T.C.

ÇANAKKALE ONSEKİZ MART ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

İSKENDERUN DEMİR VE ÇELİK A.Ş. DAĞITIK OTOMASYON VE BİLGİ SİSTEMLERİ İÇİN NETWORK ALTYAPISININ OLUŞTURULMASI

Oğuz İslam EMLİK

Bilgisayar Mühendisliği Anabilim Dalı

Tezin Sunulduğu Tarih : **12.02.2010**

Tez Danışmanı:

Yrd. Doç. Dr. İsmail KADAYIF

ÇANAKKALE

YÜKSEK LİSANS TEZİ SINAV SONUÇ FORMU

OĞUZ İSLAM EMLİK tarafından **YRD.DOÇ.DR. İSMAİL KADAYIF** yönetiminde hazırlanan **"İskenderun Demir ve Çelik A.Ş. Dağıtık Otomasyon ve Bilgi Sistemleri için Network Altyapısının Oluşturulması"** başlıklı tez tarafımızdan okunmuş, kapsamı ve niteliği açısından bir Yüksek Lisans tezi olarak kabul edilmiştir.

Yrd. Doç. Dr. İbrahim TÜRKYILMAZ

Yönetici

Yrd. Doç Dr. İsmail KADAYIF

Jüri Üyesi

Yrd. Doç. Dr. Akın ALTEN

Jüri Üyesi

Sıra No:……

Tez Savunma Tarihi: 12/02/2010

Prof. Dr. Ahmet ERDEM

Müdür

Fen Bilimleri Enstitüsü

İNTİHAL (AŞIRMA) BEYAN SAYFASI

Bu tezde görsel, işitsel ve yazılı biçimde sunulan tüm bilgi ve sonuçların akademik ve etik kurallara uyularak tarafımdan elde edildiğini, tez içinde yer alan ancak bu çalışmaya özgü olmayan tüm sonuç ve bilgileri tezde kaynak göstererek belirttiğimi beyan ederim.

Adı Soyadı : Oğuz İslam EMLİK

TEŞEKKÜR

Tezimi hazırlarken her anlamda desteğinden dolayı hayat arkadaşım Selma EMLİK'e, moral kaynağım kızım Mihrişah EMLİK'e, çok kıymetli babam Ali EMLİK ve annem Kadriye EMLİK'e, teknolojik olanak sağlanması konusunda her türlü desteği esirgemeyen değerli Başmüdürüm Hamdi AKÇETİN, Müdürüm Hakan KAYHAN ve çok değerli çalışma arkadaşım Berivan ARSLAN'ın şahsında tüm çalışma arkadaşlarıma teşekkürü borç biliyorum.

Son olarak çalışmamı bu son günlerinde yaşadığı sağlık problemlerinden dolayı çok üzgün olduğunu bildiğim anneannem Hatice KARAYAĞLI'ya ithaf ediyorum.

Oğuz İslam EMLİK

SİMGELER VE KISALTMALAR LİSTESİ

ARP (Address Resolution Protocol) : Adres Çözümleme Protokolü

AVF (Active Virtual Forwarder) : Aktif Sanal İletici

AVG (Active Virtual Gateway) : Aktif Sanal Ağ Geçidi

BPDU (Bridge Protocol Data Unit) : Köprü Protokolü Veri Birimi

CIST (Common and Internal Spanning Tree) : Ortak ve Dahili Kapsayan Ağaç

CST (Common Spanning Tree) : Ortak Kapsayan Ağaç

GLBP (Gateway Load Balancing Protocol) : Cisco Ağ Geçidi Yük Dengeleme Protokolü

HSRP (Cisco Hot Standby Router Protocol): Cisco Sıcak Beklemeli Yönlendirici Protokolü

ID (Identifier) : Tanımlama Bilgisi

IEEE (The Institute of Electrical and Electronics Engineers) : Elektrik ve Elektronik Mühendisleri Enstitüsü

IST (Internal Spanning Tree) : Dahili Kapsayan Ağaç

İSDEMİR : İskenderun Demir ve Çelik A.Ş.

LAN (Local Area Network) : Yerel Alan Ağı

MST (Multiple Spanning Tree) : Çoklu Kapsayan Ağaç

MSTP (Multiple Spanning Tree Protocol) : Çoklu Kapsayan Ağaç Protokolü

MSTI (Multiple Spanning Tree Instance) : Çoklu Kapsayan Ağaç Bölümü

MAC (Media Access Control) : Ortam Erişim Yönetimi

MTBF (Mean Time Between Failure) : Arızalar Arası Ortalama Süre

MTTR (Mean Time To Repair) : Ortalama Onarım Süresi

OSI (Open Systems Interconnection) : Açık Sistemler Bağlantısı

PVST (Per-VLAN Spanning Tree) : VLAN Başına Spanning Tree

PVST+ (Per-VLAN Spanning Tree Plus) : VLAN Başına Spanning Tree+

R-PVST (Rapid Per-VLAN Spanning Tree) : Hızlı VLAN Başına Spanning Tree

RSTP (Rapid Reconfiguration Spanning Tree Protocol) : Hızlı Yeniden Yapılandırma Spanning Tree Protokolü

VLAN (Virtual Local Area Network) : Sanal Yerel Alan Ağları

VRID (Virtual Router Identifier) : Sanal Yönlendirici Tanımlama Bilgisi

VRRP (Virtual Router Redundancy Protocol) : Sanal Yönlendirici Yedekliliği Protokolü

STP (Spanning Tree Protocol) : Kapsayan Ağaç Protokolü

SMP (Switch Meshing Protocol) : HP Switch Meshing Protokolü

TTL (Time To Live) : Paketlerin Yaşam Süresi Belirteci

TÜBİTAK: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

TÜRKSAT : Türksat Uydu Haberleşme ve Kablo TV İşletme A.Ş.

UTP (Unshielded Twisted Pair) : Zırhlı olmayan bükülü tel çifti

ÖZET

İSKENDERUN DEMİR VE ÇELİK A.Ş. DAĞITIK OTOMASYON VE BİLGİ SİSTEMLERİ İÇİN NETWORK ALTYAPISININ OLUŞTURULMASI

Oğuz İslam EMLİK
Çanakkale Onsekiz Mart Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans Tezi
Danışman: Yrd. Doç. Dr. İsmail KADAYIF
12.02.2010, 50

İSDEMİR A.Ş. bünyesinde kullanılabilirliği yüksek bir ağ oluşturmak adına OSI Referans Modelinin ilk üç katmanının her birisi için özel çözüm yaklaşımları belirlenmiştir. Bu kapsamda iş-kritik uygulamaların koştuğu her lokasyon için farklı güzergahlardan götürülen yedek kablolar çekilmiş ve yedek ağ cihazları temin edilmiştir. Uçtan uca aynı cihazlarda sonlanan yedekli kablolar için cihazlarda Link Aggregation Protokolü yapılandırması ile kablolar tek bir kablo gibi çalıştırılmıştır. Bu sayede kapasite artışı ve hat yedekliliği sağlanmıştır. Alternatif yollar üzerinden ağ bağlantısı olan anahtarlardan (switch) kenar anahtarlar RSTP, omurga anahtarlar ise VLAN taşınmasına olanak sağlayan MSTP protokolleri ile yapılandırılmıştır. Böylece döngülerden (loop) arındırılmış bir ağ elde edilmiştir. Ayrıca dört farklı lokasyonda konuşlandırdığımız omurga anahtarların VRRP Protokolü yapılandırması ile altmıştan fazla VLAN için yönlendirici yedekliliği sağlanmıştır.

Anahtar Sözcükler : Yedeklilik, Link Aggregation Protokolü, RSTP, MSTP, VRRP, Kullanılabilirliği Yüksek Ağlar, VLAN

ABSTRACT

A STUDY ON BUILDING A NETWORK INFRASTRUCTURE FOR DISTRIBUTED AUTOMATION AND INFORMATION SYSTEMS OF ISKENDERUN IRON AND STEEL WORKS CORPORATION

Oğuz İslam EMLİK
Çanakkale Onsekiz Mart University
Graduate School of Science and Engineering
Thesis of Master of Science for Chair of Computer Engineering
Advisor: Ph. D. İsmail KADAYIF
12.02.2010, 50

To build a highly available network in İSDEMİR, Co. different solutions are determined for each of the first three layers of the OSI Reference Model. On this subject, redundant cables on different path and supplied redundant devices for each locations where business-critical applications are provided. Coterminous redundant cables are employed to work as a single cable with Link Aggregation Protocol configuration on the devices. In this way, link redundancy and capacity as well increase. With the switches having network connection over the alternative paths, the edge switches are configured with RSTP, and the backbone switches are configured with MSTP protocol that allows the transport VLAN information. Thus, a loop-free network is obtained. In addition, the router redundancy for more than sixty VLANs is provided by VRRP configuration on the backbone switches that are located four different locations.

Keywords : Redundancy, Link Aggregation Protocol, RSTP, MSTP, VRRP, High available networks, VLAN

İÇERİK

Sayfa

BÖLÜM 1

GİRİŞ

İskenderun Demir ve Çelik Fabrikalarındaki en önemli süreç olan üretim sürecini temel manada yöneten iki ana sistem vardır. Bunlardan ilki üretim fonksiyonlarını birebir kontrol eden cihazlardan oluşan *Otomasyon Sistemleri,* ikincisi Otomasyon Sistemleri ile bütünleşik çalışarak süreci yönlendiren, karar organ ve mekanizmalarına bilgiler sunan uygulama ve hizmetlerden oluşan *Bilgi Sistemleri*'dir. Daha alt düzeyde bu iki sistem için altyapı niteliğinde olan ve tüm bu sistemlerin üzerinde koştuğu *Network Sistemleri* bulunur. Network Sistemleri aktif ve pasif cihazlardan meydana gelir. 7/24 çalışan fabrikamızda üretim sürecindeki planlanmamış duruş ve aksaklıkların maliyetinin binlerce dolar olduğu düşünüldüğünde, üretim sürecinde yaşanması muhtemel ağ tabanlı problemlerin önlenmesi adına şirket bünyesinde bazı projeler planlanmakta ve yürütülmektedir. Daha önceden Bilgi Sistemleri hizmetlerinin yedekliliğinin ve sürekliliğinin arttırılması amacıyla ikinci bir lokasyonda sistem odası oluşturulması planlanmış ve hayata geçirilmiştir. Bu çalışma sayesinde sunucuların uygun clustering yapılandırmaları ile iki farklı lokasyondan hizmet verilmesi sağlanmıştır. Ancak bu proje ile sadece OSI Referans Modeli'nin Uygulama Katmanı yedekliliği sağlanmıştır.

Yıldız Topolojisi referans alınarak oluşturulan İSDEMİR network sistemlerinin, şirketimiz bünyesindeki Otomasyon ve Bilgi Sistemlerinin üretim süreci üzerindeki kritik rolü sebebiyle, bu sistemler üzerinde oluşabilecek network sistemlerinden kaynaklı duruş ve kesintilerin minimize edileceği bir formasyona dönüştürülmesi hedeflenmiştir. Şuan itibariyle 200'den fazlası yönetilebilir olmak üzere 300'ün üzerinde aktif cihazdan oluşan İSDEMİR yerel ağının, tüm kritik lokasyonlarda uygun protokoller kullanılarak yapılandırılmış aktif cihaz ve kablolama yedekliliği sağlanmış bir ağ topolojisi biçimine dönüştürülmesi için İSDEMİR Ağ ve Donanım Başmühendisliği olarak çalışmalarımızı OSI Referans Modelinin ilk 3 katmanı üzerine yoğunlaştırdık. Durum analizleri yapılarak iyileştirmeye açık alanlarımız ve zayıf noktalarımız belirledik. Kakadia ve ark. (2003) tarafından yapılan çalışmada ağ kullanılabilirliği düşünüldüğünde ilk dikkate alınması gereken konulardan bir tanesinin fiziki topoloji olduğu belirtilmiştir.. İSDEMİR'de, Yıldız Topoloji referans alınarak oluşturulmuş yerel ağ, lokasyonlar arası mesafelerin uzaklığından kaynaklı birçok lokasyon için yıldızın merkezinden hat çekiminin güçlüğü nedeniyle en yakın yıldız kolundaki ağ bileşenine bağlanması ile oluşmuştur. Diğer bir

deyişle cihazlar birbirine seri olarak bağlanmıştır. Bu durumda bir önceki lokasyonda meydana gelecek bir problemden direk olarak bundan sonraki gelen lokasyonlar etkilenmektedir.

İSDEMİR'deki ağ kullanılabilirliğini etkileyen topolojik faktörlerden birisi de kritik iş süreçlerinin gerçekleştiği lokasyonlarda anahtarların tekil olmasıdır. Yani networkte bu cihazlar *Single Point of Failure* bileşen durumundadır. Bu bileşenlerden herhangi birisinde meydana gelebilecek arızalanma üretim sürecinin etkilenmesine neden olacaktır.

İSDEMİR'deki ağ topolojisi daha önceden de bahsedildiği gibi Yıldız Topolojisi referans alınarak oluşturulmuştur. Bu topolojinin doğası gereği ağ geçidi cihazı yerel ağın merkezinde bulunur. Aynı zamanda bu cihaz yerel ağı amaçlarına ve fonksiyonlarına göre sanal olarak alt ağlara ayırmak için kullandığımız VLAN'ların yönetiminin yapıldığı noktadır. Her bir VLAN'daki bilgisayar kendi alt ağında olmayan ağlara bu OSI Referans Modelinin Ağ Katmanında anahtarlama yapabilen *Omurga Anahtar* üzerinden ulaşırlar. Diğer bir deyişle omurga anahtar her VLAN'ın aynı zamanda ağ geçididir. Bu cihazın fiziksel olarak arızalanması durumunda VLAN'lardaki bilgisayarlar kendi ağ geçitlerine ulaşamayacaklarından dolayı tüm sistem kullanım dışı kalacaktır.

Yukarıda her bir katman için ortaya koyulan problemler yerel ağların kullanılabilirliklerini en çok etkileyen parametre olan *arızalar arası ortalama sürenin* (MTBF) azalmasına neden olmaktadır. MTBF süresini maksimum düzeyde tutmak adına her bir katman için bazı çözüm önerileri ortaya koyarak bunların İSDEMİR için en uygun olanını belirleme ve belirtmeye çalışılacaktır. Bölüm 2'de konu ile ilgili teorik ve pratik çalışmaların örnekleri sunulacaktır. Bölüm 3'te çözüm yaklaşımları ortaya koyulacaktır. Bölüm 4'te her katman için özel çözüm yaklaşımlarının kendi arasında üstün ve zayıf yanları ortaya koyulacaktır. Bölüm 5'te bir İSDEMİR'de uygulanan çözüm yaklaşımlarının uygulama bilgileri verilecek, uygulama sonucunda elde edilen veriler sunulacaktır.

BÖLÜM 2

ÖNCEKİ ÇALIŞMALAR

Kullanılabilirliği yüksek ağların oluşturulabilmesi için yedekliliğin sağlanması ile ilgili pratik çalışmalardan bazıları aşağıda verilmiştir. TÜBİTAK Ankara Genel Müdürlüğü, TÜRKSAT, Antalya Havalimanlarında yapılan çalışmalarda OSI referans modelinin Veri Bağı Katmanı yedekliliğinin sağlanması için MSTP ve Link Aggregation protokolleri kullanılmıştır. Ağ katmanı yedekliliğinin sağlanması için yönlendirme yapan cihazlar üzerinde VRRP protokolü kullanılmıştır. Dalaman Havaalanı, Finansbank Kredi Kartları Merkezi ve Savunma Sanayi Müsteşarlığında yapılan çalışmalarda Veri Bağı Katmanı yedekliliğinin sağlanması için RSTP ve Link Aggregation protokolleri kullanılmıştır. Ağ katmanı yedekliliğinin sağlanması için yönlendirme yapan cihazlar üzerinde VRRP protokolü kullanılmıştır. 2005 yılında İşbankası yerel ağ yedekleme ve yük paylaşımı işlemlerini sadece HP sistemlere özel bir yaklaşım olan ve OSI referans modelinin Veri Bağı Katmanı yedekliliği için STP türevlerine alternatif olan SMP (HP Switch Meshing) teknolojisi ile gerçekleştirmiştir (A. Gençay, Kişisel İletişim, HP Procurve Türkiye, 21 Ocak 2009). Grup şirketlerimiz arasındaki özel bağlantılarda Ağ Katmanı yedekliliği HSRP protokolü üzerinden sağlanmıştır. Ayrıca İzmir Ekonomi Üniversitesi'nde yapılan genişleme çalışmaları kapsamında yedeklilik konuları da göz önünde bulundurulmuştur. Mimarinin yıldız topolojisi yerine yedekliliğin sağlandığı bir topolojiye dönüştürülmesi sağlanmıştır. Çalışmalarda OSI referans modelinin Veri Bağı Katmanı yedekliliğinin sağlanması için MSTP ve Link Aggregation protokolleri kullanılmıştır. Sunucu üzerinde yönlendirmenin yapıldığı yaklaşımdan Ağ Katmanında yönlendirme yeteneğine sahip cihazların kullanıldığı yedekli bir omurga altyapısına geçiş sağlanmıştır. Ağ Katmanı için varsayılan ağ geçidi yedekliliğinin ve yük paylaşımının sunulduğu VRRP kullanılmıştır (Mutlu, 2007).

