MPLS-TE-FRR ve QoS KULLANARAK VERİ İLETİM OPTİMİZASYONU

Murat OĞUL

YÜKSEK LİSANS TEZİ

ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

MART 2010

ANKARA

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

.....

Murat OĞUL

MPLS-TE-FRR ve QoS KULLANARAK VERİ İLETİM OPTİMİZASYONU

(Yüksek Lisans Tezi)

Murat OĞUL

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
Mart 2010

ÖZET

IP'nin (İnternet Protokolü-Internet Protocol) gittikçe yaygınlaştığı ve birçok kritik verinin IP ile taşındığı günümüzde, veri kayıplarının azaltılması da önemli odak alanlarından birisi olmuştur. Bu projede, IP paket anahtarlamalı ağlarda, hat yoğunlukları ve hat problemlerinden dolayı kritik veri kayıplarının en aza indirilmesi amacıyla inceleme ve ölçümler yapılmıştır. Ölçümlerde, geleneksel yönlendirme protokollerinden OSPF (Açık En Kısa Yol İlk-Open Shortest Path First) ile etiket anahtarlama teknolojisi MPLS-TE'nin (Çoklu Protokol Etiket Anahtarlama-Trafik Mühendisliği –Multi Protocol Lable Switching-Traffic Engineering) sorun anında sorunsuz hatlara geçme süreleri ve bu süre zarfında kaybedilen veriler karşılaştırılmıştır. Ayrıca hat yoğunluklarında kritik verilerin kaybedilmeden gönderilmesi için testler yapılmıştır. Çalışma sonucunda, kritik veri taşıyan günümüz IP ağlarında bazı protokollerin kullanımının kaçınılmaz olduğu sonucuna varılmış ve kullanımı önerilmiştir.

Bilim Kodu : 905 1.063
Anahtar Kelimeler : Ağ, MPLS-TE, QoS, FRR
Sayfa Adedi : 109
Tez Yöneticisi : Yrd. Doç. Dr. Cem NAKİBOĞLU

OPTIMIZING DATA TRANSPORT BY USING MPLS-TE-FRR and QoS

(M.Sc. Thesis)

Murat OĞUL

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Mart 2010

ABSTRACT

In this project, when using OSPF and MPLS-TE in IP packet switching networks recover time was tested and compared and during that time amount of data lost in case of the link overload and failure. In addition, it's studied to be sent mission critical data without any lost during link overload. As a result of this project, some protocols are advised to be used on the networks that carry mission critical data.

Science Code : **905 1.063**
Key Words : **Ağ, MPLS-TE, QoS, FRR**
Page Number :**109**
Adviser : **Yrd. Doç. Dr. Cem NAKİBOĞLU**

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren Hocam Yrd. Doç. Dr. Cem NAKİBOĞLU'na, yardımlarını hiç esirgemeyen hocam Dr. Nursel Akçam ve manevi desteğiyle beni hiçbir zaman yalnız bırakmayıp destekleyen eşim ve çocuklarıma teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	Açıklama
bps	Bit per second
Mbps	Mega bir per second
msn	Milisaniye
sn	Saniye

Kısaltmalar	Açıklama
ADSL	Asynchronous digital subscriber line
AS	Autonomous system
ATM	Asynchronous transfer mode
BA	Behavior aggregate
BGP	Border gateway protocol
CBWFQ	Class-based WFQ
CIR	Committed information rate
CRC	Cyclical redundancy check
DıffServ	Differentiation services
DNS	Domain name system
DSCP	Differentiated services code point
FDDI	Fiber distributed data interface
FEC	Forwarding equivalence class
FIB	Forwarding information base
FIFO	First-in-first-out
FQ	Fair-queuing
FRR	Fast reroute
GSM	Global system for mobile communications
HTTP	Hypertext transfer protocol
HTTPS	Hypertext transfer protocol secure

Kısaltmalar	Açıklama
ICMP	Internet control message protocol
IETF	Internet Engineering Task Force
IGP	Interior gateway protocol
IntServ	Integrated service
IP	Internet protocol
IS-IS	Intermediate system to intermediate system
LAN	Local area network
LDP	Label distribution protocol
LER	Label edge router
LFIB	Label forwarding information base
LIB	Label information base
LSP	Label switched path
LSR	Label switch router
MAC	Media access control
MF	Multi-field
MPLS	Multi protocol lable switching
NAT	Network address translation
OSI	Open system interconnection
OSPF	Open shortest path first
PBX	Public branch exchange
PDU	Protocol data unit
PIR	Peak information rate
PQ	Priority queuing
PSTN	Public switch telephone network
QoS	Quality of service
RED	Random early detect
RFC	Request for comment
RIB	Routing information base
RIP	Router information protocol
RRO	Record route object

Kısaltmalar	Açıklama
RSVP	Resource reservation protocol
SMTP	Simple mail transfer protocol
SSH	Secure shell
TE	Traffic engineering
TOS	Type of service
TTL	Time to live
UDP	User datagram protocol
WAN	Wide area network
WFQ	Weighted fair queuing
WRED	Weighted random early detect
WRR	Weighted round robin

1. GİRİŞ

Günümüzde telekomünikasyon teknolojisi inanılmaz bir hızla gelişmektedir. Telekomünikasyonun tarihi gelişim süreci incelendiğinde, yakın tarihlere kadar iletişim gelişim hızı lineer bir seyir göstermekte iken günümüzde eksponansiyel bir gelişim göstermektedir. İnternetin hayatımıza girdiği ilk yıllarda 56Kbps'lik analog hatlarla verilen internet imkânından, bir üniversitenin tüm öğrencileri yararlanmaya çalışıyordu ve bu bizim için çok orijinal bir gelişmeydi. Şimdilerde analog hatlardan değil mobil telefonlardan bile Mbps'ler düzeyinde erişim hızları sunulmaktadır. İletişim teknolojilerinin bu denli gelişim göstermesi beraberinde hızlarının bu denli arttığı günümüz ağlarında birçok şirket ses için kullandıkları PBX(Public Branch Exchange) santraller yerine ses, video ve normal verileri aynı ağ ortamından taşımayı maliyet ve esneklik açısından avantajlı bulmuşlar ve uygulamaya başlamışlardır. Bu durumda birçok farklı veriyi aynı fiziksel ortamlardan taşımada kullanılan IP ağlarının devamlılığı, sorun anında alternatif yolların tespiti ve veri kayıplarının minimize edilmesi kritik hale gelmiştir.

Geleneksel yönlendirme protokollerinde (OSPF, BGP… vb) sorun anında alternatif yolların bulunması süresi uzun olduğundan bu süre zarfında ciddi veri ve buna bağlı itibar kaybı yaşanmakta iken, günümüzde MPLS-TE-FRR teknolojisi sayesinde bu sorun ciddi oranda azaltılmıştır. Ayrıca, kritik veri ile normal verileri aynı anda taşıyan ağlarda değişik nedenlerle ortaya çıkan hat sıkışmalarında kritik verilerin atılmadan iletimi önem kazanmıştır.

Bu çalışmada, kritik veri taşıyan IP ağlarında meydana gelen hat problemlerinden dolayı trafiğin alternatif yollara geçiş süresi, geleneksel yönlendirme protokollerinden OSPF ile ve MPLS-TE-FRR ile laboratuar ortamında test edilerek karşılaştırıldı. Bununla beraber, hattın kapasitesini aşan durumlarda, kritik verilerin en az etkilenmesi amacıyla servis kalitesi testleri yapılarak günümüzde kritik veri taşıyan ağlarda uygulanmasında fayda görülen protokollerin kullanımı önerildi.

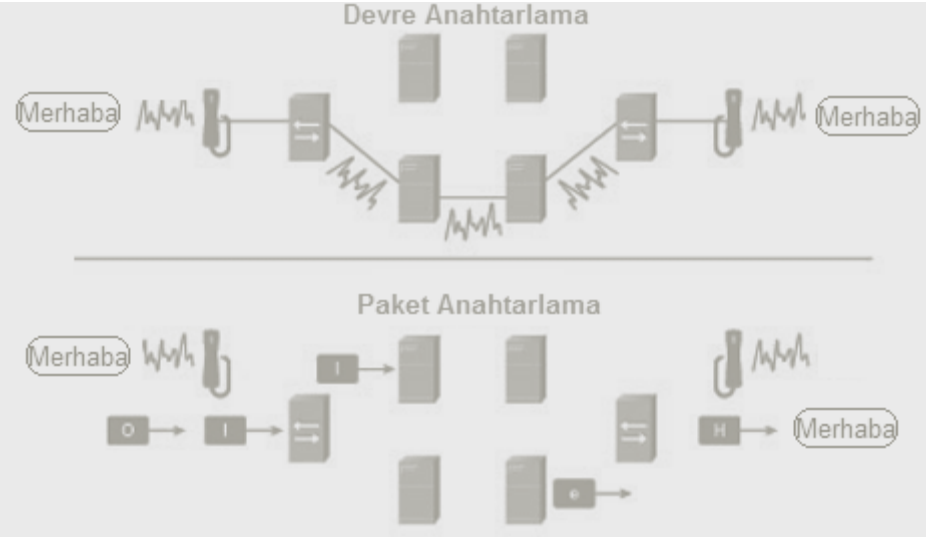
2. BİLGİSAYAR AĞLARI VE TCP/IP

TCP/IP'nin (Transmission Control Protocol/Internet Protocol) temelleri 1970'lerin başında Amerikan Savunma Bakanlığı'nca yürütülen paket anahtarlamalı ağ deneylerine kadar uzanır. TCP/IP'nin geliştirilmesinde, ABD'deki bilgisayarların bir felaket durumunda bile birbirleriyle iletişimini devam ettirebilmeleri amaçlanıyordu [1]. TCP/IP'nin vazgeçilmez olması paket anahtarlama teknolojisine dayanan esnek yapısından kaynaklanır [2].

IP'nin esnek yapısı ve yaygın kullanımından dolayı çıktığı ilk günden günümüze kadar olan ilerlemesi baş döndürücüdür. Geçmişte sadece devre anahtarlamalı sistemlerle çalışabilen birçok uygulama bugün IP üzerinden çalıştırılmaktadır. Öyle ki, geçmişte sadece devre anahtarlamalı altyapılarda çalışan telefon görüşmeleri bile bugün yoğun olarak IP üzerinden taşınmakta ve ciddi maliyet avantajı ile beraber IP'nin üstün meziyetlerinden yararlanılmaktadır.

2.1. Devre Anahtarlama ve Paket Anahtarlama (Circuit Switching/Packet Switching)

Devre anahtarlamada iletişimin gerçekleşmesi için bir adet bağlantı karşılıklı olarak kurulur ve bu çift yönlü bağlantı "devre" olarak adlandırılır. Devre anahtarlamayı en iyi klasik telefon (PSTN- Public Switch Telephone Network) bağlantıları ifade eder. Bir telefon görüşmesinde taraflardan birinin aramayı başlatması ve sonrasında karşı taraftaki diğer kişinin çalan telefonu kaldırması ile devre iki taraf arasında kurulmuş olur ve çift yönlü çalışır. Bir tarafın telefonu kapatması ile devre anahtarlamalı iletişim kesilir. Paket anahtarlamada ise veriler belirli protokoller yardımıyla paketlere bölünür ve devrenin kurulması beklenmeksizin gönderilmeye başlanır. Devre anahtarlamada paketlerin gönderileceği yol önceden belirlenmesine karşın, Şekil 2.1'de görüldüğü gibi paket anahtarlamada böyle bir zorunluluk bulunmamaktadır.



Şekil 2.1. Devre anahtarlama, paket anahtarlama yapıları

Günümüzde elbette devre anahtarlamalı yapılar bulunmaktadır, ancak paket anahtarlamalı ağlar ve bunlardan en büyüğü olan internet o kadar büyümüştür ki neredeyse her tür iletişim bir paket anahtarlamalı yapı olan internet üzerinden gerçekleşmektedir. İnternet üzerinden, ucuz uzak nokta ses hizmeti veren servis sağlayıcı şirketlerden tutun da GSM (Global System Mobile) operatörlerine kadar birçok şirket önceden devre anahtarlamalı yapılar üzerinden verilen servisleri artık paket anahtarlamalı yapılar üzerinden müşterilerine sunmaktadır.

IP, MPLS (Multi Protocol Lable Switching) ve ATM (Asynchronous Transmission Mode) paket anahtarlamalı ağlara örnek olurken, devre anahtarlamaya verilebilecek en iyi örnek PSTN hizmetidir.

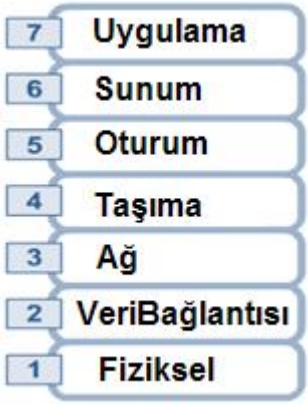
2.2. OSI Modeli ve Paket Zarflama

Paket anahtarlamalı ağların günümüzde en önemli bileşeni şüphesiz IP'dir. Paket anahtarlama ve IP'yi daha iyi anlamak için OSI (Open Standard International) referans modelini bilmek gerekir.

Ağ modellerinde, fonksiyonları sadeleştirmek ve anlaşılır kılmak amacıyla katmanlar kullanır [2]. OSI referans modeli ağ iletişimi için en temel modeldir. Başka bir

deyişle OSI referans modeli bilginin ağ üzerinde nasıl seyahat ettiğini anlamamızı sağlayacak bir iskelettir.

Şekil 2.2'de görülen OSI referans modelinde her biri farklı ağ fonksiyonunu açıklayan 7 adet katman bulunur. Bu fonksiyonlara ayırma işlemine "katmanlama" adı verilir.

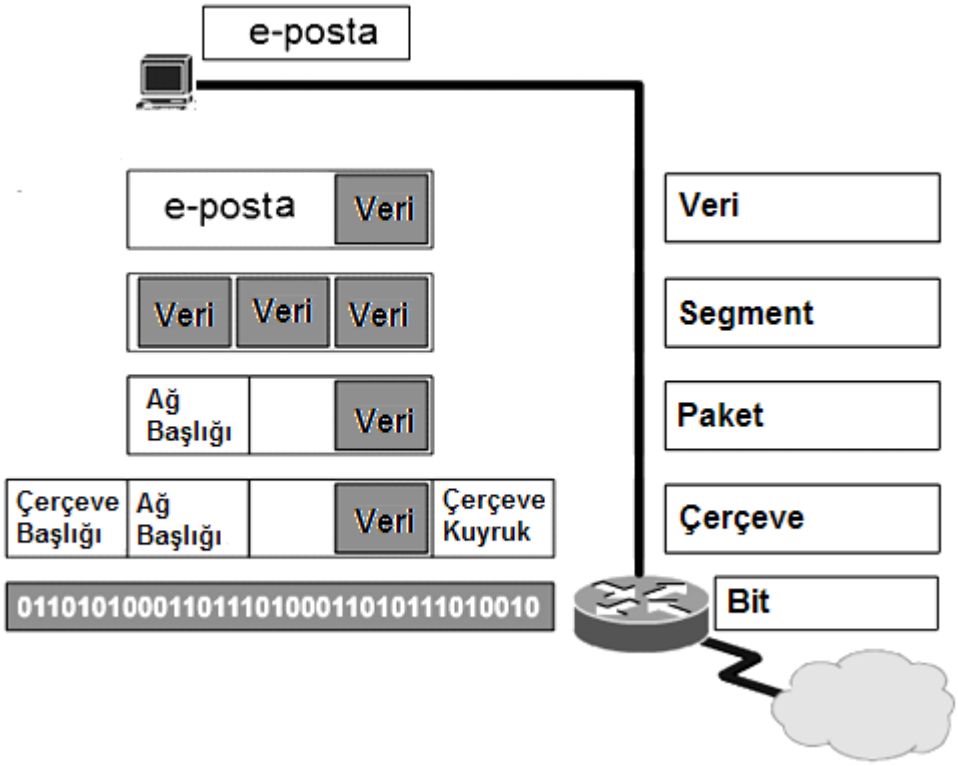


Şekil 2.2. OSI referans modeli katmanları

Katmanlama işleminin sağladığı bazı avantajlar şunlardır:

- Ağ işlemleri daha küçük ve basit anlaşılır parçalara bölünmüş olur [3].
- Bir katmandaki değişikliklerin ve hataların diğer katmanları etkilemesi engellenir.
- Değişik tipteki donanım ve yazılım network elemanlarının birlikte çalışmasını sağlar.
- Network elemanlarını standart hale getirerek çeşitli üreticilere imkân verilmiş olur.

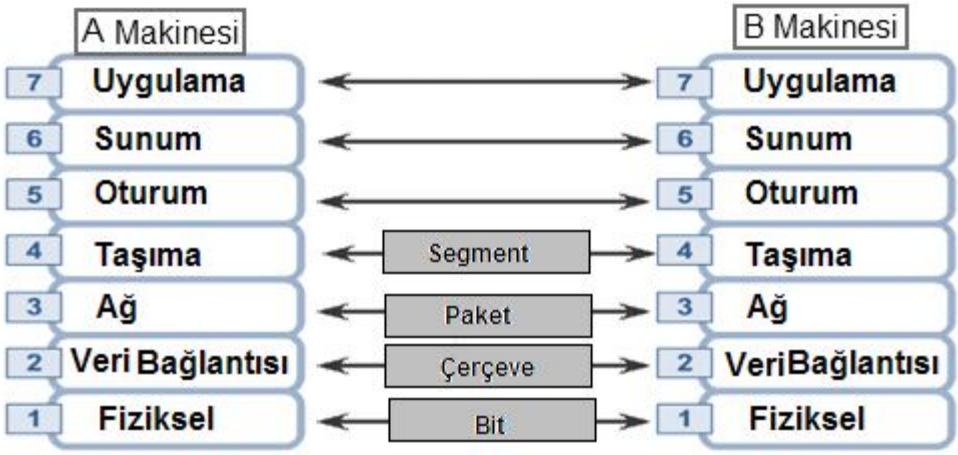
Her katmada yapılan işlem farklı olur ve bir veri kullanıcıdan fiziksel iletim ortamına indirilene kadar değişik evrelerden geçer. Görsel olarak kullanıcı ile iletişimde görünen bir verinin (resim, ses, e-posta… vb) karşı taraftaki bir başka makineye ağ üzerinden gönderilirken geçtiği evreleri Şekil 2.3'te görülmektedir. Verinın bu şekilde geçirdiği evrelere paket zarflama işlemi denmektedir.



Şekil 2.3. Veri paket zarflama işlemi

Verinin paket zarflama sürecinde her katmanda farklı işlemler gerçekleşir. İletim ortamına sadece 1 ve 0'lara karşılık gelen elektrik veya ışık sinyallerinden ibaret ham veri olarak verilir. Paket zarflama işleminde paket her katmanda o katman protokollerinin anlayacağı şekilde düzenlenir [4].

Veri paketlerinin kaynaktan hedefe yolculuğu sırasında kaynak makinedeki OSI modelinin her katmanı, hedef makinede kendi eş katmanıyla konuşur. Bu tip iletişime peer-to-peer iletişim denir. Bu sırada Şekil 2.4'te görüldüğü gibi her katmanın protokolü kendi eş katmanıyla bilgi alışverişinde bulunur. Bu bilgilere protokol veri birimleri (PDU-Protocol Data Units) adı verilir. Özetle kaynaktaki her katman hedefteki eş katmanıyla PDU'lar aracılığıyla konuşur [2].



Şekil 2.4. Peer to peer iletişim

OSI modelinde, her katman kendi üstündeki katmana servis vermekle yükümlüdür. Bu servisi sağlamak için alttaki katman üst katmandan gelen veriyi paket zarflama işleminden geçirir. Bu işlemi açıklayalım. Bir katman, üst katmandan gelen PDU yu veri alanına yerleştirir, kendi protokolüne ait bilgileri (header-başlık, trailer-artbilgi) ekler ve yeni oluşan PDU'yu bir alt katmana gönderir. Bu işlem her katmanda tekrarlanır. Yani veri katmanlar arasında aşağı doğru ilerlerken her katmanda yeni başlık ve artbilgi eklenir. 4.katmandan itibaren PDU'lara özel isimler verilir. 4. katmanda PDU segment, 3.katmanda paket, 2.katmanda ise çerçeve adını alır.

Örneğin, bu bir IP paketi ise üçüncü katmanda, dördüncü katmandan alınan paketin önüne IP bilgileri eklenerek ikinci katmana gönderilir. İkinci katmanda da paketin hangi ikinci katman protokolleri ile gönderileceğine bağlı olarak gerekli bilgiler pakete eklenir. Son olarak, yine paketin birinci katmanda ne şekilde kodlanarak iletim ortamına verileceğine bakılar iletim ortamına verilir.

2.3. LAN ve WAN Kavramları

Yerel ağ olarak tanımlanan LAN (Local Area Network), aynı yapı içindeki sınırlı bir alanda bir birine bağlanmış bilgisayarlardan oluşur. Internet kafeler, şirketlerin lokal ağları LAN'a örnek verilebilir.

Geniş alan ağları diye tanımlanan WAN (Wide Area Network) ise daha çok uzak mesafe bağlantıları ifade eder. Örneğin ADSL modem ile internet bağlantısı, şirketlerin farklı ülkelerde, şehirlerde buluann binalarının birbirlerine bağlantıları, kısaca lokasyon olarak farklı yerlerde bulunan uzak mesafeleri birleştiren ağlara denir. WAN 'da genellikle arada bir veya daha fazla servis sağlayıcı olur ve uzak mesafe bağlantılar bu servis sağlayıcı üzerinden gerçekleşir. Her şirketin kendi kapalı WAN yapısı olabileceği gibi, internet erişim olan noktalardan şirketler veya ev kullanıcıları da en büyük WAN olan internete bağlanırlar.

2.4. Ağ Cihazları

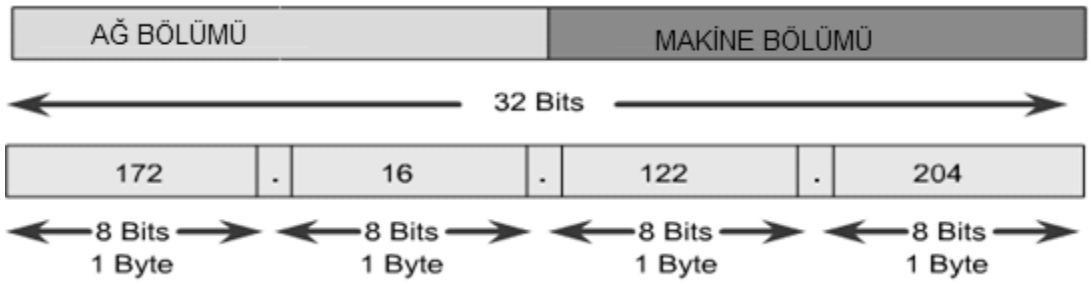
Veri ağlarında birçok cihaz kullanılır. Yönlendiriciler, OSI modelinin üçüncü katmanında çalışırlar. Yani, üçüncü katman bilgilerini baz alarak paketleri yönlendirebilen yönlendiriciler bu yeteneklerinden ötürü Internet'in iskeletini oluştururlar. Yönlendiricilerin temel görevi, gelen paketi incelemek, bu paket için ağ üzerinde en iyi yolu belirlemek ve bu yolu izlemek üzere paketi en uygun portundan dışarı göndermektir. Yönlendiriciler özellikle büyük ağlarda trafiği düzenlemek için kullanılan en önemli cihazlardır. Yönlendiriciler ayrıca birbirinden farklı 2. katman ağlarını (Ethernet, Token-Ring, FDDI gibi) birbirine bağlayarak bunlar arasında geçit görevi görürler. Bir diğer önemli ağ cihazı anahtardır. Anahtarlar da ikinci katman cihazlarıdır. Anahtarların MAC adresine göre bazı kararlar alabilme yetenekleri vardır. Bu yetenekleri sayesinde bir LAN 'ı daha hızlı ve verimli hale getirirler. Anahtarlama işlemi, bir porttan alınan veriyi sadece uygun (gereken) porta yönlendirirken diğer portları meşgul etmemiş olur. Yönlendirici ve anahtar dışında hub, repeater (tekrarlayıcı), modem gibi cihazlar eskiden çok kullanılmasına karşın günümüzde çok az kullanılan cihazlardır.

2.5. IP Adresleme

LAN veya WAN'da her bir cihazı ifade eden adresler vardır. Aslında bu adreslerin günlük hayatta kullanılan adresten pek bir farkı yoktur. Adres, OSI modelindeki özellikle ikinci ve üçüncü katmanlardaki protokollerce kullanılır. Bugün, internetin ve bilgisayar ağlarının olmazsa olmazı konumundaki IP adresleri haytamızda önemli

bir yere sahiptir. Yakın zamana kadar sadece bilgisayar ve ağ cihazlarında kullanılan bu adresler şimdilerde netbook'lar, cep telefonları, güvenlik kameraları gibi cihazlarda kullanılmaktadır. Gelecekte ise araçlarda, ev eşyalarında ve daha birçok cihazda kullanılacağı öngörülmektedir.

IP Protokolü kullanan her bir makine 32 bitten oluşan bir IP adresine sahiptir. IP adresi herbiri 8 bitten oluşan 4 gruba ayrılır. Bu gruplara oktet adı verilir. Her bir oktet birbirinden noktalarla ayrılır ve ondalık düzende gösterilir [5]. Şekil 2.5'de de görüldüğü gibi IP adresi temel olarak ağ ve makine olmak üzere iki ana parçadan oluşur. Ağ kısmı cihazın bağlı olduğu ağı tanımlarken, makine kısmı o ağ üzerinde bulunan özel bir cihazı belirtir.



Şekil 2.5. IP adres yapısı

IP adres blokları ARIN (American Registry of Internet Numbers) adlı organizasyondan ya da Internet Servis Sağlayıcılarından temin edilir [2]. IP adresleri A, B ve C olmak üzere 3 sınıfa ayrılmıştır. A sınıf adresler genelde hükümetlere ve de az sayıda çok büyük şirketlere verilir. Orta büyüklükte şirketlere B sınıfı, geri kalan tüm istekçilere C sınıfı adresler verilir. Bunların dışında D sınıfı adresler çoklu yayınlar (multicat) için, E sınıfı adresler ise araştırma amaçlı kullanımlar için ayrılmıştır. Adreslerin bu şekilde sınıflara ayrılmasının en önemli neticesi adres sınıflarının içerdiği IP sayısıdır. A sınıfı adres kullanan bir organizasyonda toplam 16.777.214 adet makine ağa bağlanarak adreslenebilir. A sınıfı adreslerde ilk oktet mutlaka 0-126 aralığında bir değer alır. Örneğin 122.92.45.11 A sınıfı bir adrestir, çünkü ilk okteti 0-126 arasındadır. Bir adresin ilk okteti 128-191 arasında bir değer ise B sınıfı adrestir. Ağı belirtmek için ilk iki oktet birlikte kullanılır. Geri kalan iki oktet (16 bit) ise ağdaki makine sayısını belirtir. B sınıfı bir adres 65.536 adet adres

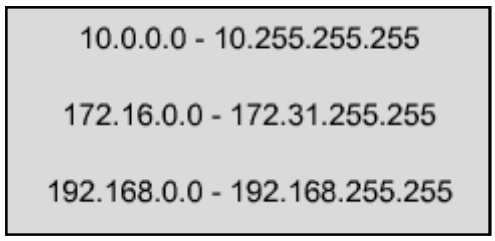
içerir. C sınıfı adreslerin ilk 3 biti daima 1 1 0 (bir bir sıfır) değerindedir. C sınıfı adreslere ilk oktetin alacağı değerler 192-223 arasındadır. Örneğin 201.113.102.64 C sınıfı bir adrestir. C sınıfı adreslerde ilk 3 oktetin tamamı ağ için kullanılırken sadece 1 oktet makineleri belirtmek için kullanılır. Bir C sınıfı ağ toplam 254 cihaz tanımlanabilir [6].

224-239 ile başlayan adresler çoklu yayın için kullanılan adreslerdir [6]. Bunlar yönlendirme protokolleri (OSPF, BGP, IS-IS…vb) tarafından ve ağ üzerinden video yayını yapan uygulamalarca kullanılır. IP protokolü ile Unicast, broadcast ve multicast iletişim mümkündür. Unicast, bir makinenin göndereceği veya alacağı verileri sadece bir makineye gönderip almasına kısaca, bir makine ile iletişime geçmesine denir. Broadcast, IP adresi bilinmeyen bir makinenin IP sinin öğrenilmesi için o adres bloğunun tamamındaki IP'lere gönderilerek kurulan iletişim şeklidir. Broadcast iletişime örnek vermek gerekirse, ziyarete giden bir kişinin gideceği adresi bilmesine rağmen daire numarasını bilmediği için tüm dairelerin ziline basması ve herkese sorması ve herkesi rahatsız etmesine benzer. Aradığı kişinin hangi dairede olduğunu tam olarak bilen kişinin başkalarını rahatsız etmeden gideceği daireye gitmesi unicast iletişime örnek gösterilebilir. Multicast, biraz farklıdır. Broadcast'te bir paket gönderilen ağdaki tüm makinelere giderken multicast'de paket sadece yayın yapılan IP adresinin temsil ettiği gruba üye olan adreslere gönderilir [6]. Dolayısıyla her makine gereksiz yere meşgul edilerek ağ kaynakları gereksiz kullanılmamış olur. Multicast iletişim günümüzde ağ üzerinden yayın yapan uygulamalarca kullanılır. Örneğin, Amerika'daki bir üniversitede verinlen bir dersin veya konferansın eş zamanlı olarak dünyanın başka bir yerindeki kullanıcılar tarafından izlenebilmesi veya bir genel müdürün konuşmasının multicast ile yayınlanması, isteyen kullanıcıların yayın linkini açarak multicast yayın grubuna üye olup yayını izlemeye başlaması gibi.

Satın alınan IP adresi ihtiyaca göre alt ağlara bölünerek kullanılabilir buna "subnetting"(alt ağlara ayırma) denir. Ağın esnek ve kullanışlı olabilmesi için "subetting" çok iyi planlanmalıdır. Örneğin, bir WAN bağlantısında karşılıklı bağlı yönlendiriciler için iki adet IP'ye ihtiyaç varken bütün bir C sınıfı IP bloğunu

kullanmak yanlış olur. IP adreslerinin alt ağlara ayrılıp ayrılmadığını, verilen IP adres bloğu kullanılarak kaç farklı makineye IP verilebileceğini ağ maskesi belirler. Gerçekte elimizde A, B veya C sınıfı bir adres olsa da bunun hepsini tek bir blok olarak kullanmak doğru olmaz. Zira günümüzde kullanılmayan IP blokları bitme noktasına gelmiştir. Buna önlem olarak servis sağlayıcılar müşterilerinin ihtiyacını karşılayacak kadar IP vermekteler. Örneğin, küçük bir şirkete C sınıfı bir IP almak çok lüks ve gereksiz olur. Onun yerine bir veya birkaç IP almak daha anlamlı olacaktır.

IP adresleri sadece A, B, C, D ve E sınıflarından ibaret de değildir. Bunlara ilaveten Şekil 2.6'da bazıları görülen ve özel kullanım amaçlı IP aralıkları da vardır.



