T.C
BAHÇEŞEHİR ÜNİVERSİTESİ

PAKET YÖNLENDİRME YARDIMI İLE MOBİL İNTERNET SERVİS SAĞLAYICI AĞLARININ İZLENMESİ

Yüksek Lisans Tezi

TAHİR AYKUTLU

İSTANBUL, 2015

T.C
BAHÇEŞEHİR ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİ TEKNOLOJİLERİ

PAKET YÖNLENDİRME YARDIMI İLE MOBİL İNTERNET SERVİS SAĞLAYICI AĞLARININ İZLENMESİ

Yüksek Lisans Tezi

TAHİR AYKUTLU

Tez Danışmanı: Yrd. Doç. Dr. Yalçın ÇEKİÇ

İSTANBUL, 2015

T.C
BAHÇEŞEHİR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİ TEKNOLOJİLERİ

Tezin Adı: Paket Yönlendirme Yardımı İle Mobil İnternet Servis Sağlayıcı Ağlarının İzlenmesi
Öğrencinin Adı Soyadı: Tahir Aykutlu
Tez Savunma Tarihi: 26.05.2015

Bu tezin Yüksek Lisans tezi olarak gerekli şartları yerine getirmiş olduğu Fen Bilimleri Enstitüsü tarafından onaylanmıştır.

Doç. Dr. Nafiz ARICA
Enstitü Müdürü
İmza

Bu tezin Yüksek Lisans tezi olarak gerekli şartları yerine getirmiş olduğunu onaylarım.

Doç. Dr. Mehmet Alper TUNGA
Program Koordinatörü
İmza

Bu tez tarafımızca okunmuş, nitelik ve içerik açısından bir Yüksek Lisans tezi olarak yeterli görülmüş ve kabul edilmiştir.

Jüri Üyeleri	İmzalar
Tez Danışmanı Yrd. Doç. Dr. Yalçın ÇEKİÇ	----------
Üye Yrd. Doç. Dr. Oğuzhan Ertaş	----------
Üye Doç. Dr. M. Alper TUNGA	----------

TEŞEKKÜR

Bu tez çalısmasının yürütülmesinde bilgi ve tecrübelerinden yararlandığım, bilgilendirme ve yönlendirmeleriyle çalısmamın bilimsel temeller ışığında sekillenmesine yardımcı olan, pozitif kişiliği ile beni sürekli motive eden danışman hocam sayın Yrd. Doç. Dr. Yalçın ÇEKİÇ' e sonsuz tesekkürlerimi sunarım.

Bu zorlu süreç boyunca bütün desteği ile yanımda olan sevgili eşim Selin Aykutlu' ya tüm kalbimle teşekkür ederim.

Mayıs, 2015 **Tahir AYKUTLU**

ÖZET

PAKET YÖNLENDİRME YARDIMI İLE MOBİL İNTERNET SERVİS SAĞLAYICI AĞLARININ İZLENMESİ

Tahir Aykutlu

Bilgi Teknolojileri

Tez Danışmanı: Yrd. Doç. Dr. Yalçın Çekiç

Mayıs 2015, 55 Sayfa

Mobil internet teknolojisinin hızla ilerlemesi, buna paralel olarak artan kullanıcı ve uygulama sayıları ile birlikte bu hizmeti veren servis sağlayıcı ağlarıda büyüyerek karmaşık bir hal almıştır. Bu karmaşık yapı içerisinde ağdaki problemleri en kısa sürede tespit etmek gerek müşteri gerek firma açısından hayati önem taşımaktadır. Mevcut durumda erişim problemleri çoğunlukla müşteri şikayetleri sonucu fark edilmektedir. Bu çalışmada erişim problemlerinin en kısa zamanda tespit edilmesi amacıyla ağda kullanılan cihazların çeşitli özelliklerinden faydalanılmıştır. Çalışma, mobil internet servis sağlayıcısı ağına uygulanarak işlevselliği test edilmiştir. Bu tez çalışması mobil internet servis sağlayıcısı firmasında teknik ve yönetim ekipleri ile tartışılarak ve destek alınarak geliştirilmiş olup ihtiyaçlara ve gereksinimlere uygun olarak ortaya çıkarılmıştır.

Anahtar Kelimeler: Mobil Ağ, Servis Sağlayıcı, Ağ İzleme, İnternet, Erişim Problemleri,

ABSTRACT

MONITORING INTERNET SERVİCE PROVİDER NETWORKS WITH THE HELP OF PACKAGE ROUTİNG

Tahir Aykutlu

Information Technologies

Thesis Supervisor: Assist. Prof. Dr.Yalçın ÇEKİÇ

May 2015, 55 Page

As the rapid growth of the mobile Internet technology and the rising number of users and applications in parallel with this growth, the networks of the service providers have become larger and more complicated. Detecting the problem in the shortest time in this complicated mobile network has a vital importance by means of both the service provider companies and the customers. In the current situations, the access problems are mainly recognised by the reports from the customer complaints. In this study, in order to detect the access problems in the shortest possible time, the capabilities and specifications of the devices on the network were used. This study was applied to the mobile service provider network to test its functionality. This thesis study, designed according to the mobile network needs and requirements, was prepared in the mobile service provider company by discussing with its technical and executive teams and with the help of those teams.

Keywords: Mobile Network, Service Provider, Network Monitoring, Communications Problems, İnternet

İÇİNDEKİLER

TABLOLAR

ŞEKİLLER

KISALTMALAR

ADLS	:	Asymetric Digital Subcriber Line
ARPA	:	Address and Routing Parameter Area
ATM	:	Asynchron Transfer Mode
BGP	:	Border Gateway Protocol
CIDR	:	Classless Inter Domain Routing
DARPA	:	Defense Advanced Research Projects Agency
DHCP	:	Dynamic Host Configuration Protocol
DNS	:	Domain Name System
ELSR	:	Egress Label Switched Router
FEC	:	Forwarding Equivalence Classes
FTP	:	File Transfer Protocol
HTTP	:	Hyper Text Transfer Protocol
HTTPS	:	Hyper Text Transfer Protocol Secure
ICMP	:	Internet Control Messaging Protocol
IEEE	:	Institute of Electrical
IETF	:	Internet Engineering Task Force
IP	:	Internet Protocol
IPV4	:	Internet Protocol Version 4
IPV6	:	Internet Protocol Version 6
ISDN	:	Integrated Service Digital Network
ISP	:	Internet Service Provider
ISS	:	Internet Servis Sağlayıcı
LAN	:	Local Area Network
LDP	:	Label Distribution Protocol
LER	:	Label Edge Router
LSP	:	Label Switched Path
LSR	:	Label Switched Router
MPLS	:	Multi Protocol Label Swithching
MTU	:	Maximum Transmit Unit
NIC	:	Network Interface Card

OSI	:	Open System Interconnection
OSPF	:	Open Shortest Path First
QOS	:	Quality of Service
POP	:	Point of Presence
RFC	:	Request for Comment
SMTP	:	Simple Mail Transfer Protocol
SNMP	:	Simple Network Management Protocol
TCP	:	Transmit Control Protocol
TE	:	Traffic Engineering
TELNET	:	Telecommunication Network
TFTP	:	Text File Transfer Protocol
TTL	:	Time To Live
TTNET	:	Turk Telekom Network
UDP	:	User Datagram Protocol
VLAN	:	Virtual Local Area Network
WAN	:	Wide Area Network

1. İNTERNET

1.1 İNTERNETİN TANIMI

İnternet, birden çok bilgisayar ağının birbirine bağlı olduğu, dünya üzerinde sürekli büyüyen ve yaygın olarak kullanılan bir iletişim ağıdır. Bu büyük ağda bilgisayarlar birbirlerine kablolar, uydu bağlantıları, kablosuz erişim noktaları vb. şekilde bağlıdır. Örnek şekil 1.1' de görüldüğü gibi internet dünyanın farklı yerlerinde bulunan bilgisayarların birbirleriyle iletişimlerini sağlar.

Şekil 1.1: İnternet topolojisi

Kaynak: http://mas-alla-de-somosaguas.blogspot.com.tr/2008_11_01_archive.html

Bu bağlantı üzerinde özel protokollerle (TCP/IP gibi) birbirine bağlı bilgisayarlar arasında dosya alış verişi, yazıcı paylaşımı, sohbet vb. gibi birçok iş yapılabilir. Bu noktada internetin temel mantığının bilgiyi saklama, paylaşma ve ona kolayca erişme olarak ifade edilebilir.

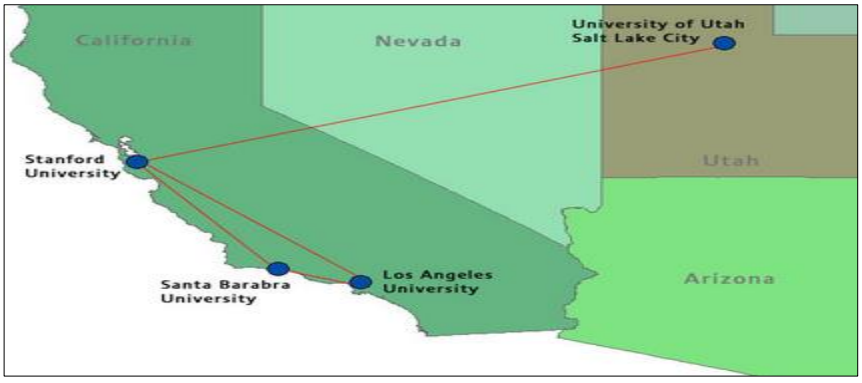
İnterneti, kişilerin düşüncelerini serbestçe söyleyebildikleri, evden alışveriş ve bankacılık hizmetlerini gerçekleştirebildikleri, günlük gazeteleri ve yayınları takip edebildikleri, birbirleriyle çeşitli uygulamalar yardımı ile haberleşebildikleri, hayatımızı oldukça kolaylaştıran bir sosyal platform olarak da değerlendirilebiliriz.

Günümüzde internet kullanıcı sayısı 2.4 milyar kişiye ulaşırken, her bir dakika da gerçekleşen paylaşım sayısı da her yıl katlanarak devam etmektedir. Dijital dünyaya gidişi örneklendirmek gerekirse, 2013 yılında internet ortamında 127 milyon mail gönderildiği ve google üzerinden 2 milyon arama yapıldığı belirlenmiştir. 2014 yılında ise dakikada 137 milyon e-posta gönderildiği, google üzerinden dakikada 4 milyon arama yapıldığı belirlenmiştir. Youtube üzerine 2013 yılında ortalama 30 saatlik video yüklenirken 2014' de bu sayı 72 saate çıkmıştır.

1.2 İNTERNETİN TARİHİ

İnternetin ortaya çıkışı Amerikan Federal Hükümeti Savunma Bakanlığı'nın araştırma ve geliştirme kolu olan Savunma İleri Düzey Araştırma Projeleri Kurumuna (DARPA) dayanır. 1969 yılında Savunma Bakanlığı, bilgisayar bilimlerini ve askeri araştırma projelerini desteklemek amacıyla ARPANET adında paket anahtarlamalı bir ağı oluşturmaya başladı. Örnek şekil 1.2 ARPANET' in 1969 yılındaki topolojisini görebiliriz.

Şekil 1.2: ARPANET 1969



Kaynak: http://redestelematicas.com/wp-content/uploads/2013/09/arpanet.jpg

Bu ağ zaman içerisinde ABD' de bulunan üniversite ve araştırma kuruluşlarına ait bilgisayarların da katılımı ile giderek büyüdü. Bu büyüme neticesinde ilerleyen yıllarda ARPANET kullanımdan kaldırıldı. 1990 yılında gerçekleşen bu olaydan sonra ARPANET' in yerini ABD, Avrupa, Japonya ve Pasifik ülkelerindeki omurgalar (backbone) aldı.

Türkiye internetle Nisan 1993' de tanıştı. ODTÜ' den gerçekleştirilen ilk bağlantı 64kbit/sn hıza sahip olmasının yanında uzun süre tüm ülkenin tek internet çıkışı olma özelliğine de sahipti. Ardından diğer üniversiteler sırasıyla internet bağlantılarını gerçekleştirdiler. 1996 yılında TURNET çalışmaya başladı, ardından 1997 de akademik kuruluşların internet bağlantısını sağlayan ULAKNET çalışmaya başladı. 1999 yılına gelindiğinde ise ticari ağ altyapısında yaşanan büyük değişiklikler sonucunda Turnet' in yerini TTNET almıştı. 2000 yılında ticari kullanıcılar TTNET üzerinden, akademik kuruluşlar ise ULAKNET omurgası üzerinden internete erişmeye başladı.

Türkiye' nin internete erişimini sağlayan merkezler 3 ana grupta toplanabilir;

1. Ticari kuruluşların ve internet servis sağlayıcıların (ISP), TTNET üzerinden yararlandığı çıkışlar.
2. Üniversite ve akademik kuruluşların internet çıkışları.
3. Bazı özel şirketlerin ve ISP' lerin TTNET ile yaptıkları anlaşma sonucu kullandıkları doğrudan yurtdışı internet çıkışları.

1.3 DNS VE İNTERNET ADRESLERİ

İnternet üzerinde bulunan her bilgisayarın kendine özgü bir adresi vardır. Domain Name System (DNS) olarak adlandırılan hiyerarşik bir isimlendirme sistemi yardımı ile internete bağlı bilgisayarlara ve bilgisayar sistemlerine isimler verilir. Bu durum şu şekilde ifade edilebilir, internete bağlı her bilgisayarın kendine özgü bir adresi vardır ve DNS, host isimlerini IP adresine çevirmeye yarayan sistemdir.

DNS ihtiyacı ilk olarak ARPANET zamanında ortaya çıkmıştır. Bilgisayar ağları bu dönemde günümüz ağları ile karşılaştırılamayacak derecede küçük durumdaydı. Birkaç yüz ile sayılabilen sitelere erişim için hosts dosyası kullanılıyordu. İnternetteki bilgisayarların isimleri ve IP adresleri bu dosyanın içine elle kaydediliyordu. İnternetteki her bilgisayarda bu dosyanın bir kopyası bulunmaktaydı. Sistem, isimlendirme için tek bir noktada dosya tutulması ve diğer tüm sistemlerin bu dosyayı belli aralıklarla kendi taraflarında güncellemesi şeklinde çalışıyordu. Örneğin bir bilgisayar başka bir bilgisayara erişmek istediğinde bu dosyanın içerinde bulunan IP adresini alıp iletişime geçiyordu. Hosts dosyası SRI tarafından SRI-NİC (Stanford Research Institute – Network Information Center) adında bir bilgisayarda tutulmaktaydı.

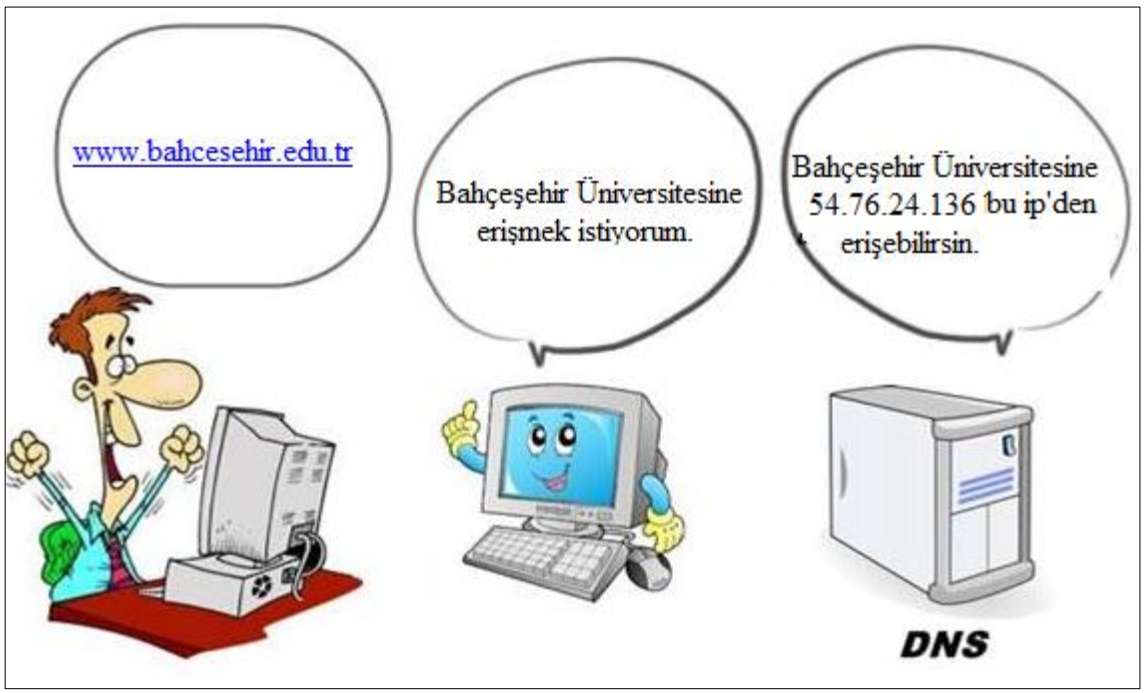
İnternetteki bilgisayar sayısı arttıkça hosts dosyasının yönetimi zorlaştı. Hem dosyanın büyüklüğü olağanüstü boyutlara ulaştı hem de internetteki bilgisayarların dosyayı kopyalamak için yaptıkları bağlantı Stanford' da ki bilgisayarları kilitlemeye başladı. Bu sorunların ortaya çıkmasından sonra 1984 yılında DNS üretildi. DNS sayesinde bilgisayarlar bulundukları yerlere ve ait oldukları kurumlara göre sınıflandırılmaya başlandı. Örneğin Türkiye' deki bilgisayarların listesini(.tr domaini) Türkiye'den sorumlu olan DNS sunucu makinede tutulmaktaydı. Böylece DNS sayesinde internet bulutunda bulunan bütün bilgisayarların bilgisinin tek bir yerde tutulması zorunluluğu kalmıyordu.

Network ağınız üzerinde yada internette herhangi bir web sayfasına, kaynağa, dosya sunucusuna, mail sunucusuna ismiyle ulaşmak istediğimizde, bilgisayarımıza o kaynağın IP adresini DNS bildirir. Yani bir web adresine erişmek istediğinizde, DNS, hangi site nerede hangi IP hangi bilgisayara ait olduğunu belirler ve sizin erişiminizi sağlar.

Örnek olarak, Bahçeşehir Üniversitesi' nin web sitesini tuttuğu bilgisayarın IP adresi 54.76.24.136 ; biz eğer Bahçeşehir Üniversitesi' nin web sitesine gitmek istediğimizde DNS olmasaydı adres satırına http:// 54.76.24.136 yazmamız gerekirdi. Oysa www.bahcesehir.edu.tr hatırlanması daha pratik ve kolay bir adres. İşte

www.bahcesehir.edu.tr adresinin 54.76.24.136’ ya dönüştürülmesi işini yapan sisteme Domain Name System (DNS) denilmektedir. Alan adını yada diğer bir deyimle adresi, IP adresine dönüştürme işine ise DNS Name Resolotion (Alan Adı Çözümleme) denilmektedir. Örnek şekil 1.3’ de DNS çalışma mantığı resmedilmiştir.

Şekil 1.3: DNS çalışma mantığı



Kaynak: Bu şekil Tahir Aykutlu tarafından hazırlanmıştır.

DNS sistemi isim sunucularından ve çözümleyicilerden oluşmaktadır. İsim sunucu olarak konfigüre edilen bilgisayarlar host isimlerine karşılık gelen IP adresi bilgilerini tutarlar. Çözümleyicilere ise DNS istemciler olarak isimlendirebiliriz. DNS istemcilerde, DNS sunucu yada sunucularının adresleri bulunmaktadır.

İstemciler bir bilgisayarın host ismine karşılık gelen IP adresini bulmak istediğinde isim sunuculara gider. İsim sunucu (DNS sunucu) eğer kendi veri tabanında öğrenilmek istenen host ismine karşılık gelen IP adresi varsa bunu istemciye gönderir.

İnternet adresleri öncelikle ülkelere göre ayrılmaktadır. Adreslerin sonunda bulunan Türkiye için "tr", Almanya için "de", İngiltere için "uk", Rusya için "ru" ifadeleri adreslerin bulundukları ülkeleri gösterir. Buna İnternet Ülke Alan Kodu denir. Her internet sitesinde ülke alan kodu bulunmamaktadır. ABD ve Kanada adreslerinin çoğu ve bazı geniş kitlelere servis sunan adresler buna örnek verilebilir.

İnternet adresleri ülkelere ayrıldıkdan sonra değişik gruplara da(.com, .net, .edu) ayrılabilir. İnternet adresi hangi gruba dahilse ilgili kısaltmayı mutlaka içerir. Tablo 1.1' de internet adreslerinin uzantıları ve açıklamaları verilmiştir.

Tablo 1.1: İnternet adreslerinin uzantıları

.com	Genel ve ticari konularda kullanılır.
.net	Ağ ve örgütlenme anlamında kullanılmaktadır.
.org	Organizasyonlar için kullanılır.
.edu	Eğitim kurumlarına ait olan sitelerde kullanılmaktadır.
.mil	Askeri kurular tarafından kullanılmaktadır.
.int	Uluslararası organizasyonlar ve kuruluşlar

Kaynak: Bu tablo Tahir Aykutlu tarafından hazırlanmıştır.

İnternet adresi eğer özel amaçlı bir servis ise, adresin başında kullanılan (ftp, gopher, www, http) bir kısaltma yardımı ile belirtilir. Tablo 1.2' de bu kısaltmalar ve açıklamaları verilmiştir.