Yukarıda verilen pratik çalışmalara ek olarak protokollerin geliştirilmesi için yapılmış bazı akademik çalışmalar aşağıda verilmiştir. Buregoni (2007) yaptığı çalışmada anahtarlardaki STP etkinleştirilmiş portlar üzerinden yönlendirilmiş trafiğin desteklenmesini sağlarken, yönlendirilmiş trafiğin verimli yönetimi için basit ve yeni bir çözüm sunmuştur. Watanabe ve ark. (2008) yaptıkları çalışmada büyük ölçekli PC kümelemelerinde Link Aggregation protokolü kullanılarak broadcast stormların oluşumunu engelleyerek performans artışları sağlamışlardır. Bu çalışmada sistem

yazılımını değiştirmeden sistem yapılandırmasını basitleştirmek için topolojilerin önceki tanımlamalara ek olarak kendi tanımlarında anahtarlarda çerçevelere VLAN etiketleri eklemişlerdir. Böylece her uç kullanıcı için kendi fiziksel arayüzü üzerinde farklı bir yerel adrese sahip bir VLAN arayüzü yaratarak broadcast ile anahtarın bir PC kümelemesi içindeki uç kullanıcı için MAC adresini öğrenebilmesini sağlamışlardır. Ahmadi ve Zamani (2009) yaptıkları çalışmada ağaç topolojisinde kök eleman üzerindeki iletişim trafiğinin dengesiz dağılımdan dolayı trafik yönetimi açısından STP performansının zayıflığının STP mekanizmasına Hiper-Küp fikrini dahil etmek suretiyle azaltılabileceğini göstermişlerdir. STP algoritması içerisinde Hiper-Küp yönlendirmesinin sıkışıklık denetimi mekanizması olarak kullanılması değişikliği fikrini benimsemişlerdir. Çalışmalarının sonucunda önerilen metodun STP algoritmasına üstünlüğü açıkça ortaya koyulmuştur. Santos ve ark. (2009a) yaptıkları çalışmada Spanning Tree yönlendirmesi üzerine tasarlanmış iletişim ağlarındaki optimal yük dengelemesine odaklanmışlar ve üç farklı yük dengelemesi modeli ortaya koymuşlardır. Adreslenmiş optimizasyon problemleri için alt sınır ve uygulanabilir çözümlerin hesaplanması için yaklaşımlar sunmuşlar, sonuç olarak farklı çözüm tekniklerinin verimliliği ve etkinliğini ölçmüşler, her problem için diğer problemlerin optimizasyon kriterini göz önünde bulundurarak çözümün kalitesini kıyaslamışlardır. Yine Santos ve ark. (2009b) yaptıkları çalışmada Telekomünikasyon ağları üzerinde trafik mühendisliği üzerine yoğunlaşmışlar ve maksimum hat yoğunluğunun nasıl azaltılabileceğini göstermişlerdir. IEEE-802.1s MSTP üzerinde optimizasyon problemlerinin belirlendiği iki kompakt sayı doğrusal programlama modeli ve dal-ve-bedel yaklaşımı ile çözülen Dantzing-Wolfe ayrışım prensibini baz aldıkları değişik modeller belirlemiş ve kıyaslamışlardır.

BÖLÜM 3

MATERYAL VE YÖNTEM

Amaç ağ yedekliliği ve kullanılabilirliğin arttırılması olduğunda OSI referans modelinin ilgili katmanları üzerinde farklı çözümlerin uygulanması gerekir. Bu bölümde her bir katman için ayrı materyal ve yöntemin kullanıldığı çözüm yaklaşımları ortaya koyulacaktır.

3.1. Fiziksel Katman Çözüm Yaklaşımları

Fiziksel katman için çözüm yaklaşımı her bir bileşenin fiziksel yedeğinin temin edilmesine dayanır. Yapılacak iş, iş-kritik uygulamaların koştuğu her lokasyon için farklı güzergahlardan götürülecek ikinci bir fiziki kablo çekmek ve aktif ağ cihazlarının da fiziksel olarak yedeklenmesini sağlamaktır.

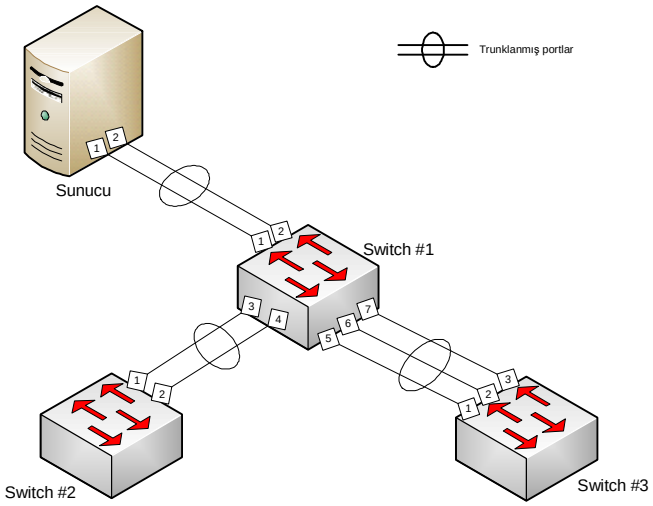
3.2. Veri Bağı Katmanı Çözüm Yaklaşımları

Fiziksel katman için uygulanan ikinci kablonun çekilmesi ile sağlanan fiziksel yedeklilik cihazlar üzerindeki yapılandırmaların yapılmaması durumunda *Broadcast Stormlar* yaratarak tüm yerel ağı ya da kendi yerel ağının tanımlandığı VLAN için yapılandırma yapılmış anahtarların üzerindeki ağları çalışamaz duruma getirebilir.

Birden fazla çekilen hatların sonlandıkları noktalara göre amaçları belirlenir. Bazen sadece yedeklilik için çekilen hat, bazen yük paylaşımı ve hat kapasitesinin arttırılması için çekilmiş olabilir. Bu yüzden ağ cihazlarının Veri Bağı katmanına özel uygun protokoller ile yapılandırılması gerekir. Bu sebeple cihazlar buna elverişli, yani yönetilebilir olmalıdır.

3.2.1. Link Aggregation/Port Trunking

Uçtan uca aynı fiziksel cihazlarda sonlanan yedekli kablolar için Link Aggregation Protokolü (IEEE-802.3ad) kullanılarak yedeklilik, yük paylaşımı ve kapasite arttırılması sağlanabilir, böylece hat kullanılabilirliği arttırılabilir. *Link Aggregation* veya *Port Trunking*, birden fazla fiziksel port veya fiziksel kablonun tek bir fiziksel kablo veya fiziksel port gibi kullanılmasını sağlar ve genelde ağ cihazları arasındaki kapasite arttırılması için en verimli yollardan bir tanesidir (Anonim, 2006). Bunun yanında hatlar birbirini yedekler durumda olduklarından ağ kullanılabilirliği de arttırılmış olacaktır.



Şekil 1. Link Aggregation Protokolü kullanımı örneği.

Yukarıdaki şekil üzerinden Link Aggregation protokolünün bazı uygulama örnekleri aşağıda açıklanmıştır. Şekilde görüldüğü gibi Switch#1 üzerinde 1 Gbps'lik [1,2], [3,4] ve [5,6,7] numaralı portlar kendi aralarında olmak üzere üç adet trunk grubu tanımlanmıştır. Böylece [1,2] numaralı portlar üzerinde oluşturulan trunk grubu sayesinde Sunucu ile 2 Gbps'lik bir bant genişliğine sahip ve bir fiziki kablo veya ağ arayüzünün arızalanmasına toleranslı bir hat elde edilmiş olur. Yine [3,4] numaralı portlar üzerinde oluşturulan trunk grubu sayesinde Switch#2 ile 2 Gbps'lik bir bant genişliğine sahip ve bir fiziki kablo veya ağ arayüzünün arızalanmasına toleranslı bir hat elde edilmiş olur. Son olarak [5,6,7] numaralı portlar üzerinde oluşturulan trunk grubu sayesinde Switch#3 ile 3 Gbps'lik bir bant genişliğine sahip ve iki fiziki kablo veya ağ arayüzünün arızalanmasına toleranslı bir hat elde edilmiş olur. Switch#2 üzerinde [1,2] numaralı portlar kendi aralarında olmak üzere bir adet trunk grubu tanımlanmıştır. Böylece [1,2] numaralı portlar üzerinde oluşturulan trunk grubu sayesinde Switch#1 ile 2 Gbps'lik bir bant genişliğine sahip ve bir fiziki kablo veya ağ arayüzünün arızalanmasına toleranslı bir hat elde edilmiş olur. Switch#3 üzerinde [1,2,3] numaralı portlar kendi aralarında olmak üzere bir adet trunk grubu tanımlanmıştır. Böylece [1,2,3] numaralı portlar üzerinde oluşturulan trunk grubu sayesinde Switch#1 ile 3 Gbps'lik bir bant genişliğine sahip ve iki fiziki kablo veya ağ arayüzünün arızalanmasına toleranslı bir hat elde edilmiş olur. Sunucu üzerinde [1,2] numaralı ağ arayüz kartları port trunklaması yapılmıştır. Böylece [1,2] numaralı ağ arayüz kartları üzerinde oluşturulan trunk grubu sayesinde Switch#1 ile 2 Gbps'lik bir bant genişliğine sahip ve bir fiziki kablo veya ağ arayüzünün arızalanmasına toleranslı bir hat elde edilmiş olur.

3.2.2. HP Port Trunking

Uçtan uca aynı fiziksel cihazlarda sonlanan yedekli kabloların tek kablo gibi kullanılmasını sağlayan port trunklama yöntemlerinden bir tanesidir. Ancak standartları belirlenmiş herhangi bir protokol ile tanımlanmayan, sadece HP ürün ailesine özel bir yaklaşımdır (Anonim, 2006).

3.2.3. STP (Spanning Tree Protocol)

Yedek hatlar kullanılabilirliği arttırmak adına çekilmesine rağmen köprülerin çerçeveleri (frame) sonsuza dek iletilmesini sağlayan döngüler meydana getirir (Kakadia ve ark., 2003). Bu döngüleri elimine etmek adına tümü OSI referans modelinin Veri Bağı katmanında çalışması koşulu ile ağ hizmetlerinin sunulması amacıyla bir ağ cihazına en az iki fiziksel ağ cihazından çekilen hatlar için Spanning Tree Protokolü (IEEE-802.1d) kullanılarak ağ kullanılabilirliği arttırılabilir. Bu durumda veri ağa birden fazla nokta üzerinden akabilecektir. Böylece ağın bazı hatlar veya cihazlar çalışamaz duruma gelse bile fonksiyonlarını yerine getirmesini ve kullanıcılar için iş-kritik servisleri sunmasını sağlar (Anonim, 2006). Aynı zamanda döngülerden arındırılmış bir ağ yaratmayı hedefleyen STP ile ağın güvenirliği de arttırılmış olur.

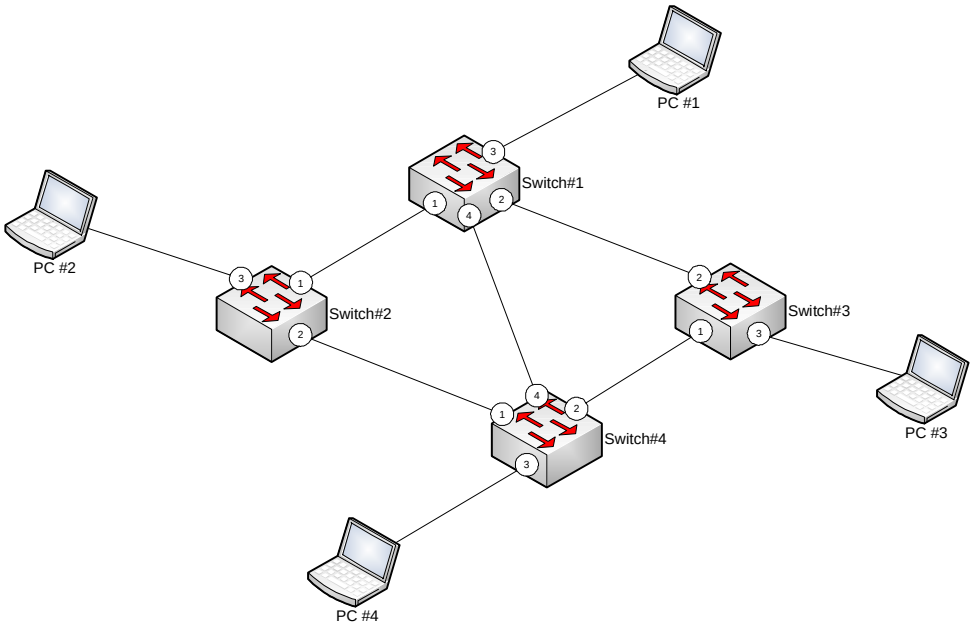
Spanning Tree aktif ise, anahtarlar *kök köprü* olacak anahtarı seçerler, ağ üzerindeki tüm döngüleri belirlerler ve sonra da kök köprüye doğru olan en ucuz yolu bulurlar (Anonim, 2006).

Köprüler belirli aralıklarla portlarından gelen BPDU (Bridge Protocol Data Units) adı verilen çerçeveleri alır ve kendisine ait çerçeveleri de diğer köprülerin kullanması için gönderirler. Tipik BPDU çerçeveleri *köprü ID*, *port ID* ve *kök yol maliyeti* (Root Path Cost) temel alanlarından oluşur.

Kök köprünün seçimi için BPDU'daki köprü ID verisi kullanılır. En düşük köprü ID'ye sahip olan kök köprü olarak seçilir. Köprü ID, kullanıcı tarafından belirlenmiş *köprü öncelik değeri* (Bridge Priority) ve cihazın MAC adresinden hesaplanır.

Kök köprü seçiminden sonra en ucuz yolun belirlenmesi için BPDU'daki kök yol maliyeti verisi kullanılır. Tüm köprüler aldığı BPDU üzerindeki kök yol maliyeti verisini aldığı portun *maliyet* (Port Cost) değerini ekleyerek günceller ve kendine komşu köprülere gönderirler. Ağdaki bütün hesaplamalar sona erdiğinde köprü üzerindeki kök yol maliyeti değeri en düşük port *iletim durumu*'na (Forwarding State) çekilir. Bazı durumlarda minimum kök yol maliyeti değeri birden fazla port üzerinde aynı olarak hesaplanır. Bu durumda komşu köprülerin bağlandıkları, önceliği en yüksek verilen port iletim durumuna

geçer. Diğer tüm yedek hatların bağlandığı portlar *bloklama durumu*'na (Blocking State) çekilip aktif hat üzerinden ağ kaynaklarına erişim sağlanır. Aşağıdaki şekil üzerinden STP'nin kullanım amacı ve çalışma prensipleri örneklenmiştir.



Şekil 2. Spanning Tree Protokolü kullanımı örneği.

Yukarıdaki topoloji dikkate alındığında eğer herhangi bir STP türevi ile korunmuyorsa bu ağdaki PC'lerin birbirleri ile görüşmeleri birkaç saniyeden sonra mümkün olmayacaktır. Bu ağdaki tüm köprüler tek ARP çerçevesinin dahi neden olacağı döngüler nedeniyle saniyeler içinde cevap veremez hale geçeceklerinden hiçbir ağ kaynağına erişim sağlanamayacaktır. Yedek çekilen hatların döngülere neden olmasını engellemek için cihazların STP ile yapılandırılmaları gerekir. Yapılandırma için gerekli bilgiler aşağıdaki gibidir.

Çizelge 1. Spanning Tree Protokolü kullanımı örneği için köprü bilgileri

Köprü Adı	Köprü Öncelik Değeri	MAC Adresi
Switch#1	1	00:00:00:00:00:01
Switch#2	2	00:00:00:00:00:02
Switch#3	3	00:00:00:00:00:03
Switch#4	4	00:00:00:00:00:04

Çizelge 2. Spanning Tree Protokolü kullanımı örneği için port maliyet değerleri

Köprü Adı	Port#1	Port#2	Port#3	Port#4
Switch#1	2.000	20.000	-	20.000
Switch#2	2.000	2.000	-	-
Switch#3	2.000	20.000	-	-
Switch#4	2.000	2.000	-	20.000

Yukarıdaki tablolardan yola çıkarak STP'nin çalışma mekanizması anlatılmıştır. İlk adım kök köprünün seçilmesi adımıdır. Yukarıda da bahsedildiği gibi kök köprü, köprü ID'si en küçük olan köprüdür. Buna göre her köprü için 64 bit'lik köprü ID değişkeni kullanıcı tarafından belirlenen köprü öncelik değeri ile standart olarak 4096 sayısının çarpımı ve köprünün MAC adresi ile elde edilir.

Çizelge 3. Spanning Tree Protokolü kullanımı örneği için belirlenen köprü ID'ler

Köprü Adı	Köprü Öncelik Değeri (16bit)	MAC Adresi (48 bit)		Köprü ID (16+48=64 bit)
Switch#1	1*4096=10:00	00:00:00:00:00:01	**à**	10:00:00:00:00:00:00:01
Switch#2	2*4096=20:00	00:00:00:00:00:02	**à**	20:00:00:00:00:00:00:02
Switch#3	3*4096=30:00	00:00:00:00:00:03	**à**	30:00:00:00:00:00:00:03
Switch#4	4*4096=40:00	00:00:00:00:00:04	**à**	40:00:00:00:00:00:00:04

Tabloya göre en küçük köprü ID değeri Switch#1 köprüsüne ait olduğundan kök köprü Switch#1 köprüsü olarak seçilir. Bir sonraki adım tüm köprülerin BPDU çerçevelerini aldığı her port için kök yol maliyeti değerini hesaplamasıdır. Yukarıda da bahsedildiği gibi kök köprüden başlayarak yayılan BPDU'lar üzerinden her köprü kendisinin üzerindeki portlar için kök yol maliyeti hesaplaması yaparken BPDU'lardaki kök yol maliyeti değerini kendi portu için tanımlanmış maliyet (cost) değeri ile toplayarak bulur. Sonuç olarak en küçük kök yol maliyeti değerinin oluştuğu port iletim durumuna çekilir, diğer tüm yedekli portlar bloklama durumuna çekilerek iletişim kurmaları engellenir.

Switch#1'in kendisi kök köprü olduğu için kök yol maliyeti değeri 0'dır. Switch#1 BPDU çerçevesini kendisine bağlı tüm köprülere gönderir, ancak her köprü BPDU'ları alırken ilgili port için maliyet değerini ekleyerek kök yol maliyetini elde ederler. Kendi

kök yol maliyeti değerinden daha küçük bir kök yol maliyeti değeri alan köprü kendi BPDU'larını göndermeyi bitirirken diğer köprülerden gelen kök yol maliyeti değerini diğer köprülere iletmeye devam eder.

Çizelge 4. STP kullanımı örneği için belirlenen kök yol maliyeti değerleri - 1

Köprü Adı	Port	Kök Yol Maliyeti
Switch#1	1	0
Switch#1	2	0
Switch#1	3	0
Switch#1	4	0
Switch#2	1	0 + 2.000 = 2.000
Switch#2	2	-
Switch#2	3	-
Switch#3	1	-
Switch#3	2	0 + 20.000 = 20.000
Switch#3	3	-
Switch#4	1	-
Switch#4	2	-
Switch#4	3	-
Switch#4	4	0 + 20.000 = 20.000

Köprüler, kök köprüden kendisine gelen BPDU'ları diğer portlarına gönderir. Ayrı ayrı incelendiğinde Switch#2'nin gönderdiği BPDU'yu alan Switch#4 kendi parametrelerini aşağıdaki gibi düzenler.

Çizelge 5. STP kullanımı örneği için belirlenen kök yol maliyeti değerleri - 2

Köprü Adı	Port	Kök Yol Maliyeti
Switch#4	1	2.000 + 2.000 = 4.000
Switch#4	2	-
Switch#4	3	-
Switch#4	4	20.000

Switch#4'ün gönderdiği BPDU'yu alan Switch#2 kendi portları üzerindekinden daha küçük bir kök yol maliyeti değeri ile gelmediğinden bu çerçeve için bir değişiklik yapmaz.

Çizelge 6. STP kullanımı örneği için belirlenen kök yol maliyeti değerleri - 3

Köprü Adı	Port	Kök Yol Maliyeti
Switch#2	1	2.000
Switch#2	2	-
Switch#2	3	-

Switch#4'ün gönderdiği BPDU'yu alan Switch#3 kendi parametrelerini aşağıdaki gibi düzenler.

