İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

MPLS VPN AĞLARINDA SERVİS KALİTESİ İNCELEMESİ

Yüksek Lisans Tezi

Müh. Özgür SAVAŞ

Bölüm: **Bilgisayar Mühendisliği**

Program: **Bilgisayar Mühendisliği**

Tez Danışmanı : Prof. Dr. Emre HARMANCI

HAZİRAN 2005

ISTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

QUALITY OF SERVICE ANALYSIS ON MPLS VPN NETWORKS

M.Sc. Thesis by

Özgür SAVAŞ, B.Sc.

Department: **Computer Engineering**

Programme: **Computer Engineering**

Supervisor : Prof. Dr. Emre HARMANCI

JUNE 2005

ÖNSÖZ

Bu tez kapsamında son yılların en dikkat çekici ağ uygulamalarından olan MPLS VPN teknolojisine ve MPLS/VPN omurgası üzerinden IP Servis Kalitesi tanımlarının taşınmasına yer verilmiştir. MPLS/VPN kavramı yüksek seviyeli bir ağ teknolojileri konusu olduğu için tezin içeriğinden tam olarak faydalanabilmek için okuyucuların, dahili IP yönlendirme protokolleri (RIP, OSPF), otonom sistemler arası haberleşme protokolleri (EGP, BGP) ve OSI başvuru modeli katmanları ve katman fonksiyonları konusunda detaylı bir ön bilgiye sahip olmaları gerekmektedir. Tez kapsamında çerçeve modlu MPLS omurgaları incelendiğinden BGP protokolünün ve haberleşme mimarisinin iyi bilinmesi, kapsülleme mantığı, IPSec VPN konularının bilinmesi tezin anlaşılmasını kolaylaştıracaktır. Okuyucunun önceden bilmesi gereken kavramlar hususunda kısaltmalar kısmı bir fikir verebilir. Tez kapsamında mümkün olduğunca tüm konulara yer verilmeye çalışılsa da okuyucunun bu konuları temel ağ teknolojileri kaynaklarından takip etmesinde yarar görülmektedir. Tezimizin, günümüzde giderek yaygınlaşan ve önümüzdeki birkaç yıl içerisinde tüm servis sağlayıcı ve büyük omurgalarda yaygınlaşması beklenen MPLS teknolojisi üzerindeki VPN ve servis kalitesi tanımları açısından dilimizde yer alan ilk kaynaklardan olması önemini arttırmaktadır. Bazı terimler de orijinal karşılıklarından dilimize ilk kez kazandırılmaktadır. Tezimizin bu konuda çalışacak tüm akademisyen ve mühendislere katkıda bulunabilmesi, ve üzerine yapılacak çalışmalara kaynaklık edebilmesini dilerim.

Bu tezin hazırlanması sırasında seçtiğim konuyu benimseyen ve tezim için beni destekleyen danışmanım Sayın Prof. Dr. Emre Harmancı'ya, NS simülasyonu kısmında danışmanlığımı üstlenen Sayın Dr. Erdal Çayırcı'ya, gerçek bir ağ ortamında teorik çalışmaları pratiğe dönüştürmem için lab ve cihaz kullanımı konusunda Cisco Systems İstanbul ofisi mühendislerine, simülasyon ve test çalışmalarımdaki desteklerinden dolayı Müh. Osman Korkutan ve ablam Özlem Savaş'a, yüksek lisans için beni yüreklendiren aileme ve ismini anamadığım destek veren herkese teşekkürlerimi sunarım.

Haziran 2005 Müh. Özgür Savaş

İÇİNDEKİLER

KISALTMALAR

AF	: Assured Forwarding
AH	: Authentication Header
ARIS	: Aggregate Route-Based IP Switching
ARP	: Address Resolution Protocol
AS	: Autonomous System
ATM	: Asyncronous Transfer Mode
ATMARP	: Asyncronous Transfer Mode Address Resolution Protocol
BE	: Best Effort
BGP	: Border Gateway Protocol
CBR	: Constant Bit Rate
CBS	: Committed Burst Size
CE	: Customer Edge
CIR	: Committed Interface Rate
CLI	: Command Line Interface
CLP	: Cell Loss Priority
CPU	: Central Processing Unit
CSR	: Cell Switching Router
DiffServ	: Differentiated Services
DLCI	: Data Link Connection Identifier
DMVPN	: Dynamic Multipoint Virtual Private Network
DSCP	: Differentiated Services Code Point
DSL	: Digital Subscriber Line
EAP	: Extensible Authentication Protocol
EBS	: Excess Burst Size
ECR	: Eggress Committed Rate
EIGRP	: Enhanced Interior Gateway Routing Protocol
EF	: Expedited Forwarding
ESP	: Encapsulating Security Payload
EXP	: Experimental
FEC	: Forwarding Equivalence Class
FR	: Frame-Relay
FTP	: File Transfer Protocol
FXS	: Foreign Exchange Station
GRE	: Generic Routing Encapsulation
GSMP	: General Switch Management Protocol
ICR	: Ingress Committed Rate
IETF	: Internet Engineering Task Force
IFMP	: Ipsilon Flow Management Protocol
IGP	: Interior Gateway Protocol
IKE	: Internet Key Exchange

IntServ : Integrated Services
IOS : Internetworking Operating System
IP : Internet Protocol
IPCP : IP Control Protocol
IPLPDN : Internet Protocol over Large Public Data Networks
IPSec : Internet Protocol Security
IPX : Internet Protocol Exchange
ISDN : Integrated Services Digital Network
ISLL : Integrated Services over Specific Link Layers
ISP : Internet Service Provider
LAN : Local Area Network
LC-ATM : Label Controlled Asyncronous Transfer Mode
LCP : Link Control Protocol
LDP : Label Distribution Protocol
LFIB : Label Forwarding Information Base
LIB : Label Information Base
LIS : Logical Internet Protocol Subnet
LSP : Label Switched Path
LSR : Label Switching Router
L2F : Layer 2 Forwarding
L2TP : Layer 2 Tunneling Protocol
MP-BGP : Multi Protocol – Border Gateway Protocol
MPLS : Multi-Protocol Label Switching
MPOA : Multiprotocol over Asyncronous Transfer Mode
NCP : Network Control Protocol
NNI : Network-Network Interface
NS : Network Simulator
OSPF : Open Shortest Path First
P : Provider
PBR : Policy Based Routing
PE : Provider Edge
PHB : Per Hop Behavior
PIM : Protocol Independent Multicast
PPP : Point-to-Point Protocol
PPTP : Point-to-Point Tunneling Protocol
PSTN : Public Switched Telephone Network
PVC : Permanent Virtual Circuit
QoS : Quality of Service
RFC : Request For Comments
RIP : Routing Information Protocol
ROLC : Routing over Large Clouds
RSpec : Reservation Specification
RSVP : Resource Reservation Protocol
SNA : System Network Architecture
SNMP : Simple Network Management Protocol
SVC : Switched Virtual Circuit
TCP : Transfer Control Protocol
TDP : Tag Distribution Protocol
TER : Tag Edge Router

TFIB : Tag Forwarding Information Base
ToS : Type-of-Service
TSpec : Traffic Specification
TSR : Tag Switching Router
TTL : Time-to-Live
UDP : User Datagram Protocol
UNI : User-Network Interface
VC : Virtual Circuit
VCI : Virtual Circuit Identifier
VPI : Virtual Path Identifier
VPN : Virtual Private Networking
WAN : Wide Area Network

TABLOLAR

Sayfa No

ŞEKİLLER

Sayfa No

ÖZET

Günümüzde hızla artan İnternet kullanıcısı sayıları, WAN bağlantılarının yaygınlaşması ve çokluortam uygulamalarına olan talebin artması İnternet servis sağlayıcılarının yüksek performanslı omurgalar tasarlamasını gerektirmektedir. Bu amaçla kullanılan ATM şebekelerinin ortaya çıkardığı ölçeklenebilirlik problemi, sanal devre üzerinde kaynak rezervasyonu nedeniyle kaynakların verimsiz kullanımı ve IP paketlerinin omurga girişinde hücrelere dönüşümünün yarattığı performans kaybı nedeniyle MPLS'e doğru bir yönelim gözlenmektedir. MPLS teknolojisi getirdiği yeni yaklaşımlar ve avantajları ile dikkat çeken bir teknoloji olarak dikkat çekmektedir. Halihazırdaki IP yönlendirme mimarisindeki ihtiyaçları karşılaması, yönlendiricilerin yüksek performans/hız sağlaması, ölçeklenebilirlik problemini aşması, getirdiği etiket yığını yapısıyla VPN teknolojisini desteklemesi, IP QoS özelliklerini MPLS omurgası üzerinden taşımayı sağlaması ve ortaya koyduğu yeni yönlendirme özellikleri ile etiket anahtarlama büyük kurumlar ile servis sağlayıcı omurgalarında giderek yaygınlaşmaktadır.

Tez kapsamında MPLS teknolojisinin bahsedilen temel özellikleri, etiket anahtarlama temel kavramları, MPLS mimarisi, VPN desteği ve QoS uygulamaları detaylı bir incelemeye tabi tutulmakta ve gerçek bir ağ platformunda MPLS omurgası kurularak, bu omurga üzerinde VPN ve DiffServ ile servis kalitesi uygulamalarına yer verilerek, MPLS VPN üzerinden IP QoS mekanizmalarının devamlılığı ve bu uygulamaların paket iletimi üzerindeki etkileri analiz edilmektedir. Gerçeklenen bir ağ uygulaması yanı sıra NS ortamında bandgenişliği değişimlerine bağlı olarak paket kaybı, gecikme ve seğirtim değerleri incelenmekte, MPLS üzerinde QoS özellikleri uygulamanın iletim üzerindeki etkisi analiz edilmektedir.

SUMMARY

Increasing number of Internet users, growing amount of WAN connections and demand on multimedia applications, obligated the Service Providers to design and supply high performance backbone networks. Since ATM networks brings some disadvantages such as scalability issues, inefficient use of resources because of resource reservation method and the necessity to convert IP packets into cells, along with its advantages, migration to MPLS technology became wide-spread. MPLS technology is said to be considerable because of new approaches and advantages that it bring. Since it fulfils the requirements on IP routing architectures and perfomance, removes the complexity and problems such as scalability that ATM has, and supports label stacking for VPN needs, label switching begin to be standardized on enterprise and ISP backbones.

In this thesis, specialities of MPLS architecture, VPN support and QoS approach investigated in detail, and on the last section they have proven on a real MPLS backbone design. Using MPLS/VPN and DiffServ applications on emulation network, it is showed how IP QoS definitions can be transferred over MPLS backbone using VPN tunnels, and the effect on packet transmission is defined. Along with a real time running environment, a simulation is generated using NS, furthermore according to backbone bandwidth modification, variation of QoS parameters such as packet loss, delay and jitter is examined.

1. GİRİŞ

Günümüz dünyasında teknoloji karşı konulmaz bir hızla ilerlemekte ve her geçen gün yeni teknolojiler hayatımızın vazgeçilmezleri haline gelmektedir. Özellikle 2.Dünya savaşı dönemiyle birlikte savunma sanayiinde kendini gösteren teknolojik atılımların sıcak savaş döneminden soğuk savaş dönemine geçildikçe yerini sanayi toplumunun son aşaması olan toplumsal refah - yüksek tüketim toplumuna ulaşmaya yönelik araştırmalara bırakması, 1960'ların ikinci yarısında meydana gelen dünya ekonomik bunalımı ve 1973'teki dünya petrol krizi ile insanoğluna hakim olan sınırsız doğa kaynakları kullanımı mantığının yerini yavaş yavaş doğa kaynaklarının dikkatli ve verimli kullanım anlayışının alması insanoğlunu bilgisayar kavramı ile tanıştırdı. Bilgisayar kavramı 50'lerden bu yana var olmasına karşın o tarihlerde bilgisayarın günlük hayata entegre edilmesine dair hiçbir girişimde bulunmaya gerek görülmemişti. Ancak bahsedilen dönemin ardından yeni çağın rekabetçi yapısının beraberinde yarıiletken teknolojisindeki gelişmeler ve mikroelektronik ve tümdevre kavramlarının ortaya çıkarması, başlangıçta yalnızca askeri ve kısmen akademik amaçlarla düşünülen bilgisayarların hem boyutsal, hem de fiyat açısından kullanılabilir seviyelere indirgenmesini ve günlük hayata ve kişisel kullanım amaçlarına girmesini sağladı.

Bireylerin bilgisayarla tanışması teknolojinin yayılım hızını tahminlerin ötesinde hızlandırması yeni ihtiyaçların ortaya çıkmasına yol açmıştır. Bunlardan en önemlisi hiç şüphesiz bilgisayar haberleşmesi yani ağ kavramı ve daha sonra arkasından gelen Internet'tir. Internet'in hayatımızdaki etkisi geçmiş yüzyıldaki tüm teknolojilerden daha büyük ve kökten olmuştur. Artık günümüzde kişisel bilgisayarlardan, analog telefonlarla santral haberleşmesinden değil, kablosuz el bilgisayarlarından, IP üzerinden ses taşınmasından (VoIP), video haberleşmesinden bahsedilmektedir. Bunlar Internet'in de yaygınlaşması ve bilgisayar ağ teknolojilerinin gelişmesi ile erişilen noktanın net göstergeleridir.

Internet'in kişisel amaçlarla kullanımını yaygınlaşması bu hizmetleri son kullanıcı ve tüketiciye götürebilecek hizmetlerin de verilmesini zorunlu kılmıştır. Bu hizmetleri sağlamak üzere "Internet servis sağlayıcı" (ISP) şirketler kendi bünyelerinde yüksek kapasiteli omurga ağları kurmakta ve hali hazırdaki telefon (PSTN) şebekesi üzerinden çevirmeli arama (dial-up), DSL, ISDN ya da televizyon amaçlı olarak yaygın olarak kablo şebekesi üzerinden veri taşınması yoluna gitmektedirler. ISP şebekeleri üzerinden taşınan veri miktarının ve trafiğin giderek artması, uygulamaların gerektirdiği bandgenişliği miktarlarının yükselmesi ISP omurga ağlarının bu isteği karşılayabilecek kapasiteler için yenilenmesini ve dolayısıyla yeni teknolojileri beraberinde getirmektedir.

Bilindiği gibi bilgisayar haberleşmesi terminolojisinde haberleşmede kaynaklanabilecek sorunları daha kolay çözebilmek, farklı üreticiler arasında eşgüdümü sağlayabilmek ve haberleşme sistemlerinin işleyişini basite indirgeyebilmek için mantıksal olarak katmanlı bir yapı tasarlanmıştır. Bu katmanlı yapı, en üstte kullanıcıların kişisel bilgisayarları ya da terminaller üzerinde uygulamalarını çalıştırdığı *uygulama katmanı,* onun altında uygulamalardan alınan verilerin formatlarının düzenlenip uzantılarının belirlendiği *sunum katmanı,* karşılıklı haberleşen çiftleri arasında senkronizasyonun sağlandığı *oturum katmanı,* iki oturum arasında verinin segmenler içerisine alınarak taşınmasından sorumlu *taşıma katmanı,* verinin bir adresten diğerine en uygun yoldan paketlere dönüştürülerek gönderilmesinden yani yol atama ve yol bulma işlerinin yapıldığı *ağ katmanı,* paketlerin çerçeveler içerisine alınarak ağ katmanında belirlenen mantıksal adreslerin fiziksel adreslere dönüşümünün ve son iletimin yapıldığı *veri bağı katmanı* ve son olarak verinin elektriksel işaretlere dönüştürülerek taşındığı *fiziksel katmandan* oluşmaktadır. [7]

Bu katmanlı yapı içerisinde ağ katmanı yol atama ve en kısa yol bulma işlerini gerçekleştirirken mantıksal adresleri kullandığı için uzun bir işlem süreci geçirmektedir. Kullanıcı ve dolayısıyla adres sayılarının artması bu işlemi gerçekleştiren *yönlendirici (router)* cihazlarının bilgi tablolarının daha da uzamasına ve sürecin daha da uzamasına yol açtı. Halbuki ikinci katmanda iletim gerçekleştiren *anahtarlar (switch)* fiziksel adrese göre karar verdikleri için çerçeve içinde gelen paketin içini açarak bir değişiklik yapmamakta dolayısıyla son derece hızlı iletim gerçekleştirebilmektedirler. Bilgisayar ağlarının temel cihazları olan yönlendirici performanslarındaki bu olumsuz nitelik bilim

adamlarının dikkatlerini bu noktaya çekti. Amaç anahtarlama hızında yönlendirme gerçekleştirebilecek yeni bir teknoloji oluşturmaya yönelmeye başladı.

Bilindiği üzere sanal devre kavramı ve katmanlı yapı ilk olarak 1970'lerde *X.25* adı verilen teknoloji ile ortaya konmuştur. X.25 teknolojisi temelde sanal devre üzerinden paket anahtarlamaya dayanan senkron veri aktarım protokolüdür. Hizmet kalitesinin pek dikkate alınmadığı ortamlarda uzun yıllar boyunca yaygın olarak kullanılmıştır. Zaman içerisinde yüksek hız gereksinimlerini karşılamadığı için yerini X.25'e benzeyen ancak çok daha basit yapıdaki ve yüksek bandgenişliği sağlayan *Frame Relay* teknolojisine bırakmıştır. FR'de PVC (Permanent Virtual Circuit) ve SVC (Switch Virtual Circuit) olmak üzere iki tip sanal devre tanımlanmış ve devreler DLCI (Data Link Connection Identifier) adı verilen numaralar ile etiketlenmiştir. Böylece aralarında sanal devre kurulmuş iki düğüm arasında DLCI numarası kullanarak hızlı iletim gerçeklenmiştir. [7]

Sanal devre mantığının en büyük getirisi artık sanal devre üzerinden haberleşen düğümlerin yönlendirme işleminin gecikmesine maruz kalmadan sanal devre numarasını kullanarak hızlı iletimi gerçekleştirebilmesidir. Genellikle sanal devreyi niteleyen bu numaralara *etiket* adı verilmektedir. FR teknolojisinden sonra etiket kavramı ilk olarak yüksek kapasiteli omurga teknolojisi olarak halen de günümüzde yaygın bir kullanıma sahip olan *Asenkron İletim Modu – ATM (Asyncronous Transfer Mode)* teknolojisinde görülmektedir. ATM, IP adres yapısından farklı bir adresleme ve katmanlı yapı sunmaktadır. Özellikle hizmet kalitesi (QoS) konusunda getirdiği yenilikler ve yüksek bandgenişliği imkanı sunması özellikle yüksek kapasite gerektiren omurgalar ve çekirdek ağlarında ATM'in hızla yaygınlaşmasına yol açtı. Başlangıçta ATM teknolojisinin gelişimi ile beklenen zaman içerisinde hali hazırdaki düşük hızlı IP ağlarının yerini alması ve ağların tamamen ATM haline gelmesiydi. Ancak Internet'in de yaygınlaşması ile IP teknolojisinin yaygınlığı ve sunduğu adresleme yönteminin kolaylığı bu öngörünün geçersiz olduğu sonucunu ortaya koymuştur. Omurgalarında ATM çalıştıran hizmet sağlayıcılar (ISP) müşterilerinin IP ağı kullanması nedeniyle omurgaya kadar paketleri IP olarak taşıyıp uç ATM yönlendirilerinde paketleri hücrelere çevirerek iletmeye başladılar ki bu durumda omurga her ne kadar yüksek kapasiteli de olsa bu çevrim işlemi ATM'in VPI (Virtual Path Identifier) – VCI (Virtual Circuit Identifier) değerlerine bakarak hücreleri açmadan hızlı iletim yeteneğinden sağlanan getirinin kaybedilmesine yol açtı.

Bundan dolayı çeşitli firmalar paketlerin tüm ağda IP paketi şeklinde taşınmasını sağlayacak ancak VPI-VCI değerleri gibi *etiketleme* ile iletimi gerçekleştirecek çözümler üzerinde durmaya başladılar.

Yapılan bu araştırmalar sonucunda farklı üreticiler farklı teknolojiler ile ortaya çıktılar. Bu öncül teknolojilerin en önemlileri *Ipsilon* firmasının geliştirdiği ve bugün genel bir haberleşme kavramı ile eş anlamlı hale gelen *IP Anahtarlama (IP Switching)* teknolojisi, ondan önce *Toshiba* firmasının geliştirdiği *Hücre Anahtarlamalı Yönlendirici (Cell Switching Router - CSR)* teknolojisi, *IBM*'in *Bütünsel Rota-tabanlı IP Anahtarlama (Aggregate Route-based IP Switching - ARIS)* ve *Cisco*'nun *Takı Anahtarlama (Tag Switching)* teknolojileridir. [2]

Tüm bu teknolojilere baktığımız zaman dikkat çeken ortak nokta hepsinin etiket ya da benzeri bir başlık eki üzerinde *etiket değiştirme (label swapping)* tekniği kullanıyor olmasıdır. *Etiket* genel anlamda paketlerin hızlı iletimi için kullanılan sabit uzunluklu görece kısa belirteçlere verilen addır. Etiket değerleri genellikle paketi oluşturan yönlendiricinin doğrudan bağlı olduğu linkleri temsil ettiği için global geçerliliğe sahip değildirler. Etiket anahtarlayan cihazlar ya da yaygın kullanılan adıyla *Etiket Anahtarlama Yönlendiricileri (Label Switching Router - LSR)* kendisine gelen bir paketi anahtarlamak için paketi aldığı linkteki etiketi koyduğu linkteki ile değiştirerek iletimi sağlar yani *etiket değişimi* ile iletim gerçekleşir. LSR'lar standart OSPF, BGP gibi yönlendirme protokolleri ile çalışırlar. Genel anlamda LSR denilen cihazlar öncül teknolojilere göre özel isimlere de sahiptirler. *Hücre Anahtarlayici Yönlendirici (Cell Switching Router - CSR), IP Anahtari (IP Switch), Takı Anahtarlayıcı Yönlendirici (Tag Switching Router – TSR)* ve *Bütünleşik Anahtar Yönlendirici (Integrated Switch Router - ISR)* teknolojiye özel LSR isimleridir. [2]

Her üreticinin kendine özgü olan bu teknolojiler daha sonra Cisco System şirketinin öncülüğünü yaptığı bir IETF çalışma grubu ile standardize edilmiş ve bu teknolojilerin iyi özellikleri mümkün olduğunda bir araya getirilerek *Çok Protokollü Etiket Anahtarlama – MPLS (Multiprotocol Label Switching)* teknolojisi oluşturulmuştur.

MPLS teknoljisinin hızla yaygınlaşarak standardlaşma yoluna girmesinin birçok nedeni vardır. Bunun en önemli nedenleri anahtarlama hızında yönlendirmeye olan ihtiyaç ve

yönlendirici maliyetlerinin uygun fiyat avantajından tasarım amaçlı olarak faydalanabilme isteğidir.

MPLS'in hızla yaygınlaşmasında en önemli etkenlerden biri de o ana kadar kullanılmakta olan iletim ve yönlendirme tekniklerinin çok yaygınlaşması ve ortaya çıkan yeni ihtiyaçlar doğrultusunda iletim mekanizmalarının değiştirilmesinin oldukça karmaşık ve zorlu bir iş olmasıdır. MPLS teknolojisinin en çekici yanlarından biri iletim algoritmasının (etiket değiştirme) oldukça basit olması ve yeni ihtiyaçlar doğrultusunda üzerinde değişiklik yapmayı gerektirmeden yeniliklere olanak vermesidir. Çok sayıda yeni kontrol modülü anahtarlama sürecini etkilemeyecek şekilde ayni iletim algoritması üzerinde desteklenebilir. Yeni bir yönlendirme fonksiyonuna ihtiyaç duyulduğunda iletim algoritmasının donanım ya da yazılım üzerine yerleştirilerek değişime ihtiyaç duymaksızın desteklenmesi mümkün olmaktadır. En basit örnek olarak IPv4'ten v6'ya geçişte iletim algoritması üzerinde bir değişikliğe gitmeye gerek yoktur. [2]

Tüm bu özellikler bir yana günümüzde hizmet sağlayıcı omurgalarında kullanılan ATM teknolojisinden MPLS'e doğru hızlı bir gidiş olmasının temel nedeni giderek yaygınlaşan çokluortam (multimedia) uygulamalarının büyük oranda hizmet kalitesi parametrelerine ihtiyaç duyması ve güvenlik amaçlı olarak paketlerin sanal özel ağlar VPN (Virtual Private Network) üzerinden taşınmasına olanak vermesidir. ATM teknolojisi de oldukça geniş bir QoS spekturumu sunmaktadır ancak MPLS buna ek olarak daha önceki teknolojilerde olmayan etiket yığını taşımasını sağlayarak iki düğüm arasındaki haberleşmenin ara düğümlerden soyutlanmasına ve böylece geniş alan ağı üzerinden yerel ağın genişletilmesine ve güvenli iletişimi izin vermektedir.

Son olarak MPLS teknolojisinin getirdiği diğer bir üstün özellik trafik mühendisliği uygulamalarını desteklemesidir. Trafik mühendisliği ile ağdaki trafiğin bir yada birden fazla yolu ne şekilde alacağına, buna bağlı olarak trafik sınıflarının performans karakterlerine müdahale edilebilmekte ve böylece ağdaki bandgenişliğinin etkin kullanımı sağlanabilmektedir. Trafik mühendisliği tezimiz kapsamında incelenmemektedir.

Tezimiz kapsamında MPLS teknolojisinin bahsedilen özellikleri detaylı bir incelemeye tabi tutulmaktadır. İkinci bölümde MPLS öncesi teknolojiler incelenmiş, üçüncü bölümde

tüm bu teknolojilerin ortak özellikleri olan etiket anahtarlama teknolojisinin temel protokolleri ve yapısı detaylı olarak açıklanmıştır. 4. bölümde MPLS teknolojisi ve kullanılan protokoller, etiket yapısına yer verilmiş, 5. bölümde etiket yığını kullanımı ile VPN oluşturulması ve IP paketlerinin MPLS omurgası üzerinden tünelleme yoluyla aktarımı incelenmiştir. 6. bölümde MPLS VPN ağlarında hizmet kalitesi parametreleri, hizmet sınıflarının oluşturulması, paket ve protokol yapıları detaylı olarak açıklanmıştır. Tezimizin 7. bölümünde ise gerçek bir ağ platformunda MPLS omurgası kurularak, bu omurga üzerinde VPN ve DiffServ ile servis kalitesi uygulamalarına yer verilmiş ve bu uygulamaların paket iletimi üzerindeki etkileri analiz edilmiştir. Tezimizin 8. bölümünde daha kurulmuş olan MPLS/VPN topolojisi NS simülasyon platformuna aktarılarak TCL dilinde geliştirilen simülasyon topolojisi üzerinde paket kaybı (packet loss), gecikme (delay) ve seğirtim (jitter) gibi temel QoS parametrelerinin omurga bandgenişliğindeki değişikliklere göre değişimi incelenmektedir. Sonuç bölümünde ise tezin genel bir değerlendirilmesi yapılmakta, önerilerde bulunulmaktadır.

2. MPLS ÖNCESİ TEKNOLOJİLER

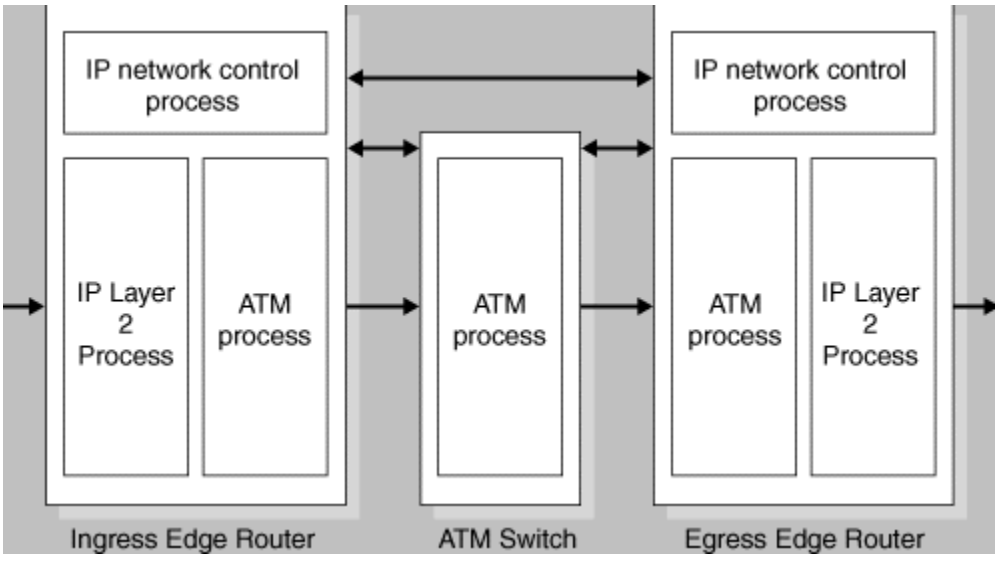
MPLS teknolojisi ortaya çıkarılmadan önce etiket ya da benzeri başlık takılarına dayanarak anahtarlama ile iletim başka teknolojilerde de kullanılmıştı. Bunlar *Ipsilon* firmasının geliştirdiği ve bugün genel bir haberleşme kavramı ile eş anlamlı hale gelen *IP Anahtarlama (IP Switching)* teknolojisi, ondan önce *Toshiba* firmasının geliştirdiği *Hücre Anahtarlamalı Yönlendirici (Cell Switching Router - CSR)* teknolojisi, *IBM*'in *Bütünsel Rota-tabanlı IP Anahtarlama (Aggregate Route-based IP Switching - ARIS)* ve MPLS'in temel dayandığı öncül teknoloji olan *Cisco*'nun *Takı Anahtarlama (Tag Switching)* ve geliştirildiği yıllarda yüksek hız ile geleceğin teknolojisi olmaya kesin gözüyle bakılan ancak var olan IP mimarisinin yaygınlığı nedeniyle gözden düşen ATM üzerinden IP paketlerinin taşınması prensibine dayanan *IP over ATM* teknolojileridir. Bu bölümde bu teknolojiler arasından MPLS'e katkıları en üst düzeyde olan IP over ATM, IP Switching ve Tag Switching teknolojilerinden kısaca bahsedeceğiz.

2.1 IP over ATM

IP paketlerinin ATM üzerinde taşınması 1980'lerden beri üzerinde çalışılan bir konudur. Bu amaçla çeşitli çalışma grupları oluşturulmuş ve standardizasyon yolunda ilk adım 93-94 yıllarında yayınlanan RFC 1483 ile atılmıştır. Daha sonra RFC 1577 ile Klasik IP over ATM modeli ortaya konmuştur.

ATM mimarisi IP mimarisinden tamamen farklı olduğu için bir bütünlük sağlamak zordur. IP *Datagram* ile *bağlantısız* haberleşme kullanırken ATM *Sanal-devre temelli bağlantılı* bir haberleşme sağlamaktadır. IP ile ATM'in adresleme, kaynak atama gibi yöntemleri ve katmanlı yapısı da birbirlerinden farklıdır. Bu nedenle bu iki mimariyi bütün halde kullanabilmek en büyük problemlerden biri olarak haberleşme dünyasını yillarca meşgul etmiştir.

İlk ortaya çıktığı zamanlarda genel inanış ATM teknolojisinin baskın teknoloji olarak IP'nin yerini alacağı yönünde idi ancak geçen zaman IP'nin oturmuş protokol yapısının ATM ağlarında da kullanılmaya devam ettiğini ve ATM ağlarının ağırlıklı olarak IP paketlerini taşımaya devam ettiğini göstermiştir. ATM'in WAN için tasarlanmış yüksek hizli mimarisi onun aynı zamanda ağların omurgada kullanılabilmesini gündeme getirmiştir. Günümüzde birçok servis sağlayıcı omurgada ATM çalıştırmakta, yüksek hızlı ATM anahtarın etrafında ise çok sayıda görece düşük hızlı yönlendiriciler bulunmaktadır (Şekil 2.1). Bu tip ağlara *Kaplama Modeli (Overlay Model)* adı verilir. Bu tip ağlarda temel mantık ATM ağının internetwork haberleşme için çekirdekte yüksek hızlı bağlantı sağlaması ve sanal devrelerle ATM anahtara bağlı IP ağlarının yerelde IP datagram iletimini devam ettirmesidir.



Şekil 2.1: Kaplama (Overlay) Model

IP paketlerinin ATM omurgası üzerinden taşınması *IP over ATM* olarak adlandırılır. IP over ATM problemi ve standardizasyon üzerine çalışan çok sayıda çalışma grubu mevcuttur. *IP over ATM Working Group, IP over Large Public Data Networks (IPLPDN) ve Routing over Large Clouds (ROLC), LAN Emulation Working Group,Multiprotocl over ATM (MPOA) Working Group ve Integrated Services over Specific Link Layers (ISLL) Working Group* bunların en önemlileridir. Temel amaç birbirinden tamamen bağımsız olarak tasarlanan IP ile ATM'in farklı adresleme, yönlendirme, kaynak atama

yöntemleriyle çalişan iki farkli protokol mimarisi olarak kullanımına devam etmek yerine doğrudan ATM mimarisi üzerinde IP mekanizmalarının çalışmasını sağlayabilmektir. Bu yapıda ATM anahtarlar etiket değiştirme ile paket iletmeye devam edecek ancak iletim/yönlendirme tabloları ve kaynak atama mekanizmaları IP ile kontrol edilecektir. Böylece ATM anahtarlar IP ile ATM ağlar arasında eşleştirme (mapping) yapmaya gerek bırakmayacak IP yönlendiricilere dönüşmektedir. IP over ATM'den MPLS'e geçiş bu şekilde olmuştur. [2]

İkinci katmanda *tam-bağlı (full-mesh)* bir topolojik yapı düşünelim. *n* adet yönlendiricinin bulunduğu ağda en az *n.(n-1) / 2* adet sanal devre yönlendiriciler arasında kurulmalıdır. Yönlendiriciler çalışırken doğrudan bağlı oldukları yönlendiriciler ile *komşuluk* kurar. Overlay model ile çalışan bir topolojide omurgada çalışan ATM anahtarlar ağda *görünmez* durumdadırlar. Yani IP yönlendiricilerin doğrudan komşuluk kurabilmesi için birbirlerine ATM anahtarlar üzerinden sanal devrelerle bağlanması mümkündür. Böyle bir topolojide ağa yeni eklenmek istenen bir yönlendirici olduğunda *n* tane daha sanal devrenin daha ağa eklenmesi gerekir. Her yönlendirici diğerleri ile doğrudan bağlı olduğu için herbirinin yönlendirme tablolarındaki bilgileri kendi tablosuna alır böylece yönlendiriciler üzerindeki yönlendirme bilgileri gerek olmamasına karşın artan yönlendirici sayısı ile çok yüksek boyutlara ulaşarak yönlendiricinin taşıyamayacağı bir seviyeye gelebilir. Bu ciddi anlamda bir *ölçeklenebilirlik* problemini içinde barındırmaktadır. [2]

Klasik IP over ATM modelinde IP cihazlarının farklı alt-ağlarda olabilecek şekilde ATM çekirdeğine bağlanması öngörülmüştü. Bunun için Mantıksal IP Alt-ağı kavramı *(LIS – Logical IP Subnet)* kavramı geliştirilmişti. LIS, aynı alt-ağ adresini paylaşan bir ATM ağı ve buna bağlı IP cihazlarına verilen isimdi. Buna göre bir LIS'ten diğerine geçiş aradaki yönlendiriciler üzerinden olacaktı. Burada dikkat çeken nokta aynı ATM ağına bağlı ancak ayrı LIS'lerdeki iki IP cihazının haberleşirken doğrudan bir sanal devre üzerinden değil bir yönlendirici üzerinden haberleşmesinin gerekmesiydi. Bu performansı düşüren bir sorundu. Bunun için tüm ATM ağının aynı LIS üzerinde olması önerildi ancak bu kez de karşımıza yönetimsel karmaşıklığın artması sorunu çıkmaktaydı. Örneğin aynı ATM çekirdeğine bağlı iki ayrı kurumun aynı alt-ağ adresini kullanması beklenemezdi.

Klasik IP over ATM modelinde RFC 1577 ile ortaya konulan kavramlardan biri de *ATMARP* idi. ATM Adres Çözüm Protokolü (ATM Address Resolution Protocol) ile aynı LIS üzerinde yer alan iki IP cihazının aynen ethernette olduğu gibi birbirlerinin ikinci katman (burada ATM) adreslerini öğrenmek için kullandıkları yöntemdir. Bilindiği gibi ethernet üzerinde ARP protokolu veri bağı katmanı tüm-yayın (broadcast) prensibine dayanır. ATM üzerinde ikinci katman tüm-yayın mümkün olmadığı için ATMARP için bir sunucuya ihtiyaç vardır. [18]

RFC 1577 ile çözülemeyen farklı LIS'ler üzerinde yer alan IP cihazlarının haberleşebilmesi problemi için *Routing over Large Clouds (ROLC)* çalışma grubu kurulmuştur. Iki IP cihazın bir yönlendirici üzerinden haberleşmesi zorunluluğu *Sonraki Sekme Çözüm Protokolu (NHRP – Next Hop Resolution Protocol)* ile çözülmüştür. Burada ayrıntılarına girmediğimiz NHRP protokolü ile farklı alt-ağdaki iki IP cihazı birbirleriyle aradaki yönlendiriciye gerek duymaksızın haberleşebilmektedir. Bunun için aynen ATMARP'ta olduğu gibi ikinci katman adresinin öğrenilmesini sağlayan bir yöntem kullanılmakta ve böylece iki cihaz arasında sanal devre kurulabilmektedir. Bu çözümde de ortamda NHRP sunucularına ihtiyaç vardır. [2]

Zaman içerisinde ortaya çıkan IP over ATM uygulamaları ile temel amaç tamamen bağımsız olarak tasarlanan IP ile ATM'in farklı adresleme, yönlendirme, kaynak atama yöntemleriyle çalışan iki farklı protokol mimarisi olarak kullanımına devam etmek yerine doğrudan ATM mimarisi üzerinde IP mekanizmalarının çalışmasını sağlayabilmeye dönüsmüstür. Bu yapıda ATM anahtarlar etiket değiştirme ile paket iletmeye devam edecek ancak iletim/yönlendirme tabloları ve kaynak atama mekanizmaları IP ile kontrol edilecektir. Böylece ATM anahtarlar IP ile ATM ağlar arasında eşleştirme (mapping) yapmaya gerek bırakmayacak IP yönlendiricilere dönüşmektedir. IP over ATM'den MPLS'e geçiş bu şekilde olmuştur. MPLS mimarisi ilk bölümde bahsedilen komsuluk kurma problemi, ATMARP, NHRP, overlay modelden kaynaklanan ölçeklenebilirlik problemlerini ve karmaşıklığı ortadan kaldırdığı için IP over ATM'in yerini almaya başlamıştır. [2]

2.2 Ipsilon IP Anahtarlama (IP Switching)

IP Anahtarlama teknolojisi, etiket anahtarlama ve etiket değiştirme ile iletim tekniklerini kullanan bir teknolojidir. Bu teknoloji ile bir etiket dağıtım protokolünün yanı sıra *GSMP (General Switch Management Protocol)* adı verilen bir anahtar yönetim protokolü de tanımlanmıştır. Bu protokol ile standart bir ATM anahtar bir IP anahtar haline dönüştürülmektedir.

IP Anahtarlama teknolojisinin ardında yatan temel neden de IP over ATM modelinin oldukça karmaşık olması ve etkin çalışmamasıdır. IP Anahtarlama IP over ATM yöntemindeki gibi ikinci katmanda ATM protokollerini çalıştırıp üçüncü katmanda IP yürütmez. Bunun yerine diğer etiket anahtarlama teknolojilerinde olduğu gibi yalnızca IP bileşenleri ile bir etiket dağıtım protokolu kullanır. IP anahtarlamada etiket dağıtım protokolü *Ipsilon Akış Yönetim Protokolü'dür (IFMP - Ipsilon Flow Management Protocol).* Şekil 2.2 ve 2.3'te bu yapılar net olarak görülmektedir. [2]

<table>
<tr><td colspan="3">IP</td></tr>
<tr><td>ATM ARP</td><td>MARS</td><td>NHRP</td></tr>
<tr><td colspan="3">PNNI</td></tr>
<tr><td colspan="3">Q.2931</td></tr>
<tr><td colspan="3">ATM Hardware</td></tr>
</table>

Şekil 2.2: Standart IP over ATM

<table>
<tr><td>IP</td><td>IFMP</td></tr>
<tr><td colspan="2">ATM Hardware</td></tr>
</table>

Şekil 2.3: Ipsilon IP Anahtarlama

Şekilden görüldüğü üzere ATM donanım yapısını doğrudan kontrol eden bir etiket dağıtım protokolü (IFMP) mimariye entegre edilmiştir.

ATM kontrol tabakasına olan ihtiyaç ortadan kaldırıldığı için IP anahtarlamada IP anahtarlar birbirleriyle doğrudan bağlantı kurabilecekleri gibi, ATM bulutu üzerinden de sanal devreye kurmaya devam edebilirler.

Ipsilon IP Anahtarlama teknolojisi ATM anahtarların performans özelliğini yönlendirme fonksiyonuyla birleştirmektedir. Günümüzde yüksek performans sağlayan hızlı yönlendiriciler ATM anahtarların performansına erişememiş olduğu için bu büyük bir getiridir. IP Anahtarlama teknolojisi ayrıca son derece karmaşık bir yapı halini alan IP-ATM eşleme işlemine olan gereksinimi kaldırarak ATM kontrol protokollerine olan ihtiyacı ortadan kaldırmıştır. [20]

Ipsilon IP Anahtarlama teknolojisi de RFC yayınlanarak açık bir standard haline getirilmiştir. Burada açıklanan yapı MPLS teknolojisinin de oluşmasında rol oynamıştır. Özellikle burada açıklanan basit anahtar kontrol protokolü GSMP ve bir dış kontrolör yardımı ile ATM anahtarların IP anahtarlara dönüştürülmesi oldukça ilgi görmüştür. İlk ortaya koyulduğunda büyük ilgi çeken bu teknoloji Cisco Takı Anahtarlama (Tag Switching) ve daha sonra MPLS teknolojilerinin ortaya çıkmasıyla standartlaşamadan önemini kaybetmiştir.

2.3 Cisco Takı Anahtarlama (Tag Switching)

Ipsilon firmasından birkaç ay sonra Cisco Systems etiket anahtarlama konusunda yeni bir yaklaşım olan Takı Anahtarlama teknolojisini duyurdu. IP Anahtarlama teknolojisinden farklı olarak Takı Anahtarlama teknolojisi yalnızca ATM donanımları üzerinde çalışmakla sınırlı değildi. IP yönlendiriciler üzerinde Takı Anahtarlama çalıştırabilmek için herhangi bir donanımsal değişiklik yapmak gerekmez. ATM anahtara üzerinde ise yazılımsal bir güncelleme yapmak yeterlidir.

Takı Anahtarlama terminolojisinde etikete denk düşen bilgilere *takı,* üzerinde Takı Anahtarlama çalışan donanımlara *Takı Anahtarlayıcı Yönlendirici – TSR (Tag Switching Router)* adı verilmiştir. Sınırda yer alan ve takısız paketleri takılı hale getiren sınır TSR'lara ise *Takı Sınır Yönlendiricisi – TER (Tag Edge Router)* adı verilmiştir. Her TSR kendi üzerinde geliş ve gidiş hatlarına ait geliş ve gidiş takı bilgilerini bir *Takı İletim Bilgi Tablosu – TFIB (Tag Forwarding Information Base)* tablosunda tutmaktadır.

Takı Anahtarlamanın da temel amacı ATM anahtarın performansı ile IP yönlendirici fonksiyonlarını yerine getirebilmektir. Bunun için Takı Anahtarlama teknolojisi performans ve ölçeklenebilirliği arttırmak üzerine odaklanmıştır.

Takı Anahtarlama teknolojisinde aynen IP yönlendirmede olduğu gibi hedef ağ adresleri ve bu adreslere gitmek için kullanılacak sonraki-sekme bilgisi bir tabloda tutulur. Ancak farklı olarak bu ağ adreslerine ilişkin bir takı belirlenerek bu bilgi iletimde kullanılmak üzere tabloya yazılır. MPLS'te de göreceğimiz üzere bu hedef adres bilgilerine *iletim denklik sınıfı – FEC (forwarding equivalence class)* adı verilir. [5]

FEC bilgileri alınınca TSR'lar bu FEC'e ilişkin kendi takı havuzlarından bir takı belirleyerek bunu tablolarına yazarlar. Daha sonra bu bilginin iletim sırasında kullanılabilmesi için bunu diğer TSR'lara yollarlar. Bunu alan TSR bu FEC'e ilişkin takı bilgisinin kendisinde var olup olmadığına bakar, eğer yoksa ve bu bilgi o FEC'e ilişkin kendisine göre sonraki-sekme konumunda olan TSR'dan geldiyse bu bilgiyi tablosuna alır ve çıkış takısı olarak belirler. Böylece tüm TSR'larda hangi FEC'e hangi takıyı koyup hangi porttan göndereceği bilgisi oluşur. Takıların TSR'lar arası dağıtımında *Takı Dağıtım Protokolü – TDP (Tag Distribution Protocol)* kullanılır. [2]

İlerleyen kısımlarda MPLS'te de göreceğimiz gibi Takı Anahtarlama teknolojisi tamamen günümüzdeki MPLS protokolü mantığı ile çalışmaktadır. Cisco Systems tarafından bu teknoloji IETF yoluyla standard haline getirildikten sonra teknolojide çok fazla değişiklik olmaksızın bir açık standard haline gelmiş ve çok protokollülük desteği olduğu için yeni bir isim ve terminoloji ile kullanılmaya başlanmıştır.

3. ETİKET ANAHTARLAMA TEMEL KAVRAMLAR

Bu bölümde MPLS teknolojisinin temelini oluşturan etiket anahtarlama kavramı ve temel protokolleri incelenecektir. İlk olarak ağ katmanında çalışma anlatılacak ve buradaki fonksiyonel olarak belirlenen denetim ve iletim bileşenleri incelenecektir. Bu bileşenlerdeki tasarım kriter ve alternatifleri incelenecek, daha sonra etiket atama ve anahtarlamadaki temel protokol ve prensiplerden bahsedilecektir.

