T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SANAL ÖZEL AĞ SERVİSLERİNDE YEDEKLİLİK TEKNİKLERİ VE UYGULAMALARI

Dilara ATBAN

YÜKSEK LİSANS TEZİ
Elektronik ve Haberleşme Mühendisliği Anabilim Dalı
Elektronik Programı

Danışman
Doç. Dr. Hacı İLHAN

Kasım, 2019

T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SANAL ÖZEL AĞ SERVİSLERİNDE YEDEKLİLİK TEKNİKLERİ VE UYGULAMALARI

Dilara ATBAN tarafından hazırlanan tez çalışması 06.11.2019 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Haberleşme Mühendisliği Anabilim Dalı Elektronik Programı **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Doç. Dr. Hacı İLHAN
Yıldız Teknik Üniversitesi
Danışman

Jüri Üyeleri

Doç. Dr. Hacı İLHAN, Danışman
Yıldız Teknik Üniversitesi _____

Doç.Dr. Tansal GÜÇLÜOĞLU, Üye
Yıldız Teknik Üniversitesi _____

Dr. Öğr.Üyesi Erdoğan AYDIN, Üye
İstanbul Medeniyet Üniversitesi _____

Danışmanım Doç. Dr. Hacı İLHAN sorumluluğunda tarafımca hazırlanan Sanal Özel Ağ Servislerinde Yedeklilik Teknikleri ve Uygulamaları başlıklı çalışmada veri toplama ve veri kullanımında gerekli yasal izinleri aldığımı, diğer kaynaklardan aldığım bilgileri ana metin ve referanslarda eksiksiz gösterdiğimi, araştırma verilerine ve sonuçlarına ilişkin çarpıtma ve/veya sahtecilik yapmadığımı, çalışmam süresince bilimsel araştırma ve etik ilkelerine uygun davrandığımı beyan ederim. Beyanımın aksinin ispatı halinde her türlü yasal sonucu kabul ederim.

Dilara ATBAN

Aileme

TEŞEKKÜR

Bu tezin gerçekleştirilmesi sırasında desteğini esirgemeyen sayın tez danışmanım Doç. Dr. Hacı İLHAN'a, tezimin her aşamasında bana destek olan eşime ve aileme, beni bu süreçte tezimi tamamlamam yönünde motive eden, yardımlarını ve desteklerini esirgemeyen arkadaşlarıma sonsuz teşekkür ederim .

Dilara ATBAN

İÇİNDEKİLER

SİMGE LİSTESİ

H	Hedef
K	Kaynak
Y	Yönlendirici

KISALTMA LİSTESİ

LAG	Link Aggregation Group
LDP	Label Distribution Point
LER	Label Edge Router
VPLS	Virtual Private LAN Services
MC-LAG	Multi-Chassis Link Aggregation Group
MPLS	Multi Protocol Label Switching
OSPF	Open Shortest Path First
P	Provider
PE	Provider Edge
RSVP	Resource Reservation Protocol
SDP	Service Distribution Point

ŞEKİL LİSTESİ

ÖZET

Sanal Özel Ağ Servislerinde Yedeklilik Teknikleri ve Uygulamaları

Dilara ATBAN

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı
Yüksek Lisans Tezi

Danışman: Doç. Dr. Hacı İLHAN

Sanal Özel LAN Hizmetleri (VPLS), yönetilen bir IP/MPLS ağı üzerinden tek bir köprülü alanda birden fazla sitenin baglantısını destekleyen bir VPN(Sanal özel Ağ-Virtual Private Network) sınıfıdır.VPLS(Sanal Özel Yerel Ağ Servisi-Virtual Private LAN Service), müşterilere bir ethernet arayüzü sunar.Servis saglayıcıları ve müşteriler için yerel ve geniş alan ağı sınırını basitleştirir. Bir VPLS'deki tüm servisler, konumlarına bakılmaksızın, aynı yerel ağda görülmektedir. VPLS teknolojisinde, VPN temelinde öğrenebilen, tünel kurabilen ve çoğaltabilen yönlendiriciler kullanılır. Bu yönlendiriciler, her birinden herhangi bir bağlantıya olanak sağlayan bir tünel ağı ile bağlanmıştır. Kesinti durumlarında servis devamlılığını sağlamak maliyet ve servis devamlılığı açısından oldukça önemli ve gereklidir. Bu tezde VPLS servisleri için yedeklilik yöntemleri test edilmiştir. Dahili geçit protokolü olarak OSPF (Açık ve Kısa Olan Öncelikli Yol-Open Shortest Path First), MPLS(Multi Protocol Label Switching-Çoklu protokol etiket anahtarlama) sinyallenmesi için ise LDP(Etiket dağıtım protokolü-Label Distrubiton Protocol) kullanılmıştır. Kullanılan yedeklilik sistemlerinde konfigurasyon örneklerinin gösterimi için Alcatel cihazları arayüzü tercih edilmiştir.

Anahtar Kelimeler VPLS, yedeklilik, ağ

YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ABSTRACT

Redundancy Techniques and Applications in Virtual Private Network Services

Dilara ATBAN

Department of Electronics and Telecommunication Engineering
Master of Science Thesis

Advisor: Assoc. Prof. Hacı İLHAN

Virtual Private LAN Services (VPLS) is a class of VPN (Virtual Private Network) that considers the connection of multiple sites in a bridged network through an IP/MPLS network.VPLS (Virtual Private LAN Service - Virtual Private LAN Service) provides service to customers by using ethernet.This simplifies the local and wide area network boundary for service providers. VPLS is fast and flexible since service bandwidth is not tied to the physical interface.All services in a VPLS seems to be on the same local network, regardless of their location. VPLS technology uses routers that can learn, tunnel and replicate VPN information.These routers are connected by a tunnel network that allows any connection from each. In case of interruption, service continuity is very important in terms of cost and service continuity. In this thesis, redundancy techniques are tested for the VPLS service.OSPF (Open and Short Priority Path-Open Shortest Path First) as an interior gateway protocol, LDP (Label management protocol-Label Distribution Protocol) for MPLS (Multiple Protocol Label Switching-Automatic protocol label switching) signaling are used.

Keywords: VPLS, redundancy, network

YILDIZ TECHNICAL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

1
Giriş

Ethernet, yerel alan ağı için baskın teknoloji haline gelmiştir ve özellikle metropolitan ve geniş alan ağlarında erişim teknolojisi olarak kabul görmektedir. Sanal özel yerel ağ teknolojisinin arkasındaki ana motivasyon coğrafi olarak servislerle bağlantı kurmaktır [1]. VPLS "Sanal Özel LAN Servisi" anlamına gelir. Iki uzak ağı tek bir köprülü bağlantıya bağlamak için kullanılan bir protokol olarak tanımlanır. Başka bir deyişle VPLS, bir VPN üzerinden bir LAN'a bağlanmayı sağlar.Böyle bir sistemin yararı, her biri yerel bir ağın güvenliğinden birbirleriyle iletişim kurabilen coğrafi olarak dağılmış bölgeleri birbirine bağlayabilmesidir. Bir VPLS'nin en iyi çözüm olabileceği durumlara bir örnek, bir kullanıcının saha dışındaki bir depoya veya veri merkezine güvenli bir şekilde bağlanması gerekmesi verilebilir. VPLS'nin temel avantajlarından bir diğeri sunulan güvenlik seviyeleridir. VPLS'nin katman 3 yönlendirme tablolarını servis sağlayıcı ile paylaşmaması, VPLS'nin genellikle yüksek hassasiyete sahip veriler için iyi bir çözüm olduğu anlamına gelir [2].Ancak, ethernet kullanarak her zaman aktif olması için servis devamlılığı gereksinimleri ortaya çıkmıştır. Bu sebeple VPLS üzerinde yedeklilik sistemleri gündeme gelmiştir.Tezimizde, VPLS servisinin çalışabilmesi için bazı yönlendirme protokolleri kullanılmaktadır.Yönlendirme protokolleri, yönlendirme tablosu oluşturup yönlendirilmesini sağlayan protokollerdir. Bu protokolleri iç (interior) ve dış (exterior) olarak sınıflandırabiliriz. İç protokoller genellikle büyük olmayan ağlar içinde kullanılır.Dış protokoller ise özellikle birbirinden bağımsız ve büyük ağlar arasında kullanılmaktadır [3]. Çalışmada yönlendirme protokolü olarak OSPF (Açık ve Kısa Olan Öncelikli Yol-Open Shortest Path First) seçildi.OSPF komşulukları kurulup çalışırlığı test edildi.Sonrasında MPLS ve VPLS servisleri kurulup çalışırlığı test edildi. Hazır hale gelen cihazlarda yedeklilik testleri gerçekleştirildi.Test kapsamında her bir çözüm için trafiği aktif halde taşıyan cihazın linklerinden biri kapatılarak, yedekteki cihazın trafiği üzerine alması test edildi.

1.1 Tezin Amacı

Günümüz gelişen teknolojisi ile internet erişimi zorunlu bir gereksinim haline gelmiştir.İnternet ortamını oluşturan donanımsal cihazların her elektronik cihaz gibi arızalanması kaçınılmazdır.Bu sebeple yedeklilik çözümleri gereksinimleri ortaya çıkmıştır. Günümüze kadar bu tezde bahsedileceği üzere bir çok yedeklilik çözümü sunulmuştur ve VPLS servisi için sunulan yedeklilik sistemlerinin testleri gerçekleştirilmiştir.Sonuç kısmında ise yedeklilik sistemlerinin test sonuçlarına göre uygulanabilirliği, performansı gibi parametreler açısından değerlendirmesini yapılmıştır.

1.2 Literatür Araştırması

LDP sinyallemeli VPLS teknolojisi RFC4762 (TCP/IP standartları) ile tanıtılmıştır [4]. Bu RFC'de Sanal Özel LAN Hizmeti (VPLS) çözümü açıklanmaktadır. Bir VPLS, belirli bir kullanıcı grubu için bir LAN segmenti oluşturur ve boylelikle tamamen MAC iletimi yapabilen bir katman 2 yayın alanı yaratır. Bu RFC'de sinyalleme protokolu olarak Etiket Dağıtım Protokolü(LDP) kullanılmıştır.

Bazı müşteriler ise internet yönlendirme protokolu olarak da bilinen BGP(Sınır Geçit Protokolü-Border Gateway Protocol) protokolünü kullanır. Bu gibi ortamlarda, LDP konfigurasyonu eklemek, istenmeyen ilave karmaşıklık olarak kabul edilir. Ayrıca bazı operatörler bir servise katılan yönlendiricileri keşfetmek için otomatik keşif mekanizmasını kullanmak istemektedir.Bu gibi durumlarda, BGP VPLS veya BGP-AD(Sınır geçit Protokolü-Otomatik Keşif-Border Gateway Protocol-Auto-Discovery) adı verilen bir çözüm kullanılabilir. Bu çözümün de sağlanabilmesi için BGP sinyallemeli VPLS RFC4761 ile tanıtılmıştır [5].BGP-VPLS, bir VPLS hizmetine katılan tüm yönlendiriciler için servis dağıtım noktalarının(SDP) otomatik olarak oluşturulmasına izin verir.Bu SDP'ler otomatik olarak oluşturulacak ve mevcut bir LDP aktarma tüneli kullanılacaktır. Taşıma tünellerini oluşturmak için LDP bağlantısını kullanmak istemeyenler için, BGP VPLS otomatik olarak bulunan köşe sağlayıcı yönlendiricisine varolan bir SDP seçecektir. BGP-VPLS sinyalli servis etiketi otomatik olarak bir SDP'ye bağlanacaktır. Bu, bir VPLS servisinin konfigürasyonunu büyük ölçüde kolaylaştırır. BGP ve LDP sinyallenen VPLS bir çok çalışma yapılmıştır ve bu teknoloji sürekli gelişme halindedir.

Zaman içinde MPLS VPN ve VPLS'nin durumunu izlemek için bir metodoloji önerilmektedir. Metodolojinin amacı, VPN bilgisini yaymak için yönlendiriciler tarafından gönderilen BGP sinyal mesajlarının toplanması, bu mesajların içeriğine dayalı olarak her VPN'nin görünürlük durumunun yeniden yapılandırılması ve bu

tür bilgilerin hemen anlaşılmasını kolaylaştıran görsel bir biçimde sunulması ve olası anomalileri tespit etmektir. Sağlanan yararlar ise:

- Yapılandırmalar gibi ağ olaylarının etkilerini ayrıntılı bir şekilde gözlemleme yeteneği ve cihaz arızaları,
- Bir ağ probleminin kaynağını bulmak için bu tür bilgileri ilişkilendirme imkanı,
- Bu değişikliklerin zamanında tespit edilmesi vardır.

Böyle bir metodolojinin, yönlendirme olaylarının analizini desteklemeye katkıda bulunabileceğini iddia edilmektedir. Benzer bir yaklaşımı benimseyen araçlar olmasına rağmen bu metodoloji, ağ olaylarının gözlenebilir etkilerinin ayrıntılı bir analizine dayanmaktadır. Dahası, zaman içinde ağ durumunun sezgisel bir grafik görünümünü sunmak üzere tasarlanmıştır [6].

"IP/MPLS Ağlar Üzerinde Sanal-Yerel Servisler ve Yönlendirici Konfigürasyonları." yayınında bu tezde de uygulandıgı üzere servis yönlendirici cihazları üzerinde VPLS konfigurasyonlarının gerçekleştirilmesi üzerine çalışılmıştır [7].

Güvenilir bir şekilde IPTV yayının VPLS ile sağlanması ele alınması hakkında da çalışmalar yapılmıştır. Dijital televizyon yayıncılığı için yönetilen minimum maliyetli ağaç yapısı önemli ölçüde çekirdek bant genişliği tasarrufu ve hızlı kanal erişimi sağlar. Esnek multimedya sağlamak için ağaç tabanlı VPLS (TVPLS) önerilmektedir. VPLS ağındaki hedef sağlayıcı kenar yönlendiricileri ayrık ağaçlara bağlanır, böylece servis sağlanabilmektedir. Arıza durumunda, hatalı ağaçtaki servisler değiştirilir [8].

