**T.C.**
**BAHÇEŞEHİR ÜNİVERSİTESİ**

# PARALEL HİYERARŞİK DİZAYN METODOLOJİSİ KULLANARAK ŞİRKET BİNALARININ NETWORK VE ALTYAPI PROJELERİNİN DİZAYNI

**Yüksek Lisans Tezi**

**MEHMET TURUNÇ**

**İSTANBUL, 2012**

**T.C.**
**BAHÇEŞEHİR ÜNİVERSİTESİ**

**FEN BİLİMLER ENSTİTÜSÜ**

**BİLGİ TEKNOLOJİLERİ ( TÜRKÇE - TEZLİ) PROGRAMI**

# PARALEL HİYERARŞİK DİZAYN METODOLOJİSİ KULLANARAK ŞİRKET BİNALARININ NETWORK VE ALTYAPI PROJELERİNİN DİZAYNI

**Yüksek Lisans Tezi**

**MEHMET TURUNÇ**

**TEZ DANIŞMANI: YRD. DOÇ. DR. YALÇIN ÇEKİÇ**

**İSTANBUL, 2012**

**T.C.**
**BAHÇEŞEHİR ÜNİVERSİTESİ**
**FEN BİLİMLERİ ENSTİTÜSÜ**
**BİLGİ TEKNOLOJİLERİ ( TÜRKÇE - TEZLİ) PROGRAMI**

Tezin Adı:
Öğrencinin Adı Soyadı: Mehmet Turunç
Tez Savunma Tarihi: 10.02.2012

Bu tezin Yüksek Lisans tezi olarak gerekli şartları yerine getirmiş olduğu Enstitümüz tarafından onaylanmıştır.

Doç. Dr., F. Tunç BOZBURA
Enstitü Müdürü
İmza

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

Yrd. Doç. Dr., Alper TUNGA
Program Koordinatörü
İmza

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

| Jüri Üyeleri | İmzalar |
|---|---|
| Yrd. Doç. Dr., Yalçın ÇEKİÇ | ---------- |
| Üye<br>Yrd. Doç. Dr., Y. Batu SALMAN | ---------- |
| Üye<br>Yrd. Doç. Dr., Orhan GÖKÇÖL | ---------- |

# ÖZET

PARALEL HİYERARŞİK DİZAYN METODOLOJİSİ KULLANARAKŞİRKET BİNALARININ NETWORK VE ALTYAPI PROJELERİNİN DİZAYNI

Fen Bilimleri Enstitüsü,

Bilgi Teknolojileri (Türkçe-Tezli) Bölümü

Mehmet Turunç

Şubat 2012, 89 sayfa

Günümüzde teknolojinin de ilerlemesi ile network tasarımları hem teknoloji hızına yetişebilme yönünden, hem de ürün çeşidi yönünden karmaşık bir hal almıştır. O kadar çok alanda dikeylemesine uzmanlaşmanın daha zor olacağı varsayılırsa, bir rehber doğrultusunda network dizaynlarını yapabilme, tüm sistemlerin birbirleri ile entegre ve stabil çalışmalarını sağlamaya ihtiyaç duyulmaktadır. Bu çalışma var olan dizayn metodolojilerini tamamen yok saymadan, onlardan yararlanarak ve onları geliştirerek ortaya çıkan bir yaklaşım doğrultusunda (paralel hiyerarşik yaklaşım), network tasarımı yapabilmeyi konu edinmiş; gerçek anlamda pratik uygulama ile desteklenmiş ve işlevselliği yüksek bir ürün ortaya koymuştur. Paralel hiyerarşik yaklaşım yeni yapılan modern şirket binalarının tasarımlarında teknik kadro ve yönetim ekibi ile tartışarak, gerekli görüldüğü yerlerde üreticilerden de destek alarak geliştirilmiş olup, yeni yapılacak network projeleri için de yararlanılabilecek bir kaynak olabilmeyi hedeflemektedir.

**Anahtar Kelimeler:**Network Dizayn, Network Tasarım, Paralel Hiyerarşik Yaklaşım, Yukarıdan Aşağıya Network Dizaynı.

## ABSTRACT

DESIGN FOR INFRASTRUCTURE AND NETWORKING SYSTEM OF NEW COMPANY BUILDINGS USING A NEW NETWORK METHODOLOGY: "PARALLEL HIERARCHIC APPROACH"

Mehmet Turunç

Graduate School of Natural and Applied Sciences
Master of Science in Information Technologies(MSc in IT)

February 2012, 89pages

Nowadays, network design has been quite complicated in terms of both product varieties and of difficulty in being able to chase the speed of technology due to fast development and progress in technology. When agreed that it would be harder and harder to reach at mastery in various and many different sub-fields of network design; there would of course be some need for being able to design networking systems with the help of a guide, as well as need for a confirmation to prove that all the systems are integrated and are stable enough as they function. This study has focused on achieving a new way of networking design, entitled PARALLEL HIERARCHY APPROACH by the researcher, without ignoring current networking design methodologies yet by getting help from them as well as adding to their design methodology. On the other hand, the study has been supported with practical application and has presented a functionally-high product. PARALLEL HIERARCHY APPROACH has been developed through several negotiations and discussions among technical and administrative staff when decided as necessaryby the researcher, as well as through support by the network-design-tools producers; as they work cooperatively to design new network systems for newly constructed modern company buildings. The approach has also aimed at managing to be a new resource for new network projects to be done.



**Key Terms:** Network Design, Network Devise, Parallel Hierarchic Approach, Top Down Network Design

# 1. GİRİŞ

Bu tez çalışmasının konusu, var olan network dizayn metodolojilerinden esinlenerek yeni bir network dizayn yaklaşımı oluşturmak ve bunun başarılı olup olmadığını örnek bir uygulama içerisinde göstermektir. Bu araştırmanın yapılma sebebi, network dizaynlarında karşılaşılan sorunları minimize edebilmek ve sistematik bir çalışma biçimi oluşturabilmektir. Bu tez çalışmasının anlaşılabilmesi için IP network sisteminin temel düzeyde bilinmesi, genel dizayn yaklaşımlarından haberdar olunması ve bu tez çalışmasında bahsi geçen temel network, güvenlik, tümleşik iletişim, kablosuz iletişim ve altyapı kablolama teknolojilerine genel anlamda hakim olmak gerekir. Türkiye'de yapılmış çalışmalarda bu tez çalışmasındaki gibi bir yaklaşımda bulunulmamış, yabancı kaynaklarda teknolojiye özel bazı yaklaşımlarda bulunulmuştur. Bu çalışmada, o kaynaklardan da yararlanarak komple bir network sisteminin nasıl oluşturulacağına dair yeni bir yaklaşım ve öneriler sunulmuştur. Bu çalışma sonucunda komple network dizaynını sorunsuz ve sistematik bir şekilde yapmak isteyen kişiler için kaynak teşkil edecek nitelikte bir çalışma ortaya çıkarılmıştır.

İlk bölümde müşterinin teknik ve iş ihtiyaçlarını anlayarak bir analiz yapma çalışmasına dair bilgiler verilmiştir. İkinci bölümde bu analiz sonuçlarına göre oluşturulacak olan mantıksal network dizaynı konusunda çalışma yapılmıştır. Son bölümde ise mantıksal network dizaynına bağlı fiziksel network dizaynı irdelenmiş olup, teknolojilerin ve teknik ekipmanların nasıl seçileceğine dair öneriler sunulmuştur. Üç bölümde de bu tez çalışmasında ortaya konulan "Paralel Hiyerarşik Yaklaşım" evreleri baz alınarak gerek analiz safhasında, gerek dizayn safhalarında bu yaklaşım ile ilerleme kaydedilmiştir.

# 2. LİTERATÜR TARAMASI

Bu bölümde network dizaynı ile ilgili Türkiye'de ve dünyada yapılmış çalışmalar irdelenmiş ve yapılan çalışma ile en az ilgili olan kaynaklardan en çok ilgili olan kaynaklara doğru bir sıralama yapılmıştır. Kitaplar, makaleler ve yapılan çalışmalar incelenmiştir.

## 2.1 TCP/IP KONUSUNU İRDELEYEN KAYNAKLAR

(Albitz 2006) "DNS and BIND" çalışmasında DNS'in çalışma mantığı ve dizayn kriterlerine ilişkin çalışma yapılmıştır. DNS dizaynı için örnek gösterilen ve MIT, Stanford gibi üniversitelerde kaynak kitabı olarak kullanıldığından bu kitap incelenmiştir. Ancak genel olarak network üzerine değil de sistem üzerine yoğunlaşmış bir çalışma olarak kabul edilebilir.

OSPF'i anlatan başucu kaynağı olarak gösterilen çalışmada (Moy 1998), Dijkstra algoritmasının temellerine, bağlantı durumlu dinamik yönlendirme protokollerinin kullanılış biçimine ve uygulamalarına yer verilmiştir. Kitap biraz eski olmasına müteakip, yeni uygulamaya konulan yönlendirme protokollerini açıklayamamaktadır.

## 2.2 NETWORK PROBLEM ÇÖZME KONUSUNU İRDELEYEN KAYNAKLAR

Problem çözümüne ilişkin çok yönlü çalışmalara yer veren "Troubleshooting IP Routing Protocols" kaynağı (Faraz, Aziz, Lui, Martey & Aziza 2002) özellikle networkte yaşanan sorunlara karşı sistematik bir çözüm geliştirme tekniği sunmaktadır. Bu kaynak Cisco ağ ürünleri ile uğraşıp, problem çözme alanında bire bir çalışan kişilerin irdelemesi gereken bir kaynak olarak gösterilmektedir.

## 2.3 SİSTEM GELİŞTİRME KONUSUNU İRDELEYEN KAYNAKLAR

Biraz ansiklopedi hissi veren bu kaynak (Lewis 2008), SDLC üzerine kritik nitelikte işe yarayacak, nokta atışları yapabilen şekilde bilgiler vermektedir. Bu metodolojiler genellikle sistem ve yazılım çözümleri üzerine yoğunlaşmış, network çözümleri konusunda kısır kalmışlardır. Ancak genel fikri açısından yaklaşımlarından yararlanılmıştır.

Yeni bir kaynak olan ve detaylı bir çalışma yapan kaynak (Roebuck 2011), detaylı ve güncel bilgiler eşliğinde yol gösterici olmaktadır. Ancak diğer kaynakta da karşımıza çıkan network projeleri üzerine yoğunlaşmama konusu burada da mevcuttur. Günümüze daha yakın güncel bilgiler içerdiğinden bu kaynak literatür taraması sürecinde irdelenmiştir.

## 2.4 GÜVENLİK KONUSUNU İRDELEYEN KAYNAKLAR

Network güvenliği üzerine temel yapıtlardan birisi olan (Hines 2003) kaynak, özellikle güvenilirlik ile güvenlik arasındaki bağa vurgu yaparak networklerin daha stabil çalışmasını sağlayacak önerilere yer vermektedir. Bu nedenle incelenmiştir.

Michael Howard ve James A. Whittaker'in 2005 yılında IEEE'de yayınladıkları "Network Security Basics" adlı makalede temel network güvenlik metrolojilerinden bahsedilmiş ve katmanlı yapının önemine vurgu yapılmıştır. Güvenlikteki katmalı yapının nasıl dizayn edileceğine dair bilgiler ve önerileri içerdiğinden dolayı incelemeye alınmıştır.

Kurumsal network sistemlerinin güvenlik politikaları için yararlanılan P. Bera, K. Ghosh ve Pallab Dasgupta'nın 2010 yılında IEEE'de yayınladıkları makalede kurumsal güvenlik stratejileri ve politikaları irdelenmiş, bu kaynaktan faydalanılarak tez çalışmasındaki güvenlik tasarımında kaynak olarak kullanılmıştır.

(Performance and Manageability Design in an Enterprise Network Security System 1997) Makalede network güvenlik tasarımı yaparken ortaya çıkabilecek performans ve yönetim sorunlarıyla ilgili bir inceleme yapılmıştır. Güvenlik tasarımındaki çeşitlilik arttıkça network performansında görece düşme ve sistemin yönetiminde zorluklar ortaya çıktığı anlaşılmıştır.

## 2.5 KABLOSUZ NETWORKLER KONUSUNU İRDELEYEN KAYNAKLAR

(Gast 2002) 802.11 kablosuz networklerinin çalışma mantığını anlatan bu eser, yetkilendirme ve denetleme üzerine de kaynak olarak kullanılabilir. Kablosuz ağların standardizasyonundan sonra yazılan en kapsamlı kaynak olmasından ötürü bu tez çalışmasında kaynatan yararlanılmıştır. Ancak yazıldığı yıl nedeniyle 802.11n networkleri konusunda bilgi vermemektedir.

## 2.6 YEREL ALAN AĞLARI (LAN) KONUSUNU İRDELEYEN KAYNAKLAR

Her network mühendisinin başucu kaynağı olan bu kitap (Clark & Hamilton 1999) LAN teknolojisinin temellerini anlatmakta, özellikle anahtarlama sistemi ve protokolleri yönünden detaylı bilgiler içermektedir.

## 2.7 NETWORK DİZAYN KONUSUNU İRDELEYEN KAYNAKLAR

(Darren 2002) Network dizayn üzerine temel bir çalışma yapmış olan bu kaynak, yönlendirme ve anahtarlama teknolojileri üzerine yoğunlaşmış, kablosuz ağlar, tümleşik iletişim, güvenlik ve altyapı kablolama alanlarında zayıf kalmıştır.

IBM'in network dizaynı konusunda önemli eserlerinden birisi olan kaynak (Martin, Lee, Paolo & Karl 1995) sistem ve network entegrasyonu sınırları dahilinde network dizaynını açıklamıştır.

Mark Norris ve Steve Pretty'nin 2000 yılında kaleme aldıkları eser olan "Designing the Total Area Network", network yaşam döngüleri ve tasarım adımları konusunda fikir ve öneriler vermektedir. Yapıyı biraz daha büyük pencereden görmek isteyen yazarlar, adımları ihtiyaçları topla, uygula ve test et olarak belirlemişler ve derinlemesine çalışmaya inmedikleri için adımlar arası boşluk tasarımcıyı rahatsız etmektedir.

"The Design and Simulation of the Enterprise's VoIP Network" makale çalışmasında ses networkleri tasarımı üzerine oldukça açıklayıcı ve yol gösterici örneklerde bulunan Lily Chu, Xiaolei Lan ve Yiwen Tan; makaleyi mantıksal ve deneysel örneklemeler ile beslemişler ve reel bir sonuç ortaya çıkarmışlardır. Ancak çalışma sadece ses networklerini baz aldığından tasarımın tümünü görmeye engel teşkil etmektedir.

Kurumsal networklerin nasıl tasarlandığını anlatan çalışma (Planning Enterprise Networks to Meet Critical Business Needs, 1997), teknoloji ve iş hedefleri açısından bakışı konu alarak dizaynın SWOT analizini yapmaya kadar geniş ölçekte düşünebilmeyi konu alan bir makaledir. AT&T'de müdür olan Michael A. Weinstein'in makalesi, tasarımın gerçek hayata uygulanabilirliğine yönelik pratik bilgiler içermektedir.

Kuveyt Üniversitesi'nden S.J. Habib'in kaleme aldığı "Redesigning Network Topology with Technology Considerations, 2005" makalesinde teknolojinin gelişmesi ile artan yeterlilik kriterlerinin sınanması, ihtiyaçların ve amaçların büyümesiyle birlikte mevcut network sisteminde yapılması gereken değişiklik ve yükseltmelerin nasıl yapılacağı konusunda fikirler verilmektedir. Topolojinin de dizaynı oluşturmanın bir parçası olduğu kabulünden yola çıkarak, bu çalışmada fikir verici unsurlar arasında yer almıştır.

# 3. VERİ VE YÖNTEM

Veri ve yöntem kısmında önce konu ile ilgili teorik bilgilendirmelere yer verilecek, daha sonra kullanılanacak olan "Paralel Hiyerarşik Yaklaşım"ın tanımı yapılacak ve örnekler ile desteklenecektir. En sonunda ise paralel hiyerarşik yaklaşım ile bir şirket binasının network ve altyapı dizaynı yapılacak ve sonuçlar paylaşılacaktır. Tez çalışması veri ve yöntem kısmında savunulan paralel hiyerarşik yaklaşımı uygulayabilmek için gerçekleştirilen tasarım safhası üç ana başlığa bölünerek incelenecektir:

1) İhtiyaçları anlamak ve yönlendirmek
2) Mantıksal network dizaynı
3) Fiziksel network dizaynı

Her bölümde öncelikle teorik bilgiler aktarılacak, daha sonra mevcut yaklaşımlar ile nasıl uygulandığı irdelenecek, daha sonra ise "Paralel Hiyerarşik Yaklaşım"ın uygulanması neticesinde ne gibi avantajlar sağlandığına değinilecektir.

## 3.1 İHTİYAÇLARI ANLAMAK VE YÖNLENDİRMEK

Bu bölüm aslında tüm sisteme veri sağlayacak olan kaynağı oluşturur. Müşterinin ihtiyaçlarını belirlemek, onu doğru yönlendirip istenilen hedeflere ulaşabilmesini sağlamak tam bir mühendislik ve satış disiplini gerektirir. İş (yönetim) hedeflerinin belirlenmesi ve analizi, teknik amaçların belirlenmesi ve analiz edilmesi, genişleye bilirliği sağlayabilme, yeni dizayn ile oluşacak yapının getirilerinin şimdiden hesaplanabilmesi gibi bir çok faktör bu bölümde hesaba katılması gereken kriterler arasındadır.

Bölümde amaç ve ihtiyaçların belirlenmesi anlatılacak olup iş ihtiyaçları ve teknik ihtiyaçlar olarak iki gruba ayrılmıştır. İş ihtiyaçları yönetim kadrosunun karar vereceği,

şirketin hedef ve vizyonu ile ilgili alınacak kararlardır. Teknik ihtiyaçlar ise teknik ekibin hedeflediği ve teknik açıdan olması gereken gereksinimlerdir.

### 3.1.1 AMAÇLARIN VE İHTİYAÇLARIN BELİRLENMESİ

Burada amaçtan kasıt hedeflenen sonuca olan ulaşılabilirliktir. Hedefler üst yönetim tarafından konulan ve yapılması şirketin satış ve pazarlama faaliyetlerine olumlu katkı sağlayacak olan iş (yönetim hedefleri); ve teknik anlamda projenin sağlıklı bir biçimde oluşturulmasıyla kurulacak stabil yapının düzgün çalışması hedefleri olarak anlatılabilir. Burada bu iki bölümden iş hedefleri ve teknik hedefler olarak bahsedilecektir.

#### *3.1.1.1 İş (Yönetim) İhtiyaçlarının, Hedef ve Amaçlarının Belirlenmesi*

İş hedefleri, şirketlerin kurumsal hedefleri ve planları için oluşturulmuş uygulamalar, bunların hedef kitleye doğru ve sağlıklı bir biçimde ulaşması; proje yatırımı, personel yatırımı, kısıtlı proje tamamlanma zamanı gibi bazı kısıtlamaları da göz önünde bulundurarak hedef-yararlılık-yatırım üçgeninin doğru bir biçimde çalışabilirliğini sağlamaktır.

Bir network projesini dizayn ederken öncelikle hesaba katılması gereken şey iş hedef ve ihtiyaçlarının iyi analiz edilmesi ve buna uygun bir tasarım yapılması olarak gösterilebilir. Burada tasarım yapan kişinin de teknik bilgi düzeyi ve müşteriyi yönlendirebilme kabiliyetine binaen, hedeflere uygun mantıklı ve ölçeklendirilebilir projeler ortaya çıkabilmektedir. Oluşturulan network dizaynının başarılı olabilmesi için kurumsal hedef ve politikaları iyi belirlemek ve bunları dizayna direk müdahale ederek kullanmanın getireceği olumsuz etkileri minimize etmek gerekir. Müşterinin istediği bir özellik çok daha fazla yük ve yatırım gerektirebilir; ya da istenilmeyen bir özellik aslında basit bir konfigürasyon değişikliğiyle sağlanabilir. Burada analiz ve analiz sonuçlarına dayanan reel ve mantıklı dizayn önem arz etmektedir.

Dünyada kabul görmüş dizayn metodolojilerinden yararlanmak hem projenin salahı, hem de proje planının yapılması ve uygulanması aşamasında tasarımcının yol göstericisi olacaktır. Bu tez çalışmasında iki adet dizayn metodolojisinden yararlanılmıştır.

#### *3.1.1.1.1 Sistem Geliştirme Yaşam Döngüsü (System Development Life Cycle – SDLC)*

Sistem geliştirme yaşam döngüsü büyük projelerin daha küçük adım taşları bölümlerine bölünerek çalışılmasını gerektiren bir proje yönetim tekniğidir. Bir sistemin oluşumundan, işlevini tamamlamasına kadar olan ömür döngüsüdür (Kevin 2011, p.39). Sistem geliştirme yaşam döngüsü temel olarak aşağıdaki evrelerden oluşur:

**Ön görüşme aşaması:**

Ön görüşme safhası, sistemi ilerletme, düzeltme, tamir etme, ekleme fırsatı görüldüğü ve bir kuruluştan resmi olarak istendiği zaman başlar. Bir iş önerisi (business case) hazırlanır. Bu öneri, temel hatlar olarak önerinin sebebi, beklenen getirileri, önerinin şirketin yönetim stratejisine nasıl ve neden uyduğu, alternatif çözümler ve mümkün olduğunca detaylı bir şekilde fonksiyonel, network, bilişim anlamda gereksinimleri tanımlanmalıdır. Bir önerinin yönetim tarafından değerlendirilmesi önemlidir. Bu safhada yönetim bütün etkilenen departmanlardan fikir alır ve çeşitli değerlendirmeler yaparak bu önerinin tümünü veya bir bölümünü iptal etme imkânına sahip olurlar ki bu çok önemli bir kabiliyettir. Ön görüşme safhasının önemli bir basamak olmasının sebebi ön görüşme safhasında kabul edilen önerilerin daha sonra daha detaylı bir araştırma ve raporlama safhasından geçmesidir. Bu araştırma ve raporlama safhası uzun ve yorucu bir işlemdir ki bu safhada birçok kaynak harcanır. Eğer yönetim daha ön görüşme safhasında gereksinim dışında ve ihtiyaç duyulmayan bir projenin tamamı veya bir parçasını iptal ederse bu aslında şirkete büyük bir getiri anlamı taşımaktadır. Çünkü daha sonraki safhalarda bu iptal edilen önerinin tamamı veya bir parçasına detaylı araştırmada harcanacak kaynaklar harcanmamış olur.

**Planlama aşaması:**

Hemen hemen her projede olduğu gibi sistem geliştirme yaşam döngüsünde de planlama evresi en çok zaman harcanan ve en önemli olan evredir. Planlamanın derinliği ve ayrıntısı genelde projenin riski, karmaşıklığı ve büyüklüğü ile doğru orantıda olur.

Kilit rollerin veya çalışanların sorumlulukları, takım çalışanlarının bilgileri belirtilmelidir. Eğer varsa, dışarıdan destek verenlerin sorumlulukları da belirtilmelidir. Mümkünse iletişim kanalları ve yolları da tanımlanmalıdır. Standart raporlamalar, raporlama standartları ve toplantı programı plan dahiline alınmalıdır.

Yönetim tarafından projenin her safhasında kabul edilebilir tamamlama standartları belirlenmelidir. Bunların yanı sıra her adımın başarı ile tamamlanmasını garantilemek için tamamlama testleri, tamamlama prosedürleri detaylı bir şekilde açıklanmalıdır. Detayları ile çizilmiş başarı sınırları ve beklentileri, projenin başarısı için önemlidir. İyi bir planlamanın en önemli adımlarından biri de planlama safhasında yapılan otomatik kontrol ve güvenlik adımlarının genel hatlarının belirlenmesidir. İlk planlamada bu güvenlik ve kontrol adımlarını tanımlamak zor olabilir fakat planlamanın bu adımını projenin her safhasında tekrarlamak kaydı ile zaman içinde hedeflere ulaşılabilir.

**Dizayn aşaması:**

Dizayn evresinde hedef, ön-görüşme ve planlama safhalarında belirlenen ihtiyaç, sınır, başarı hedeflerine ulaşacak genel hatları sistemin altyapısına uygun bir şekilde çizilmesidir. Sistemlerin dizaynları birçok şekilde yaratılabilir. Örneğin "yukarıdan aşağıya" yaklaşımı vardır. Bu bakış açısıyla hazırlanan sistemlerde ilk önce sistemin en ana hatlarını belirlenir ve dizaynı geliştirilir. Daha sonra bu ana temelin altında çalışacak alt sistemler veya görevler dizayn edilir. Yani bu aslında en büyükten en küçüğe doğru izlenen bir yoldur. Birde bunun tam tersi "aşağıdan yukarıya" yaklaşımı vardır. "Aşağıdan yukarıya" yaklaşımda, projenin detay hatları ilk önce uyarlanır ve dizaynı tamamlanır. Daha sonra bu detayların ihtiyaç ve beklentileri bağlamında yavaş yavaş daha üst katmanlar dizayn edilir.

Bu tez çalışmasında "yukarıdan aşağıya" dizayn metodundan esinlenerek "Paralel Hiyerarşik Dizayn Modeli" belirlenmiş ve tüm çalışmalar bu dizayn yapısını destekleyecek şekilde örneklendirilmiştir.

**Test aşaması:**

Test safhası sistemin çeşitli testlerden geçirilerek işlerliğinin kontrolünden ibarettir. Bu testler çeşitlere ayrılırlar ve birden fazla yolla birden çok test yapılır. Genel test, sistemin her yönü ile çalıştığından emin olmak için önemlidir. Organizasyonlar eğer doğru proje geliştirme teknikleri ile çalışıyorlarsa zaten test planları daha bu safhaya gelmeden çok önce hazırlanmış olmalıdır. Aceleci istekler ve zaman sınırlamaları test hazırlıklarının önceden başlamasını engellemesine neden olabilir. Test hazırlıklarının ve planlarının önceden yapılması kurulum evresinden sonra karşılaşılabilecek hataların test aşamasında yakalanmasını kolaylaştırır.

**Kurulum ve devreye alma aşaması:**

Bu evrede hazırlanan ve kabul edilen sistemin devreye alınmasından oluşur. Bu bölümde yapılması gereken başlıca görev doğal olarak içinde sistemin etkileyeceği kişilere ve çalışanlara sistemde yapılacak değişiklik ve devreye almanın önceden bildirilmesidir. Bu evrede işlemler; kurulum ve devreye alma planının herkese ulaştırılması, son kullanıcı ve operatörlerin eğitimi olarak sıralanabilir. Yönetim gerekli verilerin sisteme girilmesi, devreye alma öncesi testlerin yapılması, devreye alma öncesi güvenlik birimlerinin kontrolü ve devreye alma sonrası testlerden sorumludurlar.

**Değerlendirme aşaması:**

Bu evrede görev tamamı ile proje yönetim gurubunundur. Kurulum ve devreye alma evresi sonrası bir değerlendirme yapılır. Bu değerlendirme kıstaslarını hazırlarken önemli faktörler arasında, sistemin içerisindeki tüm birimler ile aktif olarak görüşülür ve herhangi bir problem var ise raporlanır.

Yönetim, projenin işlerliğini ve değerini hesaplarken projenin varsayılan bütçesi ile maliyetini karşılaştırır. Maliyet/yarar oranı ve üretim zamanı da rapora eklenmelidir. Bu

rapor sistemin kullanıldığı şirketin yönetim kuruluna veya ilgili birimlerine iletilir. Bu bölüm daha çok işletme tabanlı bir işlemdir.

