YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MPLS TEKNOLOJİSİNİN ANALİZİ VE AĞ OMURGALARI ÜZERİNDEKİ UYGULAMALARI

Elektronik ve Haberleşme Mühendisi Kerem EKEN

FBE Elektronik ve Haberleşme Müh. Anabilim Dalı Haberleşme Programında Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı : Yrd. Doç. Dr. N. Özlem Ünverdi
Yrd. Doç. Dr. Soner Özgünel
Prof. Dr. Osman Nuri Uçan

İSTANBUL, 2008

İÇİNDEKİLER

Sayfa

KISALTMA LİSTESİ

ATM : Asynchronous Transfer Mode

BGP : Border Gateway Protocol

COS : Clas

CSR : Cell Swithing Router

FEC : Functional Equivalence Classes

IGP : Interior Gateway Protocol

ISS : Internet Servis Sağlayıcısı

IP : Internet Protocol

LAN : Local Area Network

LDP : Label Distribution Protocol

LSP : Label Switched Path

LSR : Link State Router

MPLS : Multi Protocol Label Switching

OSPF : Open Shortest Path First

QOS : Quality of Service

RSVP : Resource Reservation Protocol

TCP : Transmission Control Protocol

TE : Traffic Engineering

TTL : Time To Live

VC : Virtual Circuit

VPN : Virtual Privite Network

WWW : World Wide Web

ŞEKİL LİSTESİ **Sayfa**

RESİM LİSTESİ **Sayfa**

ÖNSÖZ

Bu çalışmanın hazırlanması sürecinde yol göstericiliğinden ve özellikle gelecekte çok fazla kullanılacak olan bu teknoloji ile daha yakından ilgilenmemi sağlayan ve benden yardımını hiç esirgemeyen sayın tez danışmanım Yrd. Doç.Dr. N.Özlem Ünverdi'ye teşekkürlerimi sunarım.

Çalışmam esnasında bana gerekli donanımı sağlayan Teletek Telekomunikasyon Hizmetleri A.S.' ye ve bana olan desteğinden dolayı arkadaşım Gökhan Gümüş'e teşekkürlerimi sunarım.

Son olarak çalışmalarıma sonsuz katkıları olan aileme ve bütün arkadaşlarıma teşekkür etmek isterim. Onlar olmadan bütün bu çalışmaları yapabilmem mümkün olmazdı.

MPLS TEKNOLOJİSİNİN ANALİZİ VE AĞ OMURGALARI ÜZERİNDEKİ UYGULAMALARI

ÖZET

Veri katmanında yapılan anahtarlama işlemi hızlı olmakla birlikte yönetilebilirlik ve esneklik açısından çok avantajlı değildir. Bu bize büyük ve bir çok yönlendiriciden oluşan ağlarda sorunlar yaratabilir. 3. Katmanda yapılan yönlendirme işlemi ise hızlı olmamakla birlikte esnek ve daha yönetilebilirdir. MPLS teknolojisi bu iki işlemi birleştirerek büyük ağlara hem hızlı hem de esnek bir yönetim imkanı sağlar. Ağın giriş noktalarında yapılan yönlendirme işlemi sırasında veri paketlerine atanan MPLS etiketleri ile ağ içinde bu etiketlere göre hızlı bir şekilde anahtarlama yapılması yeterli olmaktadır.

Bu tez kapsamında ilk bölümde MPLS teknolojisine gelinen noktada, internetin ağlar içindeki gelişimi anlatılmıştır. İkinci bölümde günümüzün ağ teknolojileri ve yönlendirme mantığı anlatılmış ve geniş ölçekli ağların yönetimi üzerinde durulmuştur.. üçüncü ve dördüncü bölümlerde MPLS teknolojisinin çalışma mantığı, paket yapıları, etiket dağıtımı, paketlerin iletimi, ATM omurgalarda yönlendirme işlemleri ve MPLS ile birlikte kullanımı, MPLS' in faydaları konuları incelenmiş ve MPLS' in çalışma mantığı her noktasıyla ortaya konmuştur. Beşinci bölüm olan Uygulama bölümünde ise, dinamik bir yönlendirme protokolü olan OSPF ile çalışan bir ağ, çalışır duruma getirilmiş, bunun üzerinde incelemeler ve analizler yapılmış eksi yönleri ortaya konmuştur. İkinci uygulamada MPLS ile trafik mühendisliği yapılarak ilk uygulamanın eksiklikleri giderilmiş ve analizi yapılmıştır. Son uygulama da ise, günümüzde servis sağlayıcıları için çok kullanışlı olan MPLS VPN üzerinde durulmuş, sistem ağ içinde çalışır duruma getirilmiş ve incelenmesi yapılmıştır.

Anahtar Kelimeler: MPLS, trafik mühendisliği, MPLS VPN

ANALIZING OF MPLS TECHNOLOGY AND APPLICATİONS ON NETWORK ARCHITECTURES

ABSTRACT

Switching, in the Data-link layer is fast but it has no advantage for manageablity and flexibility. It could give us some problems in the networks that have lots of routers. Routing, in the network layer is more manageable and flexible but is not fast. MPLS technology combine these functions and it gives the advantage of fast, manageable and flexible network. During the routing, that starts in the entry of the network MPLS labels are attached to the packets so with these labels it is possible to switch faster.

With this study, in the first chapter, the development of the internet in networks had been defined at the reached point of MPLS technology. İn the second chapter, contemporary network technologies and routing algoritym had been defined and the management of large scaled networks had been accentuated. İn the third and fourth chapter the working algoritym of the MPLS technology, package structures, label allocation, packet transmission, the routing processes in the ATM Networks and the usage of this system with MPLS, the advantages of MPLS had been examined and every single point of the working algoritym of MPLS had been stated. İn the fifth chapter which is the execution section, a network, running with OSPF that is a dynamic routing protocol, had been ran, by doing researches and analysis on it, weak points of the system had been figured. İn the second execution, traffic engineering had been made by means of MPLS and the weak sides of the first execution had been removed. İn the last execution, MPLS VPN system that is so practical for service providers nowadays had been explicated, the system had been made work in a network and the analysis of the system had been made.

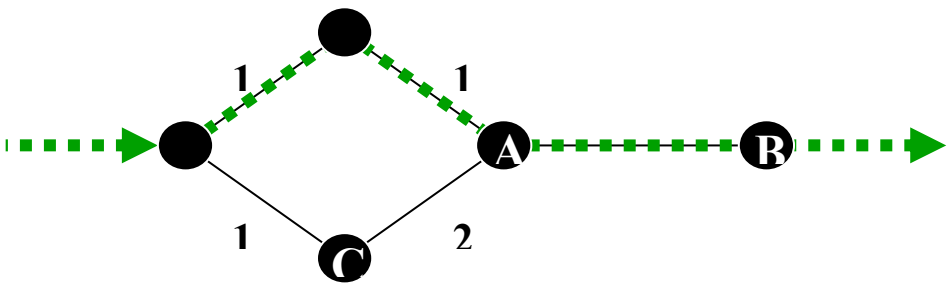
Keywords: MPLS, trafik Engineering, MPLS VPN

1. GİRİŞ

1.1. İnternet Altyapılarının Gelişimi

2. Dünya üzerinde World Wide Web (WWW) yani internetin bir anda geniş bir kullanım alanı bulmasının ardından internet teknolojilerinde önemli ölçüde gelişmeler meydana gelmiştir. Tüm dünyada son birkaç yıl içerisinde yüzbinlerce kurumsal ve milyonlarca bireysel internet kullanıcısı ortaya çıkmıştır. İvmesi sürekli artan kullanıcı sayısı, internetin geniş kitlelere ulaşmasını sağlayan internet altyapısının da aynı ivmeyle artan bir şekilde gelişmesini, hızlanmasını, hizmet kalitesinin ve servis çeşitlerinin artmasını öngörmektedir. Bundan ötürü gerek çok büyük, gerekse küçük çaplı internet servis sağlayıcıları, hem bu hızlı büyümeyi destekleyecek, hem de daha güvenilir ve daha farklılaştırılmış hizmetlerin sağlanması yönünde kullanıcılarından gelen istekleri karşılayacak şekilde kendi altyapılarını sürekli yeni durumlara adapte etmek zorunda kalmaktadırlar.[1]

1990 ların başlarında (global açıdan bakarsak); Internet altyapıları 1,544 Mbps(T1) ve 44.736 Mbps(T3) lardan oluşan kiralık hatlardan ibaretti. İnternetin kullanımında henüz çok yaygınlaşmamış olduğu için, ISP lerin kullandıkları yönlendiriciler ve bu hızdaki linkler müşterilerinin isteklerini karşılamaktaydı. Network yöneticileri trafik akışlarının kontrolünü sağlarken Interior Gateway Protocol (IGP) tabanlı metrikleri kullanıyorlardı ve trafik yoğunluğu çok fazla olmadığı için de bunların kontrolü kolaylıkla sağlanmaktaydı.



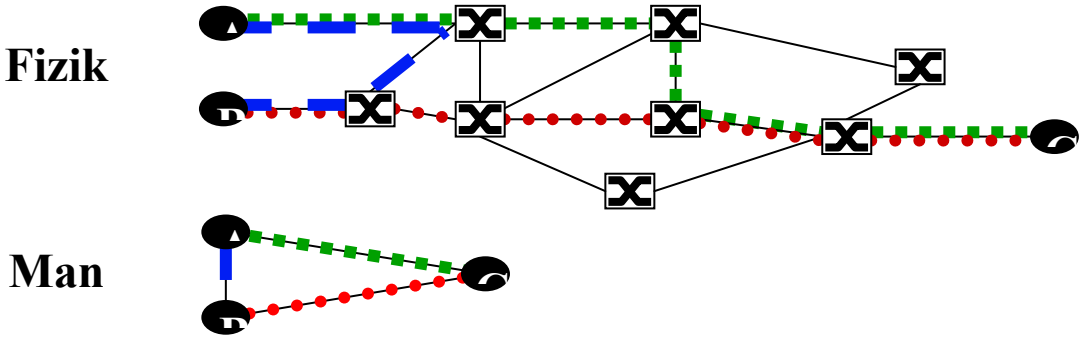
Şekil 1.1 - Yönlendiricilerle oluşturulmuş bir ağın metric değerlerine göre trafik akışı

Şekil 1'deki topoloji de trafik akışı metriklerle kontrol edilmektedir. Şekil 1.1' de görüldüğü üzere; trafik yeşil ile işaretlenmiş olan yolu izleyecektir. Çünkü o yolun metriği daha azdır. Fakat bu durumda şöyle bir problem ortaya çıkmaktadır. Eğer yeşil ile belirtilen yoldaki hatlar, iletilen trafik yoğunluğunu karşılayamaması durumu düşünülmelidir.

IGP tabanlı protokollerin yol seçimi belli bir algoritmaya ve belli değerlere göre uygulandığından ve her yönlendirici kendine göre bir topoloji hesabı yapmasından dolayı ağ içinde belli hatlar şişmeye ve istenileni verememeye başlamıştır.. Ağlar büyümeye devam edip, ağ içindeki bazı hatlar çok yoğun kullanılırken bazıları ise hiç kullanılamamaya başlamıştır.

Ağ yöneticileri bu durumu hatların metrik değerlerini manuel olarak değiştirerek çözme yoluna gitmeye karar vermişlerdir. Yeşil ile belirtilen yolda herhangi bir trafik artışı olması durumunda trafiğin yönünü diğer tarafa alarak çözerler. Fakat görüldüğü gibi bu çok da esnek ve kolay bir yöntem değildir. Özellikle ağdaki yönlendiricilerin artması durumunda bu hiç de kolay bir hal almayacaktır. 1994 ve 1995'e gelindiğinde metrik değerleri ile oynayarak ağın dinamik hale gelemeyeceği anlaşılmış, metrik değerleri ile oynayarak ağın bir tarafındaki sorun çözülürken diğer taraftan başka problemler çıkmaya başlamıştır.

1990 ların sonlarına gelindiğinde; ISP' ler müşteri trafiklerinin artmasından dolayı artık IGP tabanlı metrik ile kontrolü sağlayamamaya başlamışlardır. Daha çok müşteri daha fazla trafik demektir. Doğal olarak var olan interface hızları ise bu trafiği taşımaya yetmemeye başladı. Bu durumda, ISP' ler ağ altyapılarını ATM altyapısına geçirmeye karar verdiler. ATM teknolojisi ile arayüz hızları da OC-3 (155.52 Mbps) den başlayıp OC-12 (622.08 Mbps) lara kadar ulaşmıştır.



Şekil 1.2 - ATM anahtarlardan oluşan bir ağ yapısının fiziksel ve mantıksal görüntüsü

Artık ağlar bir yerden bir yere paket iletimi yaparken IGP metrik hesabı yerine kurulan VC (Sanal devre) leri kullanmaya başladılar. ATM altyapısında uçtaki yönlendiriciler birbirlerine VC ler ile bağlandılar ve ortaya mantıksal bir uçtan uca mesh yapı ortaya çıktı ama fiziksel olarak yönlendiriciler birbirine noktadan noktaya bağlı değil sadece ATM anahtarlar üzerinden yapılan tanımlara göre iletimi sağlamaktaydı. Paketin iletilmesine ve nereden nereye gideceğine, kurulan VC ler karar vermekteydi. Eğer herhangi bir link in trafiği taşıyamaması durumunda backbone larda bulunan ATM anahtarlar yardımıyla aradaki bağlantı başka bir VC yol üzerine taşınır ve bu şekilde iletim sağlanır. Paket iletimi yapılırken tabii ki yine IGP kullanılır fakat burada hatların metriklerini manuel olarak değiştirmek yerine otomatik olarak backbone da bulunan ATM anahtarlar devreye girmiştir.

Aynı zamanda her PVC için ATM üzerindeki trafiği görüntüleme şansı da verir, böylelikle ağ mühendisleri hatta herhangi bir doluluk ve sıkışma gördüğünde mevcut trafiği sanal ağlar üzerinden başka bir hatta aktararak trafiği bölmüş olurlar.

Internetin yaygınlaşması ile birlikte ISP lerin de ihtiyaçları ve kullandıkları teknolojiler artmaya başlamıştır. Bu teknoloji gereksinimi beraberinde MPLS teknolojini de getirmiştir.

MPLS teknolojisi halihazırda kullanılmakta olan, standart varış adresine göre düğümden düğüme aktarma yöntemi yerine etiket değiştirerek – aktarma yöntemini getirmiştir. Bu ise, paket iletimi işlemlerini sadeleştirdiğinden veri iletimini oldukça hızlandırmakta ve ölçeklenebilirliği arttırmaktadır. Üstelik bu teknoloji yönlendirme işlemini, aktarma işleminden ayırdığından, aktarma yolunda hiçbir değişiklik yapmadan, yeni özelleştirilmiş veya değiştirilmiş yönlendirme servisleri uygulanabilir.

MPLS, ağırlıklı olarak piyasada halen kullanılmakta olan ATM gibi yüksek hızlı "etiket – değiştirerek aktarma" teknolojilerinin, var olan yönlendirmeli ağlarla bir arada kullanılmasının gerekliliğinden dolayı ortaya çıkmıştır. Böylelikle IP teknolojisinin datagram yapısı, anahtarların etiket kullanım mekanizmaları ile entegre edilmiş olmaktadır. Bu sayede bağlantı tabanlı bir ağ altyapısının (ATM) üzerinde IP protokolünü yapay olarak kullanmaya çalışmanın getirmiş olduğu sorunların birçoğu çözülmektedir.

1.2. Alt Tanımlar

Çok yeni bir teknoloji olan MPLS konusunun açıklanmasında yine birçoğu yeni olan fazla sayıda terim kullanılmak zorunda kalınmaktadır. Bu sebepten aşağıdaki bölümlerde bu terimlerin açıklamaları yer almaktadır.

1.2.1. Fonksiyonel Denklik Sınıfları

Aynı şekilde işlem gören ve aynı şekilde iletilen IP paketleri grubuna Fonksiyonel Denklik Sınıfı denir. Örneğin aynı yol üzerinden giden paketler bir FEC sınıfı oluştururlar. FEC terimi genelde değişik paketlerin, aynı varış adresine göre gruplandırılmasını ifade etmektedir.

FEC sınıflarının kullanılma nedenlerinin başında paketlerin sınıflandırılması yeralmaktadır. Bu sınıflandırma sayesinde, her paketin ait olduğu FEC sınıfına göre paketin işlenmesine öncelik verilebilir, bazı FEC'lere diğerlerinden daha fazla öncelik verilmesi gerçeklenebilir. Ayrıca bu sınıflar daha verimli servis kalitesinin (QoS) sunulmasını sağlarlar. Örneğin herhangi bir FEC gerçek zamanlı bir ses trafiği olarak

işlenebilirken bir diğeri ise çok daha az öncelikli haber grubu sınıfı olarak işlenebilir. Bir paket ile o paketin ait olduğu FEC sınıfı arasındaki bağı, pakete verilen etiket kurar.

1.2.2. Noktadan Noktaya İletişim

Bir bilgisayar ağında bir tek gönderici ile bir tek alıcı arasında gerçekleştirilen iletişime "Unicast" denir. Bu terim "multicast" teriminin zıt anlamlısı olarak kullanılır. Daha önceleri "Unicast" iletişim yerine "noktadan – noktaya" iletişim kullanılmaktaydı.

1.2.3. Çoklu Yayın

Bir bilgisayar ağında bir tek gönderici ile birden fazla alıcı arasında gerçekleştirilen iletişime "Çoklu Yayın" denir. Gazete ya da dergilerin periyodik güncellenmesi bu tarz bir iletişime örnek olarak verilebilir. Unicast ve anycast gibi multicast iletişim türü de IP Versiyon 6'nın paket türlerinden bir tanesidir.

Çoklu Yayın ayrıca CDPD Mobil Sayısal Veri Paketi'nin bir parçası olan kablosuz veri haberleşmesinde de kullanım alanı bulmaktadır.

Canlı videoları ve sesleri internet üzerinden alan yazılımların yüksek bant genişliği noktalarında çalışmalarını sağlayan bir sistem olan Mbone üzerinde programlar yazılmasında da Çoklu Yayın kullanılır.

1.2.4. RSVP – Kaynak Rezervasyon Protokolü

RSVP, internetteki kanalların veya yolların video, ses ve diğer yüksek band genişliği isteyen mesajların, çoklu yayın olarak iletilmesini sağlamak üzere rezerve edilmesini sağlayan bir protokoldür. RSVP, İnternet Tümleşik Servisler modelinin bir parçasıdır. Bu servis modeli elden gelenin en iyisi servisi, gerçek zaman servisi ve kontrollü bağlantı paylaşmayı düzenlemektedir.

İnternet üzerindeki en temel yönlendirme felsefesi "elden gelenin en iyisi" (best-effort) şeklindedir. Bu felsefede çalışan bir sistemde, sistem tüm kullanıcılara makul bir seviyede hizmet edebilir ancak internet üzerinden sürekli video ve ses verilerinin

iletilmesini bekleyen yazılımlar açısından yeterli hizmeti kullanıcılarına sunamaz. RSVP kullanıldığında ise internet üzerinden belirli bir programı (internet üzerinden yayın yapan bir televizyon programı bile olabilir) isteyen bir kullanıcı, kullandığı yazılımın da yardımı ile internette belirli bir band genişliğini kendine özel olarak rezerve edebilir ve böylelikle alması gereken verileri, normalden daha yüksek hızlarda ve daha güvenilir bir şekilde alabilir. Program başladığında, daha önce yönlendirme önceliği rezervasyonunda bulunan bu kullanıcılara, çoklu yayın yapmaya başlar. RSVP protokolü, noktadan noktaya ve çok – kaynaktan bir hedefe olan iletim türlerini de destekler.

RSVP protokolünün çalışma şeklini daha iyi anlamak için Pazartesi gecesi belirli bir saatte başlayacak olan bir video programını göz önüne alalım. Herhangi bir kullanıcı eğer bu programı izlemek istiyorsa, gerekli band genişliğini ayırmak ve paket gönderme önceliklerinin belirlenmesini sağlamak üzere, yayın başlamadan önce bir RSVP isteği göndermelidir. Bu isteği göndermek için kullanıcının özel bir istemci yazılımına ya da tarayıcısının bulundurduğu bir takım özelliklere ihtiyacı vardır. Bu istek, en yakındaki RSVP sunucusu bulunan bir ağ geçidine iletilir. Burada kullanıcının böyle bir istekte bulunmaya yetkili olup olmadığı ve eğer yetkisi varsa bu isteğin karşılanması durumunda, daha önceki rezervasyonlar için gerekli bant genişliğinin kalıp kalmayacağı araştırılır. Eğer kullanıcının rezervasyon isteği kabul edilmişse bu ağ geçidi, bu rezervasyonu hedefe doğru olan yol üzerindeki diğer ağ geçidine gönderir. Bir sonraki ağ geçidi de aynı araştırmaları yapar ve tüm yol boyunca böyle bir rezervasyonun yapılıp yapılamayacağı belirlenir. Eğer arada bir yerlerde rezervasyon yapılamazsa, daha önceki tüm rezervasyonlar iptal edilir.

Yayın başladığında ise kaynaktan gelen paketler yüksek önceliğe sahip olarak internet üzerinde yol alırlar. Paketler bir ağ geçidine vardığında, bu paketler sınıflanır, ve bir takım kuyruklar bazı durumlarda da zamanlayıcılar kullanılarak aktarılırlar. Bir RSVP paketi çok değişken olabilir. RSVP paketlerinin büyüklüğü, veri tiplerinin ve nesnelerinin sayısı her pakette farklı olabilir. Bu paketler, RSVP protokolünü desteklemeyen ağ geçitlerinden geçmek zorunda kaldıkları durumlarda ise sanki normal paketlermiş gibi ilgili “tünellerden” gönderilirler. RSVP protokolü hem IP sürüm 4 hem de IP sürüm 6 ile çalışabilmektedir.

1.2.5. Yönlendirme

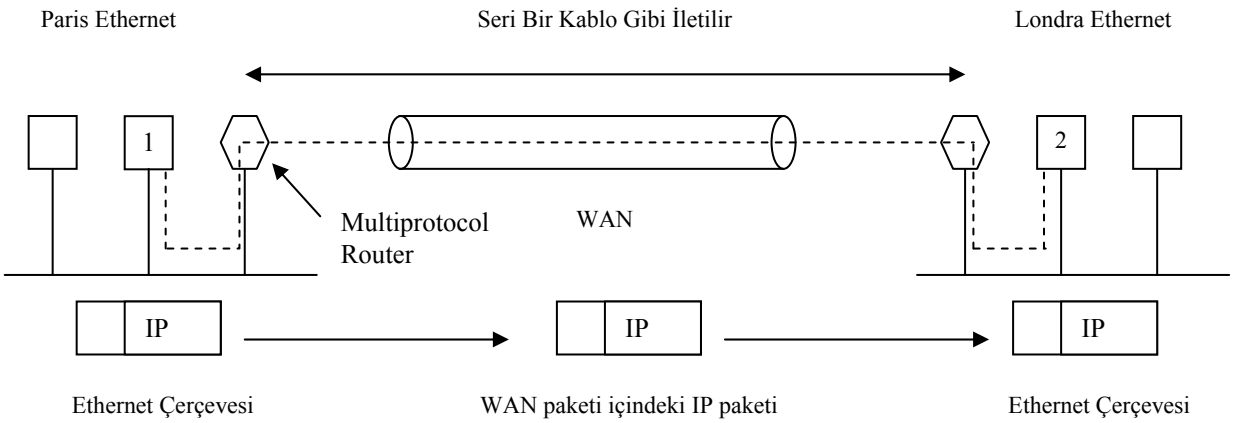
İnternet ağında paketler, kaynak adreslerinden alınıp varış adreslerine kadar yönlendirme işlemine tabi tutularak aktarılırlar. Her yönlendirici kendisine gelen paketin varış adresini ve kendisinin yönlendirme tablosunu inceleyerek paketin iletmesi gereken en yakın yönlendiriciyi belirler. Kısaca yönlendirme işlemi, bir cihazda çalışan yazılım ve bu cihazın belleğinde (genelde RAM'de) saklanan yönlendirme tabloları aracılığı ile gerçeklenen anahtarlama kararlarının verilmesidir. Bu yönlendirme işlemi sırasında genelde baz alınan adres 3. katman adresidir. Günümüzde bu adresler genellikle IP adresi ya da IPX adresi olmaktadır.

1.2.6. Anahtarlama

Anahtarlama işlemi yönlendirmeden farklı olarak çok daha basit, çoğunlukla donanım tarafından, uygulamaya özel tümdevrelerle (ASIC – Application Specific Integrated Circuit) gerçekelenen anahtarlama kararlarıdır. Çoğu kez bu karar verme işleminde kullanılan adres, 2. katman adresi yani 48 bitlik IEEE MAC adresi olmaktadır.

1.2.7. Tünel

İki ayrı bilgisayar ağının, tek bir ağ gibi bir arada çalışmasını şekilde yeni bir yapı kurmak çok zordur. Ancak gene de nispeten çok daha kolay halledilebilen ve sık karşılaşılan bir durum vardır. Bu durum, kaynak ve varış konaklarının aynı tip ağda bulunduğu fakat bu iki nokta aralarında farklı bir başka ağın bulunduğu durumdur. Örnek olarak Şekil 1.3' deki gibi Paris' de ve Londra' da TCP/IP tabanlı Ethernet tabanlı bir şubeleri olan bir uluslararası banka düşünelim. Paris'teki şube ile Londra'daki şube arasındaki bağlantı PTT WAN'la sağlanmakta olsun:



Şekil 1.3 – İki ayrı şehirdeki Ethernet tabanlı ağın bir tünelle tek bir ağ gibi çalışması

Bu sorunun çözümüne "Tünelleme" adı verilmektedir. 1 nolu konak 2 nolu konağa veri göndermek için öncelikle 2 nolu konağın IP adresini içeren paketi, Paris'teki çok protokollü yönlendiricinin adresine gönderdiği bir Ethernet çerçevesinin içine koyar. Çok protokollü yönlendirici bu paketi aldıktan sonra çerçevenin içindeki IP paketini çıkartır ve bunu WAN ağının paketine koyar ve bu paketi Londra'daki çok protokollü yönlendiricinin adresine gönderir. Bu WAN paketi hedefine ulaşınca Londra'daki çok protokollü yönlendirici IP paketini WAN paketi içinden çıkartır ve 2 nolu konağa gidecek olan bir Ethernet çerçevesi içine yerleştirir.

WAN ağı, bizim bankamız açısından iki çok protokollü yönlendirici arasında uzanan büyük bir tünel olarak görülebilir. IP paketi bu tünelin içinde bir uçtan diğerine hareket eder. WAN ağı içerisindeki hiçbir şey ne IP paketini ne de konakları ilgilendirmez. Sadece, çok protokollü yönlendiriciler IP paketlerini ve WAN paketlerini yorumlayabilme yeteneğine sahip olmalıdır. Bir çok protokollü yönlendiriciden diğer çok protokollü yönlendiriciye giden mesafe olduğu gibi seri bağlanmış bir hat gibi davranmaktadır.

2. GÜNÜMÜZÜN GENİŞ ALAN AĞLARI

2.1. Kamusal Ağlardaki Gelişmeler

2.1.1. IP İletişiminin Hızla Yaygınlaşması

IP (Internet Protocol) iletişiminin tarihi, 1970'li yıllarda akademik çevreler tarafından IP'nin kullanılmasıyla başlamaktadır. O zamanlarda paket iletişiminde gerçekleştirilmeye çalışılan en önemli motivasyon, paketlerin doğru olarak kayıpsız bir şekilde iletilmesiydi. Paketlerin belirli bant genişliklerinde iletilmesi ya da gecikme süreleri önemli bir faktör değildi. Her ne kadar IP iletişimi, Servis Tipi (TOS) alanı üzerinden farklılaştırılmış paket iletimi fikrini içermekteyse de bu özellik şimdiye dek etkin bir şekilde kullanılamamıştır. Sonuç olarak IP ağları ve internet, bağlantısız, paket anahtarlamalı bir model kullanılarak inşa edilmiştir ve bu ise verilen servis kalitelerinde farklılaştırılmayı önlemektedir.

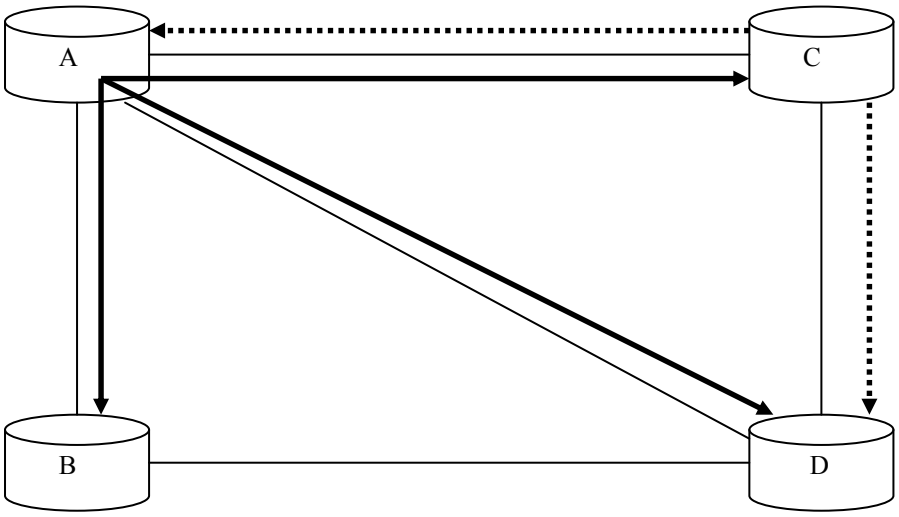
İnternet dünyasının hızla büyümesi ve WWW (World Wide Web) ağının ortaya çıkmasıyla birlikte İnternet Protokolü olan IP, iletişim dünyasının gündeminde baş sıraya gelmiştir. Hem kamusal ağlar, özellikle de İnternet, hem de şirket içi ağlar gibi kurumsal ağlar, IP protokolünü veri paylaşımını sağlamak üzere geniş çapta kullanmışlardır. Günümüzde birçok servis sağlayıcı şirket var olan IP tabanlı altyapılarını müşterilerin istekleri doğrultusunda yeniden kurmak ya da iyileştirmelere gitmek istemektedirler. Ancak sesin, verinin, multimedya uygulamalarının aktarım gereksinimleri, birbirleri ile çok derin ayrılıklar göstermektedir. İnternet Protokolü IP'nin de bu çok farklı isteklere cevap verecek şekilde yavaş yavaş kendini değiştirmesi gerekmektedir.

2.1.2. Yönlendirmenin Rolü

IP paketlerinin başlıklarında bu paketi IP ağı içerisinde doğru yere iletmeye yarayacak yeteri kadar bilgi bulunmaktadır. Paketlerin iletilmesi geleneksel olarak datagram yönlendirme işlemi gerçekleştirilerek yapılır. Datagram yönlendirme tekniğinde paketler varış adreslerine göre iletilirler. Yani herhangi bir IP paketinin ağ içerisinde izleyeceği

yol, her seferinde, paketi ileten yönlendiricinin baktığı paketin başlığındaki varış adresine göre yapılır. IP ağlarında yönlendiricilerin paket iletiminde kullandıkları yöntem düğümden-düğüme yöntemidir. Bu yöntemde paketin ağ içerisinde izleyeceği yol önceden belirlenmemiştir. Paket bir yönlendiriciye girdikten sonra ilgili yönlendirici, paketin varış adresini ve kendi yönlendirme tablolarını inceleyerek paketi ileteceği bir sonraki yönlendiriciyi belirler. Böylelikle paket, ağ içerisinde varış adresine doğru iletilir. Her paket ağ içinde varış adresi doğrultusunda ayrı ayrı yönlendirildiğinden ve paketlerin gidecekleri, daha önce belirlenmiş bir yol bulunmadığından tüm ağ "bağlantısız" olarak kabul edilmektedir. [2]

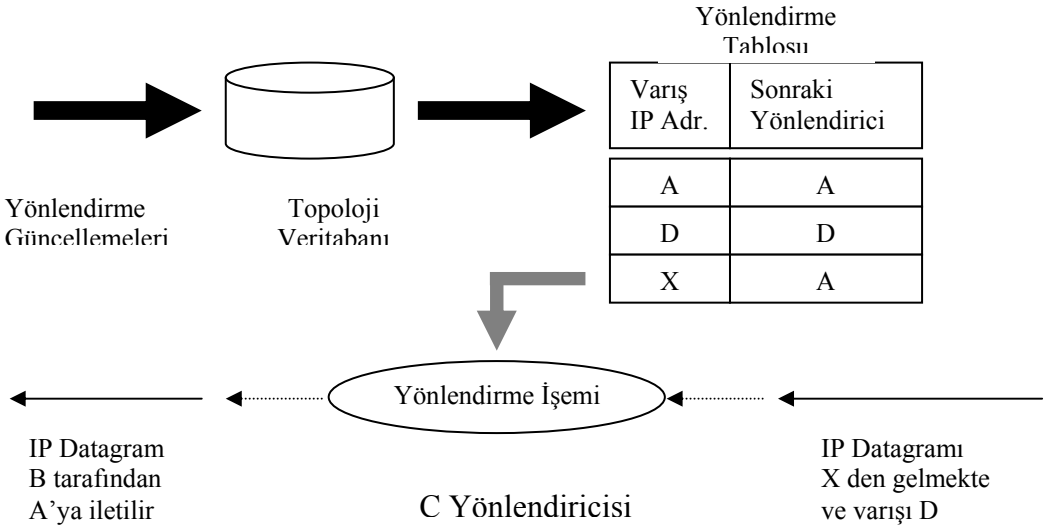
Her yönlendirici, fiziksel olarak doğrudan bağlı olduğu komşu yönlendiriciler ile veri alış-verişi yaparak bir komşuluk ilişkisi kurar. Örneğin şekil 4'de, görüleceği üzere A yönlendiricisinin kendisine doğrudan bağlı üç adet komşusu (B, C, D) vardır. Aynı şekilde C yönlendiricisinin sadece iki tane kendisine doğrudan bağlı komşusu (A ve D) bulunmaktadır.