Eski VPLS mimarilerinin tünel oluşturma mekanizmaları uygulamada statik, karmaşık ve esnek olmaması üzerine çözümler geliştirilmiştir. Güvenli VPLS mimarileri, sınırlı ölçeklenebilirlik, ağ kaynaklarının kullanımı, yüksek tünel tesislerinde gecikme ve yüksek işletme maliyeti gibi sınırlamalardan muzdariptir. Bu makalede, mevcut güvenli VPLS mimarilerinde tünel yönetimi sınırlamalarının üstesinden gelmek için yeni bir yazılım tanımlı ağ (SDN) tabanlı VPLS mimarisi önerilmektedir. Önerilen mimaride, yönlendiricilere akış kuralları kurmak için IPsec (IP Güvenliği-IP Security) protokolü ve tünel oluşturma fonksiyonlarını yönetmek için merkezi bir kontrolcü kullanılır. Gerçek zamanlı oturum özelliklerine dayanarak tünel süresini tahmin edebilecek yeni bir tünel yönetim mekanizması önerilir. Ayrıca, tünellerin oluşum süresinin gecikmesini azaltmak için yeni bir yeniden tünel başlatma mekanizması önerilmiştir. Önerilen mimarinin performansı bir simülasyon modeli ile test edilmiş ve uygulama kullanılarak analiz edilmiştir [9].

Mevcut hiyerarşik VPLS mimarileri, bir VPLS ağı için yeterli bir güvenlik seviyesi sağlayamamaktadır. Bu nedenle, hem VPLS güvenliği hem de ölçeklenebilirliği aynı anda sağlamak hala açık bir konudur. Bazı çalışmalarda hem güvenlik hem de ölçeklenebilirlik sınırlamalarının üstesinden gelmek için yeni bir hiyerarşik VPLS mimarisi önerilmektedir. Önerilen mimari, VPLS ağını oluşturmak üzere yönlendiriciler arasında hiyerarşik bir şekilde tüneller kurar. VPLS ağının operasyonlarını yönetmek için yeni bir sinyalleme tabanlı kontrol protokolü de önerilmiştir. Bu nedenle, önerilen mimari hiyerarşik sunucu kimlik kontrol protokolü (HIP) destekli sanal özel LAN Hizmeti (H-HIPLS) olarak adlandırılmaktadır [10].

HIP özellikli sanal özel LAN servisleri (HIPLS) ilk önerilen güvenli VPLS mimarisidir. Bununla birlikte, HIPLS mimarisinde kontrol, iletme ve güvenlik düzlemlerinde ölçeklenebilirlik eksikliği vardı. Daha sonra, hiyerarşik HIP özellikli sanal özel LAN Hizmeti (H-HIPLS) adlı HIP'e dayanan bir hiyerarşik VPLS mimarisi önerildi. Bu çalışmada, hem güvenlik hem de ölçeklenebilirlik sınırlamalarının üstesinden gelmek için HIP'e alternatif herhangi bir protokole dayanan daha verimli bir VPLS mimarisi olasılığı araştırılmıştır [11].

Gelişen teknoloji, internet kullanımın artması ile sürekli internet hizmeti sağlanması kritik seviyelere gelmiştir. Bu sebeple yine RFC4762'de belirtildiği üzere VPLS servisleri için yedeklilik sistemleri geliştirme gerekliliği ortaya çıkmıştır. Servis sağlayıcıların ağ yapılarına göre farklı yapıda yedeklilik sistemi gereksinimleri ortaya çıkmıştır [12].

1.3 Hipotez

Bu tezde, cihaz tiplerinin, topoloji büyüklüklerinin yedeklilik sistemlerindeki gecikme sürelerine etkileri test edilmiştir. Cihaz tiplerinin değiştirilmesinde gecikme sürelerine etki tespit edilmezken, STP çözümünde topoloji büyüklüğünün artmasının gecikme süresini arttırdığı tespit edilmiştir.

2
Genel Bilgi

2.1 Tezde Kullanılan Protokoller

2.1.1 Ethernet Çerçeve Formatı:

Bu çalışmada içerisinde paket/çerçeve yapısından bahsedileceği üzere genel çerçeve yapısı hakkındaki bilgiler aşağıdaki gibi verilebilir.

IEEE 802.3 ve Ethernet II olmak üzere iki adet Ethernet çerçeve formatı bulunmaktadır. Bu iki format genel olarak aynı olmak ile beraber tek farkları olarak Uzunluk/Tip (Lenght/Type) değişkenleri gösterilebilir [13].Çerçeve yapısındaki bileşenler aşağıdaki gibi verilebilir:

Başlangıç(Preamble): Bu bit dizisi alıcı ve vericinin senkronize olmasını sağlamaktadır.

Çerçeve Başlangıç Ayırıcı(Start Frame Delimeter (SFD)): 10101011 şeklindedir ve çerçevenin başladığı bilgisini vermektedir.

Hedef MAC(Destination MAC(DA)): Alınan datanın MAC adresidir.

Kaynak MAC(Source MAC(SA): Gönderilen datanın MAC adresidir.

Uzunluk/Tip(Lenght/Type): Bu değer 1536 Byte'tan büyükse bu değer Ethernet II olduğunu göstermektedir ve data uzunluğu demektir. 1536 Byte'tan küçük olduğunda ise 802.3'tür ve data tipini göstermektedir.

Paket Yükü(Payload): Bu değer data yükünü göstermektedir ve 46 ile 1500 byte arasında değişkenlik göstermektedir.

Çerçeve Kontrol Sırası(Frame Check Sequence (FCS)): Bu değer ile çerçevenin iletim sırasında bozulup bozulmadığı kontrol edilir. Alıcı tarafta hesaplanan FCS değeriyle datada olan FCS değeri eşleşmediği takdirde paket kabul edilmez.

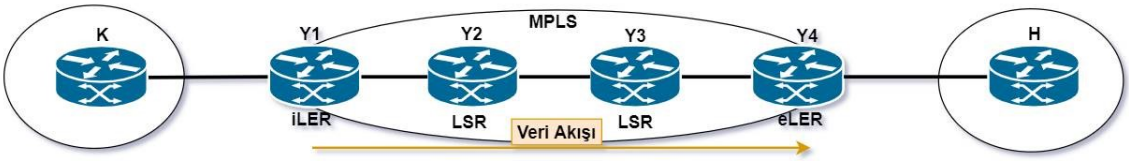
2.1.2 Açık ve Kısa Olan Öncelikli Yol

Açık ve Kısa Olan Öncelikli Yol (Open Shortest Path First, OSPF), RFC1247 ile tanıtılmış bir yönlendirme protokolüdür.OSPF bugün, en çok tercih edilen bağlantı durumu IP yönlendirme protokolüdür ve bu yerini de bir süre koruması muhtemeldir.Çalışma performansı iyi oldugu için kullanımı yaygındır ve yeni gereksinimlere uyum sağlamak için senelerce üzerine eklenmiş özelliklere sahiptir.OSPF'in temel işletimi, uzaklık vektörüne dayanan protokollerinin işletiminde farklıdır.Farklılıklardan biri, OSPF'nin nasıl ve ne zaman yönlendirme bilgisi gönderdiğine ilişkindir. Bir yönlendirici, ortak alt ağ üzerinden OSPF işletim sistemi kuran başka yönlendiricileri keşfetmeden, yönlendirme bilgisi gönderemez [14].Bu sistem için, bağlantı durumu protokolü yürüten her yönlendirici, uzaklık vektörlerine kıyasla, daha fazla bellek ve işlem çevrimi kullanmaktadır.Topoloji güncellemeleri her alt ağ, her yönlendirici ve hangi yönlendiricinin hangi alt ağlara bağlı bulunduğuna ilişkin detayları vermek için daha fazla miktarda paket gerekmektedir.Ancak OSPF tam güncellemeleri kısa aralıklarla yollamadığından, yönlendirme paketlerinin sayısı genellikle azdır.Ayrıca OSPF, uzaklık vektörü protokollerinden çok daha hızlı yakınsama sağlamaktadır ve hızlı yakınsama bir yönlendirme protokolünün en önemli özelliklerinden biridir [15].OSPF, metrik için bedel (cost) denen bir kavramdan yararlanmaktadır. Her bağlantının bir bedeli olduğu kabul edilmektedir ve her bağlantıya ait bedelin toplamıdır.OSPF'e ilişkin bazı nitelikler:

- Çok hızlı yakınsama olur, bir arıza fark ettiği andan itibaren, genellikle 10 saniyeden kısa bir süre içerisinde yakınsama gerçekleşir.
- Kısa süreli ve düzenli aralıklarla hello mesajlarını kullanır. Belirlenen sürelerde Hello mesajları alınıp verilemediyse, bir komşuya artık ulaşılamıyor demektir.
- Bağlantı durumu değiştiğinde kısa güncelleme, her 30 saniye de bir de tam güncelleme gönderilir.
- Metrik için bedel kullanılır.
- OSPF, bir ağın topolojisinin verilerini yaratan "kısa öncelikli yol" ve hat durumu protokolünü kullanan bir iç yönlendirme protokolüdür. OSPF'le birlikte yönlendiriciler her yönlendiricinin çalışma durumunu ve diğer yönlendircilerden yollanan trafik miktarını bilmektedirler.
- Ayrıca OSPF'te bölge yapısı bulunmaktadır.Üzerinde OSPF çalışan yönlendiriciler topolojinin tamamını görebilmektedir.

2.1.3 Çoklu Protokol Etiket Anahtarlama

Çoklu protokol etiket anahtarlama (Multi Protocol Label Switching, MPLS) yüksek performanslı ağlarda bir bilginin bir ağdan diğerine aktarılmasını sağlayan bir mekanizmadır. RFC3031 ile tanıtılmıştır. MPLS'nin amacı, etiket adı verilen özel bir başlık ekleyerek, müşteri paketlerini, sağlayıcı ağı üzerinden iletmek için bir tünel servisi oluşturmaktır. Etiket, sadece sağlayıcı ağına gelen paketlere eklenen ilave bir başlıktır. Bir MPLS ağında, yönlendiriciler etiket köşe yönlendirici (Label Edge Router(LER)) veya etiket anahtarlamalı yönlendirici (Label Switch Router(LSR)) olarak sınıflandırılır. LER'ler, etiket anahtarlamalı yollar olarak bilinen MPLS tünellerinin uç noktalarıdır ve ağın kenarında bulunmaktadır. Giriş LER (i-LER), tünel yolunun başlangıç noktası veya tünelin başlangıcıdır. Çıkış LER (e-LER), tünel yolunun bitiş noktası veya tünelin sonudur. LSP'ler (Etiket Anahtarlamalı Yollar), LDP (Etiket Dağıtım Protokolü) ve RSVP-TE (Trafik Mühendisliği uzantılarına sahip Kaynak Rezervasyon Protokolü) gibi MPLS sinyal protokolü kullanılarak kurulur. LSR'ler ağın merkezindedir ve LER'ler arasında bağlantı sağlar. MPLS özellikli yönlendiriciler (LER'ler ve LSR'ler), etiketleri ağa dağıtmak için bir sinyal protokolü kullanır. Bu etiketler IP adresi yerine, gelen trafik için yönlendirme kararını vermek için kullanılır [16].



Şekil 2.1 MPLS Topoloji Örneği

Müşteri Köşe Cihazları (CE): Müşterinin servis sağlayıcıya erişimini sağlayan cihazlardır. Bu cihazları VPN ve tünelleme protokollerinden habersizdir. Şekil 2.1'de Kaynak(K) ve hedef(H) olarak isimlendirilmiştir.

Provider Edge Cihazları (PE): Bu cihazların müşteri cihazlara ve çekirdek cihazlara en azından bir link olmak üzere bağlantısı vardır. BU cihazlar müşterinin VPN servislere ulaşımı için kullanılır. Şekil 2.1'de Yönlendirici1(Y1) ve Yonlencirici4(Y4) cihazları olarak gösterilmiştir.

Servis Sağlayıcı Cihazı (P): Bu cihazlar çekirdek ağda bulunur ve müşteri cihazlarına direkt olarak hiçbir bağlantısı yoktur. şekil 2.1'de Y2 ve Y3 olarak gösterilmiştir.

Etiket Köşe Cihazı(LER): LER cihazı MPLS ve müşteri cihazı arasındadır. PE cihazlara benzemektedir. LER cihazı

- MPLS networküne giriş cihazı (ILER) olabilir ve bu durumda müşteriden gelen

paketleri etiketleme işleminden sorumlu olur.

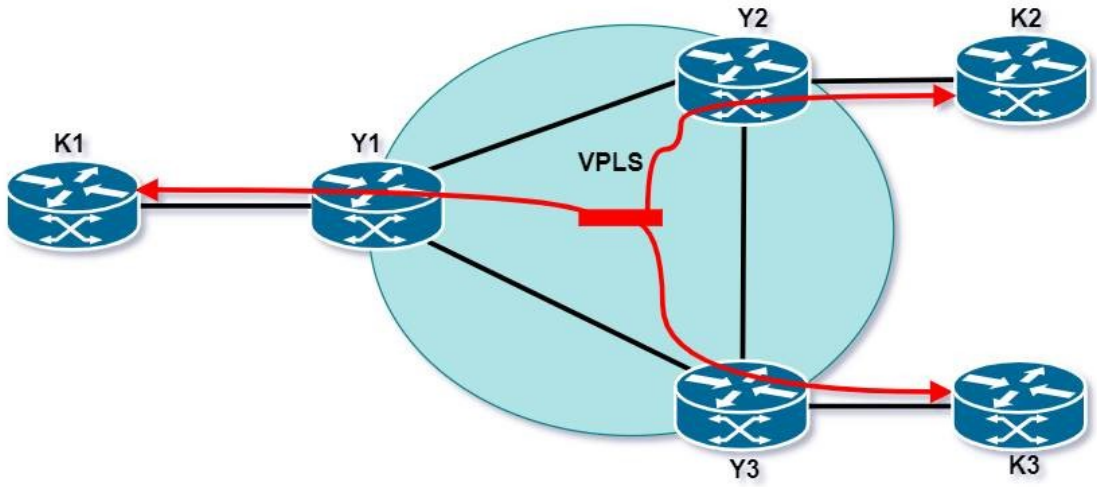
• MPLS networkünden çıkış cihazı (ELER) olduğunda ise etiketleri sökme ve bunları müşteriye iletme görevi olmaktadır.