**Yapılandırma ve onarma aşaması:**

Bu evre sistemdeki donanım, yazılım ve dokümantasyonda değişiklikleri kapsar. Sistemin performansının arttırılması asıl hedeftir. Sistemdeki hataların düzeltilmesi, güvenliğin arttırılması diğer hedeflerdir. Sistemde yapılan değişikliklerin sistemin işleyişini herhangi bir şekilde olumsuz etkilerinin olmaması için belli değişiklik ve düzeltme standartlarının oluşturulması önemlidir. Her değişiklik her zamanki gibi dokümante edilmelidir.

Sistemde yapılan her değişiklik, daha değişiklik yapılmadan önce sistemdeki donanım, yazılım gibi tüm etkenlerle etkileşiminin iyi olması ve farkında olunamayabilecek herhangi bir hataya mahal vermemesi sağlanmalıdır. Bu arada versiyonlama da es geçilmemelidir. Her değişiklik farklı bir sürüm demektir. Sistemin hazırlanmasında birde acil durum versiyonu hazırlanması en güvenli olanıdır. Bu acil durum versiyonunda sistemde en temel ihtiyaçlara yer verilmeli ve mümkün olduğunca basite indirgenmiş bir temel oluşturulmalıdır.

**Yok etme (Çöpe atma) aşaması:**

Çöpe atma safhası oldukça basit bir safhadır. Bu safhada eski sistemden kalan ve artık gereksiz hale gelen teknoloji, donanım, yazılım ve hatta çalışanlar sistem dışına alınır.

Bu evrede önemli noktalardan birisi, yok etme sırasında izlenecek yoldur. Mesela bir hard disk yok edilecekse bu hard diskin üzerine komple gereksiz veriler kayıt edilmeli veya hard disk komple manyetik alan tabii tutularak silinmelidir. Çünkü farkında olmadan çök önemli ve şirketin mahrem sayılabilecek bilgilerini istenmeyen bireylerin çöpten alması uygun olmayan bir durum oluşturabilir.

#### *3.1.1.1.2 Planlama, Dizayn, Kurulum, Devreye Alma, Optimizasyon (PDIOO – Plan, Design, Implementation, Operation, Optimization)*

Dünyanın önde gelen network ekipman üreticisi Cisco'nun belirlediği bu standart "Sistem Geliştirme Yaşam Döngüsü"ne benzer bir dizayn metodolojisini anlatmaktadır. PDIOO İngilizce kelimelerinin baş harflerinden oluşan Planlama (Plan), Dizayn (Design), Kurulum (Implementation), Devreye alma (Operation), Optimizasyon (Optimization) evrelerinden oluşmaktadır (Oppenheimer 2011, p.7). PDIOO yaşam döngüsünü detaylı şekilde aşağıdaki gibi inceleyebiliriz.

**Şekil 3.1: PDIOO Süreçleri**


*Kaynak:* Oppenheimer, 2011, p.7

**Planlama:**

Bu fazda network gereklilikleri ve ihtiyaçları tanımlanır. Ayrıca network'ün nereye kurulacağı, bu network servisinden kimlerin faydalanacağı gibi detaylı analizler bu safhada yapılır.

**Dizayn:**

Bu bölümde tasarımcının hem mantıksal hem de fiziksel olarak dizaynı nasıl şekillendireceğine yer verilir. Planlama safhasından alınan veriler ve müşteri ihtiyaçları neticesinde, teknik olarak uygun bir tasarım yapılır.

**Kurulum:**

Dizayn evresi bittikten sonra projenin tasarımı çıkmış demektir. Bir önceki fazdaki çıktıları bu faz için girdi kabul edersek, dizayna uygun network bu bölümde kurulmaya başlanır. Kurulum aşamasında teknik operasyon ve saha tecrübesi yeterli personel ile çalışmak son derece önemlidir.

**Devreye alma:**

Bu fazda yapılacak olan hamle kurulumu yapılan networkün devreye alınması işlemidir. Devreye alma sırasında oluşacak ilk hatalar gözlemlenir ve sistem monitör edilir. Bu fazın çıktıları sonucunda optimizasyon safhasına veri sağlanır.

**Optimizasyon:**

Network dizayn edilip, kurulup, devreye alma işlemi gerçekleştirildikten sonra son olarak optimizasyon ayarlarının yapılması gerekir. Optimizasyon evresi diğer evrelere nazaran daha uzun sürer. Bu fazda kurulan network mükemmele yakın hale getirilmeye çalışılır; performans testleri sonucu ortaya çıkan iyileştirmeler ve yapılan dizayn hatalarının açıkça gözlemlenebileceği bir pilot test ortamı oluşturulur.

#### *3.1.1.2 Teknik İhtiyaçlarının, Hedef ve Amaçların Belirlenmesi*

Teknik ihtiyaçların belirlenmesinde belirli bir dizayn yaklaşımına müteakip yol izlenmelidir. Yukarıdan aşağıya, aşağıdan yukarıya, kompozit gibi dizayn yaklaşımları bulunmakla beraber, bu tez çalışmasında tez başlığından da anlaşılacağı üzere "paralel hiyerarşik" dizayn yaklaşımı izlenmiştir. Bu dizayn yaklaşımı canlı bir uygulama ile

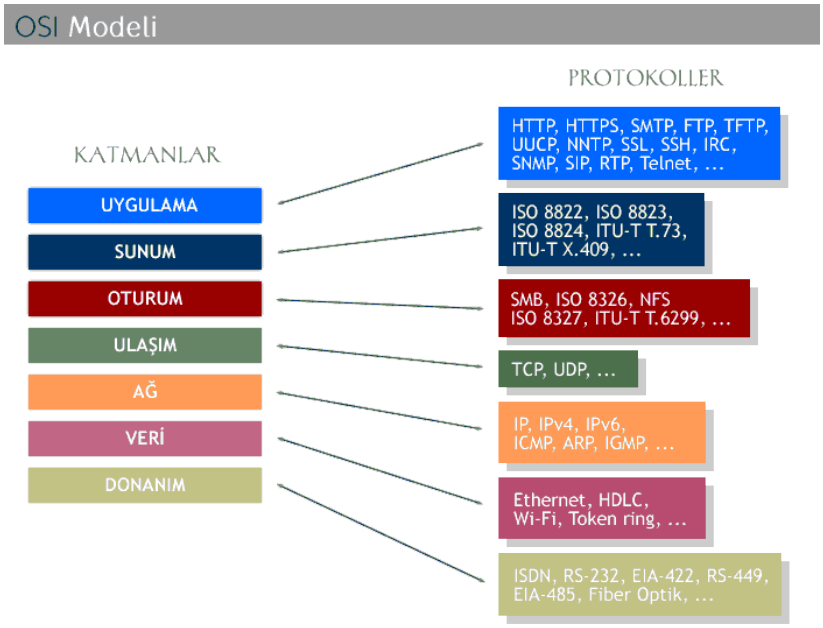
harmanlanmış ve özgün bir metot haline getirilmiştir. Bundan sonraki yapılacak olan çalışmalarda da bu tez çalışması başvurulabilecek bir kaynak olarak kullanılabilir.

#### *3.1.1.2.1 Paralel Hiyerarşik Dizayn Metodolojisi*

Network uzmanları çok karmaşık yapıda bir network dizayn etmenin çok iyi bir mühendislik çalışması olduğunu düşünebilirler. Ancak aslında bu, daha sonra ortaya çıkabilecek olan problemlerin çözümünde durumun içinden çıkılamayacak hal almasına yol açar. Bir dizayn temelde ne kadar basit ise, o kadar hızlı ve sağlıklı büyüyebilir.
Paralel hiyerarşik dizayn metodolojisi şöyle tanımlanabilir: Yukarıdan aşağıya metodolojisi ile farklı teknoloji dizaynlarını bir araya getiren yaklaşımdır. Yani bir disipline ait tasarımı yukarıdan aşağıya şeklinde dizayn ederken, paralelde diğer disiplinlere göre tasarımın işlevselliğini aynı anda kontrol etmektir. Bu sayede dizayn daha sağlıklı ve uzun ömürlü olur; problemler daha sistematik, daha kolay ve etkileyeceği kısımların önceden tahmin edilebileceği şekilde daraltılmış olarak belirlenebilirler.

Network dizayn projelerinde kullanılan "yukarıdan aşağıya" metodu OSI referans modeline göre sistemin üst katmanlarından başlayarak alt katmanlara doğru gidilmesi ile kolayca eşleştirilebilir. Yani yönlendirici, anahtar, kablo gibi temel ekipmanları seçmeden önce, sistemde hangi uygulamaların çalışacağı, oturum bilgilerinin nasıl olacağı, hangi portlar üzerinden çalışmasının düşünüldüğü gibi örnekleme yapılabilir (Wetteroht 2001). OSI referans modelini bir hatırlanacak olursa:

**Şekil 3.2: OSI Katmanları**




*Kaynak:* http://www.bidb.itu.edu.tr/?d=496

**Uygulama Katmanı:**

Kullanıcı tarafından çalıştırılan tüm uygulamalar bu katmanda tanımlıdırlar. Bu katmanda çalışan uygulamalara örnek olarak, FTP FTP, SNMP, e-posta uygulamaları verilebilir.

**Sunum Katmanı:**

Bu katman adını amacından almıştır. Yani bu katman verileri uygulama katmanına sunarken veri üzerinde bir kodlama ve dönüştürme işlemlerini yapar. Ayrıca bu katmanda veriyi sıkıştırma/açma, şifreleme/şifre çözme, karakter kodlaması dönüşüm işlemlerini de yerine getirir.

**Oturum Katmanı:**

İletişimde bulunacak iki nokta arasındaki oturumun kurulması, yönetilmesi ve sonlandırılmasını sağlar. Bu katmanda çalışan protokollere örnek olarak NFS, SQL, RPC, ASP, DNA SCP ve X Window verilebilir.

**Taşıma Katmanı:**

Bu katman iki düğüm arasında mantıksal bir bağlantının kurulmasını sağlar. Ayrıca üst katmandan aldığı verileri segmentlere bölerek bir alt katmana iletir ve bir üst katmana bu segmentleri birleştirerek sunar. Bu katman aynı zamanda akış kontrolü kullanarak karşı tarafa gönderilen verinin yerine ulaşıp ulaşmadığını kontrol eder. Karşı tarafa gönderilen segmentlerin karşı tarafta gönderenin gönderdiği sırayla birleştirilmesi işinden de bu katman sorumludur.

**Ağ Katmanı:**

Bu katman, veri paketlerinin ağ adreslerini kullanarak bu paketleri uygun ağlara yönlendirme işini yapar. Yönlendiriciler bu katmanda tanımlıdırlar. Bu katmanda iletilen veri blokları paket olarak adlandırılır. Bu katmanda tanımlanan protokollere örnek olarak IP ve IPX verilebilir. Bu katmandaki yönlendirme işlemleri ise yönlendirme protokolleri kullanılarak gerçekleştirilir. Yönlendirme protokollerine örnek olarak RIP, IGRP, OSPF ve EIGRP verilebilir. Burada dikkat edilmesi gereken önemli bir nokta da yönlendirme protokolleri ile yönlendirilebilir protokollerin farklı şeyler olduğudur. Bu katmanda kullanılan yönlendirme protokollerinin görevi, yönlendirilecek paketin hedefe ulaşabilmesi için geçmesi gereken yolun hangisinin en uygun olduğunu belirlemektir. Yönlendirme işlemi yukarıda bahsettiğimiz yönlendirme protokollerini kullanarak dinamik bir şekilde yapılabileceği gibi, yönlendiricilerin üzerinde bulunan yönlendirme tablolarına statik olarak kayıt girilerek de paketlerin yönlendirilmesi gerçekleştirilebilir.

**Veri Bağlantısı Katmanı:**

Network katmanından aldığı veri paketlerine hata kontrol bitlerini ekleyerek çerçeve (frame) halinde fiziksel katmana iletme işinden sorumludur. Ayrıca iletilen çerçevenin doğru mu yoksa yanlış mı iletildiğini kontrol eder, eğer çerçeve hatalı iletilmişse çerçevenin yeniden gönderilmesini sağlamak da bu katmanın sorumluluğundadır. Bu katmanda ,iletilen çerçevenin hatalı olup olmadığını anlamak için CRC yöntemi kullanılır. Anahtarlar bu katmanda tanımlıdırlar.

**Fiziksel Katman:**

Verilerin fiziksel olarak gönderilmesi ve alınmasından sorumlu katmandır. Hub'lar fiziksel katmanda tanımlıdırlar. Bu katmanda tanımlanan standartlar taşınan verinin içeriğiyle ilgilenmezler. Daha çok işaretin şekli, fiziksel katmanda kullanılacak bağlantı türü, kablo türü gibi elektriksel ve mekanik özelliklerle ilgilenir. Örneğin V.24, V.35, RJ45, RS-422A standartları fiziksel katmanda tanımlıdırlar.

Yukarıdan aşağıya tasarımda bu OSI katmanlarının sırası göz önüne alınmalı, network tasarımcısının başucu rehberi olmalıdır. Bu referans modeli sayesinde proje de tanımlı parçalara bölünmüş olur; hem kurulum aşasında, hem de problem çözme aşamasında çok büyük kolaylıklar sağlar. Modüler yapı esastır. Proje fonksiyonel olarak parçalara ayrıldığında proje yönetimi de daha kolay olmaktadır. Daha sonra yapılacak olan değişiklikler ya da versiyon artırımı gibi aksiyonlar da daha kolay ve sistematik bir biçimde yapılabilmektedir.

Yukarıdan aşağıya yapının özellikleri şöyle sıralanabilir:

i. Sistem yukarıdan aşağıya gidecek şekilde dizayn edilir.
ii. Tasarım sırasında mevcut sistemi karakterize eden, yeni ihtiyaçları ve gelecekteki yapıyı az çok belirleyen modelleri karakterize etmek için çeşitli teknikler kullanılır.
iii. Verinin akışını, tipini ve uğrayacağı işlemleri inceleyen ayrı bir çalışma yapılır.
iv. Önce mantıksal topoloji oluşturulur, daha sonra daha spesifik teknolojiler ve kurulum işlemleri de hesaba katılarak fiziksel topoloji oluşturulur.
v. Her bir ekipmanın ve fonksiyonun özelliği dizaynın en başında belirtilir ve en alt katmana gelinene kadar en üstteki temel bilgi ve fonksiyonlar korunur.

Bu yaklaşım ile her modül ayrı olarak tasarlanır. VE tasarlanan bu her modülde yukarıdan aşağıya anlayışı benimsenir. Bu çalışmada komple bir network dizaynı yapılmış ve bu dizayn temel network dizaynı, network güvenlik dizaynı, tümleşik iletişim dizaynı, kablosuz network dizaynı ve alt yapı kablolama dizaynı gibi alt parçalara bölünmüştür. Bu her parça kendi içerisinde yukarıdan aşağıya tasarım metodolojisi benimsenerek, yapısal ve modüler bir anlayışla inşa edilmiştir.

#### *3.1.1.2.2 Teknik Yeterlilik Kriterleri*

Teknik yeterlilikler projenin ayakta kalması ve sağlıklı biçimde çalışabilmesi için gerekli olan, teknik olarak alanında uzman kişilerin denetlediği ve gözlemlediği kıstaslardır. Bu kıstaslar herhangi bir felaket durumuna, ya da işlevselliği bozan bir uygulama hatasına karşı networkü denetleyebilmeyi sağlamada ana faktörler olarak rol oynamaktadırlar (Anthony & Jacqueline 2000, p.78)

**Ölçeklenebilirlik:**

Ölçeklenebilirlik network dizaynının ne kadar genişleyebileceğinin desteği olarak tanımlanabilir. Birçok büyük organizasyonlarda istenilen en temek özelliklerden birisidir. Çünkü böyle yapılarda sistemler çok dinamik olarak gelişmekte, genişlemekte ve bunların yan etkisi olarak yapılar karışmakta, karmaşıklaşmakta ve problem durumlarında içinden çıkılamayacak hale bürünmektedir. Bu nedenle ölçeklenebilirliğin teknik yeterlilik kriterleri arasındaki rolü çok büyük ve önemlidir. Networkün büyümesi yönünde planlama yapılması bu noktada öne çıkabilecek sorulardan biridir. Örneğin; "Önümüzdeki yıl kaç bölge daha mevcut yapıya katılacak?", "Yeni bölgelerin trafik ve yük yoğunluğunu merkezdeki tasarım kaldırabilecek mi?", "Önümüzdeki yıllarda sisteme kaç adet kullanıcının dahil edileceği analizleri yapıldı mı?", "Sisteme ileriki yıllarda kaçar adet sunucu, network ekipmanları vs. gibi aktif cihazların sayısı ile ilgili bir analiz yapıldı mı?" gibi sorulara yanıt aramak aslında ölçeklenebilirliğin hesaplanmasında en büyük yardımcı olacaktır.

**Güvenilirlik:**

Güvenilirlik networkün ne kadar süre ile kesinti olmadan ayakta kalabileceğinin göstergesidir. Genellikle de günde, haftada, ayda ve yılda yüzde kaç kesinti olduğuyla da belirtilebilir. Güvenilirlik biraz da yedekliliği anlatır. Networkün kesintisiz bir şekilde çalışmasına devam edebilmesi için, bir sistemin çöktüğünden ya da çalışması durduğunda onun işlevini alabilecek aktif ya da pasif olarak yedekte bekleyen sistemin faaliyete geçmesi gerekir. Bu da tüm sistemin ayakta kalma süre yüzdesini arttıran ancak aynı zamanda maliyet getiren bir kalemdir. Yedekliliğin maliyet-performans-risk

üçlüsüne göre değişebilen şekilde çeşitleri bulunmaktadır. Örnek vermek gerekirse 1:1 yedeklilik aynı sistemin bir yedeğinin atıl olarak dizayn içerisinde durması, herhangi bir kesinti durumunda tüm fonksiyonları yerine getirebilecek şekilde devreye girmesidir. 1:2 yedeklilik ise mevcut sistemdeki parçaların risklerini ayrı ayrı hesaplayarak performans açısından daha az ekipmanın yedeğinin durması anlamındadır. Burada yedekte duran sistemin performansı daha düşüktür ancak maliyet açısından da daha avantajlıdır. Yukarıda da belirtildiği gibi maliyet-performans-risk üçlüsünün iyi analiz edilip, ona göre bir tasarım yapılması gerekmektedir.

**Network performansı:**

Network performansı teknik ekibi ilgilendiren belki de en önemli kıstaslardan biridir. Mevcut yapı kontrol edilirken, yeni yapının dizaynında performansa ait kriterler önem kazanır. Kurulacak olan yeni sistemin etkinliği, bant genişliği, gecikmeleri ya da uygulamaların ve sunucuların cevap süreleri çok daha iyi olmalıdır. Mevcut yapının zaafları analiz edilmeli ve tasarımı yapılan yeni network hakkında kıyaslama kriterleri oluşturmalıdır. Network performansı deyince akla birçok kriter gelebilir. Bunlara genel olarak kısa bir şekilde değinebiliriz. Bant genişliği ya da kapasite; bir devre ya da bir network üzerinde data iletimindeki taşıma yeteneği olarak tanımlanır. Genellikle saniyedeki bit sayısı (bit per second – bps) ile ölçülür. Kullanım; tüm network sistemi için kullanılan kapasite yüzdesidir. Ortalama kullanım da bunun ortalamaya vurulmuş halidir. Üretilen iş miktarı (throughput); network dünyasında en çok kullanılan kapasite terimlerinden birisidir. Belli bir zaman diliminde noktalar arası geçebilen hatasız veri sayısı olarak tanımlanabilir. Gecikme; Bir ağdan başka bir ağa, ya da aynı network içerisinde toplama noktaları arası kaybedilen zamandır.

**Güvenlik:**

Güvenlik kriteri dizaynda rol alsın almasın herkesin kafasında soru işaretleri bırakan, çoğu kişinin belli belirsiz fikir sahibi olduğu, yönlendirmeye ve manipülasyona çok elverişli bir teknik kıstastır. Bu işin kesinlikle işinde uzman kişiler tarafından yapılması, bu şekilde dizayn edilmesi ve devreye alınması gerekir. Network güvenliğinden, kullanıcı güvenliğine, veri merkezinin güvenliğinden, dışarıdan gelecek saldırılara karşı

proaktif olmaya kadar birçok alt başlığı bulunmakla birlikte temel amacı açık ve nettir; analiz sonucu ortaya çıkan önemli bilgileri koruyabilmek.

**Yönetilebilirlik:**

Yönetilebilirlik, tasarımı yapılan sistemin yönetiminin kolay, anlaşılır, sistematik ve raporlanabilir olmasıdır (Oppenheimer 2011, p.49). Bu sayede yapılan çalışma hem güvenlik, hem servis kalitesi hem de ölçeklenebilirlik anlamında raporlanabilir; bu aksiyonları almak adına kolay geliştirmelere imkan tanır.

**Kullanışlılık:**

Tanım olarak kullanışlılık, en temel düzeyde kolayca teknik ekibin ya da kullanıcıların sisteme olan alışkanlık düzeyinin yüksekliği, o sistemi aşırı çaba sarf etmeden yönetebilmeleri anlamındadır. Dizayn edilen sistemlerde de kullanışlılık ne kadar iyiyse sisteme alışabilirlik o kadar fazladır. Öğrenilme kabiliyeti artmış, çok fazla çaba ve uzman gerektirmeden sistemin operasyonunun yapılabilmesidir.

**Geliştirilebilirlik:**

Geliştirilebilirlik, sistemin yeni versiyonlara kolayca adapte olabilmesi, sistemin sağlıklı bir biçimde büyüyüp genişleyebilmesi yönünden avantaj arz etmesidir. Bu aslında tasarımın başarısını belirleyen faktörlerden biridir. Çünkü iyi bir tasarım gelecekteki versiyon değişikliklerine ve büyümelere karşı açık olmalı, minimum maliyet ile maksimum verimi alabilme yönünden etkin olmalıdır.

**Hesaplılık:**

Maliyet yeni sistem tasarlamanın önündeki en büyük engellerden biridir. Çünkü müşteriler ya da sistemi satın almak isteyen kişi ve kurumlar yapacakları yatırımın geri dönüşünün nasıl olacağını hep merak ederler. Geri dönüş süresi ve sistemin ne kadar daha aktif olarak kullanılacağı maliyet faktörünü hesaplılık açısından destekleyen öğelerdendir. Hesaplılığı uygun olan bir sistem bir network dizayn mühendisinin elinden çıkmış, uygun bir sistemdir denilebilir.

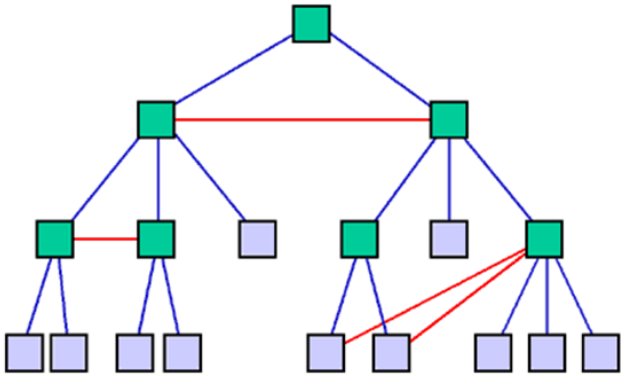
## 3.2 MANTIKSAL NETWORK DİZAYNI

Network topolojisini dizayn ederken ki ilk adım bir dizayn metodolojisi seçerek mantıksal network tasarımına başlamaktır. Mantıksal tasarım, kablo bağlantıları, uç sayıları, port numaraları gibi bilgileri içermez. Genel olarak yapının tasvir edilmesi, kullanılacak yedeklilik metotlarının seçimi, anahtarlama ve yönlendirme protokollerinin belirlenmesi, veri merkezinin diğer hizmet veren yapılara göre konumu gibi birçok kriteri düşünmeyi gerektirir. Mantıksal dizayn, fiziksel dizaynın da temelini oluşturur. Ana hatları ile yapıyı belirler; kullanılacak teknolojilerin ve bağlantıların nasıl kurulacağı yönünde bilgiler verir.

### 3.2.1 PARALEL HİYERARŞİK DİZAYN MODELİ

Müşterinin iş ve teknik hedeflerini anladıktan sonra bir mantıksal network topolojisi üzerinde çalışmak gerekir. Hiyerarşik network dizayn modeli burada tasarımın modülerleştirilmesi açısından çok büyük avantajlar sağlar. Paralel hiyerarşik dizayn modeli ise, hiyerarşik modelin tezlerini kabul ederek, bunu birçok farklı teknolojiye paralel olarak yayarak, tüm networkün tasarımının da paralel zamanda yapılmasını sağlar. Her katmanı ayrı ayrı dizayn etmek hem resmin bütününü görebilmek açısından, hem de dizaynın geliştirilmesi açısından tasarımcıya kolaylık sağlar.

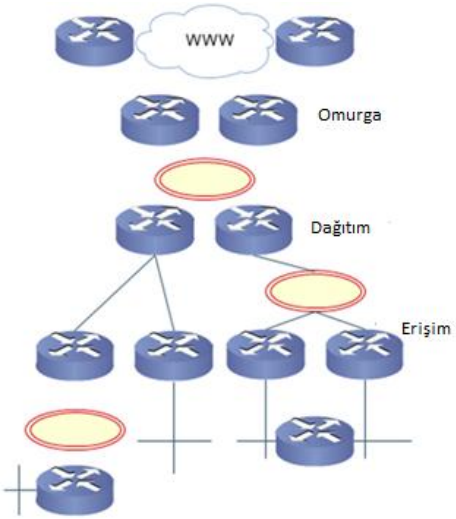
**Şekil 3.3: Paralel Hiyerarşik Dizayn Yapısı**



Yüksek kapasiteli anahtarlama için omurga anahtarlamayı yapacak olan katman dizayn edilir. Bu çalışmada önce katmanlar teker teker belirtilecek, sonra kapasite ve trafik akışına uygun cihazlar tasarıma yerleştirilecektir. Sonrasında ara katman olan daha düşük anahtarlama kapasitesine sahip ancak güvenlik, ses networkü için gerekli özellikler gibi diğer fonksiyonları daha özelleşmiş olan dağıtım katmanı tasarlanır. Topolojinin en altında bilgisayar, IP telefon, video konferans cihazı, erişim noktaları gibi kullanıcıya bakan uç cihazların konfigürasyonu yapılır. Bu katman erişim katmanı olarak adlandırılır ve kullanılacak olan uç cihazın tipine göre farklı farklı cihazlar ile genişletilir.

Kampüsün internet bağlantısı için ayrı bir birim tasarlanır. İnternet katmanı olarak adlandırabileceğimiz bu kısım, daha çok gelişmiş yönlendirme protokollerinin yüksek performanslı olarak çalışabilecekleri ve yönlendirme fonksiyonlarının çalıştığı algoritmaları yönetebilecek özelleşmiş işlemcilerle donatılmış özel cihazlar ile desteklenir. Burada amaç farklı network bulutları arası geçişin sorunsuz bir şekilde yapılabilmesidir. Uygulamaların koşacağı sunucuları barındıran veri merkezi katmanında yüksek kapasiteli sunucuların oluşturacağı yüksek bant genişliğine sahip verileri işleyebilecek veri merkezi kullanımında özelleşmiş anahtarlar kullanılır. Bunların çeşitleri de kullanılan protokollere, trafiğin kapasitesine göre değişebilen şekilde dağılım gösterir.