Şekil 2.6. Özel amaçlı IP blokları [7]

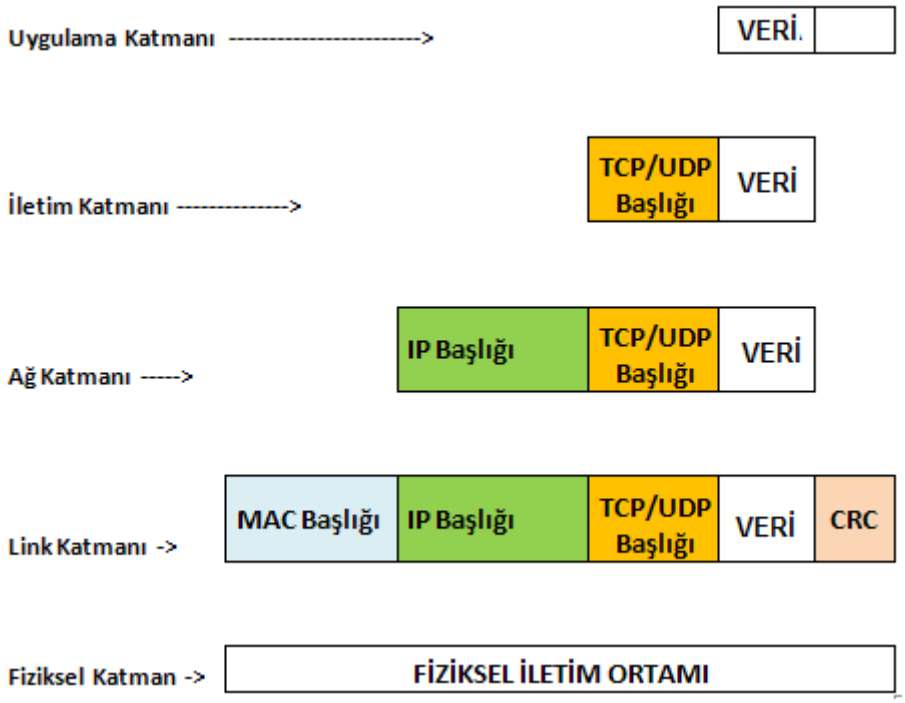
Bu IP'lerin en önemli özelliği internet dünyasında kullanılamayıp sadece şirketlerin dahili ağlarında kullanılabilecek olmalarıdır. Bu IP'ler internet erişimlerinde kullanılsa bile gerekli yönlendirmeleri servis sağlayıcılar tarafından yapılmadığından hiçbir yere erişim sağlayamazlar. Dahili kullanım amaçlı bu IP'leri de gerekli kılan yine IP adreslerinin bitme noktasına gelmiş olmasıdır. Bugün büyük, küçük hemen her şirket bu IP bloklarını kullanmaktadır. Peki, bu IP'lerle internete erişim sağlanamıyorsa nasıl oluyor da kullanılabiliyor? Burada NAT (Network Adress Translation) imdadımıza koşuyor. Dâhili ağda kullanılan IP'ler internete çıkarken yönlendirici veya güvenlik duvarlarınca başka bir IP'ye NAT yapılır. İçerdeki özel kullanım amaçlı IP'ler bu sayede internette yönlendirilebilen bir IP veye IP'lere dönüştürülerek dış dünyaya açılım sağlanmış olur.

Her şeyin IP ile taşınmaya başlandığı sanal iletişim ortamlarında, IP adreslerinin tükenme noktasına gelmesi hayatımıza IPv6 (Internet Protocol version 6) kavramını

getirmiştir. IPv6, bugün kullandığımız IPv4'e göre birçok avantajı beraberinde getirmektedir. IPv6'in çıkmasındaki öncelikli amaç, IPv4'lerin tükenme noktasına gelmesidir. Bununla beraber mevcut IPv4 birçok güvenlik zafiyeti içermekte olup bunların birçoğu IPv6 ile giderilmiştir.

2.6. IPv4 Paket Yapısı

IPv4'ün paket yapısına kısaca bakmak gerekirse, Şekil 2.7'de bir IP paketinin uygulama katmanından fiziksel katmana kadar nasıl değiştiği görülmektedir.

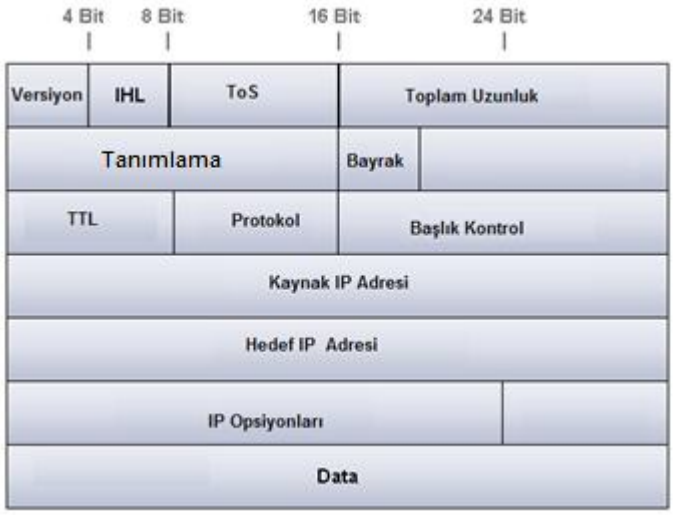


Şekil 2.7. IP paketinin başlıkları

Şekil 2.7'de görülen pakete iletim katmanında, uygulama katmanındaki uygulamanın kullandığı protokol tipine göre TCP veya UDP başlığı eklenir. TCP veya UDP başlıkları birbirinden tamamen farklıdır. TCP bağlantı odaklı bir protokolken UDP bağlantısız bir protokoldür. Bağlantı odaklıdan kasıt, veri iletimine başlamadan önce iletişim kuracak makinelerin iletişim öncesi birbirlerine senkronizasyon paketleri göndererek iletişime hazır olup olmadıklarını bildirmeleri ve teyit etmeleriyle başlamasıdır. Ayrıca iletimin devamında gönderilecek paketlerin sayısı, sırası

bağlantının bitip bitmediği gibi bilgiler sürekli karşılıklı teyitleşerek iletişim devam ettirilir. Bu iletişimin kısmen yavaşlamasına neden olur. Bununla beraber hata kontrol mekanizması olduğundan verilerin kayıp olması veya bozulması durumunda bunların düzeltilme veya tekrar gönderilmesi söz konusu olabilmektedir. UDP'de (User Datagram Protocol) ise bağlantı olmayan bağlantısız bir protokol olup, karşı tarafın veriyi alıp almadığı, iletim ortamında verinin bozulup bozulmadığı kontrol edilmeksizin veri gönderilir. Daha hızlıdır, ancak hata denetim ve düzeltme mekanizması yoktur. UDP, hızlı iletimin önemli olduğu uygulamalarca kullanılır. Örneğin, Ses, video, DNS(Domain Name Protocol) bunlardan bazılarıdır. Diğer taraftan, TELNET, SSH (Secure Shell) gibi bazı uygulamalar TCP protokolünü kullanırlar. Uygulama katmanında kullanılan uygulamanın tipine göre iletim katmanında pakete UDP veya TCP başlığı eklenir. Normal TCP başlığı 20 byte iken opsiyonların kullanılması durumunda biraz daha artabilmektedir. Normal UDP başlığı 8 byte'tır.

TCP ya da UDP başlığı eklenen paket ağ katmanına gönderilir, burada pakete IP başlığı eklenir. Şekil 2.8'de de görüldüğü gibi normal IP başlığı da 20 byte'dır [7].

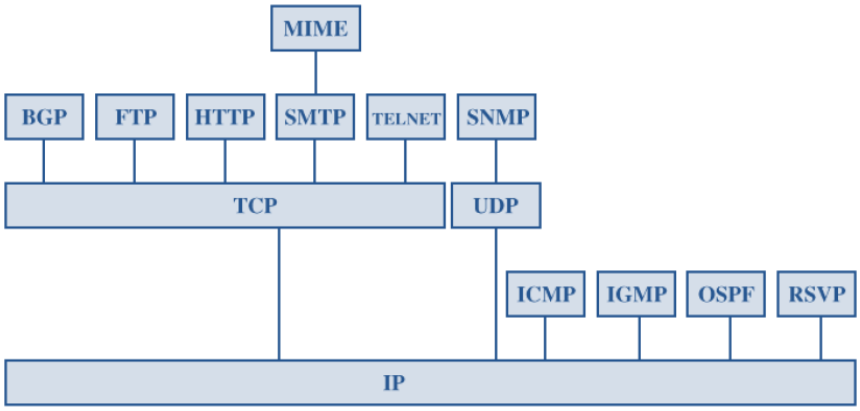


Şekil 2.8. IP başlığı

IP başlığında birçok bileşen olmakla beraber kaynak IP adres, hedef IP adres ve protokol en çok bilinen alanlardır. Adlarından da anlaşılacağı gibi paketin gideceği

hedef adresi “Hedef IP Adresi” , paketi gönderen makinenin adresini “Kaynak IP Adresi” ve üst katmanda (İletim Katmanı) kullanılacak protokolü (TCP/UDP) “protokol” alanı belirtir.

Şekil 2.8’de görüldüğü gibi paketin veri alanından sonra gelen iletim katmanı başlığı (TCP/UDP) IP başlığından önce gelir. Burada paketin üst katmanlarda hangi uygulamaya çıkartılacağını belirten port numaraları bulunur. Örneğin, TELNET uygulaması için TCP/23, SSH uygulaması için TCP/22, DNS isim çözümlemesi için UDP/53, NTP(Network Time Protocol) zaman senkronizasyonu için UDP/123 gibi. Şekli 2.9’da da IP, TCP ve UDP ile, bunlar üzerinde çalışan bazı uygulamaların ilişkileri görülmektedir.



Şekil 2.9. IP, TCP ve UDP protokolleri ve ilişkili uygulamaları

2.7. TCP

Daha önce de bahsedildiği gibi protokoller bağlantı odaklı ve bağlantısız olabiliyorlar. TCP protokolü bağlantı odaklı bir protokol olarak iletimin daha güvenli olmasını, gönderim sırasında hata oluşması durumunda bunun fark edilmesi ve düzeltilmesi gibi avantajları bulunmaktadır. Örneğin, UDP’de bu özellikler yoktur. Elbette bu avantajların yanı sıra UDP’ye göre daha yavaş iletim sağlanması, veri paketlerine eklenen başlık boyutunun fazla olması gibi dezavantajları da mevcuttur. TCP, IP ile birlikte kullanıldığından IP’nin bağlantısız bir protokol olmasından kaynaklanan eksiklerini de gidermektedir. Yani, kritik verilerin ne şekilde olursa

olsun yerine ulaştığından emin olmak istenmesi gibi bir durum söz konusu olunca IP/UDP ile bu durum sağlanamaz. Zira her iki protokol de bağlantısızdır, en iyi performans mantığına göre çalışarak paketleri gönderecekleri hedefe sürekli gönderirler. Hata kontrolü ve düzeltme ile zaman kaybetmezler. Bu durumda TCP/IP kullanmak istenen özellikleri sağlamaktadır. Bu şekliyle bakıldığı zaman TCP protokolü devre anahtarlamalı yapıya benzer.

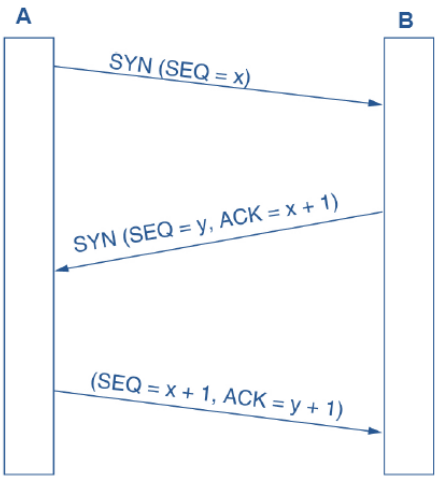
TCP'de iki makine arasında TCP verileri gönderilmeye başlanmadan önce bağlantı kurulur. Her iki taraf bağlantı şekli ve parametreleri konusunda mutabık olur, daha sonra veri gönderimi başlar. Bağlantının kurulması, sonlandırılması ve hata kontrollerinin yapılması TCP başlığında bulunan bayraklar sayesinde gerçekleştirilir. Bu bayraklar SYN, ACK, PSH, FIN, RST, URG olarak adlandırılır. Bu bayrakların kısa açıklamaları Çizelge 2.1'de verilmektedir.

Çizelge 2.1. TCP bayrakları

TCP Bayrakları	Açıklama
SYN	Sıra numarası bağlantı kurmak için başlangıçta kullanılır.
ACK	Önceden gönderilen bir veriye onay için gönderilir.
PSH	Bağlantı kurulduktan sonra veri gönderiminde kullanılır.
URG	Acil gönderilmesi gereken verilerin gönderiminde kullanılır.
RST	Bağlantı isteği kabul edilmezse kullanılır
FIN	Veri gönderimini sonlandırmak için kullanılır.

Bu aşamadan sonra PSH bitleri set edilerek veriler gönderilir. Alan taraf da verileri sorunsuz aldığını veya alamadığını ACK 'lerle bildirir. Her iki makineden biri bağlantının belirli bir anında FIN biti göndererek bağlantıyı bitirmek isteyebilir. Bunun da gerçekleşebilmesi için yine ACK ile onaylanması gerekir.

Şekil 2.10'da da A makinesinden B'ye üçlü el sıkışma işlemi görülmektedir.



Şekil 2.10. TCP üçlü el sıkışma aşaması

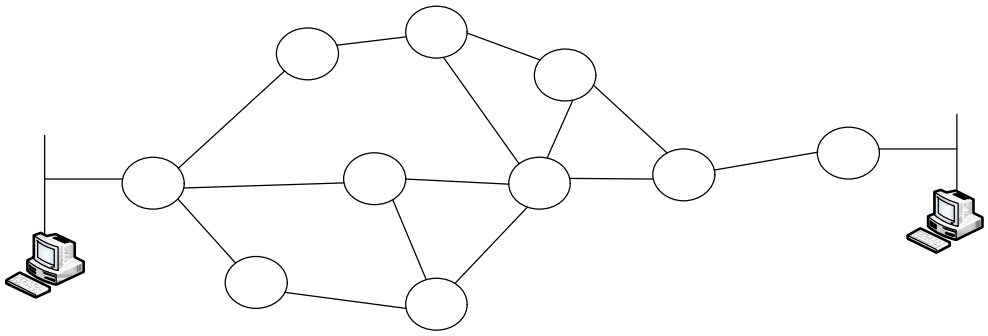
2.8. IP Yönlendirme

Herhangi bir ağa bağlı çalışan bir cihazın aynı IP ağında bulunan cihazlarla iletişimi ile farklı IP ağında bulunan cihazlarla iletişimi farklı şekillerde olmaktadır. Aynı ağda bulunan bir cihazla iletişim kurarken, zarfladığı veri paketlerine, hedef makinenin MAC adresi yazılarak gönderilir. Farklı ağlarda bulunan makinelerle iletişim kurarken paketler varsayılan ağ geçidi olarak belirlenen IP adresine gönderilir. Varsayılan ağ geçidi, ilgili ağın dışarıya açılan kapısı olarak da düşünülebilir. Bu aynı zamanda bir yönlendiricidir. Varsayılan ağ geçidine gönderilen paketler varsayılan ağ geçidindeki yönlendirme bilgilerine göre bir hedefe ulaşmak için bir sonraki cihaza gönderilirler. Yönlendiricilerde iki tür yönlendirme yapılır.

1. Statik yönlendirme,
2. Dinamik yönlendirme.

Statik yönlendirmede, hedef ağlar ve hedef ağlara gidecek paketlerin gönderileceği IP bilgileri yönlendiricilere el ile (statik) girilir. Büyük ağlarda statik olarak yönlendirme işlerini yönetmek imkânsızdır denebilir. Şekil 2.11'de görülen kısmi-mesh topolojide PC1'den PC2'ye veya ters yönde erişim gerçekleşmesi için her bir

yönlendiriciye, hem PC1'e gidecek hem de PC2'ye gidecek paketler için, yani PC1 ve PC2'nin bulunduğu ağlar için statik kayıt girmek gerekir.



Şekil 2.11. Kısmi mesh topoloji

Şekil 1.12'de yönlendiriciye statik olarak girilmiş kayıt bulunmaktadır.

```
Gateway of last resort is 192.168.113.108 to network 0.0.0.0

     212.29.212.0/32 is subnetted, 1 subnets
S       212.29.212.34 [1/0] via 192.168.113.83
S    192.168.46.0/24 [1/0] via 192.168.113.91
     212.252.111.0/24 is variably subnetted, 4 subnets, 2 masks
S       212.252.111.64/27 [1/0] via 192.168.113.143
S       212.252.111.96/27 [1/0] via 192.168.113.143
S       212.252.111.0/24 [1/0] via 192.168.113.143
S       212.252.111.192/27 [1/0] via 192.168.113.143
     85.0.0.0/8 is variably subnetted, 22 subnets, 4 masks
S       85.29.36.64/29 [1/0] via 192.168.113.34
S       85.29.32.0/24 [1/0] via 192.168.113.34
S       85.29.0.0/24 [1/0] via 192.168.113.34
S       85.29.8.180/30 [1/0] via 192.168.113.34
```

Şekil 2.12. Statik kayıt örneği

Şekil 2.12'de görülen yönlendirme tablosuna göre, yönlendirici yönlendirme tablosunda olmayan IP bilgileri için 192.168.113.108 IP'sine sahip yönlendiriciye paketlerini gönderecektir. Bunun dışında 212.252.111.64/27 IP bloğuna gidecek paketleri 192.168.113.143 IP'li yönlendiriciye, 85.29.32.0/24 IP bloğuna gidecekleri 192.168.113.34 IP'li yönlendiriciye gönderecektir.

Dinamik yönlendirme kullanılması orta ve büyük ölçekli ağlarda kaçınılmazdır. Dinamik yönlendirme, hedefe giderken alternatif yollardan en optimum olan yolun

belirlenmesi, link kesilmelerinde alternatiflerin kullanılması, yük dağılımının sağlanması gibi birçok avantaj sağlar.

Dinamik yönlendirme protokolleri temelde ikiye ayrılır [8].

1. Uzaklık vektörü,
2. Link durumu.

Uzaklık vektörü protokolünde yönlendirici, kendisine direkt bağlı diğer yönlendiricilerle bilgi alışverişinde bulunur ve bu yolla ağdaki yolların bilgisini edinir. RIP ve IGRP bilinen uzaklık vektörü protokolleridir.

Link durumu protokolünde ise, yönlendirici komşularından gelen link bilgilerini kullanarak birer veritabanı oluşturur. Bu veritabanı yolu ile tüm ağ hakkında bilgi sahibi olur. Hedefe giderken hangi yönlendiricilere paketlerin gönderileceğini bu veritabanını kullanarak hesaplar. Veri tabanı, komşulardan gelen link bilgileri ile sürekli güncel tutulur. Güvenilirliği yüzünden büyük ağlarda link durum protokolü kullanılır. Veritabanını küçültmek için de yol özeti, değişken büyüklükteki alt ağ maskeleri gibi yöntemler geliştirilmiştir. OSPF ve IS-IS (Intermediate system to intermediate system) link durum protokolleridir [8].

Şekil 2.11'de dinamik yönlendirme kullanıldığı durumda PC1'den PC2'ye giden trafik A yönlendiricisi tarafından C yönlendiricisi gönderilerek gerçekleşirken A ile C arasındaki hatta problem olması durumunda sorun A tarafından algılanarak yol hesaplaması sonucuna göre B veya E yönlendiricileri üzerinden gönderilir.

Yönlendirme protokolleri kullanıldıkları ağa göre de dâhili ve harici olmak üzere ikiye ayrılabilir. BGP (Border Gateway Protocol) dışındaki diğer protokoller dâhili olarak kullanılırlar, bununla beraber BGP'yi dahili ve harici olarak kullanmak mümkündür. Dâhili protokoller, aynı atonom sistem içindeki cihazlar arasında kullanılırken, harici protokoller otonom sistemler arasında kullanılırlar. Otonom sistemler, içinde bulunan cihazların tamamının belirli bir grup tarafından yönetildiği ağlar olarak tanımlanmaktadır.

Yönlendirme protokollerinde en önemli konulardan biri de toparlanma süresidir (convergence time). Toparlanma süresi, bir otonom sistem içinde herhangi bir yönlendiricinin işlevsiz hale gelmesi veya hatlardan birinin kopması durumunda, bu bilginin tüm yönlendiriciler tarafından öğrenilmesi ile gerekli yol hesaplamalarının yapılması ve mevcut duruma göre yönlendirme veri tabanının düzenlenmesi olarak ifade edilebilir.

3. OSPF (OPEN SHORTEST PATH FIRST)

TCP/IP'nin ilk yıllarında, RIP (Routing Information Protocol) standart routing protokolü olarak birçok ağda kullanılıyordu. Basit ve ilk olması, tercih edilmesinde en önemli faktörlerdi. Bazı kısıtlarından dolayı büyük ağlarda istenen performans alınamadığı fark edilerek, yeni bir yönlendirme protokolüne ihtiyaç duyuldu. 1988 yılında IETF (Internet Engineering Task Force), RIP tarafından karşılanamayan ihtiyaçları karşılayacak daha gelişmiş, yeni bir yönlendirme protokolü için çalışmaları başlattı. Yeni protokolün link-durumu tabanlı olması ve OSPF (Open Shortest Path First,) olarak adlandırılması kararlaştırıldı. Yeni protokole bu adın verilmesinde iki önemli faktör vardı. Bunlar; hedefe giderken kullanılacak en kısa yolun hesaplanmasında kullanılacak algoritma (SPF) ve bu protokolün herkesçe ücretsiz kullanılabileceğini belirten "Open" idi. 1989 yılında RFC 1131 ile tanımlanan ilk sürünü OSPFv1, 1992 yılında da RFC 1247 ile tanımlanan OSPFv2 sürümü kullanılmaya başlandı. Günümüzde halen dâhili yönlendirme protokolü olarak OSPFv2 yaygın olarak kullanılmaktadır [9].

OSPF yönlendirme protokolü IGP (Interior Gateway Protocol) protokolleri içinde en önemlilerindendir. Kullandığı teknoloji bakımından en çok RIP protokolü ile karşılaştırılsa da, RIP protokolüne göre çok daha üstün bir protokoldür. Kısaca bahsetmek gerekirse RIP uzaklık vektörü mantığınca yönlendirme tablolarını belirlerken, OSPF link durum algoritmasına göre yönlendirme tablolarını belirler. RIP'te her bir yönlendirici ağın tümünü komşularının gözüyle görebilir. OSPF'de komşudan alınan link durum bilgilerinin yorumlanması ve bu yorum sonucunda tabloların belirlenmesi söz konusudur.

3.1. OSPF'in Çalışma Mantığı

OSPF, Otonom Sistemlerin (OS) içinde kullanılan dahili yönlendirme protokolü olarak tasarlanmıştır. Dolayısıyla OS'ler arası kullanıma uygun değildir. Ağda meydana gelen değişikliklerin tüm yönlendiriciler tarafından fark edilerek topoloji bilgilerinin eşitlenmesi durumuna "yakınsaklık" denir. Yakınsaklık kurma süresinin kısa olması yönlendirme protokolleri için önemli bir parametre olup, link

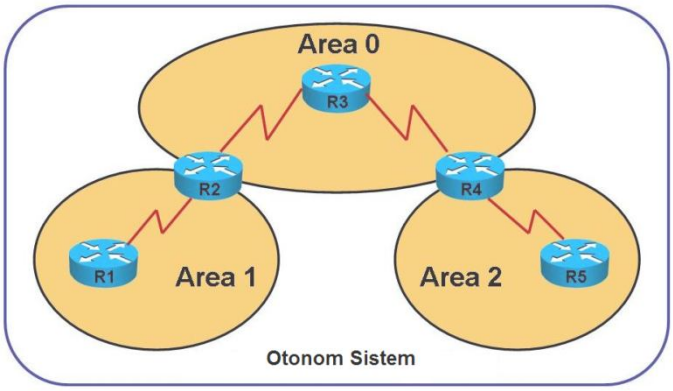
kesintilerinde servis kesintisini veya paket kaybını azaltır. OSPF'in yakınsaklık kurma süresi RIP'e göre daha düşüktür. Aynı zamanda uzaklık vektörü protokolleri gibi yönlendirme bilgileri toplamaz. Yönlendirici durum bilgileri ve link bilgileri toplayarak bu bilgilerle ağın topoloji veritabanı oluşturulur. Oluşturulan bu ağ topolojisi üzerinde Dijkstra algoritması yardımıyla en kısa yol (SPF) ağaçları oluşturulur [10]. En kısa yol ağaçları yardımıyla da yönlendirme tabloları oluşturulur. Yönlendirme tabloları, yönlendiricinin RAM'inde tutulur ve veri paketleri geldiği zaman, paketin hedef adresine bakılır. Hedef adrese en uygun sonraki yönlendirici IP'si ve bu yönlendiriciye giderken hangi yerel arabirimden gönderileceği bulunarak yönlendirme işlemi gerçekleştirilir.

OSPF, en iyi yol bulmada kıstası maliyettir [10]. Paketler hangi arabirimden gönderilecekse, o arabirimin maliyet hesabı temel alınır. Bazı yönlendiricilerde maliyet hesabı eşitlik ile yapılır.

Maliyet= 100.000.000/BW

Burada BW, ilgili arabirimin bps cinsinden bant genişliğidir. Örneğin, yönlendiriciye bağlı bir linkin bant genişliği 100Mbps ise, bunun bağlı olduğu arabirimin maliyeti, 100.000.000/100.000.000=1 olacaktır. Eğer linkin hızı 10Mbps olsaydı o zaman maliyet 10 olacaktı. Her zaman düşük maliyetli yol önceliklidir [8,10]. Maliyeti en düşük yol, en kısa yoldur diye de düşünülebilir. İhtiyaç olması durumunda BW değeri el ile girilerek değiştirilebilir.

OSPF, ağ kümelerinin gruplanmasına olanak tanır. Bu yapı "area" diye adlandırılır ve bir area'nın topoloji bilgisi başka AS'lerden gizlenebilir. Bu da yönlendirme tablolarının ciddi anlamda küçülmesini sağlar. OSPF çalıştıran her yönlendirici bir area'ya dahil olmak zorundadır. Şekil 3.1'de görüldüğü gibi her OSPF ağı sıfırıncı area (area 0 - omurga area) sahip olmalı ve diğer tüm area'lar omurga area'ya dokunmalıdır [10].



Şekil 3.1. OSPF area yapısı

Aynı area'da bulunan yönlendiriciler aynı topoloji bilgisine sahiptirler. Bu yönlendiricilerden birinin link durumu değiştiğinde hemen diğerlerine haber verir ve diğerleri de kendi topolojilerini buna göre güncellerler [11].

3.1.1. OSPF komşuluk kavramı

OSPF çalışan ortamda her bir yönlendirici aynı area içindeki diğer yönlendiricilerle komşuluk ilişkisi kurar. Komşuluk ilişkisi kurulurken yönlendiriciler birbirlerine Çizelge 3.1'de görülen beş farklı tiplerde paket gönderirler.

Çizelge 3.1. OSPF paket tipleri

OSPF Paket Tipleri	Açıklama
Tip-1 Merhaba (selamlaşma)	Komşularla yakınlık ilişkisi kurma ve yönetmede kullanılır.
Tip-2 Veritabanı Tanımlama Paketi (VTP)	Yönlendiricinin link durum veritabanının içeriğini tanımlar.
Tip-3 Link Durum İsteği (LDİ)	Komşu yönlendiricinin link durum veritabanının belirli bir bölümünü istemek için kullanılır.
Tip-4 Link Durum Gönderme (LDG)	Komşu yönlendiricilere link durum bilgilerinin göndermede kullanılır.
Tip-5 Link Durum Onaylama (LDO)	Komşu yönlendiricinin gönderilen link bilgilerini aldığını onaylamasında kullanılır.

OSPF, Katman 3 protokolü olan IP'nin hemen üstünde çalışır. Tüm OSPF paket tipleri gönderilirken IP başlığının üstünde Şekil 3.2'de görülen OSPF başlığı eklenerek gönderilir.

Şekil 3.2. OSPF paket başlığı

OSPF protokolü kullanılan ortamdaki yönlendiriciler birbirlerine belirli bir sürede "Merhaba" (selamlaşma) paketleri gönderirler. Selamlaşma paketleri Şekil 3.3'de de görüldüğü gibi özel bir pakettir. Komşu kimlik bilgileri, AY ve YY bilgileri ile yönlendirici öncelik bilgisi gibi komşuluk kurulması aşamasında gerekli olan önemli bilgiler içermektedir.

Şekil 3.3. Selamlaşma paketi yapısı

Bir area içindeki her yönlendiricide selamlaşma süresi aynı olmak zorundadır. Aksi halde komşuluk ilişkisi kurulamaz. Komşusundan selamlaşma süresinin 4 katı süresince selamlaşma paketi alamayan bir yönlendirici komşusunun işlevsiz olduğuna hükmeden ve topoloji bilgilerini tekrar günceller. Yönlendiriciler birbirlerine OSPF paket tiplerini gönderirken çoklu gönderme kullanırlar. Çoklu gönderme için ayrılmış 224.0.0.6 ve 224.0.0.5 IP'leri OSPF yönlendiricilerin dâhil olduğu çoklu gönderim gruplarını ifade eder. OSPF çalıştıran her bir yönlendirici durumuna göre bu çoklu gönderim IP'leri ile ifade edilen gruplardan birine dâhildir.

3.1.2. OSPF operasyonu içinde OSPF durumları

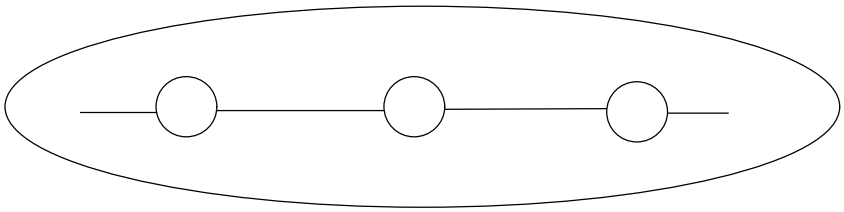
OSPF operasyonu, yönlendiriciler arasında yakınlık kurulmasından yönlendirme tablolarının oluşturulup yönetilmesine kadar beş adımdan oluşur. Bu adımları ve bunların her birinde OSPF'in durumları Çizelge 3.2'de görülmektedir.

Çizelge 3.2. OSPF adım ve durumları

OSPF Adımları	OSPF Durumları
Yakınlık Kurma	DOWN, INIT, TWO-WAY, ExSTART (AY/YY seçilme ihtiyacı yoksa)
AY/YY Seçimi	ExSTART(AY/YY ile), TWO-WAY(tüm diğer yönlendiricilerle)
Yolların Keşfedilmesi	ExSTART, EXCHANGE, LOADING, FULL
Yol Seçimi	
Yönlendirme Bilgilerinin Yönetilmesi	

3.1.3. Yakınlık kurma

OSPF komşulukları kurulurken, yönlendiriciler üzerinde OSPF'in çalıştığı arabirimler farklı durumlarda bulunur. En başta OSPF yönlendirici arabirimleri DOWN durumundadır. Şekil 3.4'deki B yönlendiricisi, kendisinde OSPF'in aktif edildiği tüm arabirimlerden 224.0.0.5 IP'sine selamlaşma paketleri gönderir [10]. Bu paketler B'nin yönlendirici IP'sini (yönlendirici kimliği) içerir. Area0 içinde bulunan ve OSPF çalıştıran A ve C yönlendiricileri 224.0.0.5'e gönderilen bu selamlaşma paketlerini alırlar. B'nin yönlendirici kimliğini öğrenen A ve C yönlendiricileri bu kimlik numarasını kendi gönderecekleri selamlaşma paketlerinin komşu alanına ekleyerek selamlaşma paketlerini B'ye gönderirler. Bu aşamada A ve C yönlendiricileri ilgili arabirimlerini INIT durumuna geçirirler.