• Etilet değişme cihazı (LSR) MPLS ağında yer almaktadır. ILER ve ELER cihazları ile doğrudan bağlantısı vardır. Bu cihaz gelen etiketli paketleri değiştirerek bir sonraki cihaza göndermektedir.

2.1.4 Sanal Özel LAN Servisleri

Sanal Özel LAN Servisleri (Virtual Private LAN Services, VPLS), RFC 4905'de tanımlanmıştır. Buna göre servis sağlayıcı tarafından yönetilen bir IP/MPLS ağı üzerinden birden fazla sitenin bağlanmasına izin veren bir sanal özel ağ hizmetidir. Bir VPLS örneğindeki müşteri siteleri, konumlarından bağımsız olarak aynı LAN'da görünür [17]. VPLS, her müşterinin kendi yönlendirme stratejilerini kontrol etmesini sağlar. VPLS hizmetindeki tüm müşteri yönlendiricileri, birçok ayrı noktadan noktaya bağlantıdan oluşturulan bir ağa kıyasla, aynı alt ağın bir parçasıdır. Bir VPLS servisi bir veya daha fazla servis yönlendiricileri üzerinde iki veya daha fazla servis erişim noktası arasında bağlantı sağlar. Bağlantı, müşteri sitelerine köprülenmiş bir etki alanı gibi görünmektedir. Böylece yönlendirme protokolleri de dahil olmak üzere protokoller VPLS hizmetine geçebilir. VPLS şeffaf, protokolden bağımsız bir hizmettir [18].

2.1.5 VPLS Etiket ve Paket Sistemi



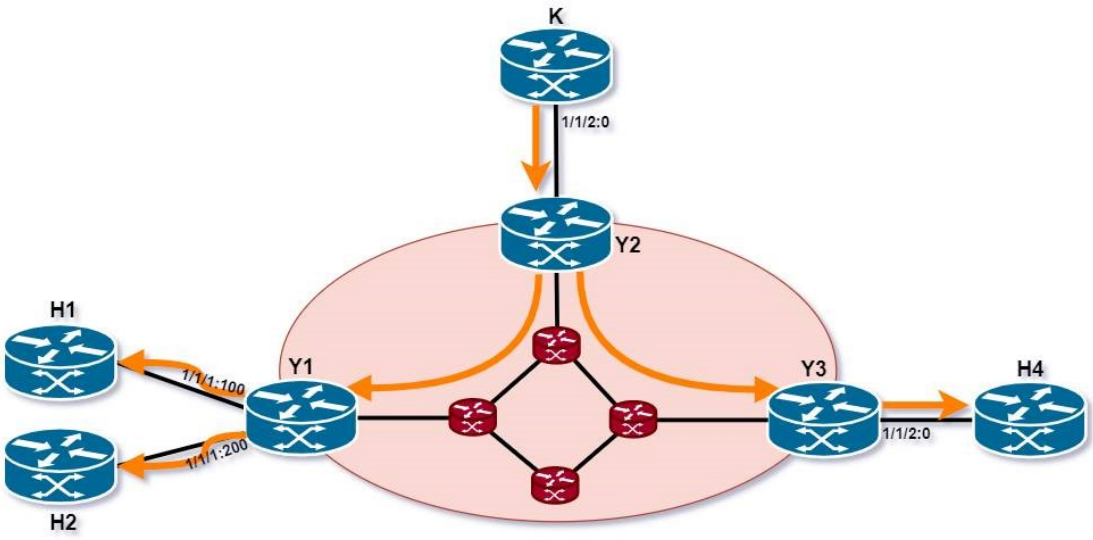
Şekil 2.2 VPLS Etiket Sistemi

Her yönlendirici hedef uca sistem IP adresini kullanrak hedefli bir LDP kurar. Hedef uca, her servise paket kullanırken kullanacagı kendi servis etiketini söyler. Şekil 2.2'de

etiket iletim sistemi için örnek topoloji gösterilmektedir.

Şekil 2.3'te VPLS paket ilerleme sistemi gösterilmektedir.

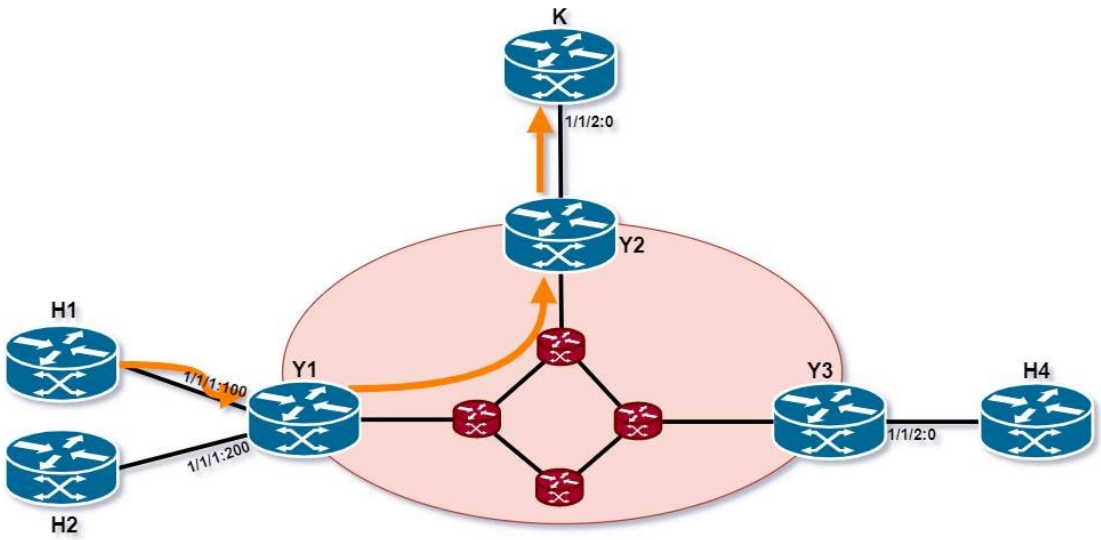
- Y2 cihazı, K3 cihazına port 1/1/2:0 ile ulaşıldıgını öğrenir.
- Y1 cihazı, Y2'den gelen VC etiketinden K3 cihazının Y2 cihazının arkasında oldugunu öğrenir.
- Y1 cihazı, H1 ve H2 cihazlarına 1/1/1:100 ve 1/1/1:200 portlarından paket gönderir.
- H1 paketleri kabul eder.
- K3 cihazı, K3 cihazının K2 cihazının arkasında oldugunu öğrenir.
- K3 cihazı 1/1/2:0 portundan paket gönderir.



Şekil 2.3 Kaynak3'ten Kaynak1'e VPLS Paket İlerleme Sistemi Örneği

Şekil 2.4'te ise;

- Y1 cihazı, K3 cihazına Y2 ile erişebileceğini bilmektedir.
- Y1 cihazı Y2 cihazına Y2'den gelen VC etiketi ile paket gönderir.
- Y2 cihazı K3 cihazına port 1/1/2:0 ile ulaşmaktadır.



Şekil 2.4 Kaynak1'den Kaynak3'e VPLS Paket İlerleme Sistemi Örneği

3
VPLS Yedeklilik Sistemleri ve Konfigürasyonu

3.1 Yönlendirme Protokolü-OSPF kurulumu

OSPF bir bağlantı yönlendirme protokolüdür. Bu nedenle, ağdaki her hedefe en kısa yolu bulmak için SPF(En Kısa Öncelikli Yol-Shortest Path First) algoritmasını kullanır. Bağlantı durumu yönlendirme protokolleri hızlı bir yakınsama süresine sahiptir. Bağlantı durumu yönlendirme protokollerinin ölçeklenebilirliği sınırlıdır. OSPF hiyerarşik alan konseptini destekler. Daha verimli adres yönetimi sağlamak için rota birleştirme de desteklenir. OSPF, güvenlik için kimlik doğrulamayı destekler. OSPF maliyet ölçümü, portun fiziksel bant genişliğine dayanmaktadır. Bu, OSPF'nin yol kararlarını en az atlama sayısından ziyade en fazla bant genişliğine sahip yola dayanarak vermesini sağlar.OSPF'ye trafik mühendisliği uzantıları, protokolün mevcut bant genişliğini, yönetim gruplarını, maksimum atlama sayısını vb. izlemesini ve sağlar. Bu özellik MPLS tarafından trafik tünelleri oluşturmak için kullanılır [19].

3.1.1 OSPF Konfigürasyonu

Örnek OSPF konfigürasyonu aynı alanda olmak üzere gerçekleştirilmiştir.

K1>config>router>ospf>area info

———————————————-

interface "system"
no shutdown
exit
interface "toR2"
interface-type point-to-point
no shutdown
exit
interface "toR3"
interface-type point-to-point
no shutdown

```
exit
interface "toR5"
interface-type point-to-point
no shutdown
exit
interface "toR6"
interface-type point-to-point
no shutdown
exit
```

Aşağıdaki şekilde komşuluk kurulması kontrol edilmiştir. Full durumunda olması komşulukların kuruldugu anlamına gelmektedir.

```
K1>show router ospf neighbor
===============================================
Rtr Base OSPFv2 Instance 0 Neighbors
===============================================
Interface-Name Rtr Id State Pri RetxQ TTL Area-Id
-----------------------------------------------
toR2 10.10.10.2 Full 1 0 36
0.0.0.0
toR3 10.10.10.3 Full 1 0 37
0.0.0.0
toR5 10.10.10.5 Full 1 0 37
0.0.0.0
toR6 10.10.10.6 Full 1 0 37
0.0.0.0
-----------------------------------------------
No. of Neighbors: 4
```

3.2 MPLS Kurulumu ve Konfigürasyonu

MPLS'nin amacı, etiket adı verilen özel bir başlık ekleyerek, müşteri paketlerini sağlayıcı ağı üzerinden iletmek için bir tünel servisi sağlamaktır. Etiket sadece sağlayıcı ağına gelen paketlere eklenen ilave bir başlıktır. Bir MPLS ağında, yönlendiriciler Label Edge LER veya LSR olarak sınıflandırılır. LER'ler, Etiket Anahtarlamalı Yollar (LSP'ler) olarak bilinen MPLS tünellerinin uç noktalarıdır ve ağın kenarındadır. Giriş

LER (iLER), tünelin başlangıç noktasıdır. Çıkış LER (eLER), tünelin son noktasıdır. LSP'ler (Etiket Anahtarlamalı Yollar), LDP (Etiket Dağıtım Protokolü) ve RSVP-TE (Trafik Mühendisliği uzantılarına sahip Kaynak Rezervasyon Protokolü) gibi MPLS sinyal protokolü kullanılarak kurulur. LSR'ler ağın merkezindedir ve LER'ler arasında bağlantı sağlar. MPLS özellikli yönlendiriciler (LER'ler ve LSR'ler), etiketleri ağa dağıtmak için bir sinyal protokolü kullanır. Bu etiketler IP adresi yerine, gelen trafik için yönlendirme kararını vermek için kullanılır [20].

3.2.1 MPLS Konfigürasyonu

Örnek MPLS konfigurasyonu LDP protokoluyle gerçekleştirilmiştir.

```
K1>config>router>ldp info
_____________________________
interface-parameters
interface "toR2" dual-stack
ipv4
no shutdown
exit
no shutdown
exit
interface "toR3" dual-stack
ipv4
no shutdown
exit
no shutdown
exit
no shutdown
```

LDP kurulumu aşağıdaki gibi kontrol edilmiştir.

```
K1>show router ldp session
=========================================
LDP IPv4 Sessions
=========================================
Peer LDP Id Adj Type State Msg Sent Msg Recv Up Time
_____________________________
10.10.10.2:0 Link Established 549105 549152 16d 23:30:58
10.10.10.3:0 Link Established 548642 549112 16d 23:30:02
```

No. of IPv4 Sessions: 2

==========

3.3 Servis Dağıtım Noktası

Bir servis dağıtım noktası (Service Distrubition Point, SDP), trafiği tek yönlü bir servis tüneli üzerinden bir yönlendiriciden diğerine yönlendirmek için bir yol görevi görür. SDP, paketleri bu cihazdaki servis erişim noktalarına(SAP) doğru hizmete yönlendiren uzak uçtaki cihazda sona erer. Dağıtılmış bir servis, yerel bir cihazda en az bir SAP, hedef cihazda bir SAP ve servisi servis tüneline bağlayan bir SDP'den oluşan bir konfigürasyondan oluşur. Bir SDP aşağıdaki özelliklere sahiptir:

- Bir SDP, katılan yönlendiricilere yerel olarak benzersizdir. Bir SDP, uzak uç yönlendiriciyi tanımlamak için cihazın IP adresini kullanır.
- Bir SDP oluşturulduktan sonra, servisler SDP'ye bağlanır. Bir SDP, kendisiyle ilişkili birden fazla servisi de taşıyabilir [21].
- Bir SDP ile eşlenen tüm servisler, SDP için tanımlanan aynı taşıma tipini kullanır.
- SDP yapılandırması ve içinde taşınan hizmetler bağımsız olsa da ilgili nesnelerdir. SDP'deki işlemler, SDP ile ilişkili tüm hizmetleri etkiler. Örneğin, bir SDP'nin operasyonel ve idari durumu, SDP'ye bağlı hizmetlerin durumunu kontrol eder. Her cihaz, hizmet vermek istediği her uzak yönlendirici için tanımlanmış bir SDP'ye sahip olmalıdır.

Bir SDP bir servise bağlı olduğunda, bir Spoke-SDP veya Mesh-SDP olarak bağlanır. SDP türü, trafiğin nasıl iletildiğini gösterir. Bir Spoke-SDP, konuşturan SDP'ye gelen trafiğin diğer tüm "portlarda" (diğer Spoke ve Mesh SDP'lerde veya SAP'lerde) çoğaltıldığı ve alındığı porta geri iletilmeyen geleneksel bir köprü "port" eşdeğeri gibi muamele görür [22].