3.1 Geleneksel Ağ Katmanı – Denetim ve İletim Düzlemleri

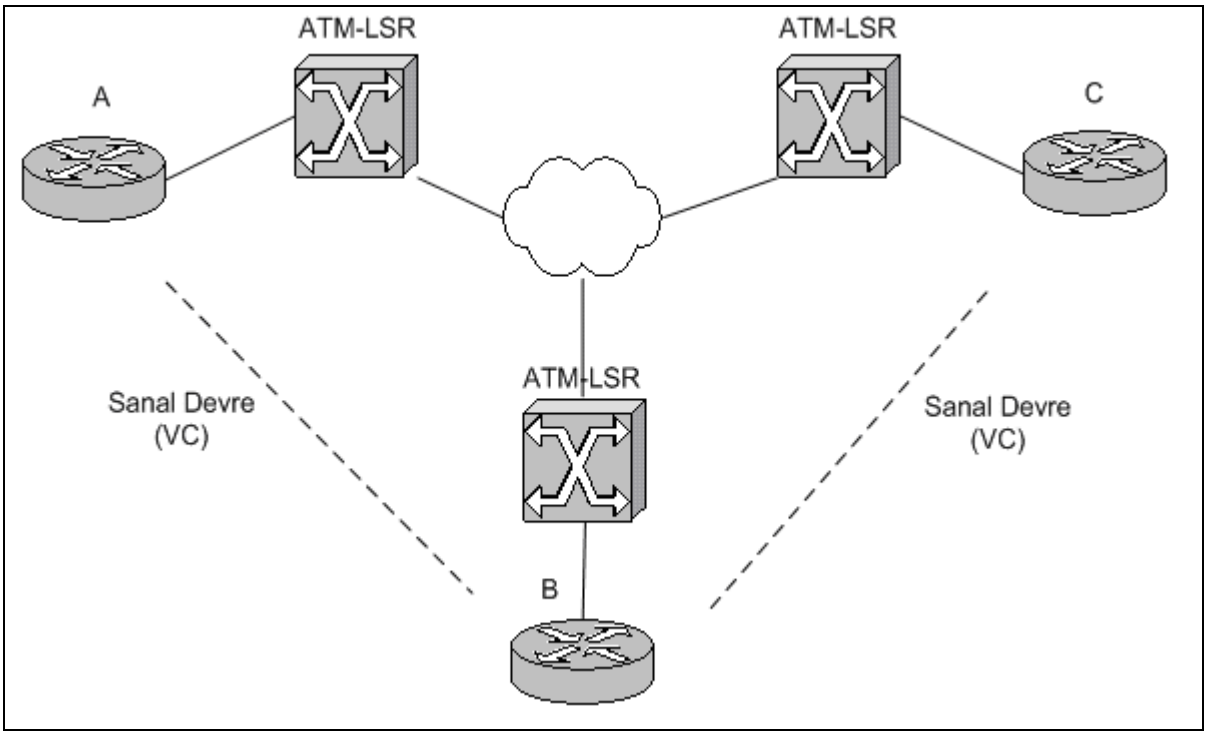
Geleneksel IP iletim yöntemine baktığımız zaman hedef IP adresi bilgilerinin her pakette incelenerek iletim yapıldığını görürüz. Yani ağdaki yönlendiricilerin tamamı paket kendilerinden geçerken paketi açar inceler. Bu yöntemin bir takım yetersizlik ve eksiklikleri mevcuttur. Bu tip ağlarda yol oluşturma dinamik yönlendirme protokolü ile ya da statik rota ile bulunur. Eğer varış ile kaynak arasında birden fazla yol varsa kullanılan protokolün niteliğine bağlı olarak yük dengelemesi ya da paylaşımı yapılabilir (OSPF eşit ağırlıklı hatlar arası yük dengeleme yapabilirken EIGRP ile eşit ağırlıklı olmayan hatlar arasında da dengeleme yapılabilir).

Ağ üzerindeki yönlendiriciler birbirlerine doğrudan noktadan-noktaya bağlanabilecekleri gibi LAN ya da 2. katman anahtarlar (FR ya da ATM) üzerinden WAN ile de bağlanıyor olabilirler. Bu durumda paketler 2. katman anahtarlardan geçer ancak bu cihazlar 3. katman bilgisine göre değerlendirme yapamadıkları için yönlendirme prosedüründe yer alamazlar.

WAN bağlantıları genellikle noktadan-noktayadır. Bu durumda arada bir sanal devre (VC) kurmak gerekebilir. Bir yönlendirici WAN üzerinden diğer bir yönlendiriciye paket göndermek istediğinde aradaki sanal devrenin kurulmasını beklemelidir.

Şekil 3.1'deki gibi bir topolojide A ile C haberleşmek istediği zaman aralarında bir sanal devre bağlantısı olmadığı için bağlantının B üzerinden yapılması gerekir. Bu durumda

tüm haberleşen çiftleri arasında sanal devre kurulması gerektiği için kaynakların verimsiz kullanımı söz konusu olmaktadır. Büyük ölçekli ağlarda tam-bağlı bir yapının kurulması ölçeklenebilirlik problemini de beraberinde getirir. Ağa yeni bir yönlendirici eklendiğinde onun tüm önceki yönlendiricilerle sanal devre bağlantılarının kurulması gerekir. Dahası ağdaki tüm yönlendiricilerin birbirleriyle sanal devre kurması demek komşuluk oluşması anlamına gelir. Bu durumda tüm yönlendiriciler ağdaki diğerleri ile tablo değişimi ve güncelleme yapacağından yönlendirme tabloları çok yüksek boyutlara ulaşır, böylece ağdaki güncelleme bilgileri ile trafik artarken yayılım gecikmesi artar. [2]



Şekil 3.1: Sanal Devre üzerinden haberleşme

Ağda oluşabilecek bir diğer problem de kurulum aşamasında ağdaki iki yönlendirici arasında oluşabilecek trafik tam olarak bilinemeyeceği için hatta verilecek hizmet tipinin tam tespit edilememesidir. Bunun için çoğu servis sağlayıcılar kurulumu kolaylaştırmak için eksik servis garantisi verirler. Sadece IP ya da 2. katman servisleri veren ISP'ler için bu bahsedilenler büyük problem değildir ancak ISP'lerin çoğunda yüksek performans ihtiyacını karşılamak için omurgada ATM teknolojisi kullanılmakta ve Şekil 3.1'deki gibi '*kaplama - overlay*' modeli tercih edilmektedir. Sonuç olarak bize gereken 3. katman

bilgisini kaynaktan varışa aktaran ancak aradaki anahtarların da yönlendirme sürecinde yer aldığı bir yapıdır. [1]

Ağ katmanı iki ana bileşene ayrılabilir. Bunlar denetim ve iletim düzlemleridir. *Denetim düzlemi* paketlerin girişten çıkışa anahtar ya da yönlendirici üzerinden iletiminden sorumludur. Paketlerin iletimi için iki bilgi kaynağı kullanılır; yönlendirici tarafından oluşturulan iletim tablosu ve paketin kendi içinde taşınan etiket bilgisi. Denetim bileşeni iletim tablosunun oluşturuluması ve güncellenmesinden sorumludur. Bunun için standard IP yönlendirme protokolleri kullanılır.

İletim düzleminde paketlerin iletimine karar verme süreci birkaç prosedüre bağlıdır. İletilen paket bir tekyayın paketi ise karar verme hedef adrese göre gerçekleşir. Yönlendirici iletim tablosuna bakar en uzun eşleşme kriterine göre çıkış aradüzlemi seçilir. Eğer gönderilen paketin ToS - hizmet tipi biti çekili ise iletim tablosu incelenirken ToS bitinin de eşleşmesi beklenir. Gönderilen paket bir çokluyayın paketi ise giden paketin kaynak, hedef adresleri ve geldiği arayüz bilgisi de dikkate alınır.

3.1.1 İletim Denklik Sınıfları

İletim tablosunda bilgiler ağ adresleri ile tutulur. Tabloda bir arama yapılmak istendiğinde yönlendiricinin maskesi ile hedef adres ‘ve’ işlemine tabi tutulur ve çıkan ağ adresine göre çıkış arayüzü belirlenir. Dolayısıyla aynı alt ağ içerisinde yer alan tüm hedef adreslere giden paketler aynı işleme tabi tutulur. Bu nedenle bu tip adresler aynı *İletim Denklik Sınıfı (Forwarding Equivalence Class - FEC)* içerisinde değerlendirilir.

Eğer iletilen paketin ToS biti çekili ise daha önce söylediğimiz gibi ağ adresine göre arama yapmanın yanısıra ToS değerinin de eşit olması beklenir. Bu nedenle aynı alt ağda bulunan ancak farklı ToS değerlerine sahip paketler farklı FEC içerisinde değerlendirilirler. [1] [2]

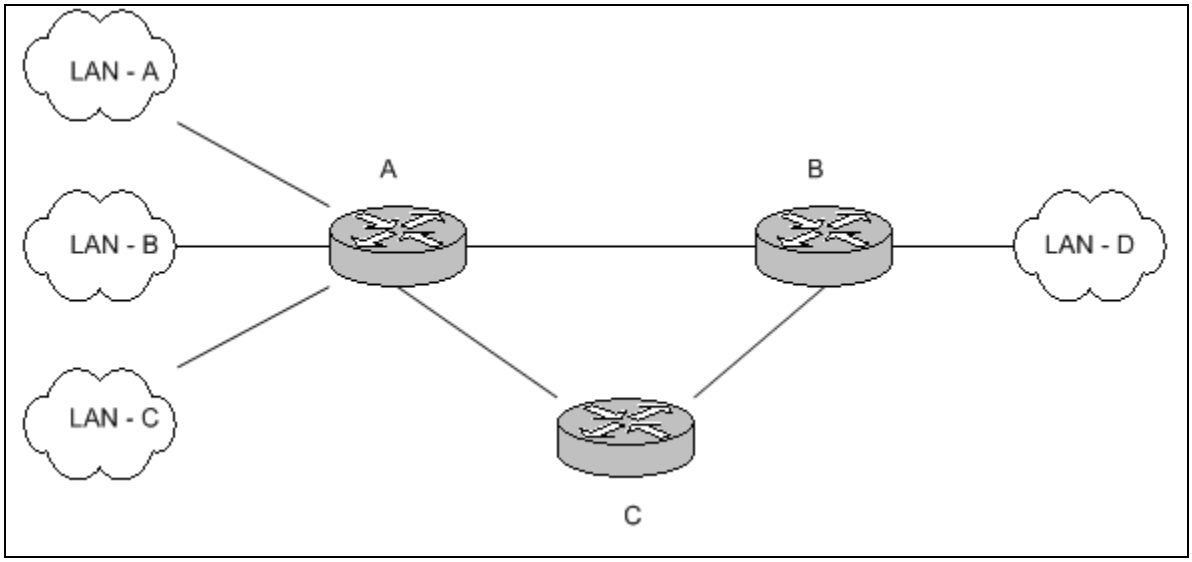
3.2 Etiket Anahtarlama İletim Düzlemi

Ağ katmanındaki iletim ve denetim düzlemleri ayrımı etiket anahtarlama teknolojilerine de uygulanabilir. Etiket anahtarlama iletim düzleminde iletim kararını vermek için iki

kaynak kullanılır; Etiket Anahtarlayıcı Yönlendirici (LSR) tarafından oluşturulan iletim tablosu ve paket içerisindeki etiket bilgisi.

3.2.1 Etiket Anahtarlama ile İletim

Geleneksel IP yönlendirmede Şekil 3.2'deki gibi bir yapıyı ele alalım.



Şekil 3.2: Farklılaştırılmış paket servisleri

Burada A ile B arasındaki yolun LAN A,B,C ile LAN D haberleşmesinde kullanıldığını düşünelim. A-B yolu çok yüklü iken A-C ve C-B yollarında trafik az olabilir. Bu durumu engellemek için A yönlendiricisi üzerinde '*Politika Tabanlı Yönlendirme – PBR (Policy Based Routing)*' uygulanmalıdır ki bu da performansı büyük ölçüde etkiler. Oysa bunun yerine örneğin LAN C'nin çıkış geçit yönlendiricisinde kendi trafiğinin A-C ve C-B yollarını takip etmesini istediği söylenebilmelidir. Ayrıca aynı IP ağına giden paketlerin farklı yolları izlemesi sağlanabilmeli ve sadece hedef IP adresine göre değil, ihtiyaç duyulan servis kalitesi ya da port numarası gibi bilgiler ile de iletim gerçekleştirilebilmelidir. Bunun için *etiketleme* yapılmalıdır. [2]

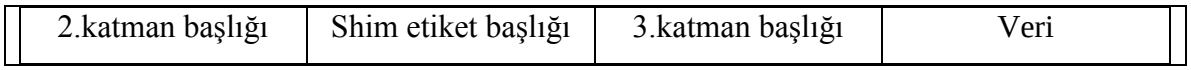
Etiket, kendi başına bir anlam taşımayan, tüm ağda ya da LSR başına ya da arayüz başına anlam taşıyan, kısa sabit uzunluklu paket içi bilgidir.

Etiket kullanımı ile yönlendirme tablosunda bir değişiklik olduğunda yeni bir etiket ataması ile IP yönlendirmedeki birleşim (convergence) gecikmesine maruz kalmadan sistemin çalışmasına devam etmesi sağlanabilir. Birleşim gecikmesi ağdaki tüm

düğümlerin aynı geçerli bilgiye sahip olmaları için geçen süredir. Diğer bir konu da; Şekil 3.2'den bakarsak A ve B yönlendiricileri üzerlerine gelen paketleri geçiriyorlar ancak buna rağmen birbirlerine komşu tüm ağ bilgilerini tablolarında bulunduruyorlar. Oysa etiket kullanımı ile bu yönlendiriciler 3. katman bilgisine bakmayacakları için doğrudan anahtarlama ile iletim yapabileceklerdir.

LSR tarafından oluşturulan iletim tablosunda her bir giriş için, geliş etiketi, çıkış etiketi, çıkış arayüzü ve sonraki sekme adresi bilgileri tutulur. Çok sayıda giriş için aynı etiket yer alabileceği gibi çokluyayın trafiğinde olduğu gibi tek bir giriş için farklı etiketler de tutulabilir. Bunun yanısıra tabloda, gelen bir paketin hangi kaynakları kullanacağı ya da hangi çıkış kuyruğuna alınacağı bilgisi de yer alabilir. Bir LSR tüm arayüzlerini içeren tek bir iletim tablosu tutabileceği gibi her bir arayüz başına ayrı birer tablo oluşturabilir böylece paketler yalnızca geliş etiketlerine göre değil geldikleri arayüze göre de farklı prosedürlere tabi tutulabilir.

Etiket bilgisi 2. katman başlığının bir parçacı olarak taşınabilir. ATM'de VPI/VCI alanlarında taşınırken Frame Relay'de DLCI alanında taşınabilir ancak etiket anahtarlamayı 2. katman ile sınırlamak esnekliği azaltacağı ve ethernet ya da noktadan noktaya bağlantılardan geçişte problem yaratacağı için bunun yerine etiketin 2. ve 3. katman başlıkları arasına yerleştirilen 32 bitlik bir *Shim* başlık içerisinde taşınması uygundur. Böylece etiket 2. katmandaki kapsülleme yönteminden bağımsız olarak ağda dağıtılabilir. Şekil 3.3'te etiketin shim başlık ile taşınması görülmektedir. [1][2]



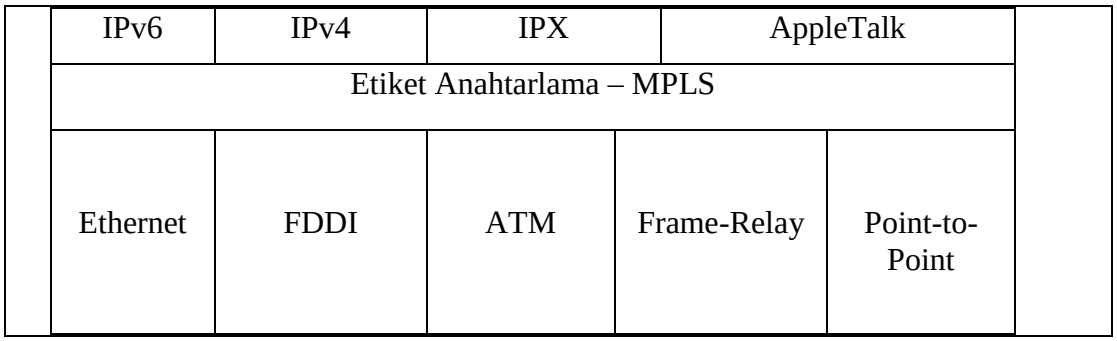
Şekil 3.3: Etiketin shim başlık ile taşınması

Etiket anahtarlama ile iletim, paketi alan her LSR üzerinde etiket bilgisinin değiştirilmesi prensibine dayalı olarak yürür. Bir LSR paketi aldığı zaman paketten etiketi kaldırır, iletim tablosuna bakar. Bulunan etiket kaydına denk düşen çıkış etiketi pakete yerleştirilerek aynı satırda yer alan çıkış arayüz bilgisi kullanılarak ilgili hattan gönderilir.

Geleneksel yönlendirmede denetim düzleminde çok sayıda özellik sağlandığı için (tekyayın, ToS ile tekyayın, çokluyayın gibi) iletim düzleminde bunları karşılamak üzere

farklı iletim algoritmaları çalışır. Ancak etiket anahtarlamada tüm fonksiyonlar için yalnızca *etiket değişimi* algoritması çalışır.

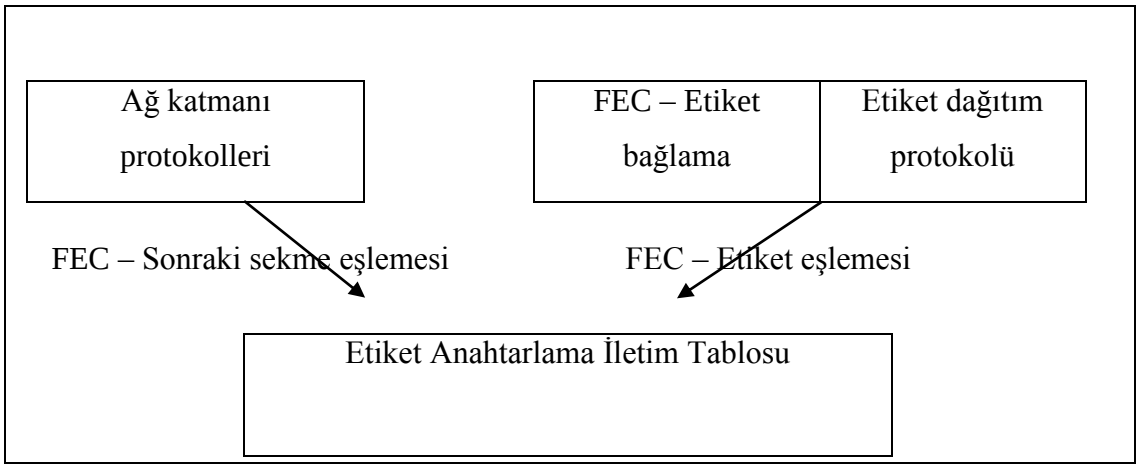
Etiket anahtarlama iletim düzlemi farklı ağ katmanı protokollerini beraberinde destekler. Aynı iletim düzlemi hem IP hem de IPX için beraber kullanılabilir. Aynı şekilde daha önce de belirttiğimiz gibi etiket anahtarlama farklı veribağı katmanı protokolleri ve kapsülleme yöntemleri üzerinde çalışabilir. Bu nedenle etiket anahtarlamaya dayanan yeni teknolojiye *Çok-Protokollü Etiket Anahtarlama (Multiprotocol Label Switching) – MPLS* adını vermeyi uygun görülmüştür. Şekil 3.4'te çok protokollülük desteği görülmektedir. [1][2]



Şekil 3.4: Çok-protokollü yapı

3.3 Etiket Anahtarlama Denetim Düzlemi

Etiket anahtarlama *denetim düzlemi* (a) yönlendirme bilgisinin LSR'lar arasında dağıtımından ve (b) yönlendirme bilgisinin etiket anahtarlama ile kullanılabilecek şekilde düzenlenmesi ve etiketlerle eşlenmesi işlerinden sorumludur. MPLS denetim düzlemi geleneksel yönlendirme mimarisinde bulunan tüm protokolleri destekler. MPLS denetim düzlemi geleneksel yönlendirme protokolleri ile oluşturulan bilgilerin yanı sıra; FEC etiket bağlamalarını ve bu bağlama bilgisinin diğer LSR'lara dağıtımını da sağlamak zorundadır. Geleneksel yönlendirme protokolleri ile sonraki sekme bilgisi oluşturulurken etiket bağlama ve dağıtım prosedürleri ile de FEC etiket eşlemeleri gerçekleştirilir. Denetim düzleminin genel yapısını Sekil 3.5'te görebilirsiniz.



Şekil 3.5: Etiket Anahtarlama Denetim Düzlemi

3.3.1 Yerel ve Uzak Etiket Bağlama

Daha önce de belirttiğimiz gibi LSR tarafından oluşturulan iletim tablosunda geliş etiketine karşılık bir ya da daha fazla çıkış etiketi yer alır. Bu iki etiket tipine karşılık olarak LSR iki tip etiket bağlama işlemi gerçekleştirir. Bunlardan ilki bir LSR yerel olarak kendi havuzundan bir etiket seçer ve bunu atarsa gerçekleşir, buna *yerel bağlama* adı verilir. Eğer bir LSR başka bir LSR'dan bir etiket bağlama bilgisi alır ve bunu atarsa buna *uzak bağlama* adı verilir. [2]

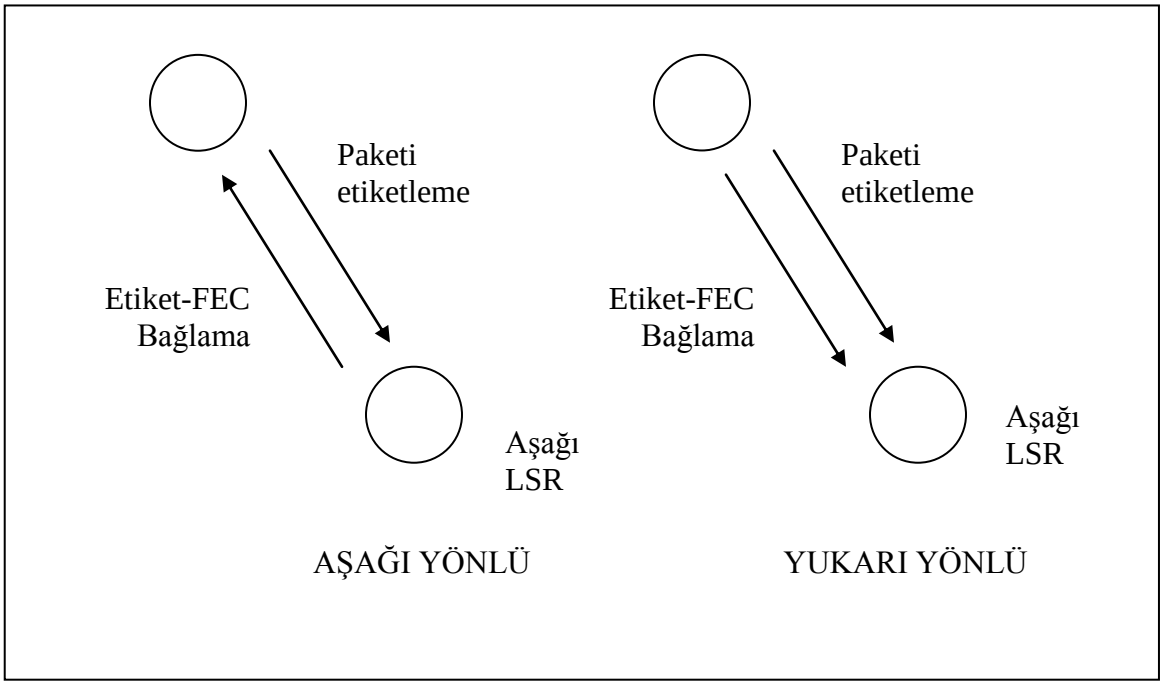
3.3.2 Yukarı (Upstream) ve Aşağı (Downstream) Yönlü Bağlama

Kullanılan yerel ve uzak etiket bağlama yöntemine bağlı olarak iki tip etiket atama yöntemi vardır. Bunlar yukarı ve aşağı yönlü atamalardır.

Eğer bir LSR yerel bağlama ile atadığı etiketleri geliş yönlü etiket olarak, uzak bağlama ile atadığı etiketi gidiş etiketi olarak kullanıyorsa bu tip etiket atamaya *aşağı yönlü* atama adı verilir. Eğer tam tersi söz konusu ise *yukarı yönlü* atama adı verilir. MPLS'de yaygın olarak aşağı yönlü atama kullanılır.

Aşağı yönlü atamada paket üzerinde taşınan etiket ile FEC bağlama işlemi etiketi pakete koyan LSR'a göre trafik yönüne göre sonraki sekme durumunda bulunan aşağı LSR tarafından yapılır. Yukarı yönlüde ise pakette yer alan etiket ile bir FEC arasındaki

eşleştirme işlemi etiketi pakete koyan LSR tarafından yapılır. Şekil 3.6'da iki yöntemin farkı görülmektedir.



Şekil 3.6: Aşağı ve Yukarı Yönlü Bağlama

Etiket atama için LSR'lar etiket havuzlarını kullanılırlar. Her LSR kendine ait olan kullanılmayan etiketlerin listesini etiket havuzunda tutar. LSR yeni bir yerel bağlama gerçekleştirdiğinde bu havuzdan boş bir etiket çekilir ve atanır. Bir etiket ağdan çıkarıldığında da etiket havuzuna geri koyulur.

Etiket bağlama ya da etiketi yok etme işlemi iki şekilde gerçekleşir; eğer etiketin atanması ya da kaldırlması veri paketleri yoluyla sağlanmışsa buna *veri yoluyla* etiket bağlama, denetim paketleriyle sağlanmışsa *denetim yoluyla* etiket bağlama adı verilir.

Denetim yoluyla bağlama tamamen denetim düzleminin denetiminde gerçekleştiği için, hem denetim hem de iletim düzlemlerinin rol almasını gerektiren veri yoluyla bağlamaya göre sisteme daha az karmaşıklık ve yük getirir. Veri yoluyla bağlama ise hattan ilk veri akışıyla birlikte arkadan gelen tüm verilerin etiketin atanmış olması nedeniyle hızla ardışık paketlerin gönderilmesini sağladığından performansa olumlu etki eder.

3.3.3 Etiket Bağlama Bilgisinin Dağıtımı

Bir etiket ile FEC arasındaki yerel bağlama ile bağ kurulduğu zaman bunun diğer LSR'lara bildirilmesi gerekir. Böylece komşu LSR'ların uzak bağ kurabilmeleri sağlanmış olur. Yani komşudan gelen bir paketin hangi arayüzden hangi etiket ile geleceği bilgisi elde edilir ki iletim bilgi tablosunda bu bilgiye karşılık bir çıkış satırı oluşturulabilsin. Etiket bağlama bilgisinin ağa dağıtılmasında kullanılabilecek iki temel yöntem vardır. Bunlar, "*Yönlendirme protokolünün üzerinde taşıma (piggybacking)*" ve "*Etiket Dağıtım Protokolü - LDP*" kullanımıdır.

Piggybacking yöntemi yalnızca denetim yoluyla bağlama gerçekleşen durumlarda geçerlidir çünkü etiket-FEC bağlama bilgisinin taşıması yönlendirme protokolünün üzerinde gerçekleştirilir. Bunun için öncelikle etiket bağlama bilgisi ile yönlendirme bilgisi tutarlı hale getirilmelidir. Etiket bilgisinin var olduğu ancak ilgili FEC için yönlendirme bilgisinin olmaması gibi durumlar ortadan kaldırılmalıdır. Bu yöntem ağda ağrı bir etiket dağıtım protokolüne gerek duymadığı için karmaşıklığı azaltır ve operasyon basitleşir. Bu yöntemin dezavantajları ise kullanılan yönlendirme protokollerinin tümünün yönteme uygun olmamasıdır. Bağ-durumu algoritmaları (OSPF vb.) çalışma prensipleri gereği bunu desteklemezler ancak BGP ve PIM bu yöntem için uygun protokollerdir. [1][2]

Etiket Dağıtım Protokolü (LDP) piggybacking desteklemeyen protokollerin kullanıldığı durumlar için çok uygundur. Ancak sistemde fazladan bir protokol çalıştığı için karmaşıklığı ve zorluğu arttırmaktadır. Ayrıca LDP kullanıldığı durumlarda çelişki ile karşılaşıldığında yani etiket bilgisi var olan ancak sonraki sekmenin tayin edileceği yönlendirme bilgisi bulunmayan FEC durumlarında sorunu gidermek çok daha zordur. Ağda yalnızca bir tane LDP çalışıyorsa etiket bağlama bilgisi ile yönlendirme bilgisini tutarlı hale getirmek daha zordur. Çünkü bazı yönlendirme protokolleri artan güncelleme ile sadece son değişikliği bildirirken (BGP, OSPF gibi), bazıları bütün güncelleme göndermektedir. Onun için biri artan güncellemeleri diğeri de bütün güncellemeleri yakalayıp bağlama bilgisini güncelleyecek iki ayrı LDP kullanılmalıdır. Bu durum ağdaki karmaşıklığı daha da arttırmaktadır. Bundan dolayı mümkün olan durumlarda daima piggybacking kullanımı tercih edilmelidir. MPLS'te güncellemenin nasıl sağlanacağı 4.

bölümde incelenecektir. Bunların yanı sıra etiket anahtarlamada çokluyayın ve çevrim durumları için de çözümler yer almaktadır. Bu konular yerı geldiginde MPLS özelinde incelenecektir.

4. MPLS MİMARİSİ VE TEMEL PROTOKOLLERİ

MPLS mimarisi ilk defa Nisan 1997'de, Cisco Systems, IBM ve Ascend Communication firmalarının araştırmacılarından oluşan bir ekip tarafından tasarlanmıştır. MPLS günümüzde önceki bölümlerde bahsedilen tüm problemlere yönelik çözümler sunmaktadır. MPLS'in kuruluşundaki temel amaç MPLS çalışma grubu tarafından hazırlanan IETF dokumanında şu şekilde açıklanmaktadır; [2][19]

> *"MPLS çalışma grubunun temel amacı etiket değiştirmeli iletim yöntemini ağ katmanında yönlendirme ile entegre edecek temel bir teknoloji standardize etmektir. Bu temel teknoloji (etiket değiştirme) ağ katmanı yönlendirmenin fiyat/performans değerini geliştirecek, ağ katmanında ölçeklenebilirliği arttıracak ve yeni yönlendirme servisleri için esneklik sağlayacaktır."*

MPLS gerçekten de 2. katman anahtarlama ile iletimin iyi yanları ile 3. katman yönlendirmenin iyi yanlarını birleştirmektedir. MPLS ile çerçeve-bazlı ya da hücre-bazlı paketlere/hücrelere sabit uzunluklıu etiketler atayarak *etiket değişimi (label swapping)* yöntemi ile iletim gerçekleştirir.

MPLS ile geleneksel WAN teknolojilerinin en önemli farkları etiketlerin atanma yöntemi ve paket içerisinde etiket yığınlarının taşınmasına izin verilmesidir. Bu sayede trafik mühendisliği, şekillendirme ve VPN gibi uygulamaların kullanımı mümkün olmaktadır.

MPLS mimarisi aynen 3. bölümde bahsettiğimiz gibi iki temel düzlem bileşeninden oluşmaktadır. Bunlar *iletim düzlemi* ve *kontrol düzlemi'*dir. İletim düzlemi bir etiket-iletim veritabanı oluşturarak iletimi gerçekleştirirken, kontrol düzlemi birbirine bağlı anahtarlar arasında etiket-FEC bağlama ve dağıtım işlemlerini gerçekleştirir.

MPLS ağında mutlaka bir IP yönlendirme protokolü de çalışıyor olmalıdır. Bu nedenle her bir MPLS birimi aynı zamanda bir IP yönlendirici gibi çalışır. IP yönlendirme tablosu komşuların belirlenip etiket değişiminin sağlanması için kullanılır. Ayrıntılarını Bölüm

4.2'de inceleyeceğimiz gibi bir MPLS ağında bir etiket dağıtım mekanizması çalışmaktadır. Komşular arası değişimler sonucu MPLS iletim tablosu oluşturulur.

4.1 MPLS Mimarisi

MPLS mimarisinde etiket dağıtımı yapan ve etikete göre iletim gerçekleştiren yönlendirici ve anahtarlara *Etiket Anahtarlayıcı Yönlendirici – LSR* adı verilir. Üstlendikleri rollere göre LSR tipleri vardır. [5]

Sınır-LSR; ağın giriş ve çıkışında bulunarak etiket koyma ve kaldırma işlemlerini gerçekleştirir. Komşuları MPLS üyesi olmayan LSR'lara Sınır-LSR denir. IP iletim tablosu kontrol düzlemindeki IP yönlendirme tablosundan elde edilir. Etiket bilgisine göre sınıra gelen ve MPLS dışı bir birime gitmek isteyen olursa etiket kaldırılır ve iletim IP tablosundaki bilgilere göre yapılır.

İç-LSR; MPLS ağının içerisinde yer alan, bütün komşuları MPLS üyesi olan ve etikete göre anahtarlama yapan standart MPLS bileşenlerine denir.

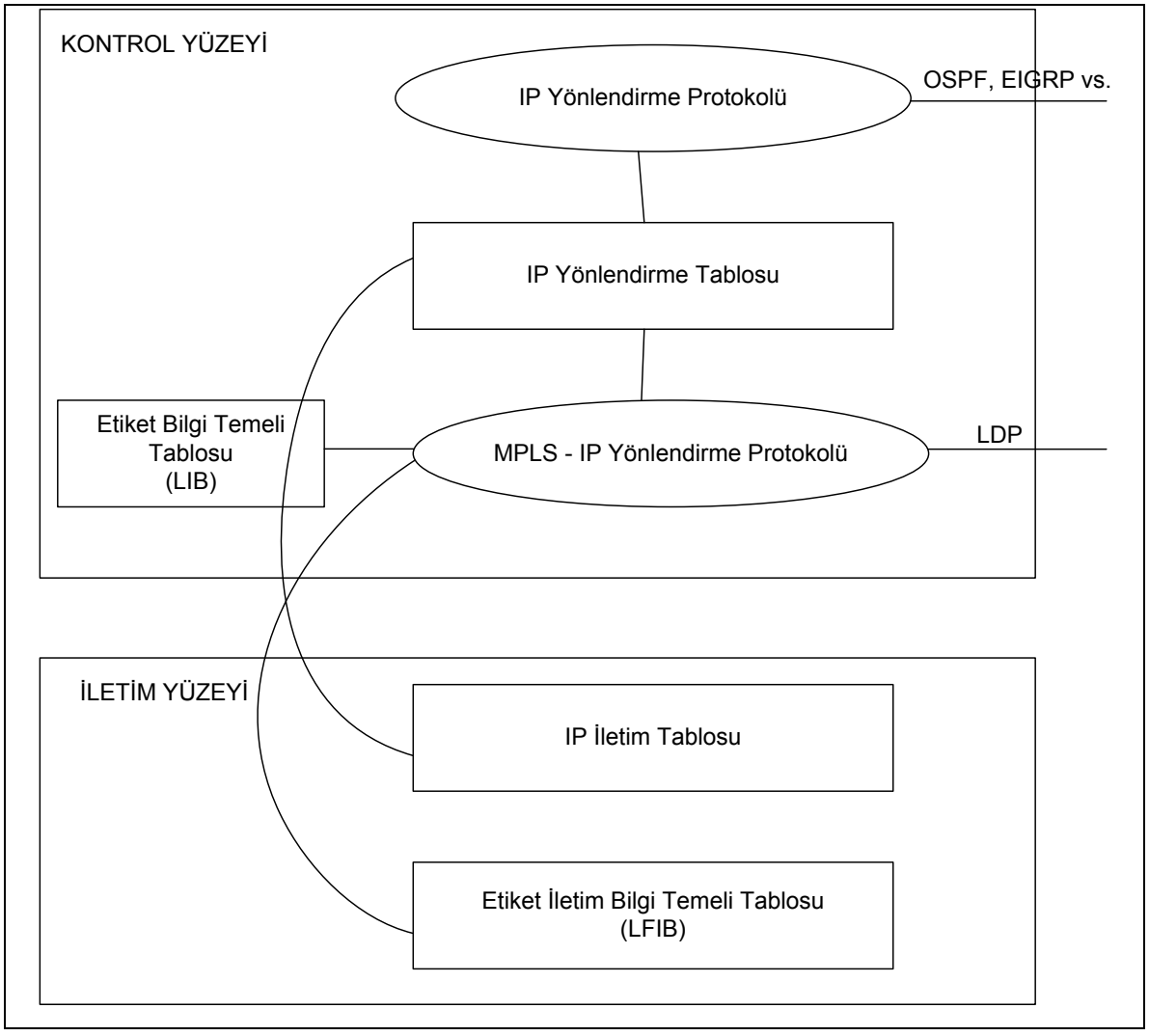
ATM-LSR; LSR gibi davranabilen ATM anahtarıdır. ATM-LSR'lar kontrol düzleminde IP yönlendirme ve etiket atama yapar ancak paketleri bildiğimiz ATM hücre anahtarlama ile gönderirler. Başka bir deyişle ATM anahtarlama matrisi etiket iletim tablosu olarak kullanılır.

ATM-Sınır-LSR; komşuları Sınır-LSR olan ATM-LSR'dır. Bunlar kendilerine gelen etiketli paketleri hücrelere çevirerek komşularına gönderirler. Aynı şekilde hücreler halinde gelen paketleri birleştirerek Sınır-LSR'lara gönderirler.

Her LSR iki adet tablo bulundurur. Bunlardan birincisi *Etiket Bilgi Temeli (Label Information Base - LIB)* tablosudur. Bu tabloda bu LSR tarafından atanan tüm etiketler ve bunların eşi olan komşu etiket bilgileri yer alır. Bu etiket eşlemeleri etiket dağıtım protokolü tarafından dağıtılır.

Aynı FEC'e ilişkin çok sayıda etiket bağlama bilgisi alınır ancak bunların hepsi bu LSR'a göre sonraki-sekme olmadığı için bazıları kullanılmaz. İşte ikinci tablo yalnızca kullanılan etiket ve bağlama bilgilerini tutar. Bu tabloya *Etiket İletim Bilgi Temeli (Label*

Forwarding Information Base - LFIB) tablosu denir. Tablolar ve ilişkileri Şekil 4.1'de görülmektedir. [2]



Şekil 4.1: MPLS düzlem tabloları arasındaki ilişkiler

MPLS mimarisi aşağı yönlü etiket anahtarlama prensibiyle çalışmaktadır. Etiket atama istek üzerine olabileceği gibi ayrıntılarını bölümün ilerleyen sayfalarında göreceğimiz gibi bağımsız atama da gerçekleşebilir. Etiketlerin global, yerel ya da arayüz başına anlamlandırılması mümkündür. Hiyerarşik etiketleme ya da VPN gibi özellikler için etiketlerin yığın olarak taşınması da mümkündür.

MPLS'de yol seçimi ve yönlendirme iki şekilde yapılır; *sekmeden-sekmeye (hop-by-hop)* veya *belirli (explicit) yönlendirme.* Sekmeden-sekmeye mekanizmasında yol seçimi kullanılan yönlendirme algoritmasının sağladığı sonuçlara göre yapılır. Belirli

yönlendirmede ise rota tamamen kaynak tarafından belirlenir. Aradaki LSR'lar yönlendirme prosedüründe yer almadan paketleri iletirler.

Önceki bölümde bahsettiğimiz gibi iki tip etiket-FEC bağlama yöntemi vardır. Bunlar veri-yoluyla ve kontrol-yoluyla yöntemleridir. MPLS mimarisi tünelleme, yönlendirme, çokluyayın gibi tüm uygulamaları için kontrol-yoluyla bağlamayı kullanır.

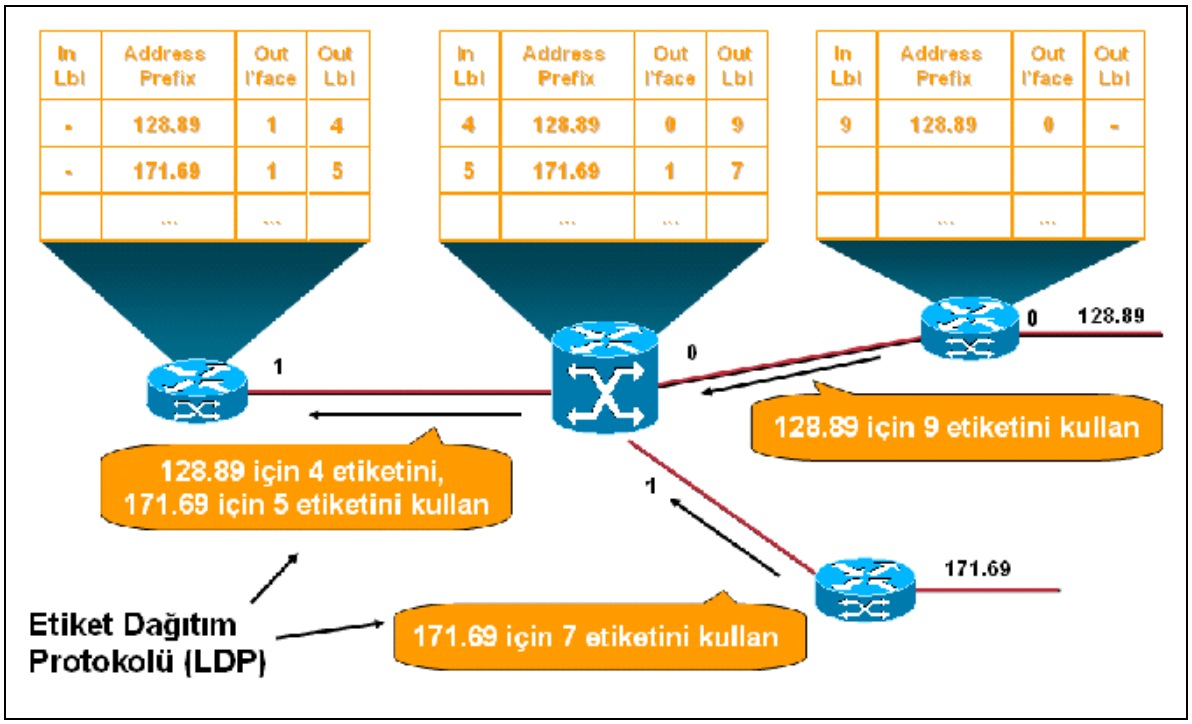
4.1.1 Sıralı ve Bağımsız Kontrol

Bilindiği üzere MPLS ağı üzerinde bir paketin giriş LSR'dan çıkış LSR'a dek izlediği yola *Etiket Anahtarlamalı Yol (LSP – Label Switched Path)* adı verilir. Yolun kurulumu kullanılan MPLS tipine göre (Hücre-Mod ya da Çerçeve-Mod) *bağimsız* olabileceği gibi *sıralı (ya da isteğe bağlı)* da olabilir. LSP kurulumu bağlantılı bir yapıdır çünkü LSP'ler trafik akmaya başlamadan önce kurulur. Ancak bu kurulum topoloji bilgisine göre önceden yapılır yani trafik akacak diye LSP kurulmaz.

Bağımsız kontrol yönteminde her LSR kendisine ağ içi kullanılan ağ katmanı yönlendirme protokolleri ile gelen FEC bilgilerine aşağısında ya da yukarısında yer alan LSR'dan bir istek ya da yol atandı bilgisinin gelmesini beklemeden FEC'e ilişkin bir etiket atar ve bunu kullanılan LDP ile komşularına duyurur.

Sıralı (isteğe bağlı) kontrol yöntemimde ise LSP ağın bir ucundan diğerine kadar sıra ile atanarak kurulur. Bu kurulum çıkıştan girişe doğru yani *aşağı yönlü (downstream)* olabileceği gibi tersi de mümkündür. MPLS'te sıralı LSP kurulumu çıkış LSR'dan başlayarak aşağı yönlü olarak yapılır. Bir çıkış sınır LSR kendisine yönlendirme güncellemesi ile FEC bilgisi geldiğinde buna ilişkin bir etiket atar, bunu kendi üst komşusuna gönderir, böylece LSP kurulur. Şekil 4.2'de sıralı LSP kurulumu ve etiket dağıtımı görülmektedir.

MPLS teknolojisi hem sıralı (isteğe-bağlı) hem de bağımsız etiket atama ve yol kurulumu tekniklerini destekler. Bir sonraki bölümde Hücre-mod MPLS ile Çerçeve-mod MPLS karşılaştırmasını yaparken açık olarak görebileceğimiz gibi her iki yöntemin de birtakım avantaj ve dezavantajları mevcuttur.



Şekil 4.2: Sıralı atama ile LSP kurulumu

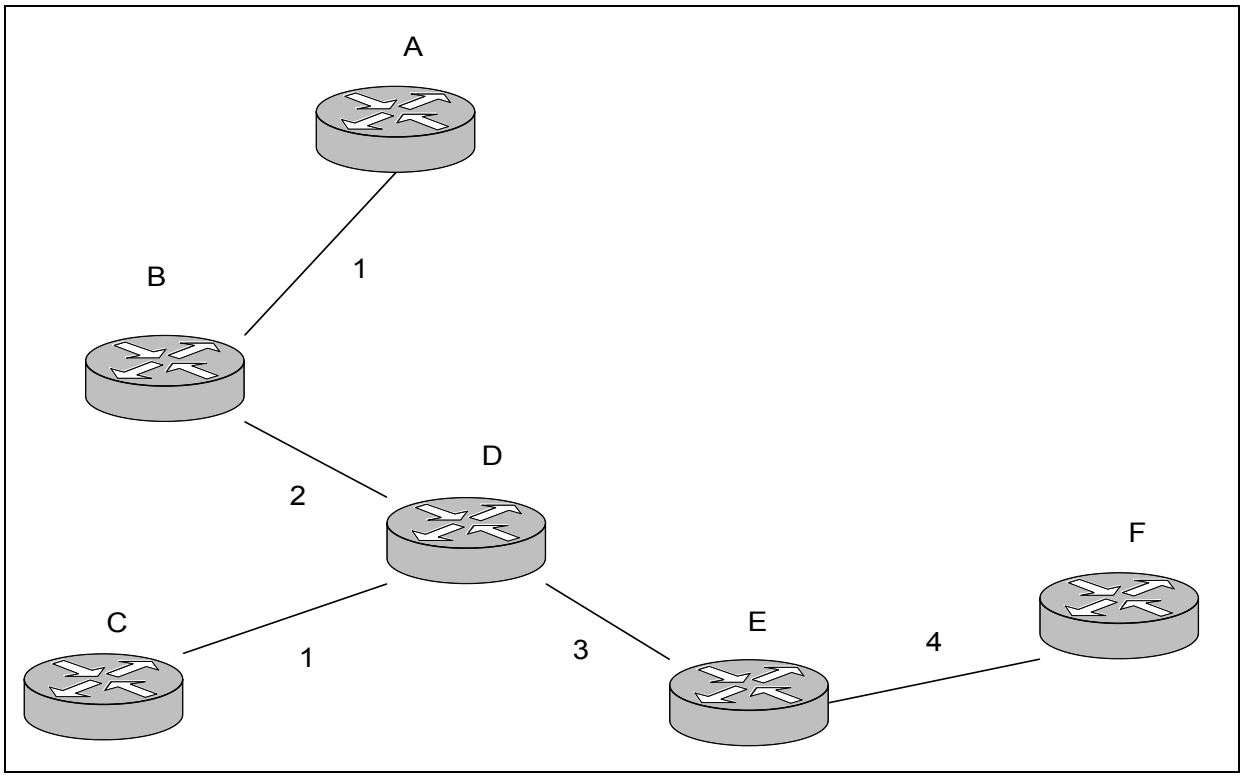
Sıralı yöntemde atama kontrollü olarak gerçekleştiği için etiket anahtarlamalı ağlarda önemli bir problem olan çevrim kontrolü ve engellemesi sağlanır. Ayrıca ağda sıkı bir kontrol ve tutarlılık sağlanmış olur. Bağımsız kontrolde her LSR kendi atama ve FEC-etiket bağlama işlemlerini kendi kararına göre gerçekleştirdiği için ağda tutarsızlıklar olabilir örneğin bir LSR FEC olarak doğrudan alt ağ adresini kabul ederken bir diğeri topaklanmış adresi kabul ederse ağda sorunlar oluşabilir. Ağda kontrol amacıyla belli bir FEC üzerine engelleme gerçekleştirilmek istendiğinde sıralı yöntem ile sadece sınır LSR üzerinde erişim kontrol listeleri yazmak yeterli iken bağımsız atamada her LSR üzerinde bu işlemin ayrı ayrı yapılması gerekir. Sıralı yöntemin dezavantajı ise LSP'nin kurulma süresini çok uzatmasıdır. Sıralı yöntem ile LSP kurulabilmesi için FEC-etiket bağlama bilgisinin tüm ağa yayılmış olması beklenir, ondan sonra LSP kurulur. Hatta bir kopukluk veya hata olduğunda bağımsız kontrol ile hattın yeniden oluşturulması LSR bazında bağlantılar düzeltildiği için hızlı olmaktadır. [1][5]

4.1.2 Çevrim Tespiti ve Önleme

MPLS üzerinde çevrim oluşumu başlığını incelerken iki konuyu ele almamız gerekir. Bunlar *çevrimi önleme* yani ağda bir çevrim oluşarak paket kaybedilmesini engelleme ve *çevrimi etkisizleştirme* yani ağda bir çevrim durumu oluştuğunda bunun etkisini en aza indirgemedir. Geleneksel IP yönlendirme protokollerinin bir çoğu kendiliğinden çevrim engelleme özelliğine sahip olmadığı için kullanılan yöntem etkisizleştirme yöntemidir. Bunun için TTL kavramı kullanılır, hatta çevrim oluşmussa bu TTL değerinin 0 olması ile anlaşılır ve paket çöpe atılır böylece çevrimin ağa etkisi en aza indirgenmiş olur. Çoğu zaman MPLS'te de aynı yöntem söz konusudur. MPLS etiketli paketler TTL değeri taşırlar ve çevrim bu şekilde etkisizleştirilir ancak her zaman bu mümkün değildir çünkü ATM gibi ağlarda TTL yoktur. Bunun yerine ATM anahtarlar her bir sanal devre başına kullanılabilecek tampon boyunu sınırlarlar. Çevrim durumu genellikle ağdaki bi değişiklik sonucu yayılım sırasında oluştuğu için tampon kullanımı ile çevrim oluşsa bile çevrim trafiğinin yönlendirme güncellemelerinin ağda dolaşmasını engellemesi sorununun önüne geçilmiş olmaktadır. [2]

MPLS üzerinde çevrim engellemenin bir diğer yolu *yol vektörleri* kullanımıdır. Yol vektörü ağda ETİKET_İSTEĞİ ve ETİKET_EŞLEME mesajlarının geçtiği LSR listesini tutan bir vektördür. BGP AS_PATH özelliğinde olduğu gibi, bir LSR kendine gelen bir mesajın yol vektörü listesinde kendi adını görürse bu paketin kendi üzerinden daha önce geçmiş olduğunu anlar ve çevrim oluşumunu tespit ederek paketi atar. [2]

Çevrim engelleme konusunda MPLS'e özel olarak geliştirilen bir diğer yöntem de *renkli teller (colored threads)* yöntemidir. Bu yöntem için sıralı LSP oluşumunun kullanılıyor olması gerekir. Bu teknikte her bir LSR LSP kurulumu sırasında gönderdiği ETİKET_İSTEĞİ mesajının içine bir renk değeri yazar. Bunun ağda tek olması için kendi IP adresini ve rastgele seçtiği bir sayıyı kullanır. Her bir düğüm ağda bu mesajlar dolaşırken kendine gelen mesajlardaki renk değerlerini tutar. Bir LSR kendine ait bir renk değerini kendine gelen bir ETİKET_İSTEĞİ mesajında görürse çevrim olduğunu anlar ve mesajı atar. Bu yöntemin bir diğer getirisi de ağdaki sekme sayısının ETİKET_İSTEĞİ mesajları içerisinde tutulabilmesidir. Böylece hiçbir ağa yeni LSR eklendiğinde çevrim denetlenebilir. Örneğin Şekil 4.3'teki durumu inceleyelim.



