BEYKENT ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

MPLS OMURGA TASARIMI

Yüksek Lisans Tezi

Taner BAŞULAŞ, B.Sc.

Bölüm: Bilgisayar-Matematik Anabilim Dalı

Program: Bilgisayar Ağları ve İnternet Teknolojileri

Tez Danışmanı: Dr. Rifat ÇÖLKESEN

İstanbul 2006

ÖNSÖZ

MPLS, günümüz veri iletişim ağlarında ATM teknolojisine göre IP portları maliyetlerinin ucuzlamasıyla ve IP trafiğinin yönlendirilmesinde sağladığı avantajlar nedeniyle servis sağlayıcılar tarafından tercih edilen bir teknolojidir. MPLS teknolojisi kullanılarak, IP üzerinden ses taşıma, IP üzerinden video ve televizyon yayını gibi servis sağlayıcıların sunmayı düşündükleri yeni nesil servisler, internet erişimi ve noktadan noktaya veri taşıma servisleri aynı omurgada sağlanabilmektedir.

Bu çalışmada omurgasını MPLS teknolojisi ile çalıştırmak isteyen servis sağlayıcıların omurga tasarımında nasıl bir yol izlemeleri gerektiği anlatılacaktır. Bu çalışmanın MPLS teknolojisinin uygulanması ve kullanılması konularında okuyanlara yol göstermesini temenni ederim.

Bana bu konuda çalışma imkanı sunan danışmanım Sayın Dr.Rifat ÇÖLKESEN (Beykent Üniversitesi) ve yorumları ile bana fikir veren çalışma arkadaşım Sayın Ercan ATASOY'a (Alcatel Teletaş) teşekkürlerimi sunarım.

KISALTMALAR

AAL : Asynchronous Transfer Mode Adaptation Layer

ADSL : Asynchronous Digital Subscriber Line

AF : Assured Forwarding

AS : Autonomous System

ATM : Asynchronous Transfer Mode

BDR : Backup Designated Router

BA : Behavior Aggregate

BGP : Border Gateway Protocol

BGP ID : Border Gateway Protocol Identification

BRAS : Broadband Remote Access Server

CLNS : Connectionless Network Service

CLNP : Connectionless-mode Network Protocol

CoS : Class of Service

CR-LDP : Constraint-based Routed Label Distribution Protocol

DOD : Downstream on Demand

DOU : Downstream Unsolicited

DR : Designated Router

DSCP : DiffServ Code Point

E-LSP : EXP-Inferred-PSC LSP

EF : Expedited Forwarding

ESH : End-System Hello

FEC : Forwarding Equivalence Class

FIB : Forwarding Information Base

ES : End System

ESH : End System Hello

Exp : Experimental

FRR : Fast Reroute

GigE : Gigabit Ethernet

G.SHDSL : Global.Standard High-Bit-Rate Digital Subscriber Line

IANA : Internet Assigned Numbers Authority

IBGP : Internal Border Gateway Protocol

IETF : Internet Engineering Task Force

IGP : Interior Gateway Protocol

IP : Internet Protocol

IPv6 : Internet Protocol version 6

IS-IS : Intermediate System to Intermediate System

L-LSP : Label-Only-Inferred-PSC LSP

LDP : Label Distribution Protocol

LER : Label Edge Router

LFIB : Label Forwarding Information Base

LIB : Label Information Base

LSR : Label Switch Router

LSP : Label Switched Path

LSA : Link State Advertisement

MD5 : Message Digest 5

MPLS : Multi Protocol Label Switching

MTU : Maximum Transmission Unit

NASP : Network Service Access Point

NSSA : Not So Stubby Area

OSI : Open Systems Interconnection

OSPF : Open Shortest Path First

OSPFv2 : Open Shortest Path First version 2

PE : Provider Edge

PHB : Per Hop Behaviour

POS : Packet over Sonet

QoS : Quality of Service

RFC : Request For Comment

RSVP : Resource Reservation Protocol

RSVP-TE : Resource Reservation Protocol – Traffic Engineering

STM : Synchronous Transfer Mode

TCP : Transmission Control Protocol

ToS : Type of Service

TTL : Time to Live

UDP : User Datagram Protocol

VPN : Virtual Private Network

ŞEKİLLER

TABLOLAR

ÖZET

Servis sağlayıcıların omurga tasarımlarında bir çok faktörü göz önünde bulundurmak durumundadırlar. Bunlar yüksek performansı sağlayacak şekilde tasarlanması, ölçeklenebilir olması ve dayanıklı olmasıdır. Omurganın fiziksel yapısı planlanırken bu üç özelliği sağlayacak şekilde tasarlanması MPLS teknolojisi ile çalışacak omurgada yeterli olmaz. MPLS teknolojisi ile çalıştırılacak bir omurgada diğer düşünülmesi gereken faktörler mantıksal protokol işleyişidir.

MPLS çalışacak omurgada kullanılabilecek dahili yönlendime protokolü OSPF veya IS-IS olabilir. Dahili yönlendirme protokolleri mantıksal IP adresleme bilgisinin omurgadaki bütün yönlendiricilere dağıtılmasından sorumludurlar. Ayrıca BGP omurganın bulunduğu otonom sistemin diğer otonom sitemlerle haberleşmesi için gereklidir. İnternet erişimi için trafik toplama noktaları olarak düşünebileceğimiz geniş bant erişim sunucuları omurgada MPLS çalışacak yönlendiricilere bağlı olacaklardır. Bu durumda MPLS yönlendiriciler internet trafiği bilgisini BGP protokolü ile öğreneceklerdir. LDP protokolü etiketleme bilgisinin omurgadaki MPLS çalışan yönlendiriciler tarafından öğrenilmesinden sorumludur. LDP hangi ağın nerede olduğu bilgisini OSPF'ten öğrenir ve OSPF'ten edindiği bilgiye göre etiketleme görevini yapar.

LDP'nin tasarım olarak barındırdığı bir dezavantajı bir ağa erişimi kaybolduğunda bir üst yönlendiriciye gönderdiği LABEL RELEASE mesajının teyitini beklemeden bu ağ ile eşleştirdiği etiketi serbest bırakmasıdır. LABEL RELEASE mesajı bir üst yönlendiriciye ulaşmadığında yönlendirici kendisine gele be söz konusu ağa gitmesi gereken paketleri yönlendirmeye devam edecek ve trafik kayıpları oluşacaktır.

Önerilen çözüme göre bu kayıpların yaşanmaması için yoğun trafik yükü taşıyan genişbant erişim sunucuların trafiği dinamik değil statik LSP'lerle taşınacaktır ve bu statik tüneller FRR yöntemi ile korunacaktır. Statik tünellerin çekirdekte sonlanacağı yapıda, statik LSP'ler için RSVP, dinamik LSP'ler için LDP kullanılacaktır. Bu şekilde üzerinde yüksek miktarda trafik bulunduran genişbant erişim sunucularının trafiği korunmuş olacaktır

1. GİRİŞ

Bu çalışmada MPLS (Çoklu Protokollü Etiket Anahtarlama) teknolojisi ve İnternet Servis Sağlayıcı'ların (İSS) omurgalarında MPLS teknolojisini nasıl kullanabilecekleri ile MPLS omurga tasarımı anlatılacaktır. Tezin içeriğinde öncelikli olarak İSS omurgasında bulunması gereken özellikler ve işleyiş şekli ele alınacaktır. Omurgada kullanılabilecek dahili ve harici yönlendirme protokolleri tanıtılacak, ardından MPLS teknolojisi özellikleri, yetenekleri ve avantajları incelenecektir. MPLS teknolojisi kullanan servis sağlayıcı omurgaların tasarımında düşünülmesi gereken faktörler ve tasarım önerileri ile MPLS çalışan omurga tasarımı ayrıntılı ortaya koyulacaktır. Son bölümde örnek tasarım önerisi sunulacak, MPLS'in bu tasarımda sağladığı faydalar belirtilecektir.

2. OMURGA TASARIMINDA BULUNMASI GEREKEN ÖZELLİKLER

2.1 Omurganın Özellikleri ve Görevi

2.1.1 Performans

Ağ tasarımında ve özellikle omurga tasarımında performans düşünülmesi gereken çok önemli bir faktördür. Bunun için ağ genelinde kullanılan cihazlar, ağ üzerinde bulunan noktaları birbirine bağlamak için kullanılan hatlar ilerleyen zamanlarda da ihtiyaca cevap verebilecek ölçekte ve yetenekte olmalıdır. Ağın performansını ölçmek için gözönünde bulundurulması gereken kriterler cevap verme süresi, ağ üzerinden taşınabilecek trafik miktarı ve kullanım oranıdır.

Cevap verme süresi, müşterilere sağlanan servis dahilinde, müşterinin servis hızını ne olarak algıladığı şeklinde yorumlanabilir. Cevap verme süresi bağlantı hızı, ağ üzerinde herhangi bir yerde meydana gelen tıkanıklık ve kullanılan protokoller ile cihazların trafiği işleme süresi ile doğrudan bağlantılıdır. Cevap verme süresi ağ üzerinde meydana gelen bağlantı kesintisi cihaz arızası gibi problemlerde, servisin kesintisiz verilmesini veya müşteriyi en az rahatsız edecek zaman aralığında sürekliliğini sağlayacak şekilde mümkün olduğu kadar kısa tutulmalıdır. Bu ise uygun yönlendirme protokollerini kullanarak sağlanabilir.

Ağ üzerinde taşınan trafik miktarı ve kullanım oranı performansı etkileyen bir diğer faktördür. Bu kriter ağ üzerinde bir düğümden geçilirken, o cihazın ilgili hattın kullanım miktarı olarak veya kullanılmakta olan cihazların birim zamanda işlediği trafik miktarı şeklinde düşünülmelidir. Ağ kullanımının %100'e yaklaştığı durumlarda performansın düşeceği aşikardır. Ağın olası trafik sıçramaları gözönünde bulundurularak her zaman için belli bir kapasitenin boş kalması gerektiği unutulmamalıdır.

Performans düşüklüğüne sebep olmamak için düşünülmesi gereken bir diğer faktör ise yönlendirme bilgisinin omurga genelinde gereksiz ise yayılmasını engellemektir. Omurga fazla büyükse ilgili anonsun ilgili alanlar içinde kalmasını sağlamak amacıyla kullanılan yönlendirme protokole göre (OSPF veya IS-IS) uç noktaların sınırlı alanlar içinde kalması ve gerekmediği taktirde omurgaya yönlendirme protokolü anonsları yapması engellenebilir.

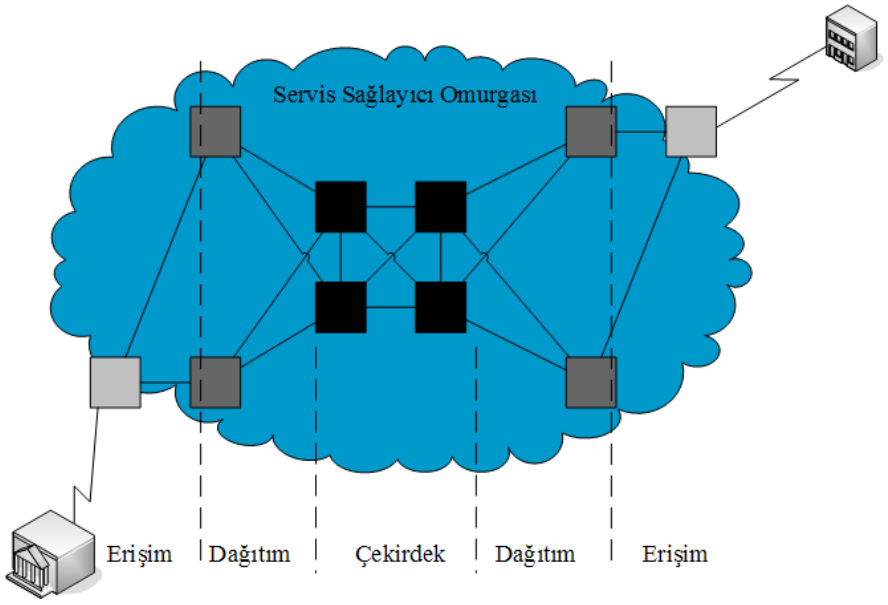
2.1.2 Ölçeklenebilirlik

Ağ tasarımında günün koşullarının sağlanmasının yanında, ilerleyen zamanlarda doğabilecek ihtiyaçlar gözönünde bulundurularak ölçeklenebilir bir şekilde tasarım edilmesi gerekir. Ağın ölçeklenebilir olması, ihtiyaç halinde genişlemeye imkan sağlayacak şekilde tasarlanmasıdır. Ölçeklenebilir bir ağ tasarımında, ölçeklenebilir olması gereken elementler topoloji ölçeklenebilirliği, adresleme ölçeklenebilirliği ve kullanılacak yönlendirme protokolünün ölçeklemeye uygun genişlemeye müsait bir yönlendirme protokolü olmasıdır.

Topolojinin genişlemeye müsait bir şekilde tasarlanması gerekir, dolayısıyla hiyerarşik bir yapıda olması gerekir. Günümüz ağlarında topoloji ölçeklenebilirliği ve hiyerarşik tasarım, ağın ölçeklenebilir olması konusunda vazgeçilmezdir. Kabul gören ve uygulanan anlayışa göre ağ hiyerarşik olarak üç temel bölümden oluşur. Bunlar sadece anahtarlama yapan ve servis kalitesi, filtreleme ve başlık biligisi değişikliği yapılmayan *çekirdek*, müşterinin IP yönlendirilmesinin yapıldığı, gerektiği takdirde servis kalitesi tanımlarının yapıldığı *dağıtım* ve müşterinin omurgaya erişimin sağlandığı ve erişim kontrollerinin yapıldığı *servis sağlayıcı uç cihazları* (PE) şeklinde sınıflandırılabilir.[1] Omurganın çekirdeği yüksek miktarda

trafik taşır ve bu yüksek miktardaki trafiği en hızlı anahtarlayacak özelliklerde olması gerekir. Dağıtım katmanının özelliği uç notaların konsantrasyon noktası olması ve çekirdek ile erişim noktaları arasında iletim görevi görmesidir. Diğer omurgalardan gelen trafik dağıtımı bu katman üzerinden yapılır. Hiyerarşik şekilde tasarlanan ağ omurgalarında tasarım adımlarını belirlemenin kolaylaşmasının yanında, olası problemlerin lokalize edilmesi ve sorunun giderilmesi de kolaylaşır.

Bir diğer ölçeklemeye müsait şekilde tasarlanması gereken IP adreslemeleridir. IP adreslerinin hiyerarşik bir yapıda dağıtılması, bir kısmının daha sonra ihtiyaç halinde kullanılmak üzere ayrılması edilmesi, hiyerarşik şekide tasarlanan toplojide adres özetlemeye inkan verecek şekilde IP adresleri dağılımı yapılması bu başlık altında düşünülmesi gereken faktörlerdir. IP adres dağılımı uygun şekilde yapılırsa, yönlendirme bilgisinin dağıtılması ve IP adreslerinin anons edilmesi için kullanılacak yönlendirme protokolünün de daha verimli çalışması sağlanabilir. Bununla birlikte kullanılan yönlendirme cihazlarında işlemci gücünün ve belleğin daha verimli kullanılması sağlanmış olur. Ağda meydana gelmesi muhtemel bağlantı kesintilerinde omurga üzerindeki yönlendirme bilgisinin daha kısa zamanda ve müşteri tarafında probleme sebep olmayacak kadar kısa bir sürede güncellenmesine uygun bir altyapı hazırlanmış olur



Şekil 2.1.2.i: Servis sağlayıcı omurgasında hiyerarşik tasarım

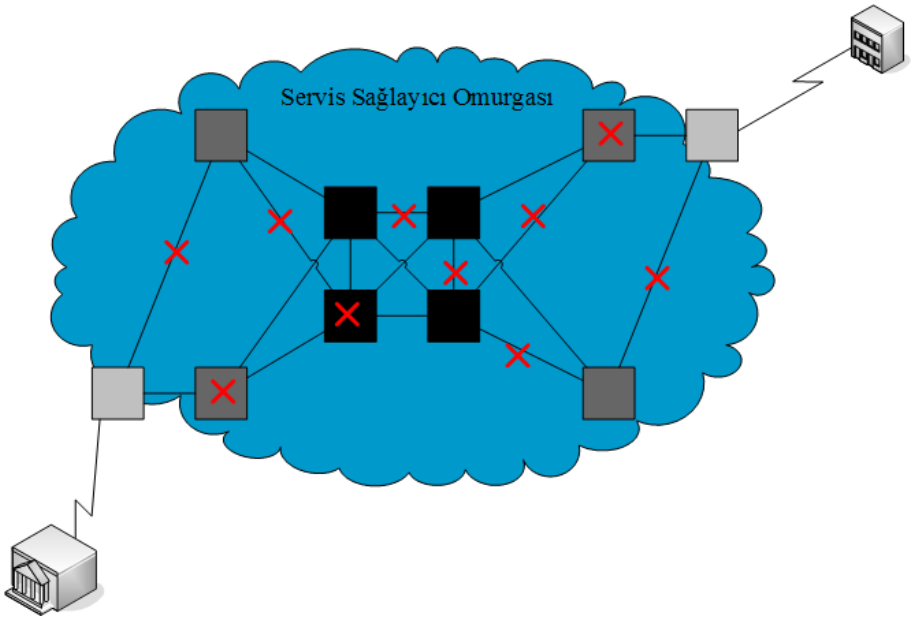
2.1.3 Dayanıklılık

Dayanıklılık, omurgada meydana gelen arıza ve problemlerin verilen servisi etkilememesi olarak tanımlanabilir. Omurga tasarımında mutlaka gözönünde bulundurulması ve uygulanması gereken bir özelliktir. Dayanıklılık, hat yedekliliği, cihaz yedekliliği ve hatta cihazlar üzerinde arayüzlerin bulundurulduğu kart yedekliliği şeklinde düşünülmelidir.

Bağlantı yedekliliği her cihaz için farklı kartlardan, farklı transmisyon alt yapısının kullanılması sağlanarak, farklı cihazlara çekirdeğe doğru yukarı yönde en az iki tane bağlantı verilmesi şeklinde olmalıdır. Bu şekilde ağ üzerinde hatlarda tek bir kırılma noktasnın önüne geçilmiş olur. Bununla birlikte sağlam kalan bağlantı bant genişliğinin toplam trafiği taşıyabilecek kapasitede olması sağlanmalıdır.

Cihaz yedekliliği, üst bağlantıların farklı cihazlara bağlı olmasının yanında, cihazın bağlantılarının farklı arayüzlerden gerçekleşmesi sağlanarak yapılmalıdır. Bu durumda bağlantının olduğu portta veya kartta meydana gelmesi muhtemel bir arıza serviste kesintiye yol açmayacaktır. Yedekli tasarlanan bir ağ, yazılım güncellemesi ile donanım güncellemesi ve bakımı gibi çalışmalarda müşteriye sunulan serviste kesintiye gidilmeden çalışılmasına da imkan sağlamaktadır. Bununla birlikte dikkat edilmesi gereken önemli bir nokta, veri ağına hizmet verecek olan iletim şebekesinin yedekliliğidir. Aynı şehirde sonlanacak bağlantıların farklı iletim şebekelerini kullanması, iletim şebekesinde meydana gelecek olan muhtemel arızalarda o noktanın hatlarının tamamı ile çalışmaz hale gelmesine engel olur. Şekil 2.1.3.i'de, iletim şebekesi veya yönlendiricilerde meydana gelen muhtemel problemler nedeniyle çarpı işaretli hatlar çalışmasa da trafik akışında sorun yaşanmayacaktır.

Yedekliliğin topolojik ve donanımsal olarak sağlanmasının yanında, meydana getirilen yedekli ağın en verimli şekilde kullanılmasına imkan sağlayan teknolojiler ile yedeklilik bütünlüğü sağlanılmalıdır. Hat yedekliliği sağlamanın yanında, bağlantıların yedekli veya aynı ayda trafik yükünü dağıtarak kullanılmasına imkan sağlayan yönlendirme protokolleri yedekli topolojinin verimli kullanımına izin verir.



Şekil 2.1.3.i: Omurgada hat yedekliliği

2.2 Servis Sağlayıcıların Sundukları Hizmetler

Servis sağlayıcıların sundukları en temel hizmet, İnternet erişim hizmeti, veya farklı lokasyonları bulunan müşterilerin lokasyonları arasında erişimi sağlamaktır. Veri haberleşmesinin en basit örneği olan bu modelde aboneler genellikle e-posta ve sunucu-istemci erişimi gibi temel sistemlerini servis sağlayıcının omurgası üzerinden taşırlar.