**Şekil 3.4: Hiyerarşik Dizayn Modeli**



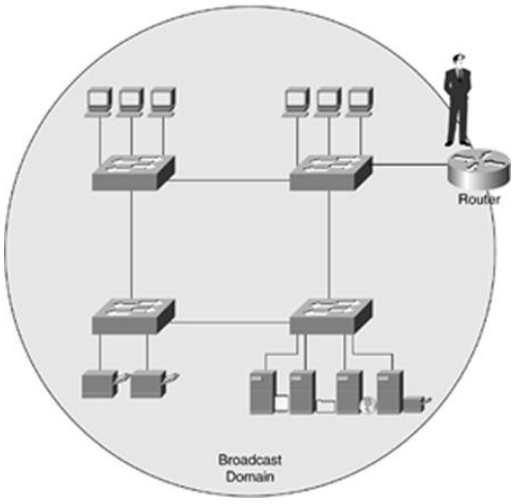

*Kaynak:* Oppenheimer 2011, p.129

Hiyerarşik modeli kullanmayan dağınık yapılar bir plan dahilinde geliştirilmedikleri için, dağınık yapılar olarak adlandırılırlar. Bu yapıda tasarlanan networklerde cihazlar ve networkler arası darboğazlar oluşur. Yapının karmaşıklığından dolayı oluşabilecek muhtemel problemlere çözüm getirilmesi de oldukça zorlaşır. Sistem kolay eklemeler ile büyüyemez, yeni devreye almalar sırasında networkte kesintiler, aksaklıklar ve kullanıcıların ulaşması gereken sunucu ve uygulamalara ulaşamama gibi problemler çıkabilir. Hiyerarşik modeli kullanma giderleri de minimize etme yolunda katkı sağlar. Her katman için ihtiyaç olan uygun cihazı belirleme işi kolaylaşır. Böylece yüksek kapasiteli ürünlerden düşük performans değerler alma gibi sorunlar çok daha az olur. Modüler yaklaşımın getirdiği kolaylık ile sanki bir bulmacanın parçalarını yerine yerleştiriyormuşçasına kolay kurulum ve operasyon sürekliliği sağlanır. Kullanılmayan bant genişliği daha az olmakla birlikte her ekipmandan yüksek verim alabilmek, hem sistem ve network yöneticilerini hem de uygulamalara kesintisiz ve verimli olarak ulaşabilen kullanıcıları mutlu eder.

**Hiyerarşik Modelin Düz (Flat) Modele Göre Farkı:**

Düz modelde aktif network cihazları birbirlerine düz biçimde bağlanırlar. Bu dizayn biçimi daha çok küçük networkler için idealdir. Tasarımı ve yönetimi kolay olmasına karşın kapasite ve ölçeklenebilirlik çok düşüktür. Ağ tasarımı küçük kalacak ise bu yöntem denenebilir ancak bu tez çalışmasında da tasarlanan kurumsal bir şirketin network altyapısı için yetersizdir (Oppenheimer 2011, p.122).

**Şekil 3.5: Düz Yapı**

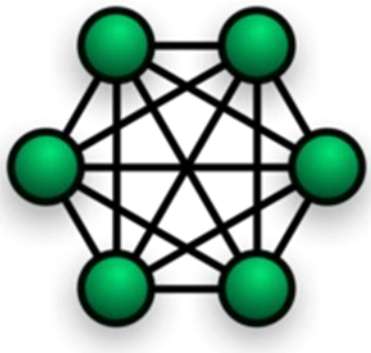



*Kaynak:* Oppenheimer 2011, p.122

**Hiyerarşik Modelin Örgü (Mesh) Modele Göre Farkı:**

Örgü topolojisi, ağdaki bütün uçların birbirine bağlı oldukları bir topoloji türüdür. Bu topoloji, karmaşık topoloji olarak da adlandırılır. Örgüde herhangi bir dağıtıcının kullanılmasına gerek yoktur. Çünkü her bilgisayar arasında mutlak bir bağlantı mevcuttur (Oppenheimer 2011, p.124). Diğer bir yandan yönlendirme işlemi, örgü topolojide önemli bir paya sahiptir. Yani veri paketlerinin izleyeceği yollar daha önceden tanımlanmış olmalıdır.

**Şekil 3.6: Örgü Yapısı**



Bu topoloji en güvenli ağ topolojisidir. Her nokta arasında bağlantı olduğu için veri aktarımı gizli yapılabilir. Örneğin; iki bilgisayar arasında veri alış verişi gerçekleşirken diğer bilgisayarlar bu verileri göremezler. Örgü tipi ağlarda iletişim her zaman vardır. Bu ağda herhangi bir bilgisayarın bozulması sadece o bilgisayarı etkiler. Yine herhangi bir kablonun kopması durumunda ağ çalışmaya devam eder, hiçbir bilgisayar ağ dışı kalmaz. Bu yüzden iletişim kopmasının tehlikeli olduğu durumlarda bu ağ tercih edilir. Mesh aynı zamanda kısa cevap zamanı sağlar. Hızlı olmasından ve yedekleme sağlamasından dolayı hat çöküntülerine karşı da dayanıklı bir yapıya sahiptir. Hiyerarşik modelin örgü modeline göre en büyük üstünlüğü de bağlantı kurulacak bilgisayar sayısı arttıkça kablo sayısının da katlanarak artmasıdır ki bu da karmaşıklığı ve maliyeti arttırır. Çünkü her yeni bir bilgisayar ile ağdaki diğer bilgisayarlar arasında ayrı ayrı hatlar kurmak gerekecektir. Bu yüzden örgü bağlantısı büyük çaplı ağlarda tercih edilmez. Daha çok özel durum gerektiren yerlerde ve küçük ağlarda kullanılır. Sınırlı bir kullanım alanına sahiptir; bu tez çalışmasında da tasarlanan kurumsal bir şirketin network altyapısı için yetersizdir.

#### *3.2.1.1 Üç Katmanlı Hiyerarşik Model*

Ağ mühendisleri, ağın dizayn edilmesini, kuruluşunu ve yönetimini kolaylaştırmak için hiyerarşik ağ modelini kullanırlar. Ağı kuran ve yöneten kişiler genellikle farklı olduğundan dolayı ağ dizaynı herkes tarafından anlaşılabilir bir şekilde modellenmesi önemlidir. Ağ kurulumları yapan mühendisler, dizayn edilen ağa hangi özelliklerde cihazların yerleştirileceğini belirleyebilmek için ağın dizaynını anlayabilmelidirler. Aynı şekilde ağ yöneticileri de kurulan ağı yönetirken çıkan aksaklıkları hemen giderebilmek için ağın dizaynını ve kullanılan cihazları bilmelidirler. Kullanıcıların farklı talepleri ve ağ üzerinde kullanılan karmaşık uygulamalar, ağ mühendislerini ağ kurarken belli bir strateji takip etmelerine zorlamıştır. Günümüzde özellikle büyük ağlarda kullanılan ortak uygulamalar ve bu uygulamaların ağın yoğunluğuna direkt etki etmesi, daha etkin bir yönlendirme ve anahtarlama tekniklerinin kullanılmasını gerektirmektedir (Clark & Hamilton 1999, p.124). Bütün bunlar ağdaki son kullanıcının ihtiyaç duyduğu servislerin gruplanması ve bu servisleri sağlayacak sunucuların doğru

konuşlandırılmasının gözetildiği bir stratejinin takip edilmesini gerektirir. Üç katmanlı hiyerarşik model bunları sağlamaktadır. Bu katmanlar şunlardır:

**Omurga Katmanı:**

Omurga katmanı, üç katmanlı hiyerarşik modelde yüksek kapasitede özelliklere sahip, sistemin omurgasına sahip yapıdır. Bu katmanın güvenilirliği en üst seviyede olduğu için, katman tasarlanırken yedekli yapı kullanılır. Bu sayede katmandaki ekipmanlar, yazılımsal ve donanımsal değişikliklere kısa sürede, hızlı bir biçimde uyum sağlamalıdır. Buradaki yönlendiriciler konfigüre edilirken paket iletim performansı en yüksek seviyede olacak şekilde ayarlanırlar. Aynı şekilde bu katmandaki anahtarlar da anahtarlama kapasitelerinin yüksekliği ile göze çarparlar. Bu sayede kullanıcıların isteklerine hızlı ve sorunsuz bir şekilde cevap verilmiş olunur. İnternet katmanı ya da uzak bağlantı ile bağlanacak kullanıcıların networkleri direk bu katmana bağlanırlar. Aynı zamanda veri merkezi yapısı da bu katmada doğrudan bağlandığı için paket alış verişlerinde dar boğazların önüne geçilir ve istekler herhangi bir beklemeye ve gecikmeye uğramadan ilgili birimlere iletilirler. Uzak bağlantılarda bağlantının çeşidine göre VPN ya da IPSec GRE gibi protokol ve uygulamalar kullanıldığında, bu katmanın önüne güvenlik fonksiyonları ile öne çıkan özelleşmiş cihazların konulmasında fayda vardır (IPS, IDS, Firewall).

**Dağıtım Katmanı:**

Bu katman omurga ve erişim katmanları arası bir geçiş konumundadır. Katmanın birçok rolü bulunmakla birlikte kaynaklara erişimin güvenlik nedenleri ile sınırlandırılması, belli bir servis seviysinde hizmet kalitesinin sağlanabilmesi için oluşturulan kalite servisi (QoS) uygulamaları ya da networkleri sanal olarak birbirinden ayıran sanal yerel alan ağlarının (VLAN) yönlendirme işlemleri gibi fonksiyonlar ön plana çıkar.

Performans kriterlerini de hesaba katarak network tasarımındaki dinamik yönlendirme protokolleri uygun bir biçimde bu katmanda uygulanabilir. Eğer yönlendirme protokolünü EIGRP olarak seçmiş isek, dağıtım katmanında da EIGRP'yi çalıştırmak mantıklı olabilir. Ancak çok daha basit algoritmaya sahip RIP gibi bir protokol kullanılıyorsa her komşu değişiklik bilgisinin bu katmana iletilmesi anlamsız olacaktır;

bu durumda RIP dinamik yönlendirme protokolünü erişim katmanına sınırlamak çözüm olabilir. Ya da; OSPF, BGP gibi daha gelişmiş algoritmalara sahip yönlendirme protokollerini tasarımımızda kullanıyorsak, daha yüksek performansa sahip omurga katmanında bu protokolleri koşturmak daha mantıklı olacaktır.

Hiyerarşinin, modülerliğin ve performansın yüksek seviyede tutulması isteniyorsa, dağıtım katmanı erişim katmanında parça parça bulunan tüm topoloji bilgisini, kendisinin bir üst katmanı olan omurga katmanından saklamalıdır. O katmana ya çok özet bilgilerle temel topoloji tasarımı ya da sadece statik yönlendirme ile tek yol bilgisi verilmelidir. Bu sayede omurga katmanı, asıl işi olan yüksek seviyede yönlendirme ve anahtarlama işine yoğunlaşabilecek, bu sayede performans ve verim açısından yüksek değerlere ulaşılabilecektir.

**Erişim Katmanı:**

Bu katman kullanıcıları lokal küçük segmentlere bağlayan bir aracı durumundadır. Bu katmanda da tasarıma göre yönlendiriciler ve anahtarlar bulunabilir. Ancak kablosuz erişim kontrol cihazları, IP telefonlar, görüntü çoklayıcıları, hublar ve hizmet alan bilgisayar, printer gibi cihazlar bu katmanda bulunurlar. Bu katmanda bant genişliği anlamında sorun olmaması için dağıtım katmanına bağlanan bağlantıların (uplink) uygun seçilmesinde yarar vardır. Sonra darboğaz, yetersiz performans, gecikme ya da paket kaybı gibi sorunlar ile karşılaşabilinir.

#### *3.2.1.2 Paralel Hiyerarşik Modelin Projeye Uygulanması*

Bir şirket binasının tüm zayıf akım network dizaynını yaparken öncelikle network topolojisi üzerinde çalışıldı. Genel yapıda:

i. 3 katmanlı hiyerarşik dizayn metodolojisi kullanılmıştır.

ii. Omurga bölümünde yüksek anahtarlama ve yönlendirme fonksiyonları ile ön plana çıkmış özelleşmiş cihazlar kullanılmıştır. Yedekli yapı kullanılmış, herhangi bir çalışmama durumunda sistem kendi içerisinde yedeklidir.

iii. Dağıtım katmanında omurga ve erişim katmanı arası geçiş için uygun cihazlar konumlandırılmıştır. Burada da yedekli yapı kullanılmış, herhangi bir çalışmama durumunda sistem kendi içerisinde yedeklidir.

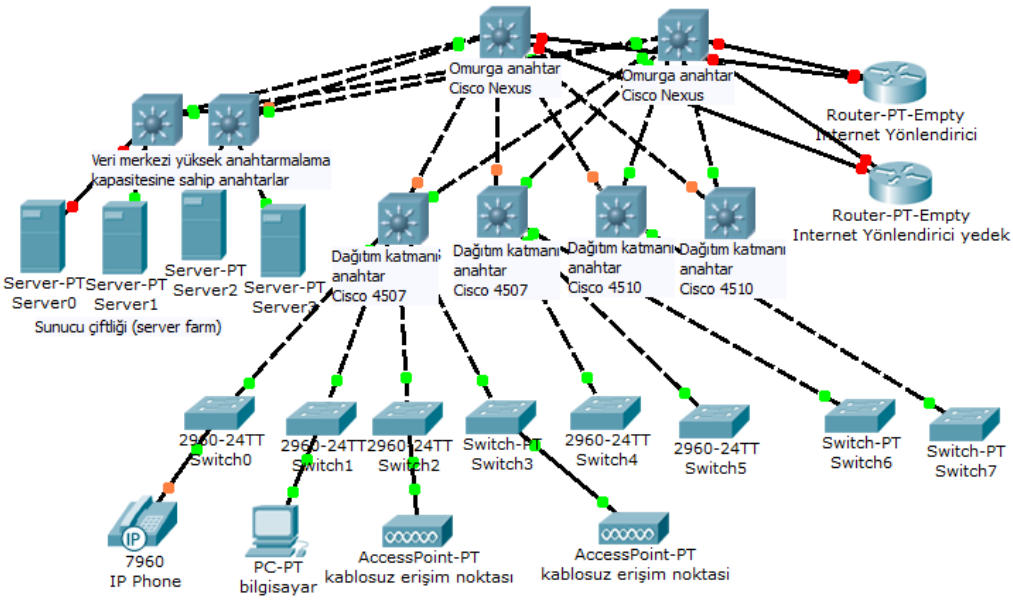
iv. Erişim katmanınında bilgisayar, IP telefon, kablosuz erişim noktası gibi uç cihazlara bağlantı verilmiştir. Buradaki bazı anahtarlar kullanılan teknolojiye göre Ethernet üzerinden gücü iletebilen (PoE) yapıdadır.

v. Güvenlik için güvenlik duvarı ve IPS konumlandırılmıştır.

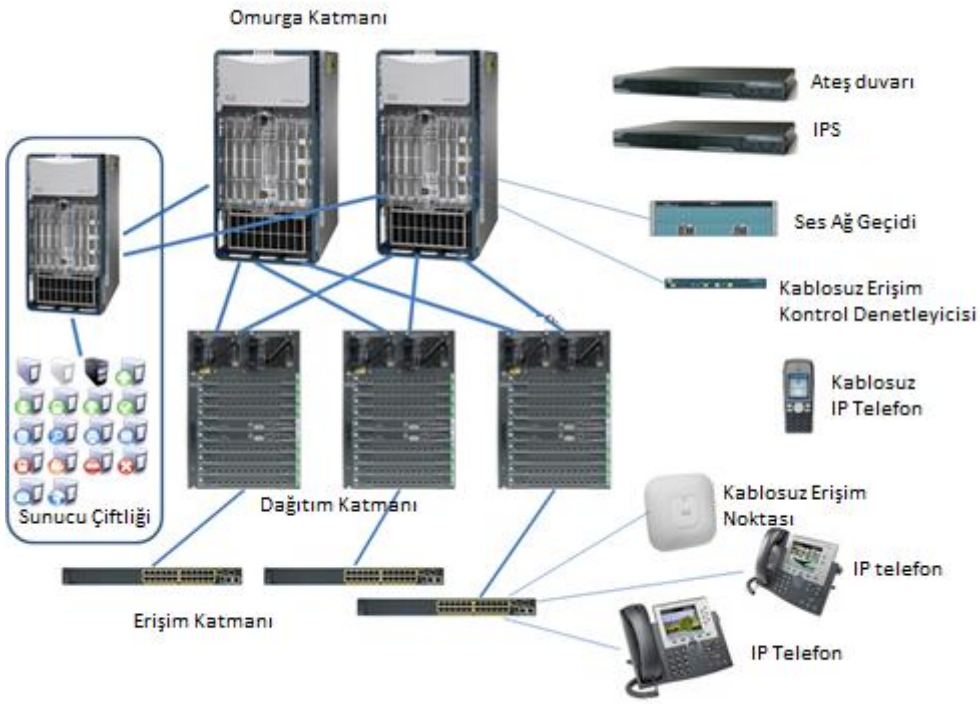
vi. Ses networkü için ses ağ geçitleri, IP telefonlar ve kontrol yazılımları konumlandırılmıştır.

vii. Kablosuz network yapısı için kablosuz erişim noktaları ve bunları kontrol eden WLAN kontrol cihazı konumlandırılmıştır.

**Şekil 3.7: Örnek bir şirket binası network topolojisi (diyagram)**



**Şekil 3.8: Örnek bir şirket binası network topolojisi (fiziksel)**




Buradaki her bir teknoloji ve cihazın ne amaçla konumlandırıldığı ilgili bölümde detaylı bir şekilde aktarılacaktır. Ayrıca teknolojiler ve çalışma mantıkları hakkındaki bilgiler de "Fiziksel Network Dizaynı" bölümünde eksiksiz bir biçimde aktarılacaktır.

### 3.2.2 ADRESLEME, İSİMLENDİRME VE NUMARALANDIRMA DİZAYNI

Bu bölümde adresleme, isimlendirme ve numaralandırmada paralel hiyerarşik yaklaşımı izlenerek nasıl çalışma yapıldığı anlatılacaktır.

### *3.2.2.1 IP Adresleme ve DHCP*

Her TCP/IP ana bilgisayarı mantıksal bir IP adresiyle tanımlanır. Bu adres TCP/IP kullanarak iletişim kuran her ana bilgisayar için benzersizdir. Her IP adresi kendi içinde iki bölüme ayrılır: Bir ağ kimliği ve bir ana bilgisayar kimliği. Her 32 bit'lik IP adresi, ağ üzerindeki bir ana bilgisayarın konumunu tanımlar. Ağ adresi olarak da bilinen ağ kimliği daha kapsamlı bir TCP/IP ağı içindeki ağlardan birini tanımlar. Aynı ağa eklenen ve erişimlerini paylaşan tüm sistemler kendi tam IP adreslerinin içinde ortak bir ağ kimliğine sahiptirler. Bu kimlik daha geniş bir ağın içindeki her ağı benzersiz olarak belirlemek için kullanılır. Ana bilgisayar adresi olarak da bilinen ana bilgisayar kimliği ağın içindeki bir TCP/IP düğümünü (bir iş istasyonu, sunucu, yönlendirici veya başka bir TCP/IP aygıtını) belirler. Her aygıtın ana bilgisayar kimliği, tek bir sistemi kendi ağı içinde benzersiz olarak belirler.

Internet topluluğu beş IP adres sınıfı tanımlamıştır. A, B ve C sınıflarındaki adresler TCP/IP düğümlerine atanmak için kullanılır. Adres sınıfı her adreste hangi bitlerin ağ ve ana bilgisayar kimlik bölümleri için kullanılacağını belirler. Adres sınıfı aynı zamanda bir ağda kaç tane ağ ve ana bilgisayar barındırılabileceğini belirler (Comer 2005, p.45).

**Tablo 3.1: IP Adres sınıfları**

| Sınıf | w değeri | Ağ kimliği | Ana bilgisayar kimliği | Ağ sayısı | Ana bilgisayar sayısı |
|---|---|---|---|---|---|
| A | 1-126 | w | x.y.z | 126 | 16,777,214 |
| B | 128-191 | w.x | y.z | 16,384 | 65,534 |
| C | 192-223 | w.x.y | z | 2,097,152 | 254 |
| D | 224-239 | Multicast | Yok | Yok | Yok |
| E | 240-254 | Deneysel kullanım | Yok | Yok | Yok |

Bir IP adresi içindeki ağ ve ana bilgisayar kimlikleri alt ağ maskesi kullanılarak ayrılır. Her alt ağ maskesi, ağ kimliğini belirlemek için hepsi birlerden (1) oluşan ardışık bit grupları ve ana bilgisayar kimliğini belirlemek için hepsi sıfırlardan (0) oluşan ardışık bit grupları kullanan bir 32 bit'lik sayıdır.

**Tablo 3.2 Alt ağ maskeleri**

| Adres sınıfı | Alt ağ maskesi için bitler | Alt ağ maskesi |
|---|---|---|
| A sınıfı | 11111111 00000000 00000000 00000000 | 255.0.0.0 |
| B sınıfı | 11111111 11111111 00000000 00000000 | 255.255.0.0 |
| C sınıfı | 11111111 11111111 11111111 00000000 | 255.255.255.0 |

BOOTP protokolünün daha gelişmiş hali olan DHCP protokolü tam dinamik bir yapıdadır ve sunucu-istemci ortamında çalışır. DHCP sunucuyu kullanarak IP adresi alacak bütün bilgisayarların otomatik olarak IP adresi alabilmesi için konfigürasyon yapılmalıdır. Ağdaki bir DHCP istemci çalıştırıldığında ortamdaki DHCP sunucudan direkt olarak IP adresi ister. Daha önceden DHCP sunucu üzerinde dağıtılacak IP adres aralıkları belirlendiğinden bu belirlenen adres aralığı içinden bir IP adresi ve alt ağ maskesi verilir. DHCP konfigürasyonu özelleşmiş bir sunucu üzerinde yapılabileceği gibi herhangi bir DHCP destekleyen yönlendirici, firewall, yük dengeleyici üzerinden de yapılabilir. DHCP mesajları altı çeşit olarak şöyle sıralanabilir (http://support.microsoft.com/kb/169289):

DHCP discovery; IP yapılandırması ayarlarını DHCP den alacak şekilde ayarlanan bir kullanıcı ilk olarak bu mesajı yollar mesaj 255.255.255.255 numaralı IP adresine yollanır yani istek tüm ağa broadcast yapılır. Bilgisayar mesajda bir DHCP sunucundan IP yapılandırması ayarlarını istediğini belirtir.

DHCP offer; DHCP Discovery mesajını alan sunucu isteği yollayan istemciye unicast olarak gerekli yapılandırmayı yollar.

DHCP request; DHCP offer istemciye bir çok sunucu tarafından yapılmış olabilir fakat istemci sadece bir tanesini kabul eder. Hangi sunucudan gelen isteği kabul ettiğini bildirmek için de ağa broadcast olarak DHCP request paketi yollar. Bu paketin Transaction ID bölgesi sayesinde sunucular hangi sunucunun teklifinin kabul edildiğini anlar.

DHCP acknowledgment; DHCP sunucusu DHCP Request mesajını aldıktan sonra sunucu istemciye DHCP ACK paketini yollar, bu paket içinde gerekli yapılandırma, lease süresi gibi bilgileri içerir.

DHCP Information; Istemci sunucudan bazı konularda ekstra bilgiler isteyebilir. Örneğin; WPAD ile web proxy kullanımında bazı ekstra bilgilere ihtiyaç vardır.

DHCP releasing; İstemcinin kendisine DHCP sunucusu tarafından atanan IP adresini kullanmayı bıraktığı zaman sunucuya bu IP adresini artık kullanmadığını belirtmek için yolladığı pakettir.

#### *3.2.2.2 Yönlendirme Protokollerinin Özetlenmesi*

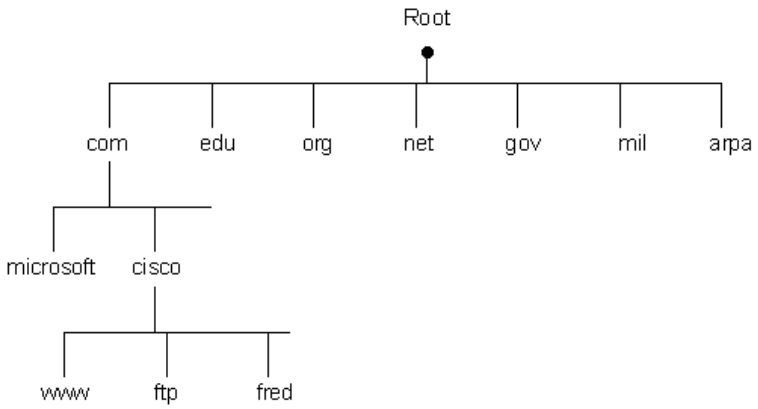
Rota özetleme, birden fazla rotanın bilgisinin tek bir rota halinde iletilmesidir. Örneğin bir LAN 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24 şeklinde üç alt networkten oluşuyor olsun. Bu networklerin bilgileri diğer bağlantı noktasına gönderilirken ayrı network yerine tek bir network olarak gönderilebilir. 192.168.0.0/22 olarak gönderildiğinde bu dört network de kapsanmış olur. Böylece daha küçük yönlendirme tabloları oluşur ve daha efektif bir yönlendirme işlemi gerçekleştirilebilir. Bu networkler öyle bir şekilde özetlenmelidir ki hem alt ağ maskesi minimum değişmeli, hem de tüm networkler bu alt ağın içine katılmalıdır. Bu nedenle IP adreslerinde değişen 8li bitler, ikilik düzende açılır. İkilik düzene açıldığında, en sağdaki 3 bitin devamlı değiştiği görülür. Bu değişen 3 bit alt ağ maskesine alınır. Böylece 24 bit olan alt ağ maskesi 21 bit olmuştur. Bu şekilde 8 adet network tek bir

network olarak gösterilebilir. Yönlendirme güncelleştirme bilgilerinin sayısı azaltılabilir.

### *3.2.2.3 DNS*

DNS (Domain Name System), internet ortamında alan adı-IP, IP-alan adı dönüşümlerini gerçekleştiren sistemdir. DNS sunucuları, URL (Uniform Resource Locator) ya da FQDN (Fully Qualified Domain Name) olarak adlandırılan adreslerin IP'lere çözümlenmesini sağlarlar. Bu işlem, hatırlaması zor olan IP adreslerini kullanmak yerine, hatırlaması daha kolay olan host isimlerinin kullanımına izin verir. DNS host isimleri ile IP adresleri arasında çift taraflı dönüşüm sağlayan dağıtık bir veri tabanıdır. DNS veri tabanı sistemi en tepede kök (root) sunucularının yer aldığı ağaç yapısındadır. Ağaç yapısındaki dallanma maksimum 127 basamaktır. Her nokta maksimum 63 karakterden oluşabilmektedir. DNS sisteminde kök nokta (.) ile gösterilir. Veri tabanı üzerindeki her bir alt nokta "domain"; bu domainden kollara ayrılan her bir parça ise "alt domain" olarak adlandırılır. Bir adres en alttan köke gelecek şekilde gösterilir. Aynı düğüm altındaki düğümlerin farklı isimde olması gerekir. Böylelikle domain adları tek olması sağlanmış ve olası çakışmalar önlenmiş olur.

