GERÇEK ZAMANLI VE KRİTİK ÇALIŞAN SİSTEMLER İÇİN MODERN GENİŞ ALAN AĞ TASARIMI

Abdullah GÜRTEKİN

YÜKSEK LİSANS TEZİ
İLERİ TEKNOLOJİLER

GAZİ ÜNİVERİSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

EYLÜL 2012
ANKARA

Abdullah GÜRTEKİN tarafından hazırlanan "GERÇEK ZAMANLI VE KRİTİK ÇALIŞAN SİSTEMLER İÇİN MODERN GENİŞ ALAN AĞ TASARIMI " adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Yrd. Doç. Dr. Nursel AKÇAM ……..
Tez Danışmanı, Elektrik-Elektronik Müh Anabilim Dalı

Bu çalışma jürimiz tarafından oy birliği ile İleri teknolojiler Anabilim Dalında Yüksek lisans tezi olarak kabul edilmiştir.

Doç. Dr. Elif ORHAN ……
İleri Teknolojiler Anabilim Dalı, G.Ü.

Doç. Dr. Erkan AFACAN ……
Elektrik-Elektronik Müh. Anabilim Dalı, G.Ü.

Yrd. Doç. Dr. Nursel AKÇAM ……...
Elektrik-Elektronik Müh. Anabilim Dalı, G.Ü.

Tarih: ……..

Bu tez ile G.Ü. Fen Bilimleri Enstitüsü Yönetim Kurulu Yüksek Lisans derecesini onamıştır.

Prof. Dr. Şeref SAĞIROĞLU ……
Fen Bilimleri Enstitüsü Müdürü

TEZ BİLDİRİMİ

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

Abdullah GÜRTEKİN

GERÇEK ZAMANLI VE KRİTİK ÇALIŞAN SİSTEMLER İÇİN MODERN GENİŞ ALAN AĞ TASARIMI

(Yüksek Lisans Tezi)

Abdullah GÜRTEKİN

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
Eylül 2012

ÖZET

Bu çalışmada, radar sistemleri, radyo haberleşme sistemleri gibi gerçek zamanlı ve kritik çalışan sistemler için veri haberleşmesinin temellerinden başlanarak, geniş alan ağ tasarım seçenekleri ve tasarım kriterleri üzerinde durularak, ileri düzeyde, örnek, modern bir geniş alan ağ tasarımı gerçekleştirilmiştir. Farklı operasyonel servis trafiklerinin, olduğu bu geniş alan ağ (WAN), ana merkezler, uzak istasyonlar (radyo ve radar istasyonları) ve uzak kuleler arasında yedekli olarak çalışmayı destekleyecek topoloji mimarileri geliştirilerek tasarlanmıştır. Çalışmada radar ve ses verilerinin sıkıştırılması ve gelişmiş IP adresleme teknikleri kullanılarak, ana merkez olan görüntüleme merkezlerine taşınması detaylı olarak anlatılmıştır. Şehirlerarası ya da şehiriçi uzak mesafelerde servis sağlayıcılardan (Telekom-Turksat) faydalanılmıştır. Telekom tarafından sağlanan hizmet karasal link olarak adlandırılmış ve ana link olarak ele alınmıştır. Uydu üzerinden alınan hizmet ise karasal linkin çalışmadığı durumlarda devreye girecek olan yedek link olarak planlanmıştır. Karasal-Uydu link geçişleri için çoklu dinamik ve statik yönlendirme yöntemleri kullanılarak otomatik geçiş sağlanmıştır. Karasal linkte çok yakın bir zamanda kullanılmaya başlayan çok noktadan çok noktaya iletişim sağlayan, Sanal Özel Yerel Ağ Hizmeti (VPLS-Virtual Private LAN Service) kullanılarak

yönlendiriciler ethernet protokolü vasıtasıyla yapılandırılmışlardır. Bununla beraber uzun süredir kullanımı devam eden noktadan noktaya erişim sağlayan TDM (Time Division Multiplexing) teknolojisi de gereken yerlerde kullanılmıştır. Ayrıca WAN (Wide Area Network) içerisindeki her link için bant genişliği, gecikme, jitter, paket kaybı v.b. gibi kriterleri ele alan QoS (Quality of Service) parametreleri yapılandırılmış ve servis sağlayıcılardan kiralanan devreler (hatlar) çeşitli ağ performansını analiz eden yazılımlar kullanarak test edilmiş, şekiller ve çizelgeler kullanılarak sonuçlar verilmiştir. Yapılan analizler ışığında, linklerin kabul edilip, edilemeyeceği sebepleriyle açıklanmıştır. Veri paketlerin geçiş önceliği için CoS (Class of Service) servisi kullanılarak, istenilen paketlerin geçişine öncelik verilmiiştir. Gerçek zamanlı veri olarak ses, kritik veri olarak radar verisi ve standart veri olarak ise yönetim için kullanılan veri paketleri belli parametrelere göre sınıflandırılmış ve istenildiği gibi önceliklendirilmiştir.

Bilim Kodu : **905.1.035**
Anahtar Kelimeler : **Modern Radar Ağı, Geniş Alan Ağ, Gerçek Zamanlı ve Kritik Sistemler, VPLS, CoS, QoS, Karasal ve Uydu Ağı.**
Sayfa Adedi : **170**
Tez Yöneticisi : **Yrd. Doç. Dr. Nursel AKÇAM**

A MODERN WAN DESIGN FOR REAL -TIME AND CRITICAL SYSTEMS
(M. Sc. Thesis)

Abdullah GÜRTEKİN

GAZI UNIVERSITY
INSTITUTE OF SCIENCE AND TECHNOLOGY
September 2012

ABSTRACT

In this study, an advanced modern WAN (Wide Area Network) has been designed for the systems like Radar Systems that carries critical data and Radio Communication Systems that carries real-time data. All the issues has been started to be explained from the fundamentals of the network technology. What is more, different type of WAN choices and some of the WAN design criterias have been also explained in detail. Designed WAN has different operational data flows between main centers and remote stations called radyo stations and radar stations that support a redundant systems architecture. In the radyo stations the analog audio has been compressed and converted to digial and by the advanced IP adressing techniques it has been send to the centers through same wires that has been used for the radar data transfer. For the data transfer between the long distances like cities, the service providers like telecommunication companies and satellite companies' existing network (infrastructure) has been used. The main link called terrestrial link is considered as the link provided by the local telecommunication company and the backup link called satellite link is considered as the link provided by the satellite company. In case, the failure of the main link, by the help of the static and dynamic routing protocols, an automatic switching from terrestrial to satellite link has been configured. VPLS (Virtual Private LAN Service) technology that has just been started to be used nowadays and provides

communication from multi point to multi point based on ethernet protocol has been used for the terrestrial link. What is more, TDM (Time Division Multiplexing) technology which has been started to be used long time ago also has been implemented for the locations where it was needed. QoS parameters (bandwidth, latency, jitter, packet loss) has been configured for each related link and also CoS (Class of Service) defining has been done for the traffics that has priority to pass. The data traffics has been classified as real--time (voice), critical data (radar data) and standard data (management telnet sessions). By the help of different software for network performance analysis all the QoS and CoS tests are done and the results are analysed with the related graphics and tables.

Science Code : **905.1.035**
Key Words : **Modern Radar Network, WAN, Real-Time&Critical Systems, VPLS, QOS, COS, Terrestrial and Satellite Network.**
Page Number : **170**
Adviser : **Assist. Prof. Dr. Nursel AKÇAM**

TEŞEKKÜR

Tez çalışmamın her aşamasında yakın ilgisini ve desteğini gördüğüm, çalışmalarımın her aşamasının yönlendirilmesi ve sonuçlandırılmasında büyük emeğe sahip olan değerli hocam Yrd. Doç. Dr. Nursel AKÇAM'a teşekkürlerimi sunarım.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge **Sayfa**

RESİMLERİN LİSTESİ

Resim **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

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

Kısaltmalar	Açıklamalar
ARP	Address Resulotion Protocol
AS	Autonomous System
BGP	Border Gateway Protocol
CIDR	Classless Inter-Domain Routing
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
DTE	Data Terminal Equipment
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
EIGRP	Enhanced Interior Gateway Routing Protocol
FTP	File Transfer Protocol
FDP	Flight Plans Data Processing
Gbps	Gigabit per second
GVS	Gateway Voice System
HSRP	Hot Standby Router Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISO	International Standarts Organization
LACP	Link Aggregation Protocol
LAN	Local Area Network
MAN	Metropolitan Area Network
Mbps	Megabit per second
MPLS	Multi Protocol Label Switching

SİMGELER VE KISALTMALAR

Kısaltmalar	Açıklamalar
OSI	Open Systems Interconnection)
OSPF	Open Shortest Path First
PIM	Protocol Independent Multicast
PSR	Primary Surveillance Radar
RDP	Radar Data Processing
RFC	Request for Comments
RHP	Radar Head Processor
SFPL	System Flight Plan
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
TDM	Time Division Multiplexer/Multiplexing
TWR	Tower Site
UDP	User Datagram Protocol
VCSS	Voice Communications Switching System
VHF	Very High Frequency
VLSM	Variable Length Subnet Masking
VOIP	Voice over IP
VPLS	Virtual Private LAN Service
VSAT	Very Small Aperture Terminal
WAN	Wide Area Network

1.GİRİŞ

Gelişen bir çok teknolojiye paralel olarak, dünya küçülmekte ve yine buna paralel olarak, insanların iletişim teknolojilerinin hızı ve kapasitesi konusunda birçok beklentileri de artmaktadır. Günümüzde, şehirlerarasında ya da ülkelerarasında bile, sağlanmış olan iletişim, yerel bir ağ içerisindeki haberleşme sistemimiz gibi gecikme, veri kaybı, işlem hacmi vb. gibi etkenler bakımından da iyi performans değerleri ışığında oluşturulabilmektedir. Coğrafik olarak birbirinden uzak bir çok noktanın (bu noktalar şehirler, ülkeler ya da kıtalar arası da olabilir) birbirleri arasında istenen şekilde iletişim kurmasında, temel teşkil eden teknoloji "Geniş Alan Ağ" (WAN-Wide Area Network) olarak adlandırılmaktadır. Bir WAN tasarımında, sistemde koşacak olan uygulamaların türü, sistemin operasyonel çalışma zamanı, akan verilerin kritik olma derecesi gibi faktörler önemli rol oynayan temel gerekliliklerdir. Bunların yanısıra, ağ'da olması gereken her bağ için işlem hacminin bilinmesi ve ona göre kullanılması gereken ilgili WAN teknolojisine karar verilmesi ise önemli teknik gerekliliklerdir. Bu teknik gerekliliklere yine paralel olarak kullanılacak olan donanımlar (yönlendiriciler, anahtarlar, kablolamalar vs.) değişiklik gösterebilir. Tasarım da önemli yer tutacak olan, veri akışının olacağı noktalar tanımlanıp, ilgili bir şekilde sınıflandırıldıktan sonra, bağlantıların lokal olarak ve genel olarak gösterileceği topoloji haritaları çizmek ve ilgili bağlantıları hem mantıksal olarak hem de fiziksel olarak detaylandırmak, WAN tasarımında önde gelen tasarım gerekliliklerindendir.

WAN iletişimdeki veri akışının, öncelikle, açık sistem bağlantı modelinde (osi-open systems interconnection) hangi katmanlarda olacağını tasarlamak, ilgili yapılandırma işlemleri için kolaylık sağlar. Bu yapılandırmalar, temel olarak aynı mantıkta olmakla beraber kullanılan donanımın marka ve modeline göre değişiklik gösterir. Örneğin, bir cisco anahtar'da VLAN yaratmak ile HP anahtar'da VLAN yaratmak için birbirlerine benzer ama farklı komutlar kullanılır. Kompleks ve gelişmiş olan WAN tasarımlarında yönlendirici ve anahtar yapılandırmaları, topolojileri iyi analiz edebilmeyi ve yapılandırma konusunda iyi tecrübe sahibi olmayı gerektirir.

Geniş alan ağ konusunda akla gelebilecek olan, farklı önemli sorular olabilir. Örneğin, A ve B arasında bir ağ kurmak istersek ve bu uzak iki nokta (şehirler arası) arasındaki bağlantının nasıl sağlanabileceği akla gelen ilk sorudur. Genellikle bir çok kurum ya da kuruluş uzak mesafeler arasındaki bağlantıları sağlayabilmek için ilgili ülkenin hat sağlayıcı firmalarından faydalanır ki bunlar genellikle ulusal telekom firmaları olur. Dünya'nın bir çok yerinde bu tür devreleri sağlayabilmek için kurulmuş olan telekomünikasyon firmalari ilk olarak telefon hizmeti vermek amacıyla, PSTN (public switched telephone network) bağlantılar için bakır kablolama ile işe başlamışlardır. Günümüzde ise bakır kablolama teknolojilerine ek olarak çok uzun mesafelerde bile verimli çalışma imkanı sağlayan ilgili fiber optik teknolojilerinden faydalanılır. Bazı noktalarda ise ne fiber optik olarak ne de bakır olarak kablolama yapmak coğrafik zorluklar nedeniyle mümkün olmayabilir. Bu tür durumlarda ise uydu, radyo link, wi-fi gibi kablosuz çalışan teknolojilerden faydalanılır. Bu işlemi tabi ki bir de ekonomik bakış açısıyla görmek gerekir. Hızla gelişen bir çok teknoloji gibi, WAN teknolojileri de son zamanlarda kendini yenilemektedir. 1980'lerden beri kullanılan X25 ya da daha sonraları kullanılmaya başlayan Frame Relay ve ATM gibi teknolojilerin yanı sıra günümüzde kullanılan, kullanıcı kısmına CE'den (customer edge), PE'ye (provider edge) ethernet protokolü ile ulaşan MPLS/IP, VPLS gibi teknolojiler sundukları ucuz hat ücretleri ve kolay yönetilebilirlikleri dolayısıyla gayet popüler olmuşlardır. Kullanmak istediğimiz teknoloji, işlem hacmi, yani bant genişliği, noktalar arasında uzaklık gibi faktörlere göre hat sağlayıcımıza ödeyeceğimiz miktar değişir. Örneğin, uzun süreden beri kullanılmakta olan, TDM (time division multiplexing) teknolojisi gibi sürekli iki noktaya özel bağlantı sağlayan teknolojiler için ödenen miktar, VPLS, IP/MPLS gibi modern teknolojilere göre daha fazla olur. Teknolojinin gelişimiyle, bu tür iletişimler için ödenen miktar bazen azalabilmektedir. Dolayısıyla, gider hesaplarını yapmak, WAN tasarımında önemli ekonomik gerekliliklerdendir.

Eğer ağ'da veri akışının olduğu bir çok nokta mevcutsa ve link bazında bir çok yedekleme işlemi yapılması isteniyorsa, bütün bu noktadan noktaya bağlantılar için örneğin, TDM teknolojisini kullanmak çok pahalıya mal olabilir. Radar verisi ya da ses haberleşme ağ'ları gibi gerçek zamanlı ve kritik veri taşıyan bir geniş alan ağ

sisteminin, daha ekonomik olabilmesi için bizde örnek olarak kurmuş olduğumuz WAN'da karasal ağ olarak, modern teknolojilerden biri olan *Sanal Özel Ağ Hizmet'inden (VPLS- Virtula Private LAN service)* faydalandık. VPLS çok noktadan çok noktaya, açık sistem bağlantı modelinin ikinci katmanı üzerinden, ethernet protokolü tabanında sanal tüneller üzerinden bağlantı sağlar.

Ağ'ın erişilebilirlik ve kullanılabilirlik değerlerinin çok yüksek olmasının gerektiği durumlarda ise tek bir hat sağlayıcıdan değil, örneğin yedek link olarak karasal hat sağlayıcıların yanısıra, uydu hat sağlayıcılarından bazı devreler kiralanabilir. Planlamış olduğumuz modern WAN'da, uydu linkleri karasal linklerde problem oluştuğu zaman otomatik olarak devreye girerek iletişimin devamlılığını sağlayacaktır. Uydu bağlantıları için star ve mesh topolojileri ilgili noktalara göre kullandık ve uydu ile karasal ağ arasındaki otomatik geçişlerin yönlendiricilerdeki öncelik yapılandırmalarından örnekler vererek nasıl yapıldığını gösterdik.

Yapmış olduğumuz bu önbilgilendirmelerin ışığında, tez çalışmamız 6 ana bölümden oluşmaktadır.

Birinci bölüm giriş bölümü olup, bu çalışmada incelenen konular ve geliştirilen teknikler hakkında genel bilgiler verilmiş, olabildiğince basit ve anlaşılır bir dil kullanılmıştır.

İkinci bölümde, veri iletişiminin temelleri anlatılmış olup, açık sistem bağlantı modeli'ne (osi-open systems interconnection) değinilmiştir. Ağ elamanlarından bahsedilmiş anahtarlar ve yönlendiriciler üzerinde bazı yapılandırma örnekleriyle durulmuştur. Yönlendiriciler hakkında detaylı bilgi verilmiş olup, bazı yönlendirme protokolleri için wireshark yazılımı kullanırak analizler yapılmıştır.

Üçüncü bölümde, WAN tanımından başlanarak, ideal bir WAN için gerekli olan tasarım kriterlerinden bahsedilmiştir. WAN kurulumu için gerekli olan basamaklar anlatılmış ve hiyerarşik tasarım modeli üzerinde durulmuştur. Daha sonra ise WAN teknolojileri bazı özelliklerine göre gruplandırılmıştır. Bu gruplandırma işleminden

sonra, bağlantılarına göre WAN teknolojileri, şekiller üzerinde daha ayrıntılı incelenmiştir.

Dördüncü bölümde, tasarım temellerinde önemli yer tutan olan ağ topoloji çizimleri yapılmıştır. Örnek olarak kurulan WAN için, bağlantı gereksinimleri, işlem hacimleri ele alınarak hesaplanmıştır. Bütün noktalar arasındaki bağlantılar hem şekilsel olarak, hemde tablosal olarak gösterilmiştir. Topoloji çizimlerini daha kolaylaştırabilmek amacıyla, bütün lokasyonlar ilgili gruplara ayrılmıştır. Daha sonra ise her lokasyonda kullanılan cihazlar gösterilmiş ve her lokasyondaki ağın mantıksal ve fiziksel olarak görünüşleri verilmiştir. Ayrıca lokasyonlar arasındaki veri akışını anlamak amacıyla, daha genel çizimler yapılmıştır.

Beşinci bölümde karasal ağ ve uydu ağ'ı üzerinde ayrıntılı durulmuştur. Karasal ve uydu ağ'ı için kullanılan teknolojiler detayları ile açıklanmıştır. QoS (quality of service) parametreleri tanıtılmış daha sonra karasal ve uydu hat sağlayıcılarının garanti ettiği QoS parametre değerleri baz alınarak testler yapılmıştır. Testler için Ixchariot programı kullanılmış ve her sonuç yine hem tablosal hemde grafiksel olarak analiz edilip, değerlendirilmiştir. Her test için belli sonuç kriterleri yazılmıştır. Daha sonra, verilerin önceliklendirilmesi için, hizmet sınıflandırması (CoS-class of service) anlatılmış ve yönlendiricilerde CoS yapılandırmasına örnek verilmiştir.

Altıncı bölümde ise genel olarak sonuçlardan bahsedilmiş, WAN tasarımında temel öneriler verilmiştir. Tezin amaç ve önemi belirtilmiş, ışık tutabileceği noktalara değinilmiştir.

2. AĞ TEMELLERİ

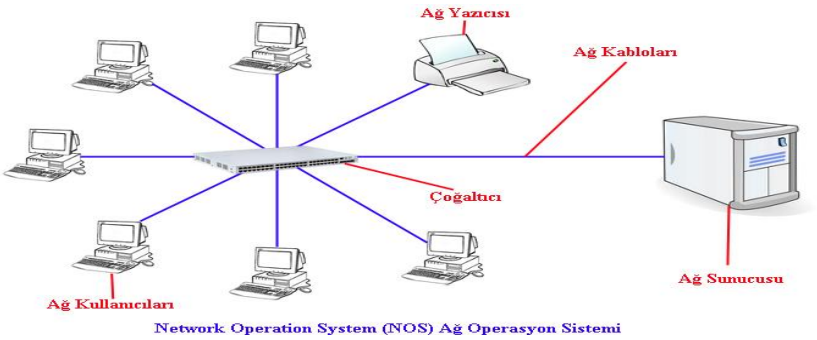
2.1. Veri Ağları

Birden çok veri iletişimi yapabilecek cihazın birbirine bağlı olduğu donanım ve yazılımların da paylaşılmasına izin veren ağlar, veri ağları olarak adlandırılmaktadır.

Bir haberleşme ağ'ına en güzel örnek, evlerimizde kullandığımız telefonlardır. Telefonlarda ses, kablolar ile ilgili santrale gönderilir, santrallerden diğer santrallere ve oradan da hedef telefona çağrı iletilir. Her telefonun kendisine ulaşmakta kullanılan bir numarası bulunmaktadır. Bu sistem incelendiğinde bir ağın nasıl çalıştığı daha kolay anlaşılabilir. Kısaca, aynı sistem bilgisayara uyarlandığında her bilgisayarın bir numarasının bulunduğu, çeşitli kablolama teknolojileri ve ağ elemanlarıyla verinin hedefe ulaştırıldığı görülür. Ağ sistemleri iki kişisel bilgisayardan oluşabileceği gibi binlerce iş istasyonundan da oluşabilir [15].

Veri ağlarının tarihine kısaca bakmak gerekirse, ilk uygulamaları 1960'lı yılların sonlarında başlamıstır. Ancak yerel bilgisayar ağlarının yaygınlaşması 1980'li yıllarda başlamış ve gelişmiştir. 1980'li yıllarda, kisişel bilgisayarların çoğalması, bilgisayar teknolojisindeki ve iletişim teknolojilerindeki gelişmeler bilgisayar ağlarının daha elverişli kullanılmasına olanak sağlamıştır.

Veri ağlarının bir çok alanda faydaları vardır. Örneğin, işletmecilik açısından ağlar, yönetime ve denetime yardımcı olurlar. Bir bankanın ya da üniversitenin çok sayıda bilgisayarını birbirine bağlı olarak kullanması, onları bağımsız olarak kullanmasından daha anlamlı ve verimli olur. Böylece birimler arası iletişim daha kolay sağlanır ve bütünleşik uygulamalar daha kolay gerçekleştirilir. Ortak kaynak kullanımı ile donanım maliyetleri düşer, ortak çalışma imkânını arttırarak takım, çalışmalarını hızlandırır, çalışanların verimini ve performansını arttırır. İletişim hızını arttırarak zaman kazancı sağlar, ayrıca önemli bilgilerin yedeklenmesi daha kolay hale gelir. Şekil 2.1'de veri ağları için yüzeysel bir gösterim mevcuttur.



Şekil 2.1. Veri ağı

2.2. Yapılarına Göre Veri Ağları

Veri ağları, kaynaklara erişim, kapsadığı alan ve söz sahibi olma şekline göre genellikle üç grup'ta incelenir.

2.2.1. Yerel alan ağları (LAN-Local Area Network)

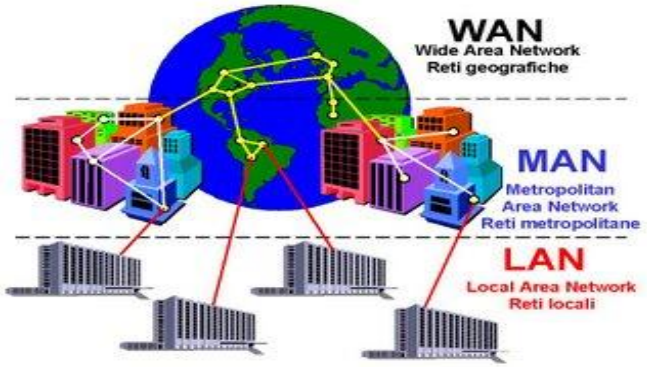
Yerel bilgisayar ağları, göreceli olarak küçük olan sistemlerden ve iletişim ortamından oluşur. Yüksek hızlı, küçük alanları (bir bina, bir firma, bir bölüm, bir oda) kapsayan bir veri ağıdır. Yerel ağ içinde bilgisayarlar, sunucular, iş istasyonları, yazıcılar ve diger çevre birimleri yer alabilir. Normalde tek tür iletisim kuralına eğilim gösterir. Ancak farklı iletisim kurallarının (ağ protokolleri) kullanıldıgı ağlar da mevcuttur. Yerel bilgisayar ağları, genellikle tek bir organizasyon tarafından sahiplenilir ve yönetilirler. Evlerde ya da ofislerde bilgisayarlar arası oluşturulan iletişim ağı yerel alan ağ'ına örnek gösterilebilir.

2.2.2. Kentsel alan ağı (MAN-metropolitan area network)

Yerel ağlarına oranla daha geniş, genellikle birkaç mevcut yerel bilgisayar ağının birleştirilmesi sonucu kurulan ağlardır. Genellikle sehir içi uzak bağlantılar söz konusu oldugundan ve şehrin bir kısmını kapsadıgından kentsel ağlar olarak adlandırılmışlardır. Üniversite kampüsü içerisinde kullanılan ağlar kentsel alan ağ'a örnek verilebilir.

2.2.3. Geniş alan ağı (WAN-wide area network)

Yerel veya kentsel ağların birlesmesi ile oluşturulurlar. Şehir, ülke, kıta, hatta dünya çapındaki bilgisayarların birbirleriyle ilişkilendirilmesi sonucunda oluşmuş veya kurulmuş olan bilgisayar ağlarıdır. Geniş alan ağı, coğrafik olarak uzak mesafelerdeki kentsel ağdan geniş, her tür ağı birbirine bağlamak için kullanılır. En bilindik geniş alan ağ internettir. Kurumların ya da kişilerin farklı amaçlar için oluşturdukları bir çok geniş alan ağ mevcuttur. Şekil 2.2'de bütün ağ çeşitleri için yüzeysel bir gösterim yapılmıştır [1, 8, 15].



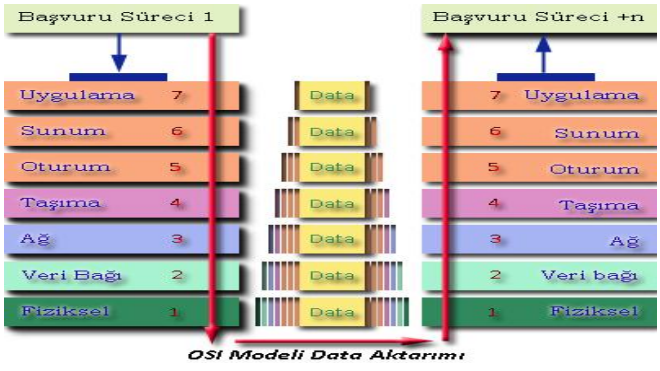
Şekil 2.2. Wan/Man/Lan

2.3. Açık Sistem Bağlantı Modeli (OSI-Open Systems Interconnection)

Bilgisayarlar arası iletişimin başladığı ilk günden itibaren farklı bilgisayar sistemlerinin birbirleri arasındaki iletişim, daima büyük problemlerden birisi olmuş ve bu sorunun üstesinden gelebilmek için uzun yıllar boyunca çeşitli çalışmalar yapılmıştır. 1980'li yılların başında Uluslararası Standartlar Organizasyonu (ISO-International Standarts Organization) bilgisayar sistemlerinin birbirleri ile olan iletişiminde ortak bir yapıya ulaşmak yönünde çabaları sonuca bağlamak için bir çalışma başlatmıştır. Bu çalışmalar sonucunda 1984 yılında Açık Sistem Bağlantıları (OSI-Open Systems Interconnection) referans modeli ortaya çıkarılmıştır. Bu model sayesinde değişik veri iletişimi cihazları üreten firmaların ürettikleri cihazlar

arasındaki iletişimi bir standarda oturtmak ve farklı standartlar arası uyumsuzluk sebebi ile ortaya çıkan iletişim sorununu ortadan kaldırmak hedeflenmiştir. OSI referans modelinde, iki iletişim sistemi arasında yapılacak olan iletişim problemini çözmek için 7 katmanlı bir ağ sistemi önerilmiştir. Bir başka şekilde, bu temel problem 7 adet küçük probleme bölünmüş ve her bir problem için ayrı ayrı bir çözüm yaratılmaya çalışılmıştır. OSI modeli, bir platformda çalışan uygulama programının, iletişim ortamı üzerinden başka bir platformda çalışan diğer bir uygulama programı ile olan iletişiminin tüm adımlarını tanımlar. En üst katmanda görüntü ya da yazı şeklinde yola çıkan bilgi, alt katmanlara indikçe makine diline dönüşür ve sonuç olarak 1 ve 0'lardan ibaret elektrik sinyalleri halini alır.

OSI başvuru modelinin katmanları, uygun katmanlara arayüz oluşturmakla tasarlanmıştır. Örneğin, sunum katmanı, uygulama ve oturum katmanları arasında arayüz oluşturmak için tasarlanmıştır. Her katmanın, diğer katmanlardan bağımsız belirgin işlevleri vardır. Bu da iletişim sisteminin bölünmesine izin verir. Böylece ağ mimarisi tasarım işlerliği her katmanda değişik problemlerin tutulmasına izin verir. Aşağıda Şekil 2.3'te OSI modeli katmanları, veri akış yönleri belirtilerek gösterilmiştir [8, 2, 17]. Burada, tüm sistemin karmaşıklığı belirli süreçlere (katmanlara) bölünerek daha kolay anlaşılabilir bir yapıya dönüşür. Bu katmanlı ağ mimarisi sayesinde, bir çok fiziksel aygıt arasındaki iletişim doğal olarak bazı süreçlere bölünür. Bu yüzden, OSI'nin gelişi her türden cihazın, bilgisayarın birbiri ile iletişimi sorununa çözüm getirmektedir. OSI modelinin yedi katmanı vardır (Bkz. Şekil 2.3).



Şekil 2.3. OSI modeli

2.3.1. Uygulama katmanı (Application layer)

OSI'deki en üst katmandır ve kullanıcıların, programların ağı kullanabilmesi için araçlar sunar. En üst katman yani son katman olduğundan diğer katmanlara herhangi bir hizmet sunmaz. Çalıştırılan uygulamalar için ağ hizmetlerini oluşturur dolayısıyla, kullanıcıya en yakın katmandır. Kullanıcı uygulamalarına dosya aktarım, elektronik mektuplaşma, uzaktan dosya erişimi, ağ yönetimi, terminal protokolleri gibi standartlar geliştirilmiştir. Ayrıca uygulamaların birbirleriyle iletişimini kontrol eder. Diğer bilgisayarlar ile haberleşen bir uygulama, OSI uygulama katmanı kavramlarını kullanıyor demektir. Uygulama katmanındaki uygulamaların haberleşme yetenekleri bulunmalıdır [17].

OSI'de uygulama katmanının kullandığı bazı uygulamalar şunlardır; telnet, üstmetin aktarım protokolü (HTTP–hypertext transfer protocol), dosya aktarım protokolü (FTP–file transfer protocol), ağ dosya yönetim sistemi (NFS –network file system), basit elektronik posta aktarım protokolü (SMTP – simple mail transfer protocol) [4].

2.3.2. Sunum katmanı (Presentation layer)

Ağ'da paylaşılan verinin karşı noktada anlaşılır bir sunuma getirilmesini sağlamaktadır. Paylaşılan verinin okunabilmesi için verinin ortak bir formata dönüştürülmesi gerekmektedir. Sunum katmanı, veriyi karşı nokta tarafından okunabilir hale getirmekten sorumlu olan katmandır. Gönderilen verinin karşı nokta tarafından nasıl okunacağını belirtir. Verinin biçimlendirilmesi, şifrelenmesi ve sıkıştırılması gibi görevleri üstlenir. Sunum katmanındaki bazı iletişim formatları örnek vermek gerekirse, GIF, DIVX, FM7, DOC, EBCDIC, TIFF, JPEG, PICT, MPEG, MIDI gibi standartlar olabilir.

2.3.3. Oturum katmanı (Session layer)

Uygulamalar arasındaki oturumların başlatıldığı, sonlandırıldığı ve yönetildiği katmandır. Oturum katmanı eşzamanlı olarak iletişimi sağlar. Oturum katmanı,

oturum (session) olarak adlandırılan konuşmaların nasıl başlayacağını, biteceğini ve kontrol edileceğini tanımlar. Bu, birden çok iki yönlü mesajın idare ve kontrol edilmesini de kapsar. Bu sayede uygulama, sadece belli mesaj dizisinin iletilmesi tamamlandığında, gerekli işlemleri yapmaya başlar. Oturum katmanının, gelen verinin kesintisiz bir görüntüsünü elde edebilmesini de, bu sağlar. Örneğin, otomatik para çekme makinelerinde siz parayı almadan, oturum katmanı, hangi işlemlerin aynı oturumun parçası olduğunu ve oturumun kapatılabilmesi için hangi işlemlerin tamamlanması gerektiğini belirleyebilir.

2.3.4. Taşıma katmanı (Transport layer)

Birincil görevi iletişimin olduğu noktalar arasındaki veri akışının kontrolü ve verinin karşıya ulaştığından emin olmaktır. Alıcı olan noktanın veriyi almaya hazır olup olmadığı ve veri gönderildikten sonra alıp almadığı gibi kontrollerin yapıldığı katmandır. Burada, gelen bilginin doğruluğu araştırılıp, hatalıysa düzeltilmesine çalışılır. Bu katman güvenilir bir dağıtımdan sorumludur. Daha çok paket dağıtım sunumunu garantilemeye çalışan taşıma katmanı veri dağıtmayı garantiler. Eğer "veri paketi" olarak anılan paket dağıtılmayabilir ise istekte bulunan sunucuya gecikmenin olacağını bildiren bir ileti gönderilir. Dağıtımı garantilemek için kullanılan yöntemler arasında, bilgilendirme iletileri, akış denetimi ve veri paketlerine atanan paket sıra numaraları yer alır. Bu katman iletinin doğru olarak dağıtıldığını garanti etmez. Sadece dağıtıldığını garanti eder. Düzeltmeye gereksinimi olan bir ileti varsa onu yeniden belirlemek ve yeniden göndermek sunum ve oturum katmanının sorumluluğudur.

Hata giderme imkânı sunan ya da sunmayan protokollerin seçimine imkân saglar. Gelen veriyi, aynı makine üzerindeki farklı uygulamalara (örneğin, TCP soketlerine) göndermek için çoğullama da bu katmanda yapılır. Sırayı bozan bir paket alındığında, paketin yeniden istenmesi de yine bu katmanda gerçekleştirilir. TCP/IP ve UDP bu katmanda çalışan en bilindik protokollerdir [17].

2.3.5. Ağ katmanı (Network layer)

Bu katman, paketlerin uçtan uca gönderimini tanımlar. Ağ katmanı veriyi ağa yerleştirmekten sorumludur. Ağ katmanı bunu yapabilmek için, uç noktaların belirlenmesinde kullanılmak üzere mantıksal adresleme yapar. Bu katman sunucu adres alanından kaynaklanan iletileri düzeltir ve daha ileri geçirir. Yönlendirme işleminin yapıldığı katmandır. Yönlendirme işlemi, iletinin uzaklara erişmesi için en kısa ve en iyi yolun bulunmasıdır. Bilginin aktarılacağı yolun bulunması bir hesaplamaya dayanmaktadır. Sınanan ileti bir sunucu için ise daha ilerde işlenmek üzere taşınma katmanında tutulur. Farklı ortamlarda, iletilebilecek maksimum veri miktarının farklı olmasından dolayı yaşanan sıkıntıları gidermek amacıyla, bir paketi daha küçük paketlere bölme işlemi de bu katmanda tanımlanır. IP, IPX, OSPF gibi protokoller bu katmanda çalışan protokollerdir.

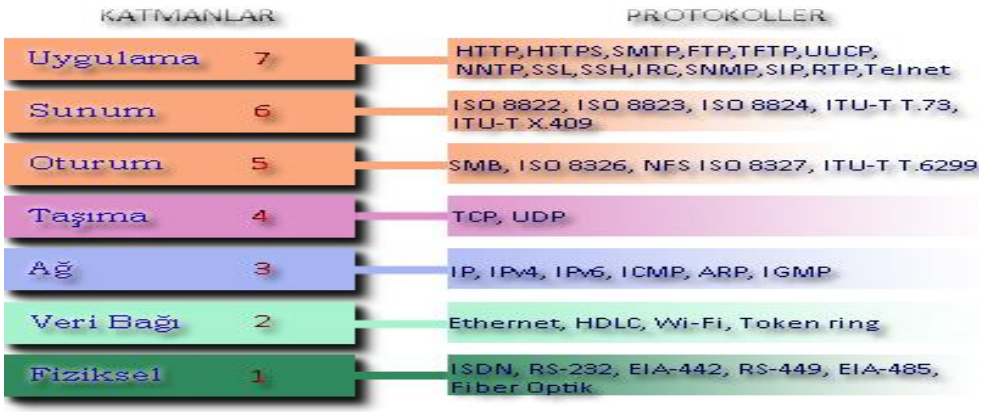
2.3.6. Veri bağı katmanı (Data link layer)

Gönderilecek verinin elektriksel sinyallere dönüştürülüp kabloya iletilmesini ve kablodan gelen elektriksel sinyallerin veriye dönüştürülmesini sağlayan katmandır. Bu dönüştürme işlemi kullanılan ağ teknolojisine göre değişkenlik gösterebilir. Elektriksel sinyallerin kablo üzerinde sorunsuz bir şekilde ilerleyip ilerleyemediğinin kontrolü bu katmanda yapılır. Ayrıca bu katmanda fiziksel adresleme yapılır. Fiziksel katmandan gelen bir dizi 0'lar ve 1'ler çerçeve ve paketlere dönüştürülür. Çerçeveler ve paketler, iletilerin kaynak ve varış adresleri, gerçek ileti daha sonraki katmanlarda istenen herhangi bir denetim bilgisini içerir. Veri Bağı katmanı veriyi fiziksel katmana göndermeden önce özel denetim bilgilerini ekler ve bu bilgileri veriyi ağ katmanına göndermeden önce bilgiden soyar alır. Veri bağı katmanında bazı hata düzeltme işleri yapılır. Döngüsel Yineleme Sınaması (CRC-Cyclic Redundancy Check) Hata Düzeltme Kodu (ECC-Error Correction Codes) ile bit hatası yakalanır, düzeltilir. Ethernet protokolü bu katmanda da çalışmaktadır [8].

2.3.7. Fiziksel katman (Physical layer)

Veri bağı katmanı tarafından elektronik sinyallere dönüştürülen verinin taşınmasın dan sorumludur. Gerçek kablolama ile verinin konulması ve alınmasının yapıldığı katmandır. Fiziksel kablolama ve elektriksel sinyallerin ayrıntıları burada tutulur. Bu ayrıntılardan bazıları; kullanılan konnektör bağlayıcı tipi, kullanılan ortamın tipi (eşeksenli, bükülmüş tel çifti veya fiber optik gibi) ve bant genişliğidir. Bu katman duvarlar boyunca koşan kablolar, her bilgisayarın arkasında yer alan bağlayıcılar ve elektriksel sinyallerin özellikleri ile ilgilidir.

OSI modelinde her katmanda çalışan protokoller aşağıdaki Şekil 2.4'te gösterilmiştir.



Şekil 2.4. OSI modelinde protokoller

2.4. Veri Haberleşmesinde Önemli Kavram ve Standartlar

Veri haberleşmesinin tarihsel gelişimine paralel olarak bir çok önemli kavram ve standardlar oluşturulmuştur. Bunların hepsinden değil, sadece gerçekleştireceğimiz projede işimize yarayacak olan bazı önemli kavramlardan aşağıda bahsedeceğiz

2.4.1. Ethernet kavramı

Tarihsel olarak ethernet protokolünün gelişimine bakarsak, ilk olarak Xerox Palo Alto Research Center (PARC)'da, 1976'da geliştirilmiştir. Ethernet, 1980'de ise ilk

olarak yayınlanan Elektrik Elektronik Mühendisleri Enstitüsü (IEEE-Institute of Electrical and Electronics Engineers) 802.3 standardına teknolojik olarak temel sağlamıştır. Bundan kısa bir süre sonra, Digital Equipment Corporation, Intel Corporation, ve Xerox Corporation beraberce IEEE 802.3 ile uyumlu bir Ethernet (sürüm 2.0) standardını geliştirdiler ve duyurdular. Ethernet ve IEEE 802.3, birlikte, şu anda yerel ağ protokolleri pazarında en büyük pazar payına sahiptir. Bugün Ethernet terimi genel olarak IEEE 802.3'ün de dahil olduğu Ethernet standartlarına uyan tüm Taşıyıcı Sinyalin Algılanması, Çoklu Erişimce Çarpışmanın Tespiti (CSMA/CD-Carrier Sense Multiple Access/Collision Detection) ağları için kullanılır [11, 19].

İlk geliştirildiğinde ethernet, uzun mesafeli düşük hızlı ağlar ve özel yüksek hızlı veri taşıyan, ancak mesafe kısıtlaması olan veri odası ağları arasındaki boşluğu doldurmak için tasarlanmıştı.

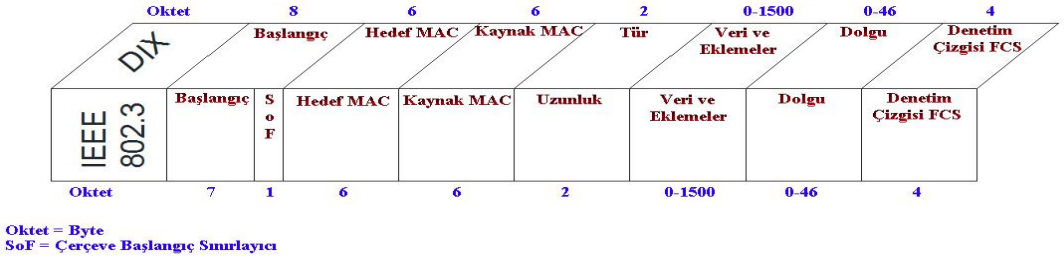
Ethernet, yerel haberleşme ortamının dağınık bazen yüksek oranda ağır trafik taşıması gereken uygulamalar için uygundur. Ethernet veriyi elektrik sinyaliyle kodlar. 10 Mbps (Megabit per second-Saniyede Bir Milyon Bit) sistemlerde kodlama biçimine Manchester kodlaması denir. Bu sistem voltajda değişiklik yaparak ikilik sayıları sıfır ve bir olarak gösterir. Bir zaman diliminde voltajdaki artış ya da düşüşe bit periyodu denir, bitin ikili sayı değerini gösterir.

Ethernet'ler, kullanılan kablo ve iletişim hızlarına göre ayrıca sınıflandırılırlar. 10 Mbps hızıyla haberleşenler genel olarak Ethernet, 100 Mbps hızıyla haberleşenler Fast Ethernet, 1000 Mbps hızıyla haberleşenler Gigabit Ethernet olarak isimlendirilirler.

Çizelge 2.1 Ethernet standartları, kablo tür ve mesafeleri verilmiştir [5].

Standart İsmi	Tanımı	Tarihi	Band Genişliği	Maksimum Mesafe	Kullanılan Kablo
IEEE 802.3	10Base-5 (Thicknet)	1985	10Mbps	500 metre	50 ohm sonlandırıcı kalın koaksiyel kablo
IEEE 802.3a	10Base-2 (Thicknet)	1986	10Mbps	185 metre	50 ohm sonlandırıcı ince koaksiyel kablo
IEEE 802.3j	10Base-T	1991	10Mbps	100 metre	Cat 3,Cat 4, Cat 5 UTP
IEEE 802.3j	10Base-F	1994	10Mbps	2 km	Fiber Optik
IEEE 802.3u	100Base-TX	1995	100Mbps	100 metre	Cat 5UTP veya Type 1 STP
IEEE 802.3u	100Base-T4	1995	100Mbps	100 metre	Cat 3,Cat 4,Cat 5 UTP
IEEE 802.3u	100Base-FX	1995	100Mbps	450 metre- 2 km	Fiber Optik
IEEE 802.3z	1000Base-LX	1998	1000Mbps	440 metre- 3 km	Single Mod veya Multi Mod Fiber Optik Kablo
IEEE 802.3z	1000Base-SX	1998	1000Mbps	260-550 metre	Multi mod Fiber Optik Kablo
IEEE 802.3z	1000Base-CX	1998	1000Mbps	25 metre	Bakır Kablo
IEEE 802.3ab	1000Base-T	1999	1000Mbps	100 metre	Cat 5 UTP
IEEE 802.3ae	10GBase-xR	2003	10Gbps	26 metre- 80 km	Single Mod veya Multi Mod Fiber Optik Kablo
IEEE 802.3ae	10GBase-xW	2003	10Gbps	26 metre- 80 km	Single Mod veya Multi Mod Fiber Optik Kablo
IEEE 802.3an	10GBase-T	2006	10Gbps	100 metre	Cat 6 UTP veya STP

Ethernet ağ cihazlarına, 48 bitlik, onaltılık sayı düzeninde ve bir eşi daha olmayan seri numarası verilir. LAN içerisindeki yerel erişimler bu adresler kullanılarak gerçekleşir. Bu numaralar, üretici firmalar tarafından fabrikada verilmektedir. Örnek olarak 12:34:56:78:90:AB bir *MAC (Media Access Control - Ortam Erişim Kontrol)* adresidir. Her üretici firmanın kendi ürünleri için kullanabileceği belli bir MAC adresi alanı vardır. Ethernet çerçeve yapısı Şekil 2.5'te gösterilmiştir.



Şekil 2.5. Ethernet yapısı

2.4.2. Taşıyıcı sinyalin algılanması, çoklu erişimce çarpışmanın tespiti (CSMA/CD -Carrier sense multiple access/collision detection)

CSMA/CD ethernet'te veri iletim yoluna erişmek (fiziksel ortama giriş) için kullanılan tekniktir. Ethernet, bir tüme gönderim (broadcast/yayın ağ) teknolojisidir. Bu teknik veri iletim yoluna bağlı tüm birimlerin ağ ortamına erişmesini sağlar. Sadece bir düğüm belli bir zamanda ağı kullanmaya elverişlidir. Bu kavramda bir istasyon ağa bir çerçeve iletmek istediğinde ağın başka bir istasyon tarafından kullanılmadığından emin olmalıdır. Veri iletim yolu, bağlı olan tüm birimlerin veri aktarımına açık olduğu için aynı anda farklı birimler tarafından veri aktarılmaya çalışılması, çarpışmaya (collision) neden olur. Çarpışma durumunda tüm veriler bozulur ve yeniden aktarılması gerekir. Bu nedenle veri gönderen bir düğümün aktarım sonrası hattı dinlemesi ve olası çatışmaların farkına varması gerekir. Çarpışma denetimi, veri aktarmak isteyen her iki istasyonun benzerliğini fark eder ve eş zamanlı olarak ağın boş olduğunu tespit edebilir.

Her iki istasyon da ağa çerçeve gönderdiğinde milisaniyeler sonra her iki çerçeve çarpışır. Çarpışmalar ethernet'te normal olaylardır. Böyle bir çarpışma olduğunda iki istasyon da taşımayı durdurur rastgele bir gecikmeden sonra çerçeveyi yeniden gönderir. Gecikmenin rastgele olması önemlidir, aksi takdirde aynı çarpışma çok kez ortaya çıkacaktır. Her iki bilgisayar da çatışmayı sezince, veri aktarımına bir süre ara verip, ikili üssel geri çekilme (binary exponential backoff) algoritmasını kullanılarak iletimi tekrarlarlar. Ethernet'te kullanılan CSMA/CD, veri çerçevelerini alır ve taşır, veri çerçevelerini OSI üst katmanına geçirmeden önce çözer, adreslerin geçerliliğine bakar ve ağda ya da veri çerçevesinde oluşan hataları tespit eder [19].

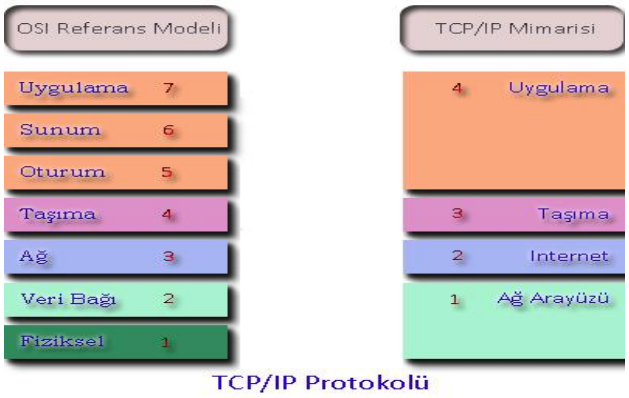
2.4.3. İletim kontrol protokolü/internet protokolü (TCP/IP Transmission control protocol/internet protocol)

TCP/IP birçok küçük protokolden oluşur. Adını en çok bilinen ikisinden (TCP ve IP) alır. TCP/IP protokol kümesinde yaklaşık 100 protokol bulunur. Birçoğu, IP paketlerinin alt katman protokollerine nasıl taşınacağını gösterir. Setteki anahtar

protokoller iletim kontrol protokolü (TCP), internet protokolü (IP) ve kullanıcı datagram protokolü'dür (UDP- User Datagram Protocol). TCP/IP ilk günden beri yerel alan ağları, yerel ve geniş alan ağları bağlantısı, bilgisayar ağı yönetimi ve bilgi servisi sağlanması gibi yeni ortaya çıkan konulara hitap etmektedir. Bu protokol kümesi akla gelebilecek her tip bilgisayara destek vermektedir. TCP/IP'nin kaynak kodu genel ortamda bulunup, kullanımı teşvik edilmektedir.

TCP katmanı komutların karşı tarafa ulaştırılmasından sorumludur. Karşı tarafa ne yollandığı ve hatalı yollanan verilerin tekrar yollanmasının kayıtlarını tutarak gerekli kontrolleri yapar. Eğer gönderilecek veri bir kerede gönderilemeyecek kadar büyük ise TCP onu uygun boydaki bölütlere (segment) böler ve bu bölütlerin karşı tarafa doğru sırada, hatasız olarak ulaşmalarını sağlar. TCP ayrı bir katman olarak çalışmakta ve tüm diğer servisler onun üzerinde yer almaktadır. Böylece yeni bir takım uygulamalar da daha kolay geliştirilebilmektedir. Üst seviye uygulama protokollerinin TCP katmanını çağırmaları gibi benzer şekilde TCP'de IP katmanını çağırmaktadır. Ayrıca bazı servisler TCP katmanına ihtiyaç duymamakta ve bunlar direk olarak IP katmanı ile görüşmektedirler.

Belirli görevler için belirli hazır yordamlar oluşturulması ve protokol seviyeleri inşa edilmesi stratejisine katmanlaşma adı verilir. En genel haliyle TCP/IP uygulamaları da 4 ayrı katman kullanır. Uygulama katmanı altında sırasıyla taşıma, yönlendirme ve fiziksel katman yer alır. Taşıma katmanında TCP ve UDP protokolleri, yönlendirme katmanında IP, internet kontrol mesajı protokolü (ICMP-Internet Control Message Protocol), Adres Çözümleme Protokolü (ARP-Address Resolution Protocol) tanımlıdır. Fiziksel katman için var olan tanımlar (ethernet) geçerlidir. Şekil 2.6'da TCP/IP mimarisinin OSI sistemindeki karşılaştırması verilmiştir.



Şekil 2.6. TCP/IP mimarisi ve OSI modeli karşılaştırması

2.4.4. Uygulama katmanı protokolleri

Uygulama katmanı, SMTP, HTTP, FTP, Telnet gibi protokoller üstünde bulunan programlara hizmet verirler.