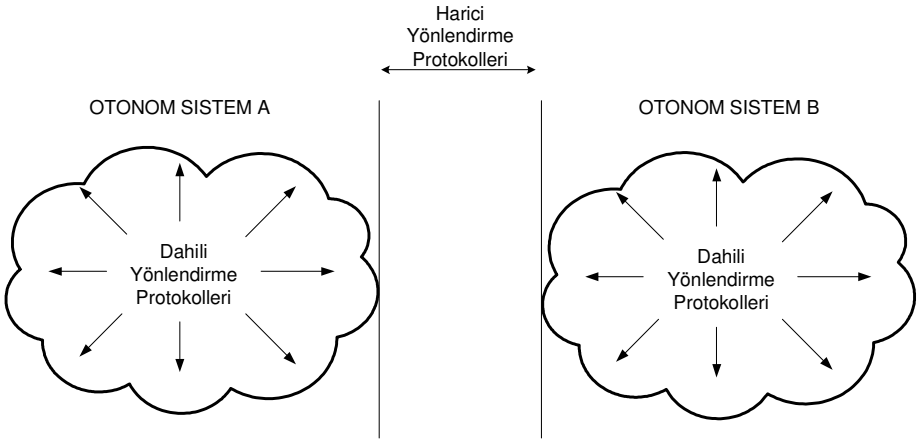
Bir diğer hizmet günümüzde popüler hale gelen ses taşımasıdır. Klasik santral sistemlerinin maliyetlerinin İnternet üzerinden ses taşıma maliyetleri ile rekabet edememesi sonucu olarak İnternet üzerinden ses taşımak özellikle de uzak mesafeler için oldukça cazip hale gelmiştir. Günümüzde servis sağlayıcı şirketler ilgili lisansları ile ses taşıma hakkına sahip oldukları takdirde, bunu ürün olarak abonelere ses taşıma hizmeti olarak sunmakta ve ses iletimini kendi omurgaları üzerinden sağlamaktadırlar. Ancak ses iletimi servisinin kaliteli bir şekilde yapılması için servis kalitesinin üst düzeyde sunulduğu, yüksek hızlı bağlantılardan kurulu omurgalar kullanılmalıdır. Dolayısıyla veri ağları için tasarlanmış ağlar üzerinden yüksek kaliteli ses taşıması yapmak ek yatırım ve bant genişliği ile ekstra maliyet getirmektedir.

İnternet erişiminin yaygınlaşması yeni servislerin İnternet üzerinden sağlanması fikrini doğurmuştur. Bu servislerin konvansiyonel eşleniklerine göre daha rekabetçi ve cazip maliyetleri günümüzde İnternet'in rotasını çizmektedir. Günümüzde MPLS tabanlı çalışan omurgalar tüm bu ihtiyaçlara cevap verecek özellikleri barındırmaktadır.

3. OMURGANIN İŞLEYİŞİ

3.1 Kullanılan Protokoller

Omurga üzerinde yönlendirme bilgisininin, diğer bir deyişle hangi ağa nereden erişilebileceği, hangi ağın nerede olduğu bilgisi taşınması gereklidir. Omurga üzerinde bu işlem yönlendirme protokolleri yardımı ile kotarılır. Yönlendirme protokolleri, kullandıkları algoritmalar yardımı ile yönlendiricilere ağ üzerindeki en kısa yol bilgisini oluştururlar. OSI referans modelinin [2] üçüncü katmanı olan ağ katmanında çalışan yönlendirme protokolleri, bu katmanda kullanılan mantıksal adres bilgisinin güncel tutulmasından sorumludurlar. OSI protokolleri farklı üreticilere ait cihazların uyumlu çalışmasını sağlamak amacıyla uluslararası standartları tanımlar Yönlendirme protokolleri işlevlerine göre "Dahili Yönlendirme Protokolleri" ve "Harici Yönlendirme Protokolleri" olmak üzere iki ana sınıfa ayrılırlar. [3]



Şekil 3.1.i: Dahili ve harici yönlendirme protokollerinin çalışma alanları

3.1.1 Dahili Yönlendirme Protokolleri

Dahili yönlendirme protokolleri tek bir yönetimsel ağın [4] yönlendirme bilgisinin bu ağ içerisinde yönlendiricilere ulaştırılmasında kullanılır. Yönetimsel ağ, diğer ağlardan bağımsız tek bir otonom sistem olarak düşünülmelidir. Dahili yönlendirme protokolleri yönlendirme bilgisinin bu ağ içerisinde dağıtılmasından sorumludurlar.

3.1.1.1 OSPF

Ekim 1989'da IETF tarafından standart [5] olarak kabul edilen OSPF, bu tarihten günümüze kadar bir çok geliştirmeler ile günümüze kadar gelmiş dinamik yönlendirme protokolüdür. OSPF, ağ üzerindeki en kısa yolu bulmak amacıyla, matematikte bir noktalar kümesinde, bir noktadan diğer noktaya en kısa yolu bulma problemini çözen "Dijkstra'nın Algoritması"nı [6] kullanır.

OSPFv2, IP paketindeki IP adresinin başlık bilgisinde okuduğu hedef adres bilgisine göre yönlendirme yapar [7]. OSPF, ağ topolojisinde meydana gelen değişiklikleri kısa sürede algılamak ve bu değişiklik bilgilerini yönlendiricilere kısa sürede aktarmak üzere tasarlanmış bir yönlendirme protokolüdür. OSPF "Bağlantı-Durum" bir yönlendirme protokolüdür. Yönlendirme kararları, otonom sistemde bulunan yönlendiriciler arası bağlantıların durumuna göre yapılır. Her yönlendirici ağ üzerindeki cihazların bağlantılarını ve kullandığı arayüzleri içeren veritabanı barındırır ve bu veri tabanı sürekli olarak güncellenir. Her yönlendirici bulunduğu otonom sistem içinde bulunduğu alandaki bütün yönlendiricilere kendi üzerindeki arayüzleri ve bu arayüzlerden hangi ağlara erişimi olduğu bilgisini, "bağlantı-durumu" bilgisini gönderir.

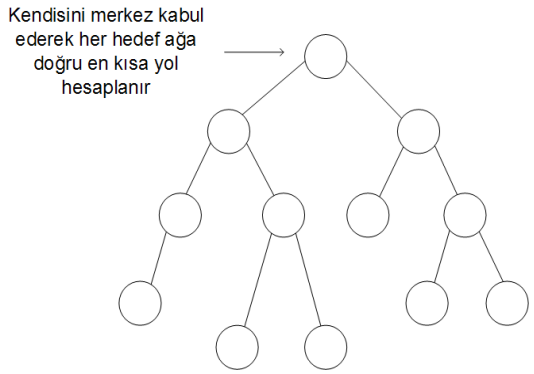
Kendinden öncekilere göre OSPF'i avantajlı kılan ve öne çıkaran özellikler şunlardır:

- Gidilmek istenen son noktaya kadar atlanılması gereken yönlendirici konusunda sınır yoktur.
- Kendi bağlantı-durumu bilgisini gönderirken çoklu yayın adresi kullanır, bu diğer yönlendiricilerin kendisine gelen bütün paketleri dinlemesi zorunluğunu kaldırır ve işlemcinin daha verimli kullanılmasını sağlar. Ayrıca yönlendirme tablosunun tamamının transferi söz konusu olmadığı için diğer yönlendiricilerde belleğin daha verimli kullanılmasını sağlar.

- Değişiklik bilgisi, değişiklik oluştuğu anda yollanır. Periyodik güncellemenin sebep olduğu, ağın uzun zamanda yakınsaması sorunlarını ortadan kaldırır.
- Hiyerarşik tasarıma izin vererek ağın daha verimli çalışmasını sağlayacak mimari oluşturulması imkanı sağlar.
- Otonom sisteme, harici yönlendirme bilgilerinin dağıtılmasına imkan verir.

OSPF, bütün hedeflere en kısa yolu bulmak için bağlantı-durum algoritması kullanır. Algoritma tek başına oldukça ayrıntılıdır. Algoritmanın işleyişini temel olarak şu şekilde özetleyebiliriz: [8]

- İlk çalışmaya başlanılan anda ve yönlendirme bilgisinin değiştiği durumlarda yönlendirici bağlantı durum anonsu (LSA) gönderir.
- Yönlendiriciler bağlantı durumlarını diğer bütün yönlendiricilere anons ederler. İşleyiş, gelen bağlantı durum bilgisini okumak, kendisine bir kopya alıp bunu veri tabanına işlemek, ardından bağlantı durum bilgisini diğer bütün yönlendiricilere göndermek şeklindedir.
- Yönlendiricier kendi veri tabanlarını güncelledikten sonra ağ üzerindeki bütün noktalara en kısa yolu bulmak için Dijkstra algoritmasını kullanarak merkezi kendileri kabul ederek en kısa yol ağaçlarını oluştururlar. (Şekil 3.1.1.1.i)

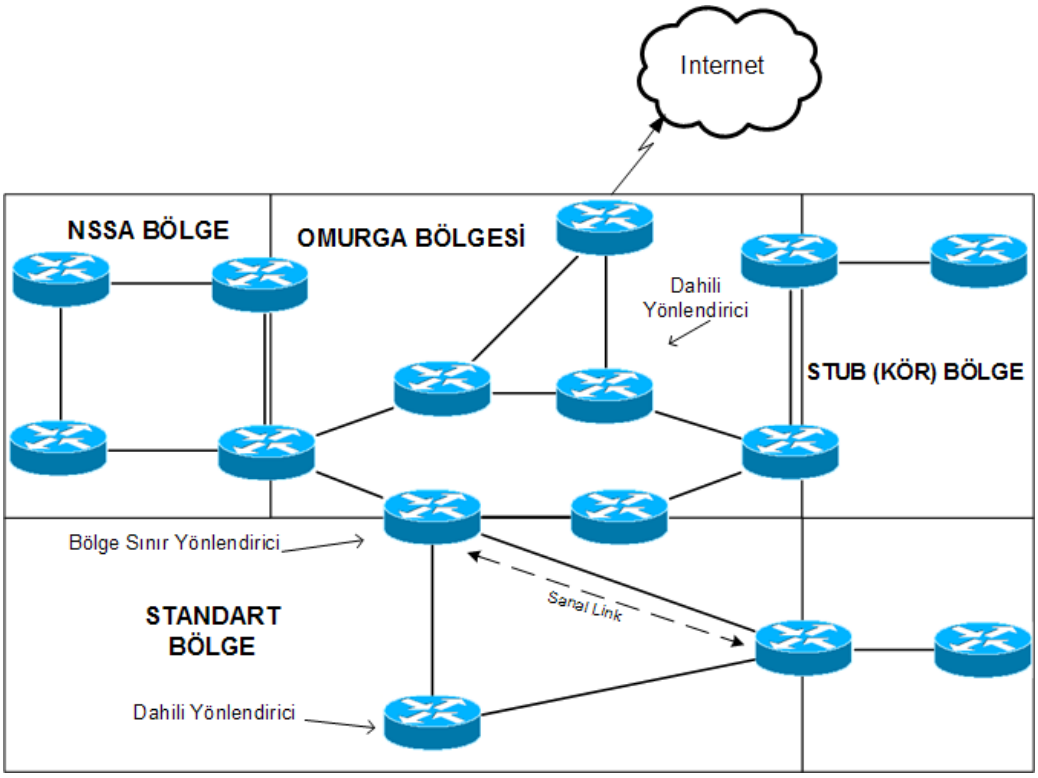


Şekil 3.1.1.1.i : En kısa yol ağaçları

- En kısa yol bilgileri oluşturulduktan sonra bu bilgiler yönlendirme tablosuna işlenir. Yönlendirme tablosundaki bilgiler değişiklik olmadığı sürece sabittir. Değişiklik olmadığı sürece OSPF'in işleyişi sessizdir. Değişiklik bilgisi alınırsa, tekrar en kısa yol bilgileri hesaplanıp yönlendirme tablosuna bu bilgiler işlenir

OSPF'in çok kısa sürede yakınsamasındaki en önemli faktörlerden biri de OSPF otonom sisteminin hiyerarşik yapıdaki OSPF bölgelerinden oluşmasıdır. OSPF bölgeleri ve temel özellikleri şunlardır: [9]

- Omurga Bölgesi: Transit bölge olarak da bilinir. Diğer bölgelerin hepsi bağlantı-durum bilgisi alış-verişi için doğrudan bu bölgeye bağlı olmak zorundadır. Eğer doğrudan bir bağlantı yoksa, sanal bağlantı kullanmak gerekir (Şekil 3.1.1.a.ii)
- Standart Bölge: Bu bölge standart bağlantı durum güncellemelerini, yön bilgisi özetlerini ve harici yön bilgilerini kabul eder.
- Kör (STUB) Bölge: Bu bölge harici yön bilgisi güncellemelerini kabul etmez. Bu bölgedeki yönlendiriciler harici yön bilgilerini saklamazlar. Kendilerini omurga bölgesine bağlayan bölge sınır yönlendiricilerine doğru varsayılan rotaları vardır.
- NSSA Bölge: Bu bölgeye de harici yön bilgileri sınır yönlendiriciler tarafından anons edilmez. Ancak bu bölgedeki yönlendiriciler tarafından öğrenilen rotalar içeride diğer yönlendiricilere "Tip-7" anonsu olarak duyurulurlar.



Şekil 3.1.1.1.ii: OSPF bölgeleri

OSPF, yönlendiriciler arasında komşuluk kurulması, bağlantı-durum bilgilerinin senkronizasyonu, yönlendirme tablolarının güncellenmesi ve dolayısıyla otonom sistem içinde düzenli işleyişin devamı için beş çeşit paket kullanır. Bu paket çeşitleri:

- Hello (Merhaba) Paketleri: OSPF yönlendiricileri arasında komşuluk kurulması sırasında ve kurulan komşuluğu devam ettirilmesi için kullanılırlar. İlk komşuluk

kurulma anında 224.0.0.5 adresine çoklu yayın olarak gönderilirler, komşuluk kurulduktan sonra ise komşunun adresine unicast olarak gönderilir.

- Veri Tabanı Tanım Paketleri: OSPF yönlendiricileri arasında komşuluk kurulurken kullanılırlar. OSPF yönlendirici veri tabanı içeriğini diğer yönlendiriciye söylemek için kullanılırlar.
- Bağlantı-Durum İstek Paketleri: Komşuluk kurulan yönlendiriciden belirli rotalara ait bilgi istemek amacıyla kullanılırlar.
- Bağlantı-Durum Güncelleme Paketleri: Komşuluk kurulan yönlendiriciler arasında bağlantı-durum bilgilerini güncellemek amacıyla kullanılırlar. Yedi tanesi standart haline gelmiş toplam onbir tane bağlantı-durum güncelleme paket çeşidi mevcuttur. (Şekil 3.1.1.a.iii) [10]

Tablo 3.1.1.1.iii: Bağlantı Durum Güncelleme Paketleri

Bağlantı-Durum Anonsu tipi	Tanımı
1	Yönlendirici bağlantı anonsu
2	Ağ bağlantı anonsu
3 ve 4	Özet bağlantı anonsu
5	Otonom Sistem Harici bağlantı anonsu
6	Çoklu yayın OSPF bağlantı-durum anonsu
7	NSSA bölge için harici rota anonsu
8	BGP için harici özellikler bağlantı-durum anonsu
9, 10, 11	Opak bağlantı-durum anonsları

OSPF hedef ağa en kısa yolu bulmak için en kısa metriğe sahip yolu tercih eder. OSPF'te metrik olarak masraf (cost) kullanılır. OSPF'te metrik bant genişliği göz önüne alınarak hesaplanır ve hedef ağa kadar olan metrikler toplanarak yönlendirme veri tabanına kaydedilir. Eğer hedef ağa birden fazla yol varsa, veri tabanından bu yollardan en düşük metriğe sahip olan yol kullanılmak üzere tercih edilerek yönlendirme tablosuna eklenir. Yönlendiriciler genellikle trafik yönlendirmesine müdahale imkanı sağlamak amacıyla iki yönlendirici arasındaki bağlantı üzerinde metriğin manuel olarak tanımlanmasına imkan sağlarlar. OSPF yönlendiricler arası bağlantılara, bant genişliğine göre "10^8/bant genişliği" formülüne uygun olarak metrik atar. Ancak günümüzde omurga çekirdeğinde merkezler arası iletim

devrelerinde POS STM-256 (43 Gbps) veya yerel ağlarda 10 GigE (10 Gbps) ve üzeri hızlara ulaşılmış olması nedeniyle söz konusu formül en iyi metrik atamasını sağlayamamaktadır. Omurgalarda trafik yönlendirilmesine müdahale etmek için metrikleri ağ tasarımının başlangıcında belirlemek ve yönlendiriciler arasındaki devre hızlarına göre atamak, ince ayar yapmak için gereklidir.

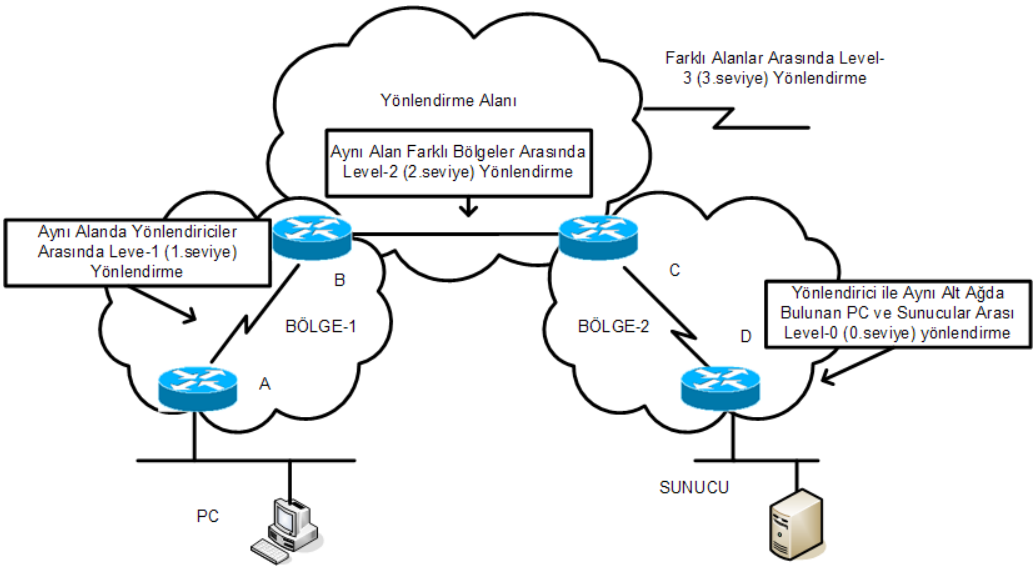
OSPF çalıştıran yönlendiriciler komşuluk kurduktan sonra atanmış yönlendirici (DR) ve yedek atanmış yönlendirici (BDR) seçerler. Noktadan noktaya bağlantılarda çok kullanışlı olmasa da, açık-yayın (broadcast) ortamlarda, bağlantı-durum anonslarının kontrol altında tutulmasında bu mekanizma önemlidir. Buna göre bağlantı durumunda değişiklik olan yönlendirici bu bilgiyi atanmış yönlendiriciye söyler, o da aynı açık-yayın ortamında bulunan diğer yönlendiricilere bu bilgiyi anons eder. Atanmış yönlendiricilere yapılan anons 224.0.0.6 ile yönlendirilir. Atanmış yönlendiriciler de bu çoklu yayın adresi ile gelen anonsu alıp işledikten sonra 224.0.0.5 ile diğer yönlendiricilere gönderirler. 224.0.0.6 ile gelen anonsu atanmış olmayan yönlendiriciler almazlar.

Servis sağlayıcı omurgaları her zaman saldırıya açık ağlardır ve güvenliğin en üst seviyede tutulması gerekir. OSPF çalışan bir omurga tasarlanacaksa güvenlik için OSPF'in sağladığı özellikleri de kullanma imkanı vardır. OSPF komşular arası yapılan yönlendirme bilgisi güncellemeleri yapılmadan güvenli bir komşuluk kurulduğu, diğer bir deyişle doğru yönlendirici ile komşuluk kurulduğundan emin olmak gerekir. OSPF komşuluk kurarken MD5 [11] ile kimlik doğrulaması yapılması imkanı sağlar. Omurgaların İnternet üzerinden gelen saldırılara açık olduğu düşünüldüğünde kimlik doğrulaması omurgalar için gerekli bir özelliktir.

3.1.1.2 IS-IS

IS-IS, ISO tarafından ISO/IEC 10589'da [12] tanımlanmıştır. Tam adı *"Intermediate System to Intermediate System Intra-Domain Routeing Exchange Protocol for use in Conjuction with the Protocol for Providing Connectionless-mode Network Service"* (Bağlantısız mod ağ servisi sağlamak amacıyla alan içi orta-sistemden orta-sisteme yönlendirme protokolü) olan IS-IS, adından da anlaşılacağı gibi CLNP [13] için yönlendirme protokolü olarak tasarlanmıştır. CLNP, IP protokol kümesine karşılık

gelen ISO standardıdır. Orta-Sistem (IS) OSI terminolojisinde yönlendiricileri tanımlar. Uç-Sistem (ES) ise yönlendirici ile aynı alt ağda bulunan bilgisayarlar ve sunuculardır.