3.3.1 SDP Konfigürasyonu

Örnek SDP konfigürasyonu aşağıdaki gibi yapılmıştır.

sdp 2 mpls create
far-end 10.10.10.2

ldp
keep-alive
shutdown
exit
no shutdown
exit
sdp 3 mpls create
far-end 10.10.10.3
ldp
keep-alive
shutdown
exit
sdp 4 mpls create
far-end 10.10.10.4
ldp
keep-alive
shutdown
exit
no shutdown
exit
sdp 5 mpls create
far-end 10.10.10.5
ldp
keep-alive
shutdown
exit

SDP çıktıları aşağıdaki gibi kontrol edilebilir.

show service sdp
==========
Services: Service Destination Points
==========
SdpId AdmMTU OprMTU Far End Adm Opr Del LSP Sig
———————————-
2 0 8914 10.10.10.2 Up Up MPLS L TLDP
3 0 8914 10.10.10.3 Up Up MPLS L TLDP
4 0 8914 10.10.10.4 Up Up MPLS L TLDP
5 0 8914 10.10.10.5 Up Up MPLS L TLDP

3.4 Yedeklilik Sistemleri

Tezimizde üzerinde durdugumuz yedeklilik sistemleri STP, LAG, MC-LAG, Aktif/Pasif sözde bağlantı çözümleridir.

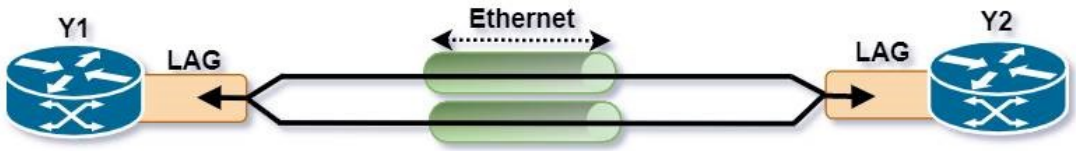
3.4.1 Kapsayan Ağaç Protokolü

Kapsayan Ağaç Protokolü (Spanning Tree Protocol,STP), aynı hedefe birden çok yol olsa bile, herhangi bir döngünün oluşmasını engelleyen bir ağ üzerinden tek bir yol oluşturan protokoldür.Servis erişim noktalarına bağlı ekipman ethernet paketlerini VPLS servisine iletir. Servise katılan yönlendirici, müşteri MAC adreslerinin nerede olduğunu, giriş servis erişim noktalarında veya giriş servis dağıtım noktalarında bulunduğunu öğrenir.Bilinmeyen varış yerleri ve diğer tüm serviş erişim noktalarına paket gönderir. Servis erişim noktaları yanlış yapılandırmayla birbirine bağlanırsa istenmeyen döngüler oluşabilir ve paketler ağda istenmeyen şekilde akmaya devam edebilir. Kapsayan Ağaç Protokolü (STP) uygulaması, bu döngüleri VPLS topolojisinden çıkarmak için tasarlanmıştır. VPLS'nin operasyonel özelliklerini daha etkili kılmak için bazı değişiklikler içermektedir. STP parametreleri, esneklik ve aşırı yakınsamaların hızı arasındaki dengeyi sağlar. Belirli parametreleri değiştirmek davranışı etkileyebilir.

Yönlendiricileri ağ boyunca birbirine bağlamak için servis tünelleri kullanılır. Yayılma Ağacı Protokolü'nü (STP) uygulaması, VPLS'nin operasyonel özelliklerini daha etkili hale getirmek için bazı geliştirmeler içermektedir. STP çalıştırılırken, SDP'ler yapılandırılamaz.Her VPLS ağına katılan yönlendiriciler için yönlendiricinin hangisinin hedefe en yakın olduğunu belirlenir ve bu yönlendirici VPLS ağının birincil yönlendiricisi olarak adlandırılır. Bunun bir sonucu olarak, birincil yönlendirici tüm ağ bağlantı noktalarına belirlenmiş bağlantı noktası rolü atanır ve bu nedenle iletme durumunda kalır. STP ağına katılan kalan yönlendiricilerin, servis dağıtım noktası portlarını ağ için harici bir yol yerine kök için daha düşük bir maliyet yolu olarak görmesini sağlar. Sonuç olarak, ağın içinden geçen yol herhangi bir alternatiften daha düşük maliyetli olarak görülmektedir ve yönlendirici, ağ portunu birincil port olarak atar. Bu yaklaşım, ağ bağlantı noktalarının her zaman iletim durumunda kalmasını sağlar. Bu iki özellik bir arada, ağ bağlantı noktalarının hiçbir zaman engellenmemesini ve STP örneklerini çalıştıran ağın dışındaki köprülerle birlikte çalışabilirliği sürdürmesini sağlar [23].

3.4.2 Birleşmiş Link Grubu

Birleşmiş link grubu (Link Aggregation Group,LAG), ethernet cihazları arasında çoklu fiziksel bağlantıların toplanmasına izin verir, böylece işlevsel olarak tek bir mantıksal bağlantıya eşdeğerdirler. Birden 64'e kadar portları tek linkmiş gibi birleştirir, bağlı 2 cihaz arasındaki bant genişliğini arttırır ve trafik akışının belirlenmesi için hashing algoritmasının çalışmasına olanak sağlar. Aynı kaynak/hedef MAC adres çifti arasında iletilen tüm karelerin, aynı fiziksel bağlantı boyunca iletilir. Paketteki bazı bağlantıların diğerlerinden daha fazla trafiğe sahip olmayabilir. Bu nedenle trafik tüm bağlantılarda tam olarak yük dengeli olmayabilir. Bir LAG, birden çok bağlantı noktasını bir mantıksal bağlantıda gruplayarak, iki yönlendirici arasındaki kullanılabilir bant genişliğini artırır. Birden fazla fiziksel bağlantının toplanması, yük paylaşımına izin verir ve kesintisiz yedeklilik sunar [24]. Bağlantılardan biri başarısız olursa, kalan bağlantılar üzerinden trafik 1 saniyeden kısa bir sürede yeniden dağıtılır. LAG, cihazlar arasında statik olarak yapılandırılabilir veya LACP kullanılarak dinamik olarak zorlanabilir. LACP, farklı üreticiler arasında bağlantı birleştirme uygulamak için standart bir yöntem sağlar. Statik yapılandırma, artan yönetim ek yükünün genişlemesiyle ağda daha fazla kontrol sağlar [25]. LAG kısaca bir ve birden fazla Ethernet portunun bağlandığı sanal bir port olarak tanımlanabilir. Bu bağlı portlar farklı hızlarda olabilir. LAG, ethernet porta göre daha dayanaklıdır. Ethernet port düşerse, ethernet portun bağlı olduğu servis de düşecektir. Ancak LAG içerisinde herhangi bir ethernet port ayakta durduğu takdirde servis de düşmeyecektir.



Şekil 3.1 LAG Örnek Gösterimi

A. LAG'ın avantajları LAG'ın avantajları yüksek band genişliği, maliyetten tasarruf, dayanıklılık/yedeklilik, endüstri standartlarına uyumluluk sayılabilir.

Yüksek Band Genişliği: LAG kısaca bir ve birden fazla ethernet portunun bağlandığı sanal bir port olarak tanımlanabilir. Örneğin 16 adet 100G port tanımlanabilir ve böylece 1.6T trafik sağlayabilmektedir. Günümüz teknolojisinde ethernet port ile bunu sağlamak mümkün değildir.

Maliyet: 2010 senesinde 100G port tanıtıldığında, fiyatı 10G portların 25 katıydı. Bu demek oluyor ki LAG altında 10 adet 10G port kullanmak 1 adet 100G port kullanmaktan daha tasarrufludur.

Dayanıklılık/Yedeklilik: Ethernet port düştüğünde, ona bağlı olan servis/protokol de düşmektedir. Ancak LAG içerisindeki herhangi bir port düştüğünde, LAG hala ayakta kalacak ve bağlı olduğu servis/protokolün trafik akışı devam edecektir.

Endüstri standartlarına uyumluluk: LAG 802.1ax standartında tanımlanmaktadır. Böylelikle tüm markalarla çalışmaya uyumludur.

B. LAG Konfigürasyon Örneği Örnek LAG konfigürasyon örneği aşağıdaki gibidir:

Y1>config>lag info
---
port 1/1/1
port 1/1/2
no shutdown

Y2>config>lag info
---
port 1/1/1
port 1/1/2
no shutdown

show lag 2 detail
LAG Details
==========
Description : N/A

Details

Lag-id : 2 Mode : network
Adm : up Opr : up
Thres. Exceeded Cnt : 2 Port Threshold : 0
Thres. Last Cleared : 10/23/2018 07:11:26 Threshold Action : down
Dynamic Cost : false Encap Type : null
Configured Address : 24:01:ff:00:01:42 Lag-IfIndex : 1342177282
Hardware Address : 24:01:ff:00:01:42
Hold-time Down : 0.0 sec Port Type : standard
Per-Link-Hash : disabled
Include-Egr-Hash-Cfg: disabled

Per FP Ing Queuing : disabled Per FP Egr Queuing : disabled
Per FP SAP Instance : disabled
LACP : disabled
Standby Signaling : lacp
Port weight speed : 0 gbps Number/Weight Up : 2
Weight Threshold : 0 Threshold Action : down
———————————————-
Port-id Adm Act/Stdby Opr Primary Sub-group Forced Prio
———————————————-
1/1/1 up active up yes 1 - 32768
1/1/2 up active up 1 - 32768

3.4.2.1 Link Birleşim Kontrol Protokolü

Link Birleşim Kontrol Protokolü (Link Aggregation Control Protocol,LACP), IEEE standartları tarafından belirlenmiş olan bir protokoldür. LACP, karşı uç ile bilgi alışverişini sağlamak için kullanılır. Bu bilgi, ethernet portların doğru yere bağlı olup olmadığı, düzgün konfigure edilip edilmediği, karşı ucun ayakta olup olmadığı hakkında detay verir. LACP aktif hale geldikten sonra LAG karşı uçta herhangi bir porttan sinyal kaybı yaşandığında farkedebilecektir. LACP olmadan LAG bunu fark edemeyecektir. LAG bant genişliğini artırır, hata oluştuğunda az bozulma sağlar ve kullanılabilirliği artırır. Tüm mevcut bağlantılarda yük dengeleme trafiğini kullanarak ağ fazlalığı sağlar. Bağlantılardan biri başarısız olursa, sistem kalan tüm bağlantılarda trafiği otomatik olarak dengeler [26]. Tipik bir LAG dağıtımı, bir erişim anahtarı ve bir dağıtım anahtarı veya müşteri kenarı cihazı arasındaki toplu ana hat bağlantılarını içerir [27]. LACP default, aktif ve pasif modda konfigure edilebilir.
Default: Port herhangi bir LACP mesajı göndermez ve almaz
Pasif: Port ancak LACP paketi aldığında cevap verir.
Aktif: Port LACP paketi gönderir ve alır.

3.4.2.2 LACP Konfigürasyonu

Örnek LACP konfigürasyonu aşağıdaki gibidir:
Y1>config>lag info
———————————————-
port 1/1/1
port 1/1/2
lacp active administrative-key 32768

no shutdown

Y1>config>lag show lag 2 detail
LAG Details
Description : N/A
———————————————————-
Details
———————————————————-
Lag-id : 2 Mode : network
Adm : up Opr : up
Thres. Exceeded Cnt : 2 Port Threshold : 0
Thres. Last Cleared : 10/23/2018 08:41:50 Threshold Action : down
Dynamic Cost : false Encap Type : null
Configured Address : 24:01:ff:00:01:00 Lag-IfIndex : 1342177282
Hardware Address : 24:01:ff:00:01:00
Hold-time Down : 0.0 sec Port Type : standard
Per-Link-Hash : disabled
Include-Egr-Hash-Cfg: disabled Forced : -
Per FP Ing Queuing : disabled Per FP Egr Queuing : disabled
Per FP SAP Instance : disabled
LACP : enabled Mode : active
LACP Transmit Intvl : fast LACP xmit stdby : enabled
Selection Criteria : highest-count Slave-to-partner : disabled
MUX control : coupled
Subgrp hold time : 0.0 sec Remaining time : 0.0 sec
Subgrp selected : 1 Subgrp candidate : -
Subgrp count : 1
System Id : 24:01:ff:00:00:00 System Priority : 32768
Admin Key : 32768 Oper Key : 32768
Prtr System Id : Prtr System Priority : 0
Prtr Oper Key : 0
Standby Signaling : lacp
Port weight speed : 0 gbps Number/Weight Up : 0
Weight Threshold : 0 Threshold Action : down
———————————————————
Port-id Adm Act/Stdby Opr Primary Sub-group Forced Prio
———————————————————-
1/1/1 up active up yes 1 - 32768

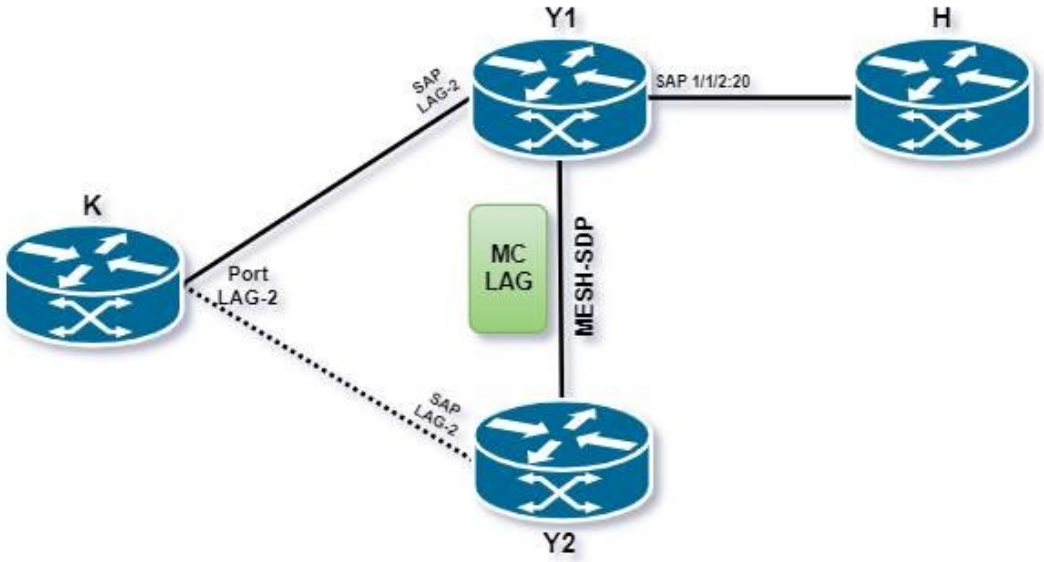
1/1/2 up active up 1 - 32768

Port-id Role Exp Def Dist Col Syn Aggr Timeout Activity

1/1/1 actor No Yes No No No Yes Yes Yes
1/1/1 partner Yes Yes No No No No Yes No
1/1/2 actor No Yes No No No Yes Yes Yes
1/1/2 partner Yes Yes No No No No Yes No

3.4.3 Çoklu Şasi LAG

LAG kullanmak sadece link yedekliliğini sağlamaktadır. Ancak yönlendirici düştüğünde, başka bir yedek yol olmayacaktır. Çoklu şasi LAG (Multi Chassis LAG, MC-LAG) çözümü ise müşteri cihazından 2 ayrı cihaza link açar. Böylece hem link hem cihaz yedekliliği sağlanmış olur. Müşteri cihazından bakıldığında tek bir LAG ve altında 2 adet alt grup LAG olarak görülür. Bu alt gruplardaki lagların hangisinin aktif olacağı LACP protokolü ile belirlenir. MC-LAG, sadece bağlantı yedekliliği sağlamakla kalmayıp aynı zamanda cihaz düzeyinde yedeklilik sağlamak için oluşturulmuş LAG özelliğinin bir uzantısıdır. Yedekli çift düğümler arasındaki bir mesajlaşma, LAG geçişini koordine etmeyi destekler.Çoklu şasi LAG, LAG geçiş koordinasyonunu destekler [28].



