleriyle yeni link bilgisi paylaşıyor (Bu şekilde yeni link bilgilerinin öğrenilmesine **Incremental Updates** deniliyor). Link bilgisinin sorunsuz ulaştırıldığını göstermek için de LSack paketi kullanılıyor.

Router Id Belirleme Süreci

OSPF başlığında da görüldüğü gibi routerlar topolojide kendilerini temsil etmek üzere Router Id değeri belirliyorlar. Bu değer 32 bit uzunluğunda IPv4 adres formatındadır. Routerda komşu routerların kaydedildiği Neighbor tablosuna routerlar Router Id değerleriyle kaydedilir. Bu adres belirlenirken göz önünde bulundurulacak parametrelerin öncelik sırası;

- 1- Network yöneticisi tarafından “**router-id <Router ID>**” komutuyla manuel olarak tanımlayabiliyor.

```
R1(config-router)#router ospf 10
R1(config-router)#router-id 5.5.5.5
```
- 2- Router Id değeri manuel olarak atanmadığı durumlarda routerda tanımlanan en büyük LoopBack ip adresi (birden fazla LoopBack adres tanımlanmış olabilir) Router Id olarak seçilir.
- 3- Routerda LoopBack interface tanımlanmamışsa **routerun aktif arayüzlerinden en büyük ip adresine sahip arayüzün ip adresi Router Id olarak seçilir.**
| → Router Id değeri bir defa seçildikten sonra herhangi bir durum değişikliği olsa da değişmemektedir. Routerda seçilen Router Id değerini değiştirebilmek için tanımlanan process’in “**clear ip ospf process**” komutuyla sıfırlanması gerekir. Bu komutu kullanmak çok tehlikelidir. Nedeni bu komut kullanıldığında routerun bütün komşulukları kaldırılır. Yeniden hesaplamaların yapılması ve komşulukların kurulması gerekir. Bu işlemler router bazında kalmayıp topolojinin değişmesine/yeniden hesaplanmasına neden olacaktır. Bu nedenle kullanılması tehlikelidir.
- 4- Son durumda routerda aktif arayüz de bulunmuyorsa OSPF protokolünün başlatılmasına izin verilmiyor.

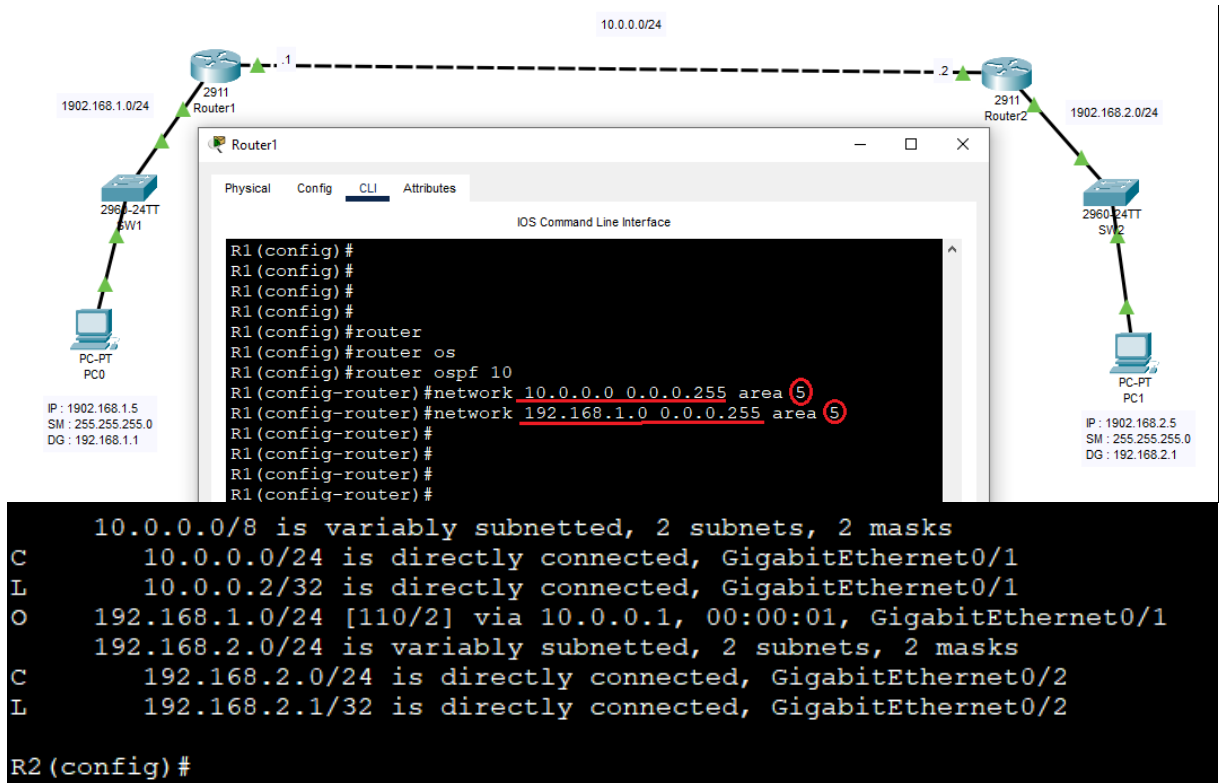
```
R1(config)#router ospf 10
OSPF process 10 cannot start. There must be at least one "up" IP interface
R1(config-router)#
```