Şekil 3.1.1.2.i: OSI yönlendirme seviyeleri ve hiyerarşik tasarım

CLNP OSI Ağ Katmanı protokolüdür. Bağlantı kontrolsüz şekilde üst katman verilerini ve hata mesajlarını taşır. CLNS, CLNP protokolünü kullanarak taşıma katmanına ağ katmanı servisleri sunar. Bunu yaparken bağlantı kontrolsüz çalışır ve hata kontrolü ve düzeltme için taşıma katmanı protokollerine güvenir.

OSI, ara-sistemler (intermediate-systems) arasında hiyerarşik yönlendirme için IS-IS yönlendirme protokolünü geliştirmiştir. IS-IS, ISO CLNS ortamında, CLNP yönlendirmesi için kullanılan dinamik ve bağlantı durumuna göre yönlendirme yapan bir protokoldür.

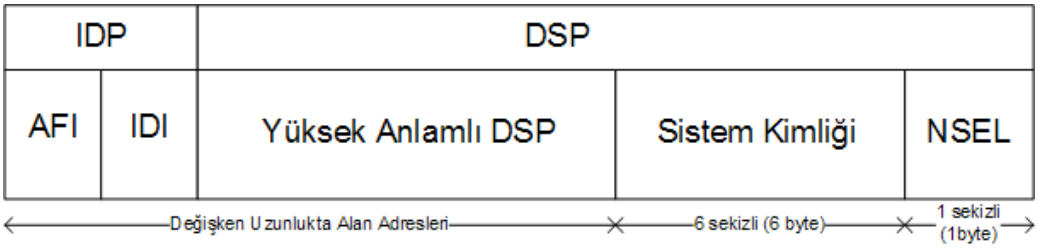
IS-IS'te, yönlendiriciler ara-sistem olarak çalışırlar ve diğer ara-sistemler ile erişilebilirlik bilgisini paylaşırlar. Şekil 3.1.1.2.i'yi göz önüne alarak, IS-IS protokolünün işleyişini şu şekilde açıklayabiliriz:

- Örneğimiz için her uç sistem (ES) farklı bölgelerde bulunur. OSI yönlendirmesi, uç sistemin ara-sistem hello paketlerini (ESH) dinleyerek en yakın ara-sistemi

bulmasıyla başlar. Bir uç-sistem, diğer bir uç-sisteme paket yollamak istediği zaman, bu paketi kendisiyle aynı ağda bulunan ara-sistemlerden birine yollar.

- Yönlendirici hedef adrese bakarak, paketi yollanabilecek en iyi yoldan gönderir. Eğer hedef uç-sistem aynı alt ağda bulunuyor ise, ara-sistem bunu uç-sistem hello (ESH) paketlerinden öğrenir ve gerektiği şekilde paketi bu uç-sisteme gönderir. Buna ek olarak, kendisi üzerinden geçen yoldan daha uygun bir yol bulunduğunu belirtmek amacıyla "redirect", yani tekrar yönlendir mesajı da gönderir.
- Eğer yönlendirme yapılacak uç-sistem aynı bölgede farklı bir ağda bulunuyor ise yönlendirici yine bu uç sistemin nerede olduğunu bilir ve paketi uygun şekilde yönlendirir.
- Eğer hedef adres farklı bir bölgede yer alıyorsa birinci seyiye yönlendirici (Level-1 IS) paketi en yakın ikinci seviye yönlendiriciye gönderir. Paket hedef bölgeye ulaşıncaya kadar ikinci seviye yönlendirme devam eder. Eğer hedef adres farklı bir yönlendirme alanında yer alıyorsa, bu durumda üçüncü seviye yönlendirme yapılır.
- Hedef yönlendirme alanına ve ardından uygun bölgeye ulaşıldıktan sonra uç sisteme kadar yönlendirme devam eder.

OSI'de, ağ adreslemesi NSAP adresleri ile sağlanır. NSAP adresleri OSI ağında her bir sistemi tanımlayabilirler. NSAP adres yapısı şu şekildedir. [14]



Şekil 3.1.1.2.ii: NSAP adres yapısı

Bu alanların anlamları ise şu şekilde açıklanabilir:

- AFI (Authority and Format ID): Adresin formatını ve bu adresin hangi organizasyon tarafından atandığını belirtir.
- IDI (Inter Domain ID): Yönlendirme alanını tanımlar.

- IDP (Inter Domain Part): AFI ve IDI bölümleri birlikte IDP'yi oluştururlar. Bu bölüm farklı yönlendirme alanları arasında yönlendirme yaparken kullanılır.
- Sistem Kimliği: Her bir OSI cihazını tanımlamak için kullanılır.
- NSEL (NSAP-Selector): İlgili cihaz üzerinde çalışan prosesi tanımlar.
- DSP: Yüksek Anlamlı DSP, Sistem Kimliği ve NSEL birlikte DSP bölümünü oluştururlar. Bu bölüm yönlendirme alanının içinde kullanılacak bilgileri içerir.

IS-IS'ten örnek olarak kullanacağımız tasarımda yer verilmeyecek olması nedeniyle daha fazla söz edilmeyecektir. IS-IS günümüzde özellikle Amerika'da yaygın olarak kullanılan bir yönlendirme protokolüdür ve teorik olarak kullanılabilecek yönlendirici kısıtlamasının olmaması, çok büyük ağlar için IS-IS'i hala popüler kılmaktadır.

3.1.2 Harici Yönlendirme Protokolleri

OSPF veya IS-IS ile yönlendirme bilgisinin dağıtıldığı yönetimsel bölgeler otonom sistemler oluştururlar. Otonom sistemler içinde yönlendirme bilgisinin dağıtılması ve güncellenmesi kullanılan protokollerle kontrol altına alınır. Otonom sistemler sadece kendi içinde yönlendirme yapmazlar. Günümüzde IP trafiğinin yönlendirilmesinde en büyük motivasyonun İnternet trafiğini yönlendirmek olduğu düşünülürse, otonom sistemler arasında yönlendirmenin ne kadar önemli bir konu olduğu daha iyi anlaşılır. Otonom sistemler arasındaki yönlendirme kontrol edilebilir olmasının yanında, büyük miktarda trafik güncellemelerini mümkün olan en kısa sürede gerçekleştirilebilmeli ve mevcut bant genişliklerinin en verimli şekilde kullanılacak şekilde yönlendirme bilgisi dağıtımı yapılmalıdır. Bu görevleri gerçekleştirmek amacıyla harici yönlendirme protokolleri kullanılmaktadır. Bununla birlikte unutulmaması gereken bir nokta da şudur ki, eğer otonom sistemin haberleşeceği diğer sistemler mevcut otonom sistemin yönlendirme politikasıyla aynı mantıkla çalışıyor ise veya otonom sistemin tek bir çıkışı varsa harici yönlendirme yönlendirme protokolü kullanılmasına gerek yoktur. Genellikle varsayılan rotalar atamak istenilen yönlendirme için yeterli olmaktadır.

3.1.2.1 BGP

Otonom sistemler arasında yönlendirme için en yaygın olarak kullanılmakta olan protokol BGP'dir. (Border Gateway Protokol). En son Ocak 2006'da RCF 4451 [15] standardı IETF tarafından tanınan BGP'nin uygulama raporları ise RFC 4276 [16] ve RFC 4277 [17] ile standartlaştırılıp yayımlanmıştır. BGP'nin IPv6'yı destekleyen standardı ise RFC 2545 [18] ile yayımlanmıştır. BGP'nin halen kullanılmakta olan versiyonu BGP-4'tür

BGP'nin temel operasyonel birimi otonom sistemlerdir. Otonom sistem numaraları RFC 1930 tanımlanmıştır. Buna göre otonom sistem numaraları 64512-65535 arası özel kullanım için rezerve edilmiş 1-65535 arası değişen numaralardır, 32 bit uzunluğundaki otonom sistem numaralarının hayata geçirilmesi ile ilgili çalışmalar yapılmaktadır. BGP otonom sistemleri bu 16 bit'ten oluşan numaralara göre ayırt eder. Otonom sistem numaraları IANA (Internet Assigned Numbers Authority) tarafından kontrollü olarak dağıtılır.

BGP trafiği taşırken güvenli bir şekilde taşır. Trafik alış-verişinin gerçekleşmesi için öncellikle arada TCP ile kontrol edilen ve aktif olarak çalışırlığı gözlenen bir oturum açılması gerekir. Trafik akışı TCP'nin 179 numaralı portunu kullanan bağlantı sağlandıktan sonra gerçekleştirilir. İki yönlendirici arasında TCP oturumu açıldıktan sonra bütün yönlendirme tabloları karşılıklı olarak paylaşılır. Bütün tablolar değiştirildikten sonra sadece güncelleme anlarında anons numaraları bir arttırılarak güncelleme yapılır. Yalnızca değişiklik halinde yönlendirme bilgisi güncellemeleri yapılır. Bunun dışında komşuluğun ilk kurulduğu andaki paylaşılan yönlendirme tablolarındaki bilgiler kullanılır.

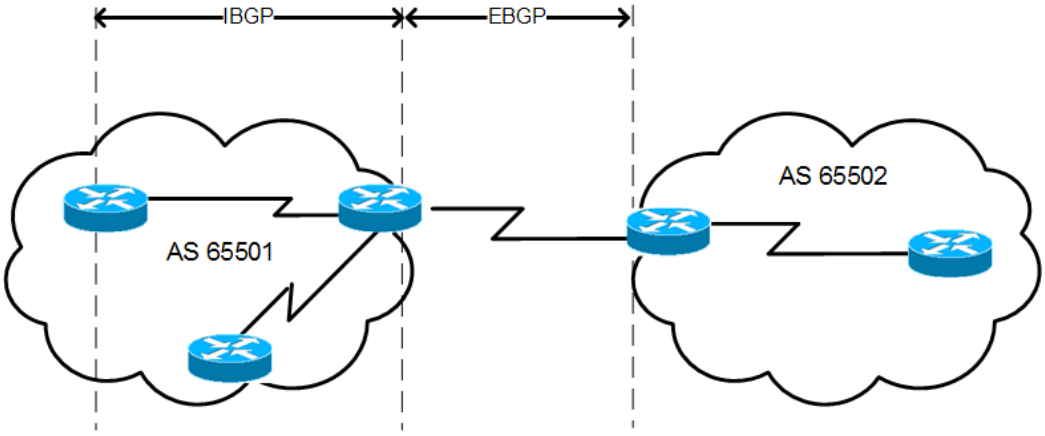
BGP'de toplam dört çeşit mesaj vardır. Bu mesajlar komşuluk kurulurken ve komşuluğun devam ettirilmesi sırasında iki yönlendirici arasında paylaşılır. BGP'de kullanılan mesaj tiplerinin özelliklerini şu şekilde özetleyebiliriz:

- Açılış (OPEN): Komşuluğun kurulması sırasında ilk olarak diğer yönlendiriciye gönderilen mesajdır. OPEN mesajının içinde karşıdaki yönlendiriciye gönderilen, gönderen yönlendiriciye ait bilgiler, versiyon numarası, otonon sistem numarası,

kurulan TCP oturumunun ne zaman güvenilmeyip kapatılacağı bilgisinin paylaşıldığı askıda kalma süresi (holdtime), BGP yönlendirici kimliği (Router ID) ve isteğe bağlı parametrelerdir.

- Canlı Tutma (Keepalive): Her yönlendirici diğerine oturum süresince canlı olduğunu bildirmek zorundadır. Bunun için kullanılan yöntem "keepalive" mesajı göndermektir. Sadece mesaj başlığı gönderilir.
- Güncelleme (Update): Komşu yönlendiriciye gönderilecek yönlendirme bilgilerini içeren mesajdır. Her mesajda sadece bir patikaya ait bilgi gönderilir. Eğer komşuya birden fazla patika hakkında bilgi gönderilecekse her patika için ayrı güncelleme mesajları gönderilmesi gerekir.
- Uyarı (Notification): Sadece hata anında gönderilirler ve gönderildikten hemen sonra komşuluk sona erdirilir. Mesajla birlikte hata kodu ve hata ile ilgili bilgi gönderilir.

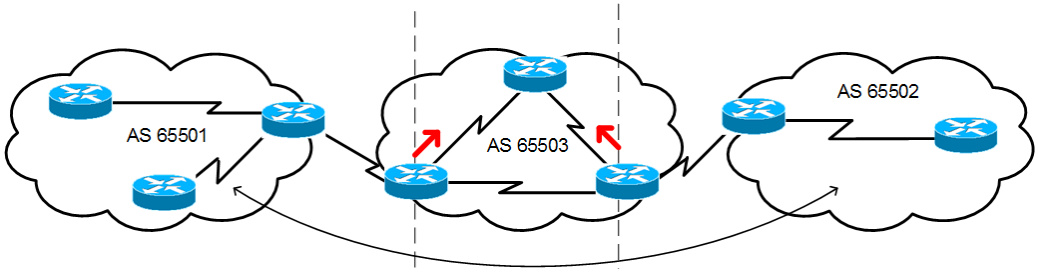
BGP'de veri akışının gerçekleştirilmesi için komşuluk kurulması gerekir. Komşuluk kurulan yönlendiricinin bulunduğu otonom sisteme göre dahili komşuluk ve harici komşuluk olarak iki çeşit komşuluk kurulur. Eğer komşuluk kurulacak yönlendirici aynı otonom sistemde ise dahili, farklı otonom sistemde ise harici komşuluk kurulur. Kurulan komşuluğa göre oturum dahili BGP (IBGP) ve harici BGP (EBGP) isimlerini alır.



Şekil 3.1.2.i: EBGP ve IBGP Alanları

EBGP komşulukları için yönlendiriciler aynı otonom sistemde bulunmazlar. Bununla birlikte EBGP komşuluğu kurulması için yönlendiricilerin birbirlerine direkt olarak bağlı olmaları gerekir, Herhangi bir yönlendirme protokolü komşuluk kurulacak yönlendiriciyi aramak zorunda olmamalıdır. Yönlendiricilere komşuluk kuracakları yönlendiricilerin IP adresleri ilk yapılandırılma sırasında belirtilir.

IBGP komşulukları kurulması için ise komşuluk kurulacak yönlendiricinin direkt bağlı olmasına gerek yoktur. İki yönlendirici de aynı otonom sistemde bulunduğundan dolayı yönlendiriciler komşuluk kuracakları yölendiricinin yerini otonom sistemde çalışmakta olan dahili yönlendirme protokolü yardımıyla, statik rotalarla veya direkt bağlı oldukları arayüzlerle bulabilirler. Genel olarak IBGP'nin otonom sistem içinde kullanılması tavsiye edilen bir durum olmasa da, eğer bu otonom sistem transit ağ olarak kullanılacaksa, diğer bir deyişle farklı otonom sistemler bu otonom sistem üzerinden trafiklerini geçirmek zorundalarsa ve otonom sistem diğerleri için taşıyıcı olarak görev yapacaksa, omurgada IBGP çalıştırmak gerekir. Çünkü IBGP kullanılmazsa yönlendirme bilgilerinin bu iki otonom sistem arasında taşınması için EBGP yönlendirme protokolü tablolarının tamamının dahili yönlendirme protokolü tablolarına aktarılması gerekir ki, bu da otonom sistem içinde yönlendiricilerin performansında ciddi bir düşüşe sebep olur. (Şekil 3.1.2.ii)



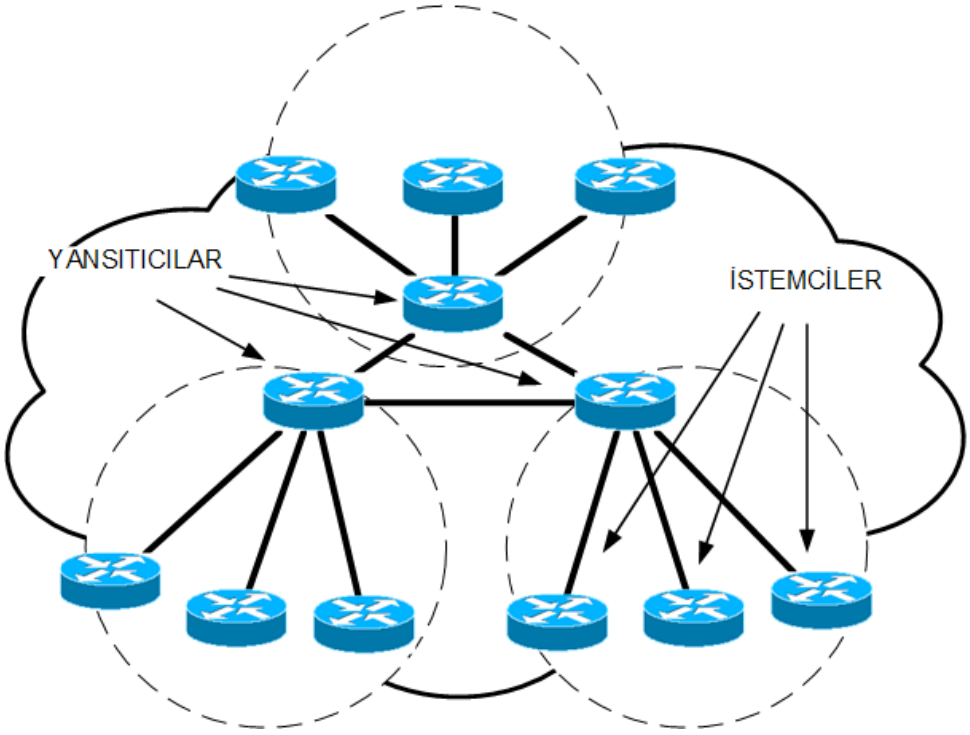
Şekil 3.1.2.ii: Transit trafik ve BGP tablolarının IGP'ye aktarılması

BGP yönlendirme işlemini yaparken dahili yönlendirme protokolündeki gibi IP adreslerini görerek yönlendirme yapmaz. Yönlendirme hedefi, anonsların yapıldığı yöne doğrudur. IBGP yönlendiricisinin diğerlerinin tümüyle komşuluk kurması BGP'nin çalışma prensibidir. Bunun sebebi yönlendirme döngülerinin ve kara deliklerin oluşmasını engellemektir. Diğer IBGP yönlendiricilerinin tümüyle komşuluk kurulduktan sonra bir IBGP yönlendiricisinden alınan yönlendirme

güncellemesi diğer bir IBGP yönlendiricisine anons edilmez. Bununla birlikte eğer bir yönlendirici diğerlerinin tümüyle komşuluk kurmazsa yönlendirme tabloları tam olarak senkronize olamaz ve bu de yönlendirmede kayıplara sebep olur.

IBGP kullanırken her yönlendiricinin diğerleri ile komşuluk kurmasının getirdiği zorlukları aşmak amacıyla rota yansıtma (Route Reflection) mekanizması geliştirilmiştir [19] Buna göre hiyerarşik tasarım ve yönlendirici grupları oluşturulur. Çalışma prensibi şu şekildedir: (Şekil 3.1.2.iii)

- Yansıtıcı olan yönlendiriciler diğer bütün yansıtıcı yönlendiricilerle IBGP komşuluğu kurmuş olmalıdırlar.
- Yansıtıcılar istemcilerden ve istemci olmayanlardan rota bilgilerini alırlar.
- En iyi yolu seçerler
- Eğer yol istemci olan yönlendirici üzerinden ise, bu bilgi bütün yönlendiricilerle paylaşılır.
- Eğer yol istemci olan yönlendirici üzerinden değil ise, bu bilgi istemci olan yönlendiriciye söylenir.



Şekil 3.1.2.iii: Rota yansıtıcıları yapılandırması

Otonom sistem içerisinde birden çok yansıtıcı kullanılabilir. Yedeklilik için iki tane kullanılması yeterlidir. Bununla birlikte yine yedekliliği sağlamak açısından bir yönlendirici aynı anda bu iki yansıtıcının istemcisi olmalıdır. Rota yansıtıcıları kullanımının paket yönlendirmesini etkilememesi ve uygulamasının kolay olması avantajları arasında sayılabilir. Rota yansıtıcıları BGP'yi ölçeklenebilir kılan önemli bir özelliktir.

BGP çalışan ağlarda hedef ağa gitmek için birçok yol bulunabilir. Bu yolların en iyileri seçilerek yönlendirme tablosuna yerleştirilir. En iyi yolun seçilip yönlendirme tablosuna işlenmesi için bir çok kriter bulunmaktadır. BGP tek bir yol kalıncaya kadar eleme işlemine devam eder. BGP'de yol seçimi bant genişliğine göre yapılmaz, ayrıca hedef ağa birden fazla yol varsa yük dağıtımı da yapılmaz. BGP'de en iyi yolun bulunması için sırasıyla bakılan özellikler aşağıda listelenmiştir. Yollardan biri tercih edilinceye kadar listedeki bütün kriterler sırayla karşılaştırılır. Eğer hedef ulaşılamıyorsa değerlendirilmeye alınmaz.