Şekil 4.3: Renkli teller ile çevrim denetimi

Şekil 4.3'te bir topoloji ve her bir hattaki sekme-sayısı bilgisi görülmektedir. Buna göre örneğin B-D hattının sekme sayısı 2'dir. Bu hatta dolaşan ETİKET_İSTEĞİ mesajlarında A'ya bağlı bir FEC için maksimum sekme-sayısı bilgisi 4 olarak görülmektedir. Örneğin LSR C A'ya bağlı bir FEC için LSR D'yi sonraki sekme olarak görsün. Etiket isteğinde bulunduğu C-D hattının sekme-sayısı değeri 1 olarak D'ye gelir. Bu değer D'nin o FEC için sonraki sekmesi olan B için B-D hattının sekme-sayısı değeri olan 2'den küçük olduğu için D bağlantının kurulmasına izin verir. Örneğin F ile D arasında yeni bir hat oluşsun bu durumda F kendisine yeni bir bağlantı geldiği için sekme sayısının 1 arttığını düşünerek sekme değerini 5 yapar. F D'yi sonraki sekme olarak görmeye başlar ve etiket isteğinde bulunur bu durumda D kendisine gelen etiket isteğinde sekme değerinin 5 olduğunu ve bu değerin 4'ten büyük olduğunu görür ve mesajı E'ye o da F'ye geçirir. F kendi rengini ETİKET_İSTEĞİ mesajında görünce bir çevrim oluştuğunu anlar. [2]

4.1.3 Kapsülleme

Geçen bölümde bahsettiğimiz gibi MPLS, etiket bilgisinin 2. ikinci katman başlığı içerisinde taşınamadığı durumlarda 2. ve 3. katman başlıkları arasına bir ara başlık - *shim* yerleştirir. Ara başlık 32 bitten oluşur ve yapısı Şekil 4.4'teki gibidir;

Etiket (20 bit)	Exp (3 bit)	Yığın (1 bit)	TTL (8 bit)

Şekil 4.4: Shim Başlık

Etiket biti, hatta atanan etiket değerini taşımaktadır. Bu değer LSR'lar üzerinden geçerken değiştirilir.

Exp biti, özel amaçlarla ayrılmıştır. Kesin kullanımı standardize edilmemiştir ancak yaygın olarak Cisco Takı Anahtarlama teknolojisinde olduğu gibi Servis Tipi (CoS) amaçlı olarak kullanılmaktadır.

Yığın biti, yığın etiketleri kullanımında yığın sonunu işaretlemek amacıyla kullanılır.

TTL biti, bir IP ağından diğer bir IP ağına geçişte transit olarak MPLS çekirdeği kullanıldığında gereklidir. Giriş LSR'da IP paketindeki TTL değeri buraya kopyalanır, çıkış LSR'da bu değer 1 azaltılır ve IP paketine geri kopyalanır böylece MPLS domeni üzerinden geçerken IP mekanizmalarının devamlılığı sağlanır. Bu özellikle paketleri takip edebilmek için önemlidir. Ayrıca MPLS domeni sanki tek bir sekmeymiş gibi algılanır.

4.2 Etiket Dağıtımı

Önceki bölümde incelediğimiz gibi etiket dağıtımı için ayrı bir dağıtım protokolü kullanılabileceği gibi piggybacking ile dağıtım mümkündür. Bu başlık altında Etiket Dağıtım Protokolü (LDP) ve BGP ile etiket dağıtımından bahsedilecektir. [1][2][5]

4.2.1 Etiket Dağıtım Protokolü (LDP)

Etiket dağıtım protokolü FEC-etiket eşleme bilgisinin MPLS ağında dağıtımından sorumlu olan protokoldür. LDP bunun için çeşitli mekanizmalara sahiptir. Bu mekanizmalar ile LSR'lar birbirleri ile komşuluk ilişkisi kurarlar ve haberleşirler.

4.2.1.1 Komşuluğun kurulması ve mesajlar

LDP'de 4 temel mesaj vardır. Bunlar LSR'ların birbirini görmesini sağlayan KEŞİF mesajları, LSR'lar arasında oturum kurulmasını sağlayan KOMŞULUK mesajları, etiket bağlama bilgilerinin duyurulmasını, istekte bulunulmasına yarayan ETİKET_DUYURU mesajları ve hata mesajlarının ve anomalilerin iletimi için kullanılan UYARI mesajlarıdır. Mesajların iletiminde mesajın tipinin anlaşılması için TLV (tip, uzunluk, değer) kodlaması kullanılır.

Mesajların güvenli iletimi için TCP kullanılır (KEŞİF hariç) çünkü mesajların anlamlı olabilmesi için sıra ile gelmesi gerekir. LDP ile haberleşmede TCP'nin tıkanıklık kontrol mekanizması haberleşmenin komşular arası gerçekleştirilmesi nedeniyle pek önem taşımasa da akış kontrol mekanizması önem taşır.

LDP keşif protokolü ise UDP ile çalışır. Bir LSR periyodik olarak ortama çokluyayın şeklinde MERHABA paketleri gönderir. Tüm LSR'lar MERHABA paketinin geldiği portu sürekli dinler durumdadır. Böylece LSR'lar kendilerine gelen MERHABA paketlerini algılarlar. Bir LSR başka bir LSR'dan haberdar olduğu anda ikisi arasında TCP oturumu açılır ve komşuluk mesajları gitmeye başlar. LSR'ların aynı alt ağda olmadığı durumlarda belirli bir IP adresine bu çokluyayın MERHABA paketi gönderilir. Bu paketi algılayanlar gönderici kişiye tekyayın paketi ile cevap verir. Komşuluk böylece kurulur.

Yukarıdaki temel LDP mesajlarının yanısıra en yaygın kullanılan LDP mesajları ise; komşuluk kurulduğu anda haberleşmenin sağlıklı sürdürülebilmesi için başlangıç parametrelerinin belirlenmesinde kullanılan BAŞLATMA mesajı, komşu LSR'ın halen ayakta olup olmadığını kontrol etmekte kullanılan CANLITUT mesajı, etiket bilgisi ile FEC bilgisini bağlamakta kullanılan ETİKET_EŞLE mesajı, FEC-etiket bağına ihtiyaç kalmadıysa eşlemeyi çözmekte kullanılan ETİKET_ÇÖZ mesajı, çözülen etiketin etiket havuzuna geri gönderilmesini sağlayan ETİKET_BOŞALT mesajı, etiket atama isteğinde bulunmak için komşuya gönderilen ETİKET_İSTEĞİ mesajı ve isteğin reddedilmesi anlamına gelen ETİKET_İSTEĞİ_REDDET mesajlarıdır.

4.2.1.2 Etiket Dağıtım Modları

Önceki bölümlerde ayrıntılarıyla anlattığımız üzere etiket dağıtımı ve atamasının nasıl olacağına dair çeşitli modlar mevcuttur. Bunlar *isteğe bağlı* ve *istekten bağımsız* etiket atama modları, *sıralı* ve *bağımsız* LSP kontrol modları (bunlar önceki ve bu bölümde açıklanmıştı) ve etiket atamada kullanılan etiketler konusunda *liberal* ve *tutucu* seçim modlarıdır.

Eğer bir LSR tutucu modda çalışıyor ise sadece o an aktif olan LSP'de kullanılan etiket-FEC eşleme bilgileri tutulur. Onun dışındaki bağlamalar çözülür. Liberal modda ise kullanılsın kullanılmasın tüm bağlama bilgileri tutulur. Liberal yöntemin avantajı yönlendirme bilgisinde bir değişiklik olduğunda etiket-FEC bağlaması halihazırda yapılmış olduğu için değişikliğe cevap vermenin hızlı olmasıdır. Dezavantajı ise kullanılmayan etiketlerin de atanması ile etiketlerin verimsiz kullanımıdır. Çok fazla sayıda farklı trafik geçiren LSR'lar için bu bir sıkıntı yaratabilir.

4.2.2 BGP ile Etiket Dağıtımı

MPLS çalışma grubu BGP4'ün etiket dağıtımı için kullanılabilmesi için üzerinde yeni özellikler tanımlamışlardır. Bu yeni eklentiler ile BGP4 hem IPv4 hem de IPv6'yı destekler durumdadır. MPLS yalnızca yeni bir adresleme yöntemi tanımlamış ve bu adres içerisinde yalnızca adres prefiksinin değil etiket bilgisinin de bulunması sağlanmıştır. Buna göre Şekil 4.5'te görülen BGP başlığında 3 Byte uzunluğunda yeni adres yapısı tanımlanmıştır. Bunun en düşük anlamlı 20 biti etiket değerini, 1 biti yığın değerini ve kalan 3 bit de 0 değerini taşımaktadır. Prefiks değeri de IPv4 için 32 bit IP adresini taşımaktadır. Bu sayede BGP konuşan tüm düğümlerin normal BGP paketlerini duyurur gibi etiket değerlerini de taşıması ve komşulara duyurması sağlanmıştır. [3]

4.3 MPLS Mimari Tipleri

MPLS uygulanan ikinci katman teknolojisine bağlı olarak etiketleme, iletim, ve kapsülleme mekanizmalarında değişiklikler mevcuttur. MPLS çerçeve mod (ethernet, FR) olabileceği gibi, hali hazırda omurgada yüksek kapasiteli iletim için kullanılan ATM donanımlarının yazılım güncellemesi ile MPLS çalışır hale getirilmesi sonucu iletimin hücre-modda yapılması da mümkündür. Aşağıda bu iki yapı anlatılmıştır. [1]

Uzunluk (1 Byte)
Etiket (3 Byte)
Opsiyonel Etiketler (Yığın için yeni etiketler tanımlanabilir)
Prefiks (BGP adres 32 bit IPv4)

Şekil 4.5: BGP ile etiket bilgisinin taşınması

4.3.1 Çerçeve-Mod MPLS

Bu modun çerçeve modu olarak adlandırılmasının nedeni etiketli paketlerin ikinci katman çerçeveleri şeklinde aktarılmasıdır. MPLS çerçeve başlığı yukarıda bahsettiğimiz *shim başlık* şeklinde 2. ve 3. katman başlıkları arasına yerleştirilir. Başlık içerisinde etiket değeri, sınıf bilgisi, TTL değeri ve yığın sonunu gösteren belirteç yer almaktadır.

Bir paket alındığı zaman bunun etiketli bir paket olup olmadığı çerçeve içerisindeki ethertip (ethertype) değerine göre anlaşılır. Burada yazılı olan değerden hangi kapsülleme yönteminin kullanıldığı ve paketin etiketli olup olmadığı anlaşılır.

Haberleşen iki yönlendiriciden biri çerçeveyi gönderirken ethertip değerini uygun bir değere çeker. Bunu alan sonraki-sekme ethertip değerinden bunun etiketli bir paket olduğunu anlar ve böylece 3. katman incelemesi yapmadan paketi etiket değerine göre iletir.

Bir LSR'da MPLS'in başlaması ile birlikte LDP süreci başlar. LDP-MERHABA paketleri ile TCP port 646'dan komşuluk kurulur ve CANLITUT mesajları hattan gidip gelmeye başlar. Komşulardan gelen etiket bilgileri ile LIB tablosu oluşturulur.

Yönlendiricilerde LIB tablosu oluşunca LIB'deki her FEC için etiketler tanımlanır. Her yeni gelen FEC için yeni bir etiket tanımlanır. Bir LSR kendine gelen FEC için etiket ataması yaparken aşağı-yönlü atamanın gereği olarak sonraki-sekmeden o FEC için atanan etiket bilgisinin gelmesine gerek duymadığı için bu işlem *istek –dışı bağımsız atama (unsolicited downstream)* olarak adlandırılır. Bir FEC için atanan etiket aşağı ya da yukarı olması farketmeksizin tüm komşulara duyurulur. Yani IP yönlendirmedeki gibi

split horizon yoktur. FEC bilgisini gönderene de bu bilgi geri gönderilir. Komşu LSR'lar FEC-etiket eşlemesi bilgisini alır ve LIB tablosuna yerleştirir. Eğer bilgi o FEC'e ilişkin yolda sonraki-sekmesi konumunda olan aşağı LSR'dan gelmiş ise bilgi LFIB tablosuna alınır. Bu yönteme *serbest alıkoyma* denir.

4.3.2 Hücre-Mod MPLS

ATM anahtarlarının normal çalışma modlarında etiket okuma yetenekleri mevcut değildir. ATM anahtarların tek yaptıkları gelen sanal devre (VC) bilgisini çıkışta bir VC ile eşlemektir. ATM anahtarlar arasında doğrudan IP paketleri aktarılamaz., önceden bir sanal devre kurulması ve paketlerin hücrelere dönüştürülmesi zorunludur.

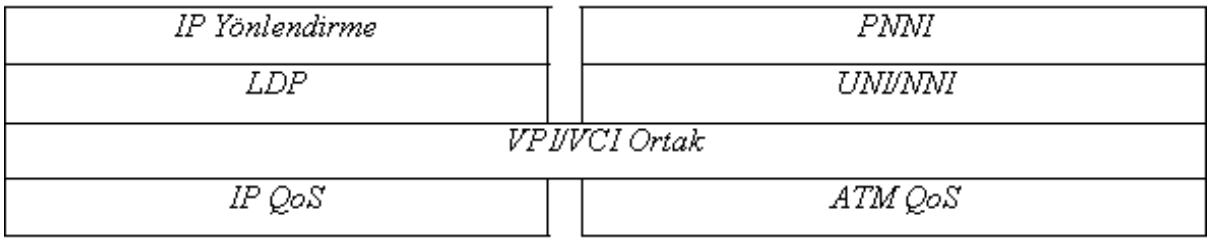
ATM anahtarlar etiketten anlamadıkları için MPLS çalıştırabilmeleri için etiket atama ve dağıtım tekniklerinde değişiklik yapılması, etiket yığınının en üstündeki bilginin VPI/VCI değerine çevrilmesi gerekir.

ATM'de MPLS için oluşturulan yeni bir terminoloji mevcuttur:

- *Etiket Kontrollü ATM Arayüzü (LC-ATM):* Bu arayüz VPI/VCI değerlerinin LDP tarafından atandığı bir arayüzdür.
- *ATM-LSR:* Kontrol düzleminde MPLS çalıştıran ve veri yüzeyinde LC-ATM arayüzler arasında ATM hücre anahtarlama ile MPLS iletimi gerçekleştiren LSR'dır.
- *Çerçeve-temelli LSR:* Çerçeve-temelli iletim gerçekleştiren standard LSR tipidir. LC-ATM arayüz de bulundurabilirler ancak hücre anahtarlama yapmazlar.
- *ATM-LSR domeni:* LC-ATM arayüzlerle birbirine bağlı ATM-LSR'ların oluşturduğu domendir.
- *ATM-Sınır-LSR:* En az bir LC-ATM arayüzü olan çerçeve-temelli LSR tipidir.

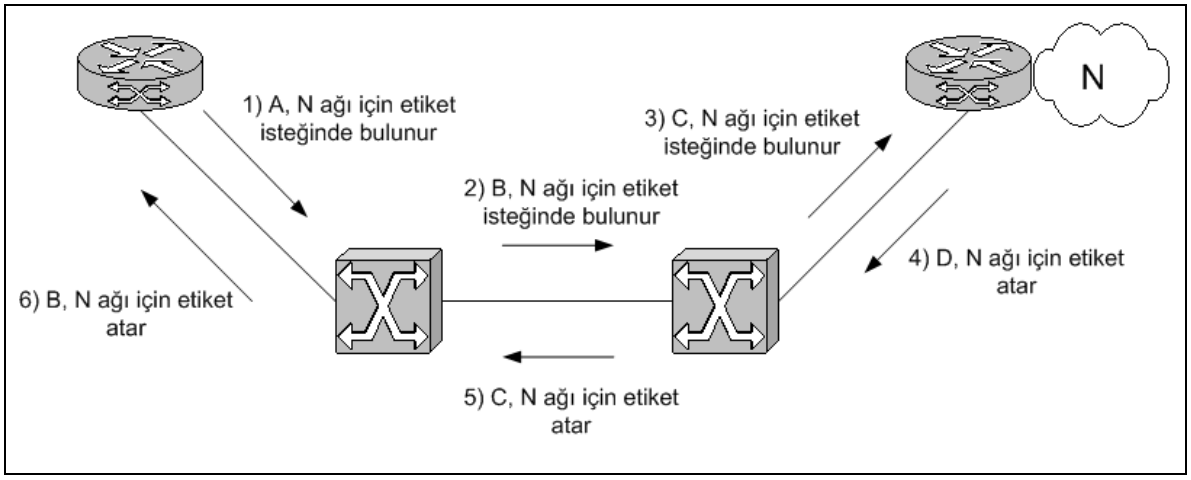
MPLS mimarisi komşu LSR'ların kontrol düzlemlerinin saf IP bağlantısı olmasını gerektirir. Böylece etiket bağlama gerçekleştirilebilir. Çerçeve-temelli yapıda bu sorun değildir ancak ATM-LSR'ların bu yeteneği yoktur. ATM-LSR'lar içerisinde MPLS kontrol düzlemleri tanımlanarak bu gerçekleştirilir. VPI/VCI değerleri iki teknoloji arasında ortak olarak belirlenir ve etiket değeri olarak kullanılmak üzere MPLS kontrol

düzleminde kullanılır. Bu işlem yazılım güncellemesi ile gerçekleştirilir. Şekil 4.6'da bu yapı görülmektedir.



Şekil 4.6: ATM ve MPLS denetim düzlemleri

ATM LSR'lar etiket değeri olarak sanal devreyi temsil eden VPI/VCI değerlerini kullandığı ve bunların da sayısı sınırlı olduğundan etiket atama serbest değil *tutucu* şekilde gerçekleştirilir. Bir LSR paket göndermek istediği zaman aşağı LSR'dan etiket isteğinde bulunur. Aşağı LSR buna bir cevap gönderir ve etiket atama *istek üzerine aşağı yönlü* olarak sağlanır. ATM anahtarlarda etiket atama ancak aşağı çıkış etiketi atandı ise gerçekleşir. Yani herkes etiket atamadan önce aşağı LSR'dan etiket gelmesini bekler. Buna *sıralı kontrol* denir. Çerçeve modda ise bu işlem bağımsız kontrolle gerçeklenirdi. Şekil 4.7'de sıralı kontrol işlemi görülmektedir.



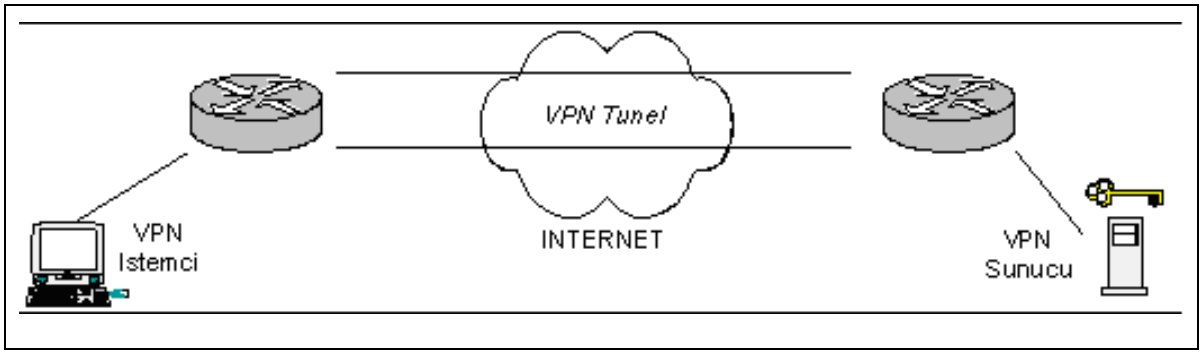
Şekil 4.7: Sıralı kontrol

Sonuç olarak, halihazırda yüksek kapasiteli omurgasında ATM çalıştıran kurumlar bir yazılım güncellemesi ile MPLS teknolojisine geçirilebilirler. Böylelikle silbaştan yatırım yapmak yerine eldeki imkanlar kullanılarak uygun maliyetle daha yüksek performanslı ve ölçeklenebilir bir teknolojiye geçiş mümkün olur. [1][2]

5. MPLS – VPN TEKNOLOJİSİ

Sanal Özel Ağ (Virtual Private Network - VPN) teknolojisi genel olarak şirketlerin, kurumların sahip oldukları özel ağların Internet gibi paylaşımlı ortamlar üzerinden genişletilmesi anlamına gelir. VPN, farklı coğrafi bölgelerdeki iki bileşenin noktadan-noktaya bağlantı mantığı çerçevesinde haberleşebilmelerini sağlar.

Bunun için, paylaşımlı ortam üzerinden aktarılan veri kapsüllenir ve iletim için uygun bir başlık eklenerek gönderilir. Paketler iki haberleşen arasında gizlilik nedeniyle kriptolanır. Uygun kripto anahtarları olmadan yol üzerindeki sekmelerde veri açılamaz. Verinin kapsüllendiği noktadan-noktaya bağlantıya *tünel,* farklı yerleşkeler arasında oluşturulmuş tüneller bütününe de *Sanal Özel Ağ – VPN* denir. Şekil 5.1'de örnek bir VPN topolojisi görülmektedir. [5]



Şekil 5.1: VPN Tünel ve iletişim yapısı

VPN bağlantısı ile paylaşımlı ortam üzerinden uzak erişim ile kurumsal sunucuları kullanmak mümkündür. Bu açıdan bakıldığında VPN istemci ile VPN tüneli içerisinden geçerek sunucu erişiminin lokal erişime göre bir farkı yoktur. Bağlantı adeta yerelde bir link üzerindeymişçesine gerçekleşir.

VPN teknolojisi günümüzde yaygın olarak gezgin ya da uzak ofis çalışanlarının merkez ofisteki sunuculara ve verilerine erişebilmeleri için kullanılır. VPN bağlantısı sayesinde şirketlerin yereldeki verilerini WAN üzerinden dağıtmaları mümkün olmaktadır.

VPN bağlantısının kurulabilmesi için uzak erişimde bulunan kullanıcıların VPN istemcileri ile VPN bağlantı isteğini karşılayacak sonlandırıcı donanımlara ihtiyaç vardır. Sonlandırıcı sunucular VPN desteğine sahip bir yönlendirici olabileceği gibi yüksek sayılarda VPN isteğini ve tünel sayılarını desteklemek üzere tasarlanmış VPN sonlandırıcı konsantratör donanımları da olabilir. İstemci için kişisel bilgisayar üzerinde çalışan bir yazılım kullanılabilir. [5]

Bir VPN çözümünde karşılanması gereken nitelikler şunlardır: [22]

- *Kullanıcı kimlik sorgulaması ve yetkilendirme (authentication-authorization)*

  VPN istemcisi ile ağa bağlanan kişinin sorgulanması ve yetkisi dahilinde yerel ağda işlem yapması ağın güvenliği açısından hayati önem taşır.

- *Adres yönetimi*

  Uzaktan erişen kullanıcıya yerel ağdaymışçasına işlem yapma imkanı veren yerel bir adresin (kullanılan teknoloşiye göre IP olabilir) atanması hizmetin sağlanması için önemlidir.

- *Veri kriptolama*

  Paylaşımlı ortamdan geçen verinin ara sekmelerde okunamaması ve değiştirilemez olması sağlanmalıdır. Ağın güvenliği, veri bütünlüğü ve güvenilirliği bu yolla sağlanır.

- *Anahtar yönetimi*

  Kriptolama için kullanılan anahtarın istemci ve sunucu arasında üretimi ve güvenlik amacıyla güncellenmesi gerekir.

- *Çok protokollülük desteği*

  VPN, ortamda kullanılan protokolden bağımsız olarak kurulabilmeli ve kaldırılabilmelidir.

5.1 VPN Tünelleme

Tünel, kapsüllenmiş paketlerin paylaşımlı ortam üzerinden aktarıldığı mantıksal yoldur. Tünel, istemciden sonlandırıcıya kadar olan kapsülleme, iletim ve kapsül-bozma süreçlerini içerir. İletilmek istenen çerçeveler tünel girişinde ek bir başlık ile kapsüllenir. Bu ek başlıkta, paketin paylaşımlı ortam üzerinden aktarımı için gerekli yönlendirme bilgisi yer alır. [22]

Tünelleme için kullanılan çeşitli teknolojiler vardır. Bunlardan bazıları artık değişen teknoloji dolayısıyla önemini kaybetmiştir. Bu eski teknolojilere en iyi örnekler:

- *IP üzerinden SNA tünelleme:* System Network Architecture (SNA) trafiği IP ortamı üzerinden genişletilmek istenirse SNA çerçeveleri UDP ve IP başlıkları içerisine yerleştirilir. Günümüzde SNA ağı pek kalmadığı için bu teknoloji de kullanımını kaybetmiştir.
- *Novell NetWare için IP üzerinden IPX tünelleme:* Bir zamanlar çok geniş kullanıma sahip olan IPX teknolojisi yerini artık IP'ye bıraktığı için bu tünelleme yöntemi de artık kullanılmamaktadır. Bir IPX paketi NetWare sunucu ya da IPX yönlendiricisine gönderilirse, sunucu ya da yönlendirici paketi UDP ve IP başlıkları içerisine gömer ve IP üzerinden gönderir. Alıcı yönlendirici UDP ve IP başlıklarını çıkarır, hedef IPX adresine paketi gönderir.

Günümüzde en yaygın kullanılan tünelleme yöntemleri aşağıdakilerdir. Bunlar bölümün ileriki kısımlarında detaylandırılacaktır:

- *Noktadan-noktaya Tünelleme Protokolü (PPTP – Point-to-point Tunneling Protocol):* PPTP teknolojisi IP, IPX ya da NetBEUI trafiklerinin kriptolanarak bir IP başlığıyla kapsüllenerek IP ağı üzerinden gönderilmesini sağlayan 2. katman tünelleme teknolojisidir.
- *İkinci Katman Tünelleme Protokolü (L2TP – Layer 2 Tunneling Protocol):* L2TP teknolojisi, IP,IPX ya da NetBEUI trafiklerinin kriptolanarak noktadan-noktaya datagram iletimine izin veren IP, X.25, Frame-Relay ve ATM gibi ortamlar üzerinden aktarımını sağlar. L2TP'nin PPTP'den farkı yalnızca IP üzerinden değil

adı geçen 2. katman teknolojileri üzerinden de kapsüllenmiş verinin iletimine izin vermesidir.

- *GRE (Generic Routing Encapsulation) Tünelleme*: GRE tünelleme Cisco Systems tarafından geliştirilmiş bir 3. katman tünelleme yöntemidir. RFC 1701'de tanımlanmıştır. GRE ile datagramların IP paketleri içerisine kapsüllenerek gönderilmesi söz konusudur. Çoklu-yayın (multicast) ve IPv6 desteği vardır. GRE PPTP ile beraber kullanılır.
- *IPSec Tünelleme:* IPSec tünelleme IP paketlerinin kriptolanarak, IP başlığının eklenmesiyle güvenli bir şekilde IP ağı üzerinden aktarılmasını sağlar. Günümüzde GRE teknolojisinin tek-yayın paketleri için kullanım yerini almıştır ancak IPSEC'te çoklu-yayın desteği olmadığı için böyle durumlarda genellikle GRE kullanılmaktadır. Detaylı bilgiye RFC 3193'ten ulaşılabilir.

Bir VPN tünelinin kurulabilmesi için istemci ve sunucunun aynı tünelleme yöntemini kullanıyor olması gerekir.

2. katman tünelleme teknolojileri (L2TP, PPTP) için tünel oturum açmaya benzer. Tünelin iki ucu konfigürasyon değişkenleri üzerinde anlaştıktan sonra tünel kurulur. Çoğu durumda veri tünelden datagramlar şeklinde gönderilir. Tünelin açık kalması için çeşitli canlı-tut mekanizmaları mevcuttur. 2. katman tünellemeyi bağlantılı bir hizmet olarak görmek mümkündür.

3. katman tünelleme teknolojileri genellikle konfigürasyon parametrelerinin önceden belirlendiği varsayımını kullanır. Burada tünelin bakımı için mekanizmalar yoktur yani ikinci katmanda olduğu gibi tünelin kurulup, canlı-tutulması ve kaldırılması gerekmez. Bu açıdan 3. katman tünelleme bağlantısız bir hizmet olarak görülmelidir.

Bir VPN tüneli 2. ve 3. katman parametreleri üzerinde anlaştıktan sonra tamamen kurulduğu andan itibaren veri gönderilmeye başlanılabilir. Tünel istemci ve sunucu verinin gönderimi için bir tünel iletim protokolü kullanırlar. İstemci veriyi gönderirken kapsüller ve sunucu kapsülü açarak yerelde kullanılan teknolojiye göre hedefe iletimini gerçekleştirir. [22]

Tünelde sağlanması gereken temel parametreler şunlardır:

- *Kullanıcı kimlik sorgulama (authentication)*

2. katman tünelleme protokolleri noktadan-noktaya protokol (PPP) ile tanımlandıkları için onun özelliklerini aynen taşırlar. PPP ayrıntıları da bölümün ilerleyen kısımlarında incelenmektedir. Çoğu 3. katman tünelleme teknolojisi istemci ile sunucu arasında kimlik sorgulamanın önceden yapıldığını varsayar yani bunun için ekstra bir mekanizma mevcut değildir. Bunun istisnası her iki uç arasında kimlik sorgulama gerçekleştiren IPSec IKE (Internet Key Exchange) protokolüdür. IPSec uygulamalarının çoğu kullanıcı kimlik sorgulama – sertifika yerine uç nokta sertifikalarına baktığı için yalnızca istemci makineler kontrol edilmekte yani o makineye kim otururs sunucuya erişebilmektedir. Bu eksikliği gidermek için IPSec ile birlikte L2TP gibi bir 2. katman protokolünün beraber kullanılması önerilmektedir.

2. katman protokolleri *EAP – Genişleyebilen Kimlik-Sorgulama Protokolü (Extensible Authentication Protocol)* kullandıkları için tek seferlik şifre, kriptografik hesaplama ya da akıllı kart gibi çok miktarda kimlik sorgulama mekanizmalarını destekler. IPSec bunlara binaen IKE protokolünü kullanır. EAP protokolü hakkında detaylı bilgi için RFC 2284'e başvurulabilir.

- *Dinamik adres atama*

2. katman tünelleme yöntemleri *NCP – Ağ Kontrol Protokolü (Network Control Protocol)* mekanizmalarına dayanan dinamik adres atama yöntemlerini desteklerken, 3. katman teknolojileri tünel kurulumundan önce adres atandığını varsayar. Bu konudaki geliştirme çalışmaları halen devam etmektedir.

- *Veri sıkıştırma*

2. katman tünelleme PPP tabanlı sıkıştırma yöntemlerini kullanır. 3. katman için standard IP sıkıştırma protokollerinin kullanılması konusunda IETF tarafından çalışmalar devam etmektedir.

- *Veri kriptolama*

2. katman tünelleme PPP tabanlı şifreleme yöntemlerini kullanır. IPSec, IKE alışverişi sırasında karar verilen çeşitli şifreleme yöntemlerini destekler. L2TP protokolü ile IPSec kriptolama yaygın bir kullanım biçimidir.

- *Anahtar yönetimi*

2. katman teknolojileri kimlik sorgulama sırasında bir anahtar oluşturur ve bu anahtar sürekli güncellenerek kullanılır. IPSec de IKE değişimi sırasında bir anahtar oluşturur ve periyodik olarak bunu günceller.

- *Çok protokollülük desteği*

2. katman protokolleri çerçevenin salt-veri (payload) kısmında IP, IPX, NetBEUI gibi farklı teknolojileri destekleyebilirken IPSec yalnızca IP destekler.

5.2 VPN Tünelleme Protokolleri

5.2.1 Noktadan-Noktaya Protokol – PPP (Point-to-point Protocol)

2. katman tünelleme teknolojileri büyük ölçüde PPP'ye dayandığı için öncelikle bu konuyu incelemekte fayda görüyoruz.

PPP, verilerin çevirmeli-arama ya da atanmış noktadan-noktaya bağlantılar üzerinden aktarımı için tasarlanmıştır. PPP, IP, IPX, NetBEUI paketlerini PPP çerçeveleri içine kapsüller ve bu paketleri noktadan-noktaya linkler üzerinden aktarır. [22]

PPP bağlantısının kurulabilmesi için 3 fazın tamamlanması gerekir;

- *1. faz – PPP link kurulumu*

PPP link kurulumu için *Link Kontrol Protokolü – LCP (Link Control Protocol)* kullanılır. Bağlantının bakımı ve sonlandırılması da LCP ile olur. 1. fazda kullanılacak kimlik-sorgulama mekanizması belirlenir. Aynı zamanda sıkıştırma ya da kriptolama kullanılıp kullanılmayacağına karar verilir (hangi algoritmaların kullanılacağı ise 3. fazda belirlenir).

- *2. faz – Kullanıcı kimlik sorgulama*

Bu aşamada kimlik sorgulama için seçilmiş olan protokol çalışır. Bu protokoller PAP ya da CHAP olabilir. Bu fazda sunucu, kullanıcı kimlik bilgilerini toplar, kendi veritabanındaki (RADIUS, TACACS vs.) bilgiler ile karşılaştırır ve erişimin kabul ya da reddetme kararı verir.

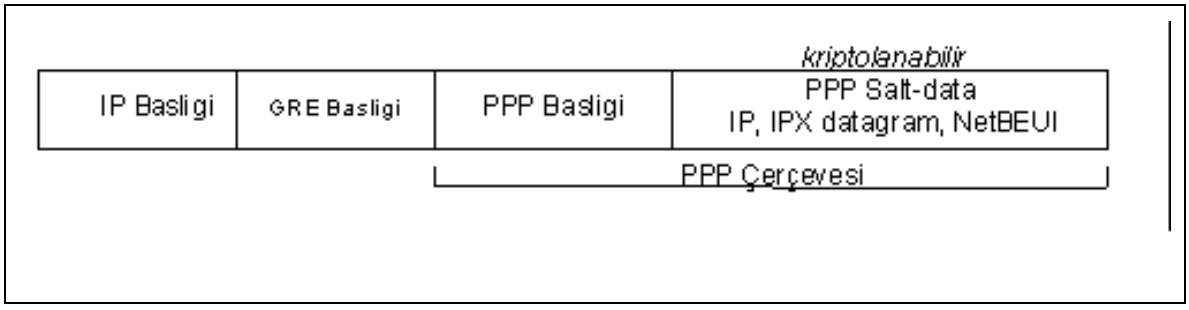
- *3. faz – Ağ katmanı protokol işlemleri*

Bu fazda 1. fazda belirlenen NCP protokolleri devreye girer. IPCP ile kullanıcıya dinamik IP adresi atanır. Eğer 1. fazda sıkıştırma ya da kriptolamaya karar verilmişse burada kullanılacak algoritma ve protokoller belirlenir. Bu aşama da tamamlandıktan sonra veri aktarımı başlar.

5.2.2 Noktadan-Noktaya Tünelleme Protokolü – PPTP (Point-to-point Tunneling Protocol)

PPTP, PPP çerçevelerini IP ortamından göndermek için onları IP datagramları içine kapsülleyen 2. katman protokolüdür. PPTP uzaktan erişim ya da yönlendiriciler arası VPN bağlantısı için kullanılabilir. PPTP, RFC 2637 ile tanımlanmıştır.

PPTP tünel bakımı için TCP ve GRE'nin bir şeklini kullanır. PPP çerçevelerinin salt-veri (payload) kısmı isteğe göre kriptolanabilir ve/veya sıkıştırılabilir. Şekil 5.2'de PPTP kapsülleme ve çerçeve yapısı görülmektedir.



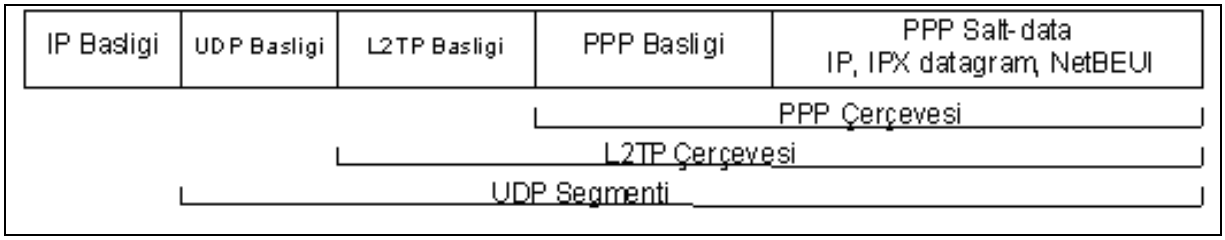
Şekil 5.2. PPTP kapsülleme

5.2.3 İkinci Katman Tünelleme Protokolü – L2TP (Layer 2 Tunneling Protocol)

L2TP, PPTP ile L2F (Layer 2 Forwarding) protokollerinin bir bileşimidir. Cisco Systems tarafından tasarlanmıştır. L2TP, PPTP ile L2F'in en iyi yanlarını biraraya getirmektedir. L2TP, PPP çerçevelerini IP, X.25, Frame-Relay ya da ATM ağları üzerinden aktarmak için kapsüller. IP kullanmak üzere gerekli ayarlar yapıldığında Internet üzerinden aktarım için L2TP kullanılabilir. L2TP RFC 2661 ile ortaya koyulmuştur. [22]

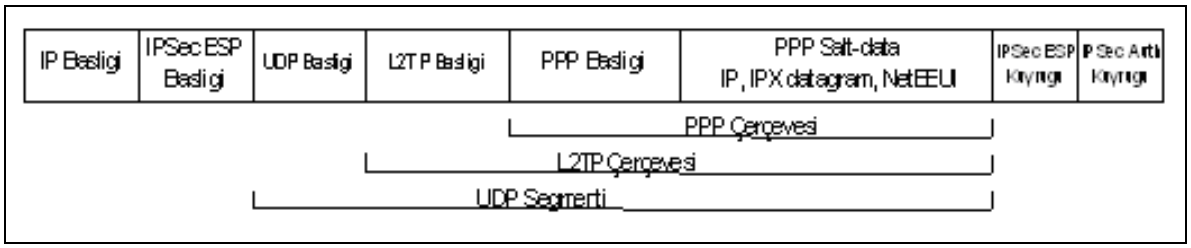
IP üzerinden L2TP, tüneli ayakta tutmak için bir dizi L2TP mesajlarını ve UDP kullanır. UDP ayrıca L2TP tarafından kapsüllenmiş PPP çerçevelerini tünelden aktarmak için de

kullanılır. PPP çerçevelerinin salt-veri kısmı istenirse kriptolanabilir veya sıkıştırılabilir. Şekil 5.3'te L2TP kapsülleme görülmektedir.



Şekil 5.3: L2TP Kapsülleme

L2TP çerçevelerinin kapsüllenmesi için IPSec kullanımı da güvenlik açısından oldukça yaygındır. Buna *L2TP/IPSec Kapsülleme* adı verilir. Bunun için IPSec *ESP (Encapsulating Security Payload)* başlığı kullanılır. Şekil 5.4'te bu yapı görülmektedir.



Şekil 5.4: L2TP/IPSec ESP Kapsülleme

5.2.4 Kapsamlı Yönlendirme Kapsüllemesi – GRE Tünelleme (Generic Routing Encapsulation)

GRE protokolü PPTP protokolü ile beraber olarak istemci sunucu arası VPN bağlantıları kurmak için kullanılır. PPTP kontrol oturumu kurulduktan sonra GRE verinin ya da salt-veri'nin güvenli bir şekilde kapsüllenmesi için kullanılır. Bu salt-veri öncelikle bir PPP çerçevesi içerisine konur daha sonra GRE paketi içerisine kapsüllenir. Veri tünelin uçları arasında bir GRE paketi halinde taşınır. GRE paketi tünelin öbür ucuna ulaştıktan sonra kapsüllenen paket açılır ve alıcıya gönderilir. GRE PPTP ile beraber kullanıldığı için kapsülleme yapısı Şekil 5.2'de verilmiştir.

5.2.5 Internet Protokol Güvenliği – IPSec Tünelleme

IPSec verinin IP ağı üzerinden güvenli aktarımı için kullanılan bir 3. katman protokol standardıdır. IPSec RFC 2401, 2402 ve 2406 ile standardize edilmiştir. IPSec veri bütünlüğü ve kriptolama için kimlik başlığı – AH (authentication header) ve ESP gibi mekanizmalara sahiptir. IPSec ile yalnızca gönderici ve alıcının bildiği bir anahtar kullanılır. Ayrıca TCP/IP ile uyumlu olarak çalışan adres, port ve protokol filtreleme gibi özellikler mevcuttur.

Güvenlik için IPSec'in yanı sıra simetrik ya da asimetrik anahtar (gizli, açık anahtar) kriptolaması, sertifikalar ve EAP gibi mekanizmalar da kullanılabilir. IPSec bir tünelleme mekanizması olarak kullanılırken güvenlik amaçlı olarak IP trafiğinin kriptolanmasının yanı sıra tünelleme için özel bir paket formatı da sunar. L2TP/IPSec'den bahsederken Şekil 5.4'te bunu sunmuştuk. IPSec tüneli, her ikisi de IPSec tünelleme için ayarlanmış ve parametreler üzerinde anlaşmış bir tünel istemcisi ile sunucusundan oluşur. IPSec tünel modu kapsülleme için bir güvenlik yöntemi belirler ve tüm IP paketlerini kriptolayarak özel ya da paylaşımlı IP ortamından gönderir. Kriptolanan salt-veri IP başlığı ile tekrar kapsüllenir ve tünel sunucusuna gönderilir. Sunucu paketi alınca IP başlığını atar ve paketi dekript ederek orjinal veriye dönüştürür. Veri bu şekliyle son alıcısına gönderilir. [5][22]

Tablo 5.1'de konuya yabancı olan kişilere bu kısma kadar adı geçen protokoller konusunda başvurabilecekleri RFC'lerin bir listesini vermeyi uygun görüyoruz.

5.3 VPN Modelleri

VPN içerisindeki tüm yerleşkeler aynı yönetim, bağlantı ve servis kalitesi politikalarına uygun olarak değerlendirilebilirler. VPN gerçekleştirmek için farklı yerleşkeler arasındaki bağlantının VPN hizmeti veren bir servis sağlayıcı üzerinden sağlanması gerekir. Bu nedenle VPN için tanımlanan politikaları servis sağlayıcının kendisi tarafından tanımlanması mümkündür. Bazı durumlarda VPN hizmeti alacak müşterinin de kendi politikalarını tanımlaması mümkündür.

Tablo 5.1: VPN teknolojisinde kullanılan protokoller ve RFC kodları

Protokol Adı	RFC No	Bağlantısı
L2TP	2661	*http://www.ietf.org/rfc/rfc2661.txt?number=2661*
PPTP	2637	*http://www.ietf.org/rfc/rfc2637.txt?number=2637*
GRE	1701	*http://www.ietf.org/rfc/rfc1701.txt?number=1701*
IPSec	2401,2402 2406, 3193	*http://www.ietf.org/rfc/rfc2401.txt?number=2401* *http://www.ietf.org/rfc/rfc2402.txt?number=2402* *http://www.ietf.org/rfc/rfc2406.txt?number=2406*
EAP	2284	*http://www.ietf.org/rfc/rfc2284.txt?number=2284*
IPSec IKE	2409	*http://www.ietf.org/rfc/rfc2409.txt?number=2409*
PPP NCP	1841	*http://www.ietf.org/rfc/rfc1841.txt?number=1841*
PPP IPCP	1332	*http://www.ietf.org/rfc/rfc1332.txt?number=1332*
PPP LCP	1570	*http://www.ietf.org/rfc/rfc1570.txt?number=1570*
L2F	2341	*http://www.ietf.org/rfc/rfc2341.txt?number=2341*

VPN kullanan kurumların yerleşkeleri arasındaki ağ grafı tam-bağlı olabileceği gibi merkez ve yerleşkeler arasında yıldız (hub-and-spoke) şeklinde olması mümkündür. Tam bağlı yapıda yerleşkeler arasında VPN bağlantısı doğrudan kurulabilirken yıldız yapısında bağlantının merkez üzerinden kurulması zorunludur. Yıldız yapısında merkezden geçmeden doğrudan yerleşkeler arasında tünel kurulabilmesi için çalışmalar devam etmektedir (Cisco Systems tarafından 2003 yılı içerisinde ortaya konulan *DMVPN - Dynamic Multipoint VPN).*

VPN teknolojisinde bir yerleşke içerisinde farklı VPN bağlantıları gerçekleştirmek mümkündür. VPN yapan yalnızca bir kurum olabileceği gibi farklı kurumların da VPN oluşturması istenebilir (örneğin tedarik zinciri içerisinde haberleşmeleri gereken şirketler ortak bir VPN içerisinde yer alarak verilerini paylaşmak isteyebilirler). VPN kullanan bir kurumun farklı yerleşkelerdeki birimleri arasında oluşturduğu ağa *intranet,* farklı kurumlar arasındaki VPN ağında da *ekstranet* adı verilir. Bir yerleşke birden fazla VPN'e üye olabilir aynı zamanda hem intranet hem de ekstranetin parçası olabilir. Bu nedenle VPN bağlantılarında servis sağlayıcının esnek olması gerekir.