2.4.5. Taşıma katmanı protokolleri

TCP/IP'de ulaşım katmanı için TCP ve UDP olarak adlandırılan iki protokol tanımlıdır. TCP bağlantılı düzene dayalı protokoldür. Bağlantılı düzende, gönderici ve alıcı iletişim başlamadan önce birbirleriyle anlaşırlar. İki taraf iletişim yapma konusunda istek ve onaylarını birbirlerine gönderirler. UDP ise bağlantısız düzenli basit bir protokoldür. Bu protokolde iletişim başlamadan önce gönderici ve alıcının bir anlaşmaya varmalarına gerek yoktur [16].

a. İletim kontrol protokolü (TCP-Transmission control protocol)

TCP, şu fonksiyonları gerçekleştirmektedir:

- Çoğullama (multiplexing),
- Hata giderme (güvenilirlik),
- Pencere kaydırma (windowing) kullanarak akış kontrolü,
- Bağlantı kurulması ve bağlantının sonlandırılması,
- Veri aktarımı.

Çoğullama: Gelen verinin hangi uygulamaya verileceğine karar verilme sürecidir. Uygulama katmanı ile taşıma katmanı protokolleri arasında port olarak adlandırılan bir geçit tanımlıdır. Her portun 16 bitlik bir numarası vardır ve her uçta 216 adet port tanımlıdır. 16 bitlik port no, bir iletim kontrol protokolü ve 32 bitlik IP adresi soketi oluşturur. Port numaraları 1 ile 65536 arasında yer alır. TCP ve UDP her biri 65,536 portu kullanmıştır. Cihazlar, port numaralarını 1024'ten başlayarak dinamik olarak tahsis ederler. Yaygın olarak bilinen port numaraları (1–1024) sunucular tarafından kullanılır. FTP, Telnet sunucular gibi, bir hizmet sağlayan uygulamalar, yaygın olarak bilinen bir portu kullanarak bir soket açarlar ve bağlantı isteklerini dinlerler. İstemcilerin yaptığı bu bağlantı istekleri hem kaynak hem de hedef port numaralarını içermek zorundadır ve sunucular tarafından kullanılan port numaraları yaygın olarak bilinen portlar olmak zorundadır. 0 ve 255 arası port numaraları, 20 standart uygulama katmanı hizmetlerine erişim için ayrılmıştır. Port numaraları birden fazla uç-nokta bağlantısı için kullanılabildiğinden, kullanıcılar bir port kaynağını eşzamanlı olarak paylaşabilir [20].

Hata Giderme: TCP güvenli veri aktarımı sağlar. Bu amaçla TCP başlığı içindeki sıra ve onay numaralarını kullanarak veri baytlarını numaralandırır. Her iki doğrultuda da güvenlik sağlar. Bunu bir doğrultuda sıra numarası (squence number) alanını ve diğer doğrultuda onay alanını (acknowledgement field) kullanarak sağlar.

Pencere kaydırma (windowing) kullanarak akış kontrolü: TCP akış kontrolünü TCP başlığındaki sıra ve onay numaralarının yanında pencere (window) alanını kullanarak gerçekleştirir. Pencere alanı, TCP penceresinde ne kadar alan olduğunu gösterir. Alış denetimi için kullanılır. 16 bitliktir. Herhangi bir anda izin verilen onaylanmamış en fazla bayt sayısını belirtir. Pencere küçük olarak başlar ve hatalar oluşana kadar büyür. Ağ performansına bağlı olarak yukarı veya aşağıya doğru kayar. Pencere dolu olduğunda, gönderici veri göndermez. Böylelikle veri akışı kontrol edilir. Pencere alanı alıcı tarafından, göndericiye bir sonraki onayı almak için durup beklemeden önce ne kadar veri gönderebileceğini söylemek için kullanılır. Diğer TCP özelliklerinde olduğu gibi, pencere kaydırma simetriktir. Her iki tarafta alır ve gönderir. Pencere kaydırma tüm durumlarda göndericinin iletim yapmayı

durdurmasını gerektirmez. Pencere dolmadan önce bir onay alınırsa, yeni bir pencere başlar ve gönderici o pencere dolana kadar veri göndermeye devam eder.

Bağlantı kurulması ve bağlantının sonlandırılması: TCP bağlantısı, diğer özellikleri çalışmaya başlamadan önce kurulur. Bağlantı kurulması, sıra ve onay alanlarına ilk değerlerin atanması ile kullanılacak port numaraları üzerinde anlaşma sürecidir.

Veri aktarımı: TCP, kaybolan segmentleri yeniden gönderir ve sıralı olarak iletilmemiş segmentleri sırasına koyar. Böylelikle yeniden iletim yapılmasına gerek kalmaz [20].

b. Kullanıcı datagram protokolü (UDP-User datagram protocol)

UDP (User Datagram Protocol), TCP / IP protokol grubunun iki taşıma katmanı protokolünden birisidir. Gelişmiş bilgisayar ağlarında paket anahtarlamalı bilgisayar iletişiminde bir datagram modu oluşturabilmek için UDP protokolü yazılmıştır. Bu protokol minimum protokol mekanizmasıyla bir uygulama programından diğerine mesaj göndermek için bir yordam içerir. Bu protokol hareket yönlendirmelidir. Paketin teslim garantisini isteyen uygulamalar TCP protokolünü kullanır. Geniş alan ağlarında (WAN) ses ve görüntü aktarımı gibi gerçek zamanlı veri aktarımlarında UDP kullanılır. UDP bağlantı kurulum işlemlerini, akış kontrolü ve tekrar iletim işlemlerini yapmayarak veri iletim süresini en aza indirir. UDP ve TCP aynı iletişim yolunu kullandıklarında UDP ile yapılan geçek zamanlı veri transferinin servis kalitesi TCP'nin oluşturduğu yüksek veri trafiği nedeniyle azalır. UDP güvenilir olmayan bir aktarım protokolüdür. UDP protokolü ağ üzerinden paketi gönderir ve gidip gitmediğini takip etmez ve paketin yerine ulaşıp ulaşmayacağına onay verme yetkisi yoktur. UDP protokolünü kullanan programlara örnek olarak 161 no'lu portu kullanan SNMP servisini verebiliriz.

c. UDP ile TCP 'nin farkları

UDP, gönderilen paketin yerine ulaştığını kontrol etmediğinden güvenilir bir protokol değildir. User Datagram Protocol'ün TCP' den farkı sorgulama ve sınama amaçlı, küçük boyutlu verinin aktarılması için olmasıdır; veri küçük boyutlu olduğu için parçalanmaya gerek duyulmaz. UDP protokolü ağ üzerinde fazla bant genişliği kaplamaz. UDP başlığı TCP başlığına göre daha kısadır. Aktarım katmanında UDP'nin oluşturduğu veri bütününe "*datagram*", TCP'nin oluşturduğu veri bütününe "*segment*" adı verilir. İkisi arasındaki temel fark, segmenti oluşturan veri grubunun başında sıra numarası bulunmasıdır. Her bir datagram veya segment IP tarafından kendi başlığı eklenerek IP paketi haline getirilir ve her bir IP paketi birbirinden bağımsız olarak hedef cihaza gönderilir. UDP kullanmanın en önemli nedeni az protokol yüküdür. Video sunucu gibi gerçek zamanlı veri akışı gerektiren bir uygulama için TCP fazla yük getirir ve görüntü gerçek zamanlı oynamaz. Bu nedenle çoğa gönderim (multicast) uygulamalarında datagram soketler kullanılır. Ayrıca video ve ses görüntülerinde genelde az bir veri kaybı sesi veya görüntüyü bozmaz. Bu nedenle sıkı paket kontrolüne gerek yoktur. Eğer iyi bir fiziksel bağlantınız varsa hata oranı düşük olacaktır ve bu nedenle TCP'nin yaptığı hatalı paket kontrol işlemleri fazladan yük olacaktır.

2.4.6 Ağ katmanı protokolleri

Yönlendirme katmanında, tanımlı protokolleri bir üst katmandan gelen segmentleri alıcıya, uygun yoldan ve hatasız ulaştırmakla yükümlüdür. Aşağıda bu katmanda çalışan bazı protokollere yüzeysel olarak değinilmiştir.

i. Adres çözümleme protokolü (ARP–Address resulotion protocol)

Adres Çözümleme Protokolü (ARP), her tür yayın ağında kullanılabilen OSI birinci katman adresleri ikinci katman adreslere çözümleyen, ikinci katmana ait genel bir protokoldür. Terminaller, yerel alan ağına dahil olduklarında ağ içindeki diğer terminallerle veri alışverişinde bulunabilmek için ARP paketleri yayınlarlar.

Bu paketler, ağa dahil olan tüm terminallere ulaşır ancak hedef IP adrese sahip olan terminal bu pakete cevap verir. Yerel ağlarda bir IP paketi gönderebilmek için veri bağı katmanı başlığı ve kuyruğu yaratılmalıdır. Bu yeni başlıktaki kaynak MAC adresi bilinmekte ancak, hedef MAC adresi bilinmemektedir. ARP, IP'nin hedef MAC adresini bulmak için kullandığı metottur.

ii. Internet kontrol mesajı protokolü (ICMP-Internet control message protocol)

ICMP, TCP/IP' nin işlemesine yardımcı olan bilgilendirme protokolüdür. Her düğümde ICMP protokolü çalışır. Hata durumunda düğüm tarafından geri bilgilendirmeyi sağlar. Şu amaçlarla kullanılır;

- Ömür (TTL - time to live) süresi dolduğu zaman paketin sahibine bildirim yapmak,
- Herhangi bir durumda yok edilen paket hakkında geri bildirim sağlamak,
- Parçalanmasın komutu verilmiş paket parçalandığında geri bildirim sağlamak,
- Hata oluşumlarında geri bildirim sağlamak,
- Paket başka bir yoldan gideceği zaman geri bildirim sağlamak,

Güvenilir bir veri dağıtım protokolü değildir. Ortama geri besleme sağlar, IP' yi güvenilir bir protokol haline sokar. IP paketinin veri bölümünde taşınır.

iii. Internet protokol-IP (Internet protocol)

Temel olarak datagram paketleri için bir iletim yolu belirleme işlevini yerine getirir. IP'nin sağladığı fonksiyonlar şunlardır ;

- Global adresleme yapısı,
- Servis isteklerini tiplendirme,
- Paketleri iletim için uygun parçalara ayırma,
- Hedef alıcıda paketleri tekrar birleştirmedir.

TCP, hedef bilgisi bulunan segmenti IP'ye verir. IP bu segmenti alır herhangi bir diğer datagram veya segmentten önce veya sonra hedef düğüme iletim için bir yol belirler. Her bir datagram veya segment IP tarafından kendi başlığı eklenerek IP paketi haline getirilir ve her bir IP paketi birbirinden bağımsız olarak hedef düğüme gönderilir. Paketler üzerinde çok sınırlı hata kontrolü vardır. IP 16 bitlik başlık hata kontrolü (checksum) sağlar. Bu IP paketini alan düğümün IP başlığında bir bozulma oluşup oluşmadığını kontrol etmesini sağlar. Onay (acknowledge) mekanizması kullanmaz. Verinin internet katmanına bozuk ulaştığını değerlendirip yeniden gönderimi sağlayabilecek fonksiyona sahip değildir. Bu görev bir üst katmandaki TCP'de yapılır, TCP'nin kullanılmadığı durumlarda daha üst katman protokollerince yerine getirilir. Akış kontrol ve paket sıralama mekanizmalarına sahip değildir. IP bağlantısız paket dağıtım servisi sunar

2.4.7. Fiziksel katman

Fiziksel katman, veri bağı ve fiziksel ortamı içermektedir . OSI referans modelindeki birinci ve ikinci katmanların görevlerini yerine getirir. Fiziksel katman için bir protokol tanımlanmamıştır. Ethernet bağlantısı, modem üzerinden çevrimiçi bağlantı ve var olan fiziksel bağlantı türlerini kullanmaktadır. Uç sistemde TCP/IP modülünün çalışması yeterlidir.

2.4.8. IP adresleme

TCP/IP kullanılan ağlarda, adresleme IP adreslere dayanılarak gerçekleştirilir. Ağda bulunan iletişim kuracak her cihaza bir IP adresi atanır, diğer cihazlar bağlantı kurmak için bu adresi kullanır. IP adresleri şu anda yaygın kullanımda olan IP sürüm 4 (IPv4) için 32 bit boyunda olup, noktalarla ayrılmış 4 adet 8 bitlik sayıyla gösterilirler. Ağ katmanında paketler bir noktadan diğer noktaya iletilirken mantıksal adresler kullanırlar. Mantıksal adresler paketin kaynak ve gideceği en son yerin (hedefin) ağ adresini içerir. Adres alanı içinde varış noktasının ağ adresi ile düğüm adresi bileşimi bulunur. Adres uzunluğu 32 bittir. 232 adet IP adresi içerir, bu durumda örneğin, 4.294.967.296 bilgisayar internete bağlanabilir. IP adresleri,

bilgisayar ağlarını bölümlemek ve farklı büyüklüklerde bilgisayar ağları oluşturmak üzere sınıflandırılmıştır. IP, 5 farklı adres formatını destekler, bunlar; A, B, C, D ve E sınıfı adreslerdir. Her adres sınıfı o adresi tanımlayan ilk baytın en anlamlı bitlerine yerleşen bir bit dizisi ile tanımlanır. Bu bit dizisini A, B, C sınıfı adreslerde ağ adresi ve sonrasında düğüm adresi takip eder.

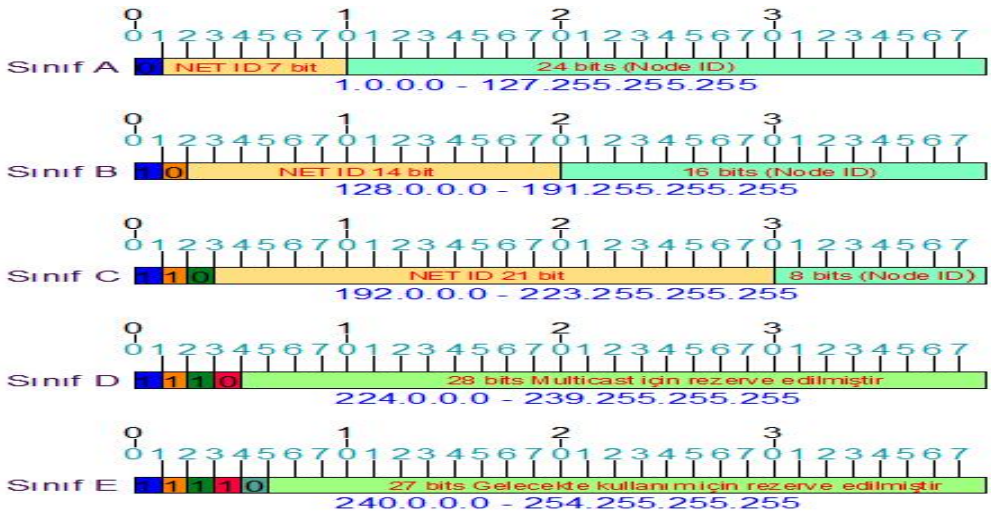
A sınıfı adreslerde ilk bayt ağı tanımlamak için kullanılır. İlk bit 0'dır. Ondan sonraki 7 bit ağ adresini oluşturur. Geri kalan 24 bit ağdaki host (makine) sayısını belirler. 224-2 ile her biri 16.777.214 adet bilgisayar içeren 126 adet altağ (subnet) kullanılabilir. Host bitlerinin tamamı 1 olan adresler yayın (broadcast) ve 0 olanlar ise ağ adresi olarak kullanılır. 27-2 ile 126 olan altağ sayısı hesaplanır. 0.0.0.0 adresi varsayılan yönlendirme 127.0.0.0 adresi ise yerel çevrim için kullanılır. İlk sekizli aralığı 1–126, geçerli ağ numaraları 1.0.0.0 – 126.0.0.0'dır.

B sınıfı IP adreslerinde ilk iki bayt, ağ adresini tanımlar ve bu iki byte'ın ilk iki biti adres sınıfını belirler, kalan diğer 14 bit ağ adresini oluşturur. Sonraki 16 bit ağda olabilecek host sayısını belirler. B sınıfı, 128.0.0.0 ve 191.254.0.0 adres aralığını kullanılır [14].

C sınıfı adreslerde ilk üç bayt ağı tanımlar. İlk üç bit (110) adres sınıfını belirler ve diğer 21 bit ağ adresini oluşturur. Kalan 8 bit ağdaki host sayısını belirler. 254 adet bilgisayar içeren 2.097.152 altağa izin verilir. 192.0.1.0 ve 223.255.254.0 aralığı kullanılır.

D sınıfı adresler multicast adresleme için kullanılır. İlk dört biti 1110 şeklindedir. 224.0.0.0 – 239.255.255.255 adresleri kullanılır.

E sınıfı adresleme yedek olarak saklı tutulmaktadır. İlk dört biti 1111 şeklindedir. Yerel ağlarda kullanılmak üzere 10.0.0.0, 172.0.0.0 ve 192.168.0.0 ağ adresleri saklı tutulmuştur. Şekil 2.7'de bütün bu sınıflandırmalar gösterilmiştir.



Şekil 2.7. IP adres sınıfları yapısı

IPv4 (32 bit) ve IPv6 (128 bit) olmak üzere iki çeşit IP adresi vardır. Günümüzde yaygın olarak 32 bitlik (IPv4) adresleme mekanizması kullanılmaktadır. İnternetin yaygınlaşması ve IPv4 adreslerinin çok hızlı tükenmesi ile birlikte IPv6 adreslerinin kullanılmasına yönelim hız kanacaktır. IPv6 işlevselliği, kullanım kolaylığı sayesinde büyük faydalar sağlayacaktır [15].

2.4.9. Ağ maskesi

Alt ağ oluşumu ağ üzerindeki yöneticiye beraber çalıştığı her bir ağ parçasının ölçüsünü belirlemeye imkân verir. Ağ üzerinde kaç segment olduğu bir kere belirlendiği zaman hangi ağda hangi aygıtın açık olduğunu belirlemek için alt ağ maskesini kullanabilirler. Bir nokta, ancak aynı ağda bulunan bir nokta ile doğrudan iletişime geçebilir. Aynı ağda değillerse dolaylı olarak iletişime geçer. Aynı ağda olup olmadığını IP adreslerini kullanarak anlarız. IP adresinin bir bölümü ağı, diğer bölümü de bilgisayarın ağ içindeki adresini tanımlar. Hangi bölümü ile ağı hangi bölümü ile bilgisayarı tanımladığını bilmek için alt ağ maskesi kullanır. Dört bölümden oluşur ve ağ adresinin hangi bölüme kadar geldiğini göstermek için kullanılır. Bilgisayar kendi ağ tanımlayıcılarını bulmak için alt ağ maskesi kullanır. Bu yüzden alt ağ maskesinin doğru şekilde girilmesi gerekir. Yanlış girilirse bilgisayarın diğer bilgisayarlarla iletişimi engellenebilir. Bilgisayar ağ

tanımlayıcısını bulmak için alt ağ maskesini IP adresini ve mantıksal işleminden geçirerek kullanırlar. Mesela, IP adresi:195.134.67.200 olsun ve alt ağ maskesi de 255.255.255.0 olsun. Bilgisayarın bu bilgilere dayanarak bulunduğu ağ tanımlayıcısı yani ağ adresi bulunabilir. IP adresi ile alt ağ maskesi işlemine tabi tutulursa:

195.134.67 .200 = 1100 0011.1000 0110.0100 0011.1100 1000
ve
255.255.255.0 = 1111 1111.1111 1111.1111 1111.0000 0000
Sonuç: 195.134.67. 0 = 1100 0011.1000 0110.0100 0011.0000 0000

İki bilgisayardan oluşan bir ağ olduğu düşünülürse (Bkz Şekil 2.8).

Şekil 2.8. Alt ağ maskesi bulma

Şekil 2.8'de görülen 195.134.67.0 adresli bilgisayarın diğer bilgisayarla iletişime geçmesi için aynı ağda olmaları gerekir. Hedef bilgisayarın aynı ağda olup olmadığını anlamak için bilgisayarların ağ adreslerine bakılır. 195.134.67.200 ve 255.255.255.0 ile işleme koyduktan sonra çıkan sonuç: 195.134.67.0 olacaktır. Bu bilgisayarın kendi ağ adresidir. Hedef bilgisayarın ağ adresi ise: 195.134.67.56 ile 255.255.255.0 ve işleme konularak 195.134.67.0 sonucu görülür. Aynı ağ adresleri çıktığı için bu bilgisayarların iletişime geçeceklerini söyleyebiliriz [15].

2.4.10. Yayın adresi (Broadcast address)

Broadcast bir tüme gönderim şeklidir. Veri ağdaki bütün noktalara gönderilir ve ihtiyacı olan noktalar veriyi kabul eder. Tabiki tüme gönderim şeklinde bir yayın yapıldığından ağda yüksek oranda bant genişliğini genellikle işgal eder. Broadcast adresi, alt ağ yapısına bağlı olarak belirlenir ve aynı ağ üzerindeki her noktada aynı

değerin kullanılması gerekmektedir. Broadcast adresleri duyuru mesajı vermek için kullanılır. Duyuru mesajı genelde bir istasyonun hangi istasyon ile konuşacağını bilemediği bir durumda kullanılan bir mesajlaşma yöntemidir. Örneğin, ulaşmak istediğiniz bir bilgisayarın adı elinizde bulunabilir; ama onun IP adresine ihtiyaç duydunuz, bu çevirme işini yapan en yakın "name server" makinesinin adresini de bilmiyorsunuz, böyle bir durumda bu isteğinizi yayın mesajı yolu ile yollayabilirsiniz. Bazı durumlarda birden fazla sisteme bir bilginin gönderilmesi gerekebilir, böyle bir durumda her bilgisayara ayrı ayrı mesaj gönderilmesi yerine tek bir yayın mesajı yollanması çok daha kullanışlı bir yoldur. Yayın mesajı yollanması biraz da kullanılan ağın fiziksel katmanının özelliklerine bağlıdır. Mesela, bir ethernet ağında yayın mümkün iken noktadan noktaya (point-to-point) hatlarda bu mümkün olmamaktadır. Bazı eski sürüm TCP/IP protokolüne sahip bilgisayarlarda yayın adresi olarak 255 yerine 0 kullanılabilmektedir.

2.4.11. Tek noktaya yayın (Unicast)

Paketin tek bir kaynak istasyondan, tek bir hedef istasyona gönderilmesidir. Türkçe tek yöne yayın olarakta anılmaktadır. Örneğin, genellikle gerçek zamanlı veri taşırken UDP protokolü üzerinden UNICAST yani noktadan noktaya ses iletişimi sağlanmaktadır. Sunucular her bir istemci için ayrı ayrı paket göndermek zorunda kalır. Genellikle TCP ve UDP protokollerini kullanır.

2.4.12. Çok yöne yayın (Multicast)

Paketin tek bir istasyondan, ağda birden fazla hedef istasyona, gruba gönderilmesidir. Örneğin, bir radar verisi, birden çok görüntüleme merkezine aynı anda gruplar belirlenerek gönderilebilmektedir. Grup adresine bir frame iletildiğinde, bu grupta olan bütün cihazlar bu veriyi alacaktır. IP protokolünün 802.3 MAC Alt Katman (802.3 MAC Sublayer) protokolünden itibaren, yani OSI katmanlı yapısının 2. seviyesinden itibaren bu tür bir destek gelmektedir. IP üzerinden çoklu gönderim yapmaya İnternet Çoklu Gönderimi (Internet Multicasting) denmektedir. Radyo yayınları, video konferans gibi bir çok uygulama da çoklu gönderimden

faydalanmaktadır. Böylece var olan ağ alt yapısının daha etkin bir şekilde kullanılması hedeflenmektedir. Çoklu gönderim sisteminde, öncelikle düğüm grupları tanımlanmaktadır. Tüm ağa belirli bir mesajı göndermek yerine, daha önceden tanımlanmış düğüm gruplarına çoklu gönderim sağlanmaktadır

Internet Protokolü (IP), D sınıfı adresleri kullanarak çoklu gönderimi destekler. Bu sınıftaki her adres bir grubu tanımlar IPv4 adreslemede, D sınıfı IP adresleri çoklu gönderim yayınlar için kullanılmaktadır

224.0.0.0/24 çoklu gönderim adresleri yerel ağ (link-local) adreslerdir. Bu adresler için TTL (time to live) değeri 1 olduğundan yerel ağ dışına çıkamayacaktır. Geriye kalan adresler (224.0.1.0 - 238.255.255.255 aralığı) genel kapsam olarak tanımlanmaktadır.

IP seviyesinde çoklu gönderimin sağlanabilmesi için, yönlendirici veya OSI 3.seviye desteği olan data anahtarlarının (switch) çoklu gönderim özelliğini desteklemesi gerekmektedir. Ipv4'de çoklu gönderim (multicast) için IGMP (Internet Group Management Protokol) kullanılmaktadır. Çoklu gönderim sisteminde, öncelikle düğüm grupları tanımlanmaktadır. Tüm ağa belirli bir mesajı göndermek yerine, daha önceden tanımlanmış düğüm gruplarına çoklu gönderim sağlanmaktadır.

Yönlendiriciler, kendi yerel ağlarında bulunan makinelere bir donanım (örneğin OSI 2. seviyesinde) çoklu gönderimi (224.0.0.1 adresine) yaparak onlardan üyesi oldukları grupları bildirmesini isterler. Her istemci de ilgilendiği bütün D sınıfı adresleri yönlendiriciye bildirir. Böylece yönlendirici, kendi yerel ağındaki çoklu gönderim alıcıları hakkında güncel bilgiye sahip olur.

IPv4'de çoklu gönderimin düzgün çalışması için istemci, sunucu ve arasındaki aktif cihazların düzgün bir şekilde ayarlanması gerekmektedir. Bu durumda sistem sorunsuz çalışacak ve ağ trafiği iyileştirilmesi sağlanacaktır.

2.5. Yerel Alan Ağ (LAN) Topolojileri

Yerel alan ağ topolojileri arasında en çok kullanılan 3 topoloji : Ortak yol, halka ve yıldız topolojileridir. Günümüzde en yaygın kullanılan yıldız topolojidir. Bunun sebebi performans, kablolama kolaylığı ve fiyatıdır.

2.5.1. Ortak yol (Bus) topolojisi

Ortak yol topolojisinde tüm iş istasyonlarının üzerinde olduğu bir hat (omurga) mevcuttur. Bütün istasyonlar hattaki tüm mesajları inceler ve kendine ait mesajları alır. Hattaki bilgi akışı çift yönlüdür. Kaynak istasyon bilgiyi hatta bırakır. Bilgi her iki yönde ilerleyerek hatta yayılır. Ancak bu topolojide aynı anda iki istasyonun bilgi göndermesi durumunda bilgi trafiği karışır. Bunu önlemek için hattın paylaşımını düzenleyen protokoller kullanılmalıdır. Ortak yol topolojisi kullanılarak kurulan ağlarda koaksiyel kablo kullanılır, her bir istasyona T-konnektör takılır. İlk ve son istasyona ise sonlandırıcı (terminator) bağlanarak ağ sonlandırılır. Şekil 2.9'da ortak yol topolojisi gösterilmiş ve Çizelge 2.2'de ise avantaj ve dezavantajları verilmiştir.

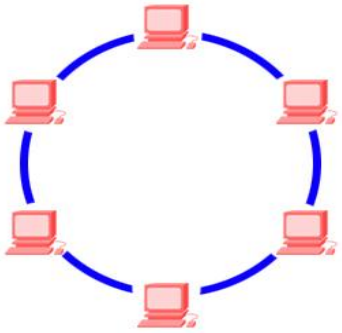
Şekil 2.9. Ortak yol topolojisi

Çizelge 2.2. Ortak yol topolojisi avantaj ve dezavantajlar

Avantajları	Dezavantajları
Kablo yapısı güvenilirdir.	Maximum 30 istasyon (değişebilir) bağlanabilir.
Yeni bir istasyon eklemek kolaydır.	Genellikle, ağ uzunluğu koaksiyel kablonun türüne göre 185-500 metre aralığından fazla olamaz.
Merkez birime ihtiyaç duyulmaz.	Bir istasyon arızalanması durumunda bütün ağı devre dışı bırakır.
	Arıza tespiti zordur.

2.5.2. Halka (Ring) topolojisi

Bu topolojide her nokta, bir halkanın elamanıdır ve halkada dolaşan bilgi bütün noktalara ulaşır. Halkadaki bilgi akışı tek yönlüdür. Yani halkaya dahil olan bilgisayarlar gelen bilgiyi iletmekle görevlidir. Ancak günümüzde pek çok halka ağı çift yönlü bilgi akışı da kullanılabilmektedir. Herhangi bir sonlandırmaya gerek duyulmaz. Bilindik bir örnek vermek gerekise, IBM tarafından oluşturulan token ring topolojisi bir halka topolojisidir. Şekil 2.10'da bu topoloji gösterilmiştir.



Şekil 2.10. Halka topolojisi

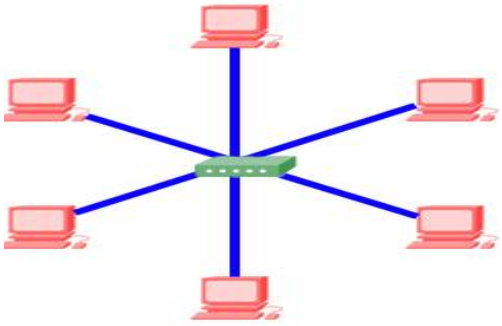
Halka içinde akan verinin denetimi amacıyla, token (jeton) adı verilen bir bilgi ağda dolanır. Token hedef noktaya ulaştıktan sonra, o nokta tarafından değiştirilerek tekrar ağa bırakılır. Yani her bir istasyon gelen veri için alıcı, giden veri için gönderici görevi görür. Halka topoloji kullanılarak 4–16 mbps hızına ulaşmak mümkündür [11]. Çizelge 2.3'te bu topolojinin avantaj ve dezavantajları verilmiştir.

Çizelge 2.3. Halka topolojisi avantaj ve dezavantajlar

Avantajları	Dezavantajları
Maliyeti düşüktür.	Halkaya dahil olan bir noktanın arızalanması, ağın çökmesine sebep olur.
Her bir nokta gönderici olarak görev yaptığından sinyal zayıflaması çok düşüktür.	Hub ile istasyon arası genelde 100 metreden fazla olamaz.
Ağda genellikle hiçbir çakışma meydana gelmez.	
Performansı yüksektir.	
Kolay ve hızlı kurulur.	

2.5.3. Yıldız (Star) topolojisi

Bu topolojide ağdaki iletişimin gerçekleşmesi için bir merkezi bir birim bulunur ve bütün istasyonlar bu merkezi birime bağlanır. Ortak yol topolojisine göre performansı daha yüksektir ve güvenilirdir fakat daha pahalı çözümler sunar. Şekil 2.11'de bu topoloji gösterilmiştir.



Şekil 2.11. Yıldız topolojisi

Bir istasyondan diğerine gönderilen bilgi önce bu merkez birime gelir, buradan hedefe yönlendirilir. Ağ trafiğini düzenleme yeteneğine sahip bu merkezi birim, hub veya anahtar (switch) olarak adlandırılır.

Bu topolojiye dayalı bir sistem kurulurken korumasız çift bükümlü UTP (Unshielded Twisted Pair-Korumasız Çift Bükümlü) veya korumalı çift bükümlü STP (Shielded Twisted Pair-Korumalı Çift Bükümlü) kablo kullanılabilir. İstasyonların merkezi birime (hub) olan uzaklığı genellikle maksimum 100 metredir. Kullanılan ağ kartına veya kabloya göre ağ farklı hızlarda çalışabilir. Çizelge 2.4'te bu topolojinin avantaj ve dezavantajları gösterilmiştir.

Çizelge 2.4. Star topolojisi avantaj ve dezavantajlar

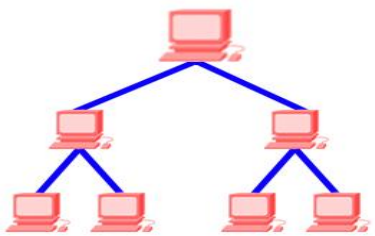
Avantajları	Dezavantajları
Bir istasyonun arızalanması ağı etkilemez.	Merkezi birimdeki hub'da oluşacak bir arıza, hub'a bağlı bütün istasyonları devre dışı bırakır.
Ağ'a yeni bir istasyon eklemek çok kolaydır.	Her bir istasyon için ayrı bir kablo çekilmesi gerekir. Bu da maliyeti ve kablo kirliliğini arttırır.
Ağ yönetimi çok kolaydır.	
Kullanılan ağ elemanlarına göre yüksek hızlar elde edilebilir	

2.6. Genel Olarak WAN Topolojileri

LAN topolojilerine değinmişken yüzeysel olarak WAN topolojilerine de aynı başlık altında devam edebiliriz.

2.6.1. Ağaç topolojisi

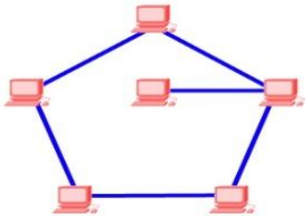
Ağaç topolojisinin diğer adı hiyerarşik topolojidir. Ağacın merkezinde sorumluluğu en fazla olan bilgisayar bulunur. Dallanma başladıkça sorumluluğu daha az olan bilgisayarlara ulaşılır. Bu topoloji çok büyük ağların ana omurgalarını oluşturmakta kullanılır [7]. Şekil 2.12'de basit bir ağaç topoloji yapısı gösterilmiştir.



Şekil 2.12. Ağaç topolojisi

2.6.2. Örgü topolojisi

Bu topolojide geometrik bir düzen yoktur. Her bilgisayar kendisine en yakın bilgisayara eklenerek yerleşim şekli oluşturulur [7]. Şekil 2.13'de basit bir örgü topoloji yapısı gösterilmiştir.



Şekil 2.13 Örgü topolojisi

2.7. Ağ Elemanları

Bir ağın bir çok temel bağlantı elemanı vardır ve bu elemanlar sayesinde, ağ üzerindeki noktalar birbiriyle bağlantı kurarlar. Tabiki bir ağı sadece bilgisayar ekleyerek genişletmek imkansızdır, bu sebeple bir ağı genişletmek, güvenliğini sağlamak ve aynı zaman da hiyerarşi kazandırmak bir çok farklı eleman kullanılmalıdır. Bu elemanların bazıları genel olarak şunlardır:

- *Dağıtıcı (Hub),*
- *Anahtar (Switch),*
- *Tekrarlayıcı (Repeater),*
- *Köprü (Bridge),*
- *Yönlendirici (Router),,*
- *Güvenlik duvarı (Firewall),*
- *Ağ geçidi (Gateway).*

2.7.1. Dağıtıcı (Hub)

Dağıtıcı (Hub), genelde en basit ağ cihazıdır denebilir. Kendisine bağlı olan bilgisayarlara paylaşılan bir yol sunar. Yani Hub'a bağlı tüm cihazlar aynı yolu kullanırlar ve bu da aynı anda haberleşmek isteyen network cihazlarının, bir tek yol olduğu için hattın boşalmasını beklemelerine sebep olur. Genellikle 8–12–16–24 portlu olarak üretilirler.Kısacası Hub'lar gelen sinyalleri elektriksel olarak paralellemeye yararlar. Anahtarlar gibi detaylı konfigurasyonların yapılabildiği gelişmiş cihazlar değildir. Genelde günümüzde kullanımları çok nadir görülen cihazlardır, günümüzdeki piyasadaki modern satıcılarda kolay bulabilecek ürünler degillerdir. Hub'lar OSI sisteminde 1.katmanda yani fiziksel katmanda çalışmaktadırlar [15].

2.7.2. Anahtar (Switch)

Kendisine bağlı cihazlara adından da anlaşılacağı gibi anahtarlamalı bir yol sunar. Hub ile kıyaslandığında en önemli farkı budur. İki bilgisayar kendi arasında haberleşirken başka bilgisayarlar da hattın anahtarlamalı kullanılmasından dolayı kendi aralarında iletişime geçebilirler. Bu sayede Hub'a göre daha yüksek bir performans sağlanacaktır. 8-12–16–24–36–48 port'lu olarak ya da şaseli üretilebilirler. Şaseli switchlerde boş yuvalar vardır ve gerektiğinde port eklenebilmektedir. Çünkü network içinde meydana gelen olayları hızlandırırlar. Switchler network üzerindeki farklı düğümlerin (ağ bağlantı noktaları, genelde bir bilgisayardır) birbirleriyle doğrudan ve sağlıklı bir biçimde haberleşebilmesini sağlar. Switchler MAC adreslerini kullanarak genellikle OSI referans modelinin ikinci katmanı olan veribağı/datalink katmanında çalışırlar. Anahtar, portlarına bağlanan bilgisayarları, MAC adreslerine bakarak tanır. Anahtarlama işlemini gerçekleştirmek için MAC adreslerini yapısında bulunan tabloda tutar. Bu tabloda MAC adresinin hangi porta bağlı olduğu bilgisi bulunur. Kendisine ulaşan veri paketlerinin MAC adreslerini inceler ve her bir porta dağıtmak yerine, sadece hedef MAC adresine sahip olan bilgisayarın bağlı olduğu porta bırakır. Böylelikle veri

paketi sadece hedef bilgisayara ait portu ve kabloyu meşgul eder. Çakışmalar engellenmiş olur ve ağ performansı artar [22].

Kullandığımız switch'lerde VLAN'lar (Virtual Local Area Network) yaratarak giderleri azaltabilir ve cihazımızı daha etkin kullanabiliriz. Vlan'ın yüzeysel olarak tanımına bakmak gerekirse:

Temel olarak VLAN diğerlerinden fiziksel yer olarak ayrılmış tekil bir broadcast domain üzerinde biraraya gruplanmış düğümler bütünüdür. VLAN'lar birden fazla switch'te yapılabilir ve aynı şekilde bir switch'te birden fazla VLAN olabilir.

VLAN aşağıda adı geçen noktalar için avantaj sağlayabilmektedir;

- *Güvenlik : Hassas bilgileri içeren sistemleri birbirinden ayırarak bunlara yapılabilecek sızma olasılıklarını azaltır.*
- *Basitleştirme : VLAN kullanılarak proje yönetimi ve özel uygulamalar daha da basitleştirilir. VLANda bütün gerekli düğümler birarada kullanılmaktadır.*
- *Performans/Bant Genişliği : Ağ trafiği daha dikkatli bir şekilde izlenebilir.*
- *Yayın/Trafik Akışı : VLAN' ın temel prensiplerinden birisi trafik akışının VLAN üyesi olmayan diğer düğümlere geçmemesidir. Böylece yapılan yayın miktarını otomatik olarak azaltır.*

A. Anahtar yapılandırma

Tabi bütün bu işlemlerin olması için switch'lerin konfigure edilmesi (yapılandırılması) gerekmektedir. Aşağıdaki yapılandırma kodlarında, oluşturmuş olduğumuz WAN'daki bir switch için bazı yapılandırma örnekleri verilmiştir.

set ip address 172.20.175.1 mask 255.255.255.0

{Normal şartlarda switchler Layer 2 'de çalışır demiştik ama burda switch'e bir IP adresi atamış oluyoruz, buda switch'lerin ayrıca Layer-3'te de çalışabilme kabiliyetlerinin olduğunu göstermektedir. Switch'lere burda IP adresi atanmasının

nedeni uzak erişim ile bağlanıp, bakım, yönetim gibi işlemlerin yapılabilmesini sağlamaktır.}

set prompt Switch_1

{İsim vermek switchler için zorunlu olan bir durum değildir ama ağ yönetmede düzen sağlayacaktır.}

set width 50
set length 22

{Komutları yazarken,istediğimiz ekranda görünümlerini istediğimiz şekilde düzenleyebiliriz.}

set cdp state disable
set ciscodp status disable
set gvrp disable
set spantree disable
set spantree portadmin *.*.* disable
set lacp disable
set port lacp port *.*.* disable

{Switch'lerin default ayarlarında otomatik olarak açık olan bir çok protocol mevcuttur ve bunlar network'te bir bant genişliğini haberleşmek için işgal ederler, buda ağ hızını düşürebilir, bu protokolleri aktif olmayan/disable konuma getirmek, ağ tıkanıklıgını gidermeye ve hızını artırmaya yarayabilmektedir.}

set lacp static lag.0.1 fe.1.23;fe.1.24
set lacp singleportlag enable

{LACP (link aggregation control protokolü) kullanılarak lag0.1. oluşturulmuş ve LACP fast ethernet 23 ve fast ethernet 24 no'lu portlar arasında yedeklilik

hazırlanmıştır, bu portlar aynı portmuş gibi davranır. Link Aggregation ayrica redundancy (yedeklilik) sağlamaktadır. Link Aggregation içindeki linklerden biri fail olursa iletim diger linklerden yapilmaya devam edecektir. Link tekrar aktif oldugunda yük tekrar dağıtılıp Load Balance (yük balansı) sağlanır. Link Aggregation olustururken portlar ayni vlan ve aynı bandwith değerlerine sahip olmasi gerekir. Karşılıklı portlar için de bu durum geçerlidir.}

set flowcontrol disable
set vlan create 17
set vlan create 101
set vlan create 100
set vlan name 17 Radar
set vlan name 101 Voice
set vlan name 100 Access_TT

{Önce isimler verilerek VLAN'lar yaratılır, daha sonra bu VLAN'lar için ayrı ayrı VLAN ID'leri atanır.}

set port vlan fe.1.1-6 101 modify-egress
set port vlan fe.1.7-10 17 modify-egress
set port vlan fe.1.11-14 100 modify-egress
set vlan egress 17,101,100 fe.1.21 tagged
set vlan egress 17,101,100 fe.1.23-24 tagged
set vlan egress 17,101,100 lag.0.1 tagged
{Son olarak, VLAN'ların etiketli veya etiketsiz olarak çalışabileceği portlar atanır}

2.7.3. Tekrarlayıcı (Repeater)

Repater bir ethernet segmentinden aldığı tüm paketleri yineler ve diğer segmente yollar. Repeater gelen elektrik sinyallerini alır ve binary koda yani 1 ve 0'lara çevirir. Sonra da diğer segmente yollar. Bu yönüyle repater'in basit bir yükseltici olmadığını anlıyoruz. Çünkü yükselticiler gelen sinyalin ne olduğuna bakmadan sadece gücünü

yükseltir. Yolda bozulmuş bir sinyal yükselticiden geçince bozulma daha da artar. Repeater ise gelen sinyali önce 1 ve 0'a çevirdiği için yol boyunca zayıflamış sinyal tekrar temiz 1 ve 0 haline dönüşmüş olarak diğer segmente aktarılır.

2.7.4. Köprü (Bridge)

İki TCP/IP ağını birbirine bağlayan bir donanımdır. Fazla karmaşık aygıtlar olmayan bridge'ler gelen frame'leri (veri paketleri) alır ve yönlendirirler. Köprüler fiziksel bağlantının yanı sıra network trafiğini kontrol eden aygıtlardır. Köprü bir çeşit yönlendirme yapar diyebiliriz fakat OSI Katmanlarından 2. katman yani Data-Link katmanında çalışmasıyla yönlendiriciden ayrılır.

2.7.5. Güvenlik Duvarı (Firewall)

Türkçe güvenlik duvarı anlamına gelen firewall, özel ağlar ile internet arasında, her iki yönde de istenmeyen trafiği önleyecek yazılımsal ya da donanımsal sistemdir. Firewall' ların verimli bir şekilde kullanılabilmesi için internet ve özel ağ arasındaki tüm trafiğin firewall üzerinden geçmesi ve gerekli izinlerin / yetkilerin kısaca erişim listelerinin uygun bir stratejiyle hazırlanmış olması gerekir.

2.7.6. Ağ Geçidi (Gateway)

Network uygulamalarında farklı şekillerde kullanılan ve kapalı bir alandan dışarıya örneğin internete çıkma olanağı sunan cihazlardır. Bir başka kullanım şekli farklı protokoller kullanan ağların birbirlerine bağlanmasını sağlamaktır. Internet ya da başka bir networke bağlanmak için kullanıldığında bilgisayarların TCP/IP yapılandırılmasında Gateway olarak tasarlanan cihazın ip adresi tanımlanmalıdır. Bu şekilde kullanımı yönlendiriciler (Router gibi) vasıtasıyla yapılmaktadır.

2.7.7. Yönlendirici (Router)

Yönlendirici (router) bir yönlendirme cihazıdır ve LAN-LAN ya da LAN-WAN arası yönlendirmelerde, kullanılır. Yönlendiricileri basit bir ağ cihazı olarak tanımlamak yetersiz olabilir. Çünkü yönlendiriciler bir işletim sistemine sahiptirler (örneğin, cisco için IOS–Internetworking Operating System) dolayısıyla programlanabilirler ve gerekli yapılandırma işlemleri sonucunda bir uzak ağ'a erişmek için mevcut birden fazla yol arasında kullanabilecekleri en iyi yolun seçimini yapabilirler (Best Path Determination). Üzerinde LAN ve WAN bağlantıları için ayrı portlar bulunur ve şaseli olarak üretilebilirler. Gereksinime göre bu yuvalara LAN ya da WAN portları eklenebilir. Şekil 2.14'te bir çok çizim ve simulasyonda kullanılan yönlendirici simgesi gösterilmiştir.

Şekil 2.14. Yönlendirici (Router)

Yönlendiriciler OSI başvuru modelinin ilk üç katmanına sahip aktif ağ cihazlarıdır. Temel olarak yönlendirme görevi yaparlar. Projemizde, yönlendiricileri LAN –WAN arasında bağlantı kurmak ve yönlendirmek amacıyla kullandık. Yönlendiricilerin üzerinde LAN ve WAN bağlantıları için ayrı ayrı portlar bulunur. Bunun yanısıra, yönlendiricilere ayrı kartlar takılarak farklı protokoller üzerinden haberleşme yapabilmeleri sağlanır. Yönlendirici görevini yaparken şu sırayı izler:

- *Bir veri paketini okumak,*
- *Paketin protokollerini çıkarmak,*
- *Gideceği network adresini yerleştirmek,*
- *Routing bilgisini eklemek,*
- *Paketi alıcısına en uygun yolla göndermek.*

B. Yönlendirici Yapılandırma

Kullanılan yönlendiriciye göre işletim sistemi değişebilir, ağ oluşturmada yönlendiricilerin yapılandırılması en önemli noktalardan biridir. Kullanmış olduğumuz cisco yönlendiricilerinin bir çok farklı modeli bulunmakla beraber, bu modellerin ait oldukları seri'ye göre (örn: 1800,2800,3000 etc.) özellikleri ve kapasiteleri değişmektedir.

C. Yönlendirici işletim sistemi (Cisco IOS)

Bilgisayarlar gibi işletim sistemi olmadan bir yönlendirici de çalışamaz. Cisco'nun kendi işletim sistemi olan Cisco IOS, cisco yönlendiricilerinin ve anahtarlarının içine yerleştirilmiş olan bir yazılım mimarisidir. Cisco bu yazılım ile aşagidaki ağ servisleri sağlamaktadır:

- *Temel yönlendirme ve anahtarlama işlemleri,*
- *Ağ kaynaklarina güvenilir ve sağlam erişim,*
- *Ağ ölçeklendirirme.*

Cisco IOS yazılımı geleneksel komut penceresi olarak CLI (command line interface) kullanir.

IOS, bir çok Cisco ürün yelpazesinde ana teknoloji olarak süregelmektedir. Uygulamadaki detaylar farklı internet çalışma yöntemlerine göre değişim gösterebilir.

CLI'ye erişmenin bir yolu konsol (console) oturumundan geçer. Konsol portu kullanıldığında, bilgisayardan veya terminalden, yönlendirici üzerindeki konsol bağlantısına doğrudan düşük hızlı seri bağlantı ile erişilir. Bunun yanısıra, IP adresi olan bir yönlendirici'ye direkt telnet seanslarıyla bağlanıp, CLI'a erişmek de mümkün olabilir. Yönlendirici telnet oturumu kurmak için en az bir tane arabirimin IP adresiyle yapılandırılmış olması ve sanal terminal oturumları şifresinin eklenmesi gerekmektedir.

Cisco komut-dizisi arabirimi hiyerarşik bir yapı kullanır, bu yapı özel görevleri yerine getirebilmek için farklı mod'larla girişe gerek duymaktadir. Örneğin, bir yönlendirici arabirimini konfigüre etmek için kullanıcı arabirim konfigürasyon moduna giriş yapmak zorundadir. Bunu takiben tüm konfigürasyonlar bu özel arabirime giriş yapacaklardır. Her bir konfigürasyon modu kendine özgü bir işaretle gösterilir ve sadece bu mod için uygun olan komutlara izin verilir

IOS, "EXEC" olarak bilinen bir komut çeviri servisi sağlar. Her bir komut girildikten sonra, EXEC komutu onaylar ve uygular. Bir güvenlik özelliği olarak Cisco IOS yazılımı EXEC oturumlarını iki giriş bölümüne ayırır.

Bu bölümler kullanıcı ve ayrıcalıklı EXEC modlarıdır. Ayrıcalıklı EXEC modu, enable modu olarak da bilinir. Kullanıcı EXEC modu yalnızca kısıtlı sayıdaki temel izleme komutlarına izin verir, bundan genellikle "yalnızca görüş" modu olarak bahsedilir. Kullanıcı EXEC modu router konfigürasyonunu değiştirebilecek hiçbir komuta müsaade etmez ve " >" imgesiyle ifade edilir.

Farkli cisco aygıt modelleri ve özellik grupları için sayısız IOS imajlari olmasına rağmen temel konfigürasyon komut yapısı aynıdır. Ürünlerin geniş bir bölümünde uygulanan her hangi bir aygıt, konfigürasyon ve hata düzeltim kabiliyetlerine sahiptir.

D. Routing protokolleri

Routing protokolleri routing algoritmaları kullanarak internetworkler arası optimum yolları bulur ve veriyi bu yollar üzerinden aktarır. Routing protokolleri Open System Interconnection (OSI) referans modelinin ağ katmanında (3. katman) işler. Bilgiyi internetwork'te aktarabilmek için, ağ katmanı adresleri başta olmak üzere ağ katmanına özgü bilgileri kullanırlar. Routing protokol algoritmaları iki ana işlevi yerine getirirler.

- *Yol Belirleme*

Yol belirleme, routing protokollerinin hedefe ulaşan yolların makul olup olmadığını belirlemesini sağlar. Bir routing protokolü, paketi yönlendirmek için en uygun router arayüzünü en iyi yolu belirleyerek seçebilir. Yolun uygunluğu bir ya da daha fazla routing ölçütüne bağlıdır. Ağ boyunca yollar statik ya da dinamik olarak belirlenebilir. Yollar oluşturulur ya da keşfedilirken, routing tablosuna birer kayıt olarak eklenirler. Periyodik routing update mesajları router tablolarındaki bilgilerin güncel tutulmasını sağlar.

- *Yol Anahtarlama*

Yol anahtarlama sayesinde yönlendirici, basit anahtarlama algoritmaları kullanarak bir arayüzden aldığı bir paketi bir başka arayüz aracılığıyla gönderebilir. Paket anahtarlama gerçekleştirilmeden önce, yol belirleme işleminin gerçekleştirilmesi gerekir. Yol anahtarlama işlemi, bir router'a paket ulaştığında, router paketi hedefe yönlendirip yönlendiremeyeceğini şu şekilde belirler:

Uç istasyonlardan birinin bir diğerine göndereceği paket vardır. Kaynak uç sistem paketleri en yakın ara düzey cihazın (router gibi) Media Access Control (MAC) adresi ve hedef uç sistemin ağ adresi ile adresler. Kaynak uç sistem paketleri belirlenen ara düzey sisteme gönderir.