- En yüksek yerel tercih değerine (local preference) sahip olan yolun önceliği vardır.
- Hedef ağa ulaşmak için en az otonom sistem geçilmesini gerektiren yolun önceliği vardır.
- Kaynağı daha düşük olan yolun önceliği vardır. Bir yol dahili yönlendirme protokolünden öğrenildiyse 0, harici yönlendirme protokünden öğrenildiyse 1, tam değil ise (incomplete) 2 verilir. Eğer IBGP komşuluğundan öğrenilen bir yol bilgisi dahili yönlendirme protokolünden de öğrenilmediyse, bu bilgi EBGP komşuluğuyla paylaşılmaz ve bu bilgi kullanılarak bir EBGP yönlendiricisine paket gönderilmez.
- Düşük MED metriğine sahip olan yol tercih edilir.
- EBGP komşuluğu kurulmuş olan yönlendiriciden öğrenilen yolların IBGP 'den öğrenilen yollara göre önceliği vardır.
- Dahili yönlendirme protokolü metriği daha düşük olan komşudan öğrenilen yol tercih edilir.
- BGP kimlik numarası (BGP ID) daha düşük olan yönlendirici tercih edilir.

BGP toplulukları (Community) aynı özelliklere sahip yollar kümesi olarak tanımlanabilir. Aynı özelliklere sahip yoların hepsine aynı anda yönlendirme politikası uygulanmasına imkan tanır. RFC 1997 (BGP Communities Attribute) ile standart haline getirilmiştir. BGP toplulukları hedef ağları gruplamak için kullanılırlar ve otonom sistemler içinde taşınırlar.

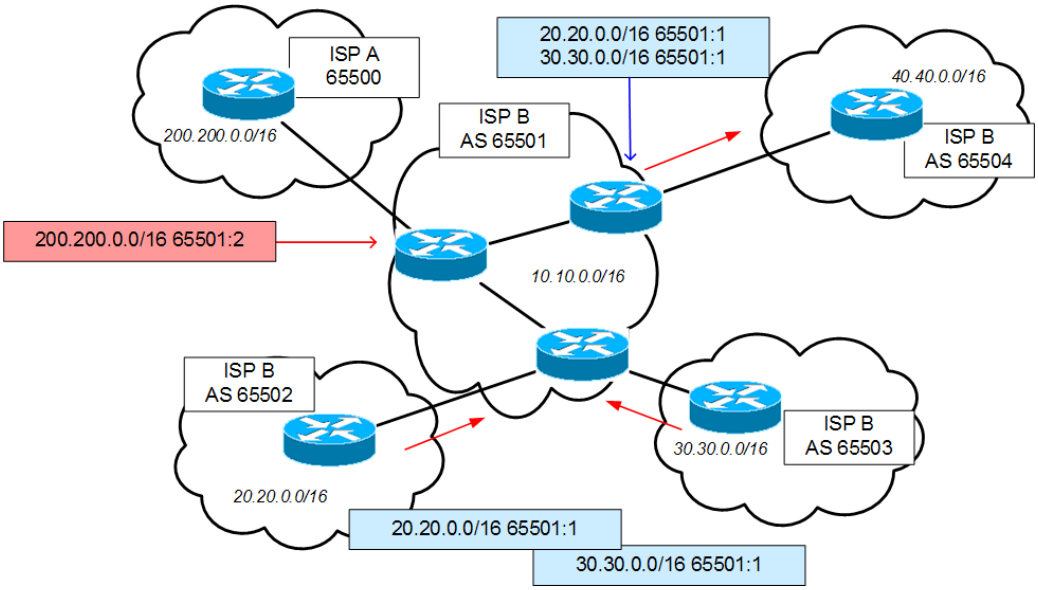
BGP topluluk kimlikleri iki tane 16-bitlik sayıyı birleştirmek üzere 32 bit olarak ifade edilirler. Yazım şekli *Lokal-Otonom-Sistem:xx* şeklindedir. *Lokal-Otonom-Sistem* değeri, toplululuğun hangi otonom sistem içinde dolaştırıldığını belirtir 0-65535 arası değer alır. *xx* değeri ise topluluk değeridir, 0-65535 arası bir değer alır. 0:0-0:65535 ile 65535:0-65535:65535 arasındaki BGP topluluk kimlik numaraları ayrılmıştır ve İnternet'te kullanılmazlar.

Bazı topluluk numaraları ise *iyi bilinen* (well known) olarak adlandırılırlar, yönlendiriciler bu numaralara sahip yollar için nasıl davranmaları gerektiğini bilirler. Bu topluluklar özetle şunlardır:

- **no-export** (65535:65281): Hiçbir EBGP komşuna anons etme.
- **no advertise** (65535:65282): Hiçbir BGP komşuna anons etme.
- **local-as** (65535:65283): Lokal otonom sistemin dışına anons etme

Aynı özellikteki ağlara aynı politikaları uygulamak için büyük kolaylıklar sağlayan BGP toplulukları otonom sistem içinde yapılan operasyonel işlenleri de azaltır.

Aşağıdaki şekilde farklı otonom sistemlerden öğrenilen yönlendirme bilgilerinin diğer otonom sisteme aynı topluluk numarasıyla anons edildiği gösterilmektedir. Buna göre ISP B, 65502 ve 65503 numaralı otonom sistemlerinden aldığı yönlendirme bilgilerine ortak bir politika uygulamakta ve bu bilgileri diğer otonom sistemini anons ederken aynı topluluk özellikleri ile anons etmektedir. ISP A'dan alınan yönlendirme bilgisine ise farklı bir topluluk ile yönlendirme tablosuna alınmaktadır.



Şekil 3.1.2.iv: BGP topluluklarının kullanımı

Günümüzdeki servis sağlayıcı mimarileri bu bölümde anlattığımız teknolojileri kullanmaktadırlar. Artan trafik miktarı, servis çeşitlendirmesi ve daha nitelikli ve katma değeri olan hizmetlerin sunulması, günümüzde yeni teknolojileri gerekli kılmaktadır. Bundan sonraki bölümde, modern ağ mimarilerinin işletilmesinde önemli imkanlar sunan ve günümüz ihtiyaçlarını karşılayarak, gelecekte ki İnternet servis ihtiyaçlarına cevap verebilecek yetenekleri barındıran MPLS teknolojisinden bahsedilecektir.

4. MPLS

4.1 MPLS Teknolojisi

4.1.1 Tarihçesi ve Gelişimi

1990'ların ortalarından itibaren İnternet servis sağlayıcılar güçlü yönlendiricilerin ATM anahtarlarla birlikte kullanıldığı IP omurgaları kurdular. Genel olarak omurgalarda ATM anahtarlar tam ağ yapısı ile birbirlerine bağlı olarak kullanıldı. Ancak İnternetin hızlı gelişimi tam ağ yapılı ATM omurgaları kurmak ve işletmek maliyetli hale geldi. Günümüzde ise IP teknolojisi ATM teknolojisine göre daha

ucuz hale gelmiştir. Zamanla IP ve ATM'in karışık halde kullanıldığı omurgalar oluşmuştur. Bu yapılarda çekirdekte ATM anahtarlar yerine IP yönlendiriciler kullanılmış, dağıtım katmanında ATM anahtarlara yer verilmiştir. Yönetimi zorlaşan bu yapılardan sonra günümüzde eğilim ATM omurgaları çalıştırmaya devam etmekle birlikte yeni kurulan omurgalarda IP çalıştırmaktır.

MPLS, IP omurgada hızlı ve kontrol edilebilir bir yapı oluşturulması amacıyla ve bir çok fikrin sentezi olarak oluşmuş bir protokoldür [20]. Bununla birlikte MPLS IP dışındaki protokolleri yönlendirme yeteneğine de sahiptir. ATM ve Frame Relay için MPLS tanımlamaları bulunmakta ve kullanılmaktadır. Bu çalışmada MPLS'e gelişmesinde ana motivasyonu sağlaması ve dünyada da genel uyguluma şekli olması nedeniyle IP taşıyan MPLS omurgaları üzerinde durulacaktır.

MPLS, *Çok Protokollü Etiket Anahtarlama* adından da anlaşılabileceği gibi etiket yönlendirme esasına göre çalışır. Buna göre gidilmek istenen hedef ağlara ulaşılıncaya kadar IP paketi MPLS paketinin içinde taşınır. MPLS günümüz ihtiyaçlarına cevap vermek ve IP omurgalarındaki hız ve servis kalitesi problemlerini çözmek amacıyla tasarlanmış IETF standardı bi protokoldür. IP mimarisinin üzerine yenilikler ekleyen bir protokol olarak da düşünülebilir. MPLS bir çok önemli yenilikler ve yetenekler barındırmaktadır. MPLS etiket anahtarlama yapması nedeniyle IP paketlerinin her düğümde açılıp hedef ağa bakılması ve yönlendirme tablosundan adres karşılaştırması yapma zorunluğunu kaldırmaktadır. MPLS trafik mühendisliği yetenekleri sunmaktadır. Buna göre kullanılan dahili yönlendirme protokolülün seçtiği en kısa yoldan değil, IP paketlerinin istenilen yoldan yönlendirilmesi imkanı sağlar. Bir diğer yenilik ATM omurgaların sağladığı güçlü servis kalitesi yeteneklerinin IP seviyesinde de yapılabilir kılınmasıdır. MPLS bütün bunların yanında *Sanal Özel Ağlar'ın* (VPN) omurgada oluşturulup kullanılmasına imkan vermesidir. [21] [22]

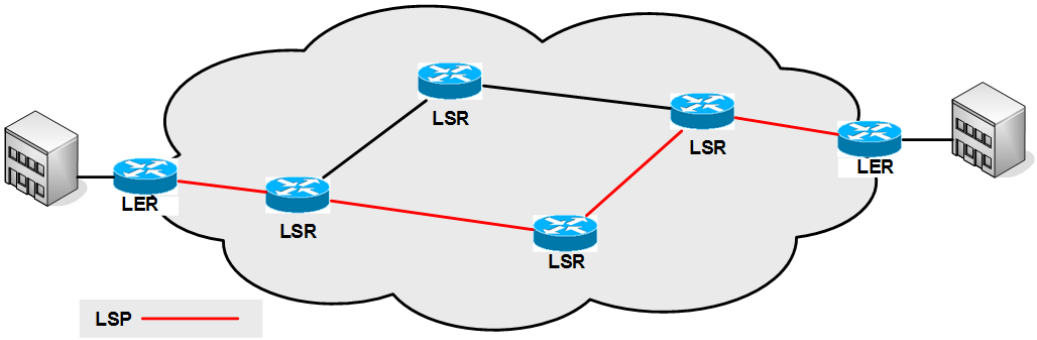
MPLS, felsefe olarak icadından itibaren ATM'le karşılaştırılmıştır. Sebebi ise omurgada ATM'e iyi bir alternatif oluşturması, hatta IP'nin ATM'e göre dezavantajlarını ortadan kaldırmasıdır. ATM'i popüler kılan en önemli özelliği 53

Bayt'lık sabit hücre uzunluğu ile anahtarlarda çabuk yönlendirilmesi ve dolayısıyla hızlı olması ile ATM Adaptasyon Katmanları (AAL) sayesinde servis kalitesi garantisinin sağlanmasıdır. IP'de servis kalitesi IP paketleri içindeki 8 bit uzunluğundaki Servis Tipi (ToS) bölümünün kullanımı ile sağlanmaktadır. Ancak omurgada bu bitlerin kullanımı yönlendirme ile beraber yapılınca ATM'e göre daha fazla zaman kaybına sebep olmaktaydı. Bu ATM'i Servis Kalitesi alanında IP'ye göre avantajlı kılan bir özellikti. MPLS Servis Kalitesi alanında ATM'in sağladıklarının üstüne yeni birşey getirmemekle birlikte hızlı çalışması ve IP'deki Servis Kalitesi yeteneklerini kullanabilmesi nedeniyle IP'nin ATM'e olan dezavantajını bu alanda kaldırmaktadır. MPLS'in Servis Kalitesi ilerleyen bölümlerde daha ayrıntılı anlatılacaktır.

4.1.2 MPLS Terminolojisi

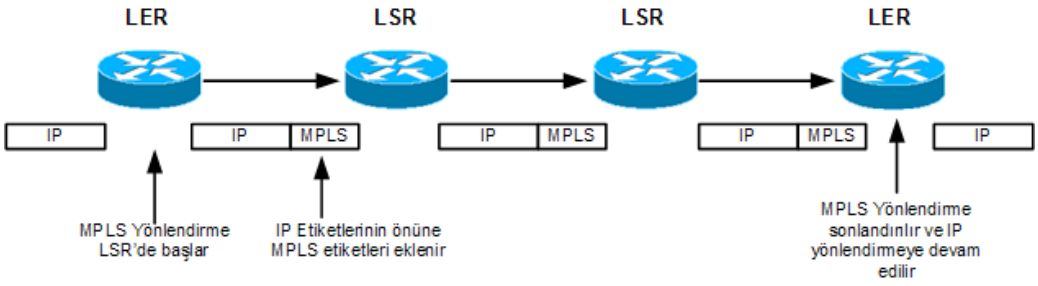
MPLS Terminolojisinde kullanılan terimler ve karşılıkları şu şekildedir:

- **LER (Label Edge Router: Etiket Kenar Yönlendiricisi):** MPLS omurgasının kenar noktalarında bulunan yönlendiricilerdir. Etiketlemenin başladığı veya bittiği yönlendiricilerdir. LER'de etiketleme ile başlayan yönlendirme MPLS omurgası boyunca devam eder ve yine bir başka LER'de etiket bilgisiyle yapılan anahtarlama sonlandırılır.
- **LSR (Label Switch Router: Etiket Anahtar Yönlendiricisi):** Bütün arayüzleri MPLS omurgasının içinde yer alan yönlendiricilerdir. Temel işlevleri kendilerine gelen MPLS paketlerini anahtarlamaktır.
- **LSP (Label Switch Path: Etiket Anahtar Patikası):** İki LER arasında MPLS omurgası boyunca oluşturulan tek yönlü patikalardır. Manuel olarak ağ yöneticileri tarafından oluşturulabileceği gibi, dinamik olarak etiket dağıtım için kullanılan LDP'den alınan bilgi ile de oluşturulabilir.



Şekil 4.1.2.i: MPLS terminolojisi

LSR'lere kadar IP yönlendirilmiş olan paketler, MPLS omurgasına dahil oldukları LER'lerde MPLS paketi başlıkları eklenerek MPLS yönlendirilmesine tabi tutulurlar. Omurgada taşındıktan sonra MPLS yönlendirmesi yine bir LER'de sonlandırılır ve bu aşamadan sonra IP paket başlığındaki hedef adrese doğru yönlendirme yapılır. (Şekil 4.1.2.ii)



Şekil 4.1.2.ii: IP ve MPLS paketleri dönüşümü

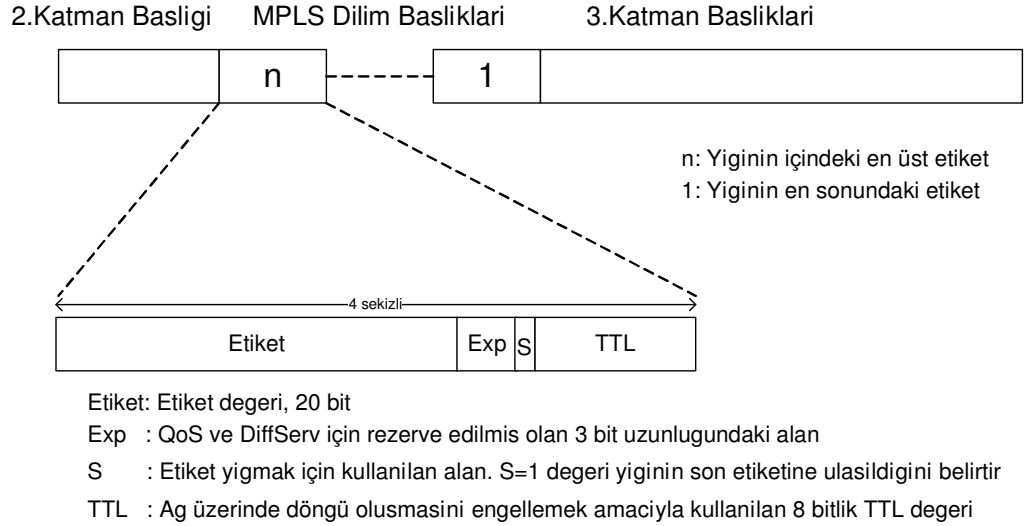
4.1.3 Çalışma İlkesi

4.1.3.1 MPLS Paket Yapısı, MPLS Etiketi ve Etiket İşlemleri

MPLS etiketleri, MPLS ağlarında temel unsurlardan biridir. MPLS çalıştırılan ortama göre dilim veya standart ikinci katman kodlaması şeklinde formları bulunur. MPLS paketinin yapısı Şekil 4.1.3.1.i 'de gösterilmiştir.

Bu noktada yönlendirme sırasında MPLS etiketlerinin tabi tutulduğu işlemleri özetlemek yerinde olur. MPLS paketleri yönlendirilirken paket başlıkları LSR'ler arasında aktarılırken sıkıştırma, çıkarma ve takas işlemlerine tabi turulurlar. Bu işlemleri şu şekilde özetleyebiliriz.

- Sıkıştırma: Mevcut yığına bir etket ekleme veya IP paketine etiket ekleme işlemidir. İşlem sonunda TTL değeri IP paketindeki TTL değerine eşitlenir.
- Çıkarma: Yığının en üstündeki etiket çıkartılır. Etiketin TTL değeri IP paket başlığındaki TTL alanına kopyalanır. LER tarafından yapılır.
- Takas: Sıkıştırma ve çıkarma işlemlerinin her ikisinin birden yapıldığı işlemlerdir. Alınan paketteki TTL değeri bir azaltıldıktan sonra oluşturulan yeni paketin MPLS başlığındaki TTL alanına kopyalanır. Sadece LSR'lerde yapılır



Etiket: Etiket degeri, 20 bit
Exp : QoS ve DiffServ için rezerve edilmis olan 3 bit uzunlugundaki alan
S : Etiket yigmak için kullanilan alan. S=1 degeri yiginin son etiketine ulasildigini belirtir
TTL : Ag üzerinde döngü olusmasini engellemek amaciyla kullanilan 8 bitlik TTL degeri

Şekil 4.1.3.1.i: MPLS paket yapısı

Teorik olarak $2^{20}-1$ adet etiket kullanılabilir. Ancak 0-15 etiketleri rezerve edilmiş ve kullanılmamaktadır, 4-15 değerleri gelecekte kullanılmak üzere rezerve edilmişlerdir. 0-3 değerleri ise şu şekilde tanımlanmışlardır: [23]

- "0" etiket değeri IPv4 Açık Sıfır Etiketi olarak anılır. (IPv4 Explicit NULL label). Kullanılır ise etiket yığınının en sonunda olması gerekir. Etiketin kaldırılması ve bundan sonra yönlendirilmenin IP başlığına göre devam edilmesi gerektiğini belirtir. MPLS'e dayalı servis kalitesi uygulamalarında kullanılır.
- "1" değeri yönlendirici uyarı etiketidir. Yönlendirme bu etiketten sonraki etikete göre yapılmalıdır. Paket yönlendirilmesine devam edildiği sürece bu etiketle yönlendirilmeye devam eder.

- “2” değeri IPv6 Açık Sıfır Etiketi olarak adlandırılır. Etiket yığınının kaldırılması ve bundan sonra yönlendirmenin IPv6 adresine göre yapılması gerektiğini belirtir.
- “3” değeri kapalı sıfır etiketidir. Bu etikeri LSR’ler atayabilir ve dağıtabilir. Bununla birlikte hiç bir zaman kapsüllemede yer almaz LSR’nin en üstteki etiketi çıkartıp ilgili arayüze -etketli veya etiketsiz- yönlendireceğini belirtir.

MPLS başlığında bulunan üç bit uzunluğundaki Exp alanı MPLS’in ilk taslaklarında Servis Sınıfı (CoS) veya tıkanıklık işareti olarak tanımlanmıştır. Bu alan servis tipi (ToS) veya DiffServ fonksiyonları için kullanılabilir.

MPLS başlığında TTL bilgisi IP ile uyumlu şekilde kullanılır. TTL alanı döngü oluşmasını engellemek amacıyla kullanılan bir mekanizmadır. MPLS paketinin takip ettiği yol boyunca üzerinden geçilen her LSR yönlendiricide TTL değeri bir düşürülür. Frame Relay veya ATM gibi TTL desteği olmayan ağlarda ise, TTL paketin omurgaya gireceği yönlendirici üzerinde, geçilecek yönlendirici kadar düşürülür. Eğer TTL değeri daha yönlendirilmeye başlamadan sıfır değerine ulaşmışsa LER yönlendirme yapmaz.