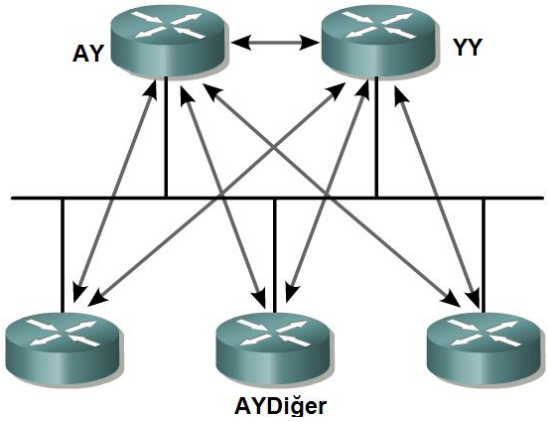
Şekil 3.4. Aynı area'da bulunan üç adet yönlendirici

Selamlaşma paketi alınır alınmaz yönlendiriciler kendilerini INIT durumuna geçirirler. Bundan sonra kendisine gelen selamlaşma paketlerinin komşu alanında kendi kimliğini gören yönlendirici kendisini TWO-WAY durumuna geçirir. Yönlendirici arabirimlerinin bağlı olduğu fiziksel ortam, ya uçtan uca (kiralık hatlar gibi) veya çoklu erişim (Ethernet gibi) ortamı olabilir. Arabirimin bağlı olduğu ortam uçtan uca bir hat ise OSPF, ilgili arabirimi TWO-WAY durumdan sonra ExSTART durumuna geçiriyor. Arabirimin bağlı olduğu ortam çoklu erişim ortamı ise OSPF, yönlendirici arabirimini asıl veya yedek yönlendirici seçimine sokuyor.

3.1.4. AY ve YY seçimi

Çoklu erişim ortamları üzerinden birbirlerine bağlı ikiden çok yönlendirici olan yerlerde AY ve YY seçimi gerçekleştirilir. AY ve YY seçimindeki amaç, komşuluk tablolarının küçük tutulması, komşuluk kurulumları için geçen süre ve gönderilen paketlerin azaltılması ve bunlara bağlı olarak link durum güncellemelerinin azaltılmasıdır. Uçtan uca bağlı yönlendiricilerde bu süreç olmaz. Zaten sadece bir komşusu vardır.

AY ve YY seçimi olan ortamlarda seçim sonucunda 3 çeşit yönlendirici oluşur. Asil yönlendirici (AY), Yedek yönlendirici (YY) ve bu ikisi dışındaki yönlendiriciler (AYDiğer). AYDiğer yönlendiricileri Şekil 3.5'te görüldüğü gibi sadece AY ve YY ile komşuluk kurar ve link durum duyurularını sadece bunlara gönderirler.



Şekil 3.5. AYDiğer yönlendiricilerin AY ve YY ile ilişkisi

Kendi aralarında komşuluk ve link durum duyurusu yapmazlar. AY ile YY sürekli birbirlerinin sağlıklı çalışıp çalışmadığını kontrol ederler. Örneğin YY belirli bir süre AY'den selamlaşma paketleri alamazsa kendisini AY ilan eder. AYDiğer konumunda olan yönlendiriciler kendi aralarında YY seçimine girer ve aralarından bir yönlendirici YY olur. Yönlendiriciler arasında AY seçilirken en büyük kimlik numaralı (yönlendirici IP) olan tercih edilir. Bununla beraber manüel olarak yönlendirici önceliği ayarlanarak da AY ve YY seçimine müdahale edilebilir. Selamlaşma paketlerinin gönderimi belirli aralıklarla sürekli gerçekleştirilir. Bu sayede yönlendiriciler komşularının durumundan haberdar olur. Link durum güncellemeleri AYDiğer yönlendiricilerden AY ve YY'ye doğru yapılır. AY, kendisine herhangi bir yönlendiriciden gelen link durum güncellemelerini diğer tüm yönlendiricilere gönderir. OSPF protokolü kullanılan ortamlarda 224.0.0.5 çoklu yayın IP'si üzerinde OSPF çalışan tüm yönlendiricileri, 224.0.0.6 ise tüm AY yönlendiricileri temsil eder [12].

3.1.5. Yolların bulunması

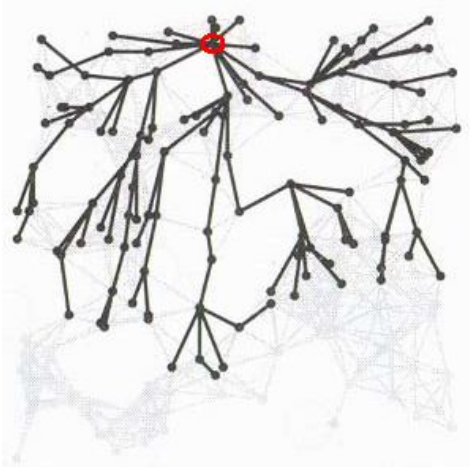
Bu aşamada yönlendiriciler veritabanı değişimi için hazırlık yaparlar. ExSTART durumuna geçilmemişse, bu aşamada ExSTART durumuna geçilir. Sonrasında yönlendiricilerin birbirlerine link durum veritabanı bilgilerini göndermesi ile devam edilir. LOADING durumunda belirli ağlar için birbirlerinden, o ağın link durum bilgilerini talep ederler. En sonunda FULL duruma geçilir. FULL duruma geçilmesi

demek artık aynı area içindeki yönlendiricilerin topoloji veritabanı ve link durum veritabanlarının aynı olduğu anlamına gelir.

ExSTART sürecinde daha büyük yönlendirici kimlik numarasına sahip olan AY olur. Diğeri ortam durumuna göre YY veya AYDiğer olur. Buna göre de veritabanı değişim süreci başlatılır. Veri tabanı değişim (exchange) sürecinde yönlendirici kendisinde olmayan bir link hattında bilgi alırsa bu bilgiyi aldığı komşusundan tüm güncellemeleri talep eder. Aldığı her güncelleme sonrasında da "güncellemeleri aldım" anlamında onay paketleri (LDO) gönderir. Bu şekilde loading süreci de tamamlanmış olur.

3.1.6. Yol seçimi

Yönlendirici tüm link bilgilerine sahip ve yönlendirme tablosunu oluşturmaya hazır durumdadır. Bunun için öncelikle link durum veritabanından SPF ağacını oluşturmak için veri tabanı üzerinde SPF algoritması (Dijkstra) çalıştırılır. SPF ağacını oluştururken yönlendirici Şekil 3.6'da görüldüğü gibi kendisini ağacın köküne yerleştirir.



Şekil 3.6. Örnek SPF ağaç yapısı

SPF ağacı oluştururken algoritmanın çalışma prensibi gereği olarak döngü ağacın bağımsız olması sağlanır.

SPF algoritması, her LDG aldığında yönlendirme tablosunu güncellemek için SPF hesaplaması yapar. Sürekli çarpan linkler sürekli SPF hesabı yapılmasını gerektirir. Bu da yönlendiriciye çok fazla yük bindirir. Bunu önlemek için LDG aldıktan ne kadar süre sonra SPF hesaplaması yapılacağı ve ardışık SPF'ler arası süreyi manüel girerek ağ yapısına göre OSPF optimizasyonu yapılabilir.

3.1.7. Yönlendirme bilgilerinin yönetilmesi

Yönlendirme bilgileri oluşturulduktan sonra yönlendiriciler bu bilgileri kullanarak paketleri kaynaktan hedefe doğru uygun yollardan gönderirler. Aradaki yol veya yönlendirici problemlerini birbirlerine haber vererek yönlendirme tablolarını sürekli yenilerler. Bu sayede ağlarda meydana gelen yönlendirici veya link problemlerinden trafik akışının ve dolayısıyla paket kayıplarının en aza indirgenmesi hedeflenir. Şekil 3.8'de Cisco cihazlardan alınmış bir yönlendirme tablosu görülmektedir.

```
B       10.232.100.16/30 [200/0] via 10.202.100.10, 1w0d
B       10.210.98.76/30 [200/0] via 10.210.100.10, 7w0d
C       10.200.100.48/29 is directly connected, Vlan12
O       10.173.17.0/24 [50/46] via 10.200.100.13, 00:28:36, Tunnel20
B       10.243.192.64/26 [200/0] via 10.150.120.10, 2w0d
O E2    10.179.224.0/23 [50/11] via 10.200.100.13, 00:28:36, Tunnel20
                        [50/11] via 10.200.100.12, 00:28:36, Tunnel10
O       10.179.96.0/24 [50/741] via 10.200.100.13, 00:28:36, Tunnel20
O       10.179.64.0/24 [50/660] via 10.200.100.12, 00:28:36, Tunnel10
O       10.179.32.0/24 [50/751] via 10.200.100.13, 00:28:36, Tunnel20
                       [50/751] via 10.200.100.12, 00:28:36, Tunnel10
```

Şekil 3.7. Cisco yönlendiricide örnek yönlendirme tablosu.

Yönlendirme tablosunda her satırın en başında görülen "O", "C", "B" harfleri bu yönlendirme bilgilerinin sırasıyla OSPF, direkt bağlı link, BGP'den öğrenildiğini gösterir.

Yönlendiriciler kendilerine gelen paketlerin katman 3 ve yukarısındaki bilgilerinde değişiklik yapmazlar. Yönlendirme yapar ve sadece paketin TTL (Time to Live) değerini bir azaltırlar.

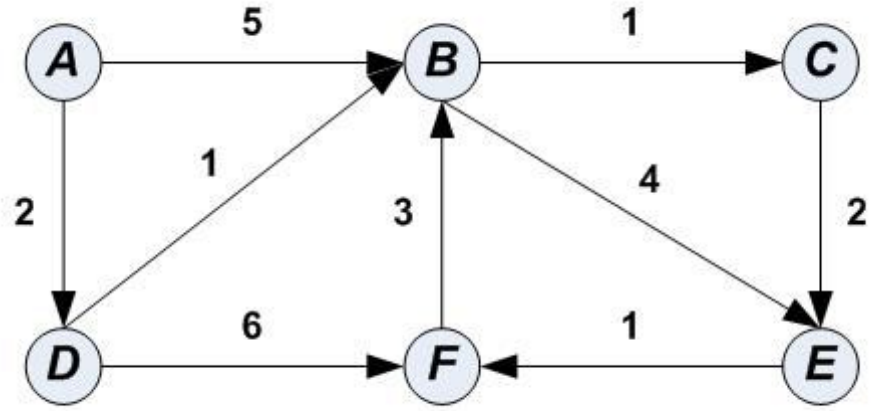
3.2. Dijkstra (Dikestra) Algoritması ile En Kısa Yolların Bulunması

Dijkstra algoritmasını 1959 yılında Hollandalı bilgisayar bilimci Edsger Dijkstra bulmuştur. Algoritma negatif olmayan ağırlıklı (weight) kenarlara sahip bir graftaki en kısa yol problemini çözmek için kullanılır. Yönlendirme algoritmaları dışında farklı amaçlarla da kullanılan Dijkstra algoritması özellikle IS-IS ve OSPF tarafından ağdaki kaynak olarak seçilen nokta ile başka noktalar arasında en kısa yolun bulunması amacıyla kullanılır. Algoritma belirli bir başlangıç düğümünden başlayıp bütün düğümlere erişene kadar grafta genişleyip en kısa yolları belirler. Bu sayede her düğüme giden minimum maliyetli yollar belirlenmiş olur [15,16].

Dijkstra algoritması düğümlere bazı etiketler atar. Bu etiketler düğümlerin başlangıç düğümüne olan uzaklıklarını gösterirler. Algoritma, kalıcı ve geçici olmak üzere iki çeşit etiket kullanır. Kalıcı etiketler ulaşılmış ve başlangıç düğümüne uzaklığı bilinen düğümlere verilir, diğer etiketler ise geçici etiketlerdir. İlk olarak başlangıç düğümü s(source) kalıcı olarak etiketlenir, diğer düğümler ise geçici olarak etiketlenir. Eğer x düğümünün etiketi dist(x) ve x ve y düğümleri arasındaki kenarın ağırlığını da wt(x,y) olarak gösterirsek, s düğümüne doğrudan bağlı olmayan düğümlerde dist(x)=∞ diğerlerinde ise dist(x)=wt(s,x) olacaktır. Daha sonra ise bütün geçici etiketler arasından en küçük olanı kalıcı etikete çevrilir ve eşitlik (3.1)'e göre bütün dist(x) değerleri güncellenir [14,15,16].

$$dist(x) = \min[dist(x), dist(y) + wt(y,x)] \tag{3.1}$$

Yukarıdaki işlem N düğümlü bir graf için en fazla N-1 kere tekrarlanır ve bunun sonucunda, graftaki bütün düğümlere erişilerek ve kalıcı olarak etiketlenmiş olurlar.

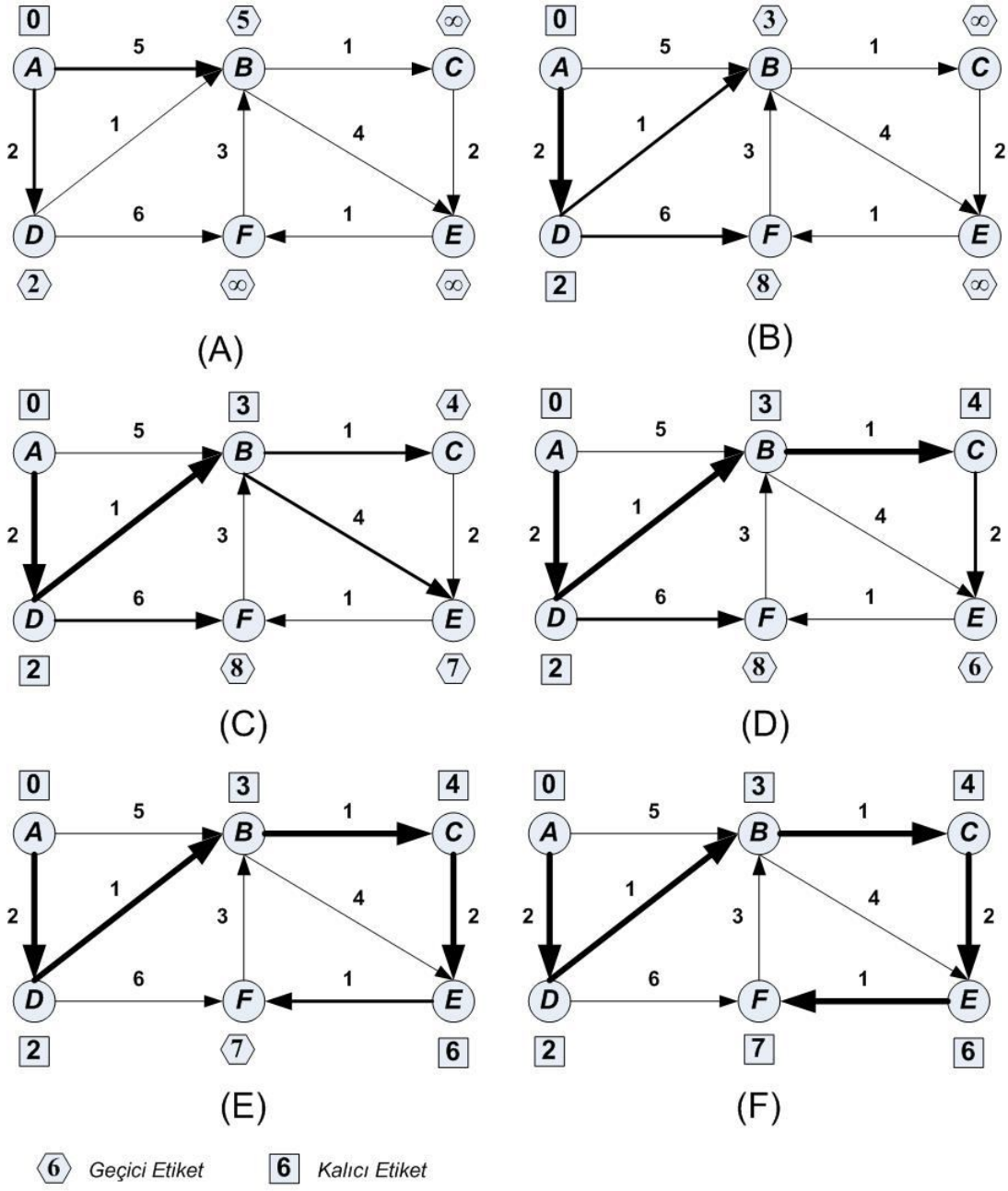


Şekil 3.8. Dijkstra algoritması için örnek graf

Şekil 3.8'de görülen örnek graf üzerinde başlangıç düğümü A seçildiğinde A'dan diğer düğümlere olan en kısa yollar hesaplanacaktır. Başlangıçta sadece A düğümü 0'la kalıcı olarak etiketlenir ve diğer düğümler geçici olarak gibi etiketlenmiştir:

dist(B)=5; dist(C)=∞; dist(D)=2; dist(E)= ∞; dist(F)= ∞

Bu etiketlere bakarak D düğümün etiketi en küçük olduğu için kalıcı etikete dönüştürülür. Etiketleme işlemleri ve etiketlerin durumu Şekil 3.9'da da adım adım gösterilmektedir.



Şekil.3.9. Dijkstra algoritmasında adım adım etiketlerin durumu [17]

Bu işlemden sonra gereken etiket güncellemeleri yapılır ve yeni geçici etiketler şu şekilde olur:

dist(B)=3; dist(C)=∞; dist(E)= ∞; dist(F)= 8

Daha sonra ise B düğümü seçilir ve etiketi kalıcı hale getirilir, B düğümüne giden en kısa yol A → D → B şeklinde bulunmuş olur, güncellenmiş etiketler ise:

dist(C)=4; dist(E)= 7; dist(F)= 8

C düğümü seçilir etiketi kalıcı hale çevrilir, ve bu duruma göre E düğümünün etiketi güncellenir ve dist(E)= 6; dist(F)= 8 olur, daha sonra E düğümünün etiketi de kalıcı yapıldıktan sonra F düğümünün etiketi dist(F)= 7 olarak güncellenir. Son olarakda F düğümünün etiketi kalıcı hale getirilir. Şekil 3.9'da da görüldüğü gibi A düğümünde F düğümüne en kısa yol yani maliyeti en az olan yol A→D→B→C→E→F şeklinde oluşmuştur. Son durumda graftaki bütün etiketler kalıcı olarak işaretlendiği için algoritma sona ermiştir [13].

Dijkstra algoritmasının program kodu ise genel olarak şu şekilde yazılabilir [14]:

```
1     for V[G] deki her v düğümü
2         do d[v] = ∞
3             p[v] = 0
4     d[s] = 0
5     S = boş küme
6     Q = V[G]
7     while Q ≠ boş küme
8         do u = Min-Çıkar (Q)
9             S = S union {u}
10            for  u'dan giden her (u,v) kenarı
11                do if d[v] > d[u] + w(u,v)
12                       then d[v] = d[u] + w (u,v)
13                            p[v] = u
```

Koddaki V[G] kümesi G grafındaki düğümleri belirtmektedir, s düğümü başlangıç düğümünü, v düğümleri ise diğer düğümleri belirtmektedir. Düğümlerin etiketleri d[v] ile kenarların ağırlıkları ise w(u,v) ile belirtilmektedir. Min-Çıkar (Q) fonksiyonu ise Q kümesinin içindeki minimum d[u] değerine sahip düğümü bulan ve

daha sonra da Q kümesinden çıkaran bir fonksiyondur. Koddaki p[v] değeri ise v düğümünün öncelikli yani, v düğümüne gitmek için gidilmesi gereken bir önceki düğümdür [14].

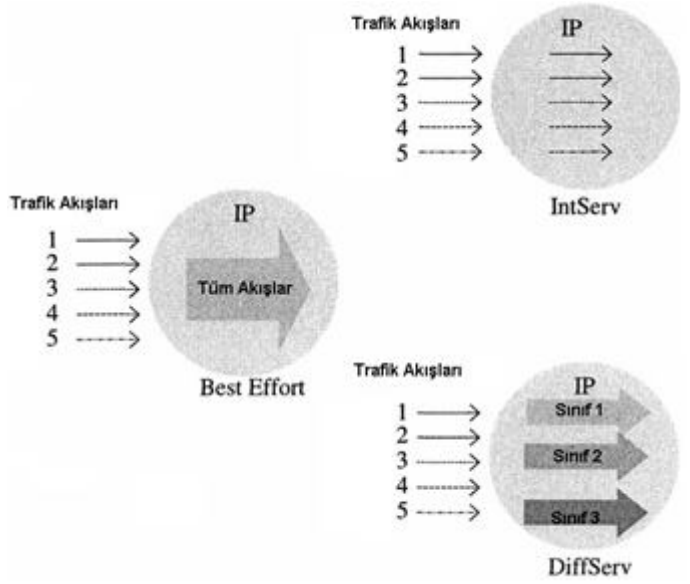
Koddaki ilk dört satır başlangıç düğümü s'in etiketini sıfır ve diğer bütün düğümlerin etiketlerini sonsuz, öncellerini ise sıfır yapmak için kullanılır. Beşinci satırda ise S kümesi boş küme haline getirilmekte ve altıncı satırda Q kümesi Q = V – S durumunu sağlaması açısından V[G] kümesine eşitlenmektedir. Daha sonraki while döngüsünde ise Q kümesindeki en küçük değerli düğüm çıkarılır ve S kümesine eklenir (döngünün ilk seferinde u = s olmaktadır), on ve onüçüncü satırlar arasında ise etiketlerin güncellenme işlemi yapılır. Bu bölümde u düğümüne komşu olan bütün düğümlerin etiketleri güncellenir. While döngüsü |V| kere tekrarlanır [14]. Bu program çalıştırıldıktan sonra, s düğümünden t düğümüne olan en kısa yolun okunması ise şu kod ile yapılabilir [16].

```
1       S = boş dizi
2       u = t
3       S = u + S   /* u düğümünü S serisinin başına ekliyor */
4       if  u = s
5           end
6       u = p[u]
7       go to 3
```

Bu kod ise düğümleri başlangıç düğümüne ulaşana kadar önceliklilerine bakarak başlangıç düğümüne ulaşana kadar S serisine yazarak algoritma ile hesaplanmış en kısa yolun bu seriye yazılmasını sağlar.

4. IP SERVİS KALİTESİ / QoS (QUALITY OF SERVICE)

IP ağlarında QoS, en basit anlamda, IP paketlerini belirli kriterlere göre ayırma ve ayrıştırılan IP paketlerine farklı muamele yapma olarak tanımlanabilir. IP ağlarında iki farklı QoS mekanizması vardır. IntServ (Tümleşik Hizmetler), DiffServ (Farklandırılmış Servisler). Günümüz IP ağlarında herhangi bir QoS mekanizması kullanılmaması durumunda paketlere "best-effort" gereğince muamelede bulunulur. Yani hiçbir veri tipi ayrıştırması yapılmaz, gelen her paket gönderilmeye çalışılır. Şekil 4.1 'de best-effort, IntServ ve DiffServ'in çalışma şekli basitçe resmedilmiştir.



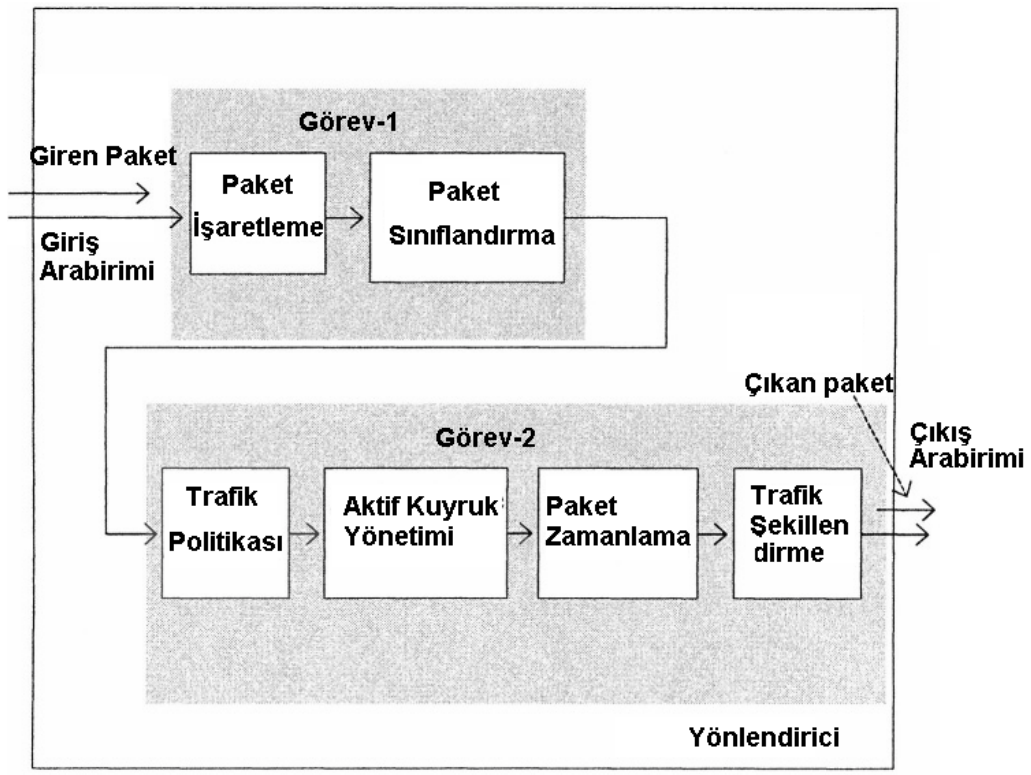
Şekil 4.1. Best-effort, IntServ ve DiffServ çalışma şekli

Best-effort'ta gelen tüm paketler trafik özelliklerine bakılmaksızın tek bir küme halinde işlem görür. DSCP(Differentiated Services Code Point) alanı "0" olarak işaretlenir [18]. IntServ'de her bir trafik türü, IP ağına gelmeden önce hedefe ulaşıncaya kadarki yol boyunca, uçtan uca gerekli kaynak ayrımı yapılır. DiffServ'de, her bir trafik türüne uçtan uca kaynak ayırma yerine trafik türleri arasında sınıflandırma yapılır. Bu trafik sınıflarına her bir düğümde (hop/yönlendirici) gerekli kaynak sağlanarak işleme sokulur.

IP ağlarında QoS uygulaması yapılabilmesi için, ağ elemanlarının iki temel özelliği sağlıyor olması gerekir.

1. Trafik ve servis tipleri arasında ayrım yapma.
2. Kaynak ayırabilmek ve farklı servis seviyeleri sunabilmek için farklı trafik tiplerine farklı muamele yapabilme.

Şekil 4.2'de görüldüğü gibi bunlardan birincisini, ağda QoS yapacak cihaz (yönlendirici) trafiğin girdiği arabirimde paket işaretleme ve paket sınıflandırma yaparak gerçekleştirir.



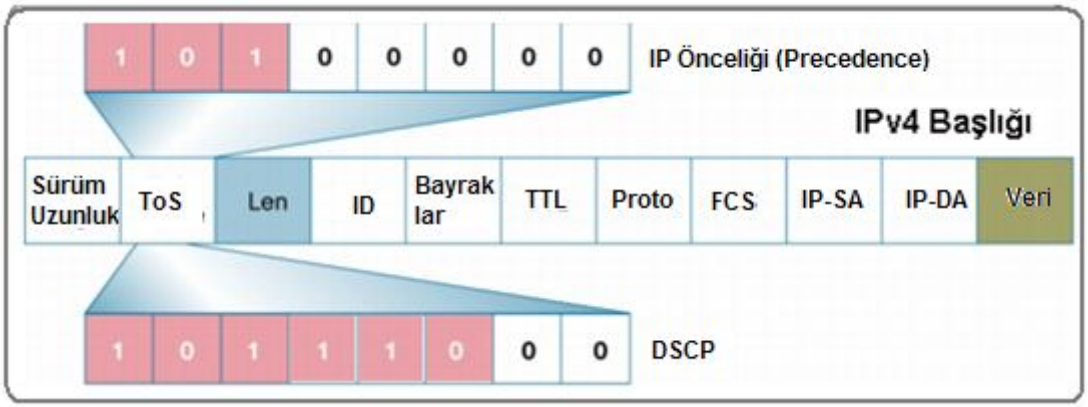
Şekil 4.2. QoS yapacak cihazın gereksinimleri

İkincisini, yönlendirici çıkış arabiriminde trafik politikası, aktif kuyruk yönetimi, paket zamanlama ve trafik şekillendirme yaparak gerçekleştirir.

4.1. Paket İşaretleme

Genel olarak bir IP paketini diğerlerinden ayırmak için IP paket başlığındaki ilgili alanların "bit" ile işaretlenerek belirli değerlerin ayarlanmasına paket işaretleme denir. Örneğin paketleri kaynak IP adresi, hedef IP adresi veya her ikisini kullanarak ayırabiliriz. Ya da Şekil 4.3'de görülen IP paket başlığındaki ToS (Type of Service)

içinde yer alan DSCP (DiffServ Code point) alanını belirli bir değere ayarlayarak da paket işaretleme gerçekleştirilebilir [19].



Şekil 4.3. ToS ve DSCP alanları

Paketler yönlendiricilere işaretlenmiş olarak da gelebilir ancak her ne kadar işaretli gelse de servis sağlayıcılar başkasının işaretlediği paketlerin işaretine güvenmeyip kendileri sınır yönlendiricilerinde işaretleme yaparlar.

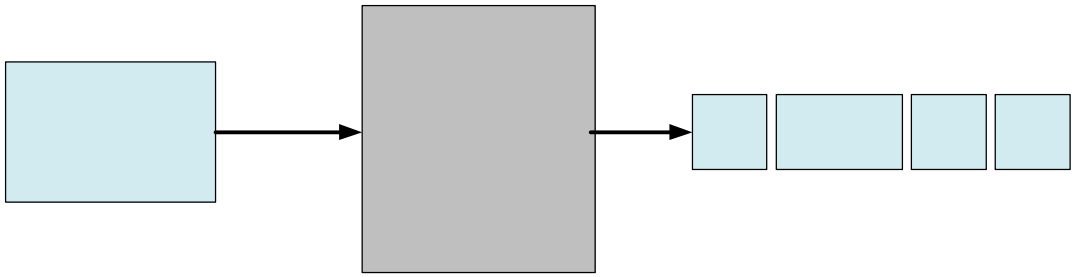
4.2. Paket Sınıflandırma

Paketlerin belirli bir kurala göre gruplandırılmasıdır. Her ne kadar işaretleme ile karıştırılsa da temelde çok farklı konulardır. Bunu şöyle örneklendirebiliriz, bir sınıftaki 20 öğrenciyi 1'den 20'ye kadar numaralandırma işini işaretlemeye benzetebiliriz. Öğrencilerden 1'den 10'a kadar numaralandırılanları bir grup, 11'den 20'ye kadar olanları başka bir grup yapma işini de sınıflandırmaya benzetebiliriz.

İki tür paket sınıflandırma tekniği vardır [20];

1. Çoklu-Alan Sınıflandırma (MF, Multi-Field)
2. Bütüncül Davranış Sınıflandırması (BA, Behavior Aggregate)

MF sınıflandırma Şekil 4.4'de görüldüğü gibi paket başlık bilgilerinden herhangi birini veya birkaçının kombinasyonunu kullanarak sınıflandırma yapabilir.