Çizelge 7. STP kullanımı örneği için belirlenen kök yol maliyeti değerleri - 4

Köprü Adı	Port	Kök Yol Maliyeti
Switch#3	1	4.000 + 2.000 = 6.000
Switch#3	2	20.000
Switch#3	3	-

Switch#3'ün gönderdiği BPDU'yu alan Switch#4 kendi portları üzerindekinden daha küçük bir kök yol maliyeti değeri ile gelmediğinden bu çerçeve için değişiklik yapmaz.

Çizelge 8. STP kullanımı örneği için belirlenen kök yol maliyeti değerleri - 5

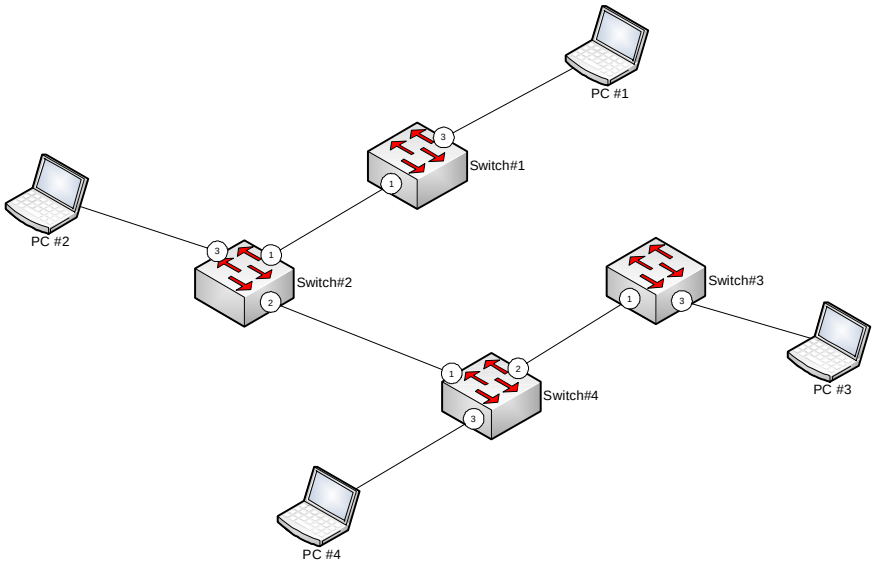
Köprü Adı	Port	Kök Yol Maliyeti
Switch#4	1	4.000
Switch#4	2	-
Switch#4	3	-
Switch#4	4	20.000

Buna göre her köprü üzerindeki minimum kök yol maliyeti değerleri aşağıdaki gibi oluşur. Tüm köprüler üzerinde minimum kök yol maliyeti değerinin oluştuğu port hariç tüm portlar bloklama durumuna alınır ve portlardan trafik geçişine izin vermez.

Çizelge 9. STP kullanımı örneği için belirlenen kök yol maliyeti değerleri - 6

Köprü Adı	Port	Kök Yol Maliyeti
Switch#1	-	-
Switch#2	1	2.000
Switch#3	1	6.000
Switch#4	1	4.000

Buna göre oluşacak döngülerden arındırılmış ağ aktif yolu aşağıdaki gibidir.



Şekil 3. STP sayesinde döngülerden arındırılmış ağ aktif yolu – 1.

Ayrıca STP ile belirlenmiş topolojideki ağ bileşenleri üzerinde oluşacak probleme karşı STP'nin nasıl davrandığı örneklemek adına Switch#2 ile Switch#1 arasındaki hattın fiziksel olarak arızalanmasını ele aldığımızda ilk olarak topoloji değişiminin olduğunu bildiren çerçevelerin gönderilmesi üzerine kök köprü seçimi tekrarlanır, yine Switch#1 seçilir. Daha sonra Switch#1'in göndermiş oluğu BPDU'ya göre hesaplanmış kök yol maliyeti tablosu aşağıdaki gibi oluşur.

Çizelge 10. STP kullanımı örneği için belirlenen kök yol maliyeti değerleri - 7

Köprü Adı	Port	Kök Yol Maliyeti
Switch#1	1	0
Switch#1	2	0
Switch#1	3	0
Switch#1	4	0
Switch#2	1	-
Switch#2	2	-
Switch#2	3	-
Switch#3	1	-
Switch#3	2	0 + 20.000 = 20.000
Switch#3	3	-
Switch#4	1	-
Switch#4	2	-
Switch#4	3	-
Switch#4	4	0 + 20.000 = 20.000

Switch#4'ün gönderdiği BPDU'yu alan Switch#2 kendi parametrelerini düzenler.

Çizelge 11. STP kullanımı örneği için belirlenen kök yol maliyeti değerleri - 8

Köprü Adı	Port	Kök Yol Maliyeti
Switch#2	1	-
Switch#2	2	20.000 + 2.000 = 22.000
Switch#2	3	-

Switch#4'ün gönderdiği BPDU'yu alan Switch#3 kendi portları üzerindekinden daha küçük bir kök yol maliyeti değeri ile gelmediğinden bu çerçeve için bir değişiklik yapmaz.

Çizelge 12. STP kullanımı örneği için belirlenen kök yol maliyeti değerleri - 9

Köprü Adı	Port	Kök Yol Maliyeti
Switch#3	1	-
Switch#3	2	20.000
Switch#3	3	-

Switch#3'ün gönderdiği BPDU'yu alan Switch#4 kendi portları üzerindekinden daha küçük bir kök yol maliyeti değeri ile gelmediğinden bu çerçeve için bir değişiklik yapmaz.

Çizelge 13. STP kullanımı örneği için belirlenen kök yol maliyeti değerleri - 10

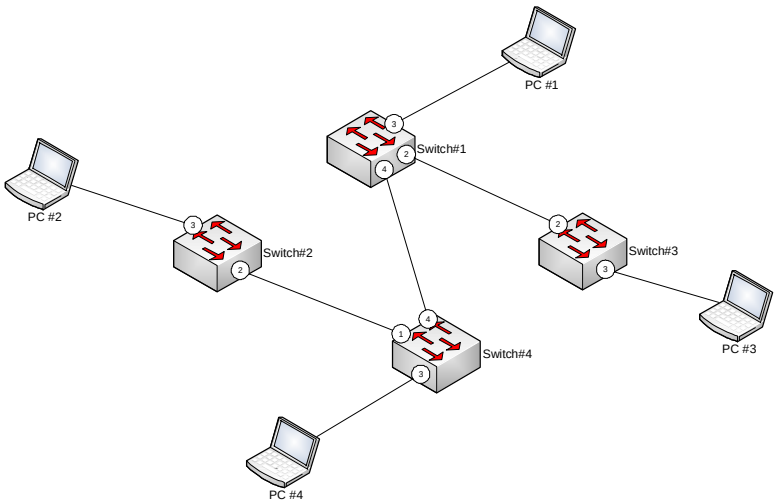
Köprü Adı	Port	Kök Yol Maliyeti
Switch#4	1	-
Switch#4	2	-
Switch#4	3	-
Switch#4	4	20.000

Buna göre her köprü üzerindeki minimum kök yol maliyeti değerleri aşağıdaki gibi oluşur.

Çizelge 14. STP kullanımı örneği için belirlenen kök yol maliyeti değerleri - 11

Köprü Adı	Port	Kök Yol Maliyeti
Switch#1	-	-
Switch#2	2	22.000
Switch#3	2	20.000
Switch#4	4	20.000

Tüm köprüler üzerinde minimum kök yol maliyeti değerinin oluştuğu port hariç tüm portlar bloklama durumuna alınarak trafik geçişine izin verilmez. Buna göre döngülerden arındırılmış ağ aktif yolu aşağıdaki gibi oluşur.



Şekil 4. STP sayesinde döngülerden arındırılmış ağ aktif yolu – 2.

Ayrıca Kök köprü olan Switch#1 cihazının fiziksel olarak arızalanmasını ele aldığımızda en küçük Köprü ID'ye sahip olan Switch#2 Kök köprü olarak belirlenir. Daha sonra Switch#2'in göndermiş oluğu BPDU'ya göre hesaplanmış Kök Yol Maliyeti tablosu aşağıdaki gibi oluşur.

Çizelge 15. STP kullanımı örneği için belirlenen kök yol maliyeti değerleri - 12

Köprü Adı	Port	Kök Yol Maliyeti
Switch#2	1	0
Switch#2	2	0
Switch#2	3	0
Switch#3	1	-
Switch#3	2	-
Switch#3	3	-
Switch#4	1	2.000
Switch#4	2	-
Switch#4	3	-
Switch#4	4	-

Switch#4'ün gönderdiği BPDU'yu alan Switch#3 kendi parametrelerini aşağıdaki gibi düzenler.

Çizelge 16. STP kullanımı örneği için belirlenen kök yol maliyeti değerleri - 13

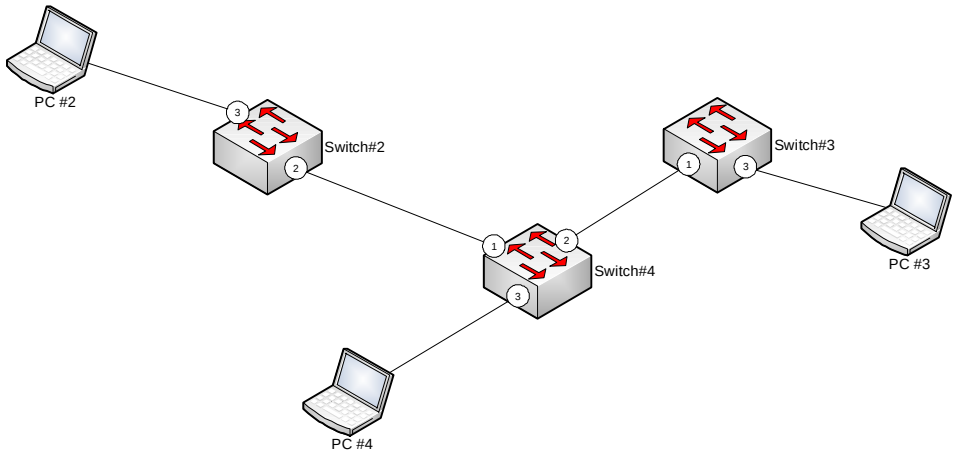
Köprü Adı	Port	Kök Yol Maliyeti
Switch#3	1	2.000 + 2.000 = 4.000
Switch#3	2	-
Switch#3	3	-

Buna göre her köprü üzerindeki minimum kök yol maliyeti değerleri aşağıdaki gibi oluşur.

Çizelge 17. STP kullanımı örneği için belirlenen kök yol maliyeti değerleri - 14

Köprü Adı	Port	Kök Yol Maliyeti
Switch#2	-	0
Switch#3	1	4.000
Switch#4	1	2.000

Tüm köprüler üzerinde minimum kök yol maliyeti değerinin oluştuğu port hariç tüm portlar bloklama durumuna alınarak trafik geçişine izin verilmez. Buna göre döngülerden arındırılmış ağ aktif yolu aşağıdaki gibi oluşur.



Şekil 5. STP sayesinde döngülerden arındırılmış ağ aktif yolu – 3.

3.2.3.1. RSTP (Rapid Reconfiguration Spanning Tree Protocol)

RSTP, 1998 yılında IEEE-802.1w standardı ile tanımlanmıştır. Ancak 2004 yılında IEEE-802.1d standardı hem STP hem de RSTP desteklenecek şekilde değiştirilip yeniden tanımlanmıştır. RSTP'nin temel fonksiyonlar bağlamında STP ile pek farkı yoktur. RSTP'nin isminden de anlaşılacağı gibi getirdiği yenilik, herhangi bir topoloji değişiminde daha hızlı şekilde aktif ağ yolunu oluşturmasıdır. STP'nin otuz ile elli saniye aralığında tepki verdiği bir topoloji değişimine RSTP, bir saniye içerisinde tepki verebilir (Conlan, 2009)

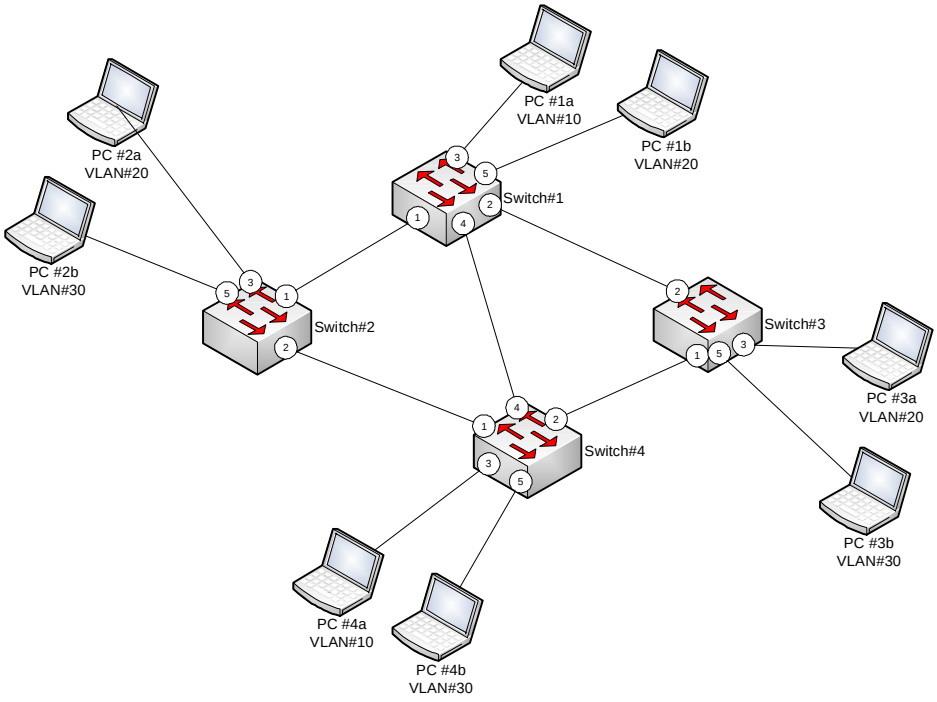
3.2.3.2. PVST (Per-VLAN Spanning Tree)

PVST, isminden de anlaşılacağı gibi her VLAN için bir Kapsayan Ağaç (Spanning Tree) oluşturarak farklı ağ yollarının kullanılması için Cisco tarafından geliştirilmiş ve Cisco'ya özgü bir çözümdür. PVST sadece Cisco tarafından kullanılan ISL VLAN kapsülleme protokolünü kullanır (Conlan, 2009). Ayrıca PVST her VLAN için bir kapsayan ağaç oluşturduğundan fazla sayıda VLAN içeren ağlarda yönetimi çok zor ve kaynak kullanımı oldukça fazladır. PVST bu sebeplerden yaygınlaşmamış, ancak yük dengelemesi açısından MSTP'nin temellerini oluşturmuştur. PVST+ ve R-PVST gibi türevleri bulunmaktadır.

3.2.3.3. MSTP (Multiple Spanning Tree Protocol)

MSTP IEEE-802.1s standardı ile tanımlanmış, daha sonradan RSTP'ye bir eklenti ile VLAN'ların kullanımına olanak sağlayan IEEE-802.1q-2003 standardına geçirilmiştir. STP ve RSTP yapılandırmaları anahtar üzerindeki diğer Veri Bağı katmanı ayarlarına bakmadan fiziksel port bloklaması yaparak çalıştıklarından VLAN'lar üzerinde olumsuz etki yaratabilirler. MSTP bunu önlemek adına her VLAN grubu için ayrı kapsayan ağaç tanımlayıp yalnız bir yol haricindeki tüm yolları bloklayarak aktif ağ yolları oluşturulmasına imkan verir. MSTP, STP'nin tasarımı esnasında gözden kaçması muhtemel eksik VLAN etiketleme işlemlerinin önüne geçmemizi sağlar. Aynı zamanda bir anlamda yedekliliğin yanında yük paylaşımı da sağlanır. MSTP BPDU'ları STP ve RSTP ile uyumlu çalışabilecek şekilde tasarlanmıştır, böylece geriye uyumluluk sağlanır (Conlan, 2009).

MSTP ile karşılaştığımız bazı kavramları mantıksal bağlılık çerçevesinde açıklamak gerekirse; MSTP'de ağ *bölgelere* (Region) ayrılarak düzenlenir. Bölgeler ise VLAN kümelemesinde kullanılan *bölümlere* (Instance) ayrılırlar. Her bölgenin kapsayan ağaç bilgisinin tutulduğu MSTI'ları vardır. VLAN'lar MSTI'larla ilişkilendirilirler. Bir MSTI'a birden fazla VLAN ilişkilendirilebilir. IST bir MST Bölgesindeki kapsayan ağaçtır. IST, diğer MSTI'lara STP topoloji bilgisini temin edebilmek için kullanılır. Tüm ağ için ise bilgilerin tutulduğu bir adet CST ağacı bulunur. CST, MST Bölge'lerini birbirine bağlantısını örnekleyen kapsayan ağaçtır. Tüm MST bölgelerindeki IST'ler ve CST birlikte tüm ağın CIST'sini meydana getirir. MSTP'nin yapısı gereği her MSTI için bir kök köprü vardır. Bu kök köprüler *bölgesel kök köprü* olarak adlandırılırlar. Ayrıca CIST için ortak bir kök köprü daha bulunur. Bu kök köprü ise *ortak kök köprü* olarak adlandırılır (Arregoces ve Portolani, 2004). Aşağıdaki şekil üzerinden birkaç örnek ile MSTP'nin kullanım amacı ve çalışma prensipleri örneklenmiştir.



Şekil 6. Multiple Spanning Tree Protokolü kullanımı örneği.

Aynı bölgedeki köprüler üzerinde MSTP yapılandırması için gerekli bilgilerin aşağıdaki gibi olduğu varsayılmıştır.

Çizelge 18. Multiple Spanning Tree Protokolü kullanımı örneği için köprü bilgileri

Köprü Adı	Köprü Öncelik Değeri	MAC Adresi
Switch#1	1	00:00:00:00:00:01
Switch#2	2	00:00:00:00:00:02
Switch#3	3	00:00:00:00:00:03
Switch#4	4	00:00:00:00:00:04

Çizelge 19. MSTP kullanımı örneği için port maliyet değerleri

Port Adı	Switch#1	Switch#2	Switch#3	Switch#4
1	2.000	2.000	2.000	2.000
2	2.000	2.000	2.000	2.000
3	-	-	-	-
4	20.000	-	-	20.000
5	-	-	-	-

Çizelge 20. MSTP kullanımı örneği için bölüm ve VLAN bilgileri

MSTI ID	VLAN ID
Instance#1	VLAN#10, VLAN#20
Instance#2	VLAN#30

Çizelge 21. MSTP kullanımı örneği için bölümlere göre köprü öncelik bilgileri

Instance#1	
Köprü Adı	Köprü Öncelik Değeri
Switch#1	1
Switch#2	2
Switch#3	3
Switch#4	4
Instance#2	
Köprü Adı	Köprü Öncelik Değeri
Switch#1	4
Switch#2	3
Switch#3	2
Switch#4	1

İlk adım yine kök köprü seçimidir, ancak kök köprü hesaplaması IST de dahil olmak üzere her MSTI için ayrı ayrı yapılır. Kök köprü seçimi yine her bölüm için en küçük köprü ID değerli köprü kök köprü olarak atanır.