Şekil 3.2 MC-LAG Örnek Gösterimi

A. MC-LAG Kontrol Bağlantısı

MC-LAG bağlantısı 2 servis sağlayıcı yönlendirici arasında IP yolu ile olmaktadır. Bu

yol ile MC-LAG kontrol paketleri iletilmektedir. Böylece hangi tarafın aktif olup trafiğin nereden gideceğine karar verilir. Bu mesajlar LACPDU diye adlandırılır ve anahtar, sistem kimliği ve öncelik bilgilerini içerir. MC-LAG'da aktif olan taraf düştüğünde pasif olarak bekleyen taraf durumu fark eder ve aktiviteyi üzerine alır. 2 taraf da aktif olacak taraf konusunda hem fikir olmalıdır. Genellikle link sayısı fazla olan ya da öncelik değeri daha yüksek olan seçilir. Tüm değerler eşit ise de ilk önce ayağa kalkan aktiviteyi alır.

B. MC-LAG Konfigürasyonu

MC-LAG konfigürasyon örneği aşağıdaki gibidir:

- MC-LAG konfigüre edilirken, "peer" komutuyla iki taraf birbirine haber edilmelidir.
- LACP parametreleri iki tarafta da aynı olmalıdır.

Y1>config>lag info
———————————————-
mode access
port 1/1/1
lacp active administrative-key 32768
no shutdown

Y2>config>lag info
———————————————-
mode access
port 1/1/1
lacp active administrative-key 32768
no shutdown

Y1>config>redundancy info
———————————————-
multi-chassis
peer 10.10.10.2 create
no shutdown
mc-lag
lag 2 lacp-key 1234 system-id 00:00:aa:bb:cc:dd system-priority 1234

no shutdown
exit
exit
exit
———————————————-

Y2>config>redundancy info
———————————————-
multi-chassis
peer 10.10.10.1 create
no shutdown
mc-lag
lag 2 lacp-key 1234 system-id 00:00:aa:bb:cc:dd system-priority 1234
no shutdown
exit
exit
exit
———————————————-

show lag 2 detail
LAG Details
Description : N/A
———————————————-
Details
———————————————-
Lag-id : 2 Mode : access
———————————————-
MC Peer Address : 10.10.10.2 MC Peer Lag-id : 2
MC System Id : 00:00:aa:bb:cc:dd MC System Priority : 1234
MC Admin Key : 1234 MC Active/Standby : active
MC Lacp ID in use : false MC extended timeout : false MC Selection Logic : MC-lag feature admin up, selected local subgroup
MC Config Mismatch : no mismatch

———————————————————
Port-id Adm Act/Stdby Opr Primary Sub-group Forced Prio
———————————————————
1/1/1 up active up yes 1 - 32768

Port-id Role Exp Def Dist Col Syn Aggr Timeout Activity

1/1/1 actor No Yes No No No Yes Yes Yes

1/1/1 partner Yes Yes No No No No Yes No

==========

Y1>config>service>vpls info

---

stp

shutdown

exit

sap lag-2 create

exit

mesh-sdp 2:10 create

exit

no shutdown

Y2>config>service>vpls info

---

stp

shutdown

exit

sap lag-2 create

exit

mesh-sdp 2:10 create

exit

no shutdown

Çoklu şasi lag detayları aşağıdaki gibi kontrol edilebilir.

show redundancy multi-chassis mc-lag peer 10.10.10.2

==========

Multi-Chassis MC-Lag Peer 10.10.10.2

==========

Last State chg : 10/29/2018 04:11:35

Admin State : Up Oper State : Down

KeepAlive : 10 deci-seconds Hold On Ngbr Failure : 3

Lag Id Lacp Remote Source Oper System Id Sys Last State Changed Key Lag Id MacLSB MacLSB Prio

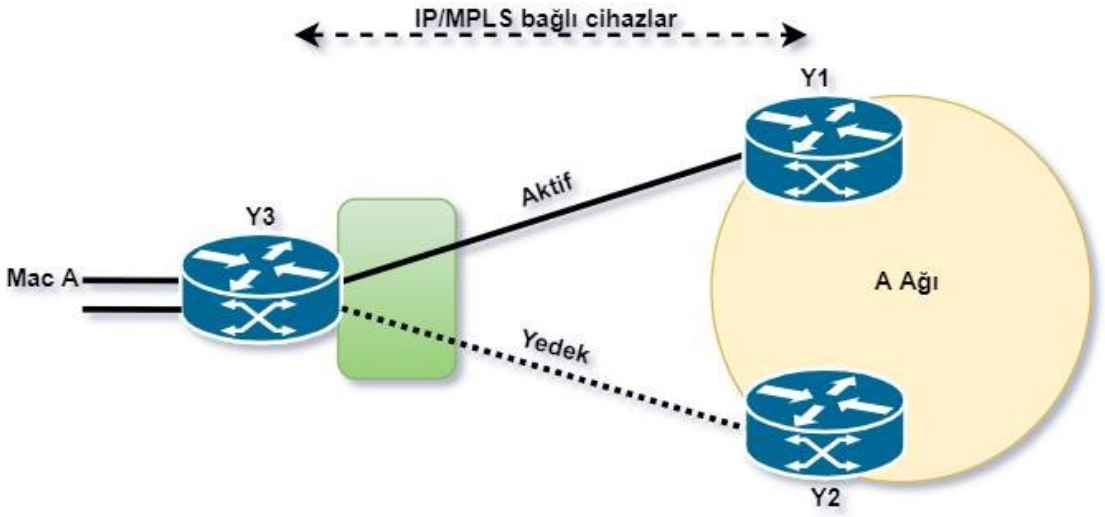
---

2 1234 2 Def n/a 00:00:aa:bb:cc:dd 1234 10/29/2018 03:48:42

Number of LAGs : 1

3.4.4 Aktif/Pasif Sözde Bağlantılar

Geniş VPLS networklerinde çok fazla hedefli-LDP kurulması gerekmektedir. Ayrıca fazlaca sayıda mesh-sdp kurulması da gerekmektedir. Ancak bu hem konfigürasyon fazlalılıgı hem de yönetimsel güçlüklere sebep olmaktadır. Buna çözüm olarak hiyerarşik VPLS çözümü sunulmuştur Bu çözümde spoke-sdpler kullanılmıştır ve tüm cihazlar arası hedefli-LDP kurulmasına gerek yoktur.



Şekil 3.3 Aktif/Pasif Sözde Bağlantı Örneği

Şekil 3.3'de görüldüğü gibi bir birden fazla servis sağlayıcı cihaza birden fazla SDP ile bağlanabilir. Bu servis sağlayıcı cihazlar kendi metro ağlarında full mesh olarak birbirlerine bağlıdırlar. Spoke-SDP'ler ile bağlantı trafikte istenmeyen bir döngüye sebebiyet verme potansiyeli vardır. Bunu önlemek için aktif/pasif sözde bağlantı (Active/Passive Pseudo-wires) çözümü önerilmiştir. Burada Y3 ile gösterilen

yönlendiriciye bağlı spoke-sdplerden biri aktif olarak seçilir ve trafik ordan akar [29].

Şekil 3.3'de Y3 cihazına gelen trafiği sadece aktif bağlantıya yönlenirir. Diğer bağlantılara göndermeyeceği için potansiyel istenmeyen döngü ihtimali ortadan kalkar [30]. Her SDP bir üstünlük değerine sahip olacaktır. Bu değer 0-4 arasında değişmektedir. Elle konfigure edilmediği takdirde 4 değerini alacaktır. Hangi SDP'nin aktif olacağı seçimi de aşağıdaki gibi yapılmaktadır:

- İlk önce SDP'nin ayakta olması gerekir. Eğer birden fazla SDP ayakta ise;
- En düşük öncelik değerindeki SDP seçilecektir. Eğer hepsi eşitse;
- En düşük SDP numaralı olan spoke-sdp seçilecektir .

3.4.4.1 Aktif/Pasif Sözde Bağlantı Konfigürasyonu

Bu örnek uygulamada "endpoint" adı altındaki son nokta VPLS altında oluşturulmuştur.

Y3>config>service>vpls info
————————————————————-
endpoint "endpoint" create
exit
send-flush-on-failure
stp
shutdown
exit
no shutdown
spoke-sdp 2:1 endpoint "endpoint" create
precedence primary
exit

Y1>config>service>vpls info
————————————————————-
spoke-sdp 6:1 create
exit

Y1>config>service>vpls info
————————————————————-

spoke-sdp 6:1 create
exit

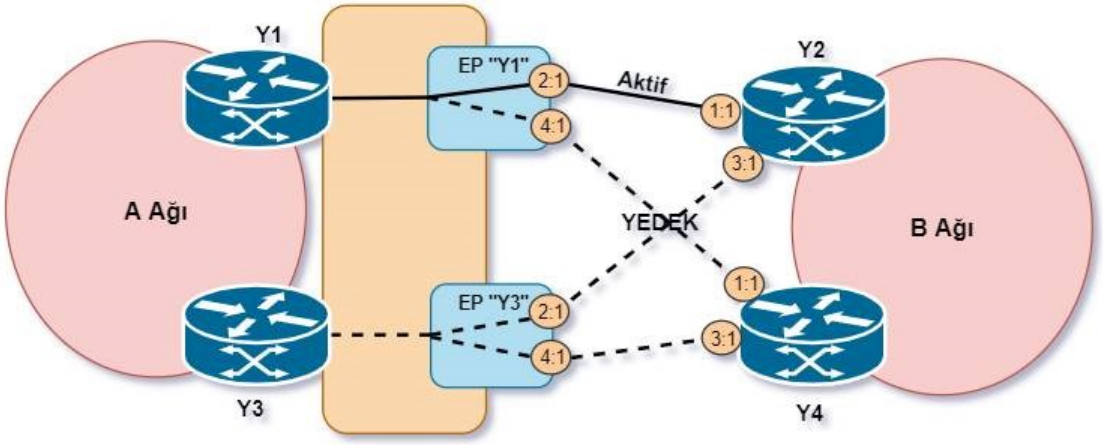
"show service id <service id> endpoint "endpoint"" komutuyla görüntülenebilir.

show service id 2 endpoint "endpoint"

```
===============================================
Service 2 endpoints
===============================================
Endpoint name : endpoint
Description : (Not Specified)
Creation Origin : manual
Revert time : 20
Act Hold Delay : 0
Ignore Standby Signaling : true
Suppress Standby Signaling : true
Block On Mesh Fail : false
Tx Active : none
Tx Active Up Time : 0d 00:00:00
Revert Time Count Down : N/A
Tx Active Change Count : 0
Last Tx Active Change : 10/24/2018 23:45:21
-------------------------------------------
Members
-------------------------------------------
Spoke-sdp : 2:1 precedence :0
Spoke-sdp : 4:1 precedence :4
```

3.4.5 Çoklu Şasi Sözde Bağlantısı

- Çoklu şasi sözde bağlantı (Multi-Chassis Pseudowire) hem yol hem de cihaz yedekliliği sağlamaktadır.
- Çoklu şasinin cihazları hangi bağlantının aktif olacağına karar verir.
- Bu çözüm hiyerarşik VPLS için maksimum yedekliliği sağlamak içindir.



Şekil 3.4 Çoklu Şasi Sözde Bağlantı Örnek Gösterimi

3.4.5.1 Çoklu Şasi Sözde Bağlantı Konfigürasyonu

Örnek çoklu şasi sözde bağlantı konfigürasyonu aşağıdaki gibidir:

```
Y1>config>redundancy>multi-chassis info
----------------------------------------------
peer 10.10.10.3 create
mc-endpoint
no shutdown
exit
no shutdown
exit

Y3>config>redundancy>multi-chassis info
----------------------------------------------
peer 10.10.10.1 create
mc-endpoint
no shutdown
exit
no shutdown
exit

Y1>config>service>vpls info
----------------------------------------------
endpoint "mc-ep" create
```

ignore-standby-signaling
mc-endpoint 1 create
mc-ep peer “PE3”
exit
exit
send-flush-on-failure
stp
shutdown
exit
no shutdown
spoke-sdp 2:1 endpoing “mc-ep” create
spoke-sdp 4:1 endpoing “mc-ep” create
exit

Y1>config>service>vpls info
———————————————-
endpoint "mc-ep" create
ignore-standby-signaling
mc-endpoint 1 create
mc-ep peer “PE1”
exit
exit
send-flush-on-failure
stp
shutdown
exit
no shutdown
spoke-sdp 2:1 endpoing “mc-ep” create
spoke-sdp 4:1 endpoing “mc-ep” create
exit

4
Sonuç ve Öneriler

Bu çalışmada yedeklilik sistemleri belirli parametreler üzerinden karşılaştırılmıştır. Yapılan testleri aşağıdaki gibi sıralayabiliriz:

- MC-LAG ve Aktif Pasif sözde bağlantı testlerinin gerçekleştirilmesi ve iki çözümün birbiriyle performans, kullanım alanı gibi parametreler baz alınarak karşılaştırılması,
- MC-LAG, Aktif pasif sözde bağlantının kullanılan cihaz kapasitesine göre hızlarının karşılaştırılması
- Topolojide cihaz sayısının arttırılmasının STP ve MC-LAG çözümlerindeki hızlara etkisi

4.1 MC-LAG ve Aktif Pasif Sözde Bağlantı Çözümlerinin Karşılaştırılması

Bu kısımda MC-LAG ve aktif pasif sözde bağlantı çözümlerinin performans, kullanım alanı karşılaştırılmaları yapılmıştır.