**Şekil 3.9: DNS isimlendirmesi**




*Kaynak:* http://www.comptechdoc.org/independent/networking/guide/netdns.html

DNS sisteminin en üstünde bulunan kök sunucuları internet ortamında kritik bir rol üstlenmektedirler. Çünkü host isimleri-ip dönüşümü ilk olarak kök sunucularında başlar. Kök sunucuları Üst Düzey Alan (TLD) sunucularının adresini bilirler ve gelen istekleri gerekli TLD sunucularına yönlendirirler. Internet üzerindeki isim çözümlemesinin doğru, güvenli ve devamlı olması için kök sunucular gereklidir. Dünya üzerinde isim bazında 13 tane kök sunucu bulunmaktadır (Albitz ve Liu, 2006, p.117). DNS domain uzayında ilk görev paylaşımı TLD'ler seviyesinde gerçekleşir. 2009 Ocak ayındaki verilere göre 20 adet jenerik TLD(gTLD) ve 248 adet ülke kodlu ccTLD (country code TLD ) bulunmaktadır. Belli başlı TLD'ler ve açıklamaları şunlardır:

**Şekil 3.10: Ülkelere ve kurumlara göre DNS isimlendirmesi**

| | | | |
|---|---|---|---|
| com | Ticari Kuruluşlar | tr | Türkiye |
| org | Ticari Olmayan Kuruluşlar | us | Amerika |
| mil | Askeri Kurumlar | gb | İngiltere |
| net | Network Organizasyonları | de | Almanya |
| edu | Eğitim Kurulumları | au | Avustralya |
| gov | Hükümet Kurumları | fr | Fransa |
| int | Uluslararası Kurumlar | it | İtalya |
| info | Bilgi Servisleri | ca | Kanada |
| name | Bireysel Kullanım | ru | Rusya |
| tel | İnternet, İletişim Servisleri | es | İspanya |

### *3.2.2.4 Telefon Numaralandırması*

Numaralandırma planı tasarımda kullanılan IP telefonlar için hem lokalde telefonların birbirlerini arayabilmeleri hem de PSTN ve mobil şebekelere çıkışta kullanacakları adres şeması olarak özetlenebilir. Nasıl ki IP adreslemesinde belli bir plan dahilinde IP adresi numaralandırması yapılıyorsa, telefon numaralandırmasında da böyle bir yapılandırma gereği duyulur. Müşterinin kendi lokasyonu ya da lokasyonları arası numaralandırma planı o kurumun alt birimleri, müdürleri, yöneticiler ya da çalışanlarına özgü jenerik bir planlama olmalıdır. Bu da fiziksel topoloji tasarımı bölümünde daha derinlemesine incelenecektir.

Lokal numaralandırma planlamasında müşterinin birimleri mantıksal bir yapı çerçevesinde numaralara ayrılır. Bu sistematik bir işlem olduğundan yapılandırması bir

zorluk teşkil etmemekte, ölçeklenebilirlik anlamında da yapıların büyümelerini göz önüne alacak şekilde tasarlanmalıdır. Müşterinin günümüz Türkiye'sinde hizmet alacağı sabit telekomünikasyon altyapılarına sahip olan Türk Telekom, Superonline gibi şirketlere kendi trafiklerini göndermeleri için çevrilen numaralara bir önek koyulmaktadır. 00[ülke_kodu]…… şeklindeki aramalar başka ülkede bulunan telefon numaralarına erişmekte kullanılır. 0[il_kodu]……. şeklindeki arama formatı şehirlerarası numaralara erişmekte kullanılırken, ……. şeklindeki arama formatı ise şehir içi haberleşmeyi sağlamada önemlidir. Mobil şebekelere çıkışta 0[5..]……. formatı ile ulaşılabilir. Buradaki [5..] ifadesi hangi mobil operatöre çıkış yapılacak ise ona uygun değişiklik göstermektedir.

Hizmet alan kişi ya da kurumlar istenildiği taktirde IP ara yüzü üzerinden sesi taşıyabilecek operatörlere de ses çıkışlarını yönlendirebilirler. Bunun için kurum ve servis sağlayıcının anlaştığı bir önek ile ses çıkışının yapıldığı ses ağ geçidi üzerinden servis sağlayıcının networküne direk girecek bir IP bağlantısına ihtiyaç vardır.

#### *3.2.2.5 Adresleme, İsimlendirme ve Numaralandırma Dizaynının Projede Uygulanması*

Bu bölümde tez çalışmasında detaylı olarak yer verilen şirketlerin yönetim binaları tüm zayıf akım network dizaynı projesinde tasarlanan adresleme, isimlendirme ve numaralandırma çalışmaları yukarıda bahsedilen teorik bilgiler ve yaklaşımlar ile harmanlanıp uygulanmıştır.

Adresleme için 10.0.0.0 networkü C sınıfı alt networklere bölünmüş, kimi zaman alt ağ maskesi değerinde oynamalar yapılıp kullanılan IP sayısı daha az ve daha verimli harcanmıştır.

i. Masaüstü kullanıcılara 10.0.1.0/24 ile 10.0.255.0/24 networkleri arası IP bloğu tahsis edilmiştir.

ii. Mobil kullanıcılara 10.1.1.0/24 ile 10.1.255.0/24 networkleri arası IP bloğu tahsis edilmiştir.

iii. Network cihazlarında ilgili ağdaki IP adreslemesine uygun .1 - .5 IP'leri arası IP'ler yönetim amaçlı verilmiştir.
iv. Sunucu çiftliği (Server farm) için 10.10.10.0/24 ile 10.10.255.0/24 networkleri arası IP bloğu tahsis edilmiştir.

DNS isimlendirmesi için TEKxxx[….] notasyonu kullanılmış ve dünyada kullanılan kullanıma açık DNS sunucular ile entegrasyon sağlanmıştır.
i. Pazarlama bölümündeki makineler için TEKxxxPAZ00017 gibi bir notasyon kullanılmıştır.
ii. DNS sunucular hem Türkiye'de hem de dünyada kullanılan aşağıdaki DNS sunucular ile entegre edilmiştir:

Telefon numaralandırma formatı için şu notasyon kullanılmıştır:
i. Müdürler için 10[..]
ii. Yöneticiler için 1[1-2][..]
iii. Satış için 13[..]
iv. Pazarlama için 14[..]
v. Teknik ekip için 19[..]
vi. Finans için 1[5-6][..]
vii. Diğer 1[7-8][..]

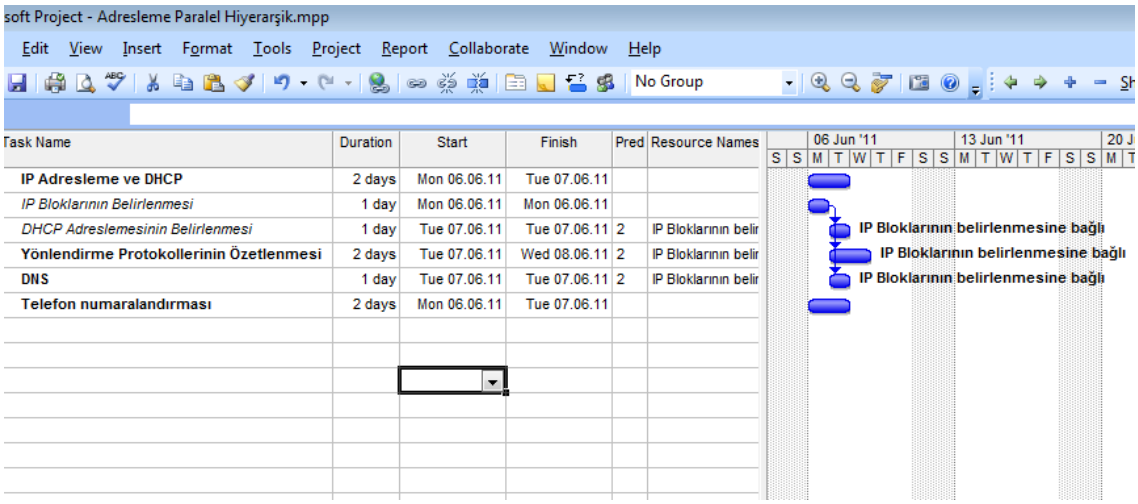
Şirket içi haberleşme 4 haneli 1[...] tuşlaması ile yapılır.
Dışarı çıkışlarda 0 hat almak için kullanılır.
i. Örneğin şehir içi aranacaksa 0[…….]
ii. Şehirler arası arama yapılacaksa 00[alankodu][…….]
iii. Cep telefonu aranacak ise 05[..][…….]
iv. Milletler arası arama yapılacak ise 00[ülkekodu][alankodu][numara] şeklinde tuşlama yapılabilir.

#### *3.2.2.6 Adresleme, İsimlendirme ve Numaralandırma Dizaynında Paralel Hiyerarşik Yaklaşımın Sonuçları*

Adresleme, isimlendirme ve numaralandırma olarak anlatılan konsept, aslında tüm dizaynın çatısını oluşturan hiyerarşidir. IP adresleme ve DHCP, yönlendirme protokollerinin özetlenmesi, DNS ve telefon numaralandırması olarak bölümlere ayrılmıştır. IP adresleme ve DHCP, IP adresi bloklarını ve hiyerarşisini belirlemek, DHCP dizaynını da buna uygun yapabilmek için tanımlanmıştır. Hangi bölüm hangi IP adres bloğunu kullanacak, güvenlik kriterlerine göre IP blokları nasıl bölünecek, DHCP server dizaynında ayrı bir DHCP server mı kullanılacak yoksa var olan yönlendiriciler üzerinden mi IP adres dağıtımı yapılacak gibi sorulara yanıt aranmaya çalışılmıştır.
Paralel hiyerarşik yaklaşımın sonuçlarını bu bölümde görebilmek için hazırlanmış proje planlarına ve zaman-maliyet gibi faktörleri konu alan proje analiz dokümanlarına bakıldığında yukarıdan aşağıya yaklaşımın ya da örgü yaklaşımın yapamadığı sonuçlar ortaya çıkmıştır.

Paralel hiyerarşik yaklaşım kullanılarak yapılan proje planında 4 ana kaleme ayrılmış olan bölümlerden IP adresleme ve DHCP'nin 2 gün süreceği varsayılmıştır. Bu bölümdeki 2 alt başlık olan IP bloklarının belirlenmesi ve DHCP adreslemesinin belirlenmesi olayları birbirlerine bağımlı işler olduğundan sıraya konulmak mecburiyetindedirler. Dayısıyla birer gün harcanarak toplanda iki günde IP adresleme ve DHCP dizaynı tamamlanabilir.

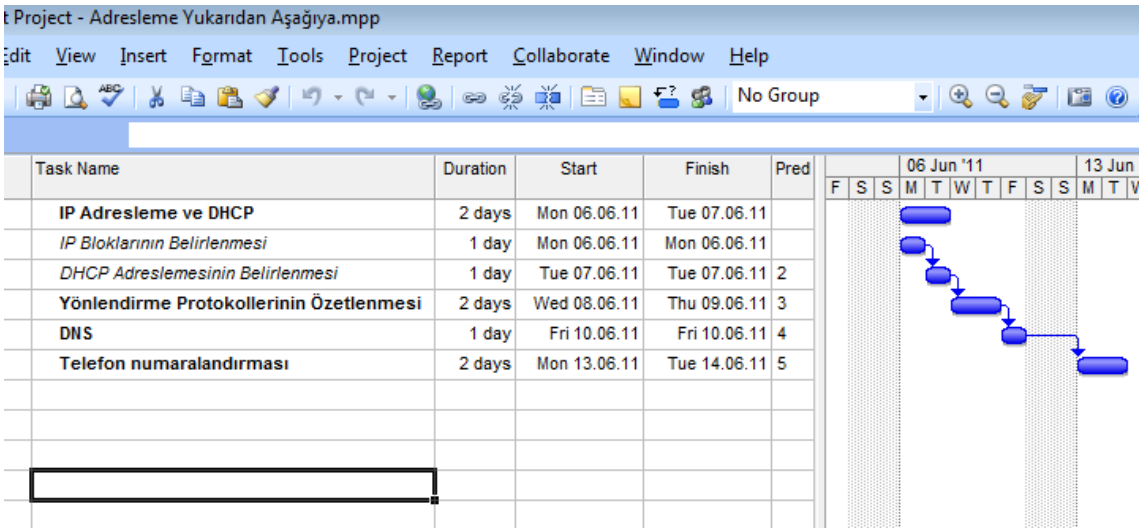
**Şekil 3.11: Paralel Hiyerarşik yaklaşımın Adresleme, İsimlendirme ve Numaralandırma dizaynındaki sonuçları**




Yönlendirme protokollerinin özetlenmesi işlemi yönlendirme güncellemelerinde hangi IP bloklarının güncelleştirmeler içerisinde gönderileceğini belirleme işlemidir. Bu adımın gerçekleştirilebilmesi IP adres bloklarının belirlenmesi ön koşulunu beraberinde getirir ancak DHCP'nin belirlenmesine bağlı değildir. Dolayısıyla plan buna göre hazırlanmıştır.

DNS dizaynında da IP adres bloklarının belirlenmesine ihtiyaç duyulduğundan proje planındaki zaman çizelgesinde ona bağlanmıştır ve işlem bir günde tamamlanmıştır.
Telefon numaralandırması diğer hiçbir işlemle bağımlılığı bulunmayan bir adım olmakla birlikte iki gün süren paralel bir çalışma ile tamamlanabileceği öngörülmüştür.
Bu çalışmada "Paralel Hiyerarşik Yaklaşım" yerine "Yukarıdan-Aşağıya hiyerarşik yaklaşım" kullanılsaydı her bir adım teker teker dizayn edileceği için paralelde üzerinde çalışılacak adımlar azalacak, dolayısıyla iş gücü gereksinimi de azalacaktır. Ancak işi bitirebilme zamanı uzayacak, hem iş gücü motivasyonu hem de projenin zamanında teslimi gibi konularda olumsuzluklara yol açacaktı. Bundan hareketle paralel hiyerarşik yaklaşımın, proje teslim süresi konusunun kritik olduğu işlerde kullanılması konusu önem kazanmaktadır.

**Şekil 3.12: Yukarıdan Aşağıya Hiyerarşik yaklaşımın Adresleme, İsimlendirme ve Numaralandırma dizaynındaki sonuçları**




Paralelde çalışan ekip sayısı azalmış ancak zaman çok etkin kullanılamamış ve dolayısıyla işi bitirme süresi gözle görülür ölçüde artmıştır. Paralel hiyerarşik yaklaşımın kullanılmasıyla proje planına göre yüzde 60 civarında zamandan verim sağlanmış, ancak işgücünde de yüzde 30 civarında artış olmuştur.

### 3.2.3 ANAHTARLAMA VE YÖNLENDİRME PROTOKOLLERİNİ BELİRLEME

Bu bölümde anahtarlama ve yönlendirme protokollerinin belirlenmesi ile ilgili önce teorik bilgilere yer verilecek, daha sonra ise uygulamada kullanımına yönelik sonuçlar paylaşılacaktır.

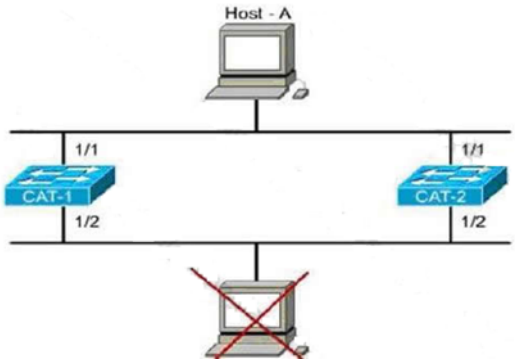
#### *3.2.3.1 Anahtarlama Protokollerini Belirleme*

Anahtarlama protokolleri çeşitlilik göstermekle birlikte amaca ve dizayna uygun protokolün seçilmesi bu bölümde anlatılacakların temelini oluşturmaktadır.

### *3.2.3.1.1 STP*

Spanning-Tree anahtarların haberleşmesi sırasında oluşabilecek döngüleri (loop) önleyen bir protokoldür. Spanning-Tree genel olarak anahtarlar üzerinde döngüyü dinamik olarak önler, ve anahtarlarda ilk konfigürasyonda açık durumdadır. Protokol networklerde döngüye neden olabilecek portları kapalı duruma alarak çalışır (Hucaby 2005). Her hedefe sadece bir yolun aktif olarak çalışmasını sağlar.

**Şekil 3.13: STP Bloklama**




*Kaynak:* http://www.ciscozine.com/2009/01/19/preventing-stp-forwarding-loops/

Şekildeki yapıda anahtarlar kendilerine gelen ve hedef adresi bilinmeyen paketleri diğer tüm portlarından geçireceklerdir. Cat 1 ve Cat 2 anahtarları 1/1 portlarına gelen paketleri geçirecek ve ayni paketleri 1/2 portlarından alacaklardır. 1/2 portundan aldığı bu paketleri 1/1 portlarından geçirecek, yine diğer portlardan alacak bu böyle durmadan devam edecektir.

Durmadan devam etmekten kasıt, anahtarların işlemci değerleri zamanla artacak ve bir süre sonra hizmet veremeyecek duruma geleceklerdir. Peki neden belirli bir süre sonra durmamaktadırlar? Çünkü ethernet paketleri (frame) TTL (Time to live) alanina sahip değillerdir. Bu yaşam döngüsü değeri paketlerde olmadığından dolayı sonsuza kadar döngü işlemi devam etmektedir. Pratik anlamda ise hizmet veremeyene kadar ya da döngüye neden olan durumu ortadan kaldırmadıkça problem devam edecektir. Durmadan devam etmekten kasıt, anahtarların işlemci değerleri zamanla artacak ve bir süre sonra hizmet veremeyecek duruma geleceklerdir. Peki neden belirli bir süre sonra

durmamaktadırlar? Çünkü ethernet paketleri (frame) TTL (Time to live) alanina sahip değillerdir. Bu yaşam döngüsü değeri paketlerde olmadığından dolayı sonsuza kadar döngü işlemi devam etmektedir. Pratik anlamda ise hizmet veremeyene kadar ya da döngüye neden olan durumu ortadan kaldırmadıkça problem devam edecektir.

STP algoritması ağda döngülerin oluşmasını önlemektedir. Anahtarlar belli aralıklarla uzatılmış ağaç topolojisi belirlemek için mesajlaşırlar. Bu mesajlara BPDU (Bridge Protocol Data Units) denir. STP topolojisi oluşturulurken anahtarların her bir portu belli durumlara sokulur. Bu durumlar şunlardır;

Bloklama (Blocking): Data gönderilmez ve BPDU mesajları dinlenir.
Dinleme (Listening): Data gönderilmez fakat datanın ulaşıp ulaşmadığı dinlenir.
Öğrenme (Learning): Data gönderilmez ve adresler öğrenilir.
Gönderme (Forwarding): Data gönderilir ve adresler öğrenilir.
Kapama (Disabled): Data gönderilmez ve BPDU mesajları dinlenmez.

**Şekil 3.14: BPDU frame yapısı**

| ALAN | BYTE |
|---|---|
| Protokol Kimliği (Protocol Identifier) | 2 byte |
| Versiyon (Version) | 1 byte |
| Mesaj Tipi (Message Type) | 1 byte |
| Bayraklar (Flags) | 1 byte |
| Kök ID (Root ID) | 8 byte |
| Kök Değeri (Cost to Root) | 4 byte |
| Köprü ID (Bridge ID) | 8 byte |
| Port ID | 2 byte |
| Mesaj Yaşı (Message Age) | 2 byte |
| Maksimum Yaş (Maximum Age) | 2 byte |
| Merhaba Zamanı (Hello Time) | 2 byte |
| Gönderme Gecikmesi (Forward Delay) | 2 byte |

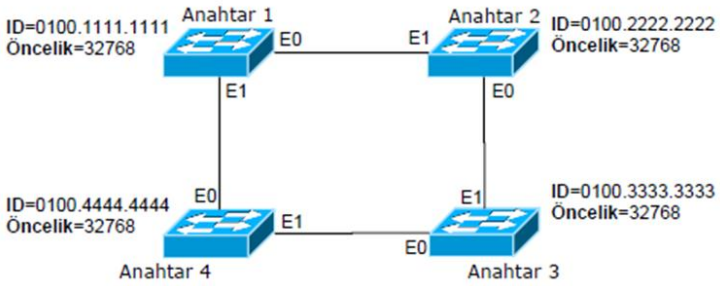
Kaynak: http://docstore.mik.ua/univercd/cc/td/doc/product/lan/trsrb2/frames.pdf

STP topolojisi üç adımdan oluşturulmaktadır.

1. Kök anahtarı (root bridge) seçme:

Topoloji oluşturulurken bütün portlar blok durumundadır. STP topolojisi oluşturulduğunda ise portlar ya blok veya gönderme durumu olarak konfigüre edilirler.

**Şekil 3.15: STP Çalışması**



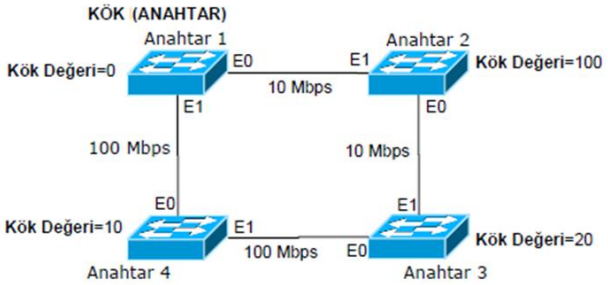

Bütün cihazlar ilk başta kendilerini kök anahtar olarak belirten BPDU mesajlarını birbirlerine gönderirler. Bu mesajlar önemli bilgiler içermektedir. Her cihaz kendini kök köprü olarak kabul ettiği için kök anahtar bilgisi içeresinde kendi bilgilerini yazar.

BPDU mesajları bütün cihazlar tarafından gönderildikten sonra kök anahtar cihazların öncelik değeri küçük olana göre seçilir. Eğer bütün cihazların öncelik değerleri eşit ise anahtarların MAC adresleri karşılaştırılır. MAC adresleri tek olduğu için mutlaka biri küçük olacaktır. MAC adresi küçük olan anahtar, kök anahtar olarak seçilir. Kök anahtar seçildikten sonra gönderilen BPDU mesajlarında her cihaz kendini kök anahtar olarak belirtmeyi durdurarak kök anahtar olarak seçilen anahtar belirtilir. Örnekte
1.nci köprü kök anahtar olarak seçilecektir. Kök anahtarın bütün portları gönderme durumuna dönüştürülerek bu portlardan veri göndermesine izin verilmektedir.

2. Kök portları (root port) seçme:

Anahtarlar, kök anahtara olan bağlantıların kök değerlerini hesaplarlar. Diğer anahtardan aldıkları BPDU mesajlarının kök değer alanına hesapladıkları kök değerlerini ekleyerek başka bir anahtara BPDU mesajı gönderirler. Aldıkları porttan mesajları geri göndermezler. Kök değerleri, 1000'in portların bağlı oldukları ortamın bant aralığına bölünmesiyle hesaplanır. Örneğin; ortam Ethernet ise kök değeri 1000/10=100, ortam Fast Ethernet ise kök değeri 1000/100=10'dur.

**Şekil 3.16: STP Çalışması -2**




Her cihaz, kök değerinin en küçük olduğu hattı belirler. Bu hatta bağlı olan portu kök port olarak seçer ve gönderme durumuna getirir. Buna göre ikinci anahtarın E1, üçüncü anahtarın E0 ve dördüncü anahtarın E0 portları kök port olarak konfigüre edilir. Kök portlar gönderme durumuna dönüştürülerek sadece veri göndermesine izin verilir.

3. Atanmış portları (designated port) seçme:

Son adımda ise kök port olmayan diğer portların blok ya da gönderme durumlarından hangisine dönüştürüleceğine karar verilmektedir. Cihazlar arasındaki segmentler incelenirse daha önce de bahsedildiği gibi kök anahtarın bütün portları ve diğer anahtarların kök portları gönderme (forwarding) durumuna getirilmişti. Gönderme durumuna dönüştürülmeyen diğer portlar ise şöyle incelenebilir:

Birinci ve ikinci anahtar arasındaki segment incelenirse, 1.nci anahtarın E0 portu kök anahtarın portu olduğu için, ikinci anahtarın E1 portu kök port olduğu için gönderme modundadır. ikinci ve üçüncü anahtar arasındaki segment incelenirse, ikinci anahtarın E0 portunun kök değeri 100; üçüncü anahtarın E1 portunun kök değeri 200'dür. Bu iki porttan en küçük kök değerli olan port atanmış port (designated) olur. Yani ikinci anahtarın E0 portu atanmış port olur ve gönderme (forwarding) durumuna getirilir. Segmentteki diğer port (üçüncü anahtarın E1 portu) blok durumuna getirilir. Birinci anahtar ile dördüncü anahtarı incelenirse, birinci anahtarın E1 portu kök anahtarın portu olduğu için, dördüncü anahtarın E0 portu kök port olduğu için gönderme (forwarding) modundadır. Üçüncü ve dördüncü anahtar arasındaki segmentte ise üçüncü anahtarın E0 portu kök portu olduğu için gönderme (forwarding) modundadır. Segmentteki diğer port da (dördüncü anahtarın E1 portu) atanmış port (designated) olur ve gönderme (forwarding) moduna dönüştürülür.

#### *3.2.3.1.2 VTP*

VTP'ye değinmeden önce VLAN'lar hakkında biraz bilgi verilmesi doğru olacaktır.

Sanal Lokal Ağ, bir veya birden fazla anahtarlarla oluşturulan bir broadcast etki alanıdır. Bilgisayarların fiziksel lokasyonlarına bağlı olmaksızın fonksiyon, departman veya kullandıkları uygulamalara göre mantıksal olarak gruplandırılarak oluşturulan ağdır. Ağda broadcast iletişim kurulmak istendiğinde anahtarlar bütün portlardan broadcast yayacaklardır. Bu broadcast yayınlarının etki alanını küçültmek ve oluşturulan yeni etki alanlardaki broadcast yayınların diğer etki alanlarını etkilememesi için sanal lokal ağlar oluşturulur. Her bir VLAN kendi STP topolojisini de oluşturmaktadır. VLAN teknolojisini kullanmaksızın lokal ağda segmentasyon, bilgisayarların bulunduğu lokasyona bağlı olarak yapılabilmektedir. Fakat VLAN teknolojisi ile bu zorunluluk ortadan kalkmaktadır. Klasik segmentasyonda sadece aynı lokasyonda bulunanları tek bir segmentte birleştirerek broadcast etki alanı oluşturulabilmektedir. Fakat VLAN teknolojisi ile farklı lokasyonlarda bulunan bilgisayarlar tek bir broadcast etki alanında birleştirilebilmektedir.

VTP, ortak yönetimin yapıldığı ağdaki aktif cihazların VLAN konfigürasyonunda tutarlılık sağlanabilmesi için kullanılan ikinci katman mesajlaşma protokolüdür. VTP, çoklu anahtar ortamındaki VLAN eklenmesi, silinmesi ve isim değişikliğini yönetir. Ayrıca VTP, oluşabilecek yanlış konfigürasyonları veya isim tekrarlanması gibi hataları minimuma indirir. VTP, 2 farklı versiyona sahiptir. VTP versiyon 1, sadece ethernet'i desteklerken, VTP versiyon 2 Ethernet ve Token Ring ağları desteklemektedir (Spohn 2002, p.51).

Çoklu anahtar ağ ortamında tek bir VTP etki alanı oluşturulur ve bütün anahtarlar aynı etki alanında toplanır. Böylece bu etki alanındaki bütün anahtarlar VTP sunucu modundaki anahtar tarafından üretilen mesajlarla ağın VLAN konfigürasyonu hakkında bilgilendirilir. Bu mesajlar beş dakikalık periyotlarla veya VLAN konfigürasyonunda bir değişiklik yapıldığında gönderilir. VTP mesajlarında VLAN isimleri ve numaraları, hangi anahtarın portları hangi VLAN'e atandığına dair bilgiler ve konfigürasyon

revizyon numarası bulunmaktadır. VTP sunucu, yeni bir mesaj ürettiği zaman bir önceki revizyon numarasını bir artırarak mesajı etki alanındaki bütün anahtarlara gönderir. Mesajı alan her bir anahtar, yeni mesajın revizyon numarası ile daha önce almış olduğu mesajın revizyon numarasını karşılaştırır. Yeni mesajın revizyon numarası daha büyükse içindeki bilgileri alarak VLAN bilgilerini günceller.