Instance#1 için kök köprü seçimi aşağıdaki veriler ışığında yapılır.

Çizelge 22. MSTP kullanımı örneği Instance#1 köprü ID listesi

Köprü Adı	Köprü Öncelik Değeri (16bit)	MAC Adresi (48 bit)		Köprü ID (16+48=64 bit)
Switch#1	1*4096=10:00	00:00:00:00:00:01	**à**	10:00:00:00:00:00:00:01
Switch#2	2*4096=20:00	00:00:00:00:00:02	**à**	20:00:00:00:00:00:00:02
Switch#3	3*4096=30:00	00:00:00:00:00:03	**à**	30:00:00:00:00:00:00:03
Switch#4	4*4096=40:00	00:00:00:00:00:04	**à**	40:00:00:00:00:00:00:04

En küçük Köprü ID değeri Switch#1 köprüsüne ait olduğundan Instance#1 için kök köprü, Switch#1 olarak seçilir. Tüm köprüler BPDU çerçevelerini aldığı her port için MSTI bilgilerine uygun kök yol maliyeti değerini hesaplamaya başlar.

Çizelge 23. MSTP kullanımı örneği Instance#1 kök yol maliyeti değerleri - 1

Köprü Adı	Port	Kök Yol Maliyeti
Switch#1	1	0
Switch#1	2	0
Switch#1	4	0
Switch#2	1	0 + 2.000 = 2.000
Switch#2	2	-
Switch#3	1	-
Switch#3	2	0 + 2.000 = 2.000
Switch#4	1	-
Switch#4	2	-
Switch#4	4	0 + 20.000 = 20.000

Köprüler Instance#1'e ait kök köprüden kendisine gelen BPDU'ları kenar port olarak belirlenmemiş portlarına gönderir. Ayrı ayrı incelendiğinde Switch#2'nin gönderdiği BPDU'yu alan Switch#4 kendi parametrelerini aşağıdaki gibi düzenler.

Çizelge 24. MSTP kullanımı örneği Instance#1 kök yol maliyeti değerleri - 2

Köprü Adı	Port	Kök Yol Maliyeti
Switch#4	1	2.000 + 2.000 = 4.000
Switch#4	2	-
Switch#4	4	20.000

Switch#4'ün gönderdiği BPDU'yu alan Switch#2 kendi portları üzerindekinden daha küçük bir kök yol maliyeti değeri ile gelmediğinden bu çerçeve için değişiklik yapmaz.

Çizelge 25. MSTP kullanımı örneği Instance#1 kök yol maliyeti değerleri - 3

Köprü Adı	Port	Kök Yol Maliyeti
Switch#2	1	2.000
Switch#2	2	-

Switch#4'ün gönderdiği BPDU'yu alan Switch#3 kendi portları üzerindekinden daha küçük bir kök yol maliyeti değeri ile gelmediğinden bu çerçeve için değişiklik yapmaz.

Çizelge 26. MSTP kullanımı örneği Instance#1 kök yol maliyeti değerleri - 4

Köprü Adı	Port	Kök Yol Maliyeti
Switch#3	1	-
Switch#3	2	2.000

Switch#3'ün gönderdiği BPDU'yu alan Switch#4 kendi portları üzerindekinden daha küçük bir kök yol maliyeti değeri ile gelmediğinden bu çerçeve için değişiklik yapmaz.

Çizelge 27. MSTP kullanımı örneği Instance#1 kök yol maliyeti değerleri - 5

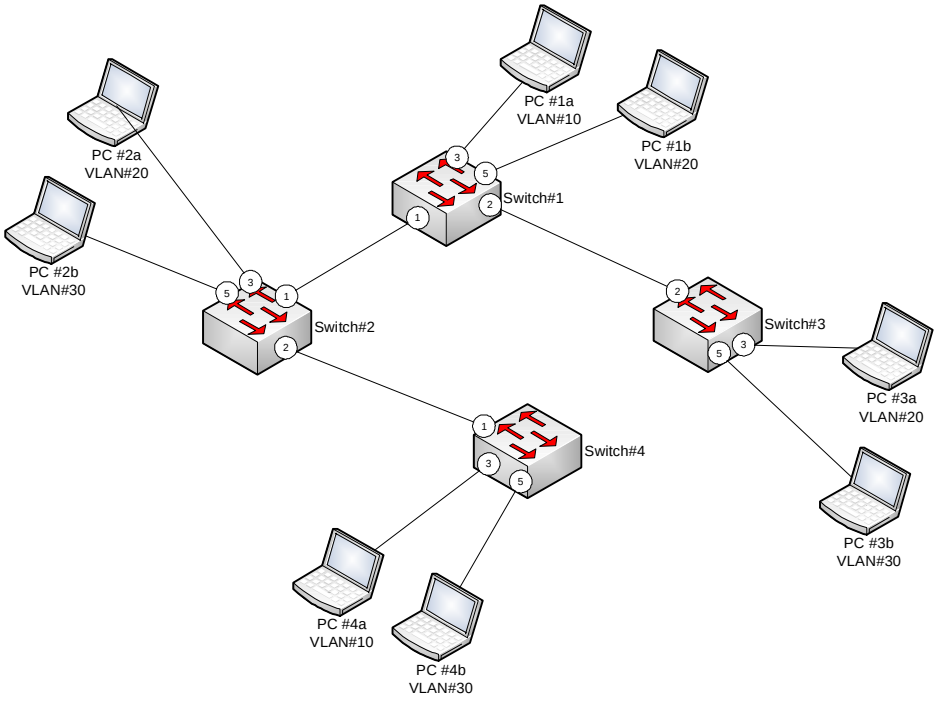
Köprü Adı	Port	Kök Yol Maliyeti
Switch#4	1	4.000
Switch#4	2	-
Switch#4	4	20.000

Buna göre her köprü üzerindeki minimum kök yol maliyeti değerleri aşağıdaki gibi oluşur. Bu MST bölümü için tüm köprüler üzerinde minimum kök yol maliyeti değerinin oluştuğu port hariç tüm portlar bloklama durumuna alınır ve sadece bu MST bölümü için bu portlardan trafik geçişine izin vermez. Bloklama fiziksel değil mantıksal olarak yapılır.

Çizelge 28. MSTP kullanımı örneği Instance#1 kök yol maliyeti değerleri - 6

Köprü Adı	Port	Kök Yol Maliyeti
Switch#1	-	-
Switch#2	1	2.000
Switch#3	2	2.000
Switch#4	1	4.000

Buna göre oluşacak döngülerden arındırılmış ağ aktif yolu aşağıdaki gibidir.



Şekil 7. MSTP sayesinde döngülerden arındırılmış ağ aktif yolu – 1.

Instance#2 için kök köprü seçimi aşağıdaki veriler ışığında yapılır.

Çizelge 29. MSTP kullanımı örneği Instance#2 köprü ID listesi

Köprü Adı	Köprü Öncelik Değeri (16bit)	MAC Adresi (48 bit)		Köprü ID (16+48=64 bit)
Switch#1	4*4096=40:00	00:00:00:00:00:01	**à**	40:00:00:00:00:00:00:01
Switch#2	3*4096=30:00	00:00:00:00:00:02	**à**	30:00:00:00:00:00:00:02
Switch#3	2*4096=20:00	00:00:00:00:00:03	**à**	20:00:00:00:00:00:00:03
Switch#4	1*4096=10:00	00:00:00:00:00:04	**à**	10:00:00:00:00:00:00:04

Yukarıdaki tabloya göre en küçük köprü ID değeri Switch#4 köprüsüne ait olduğundan Instance#2 için kök köprü, Switch#4 olarak seçilir. Tüm köprüler BPDU çerçevelerini aldığı her port için MSTI bilgilerine uygun kök yol maliyeti değerini hesaplamaya başlar.

Çizelge 30. MSTP kullanımı örneği Instance#2 kök yol maliyeti değerleri - 1

Köprü Adı	Port	Kök Yol Maliyeti
Switch#1	1	-
Switch#1	2	-
Switch#1	4	0 + 20.000 = 20.000
Switch#2	1	-
Switch#2	2	0 + 2.000 = 2.000
Switch#3	1	0 + 2.000 = 2.000
Switch#3	2	-
Switch#4	1	0
Switch#4	2	0
Switch#4	4	0

Köprüler Instance#2'e ait kök köprüden kendisine gelen BPDU'ları kenar port olarak belirlenmemiş portlarına gönderir. Ayrı ayrı incelendiğinde Switch#2'nin gönderdiği BPDU'yu alan Switch#1 kendi parametrelerini aşağıdaki gibi düzenler.

Çizelge 31. MSTP kullanımı örneği Instance#2 kök yol maliyeti değerleri - 2

Köprü Adı	Port	Kök Yol Maliyeti
Switch#1	1	2.000 + 2.000 = 4.000
Switch#1	2	-
Switch#1	4	20.000

Switch#1'in gönderdiği BPDU'yu alan Switch#2 kendi portları üzerindekinden daha küçük bir kök yol maliyeti değeri ile gelmediğinden bu çerçeve için bir değişiklik yapmaz.

Çizelge 32. MSTP kullanımı örneği Instance#2 kök yol maliyeti değerleri - 3

Köprü Adı	Port	Kök Yol Maliyeti
Switch#2	1	-
Switch#2	2	2.000

Switch#1'in gönderdiği BPDU'yu alan Switch#3 kendi portları üzerindekinden daha küçük bir kök yol maliyeti değeri ile gelmediğinden bu çerçeve için bir değişiklik yapmaz.

Çizelge 33. MSTP kullanımı Instance#2 kök yol maliyeti değerleri - 4

Köprü Adı	Port	Kök Yol Maliyeti
Switch#3	1	2.000
Switch#3	2	-

Switch#3'in gönderdiği BPDU'yu alan Switch#1 kendi portları üzerindekinden daha küçük bir kök yol maliyeti değeri ile gelmediğinden bu çerçeve için bir değişiklik yapmaz.

Çizelge 34. MSTP kullanımı Instance#2 kök yol maliyeti değerleri - 5

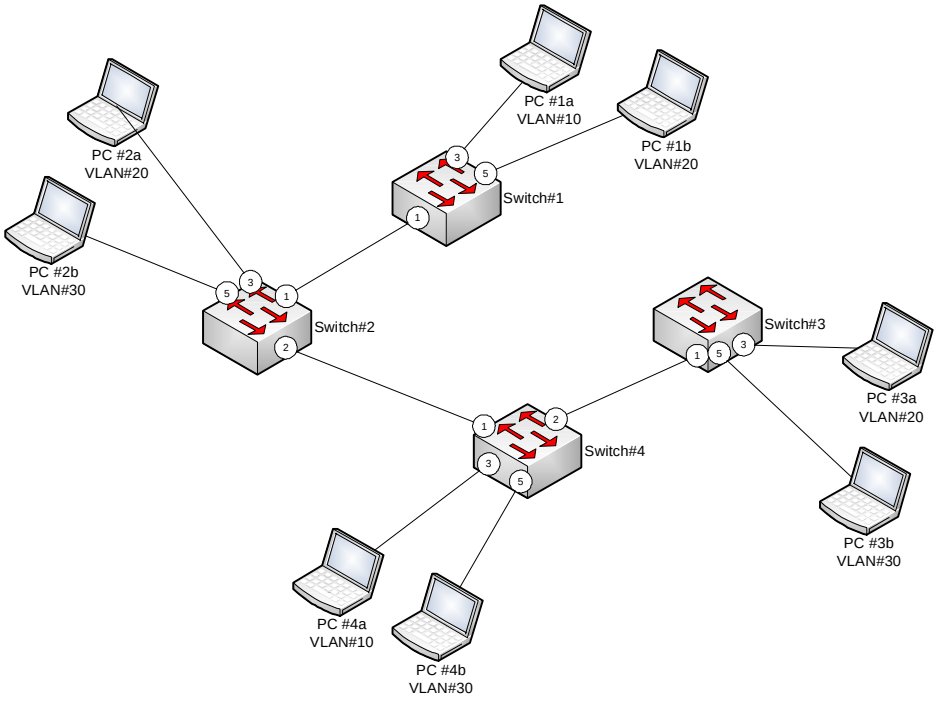
Köprü Adı	Port	Kök Yol Maliyeti
Switch#1	1	4.000
Switch#1	2	-
Switch#1	4	20.000

Buna göre her köprü üzerindeki minimum kök yol maliyeti değerleri aşağıdaki gibi oluşur. Bu MST bölümü için tüm köprüler üzerinde minimum kök yol maliyeti değerinin oluştuğu port hariç tüm portlar bloklama durumuna alınır ve sadece bu MST bölümü için bu portlardan trafik geçişine izin vermez. Yani bloklama fiziksel değil mantıksal olarak yapılır.

Çizelge 35. MSTP kullanımı Instance#2 kök yol maliyeti değerleri - 6

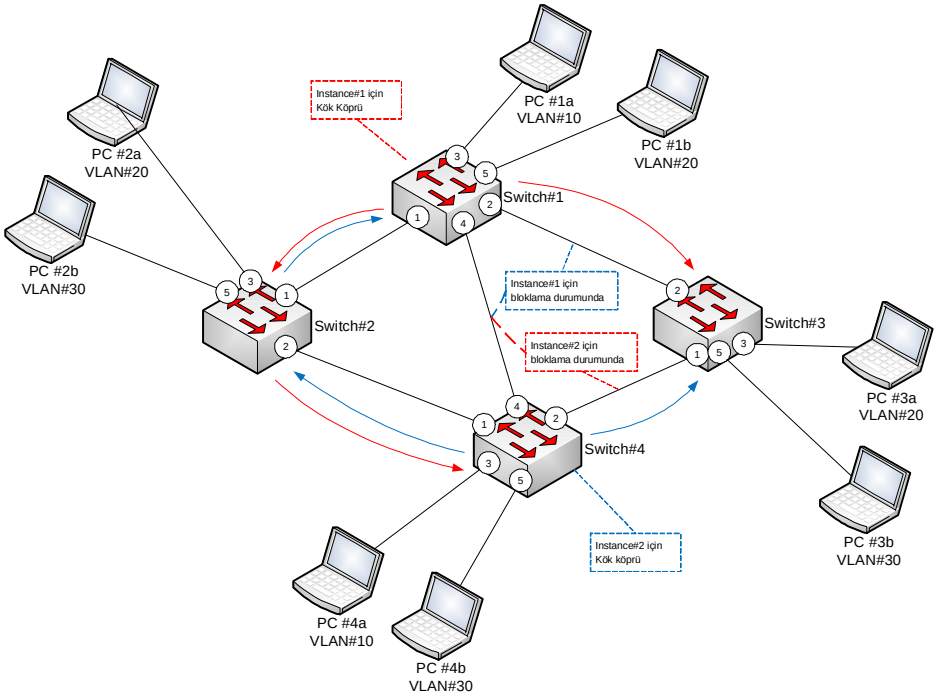
Köprü Adı	Port	Kök Yol Maliyeti
Switch#1	1	4.000
Switch#2	2	2.000
Switch#3	1	2.000
Switch#4	-	-

Buna göre oluşacak döngülerden arındırılmış ağ aktif yolu aşağıdaki gibidir.



Şekil 8. MSTP sayesinde döngülerden arındırılmış ağ aktif yolu – 2.

Instance#1 ve Instance#2 için oluşan aktif ağ ayrı trafik akış yoluna sahip olduğundan ağda bir anlamda yük dengelemesi sağlanmış olur (Bkz. Şekil 9).



Şekil 9. MSTP sayesinde döngülerden arındırılmış ağ aktif yolu – 3.

3.2.4. SMP (HP Switch Meshing Protocol)

Veri Bağı katmanı kullanılabilirliğini arttırmak için farklı iki nokta arasında bir diğer nokta üzerinden geçmek şartıyla birden fazla yol bulunan ağlarda, döngüler ağı kullanılamaz hale getirirler. SMP, STP'den farklı olarak portları bloklamak yerine onları aktif olarak kullanabileceği başka bir yaklaşımda bulunur. Bu yaklaşımda köprüler bir *Meshing Domain* içine dahil edilirler. Aynı meshing domain içindeki köprüler kendilerine gelen broadcast ve multicast trafiğini sadece bir tek yol üzerinden göndermek için bir broadcast yolu belirlerler (Anonim, 2009). Böylece yedekli hatlar bloklanmadan hem kullanılabilirlik hem de kapasite artışı sağlanır. SMP'nin HP'ye özel bir protokol olması ve Meshing Domain'de yönlendirmenin aktif edilememesi bu protokolün büyük ve geniş ağlarda tercih edilmemesinin önemli sebeplerindendir.

3.3. Ağ Katmanı Çözüm Yaklaşımları

IP adresleri tekil ve yinelemez olduklarından tüm cihazların kendi ağ blokları haricindeki diğer ağ bloklarına veya internete ulaşımını sağlayan ağ geçidi cihazları tüm ağlarda olduğu gibi İSDEMİR ağı için de *single point of failure* durumundadır. Ağ katmanı bağlamında yedeklilik, uygun protokoller yardımıyla aynı IP adresi ile birden fazla ağ geçidinin ifade edilmesidir. Ağ geçitlerinin IP bağlamında yedekliliğinin sağlanması için tanımlanmış protokolleri aşağıda açıklanmıştır.

3.3.1. VRRP (Virtual Router Redundancy Protocol)

RFC3768'de tanımlanarak standartlaştırılmış bir protokoldür. Birden fazla yönlendiricinin sanal bir IP adresi üzerinden tek yönlendirici gibi davranmasını sağlar. Yönlendiricilerden birisi *asıl* (Master) durumunda iken diğer tüm yönlendiriciler *yedek* (Backup) durumuna geçerler. VRRP'de asıl yönlendiricilerin seçimi aşamasında ilk dikkate alınan parametre belirlenen öncelik değeridir. VRRP'de *preempt* parametresinin öntanımlı olarak aktif gelmesinden dolayı öncelik değerlerinden büyük olanı, eşitlik durumunda ise IP adresi büyük olanı asıl durumuna geçer. Sanal IP adresinin yönlendiricilerin IP'lerinden farklı olması durumunda öncelik değerleri 1-254 arasındadır. Sanal IP adresi, yönlendiricilerin herhangi birisinin aynı ağ bloğundaki IP adresi de olabilir. Bu durumda öncelik değeri 255 olmalıdır. Öntanımlı öncelik değeri 100'dür (Hinden, 2004).