OSPF konfigürasyonu

- İlk olarak “**router ospf <Process ID>**” komutuyla bir sayılsa değer/id verilerek (1-65535) process oluşturulur.
| → Process numarası bilgisayarlarda uygulama başlatıldığında oluşturulan proses olarak düşünülebilir. Bu değer OSPF konfigürasyonu yapılacak routerlarda farklı olabilir.
| → Bu değer farklı verilerek bir routerda birden fazla OSPF çalıştırılabilir.
| → Process Id değeri komşu routerlarda aynı olmak zorunda değil (cihaz bazında tanımlanıyor). Process Id tanımlandıktan sonra OSPF protokolünde bir değişiklik yapılmak istendiğinde buradaki Process Id değeri altında tanımlamalar yapılıyor.

```
R1(config)#router ospf 10
R1(config-router)#?
  area                OSPF area parameters
  auto-cost            Calculate OSPF interface cost according to bandwidth
  default-information  Control distribution of default information
  distance            Define an administrative distance
  exit                Exit from routing protocol configuration mode
  log-adjacency-changes Log changes in adjacency state
  neighbor            Specify a neighbor router
  network             Enable routing on an IP network
  no                  Negate a command or set its defaults
  passive-interface    Suppress routing updates on an interface
  redistribute         Redistribute information from another routing protocol
  router-id            router-id for this OSPF process
```

- Router üzerinde tanımlı networklerden OSPF protokolü ile yönlendirilmesi istenen networkler için “**network <Network Address> <Wildcard Mask> area <Area ID>**” komutuyla network adresi, Wildcard maskesi ve “area” kelimesiyle networkün yayınlanacağı Single Area OSPF numarası verilir ve temel konfigürasyon tamamlanır.
- Bu komut sonrasında OSPF protokolüyle router “network” komutuyla tanımlanan network bilgilerini komşularına göndermeye başlar. Komşu routerlarda ise hesaplanan en iyi rota yönlendirme tablosuna “O” sembolüyle eklenir.



| → Tanımlamada network adresi vermek yerine doğrudan router arayüzüne atanmış ip adresi de kullanılabilir (Subnet Mask -> 255.255.255.255, Wildcard Mask. -> 0.0.0.0 oluyor). Bu kullanım şekli aslında network yöneticisine kolaylık sağlamaktadır. Büyük bir topolojide her routerun bağlı arayüzlerindeki networkler için teker teker Wildcard Maskesi hesaplamak yerine doğrudan arayüze atanmış ip adresi kullanılarak konfigürasyon karmaşıklığının ve hata yapma olasılığının azaltılması sağlanır.

| → Tanımlamada farklı bir kullanım şekli olarak yayınlanması istenen network adreslerini oluşturulan proses altında doğrudan tanımlamak yerine network adresinin bağlı olduğu arayüze girilerek **“ip ospf <Process ID> area <Area ID>”** komutuyla arayüzde kullanılan network bilgisinin routerun tüm portlarından yayınlanması (OSPF kullanılarak) sağlanabiliyor.