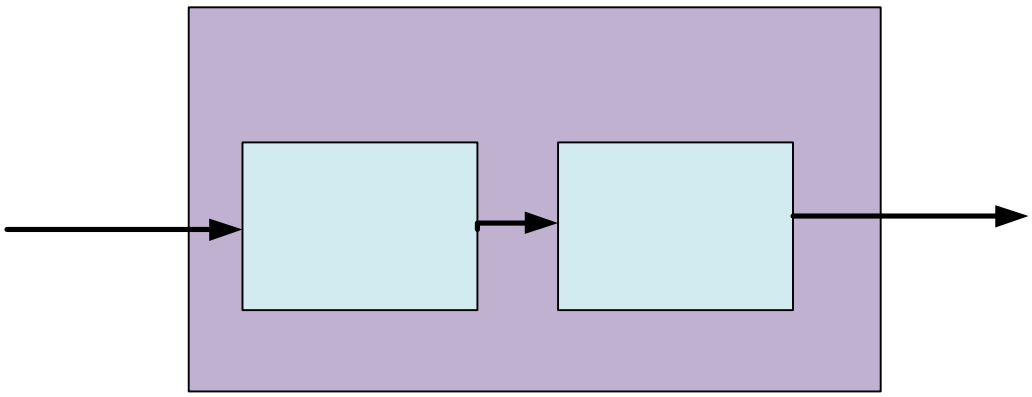


Şekil 4.4. MF sınıflandırıcı

BA sınıflandırıcı IP başlığının DSCP değerini değiştirerek sınıflandırma yapar.

4.3. Trafik Politikası/Kurallama

Servis veren taraftaki yönlendiricilerin giriş arabiriminden giren trafiğin müşteriyle anlaşılan seviyede olup olmadığını kontrol eder. Trafik politikası, önceden ayarlanan trafik oranına göre trafiği ölçme ve trafik ölçüm sonucuna göre de trafiği işaretlemeden oluşur. Şekil 4.5 'de trafik politikasının bileşenleri görülmektedir.



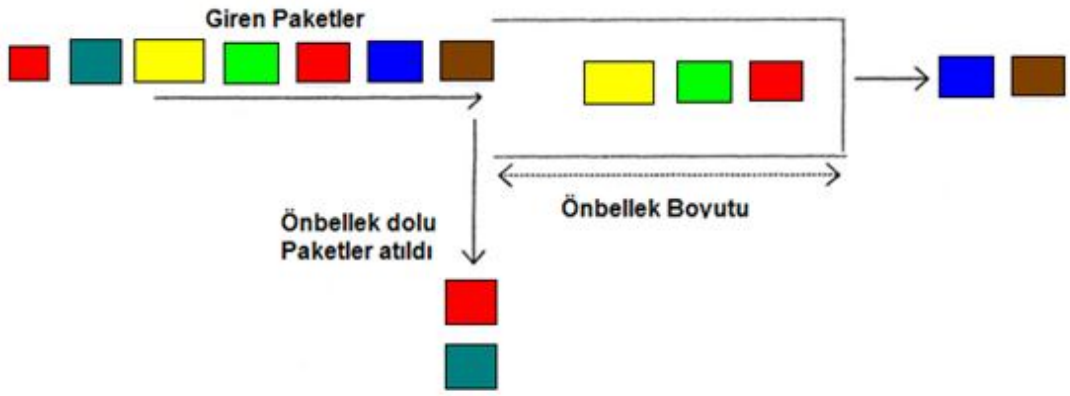
Şekil 4.5. Trafik politikası bileşenleri

Trafik politikası, arabirime gelen trafiği ya sadece CIR (Committed Information Rate) ya da CIR ve PIR'ın (Peak Information Rate) her ikisine göre kontrol eder. Bunlardan ikincisine göre, yani CIR ve PIR'ın ikisine göre kontrol etmek için ilave parametre olarak PBS (Peak Burst Size), CBS (Committed Burst Size), EBS (Excess Burst Size) kullanmaktadır [20].

4.4. Aktif Kuyruk Yönetimi

Yönlendiriciden paketler gönderilmeden önce kuyrukta belirli kurallar çerçevesinde sıralanır. Örnek vermek gerekirse, bir kuruluşun müşterilerinin işini hallederken görevlendirdiği bir yetkilisinin sıradaki yaşlı ve hamile kişileri sonra gelmiş olsalar bile sıranın en başına alması ve sırayı yönetmesi gibi düşünmek mümkündür.

Yönlendiricilerde eğer kuyruk yönetimi yapılmıyorsa varsayılan metot, Şekil 4.6'da görüldüğü gibi kuyruk sonuna kalanın atılmasıdır (Tail drop).

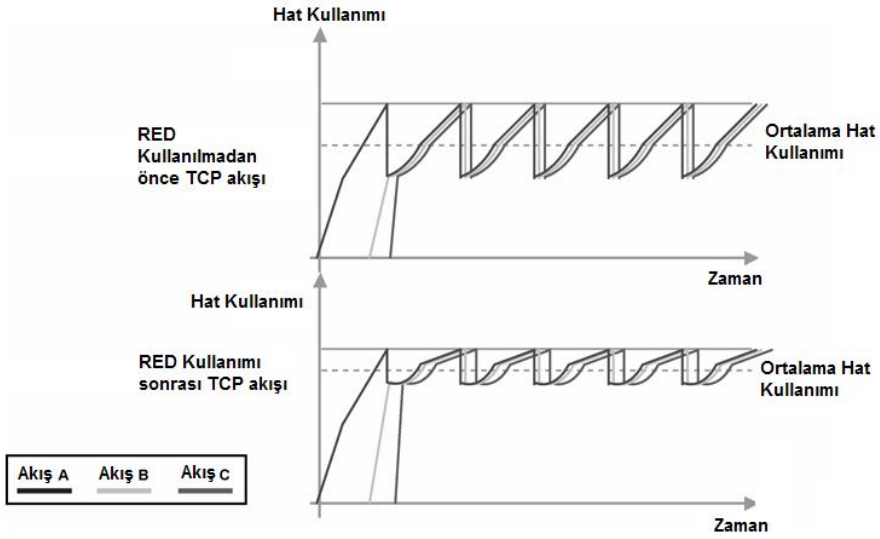


Şekil 4.6. Kuyruk sonuna kalanın atılması (Tail drop)

Paketin gönderildiği arabirim dolmuşsa, bu durumda çıkış kuyruğu da dolmakta ve kuyruk dolduktan sonra gelen paketler çöpe atılmaktadır. Bunun avantajı basit olmasıdır. Ancak TCP global senkronizasyonuna neden olması gibi ciddi bir dezavantajı bulunmaktadır.

TCP global senkronizasyon sorunu şu şekilde oluşur. Yönlendirici cihazın çıkış arabiriminde önbellek dolması sonucu bazı TCP paketlerinin çöpe atılması sonucu TCP paketlerini gönderen makineler hedef makinelerden bazı paketlerin alınamadığını gösteren NACK (Negatif-ACK) paketleri alırlar. Bunun sonucunda kaynak makineler gönderim hızlarını düşürerek çöpe atılan paketleri tekrar gönderirler. Senkronizasyon sağlandığı anda tekrar paket hızlarını arttırırlar. Şekil 4.7'de görüldüğü gibi bu işlemi birçok makinenin yapması sonucunda yönlendirici cihazın çıkış arabirimde, trafiğin alt ve üst değerleri arasındaki yüksek farkla salım

yaptığı görülür ve bu sürüp gider. Bu da ağ kaynaklarının etkin kullanımına engel olur.



Şekil 4.7. RED kullanılan ve kullanılmayan ortamda TCP trafik akışı [20]

Aktif kuyruk yönetimi (AKY), yönlendirici cihazların arabirim önbelleklerinin dolması sonucu tıkanıklıkları ve bundan dolayı veri kayıplarını önlemek amacıyla kullanılır. TCP global senkronizasyon sorunlarını da önlemiş olur. Yaygın kullanılan Aşağıdaki AKY metotları ayrıntılı olarak incelenecektir.

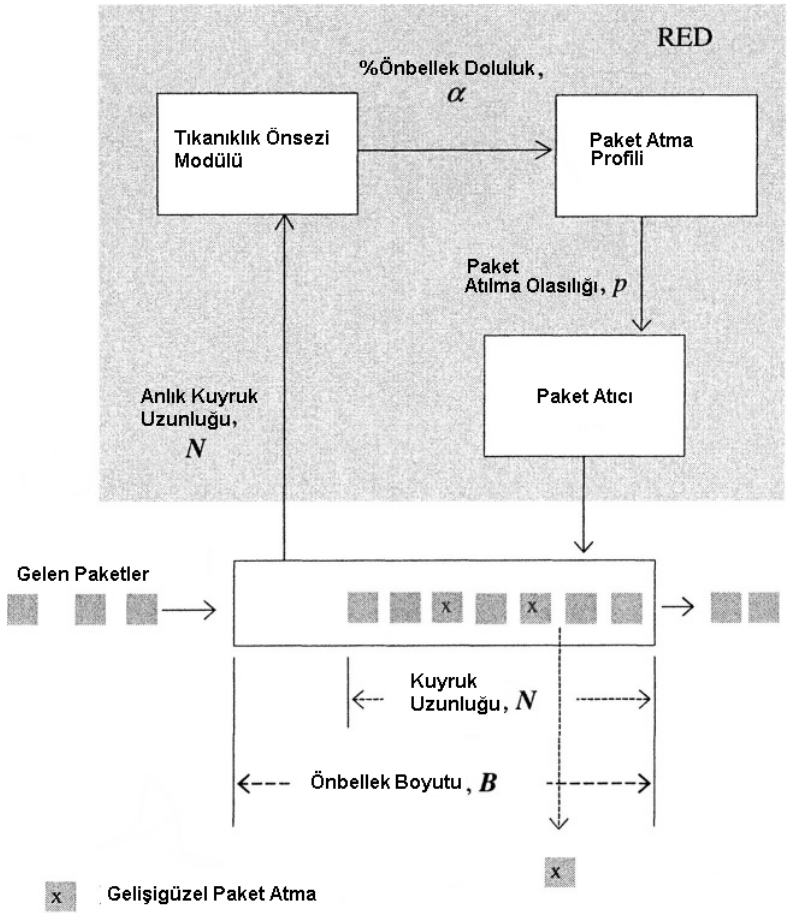
- RED (Random Early Discarding/ Gelişigüzel Erken Atma)
- WRED (Weighted Random Early Discarding / Ağırlıklandırılmış Gelişigüzel Erken Atma)

4.4.1. RED

Yönlendirici arabirimindeki tıkanma artmaya başladığı anda fark edip paketleri gelişigüzel atmaya başlar. Paketlerin drop edilmesini kaynağın fark etmesi ile kaynak gönderim hızını düşürür ve bu şeklide tıkanıklık giderilir. RED, tıkanma büyümeden müdahale ediyor ve tıkanmanın büyük bir problem olmasını engelliyor.

RED'in çalışma şekli, Şekil 4.8'de görüldüğü gibi tıkanıklık önsezi modülü, trafiğin önbellekte nasıl davrandığını ve anlık artışlarını takip eder. Oldukça karmaşık bir

algoritma ile kuyruk uzunluğunun artış eğilimini zamana göre tespit edilerek kuyruk uzunluğu eğilimi değeri hesaplanır. Hesaplanan bu değer her ne kadar ortalama değer olarak ifade edilse de anlık artışlar esas alınarak değerlendirmeler yapıldığından tam olarak ortalamayı veya anlık değeri vermez. Ani trafik artışlarından dolayı kuyruk uzunluğunun genel eğilimini verir.

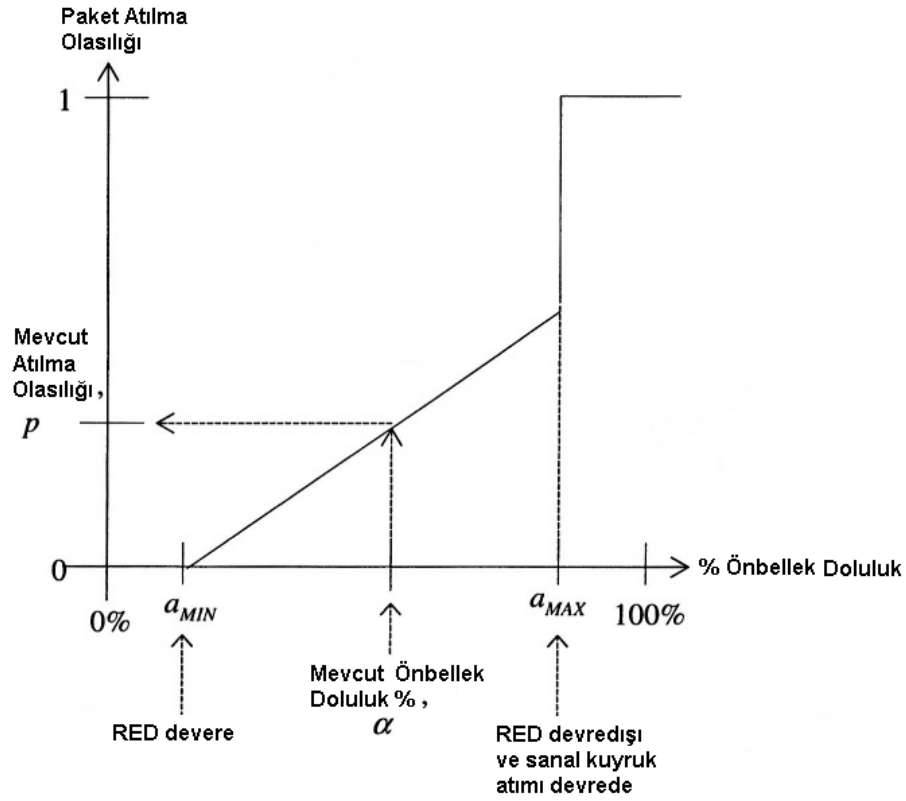


Şekil 4.8. RED'in çalışma şeması [20].

Kuyruk uzunluğu N ile önbellek boyutu B ile kuyruk uzunluk eğilimi η_N ile ve önbellek doluluk yüzdesi α ile ifade edilecek olursa, önbellek doluluk yüzdesi aşağıdaki şekilde hesaplanır.

$$\alpha = \frac{\eta_N}{B} \tag{4.1}$$

RED' de kullanılan bir diğer modül paket atma profilidir. Paket atılma olasılığının (p) hesaplanmasında paket atma profili kullanılır. Şekil 4.9'da önbellek doluluk yüzdesine göre paket atılma olasılığı grafiksel olarak görülmektedir. Kuyruk doluluk yüzde (α) değeri, önceden atanan α_{MIN} değerinin üzerine çıkmadığı sürece paketler atılmaz. Eğer α, α_{MIN}'i geçerse RED devreye girer. α_{MAX}'ın üzerine çıkarsa kuyruk, sanal kuyruk atımı (virtual tail drop) şeklinde çalışır. Bu durumda önbellek tamamen dolmuş gibi davranmaya başlar.



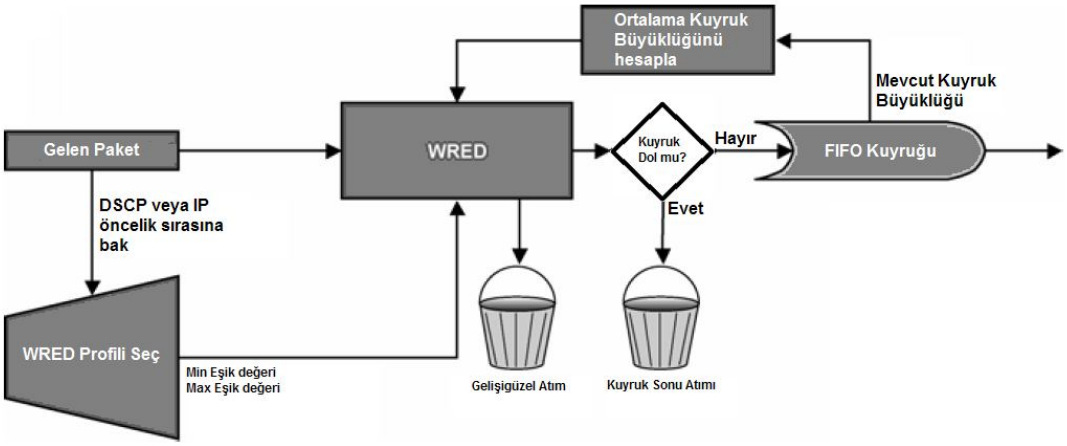
Şekil 4.9. RED paket atılma profili

α, α_{MIN} ve α_{MAX} arasında bir değer almışsa bu durumda p (Mevcut atılma olasılığı), önceden tanımlanan $p = f(\alpha)$ eşitliği ile hesaplanır. Bu değer şekilde doğrusal gibi görünse de gerçekte farklı formlarda olabilir. RED'in ne kadar etkin olduğunu p, α_{MIN} ve α_{MAX} parametreleri belirler. α_{MIN} ve α_{MAX} ne kadar büyükse RED o kadar etkin olur. Yine, p'nin eğiminin dikliği ölçüsünde RED etkin olur. RED'in etkinliğinden kastımız erken devreye girmesi ve erkenden sanal kuyruk atımının devreye girme süresinin kısa olması anlamına geliyor. Tıkanma anında RED, paketleri gelişigüzel

atarak TCP global senkronizasyon probleminin oluşmasını engeller. Bununla beraber UDP iletimi, bağlantısız olmasından dolayı atılan paketleri fark edemeyeceği için UDP paketlerine herhangi bir etkisi yoktur. Bundan dolayı, trafiğin büyük bölümü UDP olan ortamlarda RED kullanılması tavsiye edilmemektedir. RED kullanımında parametreleri doğru seçme kadar, RED'in uygulanacağı trafiğin davranışını bilme de önemlidir. Aksi halde gereksiz yere aşırı paket atımı ve dolayısı ile gereksiz kaynak kullanımı gerçekleşecektir [20].

4.4.2. WRED (Weighted random early discarding)

RED'de bir tane paket atma profili varken WRED'de birden fazla paket atma profili bulunur. Yani, her bir kuyruk için ayrı bir paket atma profili tanımlanabileceği gibi, tek bir kuyruk için birden fazla paket atma profili de tanımlanabilir. WRED profil seçimi DSCP ve IP Precedence (IP öncelik sırası) tabanlıdır. Bunlardan IP öncelik sırası kullanıldığında 8 profile kadar, DSCP kullanıldığında 64 profile kadar çıkılabilir. Bu durumda IP öncelik sırası veya DSCP ile işaretlenen paketlerden önemsiz olanlar, önemli olan paketlere göre daha hızlı atılır. WRED'de de RED gibi min ve max değerler her bir profil için ayrıca ayarlanabilir, buna göre paketler işlem görür. Max değer aşımı durumunda, RED'de olduğu gibi tail drop çalışmaya başlar ve gelen her paket işaretine bakılmaksızın atılmaya başlanır. WRED'in çalışma şekli Şekil 4.10 gösterilmektedir. Yönlendirici, WRED'i düzenli olarak hesaplanan ortalama kuyruk büyüklüğü hakkında bilgilendirir. Paketler çıkış arabirimine geldiğinde DSCP ve IP öncelik sırası bilgilerine bakılarak WRED profili seçilir. Buradan paketler WRED işlemine gönderilir. WRED mevcut paketin atılma ihtimalini hesaplar, buna göre ya paketi atar ya da çıkış kuyruğuna gönderir.



Şekil 4.10. WRED çalışma şekli

Çıkış kuyruğu dolu ise paket zaten atılır. Değilse paket kuyruğa yerleştirilir. Ortalama kuyruk uzunluğu min eşik değerinden büyük ve max eşik değerinden küçükse WRED, paketi ya kuyruğa yerleştirir veya gelişigüzel atar.

4.5. Paket Zamanlama

Şu ana kadar olan süreç özetlenirse; paketler yönlendiriciye bir arabirimden gelirler. Giriş arabiriminde paketlerin işaretlenip işaretlenmeyeceğine ve sınıflandırma yapılıp yapılmayacağına kara verilir. Yönlendirme tablosuna bakılarak paketin hangi arabirime gönderileceğine karar verilir. Çıkış arabirimine gönderilen paketin gönderim hızının garanti edilen seviyenin üzerinde olup olmadığı, garanti edilen hızın üzerine çıkan trafiğe uygulanacak politika kontrol edilir. Daha sonra çıkış arabiriminin önbelleğinin dolmasını engellemek için uygulanan kuyruk yönetimi kontrol edilir. Önbelleğin dolmasını engellemek için uygulanan kuyruk yönetim metotları uygulanarak atılmadan gönderilecek paketler kuyruğa gönderilir. Kuyruğa gelen paketler gönderilmek için sıraya giren paketler olarak düşünülebilir. Burada paketlerin gönderim sırası yani hangisinin önce hangisinin sonra gönderileceğine paket zamanlama modülü karar verir. Paket zamanlayıcıyı anlatmak için trafiğin tamamen sıkıştığı bir otoyolda bir ambulans veya polis aracına tüm arabaların yer vermesi, o aracın hepsinden önce hedefine ulaşmasının sağlanması için yol açılmasına benzetilebilir.

Paket zamanlama, QoS mekanizmasının kalbidir denilebilir. Bu kadar önemli olmasına rağmen maalesef standart bir yapısı olmayıp üretici bağımlıdır. Yukarda anlatıldığı gibi paket zamanlama da çıkış arabiriminde uygulanır. Aşağıdaki paket zamanlama metotları sırayla incelenecektir.

- FIFO (First-in-First-out - İlk ielen ilk gönderilir)
- PQ (Priority Queuing – Öncelikli kuyruklama)
- FQ (Fair-Queuing – Eşit kuyruklama)
- WRR (Weighted Round Robin - Ağırlıklandırılmış sıralı döngü)
- WFQ (Weighted Fair Queuing – Ağırlıklandırılmış eşit kuyruklama)
- CBWFQ (Class-Based WFQ – Sınıf tabanlı WFQ)

4.5.1. FIFO (First-in-first-out)

Herhangi bir paket zamanlama metodu kullanılmadığı zaman varsayılan paket zamanlama metodu olarak FIFO kullanılır. En basit metottur. Bir adet kuyruk vardır. Şekil 4.11'da görüldüğü gibi ilk önce gelen paket ilk önce gönderilir.

Şekil 4.11. FIFO

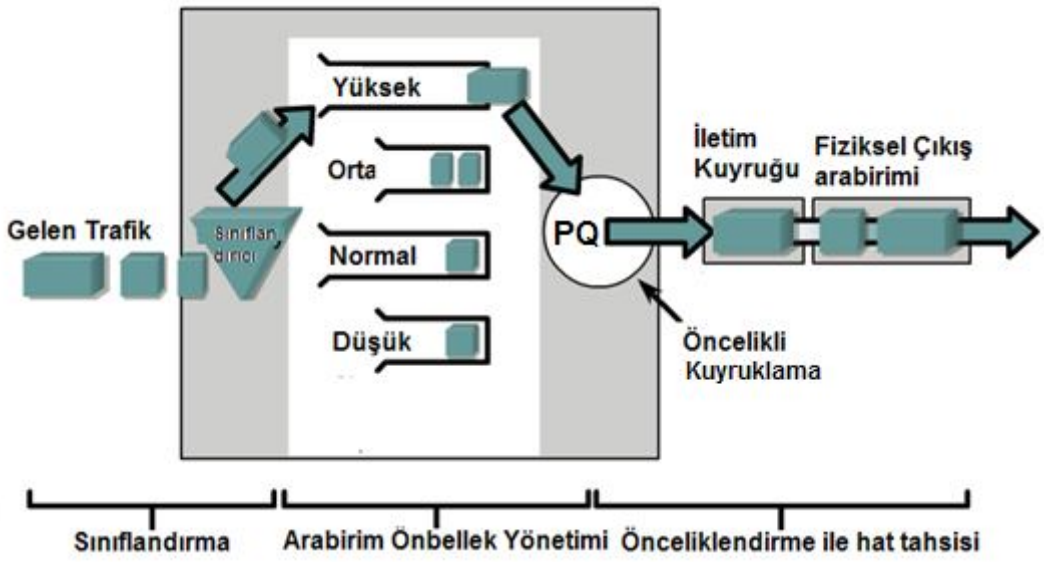
FIFO tüm paketlere eşit davranır. Dolayısıyla best-effort trafik iletimi için idealdir. En büyük dezavantajı trafik sınıflarını ayıramamasıdır. Bundan dolayı sıkışma durumunda tüm trafik türleri aynı derecede etkilenir. Kritik veri iletimi yapılan ortamlarda kullanılması önerilmez.

4.5.2. PQ (Priority queuing)

PQ, trafik sınıfları arasında ayrım yapabilir. Paket zamanlaması, öncelik sırası ve yüksek öncelikli kuyrukta paket olup olmadığına bakılarak gerçekleştirilir. Herhangi paket, ancak kendinden daha öncelikli trafik sınıfına ait paket yoksa gönderilebilir.

Kedisinden daha öncelikli trafik olması durumunda öncelikliler bitene kadar bekletilir. Bunu, sıkışık trafikteki bir ambulansa benzetebiliriz. PQ'nun çalışma şekli Şekil 4.12'de özetlenmiştir.

En büyük avantajı basit olması ve trafik sınıflarını tanıyabilmesidir. Bununla beraber en büyük dezavantajı, yüksek öncelikli ses, sinyalleşme gibi verilerin olduğu yerlerde düşük öncelikli trafiklerin çok az gönderilebilmesidir. Yani, düşük öncelikli paketlere çok önem verilmemektedir.



Şekil 4.12. PQ çalışma şekli

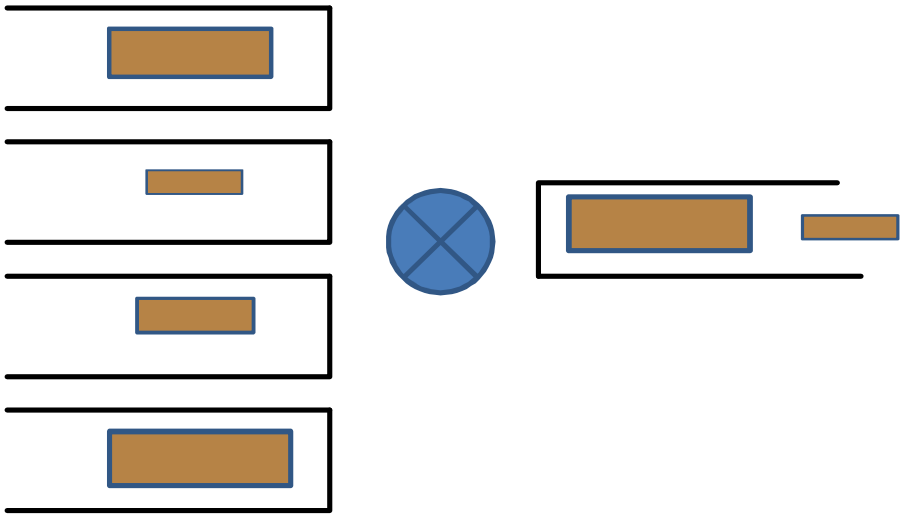
IP üzerinden ses ve görüntü gibi gerçek zamanlı trafik taşımada idealdir. Ancak TCP trafiğinin çok olduğu ortamlarda PQ kullanımı sıkışıklığı arttırabilir. Bundan dolayı TCP trafiğinin yoğun olduğu terlerde PQ kullanırken dikkat edilmelidir. Bu sorunu çözmek için de rate-controlled PQ geliştirilmiştir. Öncelikli trafik önceden belirlenen bir doyum noktasına ulaşmadığı sürece öncelik verilir, ancak doyum noktasına ulaşan trafik için önceliklendirme garanti edilmez.

4.5.3. FQ (Fair-queuing)

Akış bazlı olarak da nitelendirilen FQ, trafik sınıflarını ayrı ayrı kuyruklama özelliğine sahiptir. FQ'da gelen her bir paket farklı kuyruk sınıflarına ayrılır.

Sözgelimi, N adet kuyruk sınıfı oluşturulmuşsa her bir kuyruğa 1/N kadar çıkış arabiriminin bant genişliğinden tahsis edilir. Paket zamanlayıcı, boş sınıfları atlayarak dolu sınıfların hepsini sırayla kontrol eder ve her kontrolde her kuyruk sınıfından bir paketi kuyruktan çıkışa gönderir. Yeni bir trafik tipi geldiğinde ayrı bir kuyruk sınıfı oluşturularak aynı tip trafikler buraya yerleştirilir. N adet olan kuyruk sayısı N+1 'e yükseldiği için her bir kuyruk sınıfına tahsis edilen bant genişliği de otomatikman 1/(N+1) olur.

FQ'nun en büyük avantajı basit olmasıdır. Bununla beraber iki önemli dezavantajı vardır. Bunlardan biri kuyruk sınıflarındaki paketlerin bant genişliği, ihtiyaçlarına göre bant tahsisi yapılamayıp, her kuyruk sınıfına eşit bant genişliği tahsisi yapmasıdır. Diğeri, paket zamanlayıcısının kuyruk sınıflarını her kontrolünde paket boyutlarına bakmadan her kontrolde ilgili kuyruktan bir paket göndermesidir. Bu durumda her bir kuyruk sınıfına bant genişliği eşit dağıtılamayıp, paket boyutu büyük olanlara daha fazla bant tahsis edilmektedir. Bunun etkisini göstermesi açısından Şekil 4.13 iyi bir örnektir.



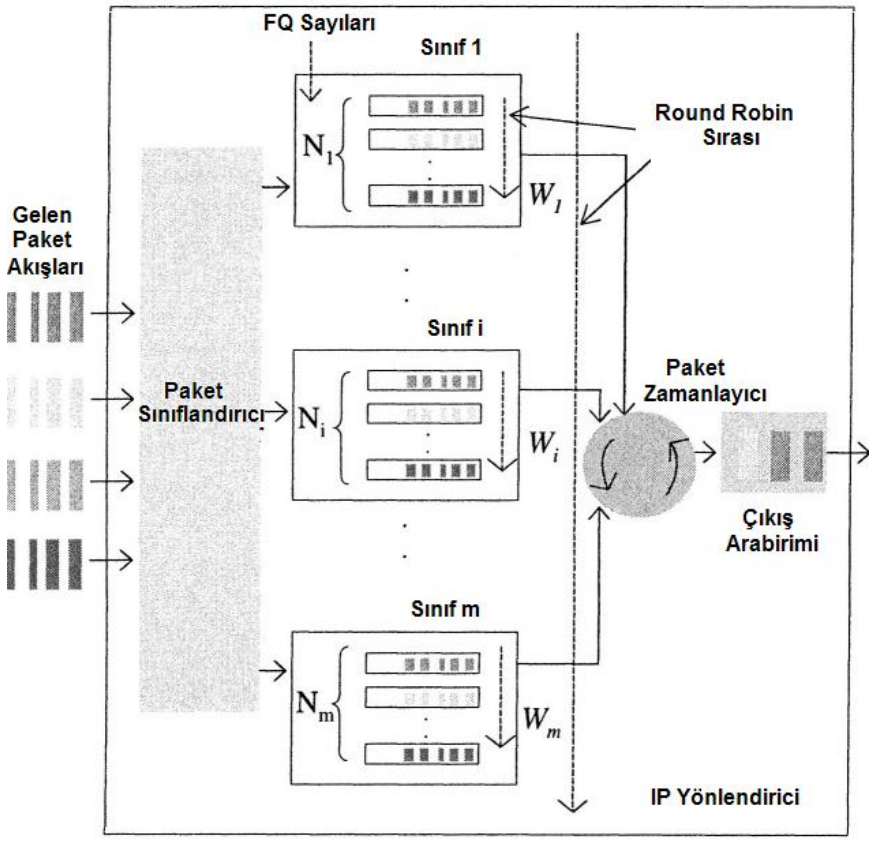
Şekil 4.13. FQ çalışma şekli

Şekil 4.13'e göre akış-1 için 200/1000 oranında yani %20 akış-2 için 50/1000 oranında yani %5, akış-3 için 100/1000 yani %10 ve akış-4 için 400/1000 yani %40 bant genişliği tahsis edilecektir. Ses paketlerinin UDP ile taşındığı UDP'nin paket

boyutunun da TCP'ye göre küçük olduğu düşünüldüğünde FQ'nun, kritik verilerin çok olduğu yerlerde iyi bir yöntem olmadığı açıktır.