Anahtarlarda VTP 3 farklı modda çalışır. Bunlar;

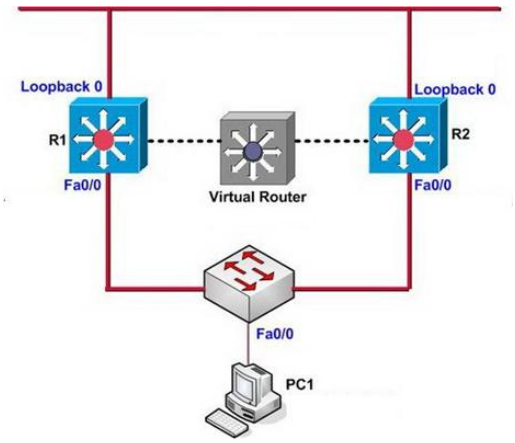
i. VTP sunucu mod: VTP sunucuları, VLAN oluşturabilir, silebilir ve değiştirebilirler. Ayrıca bütün bir etki alanı için diğer bütün konfigürasyon parametrelerini değiştirebilirler. VTP sunucuları, VLAN konfigürasyon bilgilerini NVRAM'de saklarlar. VTP sunucuda VLAN konfigürasyonu ile ilgili yapılan bir değişiklik dinamik olarak bütün trunk bağlantılardan aynı VTP etki alanındaki bütün anahtarlara gönderilir.
ii. VTP istemci mod: VTP istemciler, VLAN oluşturamaz, silemez ve konfigürasyon bilgilerini değiştiremezler. Ayrıca VLAN konfigürasyon bilgilerini NVRAM'de saklayamazlar. VTP istemci, VLAN konfigürasyon bilgilerini RAM'de sakladığı için VTP sunucunun çalışmadığı durumlarda VLAN konfigürasyon bilgileri halen kullanılabilir olacaktır. Fakat VTP sunucunun çalışmadığı durumlarda VTP istemci anahtar kapanıp açılırsa RAM'deki bütün konfigürasyonu kaybedeceği için VLAN konfigürasyonları etkin olmayacaktır.
iii. VTP şeffaf mod: Bu moddaki anahtar, mevcut VTP etki alanının bir üyesi değildir. Bu moddaki anahtar, VTP mesajlarını VTP etki alanına üye diğer anahtarlara iletmektedir. Şeffaf moddaki anahtarda yeni bir VLAN oluşturulabilir, silinebilir veya değişiklik yapılabilmektedir. Fakat bu değişiklikler mevcut etki alanına ait olmadığı için diğer anahtarlara iletilmez, sadece değişiklik yapılan anahtarı etkiler. Yapılan bütün değişiklikler NVRAM'de saklanır.

#### *3.2.3.1.3 HSRP/VRRP*

Günümüzde network ile uğraşan hemen herkes, Layer 3 çalışan ve networkun merkezinde yer alan bir cihazın herhangi bir sebepten dolayı çok az bir süreliğine de

olsa çalışmasını durdurmuş olmasının tahammül edilebilir bir durum olmadığını bilir. Bu sebepten de, Internet uygulamalarının ya da VoIP kullanımının giderek yaygınlaşmasıyla birlikte yedekliliğin önemi çok daha artmıştır. Yani bu, merkez cihazda bir problem olsa bile buna alternatif olarak çalışabilecek bir cihazın daha olması anlamına gelir. HSRP, Layer 3 anahtarların yedeklilikten faydalanarak işlem yapamama sürelerinin mümkün olduğunca azaltılmasını, hatta neredeyse sıfıra kadar indirilmesini sağlayan birkaç protokolden sadece birisidir. Bu sayede cihazların kısa bir süre çalışamamasından kaynaklı problemlerin çözümünde büyük ölçüde ilerleme kaydedilmiştir. Layer 3 anahtarlarda bu yedekliliği sağlamak için sadece HSRP kullanılmaz. Diğer protokoller VRRP (Virtual Router Redundancy Protocol) ve GLBP (Gateway Load Balancing Protocol)'dir. HSRP Cisco'ya ait bir protokoldür.

**Şekil 3.17: HSRP Çalışması**




HSRP'de iki anahtardan birisi 'Active' diğeri ise 'Standby' olarak çalışır. Yani bir tanesi aktif işlemleri yerine getirip paketleri hedeflerine ulaştırırken, diğeri bu anahtarı takip ederek herhangi bir aksaklık durumunda aktif olanın yerine geçmek için yedekte beklemektedir. Şekildeki iki Layer 3 anahtar her üç saniyede bir birbirlerine merhaba paketi göndermektedirler, her paket gönderildikten sonra merhaba zamanı çalıştırılır ve üç saniye sonunda yeni bir merhaba paketi gönderilir. 'Standby' durumunda olan cihaz 'Active' cihazın 10 sn. boyunca hiç merhaba paketi göndermemesi durumunda yönetimi devralıp kendini aktif anahtar olarak ilan eder ve aktif işlemleri kendisi yürütmeye başlar. Bununla birlikte, başlangıçta aktif olan cihaz 'Standby' durumuna geçer. Her ne kadar merhaba zamanı 3, bekleme zamanı 10 saniye olarak daha önceden belirtilmiş

değerler olsa da, bu değerleri değiştirmek mümkündür. Çalışma mantığında da iki cihaz için de geçerli olacak bir grup numarası belirlenir ve her iki cihaz da bu grup numarasıyla konfigüre edilir. Grup numarası girildiği anda sanal MAC adresi cihaz tarafından oluşturulur. Kullanıcıların hedef ağ geçidi olarak göreceği bir sanal IP adresi belirlenir. Böylece son kullanıcı hiçbir zaman gerçek Layer 3 anahtarların IP adresini bilmemiş olur, onlar her zaman sanal IP ve sanal MAC ile iletişim halindedir. Aktif - Standby geçişlerinde sanal IP aynı kaldığı için bağlantıda süreklilik sağlanmış olur.

#### *3.2.3.2 Yönlendirme Protokollerini Belirleme*

Bu belirlemede hangi yönlendirme protokollerinin niçin seçilmesi gerektiğine vurgu yapılacak, yönlendirme protokollerinin birbirlerine karşı avantaj ve dezavantajlarına değinilecektir. Öncesinde karşılaştırma yapabilmek için, yönlendirme protokolleri hakkında kısa bilgiler verilecektir.

Yönlendirme protokolleri 2 alt başlık altında incelenirler:
i. Uzaklık Vektör (Distance Vector) Yönlendirme Protokolleri
ii. Hat Durumu (Link State) Yönlendirme Protokolleri

##### *3.2.3.2.1 Uzaklık Vektör (Distance Vector) Yönlendirme Protokolleri*

Dinamik yönlendirme protokolü algoritmalarından Uzaklık Vektör Yönlendirme Protokolü (Distance Vector Routing Protocol), Bellman-Ford algoritmasını kullanır. Algoritma, periyodik olarak yönlendirme tablosunun bir kopyasının, ağ komşuluğundaki yönlendiriciye iletimi olarak tanımlanır. Her yönlendirici, yönlendirme tablosuna, algoritma sonucunda elde ettiği uzaklık vektörü değerini ekler ve bu tabloyu kendi komşuluğundaki yönlendiriciye iletir. Uzaklık vektörü değeri, kullanılan protokole göre, gecikme, yük ve sekme sayısı gibi değerler olabilir. Yönlendirme tablosunun transfer işlemi sonucunda, tüm yönlendiriciler, ağdaki diğer yönlendiricilere

olan uzaklık vektörü değerlerini öğrenmiş olur. Yönlendiriciler, paketleri, bir noktadan diğer bir noktaya iletirken yönlendirme tablolarındaki en küçük uzaklık vektörü değerine sahip olan yolları seçer ve bu şekilde ağdaki iki nokta arasındaki en uygun yol belirlenmiş olur (Faraz 2002).

RIP:

RIP, birçok yönlendirici cihazında kullanılan yönlendirme protokolüdür. Interior Gateway Protokol ailesindendir ve iç ağlarda kullanılmak üzere tasarlanmıştır. RIP, uzak vektör yönlendirme protollerindendir. Hop sayısı (geçit sayısı) hesaplayarak metrik değerlerle yol seçimi yapmaktadır. RIP ile en fazla 15 hop-sayısı kullanılabilmektedir. 30 sn.de bir yönlendirme tabloları broadcast mesajlarla anons edilmektedir. RIP protokolünde eşit metrik değerlere sahip yollar olduğu durumda 6 yola kadar yük dengeleme yapılabilmektedir. RIPv2, RIPv1 protokolünden sonra gelistirilmistir. RIPv2 nin RIPv1'e göre birçok özelliği bulunmaktadır.

IGRP:

IGRP, Cisco Systems tarafından 1980'lerin başlarında tasarlanmıştır. IGRP, otonom sistemlerde kullanılan güçlü bir protokoldür. IGRP; ağın bant genişliği, gecikme süresi, güvenilirlik, yük ve MTU değerlerine bakarak en iyi yolu bulmaya çalışır. IGRP, RIP'e göre daha geniş ağlarda çalışabilir. RIP 15 hop sayısına kadar çalışabilmesine karsın IGRP 255 hop sayısına kadar çalışabilmektedir. Karışık metrik hesaplamalarıyla yol bulmada çok başarılıdır. Karışık metrik hesaplamaları sayesinde kaynak ve hedef adres arasında çoklu yol bulma yeteneğine sahiptir. En fazla 6 tane yol belirleyebilmektedir. Sonuç olarak IGRP, RIP'e oranla daha güçlü ve daha büyük ağlarda kullanılabilecek bir protokoldür.

EIGRP:

EIGRP, Cisco Systems tarafından tasarlanmış ve IGRP'nin geliştirilmiş sürümüdür. EIGRP, Interior Gateway Protocol ailesindendir. Metot olarak uzak vektör yönlendirme protokoloüdür ama hat durumu protokolü özelliklerini de taşır. Bir ağda EIGRP'nin kullanılabilmesi için çok iyi bir tasarım yapılması gerekir. Buna karşılık olarak EIGRP

alternatif yollar arasında çok yüksek geçiş hızı sunar. EIGRP, Diffusing Update Algorithm (DUAL) kullanmaktadır. DUAL algoritmasıyla yedek yönlendirmeler hesaplanmakta ve gerektiği zaman vakit kaybetmeden bu yedek yolların kullanılmasını sağlamaktadır.

EIGRP, IGRP gibi periyodik yönlendirme güncellemesiyle çalışmamaktadır. Yönlendirme tablosunda bir değişiklik olduğunda tüm tabloyu değil, sadece güncellenen kısmı göndermektedir. Böylece yönlendiriciye getirdiği ek yük de çok düşüktür ve ağ trafiğini de optimum kullandırır. Ayrıca EIGRP; IP, IPX, AppleTalk protokollerini de desteklemektedir. Bu nedenlerle Cisco yönlendiricilerde çok tercih edilen bir protokoldür.

BGP:

BGP İnternet servis sağlayıcıları tarafından kullanılan gelişmiş bir yönlendirme protokolüdür. BGP'de yönlendiricilere otonom sistem numarası atanır. Otonom sistem numarası 1 ile 65535 arasında değişir. 64512 ile 65535 arası özel otonom sistem numarasıdır ve herkes tarafından kullanılabilir.

BGP, yönlendirme tablosunu oluşturmak için metrik hesaplarken, hedefe giderken üzerinden geçilen otonom sistem sayısını göz önüne alır. Bu durum BGP'nin uzak vektör algoritmasını kullandığını gösterir. EIGRP ve IGRP gibi otonom sistem özelliğine göre çalışan yönlendirme protokollerinin aksine BGP farklı otonom sistemlere ait yönlendiriciler arasında da çalışabilmektedir. Bir otonom sistemden çıkan BGP update (güncelleme) paketine otonom sistem numarası eklenir. Böylece otonom sistemden çıkan update (güncelleme) paketinin aynı otonom sisteme girmesi engellenerek loop (döngü) oluşması engellenir. BGP, IP adreslerinin özetlenebileceği CIDR, "Classless Inter-Domain Routing"i destekler. İletişim için TCP 179. Portu kullanır. Atmış saniyede bir 19 byte uzunluğunda bir paket TCP 179. Port kullanılarak gönderilir. BGP, TCP kullandığından dolayı diğer yönlendirme protokollerindeki gibi doğrulama işlemi yapılmaz. Güncelleme paketlerinde sadece değişen rotalar gönderilir. Bağlantının güvenliğinin sağlanması için MD5, Message Digest algorithm 5 (İleti Özeti

Algoritması 5) ile erişimin yetkilendirmesi sağlanır. BGP, otonom sistemin içinde veya dışında çalışmasına göre ikiye ayrılır:

Farklı otonom sistem içinde bulunan yönlendiricilerin birbirleriyle komşuluk kurabilmesi için EBGP kullanılır. Bu protokol kullanılarak komşudan öğrenilen ağ bilgisi yönlendirici tablosuna "administrative distance" değeri 20 olacak şekilde eklenir. Aynı otonom sistem içinde bulunan yönlendiricilerin birbirleriyle komşuluk kurarabilmesi için IGBP kullanılır. Bu protokol kullanılarak komşudan öğrenilen ağ bilgisi yönlendirici tablosuna "administrative distance" değeri 200 olacak şekilde eklenir.

#### *3.2.3.2.2 Hat Durumu (Link State) Yönlendirme Protokolleri*

Hat Durumu Protokolü algoritması, karışık ağ topolojileri veri tabanlarını destekler. Burada, Uzaklık Vektör Yönlendirme Protokolü'nden farklı olarak, yönlendiricilerin, birbirlerine nasıl bağlı oldukları, hat durumu bildirimlerinin (Link State Advertisement - LSA), diğer ağlardaki yönlendiriciler ile değişimi ile açıklanır. Hat Durumu Protokolü'nde en kısa yol, düğümlerle ilişkili etiketlerin (label) oluşturulduğu ve bu etiketlerle, kaynak düğüm ile diğer belirli düğümler arasındaki uzaklıkların gösterildiği Dijkstra algoritması ile bulunur. Algoritmadaki temel fikir, düğümlere ilişkin geçici etiketleri kalıcı etiketlere çevirmektir. Yönlendiricilerden herhangi biri bu algoritmayı çalıştırdığında, söz konusu olan yönlendirici, kaynak nokta durumuna gelir ve ağdaki diğer yönlendiricilere en kısa yoldan erişmek için hangi yolu seçeceğini ve en kısa yolun uzunluğunu belirler.

OSPF:
OSPF, IP ağlarında kullanılmak üzere Internet Engineering Task Force (IETF) tarafından tasarlanmıştır. Açık standartlara sahip bir protokoldür. OSPFv2 RFC 2328'de tanımlanmıştır.

OSPF, interior gateway protokol ailesindendir. Classless hat durumu yönlendirme protokolüdür. Shortest path first (SPF) algoritması kullanmaktadır. Periyodik güncellemeler yapar ancak güncelleme süresi çok uzundur. Ön tanımlı 30 dakikadır, ancak değiştirilebilir. Area adı verilen bölgeler ve otonom sistemler mantığıyla çalışır. SPF sayesinde her yönlendirici kendisine bir ağaç yapısı tanımlar ve kendisini bu ağacın en yukarısına alır. Bu şekilde maliyet hesaplaması yapılır ve en uygun yol bulunmaya çalışılır. Yönlendiricilere tanımlanan area'lar sayesinde güncellemeler sadece ilgili area'da kalır (Moy 1998, p.62). Böylece OSPF, broadcast değil, multicast çalışır.

#### *3.2.3.3 Protokollerin Dizaynda Belirlenme Uygulaması*

Anahtarlama ve yönlendirme protokollerini belirlemeden önce kullanacağımız teknolojilere biraz değinmekte fayda vardır. Bu sistem temel network uygulamasının yanı sıra gecikmeye ve paket kaybına karşı hassas olan ses ve görüntü networklerini de içermektedir. Dolayısıyla seçilmesi gereken protokoller hemen tepki süresi verip kendi algoritmasını uygun sürede çalıştırabilecek hızlı protokoller olmalıdır.

Bağlantılardaki döngülerin önüne geçebilmek için STP ailesinden RSTP (Rapid Spanning Tree Protocol) protokolü belirlenmiştir. Bu protocol, STP'nin daha hızlı modelidir. STP'de döngüden dolayı alternatif bağlantıya geçiş algoritması elli saniyede düzenlenirken, RSTP'de bu süre altı saniyedir. STP'den farklı olarak dinleme fazı bulunmaz iken, bloklama fazı yerine yok etme fazı kullanılır. VLAN bilgilerinin değiş tokuşu için VTP protokolü kullanılmış olup her VLAN bilgisinin cihazlar arası bilinirliği sağlanmıştır. Yedekleme amaçlı HSRP protokolü belirlenmiştir. VRRP ya da GLBP seçilmemesinin nedeni kullanılan aktif cihazların markasının Cisco olmasıdır. Kendi standardı olan HSRP protokolleri ile Cisco anahtar ve yönlendiriciler daha stabil ve daha hızlı çalışmaktadırlar.

İçeri networkte kullanılacak olan yönlendirme protokolü EIGRP olarak belirlenmiştir. Bu protokolün seçilmesinin nedenleri aşağıdaki gibi özetlenebilir:

i. Cisco'nun geliştirmiş olduğu, Cisco cihazlar ile çok hızlı aktif olabilen ve kullandığı DUAL algoritmasını hızlı ve istikrarlı şekilde çalıştırabildiği için seçilmiştir.
ii. VLSM'i desteklemektedir. VLSM bir alt ağa birden fazla alt ağ verilebilmesidir. Yani IP bloklarını değişik büyüklüklerde alt ağlara bölmemize izin verir.
iii. Parça güncellemeleri destekler. Yani ağda bir değişiklik olduğunda sadece meydana gelen değişiklik ile ilgili olarak yönlendiricileri bilgilendirir.
iv. Broadcast paketleri yerine multicast ve unicast adresler kullanır. Multicast adres olarak 224.0.0.10 ' u kullanır.
v. EIGRP çalışan bir yönlendirici, bütün komşu yönlendiricilerin yönlendirme tablolarını kopyalamaktadır. Eğer hedef networke erişmede sıkıntı olursa hızlıca alternatif yol tespitinde bulunabilir. Eğer uygun yol yoksa EIGRP komşularına alternatif yol bulmaları konusunda istekte bulunur. Bu istek alternatif yol bulunana kadar yayımlanır.

İnternet ortamına çıkıldığında ise tüm dünyanın ortak olarak kullandığı BGP protokolü çalıştırılacaktır. Bunu internet servis sağlayıcıları kendi konumlandıracakları aktif cihazlar üzerinde yaptıklarından ve kurumun internet servis sağlayıcı lisansı olmadığından, dolayısıyla bir AS numarası bulunmadığından, bu bölüm oradan gelecek bir link dışında tasarımı etkilememektedir.

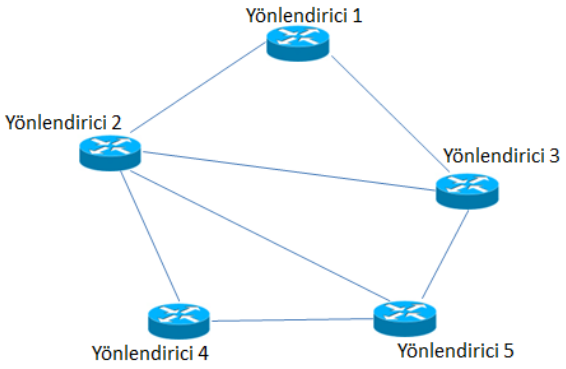
#### *3.2.3.4 Anahtarlama ve Yönlendirme Protokollerinin Belirlenmesinde Paralel Hiyerarşik Yaklaşımın Sonuçları*

Anahtarlama ve yönlendirme protokolleri bir network dizaynını temel olarak etkileyen önemli faktörlerden birkaçıdır. Bu protokoller networkün toparlanma ve hızlı hareket kabiliyeti sürelerini direk olarak etkilediğinden, son kullanıcının "network yavaş" ya da "dosya transferi hızlı gibi" gibi sonuçları ortaya çıkarmada birinci derecede etkilidirler.
Paralel hiyerarşik yaklaşım yönlendirme ve anahtarlama protokollerinin seçiminde şöyle uygulanmıştır. Her protokole kendi içerisinde analiz edilirken aynı zamanda birbirleri ile olan etkilerine de dikkat edilmiştir. Örneğin OSPF kendi içerisinde çıkarılan topolojiye göre hızlı tepki veren bir protokol olabilir; ancak STP kök anahtar seçimine

olan etkisi değerlendirmiş midir ya da HSRP protokolünün yedeklilik mimarisi STP algoritmasına ters midir gibi birçok sorunun cevabı yapılan aşağıdaki analiz ile çözümlenmiştir.

Dynagen emulasyon programı ile gerçeklenen aşağıdaki topolojide RIP, EIGRP ve OSPF protokollerinin performans analizi yapılmıştır. Örneklenen şirket binasının da topolojisi 5 adet örnek yönlendirici ile tanımlanmış ve sonuçlar aşağıdaki şekilde çıkmıştır.

**Şekil 3.18: Yönlendirici protokollerinin seçilmesi senaryosu**




Bir yönlendiriciden diğerine erişim ile hesaplanan gecikme değeri ile ölçülen gecikme değerleri aşağıdaki koşullar baz alınarak ölçülmeye çalışılmıştır.

**Tablo 3.3: Simülasyon senaryoları**

| Senaryo | Yönlendirme Protokolü | Düşen Bağlantı | Kesinti Süresi | Toparlanma Süresi |
|---|---|---|---|---|
| OSPF düzgün çalışıyor | OSPF | - | - | - |
| EIGRP düzgün çalışıyor | EIGRP | - | - | - |
| RIP düzgün çalışıyor | RIP | - | - | - |
| OSPF protokolü düştüğünde | OSPF | Yönlendirici 1-5 arası | 300s | 500s |
| EIGRP protokolü düştüğünde | EIGRP | Yönlendirici 1-5 arası | 300s | 500s |
| RIP protokolü düştüğünde | RIP | Yönlendirici 1-5 arası | 300s | 500s |

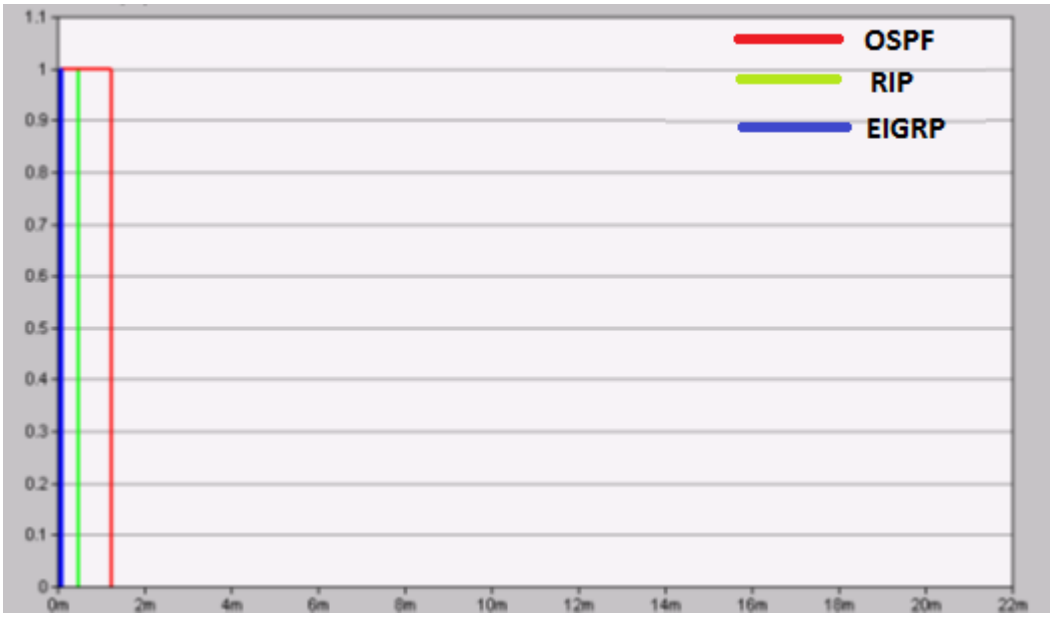
Trafik yoğunluğu ile test edilen uygulamalar da aşağıdaki gibidir:

**Tablo 3.4: Simülasyonda kullanılan uygulamalar**

| | |
|---|---|
| Video Konferans | 15 fps ile |
| Ses | IP Telefon |
| Internet | http trafiği |
| E-posta | yüksek boyutlu ekler ile |

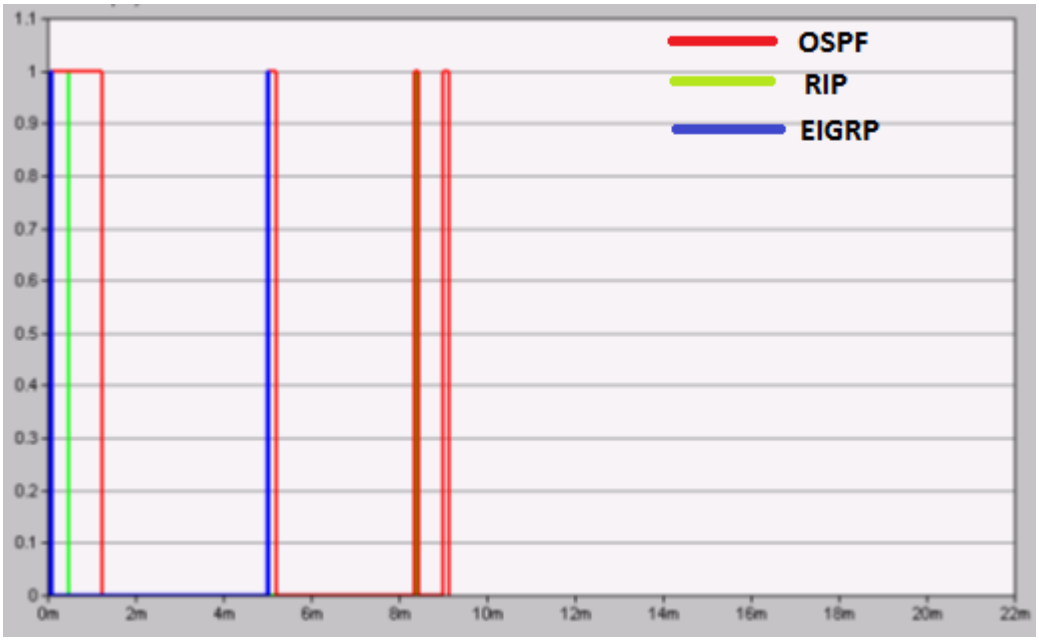
Simülasyon sonucu kırmızı ile gösterilen OSPF'i, mavi EIGRP'yi, yeşil ise RIP'i göstermektedir. Kesinti olmadığı durumda protokol algoritmalarının çalışmasıyla oluşan zaman aktivitesi aşağıdaki gibi olmuştur:

**Şekil 3.19: Protokollerin normal çalışmasındaki zaman aktivitesi**




Simülasyon sonucu kırmızı ile gösterilen OSPF'i, mavi EIGRP'yi, yeşil ise RIP'i göstermektedir. OSPF, EIGRP ve RIP protokolü düştüğünde gözlemlenen zaman aktivitesi ise aşağıdaki gibi olmuştur:

**Şekil 3.20: Protokoller düştüğündeki zaman aktivitesi**




Görüldüğü üzere normal çalışma zamanında EIGRP kendine gelme süresi en kısa yani en kısa zamanda toparlanabilen protokoldür. Kesinti olduğu anda protokollerin çalışma algoritmaları tekrardan hesaplanır ve hatların normale dönmesi ile bir toparlanma sürecine girerler. Burada en çabuk toparlanabilen protokol, algoritmasının basitliği sayesinde RIP'tir. Ancak RIP, bu senaryodaki gibi az sayıda yönlendiricinin bulunduğu durumlarda kullanılabilir. Şirket binalarında her segment için ayrılmış özelleşmiş yönlendiriciler bulunduğundan karmaşık algoritma çalıştırabilen ve RIP'ten sonra en hızlı toparlanabilen protokol olan EIGRP bu seçim için oldukça uygundur. Paralel hiyerarşik yaklaşımın bir sonucu olarak dizaynda EIGRP protokolüne yer verilmiştir.