Tablo 1.2: Servis kısaltmaları ve açıklamaları

http	İletişim protokolü
ftp	Dosya aktarım protokolü
gopher	İnternet üzerinde servis protokolü
www	İnternet ortamında bilgi sunumu, aktarımını ve paylaşımını sağlar

Kaynak: Bu tablo Tahir Aykutlu tarafından hazırlanmıştır.

2. İNTERNET SERVİS SAĞLAYICI

2.1 TANIMI VE SUNDUKLARI HİZMETLER

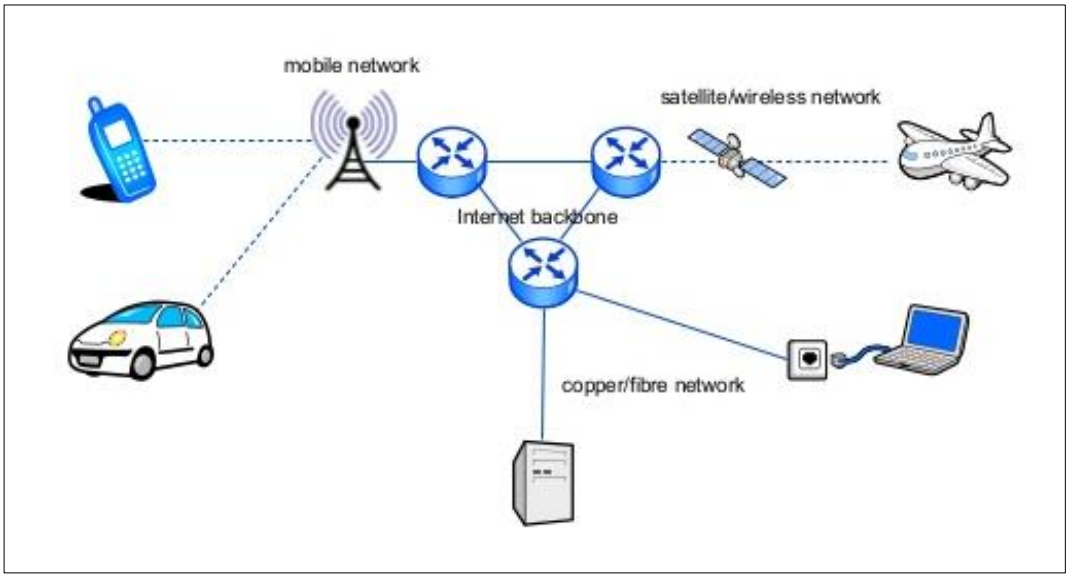
Türkçe İSS (İnternet Servis Sağlayıcı), ingilizce olarak ISP (Internet Service Provider) kısaltmasıyla ifade edilirler. Kişilere ve kurumlara belli bir ücret karşılığında internet erişimi sağlayan firmalar olarak bilinirler.

Günümüzde internet dünyası çok hızlı bir evrim geçirdiğinden İSS firmaları da sadece internet hizmeti vermekle sınırlı kalmayıp, ses ve görüntü, bilgisayarlar için yedekleme, güvenlik hizmetleri, web sitesi için alan sağlama gibi hizmetlerde vermeye başlamışlardır.

Hali hazırda GSM için kurulan firmalarda bu yeni ve daha geniş kesime hitap eden network e katılmışlardır. Bunda artan rekabet koşulları, nerdeyse gün içerisinde değişen pazar yapısı ve kullanıcıların talepleri büyük rol oynamaktadır.

İSS firmalarından bazıları artık sabit telefon hatlarının yanında mobil hatlar yardımı ile abonelerine internet erişimi hizmeti sunar hale gelmiştir. Örnek şekil 2.1' de mobil bağlantı hizmeti de sunan bir İSS topolojisi görülmektedir.

Şekil 2.1: Mobil hizmette sunan İSS



Kaynak: http://www.slideshare.net/apnic/connecting-your-bank-to-the-internet

2.2 KULLANILAN PROTOKOLLER VE TEKNOLOJİLER

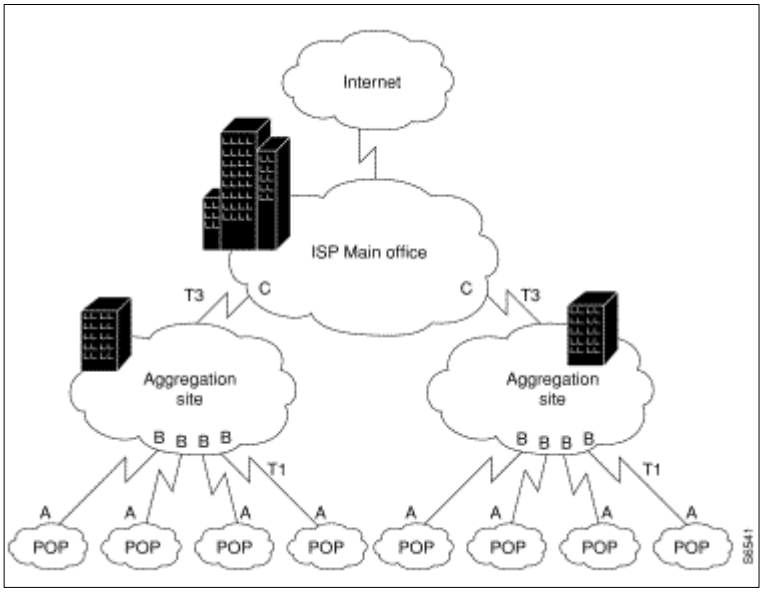
İSS firmalarının alt yapıları hizmet alma hızınızı etkiler. Bu sebeple kullanıcılar genelde kendilerine en ucuz ve en hızlı bağlantı hizmeti sağlayan firmaları tercih eder. Özellikle mobil pazarda bu müşteri eğilim daha çok görülmektedir.

Mobil cihazların destekledikleri uygulamalar da artık iş ve sosyal yaşamın önemli bir parçası haline gelmiştir. Operatörler tablet, akıllı telefon veya diz üstü bilgisayarlara sahip mobil kullanıcılarına sorunsuz bir hizmet verebilmek için çeşitli teknolojilerden yararlanmaktadır.

Bilgisayarlar yada cep telefonları internete bir ağın parçası olarak bağlanır. Örneğin bir bilgisayarınız var ve telefon hatları üzerinden internet servis sağlayıcınıza bağlanıyorsunuz. Bu artık sizin internet ağının, aynı zamanda IP ağının bir parçası olduğunuzu gösterir. Ardından internet servis sağlayıcınız başka bir ağa ve başka bir ağa bağlanır. Basit tanımıyla internet bu şekilde çalışmaktadır.

İnternet servis sağlayıcılarının çoğu kendilerine ait bir network mimarisine sahiptir. Bu network mimarisine backbone (omurga) da denilir. Backbone ağın bütün yükünü taşıyan parçası olarak görülür. Kullanıcılar İSS ağlarına POP (erişim noktaları) noktaları yardımı ile erişirler. Bu erişim çoğunlukla sabit telefon hattı, özel bir hat yada mobil şebeke yolu ile olur. Daha sonra toplama noktalarına (aggregation site) ulaşırlar. Örnek şekil 2.2' de İSS ağının görünümü resmedilmiştir.

Şekil 2.2: İSS ağının görünümü



Kaynak: http://docstore.mik.ua/cisco/

Yüksek data akışı isteyen bu omurga networklerin dizaynları yapılırken öncelikle katmanlar, bu katmanların işleyişinde kullanılacak cihazlar ve daha sonra bu cihazlar için uygun protokoller (iletişim kuralları) belirlenir.

2.2.1 TCP/IP (İletim Kontrol Protokolü / İnternet Protokolü)

TCP/IP (Transmission Control Protocol / Internet Protocol) internetin temel protokol paketidir. Bilgisayarlar üzerinden veri gönderme/alma organizasyonunu sağlayan, böylece bir yerden başka bir yere veri iletişimine olanak kılan pek çok veri iletişim protokolüne verilen genel isimdir. Verinin ağ içerisinde bir yerden başka bir yere hareket etmesi için ağın içinde bulunan tüm cihazların aynı dili konuşması yani aynı

protokolleri kullanması önemlidir. Protokol, ağ içerisinde veri iletişimini sağlıklı bir şekilde yapılmasını sağlayan kuralların tümüdür. Başka bir değişle TCP/IP bilgisayarlar arası veri iletişiminin kurallarını koyar.

TCP/IP birden çok protokolün bir araya gelmesiyle oluştuğundan, protokol paketi denir. İki katmanlı bir haberleşme protokolüdür. TCP bu protokol paketinin noktalar arası veri transferinde dikkat edilecek hususlar kısmı ile ilgilenirken, IP ise verilerin taşınacağı yol kısmıyla ilgilenir.

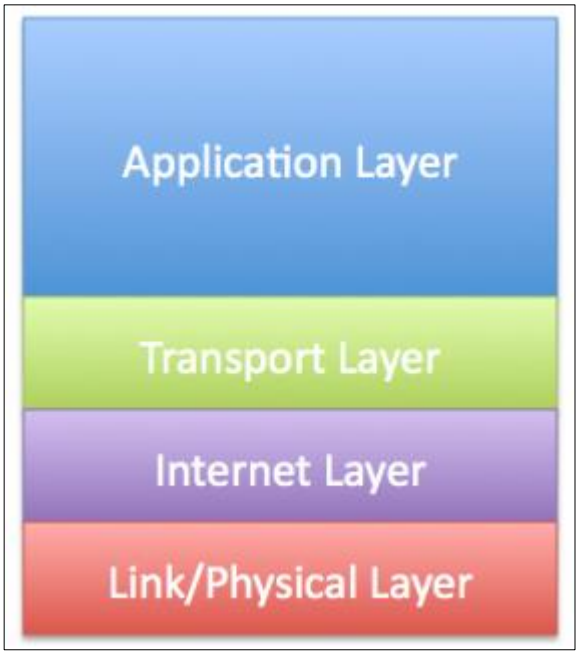
1970 yılında ARPANET bilgisayarları Network Control Protocol' ünü kullanmaya başladı. 1972' de Telnet, 1973' de FTP (File Transfer Protocol) ve 1974' de Transmission Control Program ayrıntılı bir şekilde tanımlandı. 1981 yılında ise IP standardı yayınlandı. 1982'de TCP ile IP, TCP/IP protokol suiti olarak tanımlandı. 1983 yılına gelindiğinde ise ARPANET, NCT' den TCP/IP' ye geçti. 1984 yılında ise Domain Name System (DNS) tanıtıldı. Aslında birbiri ardına gelişen bu olaylar bir bakımdan internetin kısa bir tarihidir.

TCP/IP ağında bilgisayarları üç farklı şekilde tanımlarız. Bunlar, bilgisayar adı, IP adresi ve mac adresidir. TCP/IP bu parametreleri kullanarak bilgisayarların iletişimini sağlar. Bilgisayar adı kullanıcı tarafından işletim sistemi yüklenirken verilen isimdir. Mac adresi ise bilgisayarların ağ, ethernet kartına yerleştirilen adrestir. IP adresi ise ağdaki cihazların birbirini tanıması, birbiriyle iletişim kurması ve veri alışverişinde bulunmak için kullandıkları benzersiz bir numaradır.

İnternet ağ mimarisi katmanlı bir yapı içerir. Ağ içerisindeki veri iletişimi bütün bu katmanlar tarafından yapılır. Her katman içerisinde yapılacak iş protokoller tarafından paylaşılmıştır. TCP ve IP farklı katmanlarda bulunan farklı protokoller olmasına rağmen ikisi bir arada TCP/IP olarak kullanıldığında bütün katmanları ve bu katmanlar içerisinde bulunan protokollerin bütününü ifade eder. Bundan dolayı TCP/IP bir protokoller kümesi olarak bilinir.

TCP/IP, uygulama, taşıma, internet ve fiziksel katman olmak üzere dört katmandan oluşur. Her katman farklı görevlere sahip olup altındaki ve üstündeki katmanlar ile iletişim sağlamakla yükümlüdür. Örnek Şekil 2.3' de TCP/IP katmanları görülmektedir.

Şekil 2.3: TCP/IP katmanları

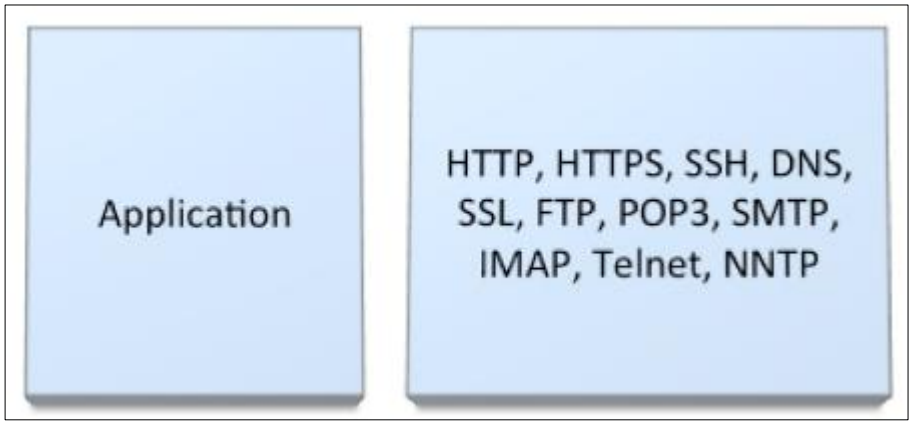


Kaynak: http://www.cellbiol.com/bioinformatics

2.2.1.1 Uygulama katmanı

En üst seviye katmandır. Uygulama katmanı için tanımlı olan FTP, SMTP vs. gibi protokoller hizmet verirler. Bunların bir üstünde ya kullanıcının doğrudan etkileşimde bulunduğu kullanıcı arabirim programları yada bilgisayara başka kullanıcılar için erişme imkanı sağlayan programlar bulunur. Örnek şekil 2.4' de uygulama katmanına ait protokolleri görülmektedir.

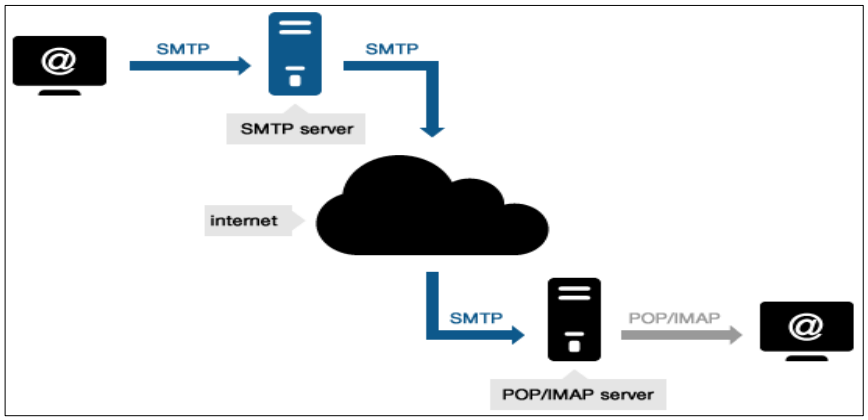
Şekil 2.4: Uygulama katmanı protokolleri



*Kaynak:*Bu şekil Tahir Aykutlu tarafından hazırlanmıştır.

SMTP (Simple Mail Transfer Protocol), elektronik posta iletimini gerçekleştirir. Elektronik postaların güvenli bir şekilde adreslerine ulaşabilmesi için TCP' den yararlanır. Elektronik posta mesajlarının standart bir formatı vardır. Mesajların bu formata uyması gerekir. Bu uyum sayesinde istemci ve sunucu arasında mesaj iletimi kolaylıkla sağlanır. Elektronik posta servisi mektupların bilgisayarlar arasında nasıl iletileceği ile ilgilenmez. Mektubun yollanması görevi TCP/IP ye aittir. SMTP protokolü ise iletim sırasında kullanılacak olan kurallar sırasını belirler. Örnek şekil 2.5' de SMTP topolojisini görmekteyiz.

Şekil 2:5 SMTP topoloji



Kaynak: http://www.serversmtp.com/en/free-smtp-server

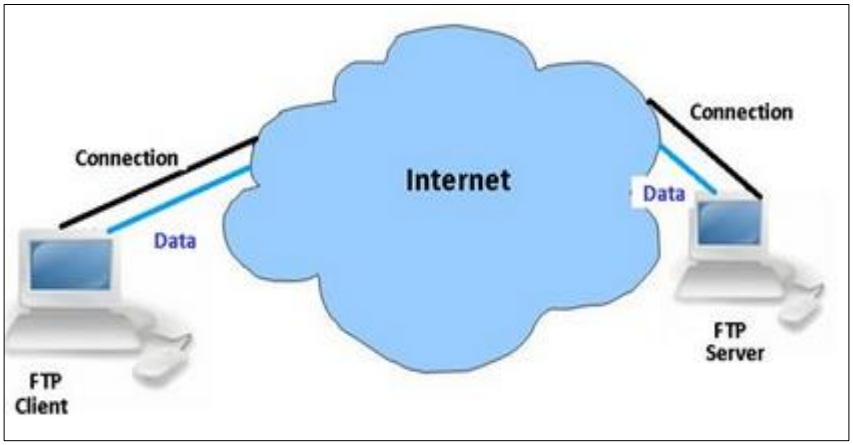
SNMP (Simple Network Management Protocol) ağ cihazlarının yönetimi için kullanılır. SNMP desteği sunan cihazlar SNMP mesajları sayesinde uzaktan yönetilebilmektedir. SNMP farklı türdeki cihazların yönetilmesi ve sorunlar hakkında bilgi sahibi olunması amacı ile tasarlanmıştır. Bu sayede yönlendiricilerin sıcaklık oranını, herhangi bir portunun üzerinde bulunan trafik miktarını yada DHCP sunucunun kaç bilgisayara IP adresi dağıttığını izleyebiliriz. SNMP, SNMP yönetim sistemleri ve SNMP ajanları olmak üzere iki kısımdan oluşur. Bunlardan SNMP yönetim sistemi özel bir yazılımdır. Ağdaki yazılım ve donanımların SNMP parametrelerini sorgular ve bunlardan çeşitli raporlar ve alarmlar çıkartır. SNMP ajanları ise kendilerine sorulduğu zaman veya daha önceden belirlenmiş olaylar gerçekleştiğinde yönetici sistemlere bilgi verirler.

TELNET (Telecommunication Network) interneti kullanarak başka bir bilgisayara bağlanılmasını sağlayan protokoldür. TELNET ile istenilen bilgisayara bağlanılıp o bilgisayarın yanındaymış gibi işlem yapabiliriz. TELNET metin tabanlı bir program olmasından dolayı bütün işlemleri komutlar ile yapabilmekteyiz. Kullanıcılar, TELNET client yazılımı kullanarak oturum başlatabilir daha sonrasında TELNET sunucusuna bağlanırlar. TELNET protokolü, bağlantı sırasında kullanılan mesajları şifrelememesi ve iletilen verilerin kolayca okunabilmesine olanak sağlamasından dolayı güvenlik zafiyeti taşır.

FTP (File Transfer Protocol) bir bilgisayardan diğer bir bilgisayara dosya aktarmamıza yarayan protokoldür. FTP protokol olmasının yanında aynı zamanda bir programdır. Protokol olarak çalıştığında, FTP uygulamaları tarafından, program olarak kullanıldığında ise kullanıcılar tarafından dosya hizmetlerini çalıştırmak için kullanılır. TCP/IP mimarisi geliştirilmeden öncede kullanılmaktaydı fakat zaman içerisinde değişerek günümüzdeki halini aldı. FTP, TCP sayesinde iki nokta arasında güvenli veri alışverişini sağlar. İlk geliştirilen internet protokolü olmasının yanında kullanıcı ile sunucu arasında görsel iletişimde sunar. Bu sayede dosya transferinin yanında kullanıcının dosyaların listelenmesi, kullanılacak komutların gösterilmesi gibi isteklerine cevap verir. FTP istemcileri TCP'yi kullanarak sunuculara bağlanırlar. İstemciler belirlenen kriterleri yerine getirdikten sonra dosya transfer işlemlerini başlatabilirler. Örneğin 50 MB boyutunda bir dosyayı göndermeniz gerekmekte. Birçok

e-mail sunucusu dosyanın boyutunun büyüklüğünden dolayı gönderimine izin vermeyecektir. İzin verse dahi dosyanın büyüklüğünden dolayı gönderim uzun zaman alacaktır. FTP böyle durumlarda iyi bir seçenektir. Bir FTP sunucu kurarak bu sorunu aşabiliriz. Ayrıca FTP e-mailden daha hızlıdır. TCP protokolünü kullandığından dolayı güvenilirdir. Oturum kapansa bile, FTP, tekrar başladığında kaldığı yerden devam eder. Şekil 2.6' da FTP' nin çalışma topolojisi görülmektedir.