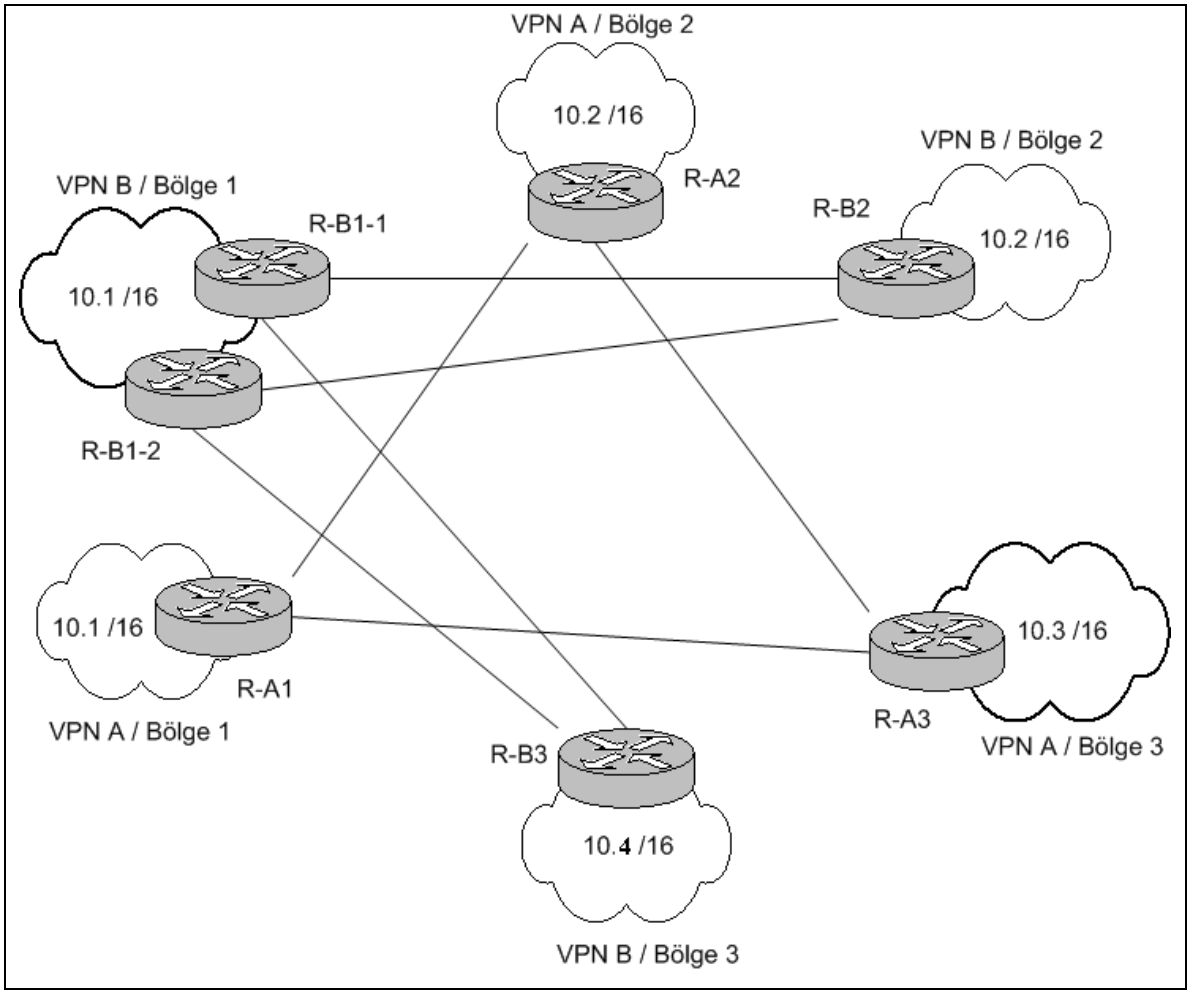
Yukarıda ve önceki bölümlerde bahsettiğimiz özellikler nedeniyle günümüzde servis sağlayıcıların çok yüksek sayılarda kullanıcılarına VPN hizmeti sundukları için hem bunları performans olarak karşılayabilecek yüksek kapasiteli bir omurgaya hem de müşterilerin kendi VPN'leri üzerinde politika tanımları yapmalarına izin verecek esnekliğe sahip olmaları zorunludur. Servis sağlayıcılar tarafından yaygın olarak kullanılan ATM teknolojisi daha önceden de bahsettiğimiz gibi ölçeklenebilirlik ve esneklik açısından sıkıntı yaratmaktadır. Bu nedenle servis sağlayıcıların güvenilir ve performanslı çok yerleşkeli VPN hizmeti vermesi zorunlu hale gelmekte bu da MPLS VPN'e geçişe olan eğilimin artmasının açık sebebi olmaktadır. MPLS VPN mekanizmalarından detaylı olarak bahsetmeye başlamadan önce VPN modellerinin kıyaslamalı tanımını ve MPLS VPN'e geçişi sürükleyen etkenleri açıklamakta fayda vardır. [5]

5.3.1 Kaplama (Overlay) Modeli

Günümüzde halen kullanılan VPN servislerinin büyük çoğunluğu *kaplama model* ile çalışmaktadır. Kaplama modelde her yerleşke VPN içerisindeki diğer yerleşkelere noktadan-noktaya bağlantısı olan bir yönlendiriciye sahiptir. Bu bağlantılar tüm yerleşkelere olabileceği gibi yalnızca belirli yerleşkelere de olabilir. Noktadan noktaya bağlantılar için kiralık hatlar, Frame-relay devreleri veya ATM devreleri kullanılabilir. Birbirleri arasındaki bağlantılarla yönlendiricilerin oluşturduğu bu yapıya *'sanal omurga' (virtual backbone)* adı verilir.

Kaplama modelin daha rahat anlaşılması için Şekil 5.5'teki örneği inceleyelim. Şekilde 3 yerleşke yer almaktadır. Bu yerleşkelerdeki herbir yönlendirici farklı bir VPN'e üye olabilmektedir. Şekilde görülen tüm VPN tünelleri bir servis sağlayıcı üzerinden sağlanmaktadır. VPN A tam bağlı yapıya sahipken VPN B 1. yerleşke üzerinden yıldız tipinde bağlanmıştır. Merkez konumundaki 1. yerleşkeye iki adet yönlendirici yedekli olarak yerleştirilerek sistemdeki kritik hata noktası güçlendirilmiş (Single-point-of-failure engellenmiş). Görüldüğü üzere VPN A ve VPN B aynı adres uzayını kullanmaktadır ayrıca bu VPN'ler ayrı yönlendirme protokolleri de koşturuyor olabilir (OSPF, RIP gibi).

Günümüzde çoğunlukla kaplama model kullanılmasına karşın bu modelin birtakım problemleri mevcuttur. Özellikle büyük ölçekli VPN çözümlerinde kaplama model yetersiz kalmaktadır.



Şekil 5.5: Kaplama (Overlay) VPN Modeli

İlk problem VPN hizmeti alan kurumların kendi sanal omurgalarını yönetmek istemelerinden kaynaklanmaktadır. Bunun için şirketlerin omurgayı yönetebilecek bilgiye sahip olmaları gerekir, bu her zaman mümkün değildir. Bunun için *'yönetilen yönlendirici' (managed router)* kavramı ortaya çıkmıştır. Yönetilen yönlendirici hizmetinde servis sağlayıcılar müşteri kurumlar adına yönetim işlevini gerçekleştirmekte ancak binlerce VPN kullanıcısı olan bir servis sağlayıcı için bu büyük bir yönetimsel yük oluşturmaktadır. [2]

Diğer bir problem de IP over ATM'de bahsettiğimiz tam-bağlı yapı problemidir. *N* yerleşkeden oluşan bir VPN için her bir omurga yönlendiricisinin *N-1* tane komşuluk yani tünel kurması gerekir. Bu da maliyeti ve ağdaki yükü arttırır. Ayrıca ağa yeni bir yerleşke eklemek gerektiği zaman bu büyük bir sorun olmaktadır.

Kaplama modelde yapılan bir değişiklik de servis sağlayıcının yönlendiricileri *'sanal yönlendirici'* olarak değerlendirmesidir. Bir yönlendirici çok sayıda sanal yönlendiriciden oluşabilir. Sanal yönlendiricilerin fonksiyonu fiziksel yönlendirici ile aynıdır ancak bunların özelliği aynı CPU, bandgenişliği ve bellek kaynaklarını kullanmalarıdır. Sanal yönlendiriciler birbirlerine noktadan-noktaya hatlarla bağlıdır. Bu hatların sayısını azaltmak için çok sayıda hat bir kiralık devre, Frame-Relay ya da ATM devresi içine çoğullanabilir. Her yerleşkenin kendine ait bir sanal yönlendiricisi vardır. Böylece bu sanal yönlendiriciler ve aralarındaki hatlar sanal omurgayı oluşturur. [2]

Sanal yönlendirici kullanımının avantajı 'yönetilen yönlendirici' hizmeti veren servis sağlayıcının yönetmesi gereken fiziksel ekipman sayısını azaltmaktadır. Çünkü her bir fiziksel yönlendirici çok sayıda yönlendiricinin yerine geçmekte ve her bir sanal yönlendirici bir VPN bağlantısı için kullanılabilmektedir. Sanal yönlendirici kullanımı bahsettiğimiz birtakım avantajları sağlasa da kaplama modelin sorunlarına bir çözüm üretmemektedir.

VPN'de yerleşkeler arası bağlantıda IPSec ve GRE tünellerinin kullanımı da kaplama modelin sorunlarına çözüm olmamaktadır. GRE tünellerinin kullanımı ile *'veri aldatma'(data spoofing)* problemi ile karşılaşmak olasıdır.GRE tünelin sonundaki bir IP adresine giden bir trafikte VPN içerisine bir paket yerleştirerek gerçek göndericiden gidiyormuşçasına göndermek mümkündür.Bu paket filtreleri ile engellenebilir ancak bu da karmaşıklığı arttırmaktadır.

Bunu engellemenin bir diğer yolu da GRE tünelleri yerine IPSec tünellerinin kullanılmasıdır. IPSec ile tünelin sonundaki alıcı ile gönderici kimlik sorgulama ile birbirlerini tanırlar böylece gerçek gönderici dışında kimsenin paketleri kabul edilmez. IPSec, veri aldatma ataklarına karşı etkin bir çözüm sunmasına rağmen kimlik sorgulama için anahtar yönetiminin gerekmesi de ekstra bir yüktür. VPN yönetiminin servis sağlayıcı tarafından yapıldığı durumlarda anahtar yönetimi de servis sağlayıcı tarafından

yapıldığı için veri gizliliği tam olarak sağlanamamış olmaktadır. Bu da IPSec'in güvenlik avantajından müşterilerin tam olarak faydalanamaması anlamına gelir.

Sonuç olarak burada bahsettiğimiz üzere kaplama model büyük ölçekli VPN çözümleri için yetersiz kalmaktadır. Bu nedenle yerleşkeler arası bağlantı çözümleri için farklı bir model üzerinde durulmalıdır.

5.3.2 Eş (Peer) Modeli

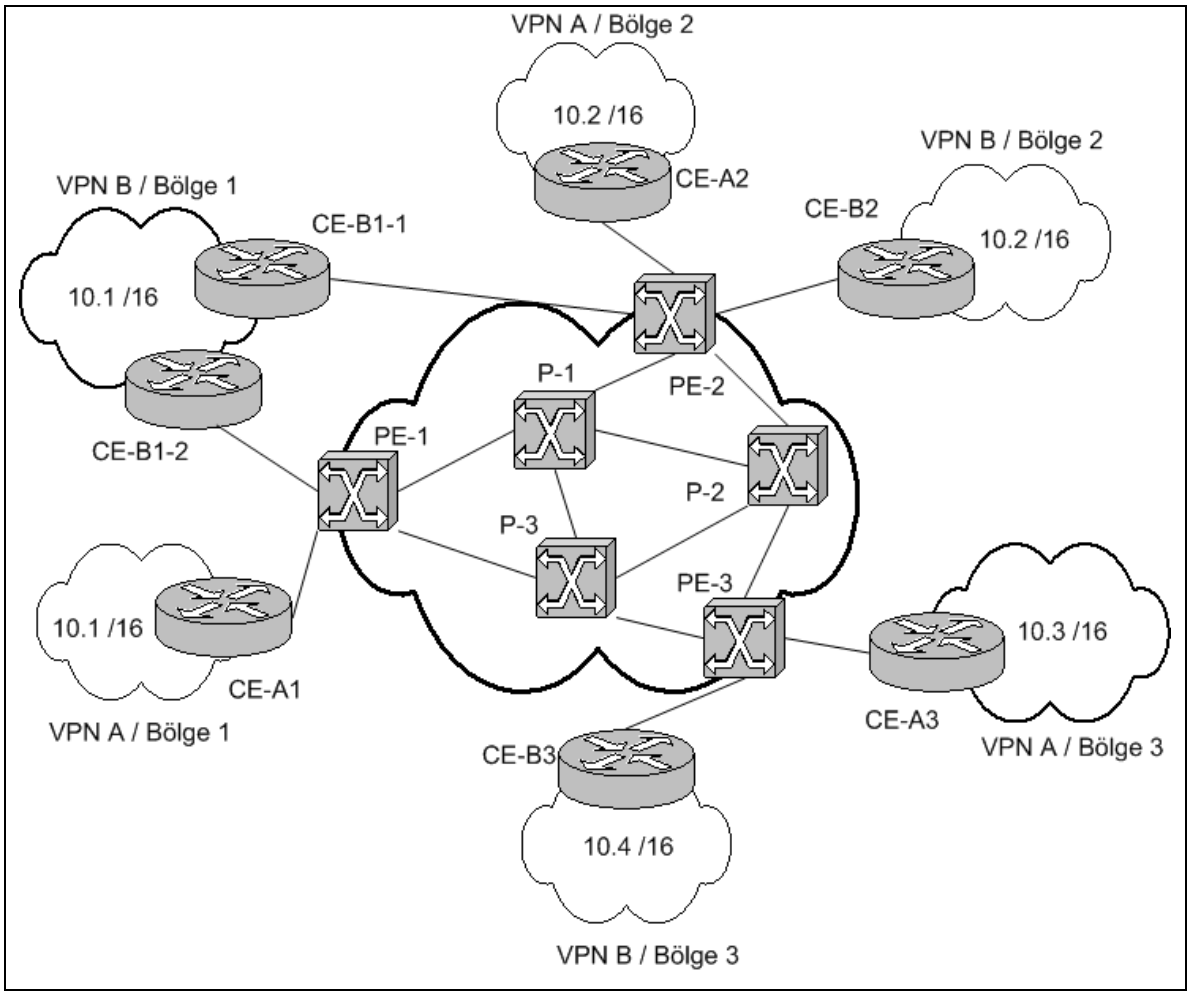
Eş modelinin ortaya koyulmasındaki temel amaç kaplama modelinden kaynaklanan kısıtlamaları aşmaktır. Bu model farklı ölçeklerdeki çok sayıda VPN hizmetinin servis sağlayıcılar tarafından farklı profildeki müşterilere verilebilmesini sağlamaktır. Ayrıca bunu gerçekleştirirken maliyetlerin düşürülmesi de hedeflenmektedir. Modeli daha iyi anlayabilmek için Şekil 5.6'daki topolojiyi inceleyelim. [2]

Şekilde görüldüğü üzere müşteri tarafındaki bir müşteri sınır yönlendiricisi (CE - Customer Edge) servis sağlayıcının sınır yönlendiricisine (PE – Provider Edge) bağlıdır. PE'ler arası haberleşme servis sağlayıcı yönlendiricileri (P - Provider) üzerinden gerçekleşir. Bir PE farklı VPN'lere ait yerleşkelere bağlanıyor olabilir. Dahası bu yerleşkeler aynı IP adres uzayını da kullanabilirler. RFC 1918 ile belirlenen özel IP adreslerinin kullanımında bir kısıtlama yoktur. Aynı VPN içerisinde tüm IP adresleri tek/eşsiz olmalıdır ancak farklı VPN'lerde aynı IP adresi kullanılabilir. Örneğin 2. yerleşkede kullanılan 10.2 /16 bloğu her iki VPN'de de kullanılmaktadır.

Bu modele eş modeli denmesinin nedeni yönlendirme bakış açısından müşterilerin birbirleriyle yerleşkeler arası VPN oluşturmak yerine, servis sağlayıcının yönlendiricileri ile komşuluk oluşturmasıdır. Bu model servis sağlayıcının omurgasında MPLS kullanımı ile konumuz açısından önem kazanmaktadır.

5.4 MPLS VPN Mekanizmaları

Bu kısımda ve ileriki bölümlerde performans ve servis kalitesi testlerinde yalnızca BGP temelli MPLS VPN incelenmektedir. [1][2][4]



Şekil 5.6: VPN Eş (Peer) Modeli

5.4.1 Yönlendirme Bilgisinin Sınırlı Dağıtımı

Yerleşkeler arası verinin akışını kontrol edebilmek için bir mekanizma gereklidir. Bu, yönlendirme bilgisinin dağıtımının sınırlandırılmasıdır. Veri akışını belirleyen, aktarımını yapan yönlendiricilerin sahip olduğu yönlendirme bilgisi olduğu için yönlendirme bilgisinin dağıtımının sınırlandırılması aynı zamanda veri akışının da sınırlandırılması anlamına gelir.

Verinin yerleşkeler arasında aktarımını aşağıdaki aşamalar sonucu gerçekleşir;

1. Müşteri yerleşkesinden servis sağlayıcıya yönlendirme bilgisinin geçişi. Bu işlem RIP, OSPF, statik yönlendirme ya da BGP ile gerçekleştirilir.

2. Giriş PE yönlendiricisinden bu yönlendirme bilgisinin diğer PE'lere P'ler üzerinden aktarılması. Bu dağıtım BGP protokolü kullanılarak gerçekleştirilir.

3. Çıkış PE yönlendiricisinden yönlendirme bilgisinin diğer müşteri yerleşkelerine CE'lere aktarılması. Bu işlem de RIP, OSPF, statik yönlendirme ya da BGP ile gerçekleştirilir.

Yönlendirme bilgisinin sınırlandırılması için filtreleme yöntemi olarak BGP komünite (community) özelliği kullanılmaktadır. Komünite bilgisi duyurulan yönlendirme bilgisine eklenen bir belirteçtir. 2. aşamada yönlendirme bilgisi bir IGP ile alındıktan sonra BGP içerisine duyurulurken komünite değeri de rota bilgisine eklenir. 3. aşamada çıkış PE yönlendiricisi yönlendirme bilgisini CE'ler ile müşteri yerleşkelerine ulaştırırken bu komünite değerine göre ilgili yerlere bu bilgiyi duyurur, ilgisizlere duyurmaz.

BGP komünite özelliği yönlendirme ve filtrelemede büyük esneklik sağlamaktadır. Bu sayede bir PE belli bir yerleşkeden gelen tüm bilgileri bir komünite içerisine alabileceği gibi bir diğeri belirli bir rotaya ilişkin bir komünite tanımlayabilir. Her bir VPN için en az bir komünite değeri tanımlanmalıdır. Komünite atama işlemleri servis sağlayıcıya ait olan PE'ler üzerinde gerçekleştirilir yani müşterilerin bu konuda bilgi sahibi olmasına ihtiyaç yoktur.

Yerleşkeler arası bağlantıyı sağlamak için kullanılan BGP/MPLS VPN mekanizmalarını incelediğimiz zaman çok sayıda getirisini görebiliriz. Öncelikle; yerleşkeler artık birbirleri arasında komşuluk kurmadıkları ve sadece ilgili PE ile komşuluk kurdukları için kurulan komşuluk sayısı VPN içerisinde yer alan yerleşke sayısından bağımsız ve sabit olmaktadır. Böylece bağlantı sayısı azalmaktadır. Tam-bağlı bir yapı kurulmak istendiğinde kaplama modelde tüm yerleşkeler arasında bağlantı çekmek gerekirken artık buna gerek kalmadan, tam-bağlı yapı servis sağlayıcı omurga yönlendiricileri üzerinden gerçekleştirilmektedir.

İkinci getirisi VPN içerisine yeni bir yerleşke eklenmek istendiğinde eş modelinde, var olan yerleşke sayısından bağımsız olarak sadece ilgili PE'ye yeni bir hat çekerek bunun gerçekleştirilebilmesidir.

Diğer bir getirisi de servis sağlayıcı omurgasında yer alan PE'lerin yalnızca kendisi ile komşuluk kuran, doğrudan bağlı yerleşkelerdeki VPN bilgisini taşıması ve kendine gelmeyen VPN bilgileri için yönlendirme tablosunda yer açmasına ve ilgilenmesine gerek kalmamasıdır.

BGP komünite belirteci 32 bitlik bir değerdir ve bunun 16 bitlik kısmı otonom sistem numarası, 16 biti ise komünite değeridir. Bu nedenle her VPN'e en az bir komünite değeri ataması da gerektiği için servis sağlayıcının taşıyabileceği maksimum VPN sayısı 2^{16} ile sınırlandırılmaktadır. Sonradan geliştirilen 'genişletilmiş komünite' (extended community) özelliği ile 16 bitlik komünite kısmı 32 bite genişletilmiş ve bu sorun da aşılmıştır.

5.4.2 Çok Sayıda İletim Tablosunun Kullanımı

Sınırlı yönlendirme bilgisi dağıtımı uyguladığımız yönlendiricilerde yalnızca bir tane iletim tablosunun bulunması durumunda tüm VPN'lere ilişkin bilgilerin bu tabloda tutulması gerekirdi. Bu durumda herbir VPN'e has bilgilerin ayırt edilmesi mümkün olmayacak ve bir VPN'den diğerine paket aktarımı söz konusu olacaktır. Oysa ki bu VPN uygulama mantığına aykırıdır.

Bunun için her PE yönlendiricisinin çok sayıda iletim tablosuna sahip olması gerekir. Genellikle bunun her VPN başına atanmış ayrı bir iletim tablosu olması tercih edilir ki böylece VPN bilgileri birinden diğerine aktarılmaz. PE yönlendiricileri hangi portun hangi müşteriye gittiğini ve bunun hangi iletim tablosu ile ilişkilendirileceğini bilirler. İletim sırasında buna göre ilgili tablodan bilgi bulunarak kullanılır.

PE yönlendiricisine gelen iki farklı kaynaktan bilgi vardır. Birincisi doğrudan bağlı olduğu CE yönlendiricilerinden kullanılan IGP ile gelen bilgiler, bunlar doğrudan o müşterinin kullandığı VPN'e ilişkin tabloya alınır. Diğer bilgi kaynağı ise PE'lerden gelenlerdir. Bu bilgiler içerisinden BGP komünite özelliğine göre belirtece bakılarak hangi bilginin hangi tabloya alınacağı belirlenir.

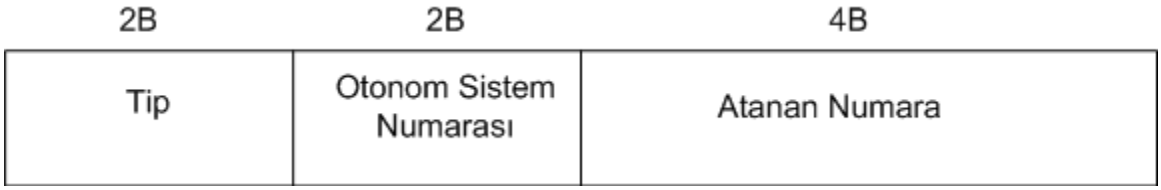
5.4.3 Çok Protokollü BGP (MP-BGP) ve VPN-IP Adresleme

Şu ana kadar VPN kullanarak yerleşkeler arası haberleşmenin nasıl sağlanacağından bahsedildi. Bahsedilen mekanizmalar BGP kullanmaktadır ve BGP protokolünün global

olarak tek/eşsiz adresleme mantığını kullanarak bu işlemleri gerçekleştirilmektedir. Oysa VPN mantığında aynı IP adreslerinin farklı VPN'lerde kullanılabildiğinden bahsetmiştik öyleyse bunu sağlayacak yeni özellikler gerekmektedir.

Bunun için kullanılan IP bloğu aynı olsa da yönlendirilen adreslerin global olarak eşsiz/tek olmasını sağlayan yeni bir IP adresi kavramı *VPN-IP* geliştirilmiştir. VPN-IP adreslerinin dağımını sağlayan BGP protokolüne de *MP-BGP* (çok protokollü BGP) adı verilir. [1][2][4]

VPN-IP adresleri, IP adreslerinin *Rota Ayrıştırıcı (Route Distinguisher)* adı verilen sabit-uzunluklu bir alan ile birleştirilmesiyle elde edilir. Rota ayrıştırıcının yapısı Şekil 5.7'de görülmektedir.



Şekil 5.7: VPN-IP Rota Ayrıştırıcı

Otonom sistem numarası VPN servis sağlayıcının otonom sistem numarasıdır. Atanan numara ise servis sağlayıcı tarafından VPN başına belirlenen değerdir. Farklı servis sağlayıcıların otonom sistem numaraları farklı olduğu için ve servis sağlayıcı tarafından herbir VPN'e atanan numara farklı olduğu için rota ayrıştırıcının global olarak birden fazla olması mümkün değildir.

MP-BGP ile VPN-IP adreslerinin dağıtımı standard IP kullanımından farklı değildir. VPN-IP adreslerinin kullanımı servis sağlayıcının kontrolündedir. Müşterilerin kendilerine atanan VPN-IP adresinden haberi yoktur. VPN-IP adreslerinin IP adreslerine dönüşümü PE yönlendiricilerinde yapılır. PE yönlendiricileri kendilerine bağlı herbir VPN için bir rota ayrıştırıcı belirler. Bilgiyi P'lere aktarırken rota ayrıştırıcı bilgisini IP adresine ekler gönderirler. Tersi durumda CE'lere bilgi aktarırken PE'ler rota ayrıştırıcıları kaldırır ve salt IP olarak gönderir. VPN-IP adresleri yalnızca yönlendirme protokolleri içerisinde taşınır. IP paket başlıklarında taşınmaz. Dolayısıyla doğrudan paket iletiminde kullanılmazlar. Paket iletimi MPLS tarafından gerçekleştirilir.

5.4.4 MPLS VPN ile İletim

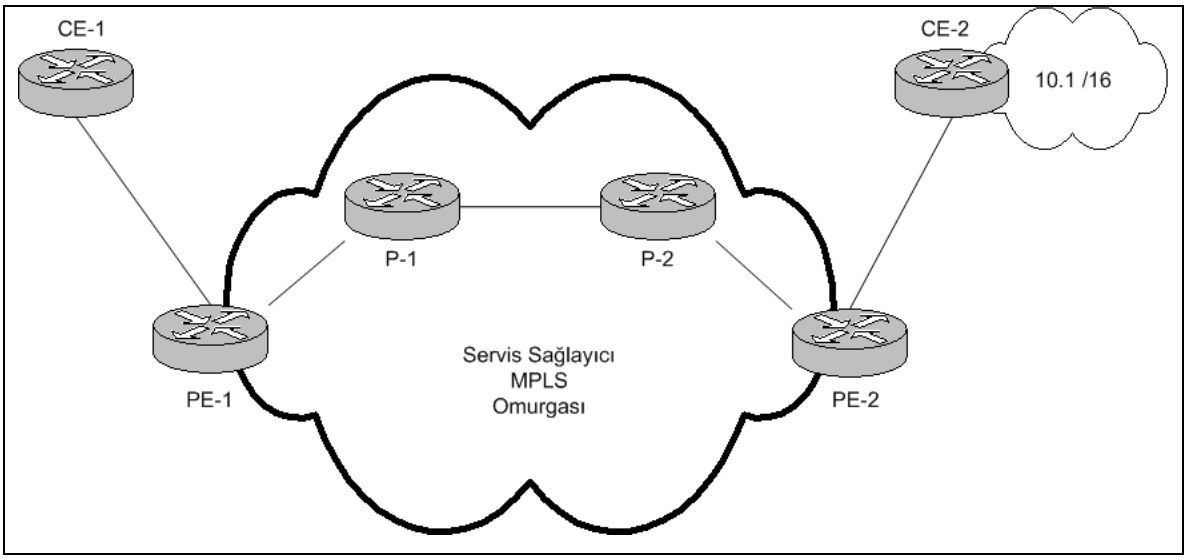
Paketlerin belirli rota boyunca VPN-IP adreslerinin kullanılarak iletiminde MPLS teknolojisi kullanılır. Bunu yapabilmemizin nedeni MPLS'in IP başlığına göre iletim yerine etiket iletimi gerçekleştirmesidir. Böylece VPN-IP adresleri ile LSP'lerin eşlenmesi mümkün olmaktadır.

Sistemin işleyişi şu şekildedir:

- Bir CE yönlendiricisi PE yönlendiricisine IP paketini gönderdiği zaman, PE paketin geldiği porta bakarak CE yönlendiricisinin hangi VPN'e ait olduğunu bulur ve bu VPN'e ilişkin LFIB'e bakar. LFIB tablosunda hedef IP adresine göre arama yapılır. LFIB tablosundan bu hedef IP'ye ilişkin etiket bulunur ve paket etiketlenerek iletilir.
- Paket etiketlenerek gönderildiği için artık PE'den etiketli paketi alan P yönlendiriciler VPN bilgisiyle daha fazla ilgilenmez. Bunu sağlayan MPLS'in hiyerarşi yapısıdır. MPLS VPN'de iki seviyeli etiketleme kullanılır. Bu etiketlerden ilki giriş PE LSR'ından çıkış PE LSR'ına kadar olan rotayı gösterirken, ikincisi çıkış PE yönlendiricisinde iletimin nereye yapılacağı ile ilgilidir. İlk seviye etiket LDP ile dağıtılır ve bir LSP'nin kurulması sağlanır. İkinci seviye etiket ise BGP ile dağıtılır. Bunu BGP ile etiket dağıtımından bahsederken incelemiştik.

Şekil 5.8'deki topoloji üzerinde bu durumu örnekleyelim:

- PE-2 yönlendiricisi CE-2 yönlendiricisinden 10.1 /16 ağına ilişkin bir yönlendirme bilgisi aldığında, PE-2 bu IP adresini VPN-IP adreslerine çevirir. BGP komünite değerini de ekleyerek bu yön bilgisini servis sağlayıcının BGP'sinin içine dağıtır. Bu dağıtım sırasında BGP 'sonraki-sekme' değeri PE-2 olarak belirtilir. Bu BGP bilgisinin yanı sıra bu rotaya ilişkin de bir etiket atanır. Bu etiket bilgisi PE-1'e BGP ile dağıtılır. PE-1 bu yön bilgisini alınca VPN-IP adresini IP'ye çevirir ve o VPN'e ilişkin iletim tablosuna yerleştirir.



Şekil 5.8: MPLS VPN İletim Mekanizması

- Bu sırada PE-1'den PE-2'ye LDP ile oluşturulan bir LSP kurulur. BGP ile dağıtılan bilgide sonraki-sekme olarak PE-2 yer almaktadır. Yani iç etiket BGP ile dağıtılan ve sonraki-sekme olarak PE-2'yi gösteren etiketlerken, dış etiket LDP ile oluşan PE-2'ye doğru LSP'yi gösteren etikettir (PE-1'in tablosunda).
- CE-1'den bir paket 10.1 /16 ağına gönderilmek istendiğinde PE-1 bunu alır. Tablosuna bakar, iki seviyeli etiket bilgisini pakete ekler ve bunu P-1'e gönderir. P-1 iletim kararını verirken paketin dış etiketine bakar ve bunu P-2'ye gönderir. P-2 kendisinin PE-2'ye doğru olan LSP için sonlandırıcı sekme olduğunu bildiği için dış etiketi kaldırır ve paketi PE-2'ye gönderir. PE-2 paketi alınca BGP ile dağıtılan etikete bakar, VPN-IP adresini IP'ye çevirir ve paketi CE-2'ye gönderir.

MPLS VPN geleneksel IP VPN ile sunulan güvenlik özelliklerinin tümünü yüksek kapasiteli bir omurga ağına uygulama imkanı vermektedir. Ancak MPLS VPN'in asıl etkisi özellikle servis sağlayıcılara getirdiği ölçeklenebilirlik ve esneklik yeteneğidir. Önceki bölümlerde bahsettiğimiz gibi MPLS-VPN kullanımı ile bir CE yönlendiricisinin kurması gereken komşuluk sayısı VPN içerisindeki yerleşke sayısı ile sınırlı olmaktadır. Böylece büyük ölçekli VPN'ler desteklenebilmekte ve VPN içerisine yeni bir yerleşke eklenmesi çok kolaylaşmaktadır.

MPLS-VPN'in ölçeklenebilirlik açısından tek getirisi bu değildir. Yönlendirme bilgisinin taşınması ve tutulması açısından da büyük avantajları mevcuttur. Örneğin P yönlendiricileri VPN bilgisinden tamamen bağımsız tutuldukları için (hiyerarşik etiketleme ile) bu yükten kurtulmuş olmaktadırlar. Örneğin toplam 200 yönlendiricinin (PE ve P) bulunduğu bir ağda ortalama 100 rotanın bulunduğu 10.000 VPN'e hizmet verildiğini varsayarsak önceden bir P yönlendiricisinin 10.000 * 100 = 1.000.000 rota bilgisi tutması gerekirken şimdi VPN bilgisi ile ilgilenmedikleri için ağdaki diğer tüm yönlendiricilere ilişkin rota bilgisinin yani 200 rotanın tutulması yeterlidir. [2]

VPN bilgisi yalnızca PE yönlendiricilerinde tutulmaktadır. Dahası PE yönlendiricilerinin tuttuğu VPN bilgisinde de büyük azalma vardır çünkü her PE artık yalnızca kendine doğrudan bağlı yerleşkelerdeki VPN bilgileri tutmakla yükümlü kılınmaktadır. Bir yerleşkeye bağlı PE üzerindeki VPN yükünün artması durumunda yeni bir PE eklenerek VPN'lerin bir kısmının diğer PE'ye transfer edilmesi yeterli olmaktadır.

Sonuç olarak, günümüzün hızlı gelişen iş ve iletişim dünyası geleneksel süreçlerden sıyrılarak etkin, verimli, hızlı ve entegre haberleşmeye ihtiyaç duymaktadır. VPN teknolojisi kurumların üretkenliklerini arttırıp maliyetlerini düşürme konusunda güvenli ve etkin bir çözüm sunmaktadır. Artık birbirinden bağımsız yerleşke içi ağlar yerine coğrafyadan bağımsız olarak etkileşebilen ve bunu yaparken ses, veri ya da video gibi veri tiplerinin tümünü destekleyen VPN sistemleri en büyük ölçekli organizasyonlardan en küçük ofislere kadar alternatifsiz olarak kullanılmaktadır. MPLS/VPN gibi yeni teknolojik mekanizmalar ile de bu yapı kurumsal ve geniş servis sağlayıcı ağları ile genişlemeye devam edecektir.

6. MPLS/VPN AĞLARINDA SERVİS KALİTESİ

Servis kalitesi (QoS), ağın belirli trafiklere daha iyi hizmet sunabilmesi için kullanılan mekanizmalar bütünüdür. Servis kalitesinin temel parametreleri garanti edilen bandgenişliği, düşük jitter, düşük gecikme ve düşük paket kaybıdır. QoS mekanizmaları ile bir trafiğin diğerlerine göre önceliklendirilmesi, ayrı kuyruğa alınması ve bu şekilde düşük gecikmenin sağlanması mümkündür.

MPLS teknolojik olarak büyük getiriler sunduğu *VPN* ve *Trafik Mühendisliği*'ne kıyasla geleneksel IP QoS mekanizmalarına çok fazla yenilik getirmemekte, yalnız performans ve esneklik konusunda olumlu katkıda bulunmaktadır. MPLS ağlarında QoS özelliklerinin daha etkin olarak uygulanabilmesi mümkündür. [9]

IP QoS uçtan-uca bir protokol ve hizmetler kümesidir. MPLS uçtan-uca yani istemci ile sunucu arasında değil omurgada kullanıldığı için QoS ile uçtan-uca bağlantıda bir hattın bir trafik için daha yüksek garantili bandgenişliğine ya da düşük gecikmeye sahip olması bağlantının bütününde değil yalnızca omurgada mümkündür.

MPLS QoS, IP QoS mekanizmalarının daha geniş bir alanda (ATM LSR'lar dahil) daha etkin uygulanmasına olanak verdiği için bu başlık altında öncelikle IP QoS mekanizmalarının neler olduğundan daha sonra bunların MPLS ağlarındaki uygulamalarından bahsetmek doğru olacaktır. Konunun son kısmında tezimizin kapsamı dahilinde olmamakla beraber MPLS'in en büyük getirilerinden biri olan trafik mühendisliğinden de fikir sahibi olunabilmesi için biraz bahsedilecektir. [1][8]

IP QoS'ta iki ana model mevcuttur. Bunlar,

- Bütünleşik Servisler (Integrated Services - IntServ)
- Farklılaştırılmış Servisler (Differentiated Services - DiffServ)

6.1 Bütünleşik Servisler (IntServ) ve RSVP

IntServ ilk olarak Haziran 1994'te RFC 1633 ile IETF çalışma grupları tarafından tanımlanmış bir modeldir. IntServ mimarisi ihtiyaç duyan kullanıcılara uçtan-uca QoS garantisi vermek amacıyla oluşturulmuştur. Bu garantiler ağdaki yol boyunca minimum bandgenişliği miktarı olabileceği gibi uçtan-uca gecikme de olabilir. Bu servis garantilerini sağlamak üzere servis sınıfları tanımlanmıştır. Servis sınıflarını kullanarak QoS isteğinde bulunabilmek için ayrı bir IETF çalışma grubu tarafından 1997'de RFC 2205 ile *Kaynak Rezervasyon Protokolü – RSVP (Resource Reservation Protocol)* geliştirilmiştir. [8]

Günümüzde büyük çoğunlukla IntServ ile RSVP birbiri ile karıştırılmakta ve aynı anlama geliyormış gibi değerlendirilmektedir, oysa ki bu yanlış bir yaklaşımdır. IntServ bir QoS modeli iken, RSVP kullanıcıların QoS isteğinde bulunabilmelerini sağlayan bir sinyalleşme protokolüdür. IntServ çok sayıda sinyalleşme protokolünü destekler, RSVP bunlardan bir tanesidir (ST-II veya SNMP diğer sinyalleşme protokolleridir, ancak pratikte yalnızca RSVP kullanılmaktadır). Benzer biçimde RSVP de farklı bilgi tiplerinin sinyalleşmesini destekler, bunların yalnızca IntServ mesajları olması gerekmez. Bizim buradaki kullanımımız QoS mimarisi olarak IntServ'in sinyalleşme protokolü olarak RSVP kullanımı üzerinedir. [2][10]

IntServ mimarisinde kullanıcıların istekte bulunabilmesi için ağdaki trafik özelliklerini de bilmeleri gerekir. Bir ağdaki trafik özelliklerine *TSpec (Traffic Specification)* adı verilir. Ağdaki yönlendiriciler gelen trafiğin TSpec'e uygun olup olmadığını kontrol ederler. Uyumlu olmayan paketler atılır.

IntServ ayrıca QoS seviyesi ve ağ kaynaklarının rezervasyonu isteğini karşılayan bir *Rezervasyon Özelliği – RSpec (Rezervation Specification)* parametresine sahiptir. Gelen istekler kabul kontrolüne (admission control) tabi tutularak kaynakların isteği karşılamaya uygun olup olmadığı belirlenir. Uygun olmayan rezervasyon istekleri reddedilir. [2][8]

IntServ ağ bileşenlerinin sağlaması gereken fonksiyonlar şunlardır;

- *Doğrulama (verifying):* Gelen trafiğin TSpec ile uygunluğunun kontrolü ve uygun olmayan trafiklerin atılması.
- *Kabul kontrolü:* QoS isteklerini karşılamak için yeterli ağ kaynağının bulunup bulunmadığının kontrolü.
- *Sınıflandırma:* Belirli seviyede ortak QoS ihtiyacına sahip olan paketlerin ayrıştırılması ve ortak politikalara tabi tutulması.
- *Kuyruklama ve sıralama:* Paketlerin ne zaman ve hangi sıra ile iletileceğinin belirlenmesi, QoS isteklerine uygun olarak öncelikle atılacak paketlerin belirlenmesi.

6.1.1 Servis Sınıfları

IntServ çalışma grubu tarafından iki servis sınıfı tanımlanmıştır. Bunlar, *garantili servis* ve *kontollü yük* sınıflarıdır. [2][8]

Garantili Servis sınıfı uçtan-uca gecikme ve bandgenişliğinin isteklere uygunluğu için katı sınırlara sahiptir. Gecikme ve bandgenişliği konusunda bu sınırlar trafiğin tepe seviyesi (peak rate), en büyük paket boyu ve geçirebileceği patlamalı trafik miktarı (burst rate, token bucket) parametrelerine göre ayarlanır. TSpec değerleri bu çerçevede ayarlanır. RSpec için garantili serviste en önemli parametre servis hızıdır (service rate). Bu değer trafiğe ilişkin bandgenişliği doğrudan ilişkilidir. Servis hızı parametresi kullanılarak bir ağdaki gecikmenin de hesaplanması mümkün olmaktadır.

Kontrollü Yük sınıfı, gecikme ve bandgenişliği sınırlarını bir kenara bırakarak onun yerine hizmetin yüksüz ve yeterli kapasiteye sahip bir ağda alınabilecek değerler ile kıyaslanabilecek bir seviyede olmasını sağlamaya çalışır. Kontrollü yük kullanan bir uygulama garantili servisteki gibi bir TSpec belirler ve ağ kaynaklarının istenen servis kalitesini karşılayabilecek seviyede olmasını sağlar (kabul kontrolü). Kontrollü yük trafikleri birbirlerinin performansını etkilemeyecek şekilde ayrı kuyruklanır.

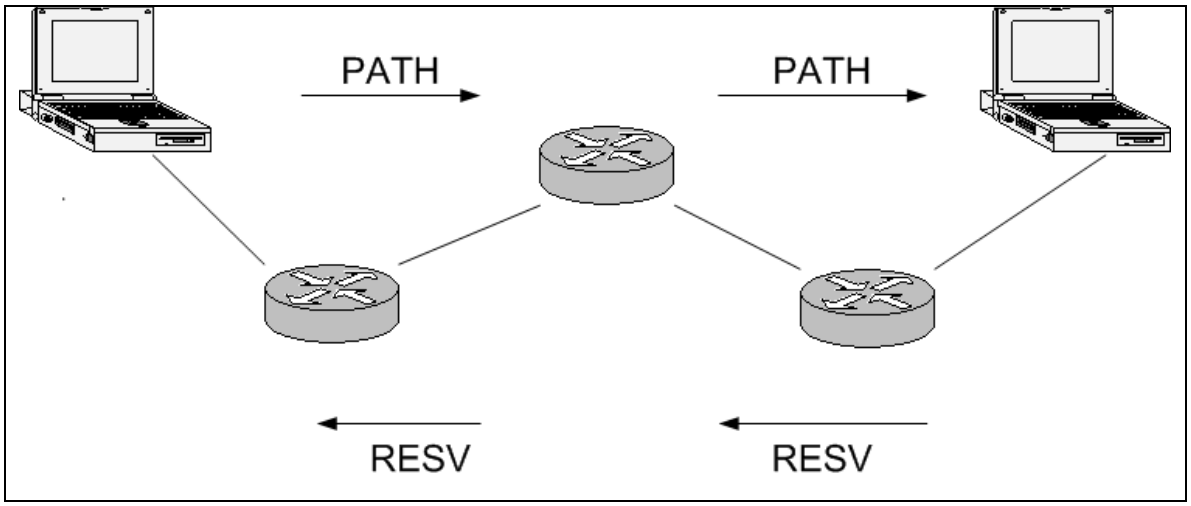
6.1.2 Kaynak Rezervasyon Protokolü - RSVP

RSVP protokolü, uygulamaların QoS ihtiyaçlarını ağa ileten ve ağın kabul ya da red cevaplarını uygulamaya bildiren bir sinyalleşme protokolüdür. RSVP iki tip bilgi taşır;

- *Sınıflandırma bilgisi:* Belirli QoS ihtiyaçları olan uygulama ve trafiklerin ağ tarafından ayrıştırılıp ortak değerlendirilmesi. Bu bilgi genellikle gönderici ve alıcı IP adresleri ve UDP port numaraları bilgilerini taşır.
- *Trafik özellikleri ve QoS ihtiyaçları:* Bu bilgi TSpec ve RSpec değerlerinin yanı sıra istenen servis sınıfı (garantili servis ya da kontrollü yük) bilgisini taşır.

RSVP bu bilgileri istemciden, ağdaki tüm yönlendirici ya da anahtarlara kadar taşır. Böylelikle ağdaki tüm bileşenler uygulamanın QoS ihtiyaçlarından haberdar olur.

RSVP bilgileri iki temel mesaj tipi ile taşınır. Bunlar, *PATH* ve *RESV* mesajlarıdır. PATH mesajı göndericiden bir ya da birkaç alıcıya TSpec ve sınıflandırma bilgilerini içerecek şekilde yollanır. PATH mesajı tek-yayın ya da çoklu-yayın olarak bir oturum adresine yollanır. Alıcı PATH mesajını aldığı zaman göndericiye RESV mesajını döner. RESV mesajı rezervasyonun yapılacağı oturumu belirler ve alıcı tarafından beklenen QoS seviyesini içeren RSpec değerini taşır. Şekil 6.1'de mesajlaşmanın nasıl gerçekleştiği görülmektedir.



Şekil 6.1: RSVP, PATH ve RESV mesajları

Alıcı ile gönderici arasında rezervasyon oturumu kurulduğu anda alıcı ile gönderici arasındaki yönlendiriciler IP ve taşıma katmanı başlığındaki bilgileri kullanarak hangi paketin hangi rezervasyona ait olduğunu tespit ederler. Tespit için kullanılan başlık alanları şunlardır; *hedef IP adresleri, kaynak IP adresleri, hedef port numarası, kaynak port numarası ve protokol numarasıdır* (TCP mi UDP mi). Bu şekilde ayırt edilen

trafiklere *rezerve akış* trafiği adı verilir. Rezerve akış içerisindeki paketler TSpec'te belirlenenden daha fazla trafik yaratmamaları için düzenlenirler (policing). Belirlenen QoS'u sağlamak için kuyruklanır ve sıralanırlar (queueing and scheduling). Bir rezervasyonun aktif durumda tutulabilmesi için PATH ve RESV mesajları periyodik olarak gönderilir ve güncellenirler. [2]

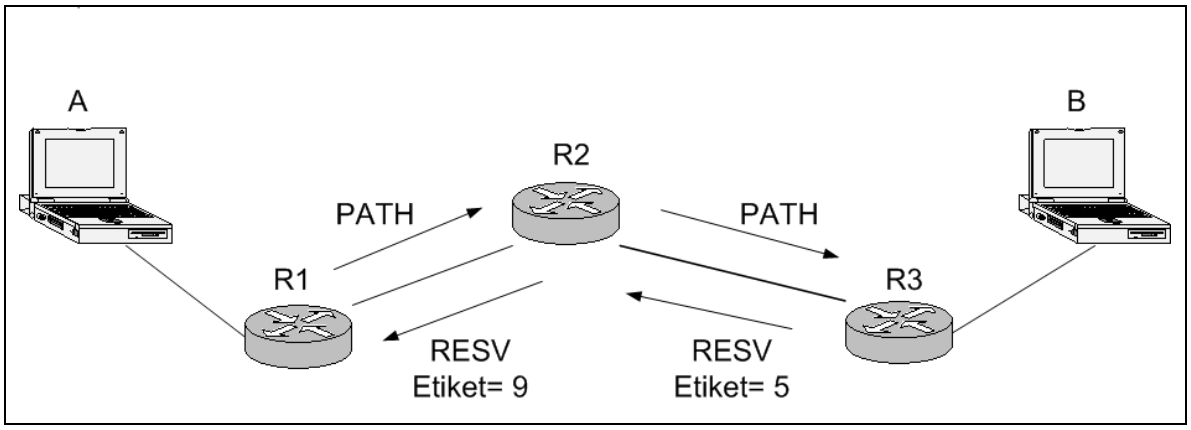
6.1.3 MPLS RSVP Desteği

MPLS'te RSVP desteğini sağlamak için ilk yapılması gereken LSR'ların rezerve akışları, IP ya da 4. katman başlıklarına göre değil etiketlerine göre ayırt etmesini sağlamaktır. Bunun için rezerve akışlar ile etiketler arasında bir eşleme ve etiket bağlama gereklidir. Rezerve akışların her birini ayrı bir FEC gibi düşünmek ve etiket atamalarının buna göre yapılmasını sağlamak bize bu bakışı kazandırır.