Anahtarlama protokolü seçiminde herhangi bir simülasyon yapılmamış ancak yedeklilik ve STP bir arada düşünülerek HSRP ve RSTP protokollerine yer verilmiştir. Burada amaç şudur; paralel hiyerarşik yaklaşımdaki paralel düşünebilme sistemini burada uygulayabilmek. Yani STP ve HSRP protokolleri de bu dizayn için düşünülebilirdi. Ancak RSTP'nin vermiş olduğu 2-4 s arası toparlanma süresi, bir yedeklilik protokolü olna HSRP'nin çalışma algoritmasını direk olarak etkileyecek ve geri dönüş zamanını azaltacaktır. Dolayısıyla paralel hiyerarşik yaklaşım sayesinde anahtarlama protokollerinin de seçimi gerçekleştirilmiş olmuştur.

### 3.2.4 NETWORK GÜVENLİK STRATEJİLERİNİ BELİRLEME

Bu bölümde öncelikle network güvenlik stratejileri anlatılacak, daha sonra bu stratejilerin projede uygulanması ve paralel hiyerarşik yaklaşımın projeye olan olumlu etkileri üzerinde durulacaktır.

#### *3.2.4.1 Network Güvenlik Stratejileri*

Güvenli ağ yaratılması, kritik IT sistemleri ve bu sistemlerin düzenli-güvenli çalışması için yaratılmalıdır. Güvenlik mimarisi, ağ segmentasyonu ve güvenlik katmanları ile oluşturulur. Hatalı network güvenlik tasarımının sonuçları iş sürekliliği kaybı, güvenlik zafiyetleri, yeni ağ tasarımı inşa maliyeti, iş kayıpları, yüksek maddi zarar, prestij kaybı gibi olumsuzluklar doğurur.

Ağ tasarımı için gerekli güvenlik mimarisi iki şekilde açıklanır.

i. Ağ segmentasyonu (güvenli bölgeler)
ii. Güvenlik katmanları (Saldırı önleme, içerik denetleme, erişim kontrolleri, katmanlı güvenlik mimarisi)

Güvenli tasarımın avantajları da Güvenli mimarinin avantajları da yüksek yalıtım, güvenli sistem, ihlal sınırlama ve maliyet tasarrufu olarak sıralanabilir. Güvenli network tasarımı yapabilmek için şunları iyi belirlemek gerekir:

i. İhtiyaçların belirlenmesi ve amaca yönelik tasarım
ii. Politikaların belirlenmesi
iii. Büyüme hızının belirlenmesi
iv. Maliyet etkinlik analizi
v. Çevirim dışı ağ kullanımı

Ağ tasarımında dikkate alınması gereken ilkeler ise modülerlik ve katmanlı yapı, derinlemesine savunma ve maksimum koruma olmalıdır. Tasarımda, güvenliği düşük

ağların izolasyonu ile saldırı potansiyeli taşıyan IT sistemlerini stratejik olarak korunmalıdır; network segmentasyonu ile güvenlik ihlallerini sınırlandırarak saldırının diğer bölgelere sızması engellenmelidir; doğru ağ erişim kontrolleri ile monitörleme, gözden geçirme, kaynak kullanımı ve yönetimi stabil gerçekleştirilmelidir; kimlik doğrulama sistemleri ile olay gerçekleşmesi minimum düzeye çekilmelidir; pahalı önlem gerektiren IT sistemleri farklı güvenlik bölgelerinde tutulmalıdır.

#### *3.2.4.1.1 Güvenlik Duvarı (Firewall)*

Güvenlik duvarı, yerel ağ ile dış ağ arasındaki güvenlik kontrol yazılımları ya da cihazlarıdır (Hines 2003, p.13). Güvenlik duvarı ilk kurulduğunda bu nokta üzerindeki bütün geçişleri durdurur. Daha önceden belirlenen politikalar dahilinde hangi veri paketinin geçip geçmeyeceği, hangi geçişlerde parola doğrulaması yapılacağı gibi bilgiler güvenlik duvarı kural tablolarına eklenir. Bu sayede sisteme ulaşan kişi ve bilgi trafiği kontrol altına alınmış olur. İçerideki ya da dışarıdaki sistemlere kimlerin girip giremeyeceğine, giren kişilerin hangi bilgisayarları ve hangi servisleri kullanabileceğini güvenlik duvarı üzerindeki kurallar belirler. Güvenlik duvarı yazılımı, adresler arası dönüştürme (NAT) sayesinde LAN'daki cihazların IP adreslerini gizleyerek tek bir IP ile dış ağlara erişimini sağlar. Adres saklama ve adres yönlendirme işlemleri güvenlik duvarı üzerinden yapılabilir. Böylece dış dünyadaki kullanıcılar yerel ağdaki kritik topoloji yapısını ve IP bilgisini edinemezler. Güvenlik duvarı yazılımı kendi üzerinde belirtilmiş şüpheli durumlarda sorumluları e-posta ya da SNMP yolu ile uyarabilir. Gelişmiş güvenlik duvarı yazılımları üzerinden geçen bütün etkinlikleri daha sonradan incelenebilmesi için kaydederler. Ek bir lisans yada modül ile birlikte VPN (Sanal Özel Ağ) denilen yerel ağa gidip gelen bilgilerin şifrelenmesi ile uzak ofislerden yada evden internet üzerinden güvenli bir şekilde şirket bilgilerine ulaşmak e-posta vb. servisleri kullanmak mümkün olmaktadır. Bu şekilde daha pahalı çözümler yerine (kiralık hatlar vb.) Internet kullanılabilir. Yalnız uzaktaki kullanıcıların güvenliği burada ön plana çıkmaktadır. Dışarıdan bağlanan kişinin gerçekten belirlenen yetkili kişi olup olmadığı önemlidir. Bu kişilerin şifresini ele geçirenler sisteme o kişilerin haklarıyla ulaşabilirler. Bu noktada kişisel güvenlik duvarı ve dinamik şifre üreten token'lar devrede olmalıdır.

Günümüzdeki gelişmiş güvenlik duvarı sistemleri içerik denetleme işlemi yapmamakta bu tip hizmetleri güvenlik duvarı sistemleriyle entegre çalışan diğer güvenlik sistemlerine yönlendirmektedir. Bu sayede güvenlik firmaları sadece odaklandıkları ve profesyonel oldukları konularda hizmet vermekte, kullanıcı da bu ayrık sistemlerden kendisi için uygun olan çözümleri tercih etmektedir. Örneğin gelen bilgilerin içerisinde virüs olup olmadığı ya da atak yapılıp yapılmadığı güvenlik duvarı tarafından kontrol edilmez. Kurallarda belirtilmişse kendisi ile entegre çalışan sisteme data paketini yönlendirir. Tarama işlemi diğer makinada yapıldıktan sonra paket tekrar güvenlik duvarına geri döner. Güvenlik duvarı yazılımının yönetim konsolu merkezi yönetim amaçlı olarak ayrı makinelere yüklenebilir. Yönetim ile ilgili kurallar, trafikle ilgili kayıtlar (log) ayrı sistemlerde tutulabilir. Kullanıcı grafik ara yüzü ile uzak makinelerden kolayca yönetim yapılabilir ve mevcut kullanıcı bilgileri (LDAP) uygulamalarından alınabilir. Aktif bağlantılar görüntülenip gerektiğinde ana güvenlik politikalarına engel olmadan bağlantılara müdahale edilebilir. Bant genişliği yönetimi sağlayan sistemlerle entegre olabilir. Güvenlik duvarı yazılımları ya da cihazları güvenliğin yapı taşları olup sistem içerisindeki diğer güvenlik yazılımları ya da cihazları ile uyumlu çalışmakta ve gelecekteki güvenlik teknolojilerine taban teşkil etmektedirler. Güvenlik duvarı yazılımı kesinlikle şart olmasına rağmen güvenlik için tek başına yeterli değildir.

#### *3.2.4.1.2 IDS (Saldırı Tespit Sistemleri)*

Saldırı tespit sistemleri, Internet dünyasının gelişim sürecinde özellikle tüm dünyada kullanılan web trafiğinin artması ve de web sayfalarının popüler hale gelmesi ile birlikte kişisel ya da tüzel sayfalara yapılan saldırılar sonucu ihtiyaç duyulan en önemli konulardan biri haline gelmiştir. Bununla birlikte kurum ya da kuruluşların sahip oldukları ve tüm dünyaya açık tuttukları e-posta, DNS, veri tabanı gibi sunucularının benzeri saldırılara maruz kalabilecekleri ihtimali yine saldırı tespit sistemlerini Internet güvenliği alanının vazgeçilmez bir parçası haline getirmiştir. Kurumların sahip oldukları çalışan sayısı ve bu çalışanların kendi kurumlarındaki kritik değer taşıyan yapılara saldırabilme ihtimalleri de iç ağın ya da tek tek kritik sunucuların kontrol

altında tutulma gerekliliğini beraberinde getirir. IDS genel olarak iki tip olarak karşımıza çıkar; sunucu tabanlı IDS ve ağ tabanlı IDS.

Ağ tabanlı IDS in görevi, bir kurum yada kuruluşun sahip olduğu ağ ya da ağlara yönlenmiş olan tüm trafiği algılayarak, bu ağa doğru geçen her bir veri paketinin içeriğini sorgulamak, bir atak olup olmadığına karar vererek kaydını alabilmek, kendisi ya da konfigüre edebildiği başka bir aktif cihaz tarafından atakları kesmek, network yöneticisini bilgilendirmek ve ilgili raporlar oluşturabilmektir. IDS bir veri paketinin atak olup olmadığını, kendi atak veri tabanında bulunan atak tipleriyle karşılaştırarak anlar ve karar verir. Sonuç olarak bir IDS in en önemli bileşeni bu atak veri tabanıdır. Söz konusu atak veri tabanının içeriği, ne kadar sıklıkla ve doğrulukla güncellendiği ve kimin tarafından oluşturulduğu, güncellendiği en önemli noktadır. Bu sebeple doğru üretici firma ve ekip seçimi çok önemlidir. Sunucu tabanlı IDS'in görevi ise kurulu bulunduğu sunucuya doğru yönlenmiş bulunan trafiği yine üzerinde bulunan atak veri tabanı baz alınarak dinlemesi ve atakları sezerek cevap vermesidir.

Genel olarak IDS iki veya daha fazla makineden oluşan bir yapıdır. Performans artırımı sebebiyle merkezi kontrol ve kayıt mekanizmasının bir makinede, trafiği dinleyen ağ tabanlı modül veya sunucu tabanlı modül ayrı makinelerde tutulur. IDS'ler, dinlediği trafiğin kaydını tutarak, gerektiğinde bu kayıtları baz alarak istenilen şekilde raporlar çıkartabilmektedir. Atak sezdiklerinde atakları önleyebilir, yöneticilerine mail ya da benzeri yollarla haber verebilirler, önceden oluşturulmuş bir program çalıştırabilir ve telnet benzeri bağlantıları kayıt ederek sonrasında izlenmesini sağlayabilirler. Tüm bu özellikleriyle IDS'ler sistemin güvenli bir şekilde işlemesine yardımcı olur ve network yöneticilerinin sistemi güçlü bir şekilde izlemesine yardımcı olmaktadırlar.

#### *3.2.4.1.3 Web Filtreleme*

Bugün çalışanların çoğunun Internet'e erişim hakları var. Fakat bunların hangi sayfalara gittikleri, oralarda ne kadar zaman geçirdikleri bunların ne kadarının işle ilgili olduğu gibi soruların yanıtlanması gerekir. Son zamanlarda yapılan araştırmalarda iş günü

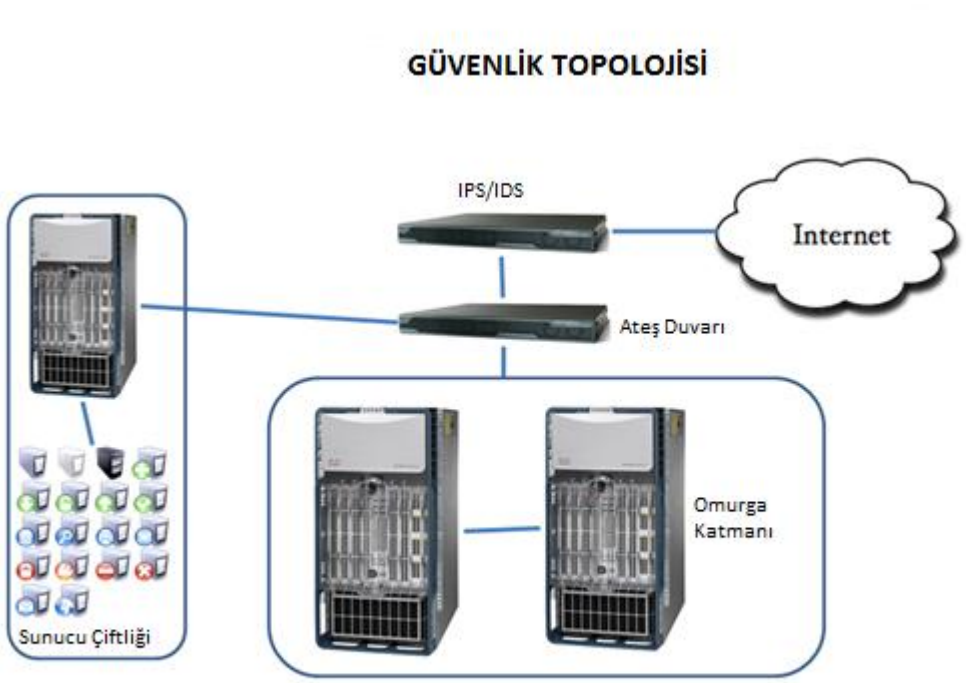
içerisinde yapılan web sayfası ziyaretlerinin çoğunun işle alakalı olmadığı, sakıncalı sayfa ziyaretlerinin sistemlere virüs ya da trojan bulaşmasına, gereksiz bant genişliği harcanmasına ve yasal olmayan sitelerden indirilen programların sistemlere sahte lisanslarla sebep olmakta olduğu gözlemlenmektedir. Bütün bunları engelleyebilmek için Web filtreleme denilen yazılımlar kullanılmaktadır. Bu yazılımların her gün güncellenen veri tabanları sayesinde dünyadaki çoğu web sayfaları sınıflandırılmış durumdadır. Bu yazılımlar kişi, grup, IP adres aralıklarına kural tanımlanmasını sağlar. Bu sayede daha önceden tanımlanmış kişilerin hangi zaman aralıklarında nerelere girebilecekleri belirlenebilir. Ya da gün içerisinde belirlenen kategoriler için zaman kotası uygulanabilir. Örneğin sabah 9:00-12:00 arası gazetelere yarım saat bakılma izni, 12:00-13:00 her yere izin verilmesi gibi uygulamalar geliştirilebilir. Web filtreleme yazılımlarıyla ayrıca anahtar kelime bazlı sınırlandırma ya da manuel olarak sayfa sınırlandırması yapılabilir. Engellenen sayfalarla ilgili olarak kullanıcı karşısına bilgilendirici bir ekran çıkar ve neden engellendiği ya da hangi zaman aralıklarında geçerli olduğu belirtilir. Burada daha önceden belirlenmiş bir sayfaya yönlendirmek de mümkündür. Bu tür yazılımlarının raporlama modülleri sayesinde kimlerin nerelere gittikleri oralarda ne kadar süre boyunca kaldıkları gibi ayrıntılı bilgilere ulaşmak mümkündür.

#### *3.2.4.2 Network Güvenlik Stratejilerinde Paralel Hiyerarşik Yaklaşım Uygulaması*

Bu tezin konusu olan şirket yönetim binaları projesinde güvenlik amaçlı ayrı bir dizayna yer verilmiştir. Yukarıda bahsedilen paralel hiyerarşik katmanlı yapı kullanılmış olup, omurga katmanına gelmeden önce internete çıkışta bir güvenlik duvarı ve hem IPS hem de IDS özelliklerini gösteren bir cihaz konumlandırılmıştır. Aslında segmentler 3'e ayrılmış olup, bir bacağı internete yani güvensiz networke bakmaktadır. Burada uzaktan bağlanan kullanıcıları VPN ile güvenlik duvarı üzerinden şirket networküne dahil edecek bir tasarım uygulanmıştır. Güvenlik duvarının diğer bacağı DMZ denilen sunucu çiftliğine bakmaktadır. Burada kurum için gerekli olan bütün uygulamaları barındıran sunucular yer almaktadır. Kullanıcılardan ayrılmasının temel nedeni, bir şirkette önemli sunuculara yapılan atakların %80'inin içerideki kullanıcılar tarafından yapılmasıdır. Bu

sayede sunucu çiftliğindeki sunucular iç networkten de izole edilmiş oldular. Son bacak ise kullanıcılara bakan bacaktır.

**Şekil 3.21: Güvenlik topolojisi**




Bu tasarım yöntemi ile güvenlik duvarının bacakları modüllere ayrılmış ve her network izole edilmiştir. Bu sayede güvenlik duvarı üzerinde kullanıcılara aktif cihazlara ya da sunuculara erişim kısıtlaması kolaylıkla yapılabilmektedir.

### *3.2.4.3 Network Güvenlik Stratejilerinin Belirlenmesinde Paralel Hiyerarşik Yaklaşımın Sonuçları*

Paralel hiyerarşik yaklaşım tanımı gereği teknolojilerin kendi içerisinde yukarıdan aşağıya hiyerarşik bir yapıda, ancak teknolojiler arası da paralel bir düşünce tarzı benimsemeyi konu edinmiştir. Network güvenliğinde oluşturulacak katmanlı yapılar aynı zamanda ses-video networkleri ya da kablosuz networkler ile de uyum ve birlikte çalışabilirlik göstermelidir.

Oluşturulan katmanlı yapıda IPS/IDS cihazı, güvenlik duvarı, web filtreleme yazılımı ve antivirus yazılım sistemi entegre halde çalışmıştır. Paralel hiyerarşik yaklaşım ile önce güvenlik sistemi kendi içerisinde hiyerarşik olarak tanımlanmıştır. Öncelikle dışarıdan gelecek tehditler için güvenlik duvarı donanımı tasarımın temel taşını oluşturmaktadır.

**Şekil 3.22: Paralel Hiyerarşik Modele Göre Güvenlik Tasarım Sırası**


Güvenlik duvarı networkü temel güvenlik açıkları ve zararlı erişimlerden koruyacağı için tasarımda birinci sıradadır. Bir bacağı dış dünyaya, bir bacağı içerideki kullanıcılara, en son bacağı ise DMZ olarak adlandırılan sunucuların bulunduğu segmente bakacak olan güvenlik duvarı tasarımından sonra sıra IPS/IDS tasarımına gelmiştir.

IPS/IDS cihazı hem ayrı ayrı donanımlar olabilmekle birlikte, aynı kutu içerisinde farklı yazılımların çalıştırılmasıyla algoritmalarını işleyebilen cihazlar olabilmektedir. Burada gösterilen örnek şirket binası network güvenlik tasarımında aynı kutu içerisine yerleştirilmiş bir cihaz olarak dikkat çekmektedir. Aynı şasi içerisinde olmasının amacı maliyet ve yönetim giderlerinin düşürülmesi ile ilgilidir.

Antivirüs tasarımında uygun üreticiyi seçmek paralel hiyerarşik yaklaşım ile tek başına yeterli bir kriter değildir. İstemci ve sunucudan oluşan virüs koruma yazılımları hem IPS/IDS cihazıyla hem de güvenlik duvarı cihazıyla ortak ve mantıklı bir veri tabanı listesine bağlanmalıdır. Bu yolla bir ürünün tehdit olarak gördüğü hareketi diğer ürün güvenilir bir aksiyon olarak görmez. Dizayn içerisindeki tüm komponentler birlikte ve tutarlı olarak hareket ederler.

### 3.2.5 NETWORK YÖNETİM STRATEJİLERİNİ BELİRLEME

Bu bölümde öncelikle network yönetim stratejileri anlatılacak, daha sonra bu stratejilerin projede uygulanması ve paralel hiyerarşik yaklaşımın projeye olan olumlu etkileri üzerinde durulacaktır.

#### *3.2.5.1 Network Yönetim Stratejileri*

Büyük bir kampüs ağında yüzden fazla aktif ağ cihazı, yüze yakın VLAN olabilmektedir. Böyle bir ağdaki trafiğin izlenmesi, özellikle bir yavaşlama ya da çalışmama durumunda sorunun hangi VLAN'da ve o VLAN'a ait hangi anahtarın hangi portundaki bilgisayarda olduğunun bilinmesi önem kazanmaktadır. Acil durum politikasında, aksaklıkların yaşanması durumunda yapılması gereken prosedürler belirlenmelidir. Network ve sistem yöneticileri ile iletişimin kurulması için gerekli telefon numaraları gibi bilgiler güncel olarak bulundurulmalıdır. Network cihazları ve sunucularından gerekli bilgileri alabilmek için Simple Network Management Protokol (SNMP) kullanılmalıdır. SNMP, cihaz ve ağ yönetimi için vazgeçilmez bir protokoldür. Bu protokol sayesinde, trafik istatistiklerinden bellek ve işlemci kullanımına kadar bir cihaz ve üzerinden geçen veri trafiği hakkında çok detaylı bilgiler edinilebilmektedir.

Cihazlarda, SNMP protokolü kullanılarak erişimde kullanılacak Oku (Read only) ve Oku-Yaz (Read-Write)parametreleri tanımlanmaktadır. Ağda bu istatistikleri toplayacak

bir veya birden fazla bilgisayar atanmalıdır. Bu bilgisayarlara ağ yönetim istasyonu merkezi (AYM) denmektedir. AYM, üzerinde çalışan yazılımlarla belirli aralıklarla ağ cihazları ve sunuculardan bu istatistikleri toparlayacak şekilde ayarlanmalıdır. Aynı zamanda cihazlarda, sistem durumunda karakteristik değişiklik olduğunda AYM'ye uyarı gönderecek şekilde ayar yapılmalıdır ki bu fonksiyon SNMP trap olarak adlandırılır. Cihazda gözlenen CPU, bellek veya hat kullanımının fazla olması bir saldırı tespiti olabilmektedir. Toplanan verileri grafiksel olarak görüntüleyen Multi Router Traffic Grapher (MRTG) veya PRTG gibi programlar bulunmaktadır.

#### *3.2.5.2 Network Yönetim Stratejilerinde Paralel Hiyerarşik Yaklaşım Uygulaması*

Tüm networkü SNMP komutlarıyla aktif olarak denetleyecek ve topoloji değişikliklerinde veri tabanını güncel tutabilecek bir yönetim yazılımı sunucu çiftliği içerisine konumlandırılmıştır. Bu sistem sayesinde hem cihazların performans değerleri hem de hatların yoğunlukları gerçek zamanlı olarak gözlenebilmekte, yakın geçmişe ya da uzak geçmişe ait raporlar düzenlenebilmektedir. Bu da mevcut sistemin takibi ve iyileştirilmesi açısından çok yararlı bir kaynaktır.

#### *3.2.5.3 Network Yönetim Stratejilerinin Belirlenmesinde Paralel Hiyerarşik Yaklaşımın Sonuçları*

Network yönetimi paralel hiyerarşik yaklaşımın tasarım modeline tam olarak oturan bir alandır. Her bir network teknoloji segmenti için bunları izleyen ve yöneten uygulamalara ihtiyaç duyulur. Örneğin IP telefon dizaynında çağrıların başarılı olup olmadıklarını ya da çağrı kalitelerinin ve servis seviyelerinin oranlarını ölçen bir yazılıma ihtiyaç vardır. Temel network dizaynında ise hatların durumlarını, anahtar ve yönlendiricilerin işlemci ve bellek seviyelerini ve durumlarını ölçen yönetim yazılımları gerekir. Güvenlik tasarımında kullanılan ekipmanların ne kadar sağlıklı çalıştıklarını gözlemlemek için atak ölçer tarzında yazılımlar, hem networkün güvenliğini nicel

olarak ölçmeye yarar hem de servis kalitesinin müşterilere olan yansımalarının gözlemlenmesini sağlayarak müşteri memnuniyetini yöönetir. Kablosuz ağların nerelerde çekip nerelerde daha sağlıksız sonuçlar verdiğini gözlemlemek bu yazılımların amaçlarından sadece birisidir.

Kullanılacak bu yönetim yazılımları kendi içerisinde de tutarlı ve birbirlerine açılan arayüzleri barındırabilen yapıda olmalıdırlar. Yani dışarıadn uygulama geliştirip tüm yönetim yazılımlarından alınan veriler ile beslenebilecek bir veri tabanı oluşturulabilmeli, özellikle şirketlerin üst kademelerindeki kişilerin önüne, tek ekrandan özet bilgilerin verilmesine olanak sağlamalıdırlar.

## 3.3 FİZİKSEL NETWORK DİZAYNI

Fiziksel network tasarımı oluşturulurken mantıksal topolojiden alınan veriler ile buna uygun fiziksel dizayn yapılır. Fiziksel anlamda dizayn yaparken oluşturulan tasarımda kullanılan teknolojiler ve bu teknolojilerin altını doldurup onları toparlayacak cihaz ve ekipmanların seçimi önemlidir. Bu çalışmada daha önceki bölümlerde de bahsedildiği şekilde şirket yönetim binaları aktif network tasarımını oluşturan teknolojiler ve bu teknolojilerin gerçek anlamda kullanımı için gerekli olan teknik ekipmanlar, bu ekipmanların niçin seçildiği ve hangi amaçlarla kullanılacağı gibi konulara değinilmiştir.

### 3.3.1 KULLANILAN TEKNOLOJİLER

Bu bölümde fiziksel topolojide kullanılan teknolojiler anlatılacak olup uygulamalı örnekler ile zenginleştirilecektir.

### *3.3.1.1 Temel Network Teknolojileri*

Günümüzde network, cihazların ve kullanıcıların ortak haberleşmesini sağlayan ağ anlamına gelmekte, bu yapının efektif bir şekilde kullanılarak daha verimli ve güvenli çalışma ortamı sağlamaya yaramaktadır. Yönlendiriciler üzerinden yapılan uzak alan ağı (WAN) networkleri ve aynı kampüs içerisinde konumlandırılan cihazların verimli ve yüksek kapasitede çalışmasını sağlayan yerel alan ağı (LAN) networkleri anahtarlar, yük dengeleyiciler gibi özelleşmiş ekipmanların sağlıklı bir biçimde dizayn edilmesiyle sağlanmaktadır. Servis kalitesi (QoS), güvenlik cihazları ve kuralları ve bant genişliğini etkin olarak kullanmayı sağlayan WAN Optimizasyon politikaları ile ağlar daha güvenli, daha verimli ve daha mobil olabilmekte; her yerden güvenli bir şekilde ilgili veriye doğru bir şekilde ulaşmanın dizaynı yapılabilmektedir (Oppenheimer 2011, p.375).