Şekil 2.1 - Klasik IP yönlendirmesi yapan yönlendiriciler

Bir paketin doğru bir şekilde hedefine iletilebilmesi için yönlendiricilerin, paketin hedef adresi yolundaki bir sonraki yönlendiriciyi belirleyebilmeleri gerekmektedir. "İlk Önce En Kısa Yolu Seç" (OSPF – Open Shortest Path First) gibi bir takım yönlendirme protokolleri yönlendiricilerin bulundukları ağın topolojisini öğrenmesine imkan verir. Bu yönlendirme protokollerinden sağlanan bilgiler ışığında her yönlendirici, bilinen her varış

adresine uygun bir sonraki komşu yönlendiriciyi tutan yönlendirme tabloları hazırlar. Bu tablolarda tutulan IP adresleri tam adresler olmayıp sadece ilgili alt ağı adresleyen IP adresinin baş kısmıdır, önekidir (prefix). Yönlendirme tablolarının oluşturulması ile paketlerin bu tablolar yardımıyla iletilmesi her ne kadar birbiriyle yakından ilişkili ise de bunlar iki ayrı fonksiyonu yerine getirirler. Daha önceleri her iki fonksiyon da tamamen yazılımla yapılırken günümüzde aktarma fonksiyonları daha çok donanım tarafından gerçeklenmektedir ancak yönlendirme/kontrol fonksiyonları ise halen yazılım ile yapılmaktadır. Şekil 2.2' de bu gösterilmiştir.



Şekil 2.2 - Klasik IP yönlendirme adımları

2.1.3. Anahtarlamanın Rolü

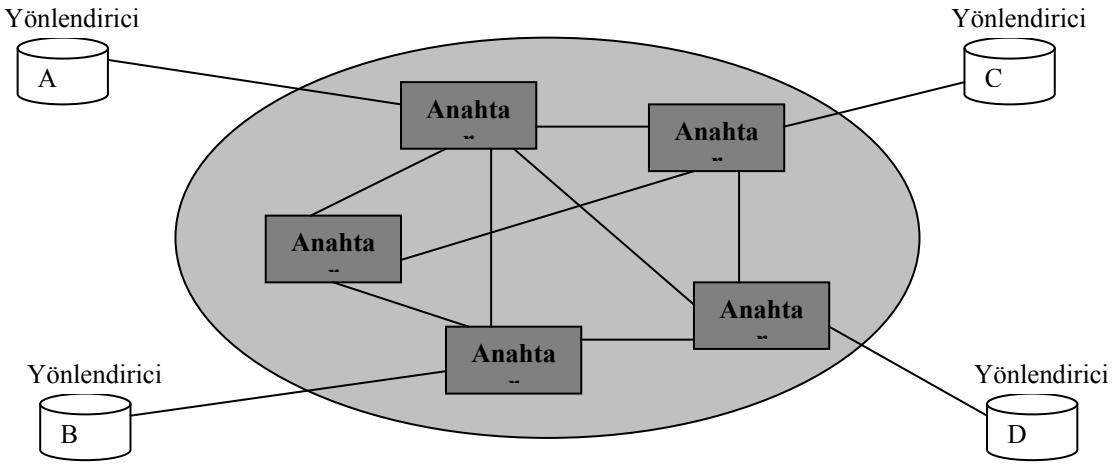
Servis sağlayıcılar ve internet altyapısı kuran şirketler, daha büyük IP ağları kurmaya başladıkça yönlendirici tabanlı ağları kurmada bir takım sorunların olduğunu gördüler. Bu sorunların başında büyük ölçüde IP yönlendiricilerinin maliyeti yüksek yazılım tabanlı yönlendirme bileşenleri yer almaktaydı. Ayrıca klasik yönlendirme protokollerinin kullanıldığı çok dallara ayrılmış bir ağda, ağın performansının önceden belirlenmesinde ortaya çıkan güçlük ise bir başka büyük sorundu.

Oysa ATM ve Frame Relay gibi anahtarlama temelli teknolojiler, etiket değiştirerek aktarma gibi çok daha değişik bir aktarım algoritması kullanmaktaydı. Bu teknolojilerin aktarım algoritması çok basit olduğundan ve genelde tamamen donanım ile

gerçeklenebildiğinden, geleneksel IP yönlendirme ile karşılaştırıldığında daha iyi fiyat/performans oranı sunmaktaydı. ATM ve Frame Relay teknolojileri "bağlantı tabanlı" temelli sistemlerdir yani iletişim yapacak iki uç arasında önce bağlantı kurulur ve artık iki uç arasında gidecek paketler daha önce belirlenmiş bu bağlantı üzerinden iletilirler. Haberleşme sırasında tüm paketlerin daha önce belirlenmiş yollardan varış adreslerine gitmesi, ağın performansının daha kolay tahmin edilebilmesine ve daha kolay yönetilebilmesine olanak vermektedir. Bu iki özellik ise çok büyük ölçekli ağların çekirdek altyapısının niye anahtarlama elemanları kullanılarak inşa edildiğini açıklamaktadır.

2.1.4. Anahtarlama ve Yönlendirme Mekanizmalarının Birleştirilmesi

Büyük ölçekli ağların çekirdek altyapısında anahtarlama temelli teknolojiler geniş çapta kullanılırken bu ağların uç noktalarında ise yönlendiricilerin kullanılması daha yaygındır. Bu iki apayrı teknolojinin bir arada kullanılmasının gereği olarak, IP teknolojisinin çekirdek teknolojisi olan ATM ya da Frame Relay teknolojisinin üstünde kullanılmasıyla karma ağlar ortaya çıkmıştır. Bu mantık Şekil 2.3' de gösterilmiştir.



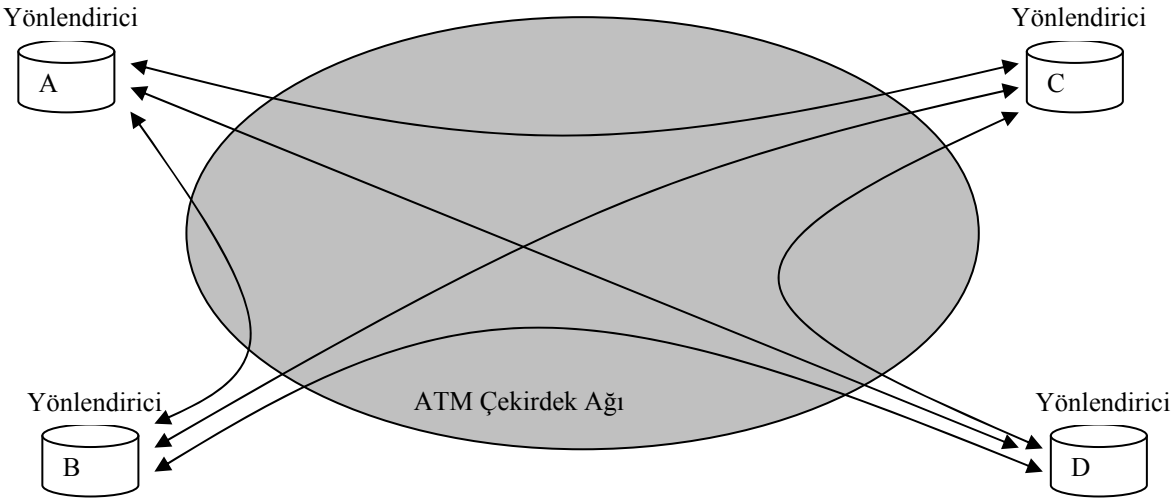
Şekil 2.3 – ATM üzerinden IP Modeli (IP over ATM – Overlay Model)

Bu karma model, anahtarlama teknolojisinin bir takım faydalarını tüm ağ çapına yaymaktadır. Örneğin böyle bir ağda yönlendiriciler arasındaki yollar anahtarlardan geçtiğinden ve bu anahtarlar da iletişim için bağlantı kurulmasına ihtiyaç

duyduklarından, ağın performansının daha kolay ve daha iyi öngörülebilmesini ve ağın daha kolay yönetilebilmesini sağlar.

Böyle bir karma modelinin kurulması ağın yönlendirme kısımlarındaki işlemleri önemli ölçüde etkiler. Bir IP ağı, ATM gibi anahtarlamalı bir ağ üzerine kurulduğu zaman, ağ katmanı açısından tüm yönlendiriciler sanki birbirleriyle bağlıymış gibi gözükmektedir. Bu da bu modelde her yönlendiricinin diğer tüm yönlendiricilerle komşu olduğunu göstermektedir. Yönlendiriciler arası bağlar artık sanal devreler ile sağlandığından (örneğin ATM'de VC Virtual Circuit), çekirdek ağda tüm yönlendiricileri birbirine bağlamak için tüm VC'ler kullanılmalıdır. Yönlendirici sayısı arttıkça kullanılması gerekecek VC sayısı n(n-1)/2 oranında artacaktır. Bu soruna genelde "n^2" sorunu denilmektedir. Sonuç olarak çok fazla sayıda VC bulunduran bir ağın yönetilebilirliği hem çok azalmaktadır hem de ölçeklemede sorunlar yaşanmaktadır.

Şekil 2.4' de görülen örtülü ağ dört yönlendiriciden ve bunları birbirine bağlamak için gereken 6 VC sanal devreden oluşmuştur. Ancak beşinci bir yönlendirici eklendiği zaman gerekli olacak sanal devre VC sayısı 10'a çıkmaktadır. Ağ büyüdükçe ve yönlendiricileri sayısı arttıkça, ihtiyaç duyulan sanal devre VC sayısı üstel olarak artmakta ve bu da tüm ağın ölçeklenebilirliğini çok sınırlamaktadır.



Şekil 2.4 – ATM üzerinden IP'de kurulması gereken sanal devreler (VC)

2.2. Geniş Ölçekli Bilgisayar Ağlarının Yönetimi

Geçmiş 100 senede telekomünikasyon alanında yaşanan hızlı değişim neticesinde, günümüz haberleşme altyapısının zaman bakımından % 99,999 oranında çalışması istenmektedir. Bu ise her yıl sadece 5 dakikalık bir "çalışamama" durumu demektir. Bu zor gereksinimi sağlayabilen ekipmanlara "taşıyıcı-sınıf" denilmektedir. Böyle bir cihazın sağlaması gereken özellikler birkaç tanedir ve ağ ekonomisinin hesaplanmasında, servis sağlayıcıların hedeflerine ulaşabilmesinde, ve zengin servis çeşitlerinin sağlanabilmesinde anahtar özelliklerdir.

2.2.1. Ölçeklenebilirlik

Çok sayıda ve değişik çeşitlerde uygulamalar çalıştırabilen PC'lerin kullanımının hızla artmasıyla birlikte bant genişliği gereksinimleri de aynı hızla artmıştır. Günümüzde ise modern bilgisayar ağları neredeyse sonsuz kapasitede ölçeklenmelidirler. Şu anda kullanılmakta olan ATM/Frame Relay Üzerinden IP ağlarının, "karma model"in, teknik açıdan, IP yönlendirme protokollerindeki etkileri açısından, çok fazla sayıdaki sanal devrenin (VC) yönetiminin getirdiği ağ yönetimi açısından birçok sınırlamaları vardır.

2.2.2. Dayanıklılık

Şu anda kullanılmakta olan telefon şebekesinin (PSTN – Public Switched Telephone Network) en önemli özelliği güvenilir olmasıdır. Bu şebekeyi kullanan tüm aboneler ahizeyi kaldırdıklarında bir çevir sesi duyacaklarından emindirler. Oysa günümüzde kullanılan veri haberleşme ağlarının aynı seviyede bir performansı yakalayabilmesi için çok geniş çapta iyileştirmeler gerekmektedir.

2.2.3. İleriye Dönük Uyumluluk

Servis sağlayıcıları genellikle özel servis hizmeti isteklerini karşılamak üzere özelleştirilmiş ağları devreye sokarak müşterilerine yeni bir takım özellikler sunarlar. Maliyetleri düşürme, toplam performansı arttırma ve halen verilmekte olan servislere ek olarak yeni yeni hizmet türlerinin kullanıcılara sunulması için ortaya çıkan rekabet ortamı

mevcuttur. Ancak ortak olan fikirlerden birisi de paket tabanlı ağların, özellikle de IP ağlarının, uçtan-uca haberleşme konusunda, yukarıda değinilen özellikleri sağlamak bakımından en uygun yöntem olduğudur. Fakat IP ağları genelde elden gelenin en iyisi mekanizmasının yeterli olduğu veri haberleşmesi durumlarda kullanılmaktadır. Ses, görüntü gibi çok daha farklı verilerin iletilmesinde IP ağlarının da IP paketlerinin yönlendirilmesi ve taşınması alanlarında büyük ölçekli değişikliklere ihtiyaç duyulmaktadır.

3. ÇOK PROTOKOLLÜ ANAHTARLAMA TEKNOLOJİSİNİN TEMELLERİ

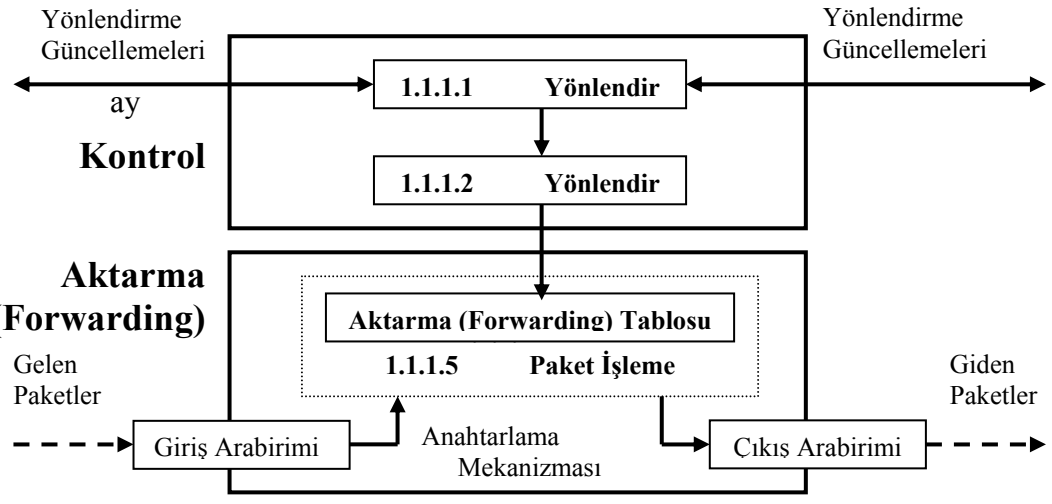
3.1. Yönlendiricilerde Temel Yapı Blokları

İnternette yeni yeni kullanılmaya başlanan çok protokollü anahtarlama teknolojisinin incelenmesine başlamadan önce piyasada bulunan tüm çözümlerinde ve MPLS teknolojisinde ortak olan temel yapı bloklarının incelenmesi yerinde olacaktır. Bu ortak yapı blokları şunlardır:

- Kontrol ve Aktarma Bileşenleri
- Etiket – Değiştirerek ve Aktarma Algoritmaları

3.1.1. Kontrol ve Aktarma Blokları

MPLS teknolojisinin de içinde olduğu tüm çok protokollü anahtarlama çözümleri, fonksiyon olarak ayrı işleri gören iki bileşenin birleşmesinden oluşmuştur: kontrol bileşeni ve aktarma bileşeni.



Şekil 3.1 – Bir yönlendiricinin temel yapı blokları

Kontrol bileşeni, yönlendirme tablosunu oluşturmak ve güncellemek için diğer yönlendiricilerle sürekli bilgi alış-verişi yapan standart yönlendirme protokollerini (OSPF, IS-IS ve BGP-4) kullanır. Paket geldiğinde aktarma bileşeni, kontrol bileşeni tarafından hazırlanan yönlendirme tablosunu arar ve her paket için bir yönlendirme kararı verir. Aktarım bileşeni, özellikle gelen paketin başlığında ki bilgiyi inceler, yönlendirme tablosunda uygun bir kayıt arar ve paketi geldiği arabirimden belirlediği çıkış arabirimine kendi anahtarlama mekanizması üzerinden iletir. Bir yönlendircinin temel yapı blokları Şekil 3.1' de gösterilmiştir.

Kontrol bileşeni ile aktarma bileşeninin birbirlerinden tamamıyla ayrılması sonucunda her bir bileşen diğerinden bağımsız olarak tasarlanabilir ve geliştirilebilir hale gelmiştir. Yapılması gereken tek şey paket yönlendirme tablosunun güncellenmesi için kontrol bileşeninin aktarma bileşeni ile sürekli haberleşmesini sağlamaktır. [3]

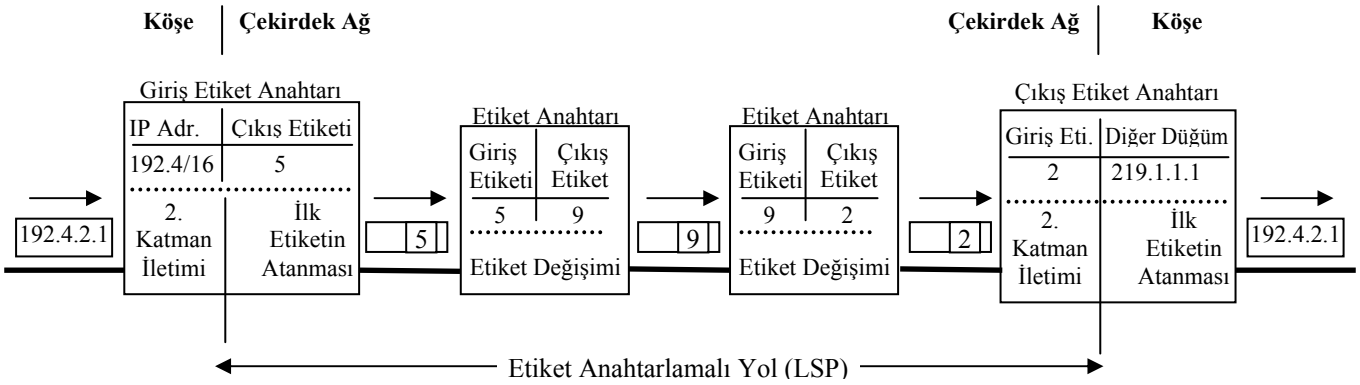
3.1.2. Etiket Değiştirerek Aktarma Algoritmaları

Tüm çok katmanlı anahtarlama çözümlerinin ve MPLS teknolojisinin aktarma bileşeni "etiket değiştirerek aktarma" algoritmasını kullanmaktadır. Bu algoritma ATM ve Frame Relay anahtarlarında kullanılan aktarma algoritmasıyla aynıdır. Bu algoritmada en önemli nokta mesajlaşma ve etiket dağıtımıdır.

Etiket, iletilen paketin başlığında yer alan ve paketin hangi Fonksiyonel Denklik Sınıfına (FEC'e) ait olduğu bilgisini taşıyan sabit uzunluklu kısa bir değerdir. Bu etiket ATM'de kullanılan VPI/VCI (Virtual Path ID/Virtual Circuit Identifier) veya Frame Relay teknolojisinde kullanılan DLCI (Data Link Connection Identifier) bağlantı belirteçleri ile aynı görevi üstlenmektedir, çünkü etiket değerleri bağlantıya özeldir ve yöreseldir. Fonksiyonel Denklik Sınıfı daha önce de belirtildiği üzere ağ üzerinde, son varış adresleri ayrı olsa dahi aynı yoldan iletilen paketler kümesidir. Örnek olarak klasik en fazla uyan IP yönlendirmesinde, varış adresleri, belirli bir IP adresinin başlangıcına uyan, noktadan-noktaya giden paketler bir FEC oluşturmaktadırlar.

"Etiket-değiştirerek aktarma" algoritması her pakete, ağa girdiği noktadaki giriş yönlendiricisi tarafından bir ilk etiket atanmasını gerektirir. Şekil 3.2' de de görüleceği

gibi giriş yönlendiricisi henüz ağa girmemiş varış adresi 192.4.2.1 olan etiketsiz bir paketi almaktadır. Etiket anahtarı yönlendirme tablosuna bakarak en fazla uyan kaydı arar ve paketi 192.4/16 FEC'ine atar. Giriş yönlendiricisi daha sonra bu pakete bir etiket değeri (burada 5) atayarak etiket anahtarlamalı yol üzerinde sıradaki yönlendiriciye iletir.



Şekil 3.2 – Çok protokollü anahtarlama teknolojisinde paket iletimi

Etiket anahtarlamalı bir yol (LSP) fonksiyonel olarak sanal devrelere benzer çünkü belirli bir FEC'e dahil olan tüm paketlerin ağ içinde giriş yönlendiricisinden çıkış yönlendiricisine doğru gidebileceği bir yol tanımlar. LSP üzerindek ilk etiket anahtarı "**giriş etiket anahtarı**" olarak adlandırılır. Aynı şekilde LSP üzerindeki son etiket anahtarı ise "**çıkış etiket anahtarı**" olarak adlandırılır.

Çekirdek ağ içerisindeki etiket anahtarları paketlerin ağ katmanı başlıklarını es geçer, yalnızca etiket değiştirerek paketleri aktarırlar. Bir anahtara herhangi bir etiketli paket geldiği zaman aktarma, bileşeni paketin geldiği port numarasını ve paketin etiketini baz alarak kendi aktarma tablosunda tam uyumlu satırı arar. Uygun bir kayıt bulduğu zaman aktarım bileşeni tablodan çıkış için kullanılacak olan etiket değerini, çıkış port numarasını ve diğer düğümün adresini alır. Daha sonra aktarma bileşeni, gelen etiketi yeni tablodan aldığı etiketle değiştirir ve LSP üzerindeki bir sonraki düğüme iletilmek üzere çıkış arabirimine gönderir.

Çıkış etiket anahtarına bir etiketlenmiş paket ulaştığı zaman, iletim bileşeni kendi iletim tablosunu inceler. Eğer bulduğu bir sonraki düğüm bir etiket anahtarı değilse, çıkış etiket

anahtarı paketin etiketini göz ardı ederek paketi geleneksel en fazla uyan IP iletim mekanizması ile iletir.

Etiket değiştirip iletme işlemi, geleneksel düğümden düğüme ağ katmanı yönlendirmesi ile kıyaslandığı zaman bir çok avantaja sahiptir:

- Paketlerin değişik FEC'lere atanabilmesi işlemi servis sağlayıcılara çok büyük bir esneklik sağlamıştır. Örneğin klasik IP yönlendirmesine benzer olarak giriş etiket anahtarı, paketleri varış adreslerine göre fonksiyonel denklik sınıflarına (FEC) sokabilir. İlave olarak paketler çok değişik kriterlere göre, sadece paketin kaynak adresine göre, paketleri gönderen - alan uygulama tipine göre, etiket anahtarlamalı ağa giriş noktasına göre, etiket anahtarlamalı ağdan çıkış noktasına göre, paketin başlığında taşınan servis sınıfı CoS (Class of Service) alanına göre veya bunların herhangi bir kombinasyonuna göre gibi

- Servis sağlayıcı firmalar özel amaçlı uygulamaları desteklemek için özel olarak belirlenmiş etiket anahtarlamalı yollar (LSP) kurabilirler. Bu yollar, (LSP'ler) düğüm sayısını en aza indirecek şekilde, bazı bant genişliklerini kesin olarak sağlayacak şekilde, zorunlu bazı performans gereksinimlerini verecek şekilde, potansiyel yığılma düğümlerini kullanmayacak şekilde, paketleri IGP tarafından belirlenen yoldan başka bir yol üzerinden geçirecek şekilde ya da paket trafiği ağdaki belirli bazı düğümlerden geçecek şekilde ve benzeri birçok kriteri sağlayacak üzere tasarlanabilirler.

- Etiket değiştirip aktarma algoritmasının en belirgin ve önemli yararı ise herhangi bir tipten kullanıcı trafiğini alıp, bunu bir FEC'e atayıp bu FEC'i de bu sınıfın gereksinimlerini karşılayacak şekilde özel olarak tasarlanmış olan bir etiket anahtarlamalı yola (LSP'ye) bağlayabilme yeteneğidir. Etiket değiştirerek aktarma algoritmasını kullanan yeni teknolojilerin piyasaya çıkması ile beraber internet servis sağlayıcıları kendi ağları üzerinden akan trafik üzerinde kesin bir kontrol sağlayabilmişlerdir. Bu daha önce görülmemiş seviyede kontrol yeteneği, daha verimli ve performansı önceden daha iyi tahmin edilebilir bir ağ kullanımını mümkün kılmıştır.

3.2. Etiket Dağıtımı ve Paketlerin İletimi

MPLS ağında bulunun etiket anahtarlamalı yönlendiriciler, (LSR) basitliği ve hızı daha fazla olan veri bağı katmanı aktarmasını kullanırlar. Normal ağ katmanı aktarımı ise paketleri iletmek için büyük paket başlıklarının incelenmesini ve "en fazla uyan" algoritmasının yürütülerek en uygun düğümün bulunmasını gerektirir. Ancak etiket - değiştirerek aktarma paket iletimi çok daha basit olan etiket eşleştirmesine dayanmaktadır. Bu ise paketlerin çok daha hızlı ve basit bir şekilde iletilmesini sağlar.

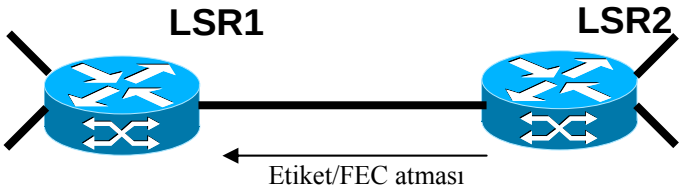
Ağ katmanı yönlendirme protokolü, paketlerin iletim kararlarını almak üzere kullanacağı bilgileri sık kullanılan OSPF, BGP gibi yönlendirme protokollerinden sağlar. Bu yönlendirme bilgileri, tüm aktarım uzayını parçalara böler ve her parçaya da daha önce değinilen Fonksiyonel Denklik Sınıfı (FEC) adı verilir. Aynı yolu izleyen ya da belirli bir FEC'e ait olan paket kümelerine "akış" adı verilir ve aynı şekilde iletilirler. Her FEC'e ise kısa, sabit uzunluklu, lokal olarak anlamlı belirleyiciler, etiketler atanır. Bir paket ya veri bağı katmanının başlığında ya da ağ katmanının başlığında uygun bir yere etiket değeri yerleştirilerek etiketlenir. Eğer her iki katmanda da etiket değerinin yazılabileceği bir alan bulunmuyorsa pakete bu işe özel bir başlık yerleştirilir.

Yönlendirme protokollerinden elde edilen bilgiler, etiketleri MPLS eşleri arasında atamak ve dağıtmak için kullanılır. Yaygın olarak bir MPLS düğümü, herhangi bir akış için bir sonraki düğüm olan yönlendiriciden "giden" etiket atamalarını alır. Kendisi ise "gelen" paketler için etiket değeri tahsis eder ve bunları belirli bir akış için kendisinden önce gelen düğümlere dağıtır. Bu etiketler tüm ağ boyunca, her MPLS düğümü giriş etiketine karşı bir çıkış etiketi eşleyinceye dek iletilir. Bu işlem sonucunda birbirini peşi sıra takip eden etiketlerin oluşturduğu yol "etiket anahtarlamalı yol" olarak adlandırılır.

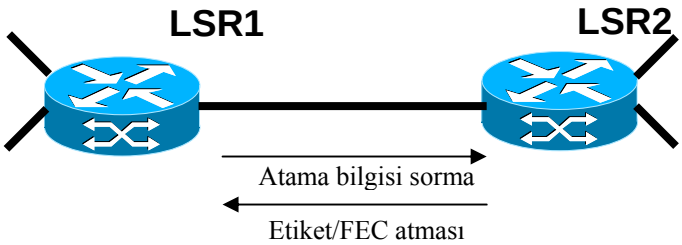
Noktadan - noktaya aktarım için etiket dağıtımı Etiket Dağıtım Protokolü ile yapılmaktadır. MPLS komşuları LDP'nin dağıtımı ve etiketi geri çekme prosedürlerini değiş tokuş etmek için bir LDP komşuluğu oturumu oluştururlar. LDP protokolü ise iki tür etiket dağıtım şeklini desteklemektedir: Bağımsız ve düzenli. Bağımsız etiket dağıtımı protokolünde her düğüm, herhangi bir "akış" algıladığı zaman, herhangi bir anda bu akışa atadığı etiketi dağıtabilmektedir. Düzenli etiket dağıtımı protokolünde ise belirli bir

akış için “çıkış” olan düğüm tarafından bu akışa ait etiket dağıtımı başlatılır. Yani herhangi bir düğümün kendi “giriş” etiketini diğerlerine dağıtmaya başlayabilmesi için ya bu düğümün, ilgili akışın çıkış düğümü olması gerekir ya da bu akışa ait bir “çıkış” etiketine sahip olması gerekmektedir. Düzenli etiket dağıtımı protokolü, etiket – akış eşleştirilmelerinin daha tutarlı bir şekilde yapılmasını garanti eder ve etiketlenmemiş paketlerin sonraki düğümlere iletilmemesi olasılığını arttırır.

MPLS içinde etiket tahsisleri akışın yönünde bir sonraki, aşağı-akış, düğüm tarafından yapılmaktadır. Etiket tahsisinde de etiket dağıtımındaki gibi iki yöntem vardır: aşağı-akış ve istek-üzerine-aşağı-akış. Aşağı-akış etiket tahsisi yönteminde akış yönünde bir sonraki düğüm tarafından etiket tahsisi yapılır ve bu etiket değerleri komşu düğümlere, komşu LSR’a, dağıtılır (Şekil 3.3) . İstek-üzerine-aşağı-akış etiket tahsisi yönteminde ise akış yönünün yukarısındaki bir düğüm (LSR) tarafından akış yönünün aşağısındaki bir düğümden o akışa ait etiket atamasının yapılması özellikle istenebilir (Şekil 3.4). Bu yöntem, etiket anahtarlamalı yolları (LSPs) birleştirilmesinin mümkün olmadığı ATM ağlarında çok kullanışlıdır. LSP birleştirmelerinden ise Bölüm 4’de ayrıntılı olarak bahsedilecektir.



Şekil 3.3 - Aşağı-akış etiket/FEC ataması



Şekil 3.4 - İstek-üzerine-aşağı-akış etiket/FEC ataması

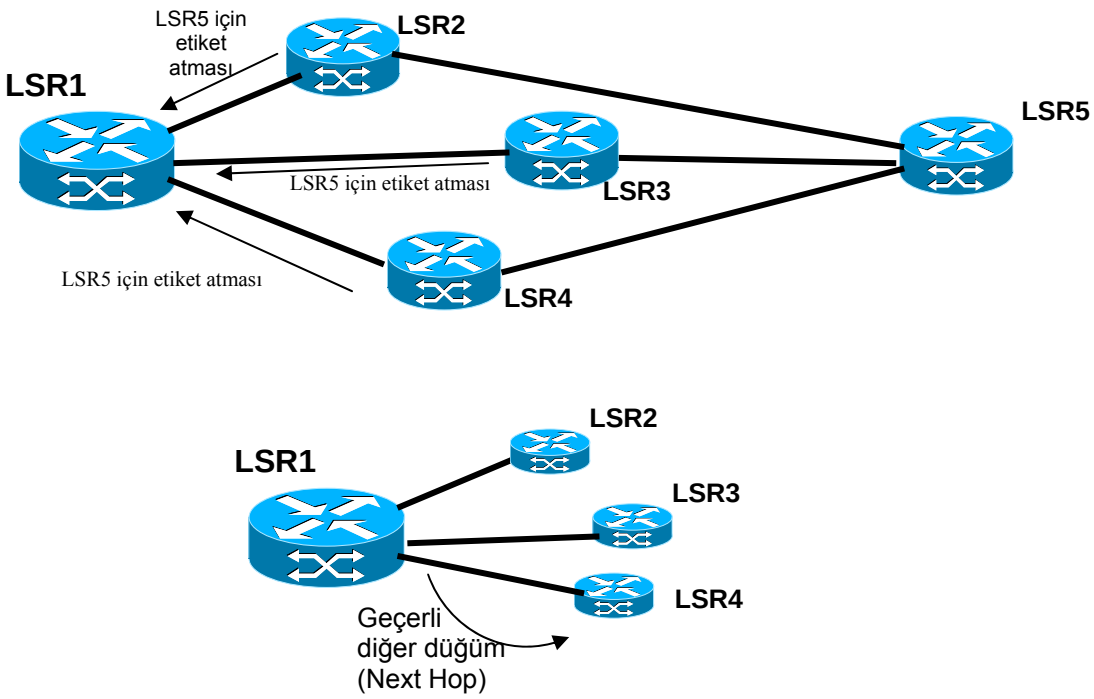
Etiket ataması ve dağıtımı konusunda başka bir noktada belirli bir anda kullanılmayacak olan etiketlerin saklanıp saklanmayacağı konusudur. Bir LSR Ru düğümü, Rd düğümünden belirli bir FEC’ ine ait bir etiket ataması bilgisi almış olsun. Ancak Rd düğümü, bu akış açısından Ru’nun bir sonraki düğümü olmasın. Bu durumda LSR

Ru'nun yapabileceği iki seçenek vardır; ya bu tarz atama bilgilerini gözardı edecektir ya da bu bilgileri ileride kullanmak üzere saklayacaktır. Eğer LSR bu bilgiyi saklarsa, ileride herhangi bir anda Rd düğümü bu akış için Ru'nun sonraki düğümü haline geçerse anında sakladığı bu bilgiyi kullanarak iletime başlayabilir. Eğer LSR Ru bu bilgiyi saklamayıp gözardı ederse ve daha sonraki bir anda Rd düğümü akış için sonraki düğüm olursa, saklamadığı bu etiket ataması bilgisini tekrar elde etmek zorunda kalacaktır.