4.5.4. WRR (Weighted round robin)

WRR, sınıf tabanlı kuyruklama (class-based queuing) olarak da adlandırılır. FQ'nun dezavantajlarından biri olan bant genişliğinin ihtiyaca göre tahsis edilememesini sorununu ortadan kaldırarak, kuyruk sınıflarındaki trafiklerin bant genişliği ihtiyacına göre tahsis yapabilir. Şekil 4.14, WRR'ın çalışmasını göstermektedir. Buna göre gelen trafik akışları "m" adet sınıf olacak şekilde gruplanır.



Şekil 4.14. WRR çalışma şekli

Her bir sınıfa, bant genişliği ihtiyacına göre %100 üzerinden ağırlık verilir. Bu durum Eş. 4.2 ile ifade edilebilir [20].

$$\sum_{i=1}^{m} W_i = 100\% \qquad (4\text{-}2)$$

Burada; trafik sınıflarının sayısını "m", i. sınıfın yüzde ağırlığını W_i göstermektedir. Her bir sınıf içindeki akışları ayrı bir round-robin zamanlayıcısı yönetir. N_i , her bir sınıf içindeki FQ sayısını gösterir. WRR içindeki toplam FQ sayısını Eş. 4.3 göstermektedir.

$$\mathrm{FQ} = \sum_{i=1}^{m} N_i \tag{4.3}$$

Şekil 4.14'de görüldüğü gibi WRR'da iki farklı round-robin işlemi çalışmaktadır. Bunlardan birisi sınıflar arasında çalışırken, diğeri her bir sınıf içindeki FQ'lar arasında çalışır. Round robin zamanlayıcısının her sınıftaki işlem süresi, o sınıfa ayrılan bant genişliği yüzdesini gösterir. Zamanlayıcı i. sınıfında iken, bu sınıf içindeki her bir kuyruğa $1/N_i$ kadar zaman ayırır. Bu durumda i. sınıf içindeki j. kuyruğa atanan ağırlık $W_{ij}=W_i x(1/N_i)$ eşitliği ile ifade edilebilir. Sınıflar içindeki her bir kuyruğa ayrılan zaman bu kuyruğun ağırlığını da gösterdiğinden, $w_{ij}=1/N_i$ eşitliği, i. sınıf içindeki j. kuyruğa verilen ağırlığı (w_{ij}) gösterir. Bu durumda, i. sınıftaki j. kuyruğun ağırlığı Eş. 4.4'deki gibi ifade edilir.

$$W_{ij}=W_i x(1/N_i) \tag{4.4}$$

Sonuç olarak, i. sınıfın yüzde olarak ağırlığını (W_i), Eş. 4.5 göstermektedir.

$$W_i = \sum_{j=1}^{N_i} w_{ij} \tag{4.5}$$

4.5.5. WFQ (Weighted fair queuing)

WRR, FQ'nun eksik yönlerinden biri olan bant genişliğini trafik sınıflarının ihtiyacına göre dağıtılmasını karşılarken paket boyutlarıyla ilgili olanı karşılamamaktadır. WFQ, bu eksikliği gidermektedir. FQ'daki gibi gelen trafik akışları m adet kuyruğa ayrılır. Her bir kuyruğa eşit miktarda bant genişliği ayırma yerine, kuyruklarda trafik akışlarının hesaplanan ağırlık değerlerine göre ayrılır. Bunu FQ'daki gibi zamanlayıcı her kuyruğa uğradığında paketlerin boyutuna

bakmadan birer adet gönderme yerine bit bazlı gönderme yapılır. Dolayısı ile büyük boyutlu paketlerin diğer kritik verileri ezmeden gönderimi sağlanmış olur.

Basit bir örnek vermek gerekirse, kuyruğun birinde 120 byte büyüklüğünde paketler varken, diğerinde 60 byte büyüklüğünde paketler bulunursa, zamanlayıcı her kuyruğa uğradığında 120 byte'lık paketlerin olduğu kuyruktan bir paket gönderiyorsa, diğer kuyruğa her uğradığında iki adet paket gönderecektir. Dolayısı ile bit bazlı bir WRR yapılacak gibi düşünülebilir.

4.5.6. CBWFQ (Class-based WFQ)

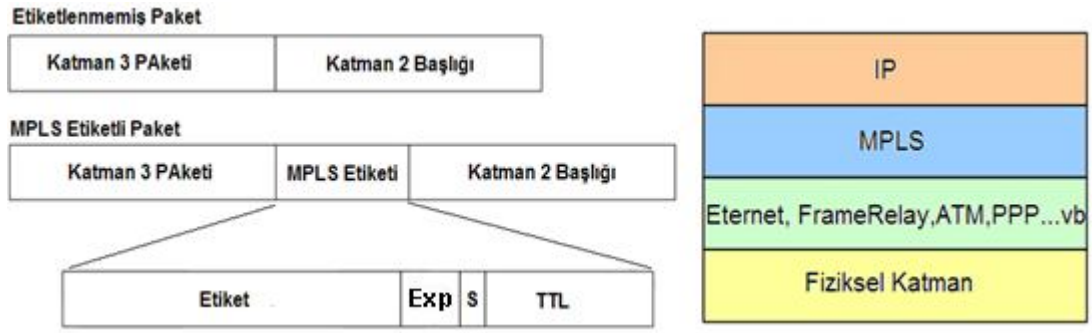
Gelen trafiğin sınıflara ayrılması her bir sınıfa ayrı bir ağırlığın verilmesi açısından bakıldığında CBWFQ, Şekil 4.14'te gösterilen WRR'ın çalışmasına benzerdir. WRR'da her bir sınıf içindeki trafik akışlarına FQ zamanlayıcısı ile işlem yapılırken CBWFQ'da ise her bir sınıf içindeki trafik akışlarına WFQ zamanlayıcısı ile işlem yapılır.

4.6. Trafik Şekillendirme

Patlamalı diye adlandırılan ve sürekli değişik hızlarda gelen yüksek hacimli trafiğin yönlendirici önbelleğine alınarak regülâsyona tabi tutulması ve çıkış önbelleğinden daha kararlı bir yapıda trafiğin gönderilmesidir. Trafik durdurulup sonra belirli bir hız verildiği için gecikmelere neden olmaktadır.

5. MPLS (MULTI PROTOCOL LABEL SWITCHING)

MPLS, adından da anlaşıldığı gibi etiket anahtarlama yapan IP'ye göre oldukça yeni bir paket iletim mekanizmasıdır. Şekil 5.1'de görülebileceği gibi MPLS etiketi, OSI katmanlı yapısı düşünüldüğünde katman 2 ile katman 3 arasında bulunur. IP'ye göre daha küçük olan etiket bilgileri kullanılarak paketler iletilir. Etiket genellikle, yönlendiricilere gelen IP paketinin hedef IP adresine uygundur ve iletim de buna göre yapılarak paketlerin doğru hedefe varmaları temin edilmiş olur. Kullanıma göre etiket bilgileri hedef IP adresi yanı sıra QoS ve kaynak IP gibi bazı kıstaslara da uygun olabilir. MPLS, sadece IP paketleri değil, 3. katmanda çalışan diğer protokol paketlerinin iletiminde de kullanılmaktadır.



Şekil 5.1. MPLS paket yapısı ve OSI'deki konumu

IP paketine eklenen her biri 32 bit uzunluğunda olan MPLS başlığı birden fazla olabilir. Bu başlıklarda teorik olarak 2^{20} -1 adet etiket kullanılabilir. Her bir başlıkta bulunan alanların açıklamaları aşağıda verilmiştir.

Etiket Alanı - 20 Bit: MPLS etiket değeri. 0-15 etiket değerleri rezerve edilmiştir. Bazı etiketlerin anlamları aşağıdaki gibi tanımlanmıştır.

"0" etiket değeri: Bundan sonra paketin IP'ye göre yönlendirileceğini yani etiketinin kaldırılacağını gösterir.

"1" etiket değeri: Yönlendirici uyarı etiketidir. Paketler bundan sonraki etikete göre yönlendirilirler.

“2” etiket değeri: Paketin etiketinin kaldırılıp, IPv6’e göre yönlendirileceğini gösterir.

“3” etiket değeri: bunları LSR’lar atayıp kaldırabilir. Enkapsüllemede hiçbir zaman görünmezler. En üstteki etiketin çıkartılıp kalan paketin etiketli ve etiketsiz olarak yönlendirileceğini gösterir.

Exp. - 3 Bit: MPLS paketlerine QoS ve DiffServ gibi servis kalitesinin uygulanabilmesini sağlar.

S Alanı - 1 Bit: Birden fazla etiket vermeyi sağlar. S=1 olması durumunda etiket yığınındaki son etiket olduğunu gösterir. S=0 ise diğer etiketleri gösterir.

TTL (Time to Live) - 8bit: Genellikle IP’deki TTL ile aynıdır. Paketlerin sonsuz döngüye girmesini önlemek için kullanılır [21].

Geleneksel IP paket yönlendirmede, yönlendirme işlemi 3. katman bilgilerine göre yapılır. Yani, yönlendirme hedef IP bilgisine uygun gerçekleştirilir. Paketin hedefe ulaşması için geçtiği her yönlendiricide paket, 3. katman başlığına kadar açılır bu başlıktaki hedef IP, yönlendiricinin yönlendirme tabloları ile karşılaştırılarak en uygun kayda göre ilgili çıkış arabiriminden sonraki yönlendiriciye gönderilir.

MPLS paket iletiminde etiket kullanması nedeniyle ve etiket iletim tabloları içinde arama yapmak, IP iletim tablolarında arama yapmaktan daha hızlı olduğundan, iletim daha hızlı olarak gerçekleştirilir. IP yönlendirmede her yönlendirici 100.000’lerle ifade edilen yönlendirme tablolarını tutmak zorundadır. Yine IP yönlendirmede eşit hızda olmayan hatlar arasında yük dağılımı yapmak pek mümkün olmamaktadır. Her ne kadar politika bazlı yönlendirme olsa da gerek aşırı kaynak kullanımı ve gerekse ölçeklenebilir olmayışından pek tercih edilmez.

MPLS ile birlikte gelen ve belki de MPLS’in en çok kullanılma nedenlerinden biri de trafik mühendisliğidir. Trafik mühendisliği, veri trafiği ağ boyunca gönderilirken kaynakların efektif kullanımı ve ağ performansını arttırmayı kontrol eden işlemdir denebilir [22]. Trafik mühendisliği ile klasik yönlendirme algoritmalarının

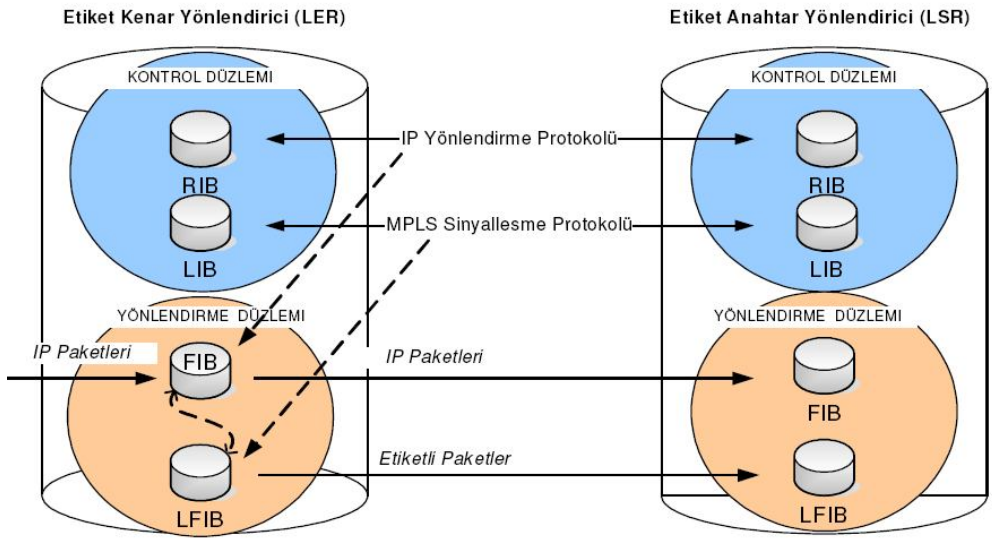
kullanıldığı ortamlarda gözlemlenen iki sorunun üstesinden gelinmiş olur. Bunlardan birisi en kısa yol olarak belirlenen yolların, bazı uzun yollardan daha elverişli olmadığı halde kullanılma riskidir. Diğeri de, en kısa yolun kullanılması neticesinde bu yolların tıkanması ve tıkanıklık devam ettiği halde boş olan alternatif yolların kullanılamamasıdır.

5.1. Etiket Anahtarlama Bileşenleri ve Yol Bulma

Geleneksel yönlendirmede, yönlendiricilerin dinamik yönlendirme protokolleri kullanarak ağ hakkında bilgi edinip, bu bilgileri kullanarak yönlendirme tabloları oluşturduklarını ve bu tablolar yardımıyla yönlendirme yaptıklarını biliyoruz. Paket anahtarlamada durum biraz daha karmaşık bir hal alıyor.

5.1.1. Kontrol ve yönlendirme düzlemleri

MPLS etiket anahtarlama ve geleneksel 3. katman yönlendirme yapan cihazlarda iki temel unsur bulunur bunlar kontrol ve yönlendirme düzlemleridir. Bunların birbirleriyle ilişkisi Şekil 5.2'de görülmektedir.



Şekil 5.2. Kontrol ve iletim düzlemi çalışma prensibi [24]

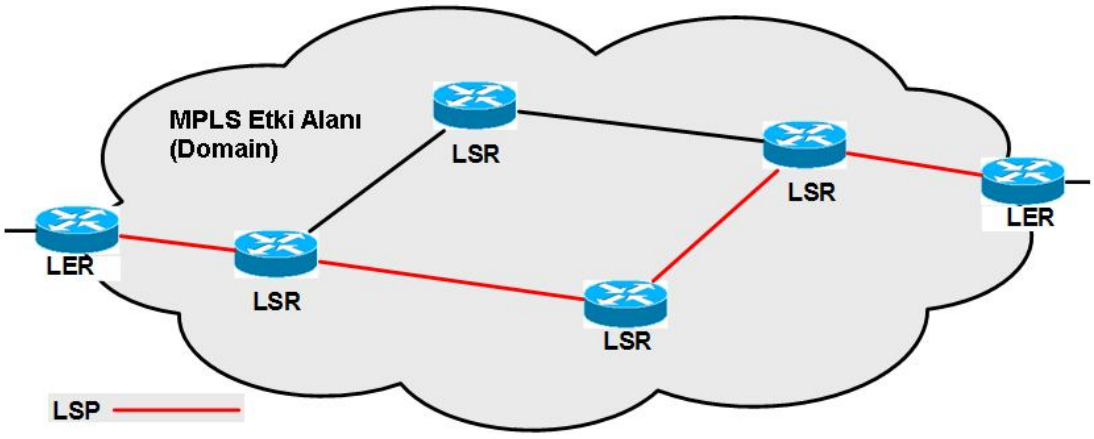
MPLS anahtarlama yapmayan yönlendiricilerde LIB (Lable Information Base), LFIB (Lable Forwarding Information Base), MPLS sinyalleşme protokolü bulunmaz.

Kontrol düzleminde bulunan OSPF, BGP gibi yönlendirme protokolleri kendi aralarında yönlendirme bilgilerini güncelleyerek yönlendirme bilgi tabanını (RIB) oluştururlar. Aynı şekilde MPLS sinyalleşme protokolleri de kendi aralarında etiket bilgi tabanı (LIB) oluştururlar. Ham bilgi içeren bu veritabanlarında bulunan bilgiler bir nevi tasnif edilerek ve düzenlenerek son şekline sokulur ve bunlardan yönlendirme bilgi tabanları oluşturulur. Hatırlanacağı gibi OSPF'de SPF algoritması (Dijkstra) ham link bilgileri üzerinde çalıştırılarak yönlendirme ağaçları elde ediliyordu.

Yönlendirme düzleminde 3. katman yönlendirme için iletim bilgi tabanı (FIB) ve MPLS için etiket iletim bilgi tabanı (LFIB) oluşturulur. Kontrol düzleminde yapılan işler yönlendirme düzlemine göre çok daha karmaşıktır.

5.1.2. MPLS etki alanı

Bir veya daha fazla MPLS özellikli yönlendiriciden oluşan yapıya MPLS etki alanı (domain) denir [23]. MPLS etki alanı içinde Şekil 5.3'te de görüldüğü gibi, iki farklı MPLS yönlendirici tipi bulunur, etiket kenar (LER) ve etiket anahtar yönlendirici (LSR).



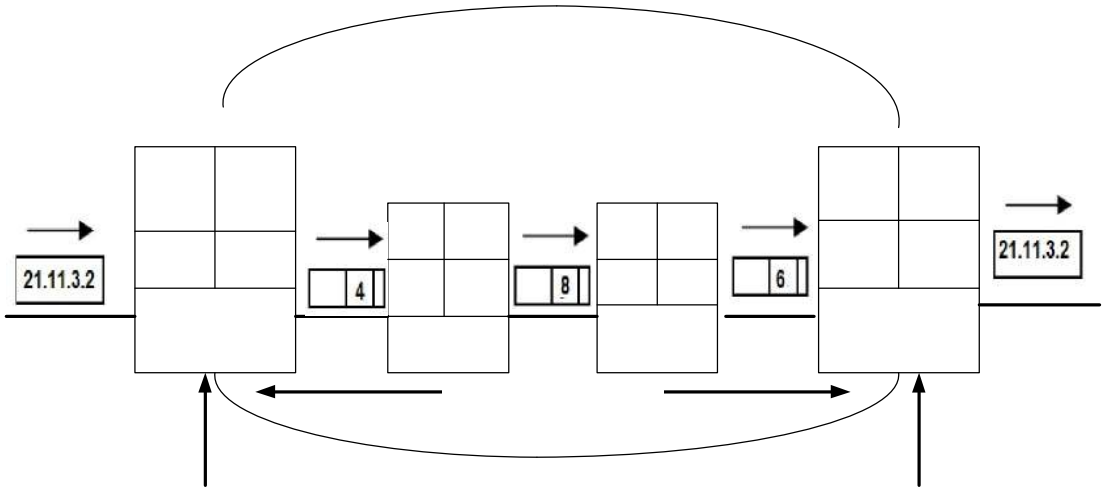
Şekil 5.3. MPLS etki alanı ve yönlendirici tipleri

LER (Lable Edge Router), MPLS domain'in giriş ve çıkışlarında bulunurlar. Etiket anahtarlamalı MPLS etki alanı ile klasik yönlendirme yapılan ağlar arasında köprü görevi üstlenirler. Temel fonksiyonları kendilerine gelen etiketsiz IP paketlerine

belirli kriterlere göre MPLS etiketi basmak ve MPLS etki alanından çıkışta da eklenen bu etiketi kaldırarak geleneksel yönlendirme yapmaktır. LSR (Lable Switching Router) yönlendiriciler ise MPLS etki alanı içinde bulunurlar ve sadece etiket anahtarlama yaparlar. LER yönlendiriciler hem LFIB ve FIB bilgileri bulundururken LSR'lar sadece LFIB bilgileri bulundururlar [25].

LSR'lar sadece etiket anahtarlama yaptıkları için gelen paketteki 20 bit uzunluğundaki en üst MPLS etiketine bakıp LFIB'de buna en uygun kaydı bularak son derece hızlı bir şekilde anahtarlama yaparlar [26].

MPLS yönlendiriciler, kendilerine gelen ve belirli kıstasları taşıyan paketlere aynı şekilde davranırlar [27]. Yani aynı etiket anahtarlama yolundan (LSP) gönderirler. Yönlendirme denklik sınıfı (FEC) diye adlandırılan bu sınıflar, yönlendirme protokollerinden alınan bilgiler ile etiket bilgileri kullanılarak oluşturulurlar. Genellikle hedef IP alt ağına göre, gelen paketin IP precedence değerine göre ve benzer birkaç farklı kritere göre oluşturulur. Belirli trafik sınıflarına (Ses, video,..vb) gereken hizmet kalitesinin sağlanabilmesi için de FEC'ler kullanılır. LER ve LSR'ın kendisine gelen bir paketi iletme biçimi Şekil 5.4'de basitçe gösterilmiştir.



Şekil 5.4. MPLS paket iletimi

Kısaca özetlemek gerekirse MPLS etki alanına giren ve 21.11.3.2 IP'li hedefe gitmek isteyen paket LER'e girdiği zaman paketin etiketsiz olduğu fark edilerek FEC kontrol edilir ve uygun bir FEC seçilerek etiket verilir. Buradaki denklik sınıfı, hedef IP alt ağına göre belirlenmiş olan FEC'dir (21.11.0.0/16). LER tarafından pakete 4 numaralı etiket verilir. LSR yönlendirici, kendisine belirli bir ara birimden gelen ve belirli bir LSP üzerinden iletilmesi gereken bu paketin etiketine bakar, kendi LFIB varitabanını kontrol eder ve pakete 8 numaralı etiketi vererek bir sonraki yönlendiriciye paketi gönderir. Sonraki LSR yönlendirici aynı şeklide kendisine gelen paketin etiketine bakarak 6 numaralı etiketi verip paketi iletir. Son olarak sınır yönlendirici tabir edilen LER yönlendiriciye gelen paket için FEC'e bakılır ve MPLS etiketleme kaydı bulunmadığından dolayı bu paketin bundan sonra etiketsiz olarak yönlendirme protokolleri ile iletileceği görülerek FIB veritabanlarını kayıtları kontrol edilir. Burada en uygun kayıt bulunarak paket sonraki yönlendiriciye gönderilir. Bu sırada LER paketin MPLS etiketini kaldırır. Paket, bundan sonra yönlendirilirken sadece IP başlığındaki hedef IP'sine (örnekte, 21.11.3.2) göre yönlendirilir. Başta da belirtildiği gibi LER yönlendiriciler MPLS etki alanının girişinde etiketsiz paketleri etiketleme, MPLS etki alanı çıkışında etiket sökme ve etiket anahtarlama ile 3. Katman yönlendirme işlemlerinin hepsini gerçekleştirebilme yeteneğine sahiptirler.

MPLS bölümünde birden fazla etiket olduğu durumda her bir yönlendirici anahtarlama işleminde en üstteki etiketi kullanır. Duruma göre bu etiket ya değiştirilir veya kaldırılır.

LSP'ler manuel veya dinamik olarak oluşturulabilir. Manuel oluşturmak esnek bir çözüm olmayıp ayrıca yönetimi zordur. Bunun yerine LSP'leri oluşturmak için MPLS sinyalleşme protokolleri olan LDP (Lable Distribution Protocol) veya RSVP (Resource Reservation Protocol) protokolleri kullanılır.

5.2. LDP (Etiket Dağıtım Protokolü)

Şekil 5.4'te görülen MPLS paket iletiminde her bir LSR kendisine gelen paketi bir LSP üzerinden taşır ve dolayısıyla o LSP'ye uygun olacak şekilde etiketleme yapılmalıdır. Yönlendiricilerin bu işlemi yapabilmesi için güçlü bir etiket veri

tabanının olması ve kendi aralarında bu etiketlerin ne anlama geldiğinin duyurulması gerekmektedir. Bu işlemler dinamik olarak etiket dağıtım protokolü (LDP) ile gerçekleştirilir. Dolayısı ile etiket anahtarlama yolları (LSP)'ler de dinamik olarak kurulur. LDP protokolü, yönlendiricinin belirli bir LSP üzerinden gönderilecek paketlere hangi etiketi vereceğini ve komşu yönlendiricilerin bu etiketlerle ilgili bilgilendirilmesini sağlar. Kontrol düzleminde çalışan LDP protokolü fonksiyonel olarak OSPF, BGP gibi yönlendirme protokollerine benzer. LSR tarafından bir paketin anahtarlanması için LFIB veritabanı kullanılır. LFIB veritabanının oluşturulabilmesi için LIB veritabanı gereklidir. LIB'de LDP ve RSVP gibi dinamik protokoller sayesinde oluşturulur [26]. LDP'nin temel fonksiyonları;

- Diğer LSR'ların keşfi
- Oturum kurma ve devam ettirme
- Etiket eşleştirmelerinin duyurulması
- Uyarı mesajlaşması

İlk aşamada LSR'lar birbirlerini "Hello" mesajları ile keşfederler. Sonraki aşamada TCP oturumu kurulur. TCP oturumu kurulması için TCP 646 portu keşif aşamasında da UDP 646 portu kullanılır. Kurulan bu bağlantı üzerinden etiket eşleştirme bilgileri yayınlanır. Eşleştirme bilgileri kullanılarak etiket kaldırma, duyurma ve değiştirme gerçekleştirilir. LDP uyarı mesajları ile komşular birbirlerine bilgilendirmede bulunurlar [26].

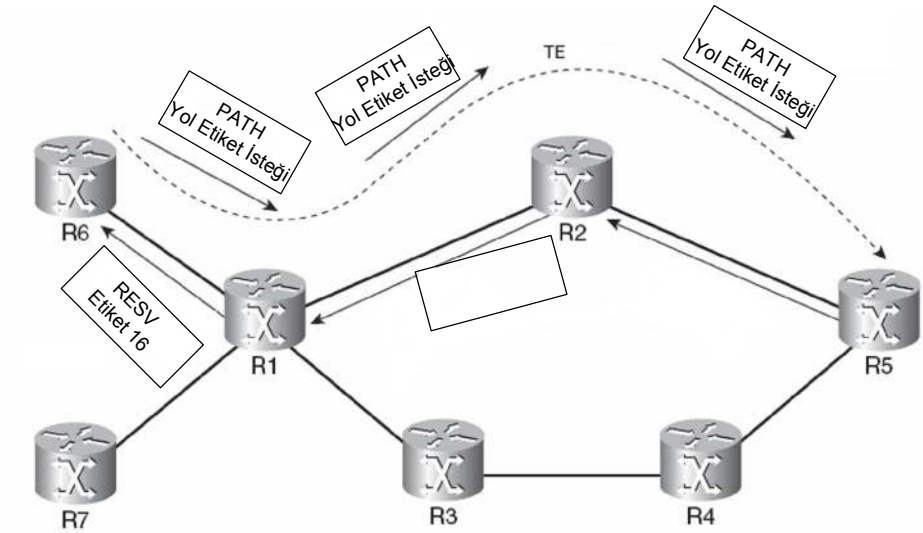
LDP protokolü "bağımsız" ve "düzenli" etiket atama yöntemlerini desteklemektedir. Herhangi bir yönlendiricinin, kendisine yeni gelen bir trafik akışına atadığı etiketi istediği zaman dağıtabilmesine bağımsız etiket atama denir. Düzenli etiket atamada yönlendirici sadece sonraki kaynak yönlendirici bilgisi belli olan ve etiket eşleştirilmesi yapılmış olan FEC adresleri ile etiket dağıtımı başlatabilir. Ayrıca düzenli etiket atamada uç yönlendiriciler arasında ilgili mesajlaşmalar gerçekleştirilmeden ve LSP'nin döngüsüz olduğundan emin olunmadan trafik o LSP üzerinden gönderilmez.

5.3. RSVP (Resource ReSerVation Protocol)

RSVP, başlangıçta bir QoS çeşidi olan IntServ için geliştirilmiş, sonrasında biraz daha geliştirilerek etiket dağıtımı ve MPLS-TE (Trafik mühendisliği) amacıyla da kullanılabilmesi sağlanmıştır. Bununla ilgili ayrıntılar RFC 3209'da ele alınmıştır.

Belirli bir LSP boyunca gerekli kaynak ayrımının yol üzerindeki tüm yönlendiriciler tarafından yapılmasını amaçlar.

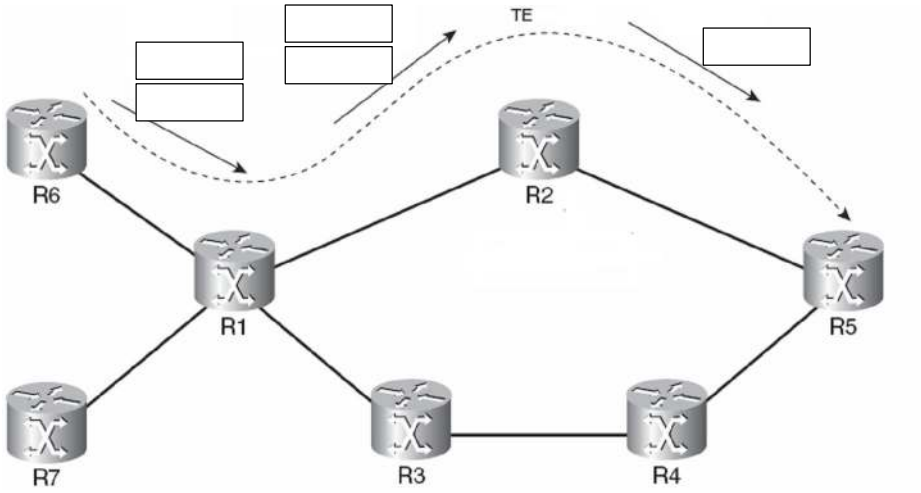
RSVP, PATH ve RESV mesajlarını kullanır. Trafik mühendisliği yapılan yolun en başındaki yönlendirici sondaki yönlendiriciye PATH mesajı gönderir. Bu mesaj içerisinde LSP boyunca geçilecek olan her bir LSR yönlendiricisinin IP'si bulunur. Bu mesajı alan yönlendirici kendi IP sini bu mesajdan kaldırır ve paketi nereye göndereceğini görür bunun üzerine sonraki LSR'a gönderir. En sonraki yönlendirici paketin kendisinde sonlandığını anlar ve geriye doğru RESV mesajları gönderir. RESV mesajları da PATH mesajları gibi aynı güzergâhtan ters yönde ilerler. RESV mesajların en baştaki LSR'a ulaştığı anda tünel kurulmuş olur [26]. Kurulan bu tünelden etiketler de taşınır.



Şekil 5.5. RSVP sinyalleşmesi

PATH mesajları içince ayrıca TSPEC ve ADSPEC bulunur. TSPEC, LSP boyunca veri hızı bilgileri ile gönderilen paket boyutları gibi bilgileri içerir. ADSPEC, LSP boyunca servis kalitesi, MTU (Maximum Transmission Unit) büyüklüğü, gecikme gibi bilgiler içerir.

Şekil 5.5'de görülen RSVP sinyalleşmesi görülmektedir. Buna göre R6 en baştaki yönlendirici, R5 en sondaki yönlendiricidir. R6, R5'ten RESV mesajlarını aldığı anda tünel kurulmuş ve sinyalleşme sorunsuz çalışıyor demektir. R5, kendisine PATH mesajları ulaştıktan sonra bu tünel için kullanılacak olan ilk etiket atamasını yapar ve RESV mesajları ile bunu R6'ya gönderir. Bundan sonra Şekil 5.6'da görüldüğü gibi R6'dan R5'e doğru trafik akışında bu etiketler kullanılarak LSP izlenmiş ve kurulan tünel güzergâhı takip edilmiş olur.