Anahtarlar MAC adreslerini kullanarak genellikle OSI referans modelinin ikinci katmanı olan veri bağı katmanında çalışırlar. Yönlendiriciler ise üçüncü katmanda çalışmaktadırlar. Bir veriyi göndermek için yönlendirici ve anahtarın kullandıkları algoritmalar birbirlerinden farklıdır. Farklardan biri de broadcast'lerin nasıl yönetildiğidir. Bir ağda broadcast paketlerinin konsepti networkün çalışabilirliğini hayati derecede etkiler. Bir cihazın dışarı bilgi aktarması gerektiğinde ancak bunu nasıl yapacağını bilmediğinde bir broadcast paketi gönderir. Örneğin ağa her yeni bilgisayar veya başka bir cihaz bağlandığında varlığından haberdar etmek için bir yayın paketi gönderir. Diğer bağlantı noktaları böyle yeni cihazı tarayıcı listelerine eklerler ve bu yeni cihazla doğrudan haberleşebilirler.

**Şekil 3.23: Cisco 3750 anahtar**

*Kaynak:*http://www.cisco.com/en/US/products/hw/switches/ps5023/index.html

Araçlar kavşaktan nereye gittikleri önemli olmadan geçerler. Bu yolun bir sınır olduğunu düşünün. Sınırdan geçerken güvenliğe nereye gittiğini belirten ayrıntılı bir adres vermek gerekir. Cihazın kendine özel bir adresi yoksa sınırdan geçemez. Bu networkleri birbirinden ayırmak için güzel bir yoldur. LAN anahtarları da paket anahtarlamasına dayanır. Anahtar iki segment arasında paketlerin aktarımı için bir bağlantı oluşturur. Gelen paketler geçici hafıza bölgesinde saklanır; çerçevenin başında bulunan MAC adresi mevcut adreslerle karşılaştırılır. Birçok anahtar OSI referans modeline göre ikinci katman yani data link katmanında çalışmasına rağmen bazı modeller üçüncü katman yani network katmanında çalışabilirler. Üçüncü katmanda çalışan anahtarlar inanılmaz derecede yönlendiricilere benzemektedirler.

**Şekil 3.24: Cisco ASR yönlendirici**

*Kaynak:* http://www.cisco.com/en/US/products/ps9343/index.html

Yönlendirici bir paket aldığı zaman 3. katman kaynağına ve paketin gönderilmesi için hedef adrese bakar. Standart anahtarlar bir paketin kaynağını ve gideceği belirlemek için MAC adresine bakmaktadırlar. Yönlendirici ve üçüncü katmanda çalışan anahtarların en temel farkı anahtarların donanımsal olarak yönlendiricilere göre daha hızlı olmasıdır. 3. katman anahtar ve yönlendiricilerde katman eşleme ve saklama benzerdir. Ancak anahtarlarda daha hızlı paket işleyebilmek mümkündür.

### *3.3.1.2 Güvenlik Teknolojileri*

Bilgi çalmaya yönelik uygulamalar konusunda her geçen gün daha büyük tehditlerle karşılaşılmaktadır. Güvenlik artık ağ tabanlı olmaktan çıktığı için uçtan uca güvenlik çözümleriyle önlem almak vazgeçilmez bir gereklilik olmuştur. Bu noktada, şirketler için sadece ağ bazında güvenlik sağlayan güvenlik ve IPS gibi ürünlerin dışında, web

güvenliği, son kullanıcı güvenliği, network erişim kontrolü, veri kaybı önleme (DLP) çözümlerini de güvenlik bütününü tamamlayan parçalar olarak düşünülmelidir.

Güvenlik duvarı (Firewall), IPS - IDS, son kullanıcı güvenliği, veri kaybı önleme (DLP), ağ erişim kontrolü (NAC), web filtreleme, şifreleme teknolojileri için özelleşmiş birçok güvenlik ekipmanı bulunmaktadır. Http, https erişimlerine izin verildiği durumlarda kurumlar buralardan gelebilecek tehditlere karşı, erişimlerinde IPS ve web güvenlik ürünleri bileşenleri kullanarak kontrol ettirmelidirler. Kurumlar güvenlik duvarı ile yerel ağlar üzerindeki kaynakları diğer ağlar üzerinden gelecek saldırılara karşı koruyabilir iç ve dış ağlar arası ağ trafiğini tanımlanan kurallara göre denetleyebilirler. Birleşik tehdit yönetimi (UTM) modeli, aynı donanım üzerinde güvenlik duvarı, ağ geçidi antivirüs, antispam, IPS/IDS, URL filtreleme gibi servisler sunarak, bu konuda önlem almak isteyen kurumlara, bir yandan pratik, hızlı uygulanabilir bir çözüm sağlarken, öte yandan maliyet ve yönetim avantajı sunmaktadır. Günümüzde işletim sisteminden ya da yazılım hatalarından kaynaklı zafiyet barındıran birçok popüler web sitesi mevcuttur ve saldırganlar tarafından zararlı kodları yaymak için kullanılmaktadırlar. Bunun dışında bot networkün bir parçası olmuş ve ele geçirilmiş birçok bilgisayar tarafından aynı anda başlatılan DDOS saldırıları ile yine popüler siteler çalışamaz hale getirilmek, DNS saldırıları sonucunda web sitelerine ulaşım engellenmekte ya da farklı sayfalara yönlendirilebilmektedir. IPS - IDS çözümleri ile şirketler imza ve davranış tabanlı olarak internet ya da farklı ağlardan gelebilecek saldırılara karşı koruma sağlayabilmektedir. Şirket çalışanlarının iş saatlerinde web erişimlerinin kontrol edilebilmesi, günümüzde nerdeyse zorunlu hale gelmiştir. Ayrıca, internet aracılığıyla yapılan web yayınları ve internet yoluyla işlenen bilişim ve diğer suçlarla mücadele edilmesi amacıyla Türkiye'de 2007'de kabul edilen 5651 sayılı yasayla beraber bugün birçok kurumdan, şirket çalışanlarının hangi web sitelerine ulaştığının bilinmesi ve raporlanması istenmektedir. Zararsız olarak görünen/bilinen web sitelerine ulaşım bile şirket bilgisayarlarına zararlı kodların bulaşmasına neden olmaktadır. Bu bağlamda web filtreleme ürünlerinin de tasarımda yer alması gereklidir.

### *3.3.1.3 Tümleşik İletişim Teknolojileri*

Ses ve görüntü hizmetlerinin IP networkleri üzerinden verilmesinden sonra bu iş için özelleşmiş santral, ağ geçidi, IP tabanlı telefon ve video konferans cihazları ön plana çıkmıştır. Bu fonksiyonu öncelik alan ağlar genellikle paket kaybı ve gecikme gibi kayıplara karşı aşırı hassastırlar. Bu networkler dizayn edilirken kullanıcıların verimli iletişim yapabilmesini sağlayan Servis Kalitesi (QoS), yasal regülasyonlar ve kullanıcı güvenliğini baz alan ses kayıt ve güvenlik teknolojileri ön plana çıkmaktadır. Artık her şeyin yavaş yavaş mobile doğru kaydığı bu günlerde, platform ve işletim sistemi bağımsız mobil ses ve görüntü uygulamaları erişilebilirliği gözle görülür ölçüde arttırmaktadır (Ahmed & Siddiqui 2011, p.157).

Tümleşik iletişim çözümlerinde web konferans, sesli ve görüntülü haberleşme, çağrı merkezi çözümleri ve IP telefon çözümleri gibi birçok alt teknoloji sıralanabilir. Tümleşik iletişim çözümleriyle, ses ve video konferans oturumlarına ilave olarak giderek artan şekilde kullanılan web temelli sunum ve dosya paylaşımı özelliklerini aynı ortamda kullanabilmek mümkündür. Bu sayede, farklı bir lokasyonda olsa dahi, aynı salonda sunumu yaparmış gibi; diğer katılımcılar sunum yapan kişiyi duyabilir, yazdıklarını görebilir ve yazdıkları üzerinde değişiklik yapıp yazılı, sesli veya görüntülü olarak iletişime geçebilirler. Ayrıca, bu sunumun daha sonra izlemek üzere kayıt edilmesi de mümkündür. Erişim altyapısı olarak artık evlere kadar gelen DSL ve kablo internet altyapıları kullanılabileceği gibi 3G teknolojilerinin hizmete verilmesi ile birlikte cep telefonlarından da sunum izleme olanağına sahip çözümler sunulabilmektedir. Çağrı merkezine olan ihtiyaç sadece finans kuruluşları ile sınırlı kalmayıp birçok büyük kurumsal firmanın müşterilerine daha iyi hizmet verebilmek, verdiği hizmetin kalitesini değerlendirip seviyesini yükseltmek amacıyla yaygın olarak kullanılmaktadır. Ayrıca, firmalar kendi çalışanlarına verdiği yardım masası hizmeti için de çağrı merkezi sistemlerini kullanmaktadır. Bu sayede, çalışanların sorunlarını daha kısa zamanda çözüp şirket verimliliğini arttırmayı hedeflemektedirler. Çağrı merkezi sistemlerinin, müşteri veri tabanı ile entegre çalışabilmesi, e-posta entegrasyonun sağlanması ve görüşmelerin ses kaydının yapılması artık bir zorunluluk haline gelmiş durumdadır. İletişim teknolojilerinin hızla gelişmesi ile birlikte yazılı ve

sesli iletişim olanakları artmış ancak bu durum görsel iletişime olan ihtiyacı ortadan kaldırmamıştır. Görsel iletişim için gerekli olan veri iletişimi altyapısı yıllar öncesinde düşük kalitede, çok da verimli olmayan ve yüksek maliyetli veri hatları üzerinde kısıtlı imkânlarla gerçekleştirilebiliyordu. Günümüzde ise, veri iletişim altyapı teknolojilerinin hızlı gelişimi ve maliyetlerin düşmesi, video konferans teknolojilerinin gelişmesine imkân sağlamıştır. Video konferans ve Telepresence teknolojilerinde, yüksek çözünürlüklü HD (720p / 1080p) kalitesinde çoklu video konferans ve Telepresence toplantıları gerçekleştirilebilmektedir. Telepresence çözümlerinde, 65 inch LCD ekranların kullanılması ve toplantı odasının uygun tasarım ile birlikte; neredeyse birebir ölçekte toplantılar yapmak, aynı odada bulunuyormuş hissini yaşamak mümkündür.

WAN bağlantıları üzerinden veri iletişiminin yanı sıra ses iletişiminin de gerçekleştirilmesi ve telefon iletişim maliyetlerinin düşürülmesi hedeflenmektedir. Ses ağ geçitleri ve geleneksel telefon santrallerinin (PBX) tam olarak entegre olmadığı hibrid yapıdaki çözüm, yerini gelişen teknoloji ile birlikte veri iletişimi için kullanılan kablolama ve ağ altyapısı üzerinde çalışan IP Telefon sistemlerine bırakmaktadır. IP Telefon sistemleri geleneksel ses iletişiminin yanı sıra gelişmiş uygulamaları da olanaklı kılmaktadır.

Bu tez çalışmasına konu olan şirketin yönetim binası network dizaynında tümleşik iletişim networkü tasarımında Cisco tümleşik iletişim ailesi ürünlerine yer verilmiştir. Bunun avantajları şöyle sıralanabilir:

i. Bir kişiye ulaşmak için birçok farklı adres yerine tek bir telefon numarası ya da internet adresine ihtiyaç duymaktadırlar.
ii. Tümleşik iletişim e-posta, anlık mesajlaşma ve takvim gibi farklı iletişim teknolojilerini telefon, sesli mesaj ya da video gibi iletişim cihazları ile bir araya getirmektedir.
iii. Bu yapı gelişmiş masaüstü fonksiyonalitesi ile basit kullanıcı arayüzü sağlamaktadır. Bu sayede kullanıcılar sadece tıklayarak sesli, web üzerinden ya da görüntülü konferans başlatabilmektedirler.

iv. Anlık mesajlaşmanın sınırlarını genişletmek ya da farklı cihazlar (mobil ya da sabit cihazlar) ve uygulamalar arasında varlık bilgilerini güncellemek gibi olanaklar sunmaktadırlar.
v. Merkezi mimarisi kurulum, yönetim ve genişletmeyi basitleştirmektedir.
vi. Tüm iletişim ve network ihtiyacını tek bir altyapı üzerine kurmak toplam sahip olma maliyetini ortalama yüzde 40 mertebesinde düşürmektedir.

#### *3.3.1.4 Kablosuz Network Teknolojileri*

Yerel iletişim ağ ortamlarında hızla mobilitenin artması ve kablolamanın kolay olmadığı ortamlar için, kablosuz ağ çözümleri kullanılarak, önceleri 2Mb/s ve 11Mb/s'lerden başlayan iletişim hızları da zamanımızda 300 Mb/s'lere ulaşmıştır. Bu çözümler kullanılarak, ofislerde kullanıcılara daha esnek ve hareketli çalışma ortamları sağlanmıştır. Kablosuz iletişim ağları çözümleri, ofis içerisinde kapalı ortamlarda kullanılabileceği gibi, ofis dışı açık ortamlarda da desteklenebilmektedir. Bu bağlamda, özellikle kampüs ortamlarında, kablo çekmenin zor olduğu binalar arası bağlantılarda kablosuz ağ çözümleri yaygın olarak kullanılmaktadır.

Kablosuz yerel ağlar havadan yayılan elektromanyetik dalgalarla bir noktadan başka bir noktaya fiziksel bağlantı olmaksızın bilgi iletişimini sağlar. Radyo dalgaları uzaktaki bir alıcıya enerji verdiği için alıcı tarafından kusursuz bir şekilde alınır. Bu metoda modülasyon da denir. Veri taşıyıcı üzerine bir kez bindirildikten sonra radyo sinyali bir frekanstan daha fazla frekans işgal edecektir. Çünkü modüle edilecek bilgi de taşıyıcının üzerine binecektir. Böylece birden fazla taşıyıcı frekans girişim olmaksızın aynı uzayda bulunabilecektir. Bilgiyi almak için alıcının belli bir frekansa ayarlaması yeterli olacaktır zira alıcı diğer frekansları reddedecektir. Tipik bir kablosuz yerel ağ konfigürasyonunda, erişim noktası denilen hem alıcı hem verici konumundaki cihaz standart kablolamayla, kablolu ağa bağlanır. Erişim noktası kablolu ağ omurgası ve kablosuz ağ arasında veri alışverişini üstlenir. Bir erişim noktası kapasite ve özelliklerine bağlı olarak birkaç yüz metreye kadar bir kullanıcı grubuna hizmet verebilir. Erişim noktası genelde yüksek bir noktaya konur fakat istenilen kapsama alanı

sağlandıkça her noktaya konulabilir. Uç noktalar ise kablosuz ağa, kablosuz ağ adaptörleriyle, dizüstü bilgisayarla, ve mobil cihazlar ile erişirler. Kablosuz ağ adaptörleri sunucudaki ağ işletim sistemi ile manyetik dalgalar arasında bir anten yardımıyla köprü oluştururlar.

Tümleşik ağ denetimi, ölçeklenebilirliği, güvenliği ve güvenilirliği için kablolu ve kablosuz ağ entegrasyonu kritik öneme sahiptir. Tümleşik ağ hizmetleri, kablosuz LAN denetleyiciler (WLAN Controller), tümleşik anahtarlar ve yönlendiriciler gibi çeşitli platformlarda sağlanır ve böylece ağ yöneticileri kurumsal sınıfta güvenli kablosuz ağlar kurabilirler. Gelişmiş yönetim, kablosuz LAN planlama, yapılandırma ve yönetiminin yanı sıra konum izleme olanağı sunar. Kablosuz LAN denetleyiciler, gelişmiş yönetim özellikleri ve gelişmiş performans için var olan kurumsal ağlarla entegre olur. Bunlar erişim noktalarıyla tüm OSI 2.katman (Ethernet) veya OSI 3. katman (IP) altyapıları üzerinden iletişim kurar ve sistem çapında işlevlerin uygulanmasından sorumludur (http://www.arubanetworks.com/pdf/technology/whitepapers/wp_PCI.pdf).

#### *3.3.1.5 Altyapı Kablolama Teknolojileri*

Koaksiyel kablo içi boş silindirik iletken metalden yapılmıştır. Etrafında iki iletken elementten yapılmış iç kablo vardır. Bu elementlerden bakır kablonun tam ortasından geçer ve kablonun esnek olmasını sağlar. Diğer element ise kablonun etrafında kabloya kalkan vazifesi görür. Bu kalkan kabloyu etrafındaki elektromanyetik dalgalara ve kemirgen haşerelere karşı korur.

Lokal ağlar için koaksiyel kablonun birkaç avantajı vardır. Kalkanlı (STP) ve kalkansız (UTP) olması fark etmeksizin tekrarlayıcıya ihtiyaç duymadan uzun mesafelerde kullanılabilmesidir. Koaksiyel kablo fiber optik kabloya göre daha ucuz olması ve teknolojisinin uzun yıllardan beri bilinmesi nedeniyle genel olarak daha fazla kullanılmaktadır. Farklı alanlarda kullanılmasına rağmen yaygın olarak her çeşit veri

transferinin yapıldığı yerler ve kablolu televizyon dağıtım şebekesi gibi yerlerde kullanılır.

Kalkanlı çift bükümlü kablo (STP) kalkanlama, bozma ve bükümleme tekniklerinin bir karışımıdır. Her kablo çifti metal kılıf içerisine yerleştirilmiştir. Metal kılıf içerisine yerleştirilen dört çift kablonun tamamı ayrıca bir metal kılıf içine daha yerleştirilmiştir. 150 ohm'luk bir kablodur. Ethernet ağlarında kullanılan STP, elektriksel gürültülerden etkilenmezler. Örnek olarak elektromotor kuvvetin yaratmış olduğu elektromanyetik dalgalar veya radyo frekansları verilebilinir. STP kablo her ne kadar dış etkenlerden daha az etkilense de UTP kablodan hem daha pahalı hem de kurulumu UTP' ye göre daha zordur.

Kalkansız bükümlü kablo çifti (UTP) bazı ağlarda kullanılan ve dört parçadan oluşan kablo çeşididir. UTP kablosunu oluşturan sekiz tane kablodan her birinin etrafı bir yalıtkan malzemeyle kaplıdır. Buna ilaveten her kablo çifti diğer çift üzerine bükülür. Bu tip kablolarda elektromanyetik dalgalardan kaynaklanan sinyal kesim etkileri kolaylıkla önlenebilir. UTP kablolarının arasındaki sinyal kesimini azaltmak kabloların büküm sayısına bağlıdır. STP kablolarına benzer olarak UTP kablolarının da bir adımdaki büküm sayısı kablonun değişik özellikler sergilemesini sağlar.

Optik fiber ağlarında kullanılan ışık bir nevi elektromanyetik enerjidir. Elektrik yük bir yerden bir yere hareket ettiğinde veya ivmeli bir hareket kazandığında elektromanyetik güç oluşur. Dalga olarak şekillenen bu enerji çeşidi bir vakuma doğru yol alır. Bu dalga enerjisinin bu özelliğine dalga boyu denir. İnsan gözüyle görülmeyen dalga boyları fiber optik veri transferinde kullanılır. Bu dalga boylarının uzunluğu kırmızı dalga boylarının uzunluğundan daha fazladır ve bu yüzden kızıl ötesi ışık diye adlandırılırlar. Kızıl ötesi ışıklar televizyonların uzaktan kumandalarında kullanılır. Optik fiber veri transferinde kullanılan dalgaların boyları 850,1310 veya 1550 nanometredir. Bu dalga boylarının seçilme sebebi, veri iletiminde diğer dalga boylarına nazaran daha iyi performans sağlamasıdır.

Tek modlu fiber kablo çok modlu fiber kablo ile aynı parçalardan meydana gelir. Tek modlu fiberin dış ceketinin rengi genellikle sarı olur. Çok modlu fiber kablo ile tek modlu fiber kablonun arasındaki en temel farklılık, tek mod fiber kablonun adından da anlaşılacağı gibi tek modda iletim yapmasıdır. Tek modlu fiberin çekirdek yarıçapı 8-10 mikron yarıçapındadır. 9 mikronluk çekirdek çok yaygındır. Kablo ceketinde yazan 9/125 olarak tanımlanan tek modlu fiber kablonun çekirdek yarıçapı 9 ve dış kılıf yarıçapının 125 mikron olduğu anlaşılır. Çok modlu fiber ise çok modda iletim yapar daha fazla veri taşıyabilmesine karşın iletim mesafesi daha düşüktür. Tek modlu fiber 60 km'ye kadar kesintisiz veri iletimi yapabilmesine rağmen, çok modlu fiberde bu mesafe 10 km'dir.

**Şekil 3.25: Fiber Zayıflama Değerleri**

| Fiber Tipi | | MULTIMODE | MULTIMODE | SINGLEMODE |
|---|---|---|---|---|
| Dalgaboyu | | 50µm | 62.5µm | 8 – 10µm |
| Zayıflama (dB/km) | 850nm | 2.5 | 3.5 | N/A |
| | 1300/1310nm | 0.8 | 1.4 | 0.3 |
| | 1550nm | N/A | N/A | 0.2 |

*Kaynak:* http://en.wikipedia.org/wiki/Optical_fiber

### 3.3.2 KULLANILAN TEKNİK EKİPMANLAR

Bu bölümde fiziksel network tasarımında kullanılan teknolojiler için konumlandırılan teknik cihazlar incelenecektir. Bu cihazların niçin, hangi fonksiyonlarla konumlandırıldıkları belirtilerek uygulamaya yönelik tasarımlar için fikir oluşturabilecektir.

### *3.3.2.1 Temel Network Dizaynında Kullanılan Teknik Ekipmanlar*

Fiziksel tasarımda kullanılan teknolojiler baz alınarak hazırlanan bu bölümde örnek bir şirket binasının network dizaynına ilişkin temel network haberleşmesi için kullanılan cihazlar, bu bölümde detaylı olarak açıklanacaklardır.

Erişim katmanında son kullanıcı cihazlarının bağlantılarının yapılabilmesi için 48 portlu Cisco marka WS-C2960S-48LPD-L anahtarları kullanılmıştır. Bu anahtar ile kullanıcıya bağlanan tarafta 1 gigabitlik bağlantılar ile kullanıcıların bilgisayar, IP telefon, kablosuz erişim noktası cihazları sonlandırılmıştır. Dağıtım katmanına bağlanan portlarda ise 10 gbps'lik 2 adet (yedekli yapı düşünülmüş) bağlantı bulunmaktadır. Bu anahtarın anahtarlama kapasitesi 88 gbps'dir. Doğal olarak anahtar 40 port üzerinden maksimum trafikte 40x10=40gbps, 2 adet 10 gbps port üzerinden de maksimum trafikte 2x10=20gbps, toplamda 40+20=60 gbps'lik bir trafik oluşturulabilir. Anahtarlama kapasitesi 88 gbps olan bu anahtarın tüm portları maksimum trafik ile dolu iken bile tıkanmasız olarak çalışabilmektedir. Bu anahtar aynı zamanda yığınlama özelliğini de desteklemektedir. Bu teknoloji anahtarın birbirine özel yığınlama kablolarıyla bağlanmasıyla sistemi yedekli bir yapıya kavuşturmaktadır. Herhangi bir anahtarın bozulması durumunda veriler yığın kabloları üzerinden diğer anahtara taşınacak ve veri iletimi kesintisiz bir şekilde devam edecektir. Kesintisiz derken bu oran, anahtarın yığın anahtarlama kapasitesine bağlıdır ki bu anahtar 20 gbps yığın anahtarlama kapasitesini desteklemektedir. Ayrıca anahtarın diğer bir özelliği Ethernet üzerinden güç transferine olanak veren PoE teknolojisini desteklemektedir. Bu sayede IP telefonlar ve kablosuz erişim noktaları için ayrıca birgüç kablosu çekilmek zorunda kalınmayacak, böylelikle güç kablosu maliyet ve dizayn karmaşıklığı masraflarından kazanç sağlanacaktır. Bu anahtardan kullanıcı sayıları, bilgisayar, kablosuz erişim noktası ve IP telefonlar hesaba katılarak 20 adet konumlandırılmıştır.

Dağıtım katmanında 20 adet erişim katmanı anahtarının bağlanabileceği Cisco marka WS-C4507R+E anahtarı konumlandırılmıştır. Bu anahtarlarda 10gbps'lik portlar sonlanacak ve omurga katmanına erişim için 4'er adet 10gbps port (toplamda 40gbps) ayrılmıştır. Yedeklilik için her omurga anahtara birer adet bağlantı yapılacaktır. Omurga

anahtara bağlanan portlar aslında 10 gbps'lik hıza sahip 4 adet porttur. Burada 4 portu hız olarak tek port gibi gösterecek olan etherchannel teknolojisi kullanılmıştır. Dağıtım katmanındaki anahtarlar yönlendirme protokollerini destekleyecek şekilde uygun lisanslamalar ile donatılmış, sistemde çalışacak olan EIGRP protokolünü sorun olmadan kaldırabileceklerdir. Ayrıca hem merkezi işlemci birimleri hem de güç kaynakları şasi üzerinde de ikişer adettir. Dolayısıyla her bir anahtar aynı zamanda kendi içerisinde de yedekli çalışmaktadırlar. Anahtarlar hem erişim katmanından gelecek bağlantılara hem de omurga anahtarına gidecek olan bağlantılara uygun kartlar ile donatılmışlardır.

Omurga katmanında ise yüksek anahtarlama yapabilecek Cisco marka Nexus N7K-C7010 anahtar konumlandırılmıştır. Yedeklilik düşünülerek iki adet omurga anahtar konumlandırılmış, bu iki anahtar da aynı zamanda birbirlerine fiziksel bağlantı ile bağlanmışlardır. Bu sayede hem yedeklilik hem de yük dağılımı yapılabilmektedir. Omurga katmanındaki anahtarlar yönlendirme protokollerini destekleyecek şekilde uygun lisanslamalar ile donatılmış, sistemde çalışacak olan EIGRP protokolünü sorun olmadan kaldırabilecek düzeydedirler. Ayrıca hem merkezi işlemci birimleri hem de güç kaynakları şasi üzerinde de ikişer adettir. Dolayısıyla her bir anahtar aynı zamanda kendi içerisinde de yedekli çalışmaktadırlar. Omurga anahtarlar hem dağıtım katmanından gelecek bağlantılara uygun, hem de sunucu çiftliği ve güvenlik duvarı bağlantılarına uygun kartlar ile donatılmışlardır. Detaylı malzeme listesi ekler bölümünde ayrıntılı olarak verilmiştir.

#### *3.3.2.2 Güvenlik Dizaynında Kullanılan Teknik Ekipmanlar*

Fiziksel tasarımda kullanılan teknolojiler baz alınarak hazırlanan bu bölümde örnek yönetim binası güvenlik dizaynına ilişkin kullanılan cihazlar, detaylı olarak açıklanacaklardır.

Güvenlik network tasarımında bir adet güvenlik duvarı yerel ağ ile dış ağ arasındaki güvenlik kontrollerini sağlayabilmek amacıyla konumlandırılmıştır. Güvenlik duvarını seçerken dikkat edilmesi gereken şey; güvenilir bir üreticinin ürününü almak, destek vb.

konularda sıkıntı çekmemek ve veri yolu genişliği (throughput) değerinin büyüklüğüdür. Dizaynda konumlandırılan güvenlik duvarının modeli Cisco marka ASA5540-K8 ve paket işleme kapasitesi saniyede 1.2 gbps'dir. Yani dışarıdan gelecek bağlantılarda saniyede 1.2 gigabitlik veriyi işleyebilir.

**Şekil 3.26: ASA 5540**

*Kaynak:*
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html

IDS/IPS sistemi olarak da yine Cisco'nun 5540 IPS versiyonu olan ASA5540-AIP40-K9 ürünü konumlandırılmıştır. Bu sayede dışarıdan ya da içeriden gelebilecek ataklar daha hazırlık aşamasındayken yakalanabilir.