Şekil 2.6: FTP topolojisi



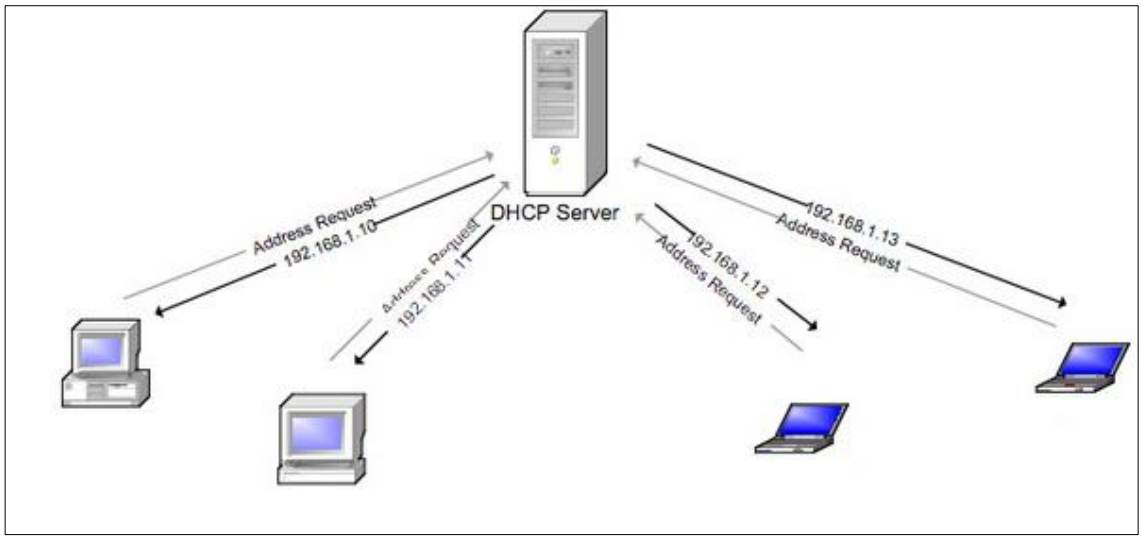
Kaynak: http://www.brighthub.com/internet/web-development

HTTP (Hyper Text Transfer Protocol) web kullanıcı programları ile sunucuların iletişim kurmasını sağlar. İnternet üzerinde bulunan sunucuların ve son kullanıcıların arasındaki veri alışverişine dair kurallar ve yöntemleri düzenler. Sunucudan istemciye, istemciden sunucuya dosya transferine olanak sağlar.

DNS (Domain Name Service) bilgisayar isimleri ve internet adreslerini çözümler. Yerel ağımızda ya da internet üzerinde herhangi bir hedefe ulaşmak istediğimizde bilgisayarımıza o kaynağın IP adresini bildirir. DNS ağ yaşamını kolaylaştırmak için tasarlanmıştır. DNS kullanmadan da bağlanmak istediğimiz web sayfasına IP adresini yazarak bağlanabiliriz. Fakat internet üzerindeki sayfaların IP adresleri aklımızda tutmak oldukça zordur. İşte DNS bize IP adresi yerine domain adı kullanma olanağını sağlar.

DHCP (Dynamic Host Configuration Protocol) IP adresi dağıtmaya yarayan protokoldür. Ağ yönetimini kolaylaştırır. Küçük yada oldukça geniş ağlarda fark etmeksizin kullanılır. Kullanıcı makinesi DHCP sunucusundan bir IP adresi istediğinde, DHCP sunucusunun istemci makineye IP adresi, subnet mask, domain ismi, default gateway, dns, ıns bilgisi gibi birçok bilgiyi sağlar. Bunlardan daha farklı ve fazla bilgi de verebilir. Fakat bunlar en yaygın olanlardır. Aktarım katmanında UDP protokolünü kullanır. Örnek şekil 2.7' de bir DHCP topolojisi görülmektedir.

Şekil 2.7: DHCP topolojisi



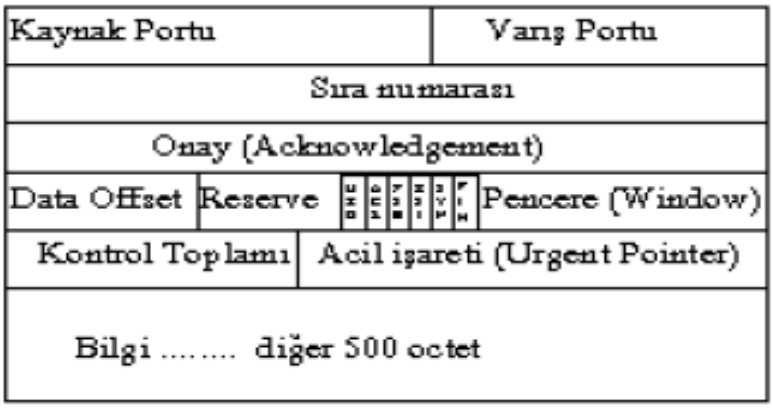
Kaynak: http://muhammedsoner.com.tr/28-dhcp-ip-havuzu-tuketme.msoner

2.2.1.2 Taşıma katmanı

TCP/IP içerisinde, uygulamalar arasında iletişimi sağlayan katmandır. TCP ve UDP olmak üzere veri iletişimini farklı yollarla sağlayan iki protokol içerir. TCP ve UDP aktarım katmanı protokolleridir. Bir üst katmandan gelen veriyi bir alt katmana iletir. Eğer veriler bir defada iletilemeyecek kadar büyükse parçalara ayrılır ve her birine bir sıra numarası verilir. TCP güvenilir iletişim sağlayan bir protokoldür. Gönderilen verinin kayıp olmadan iletimini garanti eder. UDP güvenilir olmayan bir iletişim sağlar. Bu nedenle daha çok TCP kullanılırken, UDP daha çok sorgulama amacıyla kullanılmaktadır.

TCP (Transmission Control Protocol), bağlantılı ve güvenli bir veri akışı sağlar. Verileri 8 bitlik gruplar halinde gönderir. Görevlerini yapabilmek için veri parçalarının önüne başlık bilgisi ekler. Verileri küçük paketlere ayırarak değişik yollardan ve değişik sıralar ile gönderir. Verileri göndermeye başlamadan önce kaynak makinenin TCP yığını, hedef makinenin TCP yığını ile iletişime geçer. Bu iletişim tipine connection-oriented (bağlantılı iletişim) denir. Veri hedefe ulaştığında paketlerin bir bütün olarak ve tam sırasıyla görülmesini sağlayan yine TCP' dir. Veriler ulaştıktan sonra paketler sağlam ise, TCP bir onay gönderir. Eğer paketler sağlam değilse bu paketlerin yeniden gönderilmesini sağlar. En önemli özelliklerinden biride her iki yöne ve sürekli veri akışını sağlamasıdır. TCP hizmet olarak sunduğu hata denetimi ve veri akış kontrolü yönüyle güvenilir bir protokoldür. TCP başlığı, 20 byte uzunluğundadır. İsteğe göre 24 byte' a kadar çıkabilir. Tablo 2.1' de bir tcp segmenti içeriği görülmektedir.

Tablo 2.1: TCP segmenti



Kaynak: http://yunus.hacettepe.edu.tr/~b0145561/bilgi_ilet.html

UDP (User Datagram Protocol) bağlantısız ve güvenilir olmayan veri akışı sağlar. UDP' de karşı tarafla iletişim kuralları için anlaşma gerekmediği ve giden mesajların yerine ulaşıp ulaşmadığını kontrol edilmediğinden daha hızlı bir veri iletişimi gerçekleşir. Verinin hızlı bir şekilde karşı tarafa ulaştırılması gerektiğinde, paket kaybının önemli olmadığı durumlarda kullanılır. Ses ve görüntü aktarımı gibi gerçek zamanlı veri aktarımlarında, toplu yayın-grup mesajlarında, DNS gibi istek-cevap temelli uygulamalarda son derece kullanışlıdır. Örneğin realplayerde web üzerinde bir şeyler izlerken kesintiler oluşmasının sebebi veri aktarımının denetlenmiyor olmasından

dolayıdır. UDP protokolü TCP'ye göre daha hızlı çalışır, fakat güvenirlilik ve sağlamlık kriterleri göz önüne alındığından UDP protokolünün çok fazla dezavantajı vardır. UDP ayrıca TCP' nin birçok ekstra özelliğini sağlamaz. Tablo 2.2' de TCP ile UDP farkları gösterilmiştir.

Tablo 2.2: TCP ile UDP farkları

SERVİS	TCP	UDP
Bağlantı Kurulumu	Güvenli bağlantı kurulur	Bağlantıya gerek duymaz
Teslim Garantisi	Gönderildiğini onaylar	Kaybolan paketler tekrar gönderilmez
Paketlerin Sırası Hakkında Bilgi	Ardışık numaralandırılmış paketler	Ardışık numara vermez. Paketlerin sürekli ulaştığını yada kaybolduğunu düşünür.
Akış Kontrolü	Alıcı vericiye yavaşlaması için sinyal gönderebilir	Akış kontrolü için TCP' de kullanılan onay UDP' den geri dönmez
Tıkanıklık Kontrolü	Ağ cihazları TCP onay paketleri sayesinde göndericinin tavrını kontrol edebilir	Onay olmadan ağ tıkanıklılık sinyali göndermez

Kaynak: Bu tablo Tahir Aykutlu tarafından hazırlanmıştır.

TCP yerine UDP' nin tercih edildiği durumlardan biride SNMP 'dir. SNMP ajanları uygulama katmanında çalışır. SNMP ağ üzerinde yeterince aralıklı mesajlar ile yeterince düzenli güncelleme ve alarm akımları göndererek ağı izler. Bu küçük mesajları kurmak, devam ettirmek ve kapatmak için ek yük maliyeti, sağlıklı ve hızlı çalışan bir ağ gerektirir.

UDP, segmentleri sıraya almaz, hedefe hangi sırayla ulaşacağıyla ilgilenmez. Segmentleri gönderir ve unutur. Bunlardan dolayı güvenilmez bir protokol olarak bilinir. Her ne kadar güvenilmez olarak bilinsede faydasız değildir, sadece güvenlik konularını sorun etmez. UDP ayrıca sanal devre oluşturmadığı gibi verileri göndermeden önce hedefle bağlantıda kurmaz. Bunun için connectionless (bağlantısız) olarak nitelendirilir. Tablo 2.3' de UDP segmentinin basit yapısı görülmektedir.

Tablo 2.3: UDP segmenti

Bitler	0 – 15	16 – 31
0	Kaynak Port Numarası	Hedef Port Numarası
32	Uzunluk	Kontrol Sayısı (Checksum)
64	Veri	

Kaynak: http://blog.btrisk.com/2014/05/dos-turleri.html

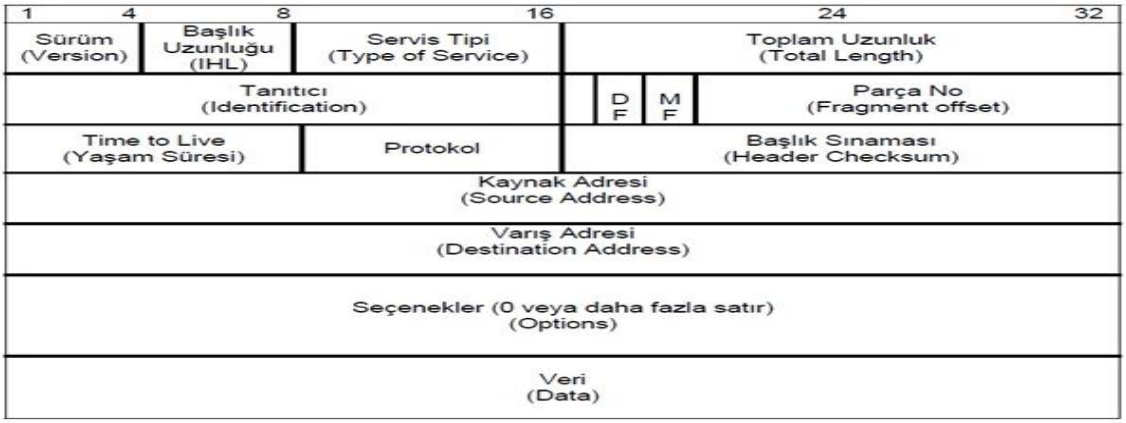
2.2.1.3 İnternet katmanı

Bu katmanın görevi üst katmandan gelen segmentleri alıcıya uygun yoldan ve hatasız olarak ulaştırmaktır. IP ve ICMP olmak üzere iki protokol bu katmanda çalışmaktadır.

Internet Protocol (IP) aslında yönlendirme katmanıdır diyebiliriz. Bu katmanda bulunan diğer protokoller, sadece ona destek vermektedir. IP her paketin adresine bakar, daha sonra bir routing tablosu kullanarak en iyi yolu bulup paketi gönderir.

İnternette bulunan bilgisayarların birbirleriyle iletişim sağlamak için kullandıkları benzersiz numaralara verilen adrese ise internet protokolü adresi denilmiştir. IP paket birimlerine ise datagram denir. Tablo 2.4' de IP başlığı eklenmiş bir datagram görülmektedir.

Tablo 2.4: IP datagram yapısı



Kaynak: http://mehmetsalihdeveci.net/2011/02/24/ip-protokolu-ve-ip-datagram-yapisi/

Ip, aktarım katmanı (host-to-host) katmanından segmentleri alır ve gerekirse onları paketlere (datagram) böler. Daha sonra hedef makinede tekrar paketleri segmentlere dönüştürür. Her pakete alıcının ve göndericinin IP adresi tanımlanır. Her yönlendirici (router) paketin hedef adresine bakarak yönlendirme (routing) kararlarını verir.

ICMP (Internet Control Message Protokol) genellikle kontrol amacı ile kullanılan bir protokoldür. Yönlendirme katmanında çalışır ve birçok farklı servis için IP tarafından kullanılır. Genel olarak sistemler arasındaki kontrol mesajlarında IP yerine kullanılmaktadır. Bir yönetim protokolüdür. İletişim sırasında meydana gelebilecek problemler hakkında bilgi verirler. ICMP paketleri kullanıcı makinelerine ağ problemleri hakkında bilgi sağladığı gibi, IP datagramlarından da enkapsüle edilirler. ICMP' nin bu özelliklerinde faydalanmak için internet üzerinde kontrol amaçlı birçok program yazılmıştır. Örneğin ping programları, ping paketleri göndererek ağ üzerindeki makinelerin erişimlerinin kontrol edilmesinde kullanılır.

ARP (Address Resolution Protocol), IP adresi yardımı ile kullanıcıların donanım adreslerini bulmamızı sağlar. ARP, IP adresi ile belirtilen makinenin donanım adresini isteyen bir broadcast (yayın) göndererek yerel ağı sorgular. Bu mesajın içerisinde belirtilen makinenin IP adresi vardır. Bunun karşılığında IP adresine ait makinenin fiziksel adresini ister. Bu istek ilgili makine tarafından cevap verilir. Tablo 2.5'de bir arp mesajının yapısı görülmektedir.

Tablo 2.5: Arp mesajı yapısı

0	8	16	24	31
Donanım Adres Tipi		Protokol Adres Tipi		
Donanım Adr. Uzunl.	Protokol Adr. Uzunl.	Operasyon		
Gönderen Donanım Adresi (ilk dört sekizli)				
Gönderen Donanım Adresi (son iki sekizli)		Gönderen Protokol Adresi (ilk iki sekizli)		
Gönderen Protokol Adresi (son iki sekizli)		Varış Donanım Adresi (ilk iki sekizli)		
Varış Donanım Adresi (son dört sekizli)				
Varış Protokol Adresi (tümü)				

Kaynak: http://mehmetsalihdeveci.net/2011/02/25/network-uzerinde-adres-cozumleme-protokolleri/

2.2.1.4 Fiziksel katman

Fiziksel ortamı belirtmektedir. İletişim ortamının özelliklerini, hızını ve kodlama şemasını belirler. Kısaca IP paketlerinin ihtiyacı olan fiziksel bağlantıların bulunduğu katmandır.

2.2.1.5 TCP/IP İle OSI arasındaki farklar

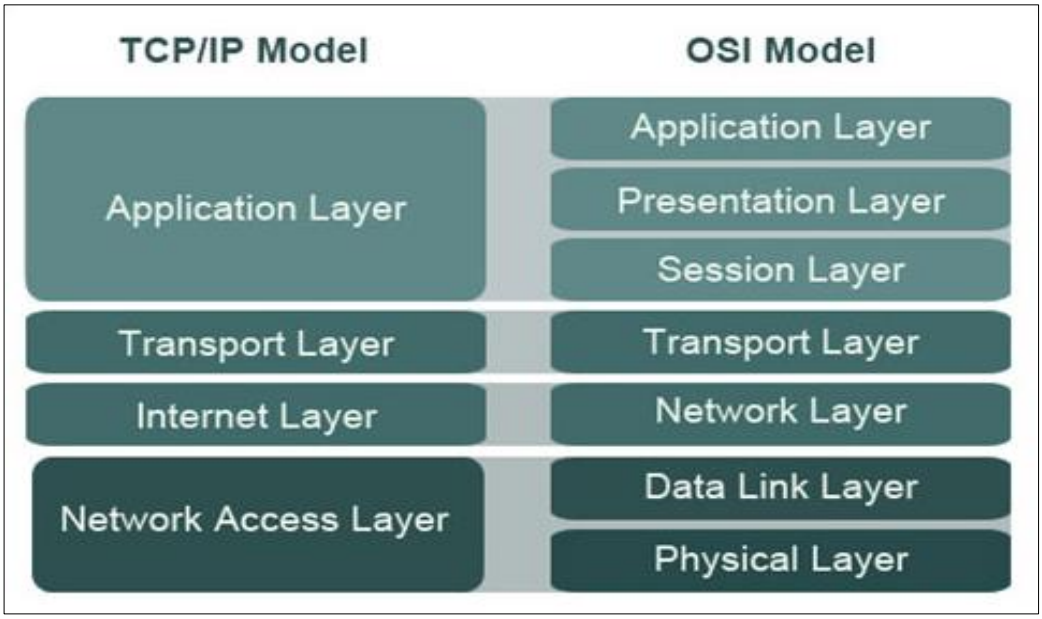
OSI referans modeli 1978 yılında ISO (International Organizations of Standarts) tarafından uzun çalışmalar sonucunda oluşturulmuştur. Farklı işletim sistemlerine sahip makinelerin birbirleri ile iletişimini sağlar. OSI içerisinde yer alan her katman bir üst katmana hizmet verecek şekilde oluşturulmuştur.

OSI referans modeli yedi katmandan oluşur. Altta yer alan iki katman yazılım ve donanım, üstte yer alan beş katman ise genel olarak yazılım ile çözülmüştür. En üst katmandan veriler indikçe, makine diline dönüşerek en son 1 ve 0' lardan oluşan elektrik sinyallerine dönüşürler. TCP/IP modelinde de OSI modelindeki gibi veriler bir sonraki katmana geçerek ilerler. TCP/IP modelinde katman içerinde bulunan protokoller birbirlerinden bağımsızdır. Her katman işini yapar ve verileri bir sonraki katmana iletir.

TCP/IP modeliyle OSI modelinin katmanlarını eşleştirirsek, uygulama katmanının OSI referans modelindeki karşılığı uygulama, sunum ve oturum katmanlarıdır. İletim

katmanı yine iletim katmanı, internet katmanı ise ağ katmanıdır. Fiziksel katmana karşılık ise veri link ve fiziksel katmandır. Şekil 2.8'de karşılıklı katmanlar görülmektedir.

Şekil 2.8: TCP/IP ile OSI katmanlarının karşılıkları



Kaynak: http://bilgisayar-muhendisleri.blogspot.com.tr/2013/07/osi-tcp-ip-karsilastirmasi.html

OSI ve TCP/IP modelleri arasındaki benzerliklerine gelirsek, her ikiside katmanlı bir yapıya sahiptir. Farklı içeriklerine rağmen her ikiside uygulama katmanına, benzer iletim ve ağ katmanlarına sahiptirler. Her ikiside devre anahtarlamalı teknolojiyi kullanır.

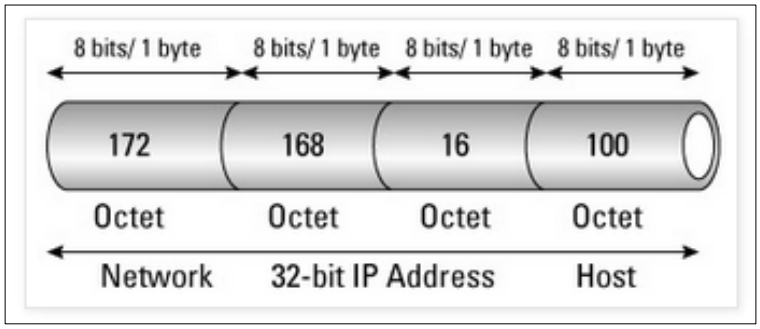
OSI ve TCP/IP modelleri arasındaki farklılıklar ise, OSI, TCP/IP' de bulunan sunum ve oturum katmanlarını uygulama katmanında birleştirmiştir. TCP/IP, OSI' nin data bağlantı ve fiziksel katmanlarını tek bir katmanda birleştirmiştir. TCP/IP daha az katmana sahip olduğundan daha anlaşılır ve kolay görülür. TCP/IP' de UDP kullanıldığı zaman iletim katmanında güvenilirlik kontrolü yapılmazken, OSI ' de bu işlem daima yapılır.

2.2.1.6 IP adresleme

Bilgisayarların birbirleri ile iletişim kurabilmesi için ağ üzerinde bulunan cihazın adresine, IP adresi denir. IPv4 (32 bit) ve IPv6 (128 bit) olmak üzere iki farklı IP adresi çeşidi bulunmaktadır. Günümüze yaygın olarak IPv4 kullanılır. İnternetin yaygınlaşması ve eldeki iplerin hızla bitmesi IPv6' ya doğru kaçınılmaz bir yönelişi de beraberinde getirecektir.

IPv4 32 bit, 4 oktet ve her bir oktetin içinde sekizerli gruplardan oluşur. IPv4 adresleri ikilik düzende yazılır fakat kolay okumak ve yazmak için onluk düzene çevrilir. Her IP adresinde 4 oktet vardır ve bu oktetler 0 ile 255 arasındaki sayılardan oluşur. Örneğin 192.168.2.1 bir IP adresidir. Her bir oktet nokta ile diğerinden ayrılır. Şekil 2.9 ' da IP adresi yapısı görülmektedir.