4.1.1 MC-LAG Test Sonuçları

İlk olarak MC-LAG çözümü üzerinde yedeklilik testi gerçekleştirilmiştir. Bu teste göre Y2 cihazındaki LAG 2 operasyonel olarak kapatılmış ve trafiğin Y1 cihazına yönelmesi incelenmiştir.

A. Multi-Chassis LAG Çözümünün Avantajları

- RSTP gerekliliği yoktur.
- Müşteri cihazları çoklu şasiden habersizdir.

- Sadece LAG/LACP konfigürasyonu varmış gibi görür.
- LACP uzun zamandan beri kullanılan ve iyi anlaşılmış bir protokoldür.
- Müşteri tarafında MPLS gibi bir tünelleme zorunluluğu yoktur.

B. MC-LAG Çözümünün Diğer Çözümlere Göre Avantajları

Müşteri tarafında görülmezdir: MC-LAG konfigürasyonu sadece servis sağlayıcı tarafında yapılmaktadır. O yüzden müşteri tarafı bu konfigürasyondan haberdar değildir.

Müşteri tarafında MPLS gerekliliği yoktur: MC-LAG müşteriye ethernet portu ile bağlıdır. Bu müşteri tarafında herhangi bir cihaz olabilir bu sebeple de müşteri açısından daha düşük maliyetle uygulanabilecek bir çözümdür.

4.1.2 Aktif Pasif Sözde Bağlantı Testi

Çoklu Şasi iletişim kesintisinde olduğu gibi çoklu şasi iletişiminde bir hata varsa da her iki yönlendirici de eşinin kapalı olduğunu varsayacak ve tek şasi moduna geri dönecektir. Çözümlerden biri, iki çekirdek yönlendirici senkronize etmek ve pasif modda yapılandırmaktır. Pasif modda, her iki eş aktif bir SDP uzak uçtan sinyal verildiği sürece pasif olarak kalacaktır. Birden fazla SDP konuşan aktif hale gelirse, en iyi SDP'yi seçilecetir. Diğer tüm konuşulan SDP'ler yerel olarak bloke edilir. Uzak yönlendiricilere hiçbir sinyal gönderilmez. Bir eş pasif modda yapılandırılmışsa, diğer eş pasif moda zorlanacaktır.

4.1.3 Aktif Pasif Sözde Bağlantı ve Çoklu Şasi LAG Çözümlerinin Birbiriyle Karşılaştırılması

- Performans açısından iki çözümde de yedeklilik sistemi <1sn sürede devreye girmiştir.
- Aktif pasif sizde bağlantı çözümünde konfigurasyon açısından MPLS ağı olması yeterlidir. Çoklu şasi LAG çözümünde ise her iki cihazın da aynı model/marka olması gerekmektedir.
- Kullanım alanı açısından aktif spasif sözde bağlantı MPLS ağına yedeklilik sağlarken, çoklu şasi lag müşteri tarafına yedeklilik sağlamaktadır.

- Aktif pasis sözde bağlantı çözümünde servis bazlı yedeklilik sağlanıp, yedeklilik mekanizması spesifikleştirilebilir. Çoklu şasi LAG çözümünde ise; yedeklilik o LAG'ı kullanan tüm servisler için sağlanacaktır.

4.2 MC-LAG, Aktif-Pasif Sözde Bağlantılarınınn Cihaz Tiplerine Göre Karşılaştırılması

Bu test ile piyasada bulunan birkaç markanın kullanım alanlarına göre cihaz tiplerinin yedeklilik sistemleri üzerindeki hızlara etkisi test edilmiştir. Ping testleri MC-LAG, Aktif-Pasif Sözde Bağlantı yedeklilik senaryoları için;

- Her cihaz tipinde grafiklerde gösterilen paket boyutlarına göre testler koşulmuştur.
- Bu testler her paket boyutu için 25 defa tekrarlanmış ve ortalama değeri alınmıştır.

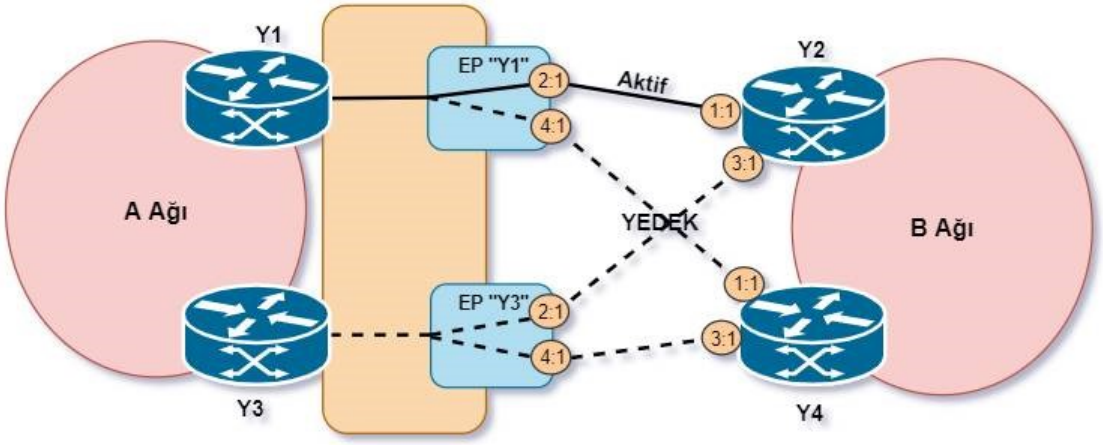
Cihaz tiplerini aşağıdaki özelliklerine göre sınıflandırabiliriz:

Servis Sağlayıcı Yönlendiri (P Router):
Bu cihazlar IP/MPLS agının çekirdek tarafında bulunurlar. Yaklaşık olarak kart başına 10Gbps trafik desteklemektedirler.

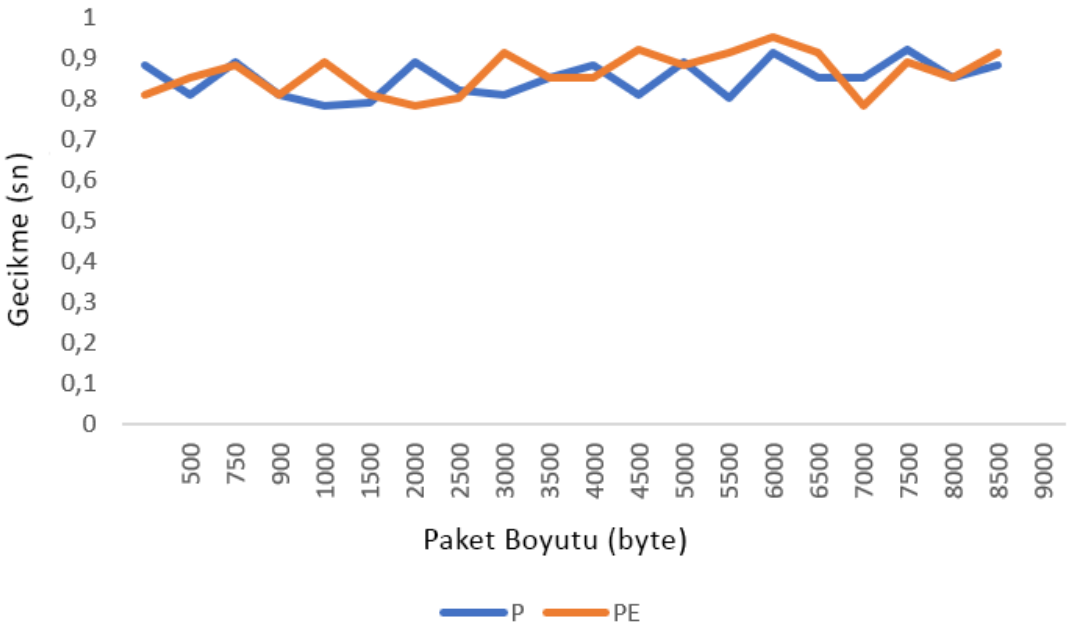
Köşe Servis Sağlayıcı (PE Router):
Bu cihazlar genellikle IP/MPLS ağının müşteri ağına sınır cihazlar olarak kullanılmaktadır. Bu testte kullanılan kartlar 100Gbps'a kadar trafik desteklemektedir.

Şekil 4.2, aktif pasif sözde bağlantı çözümünün P ve PE cihazlarında test sonuçlarının grafiklendirilmesini göstermektedir. Buna göre cihaza giden bağlantı kesildiğinde trafiğin yedek cihaza geçiş süresi ping komutu ile ölçülmüştür. Test iki cihaz tipi için de grafikte belirtilen her paket boyutu için 25 defa tekrarlanmıştır ve bu değerin ortalaması alınmıştır. Bunun sonucunda gecen sürenin 0.7-1.0 saniye aralıgında oldugu tespit edilmiştir. Ortalamasını aldıgımızda ise P cihazı için 0,89 saniye, PE cihazı için ise 0,91 saniye gecikme tespit edilmiş olmaktadır. Bu sonuç da bize cihaz kapasitelerinin yedeklilik geçisi sonucuna etkisinin olmadıgını göstermiştir. Test adımlarını özetlemek gerekirse;

- Şekil 4.1'de gördüğümüz üzere A ağındandan, B ağına uzun süreli ping testi



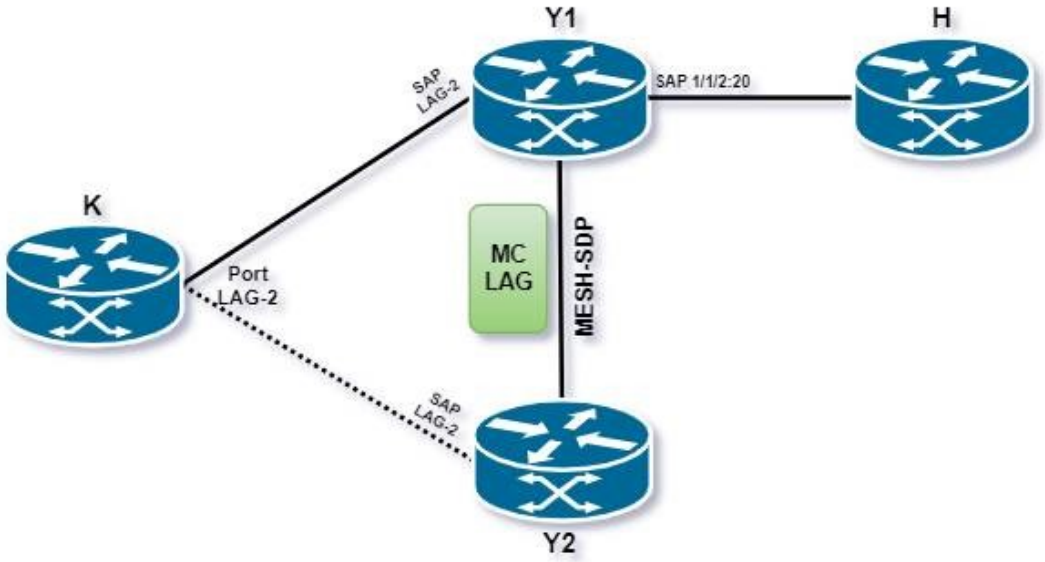
Şekil 4.1 Çoklu Şasi Sözde Bağlantı Örnek Gösterimi



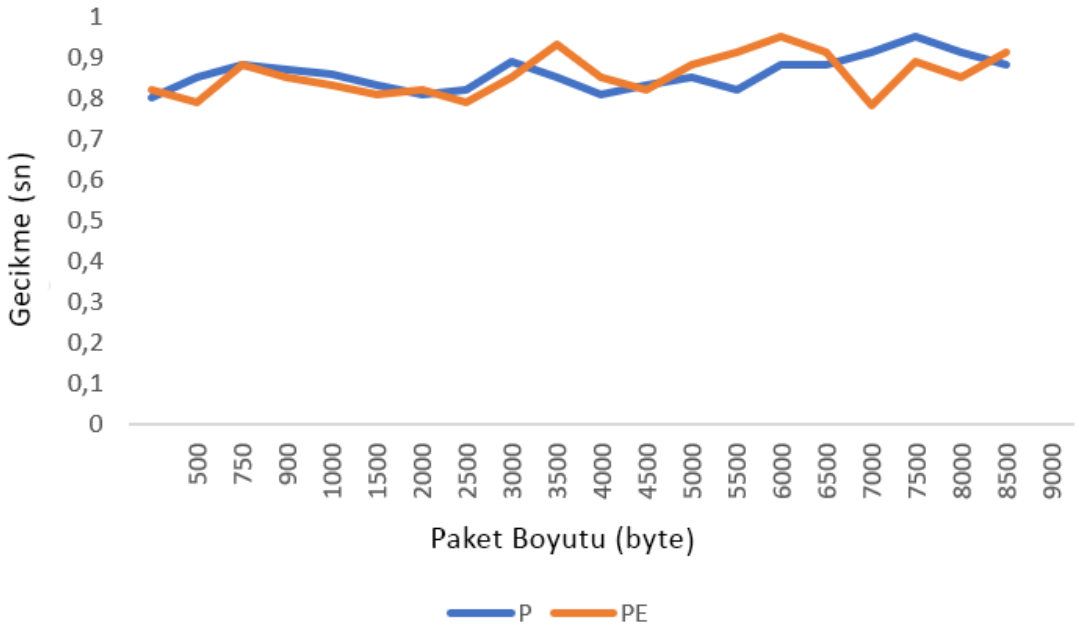
Şekil 4.2 Cihazlara Göre Aktif-Pasif Sözde Bağlantı Test Sonuçları

uygulanmıştır.