Bir LSR bir rezerve akış isteğine ilişkin RESV mesajı göndermek istediğinde etiket havuzundan bu akışa ilişkin bir etiket atar, LFIB tablosunda kayıt yaratır ve geliş etiket bilgisini RSVP nesnesine karşılık yarattığı ETİKET nesnesi içine yerleştirerek bunu RESV mesajı içerisinde gönderir. ETİKET nesnesini içeren bir RESV mesajı alındığında LSR LFIB tablosuna bu değeri çıkış etiketi olarak yerleştirir. Daha sonra bir geliş etiketi atayarak bunu komşu LSR'a bildirir. Böylece LSP boyunca QoS bilgisi ve rezervasyon tanımlanmış olur. Bu aşağı yönlü bir etiket atamadır, aynı zamanda etiket bağlama RSVP mesajları üzerine gerçekleştiği için istek üzerine kontrollü etiket atamadır. Etiket bağlama bilgisi RSVP mesajları ile taşındığı için bu aynı zamanda bir piggybacking örneğidir, etiket dağıtımı için ayrıca bir LDP'ye ihtiyaç yoktur. Şekil 6.2'de RESV mesajları ile etiket dağıtımı yer almaktadır.

A'dan B'ye giden PATH mesajına ilişkin RESV cevabı dönerken R3 yönlendiricisi geliş etiketi olarak 5 değerini ETİKET nesnesi içine yerleştirir ve RESV mesajı içerisinde gönderir. R2 bu etiketi çıkış etiketi olarak LFIB tablosuna alır ve geliş etiketi olarak 9 değerini RESV mesajı içerisinde R1'e iletir. Böylece R1 ile R3 arasında bir LSP oluşur. Bu rezervasyona ilişkin paketler R1'e geldiğinde, R1 parametrelere (varış, kaynak adresleri, varış, kaynak port numaraları ve protokol numarası) denk düşen etiket bilgisi

ile paketi R2'ye gönderir. R2 etiket değişimi yapar, paketi R3'e iletir. R3 paketi alınca etiket bilgisini paketten kaldırır ve iletim gerçekleşir.



Şekil 6.2: RSVP mesajları ile etiket dağıtımı

Bu yapının avantajlarından biri, bir rezervasyona ilişkin LSP kurulurken yalnızca ilk LSR'ın (örnekte R1) hangi paketlerin hangi rezerve akışa ait olduğunu belirlemesidir. Bu özellik sadece IP QoS'taki 5 parametreye göre değil (varış, kaynak adresleri, varış, kaynak port numaraları ve protokol numarası) çok daha geniş bir çerçevede akışların birbirlerinden ayrılabilmesini sağlar. Örneğin belli bir FEC'e giden tüm akışlar için ayrı bir LSP kurmak yerine hepsinin aynı LSP içerisinde taşınması sağlanabilir. MPLS bunun için yeni bir ETİKET nesnesinin PATH mesajları içerisinde taşınabilmesini sağlar. Bu ETİKET_İSTEĞİ nesnesidir. Böylece bu PATH içinde yeni gelen mesaja cevap olarak verilen RESV içinde etiket bilgileri atanır. Ayrıca bu sayede çok sayıda akış için yalnızca bir etiket kullanılması sağlanabilir. [2][8]

6.2 Farklılaştırılmış Servisler (DIFFSERV)

IP QoS mekanizmalarının en gelişmişi ve yaygın kullanılanı olan DiffServ modeli genellikle servis sağlayıcı ağlarında kullanıldığı için MPLS ile olan bu ortaklığı iki teknolojinin beraber kullanılması konusunda avantajlar sağlamaktadır.

IntServ modelinde akış başına kaynakların rezervasyonu söz konusudur. DiffServ modelinde ise trafik alt sınıflara bölünmüştür ve kaynaklar sınıf başına atanmaktadır. DiffServ'de öncelikle tüm paketler *olabildiğince-iyi (best-effort)* sınıfında kabul edilir,

daha sonra bunun üzerinde sınıflar tanımlanarak uygun görülenlerin bu sınıftan daha iyi hizmet alması sağlanır. [8]

DiffServ içerisinde genellikle az sayıda sınıf mevcuttur. Bir paketin ait olduğu sınıf, paketin içerisinde bilgi olarak yer alır. Bu IntServ modelinden farklılık arzeden bir durumdur zira IntServ'de paketler bu bilgiye sahip değildir, kullanılan sinyalleşme protokolü (RSVP) akışların hangilerinin ne tip QoS özelliklerine sahip olacağını belirler. DiffServ'de paketlerin sınıf bilgisi taşındığı alan IP başlığındaki 6 bitlik *Servis Tipi – ToS (Type-of-Service)* alanıdır. Bu kısım sonradan IP paket başlığında *Farklılaştırılmış Servisler Kod Noktası – DSCP (Differentiated Services Code Point)* olarak adlandırılmıştır. DSCP 6 bit olduğu için 64 farklı sınıf tanımlamak mümündür. [8]

6.2.1 Sekme Davranışı (PHB) ve İletim Sınıfları

DSCP kullanılarak *Sekme Davranışı – PHB (Per Hop Behavior)* belirlenir. DSCP'nin değerine göre her bir pakete farklı bir QoS politikası uygulanabilir. Standard sekme davranışı (PHB) 3 ana gruba ayrılabilir:

- *Olabildiğince-İyi – BE (Best Effort):* Özel bir davranış yok, olabildiğince-iyi prensibine uygun olarak paket iletimi gerçekleşir.
- *Hızlandırılmış İletim – EF (Expedited Forwarding):* EF olarak işaretlenen paketler en az gecikme ve kayıp olacak şekilde iletilmelidirler. EF paketleri bunun için ayrı bir EF kuyruğuna alınır ve bu kuyrukta geliş-hızı (arrival rate), servis hızından (service rate) daha düşük olacak şekilde gecikmenin en az olması sağlanır.
- *Güvenli İletim – AF (Assured Forwarding):* AF tipinde birkaç farklı QoS davranışı tanımlamak mümkündür. Paketler AF_{xy} şeklinde adlandırılır. Burada x paketin AF sınıfını, y ise paketin atılma önceliğini (drop presedence) belirler. Örneğin AF_{12} ve AF_{13} aynı sınıftan paketlerdir ancak bir tıkanma ya da kuyruk dolması durumunda öncelikli olarak AF_{13} paketleri atılacaktır. Aynı AF sınıfındaki paketler aynı kuyruğa alınırlar.

DSCP değerinin atanması genellikle ağın giriş yönlendiricisi üzerinde yapılır. Bunun en büyük faydası sınırda DSCP belirlenince, ağdaki sekmeler PHB'lerini DSCP değerine bakarak belirleyecekleri için, istenmeyen trafiğin baştan engellenmesi ya da sınıflandırmanın önceden yapılması ile servis kalitesinin ağın tümünde aynı şekilde uygulanabilmesidir.

6.2.2 MPLS DiffServ Desteği

Bir MPLS omurgasında DiffServ desteğinin sağlanabilmesi için en önemli konu LSR'larda DSCP değerlerinin atanmasının sağlanabilmesidir. DSCP değerleri IP başlığında taşındığı ve LSR'lar da iletim sırasında IP başlığına bakmadıkları için PHB'nin etiket başlığından tespit edilebilmesi gerekir. Bunun yöntemi kullanılan etiketleme ve etiket başlığı taşıma yöntemine göre değişir. Hatırlanacağı üzere MPLS'te etiket bilgileri bir *shim* başlık içinde taşınabileceği gibi ATM gibi bir 2. katman başlığı içerisinde taşınabilir. [1]

Shim başlık içerisinde 3 bitlik deneysel kullanım için ayrılmış bir *EXP* alanı mevcuttur. Bu alanın ayrılmasının temel nedeni MPLS DiffServ desteğinin verilebilmesidir. Normalde DSCP değeri 6 bitlik ancak EXP alanı 3 bitlik olduğu için shim başlık kullanımında maksimum sınıf sayısı 8 olabilmektedir. Bu değer günümüz uygulamaları için yeterlidir. 8'den az sınıfın tanımlı olduğu ağlarda geleneksel IP DiffServ'de olduğu gibi (DSCP ile PHB eşlemesindeki gibi) EXP değerleri ile PHB değerleri eşlenir. Bu durumda EXP alanına gereken değer atandıktan sonra iletim yapılır. Kullanılan LDP (ya da BGP ile) etiket dağıtımı gerçekleşir. EXP değeri etiket başlığı içerisinde yer aldığı için ara LSR'lar paketlerdeki EXP değerlerinden bu paketlere nasıl davranılması gerektiğini, etiket değerlerinden de nereye gönderilmeleri gerektiğini anlarlar. EXP biti kullanılarak oluşturulan bir LSP'ye *E-LSP* adı verilir. [2]

8'den fazla sınıfın tanımlanması gerektiği durumlarda EXP bitleri yeterli gelmediği için ya da ATM gibi 2. katman teknolojileri kullanıldığında bunlarda EXP diye bir alan olmadığı için PHB'nin etiket değerine bakarak tespit edilmesi gerekir. Bu durumda bize yeni bir etiket dağıtım mekanizması gereklidir. Şöyle ki; önceden etiket değerleri FEC bilgisine ilişkin olarak belirlenirken artık hem FEC hem de PHB değerlerine göre etiket

atamak gereklidir. MPLS açısından baktığımızda bu, aynı FEC ve PHB'ye dahil olanların aynı LSP üzerinden taşınması gerektiği anlamına gelir.[2]

Eğer AF kullanılıyorsa PHB'yi sınıfların yanı sıra atılma önceliğine göre de tanımlamak gerekir. Shim başlıkta düşme önceliği değeri EXP bitlerinde taşınırken ATM'de bu CLP (Cell Loss Priority) bitleri ile sağlanır.

8'den fazla sınıf tanımlamak gerektiğinde PHB bilgisinin de etiket alanı içerisinde taşınması gerekir. Bunun için yapılması gereken etiketlerin artık FEC yerine <FEC, PHB> çiftlerine göre atanmasıdır. Bu şekilde oluşturulan LSP'ye *L-LSP* adı verilir. L-LSP'ler çoğunlukla bir PHB'ye ilişkin paketleri taşırlar, EXP ve CLP bitlerinin kullanılmasına gerek kalmaz ancak bir LSP'de aynı AF sınıfından olan paketler taşınacaksa bunların atılma önceliği bilgilerinin EXP ya da CLP bitleri içerisinde taşınması gerekir. [2]

Bir paket MPLS ağına girerken sınır LSR üzerinde ya da daha önceden DSCP değeri atanmış olarak MPLS omurgasına girer. DSCP değerinin atanmış olması demek, PHB'nin önceden belirlenmiş olması demektir. Giriş sınır LSR üzerinde hangi PHB'nin hangi LSP'yi kullanacağı önceden tanımlanmıştır. E-LSP için PHB-EXP eşlemeleri konfigüre edilmiş olmalıdır. L-LSP için etiketler zaten <FEC, PHB> ikilisine göre atandığından EXP ya da CLP alanları yalnızca AF tipinde atılma önceliği ile ilgilidir ve bu eşleme statik olarak yapılır.

6.2.3 E-LSP ile L-LSP'nin Farkları

Tavsiye edilen LSP tipi öncelikli olarak E-LSP'dir çünkü böylece aynı sınıdtan olanlar aynı LSP içerisinde taşındığından LSP sayısı daha az olmaktadır. Bu da kaynakların verimli kullanımı anlamına gelir, bu nedenle mümkün olan yerlerde E-LSP kullanımı tercih edilir. E-LSP kullanmanın mümkün olmadığı ATM gibi yerlerde ya da 8'den fazla sınıfın kullanılması gerektiği durumlarda L-LSP kullanılır.

E-LSP geleneksel IP DiffServ'e daha çok benzemektedir. Çünkü her ikisinde de başlık içerisindeki bir alana bakarak karar verilmektedir. L-LSP'de PHB bazında LSP kurulduğu için trafik mühendisliğine daha uygundur. Örneğin EF trafiği düşük gecikmeli

hattan, AF trafikleri yüksek bandgenişlikli ancak yüksek gecikmeli hattan gitsin şeklinde tanımlama yapılabilir.

Sonuç olarak her iki yöntemin de birbirlerine göre artı ve eksileri mevcuttur. Kullanılan uygulama ve trafik tipine bağlı olarak ağda en uygun çözümü sağlayacak model seçilmelidir. Tablo 6.1'de E-LSP ile L-LSP'nin karşılaştırması yer almaktadır.

Tablo 6.1: E-LSP – L-LSP Karşılaştırması

E-LSP	*L-LSP*
PHB, EXP bitlerinden belirlenir.	*PHB etiket ve EXP/CLP bitlerinden belirlenir.*
Sinyalleşmeye gerek yok.	*PHB, LSP kurulumunda sinyalleşde kullanılır, LSP PHB'ye göre kurulur.*
EXP-PHB eşlemesi konfigüre edilmelidir.	*Etiket-PHB eşlemesi LSP kurulumunda sinyalleşme ile sağlanır, EXP/CLP-PHB eşlemesi statiktir.*
Shim başlık kullanılır.	*Shim başlık ya da ATM başlığı kullanılır.*
LSP başına 8 sınıf tanımlanabilir	*AF dışındakiler için LSP başına 1 PHB, AF için 2-3 PHB.*

6.3 MPLS/VPN QoS Desteği

Bir VPN topolojisinde servis kalitesi uygularken temel amaç çok sayıda VPN müşterisinin desteklenebileceği seviyede bir esneklik ve ölçeklenebilirlik sunabilmektir. Bir VPN müşterisi aynı VPN içerisindeki farklı uygulamaların farklı servis sınıflarına dahil olmasını isteyebilir. Bir uygulamanın bir VPN içerisindeki önceliği ya da servis sınıfı başka bir VPN içerisinde tamamen farklı olabilir dolayısıyla çok geniş bir alanda esneklik sağlanmalıdır. Servis kalitesi ve uygulamaların servis sınıfları tanımları VPN başına yapılmalıdır. [1][8]

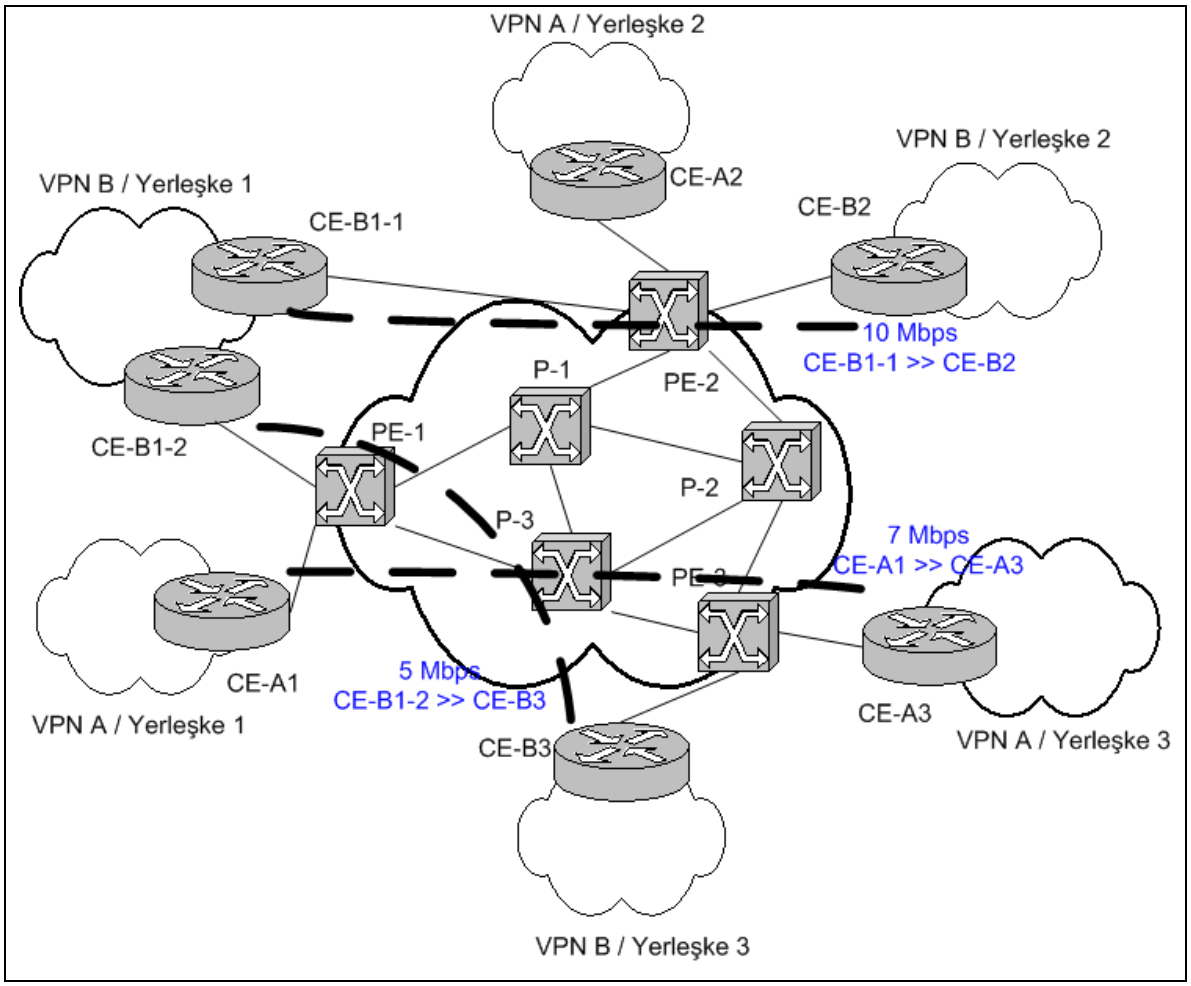
MPLS VPN'de QoS desteği iki farklı model ile verilmektedir. Bunlar, *kapsül (pipe)* ve *debi (hose)* modelleridir. Bu modeller kullanılan QoS modelinin ne olduğuna göre MPLS VPN'de uygulanır. IntServ tercih edilen durumlarda kapsül modeli uygulanırken DiffServ tercih edilen durumlarda debi modeli kullanılır.

6.3.1 Kapsül (Pipe) Modeli

Kapsül modelinde MPLS omurgasına sahip servis sağlayıcı bir müşteri sınır yönlendiricisinden (CE) diğerine bir QoS garantisi verir. Bunu iki CE arasını kapsayan bir kapsül gibi düşünüp yalnızca bu kapsül içerisinde QoS garantisi olduğunu düşünmek mümkündür. Genellikle kapsül modelinde istenen QoS garantisi en küçük bandgenişliği değeridir. Bu iki CE arasında hangi uygulama trafiklerinin QoS garantisi alacağı giriş servis sağlayıcı sınır yönlendiricisinde (PE) belirlenir.

Kapsül modeli uçtan-uca QoS sunduğu için IntServ modelinde tercih edilen yapıdır. Günümüzde Frame-Relay ya da ATM üzerinde verilen IntServ servis garantisine benzemektedir. Yalnız FR ya da ATM'de QoS garantisi çift yönlü verilirken MPLS/VPN'de tek yönlü olarak verilir. Bir yerleşkeden diğerine olan trafik ile dönüş yolundaki trafik her zaman aynı olmayacağı için (asimetrik trafik) tek-yönlü servis kalitesinin verilmesi kaynakların FR ya da ATM'dekine kıyasla daha verimli kullanımı anlamına gelir. Şekil 6.3'te kapsül modeli örneği yer almaktadır.

Şekil 6.3'te görüldüğü üzere aynı VPN içerisindeki çeşitli yerleşkeler ve CE'ler arasında en küçük bandgenişliği garantisi verilerek kapsül modeli gerçeklenmiştir. Örneğin VPN A Yerleşke 1 (CE-A1) ile VPN A Yerleşke 3 (CE-A3) arasında en küçük bandgenişliği olarak 7 Mbps garantisi verilmiştir. Benzer şekilde CE-B1-1 ile CE-B2 arasında 10 Mbps, CE-B1-2 ile CE-B3 arasında 5 Mbps bandgenişliği QoS garantisi olarak belirlenmiştir. Şekilden görüldüğü üzere aynı VPN içerisinde aynı yerleşke üzerinde birden fazla kapsül yer almakta ve farklı QoS garantileri verilebilmektedir (VPN B – Yerleşke 1). Bunların aynı CE üzerinde sonlanması ve aynı hedef yerleşkeye gitmeleri de mümkündür. [2]



Şekil 6.3: MPLS/VPN QoS Kapsül Modeli

Kapsül modeli günümüz FR ve ATM QoS uygulamalarına çok benzediği için kullanıcılar için adaptasyon kolaylığı taşımaktadır. Ancak kapsül modelinde hangi yerleşkeler arasında ne miktarda QoS garantisi isteneceğinin belirlenebilmesi için tüm yerleşkeler arasındaki trafiğin, mümkünse uygulamalar bazında tespit edilebilmesi gerekir. Trafikler çoğu durumda kestirilemez olduklarından kapsül modeli ancak küçük ölçekli ve trafik yapısı bilinen ağlarda uygulanabilmektedir. Dahası aynı IntServ'de olduğu gibi kaynakların belirli yerleşkeler arasında rezervasyonu söz konusu olduğu için kaynakların verimsiz kullanımı da söz konusudur, bu ölçeklenebilirlik problemini de beraberinde getirmektedir.

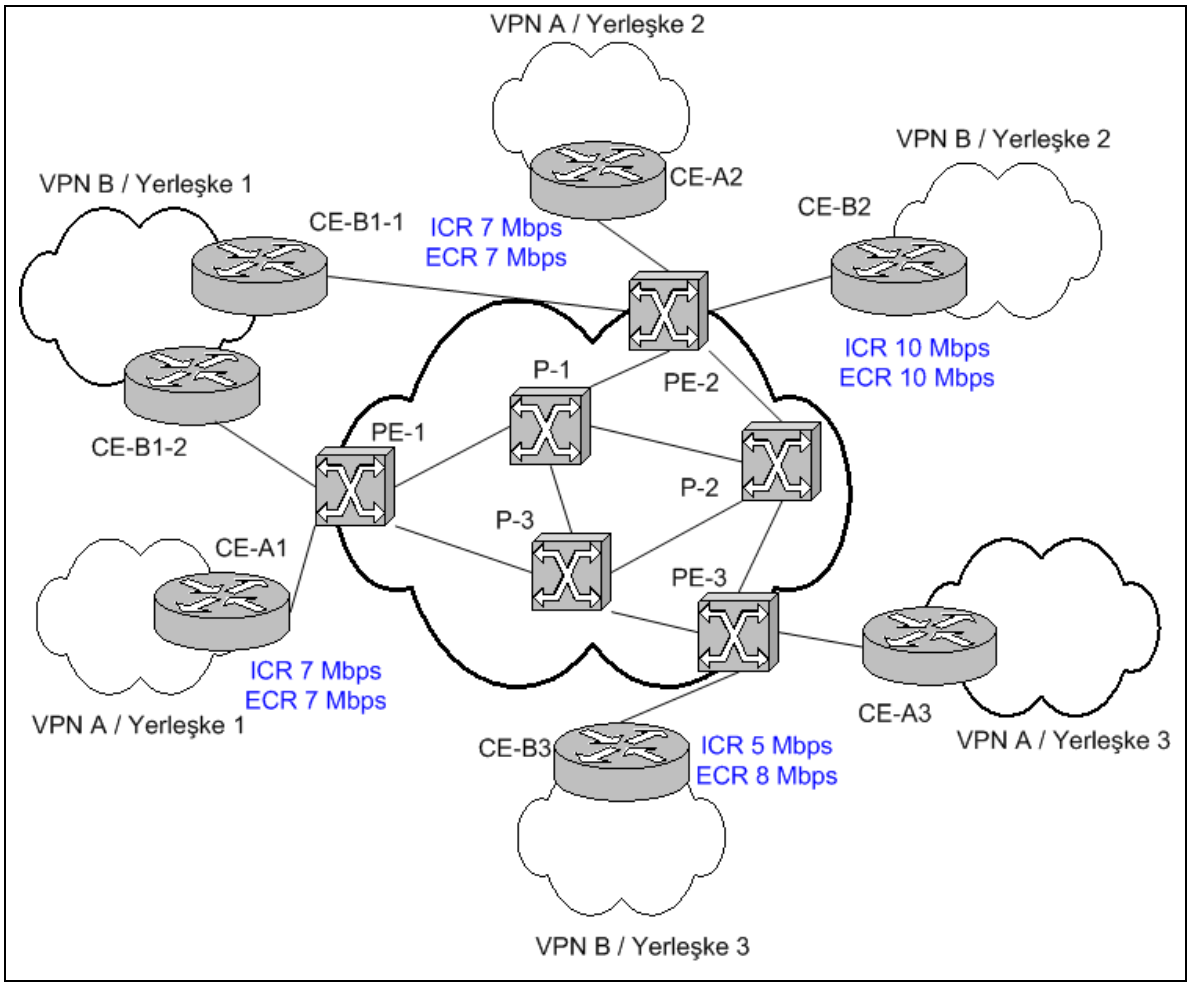
Kapsül modelinde bandgenişliği garanti edilen LSP'ler kurulmaktadır. Bu LSP'ler PE'ler arasında kurulmaktadır. Bu PE'ler arasında her CE çifti için bir kapsül kurulması gerekir. Bu ciddi oranda LSP miktarının artması demektir. Bunu engellemek için farklı CE'ler arasındaki trafiği geçiren iki PE, aynı yolu takip eden tüm kapsüller için aralarında kurdukları tek bir ortak LSP'yi kullanabilirler. Örneğin şekil 6.3'te CE-A3 ile CE-A1 arasındaki kapsül ve CE-B3 ile CE-B1-2 arasındaki kapsül aynı PE çifti üzerinden geçerek (PE-1'den PE-3'e) kurulmaktadır. Böyle bir durumda PE-1 ile PE-3 arasında iki ayrı LSP kurmak yerine garantili bandgenişliği her iki kapsüle verilen garantinin toplamı kadar olan tek bir LSP kurulabilir. Böylece kapsül modelinin ölçeklenebilirlik sorunu azaltılmış olmaktadır. [1]

6.3.2 Debi (Hose) Modeli

Debi modelinde servis sağlayıcı müşterilerinin CE'leri arasında QoS garantisi vermez, bunun yerine herbir CE'nin üzerinden geçebilecek trafik miktarı (bandgenişliği) garanti edilir. Yani herbir CE için geliş yönündeki ve gidiş yönündeki debi garanti edilir. Böylece VPN müşterilerinin yerleşkeleri arasındaki trafiği bilmelerine gerek kalmaz, yalnızca CE'leri üzerinden geçen trafik miktarını belirlemeleri ve buna göre geliş yönlü ve gidiş yönlü debileri için bandgenişliği garantisi istemeleri yeterlidir. Bu bilgi her CE yönlendiricisi üzerinden rahatlıkla alınabilen ve dolayısıyla elde olan bir veridir.

Debi modelinde iki parametre vardır, bunlar *Giriş Trafiği Hızı - ICR (Ingress Committed Rate)* ve *Çıkış Trafiği Hızı – ECR (Eggress Committed Rate)'*tir. Giriş ve çıkış terimleri omurgaya olan durumlarına göre belirlenmiştir. Yani ICR bir CE'den diğerlerine gidebilecek (MPLS omurgasına girebilecek) toplam trafik debisi, ECR ise bu CE'ye gelebilecek (omurgadan çıkan) trafik debisidir. ICR ile ECR'ın eşit olması gibi bir zorunluluk yoktur. Debi modeli, QoS modeli olarak DiffServ tercih edilen durumlarda kullanılır, farklı sınıflar birbirlerinden farklı QoS garantisi alabilirler. CE başına atanan bandgenişliği sınıfların niteliğine göre paylaştırılabilir. EF sınıfına debini büyük kısmı atanırken BE trafikleri için küçük bir kısmı ayrılabilir. [1][2]

Şekil 6.4'te debi modeline ilişkin bir topoloji görülmektedir.



Şekil 6.4: MPLS/VPN QoS Debi Modeli

Şekil 6.4'te görüldüğü üzere, VPN A Yerleşke 2 (CE-A2) için servis sağlayıcı 7 Mbps giriş (ICR), 7 Mbps çıkış (ECR) bandgenişliği garantisi vermiştir. Dikkat edilirse VPN B Yerleşke 3 (CE-B3) için verilen servis garantisinde giriş ve çıkış trafik garanti miktarları farklı olarak verilmiştir. Bu da debi modelin esneklik özelliğinin bir göstergesidir.

Servis sağlayıcıların VPN müşterilerine her durumda bu iki modelden bir tanesini seçenek olarak sunmaları zorunlu değildir. IntServ gereken durumlarda kapsül model uygulanırken aynı VPN içerisinde kullanıcı istekleri doğrultusunda debi modeli ile DiffServ desteği de vermek mümkündür. Gelen trafiğin hangi modele ilişkin olduğuna PE yönlendiricileri karar verir. Bu karar IP kaynak ve hedef adresleri, geliş port adresi, IP önceliği, TCP/UDP port numarası gibi bilgilere göre alınır.

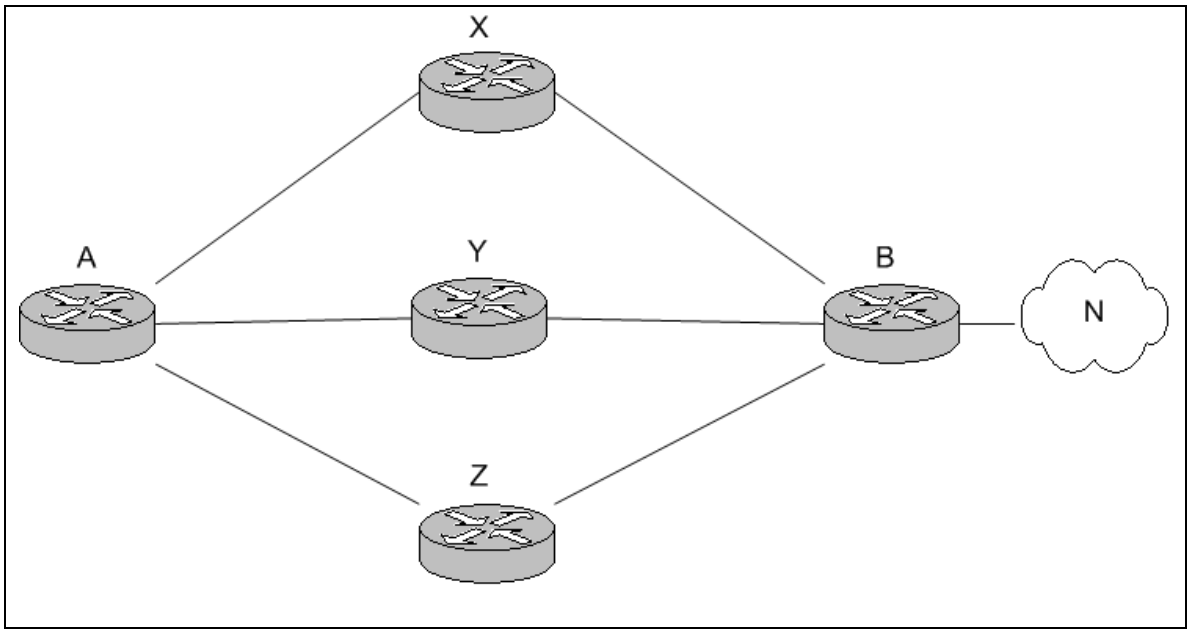
6.4 Trafik Mühendisliği

Bu bölümde çalışmamızın kapsamı içerisinde yer almamakla beraber konunun bütünlüğünün sağlanması için kısaca trafik mühendisliğinden bahsedeceğiz

Günümüzde internet trafiği geometrik bir hızla artmakta, yeni nesil uygulamaların bandgenişliği istekleri, ses ve video uygulamaların da ortaya çıkmasıyla giderek artmaktadır. Bunun yanında servis sağlayıcıların müşteri sayılarının da bandgenişliği ihityacı ile paralel olarak artması, servis sağlayıcıların kaynaklarını olabildiğince etkin kullanmaları gerekliliğini ortaya koymuştur. Bunun için tüm kaynakların kullanım oranını ve meşguliyetini en üst seviyeye çıkaracak bir takım mekanizmalara ihtiyaç duyulmaktadır. Ağdaki bazı hatlar aşırı derecede meşgul ve kapasitelerinin üzerinde yük taşımaya çalışır iken, bazı hatların kapasitelerinin çok altında trafik taşımaları istenmeyen bir durumdur. Bu nedenle trafiklerin uygun şekilde tüm hatlarda yakın yük bulunacak şekilde yük dağıtımı ve yük dengelenmesinin yapılması gereklidir. Bu başlı başına bir trafik mühendisliği işlemidir.

Bilindiği üzere trafik mühendisliğinin ilk adımı olan yük dengeleme IGP protokollerinde konfigürasyon işlemleri ile kolaylıkla gerçeklenmektedir. OSPF ve EIGRP protokolleri en yaygın kullanılan IGP protokolleri olarak eşit maliyetli ve eşit olmayan maliyetli hatlar üzerinde yük dengelemesine izin vermektedirler. [4]

Şekil 6.5'teki gibi bir mantıksal topolojide A'ya bağlı kullanıcılar N ağına gitmek istediklerinde, hiçbir trafik mühendisliği söz konusu değil ise en düşük maliyetli yol (varsayalım A-X-B) seçilecektir. Bu durumda N ağına gitmek üzere A'ya gelen tüm paketler bu yol üzerinden gönderilecektir ve A-Y-B ve A-Z-B yolları kapasitelerinin çok altında az yükle çalışırken A-X-B yolunun aşırı yükle çalışması durumu ortaya çıkacaktır. OSPF ve EIGRP protokolleri bunu engellemek üzere düşük yüklü yolların da kullanılabilmesi için paketlerin diğer yollardan da dengeli bir biçimde gönderilmesini sağlayacak konfigürasyon işlemlerine izin vermektedirler. Bu işlem maliyet metriklerinin manuel olarak değiştirilmesi ile sağlanmaktadır. Buna *metrik manipülasyonu* adı verilir.



Şekil 6.5: Trafik Mühendisliği ile yük dengeleme

Şekil 6.5'teki gibi bir mantıksal topolojide A'ya bağlı kullanıcılar N ağına gitmek istediklerinde, hiçbir trafik mühendisliği söz konusu değil ise en düşük maliyetli yol (varsayalım A-X-B) seçilecektir. Bu durumda N ağına gitmek üzere A'ya gelen tüm paketler bu yol üzerinden gönderilecektir ve A-Y-B ve A-Z-B yolları kapasitelerinin çok altında az yükle çalışırken A-X-B yolunun aşırı yükle çalışması durumu ortaya çıkacaktır. OSPF ve EIGRP protokolleri bunu engellemek üzere düşük yüklü yolların da kullanılabilmesi için paketlerin diğer yollardan da dengeli bir biçimde gönderilmesini sağlayacak konfigürasyon işlemlerine izin vermektedirler. Bu işlem maliyet metriklerinin manuel olarak değiştirilmesi ile sağlanmaktadır. Buna *metrik manipülasyonu* adı verilir.

Metrik manipülasyonu az kullanılan linkleri de kullandırtma konusunda bir çözüm sunmaktadır ancak metriklerin değiştirilmesi bir ağda ölümcül sonuçlara yol açabilir. Yönlendirme tablolarının hatalı olarak değişmesine, bu yolu kullanan başka trafiklerin de alternatif yollara yönelmesine yol açarak yanlış iletimlere de yol açabilir. Dahası bu yöntem yolların birbirini dinamik olarak yedeklemesini de sağlamamaktadır.

MPLS trafik mühendisliği uygulanan ağlarda fazlaca yüklü olan bir LSP dinamik olarak alternatif bir LSP ile değişebilir. Omurgdaki hatların bir noktasında sıkışıklık olduğu anda paketler alternatif yollardan iletilmeye başlanabilir. Bunun için yönlendirme

bilgisinin sınırlı dağıtımı kullanılabilir. Yönlendirme bilgisinin sınırlı dağıtımı konusunu 5.4.1'de ayrıntılı olarak anlatmıştık. Bu yöntem BGP'nin politika tabanlı yönlendirme mekanizmasına dayanmaktadır. Bu yöntem ile bazı FEC'lere ilişkin isteklerin bazı PE'lere ulaşması engellenebilir ya da bazı FEC'lere giden paketlerin adete kaynak yönlendirmede olduğu gibi en baştan hangi yolları izlemesi gerektiği belirlenebilir. Böylece trafikler birbirlerinden ayrıştırılarak aynı hedefe giden farklı uygulama paketlerinin farklı yolları takip etmesi de sağlanabilir. Bu da hatların optimal kullanımını sağlar. [2][4]

Trafik mühendisliği uygulanan ağlar aynı zamanda ağda bir hata oluştuğu zaman buna anında cevap verebilecek ve trafiğin akışı çok fazla etkilenmeden kendisini düzeltebilecek bir yapıda olmalıdır. Bunun için de çeşitli mekanizmalar mevcuttur. *Hızlı yeniden-yönlendirme (Fast-rerouting)* ile 1) hatta az sayıda LSP mevcut ise bunların herbirine ilişkin alternatif yedek birer LSP'nin önceden kurulması sayesinde kopan ya da sıkışıklık oluşan bir hattaki trafiğin anında diğerine aktarılması ile sorun çözülmesi ya da 2) hata oluşan link koruma altına alınarak anında bu hattı by-pass eden yeni bir LSP kurulması ve bu by-pass eden hatta yeni bir etiket atayarak sistemin devamı sağlanabilir. Hızlı yeniden-yönlendirme yöntemi ile ağda optimal olmayan bir yol oluşturulmuş olabilir bu da verimliliği düşürecektir. Diğer bir yöntem ise *optimize yeniden-yönlendirme (optimized-rerouting)* yöntemidir. Bu yöntem ile anında kopan LSP'ye alternatif olarak yeni bir optimal yol hesabı yapılarak gelen trafik bu yeni alternatif yola yönlendirilir. [1]

Detaylarına fazla girmeden anlatmaya çalıştığımız üzere trafik mühendisliği MPLS'in günümüz IP ağlarına getirdiği MPLS/VPN ile birlikte en büyük yeniliklerden biridir. Özellikle servis sağlayıcı omurga ağları gibi hataya duyarlılığın en üst seviyede olduğu ve katı servis kalitesi garantilerinin sunulduğu ağlarda hem IP QoS mekanizmalarının yüksek ölçeklenebilirlik ile etkin kullanımını sağlaması hem de trafik mühendisliği gibi mekanizmalarla hatların verimli kullanımının sağlanması ve paket kaybının en aza indirilmesi MPLS/VPN'in günümüzde giderek artan bir yaygınlıkla tercih edilmesini net olarak açıklamaktadır.

7. ÖRNEK ÇALIŞMA
BİR MPLS/VPN AĞINDA DIFFSERV İLE SERVİS KALİTESİ UYGULAMASI

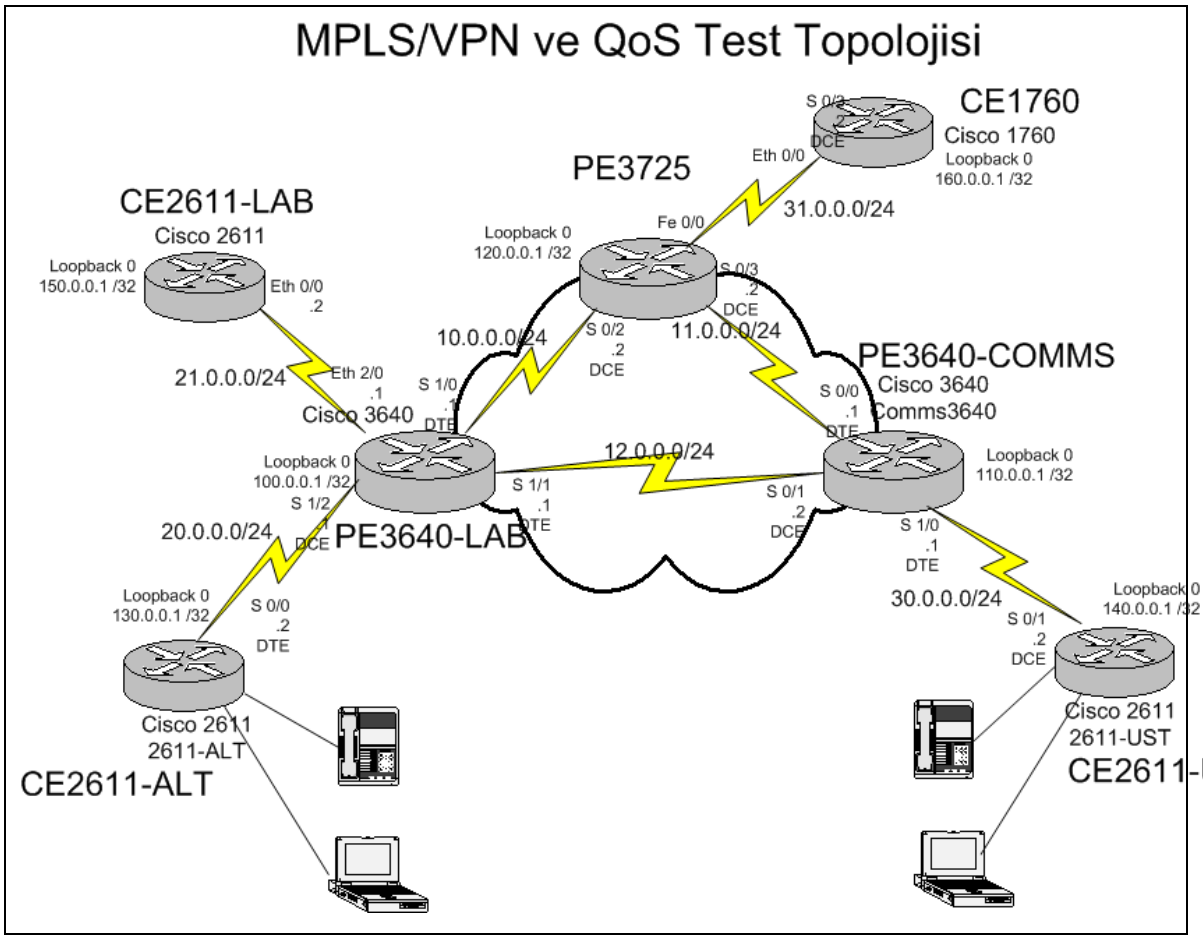
Bu bölümde önceki bölümlerde teorik bilgisi sunulan etiket anahtarlama teknolojisi ve bunun üzerinde uygulanan Sanal Özel Ağ teknikleri ile, farklılaştırılmış servisler (DiffServ) yolu ile farklı trafik sınıflarının ağ üzerinden taşınmasını göstermek üzere pratik bir örnek çalışma sunulmaktadır. Burada sunulmakta olan çalışmanın tam olarak anlaşılabilmesi için MPLS/VPN ve QoS konularında teorik bilginin tamamlanmış olması ve Cisco Systems tarafından üretilen yönlendiricilerin arayüzleri ile konfigürasyon detayları konusunda bir miktar bilgi sahibi olunması gerekmektedir.

Örnek olarak kullanılan ağ topolojisi, tüm adresleme planı Şekil 7.1'de yer almaktadır.

Testlerde Cisco Systems tarafından üretilen MPLS CE ve MPLS PE destekli yönlendiriciler kullanılmıştır. MPLS P destekli yönlendiricilerin hem temini zor olduğu, hem de topolojimizde etiket anahtarlama ve fonksiyonlarını göstermekte ihtiyaç duyulmadığı için bu yönlendiricilere yer verilmemiştir. Yazılım olarak tüm yönlendiricilerin üzerinde MPLS fonksiyonlarını destekleyen Cisco Internetworking Operating System (IOS) versiyonları tercih edilmiştir.

7.1 Yönlendiricilerin Donanım ve Yazılım Profilleri

Testte kullanılan yönlendiriciler, donanım ve yazılım profilleri aşağıda listelenmiştir. Listeleme sırasında Cisco IOS "show version" komutu kullanılmıştır.