Şekil 5.6. RSVP TE trafik akışı

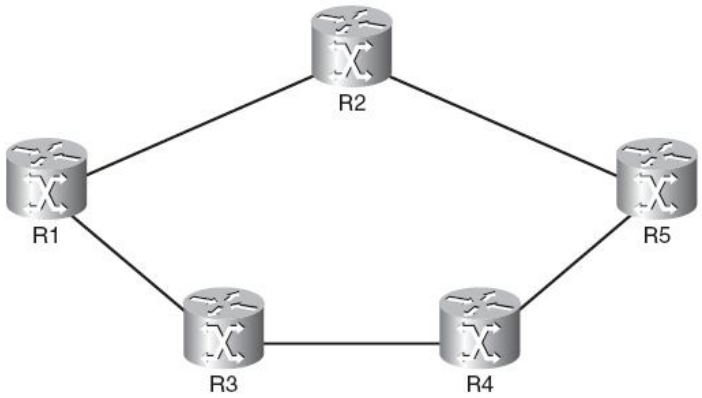
PATH ve RESV mesajlarında, RRO (Record Route Object) taşınır. RRO da içerisinde, gidilen yol boyunca geçilen her bir yönlendiricinin IP bilgisini bulundurur. RSVP yol bilgisi (Explicit Path) genellikle RRO içindeki yol bilgisiyle aynı olur.

5.4. Trafik Mühendisliği (TE)

Belirli bir noktadan bir hedefe giderken birden fazla yol alternatifi olan ağlarda yolların ve cihazların yük dağılımlarının dengelenmesi işlemine trafik mühendisliği

denir. Trafik mühendisliği ile ayrıca öncelikli yönlendirme yolunda meydana gelecek bir kesinti sonrasında trafiğin en optimum yoldan ilerlemesine müdahale edilebilir. Kısacası, uçtan uca yol seçimini yönlendirme protokollerine bırakmadan kendimiz belirleyebiliriz. Trafik mühendisliği kullanmadan yönlendirme protokolleri ile böyle bir yapı kurmak ve yük dağılımı sağlamak mümkün değildir.

Şekil 5.7'de görülen ağda R1'den R5'e iki yol var. Bunlar R1→R2→R5 ve R1→R3→R4→R5 şeklindedir. Tüm yönlendiriciler arasındaki hatların maliyetlerinin eşit olduğunu düşündüğümüzde yönlendirme protokolleri kullanıldığı zaman her iki alternatif güzergâh da çalışır durumdayken sürekli R1→R2→R5 yolu kullanılacak diğer taraf atıl kalacaktır.



Şekil 5.7. IP yönlendirme ve TE

TE kullanılarak ikisinin birlikte kullanımı sağlanmış olur.

MPLS-TE'de de normal MPLS kullanımında olduğu gibi seçilen yol boyunca yönlendiriciler (LER, LSR) birbirlerine etiket bilgilerini gönderirler ve LSP'yi sürekli canlı tutarlar.

TE'nin kullanım faydalarını özetlemek gerekirse;

- Trafiği ağa efektif dağıtma,
- Linke atanan statik bant genişliğini dikkate alma,
- Linkteki gecikme gibi parametreleri dikkate alma,
- Linkteki bant genişliği ve benzer özelliklerin değişmesine uyum sağlama,

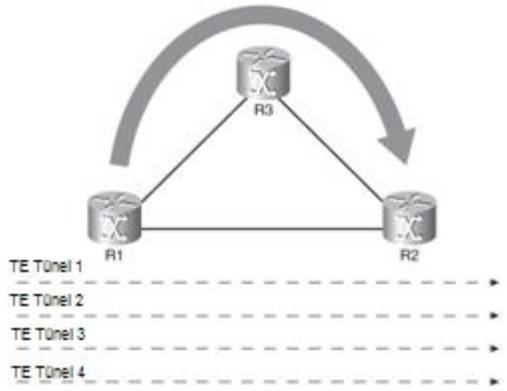
- Hedef IP bazlı yönlendirme yanı sıra kaynak IP bazlı yönlendirme de desteklemedir.

Bu özellikler değerlendirildiği zaman MPLS-TE'nin ne kadar önemli olduğu anlaşılmaktadır. Özellikle servis sağlayıcıların müşteri beklentilerine tam olarak cevap verebilmeleri MPLS-TE kullanımına bağlıdır denilebilir.

Önemli noktalardan birisi de MPLS-TE'de RSVP sinyalleşmesi kullanılır. Biz de yapmış olduğumuz uygulamada LDP yerine RSVP kullanacağız.

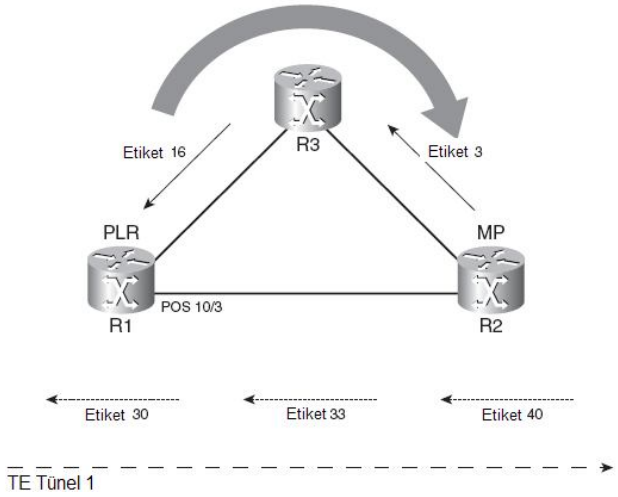
5.5. FRR (Fast Reroute)

Yüksek kapasiteli hatlardan veri taşırken oluşacak link veya cihaz sorunlarında, kesintilerin en aza indirgenmesi için ya bire bir link yedeği bulundurulmalıdır ki kesilen linkin yükü eşdeğer yedeği ile karşılanabilsin. Veya MPLS-TE yedek tüneller oluşturulmalıdır. Yüksek kapasitede devrelerin yedeğini bulundurmak oldukça maliyetli bir çözümdür. Bunun yerine MPLS-TE tünel yedekleri oluşturmak çok daha ucuz ve esnek bir çözümdür. MPLS-TE ile link ve cihaz korumaya FRR denilmektedir [26]. Link koruma (LP:Link Protection) ve cihaz koruma (NP:Node Protection) olmak üzere iki tür FRR vardır. Link korumada uygulanacak Şekil 5.8 'deki ağ yapısında öncelikli yol R1→R2 şeklinde ve bu yoldan çalışan tünellerin yedekleri R1→R3→R2 şeklinde yapılacak.



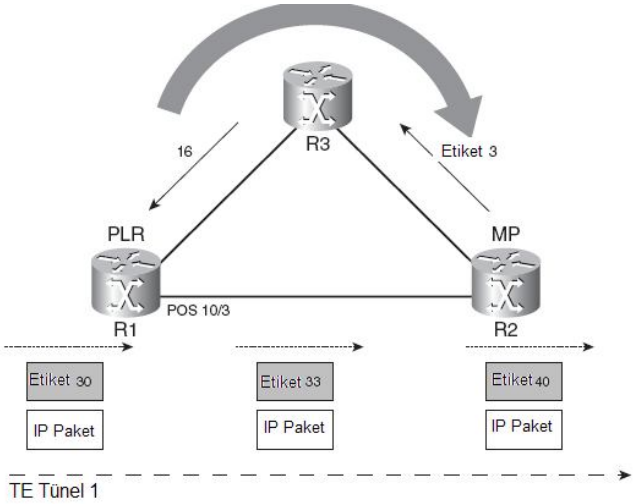
Şekil 5.8. FRR link koruma

Yedek tünel oluşturulduğu zaman RSVP protokolü etiketleri dağıtıyor (Şekil 5.9).



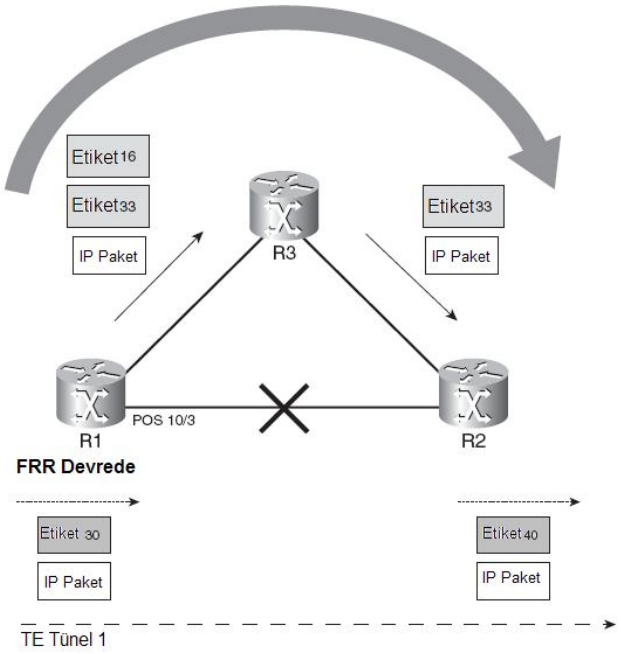
Şekil 5.9. RSVP yedek tünel ve asıl tünel için etiket dağıtımı

R1→R2 yolunda herhangi bir sorun yokken trafik akışı Şekil 5.10'daki gibi gerçekleşir.



Şekil 5.10. FRR çalışma şekli

Şekil 5.10'da görüldüğü gibi RSVP ile dağıtılan etiketler kullanılarak IP paketleri anahtarlanır. Şekil 5.11'de R1→R2 arasındaki yolda kesinti olması durumunda yedek tünelin devreye girmesi ve sonrasında IP paketlerinin yedek tünel üzerinden anahtarlanması görülmektedir.



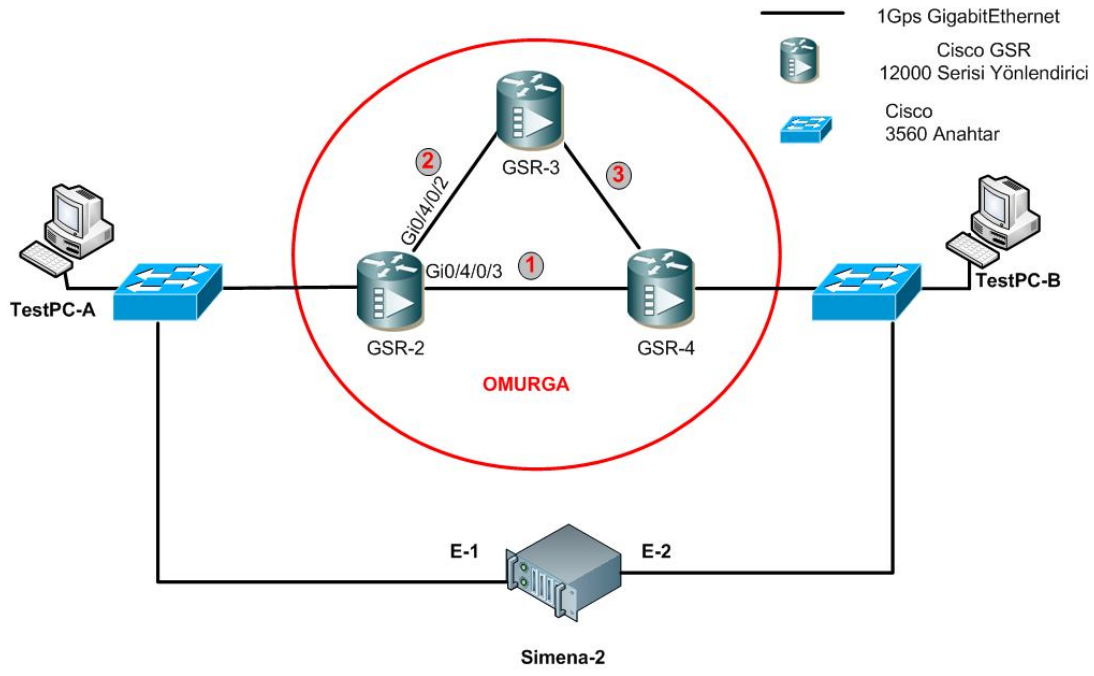
Şekil 5.11. FRR'ın devreye girmesi [26]

Şekil 5.11'de FRR'ın devreye girmesi sonucu etiket anahtarlamanın yedek tünel olan R1→R3→R2 yolu üzerinden gerçekleştirildiği görülüyor.

6. UYGULAMA

Çalışmada, günümüzde yaygın kullanılan OSPF yönlendirme protokolü ile MPLS-TE-FRR'ın yönlendiriciye direkt bağlı olan linkte kesinti olması durumunda yedek yolu kullanmaya başlaması için geçen süreler ölçüler karşılaştırılmıştır. Ayrıca hatta herhangi bir kesinti olmadığı durumlarda hattı kapasitesi üzerinde trafik oluşması durumunda kritik veri kayıplarının engellenmesi adına kritik veriler için QoS uygulaması kullanılmış ve hat kapasitesi üzerinde farklı veriler gönderilerek verilerin kaybolup olmadığı gözlemlenmiştir.

OSPF ve MPLS-TE-FRR'ın geçiş hızlarının ölçülmesinde Şekil 6.1'de görülen topoloji kullanılarak ölçümler gerçekleştirilmiştir. Laboratuarda üç adet Cisco 12000 Serisi yönlendirici (GSR), iki adet Cisco 3560 Serisi Ethernet anahtar, iki adet Simena trafik üretme cihazı, iki adet test PC'si kullanılmıştır. TestPC'lerde hping3 gibi yardımcı programlar kullanılmış ve ölçüm sonuçları bunlar yardımıyla hesaplanmıştır.



Şekil 6.1. Laboratuar ölçümlerinde kullanılan network topolojisi

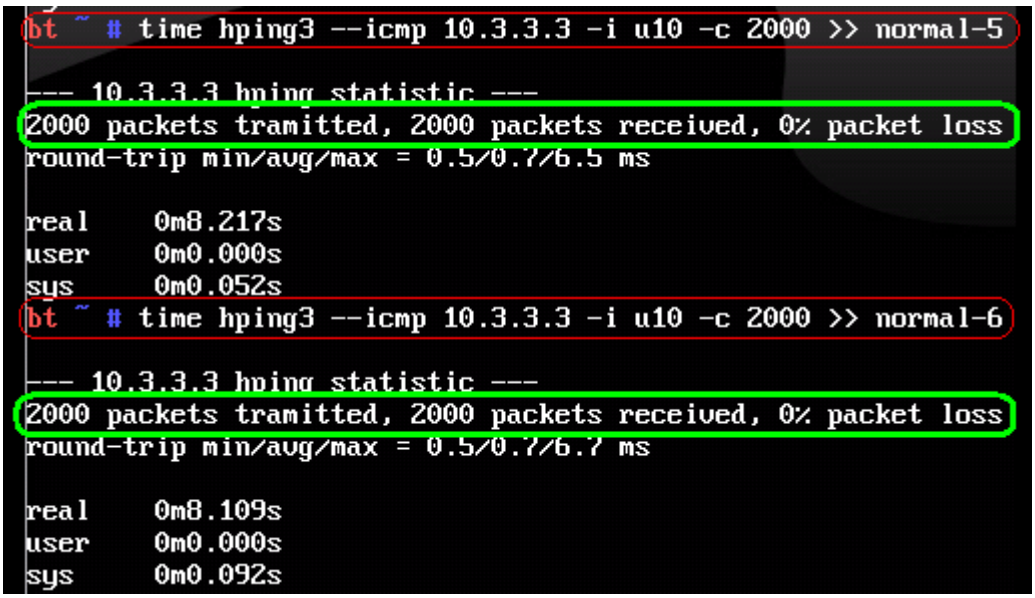
Ölçümlerin sağlıklı olması için iki farklı trafik üretme uygulaması kullanılmış ve aradaki farklar da ayrıca karşılaştırılmıştır. Bunlardan birisi Simena cihazı diğeri Linux platformlarında çalışan hping3 programıdır.

6.1. OSPF Hat Geçişlerinin ve Veri Kayıplarının Ölçüm ve Hesaplanması

Şekil 6.1'deki her üç yönlendiricide de yönlendirme protokolü olarak sadece OSPF kullanılmıştır. Simena ve Hping3 ile ayrı ayrı hat geçişi ve kayıpları ölçülmüş, hesaplamalar yapılarak sonuçları karşılaştırılmıştır.

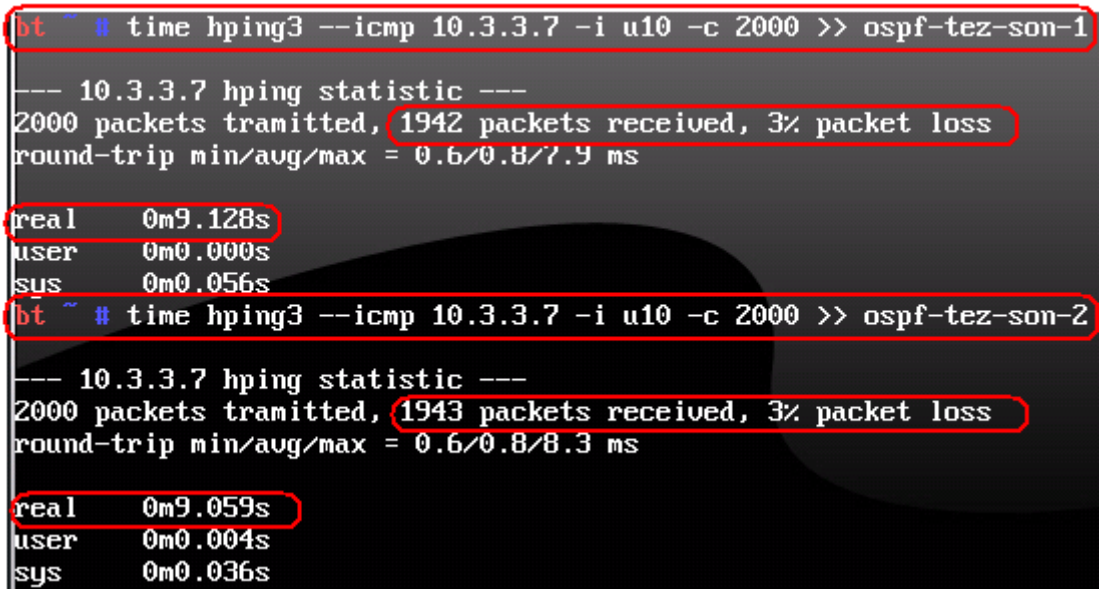
6.1.1. HPING3 Programıyla OSPF geçiş süresi ölçüm ve hesaplamaları

Topolojideki yönlendiriciler arasındaki hat hızları (1Gbps) eşit olduğu için OSPF''in öncelikli tercihi en kısa ve maliyeti düşük yol olan 1 numaralı yol kullanılır. Bu durumda TestPC-A üzerinde özel derlenmiş bir Linux olan Backtrack3 platformunda bulunan hping3 yardımcı programı kullanılarak saniyede 200 civarında toplam 2000 adet ICMP paketi TestPC-B'ye gönderildi. 1 numaralı yol kullanılırken ve hatta herhangi bir kesinti yokken, veri kaybı olup olmadığı ölçüldü. Şekil 6.2'de görülen normal trafik değerleri elde edildi.



Şekil 6.2. hping3 normal trafik değerleri

Toplam on adet ölçümün hepsinde gönderilen 2000 paketin tamamının geri alındığı, paket kaybının olmadığı gözlemlendi. Trafik başladıktan bir müddet sonra GSR-2 ve GSR-4 yönlendiricileri arasındaki (1) numaralı hat kesilerek geçiş sırasında kaybolan paketler ölçüldü buna göre geçiş süresi ve kayıplar hesaplandı. Şekil 6.3'te OSPF ölçümlerinden ikisinin sonucu görülmektedir. Tablo 6.1'de de tüm ölçüm sonuçları ile geçiş süresi hesaplamaları bulunmaktadır.



Şekil 6.3. Hping3 OSPF geçiş test sonuçları ekranı

Şekil 6.3'teki birinci ölçüm 9,128 saniyede tamamlanmış. Buna göre, bir saniyede 2000/9,128 sn = ~219 adet paket gönderilmiş ve bunlardan 58 paket kaybolmuş. 1 sn'de 219 paket gönderildiğine göre 58 paket 58/219=~0,264 sn 'de gönderilir.

Tüm test sonuçları hesaplanarak Çizelge 6.1 elde edilmiştir.

Çizelge 6.1. Hping3 OSPF ölçüm ve hesaplama sonuçları

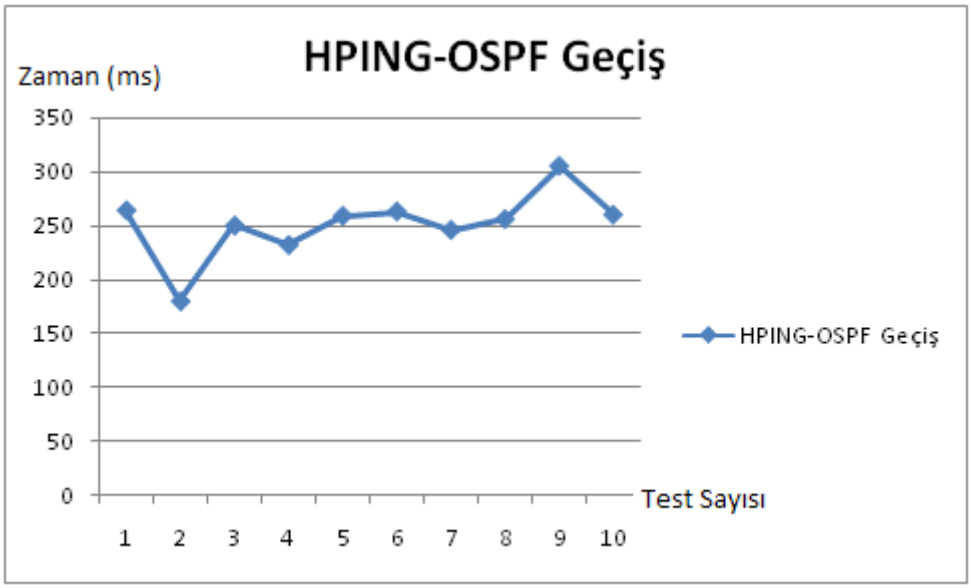
HPING-OSPF	**Test1**	**Test2**	**Test3**	**Test4**	**Test5**	**Test6**	**Test7**	**Test8**	**Test9**	**Test10**
Gönderilen Paket sayısı	2000	2000	2000	2000	2000	2000	2000	2000	2000	2000
Alınan Paket Sayısı	1942	1966	1946	1957	1943	1942	1948	1944	1933	1943
Kayıp Paket	58	34	54	43	57	58	52	56	67	57
Gönderim Süresi (sn)	9,128	10,58	9,272	10,79	9,087	9,078	9,472	9,15	9,122	9,114
Gönderilen Paket / 1 sn	219,1	189	215,7	185,3	220	220	211	218,6	219,2	219,4
Geçiş Süresi ~ (ms)	**264**	**180**	**250**	**232**	**259**	**263**	**246**	**256**	**305**	**260**

Sonuç olarak geçiş süresi 264 ms olarak hesaplanmıştır.

GSR2'nin Gi0/4/0/3 arabirimi için ayarlanan "hello" ve "dead" aralıkları aşağıdaki gibidir.

interface GigabitEthernet0/4/0/3
network broadcast
passive disable
dead-interval 4
hello-interval 1

Buna göre, GSR2 bu arabirimden her 1 saniyede komşularına "hello" paketleri gönderir. Eğer 4 sn boyunca "hello" alamazsa komşusunu yok sayar ve SPF algoritmasını tekrar çalıştırarak yol bilgilerini günceller. Buna göre gerçekte geçiş süresi en az 4-5 sn arasında olması gerekir. Ancak yönlendiriciye doğrudan bağlı bir arabirimde meydana gelen kesinti olmasından dolayı yönlendirici bu kesintiyi fark edip SPF'i hemen çalıştırıyor ve alternatif yolu hesaplama süresi veya geçiş süresi Çizelge 6.1'de elde edilen değeler olarak görülüyor.
Çizelge 6.1'de hesaplanan geçiş süreleri Şekil 6.4'te grafiksel olarak görülmektedir.



Şekil 6.4. Hping3 OSPF geçiş süreleri

6.1.2 Simena ile OSPF geçiş ölçüm ve hesaplamaları

Şekil 6.1 topolojisinde yönlendiriciler arasında OSPF kullanıldığında TestPC-A'da TestPC-B'ye doğru olan trafiğin öncelikli yolu (1) numaralı 1Gbps hızındaki yol iken bu hattın kesilmesi sonucu trafiğin alternatif yol olan (2) (3) yoluna geçişi süresi hesaplanmıştır.

Şekil 6.1'de görülen Simena-2 makinesinin E1 arabirimi kullanılarak Çizelge 6.2'de görülen hız ve sayılarda TCP paketleri GSR-2 üzerinden Simena'nın E2 arabirimine gönderilmiş ve gönderim başladıktan sonra (1) numaralı hat kesilerek paket kayıpları Simena ile ölçülmüştür. Bu ölçüm sonuçları kullanılarak geçiş süreleri hesaplanmıştır.

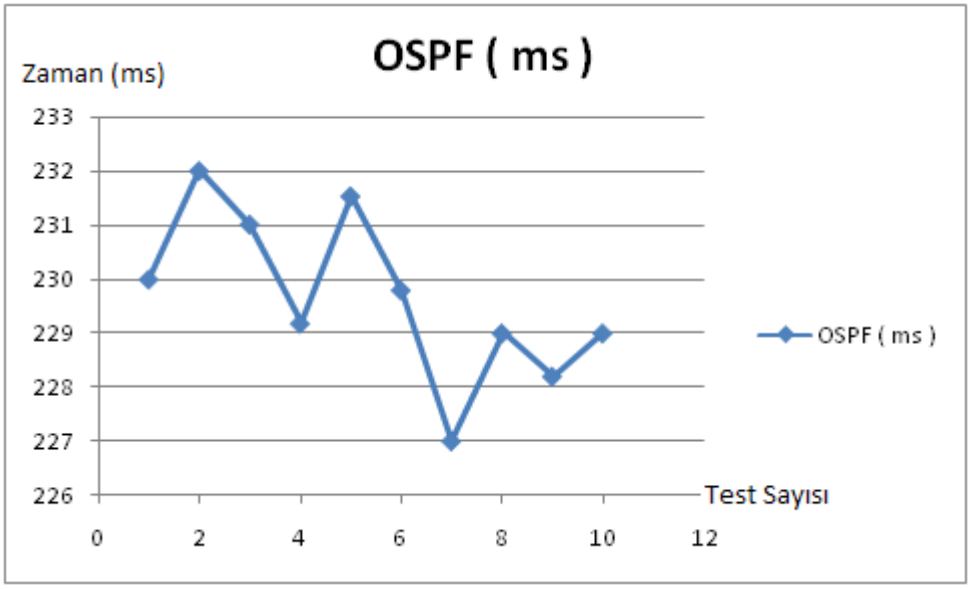
İlk testte (Test-1) 2.000.000 TCP paketi 100.000bps hızı ile E1 arabiriminden gönderilmiş ve 1.977.000 paket E2 arabiriminden alınmıştır. Geçiş sırasında 23.000 paket kaybolmuştur. Saniyede 100.000 paket gönderildiğine göre 23.000 paket için geçen süre 23.000/100.000 = 0,23 saniye yani 230 ms olmaktadır.

Çizelge 6.2'de farklı paket sayıları ve gönderim hızları için ölçüm sonuçları ve bunlara göre hesaplanan geçiş süreleri bulunmaktadır.

Çizelge 6.2. Simena ile OSPF geçişi paket kaybı ölçümleri ve geçiş süresi hesaplamaları

OSPF	Test-1	Test-2	Test-3	Test-4	Test-5	Test-6	Test-7	Test-8	Test-9	Test-10
Gönde-rilen Paket (x1000)	2.000	2.000	6.000	6.000	10.000	10.000	1.000	1.000	100	100
Alınan Paket	1.977.000	1.976.799	5.930.693	5.931.244	9.884.227	9.885.097	988.650	988.550	98.859	98.855
Kayıp Paket	23.000	23.201	69.307	68.756	115.773	114.903	11.350	11.450	1.141	1.145
Paket Gönde-rim Hızı (pps)	100.000	100.000	300.000	300.000	500.000	500.000	50.000	50.000	5.000	5.000
% Paket Kayıp	1,15	1,16	1.155	1,145	1.157	1.149	1.135	1.145	1.141	1.145
Geçiş Süresi ms	**230**	**232,01**	**231,02**	**229,18**	**231,54**	**229,8**	**227**	**229**	**228,2**	**229**
Paket boyutu (byte) (TCP)	120	120	120	120	120	120	120	120	120	120

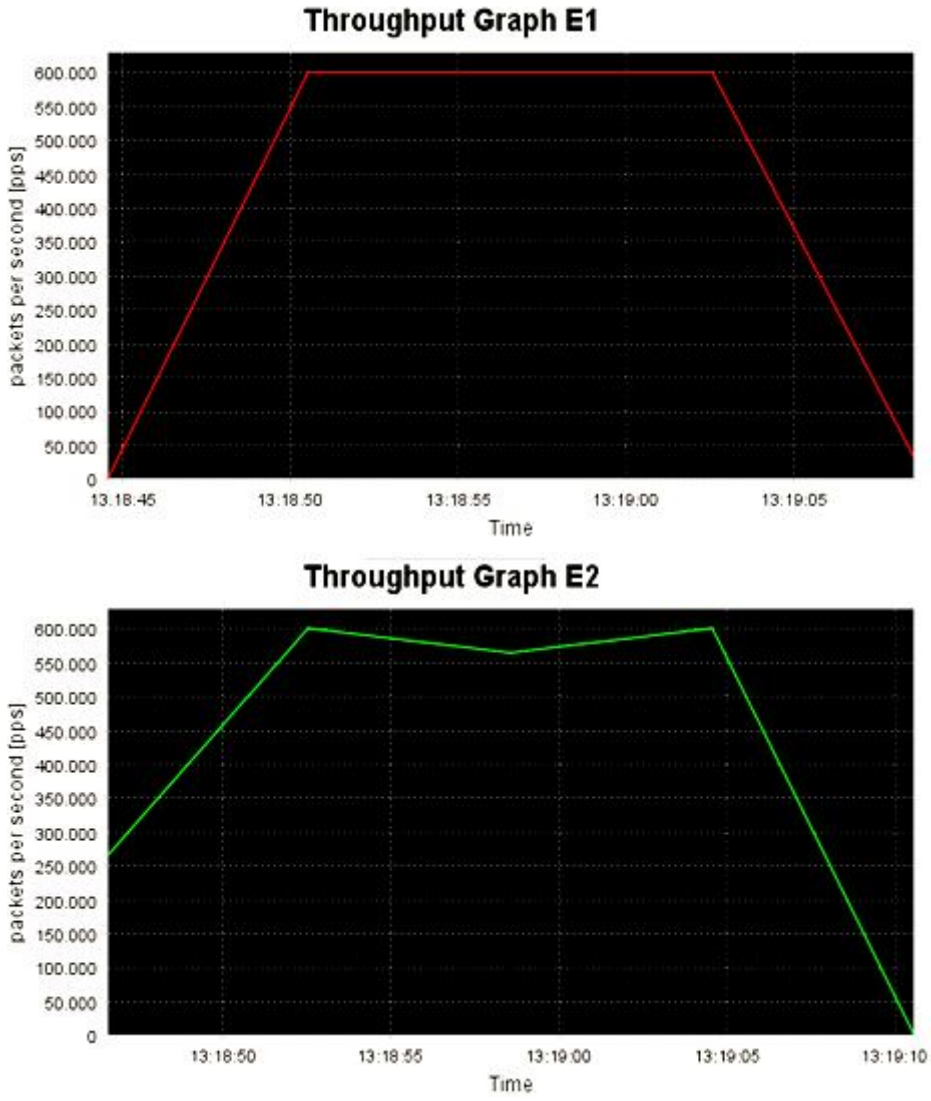
Çizelge 6.2 ‘deki geçiş süreleri Şekil 6.5’de grafiksel olarak görülmektedir.