MPLS etiketlerin hiyerarşik bir şekilde kullanılmasına imkan tanır. MPLS paketi başlığında kullanılabilecek dilim paketlerin sayısı arttığı sayıca hiyerarşi eklenebilir. Bunun için teorik olarak tek engel MPLS paketinin takip edeceği patika üzerindeki En Fazla İletim Birimi (MTU) miktarıdır. En fazla iletim birimi miktarı çok fazla yükselirse IP seviyesinde parçalama işlemi yapılabilir ancak yönlendiriciler üzerinde işlemci ve bellek kullanımını arttıracağından tavsiye edilen bir durum değildir. Paket parçalama işlemi prosedürü IETF’nin RFC 3032 numaralı standardında belirtilmiştir.

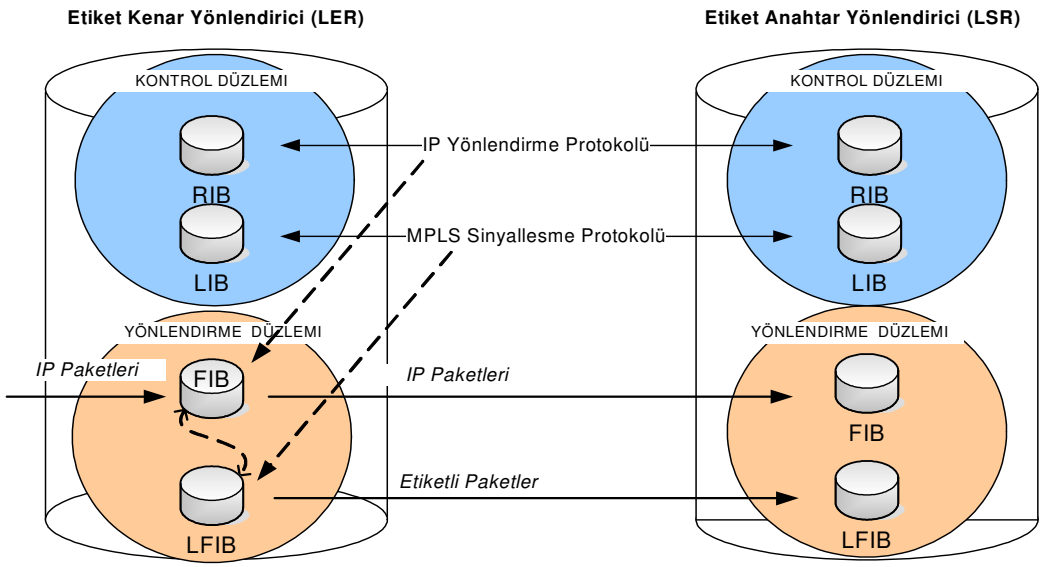
MPLS etiket yığını en son eklenen etiketin ilk önce çıkartılması esasına göre çalışır. Daha farklı ifade etmek gerekirse, x-1 sayıdaki etiketten oluşan etiket yığınına eklenen x’nci etiket, yönlendirme için ilk kullanılan etikettir. Birden fazla etiket bulunan yığınlarda LSR’ler sadece en üstteki etiketi okur ve buna göre yönlendirme yaparlar. Yönlendirilecek arayüz belirlendikten sonra MPLS başlığı çıkarılır, eğer

yeni bir etiket çıkarsa bir sonraki adımda yapılacak yönlendirme için bu başlık kullanılır. Çıkmazsa, açılan başlığın yerine yeni bir başlık eklenir ve daha önce belirlenmiş olan arayüzden paket gönderilir. Etiket yığını belli başlı üç tip uygulamada kullanılabilir. Bunlardan birincisi trafik mühendisliği yaparken daha küçük paket yönlendirme akışlarının daha büyük akışlarda toplanmasıdır. Diğer bir uygulama üstteki etiketin hedef yönlendirici, bir alttaki etiketin de bu yönlendirici üzerinde bulunan sanal özel ağ olabilir. Etiket yığınlarının bir diğer kullanım şekli ise servis sağlayıcıların birbirlerinin ağlarında tünelleme yoluyla taşımasıdır.

4.1.3.2 Kontrol ve Yönlendirme Düzlemleri

Kontrol düzlemi diğer LER ve LSR'lere ve IP yönlendiricilerine farklı yönlendirme protokolleri kullanan IP yönlendirme işlevi sağlar. Bunlarla etkileşimde bulunarak her IP adresine ulaşmak için gerekli bütün yolların tutulduğu *Yönlendirme Bilgi Tabanı* (RIB) oluşturulur. LER bu bilgileri kullanarak yönlendirme düzleminde *İletim Bilgi Tabanını* (FIB) oluşturur. [24]

Benzeri şekilde kontrol düzlemi LSR'ler ile haberleşmek için MPLS işaretleşme protokolünü kullanan bileşen içerir. Diğer MPLS çalışan yönlendiriciler ile yapılan bilgi alış verişi sonucu üzerinde anlaşılan etiket eşleştirmeleri bilgileri ile *Etiket Bilgi Tabanı* (LIB) oluşturulur. MPLS işaretleşme bileşeni IP yönlendirme işlevi ile birlikte yönlendirme düzleminde *Etiket İletim Bilgi Tabanını* (LFIB) oluşturur. [25] Aşağıdaki şekilde LER ile LSR arasındaki haberleşme ile kontrol ve iletim düzlemlerinde ilgili bilgi tabanlarının oluşturulması özetlenmiştir.



Şekil 4.1.3.2.i: Kontrol ve iletim düzlemlerinin çalışma prensibi

Yönlendirme düzlemi iki adet yönlendirme tablosundan oluşur. Bunlar karma IP ve MPLS yönlendirme bilgi tabanı (FIB) ile sadece MPLS etiketlerinin bulunduğu etiket yönlendirme bilgi tabanıdır. LSR MPLS yönlendirmesi yapan, LER ise ilk etiketlemeyi veya etiket çıkarma işlemini yapan yönlendiricidir. Şekil 4.1.3.2.i 'de görüldüğü gibi etiket kenar yönlendiricinin yönlendirme bilgi tanabı ile etiket yönlendirme bilgi tabanı varken, etiket anahtar yönlendiricinin sadece etiket yönlendirme bilgi tabanı bulunmaktadır. [24]

Yönlendirme Denklik Sınıfları (FEC), MPLS için önemli bir kavramdır. Yönlendirme denklik sınıfları, yönlendirici tarafından aynı şekilde davranılan paketlerdir. Yönlendiriciler dahili yönlendirme protokolünden paketlerin hangi ağ için nasıl yönlendirilmesi gerektiği bilgisini alırlar ve bu bilgi ile yönlendirme denklik sınıflarını oluştururlar [21]. Yönlendiriciye bir arayüzünden giren paketler bir yönlendirme denklik sınıfı ile eşleştirilirler. Bu eşleştirme için kullanılan kriterler aynı arayüzden aynı yönlendiriciye gidecek olması, aynı servis sınıfından olması, aynı kuyruğa yönlendirilecek olması ve aynı düşürme önceliği verilmesi gibi kriterlerdir. Yönlendirme bilgi tabanı belli bir alt ağa ait olan IP adresinin MPLS etiketi ve çıkış için kullanacağı arayüz gibi yönlendirme denklik sınıflarına eşleştirmeler içerir. Diğer taraftan etiket yönlendirme bilgi tabanı etiketlenmiş paket

girişleri ile operasyonları tanımlar ve bununla birlikte etiketlemiş veya etiketlenmemiş paket çıkışlarını da tanımlayabilir. Etiket kenar yönlendiricileri ile etiket anahtar yönlendiricilerine yönlendirme bilgi tabanı ve etiket yönlendirme bilgi tabanını oluşturmaları için gerekli bilgiyi sağlamak kontrol düzlemi protokollerinin görevidir. Şekil 4.1.3.2.i'de görüleceği gibi yönlendirme bilgi tabanını kullanan yönlendirme protokolleri ile etiket bilgi tabanını kullanan MPLS işaretleşme protokolleri etiketlerin dağıtılması için birlikte çalışmaktadırlar.

Bir yönlendiriciye gelen paket yönlendirilirken yapılan işlemler şu şekildedir. Gelen paketler için hangi işlemlerin yapılacağına etiket yönlendirme bilgi tabanına bakarak karar verilir. Tablo 4.1.3.2.ii'de gösterilen örnekte etiket yönlendirme bilgi tabanından öğrenilen bilgiye göre, birinci sırada gelen paketin çıkış arayüzü bu tabloya bakılarak bulunamamıştır. Bu durumda paketin MPLS başlığı çıkarılır ve içinden çıkan IP paketinin hedef ağ adres kısmında belirtilen ağa yönlendirme yapmak için IP yönlendirme bilgilerinin tutulduğu yönlendirme bilgi tabanına danışılır ve yönlendirme tablosundaki en uzun IP adres eşleştirmesine göre yönlendirme yapılır. İkinci sıradadaki paket için ise geldiği arayüz ve etiketi dikkate alınarak çıkış arayüzü olarak on iki numaralı arayüz ve etiket çıkarma işlemi belirlenmiştir. Bu durumda yine yönlendirme bilgi tabanına danışılarak IP yönlendirme yapılır. Üçüncü sırada ise üç numaralı arayüzden C etiketi ile gelen paketin on üç numaralı arayüzden etiket bilgisi değiştirilerek gönderilmesi gerektiği anlaşılmaktadır. Omurgada çalışan etiket anahtar yönlendiriciler üç numaralı işlemi yapmaktadırlar.

Tablo 4.1.3.2.ii: MPLS Paketi Yönlendirme

MPLS Paketi			Etiket Bilgi Tabani				
			Geldigi Arayüz	Etiketi	Çikis Arayüzü	Islem	
A	a.b.c.d	→	1	A	-	Etiket Çikarma	①
B	e.f.g.h	→	2	B	12	Etiket Çikarma	②
C	i.j.k.l	→	3	C	13	Etiket Takas	③

4.1.3.3 Etiket İşaretleşme Protokolleri

MPLS'in yönlendirme prensibine göre IP paketleri açılmadan, MPLS paketinin geldiği arayüze ve etiket bilgisine bakılarak hangi arayüzden yönlendirme yapılması

gerektiğine karar verilir. Ancak bu aşamaya gelmeden önce hangi etiket bilgilerinin dağıtılması, omurgada bulunan bütün ağların MPLS etiketleri ile ilişkilendirilmiş olması gerekir. Bu işlem statik veya dinamik olarak gerçekleştirilebilir.

Statik yöntemde her yönlendiricide manuel olarak hangi adrese gidileceği ve MPLS başlığında hangi etiket ile gidileceği gibi bilgiler belirtilir. Statik yöntem ağda meydana gelen değişikliklere dinamik olarak adapte olunmasını zorlaştırır ve yönetimi güçleştirir. Ağ büyüdükçe statik yerine, dinamik işaretleşme protokolleri kullanımı zorunlu hale gelmektedir. Söz konusu omurga tasarımı olduğu için dinamik işaretleşme protokolü tercih edilmelidir.

Dinamik işaretleşme protokolleri etiket bilgisi dağıtımını ve yönetimini kolaylaştırır. *MPLS Trafik Mühendisliği* bölümünde işaretleşme protokolleri seçenekleri ele alınacaktır. Bu bölümde daha genel olarak dinamik etiket dağıtım protokollerinin etiket bilgisi dağıtımı için kullandıkları yöntem iki temel yöntem ve örnek olarak LDP ele alınacaktır.

LDP (Label Distribution Protocol)

MPLS omurgasında LSR olarak isimlendirilen etiket anahtarlayıcı yönlendiricilerin MPLS paketlerinin yönlendirilmesinden sorumlu olduğu anlatılmıştı. Omurga üzerinde bu en temel işlemi gerçekleştirmek için yönlendiricilerin tutarlı bir etiket veri tabanı oluşturması ve iki yönlendiricinin etiket anlamları konusunda anlaşmaları gerekmektedir. Bu işlem *Etiket Dağıtım Protokolü* (LDP) aracılığıyla gerçekleştirilir. LDP [25] dinamik bir etiket dağıtım protokolüdür. Yönlendiriciler arasında LSP'ler dinamik olarak kurulurlar, LDP prokolü bu LSP'ler üzerinden taşınacak MPLS paketlerinin hangi etiketlerle gönderileceğini belirler ve karşıdaki yönlendiriciyi bu etiketler hakkında bilgilendirir.

LDP çalıştıran yönlendiriciler etiket değişimi yapmadan önce oturum kurmalıdırlar. LDP oturum kurmak, etiket değişimi yapmak ve etiket ver tabanını güncel tutmak için toplam dört çeşit mesaj kullanır. Bu mesajlar:

Keşif (Discovery) Mesajı: Bir LSR'nin varlığını duyurmak ve varlığını devam ettirmek için kullanılırlar.
Oturum (Session) Mesajı: LDP komşuluklarını kurmak devam ettirmek ve sonlandırmak için kullanılırlar.
Duyuru (Advertisement) Mesajı: FEC'ler için etiket eşleştirmeleri oluşturmak, değiştirmek ve silmek için kullanılırlar.
Notification (Uyarı) Mesajı: Tavsiye bilgisi sağlamak ve hata mesajı üretmek için kullanılırlar.

Bir LSR, LSP kurulumu için *bağımsız* (independent) veya *sıralı* (ordered) şekilde çalışabilirler. Bu çalışma yöntemlerine göre etiket eşleştirme metodları değişir.

Bağımsız etiket dağıtım yönteminde de iki yöntem tanımlanabilir. DOD (Downstream On Demand) yönteminde bir LSR kendisinden istenen etiket eşleştirmelerini istenilen ağa doğru olan LSR'den gelmeden kendisi oluşturup gönderebilir. DOU (Downstream Unsolicited) yönteminde ise LSR bir FEC için etiket eşleştiresi hazır hale geldiği anda kendisine bir talep gelmediği durumda da bunu komşusuna söyler. Her iki yöntemde de alt akım yönünde etiket bilgisi alınmadan üst akım etiketleri anons edilebilir.

Sıralı etiket dağıtım yönteminde ise LSR sadece sonraki düğüm bilgisi belli olan ve etiket eşleştirilmesi yapılmış olan FEC adresleri ile etiket dağıtımı başlatabilir. Etiket eşleştirilmesi yapılmamış olan diğer bütün FEC'ler için etiket dağıtımı başlatılabilmesi için alt akım LSR'sinden etiket eşleştirilmeleri alınmalıdır, aksi takdirde bu FEC'ler için etiket eşleştirmeleri yapılmaz ve üst akım LSR'lere bu bilgi söylenmez. Sıralı kontrol metodunda iki uç LSR arasında ilgili mesajlar gönderilip işlenmeden ve LSP'nin bir döngüye girmediğinden emin olunmadan veri LSP üzerinden gönderilmez.

LDP kullanılarak etiket dağıtımı yapılmadan önce iki LSR arasında arasında oturum açılmalıdır. LDP keşif mesajları için UDP 646, oturum kurulması için 646 numaralı TCP portunu kullanır.

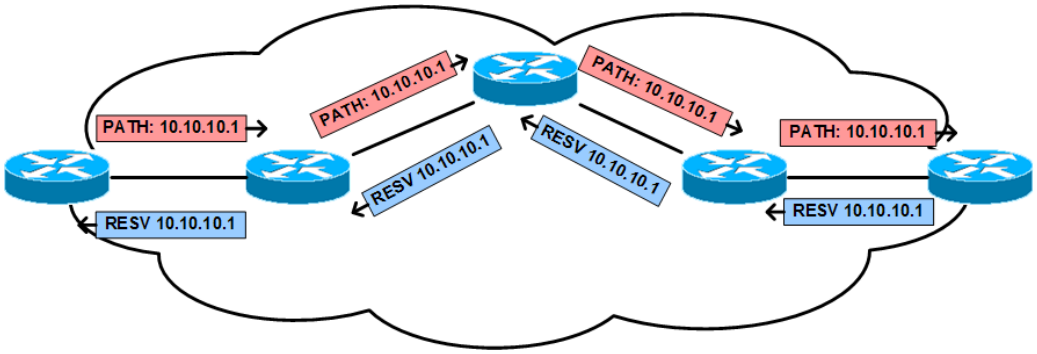
RSVP

Resource Reservation Protocol (Kaynak Ayırma Protokolü) yönlendiriciler arası trafik aktarımında kullanılmak üzere patika üzerindeki bütün yönlendiricilerde gerekli servis kalitesini sağlamak ve istenen kaynakları ayırmak için kullanılan prosedürleri tanımlayan bir ağ işaretleşme protokolüdür. [26]

RSVP, etiket anahtarlamalı patikalar kurmak için iki mesaj kullanır.

PATH Mesajı: Patika boyunca her yönlendiricide durum bilgisini saklamak amacıyla kullanılır. RSVP çalıştıran her yönlendirici patikaya doğru PATH mesajı gönderir. PATH mesajı en azından bir önceki yönlendiricinin IP adresini içerir. Bu IP adresi diğer RSVP mesajı olan RESV mesajını noktadan noktaya ters yönde göndermek için kullanılır. Önceki yönlendiricinin IP adresinin yanında PATH mesajı göndericinin *Trafik Özelliği* (Traffic Specification; Tspec) ve isteğe bağlı Adspec nesnelerini içerir. Tspec kaynaktaki yönlendiricinin en fazla veri hızı, ortalama veri hızı, zirve veri hızı, en fazla ve en az paket boyutları gibi trafik özelliklerini belirtir. İsteğe bağlı Adspec nesnesi ise patika boyunca belirli servis kalitesi hizmetlerini var olup olmadığı, patika boyunca en fazla bant genişliği, en az gecikme ve patikanın en fazla iletim büyüklüğü (MTU) gibi bilgiler ile patika üzerindeki yönlendiriciler tarafından güncellenir. Kaynaklar PATH mesajı alan yönlendiriciler RESV mesajı ile cevap verinceye kadar ayrılmaz. PATH mesajları omurgaya giriş noktasından çıkış noktasına kadar etiket eşleştirmelerini işaretleşmek ve LSP kurmak için kullanılırlar. Patika üzerindeki yönlendiricilerin etiket eşleştirmelerini bir üst yönlendiriciye göndermelerini sağlarlar

RESV Mesajı: PATH mesajını alan yönlendirciler, PATH mesajının tersi yönünde RESV mesajları ile isteklere cevap verirler. RESV mesajı patika üzerindeki yönlendiriclerde gerekli kaynak ayrımını sağlar. RESV mesajları kaynak ayrıldıktan sonra PATH mesajını gönderen yönlendiriciye gönderilir ve patika üzerindeki ilk yönlendiricinin yapılandırılması uygun trafik parametreleri ile sağlanır. PATH ve RESV mesajları periodik olarak patika üzerindeki yönendiriciler arasında gönderilmeye devam ederler. Şekil 4.1.3.3.i



Şekil 4.1.3.3.i: PATH ve RESV mesajlarının gönderimi

RSVP işaretleşme modeli DOD (Downstream On Demand) etiket dağıtım metodunu kullanır. Belirli bir LSP için etiket eşleştirme isteği omurgaya girişteki LSR tarafından PATH mesajı ile belirtilir. Bu amaç için PATH mesajı LABEL_REQUEST nesnesi ile birlikte kullanılır. [27] Alt akım yönlendiricisinde etiketler tahsis edilir ve üst akım yönlendiricisine RESV mesajı ile duyrulur. Bu amaç için RESV mesajı LABEL nesnesi ile genişletilmiştir. RSVP'nin temel çalışma esası bu şekildedir.

4.1.3.4 MPLS'te Servis Kalitesi (MPLS ve QoS)

IP "best-effort" yani "en iyi çaba" ilkesine dayalı olarak çalışır. Buna göre ağ üzerinde bir sıkışma meydana geldiği anda meydana gelen paket kayıpları trafik tipinden bağımsızdır. Servis sağlayıcılar farklı trafik tiplerine farklı öncelikler vermek, dolayısıyla servis kalitesini sağlamak amacıyla servis kalitesi uygulamaları kullanırlar.

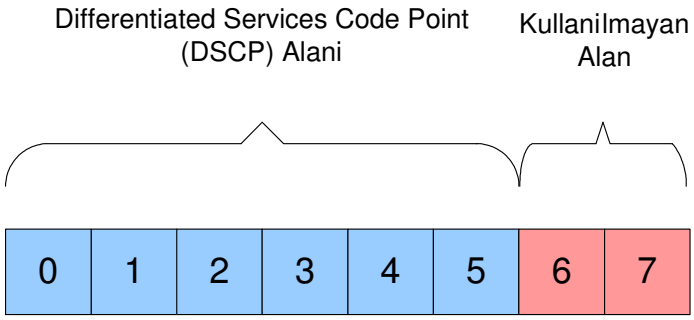
Servis kalitesi uygulamalarında iki tip yaklaşım vardır. Bunlar *IntServ* ve *DiffServ* olarak adlandırılan modellerdir.