Passive Interface

Passive Interface, normalde bir routerda OSPF protokolü başlatıldıktan sonra router bütün portlarından tanımlanan network bilgilerini (Hello paketlerini) yayınlamaya/göndermeye başlar. Bu paketler aynı zamanda ucunda router bağlı olmayan portlarından da gönderilir.

|→ Bir saldırganın bu portlara bağlanıp routerların Topology tablosunu ve dolayısıyla yönlendirme tablolarını manipüle edebilir.

|→ Bu portlarda Hello paketi gönderebilmek için gereksiz yere CPU ve bant genişliği harcanıyor.

Oluşturduğu risklerden dolayı ucunda router olmayan/bir networke hizmet veren arayüzlerde komşuluk kurulma ihtimali olmadığı için bu portlardan Hello paketlerinin gönderilmesi engellenebilir. Buna **Passive Interface** deniliyor. Passive Interface konfigürasyonu için routerda tanımlı process'e girilerek "**passive-interface <Interface ID>**" komutuyla ilgili arayüz belirtiliyor (Görselde, Gi 0/2 -> 192.168.1.0/24 networküne hizmet veren arayüzdür).

```
R1(config)#router ospf 10
R1(config-router)#passive-interface GigabitEthernet 0/2
R1(config-router)#exit
```

Routerlar komşuluk kuracakları zaman Hello paketleri içinde kullandıkları network tiplerini de birbirleriyle paylaşıyorlardı. Routerların kullandığı bağlantı tipinin **Ethernet** olduğu durumlarda bağlantının MultiAccess network olma ihtimaline karşı routerlar aralarında DR ve BDR seçimi yapmaktadır. Eğer ki routerlar birbirine doğrudan bağlıysa (yani MultiAccess bir ortam yoksa) routerlar arasındaki bağlantıyı Point-to-Point tipine dönüştirebiliriz. Bu sayede gereksiz yere DR ve BDR seçimi yapılmasına gerek kalmıyor. Bunun için routerlarda ilgili arayüze girilerek (komşu router ile bağlı olunan arayüze) "**ip ospf network point-to-point**" komutu kullanılıyor. Bu konfigürasyonun komşu routerlar arasında karşılıklı olarak uygulanması gertkiyor.

```
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip ospf network point-to-point
R1(config-if)#exit
```