VRRP paketleri 224.0.0.18 multicast adresine gönderilir. Gönderilen paketin TTL'i 255'dir. VRRP yönlendiricileri paketlerin TTL'lerini kontrol ederler ve 255'ten küçük

TTL'e sahip olan paketler yani birden fazla atlama yapan paketler dikkate alınmazlar (Hinden, 2004).

VRRP'de her VRID için farklı bir asıl yönlendiricinin belirlenmesi ve hostların bu VRID'lere dağıtılması ile yük dengelemesi sağlanabilir.

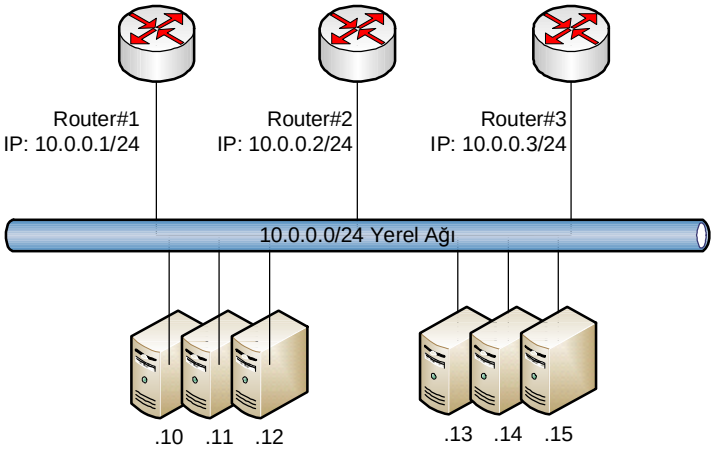
Aktif yönlendiricilerin değişmesi durumunda MAC adresi tablolarında güncelleme yapılmasının engellenmesi için her VRID'ye tanımlı sanal IP adresine ait sanal bir MAC adresi belirlenir. Bu işlem kullanılan medya tipine göre değişkenlik gösterir. Token-Ring ağlar için en fazla belirlenecek VRID sayısı 11'dir ve bu VRID'ler 1-11 arasındaki sayılardır. Bu VRID'ler için sanal MAC adresleri aşağıdaki gibidir (Hinden, 2004).

Çizelge 36. VRRP Token-Ring MAC adresi bilgisi

VRID	Token-Ring Sanal MAC adresi
1	03-00-02-00-00-00
2	03-00-04-00-00-00
3	03-00-08-00-00-00
4	03-00-10-00-00-00
5	03-00-20-00-00-00
6	03-00-40-00-00-00
7	03-00-80-00-00-00
8	03-00-00-01-00-00
9	03-00-00-02-00-00
10	03-00-00-04-00-00
11	03-00-00-08-00-00

Ethernet ve kablosuz ağlar için belirlenebilecek VRRP grup sayısı en fazla 255'tir ve VRID'leri 1-255 arasındaki sayılardan oluşur. Buna göre sanal MAC adresi 00-00-5E-00-01-(16'lık tabanda Grup ID) olarak belirlenir (Hinden, 2004).

Asıl durumdaki bir VRRP yönlendiricisi birden fazla sanal IP adresini kontrol edebilir. Aşağıdaki şekil üzerinden VRRP'nin kullanım amacı ve çalışma prensipleri örneklenmiştir.



Şekil 10. Virtual Router Redundancy Protokolü kullanımı örneği.

Herhangi bir ağda olduğu gibi yukarıdaki topoloji için de söz edilmesi gereken ilk şey hostlar için belirlenmiş varsayılan ağ geçidi yapılandırması yapılmadan bu hostların kendi alt ağları dışındaki ağlar ile iletişim kuramayacaklarıdır. Bu topoloji hakkındaki VRRP için gerekli olan bilgiler aşağıdaki gibidir.

Çizelge 37. VRRP kullanımı örneği için yönlendirici bilgileri

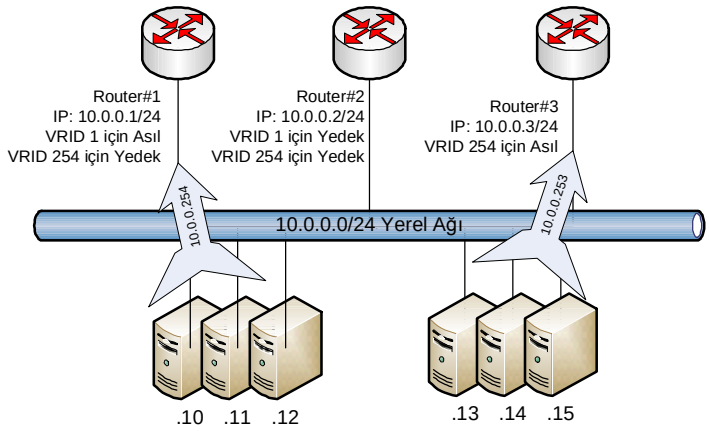
Yönlendirici Bilgileri		
Yönlendirici Adı	Yönlendirici Önceliği	VRID
Router#1	200	1
Router#1	100	254
Router#2	100	1
Router#2	100	254
Router#3	100	254

Çizelge 38. VRRP kullanımı örneği için VRID bilgileri

VRID Bilgileri		
VRID	Ağ Geçidi	MAC Adresi (00-00-5E-00-01-(16'lık tabanda Grup ID))
1	10.0.0.254	00-00-5E-00-01-01
254	10.0.0.253	00-00-5E-00-01-FE

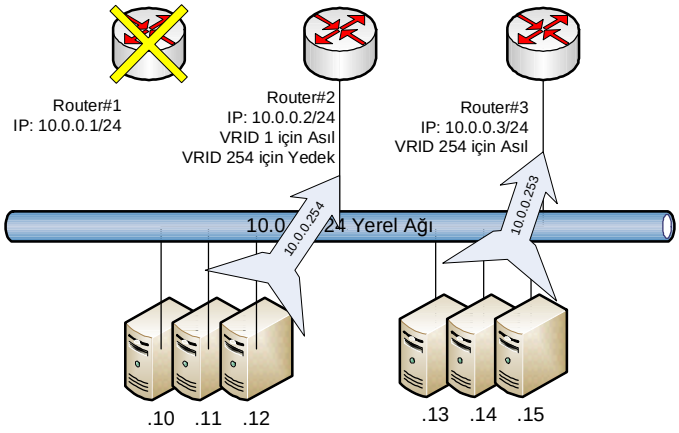
Bu bilgiler ışığında VRID değeri 1 olan grup için en yüksek öncelikli yönlendirici olan Router#1 asıl durumuna geçer. Bu VRID grubundaki diğer tek yönlendirici olan Router#2 yedek durumuna geçer. VRID değeri 254 olan grup için tüm yönlendiricilerin

öncelik değerleri aynı olduğu için en yüksek IP adresine bakılarak Router#3 asıl yönlendirici olarak belirlenir. Bu VRID grubundaki diğer yönlendiriciler yedek durumuna geçerler. Bu bağlamda VRID değeri 1 olan VRRP grubu için sanal yönlendirici IP'si olan 10.0.0.254 adresine gelen yönlendirme istekleri Router#1, VRID değeri 254 olan VRRP grubu için sanal yönlendirici IP'si olan 10.0.0.253 adresine gelen yönlendirme istekleri Router#3 tarafından kontrol edilir. 10.0.0.0/24 yerel ağı için iki farklı yönlendirici üzerinden iletişim gerçekleştirilmesi ile yedekliliğin yanı sıra yük dengelemesi de sağlanmış olur. Şekil üzerinden aşağıdaki gibi ifade edilebilir.



Şekil 11. VRRP sayesinde yönlendirici yedekliliği sağlanması – 1.

Yine bu topoloji üzerinden Router#1 yönlendiricisinde meydana gelecek olan bir problemi örnekleyecek olursak VRID değeri 254 olan VRRP grubu için yönlendirici yedek durumunda olduğu için bu değişiklik topolojiyi etkilemez. Ancak VRID değeri 1 olan VRRP grubu için bu yönlendirici asıl durumunda olduğundan belli bir süre sonra bu yönlendiriciden protokol bilgilerinin gelmemesi üzerine yedek durumunda olan Router#2 yönlendiricisi asıl durumuna geçer.



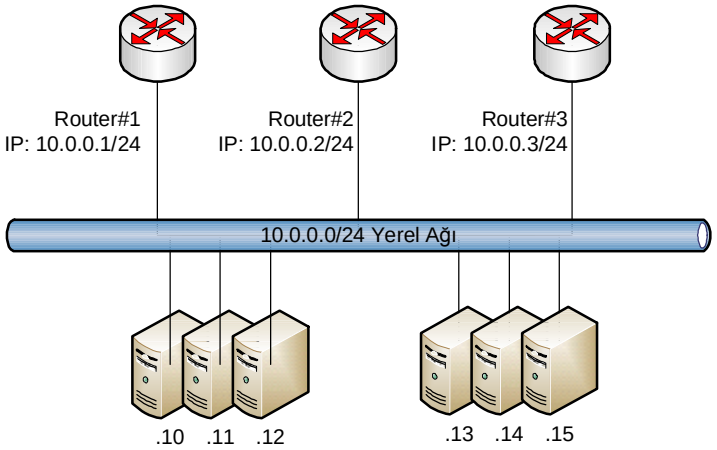
Şekil 12. VRRP sayesinde yönlendirici yedekliliği sağlanması – 2.

Router#1'in tekrar topolojiye dahil olduğuna dair protokol bilgilerini gönderdiği andan itibaren topolojinin değişimi tekrar tetiklenir.

3.3.2. HSRP (Cisco Hot Standby Router Protocol)

RFC2281 ile tanımlanmasına rağmen Cisco'ya özgü bir protokoldür. VRRP gibi birden fazla yönlendiricinin sanal bir IP üzerinden tek yönlendirici gibi davranmasını sağlar. Yönlendiricilerden birisi a*ktif* (active) durumunda iken bir yönlendirici *bekleme* (standby) durumuna geçer, diğer tüm yönlendiriciler *dinleme* (listening) durumuna geçerler. HSRP'de aktif yönlendiricilerin seçimi aşamasında ilk dikkate alınan parametre belirlenen öncelik değeridir. 0-254 arasında belirlenen bu değerden büyük olanın aktif duruma geçmesi beklenir. Ancak *preempt* parametresi ile aktif olmayan yüksek öncelikli yönlendiricinin aktif olması için yapılandırma değişikliğine gidilmesi zorlanabilir. Önceliklerin eşitliği durumunda ise IP adresi büyük olan yönlendirici aktif duruma geçer. Öntanımlı öncelik değeri 100'dür. HSRP paketleri UDP 1985 portu üzerinden kapsüllenerek 224.0.0.2 multicast adresine gönderilir. Gönderilen paketin TTL'i 1'dir. Yani sadece tek atlama sonra paket ölür. HSRP'de sanal IP adresi, her yönlendiricinin o ağ bloğundaki IP adresinden farklı bir IP adresi olarak belirlenir. HSRP'de her HSRP grubu için farklı bir aktif yönlendiricinin belirlenmesi ve hostların bu gruplara dağıtılması ile yük dengelemesi sağlanabilir. (Li ve ark., 1998)

Aktif yönlendiricilerin değişmesi durumunda MAC adresi tablolarında güncelleme yapılmasının engellenmesi için her HSRP grubu için tanımlı sanal IP adresi için sanal bir MAC adresi belirlenir. Bu işlem kullanılan medya tipine göre değişkenlik gösterir. Token-Ring ağlar için en fazla belirlenecek HSRP grup sayısı 3'tür ve grup ID'leri 0, 1 ve 2 rakamlarından oluşur. Buna göre sanal MAC adresi C0-00-00-0(2)^(Grup ID)-00-00 olarak belirlenir. Ethernet ve kablosuz ağlar için belirlenebilecek HSRP grup sayısı en fazla 255'tir ve grup ID'leri 0-254 arasındaki sayılardan oluşur. Buna göre sanal MAC adresi 00-00-0C-07-AC-(16'lık tabanda grup ID) olarak belirlenir (Li ve ark., 1998). Aşağıdaki şekil üzerinden HSRP'nin kullanım amacı ve çalışma prensipleri örneklenmiştir.



Şekil 13. Hot Standby Router Protokolü kullanımı örneği.

Herhangi bir ağda olduğu gibi yukarıdaki topoloji için de söz edilmesi gereken ilk şey hostlar için belirlenmiş varsayılan ağ geçidi yapılandırması yapılmadan bu hostların kendi alt ağları dışındaki ağlar ile iletişim kuramayacaklarıdır. Bu topoloji hakkındaki HSRP için gerekli olan bilgiler aşağıdaki gibidir.

Çizelge 39. HSRP kullanımı örneği için yönlendirici bilgileri

Yönlendirici Bilgileri		
Yönlendirici Adı	Yönlendirici Önceliği	HSRP Grup ID
Router#1	200	1
Router#1	100	254
Router#2	100	1
Router#2	100	254
Router#3	100	254

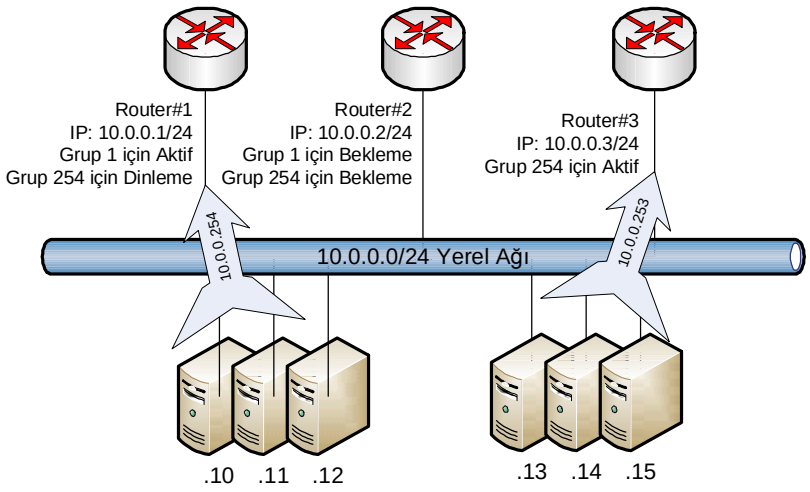
Çizelge 40. HSRP kullanımı örneği için HSRP grup bilgileri

HSRP Grup Bilgileri		
Grup ID	Ağ Geçidi	MAC Adresi (00-00-0C-07-AC-(16'lık tabanda Grup ID))
1	10.0.0.254	00-00-0C-07-AC-01
254	10.0.0.253	00-00-0C-07-AC-FE

Bu bilgiler ışığında 1 numaralı HSRP Grubu için en yüksek öncelikli yönlendirici olan Router#1 aktif durumuna geçer. Bu HSRP grubundaki diğer tek yönlendirici olan

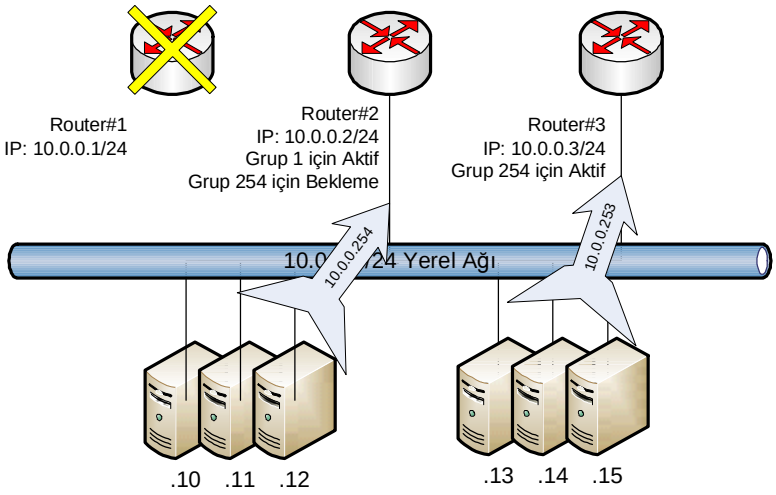
Router#2 bekleme durumuna geçer. 254 numaralı HSRP grubu için tüm yönlendiricilerin öncelik değerleri aynı olduğu için en yüksek IP adresine bakılarak Router#3 aktif yönlendirici olarak belirlenir. Bu HSRP grubundaki aktif durumda çalışan yönlendirici dışındaki en yüksek IP adresine sahip yönlendirici olan Router#2 bekleme durumuna geçerken Router#1 dinleme durumuna geçer.

Bu bağlamda grup ID'si 1 olan HSRP grubu için sanal yönlendirici IP'si olan 10.0.0.254 adresine gelen yönlendirme istekleri Router#1, grup ID'si 254 olan HSRP grubu için sanal yönlendirici IP'si olan 10.0.0.253 adresine gelen yönlendirme istekleri Router#3 tarafından kontrol edilir. 10.0.0.0/24 yerel ağı için iki farklı yönlendirici üzerinden iletişim gerçekleştirilmesi ile yedekliliğin yanı sıra yük dengelemesi de sağlanmış olur. Şekil üzerinden aşağıdaki gibi ifade edilebilir.



Şekil 14. HSRP sayesinde yönlendirici yedekliliği sağlanması – 1.

Yine bu topoloji üzerinden Router#1 yönlendiricisinde meydana gelecek olan bir problemi örnekleyecek olursak grup ID'si 254 olan HSRP grubu için yönlendirici dinleme durumunda olduğu için bu değişiklik topolojiyi etkilemez. Ancak grup ID'si 1 olan HSRP grubu için bu yönlendirici aktif durumda olduğundan belli bir süre sonra bu yönlendiriciden protokol bilgilerinin gelmemesi üzerine bekleme durumunda olan Router#2 yönlendiricisi aktif durumuna geçer. Şekil üzerinden aşağıdaki gibi ifade edilebilir.



Şekil 15. HSRP sayesinde yönlendirici yedekliliği sağlanması – 2.

Router#1'in tekrar topolojiye dahil olduğuna dair protokol bilgilerini gönderdiği andan itibaren *preempt* parametresi aktifleştirilmişse topolojinin değişimi tekrar tetiklenir. Diğer durumda Router#2 yönlendiricisinde bir problem olmadığı sürece aktif yönlendirici değişmez. p*reempt* parametresi ile aktif yönlendirici değişiklikleri yalnızca önceliklerin farklı olması durumunda gerçekleştirilir, IP büyüklüğünden dolayı geçişler bu parametre ile tetiklenemez.