Ara düzey sistem (router) paketi yönlendirip yönlendiremeyeceğini anlamak için hedef ağ adresini inceler. Yönlendiremezse paketler atılır. Yönlendirebileceği sonucuna varırsa MAC adresini bir hedefe giden yolda sonraki hop'a göre değiştirir. Sonra, paketi bir sonraki hop cihaza (başka bir ara düzey cihaz ya da hedef uç sistem) gönderir.

E. Routing protokolleri ölçütleri

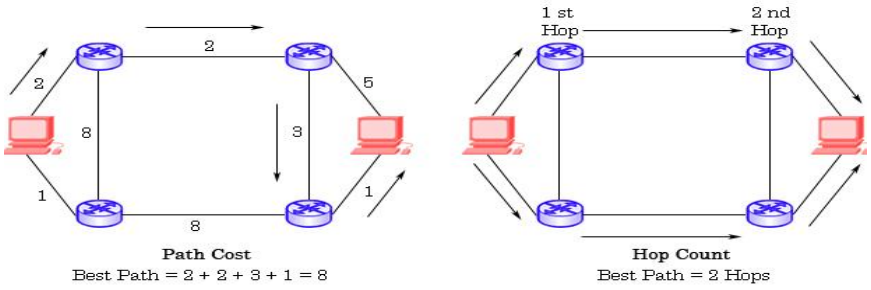
Routing ölçütleri, router algoritmaları tarafından hedef ağa olan yolun makul olup olmadığını belirlemek için kullanılır. Değişik routing protokollerinin değişik routing

ölçüt gerçekleştirimleri vardır. Routing ölçütleri ağ karakteristiklerini yansıtır. Ölçüt bilgileri routing tablolarında saklanır.

Başta, mesafe, güvenirlik, gecikme, bant genişliği, yük ve maliyet olmak üzere pek çok yaygın kullanılan routing ölçütleri mevcuttur.

- Mesafe : Mesafe ölçütü, yol maliyetine ya da hop sayısına bağlıdır.
- Yol maliyeti : Ağ yöneticisi tarafından her bir ağ hattına keyfi olarak verilen değerlerdir. Mesafe geçilen tüm hatların maliyetlerinin toplamıdır.
- Hop sayısı : Bir paketin kaynaktan hedefe ulaşmak için geçmesi gereken tüm ara düzey cihazların (router gibi) sayısıdır. Mesafe yoldaki tüm hopların toplamıdır.

Şekil 2.15'te mesafenin yol maliyetine ya da hop sayısına göre hesaplanması durumlarındaki farklar gösterilmiştir.



Şekil 2.15 En iyi yol hesaplaması

- Güvenilirlik

Güvenilirlik routing ölçütü bir çok ağ özelliğine dayandırılabilir. Bunların arasında bit-error rate (hatalı olanların toplam alınan bit sayısına oranı), her bir hattın arızalanma sıklığı ve arızalanan her hangi bir hattın ne kadar sürede onarılabileceği bulunur. Güvenilirlik genelde hatlara ağ yöneticisi tarafından keyfi verilen bir değerdir.

- Gecikme

Gecikme routing ölçütü internetworkten paketin kaynak-hedef arası aktarımının aldığı süredir. Gecikme ölçütü, tipik olarak bir çok değişkenin toplamından oluşur. Bunların arasında hatların bant genişliği, ara düzey routerların kuyruk boyları, hatlardaki trafik yoğunluğu ve kaynaktan hedefe fiziksel mesafe bulunur.

- Bant Genişliği

Bant genişliği yönlendirme ölçütü, hattın trafik kapasitesine bağlıdır. Bunun yanında, yüksek bant genişliğine sahip hatlar, yavaş hatlara oranla daha iyi yollar sağlayamayabilir, çünkü farklı yollar yüksek bant genişliğini destekleyemeyebilir.

- Yük

Yük routing ölçütü ağ kaynaklarının (router gibi) yoğunluğuna bağldır. Yük, CPU kullanımı ve saniyede işlenen paket sayısı gibi etmenlere göre hesaplanır [21].

2.8. Yönlendirme (Routing) Çeşitleri

Yönlendirme kısaca, ağ'lar arasındaki veri akışının sağlanabilmesi için gerekli olan yol bilgisinin yönlendiriciler tarafından sağlanması işlemidir. Yönlendiriciler kendilerine gelen paketlerde, hedef ip adresi olarak, nerede olduğunu ve nasıl gidileceğini bildikleri bir ağ'dan adres bulunduğunda, hedefe yönlendirme yaparlar. Aksi takdirde paketi yok ederler. Genellikle, iki çeşit yönlendirmeden bahsedilir, bunlar :

1. *Statik yönlendirme*
2. *Dinamik yönlendirme*

2.8.1. Statik yönlendirme

Ağlar arası olması gereken yönlendirmenin manuel olarak yazılmasıdır. Yani yönlendirme yapılması gereken IP adresleri elle belirtilmiştir. Küçük ölçekli

networklerde genellikle ideal çözümdür. Statik yönlendirme yapılırken hedef network adresi, subnet maskı ve bizi o hedefe götürecek bir sonraki yönlendiricinin ip adresi bilinmelidir. Bir sonraki yonlendirici (“next hop”) ile kavramlar bu noktada ortaya çıkmaktadır. Cisco yönlendiricilerde global config modda iken aşağıdaki komut düzeniyle statik yönlendirme yapmak mümkündür.

Router(config)# ip route [hedef adres] [subnet mask] [Next Hop] [distance]
ip route 192.168.151.0 255.255.255.0 10.1.151.2 200
ip route 192.168.153.0 255.255.255.0 10.1.153.2 200

Yönlendirme kaldırılmak gerektiğinde başına “no” ifadesini yazmak yeterli olacaktır. Bu komutta distance ifadesi çok önemlidir. Distance ifadesi seçimlik olup gerektiği durumlarda yönlendirmeler arasında önceliği belirlemeye yarayan “Administrative Distance” değerini değiştirmek için kullanılır. Default olarak genellikle statik yönlendirmede administrative distance değeri “1” olarak gelmektedir. Fiziksel olarak direkt bağlı olan yönlendirmelerde ise a.d. değeri “0” dır. Bu değer yükseldikçe yönlendirmedeki öncelik değeri düşmektedir. Bazı yönlendirme durum ve protokollerindeki default administrative distance değerleri Çizelge 2.5’te belirtilmiştir.

Çizelge 2.5. Protokoller için default administrative distance değerleri

Administrative Distance Route Source	Default Distance
Connecred interface	0
Static route	1
Enhanced IGRP summary route	5
External BGP	20
Internal Enhanced IGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP external route	170
Internal BGP	200
Unkown	255

2.8.2. Dinamik yönlendirme

Dinamik yönlendirme'de statik yönlendirme'de olduğu gibi sabit bir tanımlama yapmak yerine, dinamik ağ yönlendirme protokolleri ile çeşitli parametrelere bağlı olarak otomatik yönlendirmeler yapılmaktadır. Yönlendirme protokolleri, yönlendiricilerin birbirleriyle haberlesmesini ve gerekli yönlendirme bilgilerini birbirleriyle paylaşmalarını temel alan protokollerdir. Her yönlendirici kendine direkt bağlı olan network'leri tanır ve ilgili routing protokolüne göre en iyi yol seçimi (Best Path Determination) yönlendirici tarafından yapılır. Bahsedilen bu dinamik yönlendirme protokolleri 3 başlık altında incelenebilir.

1. Distance Vector Protokoller (RIP, IGRP),
2. Link State Protokoller (OSPF),
3. Hybrid Protokoller (EIGRP).

Distance Vector protokol, yönlendirici tablosunu güncelleme mantığı ile çalışır. Yani belirli zaman aralıklarında sahip oldukları network bilgilerini komşu yönlendiricilere gönderirler ve komşu yönlendiricilerden de aynı bilgileri alırlar. Bu döngünün sonunda her yönlendirici sistemde ki bütün networkler'i öğrenmiş olur ve uygun yol seçimini yapar. RIP (Routing Information Protocol) ve IGRP (Interior Gateway Routing Protocol) bu tür protokollere örnek verilebilir.

Link State protokoller ise sürekli bir güncelleme yapmak yerine, komşu routerlarının aktif olup olmadıklarını anlamak için küçük "Hello" paketleri gönderirler. Sadece gerektiği zamanlarda, yeni bir router ortama eklendiğinde veya bir router down (deaktif) olduğunda, sadece o bilgi ile ilgili güncellemeyi gerçekleştirirler. OSPF (open shortest path first) bu tür protokollere en iyi örnektir.

Hybrid Protokoller hem Distance Vector hem de Link State protokollerin bazı özelliklerini taşır. Bu gruba üye olan EIGRP (Enhanced Interior Gateway Routing Protocol) cisco tarafından ortaya çıkarılmıştır ve sadece cisco tabanlı yönlendiricilerde çalışırlar [21, 22, 23].

2.9. İlk Açık Yöne Öncelik (OSPF-Open Shortest Path First)

Daha önce belirttiğimiz gibi "OSPF" dinamik yönlendirme protokollerinden link-state routing protokolü olarak çalışmaktadır ve link-state yönlendirme protokolleri, topolojinin tamamını görebildiği gibi, ağ değişikliklerinde sürekli güncelleme gönderir ve en kısa yol hesaplamalarında, "shortest path first" algoritmasını kullanır. Ayrıca "Link-state refresh" olarak bilinen, 30 dk.' da bir periyodik güncellemeler de gönderir.

OSPF, networkde bir değişiklik olduğu zaman yönlendirme güncelleme paketi üretir. Bir linkin durumu değiştiğinde, bunu tespit eden router, LSA (Link-State Advertisement) denilen paketi yayınlar. LSA paketi, bütün komşulara iletilir. Her yönlendirici cihaz, LSA'ın bir kopyasını alır. LSDB (link-state database) 'i günceller ve LSA' yı komşu yönlendiricilerine iletir. Gönderilen bu LSA sayesinde bütün ağ, ağdaki değişikliği algılayıp bunu yeni topolojiye yansıtır. LSDB, hedef networke giden en iyi yolu hesaplamak için kullanılır.

OSPF'de 3 çeşit tablo bulunmaktadır: Komşuluk (Neighbour) Tablosu, Topoloji Tablosu ve Yönlendirme (Routing) Tablosudur. Komşuluk tablosunda, yönlendirici komşularının listesi tutulmaktadır. Topoloji tablosu ise, LSDB (Link State Data Base) olarak bilinmektedir, yönlendirme tablosunda ise ilgili yönlendirme yapılandırmaları tutulur.

OSPF Area (alan) içerisinde bütün yönlendiriciler ve onların bağlantıları tutulmaktadır. LSA' ler bu tabloda yer almaktadır. Ve en önemlisi ise area içerisindeki her yönlendiricinin LSDB' si özdeş olmak durumundadır. Yönlendirme tablosu ise yönlendirme veri tabanı olarak da (forwarding database) adlandırılır. Hedef networklere giden en kısa yolların bilgisi bu tabloda tutulur.

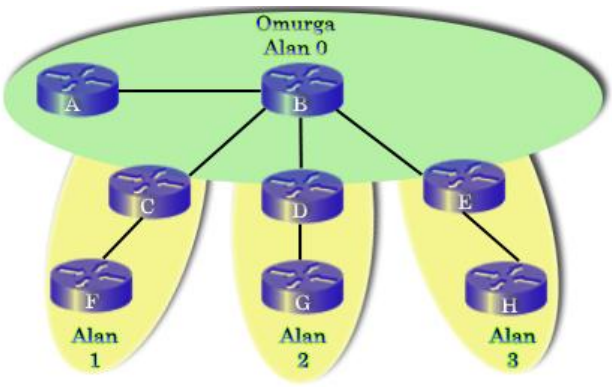
2.9.1 OSPF alan yapısı

OSPF çalışan router'lar topolojinin tamamını görebilmektedir. Eğer area yapısı söz konusu olmasaydı, performans ciddi bir şekilde düşerdi. Çünkü ağ'da bir değişiklik olduğunda bu bilginin OSPF çalışan bütün yönlendiriciler tarafından bilinmesi gerektiği için performans etkilenecektir. Bütün yönlendiriciler LSDB' nin bir kopyasını tuttuğu için topolojideki yönlendirici sayısının artması, LSDB' nin büyümesine neden olacaktır. Bir area içerisindeki yönlendiriciler o area için detaylı bilgiye sahip olurken başka area'lar için özet bilgiye sahip olmaktadır. Ayrıca area yapısı ile routing (yönlendirme) tablolarının girdilerini küçültecektir.

Backbone (omurga) area (transit area veya area 0) ve regular area (nonbackbone area) olmak üzere iki area mevcuttur. Cisco'nun önerisi her areada max 50 yönlendirici olması şeklindedir.

Backbone Area (Area 0): Temel görevi hızlı ve etkili bir biçimde IP paketlerinin gönderilmesidir. Son kullanıcılar bu areada yer almamaktadır.

Regular Area (Nonbackbone Area): Son kullanıcıların ve fax, printer vb. gibi kaynakların bağlı olduğu areadır. Bir regular area, başka areaların trafiğinin kendi üstünden geçmesine izin vermez. Farklı arealar ile iletişim backbone area ile gerçekleştirilmektedir. Standart, stub, totally stub ve not-so-stubby area olmak üzere alt çeşitleri mevcuttur [24].



Şekil 2.16. OSPF'te alan yapısı.

Şekil 2.16'da yesil alanda olan iki yönlendiricinin backbone areada yer aldığını görüyoruz. Area 0′ da yer alan yönlendiriciler backbone yönlendirici olarak adlandırılmaktadır. 1, 2 ve 3 yönlendiricileri ayrı areaları birleştirdiği için Area Border Router (ABR) olarak isimlendirilir. ABR' ların görevi diğer alanları area 0'a bağlamaktır.

ABR' ların özellikleri:

- LSA' ların iletildiği alanları ayırırlar.
- Area adres özetlemesi için öncelikli noktadır.
- Default router' lar için kaynak noktasıdır.
- Bağlı oldukları her area için LSDB' ye sahiptirler.

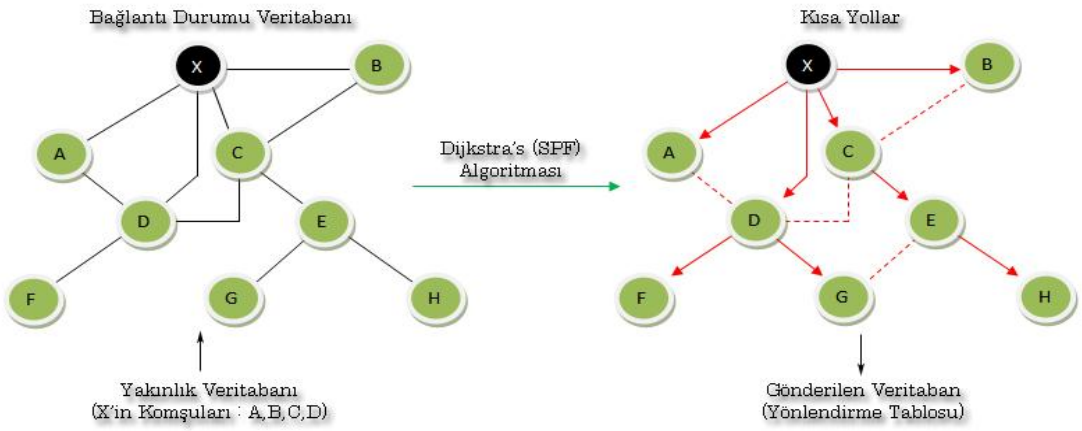
2.9.2. OSPF komşuluk veritabanı (Adjacency database)

OSPF çalışan iki yönlendirici, "Hello" paketleri ile komşuluk ilişkisi kurar. Ağa yeni dahil olan yönlendirici, komşusuna hello paketi gönderir ve komşusundan hello paketi alır. Bu işlem sırasında "multicast" adres kullanılır. Hello paketleri karşılıklı olarak değiş tokuş edildikten sonra yönlendirici komşusunu "up" kabul eder. Komşuluk ilişkisi kurulduktan sonra, yönlendiriciler LSA' lerini değiştirerek LSDB' yi senkronize etmektedirler. Buradaki amaç özdeş LSDB' ye sahip olmaktır. Bu aşamadan sonra yönlendiriciler "full adjacenct state" denilen aşamaya geçerler

2.9.3. OSPF metriğinin hesaplanması

OSPF çalışan yönlendiriciler hedef network'e giden en iyi yolu bulabilmek için SPF (Shortest Path First) algoritmasını kullanırlar. En iyi yol, en düşük maliyetli yoldur ve en iyi rotalar yönlendirme tablosunda yer almaktadır. OSPF en iyi yolu hesaplarken "cost" değerini kullanır.
Cost : 10 000 000 / Bant genişliği

Şekil 2.17'de Link State Database' de yönlendiricilerin komşuluk durumları yer almaktadır. Buradaki bilgiler doğrultusunda SPF algoritması çalıştırılarak yönlendirme tablosu oluşturulmaktadır.



Şekil 2.17. OSPF metrik hesaplaması

2.9.4. OSPF paket çeşitleri

OSPF' de hello, database description, link-state request, link-state update ve link-state advertisement olmak üzere 5 çeşit paket bulunmaktadır [24]. (Bkz Şekil 2.18). Çizelge 2.6'da paket fonksiyonları verilmiştir.

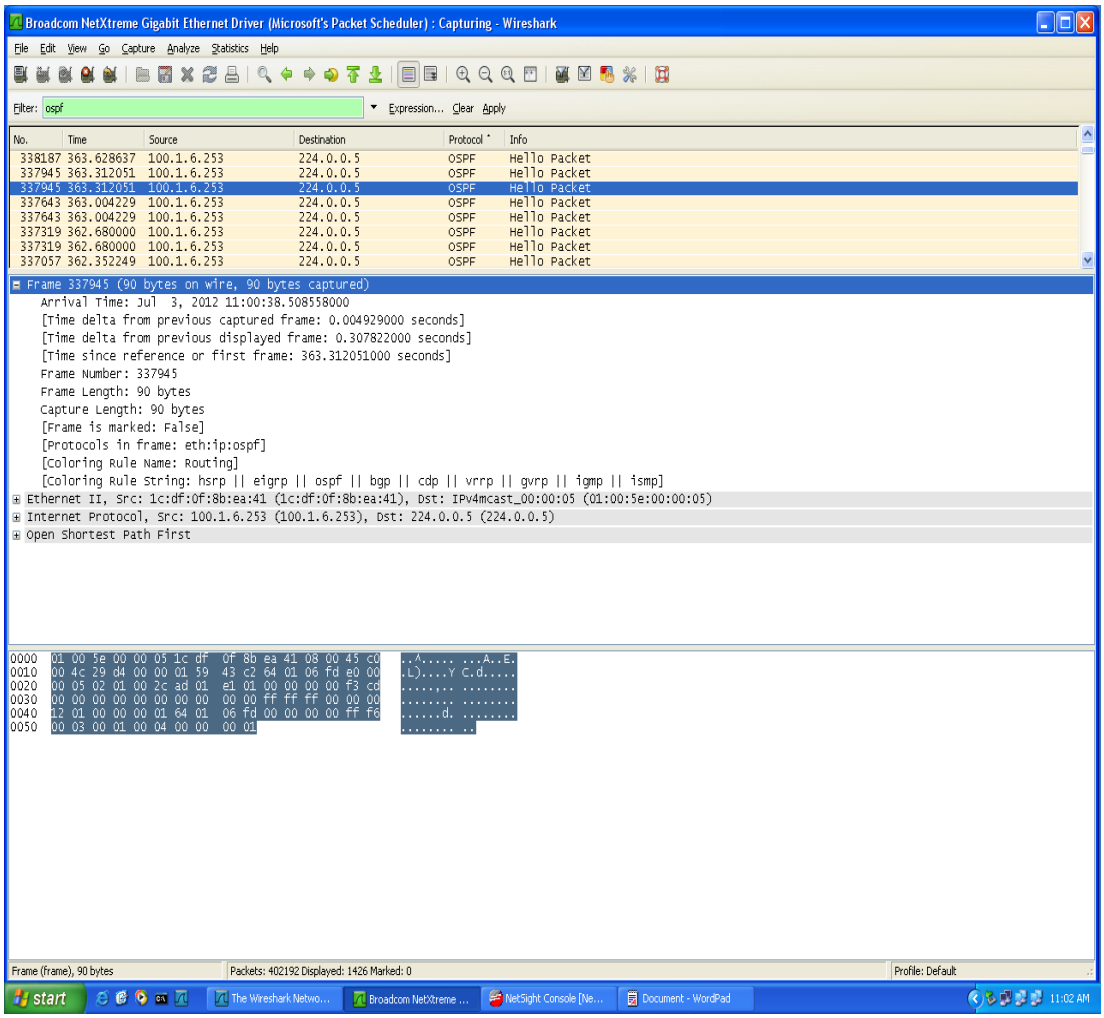
Şekil 2.18. OSPF paketleri

Çizelge 2.6. OSPF paket tanımları

Çeşit	Paket Adı	Tanım
1	Hello	Komşuları tespit edip komşuluk ilişkisi kurulurken kullanılır.
2	DBD	Yönlendiriciler arası veritabanının (LSBD) senkronizasyonunu kontrol eder.
3	LSR	Yönlendiriciden, yönlendirici belirgin link-state kaydını ister.
4	LSU	Bağlantı durumu ile ilgili güncelleme işlemleri için kullanılır.
5	LSAck	Diğer paket çeşitleri için bilgilendirme içerir.

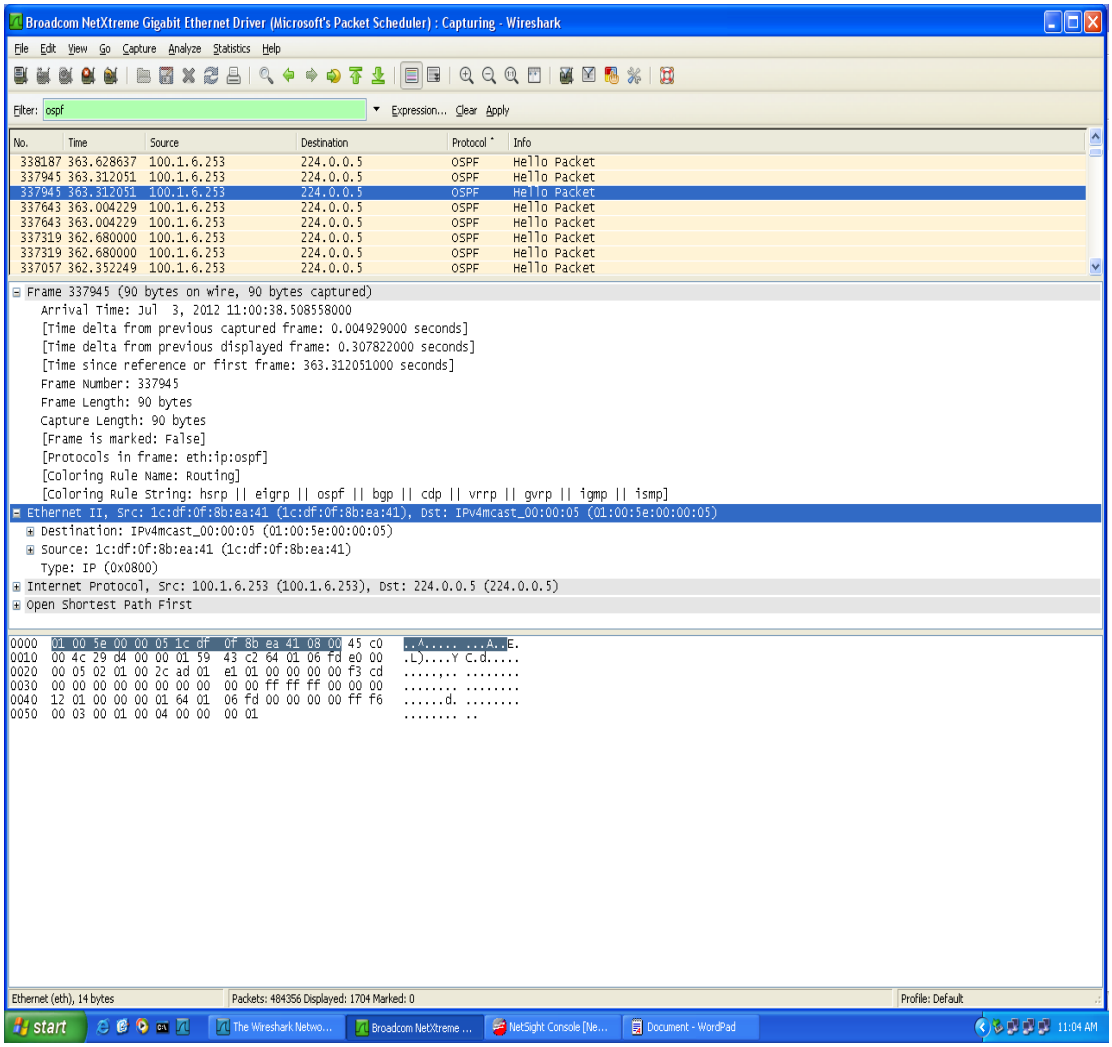
2.9.5. Wireshark ile OSPF analizi

Aşağıda yapmış olduğumuz analizin, alınan ekran görüntüleriyle açıklamaları mevcuttur.



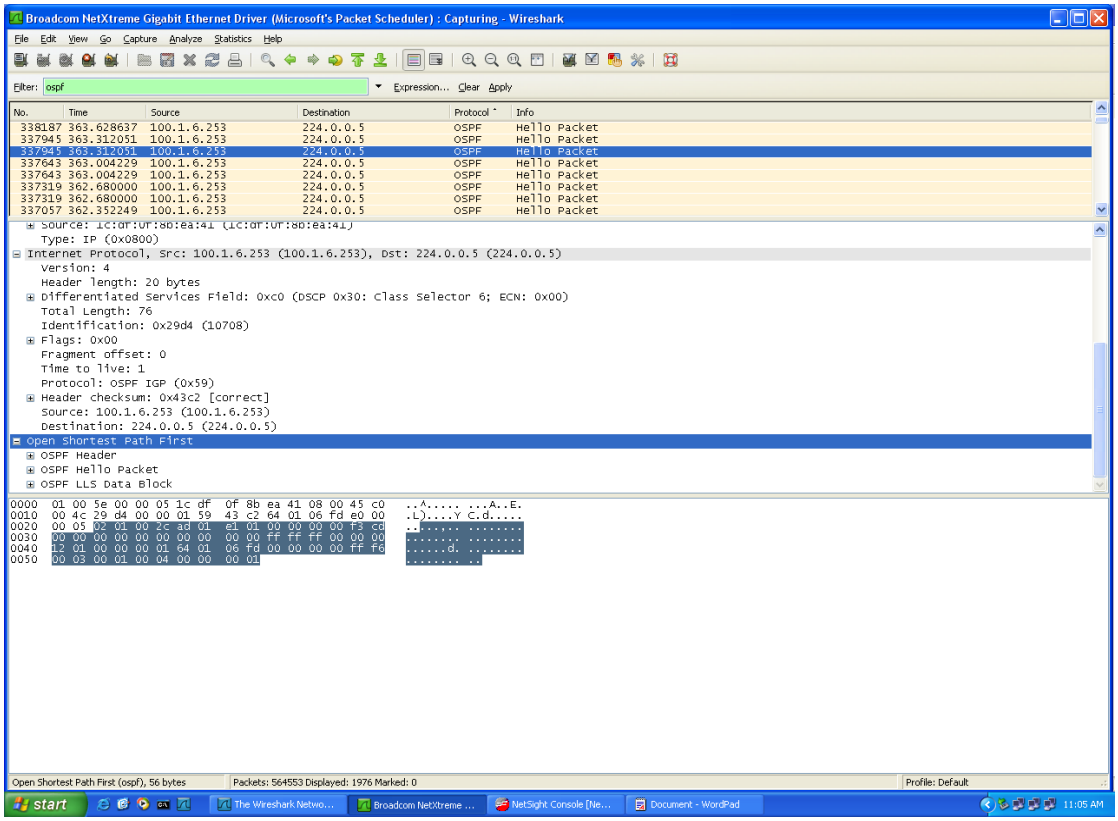
Resim 2.1. OSPF frame

Resim 2.1'de wireshark programı kullanılarak bir OSPF Hello paketi analiz edilmeye çalışılmıştır. Seçilmiş olan bölümde bütün çerçeve (frame) görünmektedir. Bu frame içerisinde Ethernet, IP, OSPF gibi bir çok protokole ait veriler bulunmaktadır. Frame sekmesi seçildiğinde, o frame ait bir çok detay için alt açıklamalar resimde görüldüğü üzere yapılmaktadır.



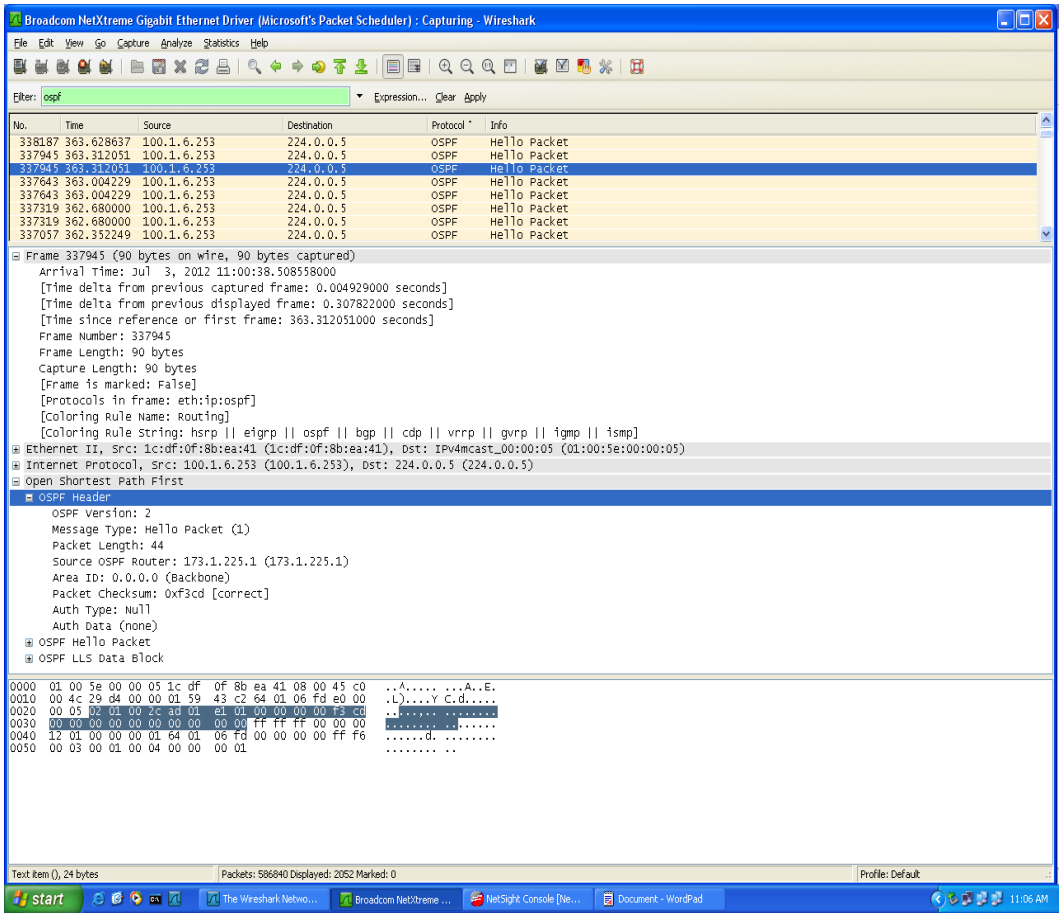
Resim 2.2. OSPF ethernet.

Resim 2.1'de analize ana çerçeve ile, başlamıştık. Resim 2.2'de ise analizin bir sonraki basamağı olan Ethernet verileriyle devam ediyoruz. IP protokolüyle beraber kullanılma özelliği olan Ethernet II protokolüne ait Kaynak, Hedef gibi detaylar Ethernet II sekmesi altında gösterilmiştir. Ayrıca en alt bölümde ise ilgili veriler HEX. olarak gösterilmiştir.



Resim 2.3. OSPF protokolü verileri-1

Analizin bir ilerki basamağını ise OSPF protokol detayları oluşturmaktadır. Resim 2.3'te OSPF sekmesi seçildiğinde, protokole ait olan veri gruplarının, (Header, Hello Packet, LLS data block) şeklinde gruplandırılmış olduğunu görebiliyoruz. Ayrıca alt bölümde OSPF protokol haberleşmesi için kullanılan bütün verilerin HEX olarak gösterimi mevcuttur.



Resim 2.4. OSPF protokolü verileri-2

OSPF header seçildiğinde Resim 2.4'te de gözlenebileceği üzere, OSPF versiyonu, paket uzunluğu, mesaj türü, kaynak ospf yönlendiricisi, area numarası vb gibi OSPF header detaylarını görmek mümkündür. Veri içerini görmek ve daha detaylı analiz yapabilmek için diğer veri gruplarını da ayrı ayrı seçip analiz yapmak gerekir. Kısacası, wireshark yazılımı ile bazı ağ protokolleri için bu şekilde detaylı analiz yapmak mümkündür.

2.9.6. OSPF yapılandırma

Ayrıca aşağıda dinamik yönlendirmeye örnek olarak yaptığımız basit bir OSPF yönlendirme işlemi detaylarıyla mevcuttur.

router ospf 1

{*Yönlendirici konfigurasyonu yapabilmek için kullanılan komuttur, ayrıca burda yönlendiricinin process ID si 1 olarak atanmıştır, her yönlendiricinin farklı process id' si olmaldır*.}

log-adjacency-changes

{Bu komut, ospf protokolü kullanıldığında, protokolün ne zaman up ya da down olduğu gibi durumları system log'u olarak tutmaya yarar.}

network 192.168.175.0 0.0.0.255 area 0
network 10.255.175.0 0.0.0.255 area 0
network 173.1.175.0 0.0.0.3 area 0
network 173.3.175.0 0.0.0.3 area 0

{Yukarı yazılan network'ler ospf protokolü üzerinden routing tablosuna eklenmiştir. Bu ağlar arasında yönlendirmeyi OSPF kendisi yapmaktadır. Ayrıca yukarıda görüldüğü üzere OSPF ağ maskesi olarak "wild card mask" kullanmaktadır.}

2.9. Sonuç

Sonuç olarak bu bölümde veri iletişiminin temellerinden başlanılmış olup, OSI modelinin üzerinde durulmuştur. Ethernet, TCP, UDP gibi günümüz veri iletişiminde temel teşkil eden bazı kavramlar ile ayrıntılı bilgi verilmiştir. Yerel alan ağ, geniş alan ağ gibi kavramların tanımları ve bir çok topoloji çeşitlerinden bahsedilmiştir.

Bir network'u oluşturan elemanlar hakkında bilgi verilmiş olup, örnek bir anahtar yapılandırma, bazı komutlar üzerindeki açıklamalarla anlatılmıştır. WAN tasarımında büyük önem teşkil eden yönlendiriciler hakkında bilgi verilmiş olup, yönlendirme işleminin incelikleri anlatılmıştır. Statik ve dinamik yönlendirme çeşitleri açıklanmış olup, OSPF dinamik yönlendirmesi üzerinde ayrıntılı durulmuştur. Ayrıca hem dinamik hem de statik yönlendirmeler için yapılmış olan konfigurasyon örneklerle gösterilmiştir.

3. GENİŞ ALAN AĞ (WAN-WIDE AREA NETWORK) TEMELLERİ

3.1.WAN Nedir?

WAN, bir çok zaman farklı iletişim sistemlerinde detaylı olarak ya da yüzeysel olarak karşımıza çıkmıştır. Genel olarak, geniş alan ağ (WAN), coğrafik olarak dağınık telekomünikasyon ağlarına verilen isimdir. Dolayısıyla, bir WAN, iki veya daha fazla yerel alan ağları (LANs) bağlamak için oluşturulan bir ağ sistemidir. Bilinen en populer WAN örneği olarak bugün kullandığımız internet'i gösterebiliriz [12].

3.1.1 WAN ve LAN

WAN'ı biraz daha iyi anlayabilmek için LAN ile ortak olan ve farklı olan noktalarını gözden geçirmemiz gerekmektedir.

Aslında bir çok ağ (özellikle kurumsal ağlar) hem geleneksel LAN hem de WAN teknolojilerini içinde barındırır. Bilinen bir ağda yerel LAN'ler bir WAN oluşturmak üzere, coğrafik olarak dağıtılmış diğer noktalara bağlanırlar.

LAN'ler özeldir ve bir tek kişinin veya kurumun kontrolü altındadır. Bu kişi/kurum, LAN'ın işlevsel inşa bloklarını oluşturan kablolamayı ve cihazları kurar, yönetir ve bakımlarını yapar. Bazı WAN'ler özel olarak sahiplenilmiştir ama bir özel WAN'ın geliştirilmesi ve bakımı pahalı olduğundan, sadece büyük işletmeler özel bir WAN'a sahip olabilir. Örneğin genelde askeri kurumların WAN'ları onlara özeldir. Şirketlerin çoğu WAN bağlantılarını bir hizmet sağlayıcıdan veya bir ISP'den (Internet Service Provider) satın alır. Genellikle ülkemizde, bu hat sağlayıcılar Türk Telekom A.Ş, Türksat A.Ş gibi büyük kurumsal firmalardır. Bu durumda, arka uç ağ bağlantılarının (LAN-WAN geçişlerinin) ve LAN'lar arasındaki ağ hizmetlerinin sağlanmasından ISP sorumlu olur.

Bir kurum çok sayıda global siteye sahipse, WAN bağlantılarının ve hizmetinin gerçekleştirilmesi karmaşık olabilir. Örneğin, kurumun ana ISP'si, kurumun bir ofise sahip olduğu her konumda veya ülkede hizmet sunamayabilir. Sonuç olarak kurumun birden fazla ISP'dan hizmet satın alması gerekir. Birden fazla ISP'nin kullanılması, genellikle sağlanan hizmetlerin kalitesinde farklara neden olur. Bir kurumsal ağın desteklenmesi için cihazların, yapılandırma ve hizmetler konusunda aynı standartlara sahip olması önemlidir. [1-2, 22]

Yüzeysel olarak LAN ve WAN teknolojilerinin özelliklerini bazı maddeler vererek gözden geçirirsek:

Bir LAN'in özellikleri:

- *Kurum, altyapının kurulmasından ve yönetilmesinden sorumludur.*
- *Ethernet, en yaygın kullanılan teknolojidir.*
- *Ağın odağı, erişim ve dağıtım katmanlarıdır.*
- *LAN, kullanıcıları bağlar, yerel uygulamalar ve sunucu çiftlikleri için destek sağlar.*
- *Bağlı cihazlar genellikle bir bina veya bir yerleşke gibi aynı yerel alandadır.*

Bir WAN'ın özellikleri:

- *Bağlı olan noktalar genellikle coğrafik olarak dağıtılmıştır.*
- *Bir WAN'a bağlanabilirlik için, verilerin ağ tarafından kabul edilebilir bir biçime konulması sağlamak üzere, modem, yönlendirici, anahtar vs. bir cihaz kullanılması gerekir.*
- *Hizmetler bir ISP tarafından sağlanır. WAN hizmetleri T1/T3, E1/E3, DSL, Kablo, Çerçeve Aktarımı, ATM, Metro Ethernet veya daha yeni teknolojiler olabilir.*
- *Altyapının kurulmasından ve yönetilmesinden ISP sorumludur.*
- *Uç cihazlar, genellikle ethernet kapsüllemesini bir seri WAN kapsüllemesine dönüştürür.*

3.2. WAN Tasarımında Önemli Kriterler

Genellikle, bir çok kurumun ya da kişinin, ağı için sadece birkaç önemli gereksinimi vardır, bunlar:

i. Kullanılabilirlik

Ağ'ın sürekli çalışabilir durumda olma oranı, kullanılabilirlik derecesini göstermektedir. Ağ'da oluşabilecek herhangi bir arıza, bu oranı aşağılara düşürmektedir. Kullanılabilirlik, daha sonra bahsedeceğimiz, bir ağ için önem teşkil eden, QoS (Quality of Service) parametrelerinden biridir.

ii. Performans

Ağ, veriyi güvenli ve kabul edilebilir sürelerde iletmelidir. Ağ'ın performansı paket kaybı, gecikme, bant genişliği gibi parametreleri analiz edilerek değerlendirilir. Bir çok özel uygulamar için ağ performansı belli değerlerin üzerinde olmalıdır.

iii. Güvenlik

Performans bir ağ'da ne kadar önemli olsa da, ayrıca ağ, güvenli de olmalıdır. Üzerinden geçen verilerin yanı sıra, bağlı aygıtlarda saklananları da koruyabilmelidir. Bazı özel uygulamalar için, güvenlik katsayısını artırmada firewall (güvenlik duvarı) gibi cihazlar kullanılır.

iv. Ölçeklenebilirlik

Ağ, büyümeye ve firmanın genel değişikliklerine uyum sağlaması için kolayca düzenlenebilir olmalıdır. Ağ trafiğini bilmek, ölçekleyebilmek ağ güvenliğini artırır, gelecekte eklenecek olan uygulamalar için bir rehber görevi üstlenir ve herhangi bir arıza durumunda problemin daha çabuk elimine edilebilmesini sağlar.

v. Yönetilebilirlik

Zaman zaman arızalanmalar olabileceğinden, sorun giderme kolay olmalıdır. Bir sorunun bulunması ve giderilmesi, fazla zaman almamalıdır. Ağ'ı daha kolay yönetbilmek için yönetim konsollarının olması büyük fayda sağlar. Ayrıca ağlara uzaktan bağlanıp sorunun giderilmesi, hem zaman olarak, hem de ekonomik olarak büyük avantaj getirir [1, 22].

3.2.1. Temel tasarım hedefleri

Temel tasarım hedeflerini karşılamak için, bir ağın esneklik ve büyümeye izin veren bir katmanlı mimari üzerinde oluşturulması gerekir. İşte bu katmanlı yani hiyerarşik olan ağ tasarımı için bazı temel noktalara değinmek gerekirse:

Hiyerarşik Ağ Tasarımı:

Ağlarda, hiyerarşik tasarım, aygıtları birden fazla ağ'da gruplamak için kullanılır. Dolayısıyla, bu ağlar, katmanlı bir yaklaşımla düzenlenir. Hiyerarşik ağların, düz ağlara göre bir çok avantajları vardır. Düz bir ağı daha küçük, daha yönetilebilir bloklara bölünür, ve yerel trafik, yerel olarak kalır. Ve sadece diğer ağlara giden trafikler bir üst katmana taşınır.

Düz bir ağdaki 2. Katman aygıtlar, yayınları kontrol etmek ve istenmeyen trafiği filtrelemek adına oldukça az olanak sağlarlar. Düz bir ağa daha fazla aygıt ve uygulama eklendikçe, ağ kullanılamaz duruma gelene kadar yanıt süreleri artacaktır. Hiyerarşik tasarım modelinde, üç temel katman bulunmaktadır:

Merkez katman: Merkez katmanı, zaman zaman ağ omurgası olarak adlandırılır. Merkez katmanı'ndaki yönlendiriciler ve anahtarlar, yüksek hızlı bağlantı sağlar. Kurumsal bir ağ'da, merkez katmanı birden fazla binayı birbirlerine bağlayabileceği gibi, sunucu çiftliğine de bağlantı sağlar. Merkez katmanı uygulamak, ağın

karmaşıklığını azaltarak, ağın yönetimini ve ağda sorun gidermeyi kolaylaştırır. Merkez katmanı tasarımı, ağın bir bölümüyle diğer bir bölümü arasında etkili, yüksek hızlı veri aktarımını olanaklı kılar. Bu katmandaki öncelikli tasarım hedefleri şunlardır:

- *%100 çalışma süresi sağlamak.*
- *İş hacmini en üst seviyeye çıkarmak.*
- *Ağın genişlemesini desteklemek.*

Merkez Katmanı'nda kullanılan teknolojilere, aşağıdakiler dahildir:

- *Aynı aygıtta yönlendirme ve anahtarlamayı bir araya getiren yönlendiriciler ya da çok katmanlı anahtarlar.*
- *Artıklık ve yük dengeleme.*
- *Yüksek hızlı ve bir arada bağlar.*
- *Geliştirilmiş iç ağ geçidi yönlendirme protokolü (EIGRP) ve öncelikle açık olan en kısa yol (OSPF) protokolleri gibi iyi ölçeklenen ve hızlı yakınsayan protokoller.*

Dağıtım Katmanı : Erişim katmanı ve merkez katman arasında bulunan yönlendirme ucunu temsil eden katmandır. Ayrıca, uzak konumlar ve merkez katmanı arasında bir bağlantı noktası olarak görev yapar.

Dağıtım katmanı genellikle 3. katman aygıtlar (yönlendiriciler) kullanılarak kurulur. Dağıtım katmanı'nda bulunan yönlendiriciler ve çok katmanlı anahtarlar, ağ tasarımının hedeflerini yerine getirmek için önemli olan işlevleri sağlarlar. Aşağıdakiler, bu hedefler arasında bulunur [22];

- *Trafik akışlarını filtrelemek ve yönetmek,*
- *Erişim denetimi politikalarını uygulama,*
- *Rotaları merkez katmanı'na tanıtmadan önce özetlemek,*

- *Merkez katmanı'nın, erişim katmanı'ndaki hatalar ve kesintilerden etkilenmemesini sağlamak,*
- *Erişim katmanı VLAN'ları arasında yönlendirmeler sağlamak.*

Erişim Katmanı: Erişim Katmanı, ağda uç aygıtların bağlandığı sınırı temsil eder. Erişim Katmanı, ağa erişim sağlamak için 2. katman anahtarlama teknolojisi kullanır. Erişim, kalıcı bir kablolu altyapı ya da kablosuz erişim noktaları aracılığıyla gerçekleşir. Örneğin, bakır kablolar üzerinden ethernet, uzaklık kısıtlamaları getirir. Bu yüzden, herhangi bir merkezin altyapısının erişim katmanı'nı tasarlarken öncelikle düşünülmesi gerekenlerden biri, aygıtların fiziksel konumlarıdır [1, 22].

Tipik bir kablolama dolabının aksine, sunucu çiftliği ya da veri merkezinin içinde erişim katmanı aygıtları çoğunlukla yönlendirme ve anahtarlama işlevlerini bir arada yürüten, artıklı, çok katmanlı anahtarlar olabilmektedir. Çok katmanlı anahtarlar, 3. katman işlevlerine ek olarak güvenlik duvarı ve izinsiz giriş koruma özellikleri sağlayabilirler. Erişim katmanına temel bağlantı sağlamaya ek olarak, ağ tasarımcısının göz önünde bulundurması gerekenler aşağıdadır:

- *İsimlendirme yapıları,*
- *VLAN mimarisi,*
- *Trafik akışları,*
- *Önceliklendirme stratejileri,*

3.3. WAN Tasarım Adımları

Adım 1: Ağ gereksinimlerini tanımlamak.
Adım 2: Mevcut ağı değerlendirmek.
Adım 3: Ağ topolojisini ve çözümleri tasarlamak.

3.3.1. Ağ gereksinimlerini tanımlamak

Öncelikle, kurulması gerekli olan WAN için hedeflerin belirlenmesi lazımdır. Bu hedefler genellikle iki kategoriye ayrılır:

Kurumun/Kişinin hedefleri : Oluşturulması planan, temel uygulama amaçları planlanır, eğer mevcutta bir ağ var ise, genişletilme ya da degiştirme sebepleri planlanır ve oluşturulacak olan ağın durumu nasıl değiştireceğine odaklanılır.

Teknik hedefler : Kullanılacak olan teknoloji, aygıtlar ve ilgili işlem hacimleri için bant genişliklerinin hesaplanma işidir. Kurum ya da kişi hedeflerine paralel olarak bu teknik hedefleri belirlemek zorundadır.

3.3.2. Mevcut ağı değerlendirmek

Mevcut ağ ve hizmetler hakkında bilgi toplanır ve analiz edilir. Mevcut ağın işlevlerini, yeni projenin belirlenen hedefleriyle karşılaştırmak gereklidir. Tasarımcı, mevcut aygıtların, altyapının ve protokollerin tekrar kullanılıp kullanılamayacağını, tasarımı tamamlamak için hangi yeni aygıtların ve protokollerin gerektiğini belirler

3.3.3. Ağ topolojisini tasarlamak

Ağ tasarımı için sıklıkla kullanılan stratejilerden biri, yukarıdan aşağı yaklaşımı kullanmaktır. Bu yaklaşımda, ağ uygulamaları ve hizmet gereksinimleri tanımlanır ve ağ, bunları destekleyecek şekilde tasarlanır. Bağlantıların yapılması gereken bütün lokasyonlar farklı kategorilerde gruplandırılır.

Tasarım tamamlandığında, bir prototip ya da konsept kanıtı denemesi gerçekleştirilebilir. Bu yaklaşım, yeni tasarımın, uygulanmadan önce beklendiği gibi çalışacağından emin olunmasını sağlar [1-2, 22].

3.4. Bazı Özelliklerine göre WAN Teknolojileri

WAN bağlantılarını, bir çok niteliklerine göre farklı katagorilerde gruplandırmak mümkündür. Aşağıda WAN için bazı farklı temel özellikler düşünülerek, WAN bağlantı çeşitleri gruplandırılmaya çalışılmıştır [25].

3.4.1. Bağlantı süresine göre (Connection duration)

Adanmış (Dedicated);

- *Her zaman aktif bağlantılardır,*
- *Dolayısıyla maliyet bant genişliği ve mesafe ile doğru orantılıdır.*

Talebe bağlı (On demand);

- *Talebe bağlı olarak bağlantı sağlanır,*
- *Dolayısıyla maliyet kullanım süresi, bant genişliği ve mesafe ile doğru orantılıdır.*

3.4.2. Anahtarlama (Switching)

1) *Devre anahtarlama (Circuit switched);*

- *Uçtan uca bant genişliği tahsis edilir ve kontrol edilir.*
- *Kalıcıdır, talep üzerine degiştirilebilir.*

2) *Paket Anahtarlama (Packet switched);*

- *Eşzamanlı olmayan iletim modu kullanılır (Asynchronous transport network),*
- *Ulaşım ağı üzerinde istatiksel olarak bant genişliği tahsis edilir,*
- *Gider dolayısıyla, bant genişliği garantisine ve diger QOS*
- *parametrelerine bağlıdır.*

3.4.3. Senkronizasyon mekanizmasına göre (Synchronization mechanism)

1) *Harici saat sinyalleri ile (External clocking);*

- *Saat sinyalleri (clocking) cihazda ayrı bir iletken tarafından belirlenir,*

- *Her bağlantı için daha kalın ve daha çok kablo kullanılır.*

2) *Embedded (Gömülü);*
- *Saat sinyalleri (clocking) data akışındaki bit zamanıyla belirlenir,*
- *Her bağlantı için daha az iletken kullanılır.*

3.4.4. Veri aktarım hızı (Data rate)

1) *Düşük bant genişliği (Narrowband);*
- *Veri aktarım hızı 128 kbps (Örneğin:dialup) ve daha düşük olan devrelerdir.*

2) *Geniş Bant (Broadband);*
- *Veri aktarım hızının düşük bant'tan daha yüksek olduğu bağlantı hızları için kullanılan terimdir. Metro ethernet, VPLS, MPLS gibi bağlantı çeşitleri geniş bant bağlantıya örnek verilebilir.*

3.4.5. Sonlandırma (Termination)

1) *Uçtan uca devreler (End-to-end circuits);*
- *Bit senkronizasyon ve data link sonlandırması devre ucunda kontrol edilerek yönetilmektedir. Servis sağlayıcı geçirgen (transparent)'dır.*

2) *Ulaşım ağı şeklindeki devreler (Transport network)*
- *Ara ağ, bit senkronizasyonunu sonlandırır. İçerik eş zamansız bağlantı olarak ulaşım ağı üzerinden taşınır. Paket anahtarlama frame relay, ATM, geniş bant access teknolojileri örnek verilebilir.*

3.4.6. İletişim araçlarına göre (Transmission media)

Bakır : Düşük veri hızları için uzun mesafelerde, yüksek veri hızları için kısa mesafelerde için maliyeti uygun olabilir. Genellikle aşağıda verilen türde bakır

kablolar kullanılır.