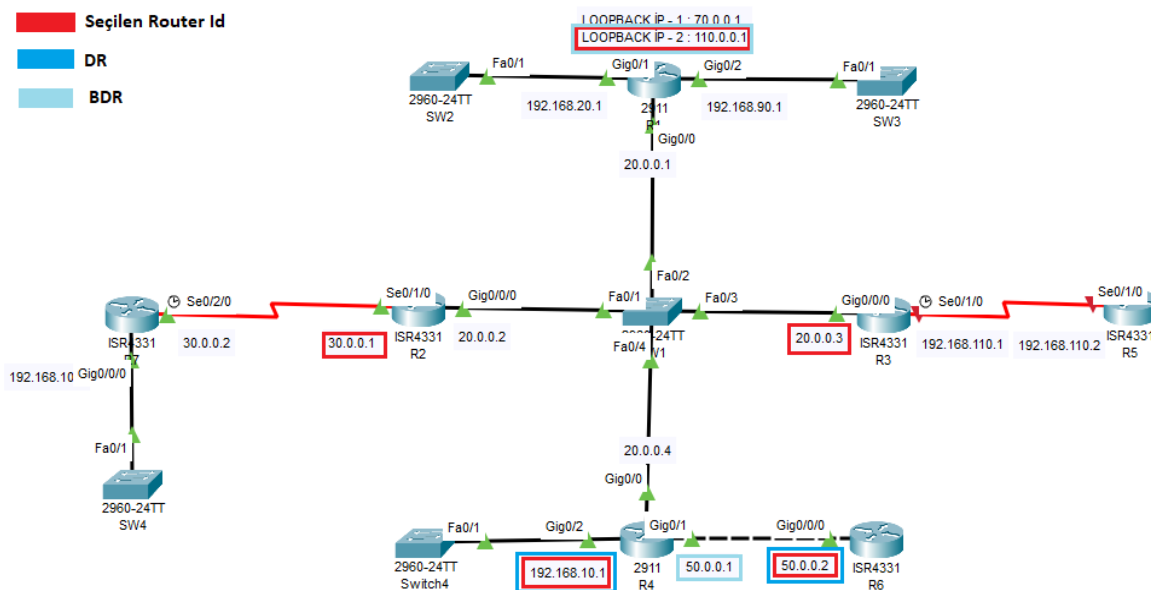
DR ve BDR Belirleme Süreci

- Sadece broadcast MultiAccess ortamlarda DR ve BDR seçimi yapılır (Ethernet topolojisi).
- Ethernet topolojisinde mutlaka bir tane DR router seçilir. BDR seçimi yapılmayabilir.
 - DR router seçiminde öncelikle routerların Priority değerlerine (Yüksek olan DR seçilir) bakılır. Bu değer varsayılanda 1'dir. Bu değer ilgili portun arayüzüne girilerek "**ip ospf priority <Priority Number>**" komutuyla değiştirilebilir.

```
RX(config)#interface gigabitEthernet 0/0/0
RX(config-if)#ip ospf priority ?
    <0-255> Priority
RX(config-if)#ip ospf priority 200
RX(config-if)#exit
```

|→ Bir arayüze Priority değeri 0 verilirse bu arayüz hiçbir zaman DR veya BDR router olarak seçilemiyor.

|→ DR ve BDR seçimi için harcanan süreye **Wait Interval** deniliyor.



OSPF Metric (Cost)

OSPF protokolünde bir paketi hedefe gönderebilmek için en iyi rota **Cost** adı verilen bant genişliklerini baz alarak belirliyor. Bu değer network admini tarafından "**ip ospf cost <Cost>**" komutuyla manuel olarak değiştirilebiliyor.

```
RX(config)#interface gigabitEthernet 0/0/0
RX(config-if)#ip ospf cost ?
<1-65535> Cost
RX(config-if)#ip ospf cost 20
RX(config-if)#exit
```

Network admini tarafından belirtilmeyen Cost değerinde ise portun bant genişliği baz alınıyor. Portun bant genişliği varsayılanda 100 Mbit gelen referans değerine bölünerek hesaplanıyor (**Cost = Bant genişliği / 100 Mbit**).

Ne yazık ki bu değer günümüz bant genişliklerine kıyasla çok düşük kalmaktadır. Yani 100 Mb'ten büyük bant genişliğine sahip portlarda sonuç her zaman 1 çıktığı için (sonuç tam sayı olmak zorunda) en iyi rota seçilemiyor. Bu nedenle OSPF tanımlı process altına girilerek referans bant genişliği "**auto-cost reference-bandwidth <Bandwidth>**" komutuyla güncellenmesi gerekiyor (giriş değeri Mbit cinsinden algılanıyor).

```
RX(config)#router ospf 10
RX(config-router)#auto-cost reference-bandwidth ?
<1-4294967> The reference bandwidth in terms of Mbits per second
RX(config-router)#auto-cost reference-bandwidth 10000
RX(config-router)#exit
```

| → Referans bant genişliği değeri topolojideki en yüksek bant genişliği baz alınarak belirlenmesi gerekiyor. Burada dikkat edilmesi gereken kritik nokta **belirlenen referans bant genişliğinin topolojideki bütün routerlarda aynı olması gerekiyor**. Aksi taktiden en iyi rota seçimi doğru şekilde yapılamayacaktır.

| → Referans bant genişliği çok yüksek verildiği zaman ise bant genişliği düşük portların Cost değerleri çok yüksek oluyor. Bu durumda rotalar belirlenirken toplanan bu değerlerin sonucu rota tanımında alınabilecek sınır değerlerini aşabiliyor.

OSPF Intervals

Routerlar arasında komşuluk kurulduktan sonra belirli aralıklarla birbirlerine Hello paketleri gönderdiklerinden bahsedilmişti. Bunlar **Hello Interval** ve **Dead Interval** olmak üzere iki tanedir. Bu süreler ise ilgili arayüze girilerek "**ip ospf (hello-interval | dead-interval) <Time>**" komutuyla konfigüre edilebiliyor.

```
RX(config)#interface gigabitEthernet 0/0/0
RX(config-if)#ip ospf hello-interval ?
<1-65535> Seconds
RX(config-if)#ip ospf hello-interval 2
RX(config-if)#ip ospf dead-interval ?
<1-65535> Seconds
RX(config-if)#ip ospf dead-interval 8
RX(config-if)#exit
```

| → Karşılıklı iki routerda Hello interval ve Dead interval süreleri aynı olmadığı durumlarda komşuluk kurulamaz. Kurulan komşuluklar da koparılır/silinir. Doğal olarak bu komşuluk üzerinden öğrenilen rotalar da yönlendirme tablolarından kaldırılır.

| → Network erişiminin kritik olduğu yerlerde kesintilerin daha hızlı anlaşılıp gerekli aksiyon alınabilmesi için bu değerler değiştirilebilir.