Şekil 2.9: IP adresi yapısı



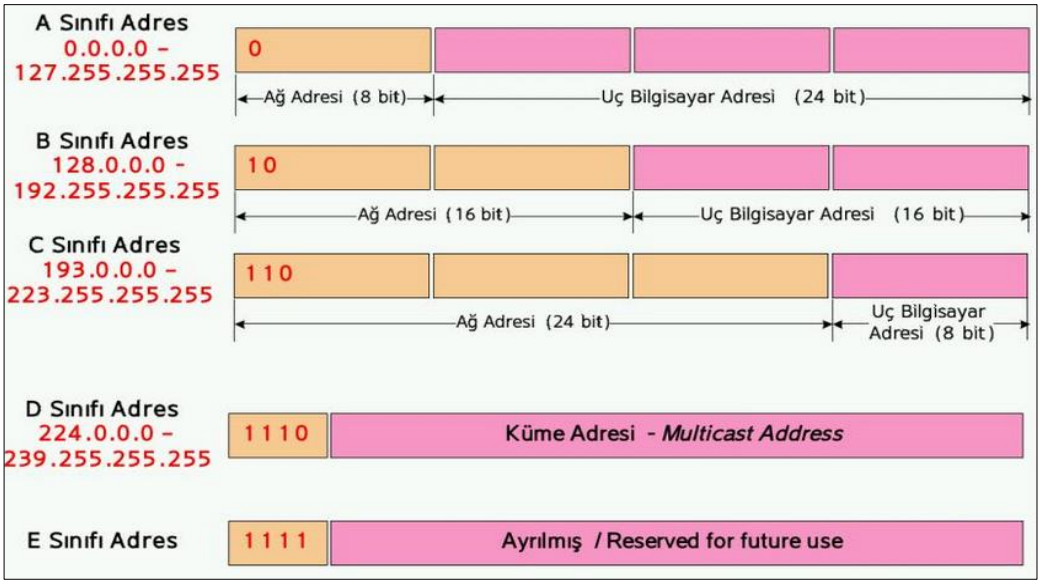
Kaynak: http://l34rn-p14y.blogspot.com.tr/2014_03_01_archive.html

IP adresleri Net ID (ağ numarası) ve Host ID (bilgisayar numarası) olmak üzere iki kısımdan oluşur. Ağ numarası (Net ID) bilgisayarın bulunduğu ağı belirtirken, bilgisayar numarası (Host ID) ağ içerisindeki bilgisayarları birbirinden ayrılmasını sağlar.

IPv4 internet ağının ana halkası olup günümüz interneti IPv4 üzerine kurulmuştur. İnternete bağlı birçok ağ vardır. Adres dağıtımını ve ağlara atanan adresleri kolaylaştırmak için IP adresleri sınıflara ayrılmıştır. A,B,C,D ve E sınıfları olmak üzere

5 temel sınıflama vardır. Bunlardan hangisinin gerektiğini bu adreslerin kullanılacağı ağın büyüklüğü belirler. Şekil 2.10' da IPv4 adres sınıfları görülmektedir.

Şekil 2.10: IPv4 adres sınıfları



Kaynak: http://www.slideshare.net/bedri20062611/p-adresi-kavramlar-ve-snflar

A sınıfı adresler 16 milyon kullanıcı barındırır. İlk okteti 1-126 arasında olan IPv4 adresleri A sınıf adresler olarak kabul edilir. İlk octet, network adresini, kalan 3 octet, host adresleri için kullanılmaktadır. Çok fazla kullanıcı içerdikleri dolayı büyük ağlar için tasarlanmıştır. İlk bit daima sıfırdır. İlk okteti 0 ve 127 ile başlayan ipler özel iplerdir. Bundan dolayı A sınıfı IPv4 adresi 126 adet ağ içerir.

B sınıfı adreslerin ilk octeti 128-191 arasındadır. B sınıfı adreslerde ağı tanımlamak için ilk 2 octet kullanılır. Son 2 octet ise host adresleri için kullanılmaktadır. İlk iki biti daima 10' dır. B sınıf IPv4 adresleri 65534 bilgisayar içeren 16382 alt ağa izin verir. Orta ve büyük ağlarda kullanılır. Birçok büyük üniversite ve İSS, B sınıfı adres alanına sahiptir.

C sınıfı adreslerin ilk octeti 192-223 arasındadır. C sınıfı IPv4 adreslerinde ağı tanımlamak için ilk 3 oktet kullanılır. Son 1 octet ise host adresleri için kullanılır. İlk 3 bit daima 110' dır.

224 ve 225 arası adresler D ve E sınıfı adresler için ayrılmıştır. D sınıfı adresler 224-239 multicast adresler için, E sınıfı 240-255 bilimsel amaçlarla kullanılmaktadır.
127.0.0.1 loopback testleri için ayrılmıştır. Ağ trafiğine neden olmaksızın hostun kendisine test paketi göndermesini sağlar. IP adresinin tamamının 0 olması, default route' u belirtmek için router' larda kullanılır. IP adresinin tamamının 1 olması, mevcut ağ üzerindeki bütün host' lara broadcast demektir.

Ağdaki her host gerçek route edilebilir IP adresine sahip değildir. Eğer olsaydı IP adresi dağıtımı yıllar önce tamamlanırdı. Bazı adresler özel amaçlarda kullanmak için ayrılmıştır. Bu adresler internete bağlı olmayan makinelerde, ya da proxy server veya NAT üzerinden internete çıkan iç network makinalarında kullanılır. NAT, özel bir IP adresini alır ve IP adresini internette kullanılması için çevirir. Böylece birçok kişi, aynı gerçek IP adresini, internet erişimi için kullanabilir. Bu sayede çok sayıda adres aralığı kazanılmış olur.

2.2.2 MPLS (Çok Protokollü Etiket Anahtarlama)

MPLS teknolojisi OSI (Open Systems Interconnection) 2. Katmandaki (veri bağlantı katmanı) veri iletimi ile 3. katmandaki (ağ katmanı) yönlendirme işlemlerinin hızlı ve güvenli bir şekilde sağlanmasıdır.

Internetin günden güne daha geniş bir alanda kullanım bulması, network teknolojilerinde önemli ölçüde gelişmeler meydana getirmiştir. Sürekli artan kullanıcı sayısı, İSS' larin altyapılarının gelişmesini, hızlanmasını, hizmet kalitesinin ve servis çeşitlerinin artmasını sağlamıştır.

Yönlendirme işlemi sırasında routerların routing tablosuna bakıp yönlendirme yapması hem routerların yükünü arttırıyor hem de işlemlerin süresini uzatıyordu. Bunun yanında birden çok protokolün birlikte çalışması sistemde gecikmelere ve sorunlara sebep oluyordu. Tüm bu problemlere çözüm getirmek için 1997 yılında IEFT (Internet Engineering Task Force) MPLS' i geliştirmeye başladı. Halen gelişme döneminde olan MPLS çok büyük IP ağlarının anahtarı olarak görülmektedir.

MPLS özetle, yönlendirme işlemini, ağın giriş yolunda, gereken çıkış yolunu belirleyerek bir kez yapmak ve ağın içinde hızlı bir şekilde anahtarlama yapmaktır. Bu yönlendirme işleminin hızlı yapılabilmesi için MPLS teknolojisinde etiketler kullanılmaktadır. Ağın giriş yolunda yapılan yönlendirme işlemi sırasında data paketlerine iliştirilen MPLS etiketleri ile, ağ içerisinde bu etiketlere göre hızlı bir şekilde anahtarlama yapılması yeterli olmaktadır.

MPLS Teknolojisi trafik mühendisliğinde (Traffic Engineering) kullanılır. Trafik mühendisliği, bir network üzerindeki yönlendiricilerin birbirleri ile olan veri iletişimini, birbirlerine olan uzaklıklarını, bir yönlendiriciden diğer yönlendiriciye en kısa yoldan ulaşılmasını ve yönlendirici haritasını çıkararak trafiği yönetmektir. MPLS teknolojisinin en büyük avantajı bir yönlendirici ile diğer yönlendirici arasındaki veri yolu tıkandığı zaman verinin en kısa mesafede bulunan başka bir yönlendiriciye yönlenmesi veya daha az tıkanabilecek başka bir yola yönlenmesidir. Böylelikle veri paketlerindeki kayıp azalır ve uzun süreli tıkanmalar yaşanmaz.

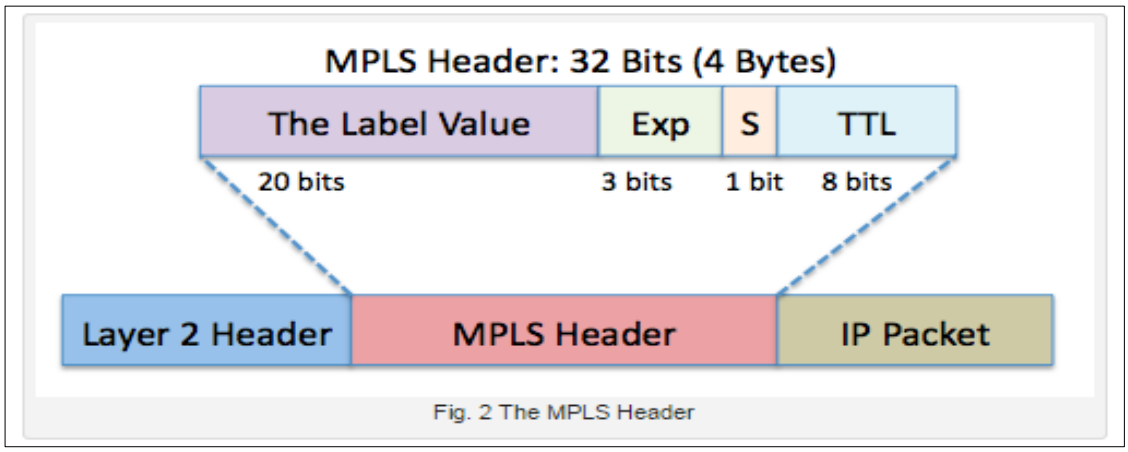
MPLS paketleri Frame Relay, Ethernet, PPP, ATM gibi 2. Katman teknolojileri üzerinden iletilebilir. MPLS, Frame-Relay tabanlı ise etiketler L2 ve L3 başlıkları arasına yerleştirilir. Bu etiketleme işlemlerine Shim Header (Pul Başlığı) adı verilir. MPLS hücre tabanlı ise ATM Frame' in VPI/VCI bölümündeki değerler etiket olarak kullanılır. Layer 2 anahtarlama teknolojileri ile Layer 3 yönlendirme teknolojilerini birleştirir. MPLS mimarisi esnektir ve tüm Layer 2 teknolojileri ile birlikte çalışabilir.

2.2.2.1 MPLS başlığı

MPLS protokolünde veri iletimi etiket anahtarlamalı yollar kullanılarak gerçekleştirilir. Başlık (label) 4 byte uzunluğunda bir tanımlayıcıdır. Etiket ile aktarma yaparken etiketler veya etiket yığınları, yaşam süresi (TTL) gibi farklı bilgiler kullanılır. Bunun yanında veri alış verişi için kullanılan farklı ortamlara göre farklı MPLS başlıkları da kullanılabilir. Örneğin ATM kullanılan bir yapıda MPLS başlığındaki bilgiler ATM başlığı içerisinde iletilir.

2. katman ve 3. Katman arasında yerleşen bu 4 bytelık etiketlerin içerisinde; 20 bit etiket, etiket değerini belirtir. 3 bit TC, başlangıçta deneysel amaçlarla kullanılması planlanmıştır fakat günümüzde Class of Service alanı olarak kullanılmaktadır. Şubat 2009 dan önce bu kısım EXP olarak bilinmekteydi. Fakat yayınlanan RFC 5462' de (Reguest For Comments) TC olarak belirtilmiştir. 1 bit S ise, Bottom of Stack (Protokol Yığını Sonu) biti olarak alınır. Burada kullanılan 1 değeri etiketin bittiğini, 0 değeri ise arkasından başka bir etiketin daha geldiğini belirtir. 8 bitlik değer ise time to live (yaşam süresi) değeridir. Örnek şekil 2.11' de bir MPLS başlığının yapısı gözükmektedir.

Şekil 2.11: MPLS başlığı



Kaynak: http://blog.ine.com/2010/02/21/the-mpls-forwarding-plane/

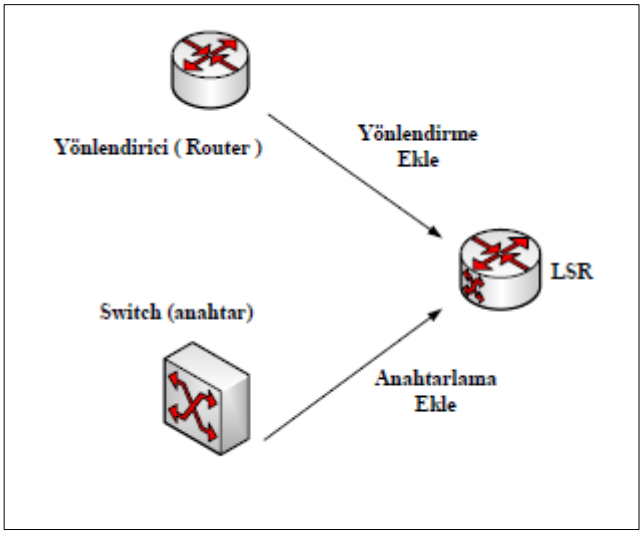
Etiket yığınlarında birkaç işlem yapılabilir. En üstteki etiket yeni bir etiketle değiştirebilir yada bir veya birden fazla etiket ekleyebilir, en üstteki etiketi yeni bir etiket ile değiştirebiliriz.

2.2.2.2 Etiket anahtarlamalı yönlendirici (LSR)

MPLS ağının merkezinde yer alan, LSP' lerin (Etiket Kenar Yönlendirici) kurulumu için kullanılan, kurulan yollar üzerinde veri trafiğinin yüksek hızda yapılmasını sağlayan, yönlendirici bir cihazdır. Anahtarlamayı MPLS etiketlerine göre yapar. LSR paketi aldığında göndereceği arayüzü (interface) belirledikten sonra etiketi çıkartır ve

yeni etiketi pakete ekler, sonunda paketi belirtilen arayüzden yollar. Şekil 2.12' de LSR' ın yapısı görülmektedir.

Şekil 2.12: LSR' ın oluşması

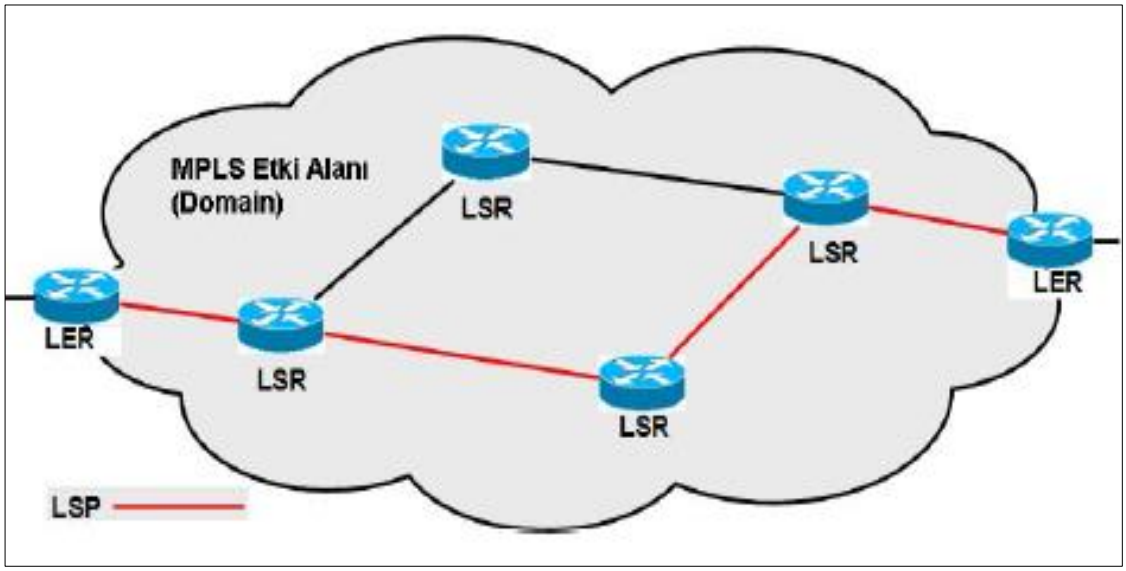


Kaynak: Bu şekil Tahir Aykutlu tarafından hazırlanmıştır.

2.2.2.3 Etiket kenar yönlendirici (LER)

MPLS ağının kenar noktalarında çalışan bir cihazdır. Paketler MPLS domainine girdiğinde, yönlendirmenin belirlenmesi ve paketlere etiket eklenmesi ilk bu düğümde gerçekleştirilir. Kısacası etiketlenmenin başladığı veya bittiği yönlendiricilerdir. Şekil 2.13' de MPLS topolojisinde LER cihazlarının konumu gözükmektedir.

Şekil 2.13: MPLS topolojisinde LER cihazlarının konumu



Kaynak: http://www.itbook.info/study/mpls3.html

2.2.2.4 İletim denkliği sınıfı (FEC)

MPLS yapısında aynı özelliklere sahip paketlerin oluşturduğu sınıfa İletim Denkliği Sınıfı (FEC) denir. Aynı rotadan yönlendirilen ve aynı şekilde işlem gören IP paketleri grubu olarak tanımlanır. Aynı rotadan giden paketler bir FEC sınıfı oluştururlar. MPLS de, belirli bir paketin, belirli bir FEC' e atanması, paket ağa girdiğinde bir kez gerçekleştirilir. FEC aynı zamanda paketlerin gruplanmasına ve bu grupların önceliklendirilmesine olanak verir. Böylece önemli olan paketlerin trafiğine yüksek öncelik, ikinci, üçüncü derece önem olan trafiklere düşük öncelik verilerek servis kalitesinde iyileştirme yapabilme olanağını sağlar.

2.2.2.5 Etiket dağıtım protokolü (LDP)

Etiket dağıtım protokolü (LDP) MPLS ağlarında etiketlerin LSR' lara dağıtılmasını sağlamak amacıyla kullanılır. Bir işaretleşme protokolüdür. Bu protokol sayesinde FEC' ler etiketler ile eşlenir ve LSP' ler oluşturulur. Etiket dağıtım protokolü çift taraflı çalışır. LDP peerlar karşılıklı olarak her oturumda birbirlerinin etiket eşleştirmesini

öğrenebilirler. LDP peer, etiket bilgilerini eşleştirmek için LDP kullanan iki etiket anahtarlamalı yönlendiriciye (LSR) verilen isimdir. Toplam 4 çeşit mesaj kullanılır.

Oturum (Session) Mesajı: LDP oturumlarının kurulması, sürdürülmesi ve sonlandırılması için kullanılır.
Keşif (Discovery) Mesajı: MPLS ağında bir LSR' ın varlığının duyurulmasını ve sürdürülmesini sağlamak için kullanılır.
Uyarı (Notification) Mesajı: Tavsiye bilgisinin ve hata mesajlarının iletilmesini sağlamak için kullanılır.
Duyuru (Advertisement) Mesajı: FEC' ler için etiket eşleştirmelerinin oluşturulması, değiştirilmesi ve silinmesi için kullanılır.

2.2.2.6 Etiket anahtarlanmış yol (LSP)

MPLS ağı içerisinde paket iletimi başlamadan önce paketlerin iletimini sağlamak için iki nokta arasına kurulmuş olan yollara Etiket Anahtarlanmış Yol (LSP) denir. MPLS' de veri iletimi LSP üzerinden yapılır. LSP üzerinde etiketler LDP veya RSVP (Resource Rezervation Protocol) gibi protokollerin yardımı ile yapılır.

Sekmeli Yönlendirme (Hop-by-hop routing) ve Mutlak Yönlendirme (Explicit) olarak LSP' ler iki şekilde kurulabilir.

Sekmeli Yönlendirme: Her LSR bir sonraki atlama noktasını verilen bir FEC için kendisi seçer. LSR bu durumda herhangi bir mevcut yönlendirme protokolü kullanabilir. Şuan IP ağlarında kullanılan yöntem budur.
Mutlak Yönlendirme: Ağa giriş LER' inden çıkış LER' ine kadar olan LSR' ların adresinin bulunduğu listeyi temsil eder. Bu listedeki adresler bir yol oluşturacak şekilde verilmiştir. Bu yol en uygun olmayan yol olabilir. Mutlak yönlendirme işlemi iki şekilde yapılır. Serbest ve sıkı yönlendirme. Sıkı yönlendirmede sadece LER tarafında önceden belirlenen LSR' lar kullanılır. Sıkı yönlendirmede LER tarafından verilen sıraya uyma zorunluluğu vardır. Serbest yönlendirmede ise gerekli görüldüğü takdirde LER tarafından belirlenen başka LSR' lar kullanılabilir.

2.2.2.7 Kontrol yapıtaşı

Gönderme tablosunun oluşturulması, bakım ve onarımının yapılması için kullanılır. Yönlendirme bilgilerinin düzenli ve sağlıklı olarak dağıtılmasında diğer yönlendiricilerin kontrol yapıtaşları ile birlikte çalışır. Bu yapı taşları ayrıca gönderme tablolarının yaratılmasında kullanılan işlemlerin güven altına alınmasını sağlar. Standart yönlendirme protokolleri olan, RIP (Routing Information Protocol), BGP (Border Gateway Protocol) ve OSPF (Open Short Path First), yönlendiricilerin kontrol mekanizmaları arasında yönlendirme bilgilerinin değişimini sağlar.