Eğer LSR "Gereksiz Etiket Bilgilerini Saklama Modu"'nu destekliyorsa bu tarz o anda kullanmadığı etiket atamaları bilgilerini saklar.

Eğer LSR "Gereksiz Etiket Bilgilerini Atma Modu"'nda çalışıyorsa o anda kullanamayacağı etiket atamaları ilgilerini gözardı eder.

"Gereksiz Etiket Bilgilerini Saklama Modu" yönlendirmede meydana gelecek değişikliklere çok daha çabuk adapte olmayı sağlar. "Gereksiz Etiket Atamalarını Atma Modu" ise LSR cihazının çok daha az tablo ile işlem yapmasını sağlayarak işlem yükünü hafifletir.



Şekil 3.5 – Gereksiz Etiket Bilgilerini İşleme Modları

3.3. Etiket Verme Kriterleri

MPLS teknolojisinin en büyük özelliklerinden bir tanesi de bir ya da daha fazla akışa bir etiket değeri atanabilmesidir. Bu akış çok yoğun bir veri iletimi de gerektirebilir, nispeten daha az bir trafik de gerektirebilir. Etiket paylaşımı, kaynakların dikkatli kullanımını sağlayarak anahtarlamanın faydalarından en yüksek oranda yararlanman isteğinden dolayı ortaya çıkmıştır. Etiket verme kriterleri çok çeşitli olabilmektedir:[4]

- **IP Önekine Göre**

Bu kritere göre etiketler varış adresinin önekine (prefix) göre verilir. Bu uygulamanın iyi tarafı, "Gereksiz Etiket Bilgilerini Saklama Modu" ile birlikte değerlendirildiği zaman, etiket atamalarının sadece bir kez ya düğüm eşleşmeleri aşamasında (peering phase) ya da bir adres öneki öğrenildiği zaman yapılmasıdır. Bu yöntem LDP mesajlaşmalarını minimum seviyeye indirmektedir. Ancak bu tarz bir etiket verme kriteri, düşük etiket uzayına sahip etiket anahtarlama yönlendiricilerinden (LSR) oluşmuş büyük ağlar için ölçeklenebilirlik sorunları doğurmaktadır.

- **Çıkış Yönlendiricisine Göre**

Bu yöntem, MPLS ağını aynı yönlendiriciden terk eden akışların ortak bir etiketi yani ortak bir etiket anahtarlamalı yolu (LSP) paylaşması anlamına gelmektedir. Herhangi bir LSR'ın, hangi akışlar için çıkış yönlendiricisi olduğu bilgisi, (BGP açısından) sonraki düğümünün gönderdiği BGP güncelleme mesajından veya OSPF yayımının içindeki yönlendirici numarasından (OSPF Router ID) anlaşılabilir.

- **Uygulama Akışına Göre**

Bu yöntemde uygulama akışı kendi yolunu belirler. Bu, bütün kriterler içerisinde en az ölçeklenebilirliğe sahip olan kriterdir. Bu yöntemin avantajı ise uçtan-uca anahtarlamayı sağlamasıdır.

4. MPLS TEKNOLOJİSİ

4.1. IP Anahtarlamanın Ortaya Çıkışı

Çok protokollü anahtarlama terimi 2. katmanda yapılan anahtarlama ile 3. katmanda gerçeklenen yönlendirme işlerinin entegre edilmesi anlamına gelmektedir. Günümüzde birçok internet servis sağlayıcı (ISS) altyapısı, 2. katmanda gerçeklenen anahtarlama teknolojisinden (ATM, Frame Relay vb.) bağımsız olarak, bu teknolojilerin üzerinden IP yönlendirmesi yapacak şekilde kurulmuştur. 2. katmandaki anahtarlama mekanizması, iletişimin yüksek hızlara çıkmasını sağlarken, ağ sınırlarındaki IP yönlendiricileri (bu yönlendiriciler birbirlerine 2. katmandaki sanal devrelerle – Virtual Circuits - bağlanmışlardır) sayesinde IP datagramlarının daha akıllı bir şekilde iletilmesine olanak verilmektedir. Bu yaklaşımın en zor tarafı ise tamamen farklı yapıda olan ve farklı topolojileri, adres uzayları, yönlendirme protokolleri, mesajlaşma protokolleri, kaynak ayırma düzeneklerine sahip olan bu iki teknolojinin birarada kullanılmasının getirdiği karmaşıklıktır. Çok katmanlı anahtarlama ve MPLS teknolojileri ise 2. katman ve 3. katman aktarma teknolojilerini bir arada kullanma çabalarının oluşturduğu karmaşıklıkları azaltmak amacıyla tasarlanmıştır.

4.2. İnternet Servis Sağlayıcıların ATM Üzerinden IP (IP Over ATM) Çözümüne Geçişi

1990'lı yılların ortalarında bazı internet servis sağlayıcıları (ISS) ATM üzerinden IP kullanımına yönelmişlerdir. ISS'lerin bu teknolojiye geçiş nedenleri arasında daha geniş bant genişliklerine duydukları ihtiyaç, belirleyici iletim performansı ve ağlarında sürekli artan talep patlamasını karşılayacak şekilde trafik yönetimi yapabilme istekleridir. ATM üzerinden IP (IP Over ATM) modeli ise etiket kullanma özelliği sayesinde bu özellikleri sağlamaktaydı.

Bu model, tamamen ATM üzerine odaklanmıştır ve ağdaki her cihazın ATM mesajlaşma yazılımlarına ve etiket-değiştirip gönderme algoritmasını yürütebilecek donanıma sahip olmasını gerektirmektedir. ATM üzerinden IP modelinde yönlendirme işleri sadece ağın sınırlarında yer alan yönlendiriciler ile yapılmaktadır, çekirdek ağda ise yüksek hızı tesis etmek için etiket değiştirme algoritmasını yürüten ATM anahtarlarına ve PVC'lere

(Permanent Virtual Circuit) güvenilmekteydi. Yönlendirme işleri sadece sınırlarda yapılmaktaydı çünkü bu görüşe göre daha eski ağ altyapılarının paket iletim hızının yavaş olmasının nedeni yazılımla tabanlı yönlendiriciler idi.

1990'lı yıllarda piyasada, özellikle internet altyapısını kurmak üzere tasarlanmış ağ cihazları bulunmadığından internet servis sağlayıcıları hızla artan talep patlamasını karşılamak üzere o anda piyasada bulabildikleri tüm cihazları kendi ağlarının performansı yükseltmek amacıyla, kendi ağlarına uygun hale getirip kullanmışlardır. O an için ATM anahtarlama cihazları ISS'lerin anlık ihtiyaçlarına cevap vermekteydi. Ancak internet altyapısı için tasarlanmış cihazlar yavaş yavaş ticari olarak satılmaya başlanınca ve internet servis sağlayıcılarının kullanıcı sayısı dolayısı ile gereksinimleri üstel olarak arttıkça, ATM üzerinden IP modelinin eksikleri göze daha çok batar oldu. Bu eksiklikler arasında ATM SAR arabirimlerinin bant genişliği sorunu, sanal devrelerin (VC) "n-kare" (n^2) sorunu, IGP protokolünün düzgün çalışmaması, iletilen hücre başına alınan %20 oranındaki vergi ve ATM olmayan altyapılarda bu modeli çalışmaması gibi problemler sayılabilir.

Yukarıda sayılan tüm bu sorunlardan daha da önemli olan konu tamamen farklı amaçlara hizmet etmek için tasarlanmış olan bu iki ayrı teknolojinin bir arada kullanılmasının getirdiği karmaşıklıktır.

4.3. ATM Üzerinden IP (IP Over ATM) Modeline Karşı Çok Protokollü Anahtarlama Alternatifleri

İnternet servis sağlayıcıları ATM üzerinden IP modeline geçerlerken bir takım teknik, finansal ve ekonomik eğilimler, internet altyapısında kullanılmak üzere yeni teknolojilerin geliştirilmesine başlanmasını sağlamıştır. Bu sırada halk da internetin yeni yeni ortaya çıkan ekonomik, yaşamsal vb. birçok etkilerini farketmeye başlamıştı. İşte tüm bu olumlu gelişmeler, internet dünyasının, tamamen internet altyapısını kurmak için dizayn edilmiş özel ağ cihazlarının yapılmasına değecek kadar büyük olduğu kanısını yerleşmesini sağlamıştır. IP protokolü bir anda IPX, AppleTalk, OSI ve SNA protokollerinden daha yaygın kullanılır olmuştu.

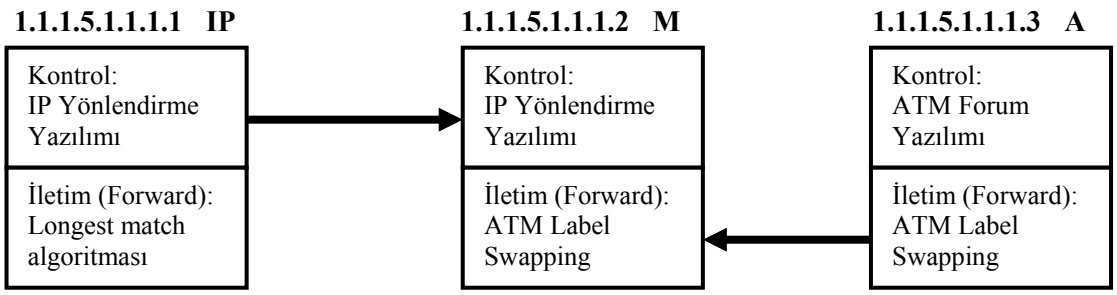
Yeni teknolojiler geliştirmek için çalışmalara başlayan firmaların hem fiyat/performans oranını düşüren, hem de ATM teknolojisinin hızını ve IP yönlendirmesinin avantajlarını daha iyi kullanan çözümleri sunmaları pek uzun bir zaman almadı. 1996'nın başlarında bir çok firma, internet altyapısı için geliştirdiği, ATM anahtarlama ile IP yönlendirme teknolojilerinin entegre olarak kullanıldığı çok protokollü anahtarlama ürünlerini tanıtmaya başlamıştı. Bu ürünlerden bazıları şunlardır:

- Ipsilon / Nokia firmasının geliştirdiği IP Switching
- Cisco'nun Tag Swicthing
- IBM Corp.'un ARIS (Aggregate Route-based IP Switching)
- Cascade/Lucent/Ascend'in ortak ürünü IP Navigator
- Toshiba firmasının Cell Swithing Router (CSR)

Her ne kadar bu teknolojilerinin çoğunun bir takım ortak özellikleri varsa da bu teknolojiler birarada aynı ağda kullanılamamaktaydı çünkü her bir ürün IP yönlendirme ile ATM anahtarlamayı entegre edebilmek için çok farklı teknikler kullanmaktaydı. Ama gene de 1997 senesinin sonlarına doğru internet çevreleri bu teknolojilerin geleceğin internet altyapılarını oluşturmada en önemli adım olduğunun farkına varmışlardır.

4.4. Çok Protokollü Anahtarlama Çözümlerindeki Benzerlikler

Her çok katmanlı anahtarlama çözümü, IP odaklı kalmak üzere ATM teknolojiyle IP teknolojisinin en iyi yanlarını bir araya getirmeye çalışmıştır. Bu ürünlerin hemen hemen tümünün tasarımında temel olarak yola çıkılan fikir, bir IP yönlendiricisinin kontrol yazılımının alınması ve bu yazılımı, bir ATM anahtarının etiket – değiştirip iletme mekanizması ile entegre ederek Şekil 3.4' deki gibi çok daha ucuz ve hızlı bir IP yönlendiricisi elde etme düşüncesidir



Şekil 4.1 – MPLS anahtarının temel yapı blokları

Kontrol bileşeni açısından her çok katmanlı anahtarlama çözümü standart IP yönlendirme yazılımları olan OSPF, IS-IS, BGP-4 yazılımlarını çalıştırmaktadır. Etiket atama mekanizması ise 3. katman yönlendirmelerini etiketlere eşleyerek (ATM'de VPI/VCI) bu eşleme bilgilerini ağda bir etiket anahtarlamalı yol (LSP) kurmak üzere komşularına dağıtmaktadır. Sadece ağ sınırlarında yönlendirme protokollerini çalıştırmak yerine ağın çekirdeğinde de yönlendirme protokollerini çalıştırmanın ağın işlerliğini arttırmak açısından bir çok yararı vardır:

- ATM üzerinden IP'deki "n-kare" tane sanal devre sorununu çözer
- Her bir yönlendiricinin komşu sayısını azaltarak IGP protokolü üzerinde oluşan yoğun iş yükünü aşırı derecede azaltır.
- Çekirdek ağın, belirli bir andaki fiziksel topolojisinin nasıl olduğu bilgisinin, 3. katman yönlendirme protokolleri tarafından öğrenebilmesini sağlar.

Aktarım bileşeni açısından çok katmanlı anahtarlar geleneksel ATM anahtarlama donanımı ve etiket değiştirme mekanizmalarını kullanmaktadırlar. Ancak yönlendirmelere etiketlerin atanmasını kontrol eden prosedürler, etiketlerin çok katmanlı anahtarlar arasında dağıtımını yapan protokoller ve iletim tablolarının oluşturulmasını sağlayan protokoller, ATM Forum protokolleri olmayıp IP tabanlı çözümlerdir.

Kurulan ağın çekirdeğinde ATM etiket değiştirerek iletme yönteminin kullanılmasının bir çok faydası bulunmaktadır:

- Etiket değiştirerek iletim yöntemi, donanım tabanlı veri iletiminin tüm faydalarını kullanılır kılarak ağın performansını arttırır.
- Etiket değiştirerek gönderme mekanizması açık yönlendirme (explicit routing) işlemini çok daha pratik hale getirir. **"Açık yönlendirme"** (explicit routing) demek, belirli bir kullanıcı trafiğinin iletilirken, servis sağlayıcının ağında geçeceği düğümlerin daha önceden belirtilmesi demektir. Böylelikle klasik "varış adresine göre yapılan yönlendirmelerden" daha farklı bir yoldan paketlerin iletilmesi sağlanabilir. Böyle açık yönlendirmeler internet servis sağlayıcılarının ağlarındaki trafik akışları üzerinde kesin bir kontrol kurmasını sağlar. Bu sayede de trafik yönetimi, Servis Kalitesi (QoS – Quality of Service) ve döngülerin önlenmesi çok daha kolay bir hale gelmektedir.

ATM Forum'unun yönlendirme ve mesajlaşma protokollerinin devre dışı bırakılmasıyla, IP ve ATM gibi iki farklı teknolojiyi bir arada kullanmak ve koordinasyonu sağlamak için ortaya çıkan karmaşıklık azaltılmıştır. Çok protokollü iletimde halen ATM' in standart VPI/VCI alanları etiket olarak kullanılmakta ise de bu değerlerin verilmesi ve dağıtılması işlemleri ATM Forum protokolleri yerine uygun IP tabanlı protokollere göre yapılmaktadır. Bu ise, iki değişik mimari arasında yapılması zorunlu olan karmaşık eşleşmeleri ortadan kaldırmaktadır. Tüm bu olumlu yanlarla berber çok protokollü anahtarlama çözümlerinin büyük çoğunluğunun sahip olduğu bir sınırlama vardır. Bu çözümlerin büyük bir kısmı sadece hücre-tabanlı ATM altyapısı üzerinde çalışacak şekilde dizayn edilmişlerdi. Halbuki internet ise giderek artan bir oranda paket-tabanlı veri iletimi kullanmaktaydı.[5]

4.5. Çok Protokollü Anahtarlama Çözümlerindeki Farklılıklar

Her ne kadar mevcut çok katmanlı anahtarlama çözümlerinin bir çok özelliği ortak olsa da aralarında çok önemli bir fark bulunmaktadır. Bu çözümler, etiket anahtarlamalı bir yol (LSP) kurmak için etiket atamasını ve dağıtımını daha önce bahsedilen iki değişik yönteme göre yapmaktadırlar: Kontrol İşaretleri İle Akış Belirleme Modeli ve Veri Yönlendirmeli Akış Belirleme Modeli.

Ipsilon'un IP Switching çözümü ile Toshiba'nın Cell Switching Router – CSR ürünü Veri Yönlendirmeli Akış Belirleme Modeli kullanan çözümlerdir. Ancak şunu da belirtmek gerekir ki MPLS standartizasyonu çalışmalarında bu model desteklenmemiştir.

Kontrol İşaretleri İle Akış Belirleme Modeli kullanan çok katmanlı anahtarlama çözümleri ise Tag Switching (Cisco Corp.), IP Navigator (Ascend/Lucent) ve ARIS (IBM)'dir.

4.6. Çok Protokollü Anahtarlama Çözümlerinin Temel Sorunu

Her çok katmanlı anahtarlama çözümü, kontrol bileşeni olarak IP kontrol bileşenini, iletim bileşeni olarak da ATM' in etiket değiştirme mekanizmasını kullanmaktadır. İnternet servis sağlayıcılarının karşılaştıkları problem ise bu ürünlerin hepsinin firmalara

özel nitelikler taşıması ve değişik firmaların ürünlerinin bir arada çalışamamasıydı. Üstelik bu ürünlerin birçoğu ATM mimarisinin kullanılmasını gerektiriyor daha farklı (Frame Relay, PPP, SONET, LAN ...) mimarileri üzerinde çalışamıyordu. Eğer çok protokollü anahtarlama teknolojisi, servis sağlayıcılar tarafından geniş şekilde kullanıma sokulacaksa, herhangi bir veri bağı katmanı (2. katman) teknolojisinde de çalışabilecek firmalar üstü bir stadartın getirilmesine ihtiyaç vardır. 1997 yılının sonlarına doğru, IETF (Internet Engineering Task Force), çok protokollü anahtarlama çözümlerinin birlikte çalışabilen ve ortak özelliklere sahip bir hale gelmesi için MPLS Çalışma Grubu'nu kurmuştur.

4.7. Multilayer Label Switching (MPLS)

MPLS teknolojisi, internet altyapısında kullanılan çok katmanlı anahtarlama teknolojisinin son halidir. MPLS, IETF'un değişik çok katmanlı anahtarlama çözümlerine bir standart getirme çabasının sonucudur.

MPLS teknolojisinde, etiket anahtarlamalı yolların (LSP) kurulması için gereken etiket atamaları ve bu atama bilgilerinin eşler arası dağıtımı işlemi Kontrol İşaretleri İle Akış Belirleme Modeline göre yapılmaktadır. Bu LSP'ler yapı olarak çok basittir (trafik akışı giriş tarafından çıkış tarafına doğru akar), iki yönlü haberleşme (duplex) için iki adet LSP gereklidir. Bir LSP kurmak için bir ya da birden fazla etiket değiştirmeli anahtar arka arkaya mantıksal olarak bağlanmalıdır. Paketler ise bir LSR'dan diğerine iletilerek MPLS etki alanı içerisinde ilerler.

MPLS' in kontrol bileşeni diğer çok katman anahtarlama teknolojileri gibi IP kullanımına odaklanmıştır. Ancak MPLS, firmalar üstü bir standart koyabilmek için var olan normal IP sinyalleşmesine ve etiket değişim protokollerine eklemeler yapmıştır ve yeni protokoller tanımıştır. ATM Forum mesajlaşması ve protokolleri, farklı iki protokol mimarisinin kullanılmasının getirdiği karmaşıklıktan kurtulmak için MPLS' de kullanılmaz. Bu açıdan MPLS, paket tabanlı iletişimlerde belirgin yararlar sağlamaktadır.

4.7.1 Gereksinimler ve Hedefler

MPLS çalışma grubunun hedeflerinin en önemlisi kontrol bileşeninde ağ katmanı yönlendirmesini, iletim (forwarding) bileşeninde ise etiket değiştirerek iletme mekanizmasının kullanılmasını sağlamak üzere bir standart teknoloji kurmaktır. Bu sonuca ulaşmak için MPLS Çalışma Grubu'nun öne sürdüğü bir takım standart gereksinimler bulunmaktadır:

- ♦ MPLS sadece ATM üzerinde değil, tüm veri-bağı katmanlarında çalışabilmelidir
- ♦ MPLS çekirdek teknolojileri hem "unicast" hem de "multicast" tipinden trafik akışlarının iletilmesini sağlayabilmelidir.
- ♦ MPLS, IETF 'un Tümleşik Hizmetler Modeline, RSVP protokolü de dahil olmak üzere, tam olarak uyumlu olmalıdır.
- ♦ MPLS, sürekli büyüyen interneti destekleyecek şekilde ölçeklenebilir olmalıdır.
- ♦ MPLS ağ üzerinde işlemlere, yönetime ve bakım özelliklerini en az IP ağlarında gerçeklendikleri kadar geniş oranda destekleyebilmelidir.

4.7.2. MPLS Çalışma Grubu'nun Tavsiyeleri

Piyasada bulunan etiket-değiştirerek aktarma algoritması ile ağ katmanı yönlendirmesini entegre eden çok protokollü anahtarlama çözümleri arasında bir standart sağlamak amacıyla MPLS Çalışma Grubu kurulmuştur. MPLS Çalışma Grubunun hedefleri arasında etiket dağıtımını ve devamlılığını sağlayan protokoller kümesinde bir standardizasyon gerçekleştirmek ve bu yeni teknolojinin değişik veri-bağı katmanı (link-level) teknolojileri üzerinde uygulanabilmesini sağlayacak yeni prosedürler tanımlamaktır. Ayrıca ağ katmanı ölçeklenebilirliliğini arttırmak, trafik yönetimini daha verimli hale getirmek ve fiyat/performans oranını düşürmek de diğer amaçlar olarak sıralanabilirler.

4.7.3. MPLS Hakkında Bazı Yanılgılar

İnternet altyapısının oluşturulmasında MPLS' in rolünün ne olduğu konusunda bir takım yanılgılar bulunmaktadır. İnternet çevrelerinin bir kısmı, MPLS' in, üreticilerin ATM

anahtarlarını, yüksek performanslı IP yönlendiricileri haline çevirmek için çıkardığı yeni bir standart olduğunu zannetmektedirler. Bu her ne kadar ilk ortaya çıkan çok protokollü anahtarlama teknolojilerinin birincil hedefi olsa da, günümüzün silikon teknolojisindeki ilerlemelerle ASIC (Application Specific Integrated Circuit) tabanlı IP yönlendirme tablosu arama cihazlarının MPLS ya da ATM VPI/VCI arama cihazları kadar hızlı çalışabilmesini mümkün kılmıştır. Ancak MPLS, işlemci tabanlı yönlendirme sistemlerinin performansını arttırabilse de, paket iletim hızının arttırılması MPLS Çalışma Grubunun kurulmasının temel nedeni değildir.

Bazı internet çevreleri de MPLS teknolojisinin, geleneksel en fazla uyan IP yönlendirmesini tamamen ortadan kaldırmak için tasarlandığını düşünmektedir. Böyle bir görüş hiçbir zaman MPLS Çalışma Grubu'nun hedefleri arasında olmamıştır çünkü bu grubun üyeleri geleneksel 3. katman IP yönlendirmesinin internet üzerinde her zaman gerekli olduğunu bilmektedirler. İnternette 3. katman IP yönlendirmesini vazgeçilmez yapan unsurlar şunlardır:

♦ Servis sağlayıcı sınırlarında ve güvenlik duvarlarında paket filtreleme işlemi, güvenliğin sağlanması ve ağ yönetiminin gerçeklenmesi açısından mutlaka desteklenmelidir. Paket filtreleme işlemi de paketlerin başlıklarının detaylı incelenmesine ihtiyaç duyduğundan 3. katman iletimi halen gereklidir.

♦ MPLS ağlarının çok fazla sayıdan konaktan oluşması mümkün değildir. Yani, bir konak tarafından iletilen bir paket halen en yakın 3. katman cihazına (layer 3 device) iletilmeli, burada da paket hedefine gönderilmeden önce paketin başlığı incelenmelidir. Bu paketi ilk alan yönlendirici paketi ya geleneksel 3. katman en fazla uyan yönlendirmesine göre bir sonraki düğüme iletir ya da paketi bir LSP üzerinden iletir.

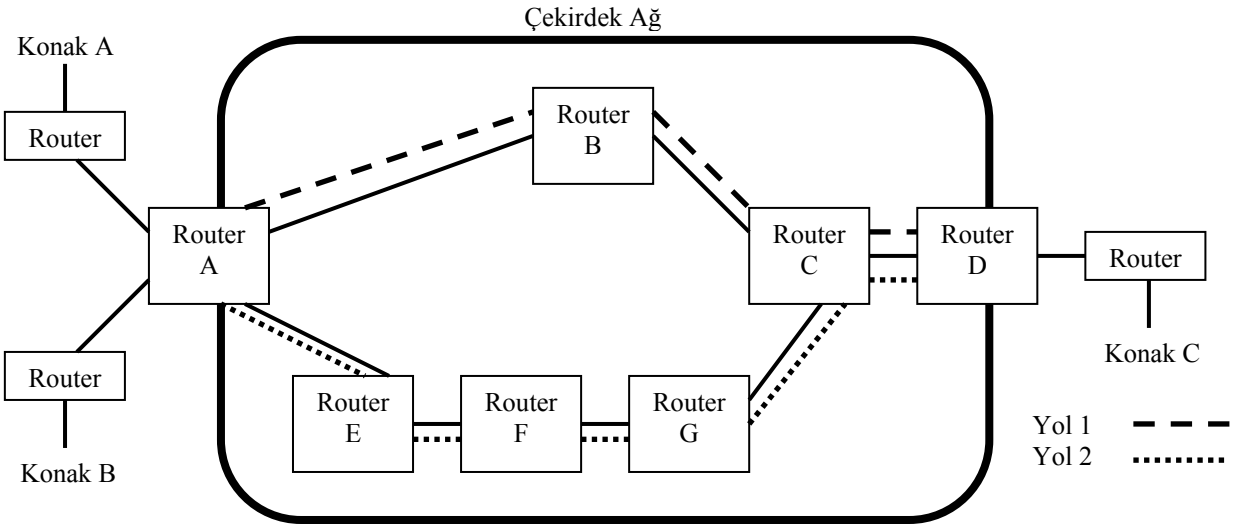
♦ Varış konağından önceki son düğümde paket, normal 3. katman yönlendirmesi ile iletilmelidir. Çünkü varış alt ağındaki her konağa ayrı bir etiket atama, pratik bir çözüm olmamaktadır.

4.7.4. MPLS Teknolojisinin Getirdikleri

Servis sağlayıcılarının alt yapılarında neden MPLS teknolojisini seçmeleri gerektiği sorusunun cevabı hiç şüphesiz ki MPLS' in, şu andaki geleneksel IP yönlendirme

teknolojisi ile kolayca sağlanamayacak yeni servis çeşitlerinin sunulabilmesine olanak sağlaması olacaktır. İnternet servis sağlayıcıları, hızlarını arttırmak zorunda kaldıkları gibi diğer firmalarla olan yarışlarında kendilerini bir adım daha ileri götürecek ve onları diğer firmalardan ayıracak hizmetler vermeleri gerekmektedir. MPLS teknolojisi de servis sağlayıcılarına masrafları kontrol etme imkanı, daha iyi servis seviyeleri sağlama ve daha çok müşteri odaklı hizmetler verebilme imkanı sunmaktadır.

Şekil 4.2' de sadece varış adresine göre iletimden daha fazlasına ihtiyaç duyan uygulamalarda MPLS' in yönlendirme yeteneklerini nasıl arttırdığı görülmektedir:



Şekil 4.2 – MPLS teknolojisinin yönlendirme işlemindeki fonksiyonelliği

Çekirdek ağdaki tüm yönlendiricileri klasik anlamda en-fazla-uyan IP yönlendirmesi yaptığını farz edelim. A konağının ya da B konağının C konağına iletmek isteyecekleri her paket, IGP tarafından en kısa yol olarak bulunan Yol 1'den (A-B-C-D) iletilecektir.

Şimdi ağ yöneticisinin ağda akan trafik istatistiklerini incelediğini ve B yönlendiricisindeki yığılmayı önlemek amacıyla bir takım tedbirler almaya ihtiyaç duyduğunu düşünelim. Bu tedbirlerden biri B yönlendiricisindeki yığılmayı azaltmak amacıyla bu yönlendirici üzerinden akan bir kısım trafiği ağ üzerindeki başka yollardan iletmek olacaktır. Diyelim A konağından C konağına gönderilen paketlerin B yönlendiricisinden geçmesine devam etmesi kararı verilsin. Ancak B konağından C

konağına gönderilen paketlerin ise başka bir yol üzerinden iletilmesi düşünülsün. Klasik IP yönlendirme ile böyle bir önlem alınması imkansızdır, çünkü A yönlendiricisinde sadece varış adresine göre yönlendirme yapılabilmektedir. Bu da doğal olarak A yönlendiricisinin kendisine gelen tüm paketleri (A konağından ve B konağından gelen) (en kısa yol olarak bulacağı) B yönlendiricisine ileteceği anlamına gelir.

Eğer bu çekirdek ağdaki yönlendiriciler etiket anahtarlamalı yönlendiriciler (LSR) olsa idi, B yönlendiricisindeki yığılmayı engellemek için böyle bir önlem rahatlıkla alınabilirdi. Ağ yöneticisi bir etiket anahtarlamalı ağ kurar (LSP 1) ve bunu Yol 1'den geçecek şekilde konfigüre ederdi. Aynı şekilde bir başka etiket anahtarlamalı yol (LSP 2) kurar ve bu yolun da Yol 2 üzerinden geçmesini ayarlardı. Son olarak da LSR A' nın , (Router A'nın yerindeki MPLS yönlendiricisi) kendisine A konağından gelen ve varış adresi C konağı olan tüm paketleri LSP 1 üzerinden göndermesini ayarlardı. Aynı şekilde LSR A' da, B konağından C konağına akan akışı da LSP 2 üzerinden göndermesini sağlayacak değişiklikleri de yaptıktan sonra B düğümündeki tıkanıklığı aşmış olurdu. Herhangi bir FEC'i isteğe göre belirlenebilen etiket anahtarlamalı yollardan (LSP) iletebilme olanağı, ağ yöneticisine, ağdan akan trafik üzerinde kesin bir kontrol sağlama imkanı verir.

Dikkatli yapılan bir planlama ile MPLS teknolojisi servis sağlayıcılara emsalsiz bir trafik kontrol seviyesi sağlar. Bunun sonucu olarak ağların verimi çok daha arttırılması, hizmetlerin daha planlı bir şekilde verilebilmesi ve sürekli değişen müşteri beklentilerine daha çabuk ve daha uygun destek verebilecek, esnekliği yüksek ağların oluşması sağlanmıştır.

Servis sağlayıcıları, yeni oluşan müşteri ihtiyaçlarını karşılamak için yeni hizmetler sunarken, MPLS altyapısı yerinde sabit kalır. Yeni hizmetler sadece yönlendiricilerin, paketleri FEC' lere koyan ve daha sonra bu Fonksiyonel Denklik Sınıflarını özel olarak kurulmuş LSP' lere eşleyen kontrol bileşenleri değiştirilerek sunulabilir. Örneğin paketler, varış altağı adresinin ve uygulama tipinin bir kombinasyonuna göre, kaynak ve varış alt ağlarının (subnet) adreslerinin bir kombinasyonuna göre, belirli bir QoS gerekliliğine göre, bir IP multicast grubuna göre veya sanal kurumsal ağ VPN numarasına göre herhangi bir Fonksiyonel Denklik Sınıfına dahil edilebilirler. Benzer

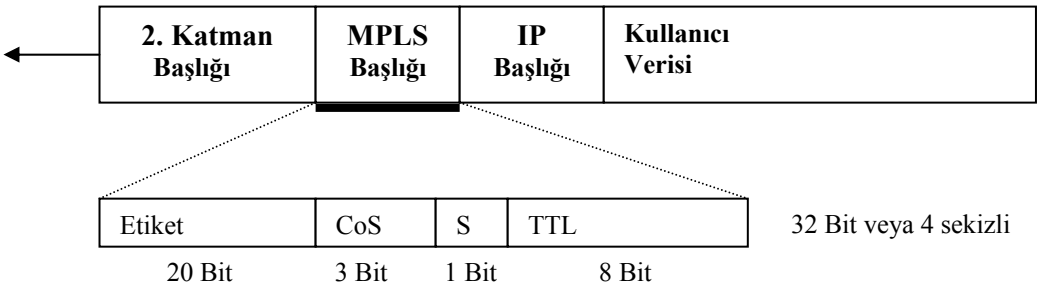
şekilde ağ yöneticileri de etiket anahtarlamalı yolları (LSP), Fonksiyonel Denklik Sınıflarının (FEC) sağlamaları gereken özelliklere göre belirleyebilirler: düğüm sayısını en aza indirecek şekilde, zorunlu bant genişliklerini sağlayacak şekilde, trafiğin ağdaki belirli bir düğümden mutlaka geçmesini sağlayacak şekilde, vb..... Son olarak sağlanan bir diğer esneklik de ağa giriş noktalarındaki "giriş" yönlendiricilerinin ayarlanarak istenilen FEC'in istenilen LSP üzerinden iletilmesi sağlanabilir.