Şekil 6.5. Simena OSPF geçiş süreleri

Ölçümlerden birine ait Simena iletim ve alım arabirimlerindeki değerleri ve kayıpları net biçimde gösteren Simena ekranı Şekil 6.6’de görülmektedir. Bir önceki Hping3

testlerinde görüldüğü gibi burada da hat geçiş hızı normalden daha hızlıdır. Çünkü doğrudan bağlı olan arabirimin kesilmesi yönlendiricinin kesintiyi hemen fark etmesine neden olmaktadır. Hat direk olarak bağlı olmasaydı yönlendirici hattın kesildiğini ilgili arabirimden "hello" paketleri alamadığında fak edecekti. Şekil 6.6'da görüldüğü gibi kesinti olduğu anda gönderilmiş olan veri paketleri kaybedilmekte dolayısıyla Simena'nın trafik gönderim arabiriminde veri sabit görünürken trafik alan tarafında veri hızının düştüğü Şekil 6.6'daki grafiğe yansımaktadır.



Şekil 6.6. Simena OSPF geçiş sırasında gönderim ve alım arabirim ekranları.

Hping3 ve Simena ölçüm sonuçları ve bu sonuçlara bağlı olarak hesaplanan geçiş süreleri incelendiğinde sonuçların birbirine yakın olduğu, birbirini desteklediği görülmektedir. Oluşan fark hping3 için kullanılan makinelerin işlem kapasitesi ve hping3 programının saniyede gönderebildiği paket sayısının sınırlı olmasından kaynaklanmaktadır. Saniyede gönderilen paket sayısı az olması daha az duyarlı ölçüm yapılmasına ve dolayısıyla sapmaların çok olmasına neden olmaktadır.

6.2. OSPF+MPLS-TE-FRR Hat Geçişlerinin ve Veri Kayıplarının Ölçülmesi

Şekil 6.1'deki her üç yönlendiricide de yönlendirme protokolü olarak OSPF kullanılmıştır. Bununla birlikte hızlı paket anahtarlama ve kesinti anında veri kayıplarını minimize etmek özelliklerinden yararlanmak için MPLS-TE ve FRR (Fast Reroute) özellikleri de yönlendiricilerde aktif edilmiştir. MPLS-TE-FRR sayesinde Şekil 6.1'deki topolojinin (1) numaralı yoluna alternatif tünel tanımı yapılmış ve bu yolda olacak kesinti anında trafiğin direkt olarak yedek tünele yönlendirilmesi sağlanmıştır. Birincil tünel ve yedek tünel tanımlarında, kullanılacak LSP üzerindeki her bir yönlendiricinin IP'leri verilerek LSP yolu netleştiriliyor. Testler sırasında GRS2 üzerindeki yapılandırma önemli olduğundan cihazın MPLS ve OSPF yapılandırması aşağıda verilmiştir. Simena ve Hping3 ile ayrı ayrı hat geçişi ve kayıpları ölçülmüş, hesaplamalar yapılarak sonuçları karşılaştırılmıştır.

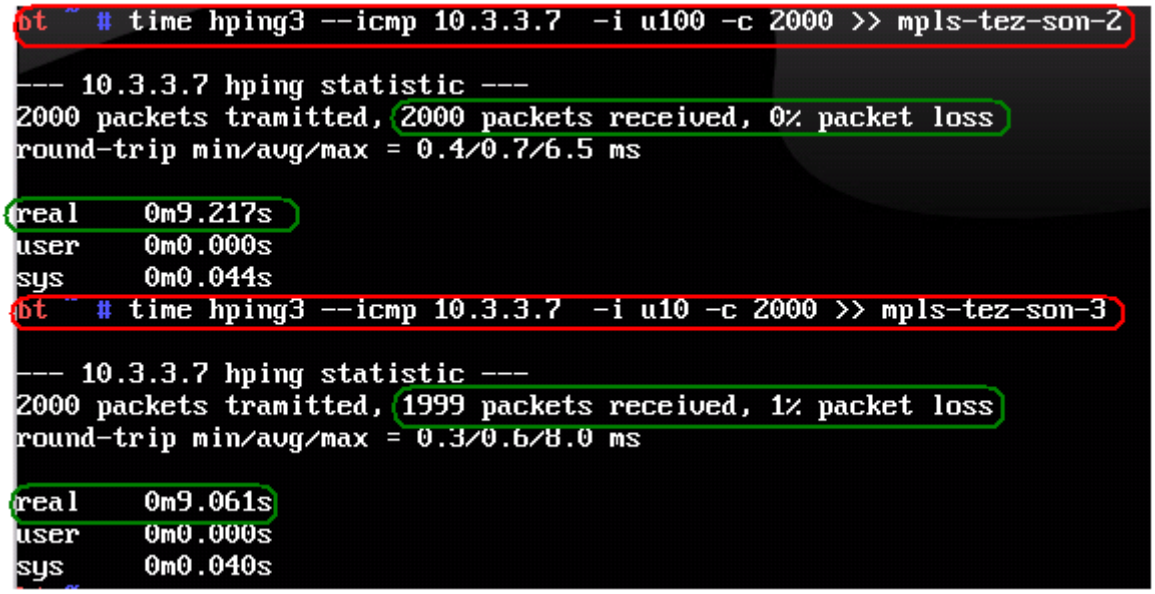
```
explicit-path name explicit_tunnel-te24          →TE tünelin kullanacağı yol tanımı
 !Primary link
 index 10 next-address strict ipv4 unicast 1.1.1.3
 index 20 next-address strict ipv4 unicast 10.200.100.12
!
explicit-path name explicit_tunnel-te234     →yedek TE tünelin kullanacağı yol tanımı
 index 10 next-address strict ipv4 unicast 2.2.2.2
 index 20 next-address strict ipv4 unicast 3.3.3.3
!
interface tunnel-te24                            →GSR2'den GSR4'e TE tüneli
 ipv4 unnumbered Loopback0
 autoroute announce
 destination 10.200.100.12                       →GSR4'ün loopback IP'si
 fast-reroute                                    → te24 down olursa FRR aktif olacak
 path-option 1 explicit name explicit_tunnel-te24
!
interface tunnel-te234                           →GSR2'den GSR4'e yedek TE tüneli
```

```
 ipv4 unnumbered Loopback0
 destination 10.200.100.12
 path-option 1 explicit name explicit_tunnel-te234
!
router ospf 1
 log adjacency changes
 router-id 150.1.2.2
 area 0
  mpls traffic-eng                    →MPLS TE tünelleri OSPF içinde kullanılacak.
  interface Loopback0
  !
  interface GigabitEthernet0/4/0/0
   passive enable
   dead-interval 4
   hello-interval 1
  !
  interface GigabitEthernet0/4/0/1
   dead-interval 4
   hello-interval 1
  !
  interface GigabitEthernet0/4/0/2
   network point-to-point
   passive disable
   dead-interval 4
   hello-interval 1
  !
  interface GigabitEthernet0/4/0/3
   network broadcast
   passive disable
   dead-interval 4
   hello-interval 1
 !
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng multicast-intact
!
rsvp                                  →TE ve FRR etiketlerinin dağıtılmasını sağlıyor.
 interface GigabitEthernet0/4/0/2
 !
 interface GigabitEthernet0/4/0/3
 !
mpls traffic-eng                      →MPLS TE aktif edilecek arabirimler
 interface GigabitEthernet0/4/0/2
 !
 interface GigabitEthernet0/4/0/3
  backup-path tunnel-te 234    →Gi0/4/0/3 arabirimi kesilirse trafik te234 tüneline tetiklenecek
```

GSR2 Yönlendiricisindeki yapılandırmada, GSR2'den GSR4'e doğru iki adet alternatif yol olduğu için "tunnel-te24" ve "tunnel-te234" adında iki adet TE tüneli oluşturuldu. Her iki tünelinde başlangıcı GSR2 'de olup sonlandığı yer GSR4 olarak belirlendi. Tüneller yeni bir arabirim olarak eklendiği için bu eklenen yeni tünel arabirimlerinin de OSPF'e dahil olması için OSPF'e eklendi. MPLS yapılandırmasında trafik mühendisliği yapılacak arabirimler belirlenerek bu arabirimlerden öncelikli kullanılanda kesinti olması durumunda geçiş yapılacak tünel (*backup-path tunnel-te 234*) bilgisi girildi. Buna göre GSR2 yönlendiricisi TestPC-B'ye giden paketler için zaten Gi0/4/0/3 arabirimini ve dolayısı ile bu arabirim ile ilişkilendirilen "tunnel-te24" tünelini kullanacaktır. Bu arabirimde oluşacak herhangi bir kesinti bilgisi yönlendiriciye ulaştığında, yönlendirici arabirim ve tünel arabirimini "down" yani kesik göreceği için bu tünelin yedeği olan "tunnel-te234" 'ü kullanacaktır. Bunu yaparken da "fast reroute" tekniği kullanarak yapacaktır. Yani yönlendirme tablosunda var olan ve fakat yedek olarak bulunan tünel arabirimini ivedilikle aktif hale getirerek paketleri buradan yönlendirmeye başlayacaktır. Bu şekilde kesinti anında milisaniyeler mertebesinde yenilemeli, hızlı yönlendirme gerçekleştirilmiş olmalıdır. MPLS-TE-FRR kullanılan ortamda hattın geçiş süresi her zaman 50ms altında olacağı garanti edilmektedir [28].

6.2.1. HPING3 Programıyla OSPF+MPLS-TE-FRR (MPLS) geçiş süresi ölçüm ve hesaplamaları

Şekil 6.1 topolojisinde yönlendiriciler arasında OSPF +MPLS +TE+FRR kullanıldığında TestPC-A'dan TestPC-B'ye doğru olan trafiğin öncelikli yolu (1) numaralı 1Gbps hızındaki yol iken, bu hattın kesilmesi sonucu trafiğin alternatif yol olan (2) (3) yoluna geçiş süresi hping3 programı yardımıyla ölçülmüştür. Şekil 6.7'de OSPF +MPLS +TE+FRR ölçümlerinden ikisinin sonucu ve Tablo 6.3'te sonuçlarla birlikte hesaplamaları görülmektedir.



Şekil 6.7. Hping3 OSPF +MPLS +TE+FRR geçiş test sonuçları ekranı

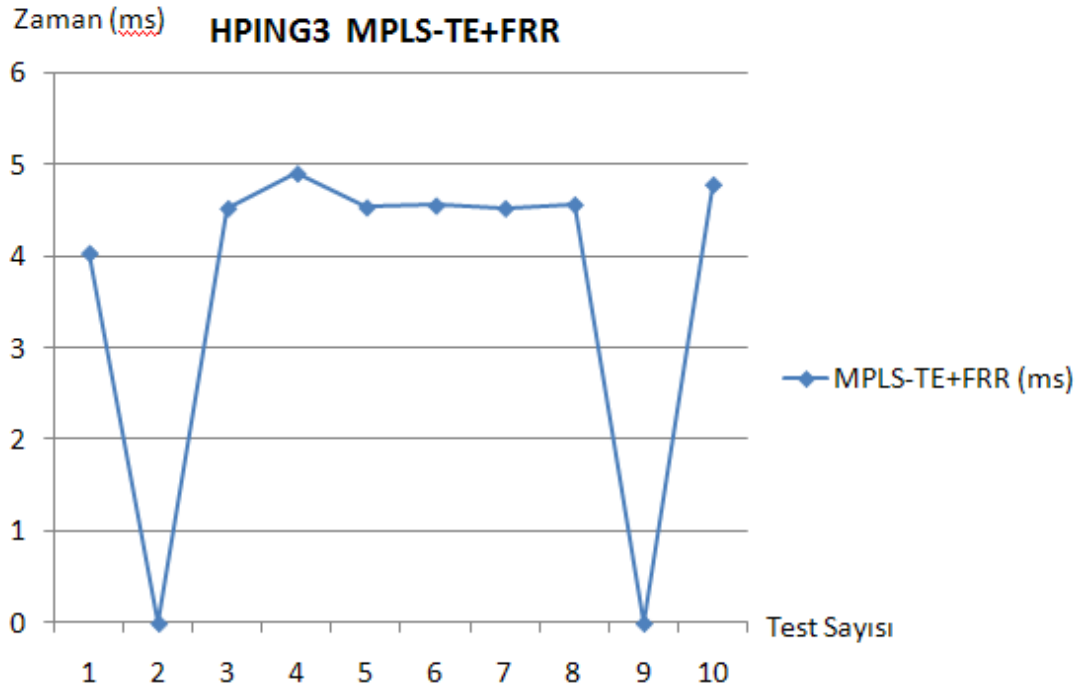
Şekil 6.7'deki ikinci ölçüm 9,061 saniyede tamamlanmış. Buna göre, bir saniyede 2000/9,061 sn = ~247 adet paket gönderilmiş ve bunlardan 1 paket kaybolmuş. 1 sn'de 247 paket gönderildiğine göre 1 paket 1/247=~0,00404 sn 'de gönderilir. Sonuç olarak, geçiş süresi 4,04 ms olarak hesaplanmıştır.

Tüm test sonuçları ve hesaplanan geçiş süreleri Çizelge 6.3'te ve bu tabloya göre geçiş sürelerinin grafiği Şekil 6.8'de görülmektedir.

Çizelge 6.3. Hping3 OSPF +MPLS +TE+FRR ölçüm ve hesaplama sonuçları

HPING-OSPF+MPLS-FRR	Test1	Test2	Test3	Test4	Tes5	Test6	Test7	Test8	Test9	Test10
Gönderilen Paket sayısı	2000	2000	2000	2000	2000	2000	2000	2000	2000	2000
Alınan Paket Sayısı	1999	2000	1999	1999	1999	1999	1999	1999	2000	1999
Kayıp Paket	1	0	1	1	1	1	1	1	0	1
Gönderim Süresi (sn)	8,091	9,217	9,061	9,82	9,08	9,127	9,076	9,147	9,362	9,582
Gönderilen Paket / 1 sn ~	247,1	216,9	220,7	203,6	220,2	219,1	220,3	218,6	213,6	208,7
Geçiş Süresi ~ (ms)	4,04	0	4,53	4,91	4,54	4,56	4,53	4,57	0	4,79

Bu sonuçlara göre MPLS-TE-FRR'ın geçiş hızı ortalama 4,5ms civarında hesaplanmıştır.



Şekil 6.8. Hping3 OSPF +MPLS +TE+FRR geçiş süreleri.

Şekil 6.8'deki grafikte de görüldüğü gibi Hping3 ile yapılan ölçümlerde saniyede gönderilen paket sayısının sınırlı olmasından örnekleme aralığı daha uzundur. Dolayısıyla, hassas ölçüm yapıldığı için bazı testlerde geçiş süresi örnekleme aralığından çok küçük olmasından dolayı paket kaybı görülmemekte ve geçiş süresi sıfır olarak hesaplanmaktadır.

6.2.2. Simena ile OSPF+MPLS-TE-FRR (MPLS) geçiş ölçüm ve hesaplamaları

Şekil 6.1'de görülen Simena-2 makinesinin E1 arabirimi kullanılarak Tablo 6.2'de görülen hız ve sayılada TCP paketleri GSR-2 üzerinden Simena'nın E2 arabirimine gönderilmiş ve gönderim başladıktan sonra 1 numaralı hat kesilerek paket kayıpları Simena ile ölçülmüştür. Bu ölçüm sonuçları kullanılarak geçiş süreleri hesaplanmıştır.

İlk testte (Test-1) 2.000.000 TCP paketi 100.000pps hızı ile E1 arabiriminden gönderilmiş ve 1.977.799 paket E2 arabiriminden alınmıştır. Geçiş sırasında 201

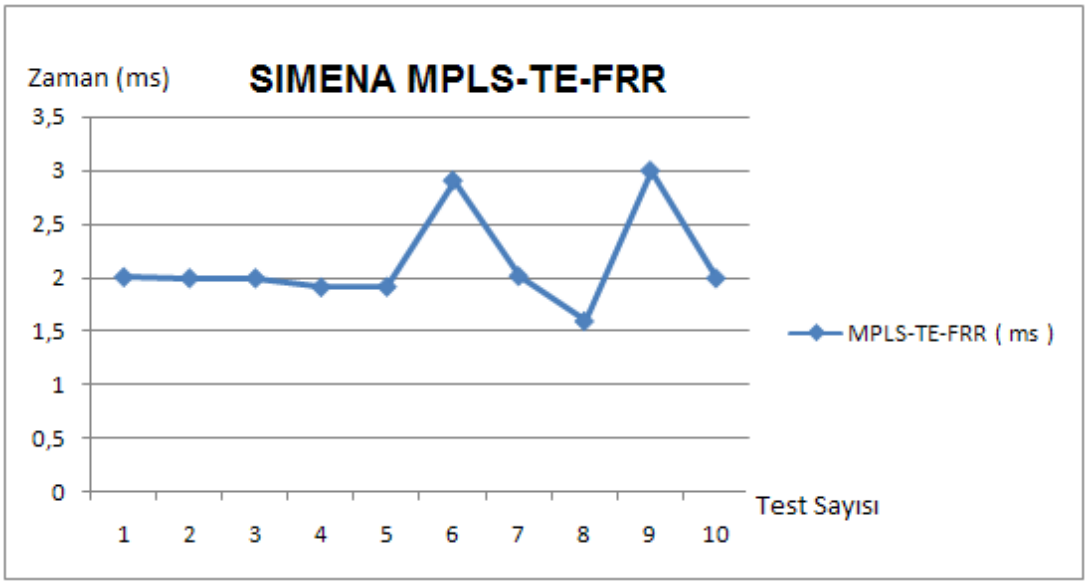
paket kaybolmuştur. Saniyede 100.000 paket gönderildiğine göre 201 paket için geçen süre 201/100.000 = 0,00201 saniye yani 2,01 ms olmaktadır.

Çizelge 6.4'de farklı paket sayıları ve gönderim hızları için ölçüm sonuçları ve bunlara göre hesaplanan geçiş süreleri bulunmaktadır.

Çizelge 6.4. Simena ile OSPF +MPLS +TE+FRR geçişi paket kaybı ölçümleri ve geçiş süresi hesaplamaları.

MPLS	Test-1	Test-2	Test-3	Test-4	Test-5	Test-6	Test-7	Test-8	Test-9	Test-10
Gönderilen Paket (x1000)	2.000	2.000	6.000	6.000	10.000	10.000	1.000	1.000	100	100
Alınan Paket	1.999.799	1.999.800	5.999.400	5.999.425	9.999.040	9.998.546	999.899	999.920	99.985	99.990
Kayıp Paket	201	200	600	575	960	1.454	101	80	15	10
Paket Gönderim Hızı (pps)	100.000	100.000	300.000	300.000	500.000	500.000	50.000	50.000	5.000	5.000
% Paket Kayıp	0,01	0,01	0.01	0.009	0.0090	0.014	0.01	0.0080	0.015	0.01
Geçiş Süresi ms	**2,01**	**2**	**2**	**1,916**	**1,92**	**2,908**	**2,02**	**1,6**	**3**	**2**
Paket boyutu (byte) (TCP)	120	120	120	120	120	120	120	120	120	120

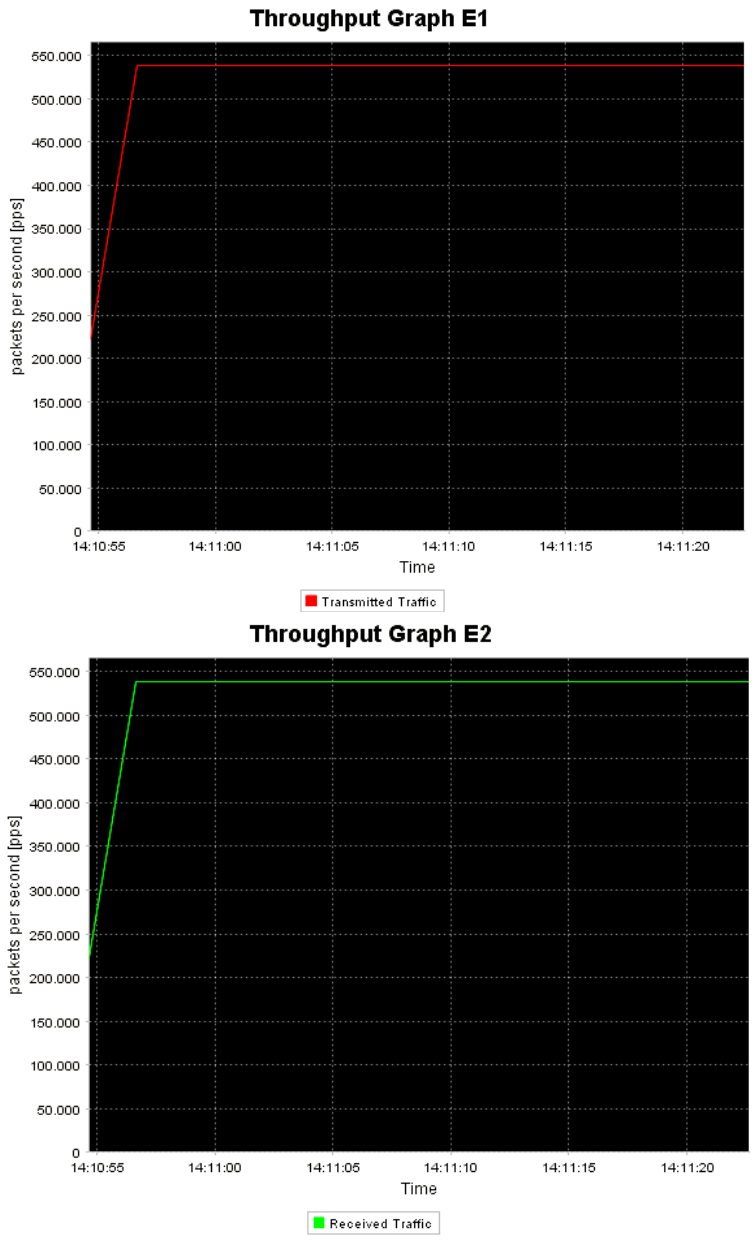
Çizelge 6.4'de hesaplanan geçiş süreleri Şekil 6.9'de grafiksel olarak görülmektedir.



Şekil 6.9. Simena OSPF +MPLS +TE+FRR geçiş süreleri

Simena ile saniyede yüz bin ile on milyon arasında farklı hızlarda paketler gönderilerek ölçüm yapıldığı için Hping3'e göre örnekleme aralığı çok daha küçük olmaktadır. Bu nedenle ölçüm ve hesaplamalar daha hassas olmaktadır.

MPLS +TE+FRR geçişlerinin çok kısa sürede gerçekleşmesinden paket kaybı çok az olmaktadır. Bundan dolayı, Şekil 6.10'da görülen Simena iletim ve alım arabirimlerindeki fark, fark edilemeyecek kadar azdır.

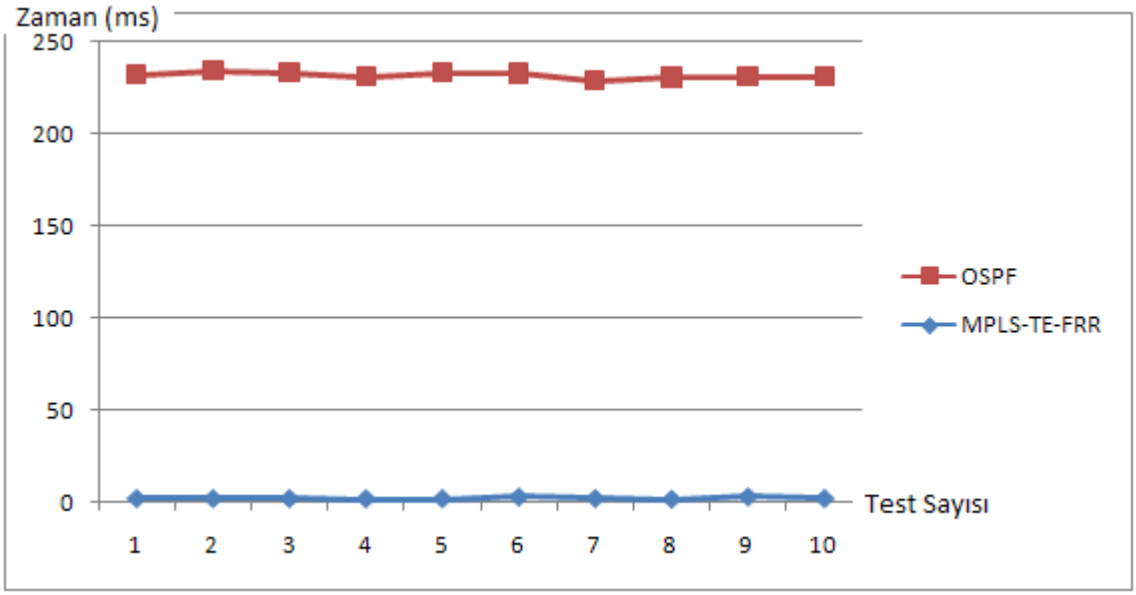


Şekil 6.10. Simena OSPF +MPLS +TE+FRR geçiş sırasında gönderim ve alım arabirim ekranları

6.3. OSPF ve OSPF+MPLS-TE-FRR Geçiş Sürelerinin Karşılaştırılması

Hping3 ve Simena ile yapılan ölçüm ve hesaplamalarda her iki sonucun birbirine çok yakın olduğu gözlemlenmiştir. Ancak Simena ile daha kısa sürede yüksek miktarda paket gönderilerek ölçümler yapılabildiği için ölçüm sonuclarının daha hassas olduğu düşünülmektedir. Bundan dolayı OSPF ve OSPF +MPLS +TE+FRR'ın Simena ile

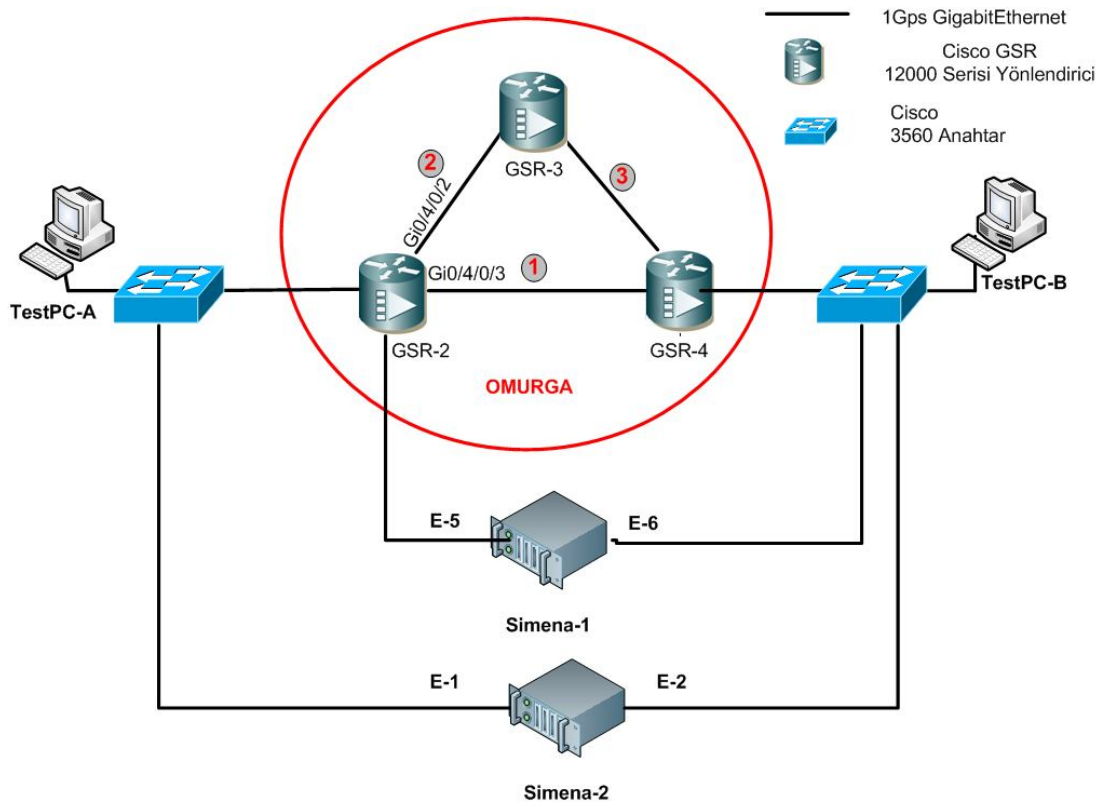
hesaplanan geçiş süreleri karşılaştırılmıştır. şekil 6.11'de OSPF ve OSPF +MPLS +TE+FRR'ın geçiş süreleri karşılaştırmalı olarak görülmektedir.



Şekil 6.11. OSPF ve OSPF +MPLS +TE+FRR geçiş hızlarının karşılaştırmalı sonuçları

6.4. OSPF+MPLS-TE-FRR +QoS Ortamında Veri Kayıplarının Ölçülmesi

OSPF ve MPLS ile hat geçiş hızlarını ve geçişler sırasında meydana gelen kayıpları hesaplandı. Bunlarla beraber gerek iç (şirket içi) gerekse dış (internet bağlantıları) veri ağlarında saldırı veya yoğun kullanımdan dolayı hat kapasiteleri aşılmakta ve yönlendirici ağ donanımları hat kapasitesinin üzerine çıkan veri miktarlarını varsayılan ayarlarına göre işlemektedirler. Birçok yönlendirici hat kapasitesinin üzerindeki verileri FIFO kuralınca işlemekte, kuyrukta kalan ve gönderim sırasını bekleyen bazı paketler de mecburen atılmaktadır. Bu durumlarda video, ses, sinyalleşme gibi kritik verilerin zarar görmeden iletilebilmesi ve atılacaksa bunların dışındaki paketlerin atılması için yönlendiricilerin trafik çıkış arabirimlerine QoS uygulanabilmektedir. QoS, yönlendiriciden hatta indirilen noktada (arabirimde) veriye uygulanır. QoS ölçümlerinde 1 Gbps'lık hat kapasitelerini doldurabilmek için Şekil 6.12'de görüldüğü gibi ikinci bir Simena cihazını GSR-2 yönlendiricisine bağlayarak ölçümler yapıldı.



Şekil 6.12. OSPF+MPLS-TE-FRR ile birlikte QoS'in de kullanıldığı topoloji

Ölçümlerde GSR2 yönlendiricisi kullanılacağı için buradaki QoS yapılandırmasıyla ilgili bazı bilgiler aşağıda verilmiştir.

```
class-map match-any prec-5          →IP Precedence-5 işaretli paketler için sınıflandırma
 match precedence 5
 match mpls experimental topmost 5
 end-class-map
!
class-map match-any prec-6          →IP Precedence 6 işaretli paketler için sınıflandırma
 match mpls experimental topmost 6
 match precedence 6
 end-class-map
!
policy-map TezLab                   →Sınıflandırılan paketlere ilişkin politikaların belirlenmesi
 class prec-5                       →Ses paketlerine uygulanacak politika
  police rate 500000000 bps burst 250000 bytes peak-burst 1 bytes →500Mbps'e kadar
   conform-action transmit          →500Mbps'e kadar iletilir
   exceed-action drop               →500Mbps'in üzrine çıkanlar atılır.
  !
  priority                          →Ses paketlerine CIR ile beraber PQ da uygulanmakta.
 !
```

```
class prec-6                    →Yönetimsel (OSPF, MPLS… vb) paketlere uygulanacak politika
 bandwidth 24870000 bps         →Sıkışma durumunda 24 Mbps garanti edilecek
!
class class-default             →Ses veyönetimsel paketler dışındakilere uygulanacak politika
 bandwidth 41450000 bps
!
end-policy-map
```

Şekil 6.1'deki yönlendirici ve Ethernet anahtarlarının bizim kullandığımız tüm arabirimleri 1Gbps hızında olmasından dolayı, Simena makinesinin birini Şekil 6.12'deki gibi direkt GSR-2'ye diğerini Ethernet anahtara bağlayarak >1Gbps trafik üretebildik. GSR-2'nin Gi0/4/0/3 arabirimine, çıkış yönünde ses paketleri için QoS uyguladık. Buna göre GSR-2 yönlendiricisinin Gi4/0/3 arabiriminde 1Gbps 'lik kapasitesinin üzerinde trafik olması durumunda ses paketlerine 500Mbps kadar kapasiteyi ayırsın, kalan kapasitenin yaklaşık 25Mbps'ini kontrol paketleri (OPSP, MPLS, RSVP… vb) için bunun dışındaki verilerin iletimi için de 414,5Mbps'lık kapasite ayrıldı.

