

**GEDİZ**ÜNİVERSİTESİ  
izmir

**GEDİZ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ**

**Sistem Mühendisliği Yüksek Lisans Programı**

## **Veri Merkezi Mimarisinde Yedeklilik ve Yük Dağılımı**

**YÜKSEK LİSANS TEZİ**

**Hazırlayan**  
**Numan Faruk KARAKAŞ**  
**(600113009)**

**Tez Danışmanı**

**Yrd. Doç. Dr. Hüseyin KUSETOĞULLARI**

**Şubat 2015**

Gediz Üniversitesi, Fen Bilimleri Enstitüsü Sistem Mühendisliği Yüksek Lisans Programı 600113009 numaralı Yüksek Lisans Öğrencisi **Numan Faruk KARAKAŞ**, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı “**Veri Merkezi Mimarisinde Yedeklilik ve Yük Dağılımı**” başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

**Tez Danışmanı:** Yrd. Doç. Dr. Hüseyin KUSETOĞULLARI

**Jüri Üyeleri:** Yrd. Doç. Dr. Durmuş UYGUN

Yrd. Doç. Dr. İbrahim Furkan İNCE

## ÖNSÖZ

Öncelikle bu tez konusu üzerinde bana çalışma imkânı sunan tez danışmanım Yrd. Doç. Dr. Hüseyin KUSETOĞULLARI'na paylaştığı bilgi ve önerileriyle çalıştığım konu hakkında beni araştırmaya yönlendirmesi ve tez süresince sağladığı her türlü destek ve yardımdan dolayı teşekkürü bir borç bilirim.

Akademik kariyerim noktasında sürekli beni destekleyen ve tez süresince manevi yardımlarını esirgemeyen sevgili aileme, bilhassa babama teşekkürü bir borç bilirim.

Ocak 2015

Numan Faruk KARAKAŞ

# İÇİNDEKİLER

## Sayfa

<b>1. GİRİŞ</b> .....	<b>1</b>
1.1. Tezin Amacı.....	1
1.2. Ön Bilgi Gerekliliği ve Literatür Araştırması .....	1
1.3 Tez İçeriği .....	1
<b>2. TEMEL TEKNOLOJİLER</b> .....	<b>3</b>
2.1. Hot Standby Router Protocol (HSRP).....	3
2.1.1. HSRP Durum Evreleri.....	4
2.1.2. HSRP Aktif – Yedek Seçimi .....	5
2.1.3. HSRP Yük Dağılımı .....	6
2.1.4. HSRP Konfigurasyonu .....	6
2.2. Virtual Router Redundancy Protocol (VRRP) .....	13
2.2.1. VRRP Aktif – Yedek Seçimi .....	15
2.2.2. VRRP Yük Dağılımı .....	15
2.2.3. VRRP Konfigurasyonu .....	16
2.3. Gateway Load Balancing Protocol (GLBP).....	22
2.3.1. GLBP Aktif – Yedek Seçimi.....	25
2.3.2. GLBP Yük Dağılımı .....	26
2.3.3. GLBP Konfigurasyonu.....	26
<b>3. YENİ NESİL TEKNOLOJİLER</b> .....	<b>33</b>
3.1. Virtual Switching System (VSS).....	33
3.1.1 Virtual Switching System Konfigurasyonu.....	35
3.1.2 Virtual Switching System de Yük Dağılımı ve Yedeklilik .....	43
<b>4. SONUÇLAR</b> .....	<b>45</b>
<b>KAYNAKLAR</b> .....	<b>48</b>
<b>ÖZGEÇMİŞ</b> .....	<b>50</b>

## ŞEKİL LİSTESİ

	<b><u>Sayfa</u></b>
Şekil 1.1: Yedekli olmayan bir ağ altyapısı. ....	2
Şekil 1.2. Yedekli bir ağ altyapısı.....	2
Şekil 2.1. HSRP ağ altyapısı.....	3
Şekil 2.2. HSRP yedeklilik işleyişi.....	9
Şekil 2.3. HSRP tracking işlemi.....	11
Şekil 2.4. VRRP ağ altyapısı.....	14
Şekil 2.5. VRRP yedeklilik işleyişi.....	18
Şekil 2.6. VRRP tracking işlemi.....	20
Şekil 2.7. GLBP ağ altyapısı.....	23
Şekil 2.8. GLBP yedeklilik işleyişi.....	29
Şekil 2.9. GLBP tracking işleyişi.....	31
Şekil 3.1. VSS ağ altyapısı.....	34
Şekil 3.2. VSS Vsl Header.....	38
Şekil 3.3. Etherchannel.....	39
Şekil 3.4. VSS Yedeklilik ve Yük dağılımı.....	44
Şekil 3.5. Gediz Üniversitesi VSS ağ altyapısı.....	44