4.8. MPLS Başlığı

Etiket ile aktarmada etiketler veya etiket yığınları, yaşam süresi (TTL) gibi çok çeşitli bilgiler aktarımda kullanılmaktadır. Bazı durumlarda bu bilgiler özel MPLS başlığının içine yerleştirilir, bazı durumlarda ise de 2. katman (veri bağı katmanı) başlığı içerisine yerleştirilir. Kullanılabilecek çok değişik MPLS başlığı çeşitleri bulunur. İletim için kullanılan ortamlara göre farklı MPLS başlıkları kullanılabilir. Örneğin ATM altyapısının kullanıldığı bir çözümde MPLS başlığındaki bilgiler ATM başlığı içerisinde iletilir. Biçimi ne olursa olsun etiket tabanlı bir aktarma işlemi için paketlere etiketlerin ve diğer bilgilerin iliştirilmesine "MPLS Eklentileri" adı verilir. "MPLS Başlığı" (MPLS Header) terimi ise etiket değerlerinin ve diğer bilgilerin 2. katman başlığında taşınamadığı durumlarda pakete iliştirilen özel amaçlı MPLS başlıkları için kullanılmaktadır.

MPLS eklentilerinde yer alan alanlar kesin olmamakla beraber bulunması zorunlu olan bilgi etiket değeri bilgisidir. Bunun dışındaki bilgilerin bu eklentilerde olup olmayacağı henüz bir standarda oturtulamamıştır. Bu konu daha sonraki çalışmalara bırakılmıştır. Başlıkta yer alması muhtemel bilgiler aşağıda verilmiştir:

- Etiket değeri
- Yaşam Süresi Değeri (TTL)
- Servis Sınıfı (CoS- Class Of Service)
- Yığın Belirteci (Stack Indicator)
- Sonraki Başlık Tipi Belirteci
- Toplama Sınaması (Checksum)



Şekil 4.3 - MPLS başlığı.

Paketlere iliştirilecek başlık bilgilerinin çok kısa olması, istenen bir özelliktir. Örneğin 4 sekizlik bir başlık, bu başlığa göre aktarma işlemini yapacak olan donanımın yapılmasını çok daha kolaylaştırmaktadır. Ancak paketle birlikte az sayıda bilgi taşımanın getireceği dezavantajlar da vardır. MPLS başlığında taşınacak bilgilerin ne olacağının seçimi konusu çok önemlidir.

4.9. Yönlendirme Hiyerarşisi ve Etiket Yığınları

Bazı durumlarda bir Ru yönlendiricisi belirli bir paketin bir Rd yönlendiricisine aktarılmasını isteyebilir. Ancak Rd yönlendiricisi paketin normal güzergahı üzerinde bir yönlendirici olmayabilir ve hatta paketin varış yönlendiricisi de Rd olmayabilir. Yani paket özellikle Rd üzerinden varış adresine gönderilmek istenebilir. Bunu sağlamak için paket varış adresi Rd'nin adresi olan yeni bir ağ katmanı paketi içine sokularak Rd'ye yollanabilir. Bu işlem Ru'dan Rd'ye bir "tünel" kurulması anlamına gelmektedir.

4.9.1. Düğümden – Düğüme Aktarma Yapılan Tüneller

Eğer paket tünele girdikten sonra Ru'dan Rd'ye doğru adım adım aktarılarak ilerliyorsa bu tip tünellere "Adım Adım Aktarma Yapılan Tüneller" verilir. Burada Ru "Gönderen Uç", Rd ise "Alıcı Uç" olarak adlandırılmaktadırlar.

4.9.2. Açık Yönlendirmeli (Explicitly Routed) Tüneller

Eğer bir paket, tünel içerisinde adım adım yönlendirmeden başka bir güzergah takip ederek ilerliyorsa bu tarz tünellere "Açık Yönlendirmeli Tüneller" denilir. Burada da gene Ru "Gönderen Uç", Rd ise "Alıcı Uç" olarak adlandırılmaktadırlar. Böyle bir tünel

kurmak için örnek olarak; gönderilecek paketi sardığımız yeni paketi "kaynaktan yönlendirmeli" bir paket olarak belirleyebiliriz.

4.9.3. Etiket Anahtarlamalı Yol (LSP) Tünelleri

LSP kullanarak bir tünel kurma imkanı da bulunmaktadır. Bu durumda tünel içinden aktarılacak paketler bir FEC oluşturmaktadır ve tüneldeki her etiket anahtarlamalı yönlendirici LSR, bu FEC'e bir etiket eşleştirmek zorundadır. Belirli bir paketin tünelden gönderilip gönderilmeyeceği ise tünelin "gönderen ucunda" verilen bir karardır. "Gönderen uç" bir paketi tünelden aktarmaya karar verince paketin etiket yığının tepesine tünel için belirlediği FEC'e eşlenmiş etiket değerini koyarak paketi tüneldeki bir sonraki düğüme iletir.

Daha sonraki paragraflarda da anlatılacağı üzere tünelin çıkış ucundaki "alıcı uç" yönlendiricisinin paketin tünelden gelip gelmediğini bilmesi gerekmez çünkü etiket yığınının tepesindeki değeri çekme işini onun adına tüneldeki sondan bir önceki düğüm yapar.

Örneğin <R1, R2, R3, R4> LSR'larından oluşmuş etiket anahtarlamalı bir yol gözönüne alalım. R1 yönlendiricisi henüz etiketlenmemiş bir IP paketi aldığında bu paketin yukarıdaki güzergahı izleyerek aktarılması için bu paketin etiket yığınının tepesine yeni bir etiket değeri koyar. Ancak bu güzergahtaki R2 ve R3 yönlendiricileri birbirlerine doğrudan bağlı olmayıp bir tünel aracılığı ile bağlı olsunlar. Yani paketin gerçekte izleyeceği güzergah <R1, R2, R21, R22, R23, R3, R4> olsun.

P paketi R1'den R2'ye doğru hareket ederken etiket yığını derinliği 1'dir. R2 yönlendiricisi gerekli etiket değişikliğini yaptıktan sonra paketin tünele girmesi gerektiğini belirler. R2 yönlendiricisi öncelikle gelen paketin "giriş etiketini" R3 için anlamlı olacak bir "çıkış etiketi" ile değiştirir. Daha sonra ise etiket yığınının tepesine R21 için anlamlı olacak yeni etiket değerini koyar. Böylelikle paketin etiket yığını 2 derinlikli hale gelir. Bundan sonra R21, R22, R23 boyunca paket yığının bu 2. seviyedeki etiket değerlerine göre aktarılmaktadır. R23 yönlendiricisi ise R2-R3 arasındaki tünelin sondan bir önceki düğümüdür. Bu R23 düğümü paketi son düğüm olan R3'e iletmeden

önce, paketin yığınının tepesindeki etiketi çekerek yığın seviyesini tekrar 1'e düşürür. R3 bu işlemlerden sonra P paketini aldığında pakette sadece yığının 1. seviyesindeki etiketi görmektedir. Ayrıca R3 etiketi de 1. seviyedeki LSP için sondan bir önceki düğüm olduğundan 1. seviyedeki etiket, R3 tarafından çekilerek R4 yönlendiricisine paket tekrar etiketlenmemiş halde aktarılır.

4.9.4. Tünellerde Etiket Dağıtımı

Tünellerde de normal etiket anahtarlamalı ağlarda olduğu gibi etiketler atanır ve dağıtılır. Etiket dağıtımı açısından eş olma ise (label distribution peers) yığın seviyelerine göre belirlenir. Yukarıda anlatıldığı gibi bir P paketi <R1, R2, R21, R22, R23, R3, R4> güzergahından aktarılsın. Bu P paketi R2 – R3 yönlendiricileri arasında aktarılırken < R2, R21, R22, R23, R3 > düğümlerinden oluşan 2. seviye etiket anahtarlamalı yoldan (LSP) aktarılmaktadır. 2. seviye LSP için R2 yönlendiricisinin etiket dağıtımı açısından eşi R21 düğümüdür. Ancak 1. seviye LSP için R2'nin etiket dağıtımı açısından eşleri R1 ve R3 düğümleridir.

Bu örnekte R2 ve R21 düğümlerinin IGP protokolüne göre komşu olma zorunluluğu varken R2 ve R3 düğümlerinin böyle bir zorunluluğu yoktur. İki etiket anahtarlamalı anahtar LSR birbirine IGP protokolüne göre komşu olduğu zaman bu iki yönlendiriciye "etiket dağıtımı açısından yerel eşler" adı verilmektedir. İki yönlendirici etiket dağıtımı açısından birbirine komşu olduğu halde IGP protokolüne göre komşu olmaz ise bu düğümlere "etiket dağıtımı açısından uzak eşler" denilir. Yukarıdaki örnekte R2 ve R21 düğümleri etiket dağıtımı açısından yerel eşlerdir ama R2 ve R3 etiket dağıtımı açısından uzak eşler olmaktadır.

MPLS mimarisi ise değişik seviyelerde etiket dağıtımı için iki değişik yolu desteklemektedir: Açık Eşleşme ve Kapalı Eşleşme.

Bir yönlendirici etiket dağıtımını, etiket dağıtımı açısından yerel eşi olan düğüme yapacağı zaman, eşinin adresine gönderdiği normal etiket dağıtım protokolü mesajlarını kullanır. Ancak etiket dağıtımı açısından uzak olan bir eşe bu bilgiyi göndermek için iki yolu vardır:

1) Açık Eşleşme

Bu yöntemde, bir yönlendirici "etiket dağıtımı açısından uzak eşi olan yönlendiriciye" etiket dağıtımı yapmak için bu eşine, sanki etiket dağıtımı açısından yerel eşi olan düğüme gönderiyormuş gibi bir etiket dağıtım protokolü LDP mesajı gönderir. Bu yöntem etiket dağıtımı açısından uzak olan eş düğümlerin sayısı az iken ya da paketlerin yığınlarının yüksek seviyelerinde etiket atamaları adedi çok fazla ise ya da etiket dağıtımı yapacak olan uzak eşlerin aynı yönlendirme alanında bulunmadığı durumlarda çok yararlıdır.

2) Kapalı Eşleşme

Bu yöntemde ise yönlendirici etiket dağıtımı açısından eşi olan düğümün adresine doğrudan bir etiket dağıtım protokolü LDP mesajı göndermez. Bunun yerine yığının tepesindeki etiket bilgisini, daha alt seviyedeki etiketin bir ek bilgisi olarak kodlar. Daha sonra bu ek bilgi ile beraber bir alt seviyedeki etiketi, etiket dağıtımı açısından yerel eşlerine gönderir. Daha sonra bu bilgiyi alan eşler de bu etiketi kendi etiket dağıtımı açısından yerel eşlerine dağıtır. Böylece kodlanmış üst seviye "etiket ataması" bilgisi uzaktaki eşe ulaşıncaya kadar adım adım iletilir. Bu teknik ise etiket dağıtımı açısından uzak olan eş düğümlerin sayısı fazla iken yararlıdır.

4.10. Etiket Kaynaştırma

Belirli bir etiket anahtarlamalı yönlendiriciye (LSR) belirli bir FEC'e ait ama değişik etiketlere sahip paketlerin geldiğini varsayalım. Bu paketleri iletirken LSR, tüm paketleri aynı çıkış etiketi kullanarak aktarmak isteyecektir. Paketlerin aynı Fonksiyonel Denklik Sınıfında olup da (FEC'de) olup da değişik "giriş etiketleri" ile gelmesinin bir önemi bulunmamaktadır çünkü ilgili yönlendirici bu paketleri aynı çıkış etiketi ile aktaracaktır. Bu işlemi yapabilme yeteneğine "Etiket Kaynaştırma" denilmektedir.

Diyelim ki bir LSR yönlendiricisi, değişik giriş arabirimlerinden ve/veya değişik etiketlere sahip paketler kendisine geldiğinde "etiket kaynaştırma" yeteneğine sahip olsun. Aynı zamanda bu şekilde gelen paketleri aynı çıkış arabirimine aynı çıkış etiketi

ile aktarsın. Paketler bu şekilde çıkış arabirimine iletildikten sonra paketlerin değişik arabirimlerden geldiği ve/veya değişik etiketlerle geldiği bilgileri kaybolacaktır.

Şimdi de "etiket kaynaştırma" yeteneğine sahip olmayan bir etiket anahtarlamalı yönlendiriciyi (LSR'ı) göz önüne alalım. Bu yönlendiriciye farklı giriş arabirimlerinden ve/veya farklı etiketlere sahip paketler geldiğinde bu paketler ya farklı çıkış arabirimlerden ya da farklı etiketlerle aktarılacaktır. SVC (Switched Virtual Circuit) veya SVP Kodlamasını kullanan ATM – LSR' ları "etiket kaynaştırma" yeteneğine sahip değildirler.

"Etiket kaynaştırma" yöntemi ile her fonksiyonel denklik sınıfı için (her FEC için) gerekecek çıkış etiketi sayısı sadece 1 iken "etiket kaynaştırma" yeteneğinden yoksun bir ortamda her FEC için gerekecek çıkış etiketleri sayısı ağdaki toplam düğüm sayısı kadar çok bile olabilir.

MPLS mimarisinde hem etiket kaynaştırabilen etiket anahtarlamalı yönlendiriciler hem de etiket kaynaştıramayan etiket anahtarlamalı yönlendiriciler bulunabilir.

4.10.1. Etiket Kaynaştıramayan LSR

MPLS aktarma prosedürleri ATM' in ya da Frame Relay teknolojilerinin aktarma prosedürleri ile çok benzerdirler. Hepsinde de paket geldiğinde "çapraz bağlantı tablosunda" bir etiket değeri (VPI/VCI veya DLCI) aranır ve daha sonra çıkış portu ve yeni etiket değeri bulunur. Aslında bu teknolojileri MPLS için de kullanmak uygundur ama bunu yapabilmek için "çapraz bağlantı tablolarının" kurulması için MPLS etiket dağıtım protokolünün LDP protokolünün işaretleşme protokolü olarak kullanılması gerekir. Ne yazık ki bu teknolojiler etiket kaynaştırma yeteneğine sahip değildirler. ATM tekniğinde bir yönlendirici etiket kaynaştırması yapmaya çalıştığı zaman farklı paketlerin hücreleri içiçe geçmeye başlar. Değişik paketlerin hücreleri içiçe geçtikten sonra da bu paketler tekrar oluşturulamazlar. Çoğu Frame Relay anahtarı da arka planda hücre anahtarlamayı kullanırlar ve aynı sebepten dolayı (hücrelerin içiçe geçmesi) bu anahtarlar da etiket kaynaştırma yapamamaktadırlar.

MPLS Çalışma Grubu bu konuda iki çözüm önermektedir. Birincisi MPLS teknolojisinin etiket kaynaştırması yapamayan yönlendiricileri de kullanabilmesi için bir takım prosedürlerin oluşturulması yönündedir. İkinci görüş ise belirli bazı ATM anahtarlarının etiket kaynaştırması yapacak şekilde yeni prosedürlerin tanımlanmasıdır.

Ayrıca MPLS teknolojisi, hem etiket kaynaştırabilen hem de etiket kaynaştırma yapamayan yönlendiricileri birarada kullanabildiği için tüm ağın doğru ve uyumlu çalışmasını temin etmek için bazı prosedürler de tanımlanmalıdır.

4.10.2. Kaynaştırma Yapabilen ve Yapamayan Etiket Anahtarlamalı Yönlendiricilerin Etiket Kullanımı

Etiket kaynaştırması yapabilen, akış yönünün yukarısındaki bir yönlendirici (LSR), aşağı-akış yönündeki düğümlerden her bir FEC için sadece 1 etiket bilgisi beklemektedir. Ancak eğer bu yönlendirici etiket kaynaştırmasını desteklemiyorsa, her bir FEC için çok sayıda etiket bilgisi beklemek zorunda kalabilir. Üstelik her bir FEC için ne kadar etiket bilgisi gerektiği konusunda da önceden bir öngörü yapılamaz.

MPLS mimarisinde eğer yukarı - akış yönündeki yönlendiricilerden bir tanesi etiket kaynaştırmayı desteklemiyorsa bu yönlendiriciye, kendisi özel olarak istemedikçe, herhangi bir FEC'e ait etiket ataması bilgisi gönderilmez. Bu yukarı – akış yönündeki yönlendirici her defasında bu tarz bir istekte bulunur ve her defasında da farklı etiket değerleri alır. Aşağı-akış yönündeki bir yönlendiriciye, bu yukarı-akış yönündeki yönlendiriciden bu şekilde bir istek geldiğini düşünelim. Eğer bu isteğin geldiği yönlendirici de etiket kaynaştırmasını desteklemiyorsa, bu sefer isteğin geldiği bu yönlendirici de kendi aşağı-akış yönündeki komşusundan bu FEC'in etiketini sormak zorunda kalacaktır.

Etiket kaynaştırmasını destekleyen ancak en fazla belirli bir sayıda giriş etiketini tek bir FEC'e kaynaştırabilen yönlendiriciler de bulunabilir. Donanımsal nedenlerden ötürü en fazla 4 tane giriş etiketini bir çıkış etiketine kaynaştırabilen bir yönlendirici düşünelim. Ancak bu yönlendiriciye belirli bir FEC'e ait 6 adet farklı etiket geldiğini varsayalım. Bu

durumda yönlendirici bu etiketleri toplam iki adet çıkış etiketine dağıtarak kaynaştıracaktır.

4.10.3. ATM'de Etiket Kaynaştırması

ATM 'de etiket kaynaştırmasını sağlamak için hücrelerin içiçe geçmesini önlemek gerekmektedir. Bu amacı sağlamak için iki ayrı yöntem bulunmaktadır:

1) SVP Çok Noktadan Kodlama ile Sanal Yol (VP) Kaynaştırması

Sanal yol VP kaynaştırılması kullanıldığı zaman, birden fazla sanal yol (VP) tek bir sanal yol olarak birleştirilir. Ancak bu yeni oluşan sanal yoldan aktarılan paketler birbirlerinden Sanal Devre Tanımlayıcı Değerleri (VCI) ile ayrılabilmektedir.

2) Sanal Devre (VC) Kaynaştıması

Sana devre (Virtual Circuit VC) kaynaştırılması kullanıldığı zaman, anahtarlar (switches) tüm paket gelinceye kadar paketin gelen hücrelerini (cell) bir tampon alanda saklamalıdır.

Bu yöntemlerden birincisi yani sanal yolların kaynaştırılması yöntemi ATM ağlarında kullanılması daha muhtemel bir tekniktir. Sanal devre kaynaştırmasından farklı olarak sanal yol kaynaştırılmasında, kaynaştırma yapılan noktalarda herhangi bir gecikmeye neden olunmaz ve ayrıca ek tampon belleklerin kullanılmasına ihtiyaç duyulmaz. Ancak gene de sanal yol VP kaynaştırmasının, VCI uzayının her sanal yolu VP için koordine edilmesinin gerekliliği gibi dezavantajı bulunmaktadır.

Halen kullanılmakta olan cihazlara uyumluluk sağlama ile protokol karmaşıklığının azaltılması ve ölçeklenebilirliğin arttırılması arasında uygun bir denge kurulması zorunlu olduğundan MPLS teknolojisi hem sanal yol VP kaynaştırmasını hem de sanal devre VC kaynaştırmasını desteklemek durumundadır.

4.11. Yaşam – Süresi (TTL – Time To Live)

Klasik IP yönlendirmesinde her paket başlığında Yaşam-Süresi (Time-To-Live TTL) değeri taşınmaktadır. Paket bir yönlendiriciden geçtiği zaman bu değer 1 azaltılmaktadır

ve eğer paket varış adresine ulaşamadan bu değer 0 olursa paket ilgili yönlendirici tarafından atılmaktadır.

Bu teknik, hatalı yapılan konfigürasyonlardan ya da yönlendirme algoritmasının yavaş çalışması veya hiç çalışmaması sonucunda ortaya çıkabilecek aktarma döngülerini önlemeye yaramaktadır. Ayrıca TTL alanı tek-noktadan çok noktaya alanının belirlenmesi "traceroute" komutunun desteklenmesi gibi bir takım fonksiyonları yerine getirmek için de kullanılmaktadır.
MPLS ağında bir LSP içerisinden ilerleyen paketin TTL alanının değeri, paket normal yönlendiricilerden oluşmuş klasik bir ağda ilerlerken aynı düğümlerden geçmesi durumunda alacağı değer ile aynı olmalıdır. Hatta paket tünellere girip-çıksa dahi paketin TTL alanının değeri, paketin fiziksel olarak geçtiği düğüm sayısı ile belirlenmelidir. TTL alanının işlenmesi, bu alanın MPLS' e özel bir MPLS başlığında mı yoksa ATM veya Frame Relay başlığı gibi herhangi bir 2. katman başlığında mı taşındığına bağlıdır.

Eğer TTL değeri 2. katman olan veri-bağı katmanı başlığı ile 3. katman olan ağ katmanı başlığı arasında yerleştirilmiş MPLS başlığı içerisinde taşınıyorsa bu alanın değeri, paket aktarılmak üzere yola ilk çıktığında, 2. katmanda başlığındaki TTL değerine eşitlenmelidir. Daha sonra da bu TTL değeri, paket iletilirken her LSR düğümünden geçerken bir azaltılmalıdır. Paket MPLS ağından (LSP'den) çıkarken de bu MPLS başlığındaki TTL değeri ağ katmanı başlığı içindeki TTL alanına yazılmalıdır.

Eğer etiket değerleri veri bağı katmanının başlığı içerisinde taşınıyorsa ve etiketlenmiş paketler bir L2 anahtarı tarafından aktarılıyorsa ve de bu veri-bağı katmanı başlığının kendisinde bir TTL alanı bulunmuyorsa, her LSR düğümünde paketin TTL değerini 1 azaltma işlemi gerçekleştirilemez. Paketin aktarıldığı yol boyunca (LSP), TTL değerini değiştiremeyecek etiket anahtarlamalı yönlendiricilerden (LSR) oluşmuş parçaya "**TTL'siz LSP segmanı**" adı verilir.

Bir paket, herhangi bir "TTL'siz LSP segmanı"ndan çıktıktan sonra, paketin fiziksel olarak geçtiği LSR'ların sayısını yansıtan bir değer TTL alanına yerleştirilebilir. Bunu gerçekleştirmek için paketin "TTL'siz LSP segmanına" ilk girdiği giriş yönlendiricisini kullanmak gerekir. Bu giriş yönlendiricisinde anlamlı bir LSP uzunluğu üretilir. Elde

edilen bu sayı, paketi "TTL'siz LSP segmanına" aktarmadan önce peşinen paketin TTL değerinden çıkartılır.

Bazı durumlarda da bir paketin TTL değerinin "TTL'siz LSP segmanını" içerisinden geçerken sıfırlanacağı bu "TTL'siz LSP segmanına" girmeden önce bu segmanın girişindeki yönlendirici tarafından belirlenebilir. Bu durumda bu paketin ilgili segmana giriş yönlendiricisinin bu paketi etiketleyerek aktarmaması gerekmektedir. "Traceroute" fonksiyonunun gerçeklenebilmesi için bu şartlar altında ne yapılması gerektiğini belirleyen özel prosedürler geliştirilmelidir. Örneğin paketler bu noktadan sonra geleneksel adım adım yönlendirme ile aktarılabilir.

4.12. Döngü Kontrolleri

Bir "TTL'siz LSP segmanında" tanım olarak TTL alanı döngüleri önlemek için kullanılamaz. Döngü kontrolü, "TTL'siz LSP segmanlarında" LSR fonksiyonlarını yerine getirmek için özel olarak tasarlanan donanımlarla sağlanabilir.

MPLS anahtarlama için ATM anahtarlarının kullanıldığını ve etiket değerlerinin VPI/VCI alanlarında taşındığını varsayalım. ATM donanımlarının TTL alanlarını bir azaltma yetenekleri olmadığından döngüler için özel bir koruma bulunmamaktadır. Ancak eğer ATM donanımı tampon belleğindeki farklı VPI/VCI değerlerine sahip hücrelere uygun bir erişim sağlayabiliyorsa, ortaya çıkacak bir döngü diğer trafik üzerinde olumsuz etki yapamayacaktır. Aksi takdirde, ATM donanımı bu tarz bir erişimi sağlayamıyorsa, çok kısa ömürlü döngüler dahi LSR'ların toplam performansını önemli ölçüde azaltabilir.

Tampon belleğe uygun bir şekilde erişim sağlansa dahi, normalden çok daha uzun süren döngüleri belirleyebilmek için bir takım yöntemler geliştirmek yararlı olacaktır.

4.13. ETİKET DAĞITIM PROTOKOLÜ

Etiket dağıtım protokolü, bir etiket anahtarlamalı yönlendiricinin (LSR) yaptığı etiket/FEC atamalarını diğer LSR'lara haber vermek için kullandığı prosedürler

kümesidir. Etiket/FEC ataması bilgisini birbirlerine aktaran iki LSR yönlendiricisine, değiş-tokuş ettikleri atama nazarında "etiket dağıtım eşleri" denir. Eğer iki LSR etiket dağıtım eşleri olarak adlandırılıyorsa bu iki LSR arasında bir "etiket dağıtım komşuluğu" vardır. Burada önemli olan iki LSR yönlendiricisinin, bir takım etiket/FEC atamaları için "etiket dağıtım eşleri" iken daha başka etiket/FEC atamaları için "etiket dağıtım eşleri" olmayabilecekleri hususudur.

Ayrıca etiket dağıtım protokolü (LDP), iki "etiket dağıtım eşi" olan LSR yönlendiricisinin, birbirlerinin MPLS yeteneklerini öğrenmek için yapmaları gereken görüşmeleri de kapsamaktadır.

Etiket dağıtımı konusunda önemli olan bir başka noktada, MPLS mimarisinin tek bir etiket dağıtım protokolü (LDP) kullanmadığıdır. Tam tersine birkaç tane etiket dağıtım protokolü, standartlaştırılmıştır. Varolan bazı protokoller, MPLS etiket dağıtımını gerçekleyebilecek şekilde yeniden düzenlenmişlerdir (MPLS – BGP, MPLS – RSVP, MPLS – RSVP - TUNNELS gibi). Ayrıca etiket dağıtımını gerçekleştirmek üzere yeni tasarlanan MPLS –LDP, MPLS - CR – LDP gibi protokoller de mevcuttur.

4.14. LDP Mesaj Değişimi

Temel olarak 4 tane LDP mesajı türü vardır:

1) Keşif Mesajları: MPLS ağındaki bir LSR yönlendicisinin varlığının belirlenmesi ve varlığının sürdüğünün kontrol edilmesi için kullanılır.

2) Oturum Mesajları: LDP eşleri arasındaki oturumları kurmak, sürdürmek ve sona erdirmek için kullanılan mesajlar.

3) İlan Mesajları: FEC'lere etiket atanması sağlanması, değiştirilmesi ve silinmesi için kullanılan mesajlar.

4) Bilgilendirme Mesajları: Yol gösterici mesajlar ve mesajlaşma hatasının bilgilerini içeren mesajlar.

Keşif mesajları, ağdaki her LSR yönlendiricisinin, varlıklarını diğerlerine bildirmek için periyodik olarak mesajları gönderebilecekleri bir mekanizma sağlamaktadır. Bu ise "ilgili altağdaki tüm yönlendiricilerin LDP portları" çok amaçlı grup adresine gönderilen bir UDP mesajı ile sağlanır. Bir LSR yönlendiricisi, varlığını aldığı "Hello" mesajı ile belirlediği bir başka LSR ile bir oturum kurmak istediği zaman ise TCP protokolü üzerinden LDP ilk işlemlerini gerçekleştirir. Başarılı bir oturum kurulduktan sonra artık bu iki LSR, LDP eşleri olmuştur ve bundan sonra aralarında ilan mesajları alış-verişi yapabiliriler.

Bir LSR yönlendiricisinin bir başka LSR yönlendiricisinden etiket bilgisi sorma işinin ya da kendi atadağı bir etiket/FEC eşleşmesi bilgisini bir başka LSR'a bildirme işinin ne zaman yapılacağı geniş çapta ilgili yönlendirici tarafından saptanır. Ama genelde bir LSR ancak bir etiket bilgisine ihtiyaç duyduğu zaman komşu LSR'dan bir etiket sorar ya da kendi atadığı bir etiket/FEC bilgisini komşu LSR'a, komşusunun bu etiketi kullanmaya başlamasını istediği zaman gönderir.

LDP protokolünün düzgün çalışması için mesajların mutlaka iletilebilmesi ve doğru sırada iletilebilmesi şarttır. Bunları sağlamak için LDP protokolü oturum, ilan, bilgilendirme mesajları yani UDP ile iletilen "Hello" mesajları haricindeki her şey için TCP protokolünü kullanmaktadır.

4.15. LDP Mesajının Yapısı

Tüm LDP mesajları "Tip – Uzunluk – Değer" TUD (Type –Length – Value TLV) kodlama sistemi kullanılarak oluşturulurlar. Yani LDP mesajının Tip - Uzunluk boyu her zaman sabittir (3 sekizli) ancak bunun içindeki bilgilerin ne olduğu ve nasıl yorumlanacağı "Tip" alanındaki değer ile belirlenir. "Boy" alanındaki bilgi ile yorumlanacak bilginin boyunun kaç bit olduğu öğrenilir. Mesajın içindeki "Değer" kısmında ise yorumlanacak değer yer almaktadır.

Bir LDP mesajında 2 bit, bu LDP mesajının tanımlanması halinde yapılması gereken işlerin kodlandığı bir alandır. Bu alan ileride gerçeklenecek yeni LDP mesajlarının kullanımına olanak sağlamak için konulmuştur.

Daha sonraki 14 bit ise tip alanını belirtir. Son olarak geriye kalan 16 bit de uzunluk alanını oluşturmaktadır. Uzunluğu burada belirtilen veri bu 32 bitlik alanın arkasına eklenir. Bu kısma ise değer alanı denilir.

4.16. Hata Kotarımı

LDP mesajlaşmasında meydana gelen hatalar ve diğer olaylar LDP eşlerine bilgilendirme mesajları ile bildirilir.

İki çeşit bilgilendirme mesajı vardır:

1) Hata bilgilendirmeleri, mühim hataları haber vermek için kullanılır. Eğer bir LSR, LDP eşinden bir LDP oturumu ile ilgili hata mesajı alırsa bu oturum için kullandığı TCP bağlantısını kapatarak oturumu sona erdirir ve bu oturum aracılığı ile öğrendiği tüm etiket/FEC eşleştirilmelerini çöpe atar

2) Bilgi verme amaçlı mesajlar ise bir LDP oturumu hakkında bilgi vermek amacıyla ya da daha önce alınan mesajların durumunu bildirmek amacıyla kullanılır.

4.17. LDP Genişletilebilirliği ve İleriye Dönük Uyumluluk

LDP'ye ileride ek bir takım fonksiyonlar dahil edilebilmelidir. Gelecekte yeni mesaj tipleri olması (yeni TUD – "TLV" tipleri) muhtemeldir. Bu yeni mesaj tiplerini ve TUD'leri tanımayan eski uygulamaların kullanıldığı ağlarda bu yenilikler de kullanılabilir olmalıdır. Gelecekte yapılacak her geliştirmenin, geriye uyumluluğu desteklemeyeceği göz önünde bulundurulursa, MPLS teknolojisinin planlanması aşamasında yeni gelecek tekniklere verilecek desteği kolaylaştırma yollarına gidilmelidir.

Bunun için tanımlanamayan mesaj tipleri ve TUD'leri (TLV) kotarılması konusunda bir takım kuralların tanımlanmasını gerektirir.

4.18. LDP İşlemleri

4.18.1. Fonksiyonel Denklik Sınıfları

Hangi LSP' ye hangi FEC'lerin atandığının kesin olarak belirlenmesi MPLS için bir zorunluluktur. Bu ise her LSP için bir FEC tanımlaması yapılarak gerçeklenir. Her bir fonksiyonel eşitlik sınıfı ise (FEC) bu etiket anahtarlamalı yoldan, LSP' den geçerek aktarılacak paketler grubunu temsil eder.

Her FEC bir ya da daha fazla FEC elemanından (FEC elements) oluşmaktadır. Her FEC elemanı da ilgili LSP' den geçerek aktarılacak paketler kümesini belirler. Bir LSP birden fazla FEC elemanı tarafından paylaşıldığı zaman bu LSP, artık bu FEC elemanlarının aynı LSP' yi kullanmalarının mümkün olmadığı düğümde (ya da düğümden önce) yok edilir.

Aşağıda FEC elemanlarının tanımlanmış bazı tipleri bulunmaktadır. İhtiyaç duyuldukça yeni tipler eklenmektedir.

1) Adres Öneki : Bu eleman sıfır uzunluktan tüm IP adresine kadar değişen uzunluklarda adres önekleridir.

2) Konak Adresli : Bu eleman ise konağın tüm adresidir.

Belirli bir IP adresinin, belirli bir IP adresi önekine tam olarak uyması için, bu IP adresinin kesinlikle bu önekle başlaması gerektiği söylenebilir.