Şekil 7.1: MPLS VPN ve QoS Test Topolojisi

7.1.1 PE Yönlendiricileri

PE3640-LAB

```
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-JK9S-M), Version 12.3(6a), RELEASE
SOFTWARE (fc4)
Copyright (c) 1986-2004 by cisco Systems, Inc.

ROM: System Bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT
RELEASE SOFTWARE (fc1)
System image file is "flash:c3640-jk9s-mz.123-6a.bin"

cisco 3640 (R4700) processor (revision 0x00) with 93184K/5120K
bytes of memory.
Processor board ID 26390216
```

```
R4700 CPU at 100MHz, Implementation 33, Rev 1.0
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
2 Ethernet/IEEE 802.3 interface(s)
4 Serial network interface(s)
2 Voice FXS interface(s)
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of non-volatile configuration memory.
24576K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
```

PE3640-COMMS

```
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-JK9S-M), Version 12.2(24), RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2004 by cisco Systems, Inc.

ROM: System Bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT
RELEASE SOFTWARE (fc1)

System image file is "flash:c3640-jk9s-mz.122-24.bin"

cisco 3640 (R4700) processor (revision 0x00) with 125952K/5120K
bytes of memory.
Processor board ID 15171476
R4700 CPU at 100Mhz, Implementation 33, Rev 1.0
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
4 Ethernet/IEEE 802.3 interface(s)
1 FastEthernet/IEEE 802.3 interface(s)
4 Serial network interface(s)
2 Voice FXS interface(s)
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of non-volatile configuration memory.
```

```
32768K bytes of processor board System flash (Read/Write)
16384K bytes of processor board PCMCIA Slot0 flash (Read/Write)
Configuration register is 0x2102
```

PE3725

```
Cisco Internetwork Operating System Software
IOS (tm) 3700 Software (C3725-IPBASE-M), Version 12.3(1a),
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.

ROM: System Bootstrap, Version 12.2(8r)T2, RELEASE SOFTWARE (fc1)

System image file is "flash:c3725-ipbase-mz.123-1a.bin"

cisco 3725 (R7000) processor (revision 0.1) with 250880K/11264K
bytes of memory.
Processor board ID JHY0741K11F
R7000 CPU at 240Mhz, Implementation 39, Rev 3.3, 256KB L2 Cache
Bridging software.
X.25 software, Version 3.0.0.
18 FastEthernet/IEEE 802.3 interface(s)
4 Serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
55K bytes of non-volatile configuration memory.
125184K bytes of ATA System CompactFlash (Read/Write)
Configuration register is 0x2102
```

7.1.2 CE Yönlendiricileri

CE2611-ALT

```
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IK9O3S3-M), Version 12.3(6),
RELEASE SOFTWARE (fc3)
Copyright (c) 1986-2004 by cisco Systems, Inc.

ROM: System Bootstrap, Version 11.3(2)XA3, PLATFORM SPECIFIC
RELEASE SOFTWARE (fc1)
```

```
System image file is "flash:c2600-ik9o3s3-mz.123-6.bin"

cisco 2610 (MPC860) processor (revision 0x202) with 61440K/4096K
bytes of memory.
Processor board ID JAB02380C1W (1340485423)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
2 Low-speed serial(sync/async) network interface(s)
2 Voice FXS interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
```

CE2611-UST

```
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IK9O3S3-M), Version 12.3(6),
RELEASE SOFTWARE (fc3)
Copyright (c) 1986-2004 by cisco Systems, Inc.

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

System image file is "flash:c2600-ik9o3s3-mz.123-6.bin"

cisco 2611 (MPC860) processor (revision 0x203) with 59392K/6144K
bytes of memory.
Processor board ID JAD04350EYO (784666934)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 Ethernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
2 Voice FXS interface(s)
32K bytes of non-volatile configuration memory.
```

```
16384K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
```

CE2611-LAB

```
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-JSX-M), Version 12.2(7a), RELEASE
SOFTWARE (fc2)
Copyright (c) 1986-2002 by cisco Systems, Inc.

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

System image file is "flash:c2600-jsx-mz.122-7a.bin"

cisco 2611 (MPC860) processor (revision 0x203) with 61440K/4096K
bytes of memory.
Processor board ID JAD04510BJA (3249365182)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
2 Ethernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
2 Voice FXS interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
```

CE1760

```
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-SV3Y-M), Version 12.2(15)T2,
RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2003 by cisco Systems, Inc.

ROM: System Bootstrap, Version 12.2(4r)XL, RELEASE SOFTWARE (fc1)

System image file is "flash:c1760-sv3y-mz.122-15.T2.bin"
```

```
cisco 1760 (MPC860P) processor (revision 0x200) with
83190K/15114K bytes of memory.
Processor board ID VMS055200HQ (161277302), with hardware
revision 0000
MPC860P processor: part number 5, mask 2
Bridging software.
X.25 software, Version 3.0.0.
Basic Rate ISDN software, Version 1.1.
1 FastEthernet/IEEE 802.3 interface(s)
2 ISDN Basic Rate interface(s)
4 Voice NT or TE BRI interface(s)
32K bytes of non-volatile configuration memory.
65536K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
```

7.2 Yönlendiricilerin Bağlantı ve Adres Planları

Tablo 7.1'de her bir yönlendiricinin arayüzleri, bu arayüzlerin bağlı olduğu karşı yönlendirici arayüzleri ve adres planları yer almaktadır. Loopback adresleri yönlendirici üzerinde tanımlanan, ve kimlik bilgisi olarak kullanılan daima açık arayüzler oldukları için karşı bağlantıları mevcut değildir.

7.3 Sistemin Çalışması

Şekil 7.1'deki sistemde 3 adet PE yönlendiricisi bir MPLS omurgası oluşturmaktadır. Bu omurgaya 4 farklı uzak noktadan CE yönlendiricisi üzerinden IP ağları bağlanmaktadır. Sistemde CE yönlendiricileri üzerinde sadece RIP konfigürasyon tanımları yapılmakta ve bu CE yönlendiricileri arkasındaki ağdan çıkan tüm trafikler RIP protokolü aracılığıyla ilgili PE yönlendiricisine gönderilmektedir. PE yönlendiricileri kendi aralarında yönlendirme bilgilerini aktarabilmek için OSPF protokolünü kullanmaktadır. Bir MPLS omurgası oluşturabilmek ve etiket bilgilerini birbirleri arasında aktarabilmek için ise BGP protokolü kullanmaktadırlar. CE yönlendiricisinden PE'ye gelen bir paket PE yönlendiricisi üzerinde oluşturulan etiket tabloları yardımıyla gitmek istediği hedef

adrese göre etiketlenmekte ve komşu PE'ye aktarılmaktadır. PE'ler arası komşuluk ilişkileri BGP protokolünün "neighbor" komutu yardımıyla kurulmaktadır. MPLS omurgası üzerinde farklı FEC'lere ilişkin paketlerin taşınabilmesi için, bu FEC'lerin karşılık düştüğü VPN bilgilerine karşılık düşen VRF tanımları yapılmalıdır. VRF tanımları yine BGP konfigürasyon menüsü altında yapılmaktadır. Topolojide iki adet VRF tanımlıdır, bunlar CE2611-ALT ile CE2611-UST arasında PE3640-LAB ve PE3640-COMMS LSR'ları üzerinden kurulan VPN1 ve CE2611-LAB ile CE1760 arasında PE3640-LAB ve PE3725 LSR'ları üzerinden kurulan VPN2'dir. [4][15][16]

Tablo 7.1: MPLS/VPN Test Topolojisindeki Cihazların Adres ve Bağlantı Planları

Yönlendirici	*Arayüz Adı*	*Arayüz IP Adresi*	*Bağlı Olduğu Yönlendirici*	*Bağlı Olduğu Arayüz Adı*	*Bağlı Olduğu IP Adresi*
CE2611-LAB	Eth 0/0	21.0.0.2 /24	PE3640-LAB	Eth 2/0	21.0.0.1 /24
CE2611-LAB	Loopback 0	150.0.0.1 /32	--	--	--
PE3640-LAB	Eth 2/0	21.0.0.1 /24	CE2611-LAB	Eth 0/0	21.0.0.2 /24
PE3640-LAB	Ser 1/0	20.0.0.1 /24	CE2611-ALT	Ser 0/0	20.0.0.2 /24
PE3640-LAB	Ser 1/0	10.0.0.1 /24	PE3725	Ser 0/2	10.0.0.2 /24
PE3640-LAB	Ser 1/1	12.0.0.1 /24	PE3640-COMS	Ser 0/1	12.0.0.2 /24
PE3640-LAB	Loopback 0	100.0.0.1 /32	--	--	--
CE2611-ALT	Ser 0/0	20.0.0.2 /24	PE3640-LAB	Ser 1/0	20.0.0.1 /24
CE2611-ALT	Loopback 0	130.0.0.1 /32	--	--	--
PE3725	FE 0/0	31.0.0.1 /24	CE1760	Eth 0/0	31.0.0.2 /24
PE3725	Ser 0/2	10.0.0.2 /24	PE3640-LAB	Ser 1/0	10.0.0.1 /24
PE3725	Ser 0/3	11.0.0.2 /24	PE3640-COMS	Ser 0/0	11.0.0.1 /24
PE3725	Loopback 0	120.0.0.1 /32	--	--	--
CE1760	Eth 0/0	31.0.0.2 /24	PE3725	FE 0/0	31.0.0.1 /24
CE1760	Loopback 0	160.0.0.1 /32	--	--	--
PE3640-COMS	Ser 0/0	11.0.0.1 /24	PE3725	Ser 0/3	11.0.0.2 /24
PE3640-COMS	Ser 0/1	12.0.0.2 /24	PE3640-LAB	Ser 1/1	12.0.0.1 /24
PE3640-COMS	Ser 1/0	30.0.0.1 /24	CE2611-UST	Ser 0/1	30.0.0.2 /24
PE3640-COMS	Loopback 0	110.0.0.1 /32	--	--	--
CE2611-UST	Ser 0/1	30.0.0.2 /24	PE3640-COMS	Ser 1/0	30.0.0.1 /24
CE2611-UST	Loopback 0	140.0.0.1 /32	--	--	--

Hangi BGP komşularının VPN haberleşmesinde komşu olarak kullanılacağı tanımlanmaktadır. Sistem üzerindeki tüm yönlendiriciler doğru olarak konfigüre edildiği takdirde 7.3.1 ve 7.3.2'de görülen komut çıktıları elde edilmektedir.

MPLS temel tanımları ve VRF bağlantıları sayesinde iki ayrı ağda yer alan ve aralarında komşuluk ilişkisi bulunmayan iki CE yönlendiricisi birbirleriyle bir VPN tüneli üzerinden doğrudan haberleşebilmekte hatta birbirlerinin yönlendirme güncellemelerini alabilmektedir (bkz. 7.3.2). Sistemde ayrıca VPN üzerinden haberleşebilen CE'lerden çıkan trafikler için servis kalitesi tanımları yapılmaktadır. Servis kalitesi yöntemi olarak Farklılaştırılmış Servisler (DiffServ) kullanılmaktadır. Sistemde GOLD, SILVER ve default olmak üzere üç tip servis sınıfı tanımlanmakta, tanımlanan sınıf sayısı 8'in altında olduğu için (Bölüm 6'da açıklanmıştı), IP paketlerinin içerisinde yer alan DSCP değerlerine karşılık MPLS shim etiket başlıklarındaki EXP alanları kullanılmaktadır. Örnek olarak VPN1 üzerinde gerçekleşen ses haberleşmesinde, ses paketleri CE yönlendiricisinde erişim listeleri yardımıyla GOLD sınıfına alınmakta, bu IP paketi PE'ye gönderildiğinde bu pakete atanan etiket başlığında ilgili MPLS EXP biti çekilerek omurgada bu paketin GOLD sınıfında taşınması sağlanmaktadır. Benzer olarak FTP trafiği SILVER sınıfına alınmış ve geri kalan trafik ise default sınıfında olabildiğince-iyi (best-effort) prensibiyle taşınmıştır (detayları için bkz. 7.5).

Sistemin çalışmasına ilişkin önemli bilgiler yönlendiriciler üzerinde tutulan çeşitli tablolar ve komut çıktıları ile elde edilmektedir. Topolojide yer alan LSR'ların çalışma prensipleri ve konfigürasyonları (tüm konfigürasyonlar için bkz. Ek-A) benzer olduğu için 7.3.1 ve 7.3.2'de birer PE ve CE yönlendiricilerinin üzerinde yer alan çeşitli tablo ve iletim bilgilerinin örnekleri verilmektedir. PE yönlendiricisi olarak örnek amacıyla PE3640-LAB seçilmiştir. CE yönlendiricisine örnek olarak da CE2611-ALT kullanılmaktadır.

PE yönlendiricisine ilişkin aşağıdaki komutların çıktıları verilmektedir: [15][16]

- Show ip route
- Show tag-switching interfaces
- Show tag-switching forwarding-table
- Show tag-switching tdp bindings
- Show ip route vrf <vrf_adı>

CE yönlendiricisinde ise MPLS'e ilişkin bilgi olmadığından yalnızca aşağıdaki komut kullanılarak IP yönlendirme tablosuna bakılmaktadır.

- Show ip route

7.3.1 PE Yönlendiricisi Komut Çıktıları

- **Show ip route**

Görüldüğü üzere bu komutun çıktısında yalnızca OSPF ile öğrenilen MPLS ağı içerisindeki dahili ağ bilgileri yer almaktadır. 10, 11 ve 12 ağları PE yönlendirileri arasındaki ağ bağlantılarıdır. 100, 110 ve 120 ağları ise aynı zamanda LSR ID'lerini de oluşturan loopback arayüzlerinin adresleridir.

```
CE3640-LAB#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     100.0.0.0/32 is subnetted, 1 subnets
C       100.0.0.1 is directly connected, Loopback0
     110.0.0.0/32 is subnetted, 1 subnets
O       110.0.0.1 [110/65] via 12.0.0.2, 5d02h, Serial1/1
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Serial1/0
     11.0.0.0/24 is subnetted, 1 subnets
O       11.0.0.0 [110/128] via 10.0.0.2, 5d02h, Serial1/0
                 [110/128] via 12.0.0.2, 5d02h, Serial1/1
     12.0.0.0/24 is subnetted, 1 subnets
C       12.0.0.0 is directly connected, Serial1/1
     120.0.0.0/32 is subnetted, 1 subnets
O       120.0.0.1 [110/65] via 10.0.0.2, 5d02h, Serial1/0
```

- **Show tag-switching interfaces**

Bu komutla hangi arayüzlerde MPLS çalıştığı görülmektedir.

```
PE3640-LAB#sh tag-switching interface
Interface              IP            Tunnel   Operational
Serial1/0              Yes (tdp)     No       Yes
Serial1/1              Yes (tdp)     No       Yes
```

- **Show tag-switching forwarding-table**

Bu komutla etiketleme yapılan ağlara ilişkin iletim tablosu görülmektedir.

```
PE3640-LAB#sh tag-switching forwarding-table
Local  Outgoing    Prefix            Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
16     Pop tag     11.0.0.0/24       0          Se1/1       point2point
17     Pop tag     110.0.0.1/32      0          Se1/1       point2point
18     Untagged    120.0.0.1/32      0          Se1/0       point2point
23     Aggregate   21.0.0.0/24[V]    0
24     Untagged    150.0.0.0/16[V]   0          Et2/0       21.0.0.2
25     Aggregate   20.0.0.0/24[V]    2080
26     Untagged    130.0.0.0/16[V]   0          Se1/2       point2point
```

- **Show tag-switching tdp bindings**

Bu komutla etiket bağlama bilgisi görülmektedir.

```
PE3640-LAB#sh tag-switching tdp bin
  tib entry: 10.0.0.0/24, rev 5
        local binding:  tag: imp-null
        remote binding: tsr: 110.0.0.1:0, tag: 16
  tib entry: 11.0.0.0/24, rev 8
        local binding:  tag: 16
        remote binding: tsr: 110.0.0.1:0, tag: imp-null
  tib entry: 12.0.0.0/24, rev 6
        local binding:  tag: imp-null
        remote binding: tsr: 110.0.0.1:0, tag: imp-null
  tib entry: 100.0.0.1/32, rev 4
        local binding:  tag: imp-null
        remote binding: tsr: 110.0.0.1:0, tag: 19
  tib entry: 110.0.0.1/32, rev 10
        local binding:  tag: 17
        remote binding: tsr: 110.0.0.1:0, tag: imp-null
  tib entry: 120.0.0.1/32, rev 12
        local binding:  tag: 18
        remote binding: tsr: 110.0.0.1:0, tag: 20
```

- **Show ip route vrf <vrf_adı>**

Bu komutla VRF'lere ilişkin yönlendirme tabloları görüntülenmektedir. Örneğin aşağıdaki tabloda VPN1'e ilişkin yönlendirme bilgileri yer almaktadır. Görüldüğü üzere, VRF üzerinden yönlendirme bilgisi BGP ile taşınmaktadır. 140 numaralı ağ VRF'in diğer ucundaki CE2611-UST yönlendiricisinin loopback adresi, 30 numaralı ağ ise CE2611-UST ile PE3640-COMMS arasındaki BGP ile öğrenilen ağdır.

```
PE3640-LAB#sh ip ro vrf vpn1

Routing Table: vpn1
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

B    140.0.0.0/16 [200/1] via 110.0.0.1, 4d02h
     20.0.0.0/24 is subnetted, 1 subnets
C       20.0.0.0 is directly connected, Serial1/2
R    130.0.0.0/16 [120/1] via 20.0.0.2, 00:00:09, Serial1/2
     30.0.0.0/24 is subnetted, 1 subnets
B       30.0.0.0 [200/0] via 110.0.0.1, 4d02h
```

7.3.2 CE Yönlendiricisi Komut Çıktıları

- **Show ip route**

Bu komutla bu yönlendiricinin öğrendiği yönlendirme bilgileri görülmektedir. Görüldüğü üzere bu yönlendirici üzerinde yalnızca RIP konfigürasyonu yapılarak komşu ağlar duyurulmasına karşın VRF içerisinden de RIP ile yönlendirme bilgisi alınmaktadır.

```
    CE2611-ALT#sh ip route
    Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
           D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
           E1 - OSPF external type 1, E2 - OSPF external type 2
           i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1,

    Gateway of last resort is not set

    R    140.0.0.0/16 [120/1] via 20.0.0.1, 00:00:00, Serial0/0
         20.0.0.0/24 is subnetted, 1 subnets
    C       20.0.0.0 is directly connected, Serial0/0
         130.0.0.0/32 is subnetted, 1 subnets
    C       130.0.0.1 is directly connected, Loopback0
         30.0.0.0/24 is subnetted, 1 subnets
    R       30.0.0.0 [120/1] via 20.0.0.1, 00:00:00, Serial0/0
```

7.4 MPLS/VPN Konfigürasyonları

Şekil 7.1'de görülen topolojiye ilişkin tüm MPLS/VPN konfigürasyonları EK-A'da görülebilir. Tüm PE yönlendiricileri ile tüm CE yönlendiricilerinde konfigürasyon mantığı benzer olduğu için burada seçilen bir PE ve bir CE üzerinde konfigürasyon

aşamaları tanıtılacaktır. Örnek PE olarak PE3640-COMMS, örnek CE olarak ise CE2611-UST yönlendiricileri seçilmiştir.

7.4.1 Örnek PE Konfigürasyonu

Örnek olarak seçilen PE3640-COMMS yönlendiricisi üzerinde yapılan önemli konfigürasyonlar şu şekildedir: [4][15][16]

- Öncelikle tüm arayüz bağlantılarına ilişkin IP adreslerinin atanması gerekir. Özellikle seri arayüzlerde saat sinyalini üreten DCE (Data Communications Equipment) uçlarında "clock rate" komutu ile iletişim hızının atanması önemlidir. MPLS omurgasına bağlanan arayüzlerde "tag-switching ip" komutu ile MPLS aktive edilmelidir. Benzer şekilde VRF haberleşmesi yapacak CE bağlantı arayüzünde de hangi VRF'e ilişkin veri iletilecekse ona göre "ip vrf forwarding" komutu ile iletim belirtilmelidir.

```
interface Loopback0
 ip address 110.0.0.1 255.255.255.255
!
interface Serial0/0
 ip address 11.0.0.1 255.255.255.0
 tag-switching ip
 no fair-queue
!
interface Serial0/1
 ip address 12.0.0.2 255.255.255.0
 tag-switching ip
 no fair-queue
 clockrate 1000000
!
interface Serial1/0
 ip vrf forwarding vpn1
 ip address 30.0.0.1 255.255.255.0
```

- MPLS haberleşmesi yapacak tüm yönlendiriciler üzerinde "ip cef" komutu ile Cisco Express Forwarding (CEF) özelliği açılmalıdır.

```
ip cef
```

- Bu PE üzerinden geçecek tüm VPN bağlantıları için birer VRF yaratılmalıdır. "ip vrf" komutu ile bu yapılırken, VPN-IP adresleri için kullanılacak rota ayrıştırıcı tanımları yapılmalıdır. Bunun için "rd <rota_ayrıştırıcı>" komutu kullanılır.

Ayrıca MP-BGP'de giriş/çıkış (import/export) trafikleri için hangi rota ayrıştırıcının kullanılacağı belirtilmelidir.

```
ip vrf vpn1
 rd 1:100
 route-target export 1:100
 route-target import 1:100
```

- PE'ler arasında kullanılacak dahili yönlendirme protokolü tanımları yapılmalıdır. Örneğimizde OSPF protokolü kullanılmaktadır.

```
router ospf 1
 log-adjacency-changes
 network 11.0.0.1 0.0.0.0 area 0
 network 12.0.0.2 0.0.0.0 area 0
 network 110.0.0.1 0.0.0.0 area 0
```

- PE-CE arasında kullanılan bir dahili yönlendirme protokolü varsa ona ilişkin tanımlar yapılmalıdır. Örneğimizde PE-CE arasında RIP protokolü kullanılmaktadır. Eğer bu RIP protokolü içerisinden VPN haberleşmesi yapılacaksa, bu VPN'e ilişkin VRF tanımı burada belirtilmelidir.

```
router rip
 version 2
 !
 address-family ipv4 vrf vpn1
 version 2
 redistribute bgp 1 metric 0
 network 30.0.0.0
 no auto-summary
 exit-address-family
```

- MP-BGP çalışabilmesi için BGP komşuları belirtilmelidir.

```
router bgp 1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 100.0.0.1 remote-as 1
 neighbor 100.0.0.1 update-source Loopback0
 neighbor 120.0.0.1 remote-as 1
 neighbor 120.0.0.1 update-source Loopback0
```

- Var olan herbir VPN için BGP altında bir address-family tanımı yapılmalı, bu adress-family içerisinde MP-BGP komşuluğu kuracaklar belirlenmelidir. Eğer omurga içerisine duyurulması istenen bir yönlendirme güncellemesi bilgi kaynağı varsa burada "redistribute" komutu ile ağa dağıtılmalıdır. Adres ailesi vpnv4

altında komşular aktive edilmeli ve aidiyet (community) değerlerinin aktarımı sağlanmalıdır.

```
router bgp 1
!
 address-family ipv4 vrf vpn1
 redistribute connected
 redistribute static
 redistribute rip
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 100.0.0.1 activate
 neighbor 100.0.0.1 send-community extended
 neighbor 120.0.0.1 activate
 neighbor 120.0.0.1 send-community extended
 exit-address-family
```

Bunların dışında opsiyonel birtakım konfigürasyonlar da yapılabilir. Detaylı konfigürasyonlar için EK-A kısmına bakınız.

7.4.2 Örnek CE Konfigürasyonu

Örnek olarak seçilen CE2611-UST yönlendiricisi üzerinde yapılan önemli konfigürasyonlar şu şekildedir:

- Öncelikle tüm arayüz bağlantılarına ilişkin IP adreslerinin atanması gerekir. Özellikle seri arayüzlerde saat sinyalini üreten DCE uçlarında "clock rate" komutu ile iletişim hızının atanması önemlidir.

```
interface Loopback0
 ip address 140.0.0.1 255.255.255.255
!
interface Serial0/0
 ip address 30.0.0.2 255.255.255.0
 clockrate 128000
```

- PE ile CE arasındaki haberleşmeyi sağlayacak statik yönlendirme ya da dahili bir yönlendirme protokolü tanımı varsa (burada RIP kullanılmaktadır), ona ilişkin tanımlar yapılmalı karşı tarafa duyurulacak ağlar belirtilmelidir.

```
router rip
 version 2
 network 30.0.0.0
 network 140.0.0.0
```

Görüldüğü gibi CE yönlendiricileri MPLS çalışan yönlendiriciler olmadığı için üzerlerinde herhangi bir detaylı konfigürasyon yer almamaktadır. QoS konfigürasyonu 7.5'te anlatılmaktadır. Tüm MPLS/VPN konfigürasyonları için EK-A'ya bakınız.

7.5 DiffServ ile QoS ve Test Amaçlı Ses Konfigürasyonları

Tez kapsamında yapılan bu çalışmamızda üç ayrı servis sınıfı tanımı kullanılmaktadır. Servis sınıfları ses için kullanılan "GOLD", öncelikli veri haberleşmesi için kullanılan "SILVER" ve geri kalan trafikler için kullanılan "default" sınıflarıdır. Default sınıfı paketlerde herhangi bir servis tanımı yapılmamakta "olabildiğince-iyi (best-effort)" prensibi benimsenmektedir. [13][14]

Testler VPN1 üzerinde gerçekleştirilmektedir. Bunun için VPN1 üzerinden haberleşen CE2611-ALT ve CE2611-UST yönlendiricileri üzerinde IP üzerinden ses (VoIP) tanımları yapılmalıdır. Öncelikli veri trafiği olarak FTP trafiği benimsenmiştir. Bu trafik yönlendiricilere Ethernet arayüzünden doğrudan bağlı dizüstü bilgisayarlar arasında uygulama katmanı seviyesinde yaratıldığı için yönlendiriciler üzerinde yalnızca bu trafiğin tanınabilmesi için ilgili porta (20/21) ilişkin bir erişim listesi tanımı yapılarak bu portu kullanan trafiğin sınıfa atanması yeterlidir.

VoIP için kullanılması gereken konfigürasyon tanımı oldukça kolaydır. Zira her iki yönlendiricinin analog telefon için arama tonu sağlayan FXS analog haberleşme portlarına birer analog telefon bağlandıktan sonra aşağıdaki konfigürasyonlar yapılmalıdır. Görüldüğü üzere her iki yönlendirici birbirlerine doğrudan bağlı olmamalarına rağmen VoIP için eş durumuna gelebilmektedirler.

CE2611-ALT

```
dial-peer voice 1 voip
 destination-pattern 100
 session target ipv4:30.0.0.2
!
dial-peer voice 2 pots
 destination-pattern 200
 port 1/0/0
```

CE2611-UST

```
 dial-peer voice 2 voip
 destination-pattern 200
 session target ipv4:20.0.0.2
```

```
!
dial-peer voice 1 pots
 destination-pattern 100
 port 1/0/0
```

Bu konfigürasyonlar tamamlandıktan sonra CE2611-ALT yönlendiricisinin FXS 1/0/0 analog ses portuna bağlı analog telefon 100 dahili numarasını almakta, CE2611-UST yönlendiricisinin FXS 1/0/0 analog ses portuna bağlı telefon 200 dahili numarasını almaktadır. İki telefon birbirlerini doğrudan dahili numaralarını çevirerek, PE3640-LAB ile PE3640-COMMS yönlendiricileri arasında kurulan MPLS VPN tüneli VPN1 üzerinden VoIP teknolojisini kullanarak arayabilmektedir. Bu özellik ses operatörlerinde, veri şebekeleri üzerinden sesi ücretsiz taşıyarak müşterilerine telekom PSTN tarifelerine göre daha düşük ücretlendirmeyle ses hizmeti vermede yaygın olarak kullanılmaktadır. Benzer şekilde WAN üzerinden ofislerini birbirine bağlayan şirketler sahip oldukları FR, ADSL ya da kiralık hatları kullanarak veri hattından bu mantıkla analog sesi ücretsiz taşıyabilmektedirler.

Ses için gerekli tanımların ardından test ağımızdaki son önemli konfigürasyon detayı servis kalitesi (QoS) konfigürasyonlarının yapılmasıdır. Tezimizin QoS ile ilgili kısımlarında anlattığımız üzere bir MPLS omurgasında DiffServ desteğinin sağlanabilmesi için LSR'larda DSCP değerlerinin atanması gereklidir. DSCP değerleri IP başlığında taşındığı ve LSR'lar da iletim sırasında IP başlığına bakmadıkları için bu tanımın etiket başlığında yapılması gerekir. Bunun yöntemi kullanılan etiketleme ve etiket başlığı taşıma yöntemine göre değişir. Hatırlanacağı üzere çerçeve-mod MPLS'te etiket bilgileri bir shim başlık içinde taşınmakta ve bu shim başlık içerisinde 3 bitlik deneysel kullanım için ayrılmış bir *EXP* alanı yer almaktadır. Bu alanın ayrılmasının temel nedeni MPLS DiffServ desteğinin verilebilmesidir. Normalde DSCP değeri 6 bitlik ancak EXP alanı 3 bitlik olduğu için shim başlık kullanımında maksimum sınıf sayısı 8 olabilmektedir. Çalışmamızda 3 adet servis sınıfı tanımı kullanıldığı için EXP değerlerinin kullanımı uygun görülmüştür.

Yapılması gereken paketler kaynakta oluşturulduktan sonra CE'ler üzerinden MPLS şebekesine girerken gelen trafiğin tipine göre önce IP tabanlı servis sınıfı tanımı yapmak ve IP QoS konfigürasyonları gereği IP başlığının içerisindeki DSCP değerinin sınıfa göre

farklılaştırılarak gönderilmesi ve bu değerin MPLS şebekesine girerken PE üzerinde MPLS EXP değerine göre değiştirilmesidir. Yani DSCP değeri "ip precendence" komutu kullanılarak "1" olarak gönderilen bir paket, etiketli olarak taşınırken, EXP değeri 1 olacak şekilde taşınmalıdır. Bu değerin bire bir aynı olması gerekmez zira servis sağlayıcı müşteri ağından öncelikli olarak gelen bir paketi kendi ağında daha düşük öncelikli ya da farklı bir sınıfta taşımak isteyebilir. Bunun için öncelikle yönlendiriciler üzerinde "sınıflar (class)" tanımlanmalıdır. Daha sonra bu sınıfların içinde yer alacağı "politika (policy)" tanımları yapılmalı, bu politikalar içerisinde sınıflara giren paketlere ne tip politikalar uygulanacağı belirtilmelidir. Buradaki örneğimizde sınıflara ilişkin bandgenişliği yüzdesi tanımı yapılmıştır. [13][14]

PE yönlendiricileri üzerinde sınıfların tanımlanması için "class-map" komutu kullanılır. Bu komut altında hangi kriterlere göre gelen paketlerin bu sınıfa dahil kabul edileceği belirtilir. Aşağıda "match mpls experimental <ip_precendence_değeri>" komutu kullanılmış, gelen paketin IP precedence değerine bakarak sınıfların ayrıştırılması sağlanmıştır. Her iki PE üzerinde tanımlar aynı olduğu için örneklemelerde PE'lerden bir tanesi kullanılmaktadır. Default class için class tanımı yapmaya gerek yoktur, politika tanımları altında herhangi bir tanımlı sınıfa girmeyen paketlere nasıl davranılacağı ayrıca belirtilebilir.

```
PE3640-LAB (config)# class-map GOLD
PE3640-LAB (config-cmap)# match mpls experimental 5
PE3640-LAB (config-cmap)# exit

PE3640-LAB (config)# class-map SILVER
PE3640-LAB (config-cmap)# match mpls experimental 3
PE3640-LAB (config-cmap)# exit
```

Görüldüğü gibi burada CE üzerinden gelen bir paket ses paketi ise, ip precedence değeri 5 olarak gönderilmekte ve PE yönlendiricisi bunun bir GOLD sınıfı paketi olduğunu anlamaktadır, 3 olarak geldiğinde SILVER, diğer değerlerle ya da atanmaksızın geldiğinde default sınıfa girdiği anlaşılmaktadır. Şimdi yapılması gereken bu tip bir paket için ne tip bir politika uygulanacağını belirlemektir. Gelen paketin MPLS EXP değeri etiketli olarak gönderildiğinde diğer LSR'ların bunun sınıfını anlayabilmesi için IP DSCP değerine uygun olarak "set mpls experimental <MPLS_EXP_değeri>" komutu kullanılarak atanmalıdır. Sınıf politikası olarak "bandwidth percent" komutuyla

kullanılabilir maksimum bandgenişliği ataması yapılmıştır. GOLD trafiği yüzde 50 bandgenişliği kullanırken, SILVER yüzde 30 kullanabilmektedir.

```
PE3640-LAB (config)# policy-map POLITIKA

PE3640-LAB (config-pmap)# class GOLD
PE3640-LAB (config-pmap-c)# set mpls experimental 5
PE3640-LAB (config-pmap-c)# bandwidth percent 50
PE3640-LAB (config-pmap-c)# exit

PE3640-LAB (config-pmap)# class SILVER
PE3640-LAB (config-pmap-c)# set mpls experimental 3
PE3640-LAB (config-pmap-c)# bandwidth percent 30
PE3640-LAB (config-pmap-c)# exit

PE3640-LAB (config-pmap)# class class-default
PE3640-LAB (config-pmap-c)# exit
```

PE üzerinde son olarak hangi arayüzden gelen trafiklere bu trafik politikasının uygulanacağını göstermektir, bunun için ilgili arayüzün altına "service-policy" komutu ile bu tanımı girmek gerekir. PE3640-LAB yönlendiricisine, diğer PE'ler ile bağlantısının olduğu Serial 1/0 ve 1/1 arayüzlerinin altında çıkış yönünde bu tanım yapılmalıdır.

```
PE3640-LAB (config)# interface Serial 1/0
PE3640-LAB (config-if)# service-policy output POLITIKA

PE3640-LAB (config)# interface Serial 1/1
PE3640-LAB (config-if)# service-policy output POLITIKA
```

PE üzerinde yapılan tanımlar çalışmamızda bununla sınırlıdır. İstendiği takdirde daha fazla servis sınıfı tanımlayarak, farklı politikalar da gelen paketlerin MPLS şebekesine girişinde uygulanabilir.

CE tarafında yapılması gereken yalnızca trafiğin tipine göre paketler gönderilmeden önce "ip precedence" değerlerinin atanmasıdır. Bunun için paketlerin ayrıştırılmasında erişim listelerinden faydalanılır. Yine servis politikası belirlenecek ve altındaki sınıflara göre "class-map" tanımları yapılacaktır. CE2611-ALT üzerinde yapılması gereken örnek konfigürasyonlar aşağıdaki gibidir.[13][14]

```
CE2611-ALT (config)# policy-map POLITIKA

CE2611-ALT (config-pmap)# class GOLD
CE2611-ALT (config-pmap-c)# set ip precedence 5
CE2611-ALT (config-pmap-c)# exit
```

```
CE2611-ALT (config-pmap)# class SILVER
CE2611-ALT (config-pmap-c)# set ip precedence 3
CE2611-ALT (config-pmap-c)# exit

CE2611-ALT (config-pmap)# class class-default
CE2611-ALT (config-pmap-c)# exit
```

Peki, hangi paketin hangi sınıfa dahil olduğu nasıl anlaşılacak, bunun için erişim listeleri (access-list) kullanılmaktadır. Örneğin SILVER sınıfına tanımımız gereği FTP trafikleri girmektedir. FTP trafiği 20 ve 21 numaralı portları kullanmaktadır. O halde 20 ya da 21 numaralı porta ilişkin bir erişim listesi tanımlar ve sınıfımızın bu erişim listesine giren tüm paketleri kapsamasını sağlarız. Örneğin FTP trafiğine ilişkin erişim listesi 102 olsun, bu durumda,

```
CE2611-ALT (config)# access-list 102 permit tcp any any eq 21
CE2611-ALT (config)# access-list 102 permit tcp any any eq 20
```

şeklinde bir tanımla bu trafiği belirleyebiliriz. Burada any any olarak verilenler kaynak ve hedef adresleridir, dolayısıyla burada özel olarak kaynek ve hedef IP adreslerini de belirtip yalnızca bu adresler arasındaki FTP trafiğinin SILVER sınıfına dahil olmasını da sağlayabiliriz. Ses trafiği bağlantının kurulması için TCP 1720 numaralı portu kullanır, daha sonra paketler UDP 16384 ile UDP 32767 port aralığından gönderilir. 101 numaralı erişim listesine uyan tüm paketler GOLD sınıfına dahil edilecektir.

```
CE2611-ALT (config)# access-list 101 permit tcp any any eq 1720
CE2611-ALT (config)# access-list 101 permit udp any any range 16384
32767
```

Aynı şeyi 101 numaralı bir erişim listesi tanımlayarak ses trafiği için de yaptıktan sonra yapmamız gereken bu erişim listelerine göre sınıfları tanımlamaktır.

```
CE2611-ALT (config)# class-map GOLD
CE2611-ALT (config-cmap)# match access-group 101
CE2611-ALT (config-cmap)# exit

CE2611-ALT (config)# class-map SILVER
CE2611-ALT (config-cmap)# match access-group 102
CE2611-ALT (config-cmap)# exit
```

Daha sonra bu servis politikası ilgili arayüze uygulanmalıdır.

```
CE2611-ALT (config)# interface Serial 0/0
CE2611-ALT (config-if)# service-policy output POLITIKA
```

Tüm bu konfigürasyonlar yapıldığı takdirde, CE2611-ALT yönlendiricisine doğrudan bağlı 100 dahili numaralı telefondan CE2611-UST yönlendiricisine bağlı 200 numaralı dahili telefona bir ses trafiği başlatıldığında CE2611-ALT yönlendiricisi üzerindeki 101 numaralı erişim listesi gereğince bu paketin ip precedence değeri 5 olarak atanarak paket PE3640-LAB yönlendiricisine gönderilecektir. Burada PE3640-LAB gelen paketin ip precedence değerini 5 olarak gördüğü için bunun GOLD sınıfından bir paket olduğunu anlayacak ve politika tanımı gereği etiket başlığını koyarken MPLS EXP değerini de 5 olarak belirleyip bandgenişliğinin yüzde 50'sini ayırarak etiketli paketi PE3640-COMMS LSR'ına aktaracaktır. Aynı tanımlar burada da olduğu için gelen paketin EXP değerinden bunun GOLD tipinden olduğu anlaşılacak bu etiket başlığı kaldırılırken paketin ip precedence değeri 5 olarak karşı tarafa gönderilecektir. Aynı şey 102 numaralı erişim listesine ilişkin bir paket geldiğinde ip precedence değeri 3 olarak gönderilirken de yapılmakta ve PE'ler üzerinde bu paketin SILVER kapsamına girdiği anlaşılmaktadır. Her iki sınıfa da dahil olmayan tüm paketler default sınıfa dahil kabul edilmekte ve olabildiğince-iyi prensibiyle iletilmektedir.

7.6 Servis Kalitesi (QoS) Testleri

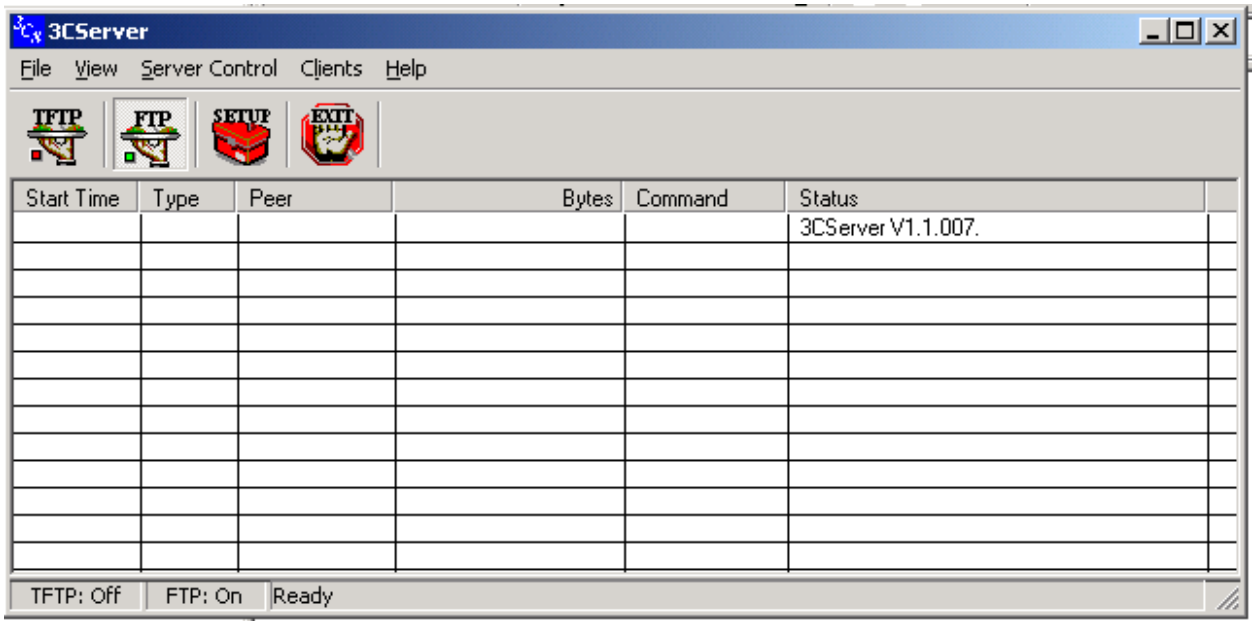
Hazırlamış olduğumuz lab ortamında 7.1'de belirtilen cihazlar ile MPLS VPN topolojisi oluşturulmuş ve bu topolojinin üzerinde önceki bölümlerde belirtilen servis kalitesi tanımları yapılmıştır. Servis kalitesi uygulaması olarak *Farklılaştırılmış Servisler (DiffServ)* tercih edilmiştir.

DiffServ amaçlı olarak topolojimizde yukarıda belirtildiği üzere üç sınıf tanımı yapılmıştır. Testler, CE2611-ALT yönlendiricisi üzerindeki FXS portuna bağlanan bir analog telefon ve ethernet portuna bağlanan bir Windows 2000 dizüstü bilgisayara karşılık, CE2611-UST yönlendiricisi FXS portuna bağlanan bir analog telefon ile bir diğer Windows 2000 bilgisayar arasında yapılmıştır.

Testler sırasında CE2611-ALT yönlendiricisine bağlı 100 dahili numarasına sahip analog telefondan, CE2611-UST yönlendiricisine bağlı 200 dahili numarası atanan analog

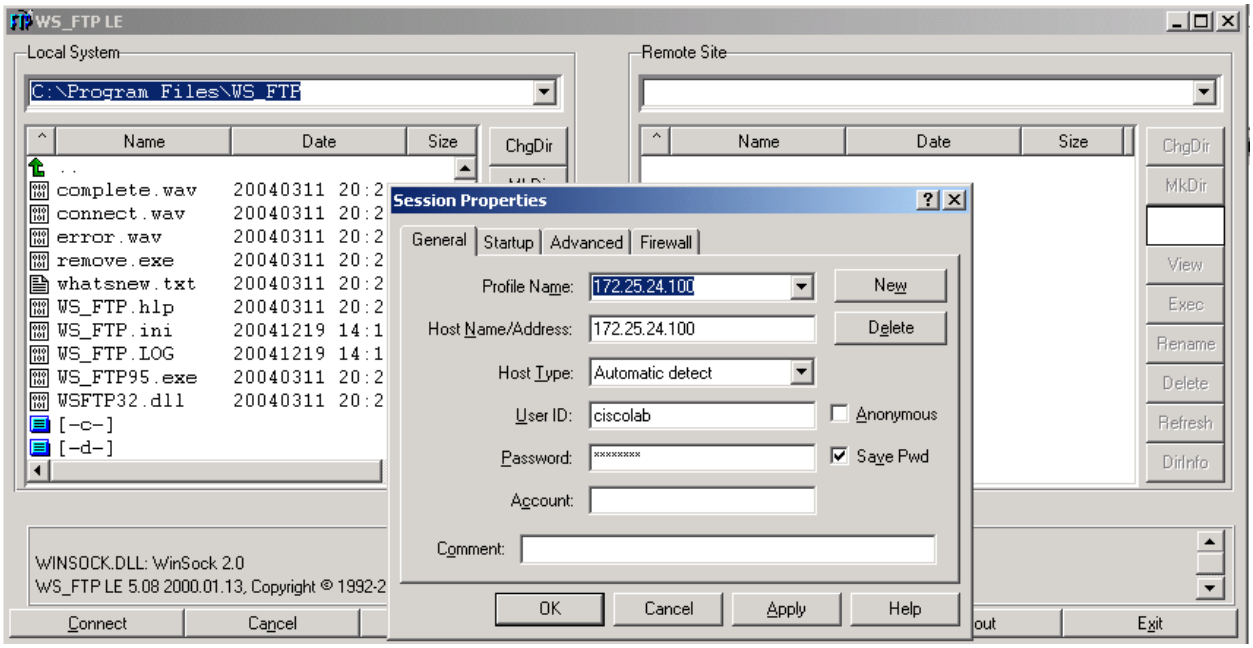
telefona VRF VPN1 içerisinden bir ses çağrısı başlatılmıştır. Ses çağrısı başlatıldığında TCP 1720 numaralı porttan oturum kurulmakta ve ses paketleri UDP 16384 ile UDP 32767 portları aralığından gitmektedir. Yapmış olduğumuz 101 numaralı erişim listesi tanımı nedeniyle oturumun açılması ya da ses çarısı sırasında giden tüm paketler bu erişim listesine girmekte ve dolayısıyla CE yönlendiricisi üzerinde "match access-group 101" komutu sayesinde GOLD sınıfına alınmaktadır.

Benzer şekilde CE2611-ALT yönlendiricisinin ethernet portuna bağlı bir dizüstü bilgisayarda Şekil 7.2'de görülen 3Com FTP sunucusu kullanılmakta, istemci olarak da CE2611-UST yönlendiricisine bağlı PC üzerinde Şekil 7.3'te görülen WS-FTP LE, FTP istemcisi yazılımı kullanılmaktadır.



Şekil 7.2: 3CServer FTP Sunucusu Programı

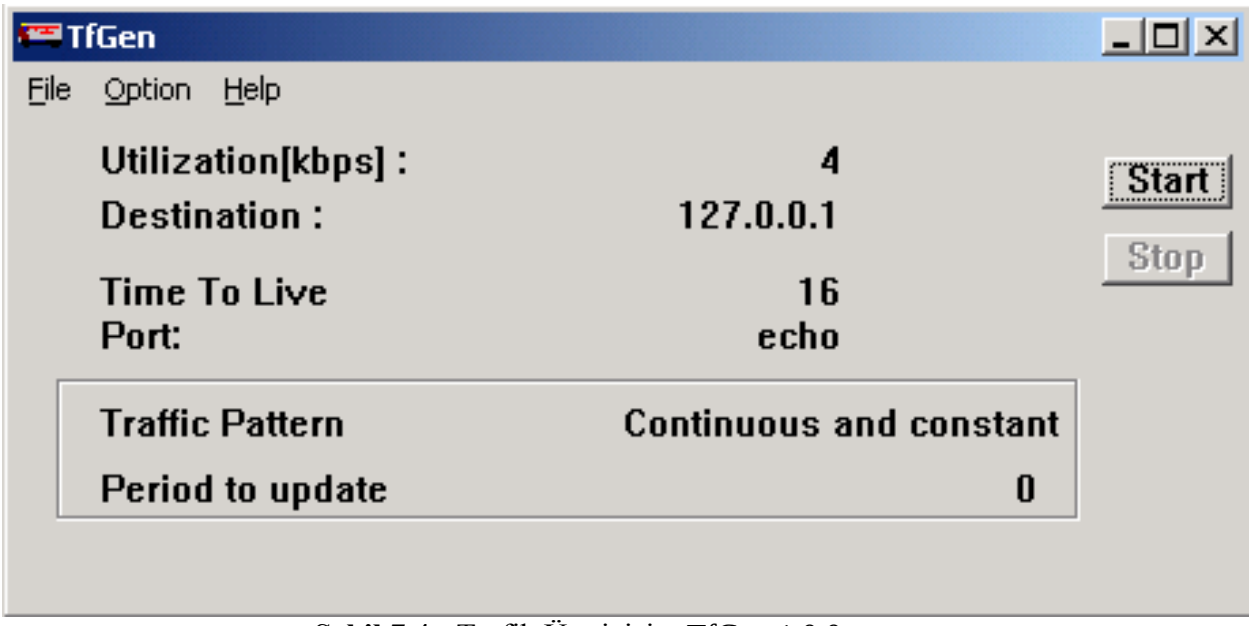
İki uç arasında FTP trafiği başlatıldığında, FTP oturumu TCP 20 ve 21. portları kullandığı için yazmış olduğumuz 102 numaralı erişim listesi satırları gelen trafiğin bir FTP trafiği olduğunu anlamakta ve bu trafiği "match access-group 102" komutu ile SILVER trafik sınıfına dahil etmektedir.



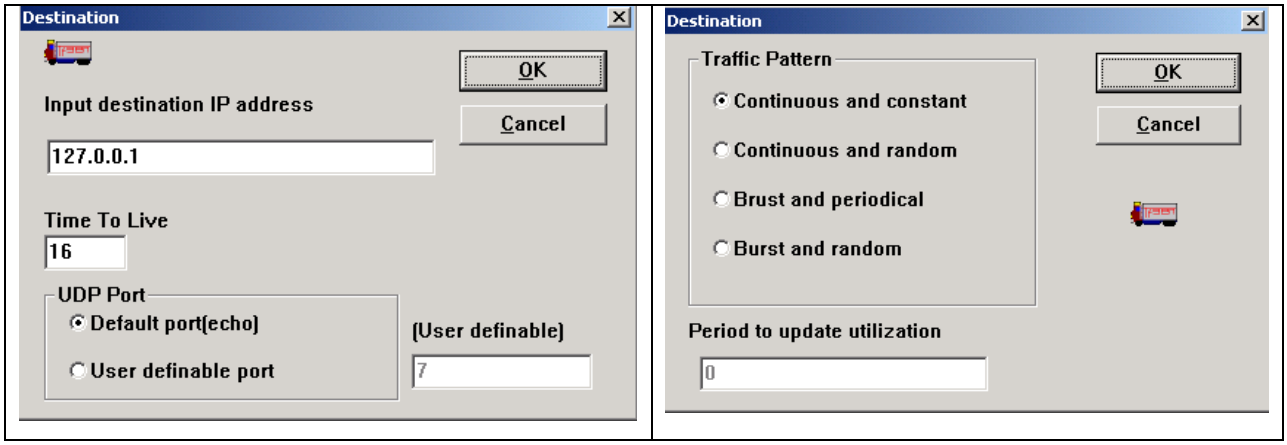
Şekil 7.3: WS_FTP LE FTP İstemcisi Programı

Son servis sınıfı olarak "default" sınıf kullanılmaktadır. Bu sınıfın kullanımı için CE2611-ALT yönlendiricisi üzerine bağlı olan PC üzerinden bir trafik üreticisi yardımıyla CE2611-UST yönlendiricisine bağlı PC'ye doğru trafik yaratılmaktadır. Trafik üreticisi olarak akademik amaçlarla ücretsiz olarak kullanıma sunulmuş olan Şekil 7.4'te görülen TfGen 1.0.0 yazılımı kullanılmıştır.