Static Default Route Propagation

Bir topolojideki network trafiğini internete çıkarabilmek için yönlendirme tablosuna default rota tanımlanması gerekiyor. Bunun için **sadece internete çıkış routeru üzerinde “ip route 0.0.0.0 0.0.0.0 <next hop>”** komutuyla statik default rota tanımı yapılıyor. Bu tanımlama sonrasında OSPF protokolünün çalıştığı process atrlına girilerek **“default-information originate”** komutuyla tanımlanan statik default rotanın OSPF protokolü üzerinden topolojideki bütün routerlara otomatik olarak bildirilmesi sağlanıyor (Burada router topolojideki diğer routerlara, kendisinde statik default rota tanımı olduğunu ve hedef adresleri yönlendirme tablosunda bulunmayan paketlerin kendine gönderilmesi gerektiğini bildiriyor). Bu sayede topolojideki herhangi bir routerun internet routeruna tanımlı rotasında bir kesinti yaşandığında, OSPF protokolü kullanılarak internet routeruna (interneteye çıkmak için kullandığı router) erişim için kullanılan default rota hesabı yeniden yapılıyor ve bu sayede routerun internete bağlantısının devamlılığı sağlanıyor.

```
RX(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.1
RX(config)#router ospf 10
RX(config-router)#default-information originate
RX(config-router)#exit
```

Buradaki 10.0.0.1 adresi, topolojideki internete çıkış routerunun ISP routeruna bağlı arayüzündeki next hop adresidir.

OSPF Protokolünde Default Statik Rota tanımının aynı Area'da bulunan routerlara öğretilmesi için **“default-information originate”** komutu kullanılıyordu. Cihaz üzerinde tanımlı tüm statik rota tanımlarının aynı Area'daki routerlara öğretilmesi isteyorsa OSPF konfigürasyon modunda **“redistribute static”** komutu kullanılıyor. Aynı komut EIGRP protokolünde de kullanılıyordu. Bu komut kullanılarak farklı dinamik yönlendirme protokolleri arasında rota aktarımı da sağlanabiliyor.

- Harici öğretilen rotalar External Route Type 1 ve External Route Type 2 olmak üzere iki şekilde öğretilabiliyor. Varsayılanda Type 2 olarak geliyor. Değiştirmek için OSPF konfigürasyon modunda **“default-information originate metric-type <Metric Type>”** komutu kullanılıyor.
- Default Cost değeri Default Statik Rota için -> 1, Harici herhangi bir Rota için-> 20 olarak belirleniyor Öğretilecek harici rota bilgisinin başlangıç değerini değiştirmek için OSPF konfigürasyon modunda **“default-information originate metric <Metric Value>”** komutu kullanılıyor.
 - o External Route Type 1, bunun anlamı harici rota tanımını OSPF protokolüne ekle ve her router için Cost değeri hesaplanarak öğretilsin demektir.
 - o External Route Type 2, bunun anlamı harici rota tanımını default bir Cost değeriyle OSPF protokolüne ekle ve aynı Area'da bulunan bütün routerlarda bu değer (Cost) değişmeden yönlendirme tablolarına işlensin demektir.

```
Router(config)#router ospf 10
Router(config-router)#redistribute ?
  bgp          Border Gateway Protocol (BGP)
  connected    Connected
  eigrp        Enhanced Interior Gateway Routing Protocol
               (EIGRP)
  metric       Metric for redistributed routes
  ospf         Open Shortest Path First (OSPF)
  rip          Routing Information Protocol (RIP)
  static       Static routes
Router(config-router)#
```

OSPF Authentication Konfigürasyonu

OSPF protokolünde güvenliği arttırabilmek için komşuluk kurulurken kimlik doğrulama mekanizması kullanılabilir. OSPFv2 için kimlik doğrulama mekanizması 3 farklı şekilde uygulanabilir (bu konfigürasyonların routerlarda karşılıklı olarak uygulanması gerekiyor. Aksi takdirde komşuluk kurulamaz). Bunlar;

- 1- Plain Text Authentication, parolal bilgisinin plain-text olarak taşındığı konfigürasyondur. Bu konfigürasyon için öncelikle ilgili arayüzde “**ip ospf authentication**” komutuyla kimlik doğrulama mekanizması devreye alınıyor. Ardından “**ip ospf authentication-key <Password>**” komutuyla komşu routerla kurulacak bağlantıda kullanılacak parola tanımı yapılıyor.

```
R1(config)#int gi 0/0
R1(config-if)#ip ospf authentication
R1(config-if)#ip ospf authentication-key MyPass
R1(config-if)#exit
```

- Parola Plain Text gittiği için güvenli değildir.