## TABLO LİSTESİ

	<b><u>Sayfa</u></b>
Tablo 2.1. Tablo 2.1: GLBP topolojisinde rol paylaşımları.....	29
Tablo 3.1. Tablo 3.1: Etherchannel 8 bitlik HASH algoritması.....	40
Tablo 4.1. Tablo 2.1: Geleneksel ve yeni nesil teknolojilerin yedeklilik ve yük dağılımı karşılaştırılması .....	47

## FIGÜR LİSTESİ

### Sayfa

Figür 2.1: HSRP Omurga1 standby konfigürasyonu. ....	6
Figür 2.2: HSRP Omurga2 standby konfigürasyonu .....	6
Figür 2.3: HSRP Omurga1 fiziksel adres gösterim konfigürasyonu .....	7
Figür 2.4: HSRP Omurga2 fiziksel adres gösterim konfigürasyonu.....	7
Figür 2.5: HSRP Omurga1 yedeklilik durum gösterimi konfigürasyonu .....	7
Figür 2.6: HSRP Omurga2 yedeklilik durum gösterimi konfigürasyonu .....	8
Figür 2.7: HSRP Omurga1 preempt konfigürasyonu .....	8
Figür 2.8: HSRP Omurga1 yedeklilik durum gösterimi konfigürasyonu .....	9
Figür 2.9: HSRP Omurga1 interface shut etme konfigürasyonu .....	9
Figür 2.10: HSRP Omurga2 debug gösterim konfigürasyonu .....	10
Figür 2.11: HSRP Omurga1 track konfigürasyonu .....	11
Figür 2.12: HSRP Omurga1 yedeklilik track öncesi durum gösterim konfigürasyonu .....	12
Figür 2.13: HSRP Omurga1 yedeklilik track sonrası durum gösterim konfigürasyonu .....	12
Figür 2.14: HSRP Omurga1 yük dağılımı konfigürasyonu. ....	12
Figür 2.15: HSRP Omurga2 yük dağılımı konfigürasyonu .....	13
Figür 2.16: VRRP Omurga1 konfigürasyonu .....	16
Figür 2.17: VRRP Omurga2 konfigürasyonu .....	16
Figür 2.18: VRRP Omurga1 fiziksel adres gösterim konfigürasyonu .....	17
Figür 2.19: VRRP Omurga2 fiziksel adres gösterim konfigürasyonu. ....	17
Figür 2.20: VRRP Omurga1 yedeklilik durum gösterimi konfigürasyonu .....	17
Figür 2.21: VRRP Omurga2 yedeklilik durum gösterimi konfigürasyonu.....	17
Figür 2.22: VRRP Omurga1 priority değerini değiştirme konfigürasyonu. ....	18
Figür 2.23: VRRP Omurga1 yedeklilik durum gösterimi konfigürasyonu.....	18
Figür 2.24: VRRP Omurga1 interface shut etme konfigürasyonu .....	19
Figür 2.25: VRRP Omurga2 debug gösterimi konfigürasyonu .....	19
Figür 2.26: VRRP Omurga1 track işlemi konfigürasyonu. ....	20
Figür 2.27: VRRP Omurga1 track öncesi yedeklilik durum gösterimi konfigürasyonu.....	21
Figür 2.28: VRRP Omurga1 interface shut olma debug gösterimi konfigürasyonu. ....	21
Figür 2.29: VRRP Omurga1 track sonrası yedeklilik durum gösterimi konfigürasyonu.....	21
Figür 2.30: VRRP Omurga1 yük dağılımı gösterimi konfigürasyonu .....	22
Figür 2.31: VRRP Omurga2 yük dağılımı gösterimi konfigürasyonu.....	22
Figür 2.32: GLBP Omurga1 konfigürasyonu. ....	26
Figür 2.33: GLBP Omurga2 konfigürasyonu .....	27
Figür 2.34: GLBP Omurga3 konfigürasyonu .....	28
Figür 2.35: GLBP Omurga1 interface shut etme konfigürasyonu. ....	29
Figür 2.36: GLBP Omurga2 debug gösterim konfigürasyonu .....	30
Figür 2.37: GLBP Omurga3 debug gösterim konfigürasyonu .....	30
Figür 2.38: GLBP Omurga1 track işlemi konfigürasyonu .....	31
Figür 2.39: GLBP Omurga1 weighting track işlemi konfigürasyonu .....	32