Belirli bir paketi belirli bir LSP' ye atamanın bir takım kuralları vardır. Her kural, paket bir LSP' ye atanıncaya kadar sıra ile uygulanır:

- Eğer paketin varış adresi ile aynı Konak Adresli FEC Elemanının kullandığı sadece bir LSP varsa, paket bu LSP' ye atanır.
- Eğer paketin varış adresi ile aynı IP adresini taşıyan Konak Adresli FEC elemanının kullandığı birden fazla LSP varsa, paket bu LSP' ler arasından seçilen bir LSP ile ilişkilendirilir. Hangi LSP' nin seçileceği ise karmaşık bir takım prosedürlerle belirlenir.
- Eğer paket tam olarak sadece bir LSP' ye uyuyorsa, bu LSP' ye atanır.
- Eğer paket birden fazla LSP' ye uyuyorsa, en fazla uyan LSP' ye atanır. Eğer gene tek bir tane LSP bulunamazsa, yukarıda olduğu gibi değişik bir takım yöntemlerle bu LSP' lerden bir tanesi seçilir.
- Eğer paketin MPLS ağını belirli bir çıkış yönlendiricisi üzerinden terk etmesi gerektiği biliniyorsa, Konak Adresli FEC Elemanlarından adresi bu çıkış yönlendiricisinin adresi olan bir LSP bulunabiliyorsa paket bu LSP üzerinden aktarılır.

4.18.2. Etiket Uzayları

Etiket ataması ve dağıtımı konularını incelerken etiket uzaylarından bahsetmek yerinde olacaktır. İki türlü etiket uzayı bulunmaktadır:

- Her arabirim için bir etiket uzayı olabilir. Her arabirime özel giriş etiketleri tanımlanır. Buna örnek olarak VCI alanlarını etiket olarak kullanan ATM arabirimleri ya da DLCI alanlarını etiket olarak kullanan Frame Relay arabirimleri verilebilir. Ancak bu yöntem, LDP eşleri birbirleriyle belirli bir arabirim üzerinden doğrudan bağlıysa ve bu etiket sadece bu arabirim üzerinden akacak trafik için kullanılacak ise anlamlıdır.
- Her platform için bir etiket uzayı. Aynı etiketleri paylaşabilen arabirimler için "giriş etiketleri" platform bazındadır.

4.18.3. LDP Belirleyicileri

LDP belirleyicisi, bir etiket anahtarlamalı yönlendiricinin etiket uzayını belirtmek için kullanılan 6 sekizlik bir değerdir. İlk 4 sekizli LSR için atanan IP numarasını, diğer 2 sekizli ise LSR içindeki etiket uzayını belirler. Platform kapsamlı etiket uzaylarının kullanıldığı LSR' larda bu son iki sekizli sıfırdır. LDP belirleyicilerinin ifade biçimi şöyledir:

< IP adresi > : < etiket uzayı numarası >
Örneğin;
171.32.27.28:0 , 192.0.3.5:2

Birden fazla etiket uzayı kullanabilen LSR' ların her etiket uzayı için ayrı bir LDP belirleyicisi kullanmak zorunda olduğu unutulmamalıdır.

Bir LSR' ın LDP eşine birden fazla etiket uzayı kullandığını bildirmesi, yani birden fazla LDP belirleyicisi kullandığını belirtmesi gereken durumlardan birisi, bu LSR' ın LDP eşine iki bağlantısının olduğu ve bu iki bağlantının da ATM bağlantısı (her arabirim için bir etiket uzayının kullanıldığı) olduğu durumdur. Bir başka durum ise LSR' ın LDP komşusuna iki bağlantısının olduğu ve bu bağlantılardan biri ATM bağlantısı iken diğerinin ethernet (her platform için bir etiket uzayının kullanıldığı) bağlantısı olduğu durumdur.

4.18.4. LDP Oturumları

Etiket değiş – tokuşu için iki LSR arasında LDP oturumu bulunmalıdır. Bir LSR, kullandığı birden fazla etiket uzayını bir diğer LSR' a iletmek istiyorsa, kullandığı her bir etiket uzayı için ayrı bir LDP oturumu açmak zorundadır.

LDP protokolü, oturumların güvenilir bir şekilde çalışabilmesini sağlamak üzere TCP protokolünü kullanmaktadır. İki LSR arasında birden fazla LDP oturumu kurulması gerektiği durumlarda, her bir LDP oturumu için ayrı bir TCP oturumu kurulur.

Bazen, veri-bağı katmanında birbirlerin doğrudan bağlı olmayan iki LSR arasında bir LDP oturumu kurulmak istenebilir.

Örneğin, bir LSRa yönlendiricisinin, belirli bir trafiği, kendisine doğrudan bağlı olmayan bir LSRb yönlendiricisine, normal yönlendirmeli bir yoldan değil de aradaki bir LSP üzerinden göndermek istediği bir "trafik mühendisliği" uygulamasını ele alalım. LSRa ile LSRb arasında birçok ara LSR (LSR1, LSR2, ... LSRn) olabilir. Arada kurulacak bir

LDP oturumu ile LSRb'nin LSRa'ya etiketlerini gönderebilemesini ve bu sayede LSRa' dan gelen trafiğin LSRb tarafından etiket anahtarlamalı olarak aktarımı sağlanabilir.

Bu durumda LSRa, belirlenen bu LSP üzerinden LSRb' ye gönderdiği trafik için iki etiket kullanmalıdır: birincisi LSR1'den öğrenilen ve paketin LSRa ile LSRb arasındaki LSP üzerinden iletilmesi için gerekli olan etiket, diğeri ise LSRb'den öğrenilen ve LSRb' nin gelen bu LSP' den gelen trafiği etiket anahtarlamalı olarak iletebilmesi için gerekli olan etiket.

LSRa öncelikle LSRb' den LSRb ile kurduğu LDP oturumundan öğrendiği etiketi paketin etiket yığınının tepesine koyar. Daha sonra da paketi LDRa-LSRb arasındaki LSP' den iletmek için gerekli etiketi yığını tepesine koyar. [8]

4.19. MPLS'in Sağladığı Yararlar

Günümüzde IP çekirdek ağları kurmak için yaygın olarak kullanılan iki yöntem vardır:

i) Datagram yönlendirici temelli ağlar
ii) ATM çekirdek üzerinden iletişim yapan datagram yönlendiricilerden oluşmuş ağlar.

MPLS teknolojisinin yararlarını daha iyi anlatmak için şu anda kullanılmakta olan teknolojilerle karşılaştırmak faydalı olacaktır. Bunu yapabilmek için bu konu iki kısma ayrılmış bir tanesinde MPLS' in saf datagram yönlendirmenin yapıldığı bir ağa göre faydaları, diğerinde ise MPLS teknolojisinin ATM çekirdek üzerinden IP iletişiminin gerçeklendiği bir ağa göre faydaları anlatılmıştır.

4.19.1. MPLS'in Yönlendiricilerden Oluşmuş Bir Ağa Göre Yararları

4.19.1.1. Basitleştirilmiş Aktarma

Etiket anahtarlamalı paket aktarımı paketteki kısa bir etiket değeri kullanılarak yapılır. Oysa normal datagram yönlendirmesinde ise çok daha uzun adreslerin işlendiği en fazla

uyan algoritması çalıştırılmaktadır. Üstelik etiket anahtarlamada kullanılan MPLS başlıkları, IP gibi datagram protokollerinin kullandığı başlıklardan çok daha basittir. Bu ise aktarma işleminin MPLS teknolojisinde çok daha sade olduğunu ve yüksek hızlı MPLS yönlendiricilerinin daha kolay yapılabileceğini göstermektedir.

Datagram yönlendiricilerden çok daha hızlı aktarma yapabilen LSR' lar her ne kadar çok daha basit ve hızlı aktarma yapabiliyorsa da bu yönlendiricilerin kullanımı uygulama detaylarına bağlıdır. Örneğin hiyerarşi sınırları gibi ağın bazı kısımlarında (tünel sınırlarında vb. sınırlarda) yüksek hızlı IP datagram yönlendirmesi de gereklidir. Bu ise yüksek hızlı IP datagram yönlendirmesi yapabilen yönlendiricilerin gerçeklenmesini zorunlu kılmaktadır. Üstelik günümüzde birçok firma yüksek hızlarda IP paketi yönlendirmesi yapabilen yönlendiriciler üretmektedirler. Geliştirme çabaları sona erip bu yönlendiriciler tam olarak kullanılmaya başlanınca muhtemelen her bir paketin iletilmesinin maliyeti, toplam ekipman maliyeti yanında çok çok küçük kalacaktır.

Ancak günümüzde de MPLS' in getireceği basitleştirilmiş aktarma işleminin faydalarından yararlanabilecek yönlendiriciler bulunmaktadır. Hatta bazı yönlendiriciler ise MPLS teknolojisini sağlayacağı basitleştirilmiş aktarmadan yararlanmak üzere birtakım ek donanımlarla üretilmiştir.

4.19.1.2. Verimli Açık Yönlendirme

Açık yönlendirme ya da kaynaktan yönlendirme çok değişik amaçlar için kullanım alanına sahip güçlü bir tekniktir. Fakat, normal datagram yönlendirmesinde, her paketle birlikte paketin izleyeceği yolun tüm bilgisinin taşınmasının doğurduğu ek yük çok fazla olmaktadır.

MPLS teknolojisinde ise bu açık yönlendirme yani kaynaktan yönlendirme işlemi için gerekli olan ek bilgiler her paketle taşınmaz, sadece etiket anahtarlamalı yol – LSP – kurulurken taşınır, ve bir kez bu LSP kurulduktan sonra bu bilgilere ihtiyaç kalmaz. Bu ise açık yönlendirmenin MPLS teknolojisinde çok pratik olarak gerçeklenebildiğini göstermektedir. Üstelik MPLS teknolojisinde, kaynaktan yönlendirmede kullanılabilecek birkaç gelişmiş yönlendirme özelliğinin devreye alınmasını sağlanabilmektedir.

4.19.1.3. Trafik Mühendisliği

Trafik mühendisliği terimi, ağda belirli bazı bağlantılarda, yönlendiricilerde ve anahtarlardaki yığılmaları azaltmak ve buralardaki aşırı yükü diğerlerine dağıtmak üzere veri akışının geçtiği yolların yeniden seçilmesi işlemidir. Trafik mühendisliği, birden fazla alternatif ya da paralel yolun bulunduğu durumlarda çok önemlidir. İnternet dünyasında meydana gelen hızlı büyüme, bant genişliği isteklerinin de çok hızlı bir şekilde büyümesini ve bazı çekirdek ağların çok aşırı "dallanması" sonucunu doğurmuştur. Tüm bu gelişmeler ise geçtiğimiz birkaç yıl içerisinde trafik mühendisliğinin önemini çok daha arttırmıştır.

Günümüzde ATM üzerinden IP (IP Over ATM) tekniğini kullanan çekirdek ağlarda yaygın olarak, değişik bağlantılar üzerindeki trafikleri eşit bir şekilde dağıtmak üzere, PVC'lerin geçtikleri yollar elle ayarlanmaktadır. Yani günümüzün ATM üzerinden IP ağlarında trafik mühendisliği elle kontrol edilmektedir.

Datagram yönlendirmede trafik mühendisliğini gerçekleştirmek ise zor bir işlemdir. Bağlantı maliyetlerini belirleyerek bir anlamda trafik mühendisliği yapılabilir. Ancak bu işlemde de birçok sınırlama bulunmaktadır. Sadece düğümden – düğüme datagram yönlendirmesinde kullanılan bağlantı maliyetlerini belirlenmesi, iki nokta arasında çok fazla alternatif yolun bulunduğu bir ağda istenilen dengelemeleri sağlayamayacaktır.

MPLS teknolojisi ise herhangi bir giriş yönlendiricisinden ağa giren ve herhangi bir çıkış yönlendiricisinden ağdan çıkan bir akışı tek olarak tanımlayabilmektedir. Yani MPLS, her bir giriş – çıkış yönlendiricisi arasında akan trafiğin ölçülmesinde ve kontrol edilmesinde çok kullanışlı yöntemler sunmaktadır. Bir önceki konuda da anlatıldığı üzere MPLS' in çok daha basit ve verimli bir şekilde kaynaktan yönlendirme ya da açık yönlendirme sağlayabilme özelliği ile, bu giriş – çıkış düğümleri arasında akan akışın istenilen yoldan gitmesi düzenlenebilir.

MPLS' de trafik mühendisliğinin en zor yanı, her etiket anahtarlamalı yolun –LSP - yönlendirmesinin (LSP' nin hangi yönlendiricilerden geçeceği) nasıl olacağı sorusudur. Bunun için birden fazla yöntem vardır. Bu kararlar elle ayarlayarak verilebilir ya da arka planda çalışarak sürekli yolların maliyetlerini ve yoldaki trafik yoğunluğunu hesap edip alternatif yollar bulmaya çalışan yönlendirme protokolleri kullanılabilir.

4.19.1.4. QoS (Servis Kalitesine Göre) Yönlendirmeler

Servis kalitesine göre (QoS) yönlendirme işlemi, belirli bir akışın izleyeceği yolun seçilirken, o akışın gerektirdiği servis kalitelerini sağlayacak şekilde bir yolun seçilmesi anlamına gelir. Çok kere servis kalitesine göre yönlendirme, açık yönlendirmenin kullanılmasını gerektirir:

- Bazı durumlarda her bir veri akışı belirli bir band genişliğinin rezerve edilmesi ve bu aralığın sadece ilgili akış tarafından kullanılması istenilir. Bu şekilde birden fazla istek olduğu durumlarda, tüm akışların ihtiyaç duydukları toplam band genişliği, belirli iki düğüm arasındaki bağlantının kaldırabileceği toplam band genişliğinin üstünde olabilir ve böyle bir durumda ağa aynı giriş yönlendiricisinden giren ve ağdan aynı çıkış yönlendiricisinden çıkan akışların ağ içerisinde aynı yoldan iletilmesi mümkün olmamaktadır. Bunun için her bir akış, ayrı olarak yönlendirilmektedir. Bu işlem de bir anlamda trafik mühendisliği sayılmaktadır fakat akışların birbirlerinden çok dikkatli bir şekilde ayrılmasını gerektirmektedir. Her akışın ayrı olarak yönlendirilmesini sağlamak ve anahtarın tekrar ilgili akışın izleyeceği yolu yeniden belirlemesini önlemek için açık yönlendirme gereklidir.

Belirli bir band genişliğine gereksinim duyan bir akışın yönlendirilmesini gözönüne alalım. Bu durumda seçilecek yolun, bu belirli band genişliğini sağlayabilecek bir yol olması gerekecektir. Sadece belirli seviyelerde band genişliklerine ihtiyaç olsa bu yol seçme işlemi kolay olacaktır ancak kuramsal olarak ihtiyaç duyulabilecek band genişliği seviyeleri çok çeşitlilik göstermektedir. Bundan dolayı olası her band genişliği ihtiyacını karşılayabilecek yolların önceden belirlenmesi imkansızdır. Eğer belirli bir akışın

izleyeceği yolun belirlenmesi isteniliyorsa, yol üzerindeki her etiket anahtarlamalı yönlendiricisini – LSR' ın – bu hesabı tekrar yapması istenmez. Bunun yerine ilk düğümün bu hesabı bir kez yapması, daha sonra akışın iletileceği yolu belirlemesi ve artık kaynaktan yönlendirme ile bu akışı ilgili yoldan göndermesi yeğlenir.

Çeşitli nedenlerden dolayı bazen servis kalitesine göre yönlendirme yapmak için kullanılan birtakım bilgiler güncelliğini yitirmiş olabilir. Bu ise servis kalitesine duyarlı bazı akışların, izleyecekleri yoldaki bir düğümün ya da bağlantının gereksinim duyulan kaynakları karşılayamaması durumunda, iletilememesine yol açar. Buna benzer durumlarda, diğer ağ elemanlarına, ilgili ağ elemanının ihtiyaç duyulan gereksinimleri karşılayamadığını bildirmek her zaman mümkün olmayabilir. Ancak eğer kaynaktan yönlendirme kullanılıyorsa, ağdaki bir elemanın ilgili akışı taşıyamadığı bilgisi, o akışın ağa giriş yönlendiricisine ulaştırılabilir. Bu giriş yönlendiricisi de bunun üzerine yeni alternatif yollar aramaya başlayacaktır.

Bu ve buna benzer örnekler, iyi seviyede bir servis kalitesine göre (QoS) yönlendirme hizmeti vermek için kaynaktan yönlendirmenin mutlaka gerekli olduğunu göstermektedir. MPLS teknolojisinde açık yönlendirme işleminin çok verimli bir şekilde yapıldığı bilindiğine göre MPLS'in servis kalitesine göre yönlendirme hizmetleri vermek için çok uygun olduğu görülür.

4.19.1.5. Değişik Servis Düzeyleri Desteği

MPLS teknolojisi, aynı ağ üzerinde birden fazla servis tipi hizmeti vermeyi sağlamak üzere tek bir aktarım yöntemi kullanmaktadır. Kontrol amacıyla etiket anahtarlamalı yönlendiricilerin – LSR' ların – tabloları için kullanılan protokollerden bağımsız olarak sadece kullanılan aktarma yönteminden dolayı aynı ağ üzerinden çok değişik servislerin iletilmesi mümkün olmuştur. Örneğin bir ATM tabanlı ağda tüm ATM servisleri, frame relay servisleri ve etiketlenmiş IP servisleri için destek bulunmaktadır. Tüm bu servislere aynı anda hizmet verebilmek için tüm etiket uzayının servisler arasında paylaştırılması gerekebilir ve tüm bu servislere destek vermek amacıyla etiket dağıtım yönetimi protokolü kullanılabilir.

Etiket anahtarlamalı yönlendiriciler – LSR'lar- üzerinden aktarılması uygun olan bazı servisler şunlardır: IP trafiği, frame relay trafiği, ATM trafiği, IP tünelleme, sanal kurumsal ağlar (VPN'ler) ve diğer datagram protokolleridir.

İlgi çekici bir diğer nokta da MPLS teknolojisinin, tüm bu iletim ortamları için zorunlu olarak tek bir başlık gerektirmediğidir. Ancak gene de belirli bir iletim ortamı için geçerli olabilecek tek bir başlık formatı vardır.

4.19.2. MPLS'in ATM ya da Frame Relay Anahtarlarından Oluşmuş Bir Ağa Göre Faydaları

Bu kısım, MPLS' i, yönlendiricileri, anahtarlama temelli çekirdek ağlar üzerinden birbirlerine bağlayan diğer metodlarla karşılaştırmaktadır. Günümüzde yönlendiricileri birbirlerine bağlamak üzere ATM üzerinden IP türünde bir yapı kullanan metodlar şunlardır:

i) ATM ağına bağlanmış "n" adet yönlendirici için "n^2" tane sanal devre kullanarak yönlendiricileri birbirlerine bağlamak .
ii) Yönlendiriciler arasında "n^2" taneden daha az sayıda sanal devre (VC) kullanmak.
iii)Sadece bazı yönlendiriciler arasında sanal devrelerle bağlantı kurma (partial mesh) ile birlikte anahtarlamalı sanal devrelerin kullanımını sağlamak üzere NHRP protokolünün uygulanması.

4.19.2.1. Yönlendirme Protokolünün Ölçeklenebilirliği

Bir ATM çekirdek üzerinden yönlendiricilerin birbirlerine bağlandığı bir yapı ile karşılaştırıldığında MPLS, eşlerin sayısını azalttığı, yönlendirme protokollerinin düzgün çalışmasını sağlamak üzere kurulması gereken "n^2" tane sanal devreye (VC) olan ihtiyacı ortadan kaldırdığı için yönlendirme işleminin ölçeklenebilirliğini çok arttırmıştır.

Tüm etiket anahtarlamalı yönlendiriciler aynı standart protokolleri çalıştırdığı için birbirleri ile iletişimde olması gereken komşu yönlendirici sayısı, bir LSR' ın doğrudan bağlı olduğu LSR ve yönlendirici sayısına indirilmiştir. Diğer metodlarda ise anahtarlamalı 2. katman yolunun uçlarındaki birçok yönlendiricinin birbirleriyle iletişim kurması gerekmektedir. Bu şekilde iletişim kurulması gereken komşu sayısının azalmasının nedeni, sınırdaki etiket anahtarlamalı yönlendiricilerin, ağın sınırlarındaki diğer tüm etiket anahtarlamalı yönlendiriciler ile komşuluk kurmasının gerekmemesidir.

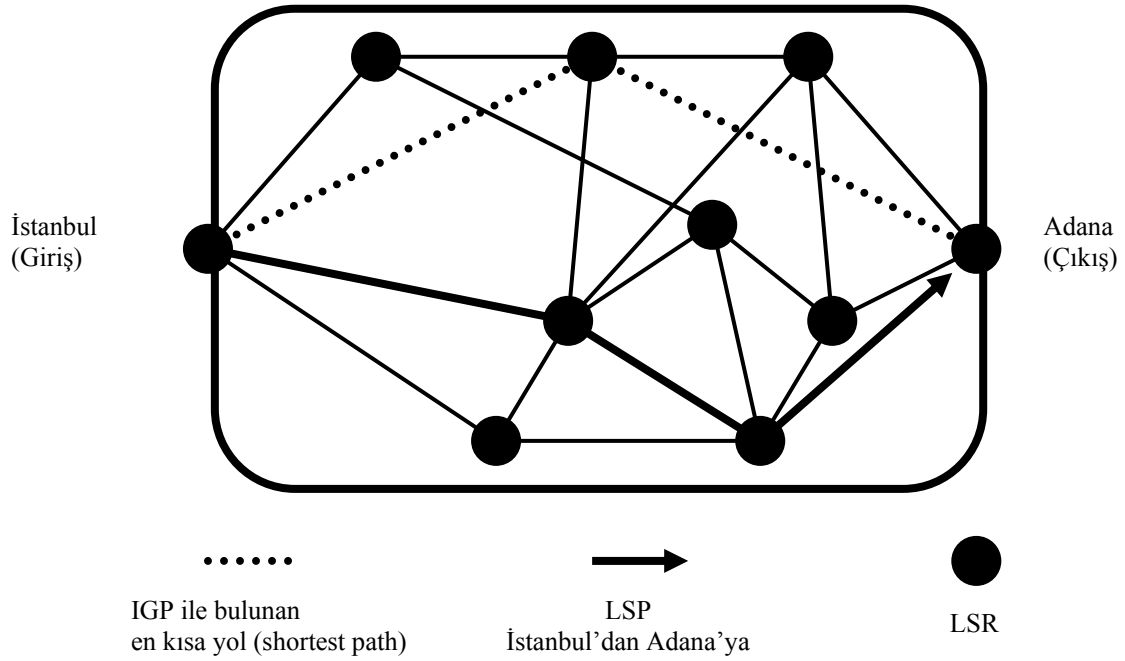
4.19.2.2. Ortak Özellikler – İşlemler

MPLS teknolojisi, paket ve hücre ortamları üzerinden ortak yönlendirme ve aktarma metodlarının kullanılmasını sağlamakta ve trafik mühendisliği, servis kalitesine göre QoS yönlendirme ve benzer diğer tüm konulara ortak bir bakış açısı getirmektedir. Bunun sonucu olarak örneğin, ATM ya da Frame Relay ağlarında veya özel MPLS başlığının (shim header) kullanıldığı noktadan noktaya (PPP) ve yerel ağlar (LAN's) gibi ağlarda aynı etiket dağıtım protokolünün kullanılması gösterilebilir.

4.20. MPLS' İ UYGULAMA YÖNTEMLERİ

4.20.1. Trafik Mühendisliği

Trafik mühendisliği yaygın olarak internet servis sağlayıcıları tarafından, ağlarından akan trafiği, Şekil 4.4' deki gibi IGP protokolü tarafından hesaplanan en kısa yoldan farklı bir yol üzerinden ve potansiyel olarak daha az yığılma olabilecek yollardan akmasını sağlamak üzere kullanılmaktadır. Trafik mühendisliği hali hazırda MPLS için en yaygın uygulama alanıdır. Bunun sebebi olarak da ağ kaynaklarında meydana gelen önceden tahmin edilmesi çok güç gelişmelerin olması, IP uygulamalarının kritik görevler yüklenmesi ve servis sağlayıcılar pazarında hızla büyüyen rekabet ortamı gösterilmektedir. Başarılı bir trafik mühendisliği çözümü ağın toplam trafik yükünü tüm bağlantılar, yönlendiriciler ve anahtarlar üzerinde dengeli bir şekilde dağıtmalı ve ağ bileşenlerinden hiçbirinin kapasitesinin çok altında ya da çok üstünde çalışmamasını sağlamalıdır. Bu sayede ağın performansı yükseltilebilir ve önceden tahmin edilebilir servisler sunulabilir.



Şekil 4.4 – MPLS ile trafik mühendisliği uygulaması

MPLS'in büyük internet servis sağlayıcılarının ağlarında trafik mühendisliği uygulamaları geliştirmek için kullanılmasının uygun olmasının nedenleri şunlardır:

- MPLS'in açık (kaynaktan - explicit) yönlendirmeye verdiği destek. Bir akışa ait paketlerin, servis sağlayıcının ağında fiziksel olarak hangi yolu izleyerek gideceğinin, ağ yöneticileri tarafından belirlenebilmesi imkanı.

- Her LSP bazında tutulan istatistiklerin ileriye dönük planlamalar yapmak, darboğazların belirlenebilmesine yardımcı olmak üzere ağ planlama ve ağ analizi araçlarına girdi olarak kullanılabilmesi.

- Belirli kriterlere göre yönlendirme yaparak bazı etiket anahtarlamalı yolların - LSP' lerin – ihtiyaç duyulan performans gereksinimlerine cevap verecek şekilde kurulmasını sağlayabilme.

- MPLS tabanlı bir çözümün paket tabanlı ağlarda da çalışabilmesi, sadece ATM altyapısı üzerinde çalışacak şekilde sınırlı olmaması.

4.20.2. Servis Sınıfları (CoS)

İnternet servis sağlayıcılarının, farklılaştırılmış hizmetler için destek vermeleri arttıkça MPLS' in getireceği faydalar da artacaktır. Farklılaştırılmış hizmetler modeli, tüm trafiği küçük bazı servis sınıflarına dağıtmak için çeşitli mekanizmalar tanımlar. Müşteriler, interneti kendi kurumsal ağları gibi, klasik dosya transferinden ses ve video gibi gecikmeye duyarlı uygulamalar benzeri çok değişik servislerden faydalanmak için kullanırlar. İnternet servis sağlayıcıları da müşterilerinin isteklerini karşılamak üzere sadece trafik mühendisliği tekniklerini değil aynı zamanda trafik sınıflandırma tekniklerini geliştirmelidir.

Bir internet servis sağlayıcısı MPLS tabanlı servis sınıfları desteği verecekse bunu iki yaklaşımla yapabilir:

1) MPLS başlığında taşınan öncelik değerine göre etiket anahtarlamalı yönlendiricinin LSR' ın- çıkış arabiriminde paketler, belirli bir etiket anahtarlamalı yoldan –LSP' den- akan trafiğe iletilmek için kuyruğa alınabilir.
2) Bir İSS (İnternet Servis Sağlayıcı) ağ sınırındaki her etiket anahtarlamalı yönlendirici arasında birden fazla etiket anahtarlamalı yol LSP kurabilir. Her etiket anahtarlamalı yol (LSP) de değişik band genişliklerini ve değişik performans kriterlerini sağlayacak şekilde ayarlanabilir. Giriş yönlendiricisi yüksek öncelikli bir trafiği belirli bir etiket anahtarlamalı yol (LSP), orta derecede öncelikliğe sahip trafiği ise bir başka LSP, elden gelenin en iyisi şeklinde bir aktarımı kabul edebilen bir trafiği üçüncü bir LSP, elden gelenin en iyisinden daha da az önceliğe gereksinim duyan bir trafiği de dördüncü bir LSP üzerinden aktarabilir.

MPLS teknolojisi bir internet servis sağlayıcısına, müşterilerine sunduğu servis tiplerini kullanmada mükemmel bir esneklik sağlar. Her paketteki öncelik bitleri, sadece paketlerin değişik servis sınıflarından bir tanesine dahil edilmesi için kullanılır. Her servis sınıfınında desteklenecek servislerin neler olduğu servis sağlayıcı tarafından belirlenmektedir.

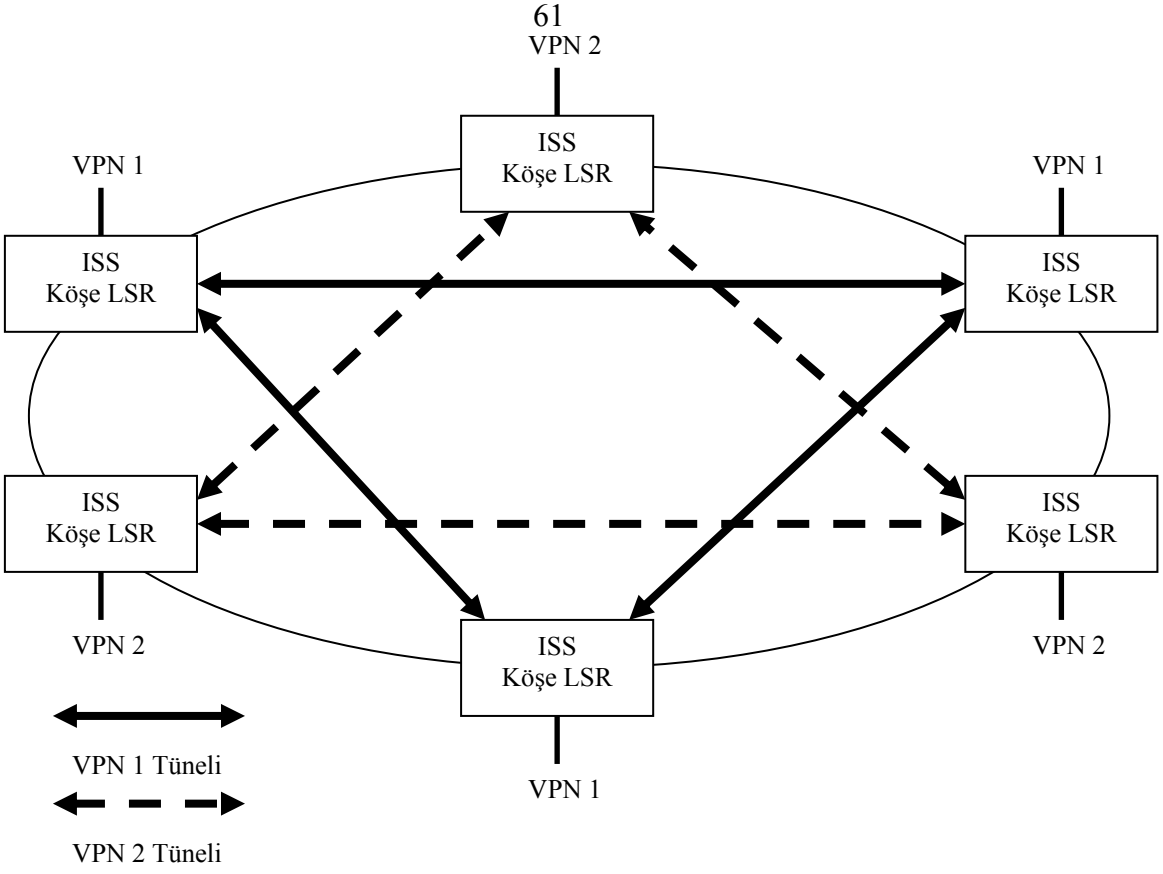
4.20.3. VPN (Virtual Private Network)

Sanal kurumsal ağlar, kamusal olan internet ağı üzerinden kurumsal geniş alan ağlarının (private wide area network WAN) kullanımını benzetimini gerçekleştirmektedir. Bir internet servis sağlayıcısı müşterilerine pratik sanal kurumsal ağ (VPN) hizmetleri vermek isterse veri güvenliğini sağlamalı ve VPN' de farklı ve sabit IP adreslerinin kullanımına destek vermelidir. MPLS teknolojisi ise bu iki gereksinmeye en iyi şekilde cevap verebilmektedir çünkü MPLS' de aktarma işlemi kararları, paket başlığındaki varış adresine göre değil, paketin etiketine göre verilmektedir.

Sanal kurumsal ağlar (VPN'ler) temel olarak aşağıdaki 4 yapıtaşının gerçeklenmesi ile kurulurlar:

- Her müşterinin ağını koruyacak ve internet ile güvenli bir arabirim oluşturacak Güvenlik Duvarları.
- Her bir müşteri ağının sadece izin verilen diğer ağlarla veri haberleşmesini sağlamak üzere yetkilendirme işlemleri.
- Verinin, internette dolaşırken okunup değiştirilmesini engellemek üzere şifreleme mekanizmaları.
- Çok katmanlı iletişim servislerini kullanabilmek ve VPN içerisinde yöresel anlamlı IP adres uzayları kullanılmasına olanak vermek için "Tünelleme" işlemi.

MPLS, internet servis sağlayıcılarına basit, esnek ve güçlü bir tünelleme mekanizması sağlayarak, ISS'lere VPN servisleri hizmetleri verme imkanını sunmaktadır.



Şekil 4.5 – MPLS ağında VPN ağların kullanılması

Şekil 4.5'de de görüldüğü üzere internet servis sağlayıcısı VPN' deki değişik ağ parçalarını (site) birbirlerine bağlamak üzere bir etiket anahtarlamalı yol LSP kümesi kurmalıdır. Bu bağlantılar kurulduktan sonra her ağ parçası, kendi içerisinde ulaşılabilir olan IP öneklerini servis sağlayıcıya bildirir. Servis sağlayıcının yönlendirme sistemi de bu bilgileri ya etiket dağıtım protokolü – LDP - aracılığı ile ya da yönlendirme protokolü güncellemeleri ile ağ içerisinde dağıtır. Sanal kurumsal ağ belirteçleri ile tek bir yönlendirme sistemi kullanılarak, kendi içerisinde aynı adres uzaylarını kullanan birden fazla değişik sanal kurumsal ağa (VPN) destek verilebilir. Her giriş etiket anahtarlamalı yönlendiricisi – LSR – kendilerine gelen trafiği, paketlerin varış adreslerini ve hangi VPN' e ait oldukları bilgilerini kullanarak farklı etiket anahtarlamalı yollar – LSP – üzerinden aktarırlar.