Testler sırasında normal veriyi Simena'nın birinden ve ses verisini diğerinden işaretleyerek gönderdik. Ses verisini UDP ve ToS A0 olacak şekilde kodlayarak işaretleme yaptık.

Simena'ların gönderim arabirimlerinden farklı hızlarda ses ve veri trafiği üretildiğinde, alış arabirimlerine ulaşan veriler Tablo 6.5'de görülmektedir.

Çizelge 6.5. Simena ile yapılan QoS test sonuçları

QoS Testleri	Veri Türü	Hız (bps)	Gönderim Hızı (bps) X1000	Alım Hızı (bps) X1000	Fark X1000bps
	Veri	400	398.988	398.986	2
Test1	Ses	490	488.817	488.787	30
	Veri	550	548.568	495.682	52.886
Test2	Ses	490	488.793	488.775	18
	Veri	900	897.780	484.396	413.384
Test3	Ses	600	598.485	500.094	98.391
	Veri	700	698.166	495.64	202.526
Test4	Ses	490	488.793	488.763	30
	Veri	900	897.786	495.586	402.200
Test5	Ses	490	488.756	488.781	-25

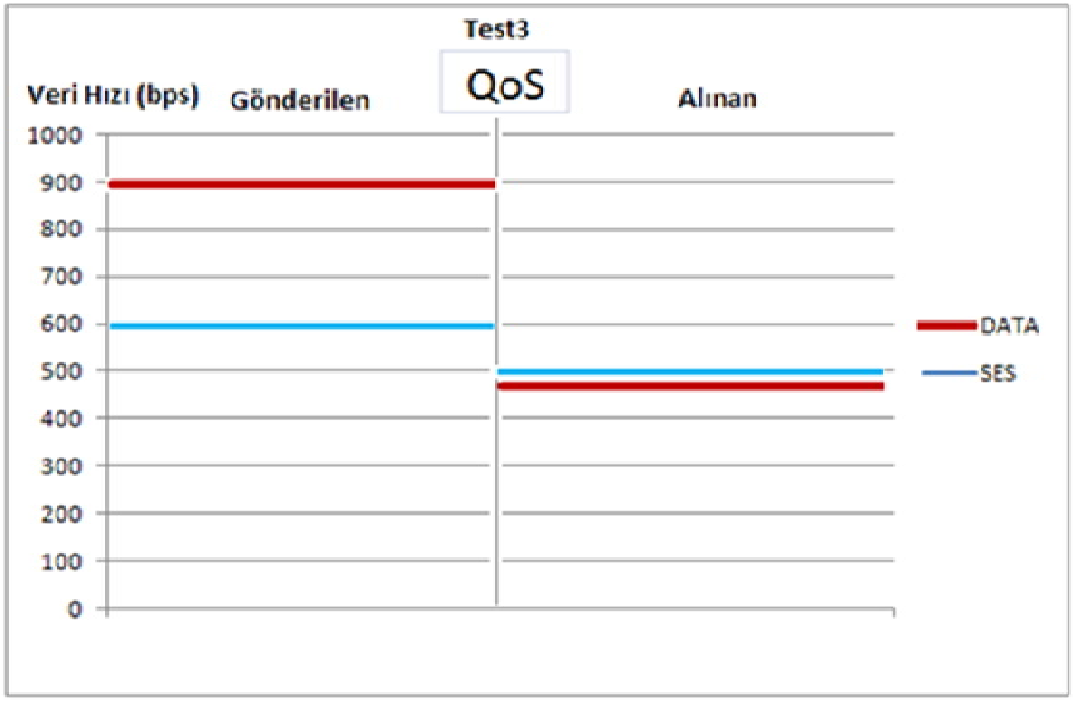
Çizelgedeki her bir test sonucu için QoS öncesi gönderilen trafik ve QoS uygulandıktan sonra alınan trafikler Şekil 6.13, Şekil 6.14, Şekil 6.15, Şekil 6.16 ve Şekil 6.17'de görülmektedir.

Şekil 6.13. 400 Mbps veri ve 490 Mbps ses, toplamının kapasiteyi aşmadığı durum.

Yukarıdaki Şekil 6.13'te GSR-2 yönlendiricisine gelen ve Gi0/4/0/3 arabiriminden gönderilen toplam trafik 400+490 = 890 Mbps olup Gi0/4/0/3 arabiriminin kapasitesi olan 1 Gbps 'dan küçük olduğu için burada uygulanan QoS devreye girmemesi ve tüm paketleri göndermesi gerekiyor. Ölçüm sonuçlarında ve grafikte bu durum görülmektedir.

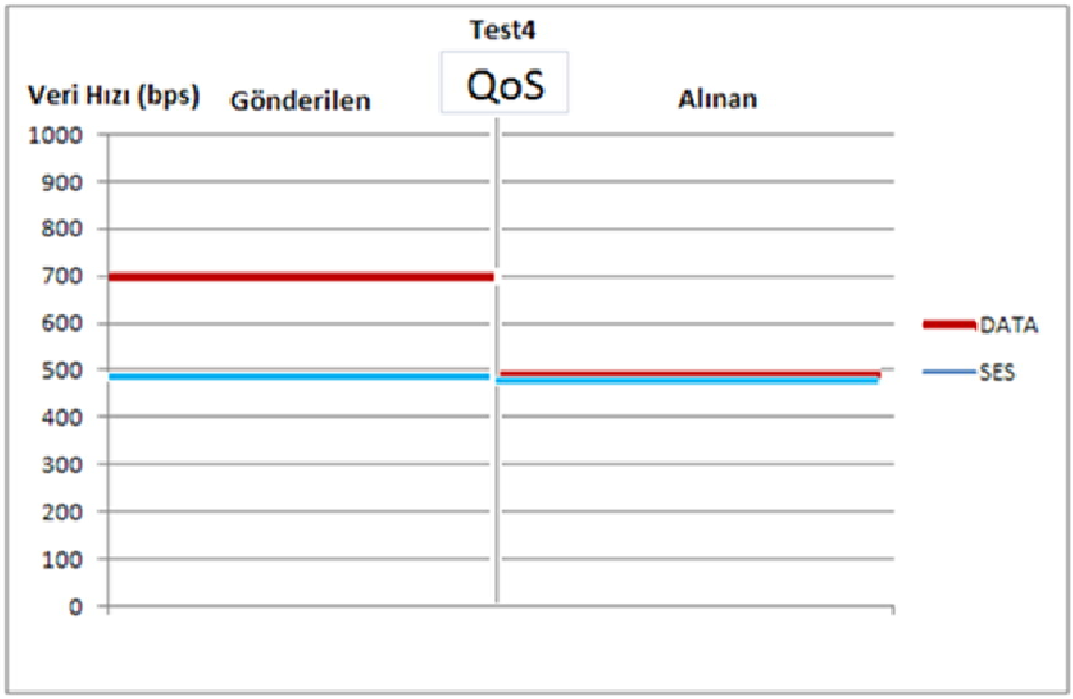
Şekil 6.14. 550 Mbps Veri ve 490 Mbps Ses, toplam gönderilen trafiğin kapasiteyi aşması durumu

Şekil 6.14 grafiğine göre 550+490=1040Mbps trafik GSR-2'nin Gi0/4/0/3 arabiriminin kapasitesinin üstünde olduğu için uygulanan QoS'in devreye girmesi ve öncelikle ses paketlerine her durumda 500Mbps'i garanti etmesi sonra kalan kapasiteyi diğer trafiklere ayırması gerekiyor. 1Gbps üzerine çıkanları da çöpe atmasını bekliyoruz. Grafikteki giren ve çıkan trafiğe baktığımız zaman QoS'in devreye girdiği görülmektedir. Hatta gönderilen trafik >1Gbps olmasına karşın çıkan trafiğin ~1Gbps civarında olduğu görülüyor.



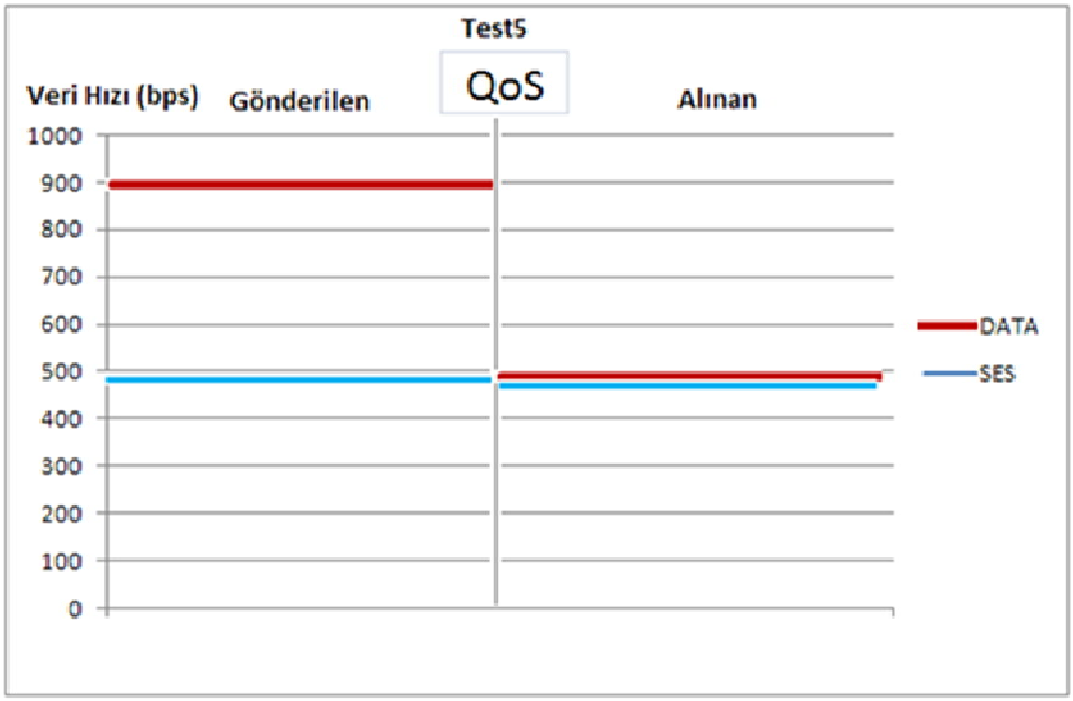
Şekil 6.15. 900 Mbps Veri ve 600 Mbps Ses, toplam gönderilen trafiğin kapasiteyi aşması durumu.

Şekil 6.15'te de gönderilen toplam trafik hat kapasitesinin üzerindedir. Ancak burada ses trafiği de bizim sese garanti ettiğimiz kapasitenin üzerinde gelmiş. Ses 600Mbps ve veri 900Mbsp gönderiliyor. Toplam 1,5Gbps olduğu için kapasitenin üzerindeki verinin atılmasını ve alış arabiriminde görünmemesini bekliyoruz. Öncelikle QoS politikamız ses'e 500Mbps garanti ettiği için her ne kadar 600Mbps göndermiş olsak da alım arabiriminde 500Mbps'lik ses görürüyoruz. Veri trafiğinde de alım arabiriminde ~500 Mbps değerinde trafik görülmekte ve fazlası olan 413Mbps 'li trafik verisi çöpe atılmaktadır.



Şekil 6.16. 700 Mbps Veri ve 490 Mbps Ses, toplam gönderilen trafiğin kapasiteyi aşması durumu

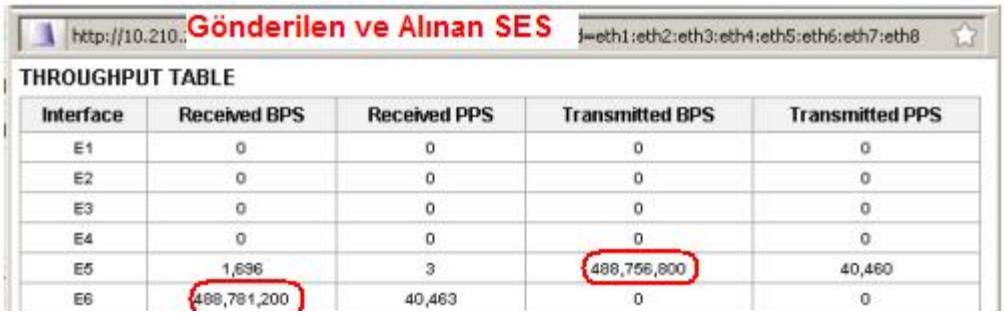
Şekil 6.16'da gönderilen ses trafiği garanti edilenden yüksek olmadığı için aynen iletilirken veri trafiği ile ses trafiği toplamı, toplam hat kapasitesinin üzerinde olduğundan, sese garanti edilen kapasiteden arta kalanı veri için kullanılması ve fazla verinın çöpe atılması beklenmektedir. Testlere bakılınca QoS'in çalıştığı ve alış arabiriminde trafik değerlerinin beklendiği gibi olduğu görülmektedir.



Şekil 6.17. 900 Mbps Veri ve 490 Mbps Ses, toplam gönderilen trafiğin kapasiteyi aşması durumu

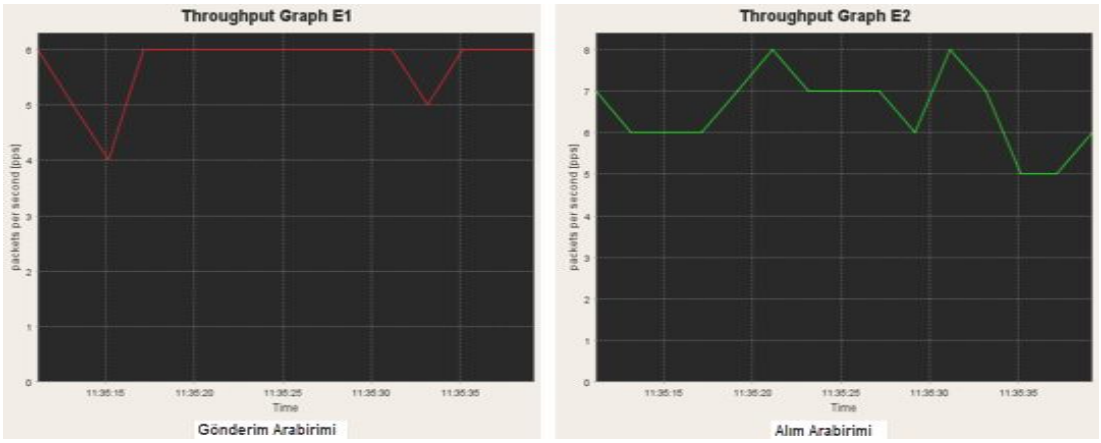
Şekil 6.17'deki durum ile Şekil 6.16'daki durum da aynı görünüyor. Ses trafiği garanti edilen aralıkta ve çöpe atılmazken veri trafiği ses trafiğine eklenince toplam kasitenin üzerine çıkan miktarı çöpe atılıyor. Gönderilen 900Mbps veri trafiğinin sadece 495Mbps'inin iletilebildiği görülüyor.

Test5'te alınan arabirimde trafiğin -25 görünmesi Simena'nın alım arabirimine fazla paket geldiğini göstermektedir. Bu, daha çok Simena'nın bağlı olduğu ethernet anahtarda çalışan STP (Spanning Tree Protocol) ve bunun gibi protokollerden gelen paketlerden kaynaklanmaktadır. Test5'e ilişkin ölçümlerdeki Simena ekran görüntüsü Şekil 6.18'de görülmektedir. Buna göre fazla gelen paket sayısı 3 olup bu da gayet normal bir değerdir. Şekil 6.18'deki "Transmitted PPS" ve "Received PPS" arasındaki farkın 3 olduğu görülmektedir. Simena alım arabirimine fazladan 3 paket geldiği görülmetedir.



Şekil 6.18. QoS Test5 için Simena ölçüm ekran görüntüsü

Simena, sadece ayarlanan trafik miktarını gönderim arabiriminden gönderir. Alım arabiriminden ölçüm sırasında ne gelirse onları alır. Hattın kesildiği anda yönlendiricilerin gönderdiği OSPF, MPLS ve anahtarların gönderdiği STP mesajları bu sayının yükselmesine neden olmuş olabilir. Bununla beraber, ölçüm hatası veya cihazla ilgili anlık bir sorun da olabilir. Şekil 6.19'de hiç trafik gönderilmediği durumda Simena'nın gönderim ve alım arabirimlerindeki trafik değerleri görülmektedir.



Şekil 6.19. Trafik gönderilmediği durumda Simena arabirimlerindeki trafik değerleri

Şekil 6.19'de de görüldüğü gibi Simena gönderim ve alım arabirimlerinde bir miktar sapma görünmektedir.

Yapılan QoS testlerinde, QoS çalışmasa veya uygulanmasaydı, toplam trafiğin hat kapasitesini aşması durumlarında FIFO kuralının geçerli olması beklenirdi. Buna

göre GSR-2 yönlendiricisinin Gi0/4/0/3 çıkış arabirimine öncelikli gelen paketlerin ne olduğuna bakılmaksızın iletilmesi ve dolayısı ile iletilen trafiklerin gönderilen trafikle orantılı olacak şekilde hat kapasitesini doldurması kalan trafiğin ise ne olduğuna bakılmaksızın atılması gerekirdi. Bu durumda, video, ses ve sinyalleşme gibi kritik trafikler de etkilenecek, ama kritik olmayan kullanıcı verileri iletilebilecekti.

Ölçüm sonuçlarından da görüldüğü gibi gönderilen trafik ne kadar olursa olsun hat kapasitesi kadar çıkışta trafik oluşmaktadır. QoS politikası bir arabirime uygulanmışsa trafik arabirimden çıkarken ve hat kapasitesinin üzerinde ise uygulanmaktadır. Uygulanan politikada belirlenen trafik türlerine istenen BW ayrılır ve kritik trafik tipinin kayıpları engellenmiş olur.

7. SONUÇ

Günümüzde teknolojik gelişmeler bir taraftan insanların yaşam standardını arttırırken, diğer yandan insanların beklentilerini de arttırmaktadır. Buna bağlı olarak da yeni araştırmalar yapılmakta ve teknolojik ilerleme hız kesmeden devam etmektedir. Bakıldığı zaman birbirini takip eden bir döngü halinde devam etmekte olan bu süreç, günümüzde iletişim teknolojilerinde çok belirgin şekilde kendisini göstermektedir.

İnternet ve ağ kavramlarının hayatımıza girmesi, iletişim teknolojilerinin kırılma noktasını oluşturmuştur denilebilir. Zira bundan sonra dünyanın dört biryanındaki işlerimizi internet üzerinde halledebilir hale geldik.

İnternetin bu denli büyümesi ve sanal sosyal ortamdan, sanal iş dünyası gibi birçok kavramın da hayatımıza girmesine neden oldu. Başta sadece dosya paylaşımı ve e-posta amacıyla kullanılan internet günümüzde ticaret, ses, video, dosya gibi birçok kritik verinin taşındığı bir ortam haline gelmiştir. Hal böyle olunca paylaşımlı ortam olan internette ve internete bağlantıda aracılık yapan servis sağlayıcılar tarafında bazı ihtiyaçlar da ortaya çıkmıştır. Örneğin, sesin daha kaliteli ve kesintisiz iletimi video görüntülerinin kesik kesik değil de akıcı şekilde iletilmesi, veri iletiminde kullanılan hatların yedeklenmesi, asıl hatlarda yaşanan sorunlardan dolayı sistemlerin yedek hatta geçiş sürelerinin azaltılması, burada yaşanan veri kayıplarının minimize edilmesi gibi ihtiyaçları ortaya çıkarmıştır.

Bu tez çalışmasında, günümüzde en yaygın kullanılan geleneksel yönlendirme protokollerinden OSPF'in hat kesilmelerinde yedek hatta geçiş süresi ve burada yaşanan veri kayıpları ile MPLS-TE-FRR teknolojisi kullanıldığında yedek hatta geçiş süresi ile veri kayıpları karşılaştırılmıştır. Ayrıca, hat kesilmesi olmaksızın hattın kapasitesinin aşılması durumunda kritik verilerin nasıl korunabileceği incelenmiştir.

Sadece OSPF protokolü kullanıldığı zaman yönlendiriciye direkt bağlı bir hat problemi durumunda yedek hatta geçiş süresinin 220 msn'ler civarında çıkarken MPLS-TE-FRR'da bu sürenin 2 msn olması dikkat çekicidir. MPLS-TE-FRR,

teknolojisi geçiş hızını her durumda 50 msn altında olacağını garanti etmekte olup yapılan testlerde 2 msn olması yönlendiriciye direkt bağlı linkte yaşanan sorunun yönlendirici tarafından hemen fark edilmesi ve MPLS-TE-FRR teknolojisinden kaynaklanmaktadır. OSPF'de sürenin uzamasının nedeni hat kesilince Dijkstra algoritmasının tekrar çalıştırılması ile alternatif yolların bulunması sürecinden dolayı uzamaktadır. Hat geçiş süresinin uzaması beraberinde geçiş süresince veri kaybedilmesine dolayısı ile müşteri memnuniyetsizliği ve servis kalitesi düşüklüğüne neden olmaktadır. Bununla beraber paylaşımlı ortamlarda çok rastlanan sorunlardan birinin hatların kapasitesinin üzerinde veri aktarımına zorlanması durumudur ki, bu durumda üreticiler genellikle varsayılan olarak son gelen paketleri atarak bu durumu idare ederler. Burada QoS teknolojisi sayesinde gelen paketlerin ses, veri, video, sinyalleşme ..vs olduğunu gösteren işaretlemeler ve işaretlenen trafik sınıflarına özel bazı iletim politikaları yapılabilmekte ve hat yoğunlaşması durumunda kritik verilerin kayıpsız iletimi sağlanırken, az kritik verilerin atılması sağlanarak, kritik verilerin sorunsuz iletilmesi sağlanabilmektedir. Yaptığımız testlerde hat kapasitesi olan 1Gbps üzerinde veri gönderdiğimizde ses için ayırdığımız 500Mbps'lik kapasitenin her zaman garanti edildiğini, bununla beraber diğer verilerin atıldığını gördük.

Ölçüm sonuçlarına göre günümüzde kritik veri taşıyan ağlarda veri kayıplarını kesinti sürelerini azaltmak ve dolayısı ile müşteri memnuniyeti ile servis kalitesini arttırmak için geleneksel yönlendirme protokollerine (OSPF, BGP, IS-IS... vs) ek olarak MPLS-TE-FRR ile birlikte hat yoğun kullanımları durumunda ise kritik verilerin atılmayıp iletimini sağlamak adına QoS mutlaka kullanılmalıdır.

KAYNAKLAR

1. Yıldırımoğlu, M., "TCP/IP İnternet'in Evrensel Dili 3. Baskı", ***Pusula***, İstanbul, 9-64 (2000).

2. Parziale, L., Brit D.T, Davis C., Forrester J., Liu W., Matthews C., Rosselot N., "TCP/IP Tutorial and Technical Overview Eight Edition", ***IBM,*** USA, (2006).

3. Lammle, T., "CCNA Cisco Certified Network Associate Study Guide, Second Edition", ***Sybex,*** USA, 1-157 (2000).

4. Odom, W., "CCNA Intro Exam Certification Guide", ***Cisco Press***, Indianapolis, 20-165 (2000).

5. İnternet: Cisco, "Networking Academy Program (CNAP)" http://www.cisco.com/web/learning/netacad/index.html***,*** (2009).

6. Blanchet, M., "IP Addressing and Subnetting: Including IPv6", ***Syngress,*** Canada, (2000).

7. İnternet: IETF, "Address Allocation for Private Internets" http://www.ietf.org/rfc/rfc1918.txt (1996).

8. Doyle, J., "Routing TCP/IP Volume I", ***Cisco Press, USA***, 9-357 (1998).

9. İnternet: "Open Shortest Path First", http://en.wikipedia.org/wiki/Open_Shortest_Path_First.

10. Moy, J., OSPF Version 2, The Internet Society, (1998) http://www.ietf.org/rfc/rfc2328.txt.

11. Naugle, M.,G., Illustrated TCP/IP, John ***Wiley & Sons,*** USA, 62-64 (1998).

12. Solie, K., "CCIE Practical Studies, Volume 1", ***CiscoPress,*** USA, 745, (2002).

13. Siva, C., Murthy, R. And Gurusamy, M., "WDM Optical Networks Concepts, Design and Algorithms", ***Prentice Hall PTR,*** New Jersey, (2002).

14. Cormen, T. H., Lierson, C. E., Rivest, R. L. and Stein, C.,. "Introduction to Algorithms", ***The MIT Press,*** Massachusetts, (2001).

15. İnternet: "Dijkstra's Algorithm", http://en.wikipedia.org/wiki/Dijkstra's_algorithm, (2010).

16. İnternet: "Dijkstra's Algorithm", http://cs.nyu.edu/courses/summer07/G22.2340-001/Presentations/Puthuparampil.pdf, (2010).

17. Genç, M.,B., "JIT protokolü kullanılan süperpaket anahtarlamalı optik ağlarda yönlendirme ve dağlagaboyu atama", Yüksek Lisans, ***İTÜ Fen Bilimleri Enstitüsü,*** İstanbul, 45 (2004).

18. Hattingh, C., Szigeti, T., "End-to-End QoS Network Design: Quality of Service in LANs, WANs, and VPNs", ***CiscoPress,*** USA, 44 (2004).

19. McQuerry, S., Jansen, D., Hucaby, D., Cisco LAN Switching Configuration Handbook, ***CiscoPress,*** USA, 223 (2009).

20. Park, II K., "QoS in Packet Networks", ***Springer, MITRE Corporation***, USA, 109-151 (2005).

21. Osborne, E., Simha, A., "Traffic engineering with MPLS", ***Cisco Press,*** USA, 25-26 (2003).

22. D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, J. McManus "Requirements for Traffic Engineering Over MPLS (RFC 2702)" http://rfc-2702.rfc-list.net/rfc-2702.htm (1999).

23. Nadeau, T.,D.,"MPLS Network Management: MIBs, Tools, and Techniques", ***Morgan Kaufmann Publishers, ,***USA, 7-21 (2003).

24. Başulaş, T., "MPLS omurag tasarımı", Yüksek Lisans Tezi, ***Beykent Üniversitesi Fen Bilimleri Enstitüsü, İstanbul,*** 28 (2006).

25.İnternet: Zulfiaji, A.,H., "MPLS Basic" http://www.zulfiaji.co.cc/2009/08/mpls-basic.html (2010).

26. Ghein, L., D., "MPLS Fundamentals: Forwarding Labeled Packets", ***Cisco Press****,USA*, 5-300 (2007).

27. Pepelnjak, I., Guichard, J., "MPLS and VPN architectures, Volume 1", ***Cisco System Inc***., USA, 16 (2002).

28. Liotine, M., "Mission-critical network planning", ***Artech House Inc.,*** USA, 100 (2003).

EKLER

EK-1 Simena QoS ölçüm sonuçlarının ekran görüntüleri

Simena ile yapılan QoS ölçümlerinde gönderim ve alım arabirimlerindeki trafik değişimlerinden örnekler Şekil 1.1 ve Şekil 1.2'de görülmektedir.

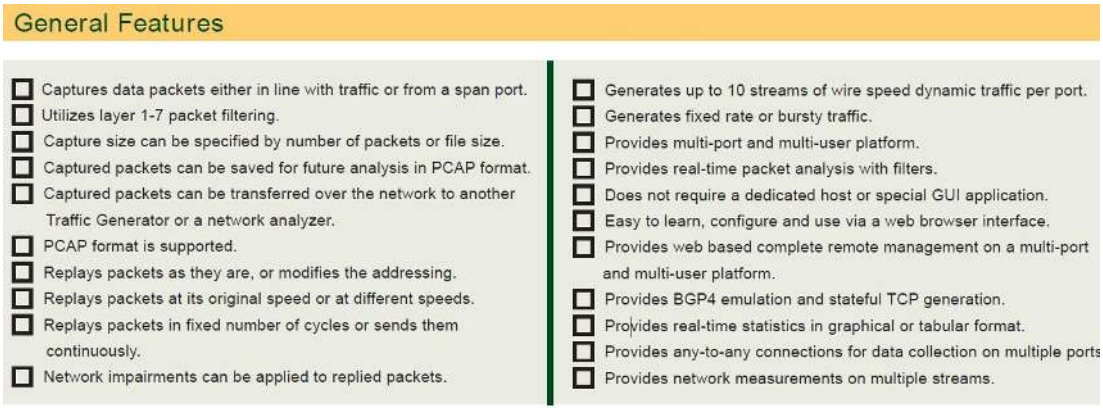
Şekil 1.1 QoS uygulandığı durumda 900Mbps veri gönderildiğinde gönderim ve alım arabirimlerinin ekran görüntüsü

Şekil 1.1'de gönderilen 900Mbps'lik veri, hat dolduğu ve QoS uygulandığı için 495Mbps olarak çıkmaktadır. Yaklaşık 405Mbps'lik trafik atılmaktadır.

Şekil 1.2 QoS uygulandığı durumda 600Mbps ses gönderildiğinde gönderim ve alım arabirimlerinin ekran görüntüsü

Şekil 1.2'de gönderilen 600Mbps'lik ses trafiği QoS'de garanti edilen değerlerin (500Mbps) üzerine çıktığından 100Mbps'lik trafiğin atıldığı görülmekte.

EK-2 Simena TG 2000 sistem özellikleri



EK-3 Cisco GSR Teknik Özellikleri

Aşağıdaki linkte ve Şekil 3.1'de GSR'ın özet teknik özellikleri bulunmaktadır.

http://www.cisco.com/warp/public/cc/pd/rt/12000/prodlit/gspel_ds.pdf

Cisco 12000 Family	Cisco 12004	Cisco 12008	Cisco 12012
Bandwidth	5 Gbps	10-40 Gbps	15 to 60 Gbps
Configurable Chassis Slots	4	8	12
Configurable Switch Fabric Slots	1	5	5
Maximum Line Card Support	3	7	11
OC-3/STM-1 ports[1]	12	28	44
OC-12/STM-4 ports[1]	3	7	11
Redundancy Options	GRP, line card, power	GRP, line card, power, fans, fabric	GRP, line card, power, fans, fabric

Şekil 3.1 GSR 12000 serisi yönlendiricilerin teknik özellikleri

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : OĞUL, Murat
Uyruğu : T.C.
Doğum tarihi ve yeri : 28.01.1976 Bozkır
Medeni hali : Evli
Telefon : 0532 2104083
Faks : -
e-mail :murat.ogul@gmail.com

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet tarihi**
Yüksek lisans	Gazi Üniversitesi /Elektrik-Elektronik Müh.	2010
Lisans	Gazi Üniversitesi/ Elektrik-Elektronik Müh.	2000
Lise	Gazi Lisesi	1993

İş Deneyimi

Yıl	**Yer**	**Görev**
2001-2006	Avea A.Ş.	Ağ ve Güvenlik Uzmanı
2006-	Turkcell A.Ş.	Kıdemli Güvenlik Uzmanı

Yabancı Dil

İngilizce

Hobiler

Yüzme, Kitap okuma, Futbol