- 2- MD5sum Hash, parolal bilgisinin MD5 algoritması kullanılarak taşındığı konfigürasyondur. Bu konfigürasyon için öncelikle ilgili arayüzde “**ospf message-digest-key <Key Number> md5 <Password>**” komutuyla kullanılacak parola bilgileri tanımlanıyor. Ardından “**ip ospf authentication message-digest**” komutuyla kimlik doğrulama mekanizması devreye alınıyor.

```
R1(config)#int gi 0/0
R1(config-if)#ip ospf message-digest-key 1 md5 My Pass
R1(config-if)#ip ospf authentication message-digest
R1(config-if)#exit
```

- MD5 algoritması günümüzde güvenli kabul edilmemektedir.

- 3- HMAC SHA Hash, parolal bilgisinin SHA algoritması kullanılarak taşındığı konfigürasyondur. Bu konfigürasyon için ilk olarak “**key chain <Key Chain Name>**” komutuyla bir key chain oluşturulur. Bu arayüz altında;

- Key tanımı oluşturmak için “**key <Key Number>**” komutuyla yeni bir anahtar numarası oluşturulur. Bu anahtar altında;
 - Algoritma seçimi için “**cryptographic-algorithm <Algorithm Type>**” komutu kullanılır.
 - Kimlik doğrulama için kullanılacak parola bilgisi “**key-string <Password>**” komutuyla tanımlanır.

Key Chain tanımı tamamlandıktan sonra kimlik doğrulama mekanizmasını uygulamak için portların arayüzlerine giriş yapılarak “**ip ospf authentication key-chain <Key Chain Name>**” komutu kullanılır.

```
R1(config)# key chain SHA256
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string ospfSHA256
R1(config-keychain-key)# cryptographic-algorithm hmac-sha-256
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)# interface s0/0/0
R1(config-if)# ip ospf authentication key-chain SHA256
R1(config-if)#
```

SORU : Broadcast MutliAcess bir ortamda sadece bir routerun Priority değeri yüksekse (bu router DR seçilecektir) BDR seçimi için hangi özelliğe bakılır ?

Router Id değerleri göz önünde bulundurularak seçilir.

SORU : Routera dışarıdan bağlanarak OSPF protokolüyle çok fazla network bilgisi göndererek Topoloji tablosunu veya yönlendirme tablosunu doldurabilir miyim ? Doldurulabilirse router nasıl davranır ?

BGP protokolüyle rota öğretilmek istendiğinde OSPF protokolü çatlatılabilir. Detaylar için **CCNP - 06 – OSPF** yazıma göz atabilirsin (ek olarak bakabilirsin; https://www.blackhole-networks.com/OSPF_overload/).

NOT :