Figür 2.40: GLBP Omurga1 interface shut etme konfigürasyonu .....	32
Figür 2.41: GLBP Omurga1 track işlemi sonrası yedeklilik gösterim konfigürasyonu.....	32
Figür 3.1: SW1 module gösterim konfigürasyonu . .....	35
Figür 3.2: SW2 module gösterim konfigürasyonu.....	36
Figür 3.3: SW1 version gösterim konfigürasyonu.....	36
Figür 3.4: SW2 version gösterim konfigürasyonu.....	36
Figür 3.5: SW1 ve SW2 virtual domain konfigürasyonu .....	37
Figür 3.6: SW1 ve SW2 , VSS priority değeri konfigürasyonu . .....	37
Figür 3.7: SW1 virtual link konfigürasyonu . .....	40
Figür 3.8: SW2 virtual link konfigürasyonu . .....	40
Figür 3.9: SW1 ve SW2 etherchanel durum gösterim konfigürasyonu. ....	41
Figür 3.10: SW1 virtual convert konfigürasyonu . .....	41
Figür 3.11: SW2 virtual convert konfigürasyonu . .....	42
Figür 3.12: SW1 VSS başlangıç süreci gösterim konfigürasyonu . .....	42
Figür 3.13: SW2 VSS başlangıç süreci gösterim konfigürasyonu . .....	42
Figür 3.14: SW1 ve SW2 VSS aktif-pasif seçim süreci gösterim konfigürasyonu . .....	43



## KISALTMALAR LİSTESİ

<b>WAN</b>	Wide Area Network
<b>RARP</b>	Reverse Address Resolution Protocol
<b>ARP</b>	Address Resolution Protocol
<b>VLAN</b>	Virtual Local Area Network
<b>UDP</b>	User Datagram Protocol
<b>TCP</b>	Transmission Control Protocol
<b>OSI</b>	Open Systems Interconnection
<b>LAN</b>	Local Area Network
<b>MAC</b>	Media Access Control
<b>ICMP</b>	Internet Control Message Protocol
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>IP</b>	Internet Protocol
<b>NAT</b>	Network Address Translation
<b>LAN</b>	Local Area Network
<b>MAC</b>	Media Access Control
<b>NAT</b>	Network Address Translation
<b>HSRP</b>	Hot Standby Router Protocol
<b>VRRP</b>	Virtual Router Redundancy Protocol
<b>GLBP</b>	Gateway Load Balancing Protocol
<b>VSS</b>	Virtual Switching System
<b>GNS3</b>	Graphical Network Simulator
<b>AVF</b>	Active Virtual Forwarder
<b>AVG</b>	Active Virtual Gateway
<b>IOS</b>	Internet Operating System
<b>MEC</b>	MultiChassis EtherChannel
<b>STP</b>	Spanning Tree Protocol

## GENEL BİLGİLER

Adı ve Soyadı : Numan Faruk KARAKAŞ  
Anabilim Dalı : Endüstri Mühendisliği Anabilim Dalı  
Programı : Sistem Mühendisliği  
Tez Danışmanı : Yrd. Doç. Dr. Hüseyin KUSETOĞULLARI  
Tez Türü ve Tarihi : Yüksek Lisans – Ocak 2015

## Veri Merkezi Mimarisinde Yedeklilik ve Yük Dağılımı

### ÖZET

Bu tezin amacı yük verimliliği ve yük dağılımı yapılan veri merkezlerinde farklı Local Area Network (LAN) altyapılarını birbirlerine bağlayan omurga cihazlarında herhangi bir trafik kesintisi olmayacak şekilde yedeklilik ve yük dağılımı sağlayan teknolojilerin araştırılmasının, karşılaştırılmasının yapılması ve yeni nesil teknolojilerin geliştirilmesine fayda sağlanmasıdır.

Yedeklilik ve Yük dağılımı sağlayan geleneksel teknolojiler 2. bölüm altında Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), Gateway Load Balancing Protocol (GLBP) başlıkları altında incelenmiştir. Bu teknolojilerin omurga altyapısındaki yedeklilik ve yük dağılımı sürecinde aktif-pasif seçimi, yük dağılımının nasıl belirlendiği ve konfigürasyonlarının nasıl yapıldığı araştırılıp, detaylı bir şekilde anlatılmıştır. Geleneksel teknolojilerin konfigürasyonu Graphical Network Simulator (GNS3) ortamında yapılmıştır.

Veri merkezlerindeki ve internet ağ altyapısındaki yüksek verimli yedeklilik ve yük dağılımı olması gereken omurga cihazlarda yeni nesil teknolojilerin kullanılmasının gerekliliği ve önemi 3. bölüm altında işlenmiştir. Yeni Nesil Teknolojilerden olan Virtual Switching System (VSS) teknolojisinin yedeklilik ve yük dağılımı algoritması anlatılmış ve Gediz Üniversitesi ağ yapısında bu teknoloji kurulmuş ve konfigürasyonu yapılmıştır.