- Ping testi devam ederken Y1 ve Y2 arasında olan aktif bağlantının kesildiğinde, hazırda bekleyen yollardan birine geçisi sırasında oluşan zaman kaybı ölçülmüştür.
- Bu test grafikte belirtilen paket boyutları için 25 defa tekrarlanmıştır.



Şekil 4.3 MC-LAG Örnek gösterimi



Şekil 4.4 Cihazlara Göre MC-LAG Test Sonuçları

Şekil 4.3, çoklu şasi LAG çözümünün P ve PE cihazlarında test sonuçlarının grafiklendirilmesini göstermektedir. Buna göre cihaza giden bağlantı kesildiğinde

trafiğin yedek cihaza geçiş süresi ping komutu ile ölçülmüştür. Test iki cihaz tipi için de 25 defa tekrarlanmıştır.

- Kaynak(K) cihazından Hedef(H) cihazına ping testi başlatılmıştır.
- Her iki cihaz tipi içinde şekil 4.3'de gösterilmiş olan K1 ve Y2 arasındaki aktif bağlantı kesilmiştir.
- Aktivitenin K ve Y1 arasındaki bağlantıya geçtiği gözlemlenmiştir.
- Bu süreçte olan gecikme hesaplanmıştır.
- Bu test şekil 4.4 gösterilen her paket boyutu için 25 defa tekrarlanmış ve her sonucun ortalaması alınmıştır.

Bunun sonucunda gecen sürenin 0.7-1.0 saniye aralıgında oldugu tespit edilmiştir. P cihazlarında ortalama süre 0,81 saniye iken PE cihazlarında bu süre 0,86 s olarak hesaplanmıştır. Bu sonuç da bize iki çözümde de cihaz kapasitelerinin yedeklilik geçisi sonucuna etkisinin olmadıgını göstermiştir.

4.2.1 Ağ Büyüklüğünün STP ve MC-LAG Çözümlerine Etkisi

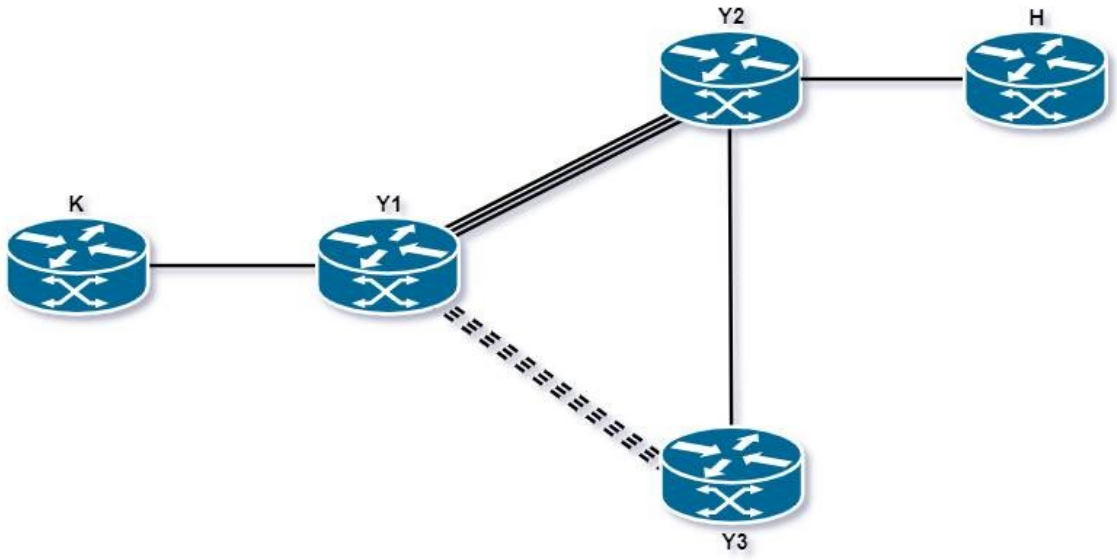
Gerçekleştirilen bu test senaryosunda ağ genişliğinin arttırılmasının STP ve çoklu şasi LAG çözümlerine etkisi ölçülmüştür. Bir önceki senaryoda oldugu üzere şekil 4.8'de gösterilen grafikteki paket boyutları için 25 defa tekrar edilerek ortalama sonuçlar grafiklendirilmiştir. kıyaslanmıştır.

A. Çoklu Şasi LAG Testi

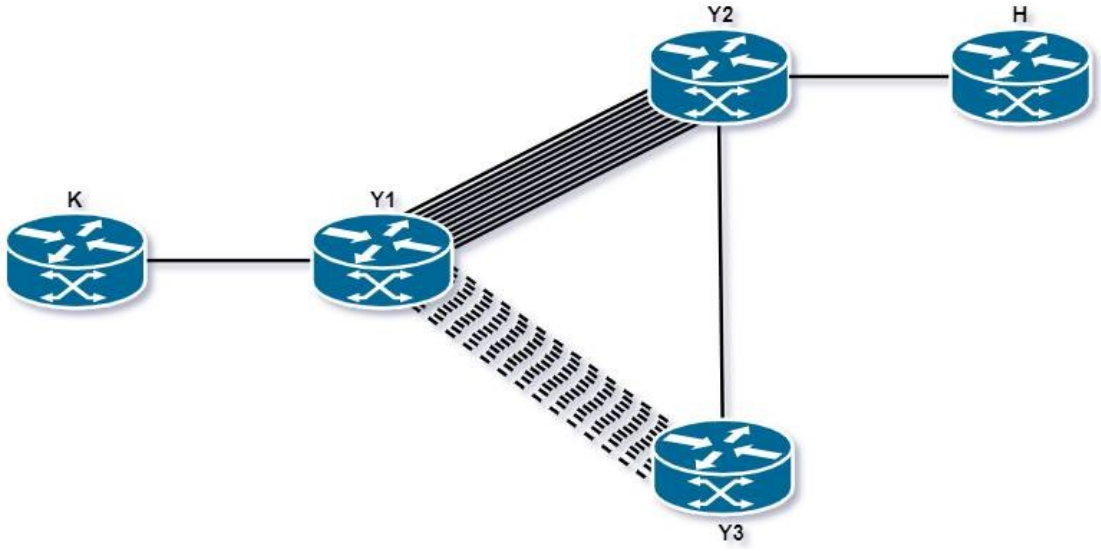
Şekil 4.5 çoklu şasi LAG çözümünün 3 link kullanılarak tasarlanmasını göstermektedir. Şekil 4.6'te ise 10 adet link kullanılarak oluşan topolojiyi göstermektedir.

Şekil 4.7 test sonuçlarımızı göstermektedir. MC-LAG çözümünde link sayısının arttırılması bize yine de stabil bir sonuç vermiştir. 3 ve 10 link sahibi 2 topolojide de değişim 0,7-1,0s aralıgında ortalama ise 0,8s olmuş ve iki topolojide de birbiriyle tutarlı sonuçlar vermiştir. Test adımları ise:

- K cihazından H cihazına ping testi başlatılmıştır.
- Her iki topolojide de şekil 4.5 ve şekil 4.6'da gösterilmiş olan Y1 ve Y2 arasındaki aktif bağlantı kesilmiştir.
- Aktivitenin Y1 ve Y2 arasındaki bağlantıya geçtiği gözlemlenmiştir.

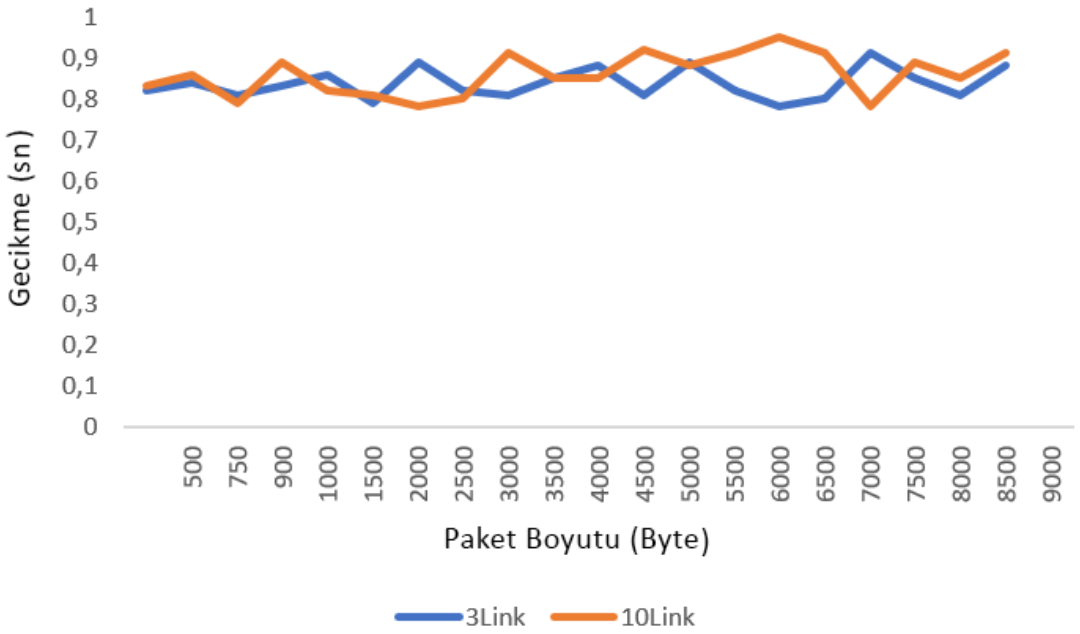


Şekil 4.5 3 Adet Link Kullanılarak Oluşturulan MC-LAG Topolojisi



Şekil 4.6 10 Adet Link Kullanılarak Oluşturulan MC-LAG Topolojisi

- Bu süreçte olan gecikme hesaplanmıştır.
- Bu test şekil 4.7'de gösterilen her paket boyutu için 25 defa tekrarlanmış ve her sonucun ortalaması alınmıştır.

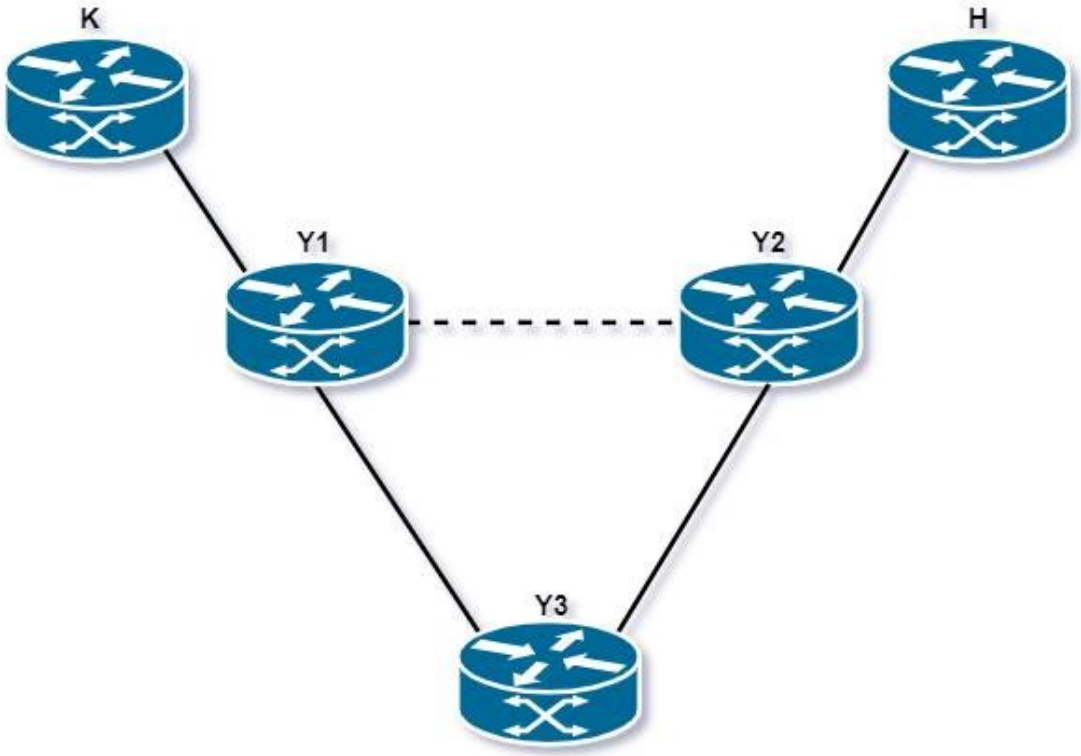


Şekil 4.7 Link Sayılarına Göre Test Sonuç Grafiği

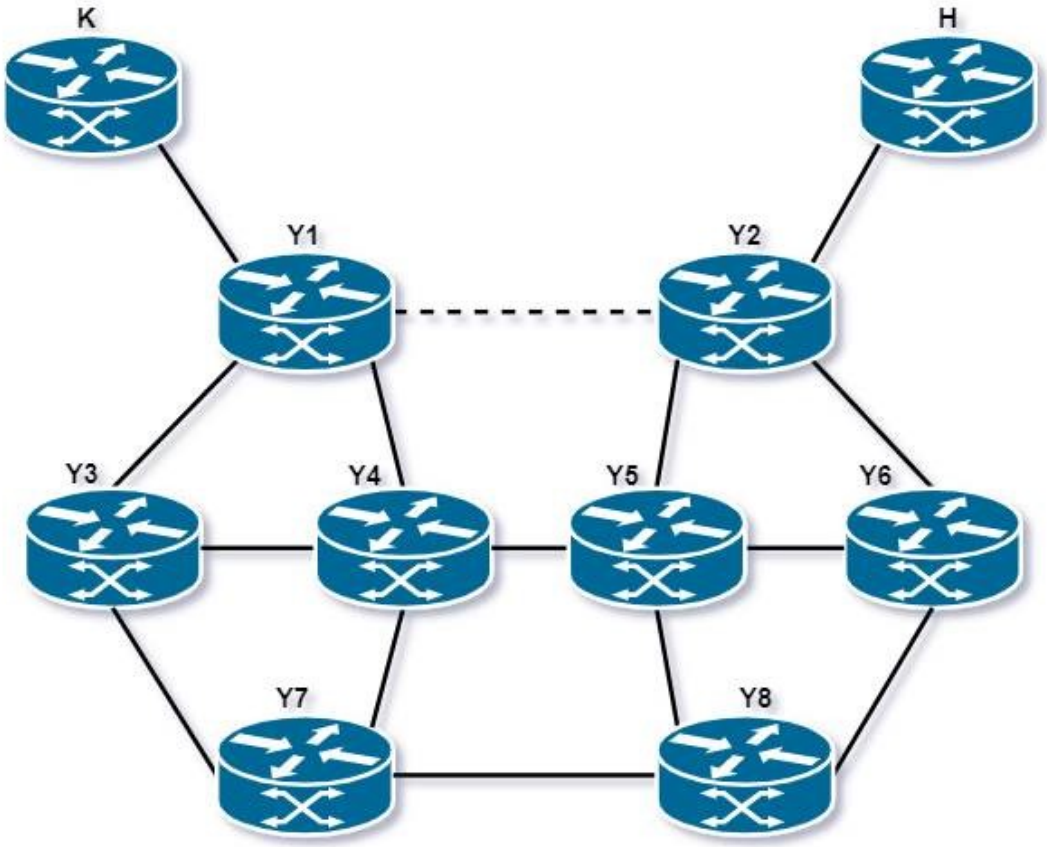
B. STP Testi

Şekil 4.8 aynı tip 3 yönlendirici kullanılarak kurulan STP topolojisini göstermektedir. Şekil 4.9 ise 10 yönlendiricili topoloji örneği göstermektedir.