5. UYGULAMALAR

Uygulama bölümü 3 uygulama şeklinde hazırlanmış olup, servis sağlayıcılar için önem taşıyan MPLS ile trafik mühendisliği ve MPLS VPN üzerinde durulmuştur. Uygulamalarda kullanılan cihazların marka ve modeli çok önemli olmamakla birlikte, buradaki mimariler için kullanılan cihazlar, servis sağlayıcılarının omurgalarında ve POP noktalarında sıklıkla kullandıkları Juniper ailesinden seçilmiştir.

Aşağıda Uygulama kapsamında kullanılan cihazların üzerinde kullandıkları arabirimler hakkında kısa bir bilgi verilmiştir.

Juniper M7i Yönlendiriciler : Üzerinde iki adet Fast Ethernet arabirimi olan üç adet yönlendirici kullanılmıştır.

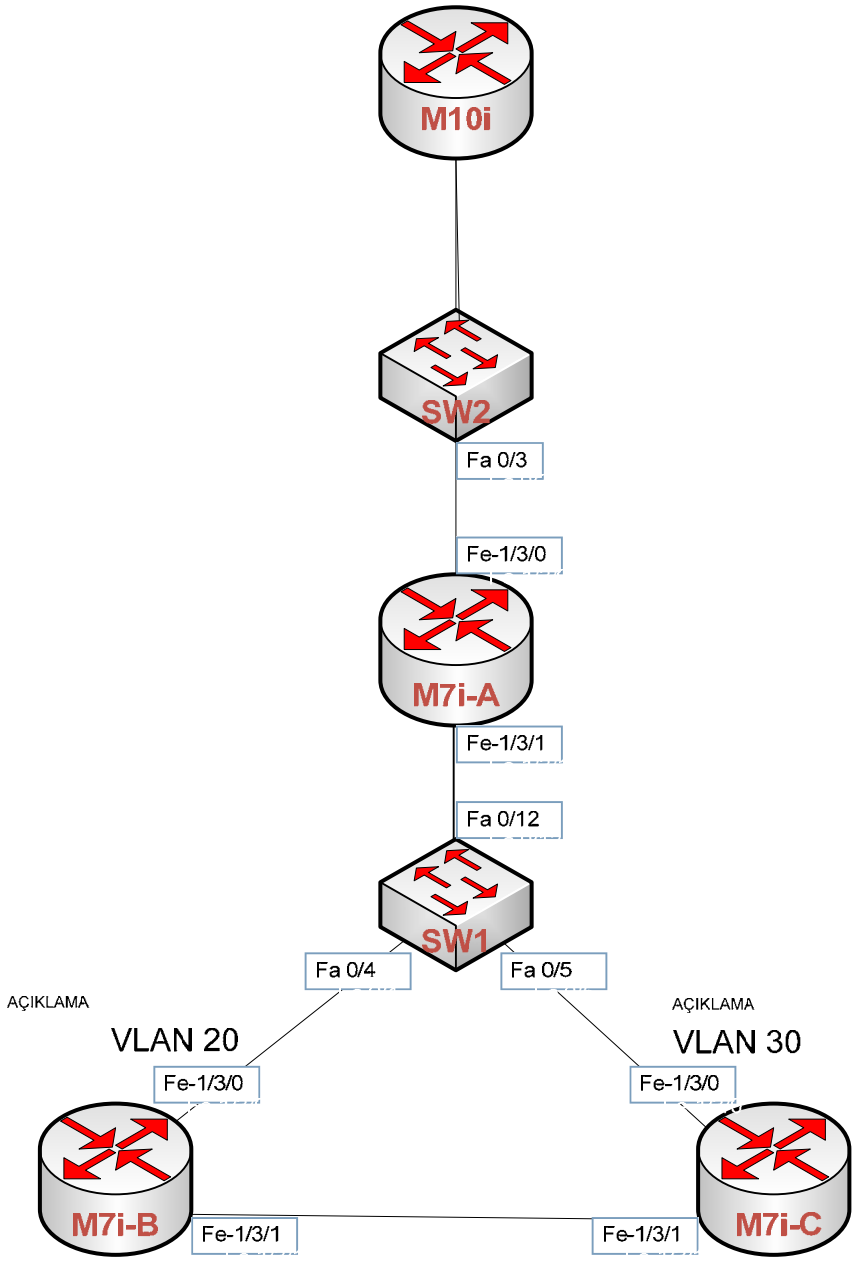
Cisco 2950 Switch : Üzerinde 12 adet port olan ve Vlan oluşturma özelliğine sahip Layer 2 switch kullanılmıştır.

5.1. UYGULAMA 1 : MPLS KULLANMADAN YÖNLENDİRME PROTOKOLLERİ İLE AĞIN ÇALIŞTIRILMASI VE GÖZLEMLENMESİ

MPLS ile ilgili uygulamalara başlamadan önce ilk olarak uygulama kapsamında kullanacağımız cihazların elektriklerinin verilmesi, birbirlerine bağlanması, MPLS kurulmadan önceki aşama olan temel konfigürasyon ve bir dinamik yönlendirme protokolü vasıtasıyla sistemin yani ağın çalışılabilir ve kullanılır hale getirilmesi gerçekleştirilmiştir.

Şekil 5.1’ de kurulmuş olan ağın fiziksel bağlantıları ve arayüzlerin birbirine ne şekilde bağlı oldukları gösterilmiştir. Burada M7i-A, M7i-B ve M7i-C isimli yönlendiriciler ve SW1 isimli anahtar, uygulamayı üzerinde gerçekleştirmiş ve konfigürasyon yapmış olduğumuz cihazlar olup, M10i ve SW2 ise sadece diğer cihazlara internetten uzaktan erişim imkanı sağlaması açısından Şekil 5.1’ de gösterilmiş servis sağlayıcısına ait cihazlardır. Bunlar üzerinde herhangi bir erişim hakkımız bulunmasa da bu cihazlar

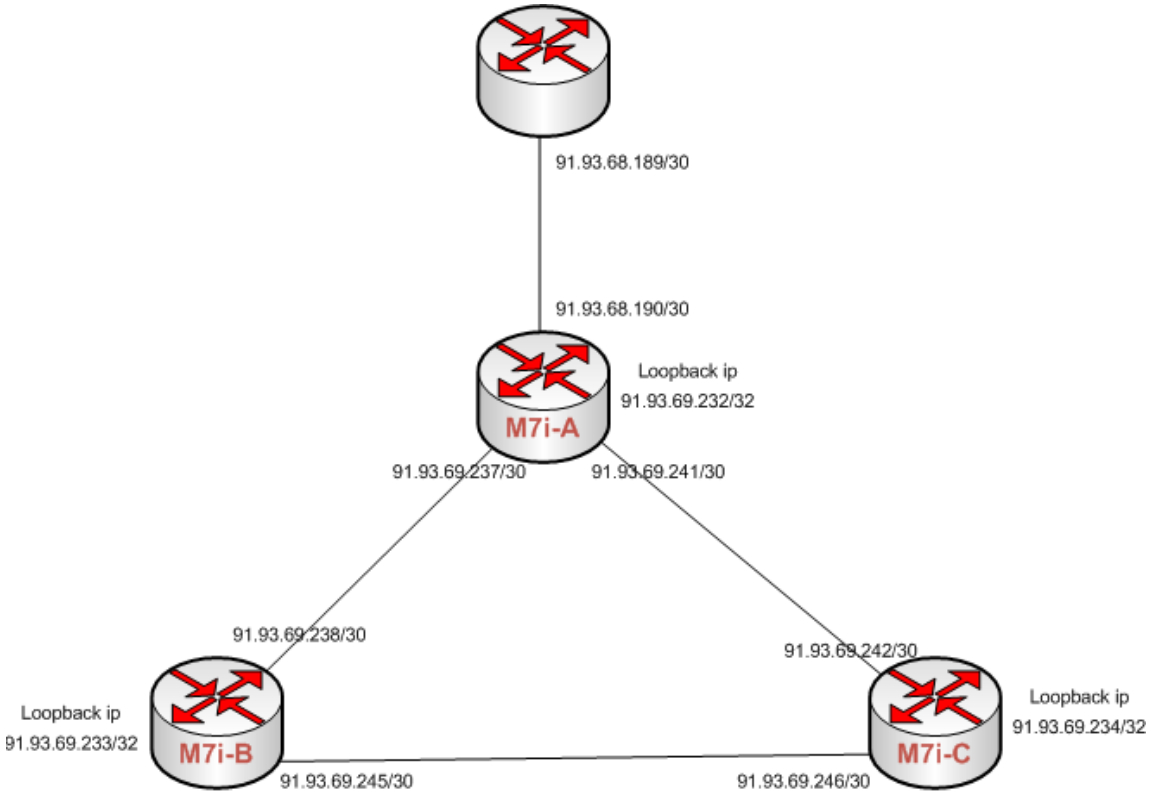
üzerinde sadece statik bir yönlendirme yazılarak, uygulama kapsamında kullanılan cihazlara erişim sağlanmıştır.



Şekil 5.1 – Oluşturulan uygulamanın fiziksel gösterilişi

Uygulamadaki amaç M7i-A, M7i-B ve M7i-C isimli üç adet yönlendiriciyi hepsi birbirine seri olarak bağlanmak koşulu ile mesh bir topoloji yaratıp böylelikle yönlendiricilerin paketleri taşırken aralarında yedekli bir yapı oluşturulması sağlanmaktır. Şekil 5.1 'deki şeklin mantıksal izdüşümü Şekil 5.2' de gösterilmiştir.

Şekilde görüldüğü gibi M7i-A üzerinde üç adet arayüz bulunmadığından araya SW1 konulmuş ve M7i-B ve M7i-C' ye bağlı bacaklarında iki adet VLAN oluşturularak bu farklı ağların M7i-A üzerindeki tek bir arayüz üzerinden birbirlerine mesh yapı ile bağlanması sağlanmıştır.



Şekil 5.2 – Oluşturulan uygulamanın mantıksal gösterilişi

Uygulamanın bundan sonraki kısımlarında SW1 anahtarını arada yokmuş gibi düşünülmesi uygulamalarda asıl yapılmak istenen MPLS uygulaması için daha verimli olacaktır. Buradaki anahtarların asıl görevi sanal ağlar yaratıp yönlendiricileri birbirine mesh bir yapı ile bağlayabilmek ve SW1 üzerinde yapılan monitor ayarı ile paketleri görüntülemek amacı ile bilgisayarımızı SW1'e bağlamak olmuştur.

Aşağıda SW1 üzerinde yapılmış olan konfigürasyon gösterilmiştir ve konfigürasyon içinde bizim için önemli olan kısımları koyu renk ile belirtilmiş ve açıklamaları yapılmıştır :

SW1#sh run
Building configuration...

Current configuration : 1171 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname SW1
!
enable password 7 09584B051C111219
!
ip subnet-zero
!
vtp mode transparent
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
!
!
vlan 20,30 ---------- Oluşturulan VLAN'lar
!
interface FastEthernet0/1
!
interface FastEthernet0/2

```
!
interface FastEthernet0/3
!
interface FastEthernet0/4 ----------------------------------
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/5 ----------------------------
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12 ----------------------------------
 switchport mode trunk
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan30 ----------------------------------------
 ip address 192.168.30.3 255.255.255.0
```

M7i-B' nin bağlı olduğu port burada M7i-B için VLAN 20 oluşturulmuş ve Fa0/4 portuna bağlanmıştır.

M7i-C' nin bağlı olduğu port burada M7i-C için VLAN 30 oluşturulmuş ve Fa0/5 portuna bağlanmıştır.

M7iA' nin bağlı olduğu port burada M7i-A için VLAN trunk oluşturulmuş, 2 VLAN' dan da gelen bilgileri alması sağlanmış ve Fa0/12 portuna bağlanmıştır.

SW1'in üzerinde oluşturulan herhangi bir Vlan' ına İp verilerek uzaktan da ulaşalabilmesi sağlanmıştır.

no ip route-cache

!

ip default-gateway 192.168.30.1

ip http server

!

line con 0

line vty 0 4

password 7 06120A2D495A0C12 ----------

Telnet sırasında şifre sorması için girilmiştir.

login

line vty 5 15

login

!

!

!

monitor session 1 source interface Fa0/4 – 5 ----------

monitor session 1 destination interface Fa0/11

Burada amaç M7i-A ve B' ye bağlı 0/4 ve 0/5 portlarından geçen paketleri kendi bilgisayarımızda görebilmek için 0/11 'inci porta , monitor işlemi ile yönlendirme yapılmıştır.

end

Bundan sonra ki aşama yönlendiricilerin arayüzlerine gerekli IP adreslerini vermek ve üzerlerinde bir yönlendirme protokolü olan OSPF' i çalıştırarak sistemin çalışması test edilmiştir. Şekil 5.2'de yönlendiricilerin arayüzüne verilen IP'ler gösterilmiştir. Şekil 5.2' den yola çıkarak, yönlendiricilerin bu aşamada üzerlerinde olan konfigürasyonu aşağıda verilmiş ve önemli kısımlarının açıklamaları yanında yapılmıştır:

teletek@M7i-A> show configuration

version 7.2R1.7;

system {

host-name M7i-A;

login {

user teletek {

uid 1903;

class super-user;

```
        authentication {
            encrypted-password "$1$/unJX2yi$Aae95btJIHSD72zRm9raV0"; ##
SECRET-DATA
        }
    }
  }
  services {
    ftp;
    telnet;
  }
}
interfaces {
  fe-1/3/0 {          ------------------------------------
    unit 0 {
      family inet {
        address 91.93.68.190/30;
      }
    }
  }
  fe-1/3/1 {
    vlan-tagging;
    unit 0 {          ------------------------------------
      vlan-id 20;
      family inet {
        address 91.93.69.237/30;

    }
    unit 1 {          ------------------------------------
      vlan-id 30;
      family inet {
        address 91.93.69.241/30;
        address 192.168.30.1/24;
```

M7i-A' nın M10i' ye bağlı olan arayüzünün tanımı ve verilen IP

M7i-A' nın M7i-B' ye bağlı olan arayüzünün tanımı ve verilen IP

M7i-A' nın M7i-C' ye bağlı olan arayüzünün tanımı ve verilen IP

```
        }
    }
    lo0 {                    ------------------------------------
        unit 0 {
            family inet {
                address 91.93.69.232/32;
            }
        }
    }
}
snmp {
    community teletek123 {
        authorization read-only;
        clients {
            84.51.14.166/32;
            84.51.14.210/32;
        }
    }
    trap-options {
        source-address lo0;
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 91.93.68.189;
    }
}
protocols {
    ospf {                   ------------------------------------
        area 0.0.0.0 {
            interface fe-1/3/1.0;
            interface fe-1/3/1.1 {
                metric 3;
```

M7i-A' nın loopback' i ve verilen IP

M7i-A üzerinde yapılan OSPF konfigürasyınu

```
        }
      }
   }
}
```

M7i-B'nin konfigürasyonu:

```
teletek@M7i-B> show configuration
version 7.6R4.3;
system {
   host-name M7i-B;
   root-authentication {
      encrypted-password "$1$baSIyn0E$Azj8UzS8vro7Z2bxv.Zkr0"; ## SECRET-
DATA
   }
   login {
      user teletek {
         uid 1903;
         class super-user;
         authentication {
            encrypted-password "$1$G21n8Lhc$ZXfiGNAItebLsCyT4UfWc0"; ##
SECRET-DATA
         }
      }
   }
   services {
      ftp;
      telnet;
   }
}
interfaces {
```

M7i-B' nın M7i-A' ye bağlı olan arayüzünün tanımı ve verilen IP

```
    fe-1/3/0 {          ------------------------------------
        unit 0 {
            family inet {
                address 91.93.69.238/30;
    }
    fe-1/3/1 {          ------------------------------------   M7i-B' nın  M7i-C' ye bağlı olan
                                                               arayüzünün tanımı ve verilen IP
         unit 0 {
            family inet {
                address 91.93.69.245/30;
        }
    }
    lo0 {
        unit 0 {            ------------------------------------   M7i-A' nın  loopback' i ve verilen IP
            family inet {
                address 91.93.69.233/32;
            }
        }
    }
}
snmp {
    community teletek123 {
        authorization read-only;
        clients {
            84.51.14.166/32;
            84.51.14.210/32;
        }
    }
    trap-options {
        source-address lo0;
    }
}
routing-options {
    static {
```

```
      route 0.0.0.0/0 next-hop 91.93.69.237;
   }
}
protocols {
   ospf {          ----------                                    M7i-B üzerinde yapılan OSPF
                                                                 konfigürasyınu
      area 0.0.0.0 {
         interface fe-1/3/0.0;
         interface fe-1/3/1.0;
      }
```

M7i-C' nin konfigürasyonu :

```
teletek@M7i-C>show configuration
version 7.6R4.3;
system {
   host-name M7i-C;
   root-authentication {
      encrypted-password "$1$INl9Z/KC$7XfU.mB2Kez7OBZLjNAJv."; ## SECRET-
DATA
   }
   login {
      user teletek {
         uid 1903;
         class super-user;
         authentication {
            encrypted-password "$1$jhIMoU/h$8u12q0tbaxLLUZE/IFsfV1"; ##
SECRET-DATA
         }
      }
   }
   services {
      ftp;
      telnet;
   }
```

```
}
interfaces {
   fe-1/3/0 {        ------------------------------------
      unit 0 {
         family inet {
            address 91.93.69.242/30;
      }
   }
   fe-1/3/1 {        ------------------------------------
      unit 0 {
         family inet {
            address 91.93.69.246/30;
      }
   }
   lo0 {             ------------------------------------------
      unit 0 {
         family inet {
            address 91.93.69.234/32;
         }
      }
   }
}
snmp {
   community teletek123 {
      authorization read-only;
      clients {
         84.51.14.166/32;
         84.51.14.210/32;
      }
   }
   trap-options {
      source-address lo0;
   }
```

M7i-C' nın M7i-A' ye bağlı olan arayüzünün tanımı ve verilen IP

M7i-C' nın M7i-B' ye bağlı olan arayüzünün tanımı ve verilen IP

M7i-C' nın loopback' i ve verilen IP

```
}
routing-options {
   static {
      route 0.0.0.0/0 next-hop 91.93.69.245;
   }
}
protocols {    ----------
   ospf {
      area 0.0.0.0 {
         interface fe-1/3/1.0;
         interface fe-1/3/0.0;
```

M7i-C üzerinde yapılan OSPF konfigürasyınu

Gerekli tanımlar yapıldıktan sonra konfigürasyonun istendiği şekilde çalışmaya başlandığı gözlenmiştir. Buna değinecek olursak, bu durumda arayüzler birbirlerine ulaşabilmekte ve OSPF üzerinden yönlendirme tablolarını oluşturmuşlardır. Dışarıdan yönlendirici üzerinde ki ve aynı zamanda sistem içindeki tüm ağlara erişim tam olarak sağlanmıştır. Aşağıda M7i-A' dan alınan ping sonuçları verilmiştir:

```
teletek@M7i-A> ping 91.93.69.238
PING 91.93.69.238 (91.93.69.238): 56 data bytes
64 bytes from 91.93.69.238: icmp_seq=0 ttl=64 time=0.888 ms
64 bytes from 91.93.69.238: icmp_seq=1 ttl=64 time=0.918 ms
64 bytes from 91.93.69.238: icmp_seq=2 ttl=64 time=0.875 ms
64 bytes from 91.93.69.238: icmp_seq=3 ttl=64 time=0.921 ms
^C
--- 91.93.69.238 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.875/0.901/0.921/0.020 ms

teletek@M7i-A> ping 91.93.69.242
PING 91.93.69.242 (91.93.69.242): 56 data bytes
64 bytes from 91.93.69.242: icmp_seq=0 ttl=64 time=0.856 ms
64 bytes from 91.93.69.242: icmp_seq=1 ttl=64 time=0.913 ms
64 bytes from 91.93.69.242: icmp_seq=2 ttl=64 time=0.942 ms
```

--- 91.93.69.242 ping statistics ---
4 packets transmitted, 3 packets received, 25% packet loss
round-trip min/avg/max/stddev = 0.856/0.904/0.942/0.036 ms

Görüldüğü gibi iki yönlendiriciye de ulaşım sağlanıyor. Aynı zaman da yine A yönlendiricisi üzerindeki yönlendirme tablosu aşağıdaki gibi görülmektedir.

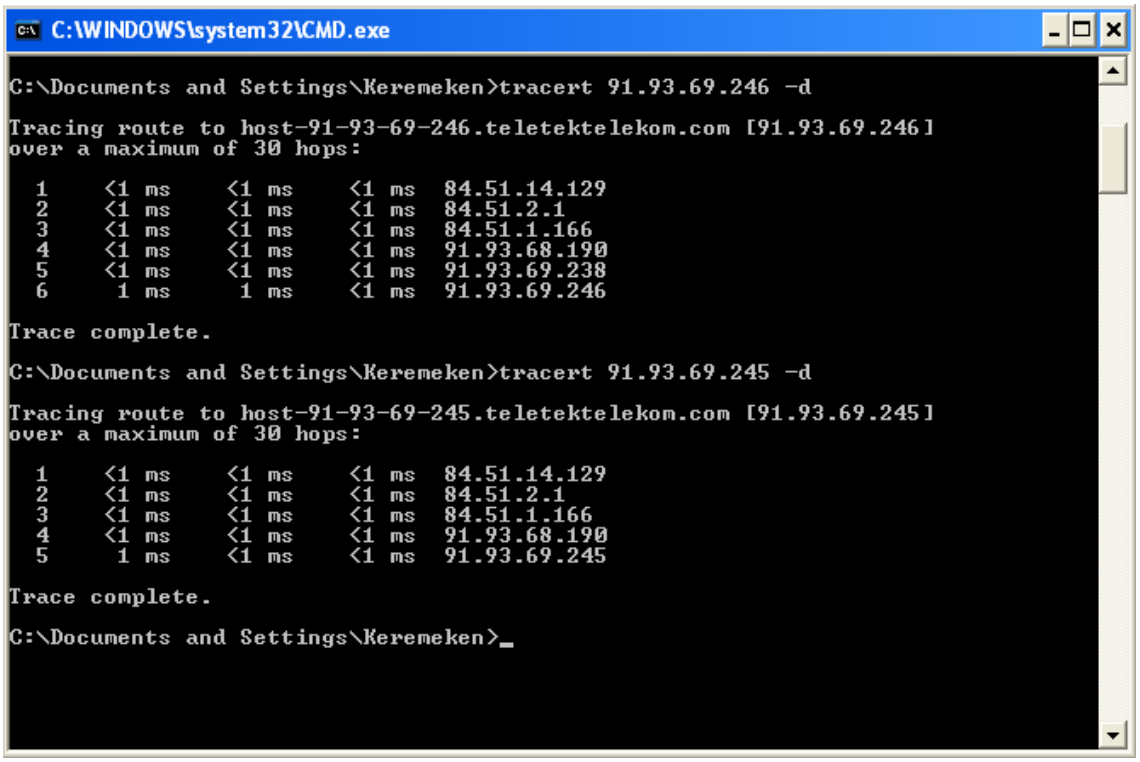
teletek@M7i-A> show route table inet.0

inet.0: 14 destinations, 15 routes (14 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0 *[Static/5] 3d 03:27:04
> to 91.93.68.189 via fe-1/3/0.0
91.93.68.188/30 *[Direct/0] 3d 04:23:42
> via fe-1/3/0.0
91.93.68.190/32 *[Local/0] 3d 04:23:42
Local via fe-1/3/0.0
91.93.69.232/32 *[Direct/0] 06:32:33
> via lo0.0
91.93.69.233/32 *[OSPF/10] 00:00:16, metric 1
> to 91.93.69.238 via fe-1/3/1.0
91.93.69.234/32 *[OSPF/10] 00:00:16, metric 2
> to 91.93.69.238 via fe-1/3/1.0
91.93.69.236/30 *[Direct/0] 04:55:50
> via fe-1/3/1.0
91.93.69.237/32 *[Local/0] 04:55:50
Local via fe-1/3/1.0
91.93.69.240/30 *[Direct/0] 04:49:48
> via fe-1/3/1.1
[OSPF/10] 00:00:16, metric 3
> to 91.93.69.238 via fe-1/3/1.0

91.93.69.241/32 *[Local/0] 04:49:48
Local via fe-1/3/1.1
91.93.69.244/30 *[OSPF/10] 00:00:16, metric 2
> to 91.93.69.238 via fe-1/3/1.0
192.168.30.0/24 *[Direct/0] 04:45:38
> via fe-1/3/1.1
192.168.30.1/32 *[Local/0] 04:45:38
Local via fe-1/3/1.1
224.0.0.5/32 *[OSPF/10] 3d 03:22:23, metric 1
MultiRecv

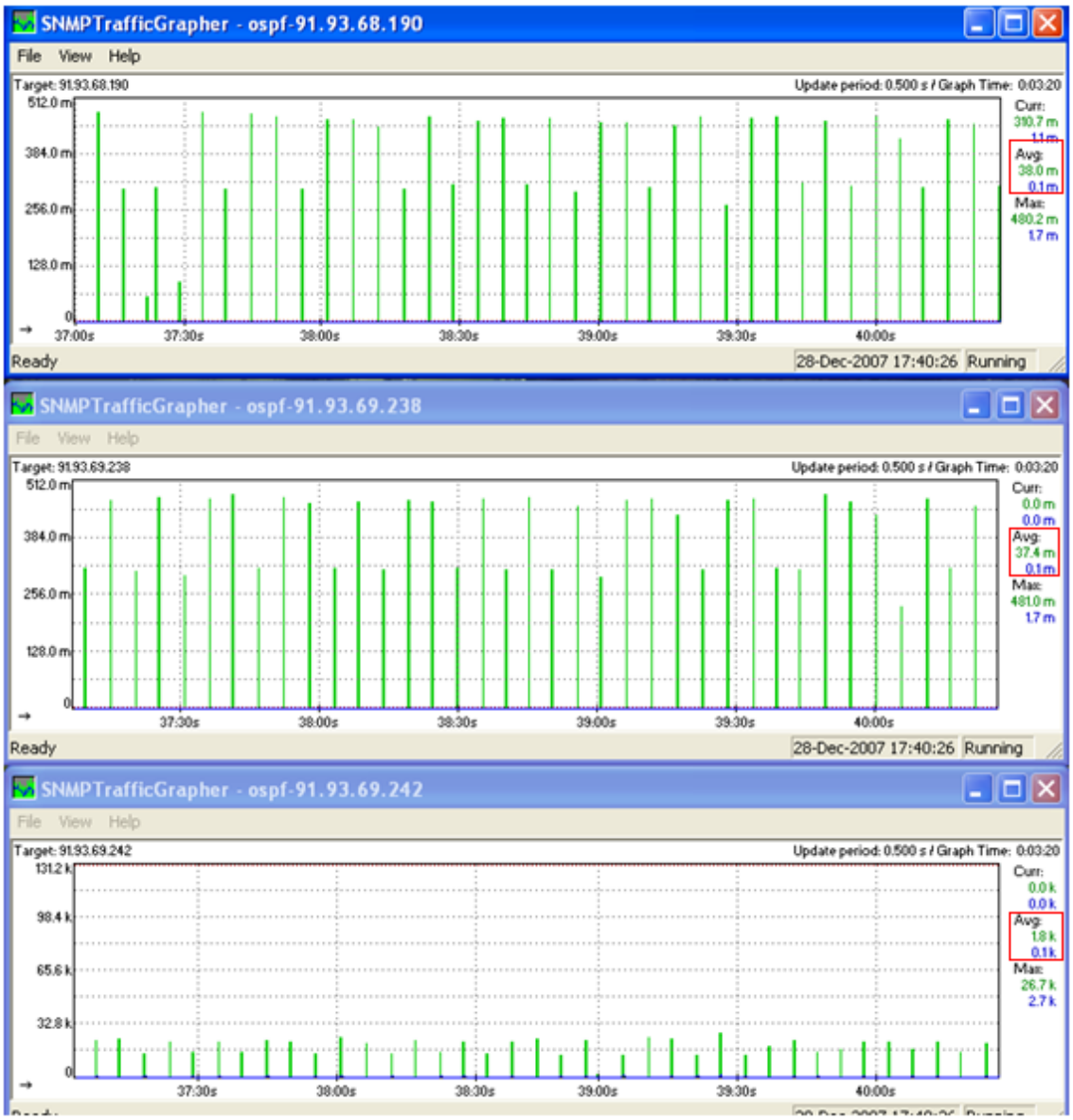
Burada dikkat edilmesi gereken nokta, A yönlendiricisinin **91.93.69.244/30** ağına yani B yönlendiricisi ile C yönlendiricisi arasındaki bağlantı, OSPF üzerinden öğrendiği daha iyi metrikli bir yol olan **fe-1/3/1.0 arayüzünün** üzerindeki **91.93.69.238** no'lu IP yolundan erişim sağlamaktadır. Bunun alternatifi olan **91.93.69.242** no'lu IP üzerinden geçen yol ise yönlendirme tablosunda gözükmeyip, kullanılmamaktadır. Şekil 5.2' ye dikkat edildiğinde gözlem daha kolay yapılacaktır. Dikkat edildiği takdirde yönlendirme tablosu üzerinde hiçbir **91.93.69.242** no'lu IP üzerinden OSPF'den öğrenilmiş bir yönlendirme de görülmemektedir. Bunun sebebi OSPF' in metrik değerini daha iyi gördüğü 91.93.69.238 numaralı yolu her zaman tercih etmek istemesidir. Bunun sonucunda ise ağ üzerinde 91.93.69.244/30 ağına ulaşmak isteyen her paket A yönlendiricisinin, B yönlendiricisine bakan yol üzerinden hedefine ulaşacaktır. Resim 5.1' deki trace sonuçlarından bu daha da iyi görülmüştür. Görüldüğü gibi B ile C yönlendiricisi arasındaki ağda bulunan iki IP olan 91.93.69.245 ve 91.93.69.246' ya aynı yoldan gidilerek yani 91.93.69.238 IP' si üzerinden ulaşılmıştır.



Resim 5.1 - OSPF çalışan ağ üzerinde alınan trace sonuçları

Aynı sonucu gözlemlemek için hatlar üzerindeki trafiği de takip etmek doyurucu sonuçlar vermiştir. Bu aşamada üç noktada yönlendiriciler üzerinde tanımlanan SNMP tanımları ve bilgisayara yüklenen trafik görüntüleme programı sayesinde yönlendiricinin o arayüzü üzerinden geçen trafiğin gözlemi yapılmıştır. Hatlar üzerinde trafik yaratmak için ise Wan Killer isimli başka bir program kullanılmıştır.

Burada gözlemi yapılan 3 noktadan birincisi tüm trafiğin geldiği M7i-A üzerindeki IP' si 91.93.68.190 olan fe-1/3/0 bacağı, ikincisi M7i-A' dan M7i-B' ye gelen trafiği görüntülemek için kullanmış olduğum M7i-B üzerindeki IP' si 91.93.69.238 olan fe-1/3/0 bacağı ve son olarak üçüncüsü M7i-A' dan M7i-C' ye gelen trafiği görüntülemek için kullanacağım M7i-C üzerindeki IP' si 91.93.69.242 olan fe-1/3/0 bacağı olmuştur. Şekil 5.3' de bu üç noktada gözlemlenen trafiğin grafiksel olarak görünümü gösterilmiştir.



Şekil 5.3 - OSPF üzerinden akan trafiğin gözlemlenmesi

Şekil 5 n trafikle, 91.93.69.238 no' lu IP olan M7i-B üzerinden geçen trafiğin aynı olduğunu grafiklerdeki Avg değerlerinden ve grafiğin kendinden rahatlıkla gözlemlenmiştir. 1. grafik ile 2. grafiğin ortalama trafik değerleri yaklaşık 38 Mbps iken 3. grafik olan ve 91.93.69.242 no' lu IP üzerinden geçen M7i-C 'de ise bu değer trafik yok anlamına gelen 1 Kbps civarlarındadır. Bu da A yönlendiricisine gelen tüm trafiğin B yönlendiricisi üzerinden aktığını gösteren kesin bir kanıt olmuştur.

5.2. UYGULAMA 2 : MPLS İLE TRAFİK MÜHENDİSLİĞİ

Bu bölümde OSPF ile kurduğumuz sistemin sorunu olan trafiğin tek bir yol üzerinden akması olayına MPLS ile çözüm üretilmiştir. Bu bölümde de kullanılan yapı aynı Şekil 5.2' deki gibidir.

Öncelikle yönlendiriciler üzerinde mevcut OSPF üzerinde çalışması için gerekli MPLS tanımları yapılmıştır. Burada, Şekil 18 de oluşturulan yapı üzerinde, dışarıdan 91.93.69.245 no' lu M7i-B üzerindeki IP'ye gitmek isteyen paketleri 91.93.69.242 no' lu IP üzerinden, yine dışarıdan 91.93.69.246 no' lu IP'ye gitmek isteyen paketleri ise 91.93.69.238 no' lu IP üzerinden göndermek amaçlanmıştır. Daha başka bir deyişle M7i-A' nın, M7i-B' nin fe-1/3/1 arayüzüne gitmek isteyen paketleri M7i-C üzerinden, M7i-C' nin fe-1/3/1 arayüzüne gitmek isteyen paketleri M7i-B üzerinden göndermesi işlemi MPLS ile gerçekleştirilmiştir.