- SPF algoritması matematik bilminde **Dijkstra** algoritması olarak da biliniyor.
- **Altın kural :** Muli Area OSPF yapılacağı durumda bir Area 0 oluşturulur (BackBone Area) ve bütün Single Area'lar Area 0'a bağlanarak farklı Single Area'lar ile haberleştirilebilir.
- OSPFv6'da IPv6 desteği gelmiştir. Yani hem IPv4 hem de IPv6 destekliyor.
- Ethernet kullanılan bağlantılarda iki router birbirine doğrudan bağlı da olsa routerlar bunu anlayamadığı için aralarında DR ve BDR seçimin yapar. Bu nedenle düzenlemenin manuel olarak yapılması gerekiyor.
- OSPF konfigürasyon sırasında dikkat edilmesi gereken nokta Multi Access Network üzerinde OSPF konfigürasyonu yapılan ilk router Router ID değerini karşılaştıracığı başla router bulamayacağı için kendisini DR ilan edecektir (DR router da bir aksilik olması süreci değiştirmiyordu). Bu nedenle OSPF konfigürasyonu yapılırken router sırasına dikkat edilmelidir.
- Aynı Router Id değerine sahip routerlar komşuluk kurmuyor. Eğer ki aynı Area içerisinde farklı routerlara bağlı durumdalarsa topolojide dalgalanmalar yaşanır.
- Bir sorun yaşandığında troubleshooting yapılırken kontrol edilen ilk şey topolojide yapılan son değişikliktir.
- Buradan OSFP protokolüyle öğrenilen rotaların Administrative Distance değerinin 110 olduğu da görülebiliyor.
- Açıklamalarda adı geçen **Ethernet/Ethernet topolojisi**, birbirine Ethernet portlarıyla (GigabitEthernet-FastEthernet) bağlanan cihazları temsil etmek için kullanılmaktadır.
- **Bir topolojide OSPF algoritması konfigüre edilirken aktif arayüzlere bağlı olarak Router Id belirleniyor. Router Id değeri ise DR ve BDR seçimini de etkili. Yani OSPF konfigürasyonunda hangi routerla konfigürasyona başladığı önemli bir ayrıntıdır. Sonuçta diğer routerlar konfigüre edilene kadar en yüksek Router Id değerine sahip router ilk konfigüre edilen router olacaktır (Unutma Router Id ve DR seçimi bir defa yapılmaktadır).**
- OSPF protokolünde portların hızı port tipine bakılarak karar veriliyor. Yani GigabitEthernet portu ise 1Gbit bant genişliği baz alınarak Cost değeri hesaplanıyor ama bu porttan 1Gbit'ten daha düşük veri iletimi yapılıyor olabilir. Bu durumda bant genişliğinin doğru hesaplanabilmesi için ilgili arayüze girilerek "**bandwidth <Bandwidth>**" komutuyla portta kullanılan bant genişliği dinamik yönlendirme protokolüne bildirilebiliyor. Bu komut sadece portun bant genişliğini dinamik yönlendirme protokolüne belirtmek için kullanılır. Yani bu komut porttaki bant genişliğini etkilemiyor.

```
RX(config)#interface gigabitEthernet 0/0/0
RX(config-if)#bandwidth ?
<1-10000000> Bandwidth in kilobits
RX(config-if)#bandwidth 100000
RX(config-if)#exit
```

- Büyük topolojilerde konfigürasyonlar yapılırken he konfigürasyonları hızlandırmak hem de konfigürasyon sırasında oluşabilecek hata riskini en aza düşürebilmek için konfigürasyonlar bir text editörüne yazılarak routerlara toplu şekilde uygulanıyor.

- Networkün kritik olduğu yerlerde belirli zamanlarda bekletilen yedeklemeler devreye alınarak kontrol ediliyor. Bu kontrolün yapılma nedeni kullanımda olan cihazlarda bir aksama olduğunda yedeklemelerin sorunsuz devreye alınıp alınmadığını /doğru çalışıp çalışmadığını kontrol edebilmektir.
- Normade Multi Access bir ortamda routerlar bütün routerlarla Full-State duruma geçmezler. Sadece DR ve BDR ile iletişim içerisinde olacağı için DR ve BDR ile Full-State'e geçerler. Bağlanan diğer routerlarla tam komşuluk kurulmaz. Two-Way State'de kalırlar.

Terimler :

- Convergence, topolojiye yeni bir network eklendiğinde bu networkü topolojideki bütün routerların dinamik olarak öğrenmesi için geçen süreye denilmektedir.
- Periodic Flooding Behavior, OSPF protokolünde her 30 dakikada bir routerların topolojiye yeni network eklenip eklenmediğini kontrol ettiği güncelleme tipidir. Yani her 30 dakikada bir router öğrendiği linklerin bir kopyasını bütün komşularına gönderiyor.
- Wildcard Mask, subnet maskesinden 255.255.255.255 çıkarılmış halidir. Yani subnet bilgisinin tam tersi de denilebilir.

Kontrol Komutları

- sh ip protocols
- sh ip ospf interface <Interface ID>
- sh ip ospf interface brief
- sh ip ospf neighbor
| → Bu komut çok önemli çünkü OSPF protokolünde bir sorun yaşandığında ilk kontrol edilen şey routerun komşuluk tablosudur (Komşuluk kurulmadan hiçbir bilgi paylaşılmıyordu).
- sh ip ospf