- *Çift bükümlü (Twisted Pair),*
- *Koaksiyel Kablo (Coaxial cable).*

Fiber: Daha yüksek veri aktarım hızları ve uzak mesafeler için kullanılır.

- *Çok Kipli (Multimode)*
- *Tek Kipli (Single mode)*

Çizelge 3.1'de niteliklerine göre WAN teknolojileri gösterilmektedir.

Çizelge 3.1. Niteliklerine göre WAN teknolojileri [25].

Bağlantı Süresi	Adanmış	Talebe Bağlı
Anahtarlama	Devre (Circuit)	Paket (Packet)
Senkronizasyon	Harici (External)	Gömülü (Embedded)
Veri Aktarımı	Düşükbant (Narrowband)	Geniş bant (Broadband)
Sonlandırma (Termination)	Uçtan uca (End-to-end)	Taşıyıcı Ağ (Transport network)
İletişim Araçları (Media)	Bakır (*Copper)* -Twisted pair -Coaxial	*Fiber* -Tek Kipli (Mutimode) -Çok Kipli (Single mode)

3.5. WAN Bağlantı Türleri

Wan bağlantı türlerini, sağlanan servise ve buna uygun teknoloji türüne göre biraz daha detaylı inceleyebilmek için göre 4 farklı kategoride toplayabiliriz.

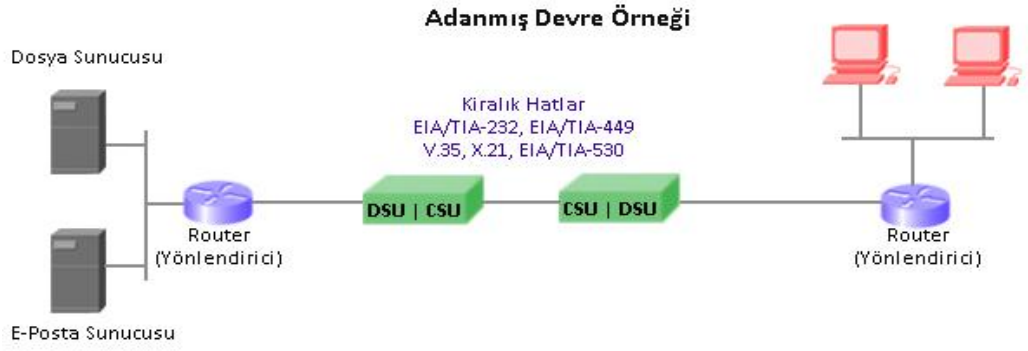
- *Adanmış devre anahtarlamalı (Dedicated circuited switched),*
- *Talebe bağlı devre anahtarlamalı (On-Demand circuit switched),*
- *Paket anahtarlamalı sanal devreler (Packet-switched virtual circuit),*
- *Genişbant bağlantı (Broadband access).*

3.5.1. Adanmış devre anahtarlamalı bağlantılar

Noktadan noktaya ve seril iletimi kullanan bu adanmış devrelerin bir diğer adı da kiralık devrelerdir. Bu tür devreler ile verinin sadece bir hat üzerinden servis

sağlayıcının DCE (Data Communications Equipment) cihazı aracılığıyla, hem saat sinyalinin, hem de verinin kanalize edilmiş formatta iletilmesi sağlanır. Bu durum daha güvenilir bir veri iletimi sağlar. Veri iletişimindeki frekans aralığının ölçüsü bant genişliği olarak bilinir ve ağ sistemlerinde bant genişliği, bir saniyede geçen veri miktarı demektir.

Bu noktadan noktaya adanmış devreler kullanıcı lokasyonundan, devre anahtarlama metodu ile taşıyıcı ağ üzerinden uzak ağ'a öncelikli olarak kurulmuş, bir WAN haberleşme yolu sağlarlar. Kurulan bu yol, taşıyıcı ağ üzerinden ulaşılan bütün uzak ağ'lar için kalıcı olarak ayarlanmıştır. Zamanlama ve veri bağlantı kontrol senkronizasyonu, uçtan uca sağlanır ve korunur. Şekil 3.1'de bir adanmış devrenin nasıl çalıştığı gösterilmiştir.



Şekil 3.1. Noktadan noktaya adanmış bir devre örneği

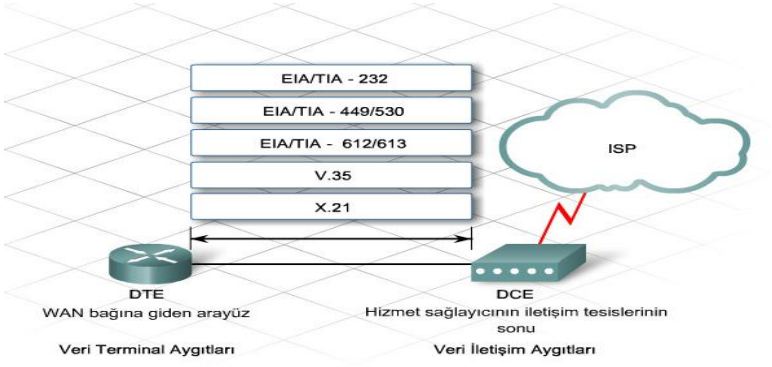
Bu adanmış bağlantılar yönlendiriciler üzerindeki eşzamanlı seri portlarda, bant genişliği 34 mbps'e kadar olan E3, 45 mbps'e kadar olan T3 standardındaki bağlantılarla yapılırlar. Kullanılan diğer bazı tipik bant genişlik standartları 56 kpbs, 64 kpbs, T1, E1'dir. Ülkemizde ise yerel telekom tarafından sağlanan adanmış standartlar şunlardır; 64Kbps, 128 Kbps, 256 Kbps, 512 Kbps, 1 Mbps, 2 Mbps, E1, E2, E3.

Şekil 3.2'de günümüzdeki yönlendiricilerin desteklediği bazı seri iletişim standartları verilmiştir, bunlar;

•*Electronic Industries Association /Telecommunications Industry Association, (EIA/TIA)-232, (EIA/TIA)-449, (EIA/TIA)-530,*

• *V.35 (48 kbps),*

• *X21 (2 mbps).*



Şekil 3.2. Seri standartlar [22].

Bu farklı kapsülleme metodları data-link katmanında kullanıcı trafiği için esneklik ve güvenilirlik sağlar. Kuracağımız WAN ‘da bunlara uygulamalı olarak örnek verilecektir.

Şekil 3.1’de gösterildiği gibi bağlanılan cihaz, CSU/DSU (Channel Service Unit/Data Service Unit) olarak adlandırılır. CSU servis sağlayıcı ağına bağlanırken, DSU ise ağ cihazının seri arayüzüne bağlanır. DSU, yönlendirici gibi seri olarak DTE (Data Terminal Equipment)’den gelen media formatının, anahtarlanmış taşıyıcı ağda, taşıyıcı ağ cihazı WAN switch vb. gibi bir cihaza adapte edilmesini sağlar. CSU/DSU ayrıca senkronizasyon için cihazlar arasındaki saat sinyalini de sağlar. Daha yüksek veri hızlarında bağlantıya ihtiyaç duyan kurum, ya da kişiler için direkt T3/E3 and SONET/SDH (Synchronous OpticalNET work/Synchronous Digital Hierarchy) kullanışlı olabilir.

Adanmış devrelerin özel yapısı, kurum için WAN üzerinde daha iyi bir kontrol sağlar. Çizelge 3.2’de adanmış devreler ile ilgili bazı standartlar verilmiştir.

Çizelge 3.2. Noktadan noktaya adanmış devre türleri

Hat Türü	Sinyal Standardı	Bant Genişliği
56	DS0	56 Kbps
64	DS0	56 Kbps
T1	DS1	1.544 Mbps
E1	ZM	2.048 Mbps
E3	M3	34.064 Mbps
J1	Y1	2.048 Mbps
T3	DS3	44.736 Mbps
OC-1	SONET	51.84 Mbps
OC-3	SONET	155.54 Mbps
OC-9	SONET	466.56 Mbps
OC-12	SONET	622.08 Mbps
OC-18	SONET	933.12 Mbps
OC-24	SONET	1244.16 Mbps
OC-36	SONET	1866.24 Mbps
OC-48	SONET	2488.32 Mbps

Adanmış bağlantılar, veri aktarım hızının sabit olduğu kritik veri trafikleri için ideal olarak düşünülebilir. Bununla beraber, mevcut hattın paylaşımlı olmamasından dolayı, adanmış bağlantılar daha maliyetli olabilir. Genel bir kural olarak, adanmış bağlantılar aşağıdaki durumlar ele alındığıda daha kullanışlı olabilir;

- *Uzun bağlantı sürelerinde,*
- *Kısa mesafelerde,*
- *Garanti edilmesi gereken kritik data trafiklerde.*

Kiralık hatların maliyetleri bir çok noktayı uzak mesafelerde birbirlerine bağladığında, çok yüksek olabilmektedir. WAN üzerinden geçen bütün trafik veri link katmanı seviyesinde kapsüllenmelidir. Kullanılan protokol verinin nasıl çerçeveler olarak kapsüllendiğini ve noktalar arasında frame'lerin transfer edilme mekanizmalarını açıklar. Kiralık hatlar için WAN bağlantıları genellikle aşağıda belirtilen veri bağı katmanı protokolleri kullanırlar. Daha sonra bu protokollerden daha detaylı bahsedilecektir.

• *T1 PPP,*

• *E1 PPP,*

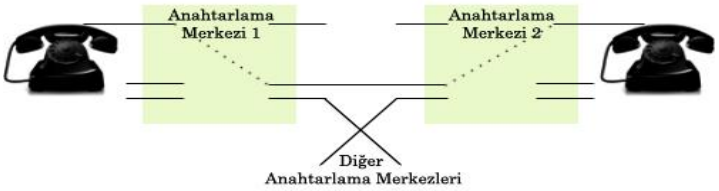
• *Ethernet.*

3.5.2. Taleb'e bağlı devre anahtarlamalı bağlantılar

Devre anahtarlama, her bir haberleşme oturumu için adanmış fiziksel devrelerin taşıyıcı network üzerinden kurulması, devam ettirilmesi ve sonlandırılması işlemlerinin yapıldığı bir WAN anahtarlama yöntemidir

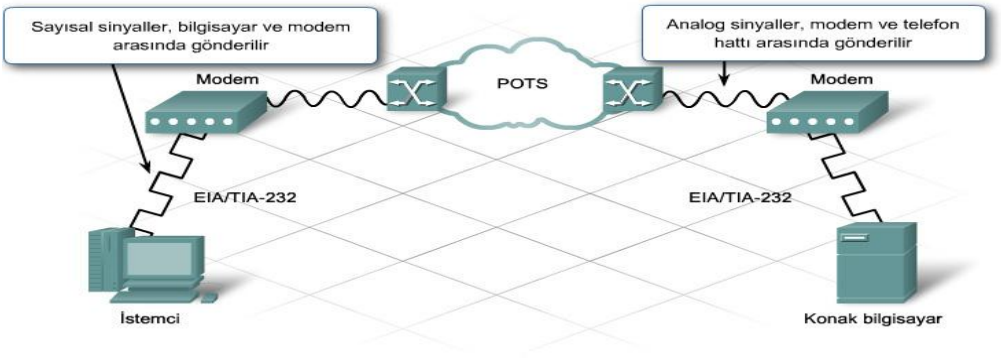
Devre anahtarlamada haberleşecek iki uç düğüm arasında yine bir yol (devre) kurulur ve bu yol, bağlantı boyunca kurulu kalır, veri aktarımı bu yol üzerinden gerçekleşir. (Bkz. Şekil 3.3). Devre anahtarlamalı veri aktarımında iki aşama vardır :

- *Devrenin kurulması aşamasında ilgili uç düğümler arasında özel sinyalleşme mesajları kullanılarak bir yol kurulur.*
- *İkinci aşamada ise veri aktarımı başlatılır.*



Şekil 3.3. Devre anahtarlama gösterimi

Birinci aşamada uç düğümler arasında bir yol kurulamazsa bağlantı gerçekleşmez. Bağlantı iki uç düğümden biri tarafından koparılabilir yani bitirilebilir. Telefon şebekesi bu anahtarlama tipine en güzel örnektir. Zamana duyarlı olan, gerçek zaman uygulamaları için devre anahtarlama en uygun ortamı oluşturur. Daha önceden kurulmuş devre üzerinden oluşturulan veri trafik, bekletilmeden aktarılır



Şekil 3.4. PSTN üzerinden iletisim [22].

Şekil 3.4'te gösterildiği üzere, isteğe bağlı olan devre anahtarlama, adanmış fiziksel bir devrenin PSTN (Public Switched Telephone Network) şebekesi üzerinden kurulması, çalıştırılması ve yönetilmesi, işlemidir.

Haberleşmede amaç verinin bir noktadan, haberleşmek istenen diğer noktaya aktarılmasıdır. Ne yazık ki, her zaman bu iki nokta arasında doğrudan bir hat bulunması pratik olarak çok masraflı ya da imkansızdır. Bu nedenle, veri anahtar adı verilen bağlantı noktalarında bir hattan diğerine aktarılarak uçtan uca iletilir. Anahtarlar ilk telefon hatlarından günümüze kadar, haberleşme sistemlerinin vazgeçilmez elemanları olmuşlardır. Kurulum başlangıcındaki ilk sinyaller iki nokta arasındaki uçtan uca bağlantıyı tayin etmeye yarar.

Bu tür devrelerin avantajı, bağlantı aktif durumda iken, devrenin uç noktasının dinamik olarak seçimi ve ulaşım için bedellerin birikimidir. Maliyet direkt olarak, bağlantı süresi ve uzaklıkla ilişkilidir. Uç noktalar arasındaki trafik hacmi arttıkça, bağlantı süresi de artar. Bazı tipik devre-anahtarlamalı bağlantılar aşağıdakilerdir:

a. Asenkron modem/seri bağlantılar (Asynchronous modem connections),

Asenkron modem bağlantıları var olan mevcut telefon ağ'ını kullanırlar ve maliyetleri düşüktür. Kullanıcılar, telefon ağının bulunduğu bir yerde merkez noktaya kolayca ulaşabilirler. Dolayısıyla asenkron bağlantılar sadece ihtiyaç duyulduğunda, modem üzerindeki asenkron seri bağlantı arayüz'ünden DDR (Dial-

on -Demand Routing) kullanılarak kolayca konfigure edilebilirler. Kısa süreli erişim gerektiği zamanlarda DDR ideal'dir. Asenkron bağlantılar aşağıdaki durumlarda kullanışlıdırlar:

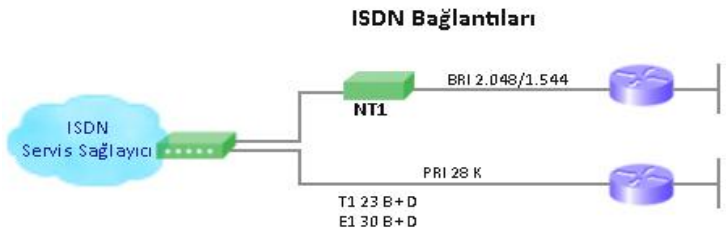
- *Bir yedek hat isteniyorsa (Backup connection),*
- *Bağlanan yer küçük çaplıysa (Mobil kullanıcı veya tek kullanıcılı ofis),*
- *Kısa süreli ve isteğe bağlı bağlantılar isteniyorsa,*
- *Daha düşük network trafiği ve daha az kullanıcı olma durumunda.*

PSTN şebekesi üzerinden taşınan asenkron bağlantılar, dijital sinyallerin analog sinyallere dönüşebilmesi için, her iki uçta da modemlere ihtiyaç duyar. Modem hızları, hat kalitesine bağlı olarak 19.2 kpbs den 56 kpbs değişebilir. Asenkron bir hat üzerinden gönderilmek istenen data trafiği düşük bant genişliği dolayısıyla limitlenebilir.

Yönlendiriciler üzerinden asenkron arama yapma, ya da arama kabul etme için asenkron seri arayüzleri kullanılmalı ve yapılandırılmalıdır. Harici bir modem bağlantısı için kullanılan seri standart EIA/TIA-232'dir. Telefon firmalarının kullandıkları arayüzler ülkelere göre farklılık gösterebilir. Ülkemizde genellikle, RJ-11 adaptör kullanılarak modem'lere bağlantı yapılır.

b. ISDN bağlantıları (Integrated services digital network),

Integrated services digital network bağlantıları, asenkron bağlantılar gibi, WAN erişimi sağlayan anahtarlamalı bağlantılardır. ISDN, PSTN gibi mevcut telefon hatları üzerinden sağlanan bir servistir, fakat dijital olarak sunulan bir servistir. Bu teknoloji ile veri, ses, video aynı anda iletilebilmektedir. Telefon şirketleri tarafından sağlanan bu servis, OSI modelindeki ağ, data link ve fiziksel katmanda bulunan standartları içerir. ISDN standartları ile, bu iletişim metodunun desteklediği donanım ve uçtan uca bağlantı kurma metodolojisi belirlenir.



Şekil 3.5. ISDN

ISDN teknolojisinde bağlantı kurulması ve datanın transferi için kanallar kullanılmaktadır B ve D olmak üzere iki tip kanal vardır. B kanalı datanın transferi, D kanalı da ISDN omurgasına bağlantının sağlanması için kullanılmaktadır (Bkz. Şekil 3.5).

ISDN teknolojisinin temel parçalarından olan B kanalı, datanın taşındığı kanal olarak bilinir. Saniyede 64000 bitlik kapasiteye sahiptir. D kanalı ise servis sağlayıcı tarafındaki ISDN anahtar ile son kullanıcı tarafındaki ISDN cihaz arasında ISDN bağlantısının kurulması için kullanılan kanaldır [7, 25].

BRI (Basic Rate Interface ve PRI (Primary Rate Interface) olmak üzere iki farklı ISDN arayüzü vardır.

ISDN BRI arayüzünde 2 adet B kanalı ve 1 adet D kanalı vardır. '2B+D' olarak da bilinir. B kanalı 64 Kbps, D kanalı 16 Kbps kapasiteye sahiptir. Toplamda 144 Kbps kapasitesi vardır. ISDN BRI iletişim yönlendirici ile bağlı olduğu ISDN anahtar arasında D kanalı daima aktiftir.

PRI için ise iki farklı ISDN arayüzü vardır. Kuzey Amerika ve Japonya'da kullanılan, T1 olarak da anılan arayüzde 23 adet B kanalı ve 1 adet D kanalı bulunur. Avrupa ve dünyanın diğer birçok yerinde kullanılan, E1 olarak da anılan arayüzde 30 adet B kanalı ve 1 adet D kanalı bulunmaktadır. ISDN PRI hatlardaki D kanalı 64 Kbps kapasiteye sahiptir [25].

3.5.3. Paket anahtarlamalı sanal devreler (Packet-switched virtual connections)

Paketler, bir bağlantı sırasında aktarılması planlanan verinin küçük parçalara bölünmüş halidir. Herkes tarafından kabul edilen tek bir paket yapısı yoktur ve donanım teknolojisine bağlı olarak paket yapısı da değişir. Bir ağ teknolojisinde paket aktarımı için oluşturulan yapıya çerçeve (frame) denir. Bir çerçeve genellikle Şekil 3.6'daki yapıya sahiptir [11].

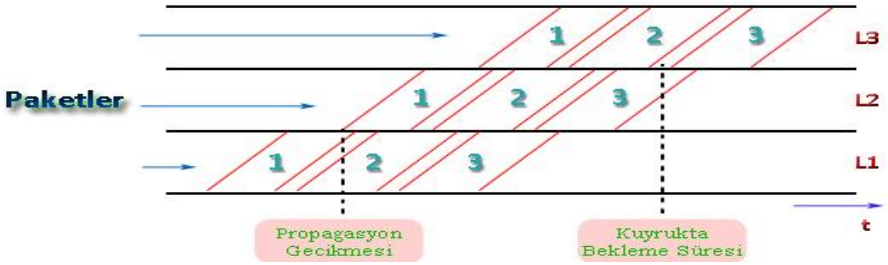
Şekil 3.6. Çerçeve yapısı

Şekil 3.6'da görüldüğü gibi verinin önünde ve arkasında çerçevenin başlangıcını ve sonunu gösteren küçük bloklar vardır. Bu bloklarda adres, hata kontrolü vb. gibi veri aktarımı sırasında kullanılan ağ teknolojisine özel kontrol bilgisi bulunur [11, 22].

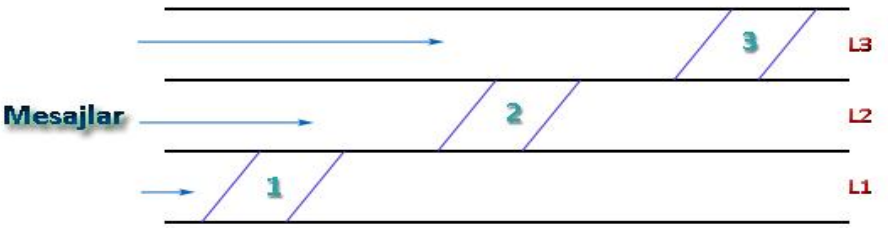
Şekil 3.6'dan anlaşıldığı gibi paketler oluşturulurken taşınan veri miktarı artar. Gerçekte taşınması istenen veriye ek olarak gönderilen fazlalıklara ek denir. Aktarım sırasında ek yük ne kadar azaltılırsa kullanıcı verisine o kadar fazla alan (kapasite) kalır.

Paket anahtarlama temelde mesaj anahtarlamadaki sakla-ve-gönder yöntemini kullanır. Ancak veri tek bir mesaj halinde gönderilmez. Daha küçük boyutlardaki paketlere yerleştirilir. Küçük paketlere yerleştirilmiş veri daha hızlı hareket edebilir. Bir bağlantıya ait paketlerden biri herhangi bir düğüme varırken aynı bağlantının başka bir paketi o düğümden çıkabilir. Paket anahtarlamada da mesaj anahtarlamada olduğu gibi bağlantı öncesinde yol kurulmaya gerek duyulmaz. Paket, mesaj ve devre anahtarlamanın çalışması, zaman bazında, Şekli 3.7'de gösterilmiştir.

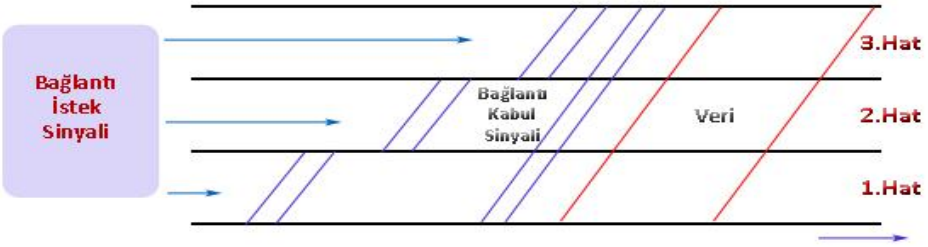
(1)



(2)



(3)



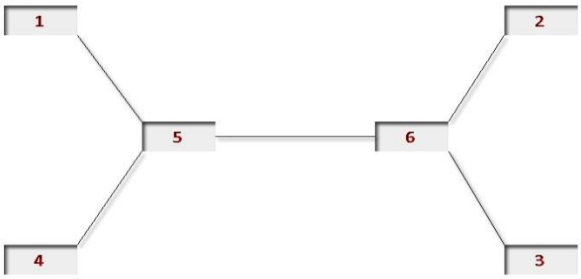
Şekil 3.7. Zaman bazında paket (1), mesaj (2) ve devre (3) paket anahtarlamanın incelenmesi

Paket anahtarlamada aynı bağlantıya ait bir paket bir öncekinden farklı bir yolu kullanarak varış noktasına ulaşabilir. Bu da paketlerin varış düğümünde sıralanmasını gerektirir. Paketlerin varış düğümüne ulaştırılırken farklı yollar izlemesi her paketin düğümler üzerinde ayrı ayrı işlenmesi ve o an için en uygun yoldan varış düğümüne yönlendirilmesinin sonucudur. Bu nokta hataya duyarlılık söz konusu olduğunda bir avantaja dönüşür.

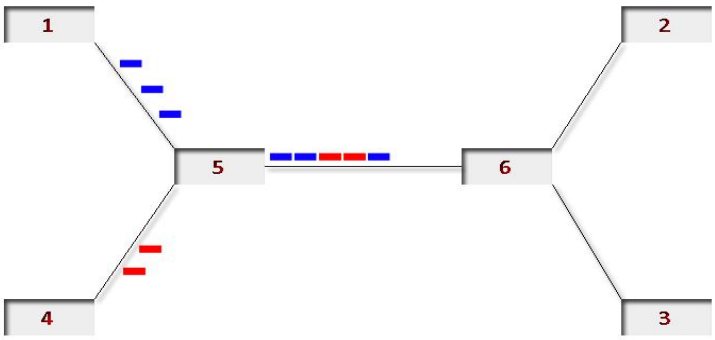
Kaynak-varış arasındaki bir düğüm bozulduğunda ya da bir bağlantı koptuğunda alternatif yolların kullanılması mümkündür. Devre anahtarlamalı yöntemde kurulan yolun değiştirilmesi mümkün değildir. Paket anahtarlama yöntemi ağ üzerindeki

kaynakları en iyi şekilde kullanmayı hedefler. Kaynakları önceden rezerve etmesi söz konusu değildir. Ancak bu durum gerçek zamanlı ve belli bir kapasiteye ihtiyaç duyan uygulamalar için istenmeyen sonuçlar yaratabilir. Bu nedenle, gerçek zamanlı uygulamalarda tercih edilen bir yöntem değildir

Paket anahtarlama temelli ağlarda ağ kaynakları daha iyi paylaşılır. Bu konuyu aşağıdaki basit örnek üzerinde anlatmak daha kolay olabilir. Altı düğümlü (1, 2, 3, 4, 5 ve 6 düğümleri) bir haberleşme ağımız olduğunu ve bu ağ üzerinde devre temelli bağlantıların kurulduğunu düşünelim. Bu durumda, 2 ve 4 düğümleri arasında kurulmuş bir bağlantı devre anahtarlama metodu ile 4-5, 5-6 ve 6-2 hatlarını kullanacaktır. Aynı ağ üzerinde, daha sonra, 1 ve 3 düğümleri arasında başka bir bağlantı kurmak istersek 4 ve 2 düğümleri arasındaki bağlantının bitmesini beklememiz gerekir. Çünkü 5-6 hattının o an meşgül olması, 1 ve 3 düğümleri arasında yeni bir bağlantı kurulmasını engeller. Şekil 3.8'de gösterildiği gibi [11, 22].



Şekil 3.8. Devre anahtarlama yöntemiyle iletişim



Şekil 3.9. Paket anahtarlama yöntemiyle iletişim

Aynı ağ yapısı üzerinde paket anahtarlama tekniği kullanılırsa her iki bağlantı da Şekil 3.9'da gösterildiği gibi gerçekleşebilir. Bu durumda ikinci bağlantı birinci bağlantının sona ermesini beklemeden paket aktarımına başlayabilir. Bu da kaynakların nasıl daha verimli kullanıldığını gösterir.

- *Sanal devreler (Virtual circuits)*

Görüldüğü gibi devre anahtarlamanın ve paket anahtarlamanın kendilerine göre hem avantaj hem de dezavantajları var. Her iki teknikte de avantajlardan faydalanmak için sanal devreler (virtual circuits) geliştirilmiştir.

Sanal devrelerde, devre anahtarlamada olduğu gibi, bağlantı isteği geldiğinde bağlantının gerçekleneceği yol belirlenir ve bu yol üzerindeki kapasitenin bir bölümü bağlantı için ayrılır. Ayrılan kapasite bağlantının ihtiyaçlarına cevap verecek düzeyde olmalıdır. Aksi halde bir devre kurulamaz ve bağlantı gerçeklenemez.

Sanal devreler üzerinde veri paketler halinde taşınır. Ancak bu paketlerin başlık bölümleri paket anahtarlamada kullanılan paketlerin başlık bölümlerinden daha küçüktür. Çünkü kurulmuş bir yol üzerinde yönlendirme yapmak daha kolaydır. Bu nedenle paketlerdeki ek yük daha az olur. Paketlerin başlıklarındaki yönlendirme amaçlı bilgiler bağlantının kurulması sırasında belirlenir ve daha sonra yaratılan paketlerin başlığında bu bilgiler kullanılır.

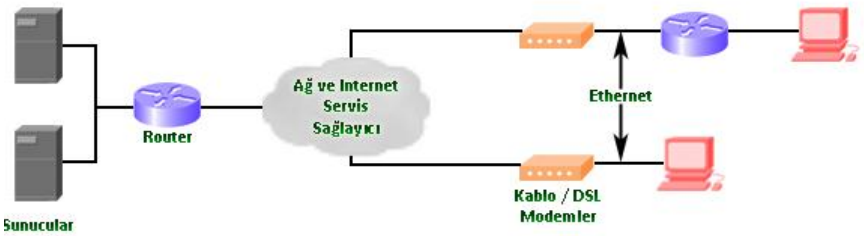
Bir sanal devreye ait paketler her zaman aynı yolu takip ederek varış noktasına ulaşır. Paketlerin sırasının değişmesi mümkün değildir.

Bir hat, kapasitesi mümkün olan en çok sanal devre tarafından paylaşılabilir ve bir sanal devre, kaynak veya varış düğümlerinden herhangi birinin isteği sonucu koparılabilir.

3.5.4. Geniş bant erişim (Broadband access)

Günümüzde evlerimizde kullanmış olduğumuz internet bağlantıları bile, dial-up modemler ve yavaş çalışan sistemlerden, geniş bant erişim sağlayabilecek olan bir çok farklı teknolojiye genellikle, mevcut telefon kabloları ve kablo tv kablolarının alt yapısını kullanarak geçmiştir. Geniş bant (broadband) terimi genel olarak 128 kpbs üzerindeki bağlantılar için kullanılmaktadır. Geniş bant bağlantılar, eski teknolojilerin aksine merkezlere, uzaktan bağlanıp yönetim, bakım gibi ayarların yapılabilmesine olanak sağlarlar. Yüksek genişbant bağlantılar, kullanılan özel sanal ağlar (VPN- virtual private networks) sayesinde, bir çok kurum kendi istasyonlarına uzaktan bağlanabilir, video ve ses konferansları yapabilir, hatta kendi WAN'ını oluşturabilmektedir [25].

Geniş bant erişim teknolojileri, kablo modem bağlantıları, bir çok farklı DSL teknolojisi, (ADSL, IDSL, SDSL) son zamanlarda daha aktif kullanılmaya başlanılan, metro-ethernet, IP-MPLS (multi protocol label switching), VPLS (virtual private lan service) gibi ethernet tabanlı çalışan teknolojileri de içermektedir. Geniş bant bağlantıları sağlamakta karşılaşılan en büyük güçlük, genellikle, mevcut alt yapının gerekli bant genişlikleri için yetersiz kalmasıdır. Şekil 3.10'da geniş bant bağlantıların çalışma prensibi yüzeysel olarak gösterilmiştir.



Şekil 3.10. Geniş bant bağlantı örneği.

Günümüzde kullanılan bazı geniş bant WAN bağlantılarına bakmak gerekirse :

I. Metro ethernet

Metro ethernet, Gpbs (Gigabits per second) bağlantıları da dahil olmak üzere, çok çeşitli yüksek bant genişlik seçenekleri sunar. Üniversiteler, bankalar gibi aynı şehir içinde birçok şubesi bulunan büyük kurumlar metro ethernet'in getirdiği faydaları kullanırlar. Metro ethernet, anahtarlama teknolojisini kullanarak, merkez ofis ile tüm uzak noktaları birbirine bağlar ve yüksek miktarda verinin diğer yüksek bant genişliği bağlantı seçeneklerine göre, daha hızlı ve daha ekonomik biçimde aktarılmasını sağlar.

Genellikle, fiber optik kablo üzerinden, 5Mbps ile 10Gbps arasında, ölçeklenebilir, esnek, düşük maliyetli ve her türlü veri akışına imkan verebilen bir teknolojidir. Protokol dönüşümlerine ihtiyaç duymadan, uçtan uca ethernet taşıyan, simetrik bir iletim yapısına sahiptir. Noktadan noktaya ya da çok noktadan tek noktaya gibi farklı erişim imkanları sağlar [6].

II. MPLS (Multiprotocol Label Switching)

MPLS (Multiprotocol Label Switching), türkçe çok protokollü etiket anahtarlama demektir ve ağ üzerinden paketleri göndermek için kullanılan bir yöntemdir. Alışılagelmiş paket gönderme yöntemlerinde veri ağ üzerinden gönderilmek için kaynak ve hedef IP'lere göre her bir pakete eklenir ve ağ üzerinden paketlerin gönderilmesi esnasında, yönlendiriciler tarafından hedef IP'ler okunur, paket alıcı sisteme yönelticilerle teslim edilir. Ayrıca, farklı iletişim teknikleri (protokolleri) kullanan her bir sistem değişikliğinde, paketler yeni sistem için hazırlanır. Bu eylemlerin devamlı tekrarlanması aktarım hızını azaltır. Bu işlemlerin aksine, MPLS'de bir etiket IP adresleri ile birlikte bir çok iletişim yöntemleri tarafından tanınan paketlere eklenir. Bu eklenmiş etiketler tüm yönlendiricilere tanıtılır.

Dolayısıyla, aynı etiketi taşıyan kaynak ve hedef noktalar tüm ağ tarafından tanınır ve bu noktalar arasındaki iletişim daha yüksek hızda yapılabilir.

Belirtildiği üzere, ağ teknolojisinde yönlendirme işlemleri yavaş yapılmaktadır. Fakat MPLS teknolojisi ile ağın giriş noktalarından çıkış noktaları belirlenerek yönlendirme işlemleri bir kez yapılır ve ağın içinde hızlı bir şekilde ilerlenir. Bu yönlendirme işleminin hızlı bir şekilde yapılabilmesi için MPLS teknolojisinde etiketler kullanılmaktadır.

MPLS teknolojisinde TE (Traffic Engineering-Trafik Yönetimi/Mühendisliği) kullanılır. Trafik yönetimi bir sistemdeki hopların (yönlendirici noktalarının) birbirleriyle olan veri iletişimini, birbirlerine olan uzaklıklarının, bir yönlendiriciden diğer yönlendiriciye en kısa yoldan ulaşılması ve yönlendirici haritası çıkarılarak, yönlendiriciler üzerindeki trafiğin yönetilmesidir [26].

MPLS teknolojisinin en önemli avantajlarından birisi, bir yönlendirici ile diğer yönlendirici arasındaki veri iletim yolu tıkandığı zaman verinin en kısa mesafede bulunan başka bir yönlendiriciye yönlendirilmesi veya daha az tıkanabilecek olan başka bir yola yönlendirilmesidir. Bu şekilde veri paketlerinin kaybı azalır ve uzun süreli tıkanmalar yaşanmaz. MPLS protokol ve birimlerine, kısaca bakmak gerekirse:

Yönlendirme (routing) : Ağ tarafında paketlerin kendi içerisinden geçirilip gönderilmesi olayını tarif etmek için kullanılır. Bir bilgisayar ağında pek çok yönlendirici bulunmakta ve ağa değişik şekillerde bağlanabilmektedir. RIP (Routing Information Protocol) ve OSPF (Open Shortest Path First) gibi yönlendirme protokolleri, kendisinden sonra gelecek olan yönlendiriciye yönlendirilmesini sağlar. Bunun için yönlendirme protokolleri yönlendirici tabloları kullanır. Bu tablolar paketin ulaştığı yönlendiricide daha sonra gideceği adres'e transfer edilmesi gereken bir sonraki yönlendiricinin belirlenmesini sağlar.

Etiket (Label) : Oldukça kısa, sabit uzunlukta ve gönderme işlemlerinde kullanılan 4 byte 'lık bir çeşit işaretleme başlığıdır (Bkz. Şekil 3.3).

Çizelge 3.3. MPLS paket yapısı [26]

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

MPLS başlığı (32 bit)	IP paketi

Etiket Alanı (20 Bit): *MPLS etiketinin gerçek değerini taşır.*

Exp. Bitleri (3 Bit): *Ağ içinde yer alan paketin kuyruğa girme ve ayırma algoritmalarını etkiler.*

S Alanı (1 Bit) : *Hiyerarşik olarak etiket depolamayı destekler.*

TTL (Time to Live) (8bit) : *Bilinen IP'deki TTL (Time to Live) ile aynıdır. Yaşama süresini belirtmek için kullanılır.*

MPLS, yığın şeklinde organize edilmiş olan etiketleri bir paket içinde taşımaya izin verir. S bitleri, o anda eklenen etiketin son olup olmadığını göstermek içindir. Etiket yığınlarında 3 tane işlem yapılabilir.

- *En üstteki etiketi yeni bir etiket ile değiştirilebilir.*
- *Yığından etiketi çekelebilir.*
- *Bir veya birden fazla yeni etiket eklenebilir.*

Bunun yanısıra, MPLS işlevlerini yürütmek adına, anahtarlama, kontrol mekanizması, iletim mekanizması, yönlendirme tablosu, FEC (Forwarding Equivalence Class), ELSR (Edge Label Switch router), LRS (Label Switch Router), etiket dağıtım protokolü (LDP- Label Distribution Protocol) gibi önemli mekanizma ve protokoller bulunur.

III. VPLS (Virtual Private LAN Service) teknolojisi

VPLS, günümüz iletişim ağı ortamında türkçe, "Sanal Özel Yerel Ağ Hizmeti" olarak adlandırılan bir terimdir. VPLS, genellikle geleceğin iletişim ağı olarak anılır. VPLS için ikinci katman MPLS terimi de kullanır, çünkü VPLS mevcut MPLS çekirdeğini ikinci katman seviyesinde (Layer-2) kullanarak çok noktadan çok noktaya iletişim sağlamaktadır. VPLS teknolojisini, getirmiş olduğu kolaylıklar, ekonomik kazanç ve diğer teknik özellikler açısından, ihtiyaçlarımız ile paralellik gösterdiği için, kurmuş olduğumuz, örnek modern WAN'da biz bu teknolojiyi kullanmayı planladık.

Bugün artan popülerliğine rağmen, VPLS aslında sadece kısa bir süredir kullanımdadır. VPLS aslında, çok noktadan çok noktaya IP/MPLS ağ'ı üzerinden ethernet tabanlı iletişim sağlayan bir teknolojidir. Dolayısıyla, ethernet VPLS'in ayrılmaz bir parçası olduğundan, ethernet'in nasıl çalıştığını ve bir işletme ağı içerisinde nasıl kullanıldığını anlamak oldukça önemlidir [13, 14].

VPLS, ethernet anahtarı işlevini şunları yaparak görür :

- *Ethernet çerçevelerini yönlendirerek,*
- *Sanal LAN (VLAN) üzerindeki tüm bağlantı noktalarına bilgileri yönlendirerek,*
- *Dinamik olarak son istasyonlar için medya erişim kontrolü (MAC) adreslerini (LAN bağdaştırıcıları ile ilişkili özgün adresler) öğrenerek.*

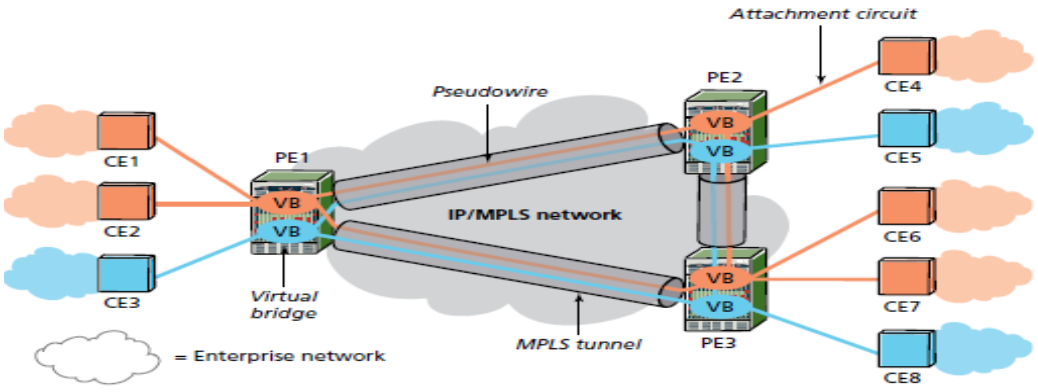
VPLS, geniş alan ağı üzerinde bir LAN'ın işlevselliği ile aynı işi yapar. VPLS, sanal olarak yaratılan tüneller sayesinde coğrafi olarak dağınık olan bir çok noktaya ethernet yayın alanları sayesinde erişir. Her yerel alan ağ, ilgili PE (Provider Edge)' ye kadar uzatılır. İlgili PE bir anahtar ya da köprü cihazı gibi davranıp, diğer bütün yerel ağ'lara bağlanmak için tek bir köprülenmiş yerel alan ağ oluşturur.

Genellikle bir VPLS, CE (Customer Edge), PE ve MPLS çekirdeğinden oluşur, bunların yapmış olduğu işlevler ise;

CE, hat sağlayıcının lokasyonunda konumlandırılmış olan, bir yönlendirici ya da anahtar cihazı olabilir ve bu cihaz hat sağlayıcı ya da hizmet satın alan kurum tarafından yönetilir. VPLS'te CE, PE'ye ethernet arayüzleri sayesinde bağlanır.

PE cihazı, diğer bütün PE'ler ile haberleşme için gerekli sanal tünellerin kurulduğu ve VPLS içinde haberleşmenin sağlandığı hat sağlayıcı ucudur. VPLS, bir ethernet ikinci katman haberleşme metodu olduğundan, PE'ler haberleşmeyi media access control (MAC) adreslerini öğrenme, köprüleme ve yenileme tabloları tutarak sağlarlar. PE'lerin birbirine bağlanması daha önce de belirttiğimiz üzere IP/MPLS çekirdeği sayesinde MPLS etkiketleri üzerinden olur. Kısaca VPLS, ethernet çerçevesini, MPLS etiketleri aracılığıyla, iletişim ağı boyunca taşır [13, 14].

Bütün VPLS'lerde, *tam örgülü (full mesh)* yapıyı sağlayabilmek için iç tüneller (pseudo wires) yaratılmıştır ve bunlar PE noktalarının VPLS'e dahil olmasını sağlarlar. Bir otomatik algılama mekanizması PE'lerin VPLS'e katılımına yardımcı olur. Şekil 3.11'de MPLS yapısı gösterilmiştir.



Şekil 3.11. MPLS genel çalışma yapısı

VPLS, işletmelerin bant genişliğini megabitlerden gigabitlere ölçeklendirmesine olanak sağlayarak, ethernet'in tüm yararlarını sunar. Donanımların iyileştirilmesi

kolay olduğu için, bant genişliği gereksinimleri kısa zamanda karşılanabilir. Daha yüksek hızda bir hizmete ölçeklendirmek, var olan donanımda küçük bir değişiklik yaparak kolay olabilir. Çoğu işletmenin hali hazırda, yerinde ethernet donanımı mevcuttur, VPLS kullanmak düşük maliyetli (cost effective) bir çözümdür. Ayrıca, yüksek hızlara ulaşmak, bakırdan fibere geçiş yapmayı gerektirmez. Hizmet, protokolden bağımsızdır, IP, IPX ve diğer protokolleri de destekler. VPLS'in yararlarından biri de, yönlendirme esnekliği ve kontrolüdür. Ethernet'in özünde olan herhangi birinden diğerine bağlanabilmek yeteneği, yeni noktaların eklenmesini veya çıkarılmasını kolaylaştırır. Bir işletme, bir kere ağa bağlandığı zaman, ağ üzerindeki herhangi bir yere ulaşabilir. Bir ethernet anahtarına benzer olarak, VPLS, yeni bir nokta çevrimiçi olduğunda, tablolarını günceller. Yeni bir siteyle iletişim kurabilmek için, ağ üzerinde var olan noktalarda bir değişiklik yapılmasına gerek kalmaz.

VPLS ile işletme, yönlendirme üzerinde kontrolü ele alır ve taşıyıcıyla 3. katman tablolarını paylaşmaz. Bu, yollarını paylaşmak istemeyen ve güvenlik endişesi taşıyan işletmeler için önemli bir faydadır. Buna ek olarak, VPLS 2. katman bir hizmet olduğundan dolayı, işletmenin sınır ağ geçidi protokolü (Border Gateway Protocol-BGP) gibi, yönlendirme protokollerinin varlığından endişe duymasına gerek kalmaz, çünkü onlar şeffaftır. VPLS, SNA, NetBIOS ve Apple Talk gibi eskiden kalma protokolleri de destekler. Ethernet yaygın bir şekilde kullanıldığı için, VPLS uygularken işletmenin personelinin eğitilmesi gerekmez, ya da çok az bir eğitim gerekir.

Eğer bir işletme, örgülü bağlantıya (meshed connectivity) ve iletişim ağını ölçeklendirebilmeye (scale the network) gereksinim duyuyorsa, VPLS iyi bir çözümdür. IP yolları bir sağlayıcıyla paylaşılmadığından dolayı, yönlendirmeyi kontrol etmek isteyen ve kendi ağlarını ve bağlantılarını yönetmek isteyen kurumlar için oldukça uygundur.

İşletmeler, var olan yerel ethernet ara yüzlerinden faydalanabilir ve iletişim ağlarını geniş alan ağlarına genişletebilirler. VPLS, örgülü olmayan ağların, ethernet

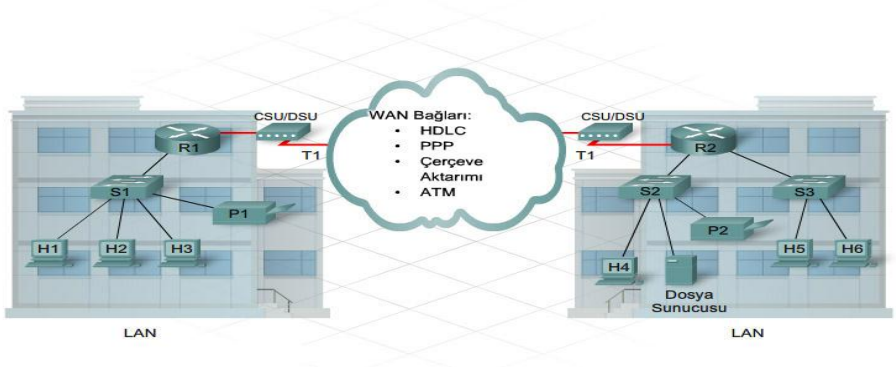
bağlantısına ihtiyaç duyulmayan, yüksek sayıdaki noktaların bir ağ içerisinde birbirleriyle iletişim kurmaları gereken yerlerin veya IP yollarını duyurmak (advertise IP Routes) isteyen bir işletmenin gereksinimini karşılayamayabilir. Ethernet'in bazı coğrafi kapsam sınırlamaları olduğu için, belirli bölgelerde daha büyük ağları tamamlamak amacıyla da kullanılabilinir, fakat coğrafik olarak dağılmış birden çok yer olduğunda yetersiz kalabilir.

Bunlara ek olarak, yönlendiricilerin barındırabileceği MAC adreslerinin de sınırları vardır. Birçok yol gerektiren daha büyük ağlar için, IP adresleme ile birlikte 3. katman (Layer 3) MPLS VPN, daha uygun olabilir. Çünkü ikinci katman'da yönlendirici tablosunda istenildiği kadar MAC adresi tutulamayabilir.

VPLS, sorun çözmek (troubleshooting) için, küme denetlemesi (cloud monitoring) araçları gerektirmesi açısından, 3. katman MPLS VPN'ye benzer. Diğer 2. Katman hizmetlerinin, bağlantının açık ya da kapalı olduğunu gösteren açık sınırlama noktaları (dmarcs) mevcuttur.
Sonuç olarak VPLS, kolay ölçeklendirilebilir mimarisine, esnekliğine ve ekonomik olarak karşılanabilirliğine bağlı şekilde, giderek daha popüler hale gelmektedir. Günümüzde kullanılan birçok teknolojide olduğu gibi, VPLS'in iyi bir çözüm olup olmadığına karar verebilmek için, işletmenin gereksinimleri göz önünde bulundurulmalıdır.

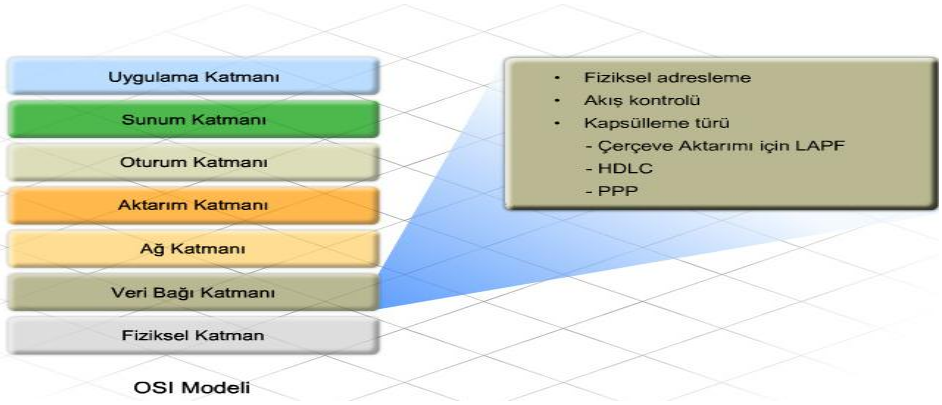
3.6. WAN Kapsülleme (Encapsulation) Protokol Belirleme

WAN, her biri farklı avantajlar sunan değişik teknolojiler kullanır. Kullanılan teknolojiye bağlı olarak, veri biçimini kabul edilebilir hale çevirmek bir modem ya da CSU/DSU gibi farklı cihazlar gerekebilir (Bkz. Şekil 3.12).



Şekil 3.12. Bazı kapsülleme örnekleri ile noktadan noktaya devreler

Kapsülleme, veriler WAN aracılığıyla aktarılmadan önce gerçekleşir. Kapsülleme, ağda kullanılan teknolojiye bağlıdır ve belirli bir biçime uygulanır. Veri hatlar üzerinden aktarılmak üzere bitlere çevrilmeden önce, 2. katman'da kapsülleme adres ve kontrol bilgileri eklenir (Bkz. Şekil 3.13).