TfGen yazılımı içerisinde yer alan trafik tipi ve hızı opsiyonları kullanılarak "olabildiğince-iyi" mantığıyla çalışan datagramlar oluşturulmaya çalışılmıştır. Program içerisinde "utilization" opsiyonu kullanılarak sistemde ne kadar bir bandgenişliği kapsayacak trafik yaratmak istendiği belirlenebilmektedir. Benzer şekilde hedef adres, trafiğin yönelmesi istenen port numarası ve trafiğin tipi "sürekli-sabit hızlı", "sürekli-rastgele", "patlamalı-sabit hızlı" ve "patlamalı-rastgele" olarak belirlenebilmektedir. Şekil 7.5'te görülmektedir.



Şekil 7.4: Trafik Üreticisi – TfGen 1.0.0



Şekil 7.5: TfGen Üzerinde Hedef Adres ve Trafik Tipi Tanımlama

Lab ortamında yapılan testlerde "sürekli-sabit hızlı" trafik tipi kullanılmıştır. Trafik hızı olarak da 100, 1000, 2000, 5000 kbps değerleri kullanılmış ancak cihazlar arasında yüksek hızlı V.35 seri bağlantılar yer aldığı için yalnızca 5000 kbps hızında trafik üretildiğinde bir sınıf tanımları nedeniyle bir miktar paket kaybı tespit edilebilmiştir.

Yapılan sınıflandırmanın çalışıp çalışmadığını anlamak üzere, Cisco IOS işletim sistem üzerinde yer alan "show policy-map interface" komutu kullanılmıştır. Bu komutun çıktısında belirli bir süre zarfında yaratılan trafikler için hangi miktarda paketin hangi

sınıfa dahil olduğu görülebilmektedir. Bu da bize test ortamında kurulan sistemin DiffServ uygulamasını doğru şekilde çalıştırdığını göstermektedir.

Sistemde deneme amaçlı olarak sınıf tanımları içerisinde yalnızca "bandwidth percent" komutu kullanılmıştır. Yani sınıflar arasındaki servis kalitesi farkını oluşturan yalnızca sınıflar bazında atanan bandgenişliği yüzdeleridir. Yapılan testlerde omurga bağlantılarında kullanılan bağlantı tipleri 10 Mbps civarında hızları desteklediği için, analog telefonlarla yaratılan ses trafiğinin ayrılmış olan yüzde 50'lik bandgenişliğini doldurmadığı dolayısıyla bir paket kaybı olmadığı gözlenmiştir. Ayrılan bandgenişliği yüzde 3'ün altına indiğinde ise ses kalitesinde belirgin bir bozulma görülmemesine rağmen ilk kez paket kaybına rastlanmıştır.

FTP trafiğinde de ise indirmekte kullanılan 650 MB'lık dosya tamamlanıncaya kadar CE üzerinde yapılan bandgenişliği ayarları yalnızca hızı etkilemektedir. İlk indirme sıralarında yüzde 30'luk bandgenişliği değerlerinde 1 Mbps seviyelerinde bir hız ile indirme görüldüğü halde bandgenişliği yüzde 5 seviyelerine indirildiğinde 100-120 kbps hızlarına kadar bir düşmeye rastlanmıştır. FTP uygulaması taşıma katmanında TCP ile çalıştığı için hiçbir şekilde paket kaybına rastlanmamıştır. Bu da TCP'nin pencere hızlarını beklendiği gibi otomatik olarak bandgenişliğine adapte ettiğini ve aktarımın güvenilir sürekliliğini sağladığını göstermektedir.

Aşağıda yapılan DiffServ tanımlarına ilişkin paket transferi ortalamaları, her sınıfa giren paket sayıları, toplam paket kayıpları sayısı, kullanılan kuyruk tipi gibi bilgilerin yer aldığı ve DiffServ'ün topolojimizde MPLS VPN üzerinden bir tünel içerisinden sağlıklı bir şekilde çalıştığını gösteren çıktı yer almaktadır. Buradan görülebileceği üzere, paket aktarımları sırasında belirli bir kurala bağlı kalmaksızın rastgele biçimde bandgenişlikleri değerleriyle oynanmış, GOLD miktarı ses trafiğinde oldukça az (adı GOLD olmasına karşın paket kaybı gözlemek amacıyla bandgenişliği zaman zaman yüzde 3 seviyelerine indirilmiştir), SILVER tipi FTP trafiği TCP üzerinde çalıştığı için aktarım hızı ortalaması değişken olmasına karşın paket kaybı sıfır, DEFAULT trafikte ise "olabildiğince-iyi" prensibiyle haberleşme gerçekleştirildiği için TfGen ile yüksek paket yoğunluğunda trafik üretimi yapıldığında ortalama olarak hissedilir ölçülerde paket kaybı gözlenmektedir. Testlerimizde amaçlanan sınıflandırmanın ve kullanılan servis kalitesi

tanımlarının MPLS omurgasında VRF tanımı ile VPN tüneli içerisinden çalışıp çalışmayacağını gözlemekti, dolayısıyla çok yüksek bandgenişliğine sahip hatlarda iletim gerçekleştirildiğinden CE-PE bağlantıları gerçekte olduğu WAN bağlantıları yerine yüksek hızlı LAN bağlantıları kullanılarak emüle edildiğinden, paket kayıpları ve servis kalitesini net olarak gözleyemesek de sınıflandırmanın çalıştığı gözlenerek amaca ulaşılmıştır. [14]

```
CE2611-ALT# show policy-map interface serial 0/0
 Serial0/0: -

 Service-policy output: POLITIKA (1283)

    Class-map: GOLD (match-all) (1285/2)
      28621 packets, 7098008 bytes
      5 minute offered rate 10000 bps, drop rate 0 bps
      Match: access-group 101 (1289)
      Weighted Fair Queueing
        Output Queue: Conversation 5
        Bandwidth 500 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 28621/7098008
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: SILVER (match-all) (1301/4)
      2058 packets, 148176 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 102 (1305)
      Weighted Fair Queueing
        Output Queue: Conversation 4
        Bandwidth 50 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: class-default (match-any) (1309/0)
      19234 packets, 9683345 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  (1313)
```

```
PE3640-LAB# show policy-map interface serial 1/1
 Serial1/1: -

  Service-policy output: POLITIKA

    Class-map: GOLD (match-any)
      10975 packets, 708402 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: mpls experimental  5
        10975 packets, 708402 bytes
        5 minute rate 0 bps
      Queueing
        Output Queue: Conversation 7
        Bandwidth 50 (%)
```

```
      (pkts matched/bytes matched) 10129/708361
      (total drops/bytes drops) 14/3089

  Class-map: SILVER (match-any)
    481221 packets, 28804432 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: mpls experimental  3
      4800 packets, 288000 bytes
      5 minute rate 0 bps
    Queueing
      Output Queue: Conversation 4
      Bandwidth 30 (%)
      (pkts matched/bytes matched) 481221/28804432
      (depth/total drops/no-buffer drops) 0/0/0
       exponential weight: 9
       mean queue depth: 0

   Class-map: class-default (match-any)
    105020 packets, 9614364 bytes
    5 minute offered rate 31000 bps, drop rate 0 bps
    Match: any
    Queueing
      Flow Based Fair Queueing
      Maximum Number of Hashed Queues 32
      (total queued/total drops/no-buffer drops) 0/0/0
       exponential weight: 9
```

7.7 Test Sonuçlarının Değerlendirilmesi ve Öneriler

Yapmış olduğumuz testlerde temin edebildiğimiz donanımlar ile kurulabilecek en uygun MPLS/VPN yapısı kurulmuş, sistem sağlıklı olarak çalıştırılarak çeşitli servis kalitesi uygulamaları (DiffServ ile) da sistemde gerçeklenmiştir. Tezde hedeflenen başta MPLS omurgası üzerinden IP paketlerinin etiketlenerek taşınmasını gözlemek, daha sonra MPLS üzerinde VRF tanımları yardımıyla VPN tünellemeyi yapabilmek ve iki uzak yerleşkeyi birbirine bir VPN tüneli içerisinden yerelde doğrudan haberleşiyorlarmış gibi bağlayabilmekti. Bunun gerçekleştiği ve iki uzak yerleşkenin çıkış yönlendiricileri CE'ler üzerinde yönlendirme tablolarına bakıldığında doğrudan bağlıymışçasına VRF tüneli içerisinden RIP güncellemelerinin gittiği ve cihazların birbirlerine erişebildiği gözlenmiştir. Sonraki aşamalarda CE yönlendiricileri üzerinde IP paketleri trafik tiplerine göre erişim listeleri yardımıyla sınıflandırılmış ve IP QoS tanımları yapılmıştır. CE'ler üzerinde IP paketi içerisindeki DSCP bitlerinin çekilmesi yardımıyla sınıf bilgileri IP üzerinden RIP protokolü ile PE'ye aktarılmış, PE üzerinde gelen paketlerin sınıfına göre bu paketlerin MPLS EXP değerleriyle eşleştirilerek ağa gönderilmesi sağlanmıştır. MPLS zaten IP QoS üzerine bir yenilik getirmemekte yalnızca getirdiği devrim niteliğindeki

etiket yığını ve VPN desteği yapısıyla IP QoS bilgilerinin tünel içerisinden WAN'a yayılmasını sağlamaktadır. Amaçlanan bu olduğu için tez amacına ulaşmıştır.

Sistem üzerinde gelecekte yapılabilecek çalışmalar için öneriler, başta bir "P" router kullanımı ile salt etiket anahtarlamanın yarattığı performans getirisinin gözlenmesidir. Bu yönlendirici üzerinde gerekli Cisco IOS komutları yürütüldüğünde bu cihazların MPLS VPN, VPN-IP paketlerini taşırken kesinlikle bunlar içerisindeki etiket yığını ve ikinci seviye etiket bilgisinden haberdar olmadıkları gözlenecektir. MPLS'in omurgada yüksek hızlı anahtarlama yapabilmesinin en önemli nedeni budur. Dolayısıyla bunun gözlenmesi faydalı olacaktır.

Diğer bir öneri de tezin QoS tarafında testlerin burada yapıldığı gibi CE-PE arasındaki yüksek hızlı bağlantılar kullanımı yerine mümkün olursa gerçek bir WAN bağlantısı üzerinden, özellikle yaygın olarak kullanılan Frame-Relay hatları üzerinden IP QoS tanımlarının denenmesidir. Bu yapıldığında servis kalitesi tanımlarının özellikle seste kaliteyi belirgin olarak nasıl arttırdığı gözlenecektir. CE üzerinde IP QoS tanımları yapılan trafiklerin MPLS şebekesine girdiği anda farklı sınıflandırma tanımlarıyla omurgada taşınması da denenebilir. Tezimiz kapsamında yalnızca bandgenişlikleri ile oynanmıştır, bu testler önceliklendirme ya da kuyruk tiplerinin değiştirilmesi yoluyla da denenebilir. Bir başka öneri olarak da artık çok fazla tercih edilmese de IntServ uygulamarı da DiffServ ile kıyaslanmak üzere denenebilir.

8. NS MPLS SİMÜLASYONU

Bu bölümde önceki bölümlerde teorik bilgisi sunulan ve 7. bölümde örnek bir topoloji üzerinde gerçeklenen topolojinin bir simülasyon ortamına aktarılarak servis kalitesi parametrelerinin incelemesi yapılmaktadır.

8.1 NS Simülasyon Parametrelerinin Tanımlanması

Servis kalitesinden bahsedildiğinde bilindiği üzere dikkate alınması gereken üç temel parametre, paket kayıp oranı (packet loss), gecikme (delay) ve seğirtim (jitter) değerleridir. Simülasyon ortamımızda bu temel ölçüm parametrelerinin omurgadaki bandgenişliği değişimine olan duyarlılıkları incelenmektedir.

Tezimiz kapsamında 7. bölümde gerçeklemiş olduğumuz MPLS/VPN ağ ortamına benzerlik arzetmesi için CE ve PE yönlendiricileri arasındaki bandgenişlikleri gerçeklenen ortam ile aynı tutulmuştur. Önceki bölümde yapılan testlerde açıkladığımız üzere omurga bandgenişlikleri yüksek kapasiteli olduğu için kuyruklama ve paket kaybı gözlenenememiştir. Bu nedenle temel değişken olarak bandgenişliği alınmış ve parametrelerimizin bandgenişliği değişikliklerine olan tepkisi ölçülmüştür.

Temel olarak 3 farklı trafik tipi tanımlanmıştır. Gerçeklenen topoloji örneğimizde olduğu gibi bir CE çifti arasında sabit miktarda veri gönderilirken, diğer bir CE çifti arasında VoIP, FTP ve UDP trafikleri yaratılmaktadır. NS ortamında VoIP trafiğinin simülasyonu exponansiyel dağılımla belirlenmektedir. FTP trafiği belirli bir TCP portunu kullandığı için simülasyon çalışmamızda FTP tanımları kullanılmaktadır. UDP trafiği ise gerçeklenen ortamımızla benzer bir şekilde CBR paketleri şeklinde sabit hızlı ve sabit aralıklı paket trafiği şeklinde simüle edilmektedir.

Simülasyonda NS (Network Simulator) aracının ns-2.1b9a versiyonu kullanılmıştır. NS simülatörünün bu versiyonunda bütünleşik MPLS NS (MNS) desteği içerilmekte, DiffServ desteği için ise bir yamanın kurulması gerekmektedir. Aşağıda NS içerisinde CE düğümlerinin ve PE MPLS düğümlerinin yaratılması görülmektedir.

```
# Basit düğümlerin yaratılması
set CE0 [$ns node]
set CE1 [$ns node]
set CE2 [$ns node]
set CE3 [$ns node]

# MPLS düğüm modunun etkinleştirilmesi
$ns node-config -MPLS ON

# MPLS düğümlerinin yaratılması
set PE4 [$ns node]
set PE5 [$ns node]
set PE6 [$ns node]

# MPLS düğüm modunun etkisizleştirilmesi
$ns node-config -MPLS OFF
```

Düğümler ve aralarındaki bağlantılar ise aşağıda görüldüğü gibi yapılandırılabilir. Burada temel olarak başlangıçta, 7. bölümde yaptığımız gibi omurga bağlantılarının 11 Mb bandgenişliğine sahip olarak yaratıldığını görüyoruz. Daha sonra bu bağlantılar değiştirilerek, 500 K, 1 Mb, 2 Mb, 5 Mb ve 11 Mb değerleri için ayrı ayrı paket kaybı, gecikme ve seğirtim değerleri incelenmektedir.

```
# MPLS düğümleri arasında omurga bağlarının yaratılması

$ns duplex-link $PE4 $PE5 11Mb 10ms RED
$ns duplex-link-op $PE4 $PE5 color "blue"
$ns duplex-link $PE5 $PE6 11Mb 10ms RED
$ns duplex-link-op $PE5 $PE6 color "blue"
$ns duplex-link $PE4 $PE6 11Mb 10ms RED
$ns duplex-link-op $PE4 $PE6 color "blue"
$ns duplex-link-op $PE4 $PE6 queuePos 0.5

# PE ve CE düğümleri arasındaki bağlantıların yaratılması

$ns duplex-link $CE0 $PE4 100Mb 10ms RED
$ns duplex-link-op $CE0 $PE4 color "green"
$ns duplex-link $CE1 $PE4 11Mb 10ms RED
$ns duplex-link-op $CE1 $PE4 color "green"
$ns duplex-link $CE2 $PE5 100Mb 10ms RED
$ns duplex-link-op $CE2 $PE5 color "green"
$ns duplex-link $CE3 $PE6 11Mb 10ms RED
$ns duplex-link-op $CE3 $PE6 color "green"
```

CE0 düğümü ile CE2 düğümleri arasında MPLS omurgası üzerinden akan sabit CBR trafiğinin yaratılması şu şekilde yapılmaktadır.

```
# CE0 ve CE2 düğümleri arasında CBR trafiğinin yaratılması

set Src0 [new Application/Traffic/CBR]
set udp0 [new Agent/UDP]
```

```
$Src0 attach-agent $udp0
$ns attach-agent $CE0 $udp0
$Src0 set packetSize_ 1500
$Src0 set interval_ 0.010

set Dst0 [new Agent/Null]
$ns attach-agent $CE2 $Dst0
$ns connect $udp0 $Dst0
```

CE1 düğümü ile CE3 düğümleri arasında MPLS omurgası üzerinden akan exponansiyel dağılımla belirlenen VoIP trafiğinin yaratılması aşağıdaki gibi yapılmaktadır. Ancak testlerimizde ses için sürekli ve deterministik bir trafik olması açısından ses trafiği de UDP/CBR ile simüle edilmiştir.

```
# CE1 ve CE3 düğümleri arasında MPLS üzerinden VoIP trafiği yaratılması

set srcv [new Agent/UDP]
set sinkv [new Agent/UDP]
$ns attach-agent $CE1 $srcv
$ns attach-agent $CE3 $sinkv
$ns connect $srcv $sinkv

set exp [new Application/Traffic/Exponential]
$exp attach-agent $srcv $exp set packetSize_ 500
$exp set rate_ 200K
```

CE1 düğümü ile CE3 düğümleri arasında MPLS omurgası üzerinden akan ve TCP ile simüle edilen FTP trafiğinin yaratılması şu şekilde yapılmaktadır.

```
# CE1 ve CE3 düğümleri arasında MPLS üzerinden FTP trafiği yaratılması

set tcp01 [new Agent/TCP]
set tcp01sink [new Agent/TCPSink]
$ns attach-agent $CE1 $tcp01
$ns attach-agent $CE3 $tcp01sink
$ns connect $tcp01 $tcp01sink

# Bir FTP trafik kaynağı yaratılarak tcp01 üzerine atanması

set ftp01 [new Application/FTP]
$ftp01 attach-agent $tcp01
```

CE1 düğümü ile CE3 düğümleri arasında MPLS omurgası üzerinden akan ve CBR ile simüle edilen UDP trafiğinin yaratılması şu şekilde yapılmaktadır.

```
# CE1 ve CE3 düğümleri arasında MPLS üzerinden UDP trafiği yaratılması

set Src1 [new Application/Traffic/CBR]
set udp1 [new Agent/UDP]
$Src1 attach-agent $udp1
```

```
$ns attach-agent $CE1 $udp1
$Src1 set packetSize_ 1500
$Src1 set interval_ 0.010

set Dst1 [new Agent/Null]
$ns attach-agent $CE3 $Dst1
$ns connect $udp1 $Dst1
```

Testlerimiz sırasında trafik CE1-CE3 trafiği omurga üzerinde PE4 ile PE6 arasından akmaktadır. Dolayısıyla kuyruklamanın bu doğrultuda yapılması gerekir. Buna ilişkin sözdizim şu şekildedir.

```
# PE4 ve PE6 düğümleri arasındaki bağa ilişin bir kuyruk yaratılması
$ns queue-limit $PE4 $PE6 10
```

Bu noktaya kadar yapılan tanımlar MPLS tipinden ve IP tipinden düğümlerin ve düğümler arasındaki trafiklerin yaratılmasıdır. MPLS protokolünün çalışabilmesi için PE düğümleri arasında bir LDP dolaşımının sağlanması gerekir. Bunun için her düğümde LDP ajanları yaratılır. Burada etiket atamanın gerçek ortamda gösterdiğimiz gibi kontrol yollu yapılmasını istediğimiz için ilgili tanımın da eklenmesi gerekir.

```
# Herbir PE üzerinde LDP ajanlarının yaratılması
for {set i 4} {$i < 6} {incr i} {
    for {set j [expr $i+1]} {$j < 6} {incr j} {
         set a PE$i
         set b PE$j
         eval $ns LDP-peer $$a $$b
    }
}
$ns enable-control-driven
```

Trafiklerimiz akarken tüm paketler analizlerinin yapılabilmesi için bir NAM dosyasına atılmaktadır. Bu NAM dosyasında herbir paketin kaynaktan çıkış zamanı, kuyruğa giriş zamanı, kuyruktan çıkış zamanı ve hedefe ulaşma zamanı bilgileri yer almaktadır. Herbir paketin tekil sıra numarasını kullanarak paketlerin analizi yapılabilmektedir. NAM dosyasının içeriğini ileride ayrıntılı inceleyeceğiz. Paket bilgilerinin bir NAM dosyasında tutulabilmesi için aşağıdaki gibi bir tanımın yapılması gerekir. Buradaki örnekte PE4 ve PE6 düğümleri arasından geçen tüm paketlerin bilgileri masaüstünde yer alan bir *MPLS_BW11.nam* isimli metin dosyasına atılmaktadır.

```
# Simülasyon sonuçlarının NAM dosyasına atılması
```

```
$ns trace-queue $PE4 $PE6 [open /root/Desktop/MPLS_BW11.nam w]
```

Son olarak yapılması gereken ana tanım simülasyonun yürütüm zamanlarının belirlenmesidir ve yordamın sonlandırılmasıdır (ayrıntılı kütüphane tanımlarına yer verilmemektedir, detayları tez CD'sinde yer alan kaynak kodu incelemesi ile elde edilebilir).

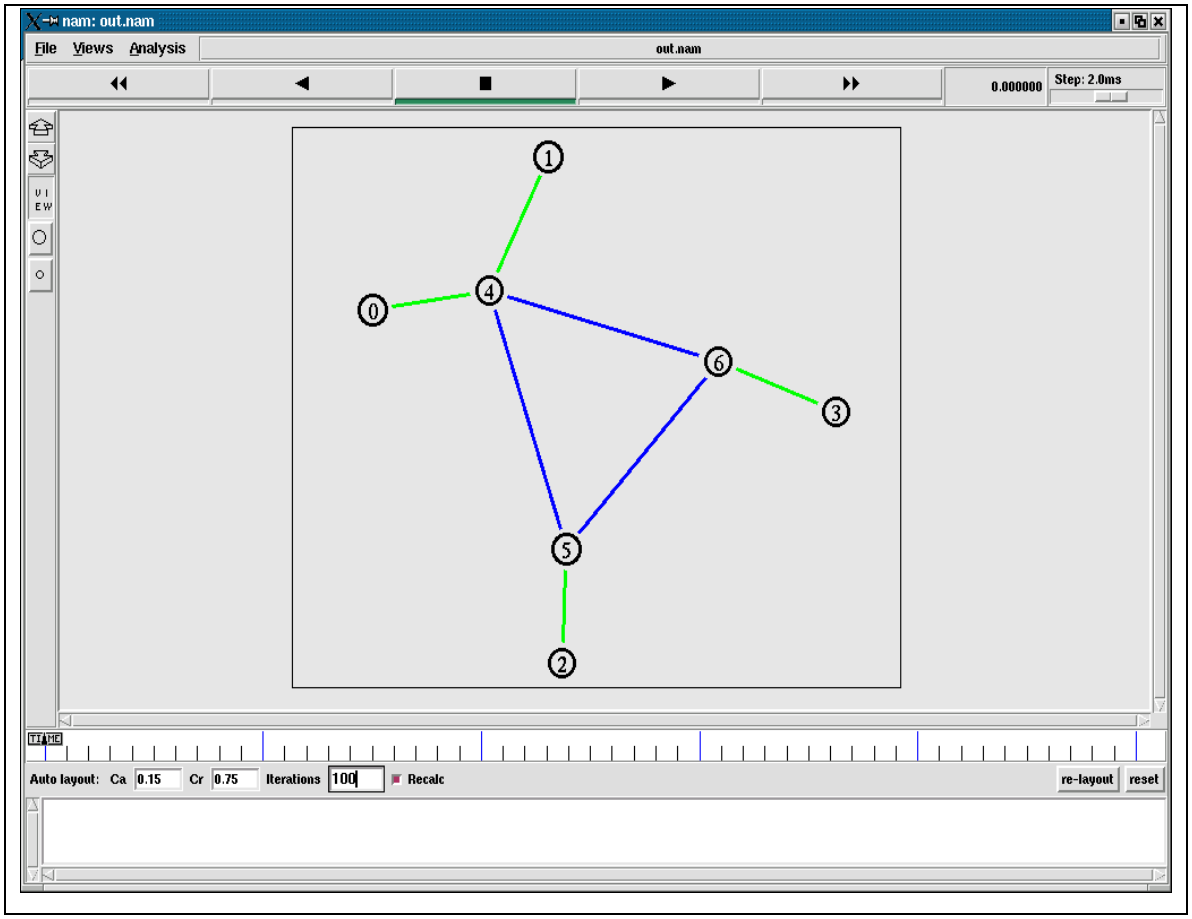
```
# Trafiklerin başlama ve bitiş zamanlarının belirlenmesi

$ns at 0.0 "$ftp01 start"
$ns at 5.0 "$ftp01 stop"
$ns at 0.0 "$Src0 start"
$ns at 5.0 "$Src0 stop"
$ns at 0.0 "$Src1 start"
$ns at 5.0 "$Src1 stop"

$ns at 0.0 "$exp start"
$ns at 5.0 "$exp stop"


# 5 saniyelik simülasyon süresinin sonunda bitiş yordamının çağırılması
$ns at 5.0 "finish"

# Simülasyonun çalıştırılması
$ns run
```

Bu değerlere göre oluşturdurduğumuz topoloji Şekil 8.1'de yer almaktadır.

Karşılaştırma yapabileceğimiz ikinci topolojinin oluşturulabilmesi için yukarıda gerekli tanımlarını yapmış olduğumuz MPLS ortamına bu kez QoS ile ilgili tanımların eklenmesi gerekmektedir. Tezimizde benzetim açısından QoS tanımı olarak 7. bölümde bahsettiğimiz gibi DiffServ ve buna ilişkin olarak trafik tipi bazında bandgenişliği yüzdesi atamayı kullanılmaktadır.

QoS yüzdeleri atanırken CIR (Committed Interface Rate) parametresi kullanılmaktadır. CIR parametresi belirli bir trafiğin sahip olması garanti edilen bandgenişliğini gösterir. Bizim tanımlarımız yüzdesel kıyaslama içerdiğinden herbir trafik için CIR, anlık omurga bandgenişliğinin ilgili yüzdesine denk düşecek şekilde (örneğin 5 Mb bandgenişliğinde VoIP için 2,5 Mb) düzenlenmiştir. Patlamalı (burst) trafik parametreleri olan CBS (Committed Burst Size) ve EBS (Excess Burst Size) sabit tutulmuştur. Örneğin aşağıda Mbps omurga bandenişliği için yapılan DiffServ tanımları görülmektedir.

```
set cir0  2500000
set cbs0     2000
set ebs0     6000
set cir1  1500000
set cbs1     2000
set ebs1     6000
set cir2  1000000
set cbs2     2000
set ebs2     6000
```



Şekil 8.1: NS MPLS Simülasyon topolojisi

NS ortamında DiffServ tanımı yaparken trafik sınıfları yalnızca kaynak ve varış düğüm çiftine göre ayırt edilebilmektedir. Bizim ortamımızda aynı kaynak-varış çiftine giden üç farklı trafiğin analizi yapıldığından, bu trafikleri birbirinden ayırt edebilmek için varış düğümü üç sanal düğüme ayrıştırılmış ve herbir trafik tipinin farklı bir düğümde sonlandırılması sağlanmıştır. Tüm trafik tipleri PE4-PE6 yolunu izlediği ve analizimiz de bu düğümler arasındaki kuyruk üzerinde yapıldığından bu tip bir bölümleme simülasyonumuzun tutarlılığını etkilemeyecektir. Bu bölümleme yapıldıktan sonra

yapmış olduğumuz DiffServ tanımlarını ilgili kaynak-varış çiftine bir politika olarak atayabiliriz. Böylece farklı trafik sınıflarının farklı QoS işlemlerine tabi tutulması sağlanmış olmaktadır.

```
# DiffServ politika tanımlarının atanması

$qE1C set numQueues_ 1
$qE1C setNumPrec 3
$qE1C addPolicyEntry [$CE1 id] [$CE3A id] srTCM 10 $cir0 $cbs0 $ebs0
$qE1C addPolicyEntry [$CE1 id] [$CE3B id] srTCM 10 $cir1 $cbs1 $ebs1
$qE1C addPolicyEntry [$CE1 id] [$CE3C id] srTCM 10 $cir2 $cbs2 $ebs2
$qE1C addPolicerEntry srTCM 10 11 12
$qE1C addPHBEntry 10 0 0
$qE1C addPHBEntry 11 0 1
$qE1C addPHBEntry 12 0 2
$qE1C configQ 0 0 20 40 0.02
$qE1C configQ 0 1 10 20 0.10
$qE1C configQ 0 2  5 10 0.20
```

8.2 Simülasyonun Gerçeklenmesi ve Trafik Analizi

Trafiklerin analizi için NAM dosyasının analizi yapılarak sonuca varılmaktadır. NAM dosyasının içerisinden görülebilecek birkaç satır aşağıdaki gibi görünür.

```
+ 1.244876 4 6 exp 500 ------- 0 1.0 3.0 0 1127
- 1.246465 4 6 exp 500 ------- 0 1.0 3.0 0 1127
r 1.257265 4 6 exp 500 ------- 0 1.0 3.0 0 1127
+ 0.691091 4 6 cbr 500 ------- 0 1.2 3.2 137 294
d 0.691091 4 6 cbr 500 ------- 0 1.2 3.2 137 294
```

Baştaki işaret ve harflerin anlamları şunlardır:

"+" Paket kuyruğa alındı.

"-" Paket kuyruktan çıktı.

"r" Paket hedefe ulaştı.

"d" Paket kuyruktan atıldı (drop).

Paketin durumunu belirten işaretten sonra gelen rakam, olayın gerçekleştiği simülasyon zamanını, 4 ve 6 rakamları paketin geçtiği düğümleri, exp ve cbr değerleri paketin tipini (bu değer TCP de olabilir, burada exp VoIP trafiğini, cbr ise UDP trafiğini göstermektedir), 500 değeri paket boyutunu, sonraki "-" işaretleri paket başlığı içerisinde atanan bir bayrak varsa o değerleri, 0 değeri akış numarasını, 1.0 değeri düğüm.arayüz formatında kaynak düğümü, 3.0 değeri hedef düğümü , sonraki değer (örnekte 0 ve 137) ağ katmanı protokol numarasını ve son değer ise tekil paket numarasını göstermektedir.

Buna göre örneğin yukarıda 1127 numaralı VoIP paketi 1.244876 sn zamanında kaynaktan çıkmış ve kuyruğa alınmış, 1.246465 sn zamanında kuyruktan çıkmış ve 1.257265 anında da hedef düğüme ulaşmıştır. Buna karşın 294 numaralı UDP paketi ise 0.691091 anında kuyruğa gelmiş ve kuyruktan düşürülmüştür.

Sistemimizde analiz yaparken paket kaybı için NAM dosyası içerisindeki "d" değerlerinin sayısına bakılmakta ve herbir paket tipine ilişkin paket kayıpları oranı bulunabilmektedir. Gecikme hesabı yaparken "+" değerleri ile "r" değerleri arasındaki fark alınmakta ve bu değerler herbir paket trafiği için ayrı ayrı bulunmaktadır. Seğirtim (jitter) hesabı için ise, gecikmeler arasındaki farkın varyans değerleri hesabından faydalanılarak standart sapma bulunmaktadır. Standart sapma (σ) hesabı, μ anlık gecikmelerin ortalama gecikmeye olan uzaklığı ve n toplam iletilen paket sayısı olmak üzere şu şekilde hesaplanır:

$$\sigma = \sqrt{\frac{(\mu_1)^2 + (\mu_2)^2 + (\mu_3)^2 + \ldots + (\mu_n)^2}{n}}$$

Analizimiz sırasında tüm örnekleme yapılmamış, 5 sn süresince simülasyonumuz boyunca geçen bütün paketler dikkate alınmış ve hesaplamaya dahil edilmiştir. Hesaplama için *Microsoft Office Excel 2003* versiyonu, hesaplama ve grafik özellikleri kullanılmıştır.

8.3 Simülasyon Analizi Sonuçları ve İncelemeler

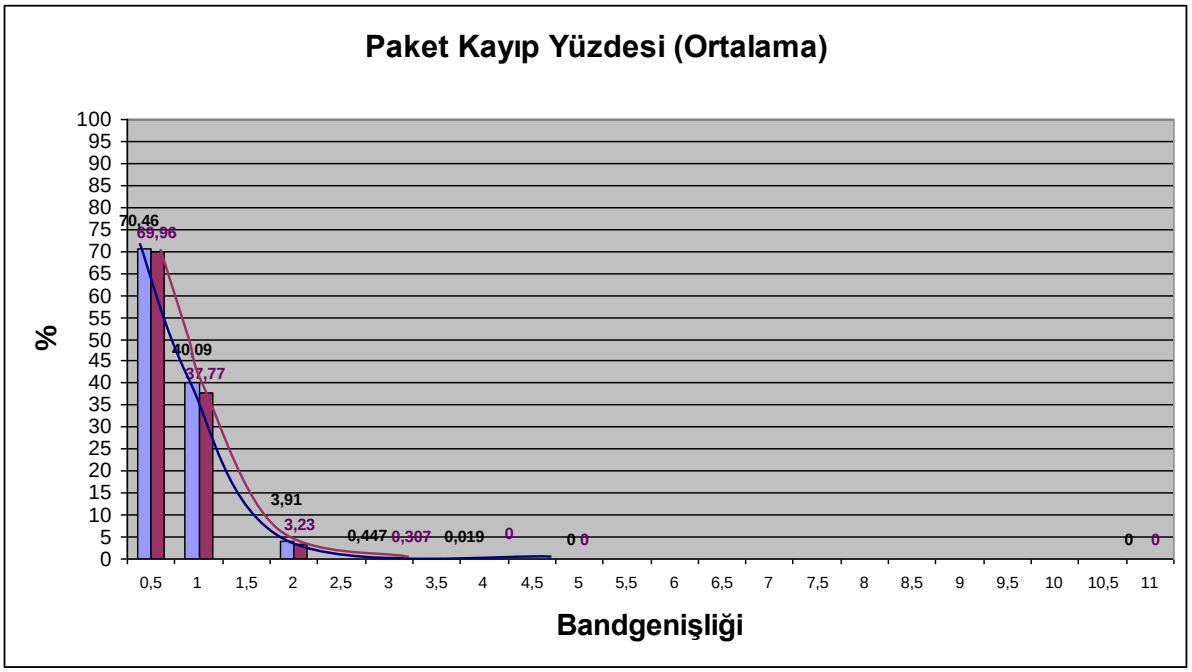
8.3.1 Paket Kaybı İncelemeleri

Paket kaybı analizlerimizde sonuçlar 5 farklı omurga bandgenişliği değerine simülasyonun verdiği tepkilere ilişkin olarak elde edilmiştir. Elde edilen sonuçlar Tablo 8.1'de yer almaktadır.

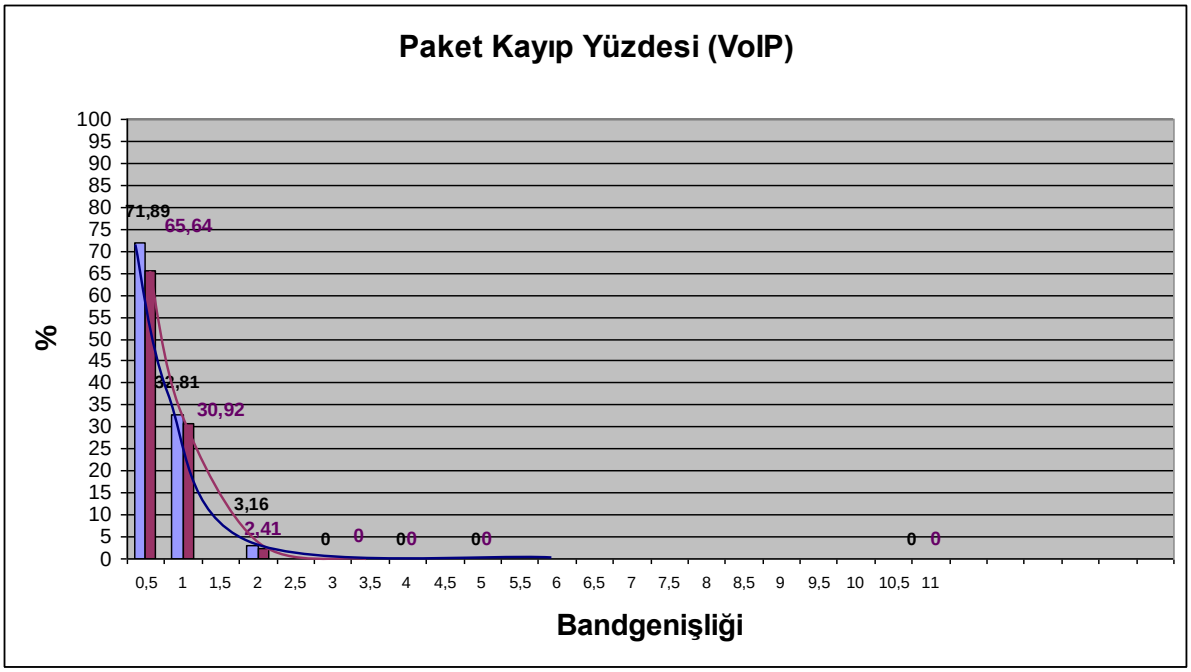
Tablo 8.1: Simülasyon Paket Kaybı Sonuçları

Kayıp BG	Ortalama MPLS	Ortalama MPLS/QoS	VoIP MPLS	VoIP MPLS/QoS	FTP MPLS	FTP MPLS/QoS	UDP MPLS	UDP MPLS/QoS
500 K	70,46	69,96	71,89	65,64	63,64	64,12	73,92	77,98
1 M	40,09	37,77	32,81	30,92	54,44	51,23	36,75	34,65
2 M	3,91	3,23	3,16	2,41	3,44	3,42	4,91	3,86
3 M	0,447	0,307	0	0	0,655	0	0,711	0,804
4 M	0,019	0	0	0	0,0747	0	0	0
5 M	0	0	0	0	0	0	0	0
11 M	0	0	0	0	0	0	0	0

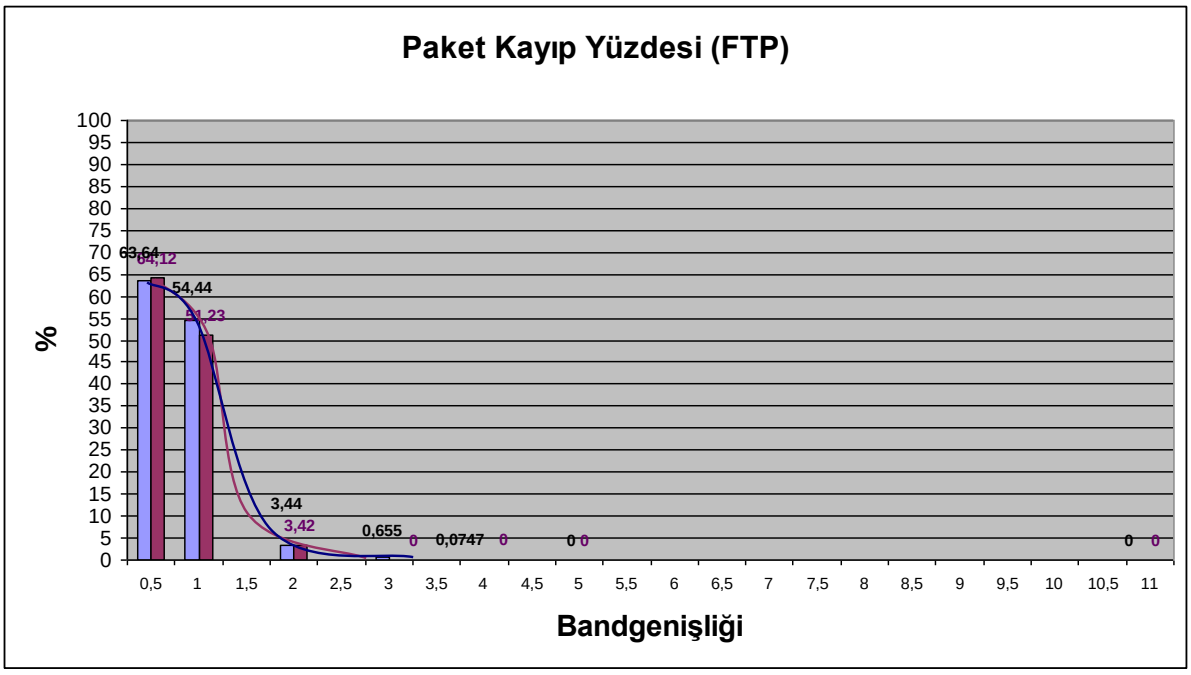
Bu değerlere ilişkin değişim grafiklerimiz Şekil 8.2 (ortalama paket kaybı), Şekil 8.3 (VoIP trafiğindeki paket kaybı), Şekil 8.4 (FTP trafiğindeki paket kaybı) ve Şekil 8.5'te (UDP trafiğindeki paket kaybı) görülmektedir.



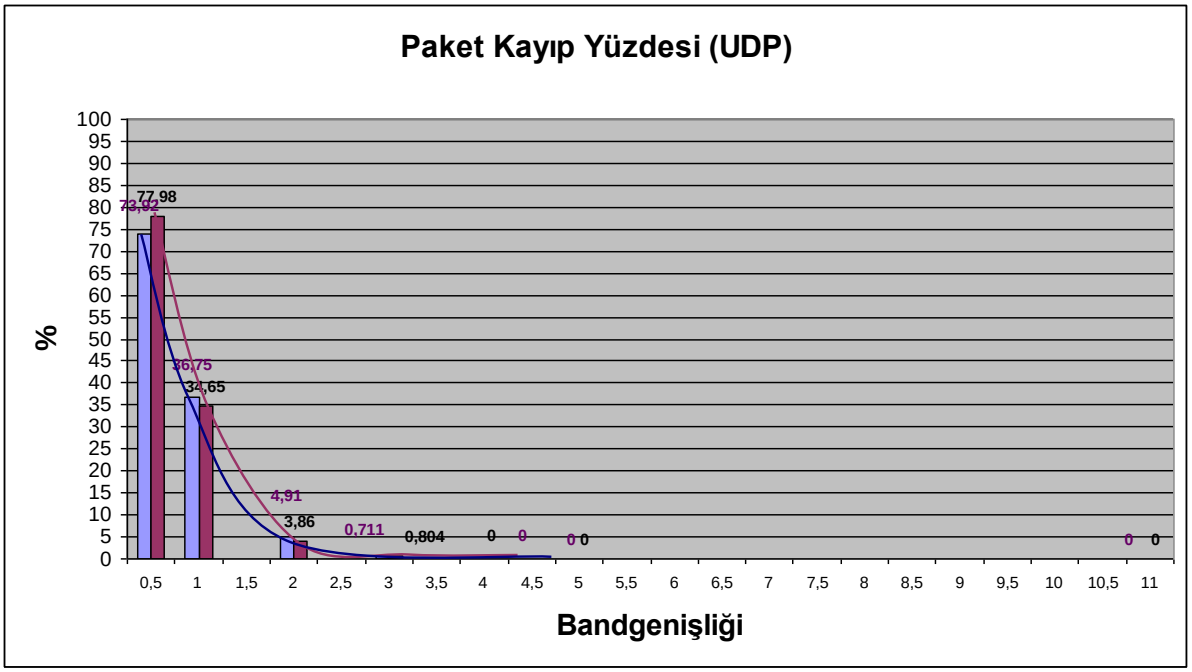
Şekil 8.2: Ortalama paket kaybı



Şekil 8.3: VoIP trafiğindeki paket kaybı



Şekil 8.4: FTP trafiğindeki paket kaybı



Şekil 8.5: UDP trafiğindeki paket kaybı

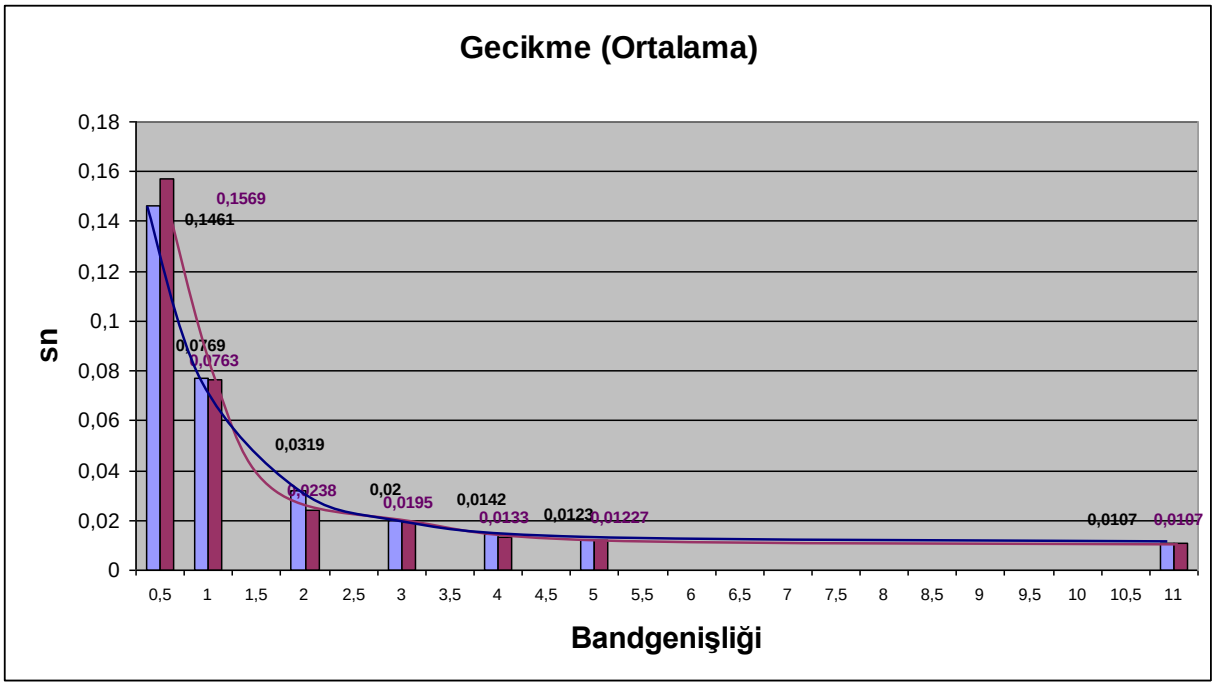
8.3.2 Paket Gecikmesi İncelemeleri

Paket gecikmesi analizlerimizde sonuçlar 5 farklı omurga bandgenişliği değerine simülasyonun verdiği tepkilere ilişkin olarak elde edilmiştir. Elde edilen sonuçlar Tablo 8.2'de yer almaktadır.