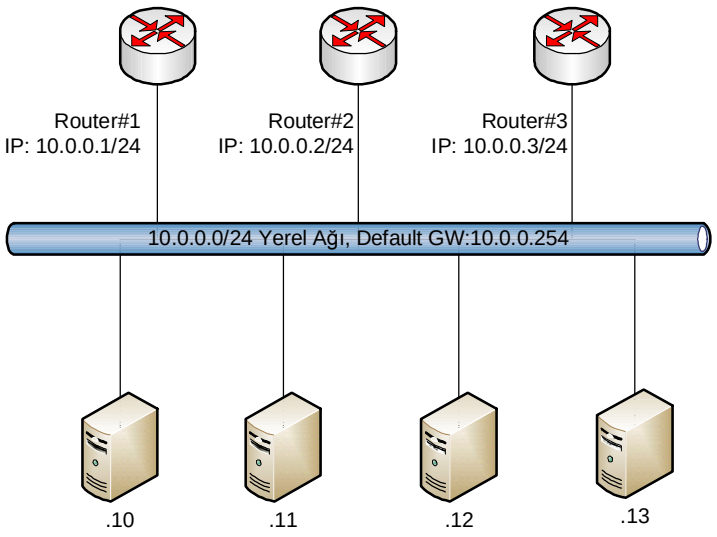
3.3.3. GLBP (Gateway Load Balancing Protocol)

Cisco tarafından tasarlanmış bir yük dengeleme protokolü olan Gateway Load Balancing Protokolü, birden çok kullanılabilir ağ geçidinin aynı anda kullanılmasını ve ayrıca buna ek olarak bu ağ geçitlerinin arıza durumunda otomatik birbirlerinin yerine geçmesini sağlar. GLBP grup üyeleri kendi gruplarında AVG (Active Virtual Gateway (Aktif Sanal Ağ Geçidi)) olması için bir ağ geçidi belirlerler. Diğer grup üyeleri AVG'nin kullanılamaz olduğu durumlar için yedekliliği sağlarlar. AVG, GLBP grup üyelerinin her birisi için bir sanal MAC adresi ataması yapar. Her ağ geçidi kendisi için AVG tarafından ataması yapılan MAC adresine gelen paketlerin iletilmesi sorumluluğunu üstlenir. Bu ağ geçitleri kendi MAC adresleri için AVF (Active Virtual Forwarder (Aktif Sanal İletici))'ler olarak adlandırılırlar. AVG, sanal IP adresleri için yapılan ARP isteklerinin cevaplanmasından sorumludur. Yük paylaştırılması AVG'nin ARP isteklerini farklı sanal MAC adresleri ile cevaplaması ile gerçekleştirilir (Conlan, 2009).

Bu MAC adresinin formatı 0007.B4xx.xxyy şeklindedir. xx.xx 16'lık tabanda grup numarası, yine 16'lık tabanda yy ise AVF numarasıdır (Arregoces ve Portolani, 2004).

Yukarıdaki alıntılarda da belirtildiği gibi AVG, sanal yönlendirici IP adresine gönderilmiş ARP isteklerini cevaplamakla görevlidir. Ancak cevaplarken, ARP cevap paketi içerisindeki MAC adresi bilgisini ağırlıklara göre sıradaki yönlendiricinin MAC adresini yazarak gönderir (Hucaby, 2004). Böylece yük dengelenmesi sağlanmış olur.

AVG'nin seçiminde VRRP ve HSRP'de olduğu gibi yine öncelik parametresi rol oynar. En yüksek öncelik değerine sahip yönlendirici AVG olurken sonraki en yüksek önceliğe sahip yönlendirici ***bekleyen AVG*** (standby AVG) durumuna geçer. Diğer yönlendiriciler ***dinleme*** (listening) durumundadır. AVG'nin erişilemez olduğu durumlarda bekleyen AVG kendisini AVG olarak tanıtır. HSRP'deki gibi önceliklerin aynı olması durumunda IP adresi büyük olan daha önceliklidir. AVF'lerin tümü yük dengeleme algoritması tarafından kullanıldıklarından aslında aktif olmaları sebebiyle birbirlerini yedeklerler (Arregoces ve Portolani, 2004). Aşağıdaki şekil üzerinden GLBP'nin kullanım amacı ve çalışma prensipleri örneklenmiştir.



Şekil 16. Gateway Load Balancing Protokolü kullanımı örneği.

Herhangi bir ağda olduğu gibi yukarıdaki topoloji için de söz edilmesi gereken ilk şey hostlar için belirlenmiş varsayılan ağ geçidi yapılandırması yapılmadan bu hostların kendi alt ağları dışındaki ağlar ile iletişim kuramayacaklarıdır. Bu topoloji hakkındaki GLBP için gerekli olan bilgiler aşağıdaki gibidir.

Çizelge 41. GLBP kullanımı örneği için yönlendirici bilgileri

Yönlendirici Bilgileri			
Yönlendirici Adı	Yönlendirici Önceliği	GLBP Grup ID	Ağırlık
Router#1	200	1000	50
Router#2	100	1000	25
Router#3	100	1000	25

Bu bilgiler ışığında protokol tarafından 1000 numaralı GLBP grubu için en yüksek öncelikli yönlendirici olan Router#1, AVG olarak belirlenirken öncelikleri aynı olan yönlendiricilerden IP adresi daha büyük olan Router#3 bekleyen AVG olur. Protokol gereği diğer yönlendirici Router#2 dinleme durumuna geçer. Bu aşamadan sonra AVG tarafından AVF'ler için belirlediği sanal MAC adresleri atamasını yapar.

Çizelge 42. GLBP kullanımı örneği için AVF bilgileri

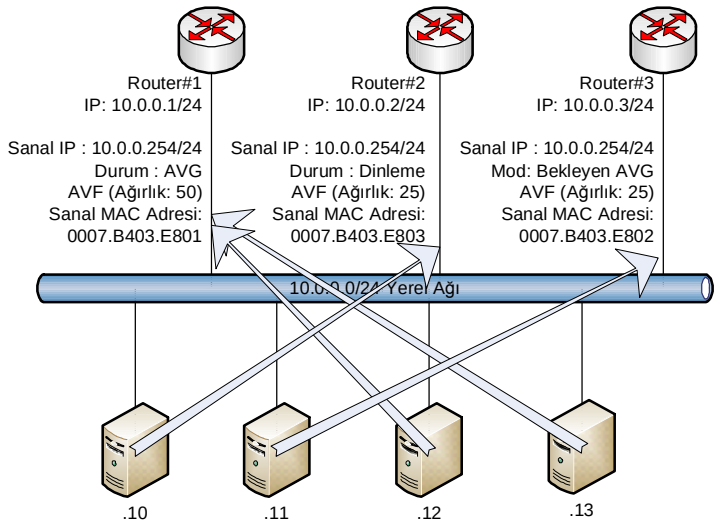
AVF Bilgileri	
AVF Adı	Sanal MAC Adresi (0007.B4xx.xxyy)
Router#1	0007.B403.E801
Router#2	0007.B403.E803
Router#3	0007.B403.E802

MAC adresi atamasından sonra GLBP hizmet vermeye hazır anlamına gelir. Gelen ARP isteklerine yönlendiriciler üzerinde belirlenmiş ağırlık parametreleri ışığında sıradaki yönlendiriciye ait sanal MAC adresleri yazılarak cevap verilir. AVG tarafından Router#1 AVF'sinin ağırlığı diğerlerinin 2 katı olduğundan gelen ARP isteklerinin her dört tanesinden ikisi Router#1 AVF'sine gönderilirken, sonraki yapılacak ARP isteğinden birisi Router#3 AVF'sine, diğeri ise Router#2 AVF'sine gönderilir. 10.0.0.13, 10.0.0.12, 10.0.0.11, 10.0.0.10 hostlarından ARP isteklerinin sırası ile yapıldığı varsayılırsa bu hostlara verilen ARP cevapları aşağıda gösterilen tablodaki gibi olur.

Çizelge 43. GLBP kullanımı örneği için ARP cevapları - 1

Host	ARP isteği yapılan IP	ARP cevabı
10.0.0.13	10.0.0.254	0007.B403.E801
10.0.0.12	10.0.0.254	0007.B403.E801
10.0.0.11	10.0.0.254	0007.B403.E802
10.0.0.10	10.0.0.254	0007.B403.E803

Görüldüğü gibi hostlara, aynı varsayılan ağ geçidi IP'si için gönderilen ARP cevapları birbiri ile aynı değildir. Bu sebeple hostlardan gönderilecek paketler farklı yönlendiricilere gidecek ve ağ trafiği yük paylaşımı sağlanmış olacaktır. Buna göre GLBP tarafından oluşturulan yönlendiricilerin yedekliliğinin ve ağ trafiği yük paylaşımının sağlandığı ağ şekil üzerinden aşağıdaki gibi ifade edilebilir.



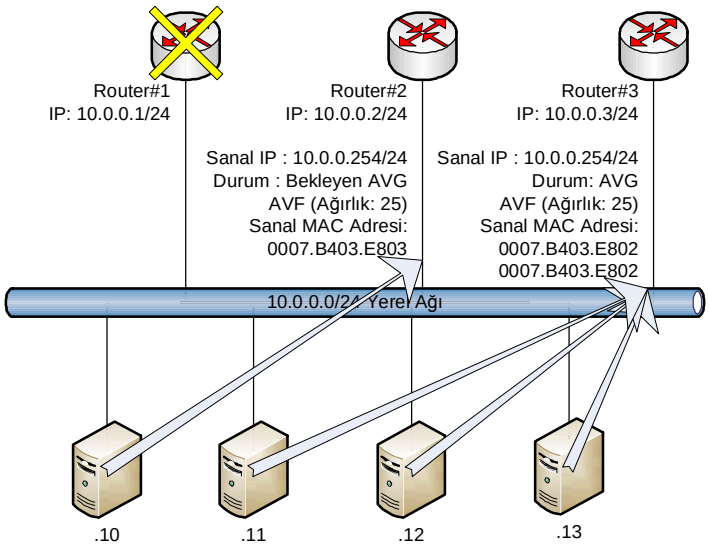
Şekil 17. GLBP sayesinde yönlendirici yedekliliği sağlanması – 1.

Yine bu topoloji üzerinden AVG olan Router#1 yönlendiricisinde meydana gelecek olan bir problem ele alındığında protokol bilgilerine ait mesajların gelmediğini fark eden bekleyen AVG olan Router#3 yönlendiricisi kendisini yeni AVG olarak anons eder. Ayrıca Router#1 AVF'sine ait sanal MAC adresine gelen paketlerin de iletimini kendisi üstlenerek hostların topoloji değişiminden etkilenmemesini sağlarken, topoloji değişimi mesajı göndererek Router#2'nin bekleyen AVG olmasını tetikler. Tüm bu işlemlerden hostlar soyutlandığından ARP tablolarında da değişiklik olmaz.

Çizelge 44. GLBP kullanımı örneği için ARP cevapları - 2

Host	ARP isteği yapılan IP	ARP cevabı
10.0.0.13	10.0.0.254	0007.B403.E801
10.0.0.12	10.0.0.254	0007.B403.E801
10.0.0.11	10.0.0.254	0007.B403.E802
10.0.0.10	10.0.0.254	0007.B403.E803

Buradaki önemli nokta, varsayılan ağ geçidinin MAC adresi Router#1 yönlendiricisinin sanal MAC adresi 0007.B403.E801 olan hostların kesintiden etkilenmemesi için bu MAC adresine ait paketler ile yeni AVG Router#3 yönlendiricisinin kendisinin ilgilenmesidir.



Şekil 18. GLBP sayesinde yönlendirici yedekliliği sağlanması – 2.

Router#1'in tekrar topolojiye dahil olduğuna dair protokol bilgilerini gönderdiği andan itibaren ***preempt*** parametresi aktifleştirilmişse topolojinin değişimi tekrar tetiklenir. Diğer durumda Router#3 yönlendiricisinde bir problem olmadığı sürece AVG değişmez. ***preempt*** parametresi ile AVG yönlendirici değişiklikleri yalnızca önceliklerin farklı olması durumunda gerçekleştirilir, IP büyüklüğünden dolayı geçişler bu parametre ile tetiklenemez.

BÖLÜM 4

ARAŞTIRMA BULGULARI VE TARTIŞMA

Önceki bölümde ağ yedekliliği ve kullanılabilirliğin arttırılması amacıyla OSI Referans modelinin ilgili katmanlarına özgü farklı çözüm yaklaşımlarını belirtilmiştir. İSDEMİR'deki iş-kritik uygulama ve süreçlerinin devamlılığının sağlanması için bu yaklaşımların kendi katmanları içerisinde birbirlerine olan üstün ve zayıf yönlerini ortaya koyarak benimsenen yaklaşımlar sayesinde oluşturulmuş ağ sistemi anlatılmıştır.

4.1. Fiziksel Katman Çözüm Yaklaşımları

Fiziksel katman için çözüm yaklaşımı her bir bileşenin fiziksel yedeğinin temin edilmesine dayandığından kablolama ve aktif cihazların birebir yedeklerinin İSDEMİR'in iş kritik süreçlerinin etkilenmemesi için temini gereklidir.

Kablolama kapsamında, istatistiksel olarak aynı anda farklı fiziksel güzergahlardan çekilen iki farklı kablo üzerinde problem oluşma ihtimali, tek bir kablo üzerinde problem oluşma ihtimalinin yarısı kadardır. Bu da ağ kullanılabilirliğini ve güvenilirliğini arttırır. Ancak yaklaşımın yapılandırma ve yönetim zorluklarını doğurması nedeniyle optimum çözüm için yukarıda da bahsedildiği gibi her lokasyon için değil, her iş-kritik süreç ve uygulamaların olduğu lokasyon için uygulanacaktır.

Ağ aktif cihazlarından kaynaklı problemlerin en aza indirilmesi amacıyla fiziki yedekliliğin sağlanması gereklidir. Yedeklilik, cihazların yedekleri ile birlikte eşzamanlı olarak çalışması ya da çalışan aktif cihazla birebir aynı en az bir adet cihazın stoklarda bulundurulması olarak düşünülmelidir. Her iki durumda da cihaz arızasından dolayı üretim sürecinin etkilenmesi ihtimali yarıya indirilir. Eşzamanlı çalışan sistemler oluşturulması için OSI Referans Modeli'nin ilgili katmanları için cihazlar üzerinde yapılandırmaların yapılması zorunluluğu vardır, ancak oluşacak problemlere en kısa zamanda müdahalenin yapılması ve sistemin herhangi bir kesintiye mahal vermeden ayakta tutulması için büyük avantaj sağlar. Cihazların birebir yedeklerinin stoklanması yaklaşımında stok maliyetleri artacağından çok iyi planlanma yapılmalıdır. Arıza veya problem anında cihazın birebir yedeği ile değiştirilmesi ikinci bir iş gücü maliyetine sebep olmaktadır. Ancak cihazlar üzerinde yedekliliğin sağlanması ile ilgili bir yapılandırma gereksinimi olmadığından ve bakım faaliyetleri için fazladan kaynak kullanılmadığından bir anlamda iş gücü kazancı sağlayacaktır. Bu bağlamda İSDEMİR'de oluşturulacak fiziksel topoloji için Yıldız

Topolojiden çok Mesh Topoloji'ye benzeyen bir topoloji mimarisi uygun görülmüştür. Bu topolojiyi elde etmek için iş-kritik süreç ve uygulamaların koştuğu her lokasyona mevcut 140 km'lik fiber-optik kabloların yedekliliğinin sağlanması adına alternatif güzergahlardan götürülen 80 km'den fazla fiber-optik kablo çekimi yapılmıştır. Bu kablolar için yaklaşık 4300 adet fiber-optik sonlandırma ve füzyon yapılarak hatlar çalışabilecek duruma getirilmiştir. Sunucular ve bazı çok önem arz eden uç nokta cihazları için ise var olan yaklaşık 90 km'lik UTP kablo yedekliliğinin sağlanması adına 30 km kadar daha UTP hat çekilmiştir. Bu kablolar için yaklaşık 600 adet UTP kablo sonlandırılması yapılmıştır. Kablolama İSDEMİR personelleri tarafından 3-4 ay gibi kısa bir sürede tamamlanmıştır. Toplamda var olan 300'den fazla aktif cihazın yedekliliğinin sağlanması ile ilgili olarak 55 adet yedek cihaz temini yapılmıştır.

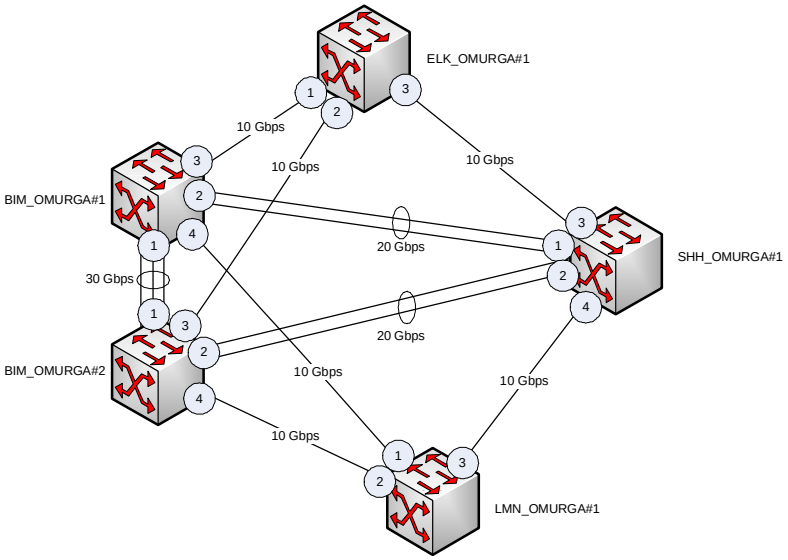
Böylece kritik iş süreçlerinin ve uygulamaların olduğu lokasyonlara ve lokasyonlardaki kullanıcılara alternatif güzergahlardan ağ bağlantısı sağlanması için altyapı tamamlanmış ve Şekil 26'da özet gösterimi yapılan bir topoloji elde edilmiştir.

4.2. Veri Bağı Katmanı Çözüm Yaklaşımları

Fiziksel katmanda yedekliliğin sağlanması adına uygulanan çözümlerin ağ üzerinde döngülere yol açmaması için belirli protokollerle desteklenmesi gerekmektedir. Ağ cihazları arasında birden fazla çekilen hatların sonlandıkları noktalara göre hangi amaçla çekildikleri anlaşılır. Bir cihazdan farklı bir cihaza doğru çekilmiş birden fazla kablo için Link Aggregation ve HP Port Trunking çözüm yaklaşımları yedeklilik ve yük paylaşımı anlamında aynı sonuçların elde edildiği yaklaşımlardır. Link Aggregation protokolünün HP Port Trunking protokolüne göre daha çok tercih edilmesinin sebebi Link Aggregation protokolünün standartlarla belirlenmiş bir yaklaşım olmasıdır. HP Port Trunking protokolü ise sadece HP cihazlara özgüdür ve sadece bu cihazlarda desteklenir. Bir cihazın ağ bağlantısı farklı cihazlara doğru çekilmiş olan kablolar üzerinden sağlandığı durumlarda Kapsayan Ağaç türevi protokolleri kullanılarak oluşması muhtemel döngü problemleri aşılır. PVST gibi Cisco cihazlara özgü protokollerin ya da SMP gibi HP cihazlara özgü protokollerin yerine uygulama alanına göre standartlarla belirlenmiş STP, RSTP ve MSTP türevlerinin kullanımı daha çok tercih edilir. Fazla sayıda VLAN'ların bulunduğu STP ve RSTP ile yapılandırılmış cihazlarda VLAN yapılandırmaları dikkate alınmaz. Bu gibi gereksinimlerin olduğu durumlarda problemlerin oluşmaması için MSTP kullanılmalıdır.