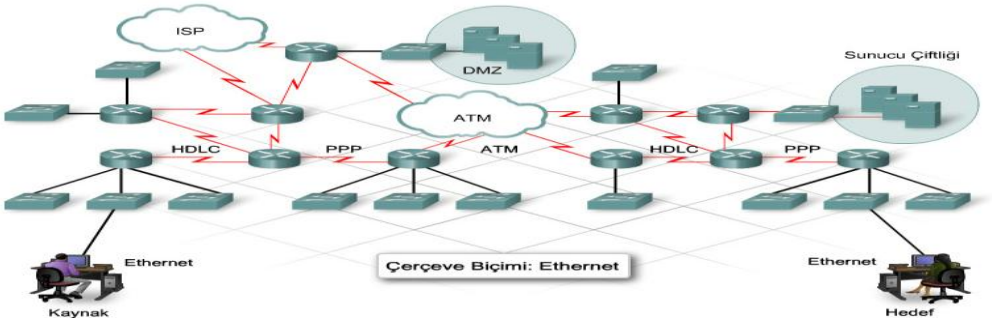


Şekil 3.13. Kapsülleme yapılan katmanlar [22]

İkinci katmanda eklenen başlık bilgileri, fiziksel ağ iletiminin türüne göre belirlenir. Bir LAN ortamında, en sık kullanılan teknoloji genellikle ethernet'tir. Veri bağı katmanı, bu yüzden paketi ethernet çerçevelerine kapsüller. Çerçeve başlıkları, kaynak ve hedef MAC adreslerine ek olarak, çerçeve boyutu ve zamanlama bilgileri gibi belirli ethernet kontrollerini içerir.

Benzer şekilde, çerçevelerin WAN ağı üzerinde aktarım amacıyla kapsüllenmesi, ağda kullanılan teknolojiyle eşleşir. Örneğin, ağda çerçeve aktarımı kullanılıyorsa,

gereken kapsülleme türü de çerçeve aktarımı'na özgüdür.Ayrıca, bir WAN'da bir çok farklı kapsülleme kullanılabilir (Bkz. Şekil 3.14).



Şekil 3.14. Bir ağdaki kapsülleme örnekleri [22]

En sık kullanılan 2. Seviye seri hat kapsüllemelerinden ikisi, HDLC (High level-data link control) ve PPP (Point to Point Protocol)'dür.

3.6.1. **Üst seviye veri bağı denetimi** (HDLC -High level-data link control)

Üst seviye veri bağı denetimi (High Level-Data Link Control), standart bir bit-odaklı veri bağı katmanı kapsüllemesidir. HDLC, iki nokta arasında hatasız iletişim sağlayan eşzamanlı seri bir aktarım kullanır. HDLC, onaylamalar ve pencere düzeni kullanarak akış ve hata kontrolüne izin veren bir 2. seviye çerçeveleme yapısı tanımlar ve her çerçeve, veri çerçevesi ya da kontrol çerçevesi olmasına bakılmaksızın aynı biçime sahiptir.

Standart HDLC çerçevesi, çerçevenin taşıdığı protokolün türünü tanımlayan bir alan içermez. Bu sebepten dolayı, HDLC temelli standartlar aynı linkte birden fazla protokolü desteklemez. Cisco HDLC ise, tür alanı olarak bilinen ve birden fazla ağ katmanı protokolünün aynı anda paylaşmasına izin veren, fazladan bir alan içerir. Cisco seri bağlarında, varsayılan Veri Bağı Katmanı kapsüllemesi, Cisco HDLC'dir.

3.6.2. PPP (Point to point protocol)

PPP ise, HDLC gibi, noktadan noktaya seri bağlantılar için bir veri bağı katmanı kapsüllemesidir. Noktadan noktaya bağ üzerinde çoklu protokol datagramları taşımak ve kapsüllemek için katmanlı bir yapı kullanır. PPP standart temelli olduğu için, farklı üreticilerin aygıtları arasında iletişimi mümkün kılar (Bkz. Şekil 3.15).

Şekil 3.15. PPP kapsülleme ile basit bir örnek

- *Aşağıdaki arayüzler PPP'yi destekler:*
- *Eşzamansız seri*
- *Eşzamanlı seri*
- *Yüksek Hızlı Seri Arayüz (HSSI)*
- *Tümleşik Hizmetler Sayısal Ağı (ISDN)*

PPP oturumları, üç aşamalı bir süreçten geçer: Bağ kurulumu, kimlik doğrulama (tercihe bağlı) ve ağ katmanı protokolü.

i. Bağ kontrol protokolü :

PPP, noktadan noktaya bağları kurmak, kullanmak, doğrulamak ve kesmek için bağ kontrol protokolü'nü (LCP-Link control protocol) kullanır. PPP, veri bağını ayarlamak ve denemek için LCP çerçeveleri gönderir. LCP çerçeveleri, bağ doğrulama, sıkıştırma ve maksimum iletim birimi (MTU-Maximum Transmission Unit) gibi ayarları gözden geçiren bir yapılandırma seçeneğine sahiptir. Eğer bir yapılandırma ayarı eksikse, varsayılan değeri verir. Bağ doğrulama ve bağ kalitesi belirleme testleri, link kurulumu aşamasında tercihe bağlı parametrelerdir. Link kalitesi belirleme testi, ağ katmanı protokollerini taşıyacak yeterliliğe sahip olduğunu doğrular. Bu gibi tercihe bağlı parametreler, yapılandırma onay çerçevesinin

alımından önce tamamlanır ve yapılandırma onay çerçevesi alınınca, bağ kurulumu aşaması tamamlanır. Ek olarak, WAN bağında bulunan kontrol seçeneklerini gözden geçirir ve ayarlar [25, 27].

LCP'nin kontrol ettiği durumların bazıları aşağıdadır:

- *Kimlik doğrulama,*
- *Sıkıştırma,*
- *Hata algılama,*
- *Çoklu bağ,*
- *PPP geri çağrımı.*

LCP ayrıca:

- *Değişken paket boyutlarını destekler,*
- *Sık görülen ayar hatalarını algılar,*
- *Bağın doğru çalıştığını ya da çalışmadığını belirler.*

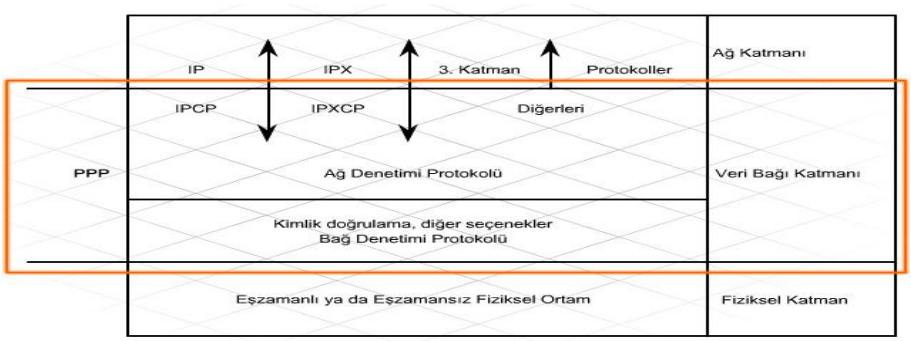
ii. Kimlik doğrulama aşaması

Kimlik doğrulama aşaması, bağlanan yönlendiricileri tanımak için parola koruması sağlar. Kimlik doğrulama, iki yönlendirici parametreleri ayarlamayı kabul ettikten sonra, ancak NCP (Network Control Protocol) görüşme aşaması başlamadan önce yapılır [25, 27].

iii. Ağ kontrol protokolü

PPP, aynı iletişim bağında çalışmaları için farklı ağ katmanı protokollerini kapsülleyen ağ kontrol protokolü'nü (NCP) kullanır. PPP, IP ya da IPX gibi bir ya da daha fazla ağ katmanı protokolünü seçmek ve yapılandırmak için NCP paketleri gönderir. Eğer LCP bağı kapatırsa, gereken eylemi gerçekleştirebilmeleri için ağ katmanı protokollerini bilgilendirir (Bkz. Şekil 3.16).

PPP bağında taşınan ağ katmanı protokollerinin hepsi, farklı birer NCP gerektirir. Örneğin; IP, IP Kontrol Protokolü (IPCP), IPX ise IPX Kontrol Protokolü'nü (IPXCP) kullanır. NCP'ler Ağ Katmanı protokolünü belirten kodları içeren alanlara sahiptir. PPP bağı kurulduğunda, LCP ya da NCP çerçeveleri bağı kapatıncaya ya da etkinlik zamanlayıcılarından biri bitene kadar etkin kalır. Kullanıcılardan biri de bağı kapatabilir [25, 27].



Şekil 3.16. PPP kapsülleme basamakları [22]

3.6.2. **Çerçeve aktarımı** (Frame relay)

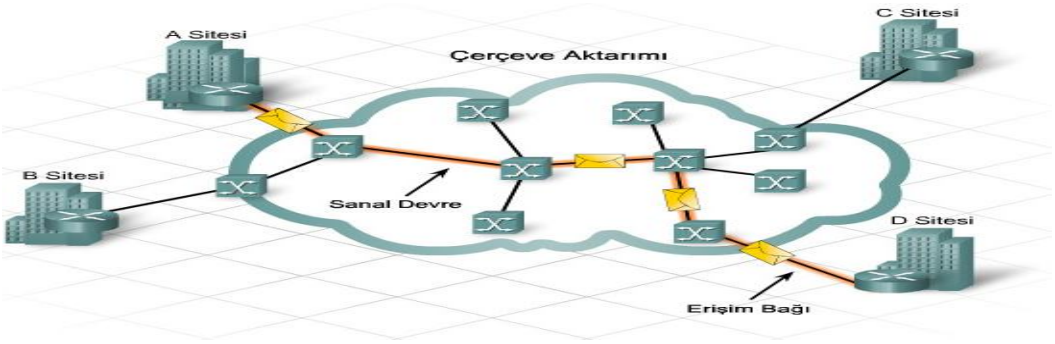
Sık kullanılan 2. Seviye WAN kapsüllemelerinden biri de çerçeve aktarımı'dır (Bkz. Şekil 3.17). Çerçeve aktarımı ağları, ethernet benzeri, ancak yayın trafiğini iletmeyen çok erişimli ağlardır. Çerçeve aktarımı, bir yayınsız çoklu erişim ağı'dır.

Çerçeve Aktarımı, değişken uzunlukta paketlerle, paket anahtarlama teknolojisi kullanır. Ayrıca, kullanılabilir bant genişliğini en iyi şekilde kullanmak için de STDM (Statistical Time Division Multiplexing)'den yararlanır.

Yönlendirici, ya da DTE (Data Terminal Equipment) aygıtı, hizmet sağlayıcısına çoğunlukla kiralık hat aracılığıyla bağlanır. Hizmet sağlayıcısının en yakın bulunma noktasına ise, bir çerçeve aktarımı anahtarı, ya da DCE (Data Communications Equipment) aygıtı aracılığıyla bağlanılır [7, 25].

Ağın hedef ucunda bulunan uzak yönlendirici de bir DTE aygıtıdır. İki DTE aygıtı arasında kurulan bağlantı bir sanal devre (VC-Virtual Circuit)'dir.

Sanal devre, hizmet sağlayıcısı tarafından önceden yapılandırılan PVC (Perminant Virtual Circuit)'ler kullanılarak kurulur. Pek çok hizmet sağlayıcısı, çerçeve aktarımı ağlarında SVC (Switched Virtual Circuits) kullanılmasını desteklemez; hatta buna izin vermez.



Şekil 3.17. Frame relay ile kapsülleme [22]

4. WAN TEKNOLOJİ SEÇİMİ

Daha önce belirttiğimiz gibi bir WAN bağlantısı seçerken verilecek karar için, büyük ölçüde WAN bağlantısının kullanım amacı doğrultusunda, bant genişliği hesaba katılarak, gereken teknoloji seçiminin yapılmasından sonra hesaplanacak maliyeti büyük önem arzeder. Genellikle küçük işletmeler için yüksek bant genişliği sağlayabilen *MPLS, VPLS, ATM* gibi bağlantı türlerini karşılamak zor olabilir ve bu yüzden daha çok DSL, T1, E1 gibi noktadan noktaya bağlantıları tercih ederler. Farklı önemli bir nokta ise, yüksek bant genişliği isteyen uygulamaların, coğrafi olarak güçlüklerin olduğu bölgelerde bulanamayabileceği riskidir. Genellikle lokasyonlar şehir merkezlerine yakın olduğu sürece desteklenen WAN bağlantı hizmetleri de doğru orantılı olarak daha çok çeşittir.

Hangi WAN bağlantısının seçileceğine ilişkin kararı etkileyen önemli faktörlerden birinin, işletmenin bağlantıyı ne amaçla kullanacağıdır. Eğer gerçek zamanlı ve kritik data taşınıyorsa, SLA'nın (Service Level Agreement) daha yüksek bir düzeyde olması gerekir. Bazı işletmeler için WAN bağlantısı ile birlikte hizmet seviyesi anlaşması (SLA) destekleme olanağının olması, verecekleri kararı etkiler. Çevirmeli bağlantı, DSL bağlantısı ve kablo bağlantısı gibi düşük maliyetli WAN bağlantılarında genellikle SLA olanağı sunulmaz.

Ağ kurulumunu planlarken dikkate alınması gereken diğer önemli bir nokta da satın alınacak olan donanımlardır. Ağ iletişim donanımları, satın alınmadan ve konak noktalara bağlanmadan önce, ağın mantıksal ve fiziksel topoloji haritalarının tasarlanıp belgelenmesi gerekir. Bu hususta, dikkate alınması gerekenleri, maddeler halinde yazarsak ;

Ağ'ın kurulacağı fiziksel ortam:

- *Sıcaklık denetimi: Tüm cihazların düzgün çalışması için belirli sıcaklık aralıkları ve nem gereksinimleri vardır.*
- *Güç çıkışlarının kullanılabilirliği ve konumlandırılması gerekmektedir.*

Ağ'ın fiziksel yapılandırması:

- *Yönlendirici, anahtar ve konak bilgisayar gibi cihazların fiziksel konumu düzenlenmelidir.*
- *Tüm cihazların birbirine bağlanma şekli ayarlanmalıdır.*
- *Kullanılacak tüm kabloların konumu ve uzunluğu hesaplanmalıdır.*
- *Konak bilgisayar ve sunucu gibi uç cihazların donanım yapılandırması yapılmalıdır.*

Ağın mantıksal yapılandırması:

- *Yayın ve çatışma etki alanlarının konumu ve boyutu düzenlenmelidir.*
- *IP adresleme şeması çıkarılmalıdır.*
- *Adlandırma şeması çıkarılmalıdır.*
- *Paylaşım yapılandırması düzenlenmelidir.*

4.1. Topoloji Belirleme

Bağlantıların kurulacağı lokasyonlar belirlendikten sonra topolojilerin çizilmesi gerekir. Genellikle bağlantılar fiziksel ve mantıksal olmak üzere iki farklı ana topoloji üzerinden değerlendirilir.

4.1.1. Fiziksel ağ topolojileri

Fiziksel ağ topolojisi, ağa bağlı cihazların fiziksel düzenini gösterir. Fiziksel katman'daki, örneğin kablolama veya donanım sorunları gibi, sorunları gidermek için cihazların fiziksel olarak nasıl bağlandıklarını bilmek gerekir. Bir fiziksel topoloji haritası konak bilgisayarları, ağ cihazlarını ve ortamlarını belgelemek için bazı simgeleri kullanır. Gelecekteki kurulum ve sorun giderme çalışmaları için fiziksel topoloji haritalarının sağlanması ve güncellenmesi önemlidir. Fiziksel ağ topolojileri genellikle şunları içerir:

- *Cihaz tiplerini,*
- *Cihazların modellerini ve üreticilerini,*

- *Konumlarını,*
- *İşletim sistemi sürümlerini,*
- *Kablo tipleri ve tanımlayıcılarını,*
- *Kablolama uç noktalarını,*

4.1.2. Mantıksal ağ topolojileri

Mantıksal ağ topolojisi, verilerin ağda nasıl aktarıldığını gösterir. Yönlendirici, sunucu, anahtar, konak bilgisayar ve güvenlik cihazları gibi ağ öğelerini göstermek için bazı simgeler kullanılır. Bir mantıksal topoloji haritası, fiziksel konumdan bağımsız olarak, ağ kullanımına göre donanımları gruplandırır. Donanımlar, adresler, grup bilgileri ve uygulamalar mantıksal topoloji haritası üzerine kaydedilir. Mantıksal ağ topolojileri genellikle şunları içerir:

- *Cihaz tanımlayıcılarını,*
- *IP adreslerini ve alt ağ maskelerini,*
- *Arayüz tanımlayıcılarını,*
- *Yönlendirme protokollerini,*
- *Statik ve varsayılan rotaları,*
- *Veri bağı protokollerini,*
- *WAN teknolojilerini.*

4.2. Kurulumu Planan WAN'daki Bağlantı Gereksinimleri

Bu ve bundan sonraki bölümlerde, kurulumu planlanan yedekli çalışan bir modern WAN örneği baz alınarak detaylı bilgilerin verilmesi planlanmaktadır.

Bu kurulumdaki amaç, VHF (Very High Frequency) ve UHF (Ultra High Frequency) radyo frekansları üzerinden gerçek zamanlı olarak taşınan ses verisi ve radar sistemlerinden gelen kritik radar verilerinin işlenip, verilerin kullanılabileceği merkezlere istenilen bir şekilde taşınması, ayrıca standart veri olarak tanımladığımız telnet seans'larıyla bakım ve yönetimin sağlanmasıdır.

Başlangıç olarak, aşağıda bağlantıların sağlanması gereken lokasyonlar, belli özelliklerine göre belirtilmiş ve gruplandırılmıştır. Daha sonra bu bağlantılar arasındaki bant genişlik gereklilikleri tablolar halinde gösterilmiştir.

4.2.1. Topolojiler için lokasyon belirleme

Genellikle WAN kurulurken verilerin aktığı lokasyonlar için belli başlı kriterlere göre sınıflandırmanın yapılması gerekir. Biz lokasyonları, merkezler ve uzak istasyonlar şeklinde sınıflandırdık. Aşağıda bu noktaların tanımları ve kendi aralarındaki sınıflandırmalar verilmiştir.

i. Tip-1 merkez lokasyonlar

Ana bağlantıların olduğu ve sistemin bütün noktalarına direkt erişimi olan ve birbirinin yedeği olan 2 lokasyondan ibaret olarak düsünülmektedir. M1 ve M2 olarak adlandırılacaktırlar.

ii. Tip-2 merkez lokasyonlar

Belli başlı uzak lokasyonlara ve bütün merkez lokasyonlara bağlantıları olan merkez lokasyonlardır. Bunlar M3, M4, M5, M6 ve M7 olarak adlandırılacaktırlar.

iii. Tip-1 uzak lokasyonlar

Bu tür lokasyonlar sadece kritik veri olarak adlandırdığımız radar verilerinin ve uzak erişimde kullandığımız telnet seanslarının aktif olduğu lokasyonlardır. R1-R4 olarak arası adlandırılacaktırlar.

iv. Tip-2 uzak lokasyonlar

Bu tür lokasyonlar sadece VHF-UHF radyo frekanslarının analog-digital dönüşümlerinin yapıldığı ve IP adresleme teknikleri kullanılarak yönlendiriciler vasıtasıyla gerçek zamanlı olarak ses verisinin taşındığı ve yönetim için Telnet seanslarının aktif olduğu istasyonlardır. Bu lokasyonlar RD1-RD24 olarak adlandırılmışlardır.

v. Tip-3 uzak lokasyonlar

Bu tür lokasyonlar hem gerçek zamanlı ses datasının hem kritik veri olarak adlandırılan radar datasının aynı anda iletiminin olduğu istasyonlardır. Bu tür istasyonlar RR1-RR14 arası olarak adlandırılmışlardır.

vi. Tip-1 uzak kule lokasyonlar

Bu lokasyonlar merkez lokasyonlardan gelen verileri kullanmak üzere planlanmıştır. K1-K12 şeklinde adlandırılacaktırlar.

4.2.2. Merkezler arası bağlantılar

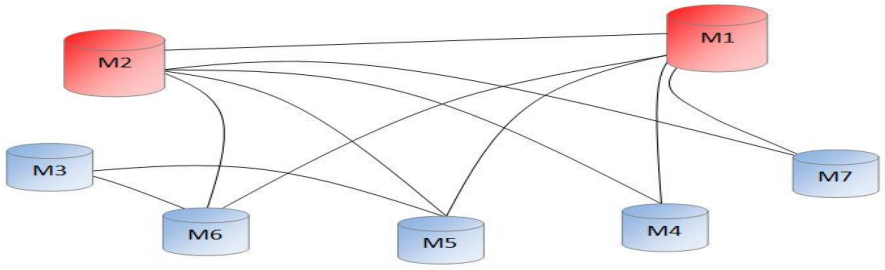
Kuracağımız WAN'da 7 adet merkez lokasyon bulunmaktadır, bu lokasyonlardan M1 ve M2 ana merkezler olup, Çizelge 4.1 ve Şekil 4.1'de gösterildiği gibi bunlar birbirlerinin yedeği şeklinde çalışmalıdır. Merkezler arası bağlantı gereksinimleri, aşağıdaki çizimde gösterilmiştir. Ana merkezler kırmızı, diğer merkezler ise mavi renk ile gösterilmişlerdir. Siyah renkli olan bağlantılar normal operasyonel kullanımda, kırmızı ile belirtilen bağlantılar ise emerjans dediğimiz, acil durumda kullanılmak için planlanmıştır.

Merkezler arası bağlantı gereksinimleri çizelgelerde de belirtilmiştir. Çizelge 4.1'de her hücre de siyah işaret (x), normal operasyonda kullanılan bağlantıya tekabül

etmektedir. Hücrenin boş olması durumu ise herhangi bir bağlantıya gerek olmadığını ifade etmektedir.

Çizelge 4.1. Merkezler ve uzak kule lokasyonlar bağlantılar.

Uzak Kule Lok.		*Merkezler*						
		M1	M2	M3	M4	M5	M6	M7
1	M1		x	x	x	x	x	x
2	M2	x		x	x	x	x	x
3	M3							
4	M4	x	x					
5	M5	x	x					
6	M6	x	x					
7	M7	x	x					



Şekil 4.1. Merkezler & merkezler bağlantılar

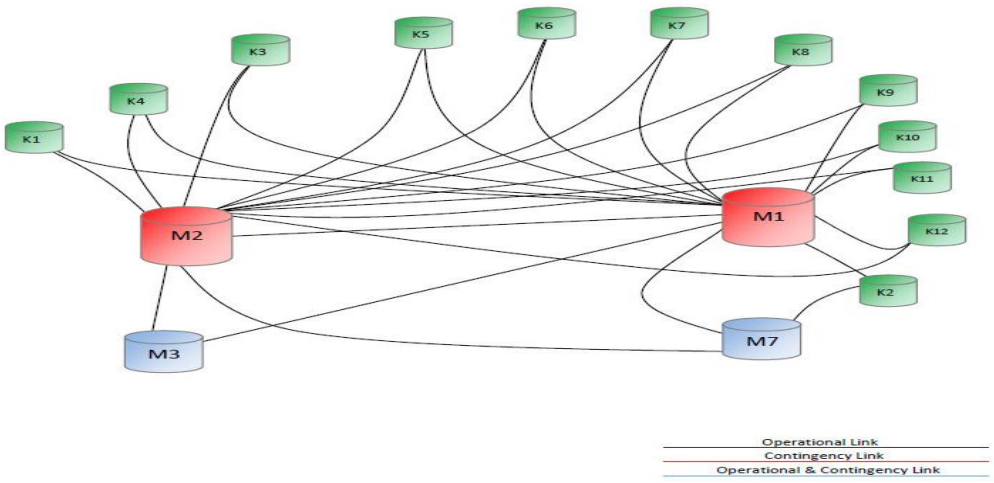
4.2.3. Merkezler ve tip-1 uzak kule lokasyonlar arası bağlantılar

Kuracağımız WAN'da 7 adet merkez lokasyon ve K1'den K12'e kadar isimlendirilen 12 adet tip-1 uzak kule lokasyonumuz bulunmaktadır. Bu merkezler ve uzak kule lokasyonlar arası bağlantılar Şekil 4.2'de belirtilmiştir.

Merkezler ve uzak kule lokasyonlar arası bağlantılar için Çizelge 4.2 'de ki her hücrede (x) işareti ile bağlantıların varlığı gösterilmiştir.

Çizelge 4.2. Merkezler ve uzak kule lokasyonlar arası bağlantılar

	Uzak Kule Lok.	Merkezler		
		M1	M2	M3
1	K1	X	X	
2	K2	X	X	X
3	K3	X	X	
4	K4	X	X	
5	K5	X	X	
6	K6	X	X	
7	K7	X	X	
8	K8	X	X	
9	K9	X	X	
10	K10	X	X	
11	K11	X	X	
12	K12	X	X	
13	K13	X	X	
14	K14	X	X	



Şekil 4.2. Merkezler ve uzak kule lokasyonlar arası bağlantılar

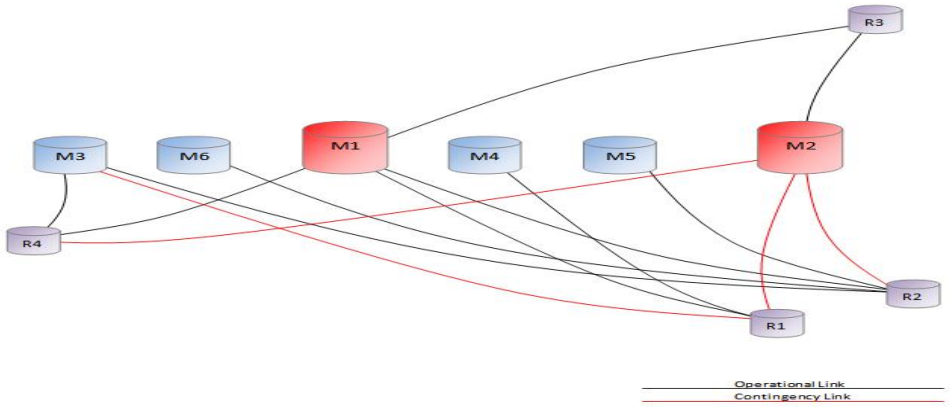
4.2.4 Merkezler ve tip-1 uzak lokasyonlar arası bağlantılar

Kuracağımız WAN'da 7 adet merkez lokasyon ve R1'den R4'e kadar isimlendirilen 4 adet tip-1 uzak lokasyonumuz bulunmaktadır. Bu merkezler ve tip-1 uzak lokasyonlar arası bağlantılar Şekil 4.3'te belirtilmiştir. Siyah renk ile gösterilen bağlantılar normal operasyonda, kırmızı renk ile gösterilen bağlantılar ise, emerjans dediğimiz durumlarda kullanılmak üzere planlanmıştır.

Merkezler ve tip-1 uzak lokasyonlar arası bağlantılar için Çizelge 4.3'de daha önceki anlatılan bağlantılarda olduğu gibi işaretlemeler normal ve emerjans durumlar için yapılmıştır.

Çizelge 4.3. Merkezler ve tip-1 uzak lokasyonlar arası bağlantılar

		Merkezler													
		M1		**M2**		**M3**		**M4**		**M5**		**M6**		**M7**	
	Uzak Lokasyon	*Op.*	*Con.*	*Op.*	*Con.*	*Op.*	*Con.*	*Op.*	*Con.*	*Op.*	*Con.*	*Op.*	*Con.*	*Op.*	*Con.*
1	R-1	X			X		X	X							
2	R-2	X			X	X				X		X			
3	R-3	X		X											
4	R-4	X			X	X									



Şekil 4.3. Merkezler ve tip-1 uzak lokasyonlar arası bağlantılar

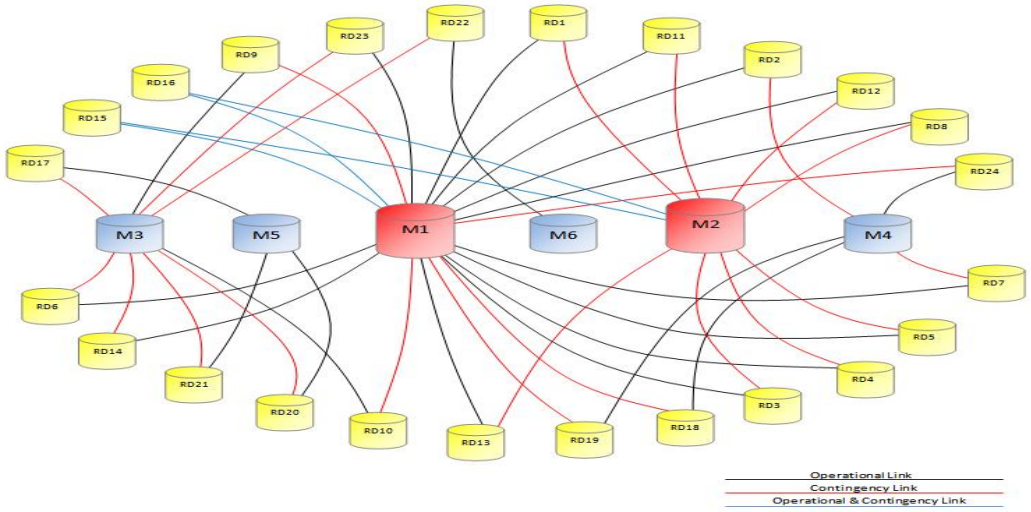
4.2.5. Merkezler ve tip-2 uzak lokasyonlar arası bağlantılar

Kuracağımız WAN'da 7 adet merkez lokasyon ve RD1'den RD24'e kadar isimlendirilen 24 adet Tip-2 uzak lokasyonumuz bulunmaktadır. RD ile belirtilen lokasyonlar sarı renk ile gösterilmişlerdir. Bu merkezler ve tip-2 uzak lokasyonlar arası bağlantılar Şekil 4.4'te daha önceki şekillerde olduğu gibi belirtilmiştir

Merkezler ve tip-2 uzak lokasyonlar arası bağlantılar için Çizelge 4.4'de daha önceki anlatılan bağlantılarda olduğu gibi işaretlemeler yapılmıştır.

Çizelge 4.4. Merkezler ve tip-2 uzak lokasyonlar arası bağlantılar

		Merkezler													
		M1		**M2**		**M3**		**M4**		**M5**		**M6**		**M7**	
	Tip-2 Uzak Lokasyon	*Op.*	*Con*	*Op.*	*Con*	*Op.*	*Con*	*Op.*	*Con*	*Op.*	*Con*	*Op.*	*Con*	*Op.*	*Con*
	RD-1	X			X										
	RD-2	X			X										
	RD-3	X			X										
	RD-4	X			X										
	RD-5	X			X										
	RD-6	X													
	RD-7	X					X								
	RD-8	X			X										
	RD-9		X			X									
	RD-10		X			X									
	RD-11	X			X										
	RD-12	X			X										
	RD-13	X			X										
	RD-14	X					X								
	RD-15	X	X	X	X										
	RD-16	X	X	X	X										
	RD-17					X				X					
	RD-18				X				X						
	RD-19				X				X						
	RD-20						X				X				
	RD-21						X				X				
	RD-22						X					X			
	RD-23						X					X			



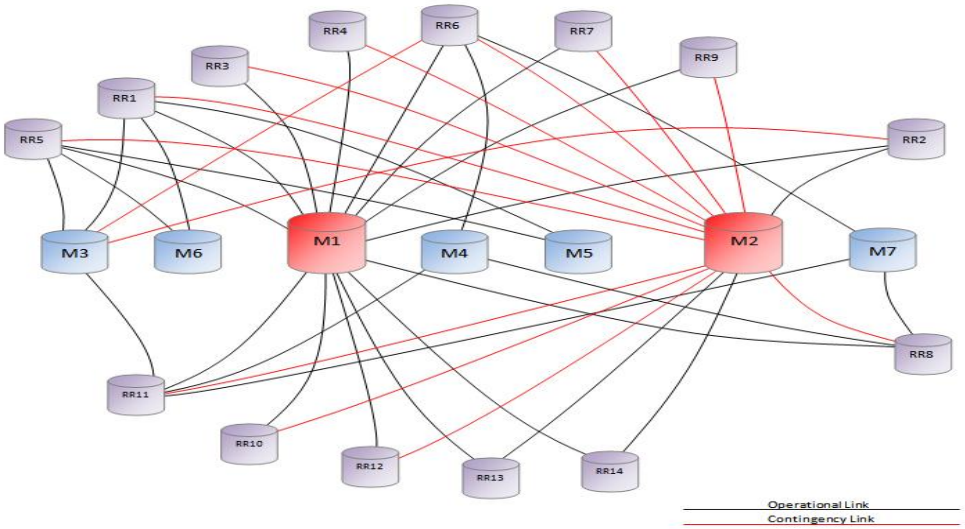
Şekil 4.4. Merkezler ve tip-2 uzak lokasyonlar arası bağlantılar

4.2.6. Merkezler ve tip-3 uzak lokasyonlar arası bağlantılar

Kuracağımız WAN'da 7 adet merkez lokasyon ve RR1'den RR14'e kadar isimlendirilen 14 adet tip-3 uzak lokasyonumuz bulunmaktadır. Bu merkezler ve tip-3 uzak lokasyonlar arası bağlantılar Şekil 4.5'te daha önceki şekillerde olduğu gibi belirtilmiştir. Merkezler ve tip-3 uzak lokasyonlar arası bağlantılar için Çizelge 4.5'de daha önceki anlatılan bağlantılarda olduğu gibi işaretlemeler yapılmıştır.

Çizelge 4.5. Merkezler ve tip-3 uzak lokasyonlar arası bağlantılar

		Merkezler													
		M1		M2		M3		M4		M5		M6		M7	
	Tip-3 Uzak Lokasyon	*Op.*	*Con.*	*Op.*	*Con.*	*Op.*	*Con.*	*Op.*	*Con.*	*Op.*	*Con.*	*Op.*	*Con.*	*Op.*	*Con*
	RR-1	X			X	X						X			
	RR-2	X		X			X			X					
	RR-3	X			X										
	RR-4	X			X										
	RR-5	X			X	X		X				X			
	RR-6	X			X									X	
	RR-7				X		X							X	
	RR-8	X			X					X					
	RR-9	X			X					X					
	RR-10	X			X										



Şekil 4.5. Merkezler ve tip-3 uzak lokasyonlar arası bağlantılar

4.3. İşlem Hacmi (Kapasite) Gereklilikleri

Tasarım seçimi, aşağıdaki alt paragraflarda belirtildiği gibi merkezler ve uzak lokasyonlar için gerekli olan bağlantıların, veri hacmi, esneklik, ölçeklenebilirlik, yönetilebilirlik parametreleri ele alınarak, gerektiğinde karasal veya uydu ağı üzerinden iletişim sağlayabilecek şekilde seçilmiştir. Ağ tasarlanırken gelişen teknolojiler ele alınarak olabildiğince modern, yedekli ve aynı zamanda ekonomik bir seçim yapılmıştır.

WAN tasarımında, IP-tabanlı iletişim, IP üzerinden ses iletimi (VoIP-Voice over IP), ses yükünü sıkıştırma (codec G.729) gibi önemli kriterlerden, kaynak hacim gereksinimlerine katkıda bulunmak ve veri yükünü azaltmak üzere faydalanılmıştır. Ses ve veri için birleşik bir ağ olması, maliyetler için tasarruf ve operasyon için kolaylık sağlar.

4.3.1. Karasal ağ işlem hacmi gereksinimleri

Karasal ağ'da merkezler için, Çizelge 4.6'da isimleri verilen servislerin WAN'da farklı ağlarda veri trafiği ürettigi varsayılmıştır.

Karasal ağ için gerekli olan data hacmi Çizelge 4.7'de gösterilmiştir ve minimum gereksinimler olarak düşünülmektedir. Bu hesaplama yapılırken yönetim, bakım gibi ek bant genişliği gerektirebilecek işlemler de düşünülmüştür. Gelecekteki uygulamalar için gerekli olabileceği düşünülerek %30 marjında fazladan bir bant genişliği eklenmiştir.

Çizelge 4.6. WAN'da kullanılan operasyonel servisler

Operasyonel Servisler
Radar verisi
Ucus parametreleri
UcusBilgileri
Guvenlik Alarmları
MTCD verisi
AMAN verisi
Yapılandırma verisi
Ses

Çizelge 4.7. Merkezlerde karasal ağ için gerekli olan bant genişliği hacimleri

Merkezler	Gerekli olan Bant Genişliği(Mbps)
M1	58
M2	82
M3	22
M4	18
M5	14
M6	14
M7	4

Karasal ağ işlem hacimleri, uzak kule lokasyonlar için Çizelge 4.8.'te gösterilmiştir ve minimum gereksinimlerdir. Radar ve ses kaynaklarına göre işlem hacim gereksinimleri ve diğer bütün operasyonel servisler, aynı zamanda yönetim trafiği için gerekli olan bant genişlikleri de hesaba katılmıştır. Ayrıca, gelecekteki uygulamalar düşünülerek %30 marjında ek bir bant genişliği de eklenmiştir.

Çizelge 4.8. Uzak lokasyon kulelerde karasal ağ işlem hacim gereklilikleri

Bazı Uzak Kule Lokasyonlaar	Gerekli olan Bant Genişliği(Kbps)
K1	2000
K2	2000
K3	2000
K4	2000
K5	2000
K6	2000
K7	2000
K8	2000
K9	2000
K10	2000
K11	2000
K12	2000
K13	7000
K14	2000
K15	2000

Çizelge 4.9. Bazı uzak lokasyonlar için karasal ağ işlem hacim gereklilikleri

Uzak Lokasyonlar	Gerekli olan Bant Genişliği (Kbps)
RR-1	2000
R-1	1500
RR-2	2000
RR-3	1000
RR-4	1000
RR-5	2000
R-2	1500
RR-8	1500
RR-2	2000
RR-7	1000
R-3	500
RD-1	500
RR-9	1000
RD-2	500
RR-10	1000
RR-11	2000
RR-12	1000
RR-13	1000
RR-14	1500
RD-3	500
RD-4	500
RD-5	500
RD-12	500

Çizelge 4.9'da bertilen kaynak hacimleri radar ve ses operasyonel servisleri dikkate alınarak hesaplanmıştır.

4.3.2. Uydu ağ işlem hacmi (kapasite) gereklilikleri

Uydu ağ kapasitesi Çizelge 4.10'da verilen işlem hacim gereksinimlerine göre boyutlandırılmıştır. Ayrıca yönetim trafiği, haberleşme protokolleri ve uydu üzerindeki trafiği kötü etkileyebilecek olan kötü hava koşulları gibi etkenler de dikkate alınmıştır.

Toplam kapasite miktarı aşağıda belirtilen tasarım parametrelerine göre yaklaşık olarak 19 MHz olarak hesaplanmıştır [36].

- *Mesh taşıyıcı kapasitesi: 0,77 MHz,*
- *Toplam mesh taşıyıcı sayısı: 22,*
- *Star inbound taşıyıcı kapasitesi: 0,77 MHz,*
- *Toplam star inbound taşıyıcı sayısı: 1,*
- *Star outbound taşıyıcı kapasitesi: 1 MHZ,*
- *Toplam star outbound taşıyıcı sayısı: 1'dir.*

Bir sonraki sayfada Çizelge 4.10'da uydu ağ'ı için uzak lokasyonlarda gereken işlem hacimleri verilmiştir.

Çizelge 4.10. Bazı uzak lokasyonlarda uydu ağı işlem hacim gereklilikleri

Uzak Istasyonlar	Trafik içeriği	G.729 Payload (Kbps)	G.729 Overhead (Kbps)	Ses Yönetimi	Ses Sinyali (Kbps)	Radar (Kbps)
RR-1	6 Freq.	48	132	100	30	
	Radar					100
R-1						
	Radar					100
RR-2	18 Freq.	144	396	100	90	
	Radar					100
RR-3	6 Freq.	48	132	100	30	
	Radar					100
RR-4	4 Freq.	32	88	100	20	
	Radar					100
RR-5	6 Freq.	48	132	100	30	
	Radar					100
R-2						
	Radar					100
RR-8	5 Freq.	40	110	100	25	
	Radar					100
RR-6	5 Freq.	40	110	100	25	
	Radar					100
RR-7	5 Freq.	40	110	100	25	
	Radar					100
R-3						
	Radar					100
R-4						
	Radar					100
RD-1	5 Freq.	40	110	100	25	
	Radar					
RR-9	3 Freq.	24	66	100	15	
	Radar					100
RD-2	4 Freq.	32	88	100	20	
	Radar					
RR-10	4 Freq.	32	88	100	20	
	Radar					100
RR-11	4 Freq.	32	88	100	20	
	Radar					100
RR-12	5 Freq.	40	110	100	25	
	Radar					100
RR-13	2 Freq.	16	44	100	10	
	Radar					100
RR-14	18 Freq.	144	396	100	90	
	Radar					100
RD-3	5 Freq.	40	110	100	25	
	Radar					
RD-4	4 Freq.	32	88	100	20	
	Radar					
RD-5	3 Freq.	24	66	100	15	
	Radar					
RD-6	3 Freq.	24	66	100	15	
	Radar					
RD-7	13 Freq.	104	286	100	65	
	Radar					
RD-8	12 Freq.	96	264	100	60	
	Radar					

4.4. Wan Topolojileri

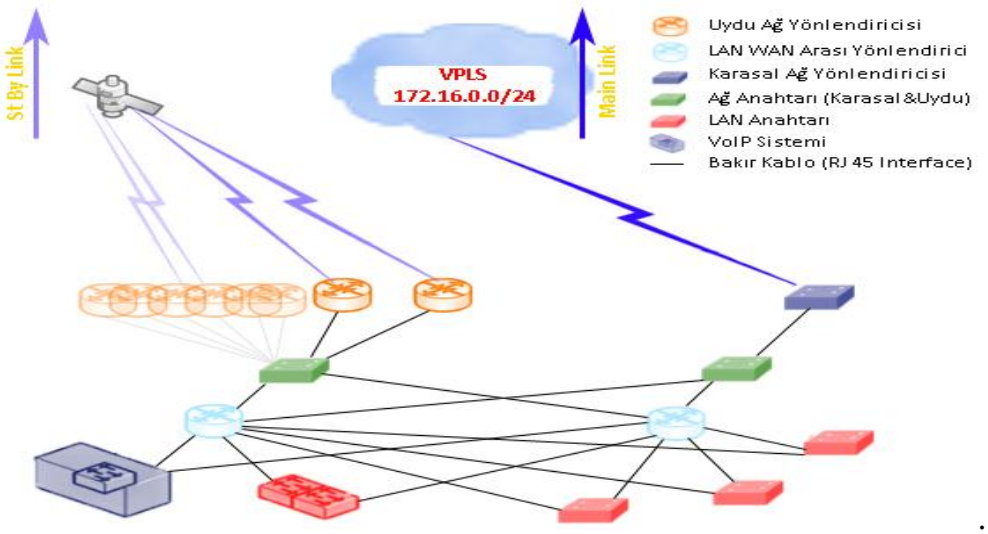
Bu bölümde merkezler ve uzak lokasyonlar arası tasarlanan WAN topolojileri üzerinde fiziksel ve mantıksal topoloji çizimleriyle tek tek duracağız. Öncelikle, daha önceki bölümlerde lokasyonlar için uyguladığımız sınıflandırma Çizelge 4.11'de verilmektedir. Lokasyonların sınıflandırılmasını anlamak, kurulacak olan WAN'da tasarımın iyi anlaşılması için yarar sağlayacaktır.

Çizelge 4.11. Merkez lokasyon ve uzak lokasyonlar

Merkezler		Uzak Lokasyonlar			Uzak Kule Lok.
Tip-1	Tip-2	Tip-1	Tip-2	Tip-3	Tip-1
M1	M3	R1	RD-1	RR-1	K1
M2	M4	R2	"	"	"
	M5	R3	"	"	"
	M6	R4	"	"	"
	M7		RD-24	RR-14	K-12

4.4.1. Merkezler

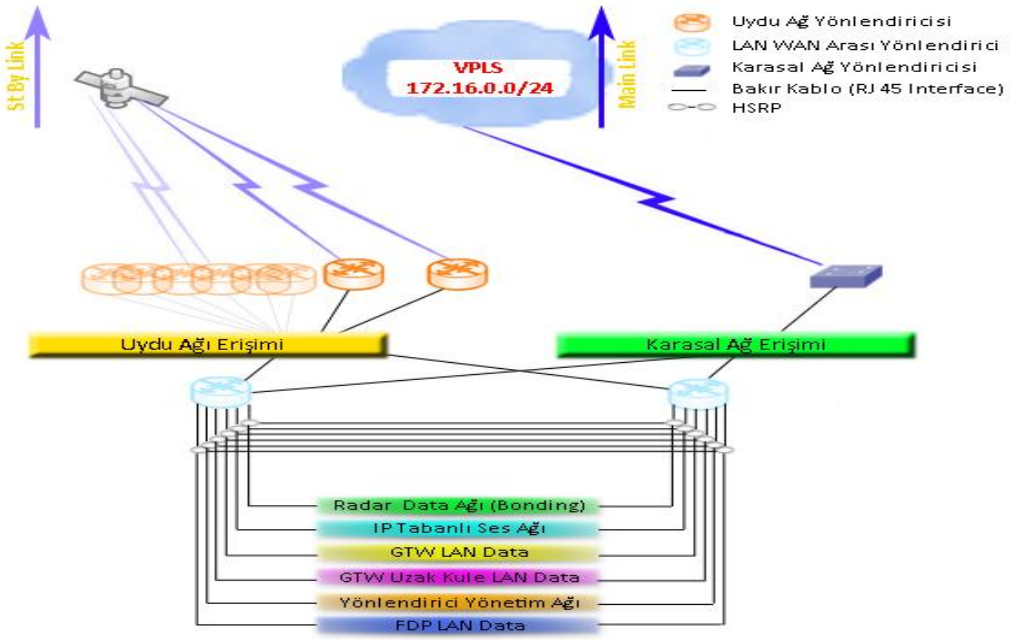
Merkezlerde, fiziksel olarak mimari ağ tasarımı Şekil 4.6'da gösterilmiştir. Her merkezde WAN'a çıkış için iki adet yönlendirici bulunmaktadır. Ana merkezdeki yönlendiriciler doğal olarak, diğer merkezlerdeki yönlendiricilere göre daha yüksek yoğunlukta iş yüküne sahip olduklarından dolayı, daha yüksek kapasitelere sahip olan yönlendiricilerdir. Bu yönlendiriciler hem karasal ağ'a, hem de uydu ağ'ına aynı anda bağlıdırlar ve mevcut duruma göre aktif olan ağın kullanımını sağlarlar. Ayrıca yönlendiriciler, HSRP (Hot Stand-by Routing Protocol) sayesinde main-standby olmak üzere yedekli çalışmaktadırlar. Yönlendiriciler uydu ağı, karasal ağ, ses ağı ve yönetim ağı gibi ağların hepsine ayrı birer anahtar ünitesi yardımıyla bağlanırlar.



Şekil 4.6. Merkezlerdeki bağlantıların fiziksel görünümü

Şekil 4.6'da gösterilen donanımları açıklamak gerekirse, uydu yönlendiricileri, her lokasyondan gelen uydu bağlantılarını, LAN-WAN arası yönlendirme yapan ana yönlendiriciye taşır. Uydu ağı ve karasal ağı yönlendiricileri, LAN geçişlerini, yedekleme sağlayabilmek için iki ayrı anahtar üzerinden sağlamaktadır. Bu anahtarlar, karasal veya uydu ağına ait olan hat sağlayıcının cihazına bağlanmayı sağlar ve ayrıca yönetim/bakım için bir iç ağ yaratmaya yardımcı olurlar. VoIP (Voice over IP) şeklinde belirtilen sistem ise, IP tabanlı ses verisinin operasyonel kullanıldığı sistem olarak düşünülmüştür.

Merkezler için mimari ağ tasarımının mantıksal topoloji çizimleri ve detayları Şekil 4.7'de gösterilmiştir. Merkezlerdeki iki ana yönlendirici, ayrı anahtarlar vasıtısayla bir çok network için uzak mesafeler arasında yönlendirme yapmaktadır. Şekilde ağ isimleri verilmiş ve farklı renklerle belirtilmiştir. Anahtar ve yönlendiriciler birbirlerine şekilde de belirtildiği gibi fiziksel olarak bakır kablolar ile *fast ethernet* ve *gigabit ethernet* protokolleri üzerinden bağlıdırlar. Yönlendiriciler hem uydu hem de karasal ağ üzerinden bağlantı sağlamaktadır. Yönlendiriciler dinamik OSPF yönlendirme, statik olarak yönlendirme, ayrıca multicast yönlendirme için PIM (Protocol Independent Multicast) protokolu ile yapılandırılmışlardır.



Şekil 4.7. Merkezlerlerdeki bağlantıların mantıksal görünümü

Şekil 4.7'de mantıksal görünüşte, yönlendiricilerin WAN üzerinden, LAN içerisindeki bazı ağlarla bağlantılarının olduğu görünmektedir.

Radar ağ'ı, uzak lokasyonlardan (radar istasyonlarından) gelen radar verileri için oluşturulmuştur. HSRP (hot-standby-routing-protocol) protokolü sayesinde iki yönlendirici arasında yedekleme sağlanmıştır. Radar ağından gelen veri, (tip-1 uzak lokasyon ve tip-3 uzak lokasyondaki radar istasyonlarından gelen veriler), merkezlere ve gerektiğinde bu merkezler arasındaki veri trafiğininin olduğu ağlara gönderilir.

Ses ağ'ı, merkezler arasındaki ses haberleşme sistemlerinin birbirleriyle, ayrıca uzak lokasyonlardaki elemanlar ve merkezler arasındaki ses haberleşme sistemleri ile haberleşmesi amacıyla oluşturulmuştur. HSRP protokolü sayesinde iki yönlendirici arasında yedekleme sağlanmıştır. Ses ağından gelen veriler, (tip-2 uzak lokasyon ve tip-3 uzak lokasyonlarındaki radyo istasyonlarından gelen veriler) merkezlere ve gerektiğinde ise, bu merkezler arasındaki veri trafiğinin olduğu ağlara gönderilir.

GTW (gateway) ağ'ı, merkezler arasındaki veri haberleşmesi için oluşturulmuştur. HSRP protokolü sayesinde iki yönlendirici arasında yedekleme sağlanmıştır.

GTW TWR (tower) ağ'ı, uzak kule lokasyonları ile merkezler arasındaki veri haberleşmesi için oluşturulmuştur. HSRP protokolü sayesinde iki yönlendirici arasında yedekleme sağlanmıştır.

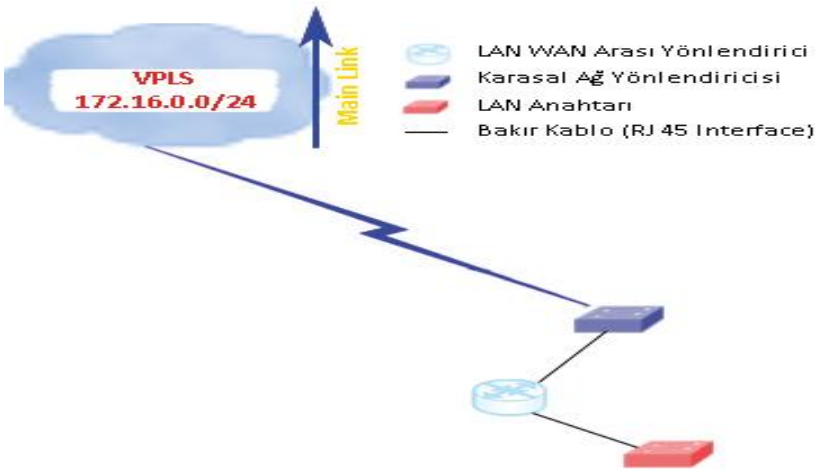
FDP ağ'ı, FDP sunucuları ve FDP konak bilgisayarlar arasındaki haberleşme için oluşturulmuştur.