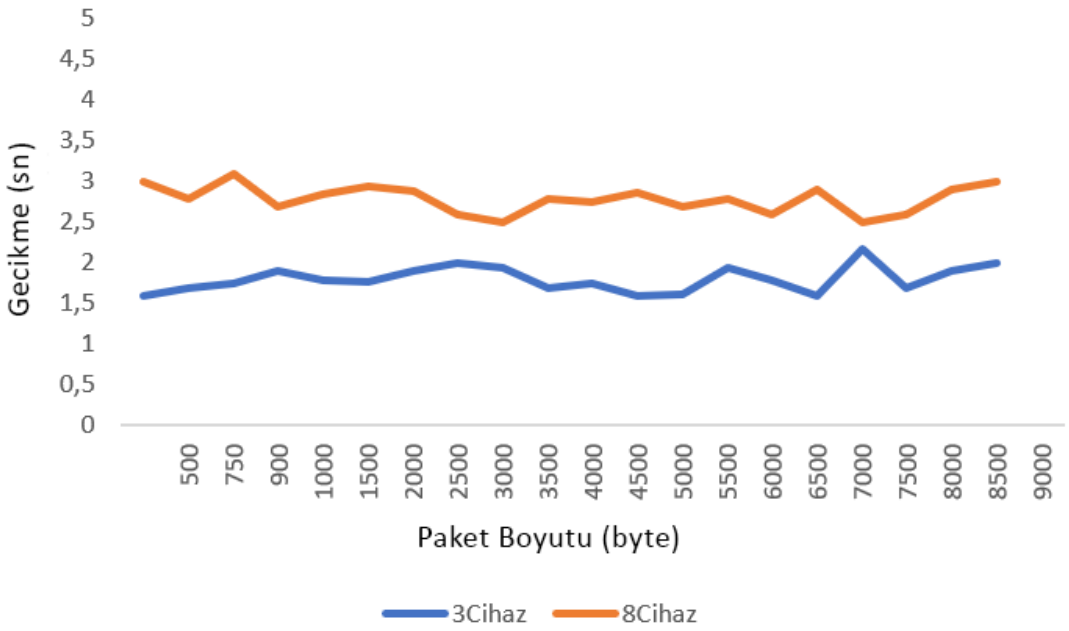
Şekil 4.8 gösterilen grafikten anlaşılacagı üzere cihaz 3 cihaz bulunan ağda gecikme süresi yaklaşık olarak 1.5 - 2,0s aralıgında ve ortalama 1,7s olmuştur. Ancak yönlendirci sayısını 10 yönlendirici olarak arttırdıgımızda yaşanan gecikme süresinin 2,2 ile 3,2s aralıgına, ortalama ise 2,8s değerine gecerek yaşanan kayıp sürede artış oldugu tespit edilmektedir. 1s'lik bir artış IP/MPLS gibi önemli ağlar için önemli sayılabilecek bir süredir. Test adımlarını özetlemek gerekirse;aktif olan Y1 ve Y2 yolu iki senaryoda da kapatılmış ve bu sürede K ve H cihazları arası sürekli bir ping koşulmuştur.



Şekil 4.8 3 Cihazlı STP topolojisi Örneği



Şekil 4.9 8 Cihazlı STP Topolojisi Örneği



Şekil 4.10 Cihaz Sayılarına Göre Test Sonuç Grafiği

A
Örnek Çıktılar

A1. MC-LAG Örnek Çıktıları

Y1>show lag 2 detail
LAG Details
Description : N/A
————————————————-
Details
————————————————
Lag-id : 2 Mode : network
Adm : up Opr : up
————————kısaltılmıştır————————
————————————————
Port-id Adm Act/Stdby Opr Primary Sub-group Forced Prio
————————————————
1/1/1 up active up yes 1 - 32768
1/1/2 up active up 1 - 32768
————————————————
Port-id Role Exp Def Dist Col Syn Aggr Timeout Activity
————————————————
1/1/1 actor No Yes No No No Yes Yes Yes
1/1/1 partner Yes Yes No No No No Yes No
1/1/2 actor No Yes No No No Yes Yes Yes
1/1/2 partner Yes Yes No No No No Yes No

Y2>show lag 2 detail
LAG Details
Description : N/A
————————————————
Details

———————————————

Lag-id : 2 Mode : network

Adm : up Opr : down

————————kısaltılmıştır———

———————————————

Port-id Adm Act/Stdby Opr Primary Sub-group Forced Prio

———————————————-

1/1/1 up active down yes 1 - 32768

1/1/2 up active up 1 - 32768

———————————————

Port-id Role Exp Def Dist Col Syn Aggr Timeout Activity

———————————————-

1/1/1 actor No Yes No No No Yes Yes Yes

1/1/1 partner Yes Yes No No No No Yes No

1/1/2 actor No Yes No No No Yes Yes Yes

1/1/2 partner Yes Yes No No No No Yes No

A2. Aktif Pasif Sözde Bağlantı Örnek Çıktıları

Öncelikle yollardan biri çalışmıyorken K cihazından H cihazı erişimi; CE6 üzerindeki bir IP'nin ping komutuyla ulaşılırlıgı kontrol edilmiştir. Aşağıdaki çıktıda görüldüğü gibi K cihazı H cihazına ulaşabilmektedir.

CE5> ping 20.1.1.5

PING 20.1.1.5 56 data bytes

64 bytes from 20.1.1.5: $\text{icmp}_s eq = 1 ttl = 64 time = 0.127 ms.$

$64 bytes from 20.1.1.5 : icmp_s eq = 2 ttl = 64 time = 0.154 ms.$

$64 bytes from 20.1.1.5 : icmp_s eq = 3 ttl = 64 time = 0.165 ms.$

$64 bytes from 20.1.1.5 : icmp_s eq = 4 ttl = 64 time = 0.143 ms.$

$64 bytes from 20.1.1.5 : icmp_s eq = 5 ttl = 64 time = 0.173 ms.$

Y1 cihazındaki LAG portu aktif oldugu için Y1 cihazı K cihazının MAC adresini K cihazına olan LAG portundan öğrenir. Y2 cihazında LAG portu down oldugu için K cihazının MAC adresini mesh-sdp üzerinden öğrenmektedir. Servislerin MAC adres tablolarına bakmak trafiğin akış yönünde kanıt niteliğindedir.

PE1>show service id 20 fdb detail

==========

Service Forwarding Database

```
==========================================
ServId MAC Source-Identifier Type Last Change Age


------------------------------
20 00:00:00:b2:3b:ac sdp:2:30 L/30 03/21/19 03:22:33
20 00:00:00:ae:9f:9f sap:lag-1:30 L/0 03/21/19 03:23:20


PE2>show service id 20 fdb detail
==========================================
Service Forwarding Database
==========================================
ServId MAC Source-Identifier Type Last Change Age


-------------------------
20 00:00:00:b2:3b:ac sap:1/1/4 L/30 03/21/19 03:23:33
20 00:00:00:ae:9f:9f sdp:1:30 L/0 03/21/19 03:24:20
```

Kaynakça

[1] “Virtual Private LAN Services (VPLS)”, https:/cisco.com/c/en/us/products/ios-nx-ossoftware/virtual-private-lan services-vpls/index.html, (Erişim tarihi: 18 Ekim 2018).

[2] “MPLS vs VPLS: What is the Right Solution for Your Business”, https://luminet.co.uk/mpls-vs-vpls-right-solution-business, (Erişim tarihi: 30 Ekim 2018).

[3] “Yönlendirme Protokolleri”, www.cisco.tr/yonlendirme-routing-protokolleri, (Erişim tarihi: 08 Ocak 2019).

[4] M. Lasserre ve V. Kompella, (2007). “Virtual private LAN service (VPLS) using label distribution protocol (LDP) signaling”, (No. RFC 4762).

[5] K. Kompella ve Y. Rekhter, (2007). “Virtual private LAN service (VPLS) using BGP for auto-discovery and signaling”, (No. RFC 4761).

[6] G. Di Battista, M. Rimondini ve G. Sadolfo, (2012). “Monitoring the status of MPLS VPN and VPLS based on BGP signaling information”, IEEE Network Operations and Management Symposium”, pp. 237-244.

[7] P. Kırcı, T. Çaglar ve F. Erdem, (2015). “IP /MPLS ağları üzerinde sanal yerel servisler ve yönlendirici konfigürasyonları”, Uludag University Journal of the Faculty of Engineering, vol. 20, pp. 155-165.

[8] B. Raahemi ve B. Bou-Diab, (2006). “A Minimum cost resilient tree based VPLS for digital tv broadcast services”, Canadian Conference on Electrical and Computer Engineering, pp. 995-998.

[9] M. Liyanage, M. Ylianttila ve A. Gurtov, (2016). “Improving the tunnel management performance of secure VPLS architectures with SDN”, 13th IEEE Annual Consumer Communications and Networking Conference (CCNC), pp. 530-536.

[10] M. Liyanage, M. Ylianttila ve A. Gurtov, (2015). “Secure hierarchical VPLS architecture for provider provisioned networks”, pp. 967-984.

[11] C. Fancy ve L.M.M. Thanveer, (2017). “An evaluation of alternative protocols-based virtual private LAN service (VPLS)”, International Conference on IoT and Application (ICIOT), pp. 1-6.

[12] M. Bocci, I. Cowburn ve J. Guillet, (2008). “Network high availability for ethernet services using IP/MPLS networks”, IEEE Communications Magazine, vol. 46, pp. 90-96.

[13] “Ethernet frame: definition and variants of the frame format, ethernet frame ”, https://www.ionos.com/digitalguide/server/know-how/ethernet-frame, (Erişim tarihi: 30 Kasım 2018).

[14] J. Moy, (1991). “RFC 1247: OSPF Version 2”.

[15] G. Warnock ve A. Nathoo, (2011). “NOKIA Network Routing Specialist II (NRS II) Self-Study Guide: Preparing for the NRS II Certification Exams”.

[16] E. Rosen, A. Viswanathan, ve R. Callon, (2001). “RFC 3031: Multiprotocol label switching architecture”.

[17] L. Andersson, I.E. Minei ve B. Thomas, (2007). " LDP Specification RFC 5036”.

[18] R. Braden, L. Zhang, S. Berson, S. Herzog ve S. Jamin, (1997). “RFC 2205. Network Working Group”.

[19] U. Lakshman ve L. Lobo, (2005). “MPLS configuration on Cisco IOS software. Cisco Press”.

[20] L. Martini, E. Rosen, ve N. El-Aawar, (2007). “Transport of layer 2 frames over MPLS (No. RFC 4906)”.

[21] P. Knight, ve C. Lewis, (2004). “Layer 2 and 3 virtual private networks: taxonomy, technology, and standardization efforts. IEEE Communications Magazine”, vol. 42, pp. 124-131.

[22] Z. Liu, L. Jin, R. Chen, D. Cai ve S. Salam, (2012)."Redundancy Mechanism for Inter-domain VPLS Service (No. RFC 7309)".

[23] “VPLS STP Solutions”, http:/www.juniper.net/documentation/en_US/release-independent/nce/topics/task/configuration/vpls-stp-solutions.html, (Erişim tarihi: 30 Mart 2019).

[24] T. Lammle, (2011). “CCNA Cisco Certified Network Associate Deluxe Study Guide. John Wiley & Sons”.

[25] G. Warnock ve A. Nathoo, (2011). “Alcatel-Lucent Network Routing Specialist II (NRS II) Self-Study Guide: Preparing for the NRS II Certification Exams. John Wiley & Sons”.

[26] R. Krishnan, L. Yong, A. Ghanwani, N. So, ve B. Khasnabish, (2015). “Mechanisms for optimizing link aggregation group (LAG) and equal-cost multipath (ECMP) component link utilization in networks”, (No. RFC 7424).

[27] L. Martini, S. Salam, A. Sajassi, M. Bocci ve S. Matsushima, (2014). “ Inter-chassis communication protocol for layer 2 virtual private network(L2VPN) provider edge (PE) redundancy, RFC 7275”.

[28] http://infoproducts.alcatel-lucent.com/html/0addh/93-0076-10-01/, (Erişim tarihi: 03 Kasım 2018).

[29] L. Martini, C. Metz, T. Nadeau, M. Aissaoui ve M. Bocci, (2011). “Segmented Pseudowire, RFC 6073”.

[30] “Multi-chassis”, https://infoproducts.alcatel-lucent.com/html/0add-h-f/9393-0267HTML/7X50AdvancedConfigurationGuide/MC-EP.html, (Erişim tarihi: 04 Mayıs 2019).