2.2.2.8 Gönderme Yapıtaşı

Direkt olarak paketlerin gönderilmesinde kullanılır. Yönlendiriciler tarafından bakım ve onarımı yapılan gönderme tablosundaki bilgileri kullanırlar. Standart yönlendiricilerde çalışan bir algoritma gönderme tablosunda bulunan paketteki gidilecek adresleri karşılaştırarak en uygun yolu buluncaya kadar çalışmasını sürdürür. Bu işlemler paket hedefe varıncaya kadar her seferinde tekrarlanır. LSR ise, etiket değiş tokuş algoritmasını kullanarak paketlerdeki etiketler ve etiket temelli gönderme tabloları yardımı ile paketler için yeni etiketler ve çıkış arayüzleri bulunmasını sağlar.

2.2.2.9 Gönderme tabloları

Gönderme yapıtaşlarına anahtarlama fonksiyonunu yerine getirmesi sırasında gerekli desteği sağlayan bilgi topluluğudur. Gönderme tablosu, gelen paketlerin gideceği adresleri belirler.

2.2.2.10 Paketlerin iletimi ve etiket dağıtımı

MPLS ağında yönlendiriciler, paketleri iletmek için paket başlıklarını inceler ve en uygun algoritmayı kullanarak paketlerin en iyi şekilde yönlendirilmesini sağlar. Etiket değiştirerek aktarma daha basit olan etiket eşleştirilmesine dayanmaktadır. Bu paketlerin çok daha hızlı ve kolay şekilde iletilmesini sağlar. Yönlendirme protokolü,

paketleri iletmek için kullanacağı bilgileri OSPF, BGP gibi yönlendirme protokollerinden sağlar. Bu yönlendirme bilgileri tüm aktarımı parçalara böler. Bu parçalara FEC adı verilir. Her FEC için bir etiket değeri atanır.

Veri iletim yolunun başındaki router'a **ingress** router denir. Veri iletim yolunun sonunda bulunan router'a ise **Egress** router denir. Ingress ve egress arasındaki belirlenen veri yolu üzerinde eğer başka bir router varsa bu router' lar transit router olarak adlandırılır.

Yönlendirme protokolleri vasıtası ile elde edilen bilgiler, etiketleri MPLS içinde atamak ve dağıtmak için kullanılır. MPLS düğümü, bir sonraki düğüm olan yönlendiriciden giden etiket atamalarını alır. Kendisi ise gelen paketlere etiket değeri tahsis eder ve bunları kendinden önce gelen düğümlere dağıtır. Birbirini sırayla takip eden etiketlerin oluşturduğu bu yola etiket anahtarlamalı yol (LSP) denir.

Bir paket LSP yoluna girdiğinde ıngress router tarafından pakete MPLS header (başlık) eklenir. LSP yolu boyunca iletilir ve egress router'da başlık atılır. LSP içinde ilerleyen paketlerin IP paket başlıklarına değil, hangi interface' den giriş yaptığına ve etiketine bakılır. Paket en son egress router' a geldiğinde ise paketin IP başlığına bakılır ve yönlendiricinin seçtiği yoldan gönderilir. LSP yolunda paketler ilerlerken etiket değiştirir. Yani router gelen paketin etiketine bakarak nereye gideceğini ve hangi yeni etiketi ekleyeceğini belirler. Eski etiketi yeni etiket ile değiştirerek gönderir.

Noktadan noktaya aktarım için etiket dağıtımı etiket dağıtım protokolü (LDP) ile yapılır. MPLS içinde LDP' nin dağıtımı için bir LDP komşuluğu oluşturulur. LDP protokolünde etiket dağıtımı düzenli ve bağımsız olarak ikiye ayrılır. Düzenli etiket dağıtım protokolünde, belirli bir akış için çıkış olan düğüm tarafından bu akışa ait etiket dağıtımı başlatılır. Yani bir düğümün kendi giriş etiketini diğerlerine dağıtmaya başlayabilmesi için ya bu düğümün ilgili akışın çıkış düğümü olması gerekir yada bu akışa ait bir çıkış etiketine sahip olması gerekir. Düzenli etiket dağıtım protokolü, etiket-akış eşleştirilmelerinin daha sağlıklı bir şekilde yapılmasını sağlar, etiketlenmemiş paketlerin ise sonraki düğümlere iletilmemesi ihtimalini arttırır.

Bağımsız etiket dağıtımı protokolünde ise her düğüm, herhangi bir akış algıladığı zaman, herhangi bir anda bu akışa atadığı etiketi dağıtabilmektedir.

MPLS içinde etiketleme akışın yönünde bir sonraki aşağı akış (downstream) düğüm tarafından yapılmaktadır. Etiket tahsisinde iki yöntem vardır. Bunlar; aşağı-akış (downstream) ve istek üzerine aşağı akış (dowstream on demand). Aşağı akış (downstream) etiket tahsisinde, akış yönünde bir sonraki düğüm tarafından etiket tahsisi yapılır ve bu etiket değerleri komşu düğümlere ve komşu LSR' a dağıtılır. İstek üzerine aşağı akış yönteminde ise akış yönünün yukarısındaki bir düğüm (LSR) tarafından akış yönünün aşağısındaki bir düğümden o akışa ait etiket atamasının

2.2.2.11 Etiket verme kriterleri

MPLS teknolojisinde kullanılmasındaki en belirgin etkenlerden bir tanesi de bir ya da daha fazla akışa etiket anahtarlamalı yol (LSP) atanabilmesidir. Bu akış daha az bir trafik gerektirebilir, ya da çok yoğun bir veri iletimi de gerektirebilir. Etiket paylaşımı, kaynakların daha etkin kullanımını sağlayarak anahtarlamanın faydalarından en yüksek oranda yararlanma istediği ile ortaya çıkmıştır. Etiket verme kriterleri çok çeşitli olabilir.

IP önekine (prefix) göre: Bu kriterde etiketler varış adresinin önekine (prefix) göre verilir. Bu uygulamanın iyi tarafı etiket atamalarının sadece bir kez ya düğüm eşleşmesi aşamasında (peering phase) ya da bir adres öğrenildiği zaman yapılmasıdır. Bu yöntem sayesinde LDP mesajlaşmaları minimum seviyeye inmektedir. Ancak bu etiket verme tarzı, düşük etiket uzayına sahip etiket anahtarlama yönlendiricilerinden (LSR) oluşmuş büyük ağlar da ölçeklenebilirlik (scalability) problemleri doğurabilir.

Çıkış (egress) yönlendiricisine göre: MPLS ağını aynı yönlendiriciden terk eden akışların ortak bir etiketi, ortak bir etiket anahtarlamalı yolu (LSP) paylaşması anlamına gelmektedir. Hangi LSR' ın, BGP açısından hangi akışlar için çıkış yönlendiricisi olduğu bilgisi, sonraki düğüm tarafından gönderilen BGP güncelleme mesajından veya OSPF yayımının içindeki yönlendirici numarasından (OSPF Router ID) anlaşılabilir.

Uygulama akışına (Application flow) göre: Bu kriterde uygulama akışı kendi yolunu belirler. Bu yöntem diğer yöntemler arasında en az ölçeklenebilirliğe sahip olan kriterdir. Bu kriterin en önemli avantajı ise uçtan uca anahtarlamayı (end to end switching) sağlamasıdır.

Etiket anahtarlama klasik yönlendirmeden çok daha etken bir dağıtım sistemidir. Aşağıdaki tabloda klasik ve etiket anahtarlama yönlendirme sistemlerinin karşılaştırması görülmektedir.

Tablo 2.6: Klasik ve etiket anahtarlamalı yönlendirme karşılaştırması

	Klasik Yönlendirme	Etiket Anahtarlama
Tam IP Başlık Analizi	Her düğümde kullanılır	Sadece etiket atama aşamasında ağın en ucunda kenar LSR`de uygulanır.
Tekli ve Çoklu Dağıtım	Çoklu karmaşık dağıtım algoritmasına gereksinim vardır	Sadece bir tane gönderme algoritmasına gereksinim vardır
Yönlendirme Kararları	Sadece adres üzerine dayalıdır	QoS veya VPN üyeliği gibi herhangi bir parametrenin numarası kullanılabilir

Kaynak: Bu tablo Tahir Aykutlu tarafından hazırlanmıştır.

2.2.2.12 Trafik mühendisliği

Trafik mühendisliği (traffic engineering) teriminin tanımı , ağ üzerindeki belirli bağlantılarda, yönlendiricilerde ve anahtarlardaki trafik yığılmalarını azaltmak ve buralardaki aşırı yükü diğer ağ elemanlarına dağıtmak için veri akışının geçtiği yolların yeniden seçilmesi işlemidir.

Trafik mühendisliği birden fazla alternatif yolun bulunduğu ağlarda çok önemlidir. İnternette yaşanan hızlı büyüme, bantgenişliği isteklerinin de hızla büyümesine ve bazı çekirdek ağların çok aşırı "dallanması" (branchy) sonuçlarını doğurmuştur. Tüm bu gelişmeler trafik mühendisliğinin önemini daha çok arttırmıştır.

Diğer teknolojilere göre MPLS, herhangi bir giriş yönlendiricisinden ağa giren ve herhangi bir çıkış yönlendiricisinden ağdan çıkan bir akışı tek olarak tanımlayabilmektedir. Bu durum MPLS' de giriş ve çıkış yönlendiricileri arasında akan trafiğin kontrol edilmesinde ve ölçülmesinde çok kullanışlı yöntemler sunmaktadır. Ayrıca MPLS' in kaynaktan yönlendirme ya da açık yönlendirme sağlayabilme özelliği ile trafik akışının istenilen yoldan gitmesi sağlanabilir.

MPLS' de trafik mühendisliğinin en zor yanlarından biri, her LSP' nin (etiket anahtarlamalı yolun) yönlendirmesinin nasıl olacağı sorusudur. Bu soru için iki çözüm vardır. Bu çözümlerden birincisi, bu kararlar elle ayarlayarak verilebilir. İkinci yöntem olarak, arka planda sürekli çalışarak yolların maliyetlerini ve yoldaki trafik yoğunluğunu hesap edip alternatif yollar bulmaya çalışan yönlendirme protokolleri kullanılabilir.

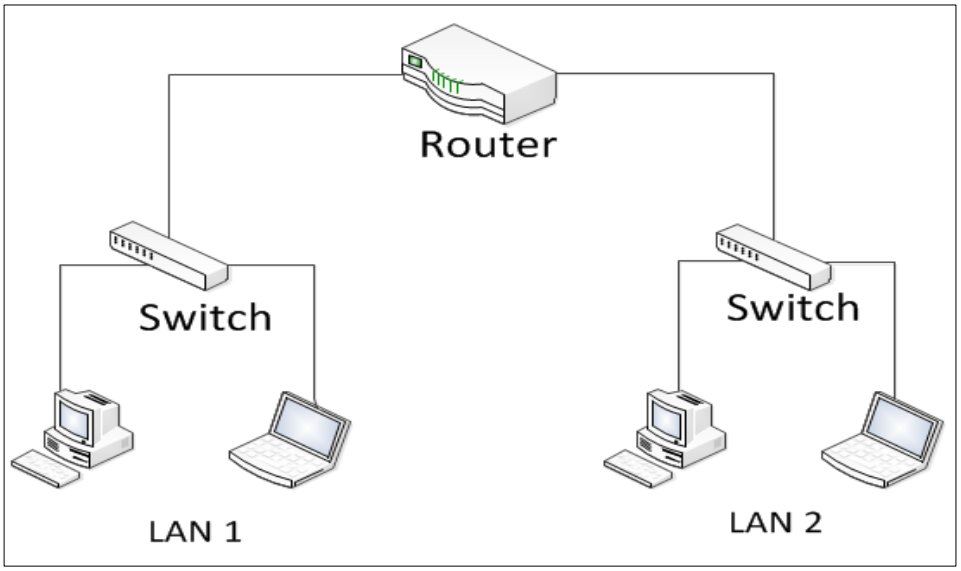
2.3 KULLANILAN YÖNLENDİRME CİHAZLARI

İnternet servis sağlayıcıların ağlarında bulunan ve kullanıcıların internete erişimlerini sağlayan cihazlardır. Bu cihazlar paket yönlendirmesi yaparak belirli yol ve yöntemler yardımıyla kullanıcıların erişimlerini sağlarlar.

2.3.1 Router

Router (yönlendirici), yönlendirme katmanında çalışan cihazdır. Paket yönlendirme yeteneğinden dolayı yönlendirici olarak adlandırılır. Şekil 2.14' de görüldüğü gibi yönlendiriciler farklı katman cihazlarını birbirine bağladığı gibi farklı ağları da birbirlerine bağlarlar.

Şekil 2.14: Farklı ağların birbirine bağlanması



Kaynak: Bu şekil Tahir Aykutlu tarafından hazırlanmıştır.

Çok sayıda network segmentinin bulunduğu farklı protokollerin ve mimarilerin olduğu bir ağda tam olarak bulunması gereken cihazdır. Büyük network ağlarında trafiğin düzenlenmesini sağlayan en önemli ağ elemanıdır. Router' ın amacı gelen paketleri inceleyerek yönlendirme yapmaktır. Paketlerin iletimi için en iyi yolu belirler. Basit bir yönlendirici gibi tanımlamak yanlış olabilir. İşletim sistemine sahiptirler. Gerekli konfigürasyonlar yardımı ile birden fazla farklı yol içinde en iyi yolu seçerek yönlendirme yapabilirler.

Routerlar, IP protokolünü kullanan internetin bel kemiğini oluşturur. İnternet' in pek çok irili ufaklı ağdan oluşan büyük bir ağ olduğunu düşünürsek bu ağ içerisinde çok sayıda router bulunmaktadır. İnternette kullanılan cihazların yüzde 85' i cisco firmasının ürettiği cihazlardır.

2.3.2 Gateway GPRS Support Node (GGSN)

Günümüzde mobil aboneler e-posta erişimlerini, internet, mobil tv, video servislerine erişimlerini ve diğer tüm internet erişim hizmetlerini mobil geniş bant bağlantısı üzerinden almaktadır. Operatörler bu talepleri karşılayabilmek için yüksek kapasitede veri trafiği işleyebilecek, yüksek güvenilirliği ve basit kullanılabilirliği olan şebeke elemanlarına ihtiyaç duymaktadır.

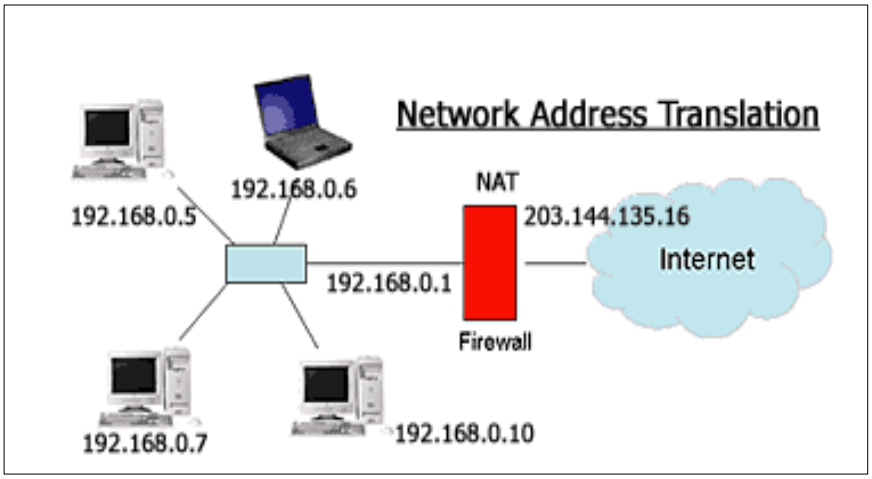
GGSN (Ağ geçidi GPRS destek düğümü), operatörlerin paket çekirdek şebekesi ile internet gibi IP tabanlı şebekeler arasında veya paket tabanlı şebekeler arasında bir ağ geçidi olarak davranır. Mobil paket çekirdek şebekesinin ortasında yer alan GGSN, abonelere servis politikası ve kalitesi uygulamalarını, şebeke koruma ve güvenlik duvarı, ön ödemeli aboneler içinse anında ücretlendirme, faturalı aboneler için faturalandırma sistemleri ile etkileşme işlerinin tümünü yürütür.

2.3.3 Network Address Translation (NAT)

İnternet üzerinde kullanılan IP adreslerini internet servis sağlayıcı firmalar ICANN adlı firmadan satın alırlar. İnternetin dünya üzerinde hızla yayılması ve giderek kullanıcı sayısında yaşanan büyüme IP adreslerinin yetmemesi gibi problem doğurmaktadır. 1990' lı yıllarda bu durumun farkına varılması ile IPv6 üzerindeki çalışmalar başlamıştır. IPv6 ile trilyonlara varan IP adresimiz olacak. IPv6' ya geçme işlemi biraz uzun süreceğinden dolayı çeşitli teknolojiler yardımı ile IP yetersizliği problemini gidermekteyiz.

IP adreslerinin yetersiz kalması nedeniyle iç ve dış networklerde IP ayrımına gidilmiştir. IP' ler Global (internet IP) ve public (iç ağ IP) olarak adlandırılmıştır. Şekil 2.15' de görüldüğü gibi NAT public IP adreslerini global IP adreslerine çeviren teknolojidir.

Şekil 2.15: NAT çalışma topolojisi



Kaynak: http://it-guides.com/training-a-tutorial/network-system/what-is-nat

Bu sayede çok sayıda iç kullanıcı az sayıdaki global IP adresi yardımı ile internete bağlanabilmektedir. Bunu şu şekilde örneklemek gerekirse; şirketimizin 10000 abonesi olduğunu varsayalım. Her birini internete çıkarmak için 10000 IP adresine ihtiyacımız olacaktı ve IP adresleri yetersiz kalacaktı. NAT yardımı ile bu problemin önüne geçilmektedir.

2.3.4 Deep Packet Inspection (DPI)

DPI (trafik yönetimi ve analizi), genel paket analizinden daha derin incelemedir. Uygulama katmanı paketlerindeki tüm uygulamaları ve içeriği analiz eder. DPI sistemi, IP ağının içine konuşlanarak servis tespiti, servis kontrolü ve servis istatislikleri gerçekleştirebilir.

DPI' ın kullanım alanları oldukça geniştir. Güvenlik amaçlı DPI, spamla mücadelede, DDoS saldırılarında, virüs ve diğer tüm tehditler konusunda güvenlik uygulamlarına yardımcı olur. Port engelleme yapar.

DPI, trafik izleme amaçlı olarak, operatörlere ağlarında neler olduğu, hangi uygulamanın ne kadar bant genilşiği kullandığı konularında yardımcı olur. Ayrıca makro ya da uygulama düzeyinde trafiği kısıtlamak, bloke etmek ve düzenleme işlerini yapar.

DPI ayrıca, paketlerin nereden gelip nereye gittiği gibi bilgilere dayanarak paket düzeyinde etiketleme ve önceliklendirme yapar. Farklı uygulamalar için uygulama, hizmet ve müşteri bazında hizmet kalite güvencesi için kullanılır. Uygulama tabanlı fiyatlandırma yapar. Müşterilere, oyuna özgü ağ trafiği sunabilir.

Paket başlığına veri ekleyerek, veri akışlarının nasıl davranacağı ya da bazı durumlarda ne tür veri akışları gönderileceği gibi kararlar verilmesi için gerekli olabilir. Operatörler bunu kullanarak cep telefonu, tablet veya bilgisayar gibi alıcı cihazın yeteneklerine bağlı olarak içeriği değiştirmek isteyebilirler.

Ebeveyn kontrol çözümleri sunar. İçerik filtrelemeye daha fazla imkan sağlar. Ağ tabanlı uzantı sayesinde istenmeyen URL' ler ya da web sayfaları ebeveyn kontrolü olduğuna bakılmaksızın DPI sayesinde engellenebilir.

2.4 SERVİS KALİTESİ

Günümüzde çok sayıda ağ trafiği türü bulunmaktadır. Her trafik türünün kendine has çalışma özellikleri mevcuttur. İnternette yaşanan inanılmaz büyüme ile günümüzde çoğu ağ trafiği IP temelli bir yapıya kavuşmuştur.

Servis kalitesi farklı teknikler ve yöntemler kullanılarak bir ağda trafik akışının istikrarlı bir şekilde sağlanmasıdır. Servis kalitesi kavramı farklı uygulamalar için farklı anlamlar içerebilmektedir. Örneğin ses iletiminde yüksek bant genişliğine gereksinim yokken, görüntü iletimi için yüksek bant genişliğine ihtiyaç duyulmaktadır. Ses ve video iletiminde uçtan uca gecikmeler ve paket kayıpları büyük önem taşımaktadır. Buna karşılık herhangi bir veri transferi yapıldığında veya bir e-mail alınması aşamasında network üzerinde yaşanabilecek gecikmeler bu tür uygulamalar için tolere edilebilir.

Servis kalitesi bir kullanıcının yada uygulamanın ağdan aldığı genel servis sürecini ve deneyimini tanımlamak için kullanılan geniş kapsamlı bir ifadedir. Kullanıcıların problemsiz bir şekilde ağ üzerinden işlem yapmaları için yaşanan süreç olarak da ifade edilebilir.