Router MNGT ağ'ı, yönlendiricilerin yönetim ve bakımı için oluşturulmuştur. Uydu erişim ağ'ı, uydu yönlendiricilerinin bağlı bulunduğu ağdır. Karasal erişim ağının yedeği olarak kullanılmaktadır.

Karasal erişim ağı, telekom elemanlarının bağlı olduğu ağdır. Bu bağlantı WAN'da ana link olarak tasarlanmıştır ve bu bağlantıda herhangi bir kesilme olduğunda otomatik olarak uydu ağının devreye girmesi planlanmıştır.

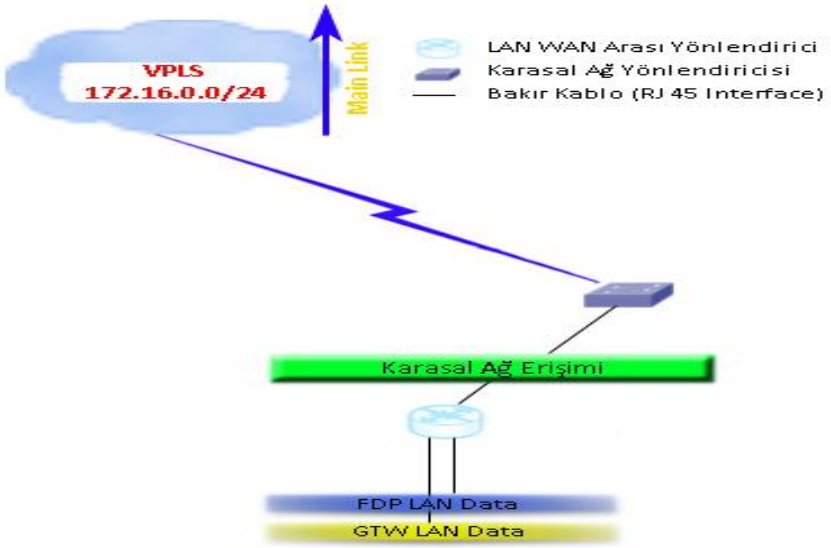
4.4.2. Tip-1 uzak kule lokasyonlar

Şekil 4.8'de tip-1 uzak kule olarak isimlendirdiğimiz lokasyonların fiziksel olarak tasarlanan mimari ağ detayları belirtilmiştir. LAN-WAN arası yönlendirici, karasal ağ anahtarı ve karasal erişim cihazı arası bağlantılar gösterilmiştir. WAN bağlantısı *fast ethernet protokolü* üzerinden VPLS bulutu vasıtasıyla karasal ağ ile sağlanmaktadır.



Şekil 4.8. Uzak kule lokasyonlardaki bağlantıların fiziksel görünümü

Şekil 4.9'da tip-1 uzak kule olarak isimlendirdiğimiz lokasyonların mantıksal olarak tasarlanan mimari ağ detayları belirtilmiştir. Tip-1 uzak kule lokasyonlar için sadece iki LAN mevcuttur ve bunlar diğer bölümlerde açıkladığımız üzere FDP ve GTW TWR LAN'dır.



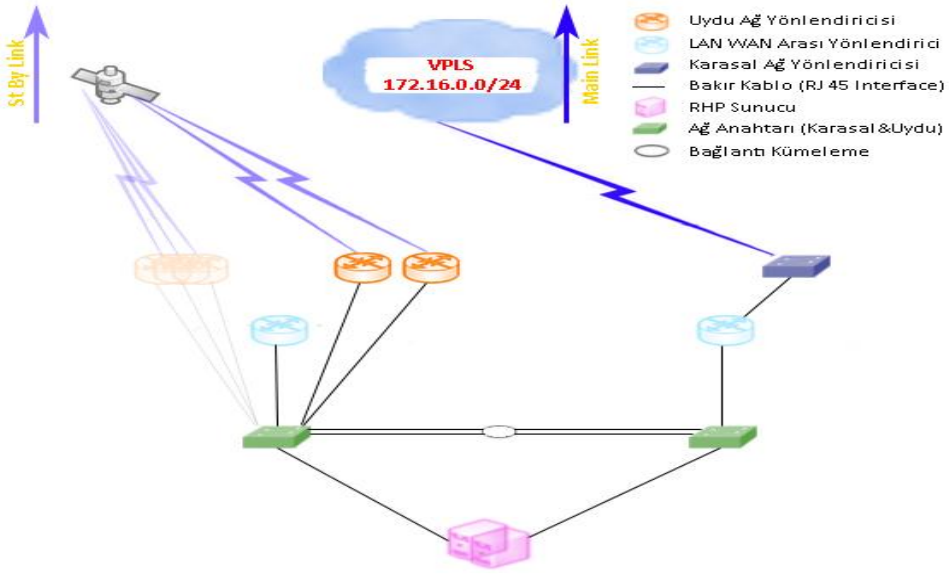
Şekil 4.9. Uzak kule lokasyonlardaki bağlantıların mantıksal görünümü

Şekil 4.9'da yönlendirici, anahtar ve karasal erişim cihazı bulunmaktadır. WAN bağlantısı fast ethernet protokolü üzerinden VPLS bulutu vasıtasıyla karasal ağ ile sağlanmaktadır. Yönlendiriciler dinamik olarak OSPF protokolü ve multicast yönlendirme için de PIM protokolü ile yapılandırılmışlardır.

Yönlendirici aşağıda belirtilen LAN'lara bağlanmıştır. Uzak kule lokasyonları ile merkezler arasındaki veri haberleşmesi için GTW TWR ağ'ını kullanmaktadırlar. FDP sunucular ile FDP konak bilgisayar haberleşmesi için FDP ağ'ı oluşturulmuş ve karasal ağ erişimi için VPLS bulutu vasıtasıyla *fast ethernet* protokolü ile bağlantılar sağlanmıştır.

4.4.3. Tip-1 uzak lokasyonlar

Şekil 4.10'da Tip-1 uzak lokasyon olarak isimlendirdiğimiz lokasyonların fiziksel olarak tasarlanan mimari ağ detayları belirtilmiştir.

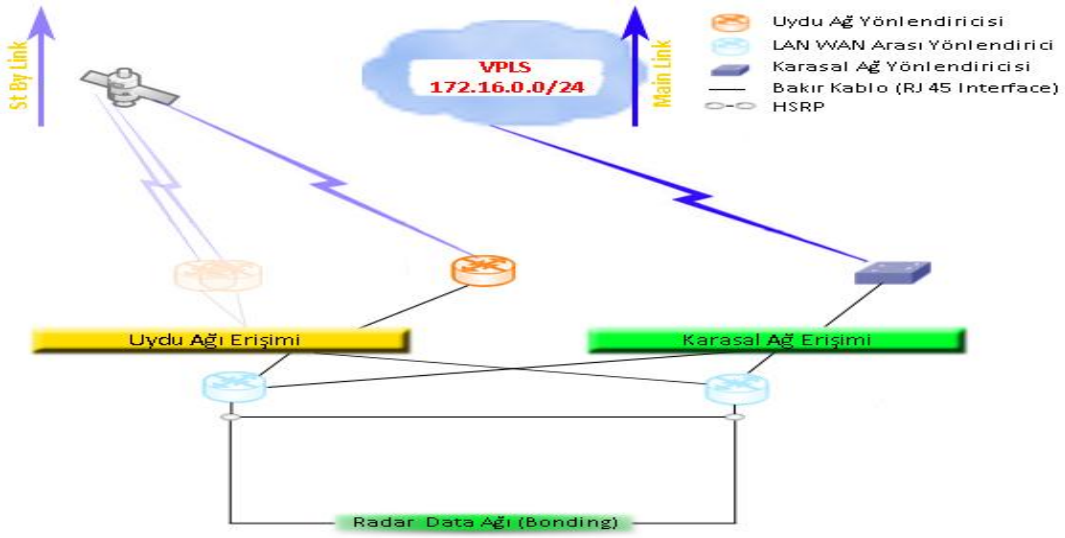


Şekil 4.10. Tip-1 uzak lokasyonlardaki bağlantıların fiziksel görünümü

LAN-WAN arası yönlendiriciler, iç network'te gelen verileri kabul eder ve gereken yerlere gönderir, ayrıca çıkış yapan verileri alıp ilgili yerlere gönderir. İki

yönlendirici yedekleme işlemini LACP (Link Aggregation Control Protocol) sayesinde, birbirlerine bakır kablo aracılığıyla bağlanarak yaparlar. Radar sistemi sunucularından gelen IP tabanlı radar verileri, yedekleme için her iki anahtara ayrı ayrı gönderilir ve anahtarlar gelen bu IP tabanlı verilerle ayrı VLAN (Virtual-LAN) sanal ağ'lar yaratarak, QoS uygulanabilmesi için yönlendiricilere gönderirler. Karasal ve uydu ağ erişim cihazları da bu noktalardan giriş/çıkış yapılmasını sağlayan hat sağlayıcıların cihazlarıdır.

Şekil 4.11'de tip-1 uzak lokasyon olarak isimlendirdiğimiz lokasyonların mantıksal olarak tasarlanan mimari ağ detayları belirtilmiştir.



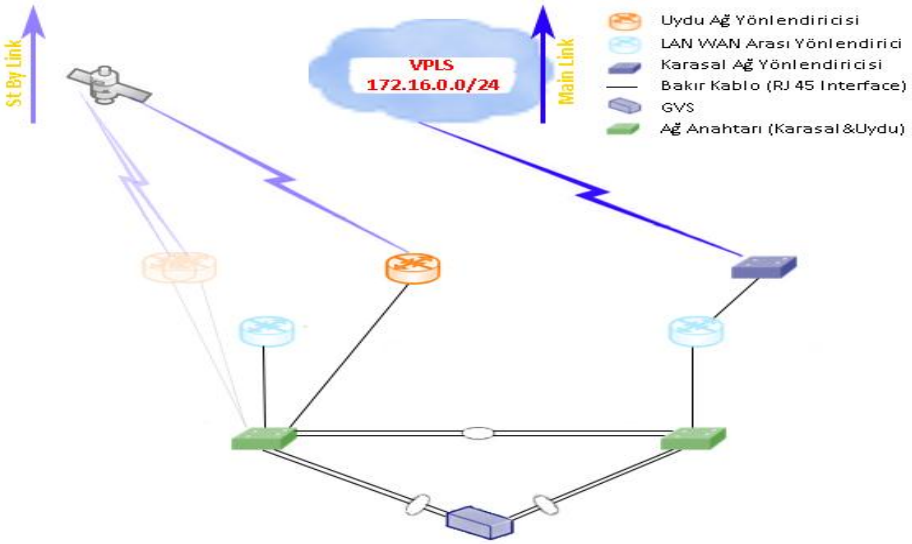
Şekil 4.11. Tip-1 uzak lokasyonlardaki bağlantıların mantıksal görünümü

Radar ağı, uzak lokasyonlardan gelen radar verileri için oluşturulmuştur. İlgili uzak lokasyonlarda, radar sistemi sunucuları radar verisini üretmektedirler. Uydu ağ erişim cihazları, uydu ağı için hat sağlayıcının yönlendiricilerinin bulunduğu alandır. Bu cihazlar uydu üzerinden giriş/çıkış yapılmakta kullanılırlar.

Karasal erişim ağ'ı, telekom donanımlarının bağlı olduğu ağdır. Bu ağ WAN'da ana link olarak tasarlanmıştır ve bağlantıda herhangi bir kesilme olduğunda otomatik olarak uydu ağ'ının devreye girmesi planlanmıştır.

4.4.4. Tip-2 uzak lokasyonlar

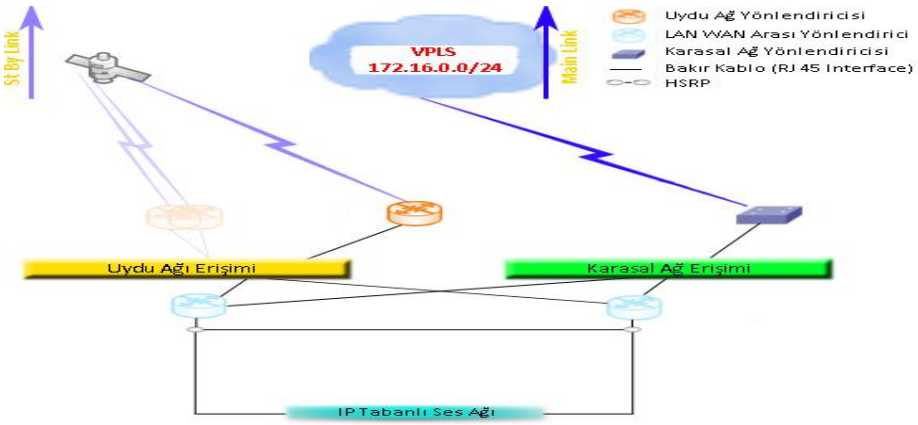
Şekil 4.12'de tip-2 uzak lokasyon olarak isimlendirdiğimiz lokasyonların, fiziksel olarak tasarlanan mimari ağ detayları, belirtilmiştir.



Şekil 4.12. Tip-2 uzak kule lokasyonlardaki bağlantıların fiziksel görünümü

GVS (Gateway Voice Service) dediğimiz cihazlar, analog/dijital çeviricilerdir ve bunlar sayesinde analog ses, IP tabanlı dijital ses verisine dönüştürülüp, yedekleme için her iki anahtara ayrı ayrı gönderilir. Anahtarlar gelen bu IP tabanlı verileri ayrı VLAN (Virtual-LAN) sanal ağ'lar ile eşleştirerek, QoS uygulanabilmesi için yönlendiricilere gönderirler.

Şekil 4.13'de tip-2 uzak lokasyon olarak adlandırdığımız lokasyonların mantıksal olarak tasarlanan mimari ağ detayları belirtilmiştir.

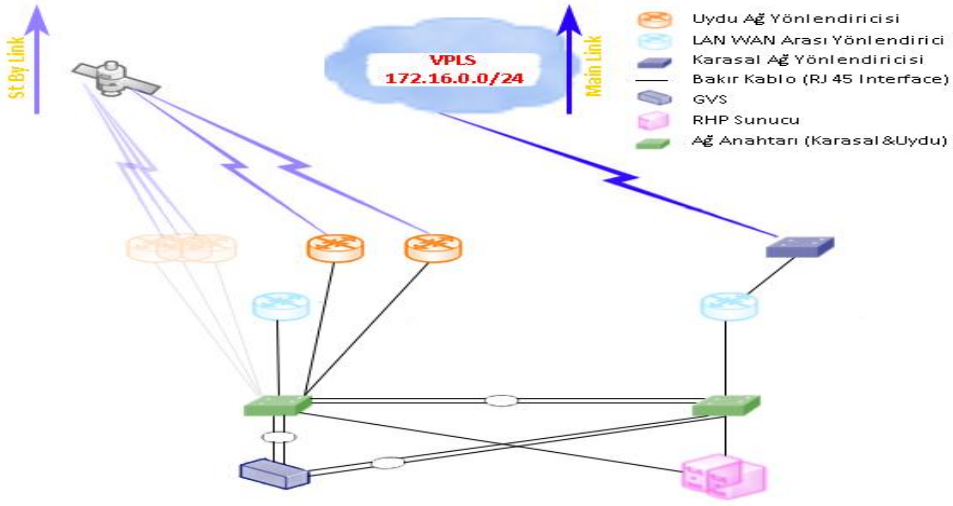


Şekil 4.13. Tip-2 Uzak kule lokasyonlardaki bağlantıların mantıksal görünümü

Ses ağ'ı, merkezler ve uzak lokasyonlar arasındaki ses haberleşme sistemlerinin birbirleriyle bağlantı kurması amacıyla oluşturulmuştur.

4.4.3. Tip-3 uzak lokasyonlar

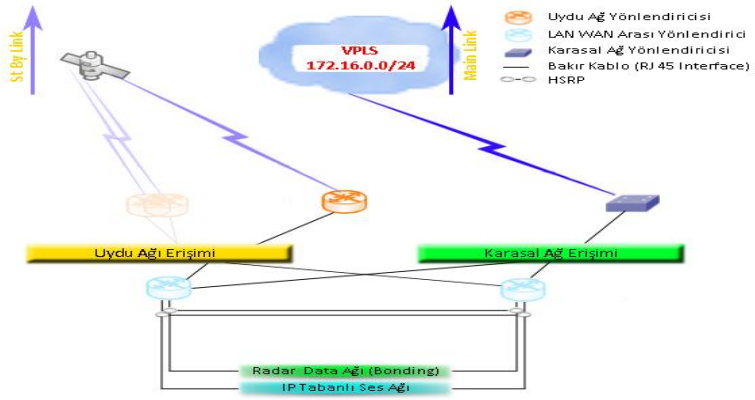
Şekil 4.14'de Tip-3 uzak lokasyon olarak isimlendirdiğimiz lokasyonların fiziksel olarak tasarlanan mimari ağ detayları belirtilmiştir



Şekil 4.14. Tip-3 uzak lokasyonlardaki bağlantıların fiziksel görünümü

Şekil 4.14'de LAN-WAN arası yönlendiriciler iç network'te gelen verileri kabul eder ve ilgili yerlere gönderir, ayrıca çıkış yapan verileri alıp ilgili yerlere gönderir. Analog/dijital çeviriciler sayesinde analog ses, ip tabanlı dijital ses verisine dönüştürülür ve yedekleme için her iki anahtara ayrı ayrı gönderilir. Radar sistemi sunucuları ise aynı şekilde IP tabanlı radar verisini anahtarlara ayrı ayrı gönderirler. Anahtarlar gelen bu IP tabanlı veriler için ayrı VLAN sanal ağ'lar yaratarak QoS uygulanabilmesi için yönlendiricilere gönderirler

Şekil 4.15'de tip-3 uzak lokasyon olarak adlandırdığımız lokasyonların mantıksal olarak tasarlanan mimari ağ detayları belirtilmiştir. Bu lokasyonda radar ve ses ağı olmak üzere iki ağ mevcuttur.

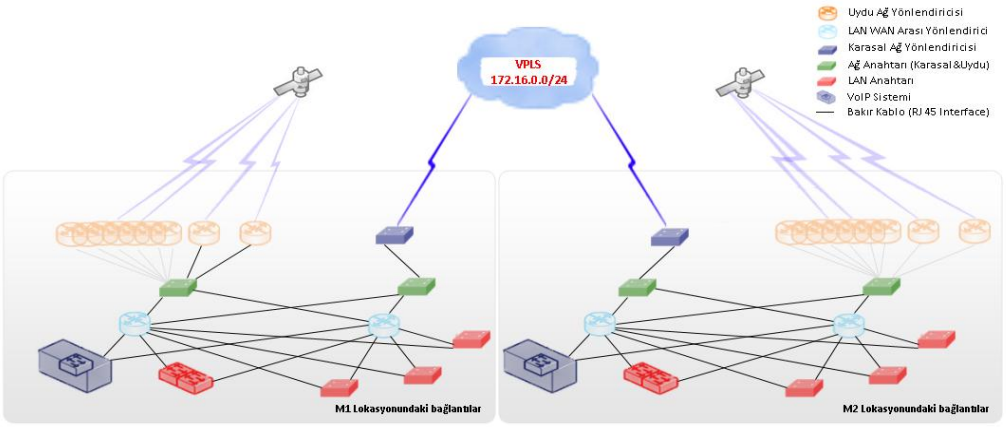


Şekil 4.15. Uzak kule lokasyonlardaki bağlantıların mantıksal görünümü

4.5. Detaylı Fiziksel Mimari Ağ Tasarımı (Low-Level Network Physical Architecture)

Bu bölümde vereceğimiz çizimlerde, "low-level network physical architecture" denilen ve ağ üzerindeki cihazların detaylı olarak bağlantılarının, fiziksel ve mantıksal olarak gösterimi üzerinde durulmuştur. Sırasıyla merkezlerin diğer lokasyonlara ve kendi aralarında nasıl bağlı oldukları genel şekiller ile açıklanmaya çalışılmıştır.

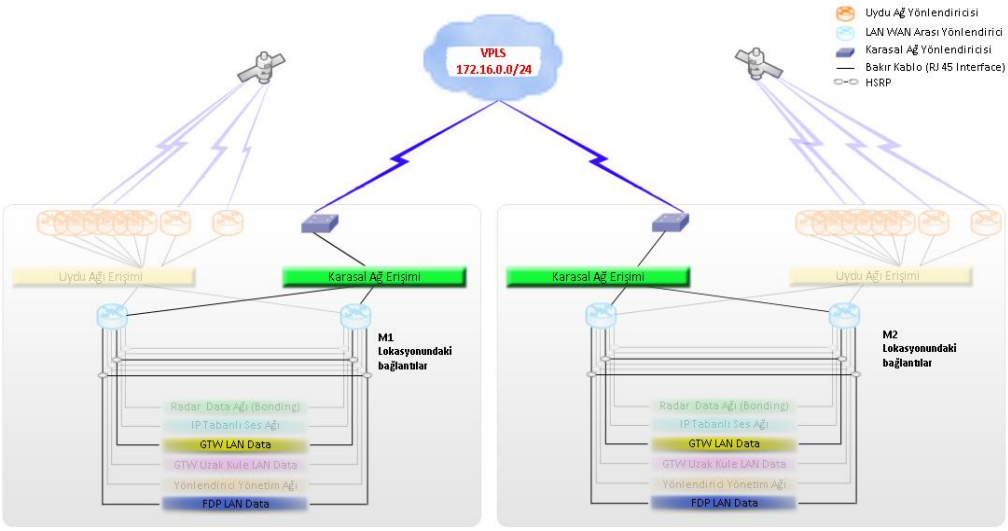
4.5.1. Merkezler ve merkezler arası bağlantılar



Şekil 4.16. Merkezler arası bağlantıların fiziksel görünümü

Şekil 4.16'da M1 ve M2 merkezinin birbiri arasındaki bağlantı detayları verilmiştir. Daha önceki bölümlerde anlattığımız üzere bu iki merkezde de benzer görevleri gören yönlendiriciler, anahtarlar, karasal ve uydu ağları için erişim arayüzleri bulunmaktadır. İki merkez arasındaki ana bağlantı karasal erişim cihazı üzerinden yapılan ve VPLS bulutuna giden bağlantıdır. VPLS'de herhangi bir arıza oluşması durumunda ise uydu ağ'ındaki bağlantının otomatik olarak devreye girmesi planlanmıştır.

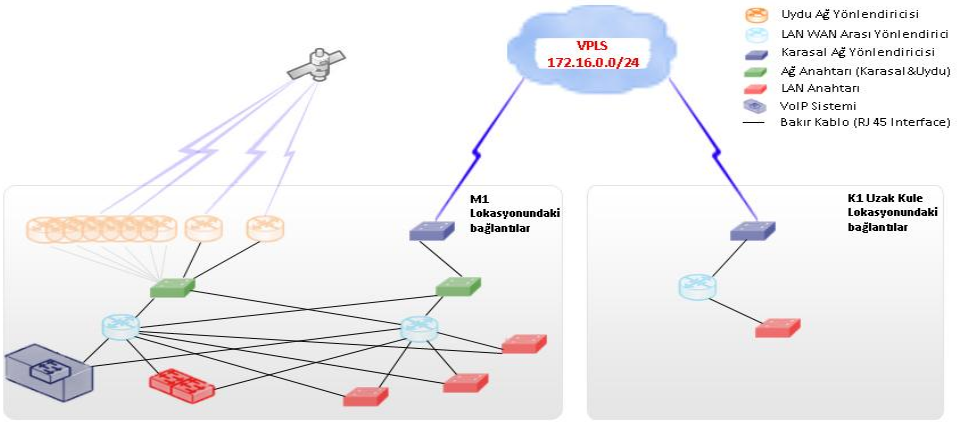
Şekil 4.17'de ise, M1 ve M2 merkezinin birbiri arasındaki bağlantı detayları mantıksal olarak verilmiştir ve her iki merkezde de LAN-WAN arası geçişler gösterilmiştir. HSRP, yönlendiriciler arasında yedekleme için kullanlmıştır ve VPLS üzerinden iki merkezde kurulan aynı LAN'lar birbirleriyle aynı yerdelermişcesine haberleşmektedirler. Merkezler arasında direkt haberleşme için kullanılan iki ağ mevcuttur ve bu iki ağ'ın farklı VLAN'lar ile eşleşmesinden sonra, yönlendiriciler üzerinde CoS (Class of Service) parametrelerinin eklenme işlemi yapılır, mevcut duruma göre karasal ya da uydu ağına yönlendirmeler yapılır.



Şekil 4.17. Merkezler arası bağlantıların mantıksal görünümü

4.5.2. Merkezler ve tip-1 uzak kule lokasyonlar arası bağlantılar

Şekil 4.18'de herhangi bir merkez ile tip-1 uzak kule lokasyon arasındaki fiziksel olarak bağlantı detayları verilmiştir.

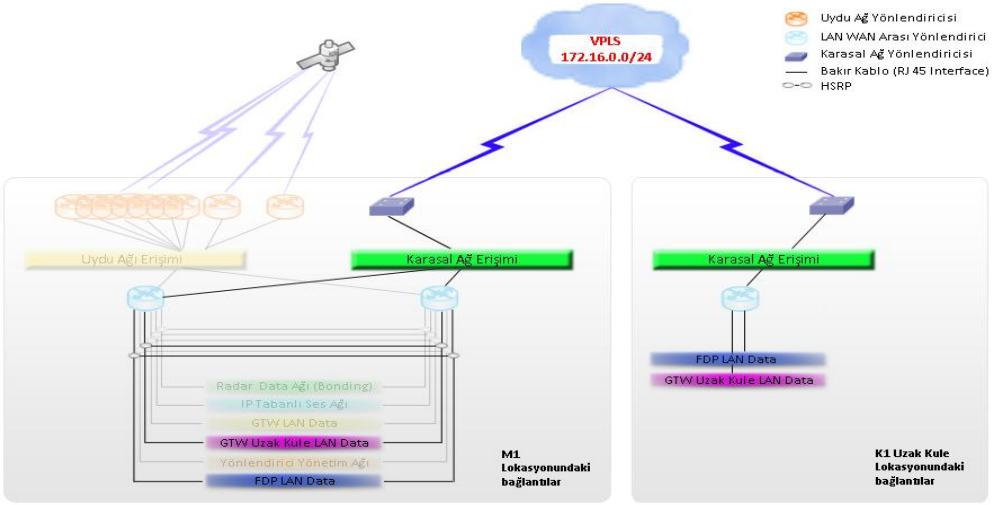


Şekil 4.18. Merkezler ve tip-1 uzak kule lokasyon arası bağlantıların fiziksel görünümü

Merkezlerde toplanan veriler yönlendiriciler vasıtasıyla, tip-1 uzak kule tarafındaki yönlendiricelere ulaşır ve buradaki anahtar vasıtasıyla kurulan iç network dahilinde ilgili konak bilgisayara iletilerek operasyon tamamlanmış olur. Uzak kule ve

merkezler arasında sadece karasal ağ mevcuttur yani ikinci bir yedek link mevcut değildir.

Şekil 4.19'da ise merkezler ve tip-1 uzak kule lokasyonlar arası bağlantıların mantıksal olarak detayları gösterilmektedir.

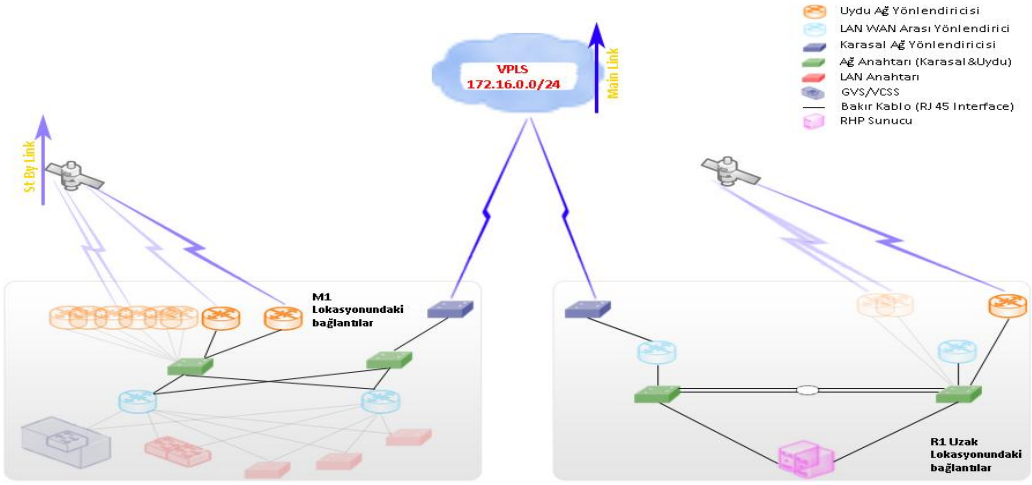


Şekil 4.19. Merkezler ve Tip-1 Uzak Kule Lokasyon arası bağlantıların mantıksal bağlantıların görünümü

Şekil 4.19'da merkezler ve tip-1 uzak kule lokasyonlarda mevcut iki ağ, aktif renkle gösterilmişlerdir. Her iki çizimde de LAN-WAN arası geçişler gösterilmiştir. VPLS üzerinden bütün uzak kuleler ve bütün merkezler çok noktadan çok noktaya olarak birbirleriyle haberleşmektedirler. Tip-1 uzak kule lokasyonlarında da direkt şekilde gösterildiği gibi haberleşme için iki network bulunmaktadır.

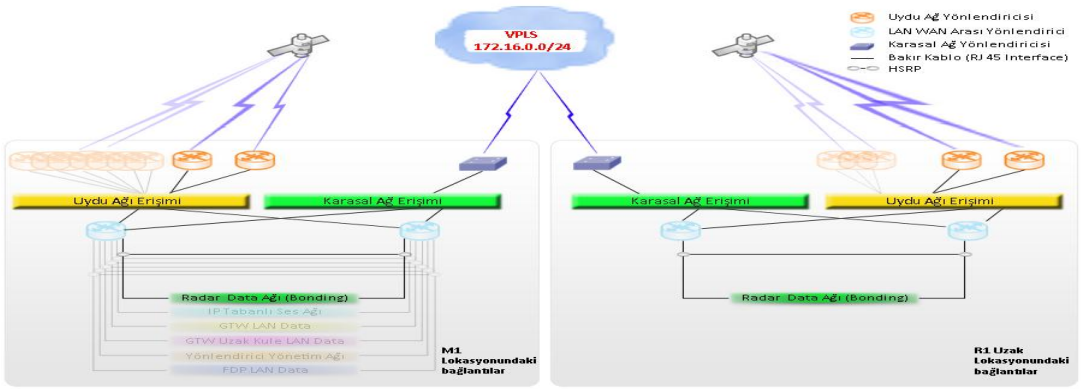
4.5.3. Merkezler tip-1 uzak lokasyonlar arası bağlantılar

Şekil 4.20'de merkezler ve tip-1 uzak lokasyonlar arası bağlantıların fiziksel olarak detayları gösterilmektedir.



Şekil 4.20. Merkezler ve tip-1 uzak lokasyonlar arası bağlantıların fiziksel görünümü

Tip-1 uzak lokasyonlardan (radar istasyonlarından) IP tabanlı radar verileri merkezlere her iki uçtaki yönlendiriciler vasıtasıyla ulaşır, bu taşıma işleminde birincil link her zamanki gibi karasal ağ'dır ve karasal ağ VPLS teknolojisini kullanmaktadır. İkincil link ise uydu ağ'ıdır. RHP dediğimiz radar sunucularının ürettiği radar verileri, QoS parametrelerinin uygulanabilmesi için, VLAN tanımlama işleminden sonra, yönlendiriciler üzerinden hat sağlayıcı ağına gönderim yapılır. Anahtarlar için ise tip-1 uzak lokasyonlarda LACP sayesinde link aggregation oluşturmuş ve yedeklenmişlerdir. Şekil 4.21'de ise merkezler ve tip-1 uzak lokasyonlar arası bağlantıların mantıksal olarak detayları gösterilmektedir.

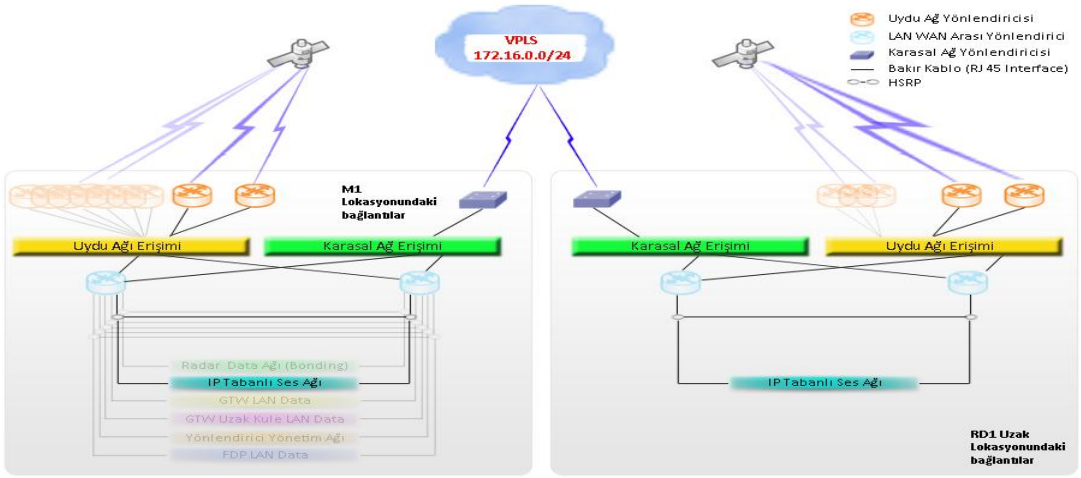


Şekil 4.21. Merkezler ve tip-1 uzak lokasyonlar arası bağlantıların mantıksal görünümü

Görüldüğü gibi, tip-1 uzak lokasyonunda sadece bir adet LAN radar ağı için oluşturulmuştur.

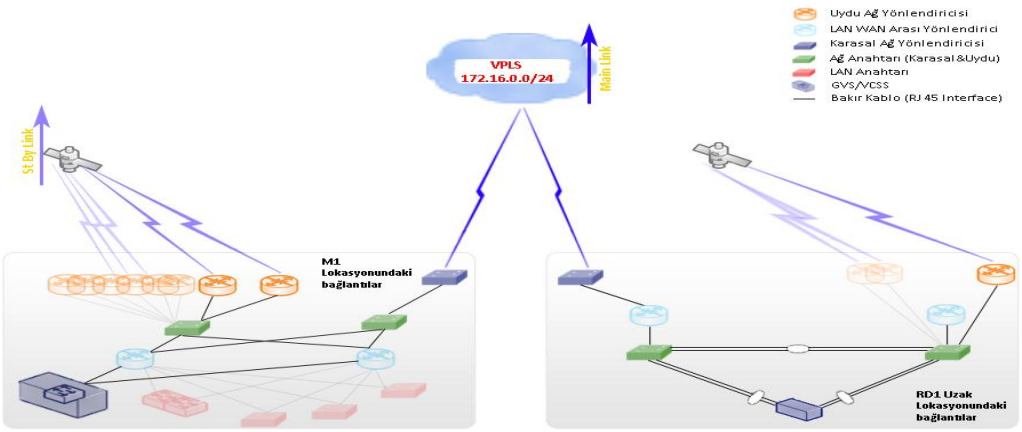
4.5.4. Merkezler ve tip-2 uzak lokasyonlar arası bağlantılar

Şekil 4.22'de merkezler ve tip-2 uzak lokasyonlar arası bağlantıların fiziksel olarak detayları gösterilmektedir.



Şekil 4.22. Merkezler ve tip-2 uzak lokasyonlar arası bağlantıların fiziksel görünümü

Tip-2 uzak lokasyonlardan (radyo istasyonlarından) IP tabanlı ses verileri merkezlere her iki uçtaki yönlendiriciler vasıtasıyla ulaşır, bu taşıma işleminde birincil link her zamanki gibi karasal ağ'dır ve karasal ağ, VPLS teknolojisini kullanmaktadır. İkincil link ise uydu ağı'dır. GVS (ses için analog/dijital dönüştürücüler) dediğimiz radyo cihazlarının ürettiği ses verileri, bir anahtarda toplanıp, QoS parametrelerinin uygulanabilmesi için belli bir VLAN eklendikten sonra, hat sağlayıcıdan önceki yönlendiricimize gönderilmektedir. Şekil 4.23'de merkezler ve tip-2 uzak lokasyonlar arası bağlantıların mantıksal olarak detayları gösterilmektedir.

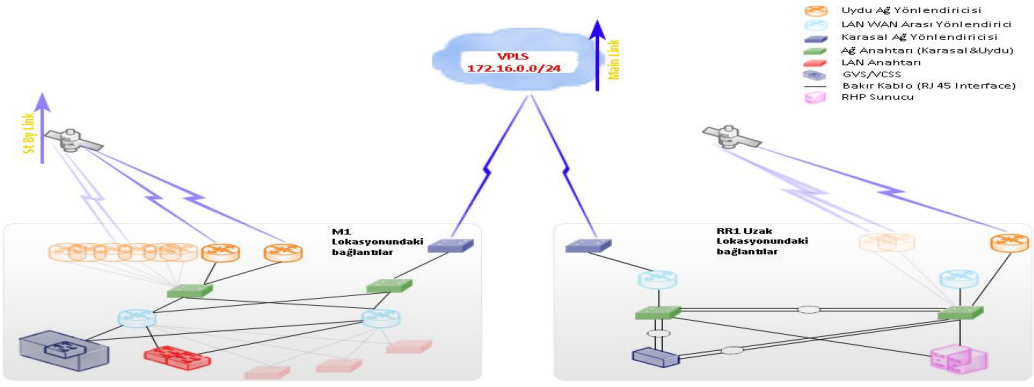


Şekil 4.23. Merkezler ve tip-2 uzak lokasyonlar arası bağlantıların mantıksal Görünümü

Görüldüğü gibi, tip-2 uzak lokasyonunda sadece ses için LAN oluşturulmuştur. Bu ses ağından veriler mevcut iç network anahtarına ulaştığında, bu ağlara farklı VLAN'lar eklenerek yönlendiricilere ulaşırlar ve yönlendirici VPLS ya da uydu ağ'ı üzerinden merkezdeki ses ağ'ına bağlanmayı ve işlemin devamlılığını sağlar. Merkezlerdeki ve tip-2 uzak lokasyondaki yönlendiriciler HSRP kullanırak, yedeklenmişlerdir.

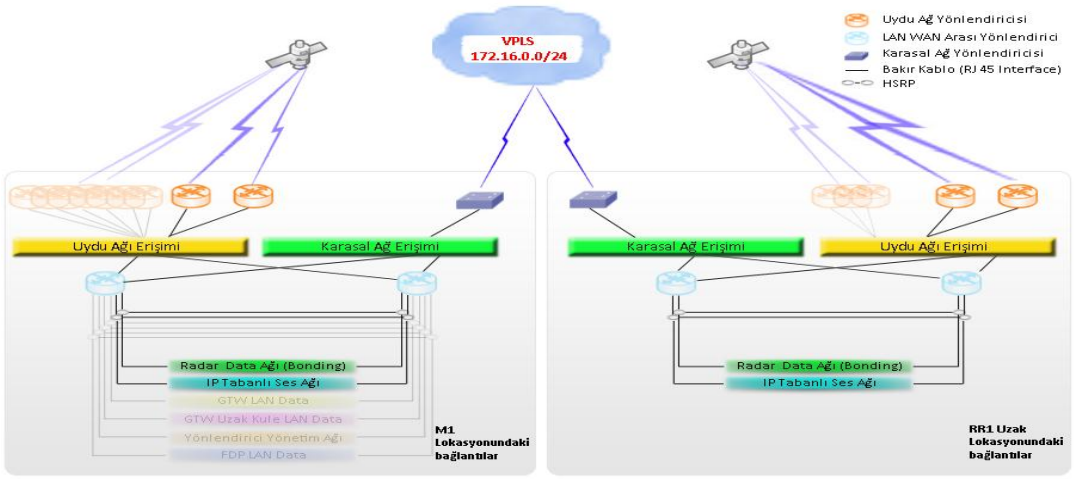
4.5.5. Merkezler-tip-3 uzak lokasyonlar arası bağlantılar

Şekil 4.24'de merkezler ve tip-3 uzak lokasyonlar arası bağlantıların fiziksel olarak detayları gösterilmektedir.



Şekil 4.24. Merkezler ve tip-3 uzak lokasyonlar arası bağlantıların fiziksel görünümü

Tip-3 uzak lokasyonlarda yani radar/radyo istasyonlarında, gelen radar ve ses verileri merkezlere her iki uçtaki yönlendiriciler vasıtasıyla taşınmaktadır. Şekil 4.25'de ise merkezler ve tip-3 uzak lokasyonlar arası bağlantıların mantıksal olarak detayları gösterilmektedir. Görüldüğü gibi, tip-3 uzak lokasyonlarda, radar ve ses ağı olmak üzere, iki adet LAN oluşturulmuştur ve her iki ağdan gelen veriler mevcut iç ağ anahtarına ulaştığında, bu ağlara farklı VLAN'lar eklenerek yönlendiricilere ulaşırlar.



Şekil 4.25. Merkezler ve tip-3 uzak lokasyonlar arası bağlantıların mantıksal görünümü

5. TEST ANALİZLERİ VE BULGULAR

Bu bölümde, öncelikle daha önceki bölümde yüzeysel olarak bahsettiğimiz karasal ve uydu ağları hakkında daha detaylı bilgi verilmiş, ayrıca karasal ve uydu ağ'ları üzerinde QoS testleri yapılmış, CoS mekanizması hakkında, yönlendirici yapılandırma komutlarından örnekler verilerek açıklamalar yapılmıştır.

5.1. Karasal Ağ

Karasal ağ olarak tanımladığımız ağ genellikle ülkelerin ilgili telekom firmaları tarafından sağlanan ağdır. Bu telekom firmaları bir çok çeşit servis sunabilmektedir. Daha önce de belirttiğimiz gibi biz karasal network için igili telekom firmasının VPLS hizmetini kullanmak istiyoruz, çünkü VPLS çok noktadan çok noktaya, WAN içerisinde bütün noktalar arasında transparan bir haberleşme sağlamaktadır. WAN içerisinde akan verilerimiz ise gerçek zamanlı data, kritik data gibi devamlılığının önemi yüksek olan veriler olduğu için bir SLA (Service Level Agreement) anlaşması yapmamız gerekmektedir. Bunun için öncelikle verileri kategorize etmemiz gerekmektedir.

- *Gerçek zamanlı veri : Video,ses, IP TV vb.*
- *Kritik veri : Radar data, Oracle, ERP, SAP, CRM vb.*
- *Standart veri : Internet, e-mail, ftp, tcp vb.*

Ses trafiği, veri trafiğinden farklıdır. Ses ve video uygulamaları, yüksek kalitede haberleşme sağlamak üzere kesintisiz bir veri akışını gerektirir. TCP'deki bildirim süreci gecikmelere neden olur ve bu da akışları keser ve uygulamanın kalitesini düşürür. Bu yüzden ses uygulamaları TCP yerine UDP'yi (kullanıcı datagram protokolü) kullanır. UDP, kayıp paketlerin yeniden iletilmesi için mekanizmalara sahip olmadığından, gecikmeleri en aza indirir.

TCP'nin UDP'ye karşı gecikmelerini anlamanın yanında, hedefine giderken trafiği işlemesi gereken ağ cihazlarının neden olduğu gecikmeleri veya gecikme sürelerini, anlamak da önemlidir. OSI 3.katman cihazları, işlemeleri gereken başlık sayısı nedeniyle 2.katman cihazlarından daha fazla gecikme oluşturur. Bu yüzden, yönlendiriciler anahtarlara göre daha uzun bir gecikmeye yol açar.

Bunun yanısıra, ağ uygulamalarının çoğu veri trafiğini kullanır. Çevrimiçi uygulamaların bazı türleri, verileri düzensiz olarak iletir. Veri saklama gibi diğer türler, belirli bir süre boyunca yüksek hacimlerde trafik iletirler.

Bazı veri uygulamaları, güvenilirlikten ziyade zaman duyarlılığıyla daha fazla ilgilenir ve veri uygulamalarının bazıları gecikmeleri hoş görebilir. Bu nedenle veri trafiği genellikle TCP'yi (İletim Denetim Protokolü) kullanır. TCP, kaybedilen paketlerin ne zaman yeniden iletilmesi gerektiğini belirlemek üzere bildirimleri kullanır ve dolayısıyla teslimatı garantiler [22].

Ülkemizde şu an karasal hat sağlayıcı, metro ethernet, mpls, vpls vb. teknolojiler için bazı farklı hizmet paketleri sunmaktadır. Biz gerçek zamanlı veri taşıdığımız için Çizelge 5.1'de belirtilen platinium paket seviyesine ihtiyaç duymaktayız.

Çizelge 5.1. Karasal ağ'da platinium pakette kullanılan veri oranları [28]

Paket	Gerçek Zamanlı Veri	Kritik Veri	Standart Veri
Platinium	45 %	30 %	25 %

Daha spesifik bakmak gerekirse, karasal hat sağlayıcı tarafından sağlanan pakete göre, satın alınan bant genişliğinin % 45'i kadar gerçek zamanlı veri ve % 30'u kadar ise kritik veri transferi yapılabilir. Kalan bant genişliği ise standart veri sınıfı için ayrılmıştır.

Karasal network 2.katman seviyesinde olan VPLS için uçtan uca QoS ve CoS, ethernet header'ında sağlanmıştır ve 3 farklı COS servisi mevcuttur. Bu SLA değerlerini QoS parametrelerini de hesaba katarak, ağ tabanlı düşünürsek kullandığımız pakete göre PE-PE arası karasal hat sağlayıcı tarafından sağlanması gereken QoS değerleri, aşağıdaki tabloda gösterildiği gibidir.

Çizelge 5.2. Karasal ağ'da QoS parametre limitleri

	Platinium
Erişilebilirlik (Availability)	99,99 %
Jitter	5 ms
Gecikme (Round Trip Delay)	60 ms
Paket İletimi (Packet Delivery)	99,70 %

- *Telekom (karasal servis sağlayıcı) PE-PE arasında yıllık ortalama data erişebilirlik değeri % 99,99'dur.*
- *Aylık jitter değeri 5 ms in altında olmalıdır.*
- *Aylık round trip (latency) gecikme değeri 60 ms.'nin altında olmalıdır.*
- *Aylık paket alım miktarı en az %. 99,70 miktarında olmalıdır.*

Yapılacak olan QoS testlerindeki sonuçların bu değerlere olan oranlarının analiz edilmesi gerekmektedir. Platin servis paketi için QoS değerleri baz alınarak test sonuçları açıklanacaktır.

5.1.2. Erişim arayüzleri

Yerel telekom (karasal hat sağlayıcı) tarafından sağlanan arayüz'ler fiziksel olarak RJ-45 ve ethernet LAN arayüzler ya da tek kipli/çok kipli fiber optik arayüzler olarak planır.

RJ-45 arayüzler için, bir çeşit bükülü kablo çifti kullanan ethernet kartları da diyebiliriz. Bu bükülü kablo çiftinin ucuna RJ-45 konnektörü takılır. 10, 100, 1000

Mbit/s hızlarında veri iletimini sağlarlar. Bu portlardan bir tanesi bir CAT-5 UTP kablo aracılığıyla bir iç anahtara bağlanır ve iç anahtar'dan yine benzer bir kablo ile yönlendiricilere bağlantı yapılır.

Bazı durumlarda ise hat sağlayıcı anahtarımıza direkt fiber optik kablo aracılığıyla bağlanabilir. TP (büklümlü çift-twisted pair) ve eşeksenliden farklı olarak, fiber optik kablolar verileri ışık darbelerini kullanarak iletir. Fiber optik kablo cam veya plastikten yapılmıştır ve bu iki madde de elektriği iletmez. Bu da fiber optik kablonun EMI'ye (elektromanyetik girişim) karşı hassas olmadığı ve girişimin sorun oluşturduğu ortamlarda kullanım için uygun olduğu anlamına gelir. EMI direncine ek olarak, fiber optik kabloların çok yüksek miktarda bant genişliğini desteklemesi onları yüksek hızlı veri omurgaları için ideal hale getirir. Her fiber optik devre gerçekte iki fiber kablodur. Biri veriyi iletmek için, diğeri ise veriyi almak için kullanılır. Biz genelde iki çeşit fiber optik kablo kullandık, bunlar bir çok kipli ve tek kipli olarak adlandırılmaktadır [31].

Fiber optik kablo çeşitleri içinde çok kipli kablo daha uygun fiyatlıdır ve daha yaygın olarak kullanılır. Işık darbeleri üreten ışık kaynağı genellikle bir LED (ışık yayan diyot)'dir. Aynı anda kablo üzerinden iletilen ve her biri veri taşıyan birden çok ışık hüzmesi bulunduğundan, buna çok kipli denir. Çok kipli çekirdekte her ışık hüzmesi ayrı bir yolu takip eder. Çok kipli fiber optik kablolar genellikle 2000 metreye kadar olan bağlar için uygundur. Ancak teknolojideki gelişmeler bu mesafeyi sürekli olarak artırmaktadır [29].

Tek kipli fiber optik kablolar, ışığın fiber üzerinde yalnızca tek bir yolu takip edebileceği biçimde oluşturulmuştur. Tek kipli fiber optik kablolar için ışık kaynağı genellikle bir LED lazeridir ve bu normal LED'lara göre çok daha yüksek fiyatlı ve daha yoğundur. LED lazerinin yoğunluğu sayesinde daha yüksek veri hızları ve daha uzun aralıklar elde edilebilir. Tek kipli fiberler, yaklaşık 3000 metre boyunca veri iletebilir ve çeşitli NOC (Network Operation Center)'lerın arabağlantısı gibi omurga kablolaması için kullanılır. Teknolojideki gelişmeler bu mesafeyi de sürekli olarak artırmaktadır.

5.2. Uydu Ağı (Yedek Ağ)

5.2.1. VSAT teknolojisi (A Very-Small-Aperture Terminal)

VSAT (Very Small Aperture Terminal) sistemi küçük çaplı antenlere (0,8 m – 2,4 m) sahip uydu yer istasyonları için kullanılan genel bir terimdir. VSAT sistemi, merkez yer istasyonu (hub istasyonu) ve coğrafi olarak birbirinden uzak noktalar arasında çift yönlü uydu iletişimini sağlayan bir sistemdir. VSAT sistemleri ses, veri, internet, intranet, video konferans vb. bir çok servisi destekler [30].

Sahip olduğu hizmet çeşitliliğiyle VSAT sistemi, sadece ulusal sınırlar içerisinde kalmayıp, uydunun kapsama alanında bulunan hemen her yerde kullanılabilir. Sistem içinde kullanılan özel algoritmalar yardımıyla güvenlik üst düzeye çıkarılabilir. VSAT sistemi hızlı bir şekilde değişen haberleşme ihtiyaçlarını karşılayabilecek esnek bir yapıya sahiptir. Sisteme dair bazı özelliklerden detaylı bahsetmek gerekirse:

Hizmet Çeşitliliği

Çok port/çok protokol özelliği VSAT sistemi üzerinden kullanıcıya birden çok sayıda uygulama seçeneğinden faydalanma imkânı sağlayabilir. VSAT şebekesi SNA/SDLC, BSC (3270/3780), X.25, X.3 PAD ve TCP/IP protokollerini destekleyebilir ve protokol aldatmacası (protocol spoofing) yaparak sorgulamayı elimine edebilir. VSAT kanallarından sadece veri iletişimi yapılır. Sorgulama bilgileri uyduya çıkmadığı için cevap süresi kısalır ve performans artışı olur.