IntServ: IntServ, servis kalitesi sağlanmasında gerçek-zamanlı uygulamalara hizmet vermek ve farklı trafik sınıfları arasında bant genişliği dağıtımını kontrol etmek için tanımlanmıştır. Buna göre IntServ mimarisinde *Garantili Servis* ve *Kontrollü Yük Servisi* isimli servis tipleri bulunmaktadır. IntServ bu servisleri sağlamak amacıyla bir çok parametreyi işaretleşmek durumundadır. Bu parametreleri işaretleşmek amacıyla RSVP kullanılır. RSVP patikalar kurulurken gerekli işaretleşmeyi yaparak parametrelerin yönlendiriciler üzerinde yüklenmesi işlemini gerçekleştirir. RSVP kullanıldığından dolayı patika üzerindeki her yönlendiricide elle yapılandırma

sağlanmalıdır. Bu ise IntServ modelini bant genişliğinin kesin bir şekilde sağlanması avantajına karşılık olarak, ölçeklenebilirlik konusunda dezavantajlı konuma düşüren bir özelliktir.

DiffServ (Differentiated Services; Farklılaştırılmış Servisler): DiifServ servis kalitesi uygulamasında IntServ ve RSVP uygulamalarının zorluğuna alternatif olarak daha kullanımı ve uygulaması kolay bir model olarak karşımız çıkmaktadır. DiffServ modelinin amacı kullanıcıların performans itiyaçlarını karşılamaktır. DiffServ modeli servis sağlayıcıların farklı müşteriler için farklı servis sınıfları sunmasına imkan verir.

DiffServ mimarisi işaretleme için IPv4 paketlerindeki servis sınıfı sekizlisini, IPv6 paketinde ise trafik sınıfı sekizlisini kullanır. DiffServ farklı özelliklerdeki trafiği işaretleyerek farklı sınıflara atar ve bu sınıflar her yönlendiricide *"düğüm davranışı"* (Per Hop Behaviour; PHB) alırlar. DiffServ mimarisi yönlendiricilerde PHB'lerin tanımlanması ve atanması, paket sınıflandırması ve trafik durumuna göre koşullandırmaları içeren işlemler topluluğudur. PHB'ler trafiğe omurga giriş noktasında daha önceden belirlenmiş olan politikaya kriterlerine uygun olarak atanır. Mevcut uygulanan iki tip PHB, "*Expedited Forwarding" (EF)* ve *"Assured Forwarding" (AF)* olarak adlandırılır. EF'nin tek bir kodu vardır (101110) ve toplamda en yüksek servis kalitesini sağlar. AF'de ise üç çeşit paket düşürme önceliği ve her paket düşürme önceliğine ait dört çeşit sınıf bulunmaktadır.

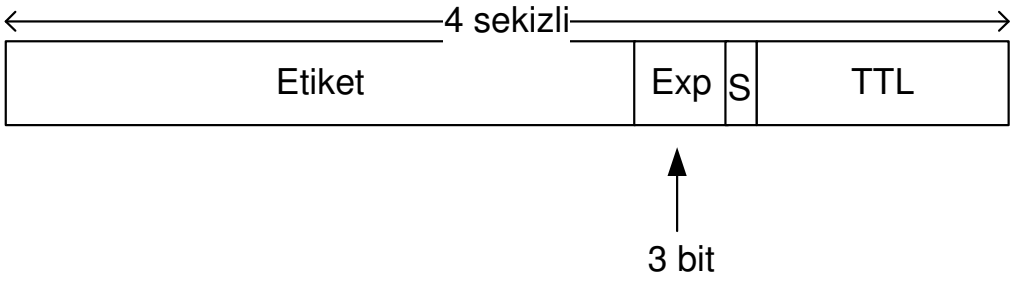


Şekil 4.1.3.4.i: DSCP sekizlisi

DiifServ sahası, birbirinin dilinden anlayan ve aynı servis kalitesi servislerini tanımlamak için kullanılan yönlendiricilerden oluşan alandır. DiffServ bu saha içinde tanımlanır ve kullanılır. DiffServ ağlarında bir pakete nasıl davranılacağına gelen IP paketinde işaretlenmiş olan DSCP (DiffServ Code Point) değerine göre karar verilir. Aynı DSCP değerine sahip olan paketler topluluğu *"davranış toplamları"*nı (BA) oluştururlar. DiffServ modeli IntServ modeline göre daha ölçeklenebilir bir modedir. Akışların sınıflandırılması, politikaların uygulanması ve işaretleme gibi servis kalitesi işlevleri DiffServ sahası sınır yönlendiriciler tarafından gerçekleştirilir. Sınır yönlendiricilerin dışında kalan yönlendiriciler sadece DSCP değerine göre yönlendirme işinden sorumludurlar. IntServ modelinde en küçük servis kalitesi uygulanan birim *"akış"* (flow) iken, DiffServ modelinden en küçük birim "*sınıf*"'tır (class)

MPLS ve QoS

MPLS ağlarında omurgaya giren bir paket, giriş noktasındaki yönlendirici tarafından bir FEC'e atanır ve bu işlem sadece omurgaya giriş sırasında ve bir kere yapılır. Diğer yönlendiriciler sadece kendilerine gelen bu pakete etiket takas işlemi uygulayarak bir sonraki yönlendiriciye aktarırlar. DiffServ ile MPLS bu noktada benzerlik göstermektedir. DSCP değerleri DiffServ sahasına girişte atanır ve DiffServ dahası terkedilinceye kadar bu alanla ilgili işlem yapılmaz. RFC 3270, MPLS ağlarında DiffServ kullanımı ile ilgili çözüm sunmaktadır. Bu çözüm MPLS ağlarında davranış toplamları ile LSP'ler arasında en iyi DiffServ eşleştirmesinin sağlamasına imkan vermektedir.

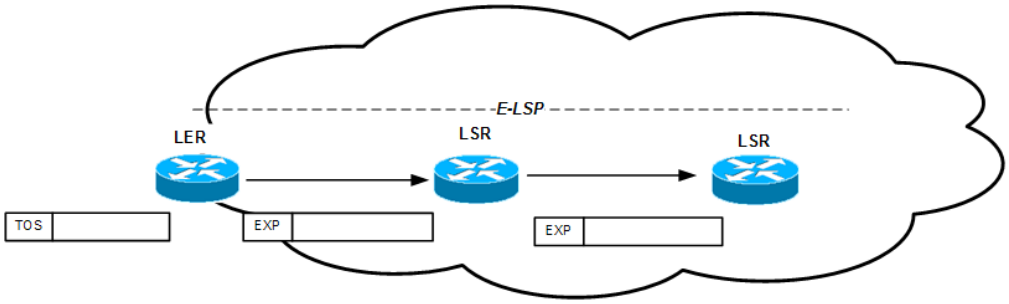


Şekil 4.1.3.4.ii: MPLS paket yapısı ve EXP alanı

IP paketi MPLS omurgasında taşınmak üzere LER'e geldiğinde LER, IP paketindeki TOS alanına bakar ve DSCP değerini öğrenir, buna göre uygun bir LSP'ye atanır.

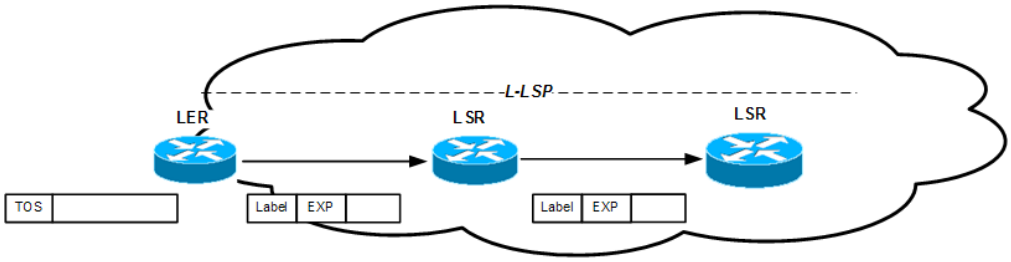
MPLS DiffServ trafiğini LSP'lere atayabilmek için iki yöntem bulunur. Bunlar E-LSP ve L-LSP olarak adlandırılırlar.

Eğer ağ en fazla sekiz çeşit düğüm davranışı (PHB) destekleyecek ise nasıl davranılacağını belirtmek için EXP bitleri yeterli olacaktır. LSR'ler EXP değerlerini PHB'ye eşleştirirler ve bu eşleştirmeye göre DSCP bitlerine göre düşürme önceliği ve zamanlama önceliği PHB davranışları gerçekleştirilmiş olur. Bu yöntem E-LSP olarak adlandırılır. Ancak şekil 4.1.3.4.i'den de görülebileceği gibi DSCP davranış toplamlarını (BA) tanımlamak için altı bit kullanabilir ve altmış dört çeşit sınıflama sağlanabilir. Bu durumda E-LSP yöntemi DSCP bitlerinde tanımlanabilen bütün davranış toplamlarının MPLS paketlerine aktarımı için yeterli olmayacaktır.



Şekil 4.1.3.4.iii: E-LSP yöntemi

L-LSP yönteminde etiket, FEC hedefini ve zamanlama önceliğini belirtmek için kullanılır. Exp alanı ise sadece düşürme önceliğini tanımlamak için kullanılır [28]. Bundan dolayı bir L-LSP yalnız bir tane sıralı toplam taşıyabilir. L-LSP yönteminde tek bir FEC+BA kombinasyonu için bir LSP kullanılır. Bu nedenle omurgada etiket kullanımı daha fazladır ancak bu yöntemle daha fazla davranış toplamı oluşturularak daha ayrıntılı servis kalitesi tanımlamaları yapılandırılabilir.



Şekil 4.1.3.4.iv: L-LSP yöntemi

4.1.3.5 MPLS Trafik Mühendisliği

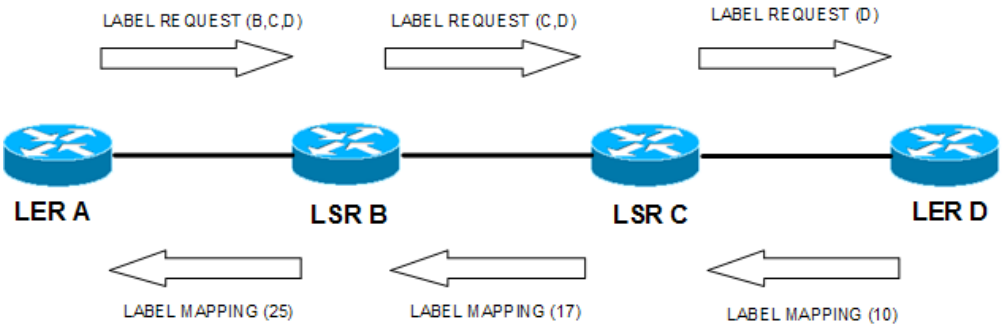
IP ağları omurgalarında trafiğin en kısa yoldan gidilmesi gereken ağa taşınıp trafiğin omurgadan çıkarılması esastır. Bu yöntem daha önce de belirtildiği gibi en iyi çaba (best effort) olarak adlandırılır. Ancak en iyi yöntem bu değildir. Trafiğin en kısa yoldan taşınması, belirlenen en kısa yol yoğun şekilde kullanıldığında bant genişliği dolsa dahi yeni trafik akışlarının yine aynı patikayı takip ederek götürülmeye çalışılmasını engellemez. Bu durumda yol üzerinde sıkışma ve dolayısıyla paket kayıpları kaçınılmazdır. MPLS teknolojisi *Trafik Mühendisliği* (Traffic Engineering) kavramıyla bu sorunu çözmeyi amaçlar. MPLS teknolojisinde IP paketleri omurgaya girdiklerinde ulaştırılmak istenen ağa göre MPLS etiketleri ile damgalanırlar ve omurga üzerinde taşınırken bu etiketlerdeki bilgilere göre yönlendirilirler. Bu paketlerin istenilen yoldan taşınabilmesi için MPLS'e avantaj sağlar çünkü MPLS dahili yönlendirme protokolünden öğrenilerek gerçekleştirilen LDP ile oluşturulan etiket ilişkilendirme işleminden daha fazlasını yaparak ilgili trafiğin taşınması için trafik mühendisliğini kullanır. Trafik mühendisliği bant genişliğinin daha etkin kullanımı, öncelikli hatta meydana gelen problemde yedek yolun kontrollü şekilde istenildiği yerden kurulması gibi avantajlar içermektedir.

Trafik mühendisliği için iki ayrı protokol kullanılabilir. Bunlar CR-LDP (Constraint-based Routed Label Distribution Protocol) ve RSVP-TE'dir (Resource Reservation Protocol – Traffic Engineering). RSVP bir önceki bölümde ele alınmıştı. RFC 3209, RSVP protokolüne bazı eklemeler yaparak onu trafik mühendisiliğine uygun hale getirir. RSVP, İnternette *Entegre Servisler* (Integrated Services) servis kalitesi uygulamaları için icat edilmiş bir protokoldür. Bu nedenle MPLS'te trafik mühendisliği uygulamaları için etiket anahtarlamalı patikalar kurmak dışında trafik mühendisliği için daha gelişmiş özellikleri içermemektedir. RFC 3209'da içerilen eklemelerle RSVP, trafik mühendisliği için daha uygun özellikler barındırmaktadır. RSVP-TE ile her bir adımın nereden geçmesi gerektiği belirtilen yollar tanımlanabilmektedir.

CR-LDP

CR-LDP, LDP'ye bazı yeni eklemeler içerir. LSP'lerin gerekli kısıtlamalarla kurulması, diğer bir deyişle kurulurken istenen kaynak ayrımları ile kurulmasını sağlar [29]. LDP'de olduğu gibi TCP oturumları kullanır.

İşleyişi şu şekilde özetlenebilir. Omurga giriş noktasında bulunan A yönlendiricisi otorum için gerekli olan parametreleri gözönünde bulundurarak kurulması gereken patikanın B yönlendiricisi üzerinden geçmesi gerektiğine karar verir ve B yönlendiricisine B,C ve D yönlendiricilerini içeren yolu ve kurulması gereken yolun parametrelerini içeren bir LABEL_REQUEST mesajı gönderir. A yönlendiricisi bu mesajı gönderirken yol için gerekli kaynakları ayırır. B yönlendiricisi LABEL_REQUEST mesajını alır ve bu LSP için kendisinin son nokta olmadığına karar verir mesajın içeriğinde bulunan B yönlendiricisine LABEL_REQUEST mesajında bulunan yol bilgisini C ve D'yi içerecek şekilde değiştirerek iletir. ve bunu yaparken gerekli kaynak ayrımını yapar. LABEL_REQUEST mesajını alan C yönlendiricisi aynı şekilde kendisinin son nokta olmadığına karar vererek mesajı bir sonraki yönlendirici olan D yönlendiricisine LABEL_REQUEST mesajındaki gerekli değişiklikleri yaparak yönlendirir.



Şekil 4.1.3.5.i: CR-LDP işaretleşmesi

D yönlendiricisi bu LSP için çıkış noktası olduğuna karar vererek gerekli kaynak ayrımını yapar ve bu LSP için etiket atar. Son şeklini almış olan kaynakların bilgisini içeren LABEL_MAPPING mesajı ile bu yola atadığı etiket bilgisini C yönlendiricisine gönderir. C yönlendiricisi de bu yol için gerekli etiket atadıktan ve bu yol için kendisinin gönderdiği LABEL_REQUEST mesajı ile karşılaştırdıktan

sonra mesajı güncelleyerek kendi atadığı etiket ile B yönlendiricisine LABEL_MAPPING mesajı gönderir. B yönlendiricisi de aynı şekilde davrandıktan sonra A yönlendiricisine LABEL_MAPPING mesajını yönlendirir. A yönlendiricisi LABEL_MAPPING mesajını alır anca kendisi bu LSP için başlangıç noktası olduğu için etiket ataması yapmaz LSP kurulumu tamamlanır. B, C ve D yönlendiricileri kendilerine gönderilen istekteki trafik parametlerine uygun cevap veremiyorlarsa en uygun kaynağı eğer LABEL_REQUEST mesajında belirtilen parametler müzakere edilebilir parametrelerse değiştirip en uygun kaynak atamasını atarlar. Yoksa LSP kurulumu yapılamaz.

CR-LDP, RSVP ile karşılaştırıldığında TCP oturumları kurarak LSP kurulumu yaptığı için daha güvenlidir. RSVP, IP kullanır ve bağlantısız şekilde çalışır. RSVP'nin bağlantısız olması trafik sıkışıklıklarında zaman aşımı nedeniyle mesajların değiş tokuş yapılamadığı durumlarda gecikmeye sebep olur. Ayrıca RSVP'nin periyodik olarak canlı tutma (keep-alive) mesajları gönderiyor olması ölçeklenebirliğini sınırlamaktadır. CR-LDP ise bu konuda TCP oturumlarına güvenir. Bu sıraladıklarımıza göre büyük omurgalarda trafik mühendisliği işaretleşmesi için CR-LDP daha uygundur.

4.2 MPLS Omurga Tasarımı

Bu bölüme kadar servis sağlayıcıların omurgalarının temel yapısı, omurgada hangi teknolojilerin kullanılabileceği konuları üzerinde duruldu. Bu bölümde daha önce bahsedilenler ışığında örnek bir omurganın nasıl tasarlanabileceği konusu tartışılacaktır.

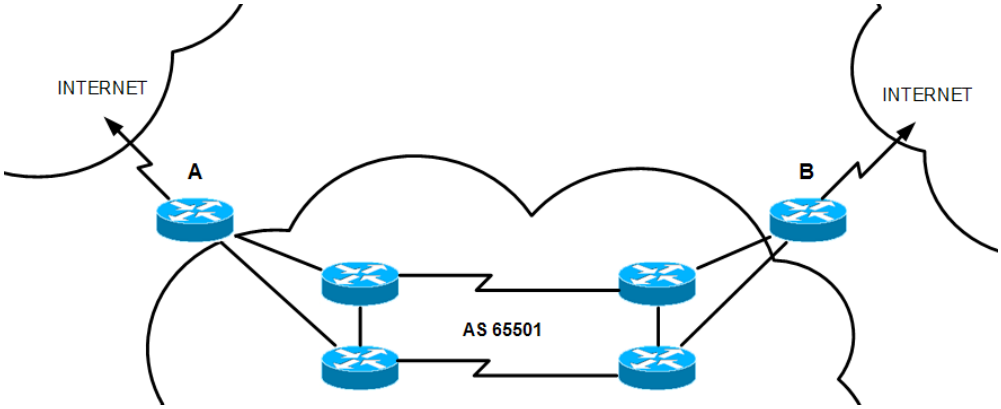
4.2.1 Tasarım

Omurga tasarımında taşınacak trafik miktarına göre uygun teçhizat ve donanımım burada bahsedeceğimiz özellikleri destekler şekilde sağlandığı, iletim şebekesinin gerekli alt yapıyı ve ilgili bant genişliklerini sağladığı ve fiziksel topolojinin bölüm 2.1'de anlatılanlara uygun olarak yapıldığı varsayılacaktır.

4.2.2 Tasarım Önerileri

4.2.2.1 Fiziksel Yapı

Otonom sistemden çıkış için çekirdekte bulunan yönlendiriciler veya bunlara doğrudan bağlanacak ve sadece bu işi yapmak için kullanılacak yönlendiriciler kullanılmalıdır.