Servis kalitesinin firmalar için ön plana çıkması, bu servisleri izleme ve takip etme zorunluluğunu da getirmiştir. Firmalar, kullanıcılara sundukları hizmetleri anlık olarak takip etmeli, yaşanan problemleri müşteriden önce fark edip müdahale etmelidir. Müşteri problem bildirimi yaptığından servis veren firmanın problem hakkında bilgisinin olması ve kullanıcıya bilgilendirme yapabilmesi önemli bir noktadır. Rekabetin yoğun olarak yaşandığı İSS sektöründe problemlerin anında fark edilip, aksiyon alınarak çözüme kavuşturulması, kullanıcı tarafında daha az iletişim problemi yaşanmasına sebep olacaktır.

2.4.1 İnternette Servis Kalitesi

İnternet, yönlendirici ağ cihazlarından ve bu yapıların birbirine bağlantısından oluşmaktadır. Bu büyük yapıda iletişim yapılırken çeşitli nedenlerden dolayı problemler yaşanabilmektedir. Bazı uygulamalar yaşanan bu problemler karşısında diğerlerinden daha fazla etkilenmektedir. Özellikle gerçek zamanlı sesler iletim gecikmelerine ve paket kayıplarına oldukça duyarlıdır. Gecikme ya da kayıp yaşanan veri iletimi, iletişimin mümkün olmasını engelleyebilir. Örneğin internet üzerinden radyo dinlenmesi yada internet üzerinden video izlenmesi sırasında yaşanan paket kayıpları yada gecikmeler, uygulama üzerinde farkedilebilir problemler yaratmaktadır.

Standart internet protokolü üzerine kurulmuş ağlar verileri hedefe belli bir süre ulaştırmak için çaba sarf eder. Bunu başaramazlarsa veri paketi ya bekletilir ya da tamamen ağdan atılır. Belli bir ağ bağlantısı üzerinden iletilen trafik, bağlantının bant genişliğinden fazla ise bu hatta tıkanıklık oluşmasına sebep olmaktadır. Bu iletim şekline “best effort” denilmektedir.

“Best effort” veri dağıtım şekli bugünün internet trafiğinin çoğu için kabul edilebilir. Fakat web tabanlı uygulamaların kullanımındaki artış, video konferans gibi gerçek zamanlı uygulama gereksinimlerinin artması, veri iletimi işinin sorunsuz bir şekilde sürdürülebilmesi için çok daha karmaşık protokollere ihtiyacı arttırmaktadır.

2.4.2 Servis Kalitesinde Yaşanan Problemler

Ağ problemleri tespit edip çözmek uzun zaman sürebilir ve beklenenden uzun uğraşlar gerektirebilir. Bunun başlıca nedenlerinden biri ağlarda fazlaca değişken olmasıdır. Birbirinden farklı cihazlarla, farklı yol ve yöntemler ile ağa bağlanan, ağdan yararlanan kullanıcılar çözümü daha da karmaşık hale getirmektedir. Kullanılan uygulamaların çeşitliliği ve çok sayıda kullanıcının farklı istekleri de bu karmaşıklığa sebebiyet veren nedenlerdendir. Günümüzde çok sayıda uygulama ve bu uygulamaların kendine özgü çalışma özellikleri bulunmaktadır.

Bazı uygulamalar, iki yada daha çok sayıda kullanıcının birbiriyle etkileşimi ile olmaktadır. Bu uygulamalar gerçek-zamanlı cevap alma ihtiyacı barındırırlar. Bundan dolayı alıcı ile gönderen arasında gecikmenin minimum olması gerekmektedir. Örnek olarak telefon görüşmeleri gerçek-zamanlı uygulamalardandır. Telefon görüşmesi, video konferans gibi uygulamalarda paket kaybı en aza indirgenmiş olmalıdır. Bu özellik sağlanmaz ise telefonda konuşurken sık sık ses kesilmeleri yaşanabilir. Bu tür uygulamalar UDP temelli olduklarından, TCP temelli uygulamalardaki gibi eksik paketler yeniden iletilmezler. Bir başka önemli noktada bu tür uygulamalar zamana duyarlı olduğundan paketlerin tekrar gönderilmesi fayda sağlamaz. İletişim devam ettiğinden, konuşma sırasında kaybolan ses paketinin tekrar gönderiminin de bir anlamı olmayacaktır.

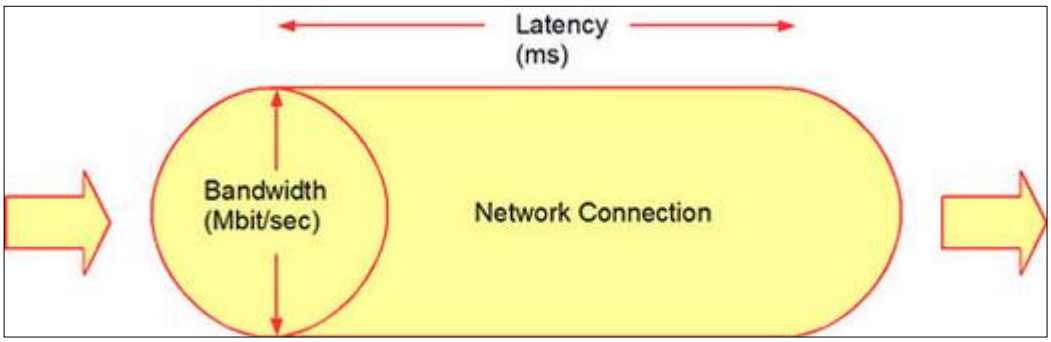
Bir diğer uygulama çeşidi ise uygulama ile ağ cihazları arasında bulunmaktadır. Kullanıcının beklentisi bu uygulamaların duyarlı olması, gönderilen talebin hızlı bir şekilde cevaplanmasıdır. Paket gecikme sürelerinin ve kayıpların düşük olması gerekmektedir. Gerçek-zamanlı uygulamalarda olduğu gibi katı bir servis kalitesi gereksinimi yoktur. İnternet radyo ve video uygulamaları örnek olarak gösterilebilir.

Bazı uygulamalar da bilginin iletimi esneklik gösterebilir. E-posta uygulamaları veya dosya iletimleri buna örnek gösterilebilir. Bir e-mailin gönderimi belirli önceliklere göre kabul edilebilir zaman içerisinde sağlanabilir. Bu kabul edilebilir zaman kesinlikle işin önemi ve önceliği ile alakalı olarak değişmektedir. Dosya gönderiminde de aynı mantık kullanılır. Bir dosya transfer edilmeye başlandığında, gecikme çoğu kez fark edilmez. Bu tür uygulamalar TCP kullandığından yaşanan paket kayıplarının yeniden iletimi, iletişimi mümkün kılar.

2.4.2.1 Bant genişliği (Bandwidth)

Bant genişliği, servis kalitesi etkileyen en önemli parametrelerden biridir. İnternetin en büyük sorunlarından biri olarak değerlendirilir. Hat boyunca iletilebilecek maximum veri miktarı olarak tanımlanır. Şekil 2.16' da görüldüğü gibi bits/second, bps: bit-per-second olarak ölçülür.

Şekil 2.16: Bant genişliği

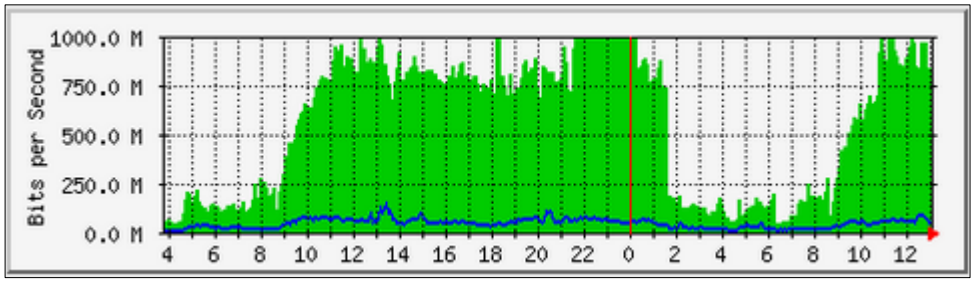


Kaynak: http://www.ibm.com/developerworks/websphere/library

Çoğu İSS firması mevcut bant genişliğinden daha fazlasını müşterilerine tanımlar. Bunun sonucunda müşterilere tanımlanan bant genişliğinin her zaman kullanıma hazır olamaması sorunu ortaya çıkar. Servis alan kullanıcılar, ağ üzerindeki diğer müşterilerin kullanımına göre az yada daha çok bant genişliği kullanırlar. Ağ üzerindeki trafiğin az olduğu zamanlarda kullanıcılar daha yüksek bant genişliği ve daha sorunsuz bağlantı sağlayabilir. Fakat bu devamlılığı olan bir durum değildir. Veri trafiği arttıkça hat üzerindeki bant genişliği ihtiyacı artar.

Özellikle Şekil 2.17' de görüldüğü gibi kullanıcıların yoğun olarak ağ üzerinden işlem yaptıkları zamanlarda oluşan büyük veri trafiği, eğer hattın bant genişliğinden fazla olursa, iletişim problemlerine yol açar.

Şekil 2.17: Bant genişliğinin grafiği



Kaynak: Bu şekil Tahir Aykutlu tarafından hazırlanmıştır.

Servis sağlayıcıları ücret karşılığından isteyen kullanıcıları için SLA içinde garanti edilmiş bant genişliği sağlamaktadır. Belirli bir bant genişliği garanti edildiğinden bu hizmetin ücreti mevcut bant genişliği hizmetinden daha yüksektir. Abonelerin aynı ağ üzerinden bulundukları durumda ISP, garanti edilmiş bant genişliği hizmeti alan kullanıcılara trafik içinde öncelik vererek garanti edilmiş bant genişliğini sağlamaktadır.

2.4.2.2 Gecikmeler (Delay)

Bir paket bir kaynaktan yola çıkarak çok sayıda yönlendiriciden geçer ve hedefine ulaşır. Paketler kaynak hostlarından hedef adreslerine giderken geçtikleri her node üzerinde gecikmeler yaşanır. Gecikme bir uygulamanın kaynak ve hedef arasındaki veri iletimi boyunca hareket ettiği zaman dilimi olarak ifade edilir.

Bazı uygulamalar bu gecikmelere karşı daha az hassas olmasına rağmen ses ve görüntü iletimlerinde önemli servis kalitesi sorunlarına neden olmaktadır. Delay (gecikme) ağ üzerinde bir kaç şekilde karşımıza çıkmaktadır.

2.4.2.2.1 Gecikme türleri

End to end delay, uçtan uca gecikmelerin toplamı olarak değerlendirilir. Hop by hop delay ise, her bir hop noktası üzerindeki proses ve kuyruklama gecikmeleri olarak değerlendirilir.

İşlem gecikmesi (processing delay), network cihazının paketi alıp, başlık bilgisine bakarak çıkış portuna yönlendirmesine kadar geçen süreye denir. İşlem gecikmesine neden olan faktörler ise donanım üzerinde bulunan fiziksel kapasitelerdir. Fiziksel kapasitelerden kasıt, işlemci hızı, işlemci kullanımı, router mimarisi ve konfigürasyonlardır.

Serialization delay (serileşme gecikmesi), başlık eklenmiş bir paketin iki port arasındaki iletimi boyunca geçen süreye denir.

Kuyruklama gecikmesi (queuing delay), paketin çıkış kuyruğuna oturması süresinde yaşanan gecikme değeridir. Paketlerin router üzerinde bekleme süreside denilebilir. Routerlar paketleri alırlar ve eğer bant genişliği uygunsa hemen gönderirler. Fakat paketler geldikten sonra önünde bekleyen paketler var ise sonradan gelen paketler kuyrukta beklerler.

Yayılım gecikmesi (propagation delay), paketin link üzerinden uç noktaya kadarki iletişiminde ortam türüne bağlı olarak ortaya çıkan gecikme türüdür.

Gecikme türlerine baktığımızda işlem gecikmesi ve kuyruklama gecikmesi router veya L3 özellikli switchlere ve bu cihazların üstünde bulunan işletim sistemlerine bağlı olduğu görülmektedir. Serileşme gecikmesi ve yayılım gecikmesi ise tamamen ortama bağlı oluşmaktadır.

2.4.2.3 Gecikme Değişikliği (Jitter)

Gecikme değişiklikleri (jitter), paketlerin gecikme sürelerindeki farklılıklardır. Aynı türdeki paketlerin kaynak ile hedef arasındaki iletimi esnasında geçen sürelerdeki farklılığı ifade eder. Gecikme farklılığı ses ve video gibi gerçek zamanlı ve gecikmeye duyarlı uygulamalarda önemli etkiler yaratabilmektedir. Bu tür uygulamalar paketleri sabit bir hızla ve sabit sürelerle almak isterler. Eğer paketlerin iletim hızları ve süreleri değişkenlik gösterirse uygulamanın performansı etkilenir.

Örnek vermek gerekirse, birinci paket geldikten sonra ikinci paket 5 sn'ye sonra geldi, üçüncü pakette ikinci paketten 5 sn'ye sonra gelmelidir. Veri paketleri jitterden bağımsızdır. Çünkü alıcı bütün veri paketlerini alıp sıraya koymadan mesajı okuyamaz.

Servis kalitesinde göze çarpan en önemli faktörlerden ikisi paket gecikmesi ve jitterdir. Paket gecikmesi, bir paketin network üzerindeki ortalama iletim hızını tanımlar. Jitter ise bir paketin hedefe varış zamanındaki farklılıkları tanımlar. Gecikme ortalama olarak kullanılır, jitter ise standart sapmadır. Her ikiside servis kalitesi açısından önemlidir.

2.4.2.4 Kayıplar (Packet losses)

Ağ üzerindeki ortaya çıkan tıkanıklıkları veya veri iletimi sırasında bazı paketlerin hedefe ulaşmamasını ifade eder. Daha çok uydu, mobil, kablosuz ağlar üzerinde görülürler. Kayıplar (Packet Losses) çevresel faktörler, yanlış yönlendirme, iletim esnasında paketlerin zarar görmesi vb. yollarla meydana gelebilir. BER (Bit Error Rate – Bit Hata Oranı) ölçümlerine göre karasal hatlarda kayıp oranı oldukça azdır.

Routerlarda ise kayıplar tail drop adı verilen paketlerin kuyruklara girmemesinden dolayı oluşur. Routerın çıkış kuyruğundan yer kalmaması durumunda gelen bütün paketler kayba uğrayacaktır. Kuyruğun dolması dışında başka tür nedenlerden dolayı da paket kayıpları oluşabilir. Örneğin işlemcimiz paketleri işleyecek durumda olmadığı zamanda paket kayıpları gözlenir.

İşlemcinin paket işleyecek durumda olmamasının nedeni ise paket giriş kuyruğunun dolu olmasıdır. Cihazlar üzerindeki buffer kapasitesinin yetersiz olması da paketlerin işleme alınmasını engeller ve paket kayıplarına neden olur.

Ağ üzerinde kaybolan paketler eğer güvenilir protokol ile gönderimi yapılıyorsa (TCP) yeniden yollanarak sorun giderilmeye çalışılabilir. Fakat UDP kullanan paketlerin telafisi olmayacaktır. Paket kayıplarında kaybolan paketlerin yanı sıra, kayıp paketlerin ne kadar ardışık olarak kaybolduğu da önemlidir. Bir ağ üzerinde kayıp ses paketleri, servis kalitesinde büyük sorunlara yol açabilir. Konuşma süresince kelimelerin anlaşılamamasına ve ses kesilmelerine yol açabilir. Genel olarak gerçek zamanlı ağlarda kabul edilebilir kayıp paket oranları yüzde 0,01 ile yüzde 0,03 arasındadır.

2.4.2.5 Cihaz Kaynaklı Problemler

Paketler internete erişirken farklı ağ cihazları üzerinden geçerler. Bu cihazlar üzerinde yaşanabilecek herhangi bir sorun doğrudan servis kalitesini etki eder. Bu sebeple cihazların sürekliliğini takip etmek, yaşanan problemlere anında müdahale etmek servis sağlayıcılar için büyük önem taşımaktadır. Çok sayıda farklı cihazın olduğu geniş networklerde bu denetimi yapmak oldukça zordur. Hangi cihazın ne tür problemlere yol açabileceğini bilmek gerekir.

Router sistemin ortasında yer alan cihaz olarak diğer network elemanları ilede haberleşme imkanı sağlar. Router üzerinde problem yaşanması ve cihazın devre dışı kalması, yönlendirmede sorunlara yol açarak, abonelerin erişimlerinde problemlere sebep olmaktadır.

GGSN' de yaşanan problemler mobil abonelerde sorunlara yol açabilir. Bir diğer sorun ise bu cihaz üzerinde yaşanabilecek problemlerde aboneler ücretlendirilemeyebilir. GGSN' de yaşanan sıkıntılar hem hizmet kalitesinde problemlere hem de ücretlendirmede sorunlar yaşanmasına sebep olur.

DNS üzerinde yaşanan problemlerde ise abonelerin isim ile ulaşmak istedikleri web sayfası, kaynak, dosya sunucusu, mail sunucusu adreslerin IP karşılıkları çözümlenemeyeceğinden erişim problemleri oluşur.

NAT' da yaşanan bir problemde cihaz isteklere yanıt veremeyeceğinden, global IP kullanımlarında sorunlar yaşanacaktır. Abonelerin çoğu internete erişemeyeceğinden istatistikler düşecek, bant genişliği yeterli olsa dahi kullanım düşük kalacaktır.

Tüm bu paket yolunda bulunan cihazların izlenmesi, sorunların hangi noktada yaşandığının çabucak belirlenmesi ve müdahalede bulunulması için çeşitli yöntemlere başvurulmaktadır. Her servis sağlayıcı bu sorunları bir şekilde çözmeye çalışmaktadır.

3. PAKET YÖNLENDİRME İLE MOBİL İSS AĞININ İZLENMESİ

3.1 PAKET YÖNLENDİRME VE AMACI

Paket yönlendirme, protokoller yardımı ile ya da statik olarak, paketlerin ağ üzerindeki kaynaktan çıkıp hedef adrese ulaşması sırasında hangi yolu izleyeceğine karar verilmesine denir.

Bu tez çalışmasında HTTP isteği, DNS ve ICMP-ECHO sorguları yardımıyla, paketlere farklı rotalar verilerek herhangi bir erişim problemi anında, sorunun fark edilip, kaynağının bulunması amaçlanmıştır. Hedefler girilirken Cisco IOS IP SLA özelliğini kullanılmıştır. Bu özellik networkte bulunan cihazları izleme ve servis kalitesini ölçme işlemlerinde kullanılmaktadır.

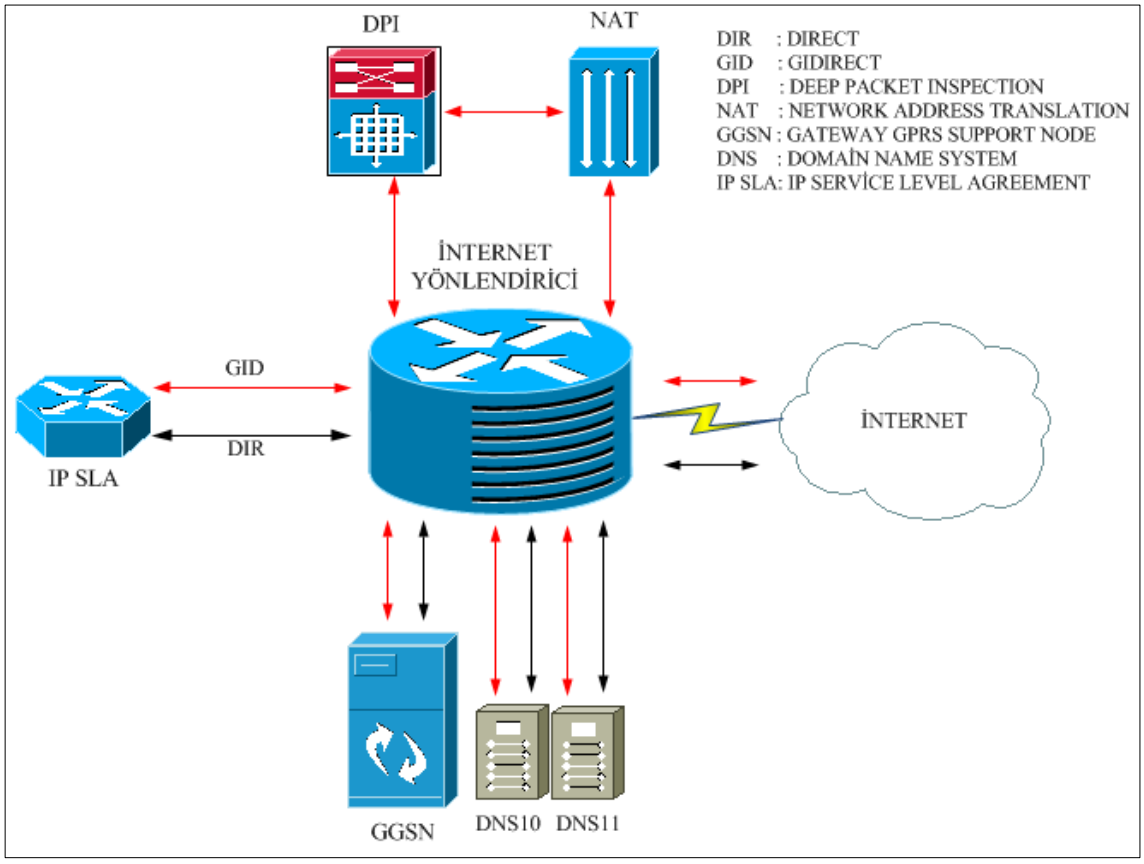
Bu çalışmada, izlenen hedef adreslere erişim olmaması durumunda IP SLA' in router üzerine log düşürmesinden faydalanılmış, düşen bu log EEM (Embedded Event Manager) yardımı ile eposta atılarak alarmın bildiriminin yapılması sağlanmıştır. Bu sayede hem cihazlar, hem cihazlar üzerinden servisler, hem de internet üzerindeki adresler izlenmiş, yaşanacak problemlere anında yorumlar getirilmeye çalışılmıştır.