Küresellik

Uydu üzerinden haberleşme olanakları yalnız ulusal sınırlarla kısıtlı kalmayıp, uluslararası servisler için de uygun bir altyapı oluşturur.

Süreklilik

VSAT'terminallerinden oluşan iletişim yapısı ile, hem en az sayıda arıza olma özelliği hem de birimlerin yedeklenmiş olması ve iki arıza arasındaki ortalama sürenin uzunluğu ile karasal sistemlere göre oldukça yüksek bir avantaj sağlar.

Yayın Özelliği

Uydu haberleşmesinin gereği olarak haberleşme yalnız noktadan noktaya bir nitelikle sınırlı kalmayıp, tek yönlü yayın özelliğini de desteklemektedir. Büyük hacimli bilgilerin birden çok merkeze aktarılmasında süre avantajı sağladığı gibi, uzak noktalara aynı anda ve sürekli data aktarımı olanağıyla kullanıcıya önemli bir avantaj sağlamaktadır.

Güvenilirlik

VSAT sisteminin sürekliliğini artıran nedenler aynı zamanda güvenilirliğini de sağlamaktadır. Kullanılan özel algoritmalar haberleşme kalitesiyle birlikte güvenilirliği de üst seviyeye çıkartmaktadır.

Esneklik ve kolay genişleme

Günümüzdeki haberleşme ihtiyaçlarının ani ve değişken olması, haberleşme altyapısının oldukça esnek olmasını gerektirmektedir. Bu yüzden tesis, servis ve gerekli yerlere, gerektiği kadar yatırım ilkesi ön plana çıkmaktadır.

Hızlı tesis ve etkin servis

VSAT terminallerinin çok küçük anten ile bina içi birimden oluşması, karasal sınırlılık ve bağımlılıklarının olmaması büyük kolaylık sağlamaktadır. Merkezi denetim ve yönetim ise bu sistemlerin aktif bir iletişim ağına dönüşmesini sağlamaktadır.

Merkezi denetim ve yönetim

Hub istasyonunun birden fazla değişik yerleşimde yedeklenmesi sonucu herhangi bir uç noktada hasar gören VSAT terminali bütün haberleşmenin sürekliliğini etkilememektedir. Ayrıca VSAT terminallerinin küçük oluşu ile hızlı tesis ve servis

olanağı, aynı bölgede haberleşmenin hızla yeniden sağlanmasına imkan vermektedir [30].

5.2.2. VSAT sistem mimarisi

VSAT sistemleri uygulamaya bağlı olarak değişik mimarileri desteklemektedir. Bunlar ;

- *Noktadan noktaya,*
- *Yıldız topoloji,*
- *Tek yönlü yayın (Broadcast) şebekesi,*
- *Çift yönlü etkileşimli (Interactive) şebekedir.*

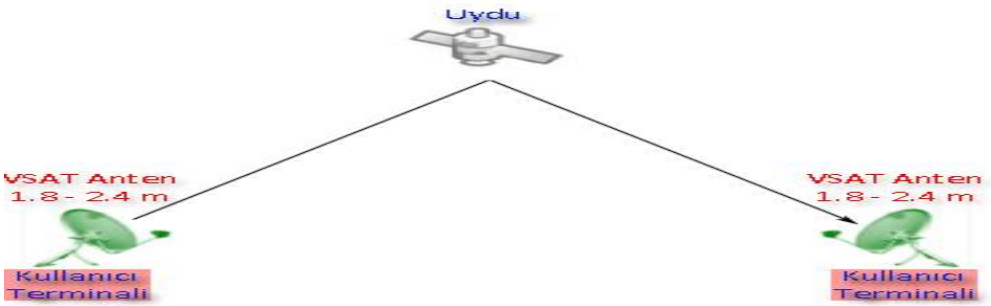
VSAT sistemleri esnek yapılarından dolayı; ses, veri ve görüntü iletimini ayrı ayrı ya da ayni anda gerçekleştirebilir. Bu esneklik, video konferans ile dağıtık veri işlem ve yedekleme türünde çeşitli uygulamalara da olanak sağlar.

Hub istasyonundan VSAT'lara olan iletişim TDM (time division multiplexed) kanalı vasıtasıyla yapılır. Her bir veri paketinin adresi bellidir. Böylece VSAT'lar kendi adreslerine yollanan mesajları alır ve diğerlerini dikkate almaz. VSAT'lardan hub istasyonuna doğru olan iletişimde TDMA (time division multiple access) tekniği kullanılır. Birçok VSAT tek bir uydu kanalını paylaşabilir ve böylece maliyetlerde azalma sağlanır.

Şebeke protokolleri, uydu iletişim kaynaklarını en etkin şekilde kullanarak VSAT'lar ve hub istasyonu arasındaki veri alış verişini sağlar. Birçok VSAT şebekesinde hub istasyonundan VSAT'lara sürekli olarak TDM sinyali gönderilir. VSAT şebekesinde kullanılan çoklu erişim tekniği, sistemin performansını ve işlem gecikmelerini kontrol eder.

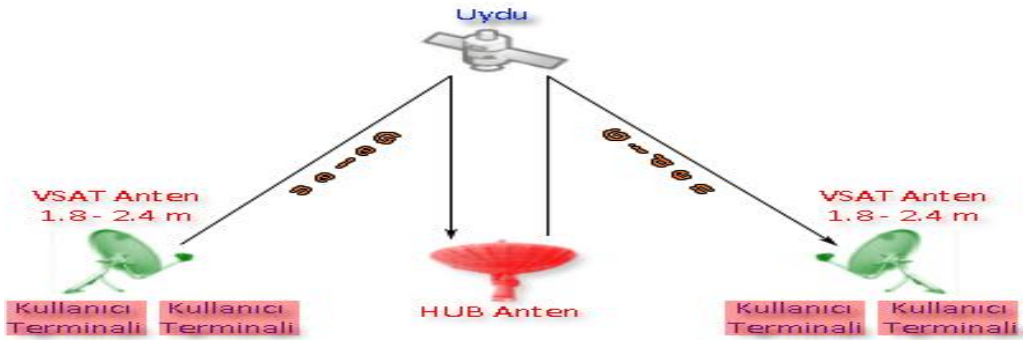
VSAT teknolojisi Türkiye'deki iletişim ortamı için ideal bir çözümdür. Kullandığımız VSAT mimarileri;

Tek bir hop kullanma : Bu tür iletişimde arada ek bir bağlantı yoktur, iki istasyon uydu üzerinden direkt haberleşir, bu bağlantı türüne ayrıca *Mesh* denmektedir (Bkz. Şekil 5.1).



Şekil 5.1. Uydu ağ'ında mesh topolojisi

İki hop kullanma : Şekil 5.2'de gösterildiği gibi bu iletişim tipinde gelen sinyal (inbound link) aradaki bir istasyona uğrar, istasyona ugradıktan sonra giden sinyal (outbound link) diğer hedef noktasına ulaşır. Bu topolojiye ise Star denmektedir.



Şekil 5.2. Uydu Ağı için STAR topolojisi

Ülkemizde uydu bağlantıları genellikle Türksat A.Ş tarafından sağlanmaktadır. Biz kurduğumuz WAN'da her uzak istasyon ve merkez arası uydu bağlantıları sağladık. Telekom tarafından sağlanan karasal hat çalışmadığında ikincil link olarak uydu hatlarının devreye otomatik olarak girmesi planlanmakadır. Karasal ve uydu ağlarının farklı alt yapılarda kuruşmuş olması yedekleme avatantajı sağlamaktadır.

Gerçek zamanlı uygulamalarda, gecikme (latency) miktarının düşük olması gerekmektedir, bu yüzden anlattığımız iki topolojiden, *mesh* yapısı tercih edilmiştir. Star topolojide ise çok noktaya yayın (multicast) radar verisi akışında kullanılmaktadır.

Uydu ağı uçtan uca QoS parametrelerini öncelikleri olabilecek olan yerlere göre ayarlayabilmektedir. Sınıflandırma Layer-3 ve Layer-4 seviyesinde yapılmaktadır. Karasal ağ'da olduğu gibi, uydu ağ'ında da bir SLA olması gerekmektedir. Uydu ağ'ı tarafından desteklenen SLA aşağıda belirtilmiştir. Uydu ağı için yapılacak olan QoS test sonuçlarıda aşağıdaki parametler ele alınarak açıklanacaktır.

Mesh bağlantısı için SLA:

- *Gecikme (Latency) < 400 ms,*
- *Jitter < 50 ms,*
- *Paket Kayıp Oranı (Packet Error Rate (PER)) < 10-3.*

Star bağlantısı için SLA:

- *Gecikme (Latency) < 700 ms,*
- *Jitter < 100 ms,*
- *Paket Kayıp Oranı (Packet Error Rate (PER)) < 10-3.*

5.2.3. Erişim arayüzleri (Uydu bağlantıları için)

Bant genişliği gereksinimlerine göre her istasyonda farklı sayıda uydu erişim arayüzleri sağlanmıştır. Bir çok karasal hatta olduğu gibi, uydu sağlayıcı tarafından fiziksel olarak LAN RJ-45 arayüzleri ve ethernet protokolleri aracılığıyla bağlantılar sağlanmıştır. Uydu yönlendiricisi ile yerel ağdaki anahtar arası bağlantı, bir UTP CAT-5 kablo ile yapılmıştır.

5.3. Quality of Service (QoS)

Hizmet Kalitesi (QoS), bir ağın seçili ağ trafiğine tercihli hizmet sağlama yeteneğini ifade eder. QoS'in birincil amacı, kontrollü atlama ve gecikme, adanmış bant genişliği ve azaltılmış paket kaybı dahil olmak üzere öncelik sağlamaktır. QoS politikaları oluştururken, hangi trafiğin tercihli hizmete gerek duyduğuna odaklanmak önemlidir. QoS sorunlarının ağdaki aygıtların yanı sıra, ağda kullanılan uygulamaları da nasıl etkileyeceğini göz önünde bulundurmalıdır.

Bazı uygulamalar bant genişliği gereksinimlerine, paket gecikmelerine, ağ atlamalarına ve olası paket kayıplarına karşı aşırı duyarlıdır. Bu tür uygulamalar genellikle gerçek zamanlı akan ses ağları olabilir. Genellikle, ses trafiği, kullanıcılar arasında basit bir bağlantıdan daha fazlasını gerektirir. İşlemlerin kalitesi, fazlasıyla önemlidir. Gecikmeler meydana geldiğinde, ses kesilir ve kelimeler bozulur. Standardın altında işlem kalitesinden kaçınmak için, QoS mekanizmalarının uygulanması gerekir. Örneğin, ses paketlerinin gecikmesinin 60 ms'den daha fazla olmaması gereklidir. QoS'nin olmadığı bir ağda, tüm paketler aynı şekilde işlenir ve gerçek zamanlı uygulamalar olumsuz etkilenir [3, 22].

Bir ağda QoS uygulamak için trafiğin doğru şekilde önceliklendirildiğinden emin olmak amacıyla üç temel adım izlenebilir:

- *Trafik Gereksinimlerini Belirlemek*

Ses, kritik data, standart data gibi farklı tür trafikler için QoS gereksinimlerini ve hangi düşük öncelikli trafiklerin olabildiğince iyi olarak işaretlenebileceğini belirlemek gerekir.

- *Trafik Sınıflarını Tanımlamak*

Veri trafikleri belirlendikten sonra, trafikler çeşitlerine göre sınıflandırılmak zorundadır. Örneğin, ses trafiği, ftp veri trafiği, telnet trafiği vb. Bütün trafik sınıfları için ayrı VLAN'lar yaratılır ve veri paketleri ait oldukları sınıfı belirtecek şekilde işaretlenir.

- *QoS Politikalarını Tanımlamak*

Son adım, sınıflara uygulanacak QoS politikalarını belirlemektir. Bu politikalar, tıkanıklığı yönetme kurallarını ve trafik kuyruklarını zamanlamayı içerir. Bir ağda trafiği yönetmek için pek çok yöntem kullanılabilir. Gelen trafik sınıflandırılır, sınıfını belirtecek şekilde işaretlenir ve iletilir.

QoS yapılandırırken belirli bit ağ trafiği seçilebilir ve bu ağ trafiği kullanımdaki önemine göre önceliklendirilebilir. QoS, ağın erişim, dağıtım ve çekirdek katmanları'nda kullanılabilir. Erişim katmanı'ndaki 2. katman anahtarlar, QoS'i IEEE 802.1p hizmet sınıfı'na (CoS) göre destekleyebilir. İkinci katman anahtarlar, QoS'i, anahtardan ağa çerçeve göndermeyi önceliklendirmek için sınıflandırma ve zamanlama kullanır. Üçüncü katman aygıtlar, QoS'i fiziksel arayüze, IP adreslerine, mantıksal bağlantı noktası numaralarına ve IP paketindeki QoS bitlerine göre destekleyebilirler. Dağıtım ve çekirdek katman aygıtlarındaki QoS, trafik akışının her iki yönünde de desteklenmelidir.

Farklı trafikler için QoS uygulanmasında biz her trafik türü için farklı VLAN (Virtual Local Area Network)'ler yarattık. Eğer bütün trafikler aynı VLAN'daysa, mevcut bant genişliği hepsi tarafından kullanılmaya çalışılır ve bu ağ'da bir tıkanıklığa sebep olabilir. Bir çatışmayı engellemenin en basit yöntemi, ağdaki trafikler için ayrı VLAN'lar kullanmaktır. Böylece, ağdaki bir problem de daha kolay analiz edilebilir durumda olur.

Kullanılan *Cisco* yönlendiricileri paketlerin sınıflandırılmasını ve etiketlendirilmesini yönetmektedir. Paketlerin farklı sınıflara ayrılması, onların operasyonel olarak öncelikleri ve performans gereklilikleri düşünülerek tasarlanmıştır.

Hem uzak istasyonlarda hem de ana merkezlerde, kullanıcı önceliği, etiket alanı, IEEE 802.1Q ethetnet frame'i ve 802.1p standartlarına göre *Layer 2 CoS* parametreleri kullanılarak tasarlanmıştır. Sınıflandırma ACL (Access control list) kullanılarak, IP tabanlı data akışı ilgili subnetlere göre düzenlenmiştir.

Tasarladığımız ağ trafiklerine göre yapacağımız QoS testlerinde hat sağlayıcılarımızın (karasal-uydu) bize kalitesini garantilediği QoS parametreleri aşağıda belirtilmiştir.

- *İşlem hacmi (Throughput),*
- *Gecikme (Latency ya da Delay),*
- *Jitter,*
- *Paket kaybı (Packet loss),*
- *Erişilebilirlik.*

5.3.1. İşlem hacmi (Throughput)

İşlem hacmi, bir noktadan diğer bir noktaya ortam üzerinde sorunsuz iletilen verilerin oranını verir. İşlem hacmi, bant genişliği kullanım oranı olarakta ifade edilir. İşlem hacmi, genelde bits/second, bps:bit-per-second cinsinden ölçülür. Aslında, işlem hacmi, bir uygulama için gerekli olan maksimum bant genişliği miktarıdır. Bu bant genişliklerinin efektif kullanılabilmesi için QoS teknolojisi gereklidir. İşlem hacmi, aynı zamanda o hattın performansını da gösterir, örneğin evde kullandığımız internet bağlantı hızının, indirme (download) ve yükleme (upload) oranına göre yükselmesini istiyorsak hattımızın bant genişliği değerini yükseltmemiz gerekir. Sistem işlemleri hacmi ya da throughput (aggregate) ise, bir ağdaki bütün terminallerin veri hızlarının toplamıdır. Kullanılan her kablo, cihaz için maksimum bir işlem hacim değeri mevcuttur ve bunun üzerindeki veri trafikleri kayıplara neden olabilir. O yüzden, WAN için bir devre kiralanması gerektiğinde, işlem hacim hesaplarının oldukça yerinde yapılması, veri akışının devamlılığı için büyük önem arz eder.

5.3.2. Gecikme (Latency)

Tek yönlü olarak düşünüldüğünde verinin alıcıya ulaşması süresince geçen zamandır. Gidiş-geliş gecikmesi (Round trip delay) ise, iki adet tek yönlü gecikmenin

toplamıdır. Genellikle ses sistemlerinde gecikme 150 ms'nin altında tutulmak istenir. Ses sistemlerinde 150 ms'nin altındaki gecikmeler genellikle pek algılanmaz. Uydu sistemlerinde gecikme, karasal iletişim sistemlerine göre çok daha yüksektir, özellikle uydu üzerinden yapılan ses görüşmelerinde problemler oluşabilmektedir. Veri haberleşmesinde ise gecikme, ses haberleşmesindeki kadar kritik değildir. Ağ üzerindeki gecikme, bir uygulamanın iletim sürecinde ağın giriş ve çıkış noktaları arasında hareket ettiği zaman dilimidir denebilir. Gecikme, ses, görüntü ve faks iletimleri gibi normalin dışındaki gecikmelerde zaman aşımına uğrayıp, iptal olan uygulamalar üzerinde önemli QoS sorunları yaratır. Bazı uygulamalar az miktarlardaki gecikmeleri tolere edebilmekte, ancak belirli bir süre aşıldıktan sonra QoS sorunu kaçınılmaz hale gelmektedir.

5.3.3. Jitter (Gecikme değişikliği)

Jitter (gecikme değişiklikleri), belirli bir trafik akışında birbiri ardına gelen paketlerin değişken karakterdeki gecikmelerinin ölçüsüdür, yani paketlerin gecikme sürelerindeki varyasyondur. Türkçe de seğirme olarak kullanılır. Gecikme değişikliğinin ses ve video gibi gerçek zamanlı ve gecikmeye duyarlı uygulamalar üzerinde önemli etkileri olabilir. Söz konusu gerçek zamanlı uygulamalar paketleri sabit bir hızda ve aralarında sabit süreler olduğu halde almak isterler. Varış hızı değişkenlik gösterdikçe uygulamanın performansı etkilenir. Gecikme değişiklikleri minimum seviyede olduğunda sorun yaşanmayabilir, ancak arttıkça uygulama kullanılamaz hale gelir. Veri uygulamaları jitter'dan bağımsız olarak doğru çalışır. Alıcı tüm veri paketlerini alıp, sıraya koymadan mesajı okuyamaz. Yani, ilk paketin 20 ms gecikme ile, sonrakinin 200 ms gecikme ile alıcıya erişmiş olmasının bir önemi yoktur. Buna karşılık ses ve video uygulamalarının tolerans gösterebileceği ve işlevsel kalabileceği gecikme değerlerinin değişmesi için kesin sınırlar mevcuttur. Jitter, gerek ses ve gerekse video sinyallerini bozar. QoS açısndan gecikme ve jitter değerleri birlikte ele alınır. Örneğin bir uygulamadaki gecikmenin max değeri 200 ms ve min değeri 190 ms olabilir. Bu uygulamada jitter'ı azaltabilmek için kullanıcı uygulamaya, "jitter" tamponları (ara bellek) eklemek durumundadır. Gecikme değişikliği tamponları sayesinde, tüm trafiğin gecikme değeri örneğin 200 ms'ye

eşitlenerek, değişme önlenmiş, yani gecikme değeri kararlı hale getirilmiş olur. Bu uygulamada kullanıcı, belirli bir maliyet ödeyerek ağ uygulamasına QoS ekleyebilmektedir.

5.3.4. Erişilebilirlik (Avalibility)

Bir ağ üzerindeki güvenilirlik, lokal (yerel) veya küresel (global) olabilir. Eğer belirli bir periyot boyunca, güvenilirlik değerleri sağlanamazsa, ağ sağlayıcıları bunu müşteriye geri öder veya bu kötüleşmeyi giderici diğer olanaklar sunarlar.

Güvenilirlik açısından bir yıl içinde, 60x60x24x365 = 31536000 saniye mevcuttur. Bu nedenle, %99.9 güvenilirlik 31536 saniye anlamına gelir (yani yaklaşık olarak 9 saat). Çalışmama veya arıza durumları segmentler halinde değerlendirilir ve bir segment yaklaşık olarak 4 saat olarak sabitlenmiştir. O halde %99.9 çalışabilirlik (veya güvenilirlik) senede yaklaşık olarak 2 adet 4 saatlik çalışmama segmentine karşı düşer. Genellikle çalışmama durumları pazar günü sabah 3:00 saatlerine denk gelirse fazla mesele yoktur. Buna karşılık eğer çalışmama durumu cuma günü saat 12:00 saatlerinde olursa, genellikle kabul edilemez.

Yüzde 99.99 çalışabilirlik senede bir saatten daha az çalışamama anlamına gelir. Bu değer, önceden planlanmış, zamanı belli donanım/yazılım bakımlarının yapılmasına bile olanak tanımayan bir süredir. Belki bu değere (bakım süresi), tüm donanım ve yazılımların yedeklemeli çalıştığı ortamlarda ulaşılabilir.

Demek istediğimiz şudur: çok yüksek oranlarda çalışabilirliğin garanti edildiği uygulamalardan şüphe edilmelidir. Her ne kadar yüzde 99.5 çalışabilirlik (yani senede 43.8 saat) ile yüzde 99.9 çalışabilirlik (yani senede 8.77 saat) arasındaki fark fazla değilse de, tüm seneye yayıldığında ortaya önemli bir süre farkı çıkmaktadır [32].

5.3.5. Kayıplar (Packet losses)

Veri iletimi esnasında bazı paketlerin hedefe ulaşamaması demektir. Yanlış yönlendirme, iletim esnasında paketlerin zarar görmesi, girişim v.b. yollarla oluşabilir. Ağ üzerinde gönderilen bir paketin ulaştığı noktalardaki hafıza kısıtlarından dolayı nokta tarafından kabul edilmemesi veya ağdaki ulaşım yollarında karşılaşılan sorunlardan dolayı hedefe ulaşmadan kaybedilmesine paket kaybı nedir. Yani paket bir hedefe ulaşmak için bir kaynaktan ayrılır ve hedefe asla ulaşamazsa kaybolmuş olarak kabul edilir.

Kaybolan paketler, guvenilir protokol ile gönderme yapılıyorsa yeniden yollanarak telafi edilmeye çalışılabilirler. Paket kayıplarında paket kayıp yüzdesinin yanı sıra kaybolan paketlerin ne kadar ardışık olduğu çok önemlidir. Çünkü üst üste bir çok paket kaybı olursa karşı taraf gelen veriyi anlamakta çok daha fazla zorluk çekecektir ya da anlamayacaktır. Örneğin bir telefon görüşmesi sırasında sadece bir kelimeyi duymadığınızı düşünürsek, konuşmanın genelinden kopma durumunuz pek olası değildir ama komple bir cümleyi duymadığınızda o anki konuşmaya normal devam etmekte zorluk çekmeniz olasıdır. Genelde gerçek zamanlı ağlarda kabul edilebilir paket kayıp oranı % 0,1- % 0,3 arasındadır.

5.4. QoS Testleri

5.4.1. Amaç

Bu testleri yapmaktaki amaç servis sağlayıcıların (karasal-uydu) tahsis etmiş olduğu hatlardaki QoS paremetlerinin bizim limitlerimizdeki değerlere uygunluğunu değerlendirmektir. Her sağlayıcı için aşılmaması gereken belli QoS parametre değerleri daha önceki tablolarda, hem uydu hem de karasal link için ayrı ayrı belirtilmişti.

Testlerde, throughput, latency, packet loss ve jitter değerleri ölçülmüştür. Bu testler için kullanılan yazılım "Ixia" tarafından sağlanan "IXCHARIOT" programıdır. Program hakkında teknik detaylar verilmiştir.

IXCHARIOT programı, gerçek dünyadaki uygulama verilerini (sunucu, client vs..) simule edebilen bir trafik üretme ve karar destek aracıdır. Simule ettiği bir çok farklı protokol ve uygulama ile IXCHAROIT yazılımı binlerce ağ uç noktası üzerinden performans değerlendirmesi ve cihaz testleri yapmayı sağlamaktadır. Bazı kullanım alanları;

- *Ağ donanım ve yazılım performans ve kapasitesini değerlendirmede,*
- *Ağ ürünlerini satın almadan önce, karşılaştırma ve deneme yapmada,*
- *Performans problemlerinin kaynağını bulmada,*
- *Yeni uygulamaların çalıştırılması durumunda etkilerinin öngörülmesinde,*
- *Tipik ağ işlemlerinin ölçümlendirilmesinde,*
- *Hat sağlayıcıdan beklenen ağ performans ve kapasitesinin değerlendirilmesi olarak sıralanabilir.*

IxChariot bir konsol programı ve ayrıca dağıtılmış olan performans uç nokta programları aracılığıyla çalışmaktadır, (Bkz Şekil 5.3). Test yapılacak konsol haricindeki her noktada, performans endpoint yazılımı kurulmuş olmalıdır. Bütün bu uç noktalarda toplanan performans ölçümleri daha sonra konsol noktasına istatistiksel olarak gönderilmektedir. *"Endpoint pair"* dediğimiz uç noktalar eşlenmiş iki bilgisayarın ağ adreslerinden oluşur. Test esnasında bir endpoint pair kullanılabilir ya da daha kompleks testlerde yüzlerce, binlerce, endpoint pair bir çok farklı protokol eklenerek kullanılabilir.Yapılacak her test için, ilgili bant genişliği ve protokoller gibi detaylar, yapılandırılarak IxChariot scriptleri hazırlanmalıdır. Bu testlerde "*console*" dediğimiz IxChariot yazılımının kurulu olduğu sunucuda bütün client'lardan yani endpoint pair'lerden gelen performans ölçüm verileri görüntülenebilir hale gelmektedir [33].

IxChariot yazılımını kullanabilmemiz için gerekli olan software & hardware Çizelge 5.3'te ve Çizelge 5.4'de verilmiştir. Minimum yazılım gereksinimleri :

Çizelge 5.3. Test için gereken minimum yazılım özellikleri

İşletim Sistemi	Protokol	Web Browser	PDF Okuyucu
Windows Server 2003 Windows XP Professional, SP2 and SP3 Windows Vista: Business, Enterprise, and Ultimate editions.	TCP/IP	Microsoft Internet Explorer 5.0 or higher	Herhangi bir PDF reader, dokumanları okuma amacıyla.

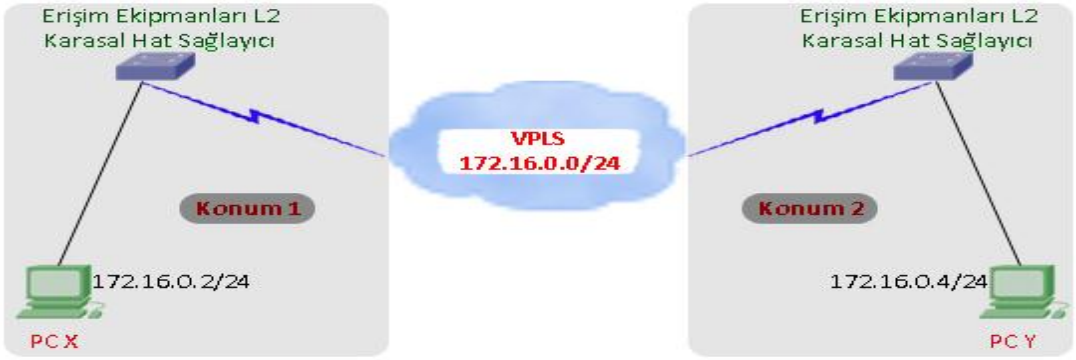
Minimum donanım gereksinimleri :

Çizelge 5.4. Test için gereken minimum donanım özellikleri

İşlemci	Ram	Hard Disk	Ekran
Pentium III processor running at 1.6 GHz.	RAM 256 MB.	Disk space 600 MB.	Display Color palette of at least 256 colors, with minimum resolution of 1152x864.

5.4.2. Test senaryosu

Karasal bağlantılar için yapılmış olan testi senaryosu Şekil 5.3'te gösterilmiştir. Şekilde, iki uç nokta (endpoint) gösterilmiştir, bu uç noktalar test yapılan iki noktayı göstermektedir. Konsol noktası ise test yapılmasını sağlayan sunucunun bulunduğu noktadır. Bütün noktalar 172.16.0.0 ağ adresi ve 255.255.255.0 (24) ağ maskesi üzerinden haberleşmektedir ve ilgili IP adresleri bu ağ ve ağ maskesi değerlerine göre verilmiştir.



Şekil 5.3. Test senaryosu

M7 ve M1 noktaları arasında unicast 4 Mbit'lik bir data trafiği için yapmış olduğumuz QoS test sonuçları ve IxChariot script yapılandırma parametreleri aşağıda Çizelge 5.5 ve Çizelge 5.6'da verilmiştir.

Çizelge 5.5. IxChariot yazılım konfigurasyonları -1

Console version	7.10 SP2
Console build level	118
Console product type	IxChariot
Filename	C:\Documents and Settings\Administrator\Desktop\M1 – M7 – unicast – fd – 4mbps.tst
Run start time	20/01/2012, 4.31.16
Run end time	20/01/2012, 4.33.59
Elapsed time	00:02:43
How the test ended	Ran to completion
Number of pairs	4

Çizelge 5.6. IxChariot yazılım konfigurasyonları-2

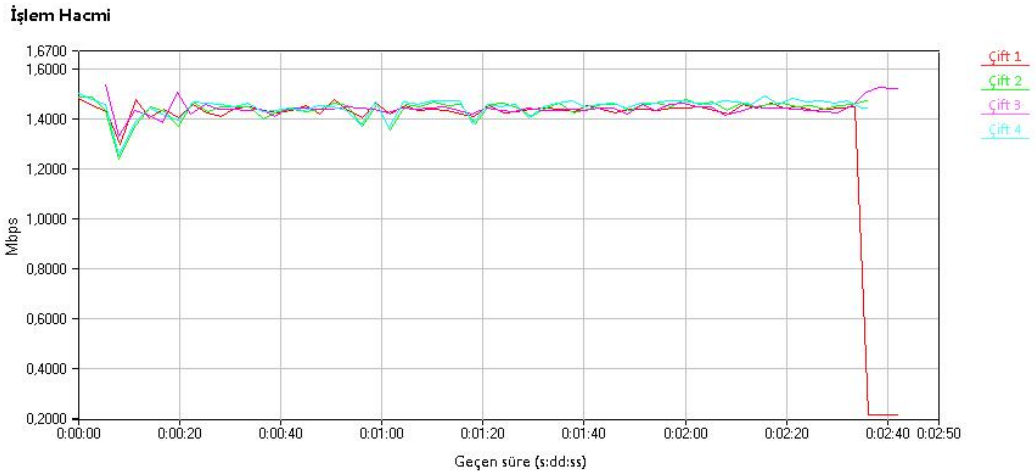
End type	Run until all pairs end
Reporting type	Batch
Automatically poll endpoints	No
Stop run upon initialization failure	Yes
Connect timeout during test (minutes)	0
Stop test after this many running pairs fail	1
Collect endpoint CPU utilization	No
Collect TCP statistics	No
Allow pair reinitialization for setup	No
Maximum number of setup reinitializations	3
Setup reinitialization wait interval (milliseconds)	10
Allow pair reinitialization at runtime	No
Maximum number of runtime reinitializations	3
Runtime reinitialization wait interval (milliseconds)	10
Validate data upon receipt	No
Use a new seed for random variables on every run	No
Datagram window size (bytes)	1500
Datagram retransmission timeout (milliseconds)	200
Datagram number of retransmits before aborting	50
Receive Timeout (milliseconds)	10000
Time To Live (Hops)	32
Low sender jitter	Yes
Limit data rate	No
Use RTP extended beaders	No
Enable Ixia hardware timestamps	No
Clock synchronization	Endpoint synchronization

5.4.3. İşlem hacmi (Throughput) sonuçları

Şekil 5.4'de M1-M7 merkezleri arasında 4 adet çift oluşturulmuştur ve her çift için ayrı ayrı işlem hacmindeki değişimler grafiksel olarak gösterilmiştir, ayrıca bu değerler, Çizelge 5.7'de de gösterilmişlerdir. Daha önce belirttiğimiz üzere "throughput" bir noktadan diğer bir noktaya ortam üzerinden sorunsuz iletilen verilerin oranını verir. 156 ms bir işlem süresi göz önüne alındığında ortalama işlem hacim değeri yaklaşık olarak 1.4 mbps'dir. İşlem hacim kapasitesinin bilinmesi, kullanılacak olan bant genişliği için bilgi vermektedir.

Çizelge 5.7. Karasal ağ için throughput test sonuçları

Grup/Çift	Ortalama Average (mbps)	Min (mbps)	Max (mbps)	İşlem Hacmi 95% Confidence Interval	Hesaplanan Süre Measured Time (saniye-secs)
Bütün Çiftler	5,562	0,215	1,534		
Çift 1	1,391	0,215	1,481	0,054	161,948
Çift 2	1,438	1,238	1,487	0,044	156,215
Çift 3	1,441	1,332	1,534	0,032	156,632
Çift 4	1,447	1,253	1,500	0,027	156,232
Toplam:	5,562	0,215	1,534		



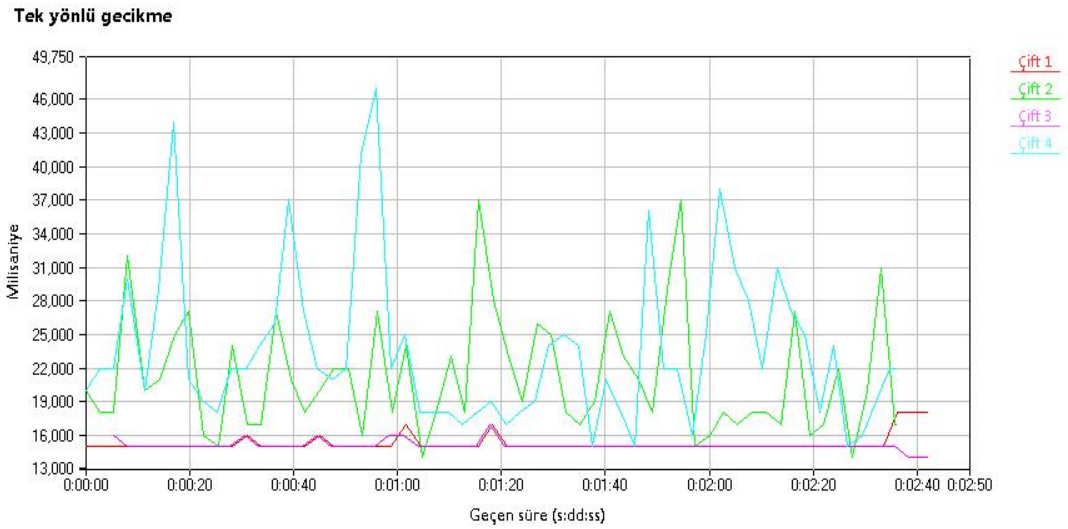
Şekil 5.4. Karasal ağ için throughput test sonuçları

5.4.4. Gecikme (Latency) sonuçları

Şekil 5.5'de M1-M7 merkezleri arasında 4 adet çift oluşturulmuştur ve her çift için ayrı ayrı tek yönlü gecikme parametresindeki değişimler grafiksel olarak gösterilmiştir, ayrıca bu değerler Çizelge 5.8'de de gösterilmişlerdir. Daha önce belirttiğimiz üzere "latency" (gecikme) paketlerin karşı tarafa ulaşması esnasında geçen zaman değeridir. Hat sağlayıcımızın satın almış olduğumuz pakete göre bize garanti ettiği gecikme değer 60 ms'dir. Yaptığımız test ile bu değerin sağlanıp sağlanmadığı bulunmaya çalışılmıştır. Bütün çiftlerin gecikme değerlerine baktığımızda ortalama olarak yaklaşık 20 ms gibi bir zamandan bahsedebiliriz ki bu değer de bizim için uygulamamızda problem olmayacak bir gecikme değeridir.

Çizelge 5.8. Karasal Ağ QoS testi gecikme parametresi sonuçları

Grup/Çift	Tek-Yönlü Gecikme Ortalama (ms)	Tek-Yönlü Gecikme Minimum (ms)	Tek-Yönlü Gecikme Maksimum (ms)	Tahmini Saat Hatası (ms)	Maksiimum Saat Hatası (ms)	Saat Sinyali (Clock)
Bütün Çiftler	19	14	47	5,267	18,481	
Çift 1	15	15	18	1,277	15,201	Uç nokta senkronizasyonu
Çift 2	21	14	37	10,563	18,481	Uç nokta senkronizasyonu
Çift 3	15	14	17	1,431	15,072	Uç nokta senkronizasyonu
Çift 4	24	15	47	7,797	16,896	Uç nokta senkronizasyonu
Toplam:	19	14	47	5,267	18,481	



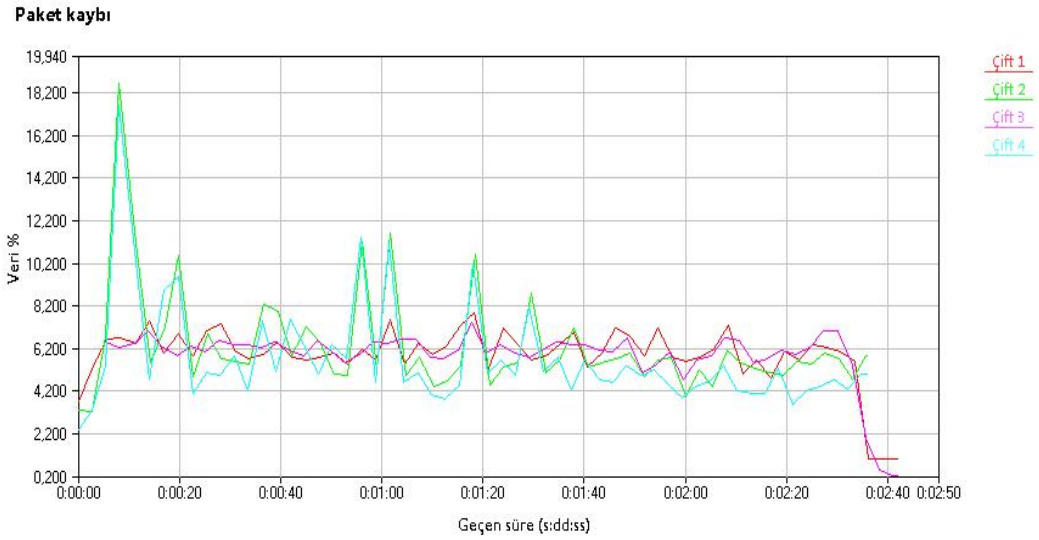
Şekil 5.5. Karasal ağ gecikme parametresi grafiksel olarak sonuçlar

5.4.5. Paket kaybı (Packet loss) sonuçları

Şekil 5.6'da M1-M7 merkezleri arasında 4 adet çift oluşturulmuştur ve her çift için uçtan uca olan iletişim esnasında kaybolan paket kayıp değerlerindeki değişimler grafiksel olarak gösterilmiştir, ayrıca bu değerler Çizelge 5.9'da da gösterilmişlerdir. Daha önce belirttiğimiz üzere, "Packet Loss" (paket kaybı) veri iletim esnasında bazı paketlerin hedefe ulaşamamasını ifade eder. Karasal link sağlayıcımızdan satın almış olduğumuz platinium tarifesine göre, paket kayıp değeri aylık olarak maksimum %0,3 oranı sınırında olmalıdır. Tabloladan görüleceği üzere kayıp olan veri %6'nın üzerindedir ve bu özellikle ses trafiği için kesinlikle kabul edilebilir bir değer değildir.

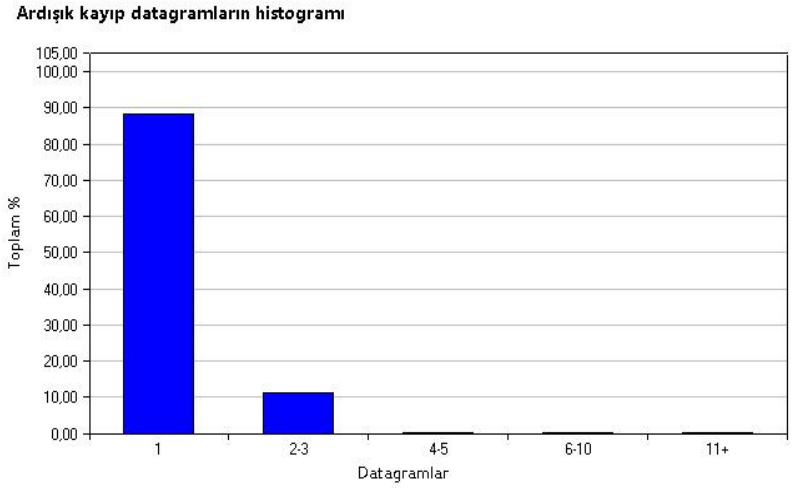
Çizelge 5.9. Karasal ağ QoS testi paket kaybı parametresi sonuçları

Grup/ Çift	Gönderilan (E1)	Alınan Bytes (E2) (Streaming)	(Byte) E1'den E2'e kayıp	(%) E1'den E2'e kayıp	E1 İşlem Hacmi (mbps)	Maksimum Ardışık Kayıp Datagramlar	Geçen Süre (saniye-secs)
Bütün Çiftler	120.000.000	112.715.450	7.284.550	6,070		250	
Çift 1	30.000.000	28.158.700	1.841.300	6,138	1,482	22	161,948
Çift 2	30.000.000	28.084.450	1.915.550	6,385	1,536	236	156,215
Çift 3	30.000.000	28.208.300	1.791.700	5,972	1,532	30	156,632
Çift 4	30.000.000	28.264.000	1.736.000	5,787	1,536	250	156,232
Tplm:	112.715.450	112.715.450	7.284.550	6,070		250	

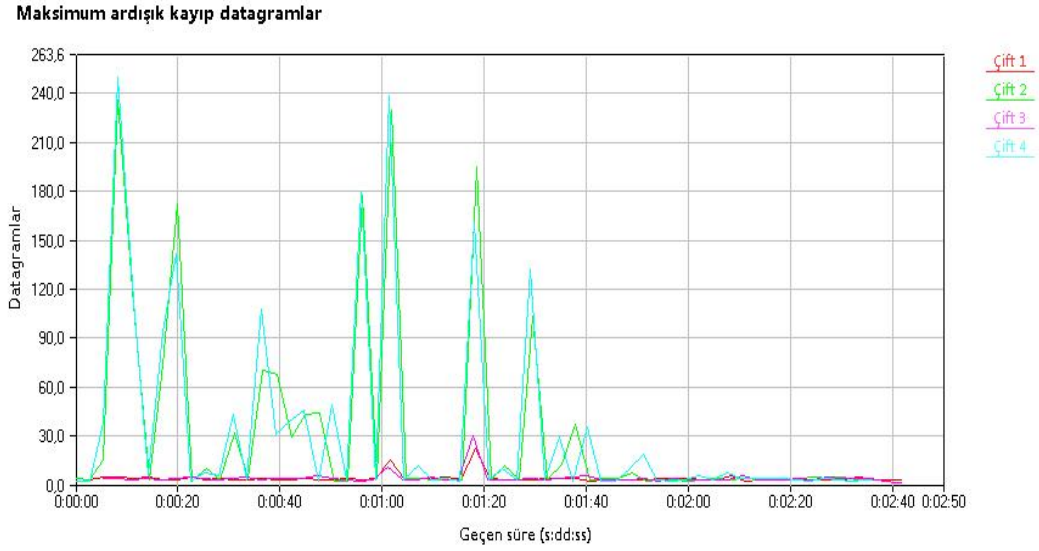


Şekil 5.6. Karasal ağ QoS testinde paket kayıp oranı-zaman grafiği

Şekil 5.7 histogramında, "Consecutive Lost datagrams" ard arda kaybolan data paketlerini işaret etmektedir. Düşük oranlardaki paket kayıpları bazen kabul edilebilirdir ve paket kayıpların ard arda gelen paketler olup olmaması hususu karşı taraftaki açılım için, yani iletişimin sağlıklı tamamlanabilmesi için gayet önemlidir. Yukarıdaki histogramda paketlerin %85 gibi bir oranının *consecutive* olmadığını yani kayıpların tek paket olduğunu görmekteyiz. Şekil 5.8'de ise bu 4 çift oluşturulmuş ve consecutive olma durumuna göre zaman-datagram grafiği gösterilmiştir.



Şekil 5.7. Karasal ağ QoS testinde ardışık kayıp datagram histogramı



Şekil 5.8. Karasal ağ QoS testinde ardarda paket kayıp oran-zaman grafiği

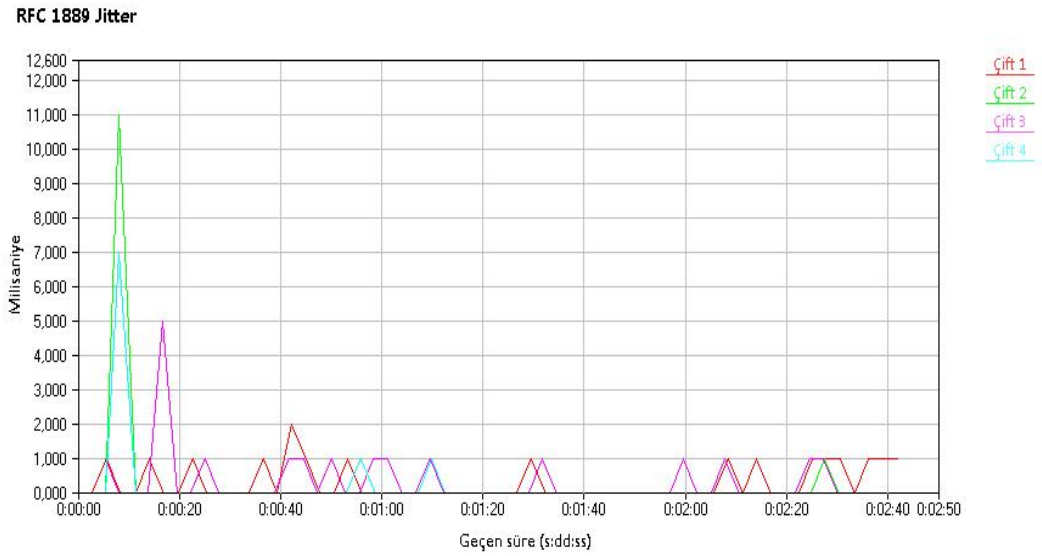
5.4.6. Jitter (Gecikmenin değişimi) sonuçları

Şekil 5.9'da M1-M7 merkezleri arasında 4 adet çift oluşturulmuştur ve her çift için uçtan uca olan iletişim esnasında jitter değerlerindeki değişimler, grafiksel olarak gösterilmiştir, ayrıca bu değerler Çizelge 5.10'da da mevcuttur. Daha önce belirttiğimiz üzere "Jitter" paketlerin gecikme sürelerindeki varyasyondur (farklılık). Jitter değeri özellikle ses uygulamaları için çok daha küçük olmalıdır. Karasal link

sağlayıcımızdan satın almış olduğumuz *platinium* tarifesine göre, jitter değeri aylık olarak maximum 5 ms sınırında olmalıdır. Tabloladan görüleceği üzere jitter değeri çok küçüktür yani *1ms'nin* bile altında bir değer çıkmıştır ve değer bizim kurmak istediğimiz WAN için gayet uygun bir QoS parametre değeridir.

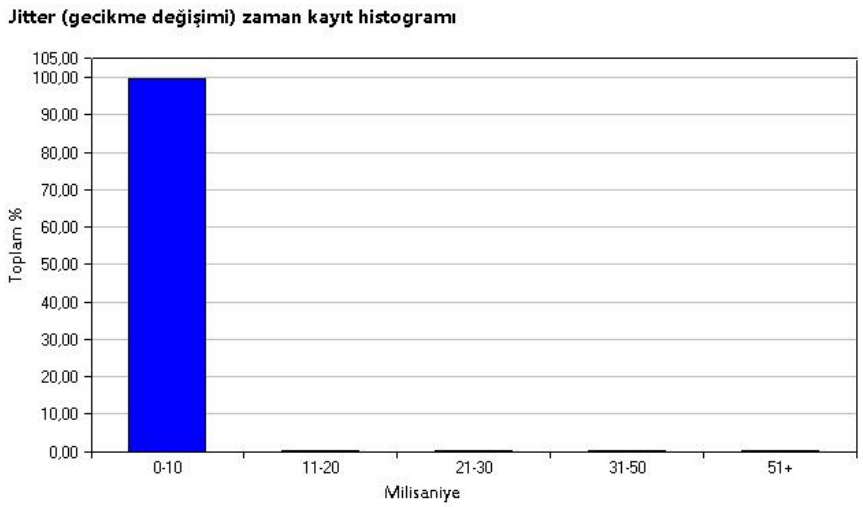
Çizelge 5.10. Karasal ağ QoS testi jitter parametresi sonuçları

Grup/ Çift	RFC 1889 Jitter Ortalama (ms)	RFC 1889 Jitter Minimum (ms)	RFC 1889 Jitter Maksimum (ms)	Jitter (gecikme değişikliği) Max. (ms)
Bütün Çiftler	0,237	0	11	225
Çift 1	0,263	0	2	219
Çift 2	0,211	0	11	215
Çift 3	0,316	0	5	225
Çift 4	0,158	0	7	214
Toplam:	0,237	0	11	225

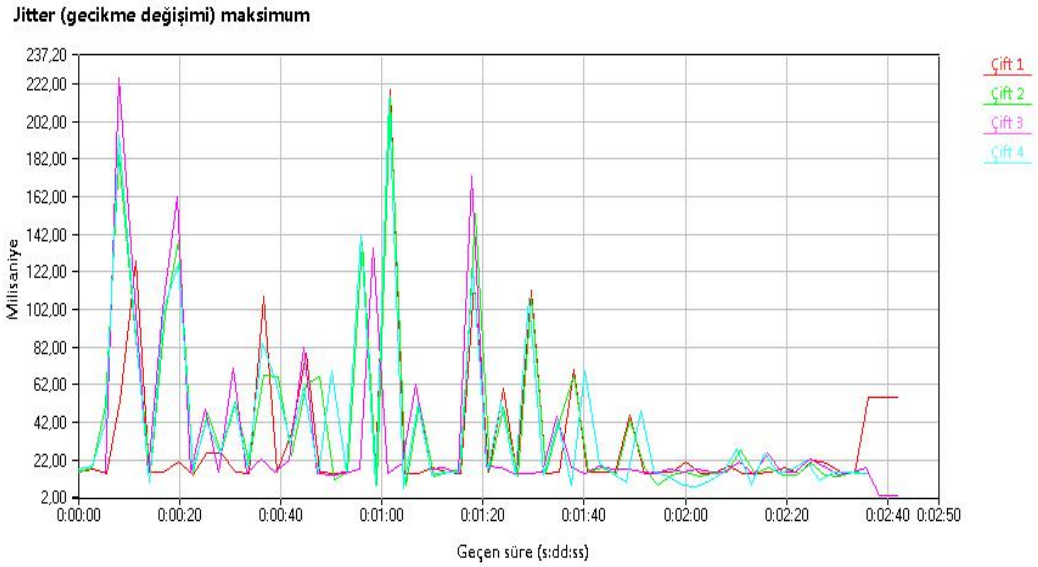


Şekil 5.9. Karasal ağ QoS testinde ardarda jitter -zaman grafiği

Şekil 5.10 histogramında, toplam da bütün paketlerin oranıyla jitter zaman değerleri gösterilmiştir. Paketlerin %100'ündeki jitter değeri 0-10 ms arasındadır. Şekil 5.11'de ise 4 çift oluşturulmuş ve bütün çiftlerin zamanla jitter değerlerindeki değişimler farklı renklerde gösterilmiştir.