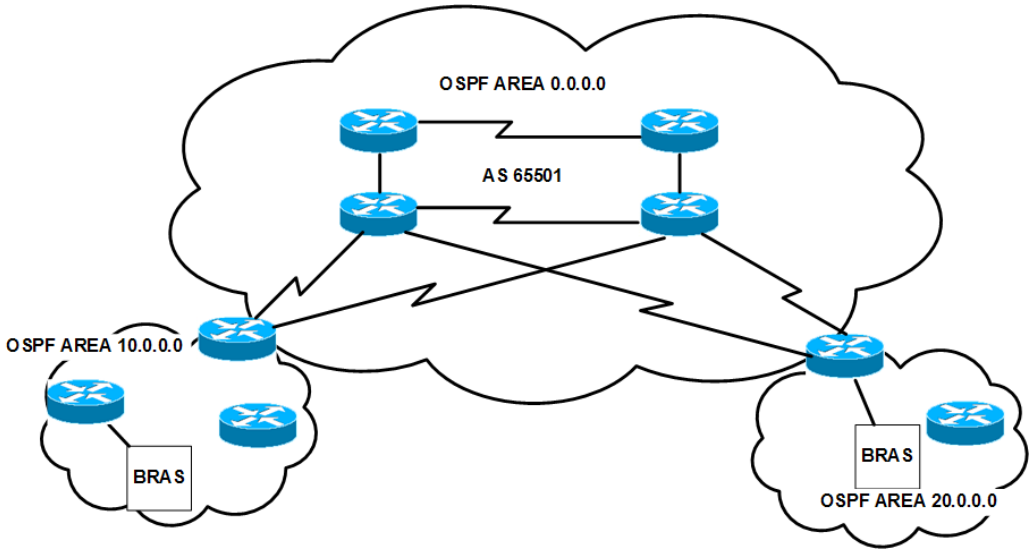
Şekil 4.2.2.1.i: 65501 Otonom sisteminin diğer otonom sistemlerle bağlantısı

Servis sağlayıcı omurgalarında hiyerarşik yapı düşünüldüğünde müşterilerin sonlandırılacağı yönlendiriciler erişim katmanında bulunur. Günümüz teknolojisinde erişim katmanında bant genişliklerini de ele alırsak uç noktalardaki yönlendiricilerde örnek vermek gerekirse ADSL aboneleri veya Metro Ethernet teknolojisi sunulan müşteriler sonlandırılmaktadır. ADSL müşterilerinin sonlandırılacağı yönlendiriciler özelleşmiş BRAS olarak anılan (Broadband Remote Access Server: Genişbant Uzak Erişim Sunucuları) yönlendiricilerdir. Temel işlevi müşteri sonlandırmak ve müşteri trafiğini omurgaya dahil etmektir. Bunun dışında omurgada bulunan ve BRAS bağlı olmayan uç noktalardaki yönlendiricilerde İnternet erişimi için veya noktadan noktaya erişim için müşteri sonlandırması yapılacaktır.

4.2.2.2 Kullanılacak Protokoller

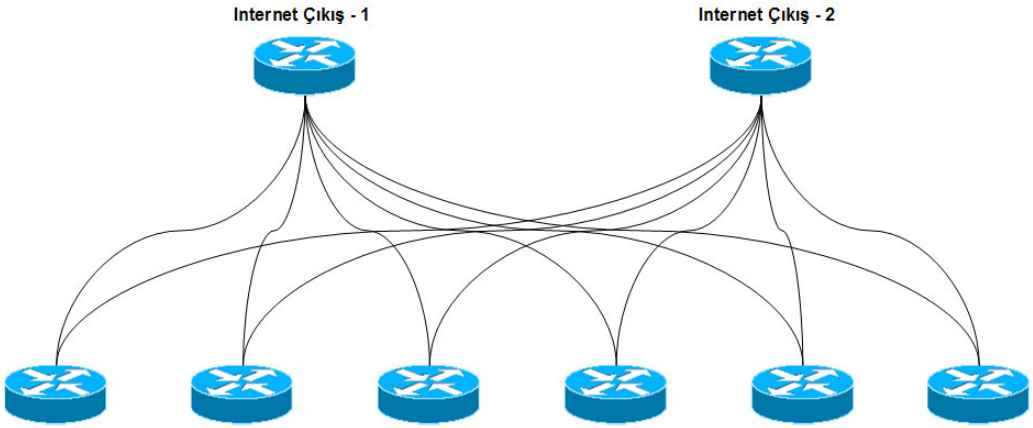
Dahili yönlendirme protokolü olarak standart bir dahili yönlendirme protokolü kullanılacaktır. Günümüzde en çok kullanılan ve ölçeklenebilirlik konusunda servis sağlayıcı omurgasına uygun olarak OSPF protokolü düşünülebilir. Müşteri

sonlandırılacak uç noktalarda NSSA veya STUB OSPF bölgeleri, omurgada daha küçük alanları içeren yönlendirme bilgilerinin dolaşmasını engeller ve gerekli bağlantı durum bilgisi anons paketleri trafik yükü zaten fazla olacak olan ve işlemci ve belleğin en verimli şekilde kullanılması gerektiği omurga yönlendiricilerde yükün azaltılmasına imkan tanır.



Şekil 4.2.2.2.i: Genişbant erişim sunucularının kullanımı

Tasarımımızda harici yönlendirme protokolü olarak BGP kullanılacaktır. Burada önemli nokta, BGP'den öğrenilen yol bilgilerinin dahili yönlendirme protokolü olan OSPF'e dağıtılmaması olacaktır. Omurgada bulunan yönlendiriciler BPG çalışacaklar, ancak çekirdek bölgesinde yer alan yönlendiriciler BGP çalışmayacaklardır. Omurgadaki yönlendiricilerin yol bilgilerini almaları için İnternet çıkış yönlendiricileri sunucu rota yansıtıcıları olarak kullanılacak, omurgadaki diğer yönlendiriciler istemci rota yansıtıcıları olarak görev yapacaklardır. Buna göre istemci rota yansıtıcıları, sunucu rota yansıtıcılardan bütün BGP anonslarını alacaklardır. Omurgada OSPF kullanıldığı ve sadece omurgadaki yol bilgileri OSPF ile dağıtıldığından dolayı, İnternet'e çıkacak herhangi bir abone BGP'den alınan yol bilgilerini kullanacakır. Şekil 4.2.2.2.ii'de rota yansıtıcı sunucuları ile istemcileri arasındaki mantıksal yapısı gösterilmektedir. BGP oturumları TCP ile kurulduğundan dolayı IBGP oturumu kuracak olan iki yönlendirici birbirine doğrudan bağlı olmak zorunda değildir.



Şekil 4.2.2.2.ii: Yansıtıcı sunucuları ile istemcileri arasındaki IBGP oturumları

Omurgada kullanılacak olan bir diğer protokol LDP'dir (Label Distribution Protokol). LDP, OSPF'ten aldığı yol bilgisine göre, gidilecek hedef ağlara etiket atar. Bir yönlendiriciden bir ağa erişmek için yönlendiriciden çıkış arayüzü bellidir. Bu arayüzden çıkacak MPLS paketinin hangi etiket bilgisi ile çıkacağına LDP karar verir.

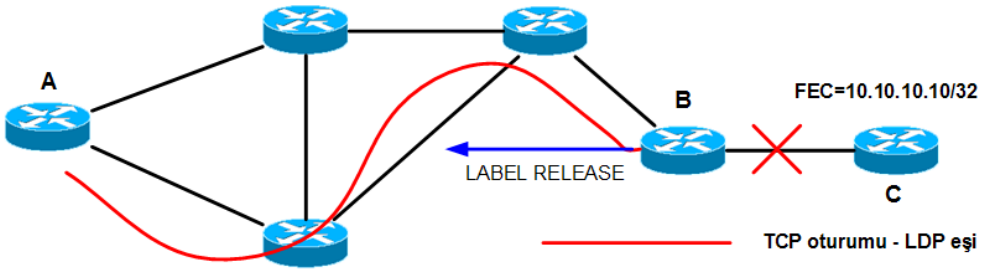
Omurgada çekirdekteki yönlendiricilerin BGP protokolü çalıştırmayacakları belirtilmişti. Burada LDP'den faydalanılacaktır. RFC 3906'da ayrıntıları verilen bu yönteme göre, uç noktalarda üzerinde abone sonlandırılan yönlendiriciler, eğer BGP'den öğrenilen bir yol için gidilecek yönlendirici LDP ile de erişilebilir durumda ise, trafik LDP ile oluşturulmuş olan LSP'ler üzerinden taşınır. Böylece çekirdekteki yönlendiriciler BGP çalıştırmıyor ve dolayısıyla yönlendirme tablolarında gidilecek adres olmasa dahi, BGP paketlerini gitmeleri gereken yere MPLS paketleri olarak yönlendireceklerdir.

4.2.3 Tasarım Önerisi

Tezin ana motivasyonunu oluşturan bu bölümde ayrıntılara geçmeden önce LDP'nin güvenilirliği tartışılacak ve FRR (Fast Reroute; Hızlı Yeniden Yönlendirme) mekanizmasından bahsedilecektir.

LDP, dinamik bir etiket dağıtım protokolü olduğundan dolayı, servis sağlayıcı omurgalarında RSVP'ye tercih edilmektedir. LDP protokolü çalıştıran LSR'ler, TCP kurarak güvenli oturum kurarlar ve protokol mesajlarını bu oturum üzerinden

gerçekleştirirler. LDP çalıştıran yönlendirici bir ağa ait yönlendirme bilgisi dahili yönlendirme protokolünden gelmiyorsa artık bu ağa erişimi olmadığını düşünür ve TCP oturumu kurduğu LDP eşine LABEL RELEASE mesajı gönderir. LABEL RELEASE mesajı "Bu etikete sahip hedef ağa gitmek için artık beni kullanma" anlamına gelir. LABEL RELEASE mesajını gönderen yönlendirici, güvenli olan TCP oturumu üzerinden mesajlaştığı LDP eşinden mesajın alınmış olduğu bilgisinin kendisine ulaşmasını beklemez. LDP'nin çalışma prensibi ile ilgili bahsedilmesi gereken diğer önemli bir nokta da iki LDP eşi arasındaki TCP oturumu kesildiği anda LSP'nin anında düşürülmesidir. Böyle bir durumda LSP kapatılır ve bu LSP için kullanılan etiketler ve kaynaklar serbest bırakılır. [30]

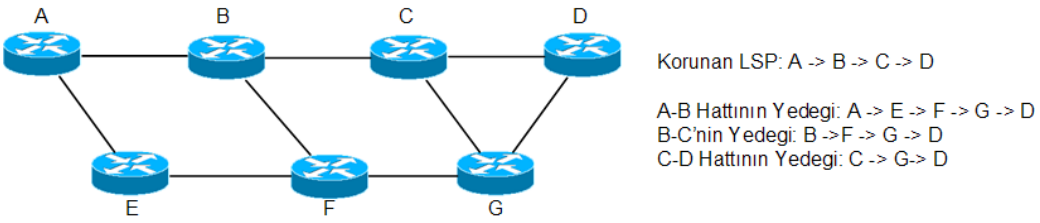


Şekil 4.2.3.i: TCP oturumu ile B ve C bağlantının aynı anda düştüğü senaryo

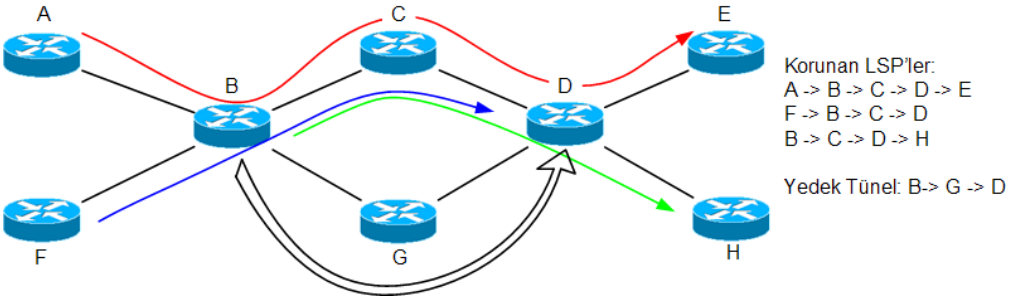
Örnek olarak şekil 4.2.3.i'de verilen senaryoda B yönlendiricisi LDP eşi olan A yönlendiricisine doğru LABEL RELEASE mesajı göndererek 10.10.10.10/32 FEC'ine gitmek için kendisinin kullanılmaması gerektiği bilgisini gönderir. Aynı sırada A ve B yönlendiricileri arasındaki TCP oturumunun farklı sebeplerden düştüğünü varsayarsak B yönlendiricisnin gönderdiği LABEL RELEASE mesajı A yönlendiricisine ulaşmayacaktır ve A yönlendiricisi bu FEC'e ulaşmak için kullandığı etiketleri kullanmaya devam edecektir. Buna göre A yönlendiricisinden 10.10.10.10/32 FEC'ine yollanması gereken MPLS paketleri aynı arayüzden gönderilmeye devam edecektir ve paket kaybı oluşacaktır. Böyle bir hatayı oluştuktan sonra düzeltecek mekanizma LDP'de bulunmamaktadır.

Aynı şekilde operatör hataları, donanım hataları gibi sebepler, yazılımda meydana gelebilecek hatalar nedeniyle MPLS etiketlerinin güncellenmemesi gibi hatalar yanlış etiket eşleştirmesi kullanımına sebep olabilir.

Burada bahsedilecek ve önerilen tasarımda kullanılacak MPLS'in sunduğu önemli bir mekanizma *Hızlı Yeniden Yönlendirme (FRR: Fast-Reroute)* mekanizmasıdır. FRR mekanizması LSP'lerin yedekli olarak kurulmasına imkan tanır. Buna göre FRR ile korunmuş bir LSP'de, herhangi bir sebepten dolayı düşme ihtimaline karşı yedek patikalar önceden belirlenerek alternatif tüneller kurulur ve etiketlenir. Bu etiketler omurgada başka bir yerde kullanılamaz çünkü tünel aktif hale gelince bu etiketle yönlendirme yapcaktır. Birincil LSP düşerse FRR ile oluşturulmuş yedek LSP kullanılır. FRR 50ms'nin altında trafiğin tekrar yönlendirilmesini hedef alır. LSP'nin korunması iki yöntemle yapılabilir; *birebir yedek* (one-to-one backup) ve *kolaylaştırılan yedekleme* (facility backup) yöntemleri iki alternatiftir. one-to-one backup yönteminde her LSP için yedek patika belirlenir. Kolaylaştırılan yedekleme yönteminde ise muhtemel problem noktasından geçen LSP demeti korunur.



Şekil 4.2.3.ii: Birebir yedekleme yöntemi

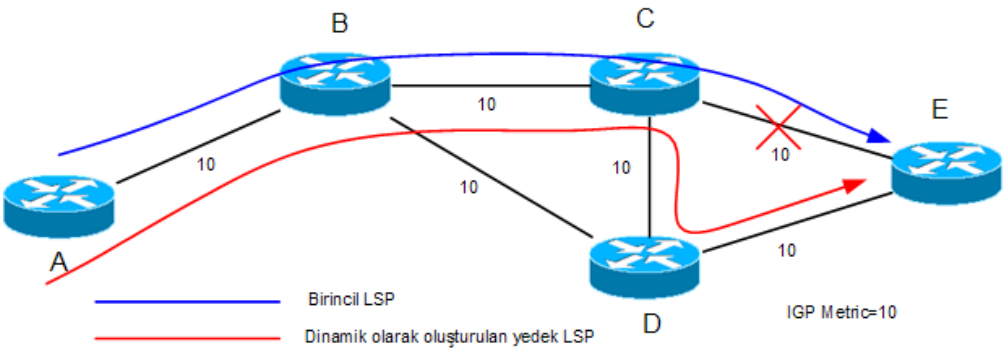


Şekil 4.2.3.iii: Kolaylaştırılan yedekleme yöntemi

Şekil 4.2.3.ii'de tek bir LSP yedeklenmiş ve muhtemel problem noktaları için yedek tüneller ayrılmıştır. Daha fazla LSP tanımlanmış olsaydı, onlar için de aynı şekilde yedek tüneller ayrıca belirlenip koruma sağlanacaktı. Şekil 4.2.3.iii'de ise B, C ve D noktalarından geçen üç ayrı tünel için, B ve C arasındaki hatta veya C noktasında meydana gelmesi muhtemel hat problemi için, B yönlendiricisi G ve D yönlendiricilerinden geçen koruma tüneli hazırlamıştır. Kolaylaştırılmış yedekleme

yöntemi aynı anda birden fazla LSP'yi koruduğu için daha az etiket rezervasyonu gerektirir ve daha ölçeklenebilir bir çözümdür. Birebir yedekleme yöntemi ise her bir LSP'yi patika üzerindeki arıza oluşması muhtemel bütün hatlar için koruma sağladığından daha güvenlidir. Sunulacak öneride omurganın tamamında LDP kullanılacağı ve sadece kritik noktalar için FRR kullanılacağı için birebir koruma yöntemi tercih edilecektir.

FRR metodu RFC 4090'da tanımlanmıştır. FRR'de kullanılan terimler şunlardır:
PLR (Point of Local Repair: Yerel Koruma Noktası): Korunmakta olan tünelin düştüğü durumda problemin meydana geldiği ve kullanılacak yedek patikanın geri kalan bölümü için kullanılacak tünelin başlangıç noktası.
MP (Merge Point: Birleşme Noktası): Oluşturulan yedek tünelin, orjinal LSP ile birleştiği nokta.
FRR'nin birebir yedekleme yöntemi ile çalışma prensibi şu şekildedir:

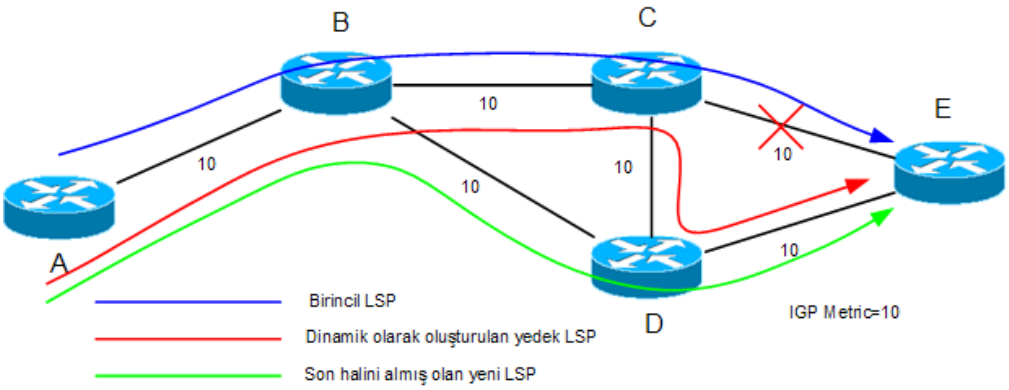


Şekil 4.2.3.iv: FRR çalışma senaryosu

A yönlendiricisinde başlayarak sırasıyla B ve C yönlendiricilerinden geçerek E yönlendiricisinde sonlanan patika kurulmuş olsun. Birebir yedekleme yöntemine göre B ve C ile, C ve E arasındaki hattın düşme ihtimali göz önünde bulundurularak yedek tüneller daha önce belirlenmiştir. C ve E arasındaki hat düştüğü anda LSP, C'den sonra D yönlendiricisi üzerinden E'ye ulaşacaktır.

Ancak bu görüldüğü gibi takip edilebilecek en iyi yol değildir. Bütün hatların metriğinin 10 olduğu düşünülürse dahili yönlendirme protokolüne göre A->B->D->E patikası daha kısa bir yoldur. Bu sırada FRR'nin *Eski Haline Alma (Revertive)*

mekanizması çalışmaya başlar. Buna göre dahili yönlendirme protokolünden alınan bilgilere göre en kısa yol hesaplanır ve trafik yeni hesaplanan yol üzerinden akmaya başlar. Örneğimize göre yeni LSP bundan sonra A->B->D->E yolunu takip edecektir. Bu durumda B yönlendiricisi MP, C yönlendiricisi PLR'dir



Şekil 4.2.3.v: Revertive mekanizması ile LSP'ye son şeklinin verilmesi

4.2.4 Önerilen Örnek Tasarım

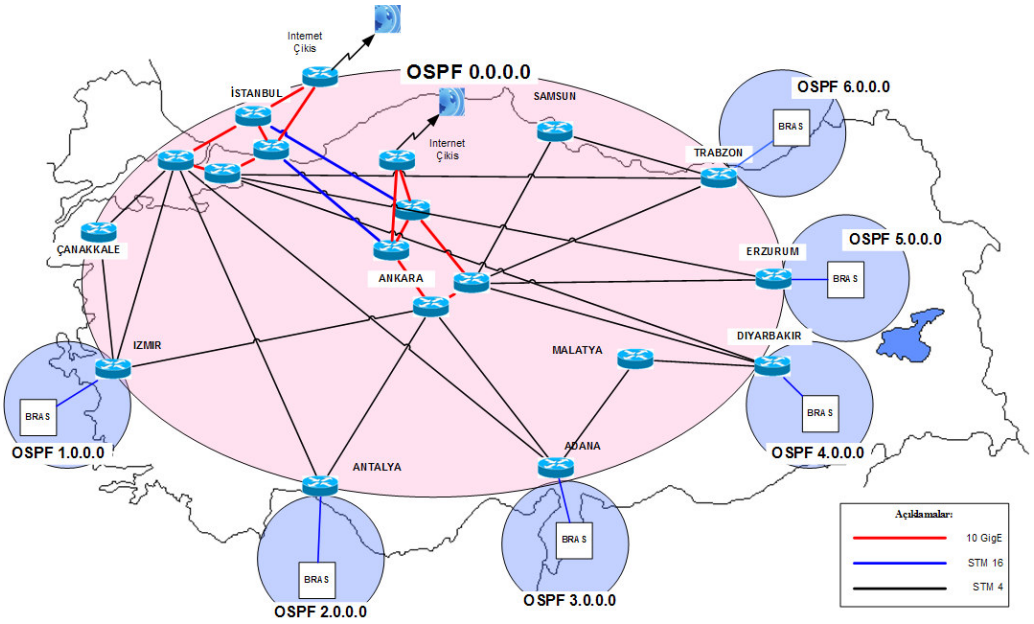
Örnek olarak Türkiye geneline yayılmış olan bir servis sağlayıcının MPLS teknolojisi kullanarak kurmak isteyeceği omurga verilecektir. Fiziksel ve mantıksal yapının ayrıntılarını şekil 4.2.4i, şekil 4.2.4ii ve şekil 4.2.4iii'de görülebilir.