Aşağıda MPLS LSP oluşturmak için yönlendirici üzerine girilen tanımlar verilmiştir. Konfigürasyon üzerinde koyu renkler ile yazılmış kısımlar MPLS ile ilgili yapılan tanımları göstermektedir, diğer satırlar Bölüm 5.1' deki zaten girilmiş tanımlardır.

M7i-A üzerindeki konfigürasyon:

```
show configuration |no-more
version 7.2R1.7;
system {
   host-name M7i-A;
   login {
      user teletek {
         uid 1903;
         class super-user;
         authentication {
            encrypted-password "$1$/unJX2yi$Aae95btJIHSD72zRm9raV0"; ##
SECRET-DATA
         }
```

```
        }
    }
    services {
        ftp;
        telnet;
    }
}
interfaces {
    fe-1/3/0 {
        unit 0 {
            family inet {
                address 91.93.68.190/30;
            }
        }
    }
    fe-1/3/1 {
        vlan-tagging;
        unit 0 {
            vlan-id 20;
            family inet {
                address 91.93.69.237/30;
            }
            family mpls;
        }
        unit 1 {
            vlan-id 30;
            family inet {
                address 91.93.69.241/30;
                address 192.168.30.1/24;
            }
            family mpls;
        }
    }
```

```
    lo0 {
        unit 0 {
            family inet {
                address 91.93.69.232/32;
            }
        }
    }
}
snmp {
    community teletek123 {
        authorization read-only;
        clients {
            84.51.14.166/32;
            84.51.14.210/32;
        }
    }
    trap-options {
        source-address lo0;
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 91.93.68.189;
    }
}
protocols {
    rsvp {
        interface all;
    }
    mpls {
        label-switched-path to-M7iB {
            to 91.93.69.233;
            install 91.93.69.245/32 active;
```

```
        no-cspf;
        primary Via_M7iC;
      }
      path Via_M7iC {
        91.93.69.242 strict;
        91.93.69.245 strict;
      }
      interface all;
    }
    ospf {
      area 0.0.0.0 {
        interface fe-1/3/1.0;
        interface fe-1/3/1.1 {
          metric 3;
```

M7i-B üzerindeki konfigürasyon :

```
show configuration |no-more
version 7.6R4.3;
system {
    host-name M7i-B;
    root-authentication {
        encrypted-password "$1$baSIyn0E$Azj8UzS8vro7Z2bxv.Zkr0"; ## SECRET-
DATA
    }
    login {
        user teletek {
            uid 1903;
            class super-user;
            authentication {
                encrypted-password "$1$G21n8Lhc$ZXfiGNAItebLsCyT4UfWc0"; ##
SECRET-DATA
            }
```

```
        }
    }
    services {
        ftp;
        telnet;
    }
}
interfaces {
    fe-1/3/0 {
        unit 0 {
            family inet {
                address 91.93.69.238/30;
            }
            family mpls;
        }
    }
    fe-1/3/1 {
        unit 0 {
            family inet {
                address 91.93.69.245/30;
            }
            family mpls;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 91.93.69.233/32;
            }
        }
    }
}
snmp {
```

```
    community teletek123 {
        authorization read-only;
        clients {
            84.51.14.166/32;
            84.51.14.210/32;
        }
    }
    trap-options {
        source-address lo0;
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 91.93.69.237;
    }
}
protocols {
    rsvp {
        interface all;
    }
    mpls {
        interface all;
    }
    ospf {
        area 0.0.0.0 {
            interface fe-1/3/0.0;
            interface fe-1/3/1.0;
        }
```

M7i-C üzerindeki konfigürasyon :

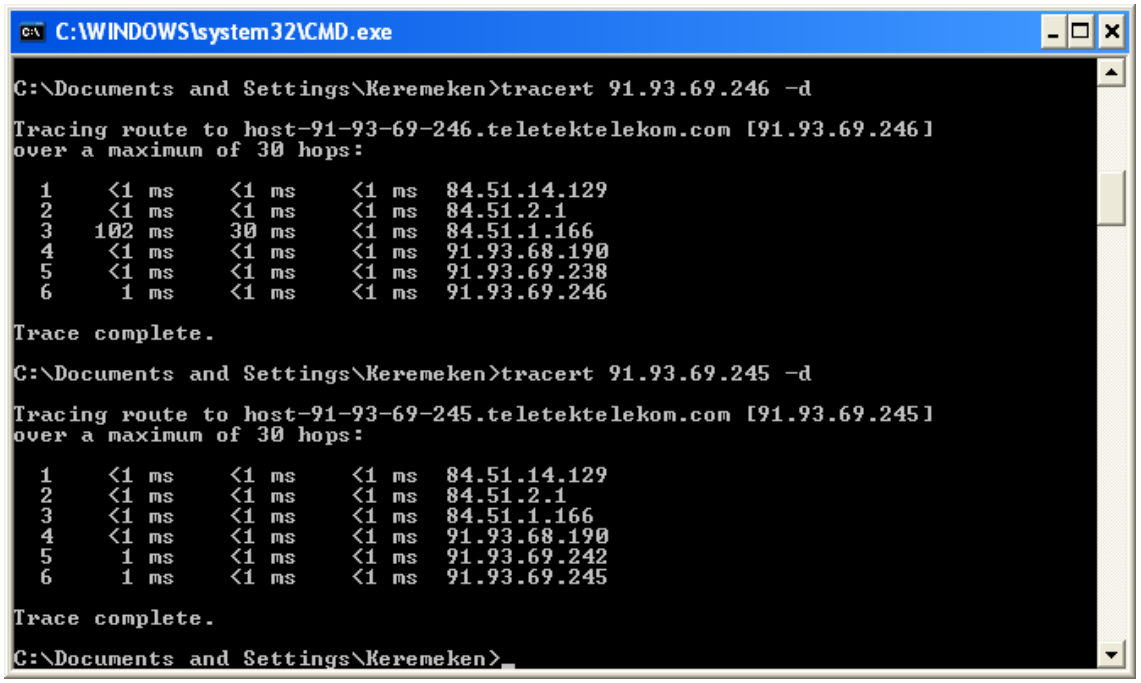
```
show configuration |no-more
version 7.6R4.3;
system {
    host-name M7i-C;
    root-authentication {
        encrypted-password "$1$INl9Z/KC$7XfU.mB2Kez7OBZLjNAJv."; ## SECRET-
DATA
    }
    login {
        user teletek {
            uid 1903;
            class super-user;
            authentication {
                encrypted-password "$1$jhIMoU/h$8u12q0tbaxLLUZE/IFsfV1"; ##
SECRET-DATA
            }
        }
    }
    services {
        ftp;
        telnet;
    }
}
interfaces {
    fe-1/3/0 {
        unit 0 {
            family inet {
                address 91.93.69.242/30;
            }
            family mpls;
        }
```

```
    }
    fe-1/3/1 {
        unit 0 {
            family inet {
                address 91.93.69.246/30;
            }
            family mpls;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 91.93.69.234/32;
            }
        }
    }
}
snmp {
    community teletek123 {
        authorization read-only;
        clients {
            84.51.14.166/32;
            84.51.14.210/32;
        }
    }
    trap-options {
        source-address lo0;
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 91.93.69.245;
    }
```

```
}
protocols {
   rsvp {
      interface all;
   }
   mpls {
      interface all;
   }
   ospf {
      area 0.0.0.0 {
         interface fe-1/3/1.0;
         interface fe-1/3/0.0;
```

Buradaki konfigürasyonlarda da görüldüğü gibi tüm arayüzlerin altında MPLS aktif edilmiş ve MPLS etiketlerinin, oluşturulan LSP' de doğru şekilde paketlerin içine yerleştirilmesi için ise RSVP protokolü etkinleştirilmiştir. Daha önceden hedeflendiği gibi M7i-A üzerinde LSP oluşturulmuş 91.92.69.245 IP' sine gönderilen IP'ler için yol olarak 91.93.69.242 ve 91.93.69.245 IP' leri üzerinden geçen yol gösterilmiştir. Bu da 245' li IP' ye gitmek isteyen paketler için yol olarak M7i-C yönlendiricisi üzerinden geçmesi sağlanmıştır.

Paketlerin istenilen yolda ilerlediğinin ispatı için, dışarıdan ağa çekilen trace sonuçlarını değerlendirilmelidir. Resim 5.2' de 91.93.69.245 ve 91.93.69.246 IP'lerine gitmek için paketlerin hangi yollar üzerinden geçtiği rahatça gözlemlenmiştir. Aynı zamanda bu veriyi Resim 5.1' deki sadece OSPF' in çalıştığı trace ile de karşılaştırıldığı zaman 91.93.69.245' e giden trace yolunun değiştiği de görülebilmiştir.



Resim 5.2 - LSP oluşturulan ağ üzerinden alınan trace sonuçları

Aşağıda gösterilen M7i-A' dan alınan yönlendirme tablosuna göre 91.93.69.245/32 IP'sine gönderilmek istenen paketlerle ilgili olarak yönlendiricinin bu paketleri oluşturulan LSP yani 91.93.69.242 IP' si üzerinden ve fe-1/3/1.1 arayüzünden göndereceği tabloda da gösterilmiştir. 91.93.69.246 IP'sine gönderilmek istenen paketler yine OSPF den gördüğü yol olan 91.93.69.238 IP'si üzerinden gönderilmeye devam edeceği görüntülenmiştir.

teletek@M7i-A> show route table inet.0

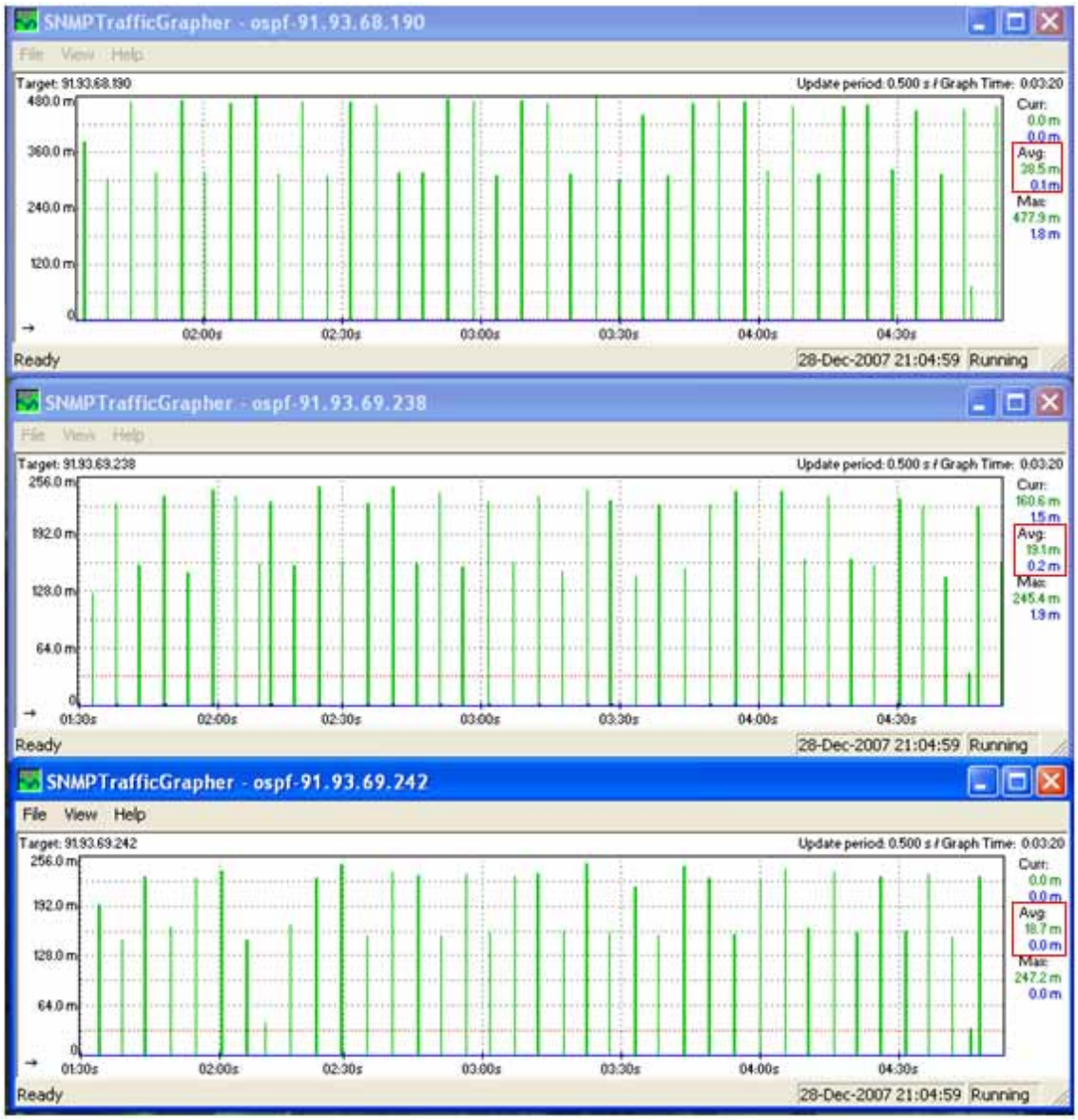
inet.0: 15 destinations, 16 routes (15 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0 *[Static/5] 3d 03:15:31
> to 91.93.68.189 via fe-1/3/0.0
91.93.68.188/30 *[Direct/0] 3d 04:12:09
> via fe-1/3/0.0
91.93.68.190/32 *[Local/0] 3d 04:12:09
Local via fe-1/3/0.0

91.93.69.232/32 *[Direct/0] 06:21:00
> via lo0.0
91.93.69.233/32 *[OSPF/10] 00:04:26, metric 1
> to 91.93.69.238 via fe-1/3/1.0
91.93.69.234/32 *[OSPF/10] 00:04:26, metric 2
> to 91.93.69.238 via fe-1/3/1.0
91.93.69.236/30 *[Direct/0] 04:44:17
> via fe-1/3/1.0
91.93.69.237/32 *[Local/0] 04:44:17
Local via fe-1/3/1.0
91.93.69.240/30 *[Direct/0] 04:38:15
> via fe-1/3/1.1
[OSPF/10] 00:04:26, metric 3
> to 91.93.69.238 via fe-1/3/1.0
91.93.69.241/32 *[Local/0] 04:38:15
Local via fe-1/3/1.1
91.93.69.244/30 *[OSPF/10] 00:04:26, metric 2
> to 91.93.69.238 via fe-1/3/1.0
91.93.69.245/32 *[RSVP/7] 00:04:26, metric 1
> to 91.93.69.242 via fe-1/3/1.1, label-switched-path to-M7iB
192.168.30.0/24 *[Direct/0] 04:34:05
> via fe-1/3/1.1
192.168.30.1/32 *[Local/0] 04:34:05
Local via fe-1/3/1.1
224.0.0.5/32 *[OSPF/10] 3d 03:10:50, metric 1
MultiRecv

Bir de bu durumu daha önce OSPF' de yapıldığı gibi çalışmanın asıl amacı olan M7i-B' nin M7i-A ile arasındaki hat yoğunluğunu bölüp trafiğin bir miktarını M7i-C üzerinden gidip gitmediğini grafiksel olarak Şekil 5.4' de gösterilmiştir. Şekil 5.3 ile kıyaslandığında MPLS' in sağladığı yarar daha net olarak görülebilmiştir. Şekil 5.4' deki kırmızı kare içine alınan ortalama trafik değerlerine bakıldığı zaman toplam trafiğin iki hat arasında oluşturulan LSP sayesinde eşit olarak dağıtılabildiği gözlemlenmiştir. Bu da

daha önce yoğunluğun hepsini taşıyan 91.93.69.238 IP' li arayüzün trafiğinde olan azalmayı da görülebilmektedir.



Şekil 5.4 - LSP üzerinden akan trafiğin gözlemlenmesi

Çalışmanın bu aşamasında, yönlendiriciler arasında kurulan LSP' nin kullandığı etiket değerleri, bunların yönlendiriciler ve yönlendiricilere gelen paketlerin switch tarafında monitor edilerek etiket değerlerinin karşılaştırılması böylelikle sistemin düzgün çalıştığının bu şekilde de gözlemlenmesi sağlanmıştır. Aşağıda verilen yönlendiricilerin bilgileriyle sniff edilen şekil 5.5' deki paketler içinde görülen etiket değerleri karşılaştırılmıştır.

Aşağıda görüldüğü gibi, M7i-A üzerinde oluşturulan LSP için A yönlendiricisi Ingress yönlendirici olup LSP' nin burada kurulduğunu göstermiştir. M7i-B üzerinde gördüğümüz bilgilere göre ise B yönlendiricisinin LSP' nin sonlandığı Egress yönlendiricisi, en sonda ise M7i-C' nin transit yönlendirici olduğu gözlemlenmiştir.

teletek@M7i-A> show mpls lsp

Ingress LSP: 1 sessions

To	**From**	**State**	**Rt**	**ActivePath**	**P**	**LSPname**
91.93.69.233	**91.93.69.232**	**Up**	**1**	**Via_M7iC**	*****	**to-M7iB**

Total 1 displayed, Up 1, Down 0

Egress LSP: 0 sessions

Total 0 displayed, Up 0, Down 0

Transit LSP: 0 sessions

Total 0 displayed, Up 0, Down 0

teletek@M7i-A> show rsvp session detail

Ingress RSVP: 1 sessions

91.93.69.233

From: 91.93.69.232, LSPstate: Up, ActiveRoute: 1

LSPname: to-M7iB, LSPpath: Primary

Suggested label received: -, Suggested label sent: -

Recovery label received: -, Recovery label sent: 100224

Resv style: 1 FF, **Label in: -, Label out: 100224**

Time left: -, Since: Fri Dec 28 18:27:56 2007

Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500

Port number: sender 1 receiver 53963 protocol 0

PATH rcvfrom: localclient

Adspec: sent MTU 1500

Path MTU: received 1500

PATH sentto: 91.93.69.242 (fe-1/3/1.1) 65 pkts

RESV rcvfrom: 91.93.69.242 (fe-1/3/1.1) 63 pkts

Explct route: 91.93.69.242 91.93.69.245

Record route: <self> 91.93.69.242 91.93.69.245

Total 1 displayed, Up 1, Down 0

Egress RSVP: 0 sessions

Total 0 displayed, Up 0, Down 0

Transit RSVP: 0 sessions

Total 0 displayed, Up 0, Down 0

teletek@M7i-B> show mpls lsp

Ingress LSP: 0 sessions

Total 0 displayed, Up 0, Down 0

Egress LSP: 1 sessions

To	**From**	**State**	**Rt**	**Style**	**Labelin**	**Labelout**	**LSPname**
91.93.69.233	**91.93.69.232**	**Up**	**0**	**1 FF**	**3**	**-**	**to-M7iB**

Total 1 displayed, Up 1, Down 0

Transit LSP: 0 sessions

Total 0 displayed, Up 0, Down 0

teletek@M7i-C> show mpls lsp

Ingress LSP: 0 sessions

Total 0 displayed, Up 0, Down 0

Egress LSP: 0 sessions

Total 0 displayed, Up 0, Down 0

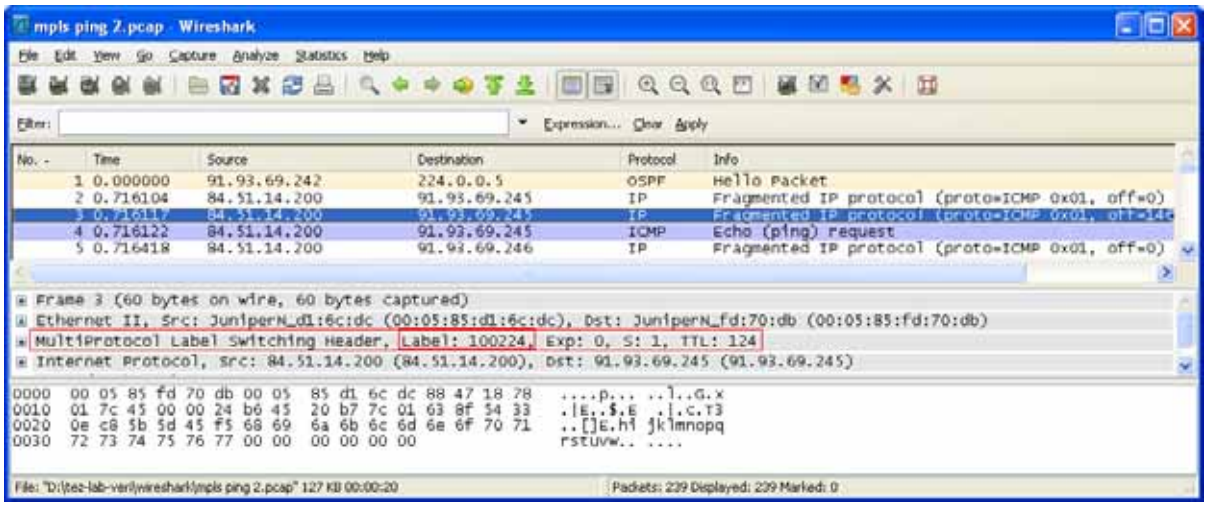
Transit LSP: 1 sessions

To	**From**	**State**	**Rt**	**Style**	**Labelin**	**Labelout**	**LSPname**

91.93.69.233 91.93.69.232 Up 1 1 FF 100224 3 to-M7iB

Total 1 displayed, Up 1, Down 0

Yukarıda aynı zamanda yönlendiricilerin kullandığı etiket değerleri de gözlemlenmiştir. Buradan rahatlıkla görüldüğü gibi M7i-A ‘dan çıkan paketlerin etiket değeri 100224’ dür. Bu, paketlerin içeriğinin görmesine yarayan Şekil 5.5’ deki programla da kıyasladığımız zaman programda kırmızı kutu içine alınan MPLS paketleri içindeki değerin aynı olduğu gözlemlenmiştir.

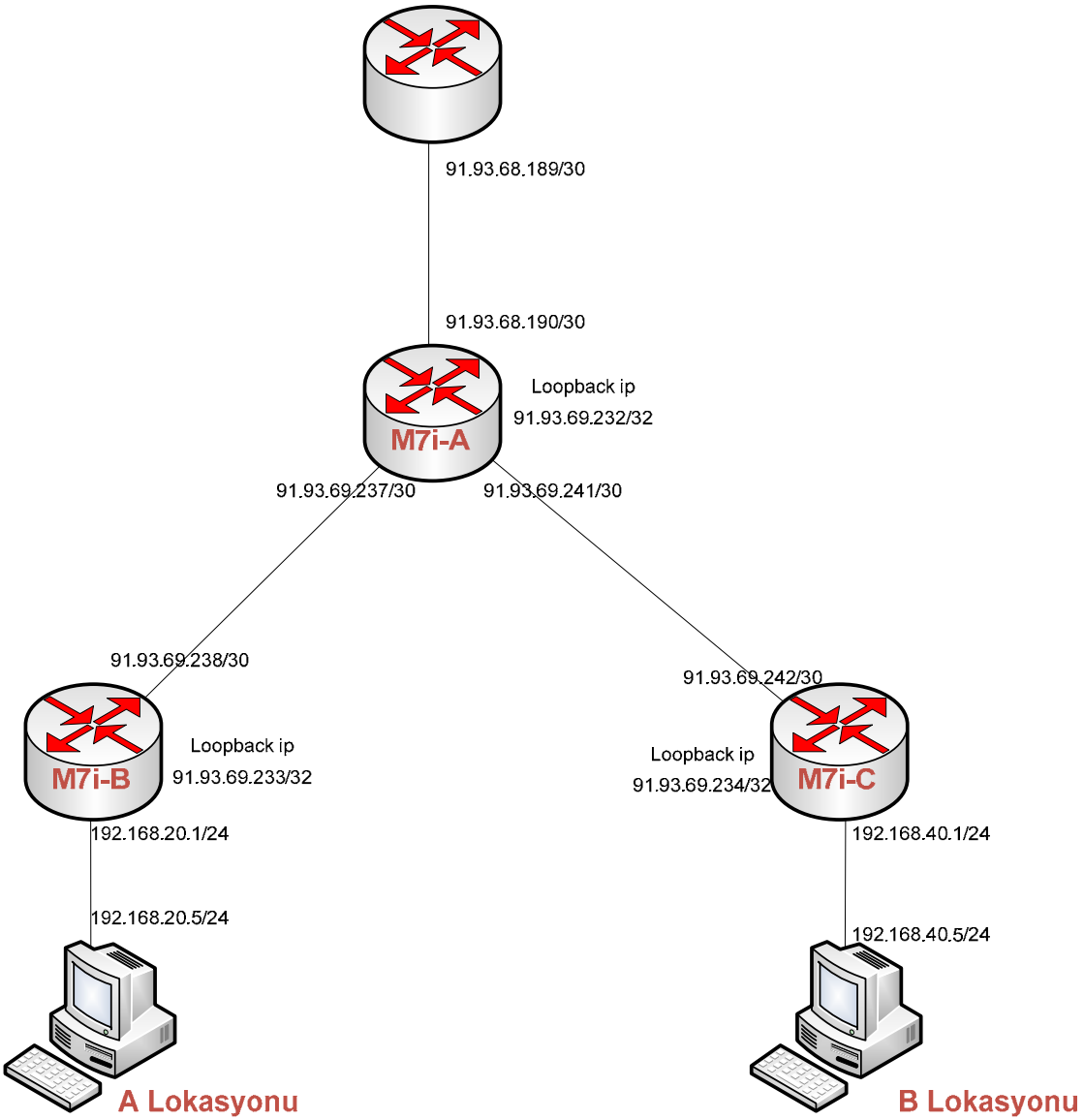


Şekil 5.5 - M7i-A’ dan çıkan MPLS paketi

Bu uygulamada görüldüğü gibi MPLS ile yapılan trafik mühendisliği bize mevcut kaynakların ağ trafiğini en uygun yerlere en uygun şekillerde yönlendirerek ağa büyük bir dinamizm kazandırmaktadır. Ağın üç adet yönlendiriciden değil de gerçek bir servis sağlayıcısı gibi onlarca hatta yüzlerce yönlendiriciden oluştuğu düşünülürse, MPLS ile trafik mühendisliği yapmak sistemimize büyük katkılar sağladığı açıktır.

5.3. UYGULAMA 3 : MPLS VPN

Bu bölümde MPLS' in servis sağlayıcılarına ve müşterilerine kattığı en büyük avantajlardan biri olan MPLS VPN uygulaması yapılmış, burada bundan önceki bölümlerden farklı olarak sistemde değişiklikler yapılması düşünülmüştür. Bunun amacı hem MPLS ile yapılan trafik mühendisliği ile MPLS VPN' in birbirinden bağımsız olarak omurgalarda kullanılabileceğini göstermek hem de ikisini ayrı olarak ele almaktır. Şekil 5.6' de bu uygulama için kullanılmış olan yapı görülmektedir.



Şekil 5.6 - MPLS VPN için kullanılan Uygulama Yapısı

Şekil 5.6’ de görüldüğü gibi B yönlendiricisi ile C yönlendiricisi arasındaki kablo çıkartılıp buralara müşteri tarafındaki farklı lokasyonları anlatan bilgisayarlar bağlanmıştır. Uçlarına ise gerçek olmayan IP’ler verilmiş ve böylelikle hiçbir şekilde internetten bu lokasyonlara ulaşmanın mümkün olmaması sağlanmıştır. B ve C yönlendiricisi arasındaki arayüzde çalışan OSPF protokolü ise o arayüzlerden kaldırılarak sadece A-B ve A-C arasında çalışılır bırakılmıştır: bu durum aşağıdaki yeni konfigürasyonlarda da görülebilmektedir.

```
teletek@M7i-A> show configuration | no-more
version 7.2R1.7;
system {
    host-name M7i-A;
    login {
        user teletek {
            uid 1903;
            class super-user;
            authentication {
                encrypted-password "$1$/unJX2yi$Aae95btJIHSD72zRm9raV0"; ## SECRET-DATA
            }
        }
    }
    services {
        ftp;
        telnet;
    }
}
interfaces {
    fe-1/3/0 {
        unit 0 {
            family inet {
                address 91.93.68.190/30;
            }
```

```
        }
    }
    fe-1/3/1 {
        vlan-tagging;
        unit 0 {
            vlan-id 20;
            family inet {
                address 91.93.69.237/30;
            }
            family mpls;
        }
        unit 1 {
            vlan-id 30;
            family inet {
                address 91.93.69.241/30;
                address 192.168.30.1/24;
            }
            family mpls;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 91.93.69.232/32;
            }
        }
    }
}
snmp {
    community teletek123 {
        authorization read-only;
        clients {
            84.51.14.166/32;
```

```
            84.51.14.210/32;
        }
    }
    trap-options {
        source-address lo0;
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 91.93.68.189;
    }
}
protocols {
    mpls {
        path Via_M7iC {
            91.93.69.242 strict;
            91.93.69.245 strict;
        }
        interface all;
    }
    ospf {
        area 0.0.0.0 {
            interface fe-1/3/1.0;
            interface fe-1/3/1.1 {
                metric 3;
            }
        }
    }
    ldp {
        interface all;
```

A yönlendiricisi üzerinde yapılan tek değişiklik yönlendiricinin gelen MPLS paketleri içindeki etiketleri değiştirebilmesi için gereken, arayüzleri üzerinde ldp protokolü aktif edilmiştir.

```
teletek@M7i-B> show configuration | no-more
version 7.6R4.3;
system {
    host-name M7i-B;
    root-authentication {
        encrypted-password "$1$baSIyn0E$Azj8UzS8vro7Z2bxv.Zkr0"; ## SECRET-DATA
    }
    login {
        user teletek {
            uid 1903;
            class super-user;
            authentication {
                encrypted-password "$1$G21n8Lhc$ZXfiGNAItebLsCyT4UfWc0"; ## SECRET-DATA
            }
        }
    }
    services {
        ftp;
        telnet;
    }
}
interfaces {
    fe-1/3/0 {
        unit 0 {
            family inet {
                address 91.93.69.238/30;
```

```
            }
            family mpls;
        }
    }
    fe-1/3/1 {
        unit 0 {
            family inet {
                address 192.168.20.1/24;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 91.93.69.233/32;
            }
        }
    }
}
snmp {
    community teletek123 {
        authorization read-only;
        clients {
            84.51.14.166/32;
            84.51.14.210/32;
        }
    }
    trap-options {
        source-address lo0;
    }
}
routing-options {
    static {
```

```
        route 0.0.0.0/0 next-hop 91.93.69.237;
    }
    autonomous-system 34104;
}
protocols {
    mpls {
        interface all;
    }
    bgp {
        group INTERNAL {
            type internal;
            local-address 91.93.69.233;
            family inet {
                unicast;
            }
            family inet-vpn {
                unicast;
            }
            neighbor 91.93.69.234 {
                family inet {
                    unicast;
                }
                family inet-vpn {
                    unicast;
                }
                peer-as 34104;
            }
        }
    }
    ospf {
        area 0.0.0.0 {
            interface fe-1/3/0.0;
        }
```

```
    }
    ldp {
        interface all;

teletek@M7i-C> show configuration | no-more
version 7.6R4.3;
system {
    host-name M7i-C;
    root-authentication {
        encrypted-password "$1$INl9Z/KC$7XfU.mB2Kez7OBZLjNAJv."; ## SECRET-
DATA
    }
    login {
        user teletek {
            uid 1903;
            class super-user;
            authentication {
                encrypted-password "$1$jhIMoU/h$8u12q0tbaxLLUZE/IFsfV1"; ##
SECRET-DATA
            }
        }
    }
    services {
        ftp;
        telnet;
    }
}
interfaces {
    fe-1/3/0 {
        unit 0 {
            family inet {
                address 91.93.69.242/30;
            }
```

```
            family mpls;
        }
    }
    fe-1/3/1 {
        unit 0 {
            family inet {
                address 192.168.40.1/24;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 91.93.69.234/32;
            }
        }
    }
}
snmp {
    community teletek123 {
        authorization read-only;
        clients {
            84.51.14.166/32;
            84.51.14.210/32;
        }
    }
    trap-options {
        source-address lo0;
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 91.93.69.241;
```

```
    }
    autonomous-system 34104;
}
protocols {
    mpls {
        interface all;
    }
    bgp {
        group INTERNAL {
            type internal;
            local-address 91.93.69.234;
            family inet {
                unicast;
            }
            family inet-vpn {
                unicast;
            }
            neighbor 91.93.69.233 {
                family inet {
                    unicast;
                }
                family inet-vpn {
                    unicast;
                }
                peer-as 34104;
            }
        }
    }
    ospf {
        area 0.0.0.0 {
            interface fe-1/3/0.0;
        }
    }
```

```
ldp {
    interface all;
```

B ve C yönlendiricileri üzerinde ki konfigürasyonda öncelikle bilgisayara bağlı olan arayüzlerin IP'si değiştirilmiş ve gerçek olmayan bir IP verilmiştir. Bu arayüz üzerinde çalışan OSPF protokolünde protokol altında o arayüzden kaldırılarak bu arayüzün tamamen dışarıya OSPF üzerinden anonsu kesilip bilgisayarların birbiri ile arasındaki bağlantı kesilmiş ve bu şekilde iki farklı lokasyonda farklı kullanıcılar yaratılmıştır.