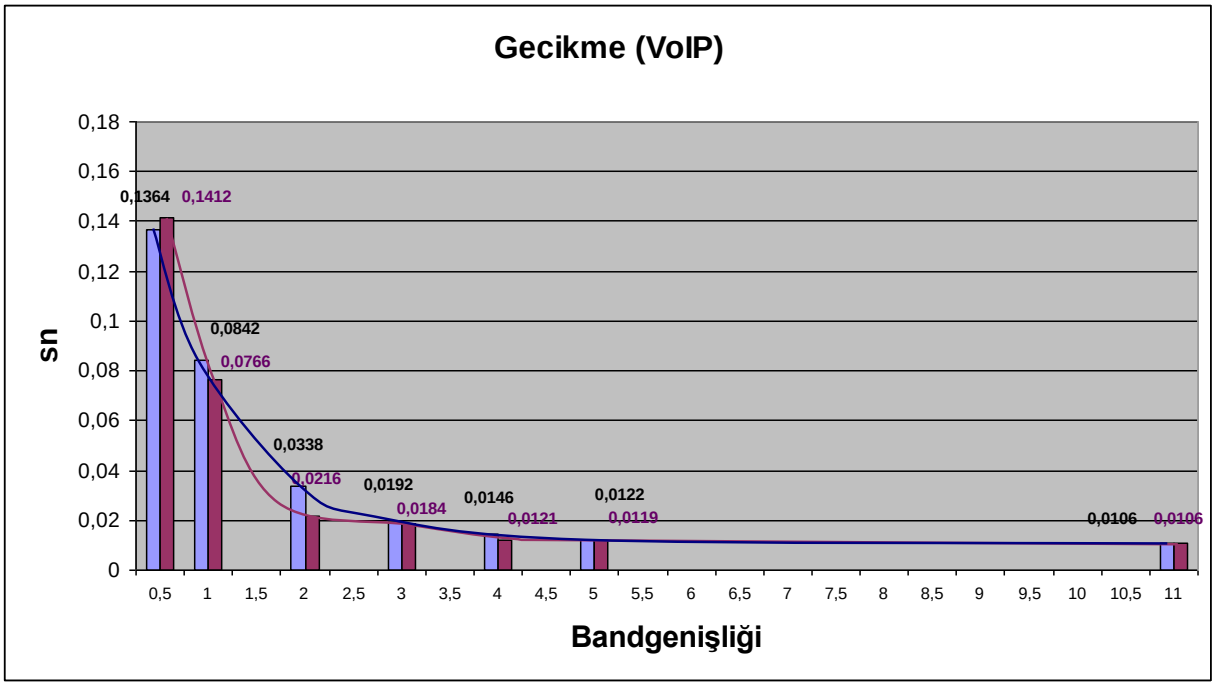
Tablo 8.1: Simülasyon Paket Gecikmesi Sonuçları

Gecikme BG	Ortalama MPLS	Ortalama MPLS/QoS	VoIP MPLS	VoIP MPLS/QoS	FTP MPLS	FTP MPLS/QoS	UDP MPLS	UDP MPLS/QoS
500 K	0,1461	0,1569	0,1364	0,1412	0,134	0,1366	0,1634	0,1756
1 M	0,0769	0,0763	0,0842	0,0766	0,0694	0,0701	0,0755	0,0819
2 M	0,0319	0,0238	0,0338	0,0216	0,0291	0,0228	0,0322	0,0267
3 M	0,02	0,0195	0,0192	0,0184	0,0212	0,0208	0,0198	0,0198
4 M	0,0142	0,0133	0,0146	0,0121	0,0142	0,0134	0,0138	0,0141
5 M	0,0123	0,01227	0,0122	0,0119	0,0125	0,0126	0,0124	0,0124
11 M	0,0107	0,0107	0,0106	0,0106	0,0108	0,0107	0,0107	0,0107

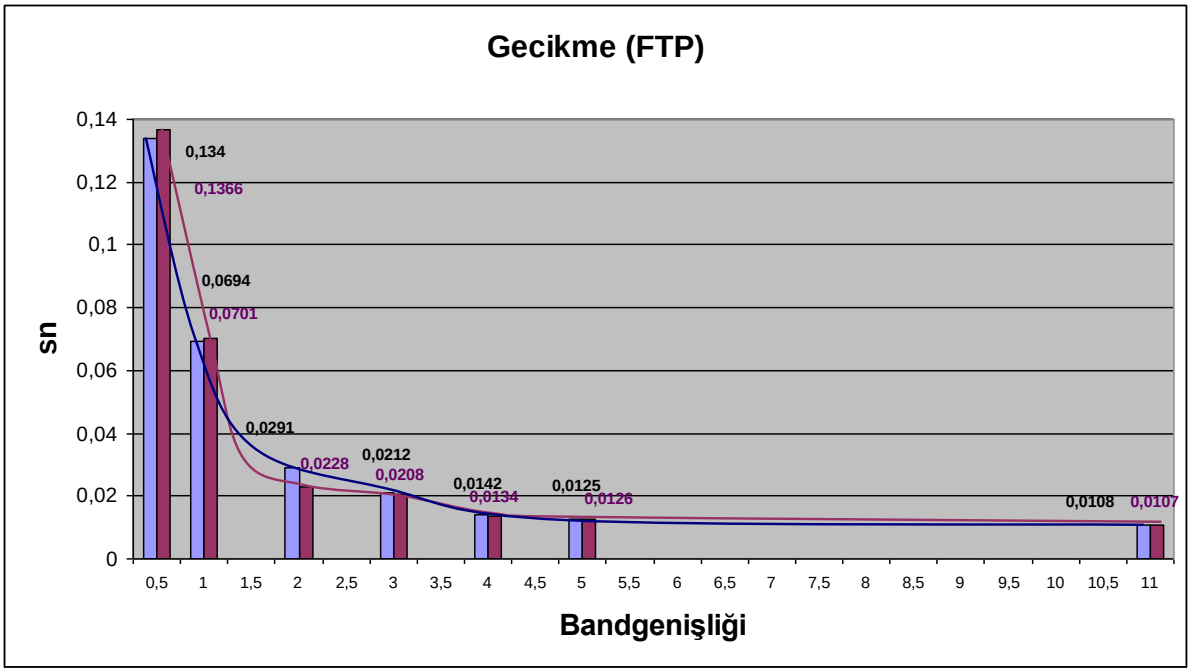
Bu değerlere ilişkin değişim grafiklerimiz Şekil 8.6 (ortalama paket gecikmesi), Şekil 8.7 (VoIP trafiğindeki paket gecikmesi), Şekil 8.8 (FTP trafiğindeki paket gecikmesi) ve Şekil 8.9'da (UDP trafiğindeki paket gecikmesi) görülmektedir.



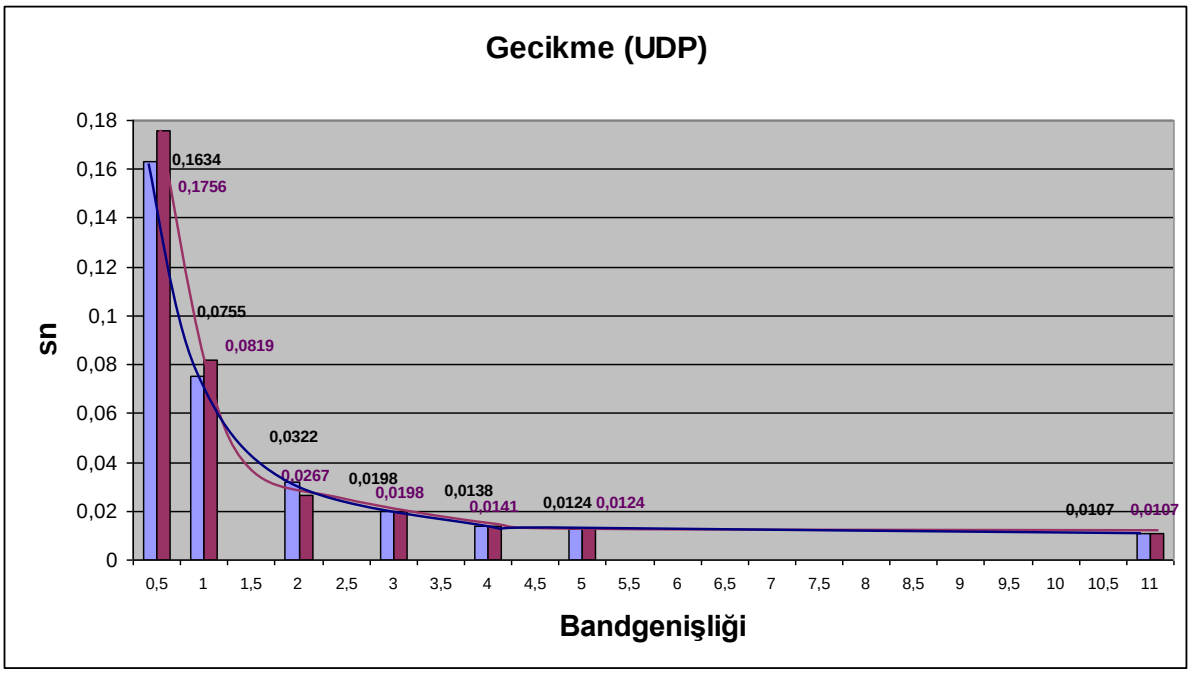
Şekil 8.6: Ortalama paket gecikmesi



Şekil 8.7: VoIP trafiğindeki paket gecikmesi



Şekil 8.8: FTP trafiğindeki paket gecikmesi



Şekil 8.9: UDP trafiğindeki paket gecikmesi

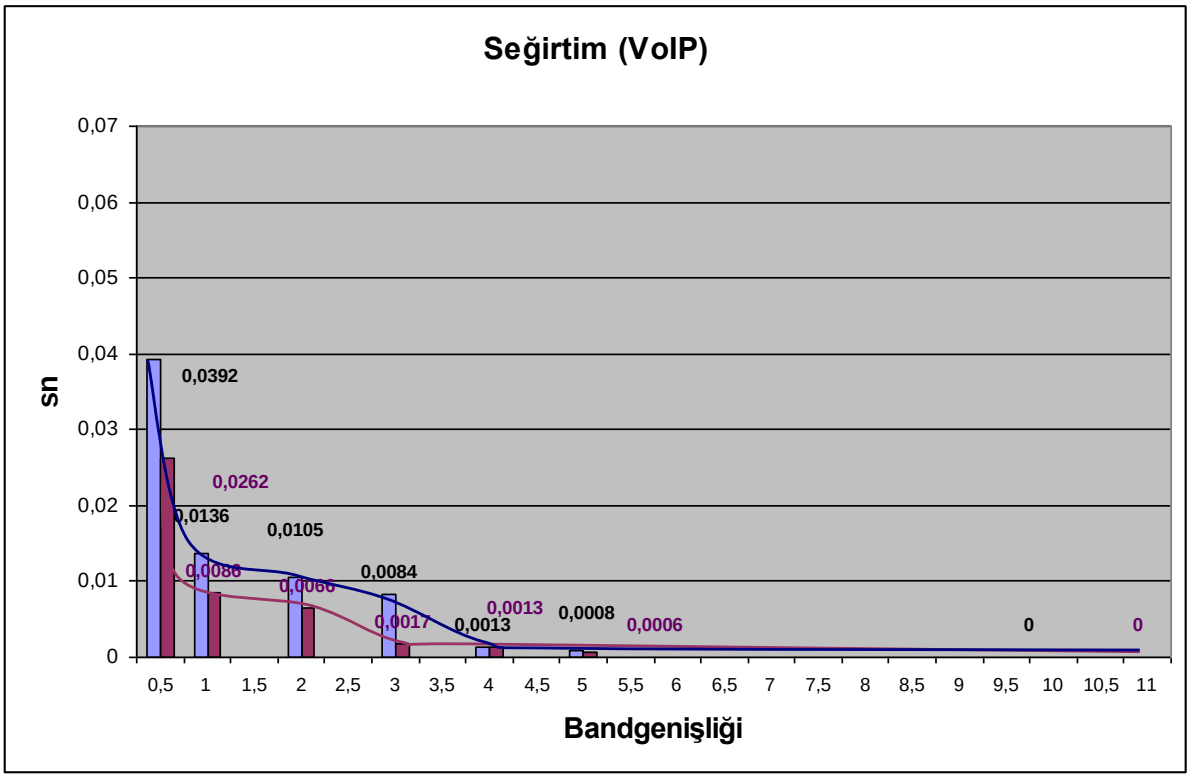
8.3.3 Seğirtim İncelemeleri

Seğirtim (jitter) analizlerimizde sonuçlar 5 farklı omurga bandgenişliği değerine simülasyonun verdiği tepkilere ilişkin olarak elde edilmiştir. Elde edilen sonuçlar Tablo 8.3'te yer almaktadır.

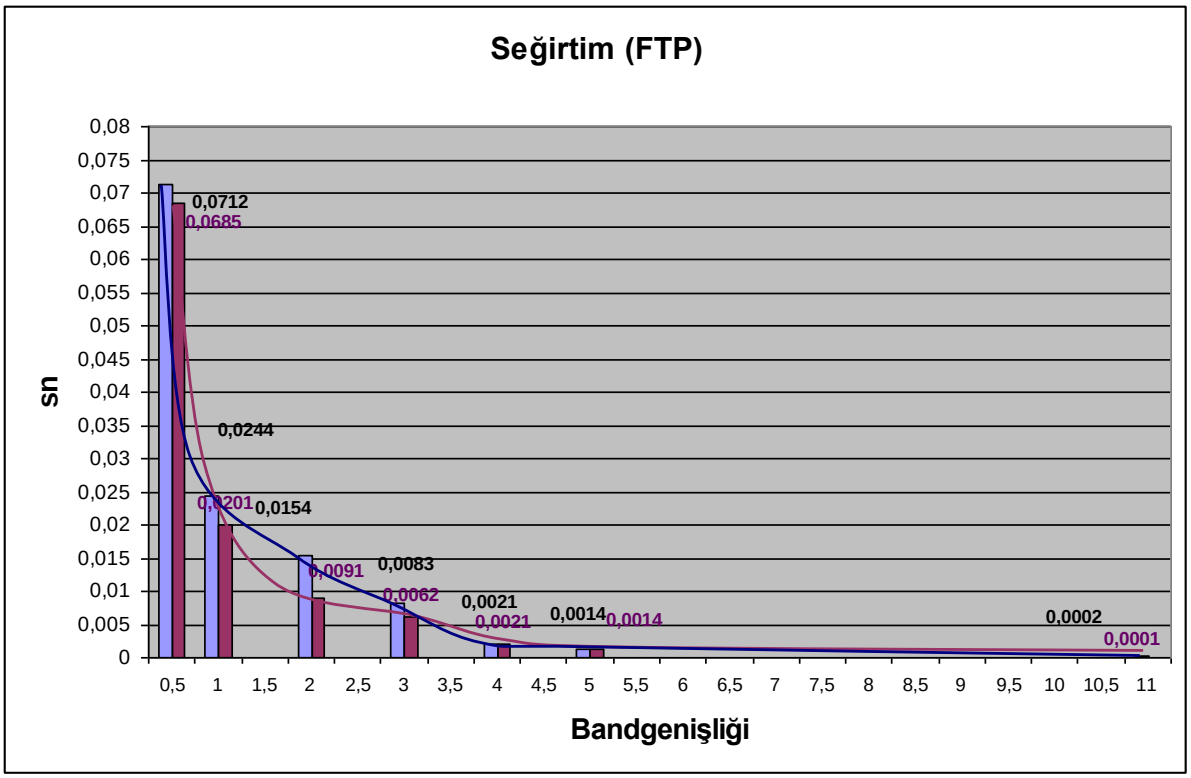
Tablo 8.3: Simülasyon Seğirtim Sonuçları

Seğirtim BG	VoIP MPLS	VoIP MPLS/QoS	FTP MPLS	FTP MPLS/QoS	UDP MPLS	UDP MPLS/QoS
500 K	0,0392	0,0262	0,0712	0,0685	0,0394	0,0288
1 M	0,0136	0,0086	0,0244	0,0201	0,0133	0,0117
2 M	0,0105	0,0066	0,0154	0,0091	0,0105	0,0101
3 M	0,0084	0,0017	0,0083	0,0062	0,0086	0,0067
4 M	0,0013	0,0013	0,0021	0,0021	0,0017	0,0017
5 M	0,0008	0,0006	0,0014	0,0014	0,0008	0,0008
11 M	0	0	0,0002	0,0001	0,0001	0,0001

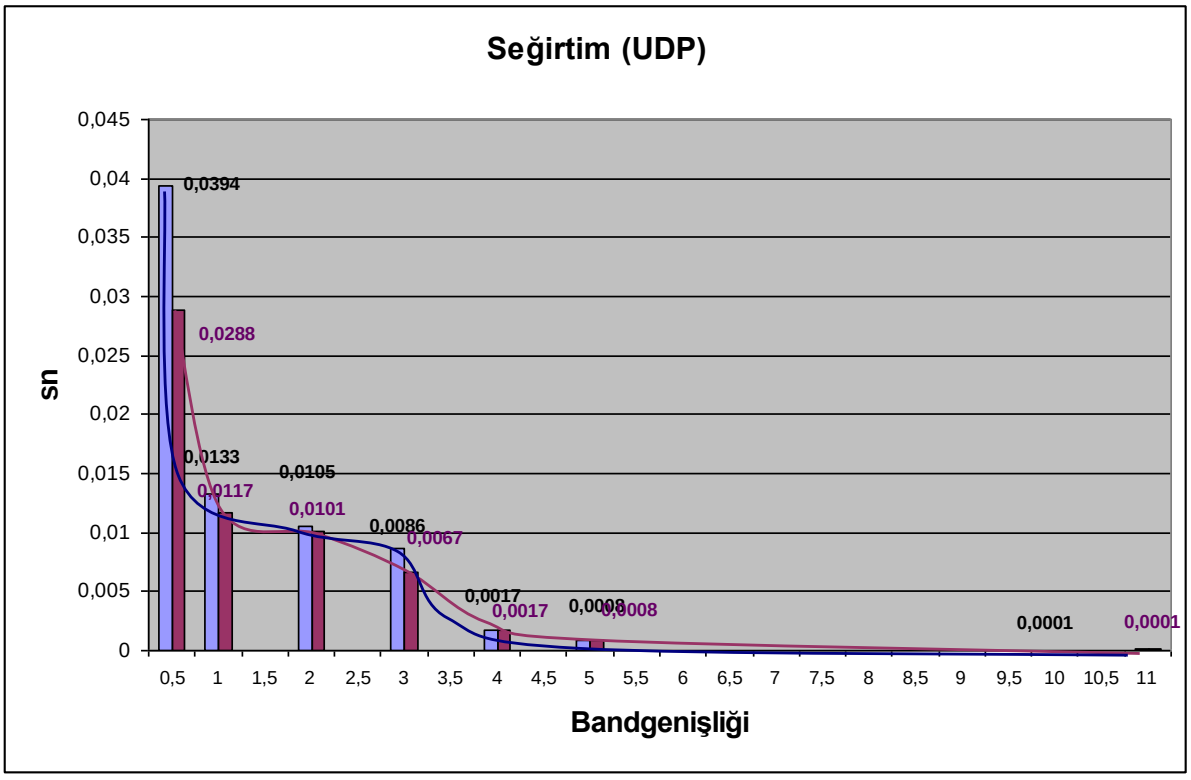
Bu değerlere ilişkin değişim grafiklerimiz Şekil 8.10 (VoIP trafiğindeki seğirtim), Şekil 8.11 (FTP trafiğindeki seğirtim) ve Şekil 8.12'de (UDP trafiğindeki seğirtim) görülmektedir.



Şekil 8.10: VoIP trafiğindeki seğirtim



Şekil 8.11: FTP trafiğindeki seğirtim



Şekil 8.12: UDP trafiğindeki seğirtim

8.4. Simülasyon Sonuçlarının Değerlendirilmesi

NS ortamında yapmış olduğumuz simülasyonda üç farklı trafik sınıfı için farklı servis kalitesi tanımlarının, bandgenişliği değişimine bağlı olarak paket kaybı, gecikme ve seğirtim değerlerine olan etkisi incelenmektedir.

Paket kaybına ilişkin sonuçları değerlendirecek olursak, CIR tipinden bir QoS tanımının trafiğin düzgün kuyruklanmasına ve dolayısıyla paket kaybının belirli düzeylerde azalmasına yol açmaktadır. Trafik bazında inceleyecek olursak VoIP trafiği CIR tanımlarına göre en yüksek bandgenişliğine sahip olduğu için gerçekten yapılan testler ortalama paket kaybının VoIP trafiğinde özellikle 500 Kbps ve 1 Mbps gibi düşük bandgenişliklerinde belirgin oranda etkili olduğu görülmektedir. FTP trafiğinde 500 Kbps değerinde QoS sonucu paket kaybının bir miktar artmasının nedeni zaten kısıtlı olan bandgenişliğinin büyük ölçüde VoIP trafiğine aktarılıyor olmasıdır. Aynı durum UDP trafiğinde de 500 Kbps değerinde görülmektedir. Bandgenişliği arttığında düzenli kuyruklamanın sonucu olarak QoS'un paket kaybının azalması yönünde etki etttiği açıkça görülmektedir.

Gecikmeye ilişkin sonuçlar incelendiğinde CIR tipinden bir QoS tanımının ortalama işleme gecikmesini arttırması nedeniyle düzenli kuyruklamanın yapılamadığı ve paket kaybının yüksek olduğu 500 Kbps değerinde ortalama gecikmeyi bir miktar arttırdığı gözlenmektedir. Tüm trafiklerde bu durumu gözlenmesi CIR tipinden bir QoS tanımının bandgenişliğinin düzenli kuyruklama için yeterli olduğu ve büyük bir darboğazın yaşanmadığı durumlarda gecikmeyi azaltma yönünde etki ettiği anlamına gelmektedir. FTP ve UDP trafiklerinde 1 Mbps değerinde de gecikmenin QoS yapıldığında arttığı gözlenmektedir. Bunun da anlamı zaten kısıtlı olan bandgenişliğinin CIR tanımı gereği VoIP trafiğine aktarılmasıdır. Zira VoIP trafiğinde bu bandgenişliği için gecikmenin azaldığı gözlenmektedir. Sonuç olarak CIR tipinden bir DiffServ tanımı düzenli kuyruklamanın yapılabildiği durumlarda atanan CIR değerine bağlı olarak gecikmenin azalması yönünde olumlu etki yapmaktadır.

Seğirtim QoS tanımlarımızın olumlu etkisinin en net gözlenebildiği parametredir. Herbir trafik sınıfı için ayrı RED kuyruklarının oluşturulması sayesinde paketlerin gecikmeleri arasındaki farklılık azalmakta ve gecikme değerinden bağımsız olarak daha düzenli bir

aktarım yapılmaktadır. Yüksek bandgenişliklerine çıkıldığında QoS'un seğirtim üzerindeki etkisi azalmaktadır çünkü QoS olmaksızın gerçeklenen MPLS trafiğinde de zaten seğirtim değeri gecikme ve paket kaybı da düşük olduğu için 0'a yakın değerlerde seyretmektedir. Sonuçlardan net olarak görülebileceği gibi CIR tipinden bir DiffServ tanımı seğirtimin azalması yönünde belirgin bir olumlu etkide bulunmaktadır.

9. SONUÇ

İnternet geçtiğimiz on yıl içerisinde ilerleyen teknolojinin sonucu olarak büyük değişikliklere uğramıştır. Internetin hızla yaygınlaşması ve kullanıcı sayısının artması servis sağlayıcıları çesitli arayışlara itmiş; artan bandgenişliği ve hız ihtiyacını karşılamak için ISP'ler yüksek performanslı anahtarlara ve yönlendiricilere ihtiyaç duymaya başlamışlardır. Artan rota sayısı yönlendirme tablolarının şişmesine ve hali hazırdaki yönlendiricilerin performanslarının yetersiz kalmasına neden olmuş, dolayısıyla ISP'ler ciddi anlamda bir performans ve ölçekleme problemi ile karşı karşıya kalmışlardır.

MPLS teknoljisinin hızla yaygınlaşarak standardlaşma yoluna girmesinin birçok nedeni vardır. Bunun en önemli nedenleri anahtarlama hızında yönlendirmeye olan ihtiyaç ve yönlendirici maliyetlerinin uygun fiyat avantajından tasarım amaçlı olarak faydalanabilme isteğidir.

MPLS'in hızla yaygınlaşmasında en önemli etkenlerden biri de o ana kadar kullanılmakta olan iletim ve yönlendirme tekniklerinin çok yaygınlaşması ve ortaya çıkan yeni ihtiyaçlar doğrultusunda iletim mekanizmalarının değiştirilmesinin oldukça karmaşık ve zorlu bir iş olmasıdır. MPLS teknolojisinin en çekici yanlarından biri iletim algoritmasının (etiket değiştirme) oldukça basit olması ve yeni ihtiyaçlar doğrultusunda üzerinde değişiklik yapmayı gerektirmeden yeniliklere olanak vermesidir. Çok sayıda yeni kontrol modülü anahtarlama sürecini etkilemeyecek şekilde ayni iletim algoritması üzerinde desteklenebilir. Yeni bir yönlendirme fonksiyonuna ihtiyaç duyulduğunda iletim algoritmasının donanım ya da yazılım üzerine yerleştirilerek değişime ihtiyaç duymaksızın desteklenmesi mümkün olmaktadır. En basit örnek olarak IPv4'ten IPv6'ya geçişte iletim algoritması üzerinde bir değişikliğe gitmeye gerek yoktur.

Etiket anahtarlama için kullanılan LSR cihazlarının gerçeklenmesi sürecine baktığımızda yönlendiriciler onlarca protokolü, değişik bağlantı hız ve tiplerini desteklediğini, buna karşın anahtarların çok basit bir iletim mekanizması ile çalıştığını görmekteyiz.

Performans açısından baktığımızda anahtarlar, birim zamanda iletilen bit ya da paket sayısı açısından ya da toplam bandgenişliği açısından ve fiyat/performans değerlendirmesinde yönlendiricilerin önünde gelmektedir. Bunları değerlendirdiğimizde karşımıza yönlendiricinin IP paketlerini iletme işini gerçekleştiren ancak anahtar gibi çalışan bir cihazın ihtiyacı çıkmaktadır. Yani fiyat/performans kriterleri açısından bir anahtarı karşılayan, fonksiyonel olarak yönlendirici gibi çalışan cihazlara ihtiyaç duyulmaktadır. İşte etiket anahlarlama ve yönlendirme fonksiyonunu birleştiren LSR'lar bu ihtiyacı karşılamak üzere tasarlanmışlardır.

İlk ortaya çıktığı zamanlarda genel inanış ATM teknolojisinin baskın teknoloji olarak IP'nin yerini alacağı yönünde idi ancak geçen zaman IP'nin oturmuş protokol yapısının ATM ağlarında da kullanılmaya devam ettiğini ve ATM ağlarının ağırlıklı olarak IP paketlerini taşımaya devam ettiğini göstermiştir. Bu tip ağlarda temel mantık ATM ağının internetwork haberleşme için çekirdekte yüksek hızlı bağlantı sağlaması ve sanal devrelerle ATM anahtara bağlı IP ağlarının yerelde IP datagram iletimini devam ettirmesidir. Bu yöntemde IP paketlerinin ATM omurgaya girerken hücrelere çevrilmesi ve sanal devre kurulumunda kaynak rezervasyonu yapılması, sistemin performansını düşürmektedir. Dolayısıyla bu konuda yeni bir yaklaşım arayışı ortaya çıkmıştır.

Buna alternatif çözüm ise etiket anahtarlamadır. Etiket anahtarlama ile yönlendiriciler IP yönlendirme yapabilen LSR'lar üzerinden birbirleriyle sanal devre kurmaksızın haberleşebilmektedir. Böylece sisteme yeni bir yönlendirici eklendiğinde sadece LSR'lardan bir tanesine bağlanması yeterli olacaktır. Tam-bağlı yapıya olan ihtiyaç ortadan kalktığı için komşuluk yalnızca LSR ile kurulduğu için komşuluk sayısı artmayacak, diğer yönlendirilerin yönlendirme tabloları gereksiz yere şişmeyecektir.

Tezimiz kapsamında detaylı olarak incelediğimiz gibi, MPLS teknolojisi getirdiği yeni yaklaşımlar ve avantajları ile dikkat çeken bir teknoloji olarak dikkat çekmektedir. Halihazırdaki IP yönlendirme mimarisindeki ihtiyaçları karşılaması, yönlendiricilerin yüksek performans/hız sağlaması, IP over ATM mimarisindeki karmaşıklığı ve problemleri ortadan kaldırması, ölçeklenebilirlik problemini aşması, getirdiği etiket yığını yapısıyla VPN teknolojisini desteklemesi, IP QoS özelliklerini MPLS omurgası üzerinden taşımayı sağlaması, 7. bölümde gösterdiğimiz MPLS'in IP üzerindeki

üstünlükleri ve 8. bölümde gösterdiğimiz QoS tanımlarının paket kaybı, gecikme ve seğirtim üzerindeki olumlu etkileri ortaya nedeniyle MPLS büyük kurumlar ile servis sağlayıcı omurgalarında giderek yaygınlaşmaktadır.

Özellikle günümüzde kurumların ve şirketlerin WAN üzerinden veri, ses ve görüntü haberleşmesi sağlamak için yatırımlarını arttırması, bu aşamada servis sağlayıcıların bu trafikleri yüksek performanslı, uçlardaki sınır yönlendiricilerinde belirlenen servis kalitesini destekleyerek ve özellikle VPN teknolojilerini kullanarak kendi omurgalarından güvenli olarak taşımaları gerekmektedir. Aynı şekilde çok sayıda uzak bağlantı noktası bulunan devlet kurumlarında da paketlerin güvenli ve birimlerden gelen trafiklerin birbirinden soyutlanması şeklinde taşınması için yoğun olarak MPLS çalışmaları sürdürülebilmektedir. Teknolojideki ve sektördeki gelişmeler MPLS teknolojisinin MPLS/VPN uygulamalarıyla yüksek performanslı omurga anahtarlamada bir standart olarak kullanılmaya başlanacağını göstermektedir. Önümüzdeki yıllarda bu konuda yeni gelişmelerin olacağı, yeni tekniklerin bulunacağı göz önüne alınırsa MPLS/VPN konusu akademik açıdan da önemli bir araştırma alanı oluşturmaya devam edecektir.

KAYNAKLAR

[1] Alwayn, V.; *Advanced MPLS Design and Implementation;* Cisco Press, 2002, ABD.

[2] Davie, B.S., & Rekhter, Y.; *MPLS: Technology and Applications*; Morgan Kaufmann, Mayıs 2000.

[3] Doyle, J. & Carroll, J.D.; *Routing TCP/IP Vol-II;* Cisco Press, 2001, ABD.

[4] Hutnik, S. & Satterlee, M.; *All-in-One Cisco CCIE Lab Study Guide;* McGraw-Hill, 2001, pp:1165-1204

[5] Pepelnjak, I. & Guichard, J.; *MPLS and VPN Architectures;* Cisco Press, 2002, ABD.

[6] Comer, E.D; *Computer Networks and Internets;* Prentice-Hall, 1999, New Jersey

[7] Tanenbaum, A.S.; *Computer Networks 3rd Edt.;* Prentice-Hall, 2001, New Delhi

[8] Vegesna, S.; *IP Quality of Service;* Cisco Press, 2001, ABD.

[9] Fineberg, V.; *QoS Support in MPLS Networks;* MPLS Forum / Frame Relay Forum, MPLS / Frame Relay Allience White Paper, Mayıs 2003, Illinois, ABD.

[10] Lee, H., Hwang, J., Kang, B. & Jun, K.; *End-To-End Qos Architecture for VPNs: MPLS VPN Deployment in a Backbone Network;* 2000 International Workshop on Parallel Processing, Ağustos 2000, Kanada.

[11] Rouhana, N. & Horlait, Eric.; *Differentiated Services and Integrated Services Use of MPLS;* IEEE Computer Society, July 2000, France, p.194.

[12] Xiao, X.; *Providing Quality of Service in the Internet;* Doktora Tezi, Department of Computer Science and Engineering, Michigan State Universitesi, 2000, ABD.

[13] Cisco IOS Quality of Service Solutions Command Reference, Release 12.1, Commands: queue-limit -- set ip precedence http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_command_reference_chapter09186a0080080786.html

[14] Cisco IOS Software Releases 12.1T, MPLS Class of Service Enhancements
http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a0080080410.html

[15] Configuring a Basic MPLS VPN
http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_example09186a00800a6c11.shtml

[16] Configuring MPLS Basic VPN with RIP on Customer Side
http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_example09186a008009445c.shtml

[17] IP Tunneling (Generic Routing Encapsulation)
http://www.qnx.com/developers/docs/momentics621_docs/neutrino/technotes/gre.html

[18] RFC 1577, Classical IP and ARP over ATM
http://www.ietf.org/rfc/rfc1577.txt?number=1577

[19] RFC 2547; BGP/MPLS VPNs
http://www.ietf.org/rfc/rfc2547.txt?number=2547

[20] RFC 1953; Ipsilon Flow Management Protocol Specification for IPv4
http://www.ietf.org/rfc/rfc1953.txt?number=1953

[21] VPN Tunnels - GRE Protocol 47 Packet Description and Use
http://support.microsoft.com/?kbid=241251

[22] Windows NT 4.0: Virtual Private Networking
http://www.microsoft.com/technet/archive/winntas/deploy/vpntwk.mspx

[23] NS by Example, Worcester Polytechnic Institute, Computer Science
http://nile.wpi.edu/NS

[24] NS Using Integrator with Flow Monitoring
http://www.isi.edu/nsnam/archive/ns-users/webarch/2001/msg03842.html

[25] The Network Simulator – NS-2
http://www.isi.edu/nsnam/ns/

[26] The NS/MPLS DiffServ Patch
http://www.eeng.dcu.ie/~murphys/ns-work/mpls-diffserv/

EK-A MPLS/VPN KONFİGÜRASYONLARI

Bölüm 7.3'te belirtilen sistemde yer alan tüm cihazlara ait konfigürasyonlar aşağıda verilmiştir. Kofigürasyonlarda CE-PE bağlantılarında RIP, PE'ler arasında ise dahili yönlendirme protokolü olarak OSPF ve etiket dağıtımı için BGP konfigürasyonları yapılmıştır. Sistemde ik adet VRF tanımlıdır. VRF1 CE2611-ALT ile CE2611-UST arasında PE3640-LAB ve PE3640-COMMS yönlendirici üzerinden geçmektedir. VRF2 ise CE2611-LAB ile CE1760 yönlendiricileri arasında PE3640-LAB ile PE-3725 üzerinden çalışmaktadır. [1][4][13][14][15][16]

A.1 PE Yönlendiricilerinin Konfigürasyonları

A.1.1 PE3640-LAB

```
Current configuration : 2630 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE3640-LAB
!
boot-start-marker
boot-end-marker
!
logging buffered 10000 debugging
no logging console
!
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
!
ip vrf vpn1
 rd 1:100
 route-target export 1:100
 route-target import 1:100
!
ip vrf vpn2
 rd 1:200
 route-target export 1:200
```

```
 route-target import 1:200
!
ip cef
!
!
interface Loopback0
 ip address 100.0.0.1 255.255.255.255
 ip ospf network point-to-point
!
interface Serial1/0
 description CONNECTION TO 3725
 ip address 10.0.0.1 255.255.255.0
 tag-switching ip
 serial restart-delay 0
 no fair-queue
!
interface Serial1/1
 description CONNECTION TO COMMS-3640
 ip address 12.0.0.1 255.255.255.0
 tag-switching ip
 serial restart-delay 0
 no fair-queue
!
interface Serial1/2
 description CONNECTION TO 2611-ALT
 ip vrf forwarding vpn1
 ip address 20.0.0.1 255.255.255.0
 serial restart-delay 0
 clockrate 1344000
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Ethernet2/0
 ip vrf forwarding vpn2
 ip address 21.0.0.1 255.255.255.0
 full-duplex
!
interface Ethernet2/1
 no ip address
 shutdown
 half-duplex
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.1 0.0.0.0 area 0
 network 12.0.0.1 0.0.0.0 area 0
 network 100.0.0.1 0.0.0.0 area 0
!
router rip
 version 2
 !
 address-family ipv4 vrf vpn2
 version 2
 redistribute bgp 1 metric 0
```

```
 network 21.0.0.0
 network 130.0.0.0
 no auto-summary
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 version 2
 redistribute bgp 1 metric 0
 network 20.0.0.0
 network 130.0.0.0
 no auto-summary
 exit-address-family
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 110.0.0.1 remote-as 1
 neighbor 110.0.0.1 update-source Loopback0
 neighbor 120.0.0.1 remote-as 1
 neighbor 120.0.0.1 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 110.0.0.1 activate
 neighbor 110.0.0.1 send-community extended
 neighbor 120.0.0.1 activate
 neighbor 120.0.0.1 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf vpn2
 redistribute connected
 redistribute static
 redistribute rip
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 redistribute connected
 redistribute static
 redistribute rip
 no auto-summary
 no synchronization
 exit-address-family
!
ip http server
no ip http secure-server
ip classless
!
voice-port 0/1/0
!
voice-port 0/1/1
!
line con 0
line aux 0
line vty 0 4
 login
```

```
!
end
```

A.1.2 PE3725

```
Current configuration : 3029 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 3725
!
boot system flash:c3725-jk9o3s-mz.123-6a.bin
!
ip subnet-zero
!
!
!
ip cef
no ip domain lookup
ip vrf vpn1
 rd 1:100
 route-target export 1:100
 route-target import 1:100
!
ip vrf vpn2
 rd 1:200
 route-target export 1:200
 route-target import 1:200
!
no ftp-server write-enable
!
interface Loopback0
 ip address 120.0.0.1 255.255.255.255
!
interface FastEthernet0/0
 ip vrf forwarding vpn2
 ip address 31.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 no fair-queue
 clockrate 2000000
!
interface FastEthernet0/1
 ip vrf forwarding vpn2
 ip address 10.51.34.1 255.255.255.0
 shutdown
 duplex auto
 speed auto
!
```

```
interface Serial0/1
 no ip address
 shutdown
 clockrate 2000000
!
interface Serial0/2
 ip address 10.0.0.2 255.255.255.0
 clockrate 1000000
!
interface Serial0/3
 ip address 11.0.0.2 255.255.255.0
 clockrate 128000
!
interface FastEthernet1/0
 no ip address
 shutdown
!
interface FastEthernet1/1
 no ip address
 shutdown
!
interface FastEthernet1/2
 no ip address
 shutdown
!
interface FastEthernet1/3
 no ip address
 shutdown
!
interface FastEthernet1/4
 no ip address
 shutdown
!
interface FastEthernet1/5
 no ip address
 shutdown
!
interface FastEthernet1/6
 no ip address
 shutdown
!
interface FastEthernet1/7
 no ip address
 shutdown
!
interface FastEthernet1/8
 no ip address
 shutdown
!
interface FastEthernet1/9
 no ip address
 shutdown
!
interface FastEthernet1/10
 no ip address
 shutdown
!
```

```
interface FastEthernet1/11
 no ip address
 shutdown
!
interface FastEthernet1/12
 no ip address
 shutdown
!
interface FastEthernet1/13
 no ip address
 shutdown
!
interface FastEthernet1/14
 no ip address
 shutdown
!
interface FastEthernet1/15
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.2 0.0.0.0 area 0
 network 11.0.0.2 0.0.0.0 area 0
 network 120.0.0.1 0.0.0.0 area 0
!
router rip
 version 2
 !
 address-family ipv4 vrf vpn2
 version 2
 redistribute bgp 1
 network 31.0.0.0
 no auto-summary
 exit-address-family
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 100.0.0.1 remote-as 1
 neighbor 100.0.0.1 update-source Loopback0
 neighbor 110.0.0.1 remote-as 1
 neighbor 110.0.0.1 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 100.0.0.1 activate
 neighbor 100.0.0.1 send-community extended
 neighbor 110.0.0.1 activate
 neighbor 110.0.0.1 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf vpn2
```

```
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
ip route vrf vpn2 31.0.0.0 255.255.255.0 31.0.0.2
!
ip http server
!
!
line con 0
line aux 0
line vty 0 4
 login
!
!
end
```

A.1.3 PE3640-COMMS

```
commslab-3640a#sh run
Building configuration...

Current configuration : 2179 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname commslab-3640a
!
logging buffered 10000 debugging
no logging console
!
ip subnet-zero
!
!
no ip domain-lookup
!
!
ip vrf vpn1
 rd 1:100
 route-target export 1:100
 route-target import 1:100
ip cef
!
```

```
call rsvp-sync
!
!
interface Loopback0
 ip address 110.0.0.1 255.255.255.255
!
interface Loopback100
 ip vrf forwarding vpn1
 no ip address
 shutdown
!
interface Ethernet0/0
 no ip address
 shutdown
 half-duplex
!
interface Serial0/0
 ip address 11.0.0.1 255.255.255.0
 tag-switching ip
 no fair-queue
!
interface Ethernet0/1
 no ip address
 shutdown
 half-duplex
!
interface Serial0/1
 ip address 12.0.0.2 255.255.255.0
 tag-switching ip
 no fair-queue
 clockrate 1000000
!
interface Ethernet1/0
 no ip address
 shutdown
 half-duplex
!
interface Serial1/0
 ip vrf forwarding vpn1
 ip address 30.0.0.1 255.255.255.0
!
interface Ethernet1/1
 no ip address
 shutdown
 half-duplex
!
interface Serial1/1
 no ip address
 shutdown
 tag-switching ip
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
```

```
router ospf 1
 log-adjacency-changes
 network 11.0.0.1 0.0.0.0 area 0
 network 12.0.0.2 0.0.0.0 area 0
 network 110.0.0.1 0.0.0.0 area 0
!
router rip
 version 2
 !
 address-family ipv4 vrf vpn1
 version 2
 redistribute bgp 1 metric 0
 network 30.0.0.0
 no auto-summary
 exit-address-family
!
router bgp 1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 100.0.0.1 remote-as 1
 neighbor 100.0.0.1 update-source Loopback0
 neighbor 120.0.0.1 remote-as 1
 neighbor 120.0.0.1 update-source Loopback0
 !
 address-family ipv4 vrf vpn1
 redistribute connected
 redistribute static
 redistribute rip
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 100.0.0.1 activate
 neighbor 100.0.0.1 send-community extended
 neighbor 120.0.0.1 activate
 neighbor 120.0.0.1 send-community extended
 exit-address-family
!
ip classless
ip http server
!
voice-port 3/1/0
!
voice-port 3/1/1
!
dial-peer cor custom
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

A.2 CE Yönlendiricilerinin Konfigürasyonları

A.2.1 CE2611-ALT

```
Current configuration : 958 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2611-ALT
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
ip cef
!
ip audit po max-events 100
!
!
interface Loopback0
 ip address 130.0.0.1 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.1.2 255.255.255.0
 half-duplex
!
interface Serial0/0
 ip address 20.0.0.2 255.255.255.0
 no fair-queue
!
interface Serial0/1
 no ip address
 shutdown
!
interface Serial0/2
 no ip address
 shutdown
!
router rip
 version 2
 network 20.0.0.0
 network 130.0.0.0
!
ip http server
no ip http secure-server
ip classless
!
voice-port 1/0/0
!
voice-port 1/0/1
!
```

```
!
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

A.2.2 CE2611-UST

```
Current configuration : 854 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2611-UST
!
boot-start-marker
boot-end-marker
!
!
memory-size iomem 10
no aaa new-model
ip subnet-zero
ip cef
!
!
!
ip audit po max-events 100
!
!
interface Loopback0
 ip address 140.0.0.1 255.255.255.255
!
interface Ethernet0/0
 no ip address
 shutdown
 half-duplex
!
interface Serial0/0
 ip address 30.0.0.2 255.255.255.0
 clockrate 128000
!
interface Ethernet0/1
 no ip address
 shutdown
 half-duplex
!
interface Serial0/1
 no ip address
 shutdown
 no fair-queue
```

```
!
router rip
 version 2
 network 30.0.0.0
 network 140.0.0.0
!
ip http server
no ip http secure-server
ip classless
!
!
voice-port 1/0/0
!
voice-port 1/0/1
!
line con 0
line aux 0
line vty 0 4
 login
!
!
!
end
```

A.2.3 CE2611-LAB

```
Current configuration : 786 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2611CE-LAB
!
ip subnet-zero
!
ip cef
call rsvp-sync
!
!
interface Loopback0
 ip address 150.0.0.1 255.255.255.255
!
interface Ethernet0/0
 ip address 21.0.0.2 255.255.255.0
 full-duplex
!
interface Serial0/0
 no ip address
 shutdown
 no fair-queue
!
interface Ethernet0/1
 no ip address
 shutdown
```

```
 half-duplex
!
interface Serial0/1
 no ip address
 shutdown
!
router rip
 version 2
 network 21.0.0.0
 network 150.0.0.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 21.0.0.1
ip http server
ip pim bidir-enable
!
voice-port 1/0/0
!
voice-port 1/0/1
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

A.2.4 CE1760

```
Current configuration : 932 bytes
!
! Last configuration change at 21:13:26 UTC Sat Mar 20 2004
! NVRAM config last updated at 21:15:43 UTC Sat Mar 20 2004
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 1760CE
!
boot-start-marker
boot-end-marker
!
!
tdm clock bri-auto
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
```

```
mmi snmp-timeout 180
voice-card 2
!
voice-card 3
!
no aaa new-model
ip subnet-zero
!
!
!
ip cef
!
!
!
interface Loopback0
 ip address 160.0.0.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 31.0.0.2 255.255.255.0
 speed auto
!
interface BRI3/0
 no ip address
!
interface BRI3/1
 no ip address
!
ip classless
ip route 0.0.0.0 0.0.0.0 31.0.0.1
no ip http server
!
!
!
!
voice-port 2/0
!
voice-port 2/1
!
voice-port 2/2
!
voice-port 2/3
!
voice-port 3/0
!
voice-port 3/1
!
!
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

ÖZGEÇMİŞ

Bilgisayar Mühendisi, Özgür Savaş, 14.02.1980 Burdur doğumludur. İlk ve ortaokulu Burdur'da, liseyi 1998 yılında Mersin Fen Lisesi'nde tamamlamıştır. 2002 yılında İstanbul Teknik Üniversitesi Elektrik-Elektronik Fakültesi, Bilgisayar Mühendisliği bölümünden, danışmanlığı Prof. Dr. Emre Harmancı tarafından yürütülmüş olan *"ADSL ağlarında hata düzeltme; Reed-Solomon kodları"* adlı teziyle mezun olmuştur.

Mühendis ünvanı yanı sıra, tüm dünyada kabul gören, *Cisco Certified Networking Professional* (CCNP-2003), *Cisco Certified Design Professional* (CCDP-2003), *Cisco Certified Networking Assocciate* (CCNA-2002), *Cisco Certified Design Assocciate* (CCDA-2002) ve *Cisco Certified Sales Expert* (CSE-2004) uzmanlık sertifika ve dereceleri sahibidir.

Biri basılmış telif, diğeri baskı aşamasında olan çeviri olmak üzere iki kitabı mevcuttur. Telif kitabı *Aydınlanma 1923 Devrimi ve 21. Yüzyılda Kemalizm,* 2004 Eylül ayında altı yazarlı ve 368 sayfa olmak üzere Toplumsal Dönüşüm Yayınlarından basılmıştır. Orjinali 2003 yılında Cisco Press'ten çıkmış olan *IT Essentials – Network Operating Systems Companion Guide* isimli 856 sayfalık çeviri kitabı *Bilişim Teknolojilerinin Temelleri II – Ağ İşletim Sistemleri Kılavuz Kitabı* adıyla Eylül 2005'te Sistem Yayıncılık'tan çıkacaktır. Kitaplarının yanı sıra, bilim felsefesi, bilgi teknolojileri ve ulusal politika üzerine çeşitli periyodik yayınlarda yayınlanmış çok sayıda makalesi bulunmaktadır. Halen Cisco Systems, Inc. şirketinde *Ağ Teknolojileri Uzmanı* olarak çalışmaktadır.