Bu bağlamda İSDEMİR'de uçtan uca aynı cihazlar arasındaki yedekli kablolar için cihazlar üzerinde Link Aggregation Protokolü yapılandırması yapılmış ve kabloların tek

bir kablo gibi davranması sağlanmıştır. Böylece hat yedekliliğinin yanı sıra kapasite artışı da elde edilmiştir. Yedeklilik bağlamında n-1 adet hat kaybına toleranslı bir sistem elde edilirken çekilen kablo sayısı ile tekil hat kapasitesi çarpımı kadar bir hat kapasitesi elde edilmiştir. Ayrıca kullanıcıların bu hatlar üzerine dağıtılması ile yük paylaşımı da sağlanmış olur. Link Aggregation Protokolü ile yaklaşık 30 adet cihazda ikili cihaz grupları arasında 98 adet trunklı hat yapılandırması yapılmıştır. Örneğin iki omurga arasında 10 Gbps'lik üç hat kullanılarak bir trunk oluşturulmuştur. Oluşturduğumuz trunk sayesinde kapasite artışı bağlamında 30 Gbps'lik bir hat, yedekliliğin sağlanması bağlamında iki adet kablonun aynı anda kopmasında dahi çalışabilecek bir hat, yük paylaşımı bağlamında ise trafiğin bu üç hat üzerinden sağlanan iletişim sayesinde bir hat üzerinde oluşması muhtemel trafik sıkışıklığına mahal vermeyen bir hat elde etmiş olduk. İş-kritik uygulamaların koştuğu lokasyonlarda cihaz yedekliliğinin sağlanması için toplam 55 adet ağ cihazı temin edilmiştir. Bir kısmı eşzamanlı çalışacak şekilde uygun protokollerle yapılandırılmış kullanılmakta, bir kısmı ise problem anında kullanılmak üzere yedek olarak stokta bekletilmektedir. Eşzamanlı çalışacak cihazlardan ağ bağlantısı en az iki alternatif noktadan olanlar üzerinde STP türevleri yapılandırılmasına gidilmiştir. Bu tip cihazlardan, kullanıcıların bağlı olduğu kenar anahtarların tamamı RSTP, omurga anahtarlar ise VLAN taşınmasına olanak sağlayan MSTP protokolleri ile yapılandırılmıştır. STP yapılandırmalarına örnek olarak omurgalar arasındaki MSTP yapılandırması gösterilmiştir.



Şekil 19. Omurgalar arası MSTP yapılandırması.

Toplam beş adet omurga cihazlardan ikisi aynı lokasyonda diğer üç tanesi diğer lokasyonlarda olacak şekilde kurulumları yapılmıştır. Omurgalar üzerinde yaptığımız yapılandırma sayesinde VLAN'ların dört farklı MSTI içerisinde gruplanıp, bu grupların alternatif yollar üzerinden haberleşmeleri sağlanmıştır.

Çizelge 45. Omurgalar arası MSTP yapılandırması için köprü bilgileri

Köprü Adı	MAC Adresi
BIM_OMURGA#1	00:17:08:ED:61:80
BIM_OMURGA#2	00:17:08:ED:55:80
SHH_OMURGA#1	00:13:21:52:BD:80
ELK_OMURGA#1	00:11:85:A1:FE:00
LMN_OMURGA#1	00:11:85:A2:B1:00

Çizelge 46. Omurgalar arası MSTP yapılandırması için port maliyet değerleri

Port Maliyetleri				
	1	2	3	4
BIM_OMURGA#1	10	20	50	100
BIM_OMURGA#2	10	30	50	100
SHH_OMURGA#1	20	30	40	70
ELK_OMURGA#1	50	50	40	-
LMN_OMURGA#1	100	100	70	-

Çizelge 47. Omurgalar arası MSTP yapılandırması için bölüm ve VLAN bilgileri

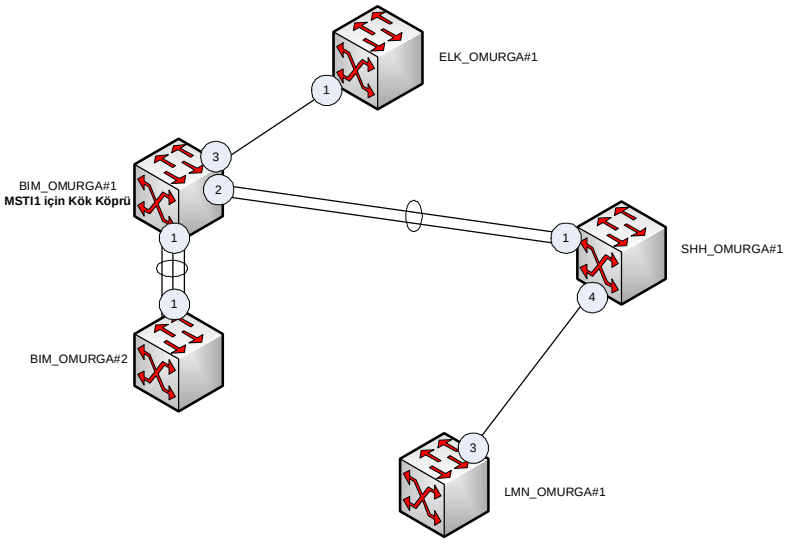
MSTI ID	VLAN ID
MSTI1	1, 2, 3 , …, 25
MSTI2	26, 27, 28, …, 40
MSTI3	41, 42, 43, …, 53
MSTI4	54, 56, 57, …, 62

MSTI1 bölümü içerisinde 25 adet, MSTI2 bölümü içerisinde 15 adet, MSTI3 bölümü içerisinde 13 adet, MSTI4 bölümü içerisinde 9 adet VLAN bulunmaktadır. Her bir bölüm için kök köprü seçiminde kullanılacak olan köprü öncelik değerleri aşağıdaki gibidir.

Çizelge 48. Omurgalar arası MSTP yapılandırması için köprü öncelik değerleri

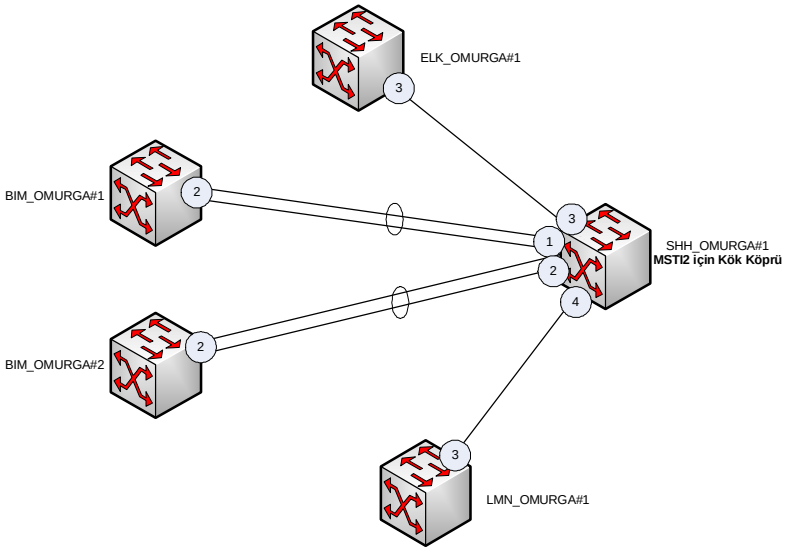
Köprü Öncelik Değerleri				
Köprü Adı	MSTI1	MSTI2	MST3	MST4
BIM_OMURGA#1	1	2	2	2
BIM_OMURGA#2	2	3	3	3
SHH_OMURGA#1	3	1	4	5
ELK_OMURGA#1	4	4	1	4
LMN_OMURGA#1	5	5	5	1

Yukarıdaki bilgilere göre MSTI1 bölümü için elde edilen en küçük kök köprü ID değeri BIM_OMURGA#1 anahtarına ait olan 10:00:00:17:08:ED:61:80 değeridir. Böylece kök köprüsü BIM_OMURGA#1 seçilen ve MSTI1'e atanmış VLAN'lar için aşağıdaki aktif ağ yolu elde edilmiştir.



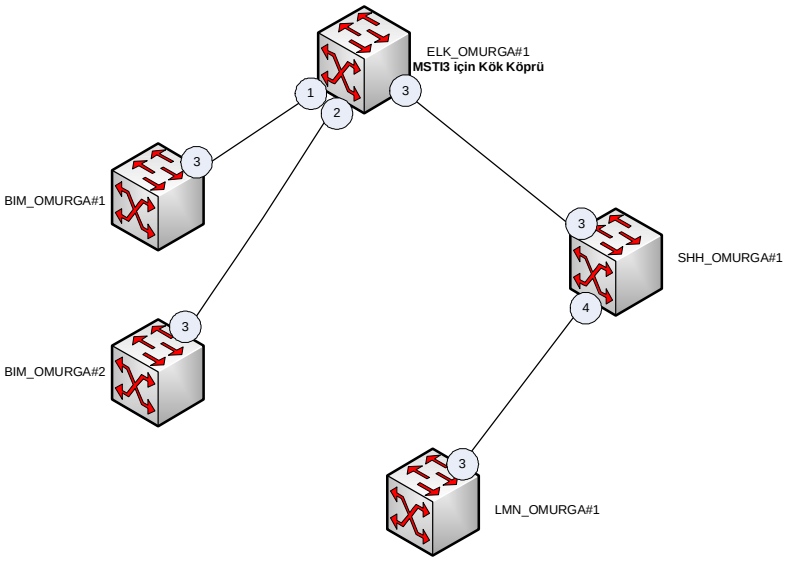
Şekil 20. Omurgalar arası MSTP yapılandırması MSTI1 bölümü için aktif ağ yolu.

MSTI2 bölümü için elde edilen en küçük kök köprü ID değeri SHH_OMURGA#1 anahtarına ait olan 10:00:00:13:21:52:BD:80 değeridir. Böylece kök köprüsü SHH_OMURGA#1 seçilen ve MSTI2'ye atanmış VLAN'lar için aşağıdaki aktif ağ yolu elde edilmiştir.



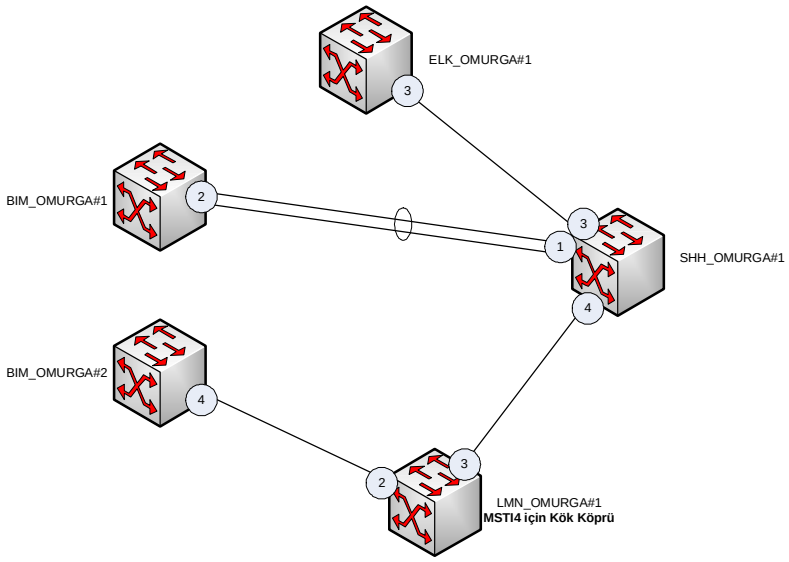
Şekil 21. Omurgalar arası MSTP yapılandırması MSTI2 bölümü için aktif ağ yolu.

MSTI3 bölümü için elde edilen en küçük kök köprü ID değeri ELK_OMURGA#1 anahtarına ait olan 10:00:00:11:85:A1:FE:00 değeridir. Böylece kök köprüsü ELK_OMURGA#1 seçilen ve MSTI3'ye atanmış VLAN'lar için aşağıdaki aktif ağ yolu elde edilmiştir.



Şekil 22. Omurgalar arası MSTP yapılandırması MSTI3 bölümü için aktif ağ yolu.

MSTI4 bölümü için elde edilen en küçük kök köprü ID değeri LMN_OMURGA#1 anahtarına ait olan 10:00:00:11:85:A2:B1:00 değeridir. Böylece kök köprüsü LMN_OMURGA#1 seçilen ve MSTI4'ye atanmış VLAN'lar için aşağıdaki aktif ağ yolu elde edilmiştir.



Şekil 23. Omurgalar arası MSTP yapılandırması MSTI4 bölümü için aktif ağ yolu.

Tüm anahtarlar üzerinde uygulanan STP yapılandırmaları ile döngülerden arındırılmış bir ağ elde edilmiştir.

4.3. Ağ Katmanı Çözüm Yaklaşımları

Ağ katmanı bağlamında yedeklilik, uygun protokoller yardımıyla aynı IP adresi ile birden fazla ağ geçidinin ifade edilmesidir. İSDEMİR'de her VLAN için tanımlı ağ geçitlerinin yedekliliği yönlendirici olarak çalışabilen omurga anahtarların ilgili protokoller yardımıyla yapılandırılmaları ile sağlanır. Bu protokollerden GLBP protokolünün diğer protokoller üzerinde yük dengelenmesi desteği ile gelmesi büyük avantaj sağlar ancak Cisco cihazların bile sadece belirli bir kısmında kullanılabiliyor olması bu avantajını kaybetmesine neden olur. Çalışma şekli neredeyse birbirinin aynısı olan HSRP ve VRRP protokollerinden HSRP Cisco özgü bir protokol olması ile VRRP'ye karşı tercih olarak geride kalır. Standartlarla belirlenmiş protokollerin kullanılması sistem genişlemelerinde üreticiye bağımlı çalışma zorunluluğunu ortadan kaldırdığından tercih edilmeleri doğaldır.

Bu bağlamda İSDEMİR'de omurga anahtarların üzerinde VRRP Protokolü kullanılmıştır. Yapılandırmada iki adet VRID grubu tanımlanmış ve altmıştan fazla VLAN bu gruplar arasında lokasyon bilgisi ve iş mantığı göz önünde bulundurularak paylaştırılmıştır. Böylece VLAN'lar için yönlendirici yedekliliği sağlanmıştır. Basitçe yapılandırmayı aşağıdaki gibi örnekleyebiliriz.

Çizelge 49. Omurgaların VRRP yapılandırması için VRID bilgileri

VRID	VLAN ID
VRID#1	1, 2, 3 , …, 40
VRID#2	41, 42, 43, …, 62

VRID#1 grubunda 40 adet VLAN, VRID#2 grubunda ise 22 adet VLAN olacak şekilde gruplara ayrılmıştır. Omurgalar üzerinde bu VLAN'lar için atanmış IP adresleri aşağıdaki tabloda gösterilmektedir.

Çizelge 50. Omurgaların VRRP yapılandırması için VLAN IP adresleri

Anahtarların VLAN IP Adresleri				
Anahtar Adı	VLAN#1	VLAN#2	VLAN#n	VLAN#62
BIM_OMURGA#1	10.150.1.1/24	10.150.2.1/24	10.150.n.1/24	10.150.62.1/24
BIM_OMURGA#2	10.150.1.2/24	10.150.2.2/24	10.150.n.2/24	10.150.62.2/24
SHH_OMURGA#1	10.150.1.3/24	10.150.2.3/24	10.150.n.3/24	10.150.62.3/24
ELK_OMURGA#1	-	-	-	-
LMN_OMURGA#1	-	-	-	-

VRID grupları içerisindeki her VLAN için belirlenmiş sanal yönlendirici IP adresleri yapılandırması aşağıdaki listede verilenlere göre yapılmıştır. VLAN'lar kendi ağ bloklarında olmayan ağlara bu iki VRID için tanımlanmış sanal IP adresleri üzerinden ulaşırlar.

Çizelge 51. Omurgaların VRRP yapılandırması için VLAN'lara göre sanal IP adresleri

VRID#1 Sanal IP Adresleri		VRID#2 Sanal IP Adresleri	
VLAN ID	Sanal IP Adres	VLAN ID	Sanal IP Adres
1	10.150.1.254/24	41	10.150.41.254/24
2	10.150.2.254/24	42	10.150.42.254/24
3	10.150.3.254/24	43	10.150.43.254/24
n	10.150.n.254/24	n	10.150.n.254/24
40	10.150.40.254/24	62	10.150.62.254/24

Her VRID grubunda omurga anahtarlar için belirlenmiş öncelik değerleri yapılandırması aşağıdaki listede verilenlere göre yapılmıştır. VRID#1 grubu için sırasıyla BIM_OMURGA#1, BIM_OMURGA#2 ve SHH_OMURGA#1 anahtarlarının asıl

yönlendirici olabilmeleri için uygun öncelik değerleri verilmiştir. Yine VRID#2 grubu için sırasıyla SHH_OMURGA#1, BIM_OMURGA#2 ve BIM_OMURGA#1 anahtarlarının asıl yönlendirici olabilmeleri için uygun öncelik değerleri verilmiştir.