### *3.3.2.3 Tümleşik İletişim Dizaynında Kullanılan Teknik Ekipmanlar*

Örnek şirket binaları network dizaynı projesinde kullanılan tümleşik iletişim yapıları için birçok ürün konumlandırılmıştır. Çağrı yönetimi için Cisco marka çağrı yönetim yazılımı olan CUCM (Cisco Unified Communications Manager), IP telefon olarak çeşitli modellerde Cisco IP telefon modelleri, PSTN hatlarına PRI ve FXO bağlantıları için Cisco CISCO3945-V/K9 modeli ses ağ geçitleri, sesli mesaj özelliklerini devreye alabilmek için Cisco sesli mesaj servisi olan Unity Connection ve yine Cisco'nun çağrı merkezi yazılımı olan UCCX (Unified Contact Center Express) konumlandırılmıştır. CUCM, Unity Connection ve UCCX yazılım tabanlı çözümler olup bunların donanımı olarak VMWare sanallaştıma ortamı üzerinden tek şaside çalışabilen UCS-C210M2-VCD2 sanal sunucusu belirlenmiştir.

Yapılan dizaynın çalışma mantığı da şöyle özetlenebilir:

Bu sistemdeki tüm haberleşme IP üzerinden gerçekleşiyor olup kontrol protokolleri iki sınıfa ayrılabilmektedir. Ses ağ geçitleri H.323, MGCP veya SIP protokolleri üzerinden; IP telefonlar ise SCCP ya da SIP protokolleri üzerinden yönetilebilmektedirler. Ses ağ geçitlerinin temel amacı PSTN bağlantılarını sonlandırmak ve tüm ses trafiğini üzerlerinden uygun biçimde geçirmektir. Dolayısıyla codec dönüşümü, analog sinyalleşmenin IP'ye dönüştürülmesi, IP paketlerinin analog sinyallere dönüştürülmesi gibi görevleri üstlenmektedir. Çağrı yöneticisi tüm ses trafiğinin kontrolünü sağlamaktadır (Ahmed & Siddiqui 2011, p.90). Üzerinden herhangi bir ses paketi geçmemektedir sadece sinyalleşme paketleri çağrı yöneticisi üzerinden geçmektedir. Bu durumda çağrı yöneticisi belirlenen kurallara, konfigürasyonlara göre yönetim yapılabilmektedir. Arama kısıtlamaları çağrı yöneticisinde belirtildiği için istenilen kişilerin belirlenen yeri arayabilmeleri ya da arayamamaları kolay bir şekilde uygulanabilmektedir. Sesli mesaj sistemi için belirlenen çözümde sesli mesaj sunucuları çağrı yöneticisi ile entegre olacaktır. Tek mesaj kutusu sesli mesajların e-posta ile de ilgili kişinin posta kutusuna gönderilmesini sağlamaktadır. Çağrı yöneticisinde yapılacak bir konfigürasyon ile cevapsız, meşgul ya da bir çok sayıda koşula göre belirlenebilecek kriterlere göre sesli mesaj sunucularına yönlendirme sağlanacaktır. Gelen çağrılar için karşılama mesajı okunarak ilgili departmanlara yönlendirme yapılabilir. İstenirse de ilgili kişinin dahilisi tuşlanarak o kişinin telefonuna da yönlendirme yapılabilir.

#### *3.3.2.4 Kablosuz Network Dizaynında Kullanılan Teknik Ekipmanlar*

Yedi katlı örnek şirket binasının kablosuz ağ tasarımında uygun şekilde yerleştirilmiş 35 adet erişim noktası bulunmaktadır. Aktif olarak kullanılan ilk 4 kata 6'şar erişim noktası kapsayacakları alanlar yaklaşık olarak öngörülerek konumlandırılmıştır. Karşılama, toplantı odaları ve misafirlerin bekleyeceği bekleme alanlarını barındıran giriş katına 7, kafeteryanın bulunduğu teras katına ise 4 adet erişim noktası yerleştirilmiştir.

**Şekil 3.27: LAP 1142 erişim noktası**

*Kaynak:* http://www.cisco.com/en/US/products/ps10092/index.html

Kablosuz erişim noktası olarak dual bantta çalışabilen (hem 2.4 ghz hem 5 ghz), 802.11n teknolojisi ile 300 mbps bant genişliğine sahip çoklu giriş ve çoklu giriş antenlerini kendi üzerinde barındıran Cisco marka AIR-LAP1142-EK9 modeli belirlenmiştir.

**Şekil 3.28: 5508 kablosuz denetleyici**

*Kaynak:* http://www.cisco.com/en/US/products/ps10325/index.html

Bu erişim noktalarını hem yayın gücü, hem de çalışma algoritması ve konfigürasyon dağıtıcısı olarak denetleyen kablosuz ağ denetleyicisi (WLAN Controller) olarak da Cisco marka AIR-CT5508-50-K9 cihazı konumlandırılmıştır. Bu cihaz 50 adet erişim noktasına kadar kontrol sağlayabildiği için ileriki zamanlardaki kablosuz ağın büyümesi ve erişim noktası sayısının artmasına göre ölçeklenebilir bir yapı sunmaktadır.

### *3.3.2.5 Altyapı Kablolama Dizaynında Kullanılan Teknik Ekipmanlar*

Bu tez çalışmasının konusu olan örnek şirket binasının altyapı tasarımında yapısal kablolama iki boyutta incelenmiştir:

İlki binanın dikey yönünde, sistem odasından kat aralarındaki dağıtım katmanı anahtarlarına ve oradan da her katta kullanıcı miktarına göre değişebilen sayıda bulunan

erişim katmanı anahtarlarına giden fiber kablolamadır. Burada veri iletim miktarı ve binadaki uzunluklar hesaba katılarak tek modlu (single mode) fiber kablo seçimi ve sonlandırması yapılmıştır. İkinci boyut ise, erişim katmanı anahtarlarından son kullanıcı uç noktalarına, IP telefonlara ve kablosuz erişim noktalarına giden UTP bakır yatay kablolamadır. UPT kablo teoride 100 metreye, pratikte ise 90 metreye kadar kayıpsız bir şekilde veri iletebildiği için, erişim noktası anahtarlarının konumları bina içi dağılıma göre değişiklik göstermektedir.

Kablo seçiminde hem bakır hem de fiber kabloda dünyaca kabul gören standartlara sahip AMP marka kablo konumlandırılmıştır. Fiber ve bakır sonlandırmada Rittal marka patch panel'ler kullanılmıştır.

Fiber sonlandırmada patch panel ile aktif cihaza giden uçtaki sonlandırma tipleri önemlidir. Bu sonlandırma tipleri anahtar markalarına göre farklılık göstermekte, dolayısıyla kablolama sonlandırma dizaynında da aktif cihaz bilgilerine göre değerlendirme yapmak esastır. En çok kullanılan fiber optik kablo konnektörü ST konnektördür. ST konnektör, barrel tipi dediğimiz BNC konnektörünün bir benzeridir. SC konnektör yeni bir tiptir ve giderek daha fazla tercih edilmeye başlanmıştır. SC konnektör, kare yüzlüdür ve montajı daha kolaydır. Dizaynda fiber sonlandırma için kullanılan Cisco SFP'lerin sonlandırma tipi SC olduğundan buradaki kablo sonlandırmaları SC olarak belirlenmiştir.

# 4. BULGULAR

Yapılan çalışma sonucunda elde edilen bulgular şöyle sıralandırılabilir:

Network dizaynı sistematik bir çalışma gerektirir. Tasarım yaparken belli bir yöntem, belli bir metodoloji belirlenmelidir. Bu sayede belli bir düzende çalışma yapılmakta ve ilerleme hızlı ve sağlam olmaktadır.

Müşteriye uygun çözümde analiz yapılırken teknik ihtiyaçlar kadar iş ihtiyaçlarına da yer verilmeli, yönetimin vizyonu ve gerçekleştirmek istediklerine dair çalışma yapılmalıdır. Çünkü asıl önemli olan sonuç kurumların işleyişlerine daha verimli ve sorunsuz bir şekilde devam edebilmeleri, bunun da şirketlere kar ve kazanç olarak geri dönebilmesidir.

Analiz yapıldıktan sonra ortaya çıkan veriler eşliğinde öncelikle sistemin mantıksal bir topolojisinin çıkarılması gerekir. Bu mantıksal çalışmada tasarım çalışmasının ne kadar kolay ve sistematik gittiğine dair sonuçlar çıkmıştır.

Mantıksal tasarım çalışmasından sonra buradan elde edilen veriler ile fiziksel çalışmaya başlamak ürün ve teknoloji seçimini çok anlaşılır ve kolay bir hale getirmiştir. Bu sayede projeyi kurulum ve devreye alma aşamasına geçecek olan operasyon ekibine bir bulmacanın parçalarını rahatlıkla yerleştirebilecek şekilde sistemli bir bilgi aktarımı gerçekleştirilebilir.

Tüm haliyle paralel hiyerarşik yaklaşım ses networkü, güvenlik networkü gibi her teknolojinin kendi içerisinde yukardan aşağıya hiyerarşik bir yapıda; kendi aralarındaki gereksinimlere göre de paralel dizayn uygulanmıştır. Bu yüzden ismi paralel hiyerarşik yaklaşımdır.

# 5. TARTIŞMA

Bu tez çalışmasında mevcut literatüre katkı olarak ortaya çıkan tüm network sistemlerini hesaba katarak yapılacak olan bir çalışmada hangi teknoloji ve ekipmanların diğerlerini nasıl ve ne şekilde etkiledikleri, dizayna başlamadan önce ve dizayn aşamasında hangi yolların izlenmesi gerektiği konularında yeni metodolojiler üretilmiştir.

Büyük bir kurumda bu çalışmayı uygulamış olmak sonuçlarının kabul edilirliği anlamında çalışmaya çok büyük katkı sağlamıştır. Diğer büyük kurumların da network dizaynlarında örnek alınabilecek bir çalışma konumundadır. Var olan, daha önceden sınanmış hipotezler bu çalışmada baz alınmıştır. Onların doğrulukları temelde kabul edilmiş, eksik yanlarına alternatif olarak yeni sistemde geliştirmeler yapılmıştır. Teze başlanırken ki amaç yeni bir dizayn metodolojisi uygulayıp bunun sağlıklı bir şekilde çalıştığını gözlemlemektir. Dolayısıyla giriş bölümünde anlatılan amaca ulaşılabilmiştir. Paralel hiyerarşik yaklaşım tez çalışması boyunca rehber edinilmiş ve sonuçları da uygulamalı olarak gösterilmiştir. Paralel hiyerarşik yaklaşım yerine yukarıdan aşağıya, aşağıdan yukarıya ya da mesh tasarım yaklaşımları kullanılsaydı; tasarımın bütününü görebilme ve her teknolojiye aynı zamanda müdahale edebilme alanımız daralacağından bu yaklaşımın avantajları proje planı ve süresini direk olarak etkilemektedir. Ayrıca kurulum yapıldıktan sonra oluşabilecek problemlerde de paralel hiyerarşik yaklaşımın avantajları olacaktır.

Bu konu ile ilgili bundan sonra yapılacak olan çalışmalarda "Paralel Hiyerarşik Yaklaşım"ın fiziksel uygulamalara olan etkilerini daha fazla örnek ile incelenip daha kesin ve somut veriler elde edilebilir. Bu tez çalışmasında sadece bir örnek üzerinden tüme varım metodu ile bir yakınsama yapılmıştır. Daha reel örnekler ile yaklaşımın var olan sonuca ne kadar etki edebildiği gözlemlenebilir. Bundan sonra yapılacak olan çalışmalar özellikle video networkleri alanına yoğunlaşabilir. Çünkü video networkleri günümüz dünyasında oldukça etkin ve kullanılır durumdadır. Mobil haberleşmenin de yaygınlaşması ile video networklerine olan gereksinim daha da artmaktadır.

# 6. SONUÇ

Bu çalışma, farklı teknolojilere ait tasarım yöntemlerini irdelemiş, bunları birleştirerek ve eksik kaldıkları yerde tamamlayarak tüm network dizaynına ilişkin bir model ortaya koymuştur. Bu model "Paralel Hiyerarşik Model"dir.

Daha sonra ortaya konulan bu yeni metodoloji saygın ve sözü geçer bir kurumda network ve altyapı proje dizaynında uygulanmıştır. Hem teorik bilgiler ile bir yöntem oluşturan çalışma, hem de verdiği pratikteki uygulamalar ile gerçek hayata yönelik olarak kullanılabilecek nitelikte sonuçlar ortaya çıkarabilir.

Paralel hiyerarşik yaklaşım ile proje teslim süresinin veriminde, proje motivasyonunun seviyesinde ve sistemin geliştirilebilirliğinde iyileşmeler ortaya çıkmakta ve bu da yapılan işin kalitesini arttırmaktadır.

# KAYNAKÇA


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

Albitz, P. & Liu C., 2006. *Dns and bind*, 5. Baskı, California: O'Reilly Media

Anthony, B., 2000. *Ccda exam certification guide*, Indianapolis: Cisco Press

Clark, K. & Hamilton K., 1999. *Cisco lan switching*, Indiana: Cisco Press

Chu L., Lan X. & Tan Y., 2011. *The design and simulation of the enterprise's voip Network*, IEEE

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

Gast, M., 2002. *802.11 wireless networks: the definitive guide*, Sebastopol, California: O'Reilly & Associates, Inc.

Glenn D., 2007. *Designing an efficient network architecture*, Broadcast Engineering

Habib S., 2005. *Redesigning network topology with technology considerations*, IEEE

Hines, Annlee A., 2003. *Planning for survivable networks*, New York: Wiley Publishing Inc.

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

Jingsha H., 1997. *Performance and manageability design in an enterprise network security system*, IEEE

Lewis, J., 2008. *Sdlc 100 success secrets - software development life cycle (sdlc) 100 most asked questions, sdlc methodologies, tools, process and business models*, Avustralya: Emereo Publishing

Michael A., 1997. *Planning enterprise networks to meet critical business needs*, IEEE

Moy, J.T., 1998. *Ospf: anatomy of an internet routing protocol*, Minnesota

Norris M. & Pretty S., 2000. *Introducing the Enterprise Network Lifecycle and Design Process*, California: Wiley

Oppenheimer, P., 2011. *Top-down network design*, 3. Baskı, Indianapolis: Cisco Press

Roebuck, K., 2011. *Systems development life cycle (sdlc): high-impact strategies – what you need to know: definitions, adoptions, ımpact, benefits, maturity, vendors*, California

Spohn, D., 2002. *Data network design*, 3. Baskı, Osbourne: McGraw-Hill

Sung E., Sun X., Rao S., Xie G., & David A., 2010. *Systematic design of enterprise networks*, IEEE

Yao, L. & Chen X., 2009. *Business video ready enterprise ıp network architecture*, IEEE

# EKLER

## DİZAYN DOKÜMAN LİSTESİ

| Product | Description | Quantity |
|---|---|---|
| WS-C2960S-48LPD-L | Catalyst 2960S 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base | 20 |
| CAB-ACE | AC Power Cord (Europe), C13, CEE 7, 1.5M | 20 |
| C2960S-STACK | Catalyst 2960S FlexStack Stack Module optional for LAN Base | 20 |
| CAB-STK-E-0.5M | Cisco FlexStack 50cm stacking cable | 20 |
| CON-CSSPD-2960S4TD | SHARED SUPP SDS Cat2960S Stk48 GigE,2x10G SFP+ LAN Base | 20 |
| SFP-10G-SR | 10GBASE-SR SFP Module | 20 |
| | | |
| WS-C4507R+E | Catalyst 4500E 7 slot chassis for 48Gbps/slot | 2 |
| PWR-C45-1400AC | Catalyst 4500 1400W AC Power Supply (Data Only) | 2 |
| PWR-C45-1400AC/2 | Catalyst 4500 1400W AC Power Supply Redundant(Data Only) | 2 |
| CAB-CEE77-C19-EU | CEE 7/7 to IEC-C19 13ft Europe | 4 |
| WS-X4712-SFP+E | Catalyst 4500 E-Series 12-Port 10GbE (SFP+) | 2 |
| SFP-10G-SR | 10GBASE-SR SFP Module | 16 |
| WS-X4712-SFP+E | Catalyst 4500 E-Series 12-Port 10GbE (SFP+) | 2 |
| SFP-10G-SR | 10GBASE-SR SFP Module | 16 |
| WS-X45-SUP7-E | Catalyst 4500 E-Series Supervisor, 848Gbps | 2 |
| WS-X45-SUP7-E/2 | Catalyst 4500 E-Series Supervisor, 848Gbps | 2 |
| WS-X4712-SFP+E | Catalyst 4500 E-Series 12-Port 10GbE (SFP+) | 2 |
| SFP-10G-SR | 10GBASE-SR SFP Module | 16 |
| C4500E-IP-ES | Paper IP to Ent Services License | 2 |
| S45U-32-1502SG | CAT4500e SUP7e Universal Image | 2 |
| CON-CSSPD-C4510R+E | SHARED SUPP SDS Catalyst 4500E 10 slot chassis for 48Gbp | 2 |
| | | |
| N7K-C7010 | 10 Slot Chassis, No Power Supplies, Fans Included | 2 |
| N7KS1K9-60 | Cisco NX-OS Release 6.0 | 2 |
| N7K-ADV1K9 | Nexus 7000 Advanced LAN Enterprise License (VDC, CTS ONLY) | 2 |
| N7K-M132XP-12 | Nexus 7000 - 32 Port 10GbE, 80G Fabric (req. SFP+) | 2 |
| SFP-10G-SR | 10GBASE-SR SFP Module | 16 |
| N7K-M132XP-12 | Nexus 7000 - 32 Port 10GbE, 80G Fabric (req. SFP+) | 2 |
| SFP-10G-SR | 10GBASE-SR SFP Module | 16 |
| N7K-M148GT-11L | Nexus 7000 - 48 Port 10/100/1000 Module with XL option | 2 |
| N7K-SUP1 | Nexus 7000 - Supervisor, Includes External 8GB Log Flash | 2 |
| N7K-SUP1 | Nexus 7000 - Supervisor, Includes External 8GB Log Flash | 2 |
| N7K-C7010-FAB-2 | Nexus 7000 - 10 Slot Chassis - 110Gbps/Slot Fabric Module | 6 |
| N7K-AC-6.0KW | Nexus 7000 - 6.0KW AC Power Supply Module | 4 |
| CAB-AC-2500W-EU | Power Cord, 250Vac 16A, Europe | 8 |
| N7K-C7010-AFLT | Nexus 7010 Air Filter | 2 |

| | | |
|---|---|---|
| N7K-C7010-FD-MB | Nexus 7010 Front Door Kit | 2 |
| N7K-SUP1-8GBUPG | Nexus 7000 Supervisor 1 8GB Memory Upgrade Kit | 2 |
| N7K-SUP1-8GBUPG | Nexus 7000 Supervisor 1 8GB Memory Upgrade Kit | 2 |
| CON-CSSPD-C7010 | SHARED SUPP SDS 10 Slot Chassis, No Power Supplies, Fans | 2 |
| | | |
| CP-7911G= | Cisco UC Phone 7911G | 155 |
| CON-CSSPD-CP7911 | SHARED SUPP SDS Cisco IP Phone 7911 | 155 |
| | | |
| CP-7942G= | Cisco UC Phone 7942, spare | 19 |
| CON-CSSPD-CP7942 | SHARED SUPP SDS Cisco Unified IP Phone 7942 | 19 |
| | | |
| CP-7945G= | Cisco UC Phone 7945, Gig Ethernet, Color, spare | 28 |
| CON-CSSPD-CP7945 | SHARED SUPP SDS Cisco Unified IP Phone 7945 | 28 |
| | | |
| CP-9951-C-CAM-K9= | Cisco UC Phone 9951, Charcoal, Std Hndst with Camera | 14 |
| CON-CSSPD-9951CSTD | SHARED SUPP SDS Cisco Unified IP Phone 9951, Charcoal, S | 14 |
| | | |
| CP-9971-C-CAM-K9= | Cisco UC Phone 9971, Charcoal, Std Hndst with Camera | 3 |
| CON-CSSPD-9971CSTD | SHARED SUPP SDS Cisco Unified IP Phone 9971, Charcoal, S | 3 |
| | | |
| CP-7962G= | Cisco UC Phone 7962, spare | 14 |
| CON-CSSPD-CP7962 | SHARED SUPP SDS Cisco Unified IP Phone 7962 | 14 |
| | | |
| CUCM-USR-LIC | Top Level Sku For User License | 1 |
| LIC-CUCM-USR-A | Unified Communications Manager Enhanced Single User-Under 1K | 233 |
| CUCM-UCS-1000-86 | Unified Communications Manager 8.6 Server Software | 1 |
| CCX-85-CMBUNDLE-K9 | CCX 8.5 5 Seat CCX ENH CM Bundle - AVAILABLE ONLY FOR NEW CM | 1 |
| CM86-UCS-1000-KIT | CUCM Auto-Expansion Media Kit | 1 |
| CUCM-PAK | Include PAK Auto-expanding PAK for CUCM | 1 |
| CUCM-USR | Include PAK Auto-expanding User for CUCM | 1398 |
| UCM-S-UCS-NODE | CUCM CUCM-UCS-1000 Node | 1 |
| CON-ESW-CMBUNDK9 | ESSENTIAL SW CCX 8.5 5 Seat CCX ENH CM Bundle - AVAIL | 1 |
| CON-ESW-CUCMUSR | ESSENTIAL SW Top Level Sku For User License | 1 |
| CON-ESW-EUSRA1 | ESSENTIAL SW Unified Comm Mgr Enh Sngle User Under 1K | 233 |
| | | |
| UCS-C210M2-VCD2 | Bare Metal UCS C210M2 Svr.,2xE5640 CPU,48GB RAM,10x146GB HDD | 1 |
| CAB-9K10A-EU | Power Cord, 250VAC 10A CEE 7/7 Plug, EU | 2 |
| UC-A01-X0109 | 2.66GHz Xeon E5640 80W CPU/12MB cache/DDR3 1066MHz | 2 |
| UC-A03-D146GC2 | 146GB 6Gb SAS 15K RPM SFF HDD/hot plug/drive sled | 10 |

| | | |
|---|---|---|
| | mounted | |
| UC-N01-M304GB1 | 4GB DDR3-1333MHz RDIMM/PC3-10600/dual rank 1Gb DRAMs | 12 |
| UC-N2XX-ABPCI03 | Broadcom BCM5709 Quad Gig E card (10/100/1GbE) | 1 |
| UC-R210-ODVDRW | DVD-RW Drive for UCS C210 M1 Rack Servers | 1 |
| UC-R2XX-PL003 | LSI 6G MegaRAID PCIe Card (RAID 0, 1, 5, 6, 10, 60) - 512WC | 1 |
| UC2-R2X0-PSU2-650W | 650W power supply unit for UCS C210 M1 Rack Server | 2 |
| CON-UCS1-C210M2VC | UC SUPPORT 8X5XNBD Bare Metal UCS C210M2 Svr.,2xE5640 CPU,4 | 1 |
| VMW-UC-STD-K9-1A | VMware ESXi 4 Standard (2 CPU), 1 yr support required | 1 |
| VMW-VS-STD-1A | VMware vSphere Standard (1 CPU), 1 yr support required | 2 |
| CON-ISV1-UCSTD1A | ISV 24X7 VMware vSphereESXi 4.0 Std,2 CPU,1yr sup | 1 |
| CON-ISV1-VSSTD1A | ISV 24X7 VMware vSphere Std (1 CPU), 1 yr supp re | 2 |

| | | |
|---|---|---|
| CISCO3945-V/K9 | Cisco 3945 Voice Bundle, PVDM3-64, UC License PAK | 1 |
| FL-SRST | Cisco Survivable Remote Site Telephony License | 1 |
| FL-CME-SRST-100 | Cisco Communication Manager or SRST- 100 seat license | 2 |
| VWIC3-2MFT-T1/E1 | 2-Port 3rd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1 | 2 |
| PVDM3-64U192 | PVDM3 64-channel to 192-channel factory upgrade | 1 |
| PWR-3900-AC/2 | Cisco 3925/3945 AC Power Supply (Secondary PS) | 1 |
| CAB-ACE | AC Power Cord (Europe), C13, CEE 7, 1.5M | 2 |
| CON-CSSPD-3945V | SHARED SUPP SDS Cisco 3945 Voice Bundle, UC License PAK | 1 |

| | | |
|---|---|---|
| ASA5540-K8 | ASA 5540 Appliance with SW, HA, 4GE+1FE, DES | 1 |
| CAB-ACE | AC Power Cord (Europe), C13, CEE 7, 1.5M | 1 |
| SF-ASA-8.4-K8 | ASA 5500 Series Software Version 8.4 for ASA 5510-5550, DES | 1 |
| ASA-ADV-END-SEC | ASA 5500 Advanced Endpoint Assessment License for SSL VPN | 1 |
| ASA5500-SC-10 | ASA 5500 10 Security Contexts License | 1 |
| ASA5500-SSL-100 | ASA 5500 SSL VPN 100 Premium User License | 1 |
| ASA-VPN-CLNT-K9 | Cisco VPN Client Software (Windows, Solaris, Linux, Mac) | 1 |
| ASA5540-VPN-PR | ASA 5540 VPN Premium 5000 IPsec User License (7.0 Only) | 1 |
| ASA5500-ENCR-K8 | ASA 5500 Base Encryption Level (DES) | 1 |
| SSM-BLANK | ASA/IPS SSM Slot Cover | 1 |
| ASA-180W-PWR-AC | ASA 180W AC Power Supply | 1 |
| ASA-ANYCONN-CSD-K9 | ASA 5500 AnyConnect Client + Cisco Security Desktop Software | 1 |
| CON-CSSPD-AS4K8 | SHARED SUPP SDS ASA5540 w500 VPN Prs, 4 GE + 1 FE, DES | 1 |

| | | |
|---|---|---|
| ASA5540-AIP40-K9 | ASA 5540 Appliance w/ AIP-SSM-40, SW, HA, 4GE+1FE, 3DES/AES | 1 |
| CAB-ACE | AC Power Cord (Europe), C13, CEE 7, 1.5M | 1 |
| SF-ASA-8.4-K8 | ASA 5500 Series Software Version 8.4 for ASA 5510-5550, DES | 1 |

| | | |
|---|---|---|
| ASA5500-SC-20 | ASA 5500 20 Security Contexts License | 1 |
| ASA5500-ENCR-K9 | ASA 5500 Strong Encryption License (3DES/AES) | 1 |
| ASA5540-VPN-PR | ASA 5540 VPN Premium 5000 IPsec User License (7.0 Only) | 1 |
| SF-ASA-AIP-6.0-K9 | ASA 5500 Series AIP Sofware 6.0 for Security Service Modules | 1 |
| ASA-VPN-CLNT-NONE | No Cisco VPN Client Software Included | 1 |
| ASA-180W-PWR-AC | ASA 180W AC Power Supply | 1 |
| ASA-AIP-40-INC-K9 | ASA 5500 AIP Security Services Module-40 included w/ bundles | 1 |
| CON-CSSPD-ASAINC40 | SHARED SUPP SDS ASA 5500 AIP Security Services Module-40 | 1 |
| CON-CSSPD-AS4A40K9 | SHARED SUPP SDS ASA5540-AIP40-K9 | 1 |

| | | |
|---|---|---|
| AIR-LAP1142N-E-K9 | 802.11a/g/n Fixed Unified AP; Int Ant; E Reg Domain | 35 |
| CON-CSSPD-L1142E | SHARED SUPP SDS 802.11a/g/n Fixed Un | 35 |

| | | |
|---|---|---|
| AIR-CT5508-50-K9 | 5508 Series Controller for up to 50 APs | 1 |
| AIR-PWR-5500-AC | Cisco 5500 Series Wireless Controller Redundant Power Supply | 1 |
| AIR-PWR-CORD-CE | AIR Line Cord Central Europe | 2 |
| CON-CSSPD-CT0850 | SHARED SUPP SDS 5508 Series Controll | 1 |