Mobil abonelerin internete erişirken kullandığı rota üzerinde denetim yaparken "GID" kodu kullanılarak diğer rota üzerindeki paketlerden ayrıştırılması sağlanmıştır. Bu sayede anlaşılacaktır ki "GID" kodu ile başlayan alarmlar üretildiğinde problemi aramaya mobil taraftan başlanılmalıdır.

Kontrol amaçlı üretilen paketlere "DIR" kodu verilmiştir. Bu paketler yardımıyla mobil taraftan gelen alarmların sağlaması yapılmaktadır.

Şekil 3.1’ de çalışmanın uygulanacağı topoloji görülmektedir. Topolojide kırmızı yön işaretleri mobil abonelerin ağ üzerindeki hareketlerini göstermektedir. Siyah yön işaretleri ise kontrol amaçlı üretilen, direkt olarak internete ve ağdaki hedeflere gönderilen paketleri ifade etmektedir.

Şekil 3.1: Paket yönlendirme ile Mobil İSS ağının izlenmesi

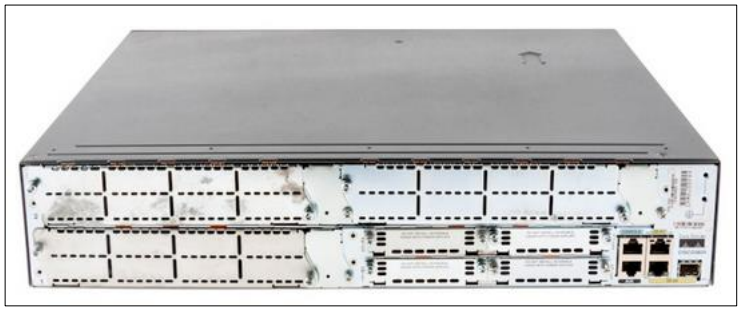


Kaynak: Bu şekil Tahir Aykutlu tarafından hazırlanmıştır.

3.2 GEREKSİNİkMLER VE KURULUM

Sistem kurulumu için Şekil 3.2’ de görüldüğü üzere Cisco 3845 model bir yönlendirici kullanılmıştır.

Şekil 3.2:Cisco 3845



Kaynak: www.cisco.com

Donanım olarak 1 Gigabit Ethernet Interface kullanılmış, IP SLA desteği vermesinden dolayı IOS olarak "flash:c3845-advipservicesk9-mz.124-22.YB8.bin" kurulumu yapılmıştır. IOS adı üzerinde “C3845” olarak ifade edilen kısım yönlendiricinin modelini, “advipservicesk9” kısmı IOS’ un ne gibi özelliklere sahip olduğunu, “mz” kısmı sıkıştırma türünü, “124-22” kısmı ise versiyonunu göstermektedir.

Aşağıda yönlendiricinin versiyon çıktısı görülmektedir.

```
Cisco IOS Software, 3800 Software (C3845-ADVIPSERVICESK9-M), Version 12.4(22)YB8, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Sat 23-Oct-10 02:33 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T11, RELEASE SOFTWARE (fc1)

R1 uptime is 6 day, 22 hours, 0 minutes System returned to ROM by reload at 10:21:22 TURKIYE Wed Mar 25 2015

System image file is "flash:c3845-advipservicesk9-mz.124-22.YB8.bin"

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

Cisco 3845 (revision 1.0) with 222208K/39936K bytes of memory.
Processor board ID FCZ13207245
1 Gigabit Ethernet interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity enabled.
479K bytes of NVRAM.
62720K bytes of ATA System CompactFlash (Read/Write)

Configuration register is 0x2102
```

Internet yönlendiricisi ile IP SLA yönlendiricisi fiziksel olarak RJ45 kablo ile birbirine bağlanmıştır. IP SLA yönlendiricisinin Gi0/0 portuna takılan fiziksel kablonun karşı ucu internet yönlendiricisinin Gi0/1/0/5 portuna takılmıştır. IP SLA yönlendiricisi üzerinde 2 adet sub-interface yaratılmıştır.

```
Interface    Status      Protocol  Description
Gi0/0         up            up
Gi0/0.11      up            up            DIR
Gi0/0.12      up            up            GID
```

IP SLA yönlendiricisi üzerinde "DIR" paketleri için kullanılacak sub-interface, GigabitEthernet0/0.11 olarak yaratılmıştır. Konfigürasyon çıktısı aşağıdaki gibidir.

```
interface GigabitEthernet0/0.11
 encapsulation dot1Q 11
 ip address 217.31.227.41 255.255.255.252
```

IP SLA yönlendiricisi üzerinde "GID" paketleri için kullanılacak sub-interface, GigabitEthernet0/0.12 olarak yaratılmıştır. Konfigürasyon çıktısı aşağıdaki gibidir.

```
interface GigabitEthernet0/0.12
 encapsulation dot1Q 12
 ip vrf forwarding HTTP
 ip address 10.148.255.253 255.255.255.252
```

IP SLA yönlendiricisi üzerinde yaratılan 2 adet sub-interface karşılığında internet yönlendiricisi üzerinde de 2 adet sub-interface yaratılmıştır.

```
Interface    Status      Protocol  Description
Gi0/1/0/5.11   up          up         DIR
Gi0/1/0/5.12   up          up         GID
```

İnternet yönlendiricisi üzerinde "DIR" paketleri için kullanılacak sub-interface, Gi0/1/0/5.11 olarak yaratılmıştır. Konfigürasyon çıktısı aşağıdaki gibidir.

```
interface GigabitEthernet0/1/0/5.11
vrf INTERNET
 ipv4 address 217.31.227.42 255.255.255.252
 encapsulation dot1q 11
```

İnternet yönlendiricisi üzerinde "GID" paketleri için kullanılacak sub-interface, Gi0/1/0/5.12 olarak yaratılmıştır. Konfigürasyon çıktısı aşağıdaki gibidir.

```
interface GigabitEthernet0/1/0/5.12
 vrf GID
 ipv4 address 10.148.255.254 255.255.255.252
 encapsulation dot1q 12
```

IP SLA yönlendiricisinin üzerinde "DIR"paketleri için global routing tablosuna statik route yazılmıştır.

```
217.31.227.0/30 is subnetted, 1 subnets
C 217.31.227.40 is directly connected,GigabitEthernet0/0.11
```

“GID” paketleri için IP SLA yönlendiricisinin üzerine “HTTP” VRF’i tanımlanmıştır. “HTTP” VRF için girilen konfigürasyon aşağıdaki gibidir.

```
ip vrf HTTP
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 media-type rj45
interface GigabitEthernet0/0.12
 encapsulation dot1Q 12
 ip vrf forwarding HTTP
 ip address 10.138.248.41 255.255.255.252
 ntp disable
ip route vrf HTTP 0.0.0.0 0.0.0.0 10.138.255.254 name
GID_ROUTE_FOR_HTTP
end
```

3.2.1 HTTP İsteklerinin Oluşturulması

Girilecek konfigürasyonlarla "DIR" ve "GID" paketleri kullanılarak HTTP istekleri yapılmıştır. HTTP isteği yapılırken www.twitter.com, www.facebook.com, www.youtube.com, www.hurriyet.com.tr ve www.sahibinden.com gibi mobil internet kullanıcıları tarafından internet üzerinde en fazla ziyaret edilen adreslerden yararlanılmıştır. Bu adreslerin belirlenmesinde DPI üzerindeki abone hareketlerinden faydanılmıştır.

Logların anlamlı bir şekilde bildirimi için etiketler (tag) oluşturulmuştur. Bu etiketler oluşturulurken sırasıyla yer bilgisi, route bilgisi, protokol bilgisi, adres bilgisi, IP SLA numara bilgisi ve istek yapılan DNS bilgisi göz önüne alınmıştır.

Logların üretilmesi için "xOfy" ve "threshold" değerleri girilmiştir. HTTP istekleri için oluşturulan konfigürasyonlardaki değerlerin tümü "xOfy 1 2" ve "threshold 900" olarak girilmiştir. Threshold 900 olarak girilen değer, istek yapılan adrese paketlerin en fazla 900 ms içinde gidip gelme süresini ifade etmektedir. Bu süre aşıldığında oluşturduğumuz "xOfy" değerine göre alarm üretmeye başlayacaktır. "xOfy 1 2" ise son iki paketten 1 tanesine 900 ms de cevap alınmaz ise "timeout" alarmı, timeout alarmından sonra gelen 2 paketten 2 taneside başarılı bir şekilde iletilirse "clear" alarmı üret anlamına gelmektedir.

Adresler için girilen konfigürasyonlardaki tek fark IP SLA numaralarıdır. Bu sebeple girilen 5 farklı adres içerisinden www.twitter.com adresine ait konfigürasyonlar örnek olarak gösterilmiştir.

Mobil tarafa yönlendirilen “GID” paketleri için girilen konfigürasyonlarda 2’ si lokalde bulunan biri Google’ a ait olmak üzere 3 farklı DNS’ den HTTP isteği yapılmıştır.

```
ip sla 420
 http get http://www.twitter.com name-server 212.55.157.201
 vrf HTTP
 threshold 900
 tag ADN:GID:WWW:TWITTER:420:NS09:
 ip sla reaction-configuration 420 react timeout threshold-
type xOfy 1 2 action-type trapAndTrigger
 ip sla schedule 420 life forever start-time now
```

```
ip sla 421
 http get http://www.twitter.com name-server 212.55.157.202
 vrf HTTP
 threshold 900
 tag ADN:GID:WWW:TWITTER:421:NS10:
 ip sla reaction-configuration 421 react timeout threshold-
type xOfy 1 2 action-type trapAndTrigger
 ip sla schedule 421 life forever start-time now
```

```
ip sla 205
 http get http://www.twitter.com name-server 8.8.8.8
 vrf HTTP
 threshold 900
 tag ADN:GID:WWW:TWITTER:GOOGLE_DNS:8.8.8.8:
 ip sla reaction-configuration 205 react timeout threshold-
type xOfy 1 2 action-type trapAndTrigger
 ip sla schedule 205 life forever start-time now
```

Girilen konfigürasyonlar sonrasında mobil tarafta yaşanacak bir erişim problemi anında gelecek “timeout” mesajları aşağıda görüldüğü gibi olacaktır.

```
ADN:GID:WWW:TWITTER:420:NS09: State: Timeout
ADN:GID:WWW:TWITTER:421:NS10: State: Timeout
ADN:GID:WWW:TWITTER:GOOGLE_DNS:8.8.8.8: State: Timeout
ADN:GID:WWW:FACEBOOK:400:NS09: State: Timeout
ADN:GID:WWW:FACEBOOK:401:NS10: State: Timeout
ADN:GID:WWW:FACEBOOK:GOOGLE_DNS:8.8.8.8: State: Timeout
ADN:GID:WWW:YOUTUBE:410:NS09: State: Timeout
ADN:GID:WWW:YOUTUBE:411:NS10: State: Timeout
ADN:GID:WWW:YOUTUBE:GOOGLE_DNS:8.8.8.8: State: Timeout
ADN:GID:WWW:HURRIYET:NS09: State: Timeout
ADN:GID:WWW:HURRIYET:NS10: State: Timeout
ADN:GID:WWW:HURRIYET: GOOGLE_DNS:8.8.8.8: State: Timeout
ADN:GID:WWW:SAHIBINDEN:NS09: State: Timeout
ADN:GID:WWW:SAHIBINDEN:NS10: State: Timeout
ADN:GID:WWW:SAHIBINDEN: GOOGLE_DNS:8.8.8.8: State: Timeout
```

Mobil taraftaki erişim probleminin düzelmesi ile birlikte gelecek olan “clear” mesajları aşağıda görüldüğü gibi olacaktır.

```
ADN:GID:WWW:TWITTER:420:NS09: State: Clear
ADN:GID:WWW:TWITTER:421:NS10: State: Clear
ADN:GID:WWW:TWITTER:GOOGLE_DNS:8.8.8.8: State: Clear
ADN:GID:WWW:FACEBOOK:400:NS09: State: Clear
ADN:GID:WWW:FACEBOOK:401:NS10: State: Clear
ADN:GID:WWW:FACEBOOK:GOOGLE_DNS:8.8.8.8: State: Clear
ADN:GID:WWW:YOUTUBE:410:NS09: State: Clear
ADN:GID:WWW:YOUTUBE:411:NS10: State: Clear
ADN:GID:WWW:YOUTUBE:GOOGLE_DNS:8.8.8.8: State: Clear
ADN:GID:WWW:HURRIYET:NS09: State: Clear
ADN:GID:WWW:HURRIYET:NS10: State: Clear
ADN:GID:WWW:HURRIYET: GOOGLE_DNS:8.8.8.8: State: Clear
ADN:GID:WWW:SAHIBINDEN:NS09: State: Clear
ADN:GID:WWW:SAHIBINDEN:NS10: State: Clear
ADN:GID:WWW:SAHIBINDEN: GOOGLE_DNS:8.8.8.8: State: Clear
```

Direkt internete yönlendirilen ve kontrol amaçlı üretilen "DIR" paketleri için girilen konfigürasyonlar ile 2' si lokalde bulunan biri Google' a ait olmak üzere 3 farklı DNS' den HTTP isteği yapılmıştır.

```
ip sla 520
 http get http://www.twitter.com name-server 212.55.157.201
 threshold 900
 tag ADN:DIR:WWW:TWITTER:520:NS09:
 ip sla reaction-configuration 520 react timeout threshold-
type xOfy 1 2 action-type trapAndTrigger
ip sla schedule 520 life forever start-time now
```

```
ip sla 521
 http get http://www.twitter.com name-server212.55.157.202
 threshold 900
 tag ADN:DIR:WWW:TWITTER:521:NS10:
 ip sla reaction-configuration 521 react timeout threshold-
type xOfy 1 2 action-type trapAndTrigger
ip sla schedule 521 life forever start-time now
```

```
ip sla 305
 http get http://www.twitter.com name-server 8.8.4.4
 threshold 900
 tag ADN:DIR:WWW:TWITTER:GOOGLE_DNS:8.8.4.4:
 ip sla reaction-configuration 305 react timeout threshold-
type xOfy 1 2 action-type trapAndTrigger
ip sla schedule 305 life forever start-time now
```

İnternet yönlendiricisi üzerinde, yada çıkış devrelerinde yaşanacak bir erişim problemi sırasında gelecek "timeout" mesajları aşağıda görüldüğü gibi olacaktır.

```
ADN:GID:WWW:TWITTER:420:NS09: State: Timeout
ADN:GID:WWW:TWITTER:421:NS10: State: Timeout
ADN:GID:WWW:TWITTER:GOOGLE_DNS:8.8.8.8: State: Timeout
ADN:GID:WWW:FACEBOOK:400:NS09: State: Timeout
ADN:GID:WWW:FACEBOOK:401:NS10: State: Timeout
ADN:GID:WWW:FACEBOOK:GOOGLE_DNS:8.8.8.8: State: Timeout
ADN:GID:WWW:YOUTUBE:410:NS09: State: Timeout
ADN:GID:WWW:YOUTUBE:411:NS10: State: Timeout
ADN:GID:WWW:YOUTUBE:GOOGLE_DNS:8.8.8.8: State: Timeout
ADN:GID:WWW:HURRIYET:431:NS09: State: Timeout
ADN:GID:WWW:HURRIYET:432:NS10: State: Timeout
ADN:GID:WWW:HURRIYET: GOOGLE_DNS:8.8.8.8: State: Timeout
ADN:GID:WWW:SAHIBINDEN:441:NS09: State: Timeout
ADN:GID:WWW:SAHIBINDEN:442:NS10: State: Timeout
ADN:GID:WWW:SAHIBINDEN:GOOGLE_DNS:8.8.8.8: State: Timeout
ADN:DIR:WWW:TWITTER:520:NS09: State: Timeout
ADN:DIR:WWW:TWITTER:521:NS10: State: Timeout
ADN:DIR:WWW:TWITTER:GOOGLE_DNS:8.8.4.4: State: Timeout
ADN:DIR:WWW:YOUTUBE:510:NS09: State: Timeout
ADN:DIR:WWW:YOUTUBE:511:NS10: State: Timeout
ADN:DIR:WWW:YOUTUBE:GOOGLE_DNS:8.8.4.4: State: Timeout
ADN:DIR:WWW:FACEBOOK:500:NS09: Timeout
ADN:DIR:WWW:FACEBOOK:501:NS10: Timeout
ADN:DIR:WWW:FACEBOOK:GOOGLE_DNS:8.8.4.4: State: Timeout
ADN:DIR:WWW:HURRIYET:431:NS09: State: Timeout
ADN:DIR:WWW:HURRIYET:432:NS10: State: Timeout
ADN:DIR:WWW:HURRIYET: GOOGLE_DNS:8.8.8.8: State: Timeout
ADN:DIR:WWW:SAHIBINDEN:441:NS09: State: Timeout
ADN:DIR:WWW:SAHIBINDEN:442:NS10: State: Timeout
ADN:DIR:WWW:SAHIBINDEN:GOOGLE_DNS:8.8.8.8: State: Timeout
```

İnternet yönlendiricisi üzerinde, yada çıkış devrelerinde yaşanan erişim probleminin düzelmesi ile birlikte gelecek olan "clear" alarmları aşağıda görüldüğü gibi olacaktır.

```
ADN:GID:WWW:TWITTER:420:NS09: State: Clear
ADN:GID:WWW:TWITTER:421:NS10: State: Clear
ADN:GID:WWW:TWITTER:GOOGLE_DNS:8.8.8.8: State: Clear
ADN:GID:WWW:FACEBOOK:400:NS09: State: Clear
ADN:GID:WWW:FACEBOOK:401:NS10: State: Clear
ADN:GID:WWW:FACEBOOK:GOOGLE_DNS:8.8.8.8: State: Clear
ADN:GID:WWW:YOUTUBE:410:NS09: State: Clear
ADN:GID:WWW:YOUTUBE:411:NS10: State: Clear
ADN:GID:WWW:YOUTUBE:GOOGLE_DNS:8.8.8.8: State: Clear
ADN:GID:WWW:HURRIYET:431:NS09: State: Clear
ADN:GID:WWW:HURRIYET:432:NS10: State: Clear
ADN:GID:WWW:HURRIYET: GOOGLE_DNS:8.8.8.8: State: Clear
ADN:GID:WWW:SAHIBINDEN:441:NS09: State: Clear
ADN:GID:WWW:SAHIBINDEN:442:NS10: State: Clear
ADN:GID:WWW:SAHIBINDEN:GOOGLE_DNS:8.8.8.8: State: Clear
ADN:DIR:WWW:TWITTER:520:NS09: State: Clear
ADN:DIR:WWW:TWITTER:521:NS10: State: Clear
ADN:DIR:WWW:TWITTER:GOOGLE_DNS:8.8.4.4: State: Clear
ADN:DIR:WWW:YOUTUBE:510:NS09: State: Clear
ADN:DIR:WWW:YOUTUBE:511:NS10: State: Clear
ADN:DIR:WWW:YOUTUBE:GOOGLE_DNS:8.8.4.4: State: Clear
ADN:DIR:WWW:FACEBOOK:500:NS09: Clear
ADN:DIR:WWW:FACEBOOK:501:NS10: Clear
ADN:DIR:WWW:FACEBOOK:GOOGLE_DNS:8.8.4.4: State: Clear
ADN:DIR:WWW:HURRIYET:431:NS09: State: Clear
ADN:DIR:WWW:HURRIYET:432:NS10: State: Clear
ADN:DIR:WWW:HURRIYET: GOOGLE_DNS:8.8.8.8: State: Clear
ADN:DIR:WWW:SAHIBINDEN:441:NS09: State: Clear
ADN:DIR:WWW:SAHIBINDEN:442:NS10: State: Clear
ADN:DIR:WWW:SAHIBINDEN:GOOGLE_DNS:8.8.8.8: State: Clear
```

“DIR” ve “GID” paketleri kullanılarak yapılan HTTP istekleri uygulamasında www.twitter.com, www.facebook.com, www.youtube.com, www.hurriyet.com.tr ve www.sahibinden.com adresleri kullanılmıştır. Adresler, 3 adet yurtdışı ve 2 adet yurtiçi olacak şekilde belirlenmiştir. Yapılan ayrımın sebebi yurtdışı çıkışlarınıda bu çalışma sayesinde gözlemlemektir.