Çizelge 52. Omurgaların VRRP yapılandırması için anahtar öncelik değerleri

Anahtar Öncelik Değerleri		
Anahtar Adı	VRID#1	VRID#2
BIM_OMURGA#1	100	1
BIM_OMURGA#2	2	2
SHH_OMURGA#1	1	100
ELK_OMURGA#1	-	-
LMN_OMURGA#1	-	-

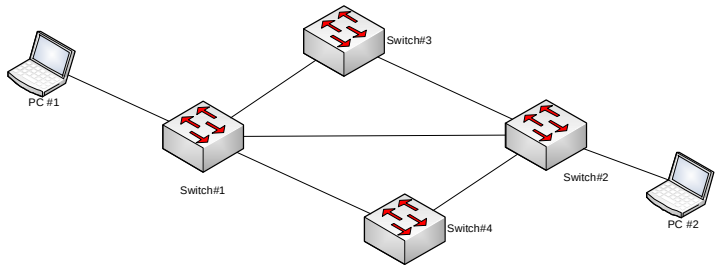
Bu bilgilere göre VRID#1 grubu için en yüksek öncelikli yönlendirici olan BIM_OMURGA#1 yönlendiricisinin bu grup için Asıl Yönlendirici olması sağlanmıştır. Grup içerisindeki diğer yönlendiriciler yedek olarak beklerler. Bu bağlamda VRID#1 grubuna atanmış bütün VLAN'lardaki kullanıcılar kendileri için tanımlanmış sanal yönlendirici IP adresi üzerinden diğer ağ bloklarına ulaşabilir duruma gelmiştir. VRID#1 grubundaki tüm VLAN trafiğinin VLAN'lar için atanmış sanal yönlendirici IP adreslerini üstlenen BIM_OMURGA#1 yönlendiricisi üzerinden iletilmesi sağlanmıştır. VRID#2 grubu için en yüksek öncelikli yönlendirici olan SHH_OMURGA#1 yönlendiricisinin bu grup için Asıl Yönlendirici olması sağlanmıştır. Grup içerisindeki diğer yönlendiriciler yedek olarak beklerler. Bu bağlamda VRID#2 grubuna atanmış bütün VLAN'lardaki kullanıcılar kendileri için tanımlanmış sanal yönlendirici IP'si üzerinden diğer ağ bloklarına ulaşabilir duruma gelmiştir. VRID#2 grubundaki tüm VLAN trafiğinin VLAN'lar için atanmış sanal yönlendirici IP adreslerini üstlenen SHH_OMURGA#1 yönlendiricisi üzerinden iletilmesi sağlanmıştır. Her VRID grubu için üç fiziki yönlendirici tanımlanması ile aynı anda iki omurganın erişilemez olma durumunda dahi yönlendirme problemlerinin yaşanmaması sağlanmıştır. Böylece yönlendirici kaynaklı oluşabilecek yönlendirme problemlerinden dolayı kritik iş süreçlerinin etkilenmesi ihtimali %66 oranında azaltılmıştır. Ayrıca VLAN'ların farklı gruplar içerisinde yer alması ve bu gruplardaki VLAN'lara ait trafiklerin farklı anahtarlar üzerinden yönlendirilmesi sayesinde yönlendiriciler üzerindeki yük paylaşımı sağlanmıştır.

Bütün bu önlemler ile oluşturulan yapı sonrası İSDEMİR ağı için performans verileri takip edilmiştir. Oggerino (2001), yaptığı çalışmada her cihaz için kullanılabilirlik oranını aşağıdaki formüller ile göstermiştir.

Cihaz Kullanılabilirlik Oranı = MTBF/(MTBF + MTTR) **(4.1)**

Önceki yıllarda en düşük kullanılabilirlik oranına sahip olan cihaz için 11385 saatlik MTBF ve 352 saatlik MTTR verileri (4.1) formülü ile hesaplanmış ve %97,0 olarak kayıtlara geçmişti. Yine aynı yöntemle iki aylık verilere göre en düşük cihaz kullanılabilirlik oranı 1640 saatlik MTBF ve 1 saat 18 dakikalık MTTR değeri ile (4.1) formülüne göre hesaplanmış ve %99,92 olarak gerçekleşmiştir.

Toplam ağ cihazı kullanılabilirliği hesaplanması için her cihazın arıza başına önceden hesaplanmış kullanılabilirlik oranlarının aritmetik ortalaması kullanılır. Ağ üzerinde referans alınan iki nokta arasındaki tüm cihazların birbirleri ile olan paralel ve seri bağlantıları göz önüne alınarak toplam ağ kullanılabilirlik oranı hesaplanır. Bu işlemi şöyle özetleyebiliriz. Seri bağlantılar için kullanılabilirlik oranları çarpılır. Paralel bağlantılar için ise seri bağlantılar için hesaplanmış kullanılabilirlik oranları 1'den çıkartılır. Yani devre dışı kalma oranları bulunur. Toplam ağ kullanılabilirliği paralel bağlantılar için hesaplanmış bu değerlerin 1'den çıkartılması ile elde edilir (Oggerino, 2001). Hesaplama aşağıda örneklenmiştir.

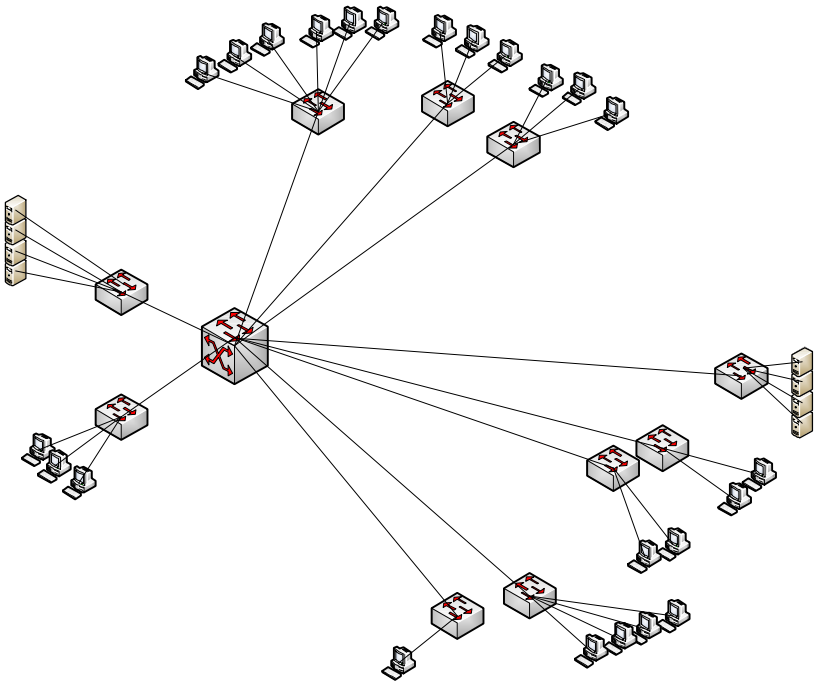


Şekil 24. Ağ kullanılabilirliği hesabı örneği topolojisi.

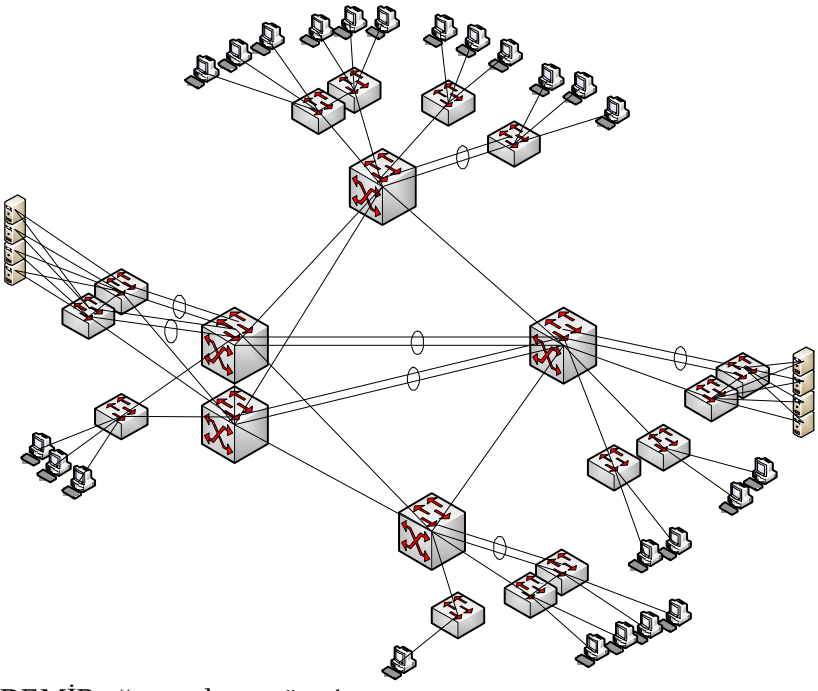
Cihaz kullanılabilirlik oranlarının sırası ile Switch#1 için %91, Switch#2 için %92, Switch#3 için %93, Switch#4 için %94 olduğunu kabul edildiğinde seri Switch#1-Switch#3-Switch#2 yolu için (0,91x0,93x0,92), seri Switch#1-Switch#2 yolu için (0,91x0,92), seri Switch#1-Switch#4-Switch#2 yolu için (0,91x0,94x0,92) değerlerinin paralel yol için kullanılması gereklidir. Bu durumda toplam ağ kullanılabilirliği 1-((1-0,91x0,93x0,92)x(1-0,91x0,92)x(1-0,91x0,94x0,92)) işleminin sonucu olan %99,232 olarak bulunur. Bu yöntemle hesaplanan geçen yıllardaki toplam ağ

kullanılabilirliği oranı %98 iken iki aylık verilere göre %99,994 olarak gerçekleşmiştir. Yani önceden yıllık toplam ağ sistemlerindeki kesintiler 175 saat iken yeni topoloji sonrasında bu değer iki aylık verilere göre 31 dakika olarak gerçekleşmiştir.

Yüzlerce anahtardan oluşan İSDEMİR ağının önceki ve sonraki hallerini özetle gösterir şekiller aşağıdadır.



Şekil 25. İSDEMİR ağı ilk durum özeti.



Şekil 26. İSDEMİR ağı son durum özeti.

BÖLÜM 5

SONUÇLAR VE ÖNERİLER

İSDEMİR için ağ yedekliliği ve kullanılabilirliğin arttırılması konusunda OSI Referans Modeli'nin ilgili katmanları için farklı çözümler belirlenmiştir. Fiziksel katman için cihaz ve kablo yedekliliği sağlanmış, Veri Bağı Katmanı için bir cihazdan aynı cihaza doğru çekilmiş olan yedekli kablolar Link Aggregation Protokolü, bir cihazdan farklı cihazlara doğru çekilmiş olan yedekli kablolar için RSTP ve MSTP yapılandırmaları yapılmış, Ağ Katmanı için VRRP protokolü ile yönlendirici yedekliliği sağlanmış, verimliliği ve kullanılabilirliği yüksek bir ağ oluşturulmasına karar verilmiştir.

Bu kapsamda iş-kritik uygulamaların koştuğu her lokasyona mevcuttaki 140 km'lik fiber-optik kabloların yedekliliğinin sağlanması için farklı güzergahlardan götürülen 80 km'den fazla fiber-optik kablo çekilmiştir. Sunucular ve bazı çok önem arz eden uç nokta cihazları için ise var olan yaklaşık 90 km'lik UTP kablo yedekliliğinin sağlanması adına 30 km kadar daha UTP kablo çekilmiştir. Kablolama İSDEMİR personelleri tarafından 3-4 ay gibi bir zaman diliminde yapılmış ve yaklaşık 4300 kadar fiber-optik, 600 kadar ise UTP uç sonlandırılmıştır. Uçtan uca aynı cihazlarda sonlanan yedekli kablolar için cihazlar Link Aggregation Protokolü ile yapılandırılarak tek bir kablo gibi çalışması sağlanmıştır. Yaklaşık 30 adet cihaz, ikili cihaz grupları arasında 98 adet trunklı hat kullanımı için Link Aggregation Protokolü kullanılarak yapılandırılmıştır. Bu sayede kapasite artışı ve hat yedekliliği sağlanmıştır. Link Aggregation Protokolü kullanılarak n adet kablo ile oluşturulan trunk sayesinde n-1 adet hat kaybına toleranslı bir hat elde edilmiştir. Ayrıca çekilen yedekli kablo sayısı ile tekil hat kapasitesi çarpımı kadar bir hat kapasitesi elde edilmiştir. Kritik iş süreçlerinin ve uygulamalarının koştuğu lokasyonlarda cihaz yedekliliği için toplam 55 adet ağ cihazı temin edilmiştir. Cihazlardan depoda pasif yedek olarak bekletilmek üzere temin edilen 5 adet cihaz haricindeki tüm cihazlar aktif yedeklilik sağlanması için sisteme dahil edilmiştir. Mesh topolojiyi andıran yeni mimaride ağa alternatif yollar üzerinden bağlantısı olan anahtarlardan, kullanıcıların bağlı olduğu kenar anahtarlar RSTP, omurga anahtarlar ise VLAN taşınmasına olanak sağlayan MSTP protokolleri ile yapılandırılmıştır. Her omurga kendi arkasındaki VLAN'ların yönetimini üstlenmesi için dört adet MST bölümü olacak şekilde yapılandırılmıştır. Böylece bilgi sistemlerine erişim için alternatif yollar üzerinden network bağlantısı sağlanırken yedekliliğin sağlanması amacıyla çekilen kabloların meydana getireceği döngülerden

arındırılmış bir ağ elde edilmiştir. Ayrıca dört farklı lokasyonda konuşlandırdığımız toplamda beş adet omurga anahtar ağ geçidi yedekliliğinin sağlanması ve yönlendirme trafiğinin dengelenmesi amacıyla VRRP ile yapılandırılmıştır. VRRP yapılandırmalarında iki adet VRID grubu tanımlanmış ve altmıştan fazla VLAN bu gruplar arasında lokasyon bilgisi ve iş mantığı göz önünde bulundurularak paylaştırılmıştır. Böylece VLAN'lar için yönlendirici yedekliliği sağlanmıştır. Her VRID grubu için üç fiziki yönlendirici tanımlanması ile aynı anda iki omurganın erişilemez olma durumunda dahi yönlendirme problemlerinin yaşanmaması sağlanmıştır. Böylece yönlendirici kaynaklı oluşabilecek yönlendirme problemlerinden dolayı kritik iş süreçlerinin etkilenmesi ihtimali %66 oranında azaltılmıştır. Ayrıca VLAN'ların farklı gruplar içerisinde yer alması ve bu gruplardaki VLAN'lara ait trafiklerin farklı anahtarlar üzerinden yönlendirilmesi sayesinde yönlendiriciler üzerindeki yük paylaşımı sağlanmıştır.

Bu yapının oluşturulmasından sonra kesintilerin kabul edilebilir sınırlar içerisinde kaldığından emin olmak için İSDEMİR ağı performans verileri düzenli olarak takip edilmiştir. Geçen yıllarda en düşük kullanılabilirliğe sahip cihaz için oran %97,0 iken cihaz kullanılabilirliği iki aylık takibe göre kullanılabilirlik oranı %99,92 olarak gerçekleşmiştir. Geçen yıllardaki toplam ağ kullanılabilirliği oranı %98 iken yine iki aylık verilere göre %99,994 olarak gerçekleşmiştir. Yani önceden yıllık toplam ağ sistemlerindeki kesintiler 175 saat iken yeni topoloji sonrasında bu değer iki aylık verilere göre 31 dakika olarak gerçekleşmiştir.

Yedekliliğin sağlanması için firma veya kuruluşun ihtiyaçlarına göre çözümler geliştirilmelidir. Çözümlerin uygulanmasında kullanılan cihazlar ve kablolar maliyetleri önemli ölçüde artırmaktadır. Uygulanan yöntemlerin getirileri sistem kurulumu maliyetlerinden fazla olmalıdır. Maliyetleri azaltmak için yedeklilik ihtiyaçlarının az olduğu durumlarda yukarıda verilen çözüm yaklaşımlarından birisi veya birkaçı kullanılmayabilir. Örneğin her lokasyon için kablo ve cihaz yedekliliğinin sağlanmasının maliyet açısından uygun olmadığı durumlarda sadece yönlendirici yedekliliği sağlanabilir. Böylece tüm yönlendirme trafiğini üstlenen tekil omurga anahtar yedeklenerek diğer alt ağlara ulaşım sağlanabilir.

KAYNAKLAR

Ahmadi M, Zamani A.A.M., 2009. A Hyper-cube Based Modified Spanning Tree Protocol for VLANs. *11th International Conference on Advanced Communication Technology.,* Phoenix Pk. 321-324.

Anonim, 2006. *Adaptive Edge Fundamentals Version 6.11 Student Guide.* Procurve Networking by HP, Module-4:2-77.

Arregoces M., Portolani M., 2004. *Data Center Fundamentals.* Cisco Press, Indianapolis. 1054 s.

Buregoni R.K., 2007. Handling Routed Traffic Over Ports Participating In Spanning Tree Protocol. *9th International Conference on Advanced Communication Technology: Toward Network Innovation Beyond Evolution.,* Phoenix Pk. 2001-2006.

Conlan P.J., 2009. *Cisco Network Professional's Advanced Internetworking Guide.* Wiley Publishing, Indianapolis. 857 s.

Hinden R., (Nisan 2004). *RFC 3768 – Virtual Router Redundancy Protocol (VRRP).*, 07 Kasım 2009, http://tools.ietf.org/html/rfc3768

Hucaby D., 2004. *CCNP BCMSN Exam Certification Guide.* Cisco Press, Indianapolis. 337-340.

Kakadia D., Halabi S., Cormier B., 2003. *Enterprise Network Desing: High Availibity.* Sun Blueprints Online, Santa Clara. 37 s.

Li T., Cole B., Morton P., Li D., (Mart 1998). *RFC 2281 – Cisco Hot Standby Router Protocol (HSRP).*, 08 Kasım 2009, http://tools.ietf.org/html/rfc2281

Mutlu A., 2007. İzmir Ekonomi Üniversitesi Kampüs Ağı Yenileme Sürecindeki Çalışmalar ve Dinamik VLAN Yapısına Geçiş. *Akademik Bilişim'07 - IX. Akademik Bilişim Konferansı.*, Kütahya. 6 s.

Oggerino C., 2001. Introduction to High Availability Networking. *High Availability Network Fundamentals.* Cisco Press, Indianapolis. 8-9.

Procurve Networking LAN Aggregation Through Switch Meshing White Paper. (b.t.). 29 Ekim 2009, http://www.hp.com/rnd/pdfs/Switch_Meshing_Paper_Tech_Brief.pdf

Santos D., de Souza A., Alvelos F., Dzida M., Pioro M., Zagozdzon M., 2009a. Traffic Engineering of Multiple Spanning Tree Routing Networks: The Load Balancing Case. *5th Conference on Next Generation Internet Networks.* Aveiro. 138-145.

Santos D., de Souza A., Alvelos F., 2009b. Traffic Engineering of Telecommunication Networks Based on Multiple Spanning Tree Routing. *1st International Workshop on Traffic Management and Traffic Engineering for the Future Internet.,* Porto. 114-129.

Watanabe T., Nakao M., Hiroyasu T., Otsuka T., Koibuchi M., 2008. Impact of Topology and Link Aggregation on a PC Cluster with Ethernet. *IEEE International Conference on Cluster Computing.,* Tsukuba. 280-285.

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı: Oğuz İslam EMLİK

Doğum Yeri: Kahramanmaraş

Doğum Tarihi: 01.06.1980

EĞİTİM DURUMU

Lisans Öğrenimi: Çanakkale Onsekiz Mart Üniversitesi, Mühendislik-Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü (1999-2003)

Yüksek Lisans Öğrenimi: Çanakkale Onsekiz Mart Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı (2003-…)

Bildiği Yabancı Diller: İngilizce

İŞ DENEYİMİ

İskenderun Demir ve Çelik A.Ş., İskenderun/Hatay, 07/2003 – 11/2007

İskenderun Demir ve Çelik A.Ş., İskenderun/Hatay, 06/2008 – …

İLETİŞİM

E-posta Adresi : oemlik@isdemir.com.tr