Şekil 5.10. Karasal ağ QoS testinde ardarda jitter değişim oranı-zaman grafiği



Şekil 5.11. Karasal ağ QoS testinde ardarda maksimum jitter değişimi -zaman grafiği

5.4.7. Sonuç

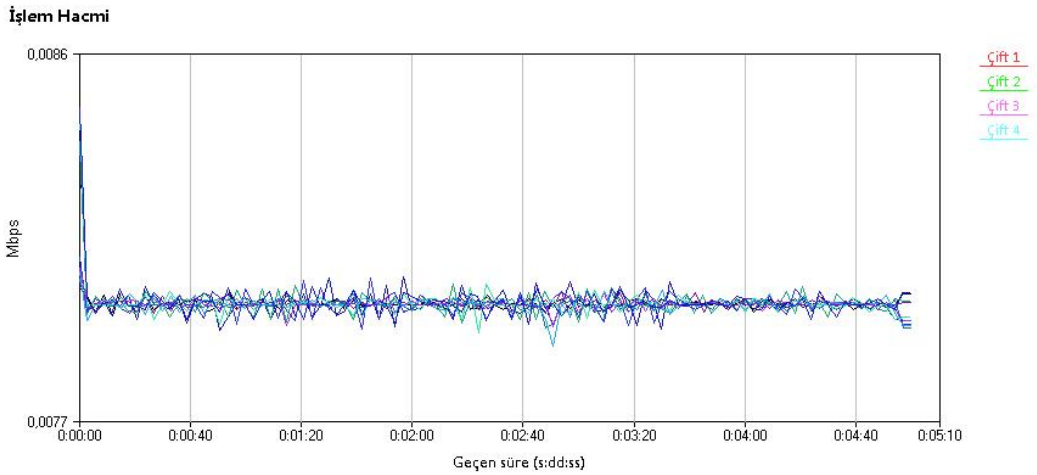
Yaptığımız bu QoS testi için genel bir sonuç çıkartmak gerekirse, jitter, latency gibi hız ile ilgili parametrelerde sorun bulunmamakta, fakat ciddi oranda bir paket kaybı bulunmaktadır, dolayısıyla servis edilen bu link kabul edilebilir değildir ve paket kaybına neden olan etkenlerin bulunup düzeltilmesi gerekmektedir.

5.5. Bir Uydu Linki için QoS Testi

Uydu linki için yapmış olduğumuz testlerde bir merkez ve radyo/radar istasyonu arasındaki VoIP (voice over IP) akışını seçtik. Dolayısıyla M1-RD5 lokasyonları arasındaki linke ait test sonuçları aşağıda gösterilmiştir.

5.5.1. İşlem Hacmi (Throughput)

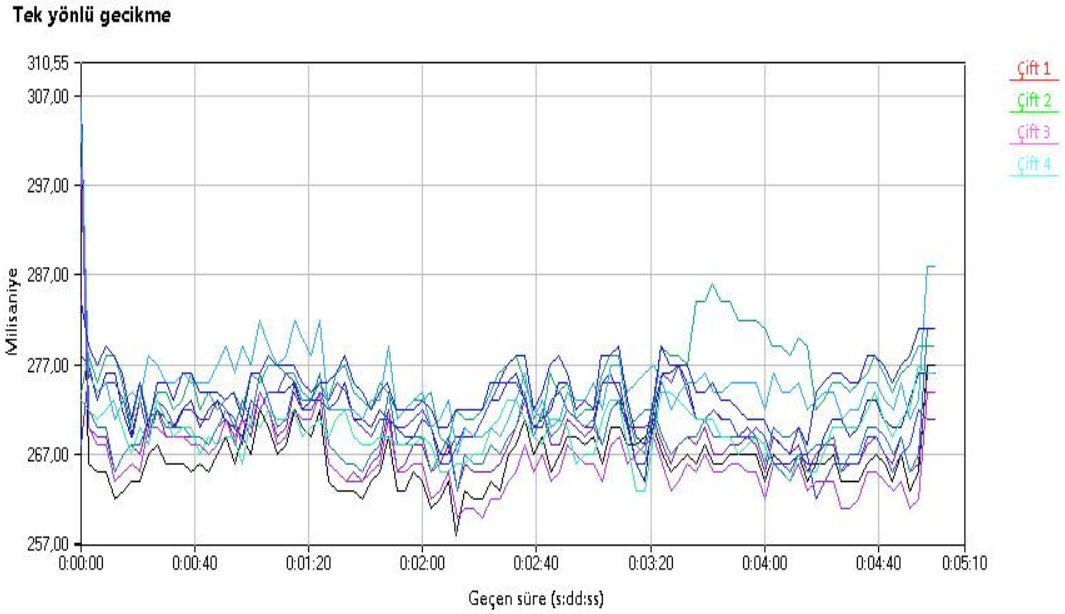
Şekil 5.12'de, M-1 merkezi ve RD-5 uzak lokasyonu arasında 10 adet çift oluşturulmuş ve her çift ayrı renklerde belirtilerek, hepsi için ayrı ayrı işlem hacmindeki değişimler grafiksel olarak gösterilmiştir. Daha fazla sonuç gözlemleyebilmek için karasal linkteki teste oranla daha çok çift oluşturulmuştur. Grafikte de görüldüğü üzere VoIP'in yer tuttuğu bant genişliği çok azdır. Yaklaşık 5 dk. devam eden bu testte ortalama işlem hacmi 0,020 Mbps civarlarındadır.



Şekil 5.12. Uydu ağı QoS testinde throughput-zaman grafiği

5.5.2. Gecikme (Latency) sonuçları

Şekil 5.13'de M-1 merkezi ve RD-5 uzak lokasyonu arasında 10 adet çift oluşturulmuş ve her çift ayrı renklerde belirtilerek, hepsi için ayrı ayrı gecikme (latency) değişimindeki değerler grafiksel olarak gösterilmiştir. Daha fazla sonuç gözlemleyebilmek için karasal linkteki teste oranla daha çok çift oluşturulmuştur. Grafikte de görüldüğü üzere, bütün çler düşünüldüğünde, ortalama gecikme yaklaşık olarak 270 ms civarlarındadır. Uydu hat sağlayıcımızdan, satın almış olduğumuz pakete göre bize garanti ettiği maksimum gecikme değeri 400 ms'den küçük olmalıdır. Karasal iletişimdeki teknolojilere göre uydu iletişiminin çok yavaş olmasından dolayı gecikme miktarlarında büyük fark görülmektedir. Sonuç olarak, uydu hat sağlayıcımızın bize örgülü (*mesh)* topolojiye göre sağlamış olduğu hattaki gecikme değeri kabul edilebilir bir değerdir.



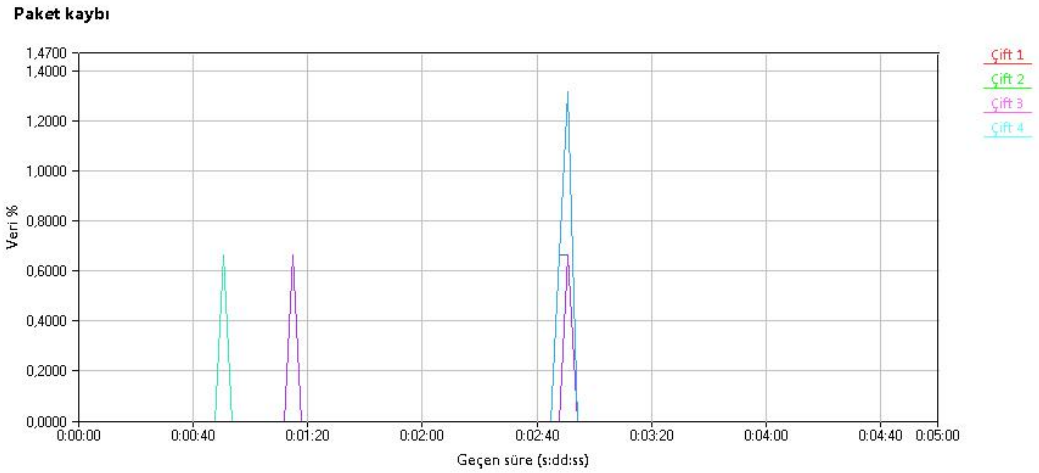
Şekil 5.13. Uydu ağı QoS testinde gecikme-zaman grafiği

5.5.3. Paket Kaybı

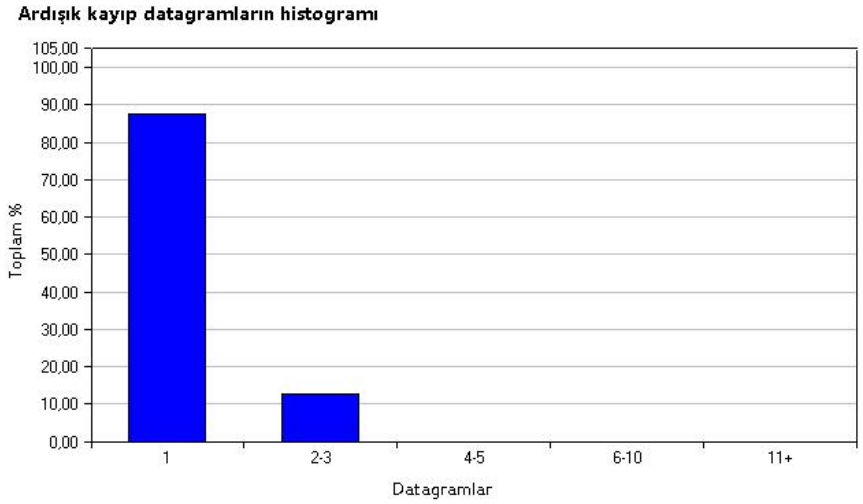
Şekil 5.14'te M-1 merkezi ve RD-5 uzak lokasyonu arasında 10 adet pair oluşturulmuş ve her çift ayrı renklerde belirtilerek, hepsi için ayrı olmak üzere *packet loss* (paket kaybı) değişimindeki değerleri grafiksel olarak gösterilmiştir ve ayrıca Çizelge 5.11'de de bu değerler mevcuttur. Daha fazla sonuç gözlemleyebilmek için karasal linkteki teste oranla daha çok çift oluşturulmuştur. Grafikte de görüldüğü üzere bütün çiftler düşünüldüğünde, ortalama paket kaybı yaklaşık olarak % 0,07 gibi bir değerdir. Daha önce de belirttiğimiz üzere ses ağlarında (VoIP) paket kaybı oranının çok düşük olması gerekmektedir. Sonuç olarak elde ettiğimiz paket kayıp değeri VoIP iletişimi için kabul edilebilir bir değerdir.

Çizelge 5.11. Uydu ağı QoS testinde paket kaybı parametresi sonuçları

Grup/ Çift	Gönderilen Bytes (E1)	Alınan Bytes (E2)	Kayıp Bytes (from E1 to E2)	(%) Kayıp Bytes (E1'den E2'ye)	E1 İşlem Hacmi (mbps)	Maksimum Ardıkış Kayıp Datagramlar	Geçen Süre(secs)
VOIP1	600.000	599.980	20	0,003		1	
Çift 1	300.000	300.000	0	0,000	0,008	0	299,931
Çift 2	300.000	299.980	20	0,007	0,008	1	299,854
VOIP2	600.000	600.000	0	0,000		0	
Çift 3	300.000	300.000	0	0,000	0,008	0	299,923
Çift 4	300.000	300.000	0	0,000	0,008	0	299,817
VOIP3	600.000	599.960	40	0,007		1	
Çift 5	300.000	299.960	40	0,013	0,008	1	299,956
Çift 6	300.000	300.000	0	0,000	0,008	0	299,936
VOIP4	600.000	599.940	60	0,010		1	
Çift 7	300.000	299.960	40	0,013	0,008	1	299,945
Çift 8	300.000	299.980	20	0,007	0,008	1	299,828
VOIP5	600.000	599.940	60	0,010		2	
Çift 9	300.000	299.940	60	0,020	0,008	2	299,953
Çift 10	300.000	300.000	0	0,000	0,008	0	299,774



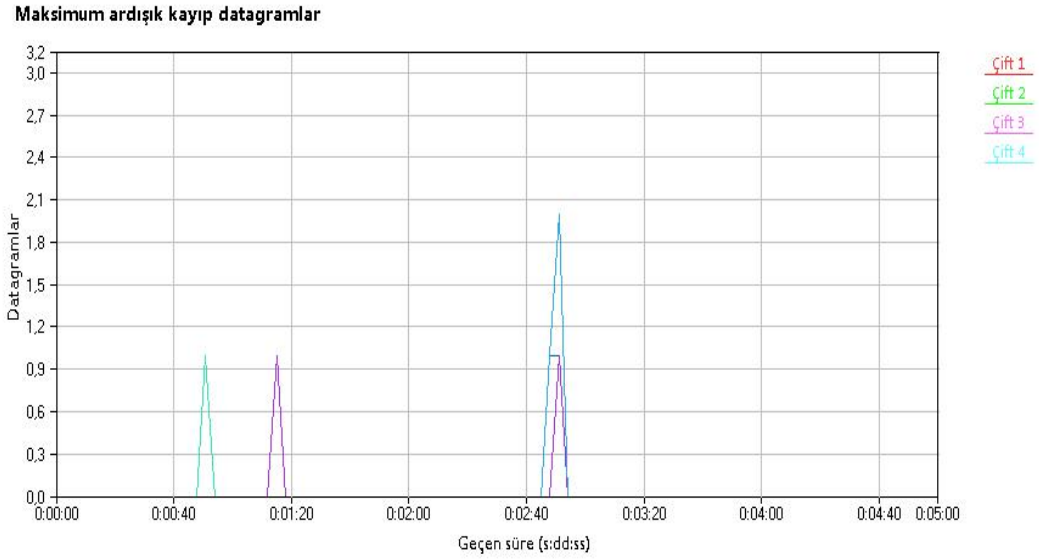
Şekil 5.14. Uydu ağı QoS testinde paket kayıp oranı-zaman grafiği



Şekil 5.15. Uydu ağı QoS testinde ardarda paket kayıp histogramı

Şekil 5.15 histogramında "Consecutive Lost datagrams" ard arda kaybolan data paketlerini işaret etmektedir. Düşük oranlardaki paket kayıpları bazen kabul edilebilirdir ve paket kayıplarının consecutive yani ard arda gelen paketler olup olmaması hususu karşı taraftaki açılım yani iletişimin sağlıklı tamamlanabilmesi için gayet önemlidir. Yukarıdaki histogramda paketlerin %85 gibi bir oranının consecutive olmadığını yani kayıpların tek paket olduğunu görmekteyiz. Şekil

5.16'da ise 10 çift oluşturulmuş ve consecutive olma durumuna göre zaman-datagram grafiği gösterilmiştir.



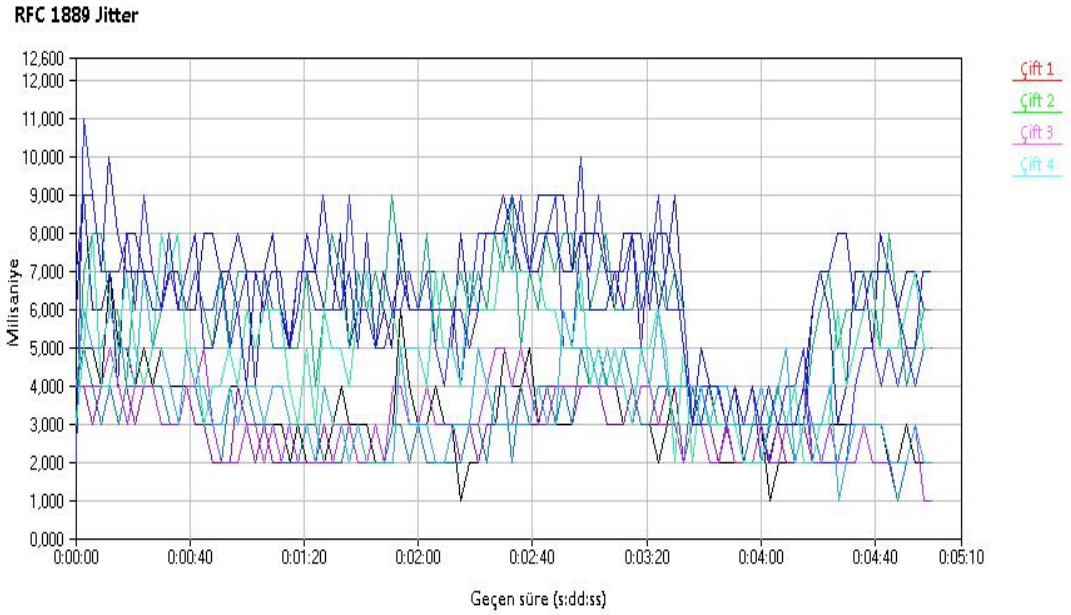
Şekil 5.16. Uydu ağı QoS testinde maksimum ardarda paket kayıp-zaman grafiği

5.5.4. Jitter (Gecikmenin değişimi) sonuçları

Şekil 5.17'de merkezi ve RD-5 uzak lokasyonu arasında 10 adet çift oluşturulmuş ve her çift ayrı renklerde belirtilerek, hepsi için ayrı ayrı jitter değişimindeki değerler gösterilmiştir. Ayrıca Çizelge 5.12'de değerler sayısal olarak verilmiştir. Daha fazla sonuç gözlemleyebilmek için karasal linkteki teste oranla daha çok çift oluşturulmuştur. Grafikte de görüldüğü üzere bütün çiftler düşünüldüğünde, ortalama jitter değeri yaklaşık olarak 4-5 ms arasındaki bir değerdir. Daha önce de belirttiğimiz üzere ses ağlarında (VoIP) jitter değerinin oranının çok düşük olması gerekmektedir. Uydu hat sağlayıcımızın bize sağlamış olduğu mesh topoloji değerlerinde jitter değerinin 50 ms altında olması gerekmektedir. Sonuç olarak, elde ettiğimiz jitter değerlerinin ortalaması istediğimiz aralıktadır.

Çizelge 5.12. Uydu ağı QoS testinde Jitter parametresi sonuçları

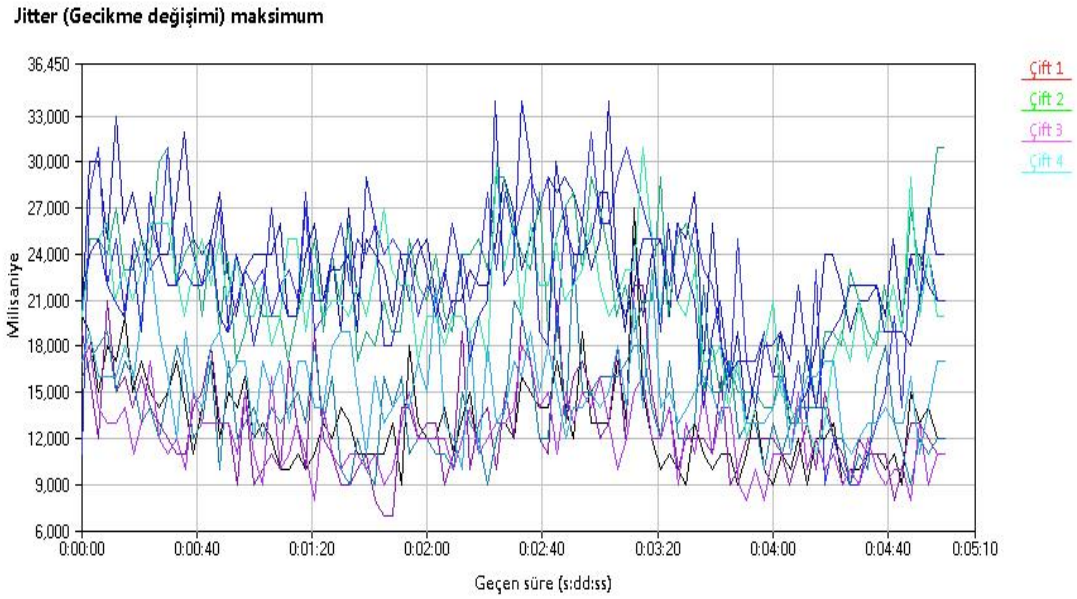
Grup/ Çift	RFC 1889 Jitter Ortalama (ms)	RFC 1889 Jitter Minimum (ms)	RFC 1889 Jitter Maksimum (ms)	Jitter (gecikme değişimi) Max. (ms)
VOIP1	4,720	1	9	34
Çift 1	3,190	1	7	27
Çift 2	6,250	2	9	34
VOIP2	4,350	1	9	31
Çift 3	2,770	1	4	22
Çift 4	5,930	2	9	31
VOIP3	4,445	1	11	32
Çift 5	3,060	1	5	24
Çift 6	5,830	2	11	32
VOIP4	3,965	1	8	31
Çift 7	3,050	1	5	18
Çift 8	4,880	2	8	31
VOIP5	4,970	1	10	34
Çift 9	3,600	1	7	24
Çift 10	6,340	3	10	34
	4,490	1	11	34



Şekil 5.17. Uydu ağı QoS testinde Jitter parametresi-zaman grafiği

Şekil 5.18 histogramında, toplamda bütün paketlerin oranıyla jitter zaman değerleri gösterilmiştir. Paketlerin %100'ündeki jitter değeri 0-10 ms arasındadır. Şekil 5.19'de ise 4 çift oluşturulmuş ve bütün çiftlerin zamanla jitter değerlerindeki değişimler farklı renklerde gösterilmiştir.

Şekil 5.18. Uydu ağı QoS testinde jitter oranı histogramı



Şekil 5.19. Uydu ağı QoS testinde maximum jitter-zaman grafiği

5.5.5. MoS (mean opinion score) değerleri

Ses paket kalitelerini incelemede MoS değeri bazı QoS parametrelerini alır ve ortalama ve kalite için ortalama bir değer sonucuna ulaşır. Aslına bakılırsa, MOS subjektif olarak geliştirilen bir metod'tur. İstatistiksel anlamda önemli sayılabilecek

50-70 kişinin akustik bir oda içerisinde ses örneklerini 0 ile 5 arasında puanlamasıyla oluşmaktadır ve böylece sesin istenen kalitede olup olmadığına karar verilir (Bkz. Çizelge 5.13). Verilen puanların ortalaması eğer 3.5 ve üzeriyse sesin kabul edilebilir düzeyde iyi olduğu anlaşılır. MOS puanları son kullanıcıların düşüncesiyle yakından alakalıdır.

Çizelge 5.13. MoS değerleri

MOS Ölçüsü		
	5	Çok iyi
	4	İyi
	3	ORTA
	2	ZAYIF
	1	KÖTÜ

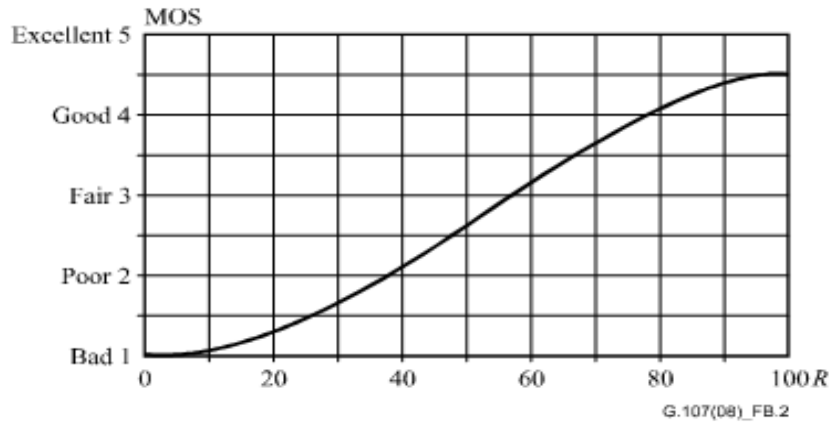
E-Model ise ağ kalitesinin objektif bir şekilde değerlendirilmesi için geliştirilen ve ITU-T G.107 standardında yer alan bir değerlendirme metodudur. E-Model MoS puanlarının, R puanlarına bağlı olarak objektif bir şekilde hesaplanmasını sağlamaktadır. Bilindiği üzere, her ses örneğinin 50-70 kişiye uygun ortamda dinletilip bir MOS puanının elde edilmesi çok zor bir hadisedir. Ancak, R puanı aşağıdaki fomül ile hesaplanabilmektedir:

$$R = R_0 - I_s - I_d - I_e + A \ .$$

Burada R_0 SNR (Signal to Noise Ratio)'u, I_s ses sinyalindeki ani yükseliş alçalışlar ve kuantulama gürültüsünü, I_d gecikmeyi, I_e ise BER (Bit Error Rate) ve paket kaybını göstermektedir. A ise kullanıcı beklentisini gösteren avantaj puanıdır. Bu puan diğer olumsuzluklara eklenmektedir. ITU-T G.107 standardı MOS puanları ile R puanları arasında bağlantı kurmaktadır. Bu standartda belirtildiği şekilde MOS puanları, R puanlarından aşağıdaki formül ile elde edilmektedir [37].

$$MOS = \begin{cases} 1 & R < 0 \\ 1 + 0.035R + (R-60)(100-R)\,7R/10^6 & 0 \le R \le 100 \\ 4.5 & R > 100 \end{cases} .$$

MOS ile R puanları arasındaki ilişki aşağıda grafiksel olarak gösterilmiştir (Bkz. Şekil 5.20).



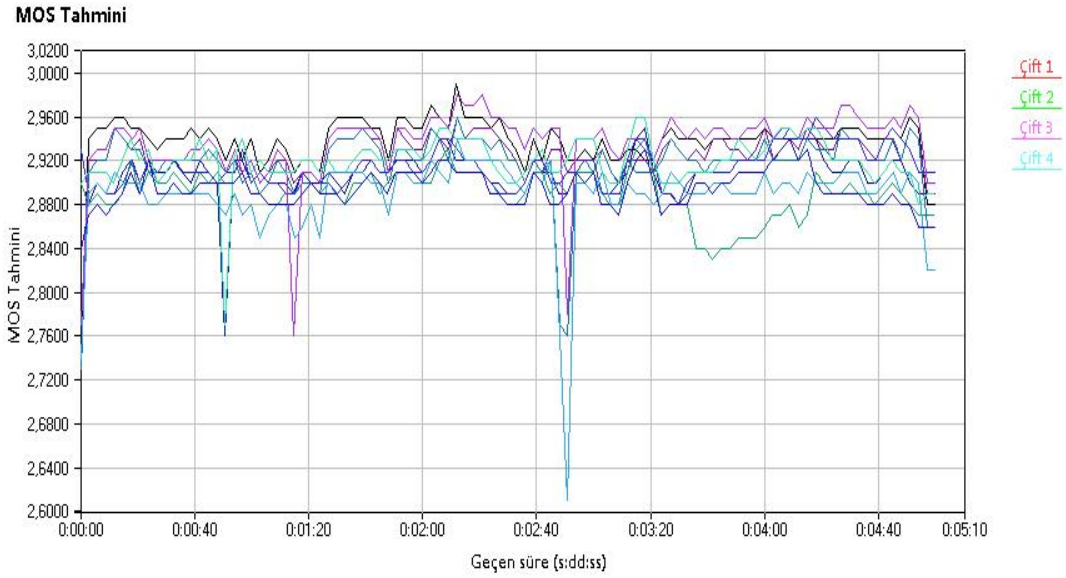
Şekil 5.20. MoS-R puanları grafiği.

5.5.6. MoS Değerleri

Çizelge 5.14'te ve Şekil 5.21'de M1-RD5 lokasyonları arası yapmış olduğumuz testlerdeki MoS değerleri mevcuttur. Görüldüğü üzere, ortalama MoS değeri 2,91 civarlarındadır ve bu değer *ITU-T G.107* standartlarına göre ortaya yakın zayıf kalite olarak adlandırılabilir. Uydu üzerinde olan ses kalitesi ile karasal ağ üzerindeki ses kalitesi arasında ciddi fark bulunmaktadır.

Çizelge 5.14. Uydu ağı QoS testinde MoS değerlendirmesi

Grup Çift	MOS Ort.	MOS Min.	MOS Max.	R-Değeri Ort.	End-to-End Delay Ort. (ms)	Tek Yönlü Gecikme Ort (ms)	Jitter Ort.	Kayıp (%)	Max. Ardışık Kayıp Datagramlar
VOIP1	2,93	2,75	2,99	56,63	344	269	4,720	0,003	1
Çift 1	2,94	2,75	2,99	56,91	341,540	267	3,190	0,000	0
Çift 2	2,91	2,76	2,95	56,35	346,500	272	6,250	0,007	1
VOIP2	2,91	2,73	2,96	56,33	347	272	4,350	0,000	0
Çift 3	2,93	2,73	2,96	56,67	343,760	269	2,770	0,000	0
Çift 4	2,89	2,83	2,94	55,99	350,290	275	5,930	0,000	0
VOIP3	2,92	2,73	2,96	56,49	345	270	4,445	0,007	1
Çift 5	2,92	2,73	2,96	56,51	344,760	270	3,060	0,013	1
Çift 6	2,91	2,88	2,96	56,46	345,780	271	5,830	0,000	0
VOIP4	2,93	2,76	2,98	56,72	343	268	3,965	0,010	1
Çift 7	2,94	2,76	2,98	56,87	341,360	266	3,050	0,013	1
Çift 8	2,92	2,77	2,96	56,56	344,500	270	4,880	0,007	1
VOIP5	2,89	2,61	2,94	56,02	350	275	4,970	0,010	2
Çift 9	2,89	2,61	2,94	55,98	349,580	275	3,600	0,020	2
Çift 10	2,89	2,84	2,94	56,06	349,540	275	6,340	0,000	0
Toplam :	2,91	2,61	2,99	56,44	346	271	4,490	0,006	2



Şekil 5.21. Uydu ağı QoS testinde MoS-zaman grafiği

5.5.7. Sonuçlar

Yapılan bu QoS testleri sonucunda, uydu ağ'ındaki ağ hızının genelde düşük olduğu bilinerek, jitter, latency ve paket kaybı gibi parametrelerin uydu ağ sağlayıcısından alınan hizmet kalite sınırları dahilinde olduğu görülmüştür. MoS değerlerine göre her ne kadar ses kalitesi zayıf olarak ölçüldüyse de operasyonel olarak çalışmanın sürdürülebilirliği açısından VoIP kalitesi yeterlidir.

5.6. Hizmet Sınıflandırması (CoS- Class of Service)

CoS, benzer türdeki trafiklerin gruplandırılması ve bu gruplandırma içindeki her sınıfa verilen hizmet önceliğini yönetmek için kullanılan bir önceliklendirme trafik yönetim methodudur. CoS, QoS'un aksine, hizmet seviyesindeki parametreleri teslim süresi açısından garanti etmez, sadece *best effort* dediğimiz yöntemi kullanır.

Öte yandan, CoS teknolojisi, bir ağdaki trafik hacmi ne kadar büyürse büyüsün, daha kolay yönetilebilir ve ölçeklendirilebilirdir. CoS teknolojisi daha genel bir şekilde önceliklendirme olarak düşünebilir, QoS ise CoS'a göre daha ayrıntılı önceliklendirme yapmaktadır.
Kullanılan 3 temel CoS teknolojisi bulunmaktadır:

i. *802.1p Layer 2 Tagging*
ii. *Type of Service (ToS)*
iii. *Differentiated Services (DiffServ)*

IEEE 802.1p ikinci katmanda etiketleme ile her paket için 3'bitlik ayrı bir ön etiket (header) kullanılır ve bu ön etiketlerde önceliklendirme derece bilgisi verilir. Biz uygulamamızda bu tür CoS teknolojisinden, faydalandık. Bu 3'bitlik önceliklendirme bilgisinin yeterli olmadığı ağlarda yeni geliştirilmiş bir protokol olan *differentiated services (DS ya da DiffServ),* IETF (Internet Engineering Task Force) çalışma grubu tarafından kullanımı biraz daha karmaşık olan bir CoS teknolojisi geliştirilmektedir. Bu teknolojide, gelen paketlerin nasıl yönlendirilmeleri gerektiği PHB (Per Hop

Bevavior) kullanılarak yapılmaktadır. PHB ile kuyruklama, bant genişliği, drop edilmesi gereken paketler gibi daha detaylı işlemler yapılabilmektedir.

3 bitlik CoS header'ı 0 ile 7 arasında önem derecesine göre değişmektedir. CS7 en yüksek önem derecesini taşırken, CS0 en düşük önem derecesinde veri demektir (Bkz Çizelge 5.15).

Çizelge 5.15. CoS değerleri

Ağ Önceliği	Kısaltma	Trafik Karakteristikleri
0 (lowest)	BK	Background
1	BE	Best Effort
2	EE	Excellent Effort
3	CA	Critical Applications
4	VI	Video, < 100 ms latency
5	VO	Voice, < 10 ms latency
6	IC	Internetwork Control
7 (highest)	NC	Network Control

Kurmuş olduğumuz ağ'daki IP akış trafiği aşağıda belirtilen özellik ve kurallara göre sağlanmaktadır :

- *VoIP ses sinyallerinin akışı, kullanılan network protokolleri (OSPF, PIM, IGMP) ve network trafiği gerçek zamanlı veri trafiği olarak adlandırılmaktadır (Cos değeri : 4).*
- *Merkezler ve uzak istasyonlar arası radar data akışı, kritik veri trafiği olarak adlandırılmaktadır ve Cos değeri 2 olarak atanmıştır.*
- *Bütün diğer IP trafikleri (TCP ip yönetimi vb.) default olarak standard veri olarak kabul edilmiştir ve CoS değerleri 0 kabul edilmiştir.*

Aşağıda gösterilen yapılandırmada, CoS haritası oluşturulurken, Real_Time veri için CoS 4 değeri kullanılmış ve kritik veri olarak adlandırdığımız radar verisi için ise CoS 2 kullanılmıştır.

(class-map match-any Real_Time

match access-group 101
match access-group 103
exit

access-list 101 permit udp 10.255.1.0 0.0.0.255 any
access-list 101 permit icmp 10.255.1.0 0.0.0.255 any
access-list 103 permit ospf any any
access-list 103 permit pim any any
access-list 103 permit igmp any any
access-list 103 permit gre any any
access-list 103 permit tcp any any eq telnet

class-map match-any Radar
match access-group 102
match access-group 104
match access-group 105

access-list 102 permit ip 100.1.6.0 0.0.0.255 any
access-list 104 permit ip 100.1.7.0 0.0.0.255 any
access-list 105 permit ip 100.1.8.0 0.0.0.255 any)

(policy-map Cos_mapping
class Real_Time
set cos 4
exit
class Radar
set cos 2
exit
exit)

5.6.1. Trafiği sınıflandırmak için VLAN (Virtual Local Area Network) kullanmak

VLAN'lar ve IP alt ağları kullanmak, kullanıcı gruplarını erişim katmanı ağında bölümlendirmek için en sık kullanılan yöntemdir. İkinci katman anahtarlamanın kullanılmaya başlanmasıyla, uçtan uca çalışma grubu ağları oluşturmak için VLAN'lar kullanılmaya başlanmış; ağlar, binalar arası, hatta altyapının bütünü arasında bağlanabilir hale gelmiştir. Uçtan uca VLAN'lar artık bu şekilde kullanılmamaktadır. Kullanıcıların artan sayısı ve bu kullanıcıların neden olduğu ağ trafiğinin hacmi, desteklenemeyecek kadar büyüktür. Günümüzde VLAN'lar, trafik akışlarını ayırmak ve sınıflandırmanın yanı sıra, tek bir kablolama dolabından ya da binadan yayın trafiğini kontrol etmek için kullanılmaktadır. Her ne kadar bütün ağları kapsayan geniş VLAN'lar artık tavsiye edilmese de, kablosuz dolaşım ve kablosuz IP telefonları gibi özel uygulamaları desteklemek için gerekli olabilirler.

Ağlar, güvenli, tahmin edilebilir, ölçülebilir ve zaman zaman garantili hizmetler sağlamalıdır. Ağlar ayrıca, trafik arttığında tıkanıklığı kontrol edecek mekanizmalara ihtiyaç duyar. Tıkanıklık, ağ kaynaklarına olan talebin, kullanılabilir kapasiteyi aşması durumunda ortaya çıkar. Tüm ağların kaynakları kısıtlıdır. Bu nedenle ağlar, QoS mekanizmalarına ihtiyaç duyar. QoS sağlama yeteneği, trafik sınıflandırmasına ve atanmış önceliğe bağlıdır.

Veriyi kaynaktayken ya da kaynağa yakınken sınıflandırmak, bu veriye ağın bütününde taşınmadan önce uygun önceliğin atanmasını sağlar. Benzer özelliklere sahip trafikleri sınıflara ayırmak ve bu trafiği işaretlemek, erişim ve dağıtım katman'larında bulunan aygıtların işlevleridir. Bu stratejinin bir örneği, erişim anahtarındaki ses trafiğini tek bir VLAN'a yerleştirmektir. Bu aygıt böylelikle ses VLAN'ından gelen trafiği, en yüksek öncelikle işaretler.

Öncelik kuyruklaması, zamana duyarlı, görevi önemli protokoller için kullanışlıdır. PQ (priority *queu*), yüksek, orta, normal ve düşük olmak üzere, her biri farklı bir öncelik seviyesi olarak hizmet veren dört çıktı arayüz kuyruğu kurarak çalışır. Bu

kuyruklar, aşağıdaki özellikler için yapılandırılabilir: Gelen trafik sınıflandırılır, sınıfını belirtecek şekilde işaretlenir ve iletilir.

Trafik, bir öncelik listesinde tanımlanan QoS politikalarına göre çeşitli kuyruklara atanır. Bu politikalar, protokol, bağlantı noktası numarası ya da belirtilen trafik türü için kullanılan diğer kriterlerleri temel alabilir. Farklı trafik türlerini dört sınıf tabanlı kuyruğa ayıran bir dizi filtreyi temsil ederler.

Ağ yöneticisi, QoS özelliklerini yapılandırırken belirli ağ trafiğini seçebilir, bu trafiği göreli önemine göre önceliklendirebilir ve seçimsel işletimini sağlamak için tıkanıklık yönetimi teknikleri kullanabilir. QoS, ağın erişim, dağıtım ve çekirdek katmanları'nda kullanılabilir.

Erişim Katmanı'ndaki 2. katman anahtarlar, QoS'yi IEEE 802.1p hizmet sınıfı'na (CoS) göre destekleyebilir. İkinci katman anahtarın QoS'si, anahtardan ağa çerçeve göndermeyi önceliklendirmek için sınıflandırma ve zamanlama kullanır.

Sınıflandırma, trafiğin gruplandırıldığı işlemdir. Sınıflandırma yapılırken, trafiğin nasıl işaretlenmiş olduğuna ya da protokole bakılır. Trafik, 2. katman hizmet sınıfı, IP önceliği sırası ya da ayrılmış hizmetler kodu noktası'nın (DSCP) değerine göre işaretlenebilir: Biz sınıflandırmada (CoS) 802.1q VLAN etiketinin ilk üç bitini kullandık. Sınıflandırma ve işaretleme, trafiğin birden fazla öncelik seviyesine ya da hizmet sınıfına bölümlendirilmesine olanak verir. Yapılandırmalarımızda kullandığımız VLAN'lara örnek vermek gerekirse aşağıda ikinci katmandaki anahtarlarda yapılan kodlara bakmak uygun olacaktır.

set vlan create 17
set vlan create 101
set vlan create 100
set vlan name 17 Radar
set vlan name 101 Voice
set vlan name 100 Karasal_Erisim

set port vlan fe.1.1-6 101 modify-egress
set port vlan fe.1.7-10 17 modify-egress
set port vlan fe.1.11-14 100 modify-egress
set vlan egress 17,101,100 fe.1.21 tagged
set vlan egress 17,101,100 fe.1.23-24 tagged
set vlan egress 17,101,100 lag.0.1 tagged

Yukarıdaki anahtar yapılandırma örneğinde, farklı trafik türleri için farklı VLAN'lar yaratılmış ve farklı olarak numaralandırılıp ve isimlendirilmişlerdir. Daha sonra bu VLAN'lar anahtardaki farklı portlara etiketli (tagged) ve etiketsiz(untagged) olarak tanımlanmışlardır.

Sonuç olarak tasarlamış olduğumuz WAN'da CoS'un bize sağlamış olduğu ağ trafik yönetim özelliklerinden faydalanmış olduk. Gerçek zamanlı veri (ses-voIP), kritik veri (radar verileri) ve diğer standart veri gibi trafikleri için ikinci katman seviyesinde anahtarlarda farklı VLAN'lar oluşturuldu. İkinci katmandaki anahtarlardan yönlendiricilere geçişte ise ACL (Access List)'ler kullanılarak CoS yolları (mapping) gerçekleştirilmiştir.

6. GENEL SONUÇLAR

Bu çalışmada, önce veri iletişiminin temellerinden bahsedildi ve iletişim akışının olabilmesi için açık sistem bağlantı modeli (OSI-Open Systems Interconnection) üzerinde ayrıntılı duruldu. Ayrıca ağ haberleşmesinde önemi büyük olan bazı protokol ve kavramlar için de bazı temel bilgiler verildi. Ağ haberleşme elamanları tanıtılıp, yönlendiricilerin önemi üzerinde ayrıntılı bir şekilde duruldu. Kullandığımız yönlendiricideki işletim sistemi v.b gibi özelliklerinden bahsedilip, yönlendirici ve anahtarlar için bazı yapılandırma örnekleri verildi. Dinamik ve statik yönlendirme protokolleri kullanımıyla uydu ağı ve karasal ağ arasındaki otomatik geçişlerin nasıl sağlandığı gösterildi. LAN ve WAN tanımlarından kısaca bahsedilerek, ilglili topolojilerden bazı şekiller ile açıklamalarda bulunuldu. Ayrıca WireShark yazılımı kullanarak, alınan/gönderilen bazı veri paketleri üzerinde analizler yapıldı.

WAN teknolojisi için genel tanımlar verilip, WAN teknoloji çeşitlerinden ayrıntılı bahsedildi, WAN teknolojileri kategorize edildi. WAN tasarım ve kurulumunda anahtar olan ve temel rol teşkil eden bazı parametreler olan işlevsellik, erişilebilirlik, ölçeklenebilirlik, performans, basitleştirme ve verilimlilik gibi WAN tasarım kriterleri üzerinde duruldu. Karasal ağ için kullanılan VPLS teknolojisi, geniş bant WAN bağlantı çeşitleri içerisinde anlatıldı.

Örnek olarak kurulan WAN için, bağlantı gereksinimleri temel alınarak, lokasyonlar arası bağlantılar için fiziksel ve mantıksal görünümler ve WAN tasarımında kullanılacak teknolojilerden bahsedildi. Merkezler, uzak lokasyonlar ve uzak lokasyon kuleler arasındaki veri akışının nasıl olduğu detaylarıyla belirtildi. WAN topoloji çizimleriyle, WAN topoloji tasarlama kriterlerinin önemlerinden bahsedildi. Veri akışının sağlanması gereken bütün noktalar için, sınıflandırmalar yapıldı ve bir çok topoloji çizimiyle genel gösterimler ve açıklamalar yapıldı.

Karasal ve uydu ağları için kullanılan, WAN teknolojileri ayrıntılarıyla tanımlandı. Karasal ağ da kullanılan VPLS teknolojisi ve uydu ağı için kullanılan, mesh ve star

topoloji özellikleri anlatıldı. QoS parametre tanımları yapıldı ve karasal ve uydu hat sağlayıcılarımızın garanti ettiği değerler baz alınarak, IxChariot yazılımı kullanılıp QoS testleri yapıldı. Her paremetre için tek tek analiz yapıldıktan sonra test için genel sonuçlar bulundu. Ayrıca CoS tanımından bahsedildi ve tasarlamış olduğumuz WAN'daki verilerin sınıflandırılıp önceliklendirime işlemlerinin yapılabilmesi için gerekli olan işlemler anlatılarak, örnek bir CoS yapılandırması anahtar ve yönlendiriciler üzerinde gösterildi.

Sonuç olarak, tasarımı yapılması gereken WAN, anlatıldığı üzere haberleşmenin amacına, haberleşme noktalarına, bütçeye v.b. bir çok farklı faktörleri ele alarak tasarlanır. Şüphesiz ki, WAN çok geniş bir kavramdır ve günümüzdeki haberleşme teknolojilerinin gelişimine gayet paralel olarak, bu teknolojide kendini yenilenmektedir. Gerçek zamanlı veri, kritik veri, standart veri gibi farklı veri türlerini taşıyan, yedekli bir şekilde çalışan ve operasyonel sürekliliğin çok önemli olduğu radar ağ'ları gibi modern bir WAN tasarlanmak istenildiğin de, hazırlanan bu doküman bir tür rehberlik sağlayabilecektir. Ayrıca hat sağlayıcılar tarafından oluşturulan sanal devreler ya da kiralanan hatların garanti edilen standard'larda olup olmadığını anlamak, ve karşılaşılan bir çok kalite probleminin analizinin yapılıp, sebeplerinin bulunarak, giderilmesi konusunda da yardımcı olacaktır.

KAYNAKLAR

1. Martin, W. Murhammer, Kok-Keong, L., Payam, M.i, Borghi,P., Karl, W., "IP Network Design Guide", ***International Technical Support Organization***, 1-65 (1999).

2. ***Procurve Networking by HP Innovation,*** "WAN Design Guide-The Two Lowest, 9-50, (2005).

3. Chen,B., ***Simon Fraser University***, "Simulation and Analysis of quality of service parameters in IP Networks with Video Traffic", 1-2, (2002).

4. Internetworking Technology Overview, ***Cisco Systems***, "Quality of Service (QoS) Networking", 18-46, (1999).

5. Özçelik, İ., ***Sakarya Üniversitesi***, "Farklı Uygulama ve Kapsama Alanları için Ethernet Teknolojileri", 3, (2010).

6. Ralph Santiro, Metro Ethernet Forum, "Metro Ethernet Services", Internet : http://www.metroethernetforum.org, (2006).

7. ***Megep***, " WAN Kablolama ", 4-20, (2008).

8. Reisoğlu, R., "Kabsoluz Ağlarda Güvenlik" ***Bahçeşehir Üniversitesi Fen Bilimleri Enstitüsü,*** 2-27 (2008).

9. ***Megep***, "Ethernet- 481BB0030 ", 3-22, (2011).

10. Huawei Technologies Co., Ltd., "Technical White Paper for VPLS", 2-15, (2007).

11. OKTUG, S., 2006, BLG433-Bilgisayar haberleşmesi ders notları, ***İstanbul Teknik Üniversitesi,*** http://www3.itu.edu.tr/~oktug/BH/notlar/bolum4.pdf, (Ziyaret Tarihi: Nisan 2012).

12. Hector Cancela, Franco Robledo, Gerardo Rubino, "A Grasp Algorithm for Designing the WAN backbone", ***Universitat dela Republica***, 1-2, (2007).

13. İnternet: ***Alcatel-Lucent***, "Technical Tutorial White Paper", http://www.fplfibernet.com/pdf/VPLSTutorial.pdf, (Ziyaret Tarihi: Mart 2012)

14. İnternet: *AT & T* , "VPLS The Switched Ethernet. "http://www.business.att.com/content/whitepaper/vplsmarch2008.pdf, (2008).

15. Megep, "Ağ Temelleri - 481BB0030 " , 1-30, (2008).

16. HERNANDEZ, L. , Back to basics: LAN technologies, ***Agilent Technologies Network Resources White Paper***, http://literature.agilent.com/litwebpdf/5968-1060E.pdf, (Ziyaret Tarihi: Mayıs 2012).

17. Sa ODOM, W. , *Cisco CCNA 640–647 sınavı sertifikasyon rehberi*, Sistem Yayıncılık, İstanbul, 975–322–301–3, (2003).

18. KAPLAN, Y. , "Veri haberlesmesi temelleri", Papatya Yayınları, İstanbul, 975–6797–15–0 (2000).

19. ***Cisco Network ACADEMY***, "CCNA 1: Networking basics v.3.1.1.″ , http://curriculum.netacad.net [Ziyaret Tarihi: Mart 2011]

20. ÇÖLKESEN, R. , 2001, "Network TCP/IP unix el kitabı", Papatya Yayınları, İstanbul, 975–6797–02–9 (2001).

21. İnternet: "The Internetworking Technologies", http://www.atam.com.tr/genel/kutuphane/CiscoCBT_TR/DATA/ITM/CDROM.HTM, (2011).

22. İnternet : ***Cisco Systems***, "CCNA Discovery- Documentations", http://www.cisco.com/web/learning/netacad/course_catalog/CCNAdiscovery.html, (Ziyaret Tarihi: Mayıs 2011).

23. İnternet : ***Academytech*** , "AcademyTech-CCNA-Turkce_EgitimNotu", http://www.academytech.com/tr/default.aspx, (Ziyaret Tarihi: Haziran 2011).

24. İnternet : CiscoTR " OSPF (Open Shortest Path First)", http://ciscoturk.wordpress.com/2010/12/05/ospf-open-shortest-path-first/ (2010).

25. İnternet : ***Cisco Systems***, "WAN Technologies and Components", http://ptgmedia.pearsoncmg.com/images/1587051486/samplechapter/1587051486content.pdf, (Ziyaret Tarihi: Haziran 2011).

26. Akın B., Nursel Köse, makale, "M P L S (Multi Protocol Label Switching)", ***TTG International***, 3-9, (2009).

27. İnternet ***: ITU/BİDB*** , "Point to Point Protocol (Noktadan Noktaya Protokolü)", http://www.bidb.itu.edu.tr/?d=971", (Ziyaret Tarihi: Ocak 2012).

28. İnternet : TT.A.Ş, " TT VPN Tarifeleri", http://www.ttvpn.com.tr/, (Ziyaret Tarihi: Şubat 2012).

29. ***Megep***, "Optik Kablolama", 4-7(2008) .

30. İnternet : ARGE24 , "VSAT Uydu Teknolojisi" , http://www.arge24.com/index.php?option=com_content&view=article&id=18:vsat&catid=1:products&Itemid=5, (Ziyaret tarihi: Haziran 2012).

31. İnternet : ***Telkolink***, "Optik Haberleşme İlkeleri", http://www.telkolink.com/downloads/optik_haberlesme_ilkeleri.pdf, (2010).

32. İnternet : Mysystem, "SSL", http://mysystem.org/elektronik/ssl.htm, (Ziyaret Tarihi: Haziran 2012).

33. Ixia, "IxChariot User Guide", Release 7.10 913-0949 Rev. A, 2-7, (2009).

34. A. Tanenbaum, "Computer Networks", Dördüncü Basım, Prentice Hall, (2002).

35. Designing Cisco Network Service Architectures, Student Guide, Volume.1, Version 2., (2007).

36. İnternet : Turksat A.Ş, "SLA", http://www.turksat.com.tr (2011).

37. Information about a New Method for Deriving the Transmission Rating Facing R from MoS in Closed Form, ***Telecommunication Standardization SectorTemporary Document XX-E WP 2/12,*** (2002).

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : GÜRTEKİN, Abdullah

Uyruğu : T.C

Medeni hali : Bekar

Telefon : +90 (542) 206 17 31

E-mail : gurtekin1@hotmail.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Lisans	ESOGU/Elektrik-Elektronik Müh.	2007

İş Deneyimi

Yıl	Yer	Görev
2007	Bundeswehr Universitesi-Almanya	Araştırma Görevlisi
2007- devam	SELEX-System Integration S.p.A	Proje Yöneticisi

Yabancı Dil

İngilizce, İtalyanca, Almanca.

Eğitimler

CCNA.

CCNP.

FDP GEOGRAPHY.

REDHAT LINUX.