İSS’ nın yurtdışı çıkış devrelerinde yaşanacak problemler sırasında yurtdışı adreslere yapılan “GID” ve “DIR” HTTP istekleri başarısız olacaktır. Bu başarısızlık sonucunda aşağıda görüldüğü üzere “timeot” alarmları üretilecektir. Bu alarmlar neticesinde yurtdışı çıkışlarında bir problem yaşandığı farkedilecektir. Bu farkındalık sayesinde İSS’ nın yurtdışına çıkışlarında kullandığı devreler kendisine ait ise kendi tarafında, eğer vendor bir firmadan kiralık bir devre kullanılıyor ise ilgili firma tarafında problem çözümünü vakit kaybetmeden arayabilecektir.

```
ADN:DIR:WWW:TWITTER:520:NS09: State: Timeout
ADN:DIR:WWW:TWITTER:521:NS10: State: Timeout
ADN:DIR:WWW:TWITTER:GOOGLE_DNS:8.8.4.4: State: Timeout
ADN:GID:WWW:TWITTER:420:NS09: State: Timeout
ADN:GID:WWW:TWITTER:420:NS10: State: Timeout
ADN:GID:WWW:TWITTER:GOOGLE_DNS:8.8.8.8: State: Timeout
ADN:DIR:WWW:YOUTUBE:510:NS09: State: Timeout
ADN:DIR:WWW:YOUTUBE:511:NS10: State: Timeout
ADN:DIR:WWW:YOUTUBE:GOOGLE_DNS:8.8.4.4: State: Timeout
ADN:GID:WWW:YOUTUBE:410:NS09: State: Timeout
ADN:GID:WWW:YOUTUBE:411:NS10: State: Timeout
ADN:GID:WWW:YOUTUBE:GOOGLE_DNS:8.8.4.4: State: Timeout
ADN:DIR:WWW:FACEBOOK:500:NS09: Timeout
ADN:DIR:WWW:FACEBOOK:501:NS10: Timeout
ADN:DIR:WWW:FACEBOOK:GOOGLE_DNS:8.8.4.4: State: Timeout
ADN:GID:WWW:FACEBOOK:400:NS09: Timeout
ADN:GID:WWW:FACEBOOK:401:NS10: Timeout
ADN:GID:WWW:FACEBOOK:GOOGLE_DNS:8.8.4.4: State: Timeout
```

Yurtdışı çıkış devrelerinde yaşanan erişim probleminin düzelmesinin ardından gelecek "clear" alarmları aşağıda görüldüğü gibi olacaktır.

```
ADN:DIR:WWW:TWITTER:520:NS09: State: Clear
ADN:DIR:WWW:TWITTER:521:NS10: State: Clear
ADN:DIR:WWW:TWITTER:GOOGLE_DNS:8.8.4.4: State: Clear
ADN:GID:WWW:TWITTER:420:NS09: State: Clear
ADN:GID:WWW:TWITTER:420:NS10: State: Clear
ADN:GID:WWW:TWITTER:GOOGLE_DNS:8.8.8.8: State: Clear
ADN:DIR:WWW:YOUTUBE:510:NS09: State: Clear
ADN:DIR:WWW:YOUTUBE:511:NS10: State: Clear
ADN:DIR:WWW:YOUTUBE:GOOGLE_DNS:8.8.4.4: State: Clear
ADN:GID:WWW:YOUTUBE:410:NS09: State: Clear
ADN:GID:WWW:YOUTUBE:411:NS10: State: Clear
ADN:GID:WWW:YOUTUBE:GOOGLE_DNS:8.8.4.4: State: Clear
ADN:DIR:WWW:FACEBOOK:500:NS09: Clear
ADN:DIR:WWW:FACEBOOK:501:NS10: Clear
ADN:DIR:WWW:FACEBOOK:GOOGLE_DNS:8.8.4.4: State: Clear
ADN:GID:WWW:FACEBOOK:400:NS09: Clear
ADN:GID:WWW:FACEBOOK:401:NS10: Clear
ADN:GID:WWW:FACEBOOK:GOOGLE_DNS:8.8.4.4: State: Clear
```

HTTP isteği yapılan adres kaynaklı erişim problemi yaşanabilmektedir. Yaşanan problem sırasında aşağıda görüldüğü üzere "DIR" ve "GID" "timeout" alarmları üretilecektir. Bu sayede problemin ilgili adres kaynaklı olduğu anlaşılacaktır.

```
ADN:GID:WWW:TWITTER:420:NS09: State: Timeout
ADN:GID:WWW:TWITTER:421:NS10: State: Timeout
ADN:GID:WWW:TWITTER:GOOGLE_DNS:8.8.8.8: State: Timeout
ADN:DIR:WWW:TWITTER:520:NS09: State: Timeout
ADN:DIR:WWW:TWITTER:521:NS10: State: Timeout
ADN:DIR:WWW:TWITTER:GOOGLE_DNS:8.8.4.4: State: Timeout
```

HTTP isteği yapılan adres kaynaklı erişim probleminin düzelmesi ile birlikte üretilecek "clear" alarmları aşağıda görüldüğü gibi olacaktır.

```
ADN:DIR:WWW:TWITTER:520:NS09: State: Clear
ADN:DIR:WWW:TWITTER:521:NS10: State: Clear
ADN:DIR:WWW:TWITTER:GOOGLE_DNS:8.8.4.4: State: Clear
ADN:GID:WWW:TWITTER:420:NS09: State: Clear
ADN:GID:WWW:TWITTER:420:NS10: State: Clear
ADN:GID:WWW:TWITTER:GOOGLE_DNS:8.8.8.8: State: Clear
```

3.2.2 DNS Sorgularının Oluşturulması

İSS ağında bulunan lokal DNS' lere sorgular oluşturulmuştur. Bu sorgudaki amaç lokal de bulunan DNS makinalarında yaşananacak problemlerin en kısa sürede fark edilmesidir. Bu sorguların oluşturulmasında www.google.com.tr adresinden faydalanılmıştır.

Logların anlamlı bir şekilde bildirimi için etiketler (tag) oluşturulmuştur. Bu etiketler oluşturulurken sırasıyla paket kaynak bilgisi, route bilgisi, DNS makinasının bulunduğu yer bilgisi, adres bilgisi ve istek yapılan DNS adı göz önüne alınmıştır.

Logların üretilmesi için "xOfy" ve "threshold" değerleri girilmiştir. DNS sorguları için oluşturulan konfigürasyonlardaki değerlerin tümü "xOfy 2 16" ve "threshold 900" olarak girilmiştir. Threshold 900 olarak girilen değer, sorgu yapılan DNS' e paketlerin en fazla 900 ms içinde gidip gelmesi gerektiğini belirtir. Bu süre aşıldığında oluşturduğumuz "xOfy" değerine göre alarm üretmeye başlayacaktır. Aşağıdaki konfigürasyonlarda görülen "xOfy 2 16" ise son 16 paketten içerisinde 2 paket iletilmez ise "timeout" alarmı, timeout alarmından sonra gelen 16 paketten 15 ya da 16 tanesi başarılı bir şekilde iletilirse "clear" alarmı üret anlamına gelmektedir. "Frequency" ise yapılan sorguların zaman aralığı olarak belirlenen değeri gösterir. Bu konfigürasyonda girilen "frequency 9" ile 9 saniyede bir yapılan sorguların tekrarlanması istenmiştir.

Mobil tarafa yönlendirilen “GID” paketleri için girilen konfigürasyonlar ile 2 lokal DNS makinasına sorgu yapılmıştır. Sorgu için kaynak ip adresi 10.248.255.253 gösterilmiştir. Kaynak gösterilen ip adresi, IP SLA yönlendirici tarafında “GID” paketleri için oluşturulan sub-interface ip adresidir.

```
ip sla 123
 dns www.google.com.tr name-server 212.55.157.202 source-ip
10.248.255.253
 threshold 900
 vrf HTTP
 tag ADN:GID:TZL:DNS:212.55.157.202:NS10
 frequency 9
 ip sla reaction-configuration 123 react timeout threshold-
type xOfy 2 16 action-type trapAndTrigger
 ip sla schedule 123 life forever start-time now
```

```
ip sla 124
 dns www.google.com.tr name-server 212.55.157.201 source-ip
10.248.255.253
 threshold 900
 vrf HTTP
 tag ADN:GID:TZL:DNS:212.55.157.201:NS09
 frequency 9
 ip sla reaction-configuration 124 react timeout threshold-
type xOfy 2 16 action-type trapAndTrigger
 ip sla schedule 124 life forever start-time now
```

Kontrol amaçlı oluşturulan “DIR” paketleri için girilen konfigürasyonlar ile 2 lokal DNS makinasına sorgu yapılmıştır.

```
ip sla 107
 dns www.google.com.tr name-server 212.55.157.202
 threshold 900
 tag ADN:DIR:TZL:DNS:212.55.157.202:NS10
 frequency 9
 ip sla reaction-configuration 107 react timeout threshold-
type xOfy 2 16 action-type trapAndTrigger
 ip sla schedule 107 life forever start-time now
```

```
ip sla 108
 dns www.google.com.tr name-server 212.55.157.201
 threshold 900
 tag ADN:DIR:TZL:DNS:212.55.157.201:NS09
 frequency 9
 ip sla reaction-configuration 108 react timeout threshold-
type xOfy 2 16 action-type trapAndTrigger
 ip sla schedule 108 life forever start-time now
```

Girilen konfigürasyonların ardından “NS10” DNS’ de yaşanacak erişim problemi sırasında aşağıdaki “timeout” alarmları üretilecektir.

```
ADN:DIR:TZL:DNS:212.55.157.202:NS10 State: Timeout
ADN:GID:TZL:DNS:212.55.157.202:NS10 State: Timeout
```

“NS10” DNS’ de yaşanan erişim probleminin düzelmesinin ardından aşağıda görüldüğü üzere “clear” alarmları gelicektir.

```
ADN:DIR:TZL:DNS:212.55.157.202:NS10 State: Clear
ADN:GID:TZL:DNS:212.55.157.202:NS10 State: Clear
```

3.2.3 ICMP-ECHO Sorgularının Oluşturulması

İSS topolojisindeki kritk öneme sahip yönlendiricilere ICMP-ECHO sorguları yapılmıştır. Bu sorgular yapılırken network cihazlarının loopback interface ip adresleri kullanılmıştır. Yapılan sorguların amacı, yönlendiricilerin izlenmesi, yaşanacak bir problemin hızlı ve anlamlı bir şekilde bildiriminin yapılmasıdır.

Logların anlamlı bir şekilde bildirimi için etiketler (tag) oluşturulmuştur. Bu etiketler oluşturulurken sırasıyla paket kaynak bilgisi, route bilgisi, sorgu yapılan cihaz bilgisi ve adres bilgisi göz önüne alınmıştır.

Logların üretilmesi için “xOfy” ve “threshold” değerleri girilmiştir. ICMP-ECHO sorguları için oluşturulan konfigürasyonlardaki değerlerin tümü “xOfy 2 16” ve “threshold 100” olarak girilmiştir. Threshold 100 olarak girilen değer, sorgu yapılan yönlendiriciye paketlerin en fazla 100 ms içinde gidip gelmesi gerektiğini belirtir. Bu süre aşıldığında oluşturduğumuz “xOfy” değerine göre alarm üretmeye başlayacaktır. Aşağıdaki konfigürasyonlarda görülen “xOfy 2 16” ise son 16 paketten içerisinde 2 paket iletilmez ise “timeout” alarmı, timeout alarmından sonra gelen 16 paketten 15 ya da 16 tanesi başarılı bir şekilde iletilirse “clear” alarmı üret anlamına gelmektedir. “Frequency” ise yapılan sorguların zaman aralığı olarak belirlenen değeri gösterir. Bu konfigürasyonda girilen “frequency 1” ile 1 saniye aralıklarla yapılan sorguların tekrarlanması istenmiştir.

“DIR” paketleri kullanılarak yapılan ICMP-ECHO sorgularının konfigürasyon bilgileri aşağıda görüldüğü gibidir.

```
ip sla 150
 icmp-echo 217.32.228.190
 Threshold 100
 tag ADN:DIR:INT90ADN01:217.31.228.190:
 frequency 1
 ip sla reaction-configuration 150 react timeout threshold-
type xOfy 2 16 action-type trapAndTrigger
 ip sla schedule 150 life forever start-time now
```

```
ip sla 151
 icmp-echo 217.32.228.191
 threshold 100
 tag ADN:DIR:INT90ADN02:217.32.228.191:
 frequency 1
 ip sla reaction-configuration 151 react timeout threshold-
type xOfy 2 16 action-type trapAndTrigger
 ip sla schedule 151 life forever start-time now
```

```
ip sla 154
 icmp-echo 217.32.228.193
 threshold 100
 tag ADN:DIR:INT90GNS01:217.32.228.193:
 frequency 1
 ip sla reaction-configuration 154 react timeout threshold-
type xOfy 2 16 action-type trapAndTrigger
 ip sla schedule 154 life forever start-time now
```

```
ip sla 155
 icmp-echo 217.32.228.194
 threshold 100
 tag ADN:DIR:INT90GNS02:217.32.228.194:
 frequency 1
 ip sla reaction-configuration 155 react timeout threshold-
type xOfy 2 16 action-type trapAndTrigger
 ip sla schedule 155 life forever start-time now
```

İSS topolojisindeki "INT90GNS01" isimli yönlendiriciye yapılan ICMP-ECHO sorgularının başarısız olması durumunda aşağıda görüldüğü üzere "timeout" alarmları üretilecektir.

```
ADN:DIR:INT90GNS01:217.32.228.193: State: Timeout
```

"INT90GNS01" isimli yönlendiriciye yapılan ICMP-ECHO sorgularında yaşanan problemin düzelmesi ile birlikte aşağıda görüldüğü üzere "clear" alarmları gelicektir.

```
ADN:DIR:INT90GNS01:217.32.228.193: State: Clear
```

4. TARTIŞMA VE SONUÇ

Bireyler günlük yaşantılarının gereksinimlerini yerine getirebilmek için mobil iletişim teknolojilerinden daha fazla yararlanmaya başlamıştır. Bu durumun en büyük sebeplerinden biri olan taşınabilir cihazlar ile birlikte bilgiye hızlı ve gereken heryerde ulaşabilmek insanların vazgeçilmezlerinden biri olmuştur. Tüm bu nedenlerden dolayı internet dünyası da hızla büyüyerek ilerlemekte ve giderek daha çok insana ulaşmaktadır.

Artan kullanıcı ve uygulama sayılarına paralel olarak internet servis sağlayıcısı ağlarıda hızla büyümüş ve giderek karmaşık bir hal almıştır. Bu karmaşık yapı içerisinde yaşanan iletişim problemlerinin tespit edilmesi ve en kısa sürede çözüme ulaştırılması gittikçe zorlaşmaktadır. Bu nedenle mobil internet erişimine ve teknolojisine yön veren şirketlerin servis kalitesi problemlerini en kısa zamanda tespit edip çözüme kavuşturabilme yeteneği gerek müşteri gerek firma açısından büyük öneme sahiptir.

Mevcut durumda mobil taraftaki problemlerin büyük çoğunluğu müşteri şikayetleri sonucu fark edilmektedir. Bu sebeple problemlerin farkına varılması belirsiz bir süre içerisinde gerçekleşmektedir. Bu belirsizliğin sebebi internet erişimi problemlerinin daha çok müşteri tarafından fark edilerek bildiriminin yapılmasıdır. İnternetin yoğun olarak kullanıldığı zamanlarda her ne kadar bu süre kısalsada yoğun olarak kullanımın olmadığı gece saatlerinde yaşanacak sorunların fark edilmesi çok daha uzun zaman almaktadır. Mevcut yapıda kullanılan, 5 dakikalık trafik ortalamalarını gösteren grafikler internetin yoğun olarak kullanıldığı durumlarda kısmen işe yaramakta fakat sorunun nerede olduğu konusunda yardımcı olmamaktadır. İnternetin yoğun olarak kullanılmadığı zamanlarda trafik miktarı zaten az olduğundan oluşturulan grafiklerde problemin fark edilmesi daha da zorlaşmaktadır. Ayrıca grafikler problemin hakkında bilgi vermediğinden, devamında uzun bir kontrol süreci başlamaktadır. İSS' lar gibi büyük ağlara sahip firmalarda problemin nerede yaşandığını bulma ve çözme süreci farklı bölümler, farklı kişiler üzerinden dakikalar hatta saatler sürebilmektedir.

Bu çalışmada erişim problemlerinin en kısa sürede tespit edilmesi ve sebebinin belirlenmesi amacıyla yeni bir izleme yöntemi geliştirilmiştir. Farklı teknolojilere ve tasarımlara sahip network cihazları irdelenmiş ve tüm mobil network ağını izlemek için yeni bir yaklaşım ortaya koyulmuştur. Paketlere yön verilmesi yardımıyla HTTP isteği, DNS ve ICMP-ECHO sorguları ile lokal ağ içerisinde ve internet üzerinde belirlenen adreslere denetimler yapılmış, yapılan bu denetimler neticesinde problemler ve problemlerin kaynağı tespit edilmiştir.

Yapılan bu çalışma sonucunda internet üzerinde yaşanacak problemler maksimum 120 saniye içerisinde fark edilmektedir. DNS üzerinde yaşanacak bir problem maksimum 144 saniye içerisinde, kritik bir yönlendirme cihazında yaşanacak bir problem ise 16 saniye içerisinde fark edilmektedir. Oluşturulan esnek yapı sayesinde süreler veya kriterler duruma göre değiştirilebilir. Tek bir servise, cihaza yada hedefe yönelik özel kriterler belirlenebilir.

Geliştirilen bu yeni yaklaşım sonucunda ortaya çıkabilecek erişim problemlerinin anlamlı bir şekilde bildiriminin yapılması sağlanmıştır. Bu sayede müşteri şikayetlerinden önce problemler tespit edilmeye başlanmıştır. Bunun sonucunda gerek firma memnuniyeti gerek müşteri memnuniyeti sağlanmış, bununla birlikte ağın servis verimi ve kalitesi artmıştır.

Bu çalışma mobil internet hizmeti sunan bir firmada teknik ve yönetim ekipleri ile tartışılarak geliştirilmiş ve uygulanmıştır. Bu aşamada tüm sorunlar ve sorular irdelenmiş en doğru ve en faydalı olacak yöntem tespit edilerek uygulanmıştır. Sektördeki büyük bir firmada bu çalışmayı uygulamış olmak ortaya çıkan sonuçların kabul edilebilirliği anlamında büyük katkı sağlamıştır. Diğer mobil İSS firmaları içinde örnek alınabilinecek bir çalışma niteliğindedir.

Bu tez çalışması üzerine daha sonra yapılacak çalışmalarda, Paket Yönlendirme Yaklaşımı tüm internet servis sağlayıcısı ağına uygulanabilir. Yapının esnekliği sayesinde günün şartlarına ve isteklerine göre arzu edilen değişiklikler rahatça yapılabilir.

KAYNAKÇA

Kitaplar

Ahmed, A. & Siddiqui, T., 2011, Voip performance management and optimization, Indianapolis: Cisco Press

Alvarez, S., 2006. QoS for IP/MPLS Networks. Indiana: Cisco Press

Aziz, Z., Liu J., Martey A. & Faraz S., 2002. *Troubleshooting ip routing protocols.* Indiana: Cisco Press

Heap, G. & Maynes, L., 2002. *CCNA practical studies*. Indianapolis: Cisco Press

Hucaby, D., 2005. *Ccnp bcmsn exam certification guide*. 3. Baskı. Indianapolis: Cisco Press

Kaplan Y., 2000. *Veri haberleşmesi (network) temelleri*. İstanbul: Papatya Yayıncılık

Lammle, T., 2008. *Cisco ağ teknolojileri yönetimi.* F. B., Baş., Üçüncüoğlu (Çev.), İstanbul: Bilge Adam Yayınları

Odom, W., 2010. *CCNP ROUTE 642-902 official certification guid.* Indianapolis: Cisco Press

Odom, W. & Cavanaugh, M., 2004. *Cisco QoS: Exam certification guide.* 2. Baskı. Indianapolis: Cisco Press

Osborne, E. & Simha, A., 2002. *Traffic engineering with MPLS*. Indiana: Cisco Press

Rosen, E., Viswanathan, A. & Callon, R., 2001. *Multiprotocol Label Switching Architecture*, RFC 3031

Szigeti T., Hattingh C., Barton R. & Briley K., 2013. *End-toEnd QoS network design.* Indianapolis: Cisco Press

Terae D., 2010. *Implementing cisco ip routing.* Indianapolis: Cisco Press

Tutku, K.H., 2012 *Network sistemleri* 2. Baskı. İstanbul: Seçkin Yayıncılık

Diğer Yayınlar

CISCO systems, Quality of Service, http://www.cisco.com/c/en/us/products/ios-nx-os-software/quality-of-service-qos/index.html [erişim tarihi 20.12.2014]

CISCO systems, MPLS/Tag Switching, http://docwiki.cisco.com/wiki/MPLS/Tag_Switching [erişim tarihi 25.12.2014]

CISCO systems, Quality of Service Networking, http://docwiki.cisco.com/wiki/Quality_of_Service_Networking [erişim tarihi 25.12.2014]

Çay, K., 2010, TCP / IP protokol grubu tarihçesi [online], Turkcenet, http://www.turkcenet.org/index.php?option=com_content&task=view&id=256&Itemid=55&limit=1&limitstart=0 [Ziyaret Tarihi: 17.12 2014].

Ercetin, C., 2010, MPLS ile tanışalım [online], http://cenkercetin.com/mpls-ile-tanisalim/ [erişim tarihi 02.12.2014]

Internet Usage in Europe, 2010, http://www.internetworldstats.com/stats4.htm [erişim tarihi: 03.10. 2014]

Internet Society, Brief History of the Internet, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet [Erişim tarihi 14.10.2014]

MEB, TCP/IP ve IP Adresleme, 2008, www.meb.gov.tr [erişim tarihi 08.11.2014]

NETAŞ, Gateway GPRS Support Node, http://www.netas.com.tr/tr/genisbant-altyapi-cozumleri/mobil-genisbant/42 [erişim tarihi 14.12.2014]

ODTU, Internet Tarihi, http://www.internetarsivi.metu.edu.tr/tarihce.php [erişim tarihi 15.11.2014

TECHNET, How DNS Works, 2013, https://technet.microsoft.com/en-us/library/cc772774(v=ws.10).aspx [erişim tarihi 15.10.2014]