Tasarımın adımları ve yapının işleyişi maddeler halinde verilmiştir.

- Ankara ve İstanbul ana merkezler olarak düşünülmektedir. Merkezlerdeki yönlendiriciler birbirlerine yerel ağda 10Gbps hızında ethernet ile bağlı olacaklardır. Ankara ve İstanbul'da ikişer tane bulundurulacak ve Ankara ile İstanbul arasındaki bağlantıyı sağlayacak olan dört adet yönlendirici, çekirdek olarak tasarlanacaktır. Ankara ile İstanbul arasında STM-16 hızında iki adet SONET hat yedekli olarak kullanılacaktır. Bu yönlendiriciler yüksek paket işleme kapasitesine sahip olacaktır. Performansı yüksek tutmak ve muhtemel sorunlarda hata gidermeyi daha kolay hale getirmek için bu yönlendiricilerde BGP çalıştırılmayacaktır. Şehirler arası akacak olan trafik çekirdekten geçecektir.
- Ankara ve İstanbul'a birer adet İnternet çıkışını sağlayacak olan yönlendirici, çekirdekte bulunan yönlendiricilere yedekli olarak bağlanacaktır. Bu yönlendiricilerin üzerinde de müşteri sonlandırması yapılmayacaktır. İnternet

çıkış yönlendiricilerinden omurgaya doğru varsayılan yol anonsu yapılacaktır. Buna göre omurgada çalışan yönlendiricilerin BGP veya OSPF yönlendirme tablosunda bulunmayan adresler için trafik İnternet çıkış yönlendiricilerine gönderilecektir.

- Omurgada bütün yönlendiricileri içerecek şekilde OSPF 0.0.0.0 bölgesi kullanılacaktır. Üzerinde ADSL, G.SHDSL ve çevirmeli bağlantı gibi uzaktan çok sayıda müşteriyi aynı anda sonlandıracak olan yönlendiriciler, 0.0.0.0 bölgesine dahil oldukları gibi, uzak erişim sunucularının sonlandırıldığı arayüzler farklı bir OSPF bölgesine dahil olacaklardır.

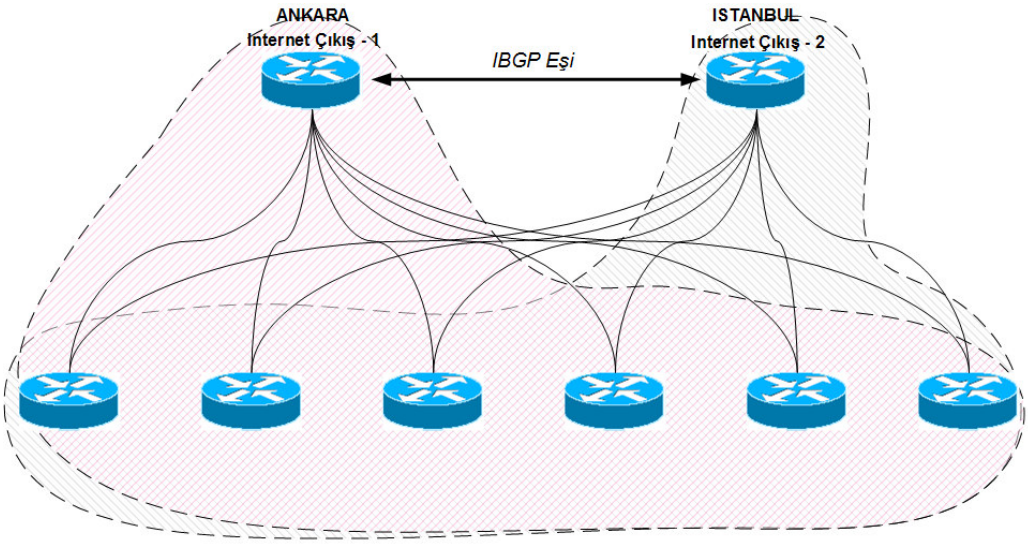


Şekil 4.2.4.i: Fiziksel yapı ve OSPF bölgeleri

Önerilen tasarımda NSSA veya STUB olarak düşünülen 1.0.0.0-6.0.0.0 OSPF bölgelerinde genişbant uzak erişim sunucuları LER'lere bağlanmıştır. Burada amaç genişbant erişim sunucularının işlemci gücünden ve bellekten tasarruf etmelerini sağlamaktadır. Üzerlerinde yapılandırılan varsayılan yol bilgileri ile bütün trafiği LER'lere yönlendireceklerdir.

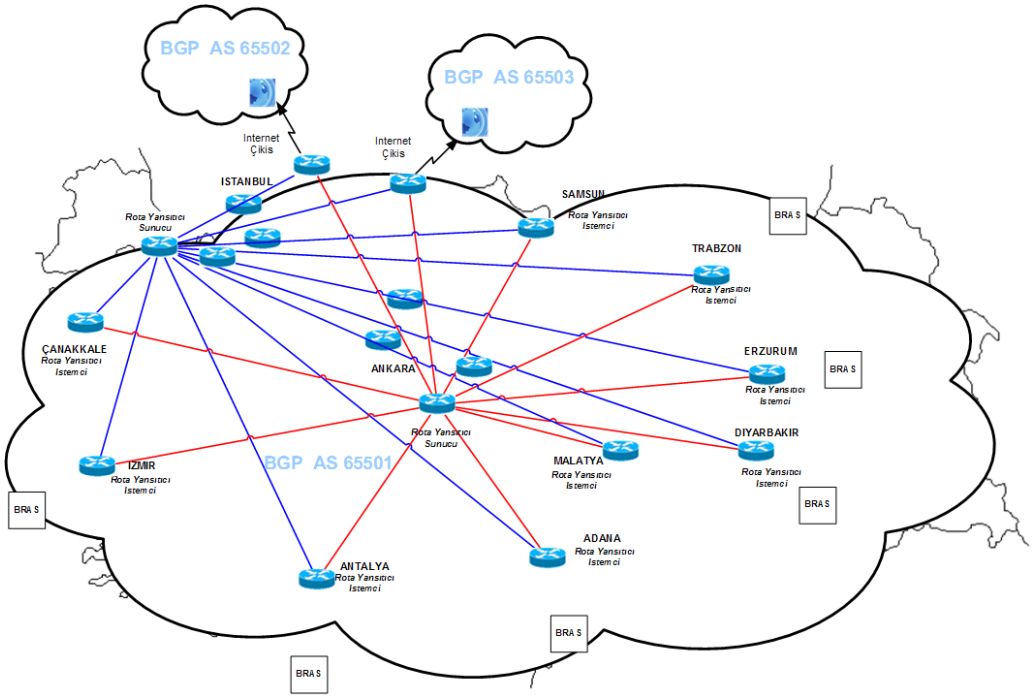
- Omurgada BGP çalışacak ve 65501 otonom sistem numarası olarak kullanılacaktır. Ankara ve İstanbul'da bulunan İnternet çıkış yönlendiricileri sırasıyla 65503 ve 65502 otonom sistemlerine bağlı olacaklardır.
- Ankara ve İstanbul'da bulunan birer yönlendirici yedekli olarak rota yansıtıcı sunucular olarak kullanılacaklardır. Bu iki yönlendirici birbirleri ile IBGP

konuşacaklardır. Aynı şekilde diğer bütün yönlendiricileri içerecek BGP bölgeleri oluşturulacak ve BGP bölgelerindeki yönlendiriciler bu iki yönlendiricinin istemcileri olacaklardır.



Şekil 4.2.4.ii: Rota yansıtıcı sunucu ve istemcileri mantıksal yapısı

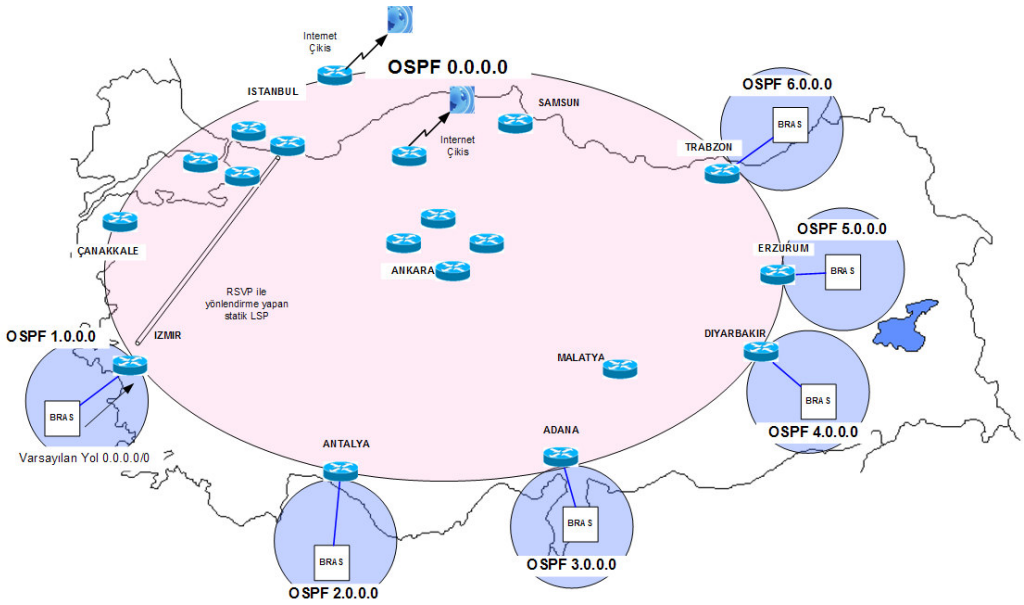
- Bütün yönlendiricilerde etiket dağıtım protokolü olarak LDP çalıştırılacaktır.
- BGP rota yansıtıcıları ile komşuluk kurularak alınan BGP anonsları sayesinde BGP yolları bütün yönlendiriciler tarafından bilinmektedir. Çekirdekteki yönlendiriciler BGP çalıştırmayacaklardır. BGP anonslarından öğrenilen adreslere gitmek isteyen yönlendiricilerde bulunan trafik, bu adresler anons eden internek çıkış yönlendiricilerine gitmek için RFC 3906'ya göre LDP kısa yollarını kullanacaktır. Buna göre dinamik olarak oluşturulmuş olan LSP'ler üzerinden İnternet erişim yönlendiricilerine ulaşılacaktır. Çekirdekteki yönlendiriciler kendilerine gelen trafiği MPLS trafiği olarak görüp gidilmek istenen İnternet çıkış yönlendiricilerine trafiği geçireceklerdir.



Şekil 4.2.4.iii: BGP yapısı ve BGP komşulukları

LDP'nin dezavantajlarından bir önceki bölümde bahsetmiştik. LDP'nin dezavantajlarının sebep olduğu etkilerden korunmak için düşünülen yapı OSPF bölge sınır yönlendiricilerini içermektedir. OSPF sınır yönlendiricileri uzak erişim yönlendiricileri ile kendisine gelen trafiği taşır. Buna göre onbinlerce aboneyi aynı anda sonlandırabilir ve aynı ayda onlarca gigabit trafik yönlendirir. Özellikle *IP Televizyon* (IPTV), *İstek Üzerine Video Yayını* (Video-on-Demand) gibi gerçek zamanlı çoklu yayın trafiği taşınıyorsa, Voice over IP gibi ses taşıma hizmetleri gerçekleştiriliyorsa bu kadar yüksek miktarda trafiğin kaybı ciddi sorunlara yol açar. LDP'nin dezavantajlarından kaynaklanabilecek olası problemlerin etkilerinden korunmak için OSPF bölgesi ile uzak erişim yönlendiricilerinin trafiğini sonlandıran yönlendiricilerin trafiğinin RSVP ile oluşturulmuş tüneller ile taşınması, bu tünellerin de Fast Reroute yöntemi ile korunması, olası problemlerde trafik kaybını en az seviyeye indirecektir. Buna göre tanımlanacak RSVP tünelleri OSPF alan sınır yönlendiricilerinden başlayacak ve çekirdek yönlendiricilerde son bulacaktır. Eğer taşınmakta olan trafik noktadan noktaya erişim trafiği ise çekirdek yönlendiricilerin OSPF veri tabanında hedef ağa ait bilgi bulunmaktadır ve yönlendirme tablosundan öğrenilen bilgiye göre trafik yönlendirilir. Eğer trafik İnternet trafiği ise, diğer bir

deyişle, BRAS'tan OSPF alan sınır yönlendiricisine gönderilmiş olan trafiğin hedefi BGP ile öğrenilmiş bir ağ ise, bu durumda çekirdekteki yönlendiriciler BGP çalışmıyor olsalar bile üzerlerinde İnternet çıkış yönlendiricileri üzerinde yapılandırılmış olan varsayılan yön bilgisine göre trafik İnternet çıkış yönlendiricilerine gönderilecektir.



Şekil 4.2.4.iv: FRR ile korunan RSVP tüneli çekirdekte sonlanır

5.SONUÇ

MPLS teknolojisinin popülerliği günden güne artmaktadır. Kullanım arttıkça farklılaşan ihtiyaçlara en iyi şekilde cevap veren MPLS teknolojisi, yeni nesil servislerin kullanımına da kolaylık sağlamaktadır. MPLS'in üzerinde çalışılan hali hazırda bir çok taslak çalışması bulunmaktadır. Bu çalışmada MPLS çalışan omurgaların handikaplarından biri olan etiket dağıtımı ve kontrol düzlemi arızalarında veya yüksek miktarda trafik taşıyan omurgalarda kaynak ayırırmı bilgilerinin eskimesi gibi durumlarda ortaya çıkan servis kalitesinin düşmesi etiket dağıtımının güncellenememe problemlerine çözüm önerisi sunulmuştur. Önerilen çözüme göre RSVP tünelleri ile LDP aynı omurgada kullanılmıştır. LDP'nin dinamik

bir etiket dağıtım protokolü olmasının avantajı ile, kritik trafiklerde FRR mekanizması ile korunan statik tünellerin garantili servis sürekliliği sağlaması avantajı beraber kullanılarak melez bir yapı kullanılmalıdır. Buna göre NSSA veya STUB OSPF bölgelerindeki trafiği çekirdeğe yönlendirecek RSVP tünelleri, OSPF veya LDP protokolünden kaynaklanacak olası problemlerden etkilenmeyecek ve trafiği çekirdek yönlendiricilere göndermeye devam edecektir.

Omurganın tamamının RSVP tünelleri ile donatılmak istenmemesinin sebebi olası gelişmelerde ölçeklenebilirlik sıkıntısı, FRR kullanıldığı zaman etiket alanının verimli kullanılamaması ve yönetimsel zorluklar getirmesidir.

Günümüzde gerek MPLS, gerekse de LDP son şeklini almış ve bütün dezavantajları elenmiş teknolojiler değildir. MPLS çalışacak bir omurga tasarlanırken bilinen dezavantajlar gözönünde bulundurularak yapılacak tasarım daha verimli çalışacaktır.

KAYNAKLAR

1. Tony Kenyon, "High Perfomance Data Network Design" Digital Press, 2002 s.92-94.
2. Matthew G.Naugle, "Network Protocols" McGraw-Hill, 1999, s.5-8.
3. James F.Kurose, "Computer Networking", Addison Wesley Longman Inc., s.321.
4. J. Hawkinson, "Guidelines for creation, selection, and registration of an Autonomous System (AS)", RFC 1930, Mart 1996.
5. J. Moy, "OSPF Specification", RFC 1131, Ekim 1989.
6. Masato Noto, Hiroaki Sato, "A method for the Shortest Path Search by Extended Dijkstra Algorithm, 0-7803-6583-6/00/$10.00, 2000 IEEE", sf.2316-2320.
7. J. Moy, "OSPF Version 2", RFC 2178, Nisan 1998.
8. Uyless Black, IP Routing Protocols, Prentice Hall Şubat 2000 s.7-12.
9. Matthew G.Naugle, "Network Protocols" McGraw-Hill, s.462.
10. Matthew G.Naugle, "Network Protocols" McGraw-Hill, sf. 463.
11. R. Rivest, "The MD5 Message-Digest Algorithm", RFC 1321, Nisan 1992.
12. ISO/IEC 10589. "Intermediate System to Intermediate System Intra-Domain Routing Exchange Protocol for use in Conjunction with the Protocol for Providing the Connectionless-mode Network Service (ISO 8473) Second Edition", Kasım 2002,
13. ISO 8473, "Protocol for Providing the Connectionless-Mode Network Service, Second Edition", Kasım 1998.
14. ISO 8348, "Informational Technology-Open Systems Interconnection- Network Service Definition, Third Edition" Kasım 2002, s.3.
15. D. McPherson, V. Gill, "BGP MULTI_EXIT_DISC (MED) Considerations" RFC 4451, Mart 2006.
16. S. Hares, A. Retana, "BGP-4 Implementation Report" RFC 4276, Ocak 2006.
17. D. McPherson, K. Patel, "Experience with the BGP-4 Protocol" RFC 4277, Ocak 2006.
18. P. Marques, F. Dupont, "Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing" RFC 2545, Mart 1999.
19. T. Bates, R. Chandra, E. Chen "BGP Route Reflection - An Alternative to Full Mesh IBGP" RFC 1966, Nisan 2000.

20. E. Rosen, A., Viswanathan, R. Callon. “Multiprotocol Label Switching Architecture” RFC 3031, Ocak 2001.
21. Arun Viswanathan, Nancy Feldman, Zheng Wang, Ross Callon, “Evolution of Multiprotocol Label Switching”, IEEE Communications Magazine, Mayıs 1998, s.165-173.
22. Grenville Armitage, MPLS: The Magic Behind the Myths, IEEE Communications Magazine, Ocak 2000, s.124-131
23. E. Rosen, D. Tappan, G. Fedorkow, Y.Rekhter, D. Farinacci, T. Li, A. Conta, MPLS Label Stack Encoding, RFC 3032, Ocak 2001
24. McDysan, David. ATM & MPLS Theory & Application: Foundations of Multi-Service Networking. Blacklick, OH, USA: McGraw-Hill Professional, 2002. s.309.
25. L. Andersson, P. Doolan, N. Feldman, A. Fredette, B. Thomas, “LDP Specification” RFC 3060, Ocak 2001.
26. R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, S. Jamin, “Resource ReSerVation Protocol (RSVP) Version 1 Functional Specification” RFC 2205, Eylül 1997.
27. D. Awduche, L. Berger, T. Li, V. Srinivasan, G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, Aralık 2001.
28. Victoria Fineberg, Cheng Chen, XiPeng Xiao, "An End-to-End QoS Architecture with the MPLS-Based Core", IEEE, 2002, s.28-29.
29. Jong-Moon Chung, "Analysis of MPLS Traffic Engineering", Proc. 43rd IEEE Midwest Symp. on Circuits and Systems, Lansing MI, Ağutos 2000, s.550-553.
30. A. Farrel, "Fault Tolerance for the Label Distribution Protocol (LDP)", RFC 3479, Şubat 2003, s.4.

Ek-1

1. Bireysel Bilgiler

Adı	: Taner
Soyadı	: BAŞULAŞ
Doğum Yeri / Tarihi	: Almanya 1978
Uyruğu	: T.C.
Adres / Telefon	: Kozyatağı Mah. Balözü Sk. No:1/17 Kadıköy İSTANBUL 0532 4039740

2. Eğitim

Beykent Üniversitesi
Fen bilimleri Enstitüsü Bilgisayar Ağları ve İnternet Teknolojileri (2004-2006)

Boğaziçi Üniversitesi
Fen ve Edebiyat Fakültesi Matematik Bölümü (1995-2003)

Bostancı Hayrullah Kefoğlu Lisesi
Türkçe-Matematik Bölümü (1992-1995)

3.Yabancı Dil

İngilizce; Çok iyi (Boğaziçi Üniversitesi Yabancı Diller Yüksek Okulu, 1995-1996)

3. Ünvanlar

B.Sc, Boğaziçi Üniversitesi Matematik Bölümü, 2003

4. Mesleki Deneyim

Alcatel Teletaş
IPD Local Support, Network Engineer (2005-..... .)

SYS Sesli Yanıt Sistemleri
Danışmanlık Departmanı, Danışman (2004-2005)

Citibank Türkiye A.Ş.
Bilgi İşlem Bölümü, Bilgisayar Ağları Uzmanı (2000-2004)