Daha önce belirtildiği gibi, MPLS VPN paketleri BGP dış protokolü üzerinde çalışmaktadır. Bu nedenle, bir MPLS uygulaması için servis sağlayıcısı tarafındaki müşteriye bakan yönlendiricilerde doğru bir BGP konfigürasyonu yapmak gerekmektedir. Bu konfigürasyon hem B hem de C yönlendiricisinde çalışır duruma getirilmiştir. Aynı zamanda A' da yapıldığı gibi LDP' de B ve C yönlendiricisinde aktif edilerek, MPLS etiketleri üzerinde değişim yapılması sağlanmıştır. Aşağıda ki B ve C üzerindeki yönlendirme tablolarına bakıldığında ikisininde karşı taraftaki ağı görmediği görülmekte ve dolayısıyla aradaki iletişimde sağlanamamaktadır.

```
teletek@M7i-B> show route table inet.0

inet.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Static/5] 05:58:52
                    > to 91.93.69.237 via fe-1/3/0.0
91.93.69.232/32    *[OSPF/10] 06:30:10, metric 1
                    > to 91.93.69.237 via fe-1/3/0.0
91.93.69.233/32    *[Direct/0] 08:04:40
                    > via lo0.0
91.93.69.234/32    *[OSPF/10] 00:13:37, metric 4
                    > to 91.93.69.237 via fe-1/3/0.0
91.93.69.236/30    *[Direct/0] 06:34:33
```

```
                > via fe-1/3/0.0
91.93.69.238/32    *[Local/0] 06:34:33
                    Local via fe-1/3/0.0
91.93.69.240/30    *[OSPF/10] 00:13:37, metric 4
                > to 91.93.69.237 via fe-1/3/0.0
192.168.20.0/24    *[Direct/0] 00:13:37
                > via fe-1/3/1.0
192.168.20.1/32    *[Local/0] 00:13:37
                    Local via fe-1/3/1.0
192.168.30.0/24    *[OSPF/10] 02:16:50, metric 4
                > to 91.93.69.237 via fe-1/3/0.0
224.0.0.5/32       *[OSPF/10] 3d 04:53:58, metric 1
                    MultiRecv
teletek@M7i-C> show route table inet.0

inet.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Static/5] 00:09:51
                > to 91.93.69.241 via fe-1/3/0.0
91.93.69.232/32    *[OSPF/10] 06:25:55, metric 1
                > to 91.93.69.241 via fe-1/3/0.0
91.93.69.233/32    *[OSPF/10] 00:15:24, metric 2
                > to 91.93.69.241 via fe-1/3/0.0
91.93.69.234/32    *[Direct/0] 08:05:15
                > via lo0.0
91.93.69.236/30    *[OSPF/10] 00:15:24, metric 2
                > to 91.93.69.241 via fe-1/3/0.0
91.93.69.240/30    *[Direct/0] 06:27:39
                > via fe-1/3/0.0
91.93.69.242/32    *[Local/0] 06:27:39
                    Local via fe-1/3/0.0
192.168.30.0/24    *[OSPF/10] 02:18:37, metric 4
```

> to 91.93.69.241 via fe-1/3/0.0

192.168.40.0/24 *[Direct/0] 00:13:19

> via fe-1/3/1.0

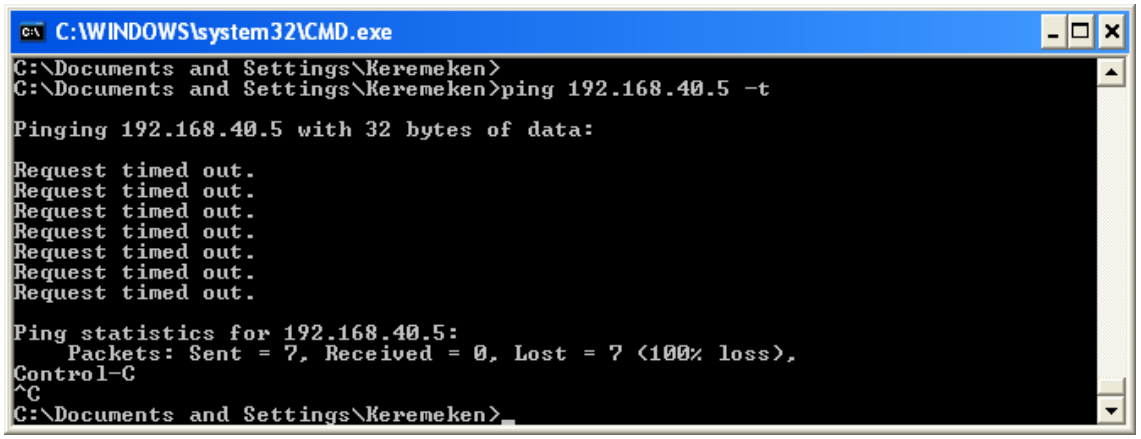
192.168.40.1/32 *[Local/0] 00:13:19

Local via fe-1/3/1.0

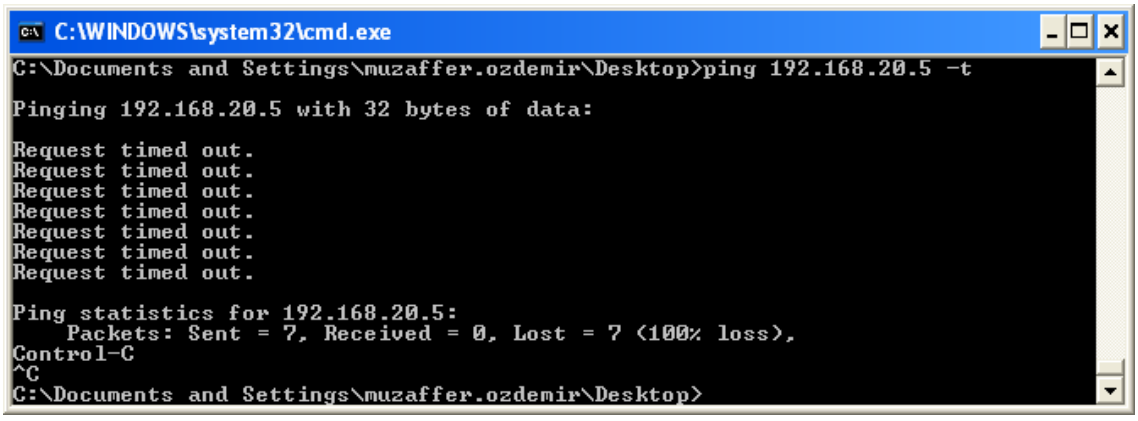
224.0.0.5/32 *[OSPF/10] 3d 04:47:30, metric 1

MultiRecv

Resim 5.3 ve Resim 5.4' deki A lokasyonu ve B lokasyonu arasınki ping sonuçlarına da baktığımız zaman aralarında hiçbir erişimin olmadığı gösterilmiştir.



Resim 5.3 - A Lokasyonundan B Lokasyonuna atılan ping sonuçları



Resim 5.4 - B Lokasyonundan A Lokasyonuna atılan ping sonuçları

Çalışmanın bu aşamadan sonraki amacı, farklı iki lokasyon olarak düşünülen A ve B bilgisayarlarının MPLS VPN ile birbirine erişilebilir hale getirilmesi ve farklı noktalar da olsalarda müşteri tarafında her hangi bir kurulum yapmadan birbirlerine erişim imkanı sağlanmasıdır. Bunun için, öncelikle konfigürasyonda yapılan değişiklikler ele alınmıştır. Aşağıda M7i-B ve M7i-C konfigürasyonları verilmiştir. M7i-A omurga router olduğu ve tek görevi gelen MPLS paketlerinin etiketlerini değiştirmek olduğundan her hangi bir değişiklik yapılmamıştır.

teletek@M7i-B> show configuration

```
version 7.6R4.3;
system {
   host-name M7i-B;
   root-authentication {
      encrypted-password "$1$baSIyn0E$Azj8UzS8vro7Z2bxv.Zkr0"; ## SECRET-
DATA
   }
   login {
      user teletek {
         uid 1903;
         class super-user;
         authentication {
            encrypted-password "$1$G21n8Lhc$ZXfiGNAItebLsCyT4UfWc0"; ##
SECRET-DATA
         }
      }
   }
   services {
      ftp;
      telnet;
   }
}
interfaces {
   fe-1/3/0 {
```

```
        unit 0 {
            family inet {
                address 91.93.69.238/30;
            }
            family mpls;
        }
    }
    fe-1/3/1 {
        unit 0 {
            family inet {
                address 192.168.20.1/24;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 91.93.69.233/32;
            }
        }
    }
}
snmp {
    community teletek123 {
        authorization read-only;
        clients {
            84.51.14.166/32;
            84.51.14.210/32;
        }
    }
    trap-options {
        source-address lo0;
    }
```

```
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 91.93.69.237;
    }
    autonomous-system 34104;
}
protocols {
    mpls {
        interface all;
    }
    bgp {
        group INTERNAL {
            type internal;
            local-address 91.93.69.233;
            family inet {
                unicast;
            }
            family inet-vpn {
                unicast;
            }
            neighbor 91.93.69.234 {
                family inet {
                    unicast;
                }
                family inet-vpn {
                    unicast;
                }
                peer-as 34104;
            }
        }
    }
    ospf {
```

```
        area 0.0.0.0 {
            interface fe-1/3/0.0;
        }
    }
    ldp {
        interface all;
    }
}
policy-options {
    policy-statement TEZ_VPN_EXPORT {
        term 1 {
            from protocol [ local direct static ospf ];
            then {
                community add TEZ_VPN;
                accept;
            }
        }
        term 2 {
            then reject;
        }
    }
    policy-statement TEZ_VPN_IMPORT {
        term 1 {
            from {
                protocol bgp;
                community TEZ_VPN;
            }
            then accept;
        }
        term 2 {
            then reject;
        }
    }
```

```
    community TEZ_VPN members target:34104:223;
}
routing-instances {
    TEZ_VPN {
        instance-type vrf;
        interface fe-1/3/1.0;
        route-distinguisher 91.93.69.233:223;
        vrf-import TEZ_VPN_IMPORT;
        vrf-export TEZ_VPN_EXPORT;
        vrf-table-label;


teletek@M7i-C> show configuration
version 7.6R4.3;
system {
    host-name M7i-C;
    root-authentication {
        encrypted-password  "$1$INl9Z/KC$7XfU.mB2Kez7OBZLjNAJv."; ## SECRET-
DATA
    }
    login {
        user teletek {
            uid 1903;
            class super-user;
            authentication {
                encrypted-password        "$1$jhIMoU/h$8u12q0tbaxLLUZE/IFsfV1";        ##
SECRET-DATA
            }
        }
    }
    services {
        ftp;
        telnet;
```

```
    }
}
interfaces {
    fe-1/3/0 {
        unit 0 {
            family inet {
                address 91.93.69.242/30;
            }
            family mpls;
        }
    }
    fe-1/3/1 {
        unit 0 {
            family inet {
                address 192.168.40.1/24;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 91.93.69.234/32;
            }
        }
    }
}
snmp {
    community teletek123 {
        authorization read-only;
        clients {
            84.51.14.166/32;
            84.51.14.210/32;
        }
```

```
    }
    trap-options {
        source-address lo0;
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 91.93.69.241;
    }
    autonomous-system 34104;
}
protocols {
    mpls {
        interface all;
    }
    bgp {
        group INTERNAL {
            type internal;
            local-address 91.93.69.234;
            family inet {
                unicast;
            }
            family inet-vpn {
                unicast;
            }
            neighbor 91.93.69.233 {
                family inet {
                    unicast;
                }
                family inet-vpn {
                    unicast;
                }
                peer-as 34104;
```

```
        }
      }
    }
    ospf {
      area 0.0.0.0 {
        interface fe-1/3/0.0;
      }
    }
    ldp {
      interface all;
    }
}
policy-options {
    policy-statement TEZ_VPN_EXPORT {
      term 1 {
        from protocol [ local direct static ospf ];
        then {
          community add TEZ_VPN;
          accept;
        }
      }
      term 2 {
        then reject;
      }
    }
    policy-statement TEZ_VPN_IMPORT {
      term 1 {
        from {
          protocol bgp;
          community TEZ_VPN;
        }
        then accept;
      }
```

```
        term 2 {
            then reject;
        }
    }
    community TEZ_VPN members target:34104:223;
}
routing-instances {
    TEZ_VPN {
        instance-type vrf;
        interface fe-1/3/1.0;
        route-distinguisher 91.93.69.234:223;
        vrf-import TEZ_VPN_IMPORT;
        vrf-export TEZ_VPN_EXPORT;
        vrf-table-label;
```

Konfigürasyonlarda koyu renk ile gösterilen kısımlar MPLS VPN için gerekli kısımlardır. Burada **TEZ_VPN** isimli bir topluluk oluşturulmuş ve bu topluluğun içine yönlendiricilerin bilgisayarlara bakan arayüzleri her bilgisayarın kendi yönlendiricisine eklenmiştir. Aynı zamanda politikalar tanımlanarak bu VPN içindeki bilgisayarların karşı taraftaki yönlendirme bilgileri alınması sağlanmıştır.

B ve C nin yönlendirme tablolarına bakıldığı zaman TEZ_VPN tablosu içinde karşı tarafın ağ adreslerinin tabloda oluştuğu gözlemlenmiştir. Aşağıda bu yönlendirme tabloları yer almaktadır:

teletek@M7i-B> show route table TEZ_VPN

```
TEZ_VPN.inet.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.20.0/24    *[Direct/0] 00:10:35
                    > via fe-1/3/1.0
```

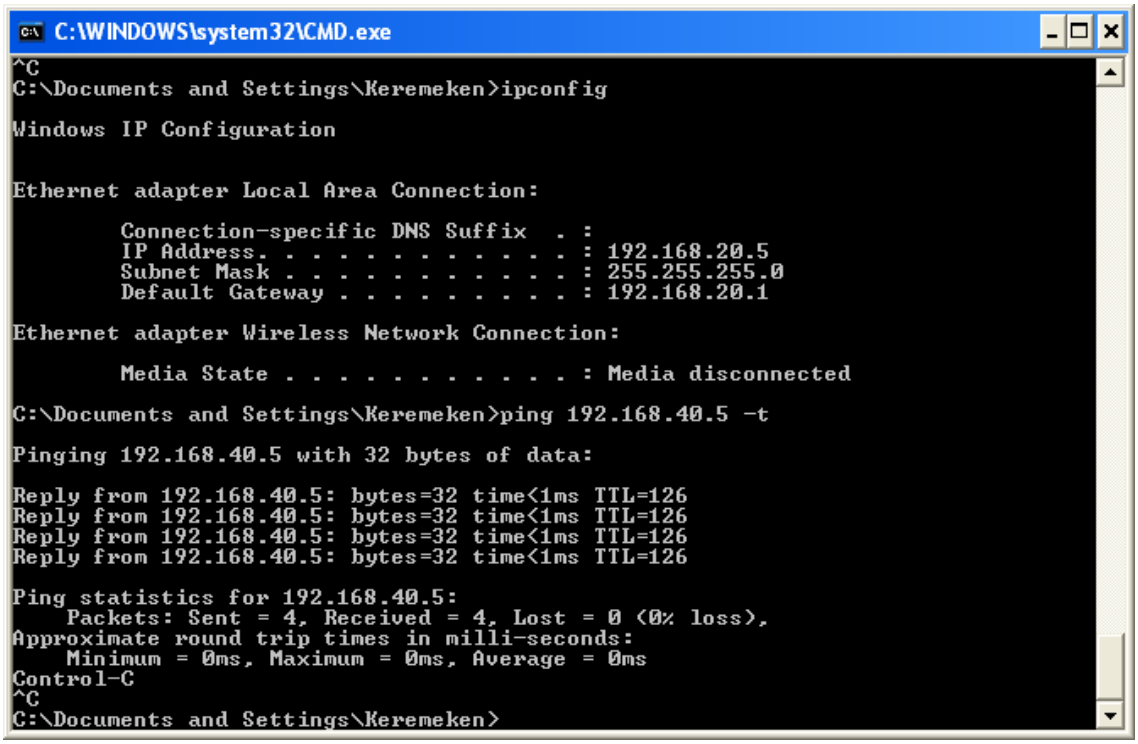
192.168.20.1/32 *[Local/0] 00:10:35
Local via fe-1/3/1.0
192.168.40.0/24 *[BGP/170] 00:09:17, localpref 100, from 91.93.69.234
AS path: I
> to 91.93.69.237 via fe-1/3/0.0, Push 16, Push 100016(top)

teletek@M7i-C> show route table TEZ_VPN

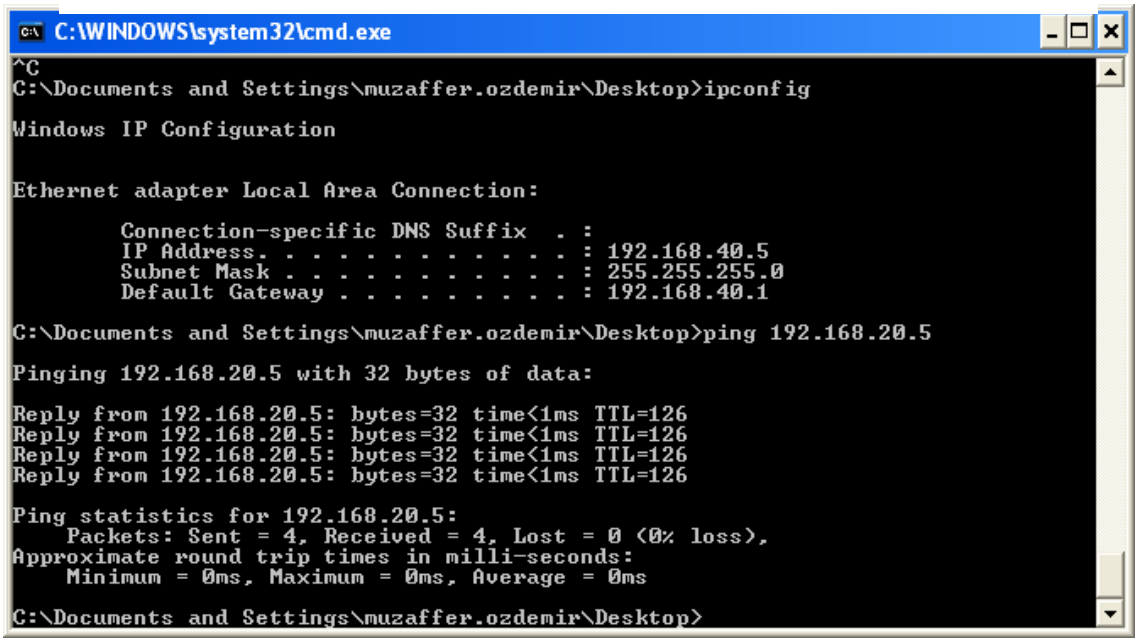
TEZ_VPN.inet.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.20.0/24 *[BGP/170] 00:16:12, localpref 100, from 91.93.69.233
AS path: I
> to 91.93.69.241 via fe-1/3/0.0, Push 16, Push 100000(top)
192.168.40.0/24 *[Direct/0] 00:16:13
> via fe-1/3/1.0
192.168.40.1/32 *[Local/0] 00:16:13
Local via fe-1/3/1.0

Bu veriler doğrultusunda Resim 5.5 ve Resim 5.6'da da görüldüğü gibi iki lokasyondaki bilgisayarlar birbirlerini pinglemeye başlamışlardır. Bu şekilde VPN bağlantısının kurulmuş olduğu test edilmiştir.



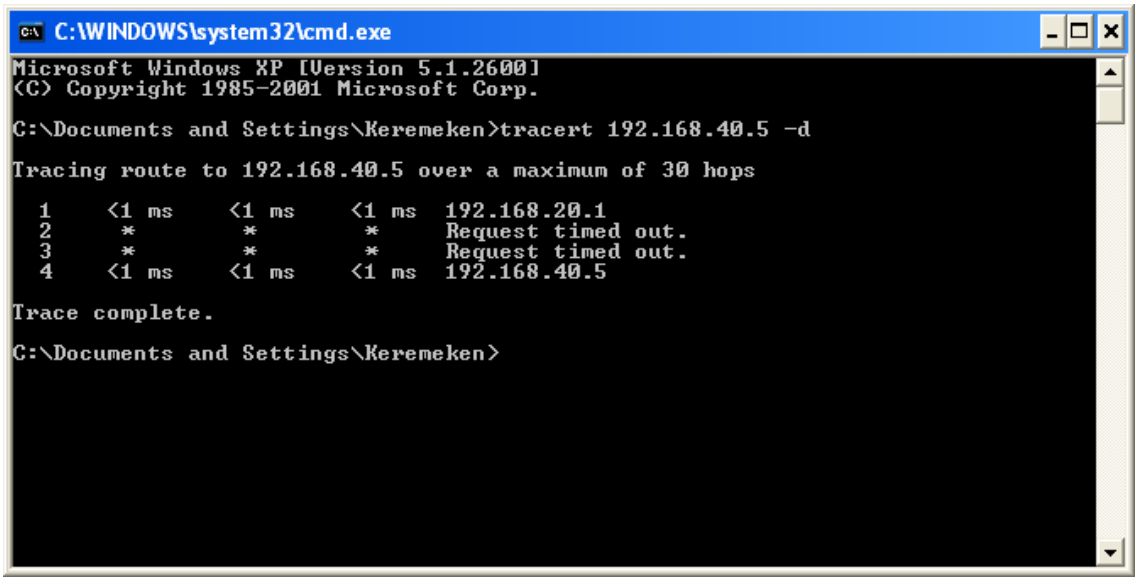
Resim 5.5 - A Lokasyonundan B Lokasyonuna atılan ping sonuçları



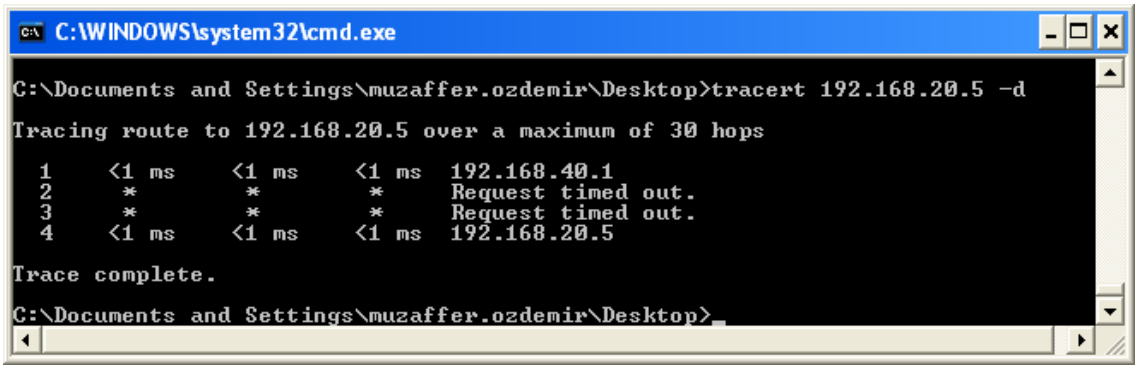
Resim 5.6 - B Lokasyonundan A Lokasyonuna atılan ping sonuçları

E ilmiştir. Burada aradaki yolların gözükmediği, sadece ilk ve son noktanın trace sonucunun görünmesi ise şunun göstergesidir: VPN' de iki farklı lokasyon arasında bağlantı kurulurken amaç, omurga üzerinden iki lokasyon arasında bir tünel oluşturmaktır.

Aradaki yolların ne olduğu müşteri tarafını ilgilendirmez böylelikle aynı lokasyonda gibi çalışabilen iki farklı ağın da birleştirilmesi sağlanmıştır.



Resim 5.7 - A Lokasyonundan B Lokasyonuna atılan trace sonuçları



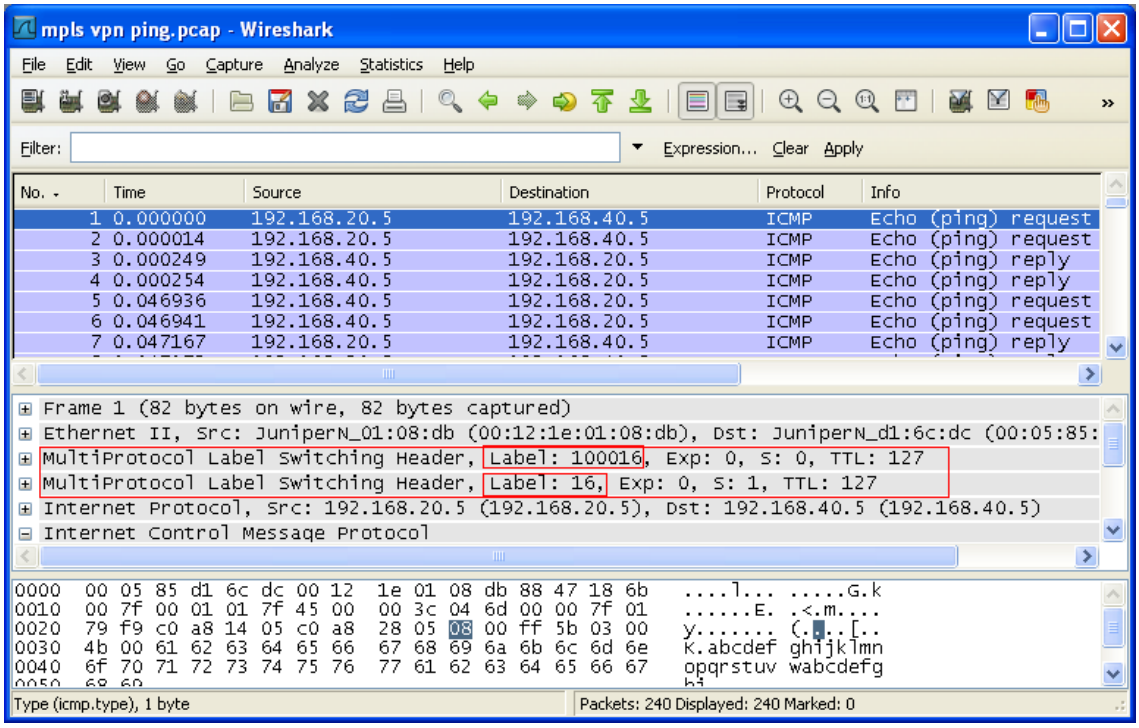
Resim 5.8 - B Lokasyonundan A Lokasyonuna atılan trace sonuçları

Son olarak MPLS VPN kurulurken kullanılan B ile A yönlendiricisi arasındaki etiketlerin yönlendiricide verilen değerle kıyaslanması için paketler sniff edilmiştir. Aşağıda M7i-B' nin üzerinden alınan etiket değerleri yönlendirme tablosunda görülmektedir. Şekil 5.7' de ise sniff progaramından alınan veriler gözükmektedir. Görüldüğü gibi iki taraftaki bilgiler birbirini tutmaktadır.

192.168.40.0/24 *[BGP/170] 00:09:17, localpref 100, from 91.93.69.234

AS path: I

> to 91.93.69.237 via fe-1/3/0.0, **Push 16, Push 100016**(top)



Şekil 5.7 - M7i-B' den çıkan MPLS VPN paketi

Bu uygulamada görüldüğü gibi, MPLS ile yapılan VPN' de son kullanıcı yani müşteri tarafında hiçbir ayarlama ve konfigürasyon yapmadan, arada hiçbir hat genişliğini meşgul edecek şifreleme yöntemi kullanmaya gerek kalmadan iki farklı lokasyon ağları birbirlerine bağlanmış olup başarılı sonuçlar alınmıştır. Bu uygulama normal hayatta servis sağlayıcıların müşterilerine kazandırabiliceği en önemli avantajlardan birini oluşturmaktadır.

6. SONUÇ

Günümüzün küçük büyük tüm internet servis sağlayıcıları, internet alanındaki hızlı büyüme ile aynı paralelde kendilerini yenileme çabası içerisinde olmak zorundadır. Çekirdek ağlarda, optik fiber teknolojisinin getirdiği avantajlar ve müşterilerin isteklerindeki artışlar, internet trafiğini, bu işe ayrılmış devreler ve dalga boyları üzerinden taşınması fikrini cazip hale getirmiştir. Aynı zamanda çoklu servislerin verildiği ortamlarda ATM üzerinden IP modelinin sağladığı çağullama yeteneği, trafik mühendisliği ve performans getirilerini kullanılması gerekldir. MPLS ise ATM üzerinden IP modelinin sağladığı avantajların yanında fazladan getirilere de sahiptir:

- Daha kolay ağ tasarımı ve yönetimi
- Geliştirilmiş ölçeklenebilirlik

MPLS, internet altyapısında kulanılan çok protokollü anahtarlama teknolojilerinin en yeni üyesidir. MPLS teknolojisi, daha önceki çok protokollü anahtarlama teknolojilerinden alınan dersler doğrulutusunda hazırlanan standartlarla oluşturulmaya çalışılan bir teknolojidir. MPLS, aktarma bileşenindeki etiket değiştirerek aktarma mekanizması ile kontrol bileşenindeki IP yönlendirme, standart IP mesajlaşmaları ve etiket dağıtım protokollerini entegre ederek bir arada kullanan bir yapıdır. Üstelik MPLS, sadece ATM altyapısında çalışacak şekilde değil, herhangi bir veri-bağı katmanı teknolojisinde çalışacak şekilde tasarlanmıştır. Böylelikle gelecek nesil olarak görülen SONET/WDM ve IP/WDM teknolojilerine dayanan optik internet altyapıları için uyumluluk sağlanmıştır.

MPLS'in en önemli faydalarından birisi de, internet servis sağlayıcılarına, klasik IP yönlendirme teknikleri ile kolayca sağlanamayacak yeni servisleri sunmasıdır. MPLS, sadece varış adresine göre aktarmadan çok daha fazlasını gerçekleyerek yönlendirme yeteneklerini çok arttırmıştır. Kontrol ve aktarma bilşenlerinin de birbirlerinden ayrılması ile aktarma bileşenin değiştirilmeden yeni kontrol fonksiyonlarının geliştirilebilmesine olanak verilmiştir.

MPLS, yeni nesil ağların tasarımında çok önemli avantajlar kazandırmaktadır. Yapılan uygulamalarda, OSPF ile yönlendirme yapan ağımızın ağın yönetimi ve esnekliğin korunması aşamasında çok avantajlı olmadığı görülmüş özellikle günümüzün servis sağlayıcıları için zorunlu bir ihtiyaç olan yedekli yapılarda çalışılırken mevcut tüm hatların efektif olarak kullanılamadığı görülmüştür. Bunun üzerine, çalışan ağımızı trafik mühendisliği ile daha efektif kullanabilmek için, MPLS tanımları yapılmış, bunun sonucunda da trafiğin çok daha efektif olarak ağımızda ilerlediği gözlemlenmiştir. Böylelikle, mevcut data hatlarımıza MPLS ile esneklik kazanması sağlanmış ve oluşturduğumuz LSP sayesinde, birbirlerine yedek oluşturması için düşünülmüş 2 hattımızın trafiği eşit ölçüde bölüştüğü gözlemlenmiştir.

Günümüzün, firmaların en önemli ihtiyaçlarının uzaktan erişilebilirlik ve güvenlik olduğu düşünüldüğünde, birden fazla lokasyonu olan firmalar mevcut veri bankalarını tek bir noktada tutmak ve buralara diğer lokasyonlardan güvenli bir şekilde bağlanılmasını sağlamak, farklı lokasyonlarda ama sanki tek bir lokasyonda çalışır gibi dinamik bir ağ yapısı oluşturmak servis sağlayıcıların müşterilerine vermek zorunda olduğu ve aranılan bir ihtiyaç konumuna gelmiştir, Bunu müşteriye her hangi bir yük getirmeden tamamiyle servis sağlayıcı tarafında yapılması ise MPLS VPN' e büyük bir avantaj kazandırmıştır. Yapılan son uygulamada farklı 2 lokasyon gibi düşünülen bilgisayarların uygulama sonunda sanki aynı ağ içindelermiş gibi birbirlerine ulaşım sağlayabilmiş olmaları MPLS VPN'in bize en büyük yararını göstermiştir, aynı zamanda yapılan uygulama ile MPLS VPN' in çalışmasıda incelenmiş ve avantajları anlaşılmıştır.

KAYNAKLAR

E. Rosen, A. Viswanathan, R. Callon, Internet Engineering Task Force, "Multiprotocol Label Switching Architecture - Draft", Ağustos 1999

E. Osborne, Traffic Engineering With Mpls-Fos Cisco Pres, Temmuz 2002

I. Pepelnjak, J. Guichard, MPLS and VPN Architectures, Cisco Pres, 2001

J. Lawrence, Designing ATM MPLS Networks, 1999

Juniper Networks, Advanced MPLS, 2001

R. Callon, P. Doolan, N. Feldman, A. Viswanathan, A. Fredette Internet Engineering Task Force, "A Framework for Multiprotocol Label Switching - Draft", Eylül 1999

İnternet Kaynakları

IETF MPLS Draftları, http://www.ietf.org/html.charters/mpls-charter.html

1] http://ieeexplore.ieee.org

2] http://en.wikipedia.org

3] http://www.mplsrc.com

ÖZGEÇMİŞ

Doğum tarihi	14.12.1981	
Doğum yeri	İstanbul	
Lise	1993-2000	Hüseyin Avni Sözen Anadolu Lisesi
Lisans	2000-2004	Yıldız Üniversitesi Mühendislik Fak. Elektronik ve Haberleşme Müh. Bölümü
Yüksek Lisans	2005-2008	Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Haberleşme Müh. Anabilim Dalı, Haberleşme Programı

Çalıştığı kurumlar

2004-2005	Elkotek Veri Çözümleri – Teknik destek müh.
2005-2007	PL4C teknoloji Çözümleri – Proje Yöneticisi
2007-	Huawei Technologies Co.,Ltd. – Ürün Müdürü