Bu tezde, yüksek verimliliğin beklendiği veri merkezlerindeki ağ altyapılarında, bütün ağ altyapısını birleştiren ve birbirleriyle haberleşmesini sağlayan omurga cihazlarında yedeklilik ve yük dağılımı için kullanılan teknolojilerin anlatılması, açıklanması, bu teknolojilerin birbirleriyle olan ilişkisi ve karşılaştırılması yer almaktadır.

**Anahtar Kelimeler:** HSRP, VRRP, GLBP, VSS, Yedeklilik, Bilgisayar Ağları, Yük Dağılımı ve Yönlendirici.

## GENERAL INFORMATION

Name and Surname : Numan Faruk KARAKAŞ  
Field : Industrial Engineering  
Program : System Engineering  
Supervisor : Asst. Prof. Dr. Hüseyin KUSETOĞULLARI  
Degree and Date : Master – January 2015

## LOAD BALANCING AND CLUSTERING IN DATA CENTER ARCHITECTURE

### ABSTRACT

The thesis aims to provide research, investigation and comparison on load-balancing and clustering in data center architecture by using the network technologies that will provide data communication without any communication traffic problem in the network infrastructure which are interconnecting between each other in the Local Area Networks (LANs) and to explain the benefits of development of new generation technologies.

Traditional technologies that provide load balancing and load distribution are examined clearly in the following subsections of Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), Gateway Load Balancing Protocol (GLBP) under the second section. During the redundancy and load distribution process in the backbone infrastructure of these technologies, active-passive selection, determination of the load distribution and the configuration process are described with the details. Traditional configurations of these technologies have been simulated by using the Graphical Network Simulator (GNS3).

The importance of the use of the new technologies in the spinal devices is explained under the third section for the load distribution and data load balancing for the data centers and internet network infrastructure. The algorithm of the load balancing and load distribution in the one of the new technology Virtual Switching System (VSS) is described and this technology has been designed as a network configuration for the Gediz University.

In this thesis, the expected high efficiency by the data network infrastructure in the data center, which combines all the network infrastructure and explains the technology used for redundancy and load distribution in the spinal device that allows communication with each other, disclosure of this technology to the comparison and relationship with each other have been provided.

**Key Words:** HSRP, VRRP, GLBP, VSS, Data Loading, Data Load Distribution, Data Router and Computer Networks.

# 1.GİRİŞ

## 1.1 Tezin Amacı

Günümüzde ses ve veri trafiğinin herhangi bir kesinti olasılığının olmaması gereken Veri Merkezlerinde, Open Systems Interconnection (OSI) katmanlarından 2.seviye ve 3. seviye olan ağ katmanında yedeklilik ve yük paylaşımı büyük önem taşımaktadır. Bu tezde Veri Merkezlerinin omurga cihazlarında yedeklilik ve yük paylaşımı için kullanılan metotların ve protokollerin anlatımı, karşılaştırılması ve geliştirilmesi amaçlanmıştır.

## 1.2 Ön Bilgi Gerekliliği ve Literatür Araştırması

Bu tezin daha sağlıklı anlaşılabilmesi için 3.seviye IP yönlendirme teknolojilerinin, OSI katmanlarının, sanal ağların (vlan), 3. seviye sanal ağ ara yüzlerinin yönlendirilmesinin (Inter-Vlan routing), Spanning-Tree protokolünün bilinmesi önem arz etmektedir.

Bu konuda yapılan akademik çalışmalar ve araştırmalar arasında Cisco CCNP ve CCIE Routing and Switching Certification Guide [1], Data Center High Availability Clusters Design Guide [2], Load Balancing Mechanisms in Data Center Networks [3], vardır. İlgilenen araştırmacılar için bu çalışmalara bağlı makalelerinin incelenmesi yararlı ve faydalı olacaktır.

## 1.3 Tez İçeriği

Günümüzde internetin her alanda etkisinin olması, kullanılan uygulamaların sayısının her geçen gün artması [4], ses ve görüntü verilerinin IP network üzerinden taşınması [5], gibi önemli unsurlar ağ altyapısının her daim, kesintisiz çalışabilir olmasını talep etmektedir. Dolayısıyla yedeklilik ve yük dağılımı, ağ mimarisinde en mühim konu haline gelmektedir [6]. Bu tezde veri merkezi mimarisinde ağ katmanında yedeklilik ve yük paylaşımı konusunda birçok sorunumuzu çözen ve verimliliği arttıran protokollerin incelenmesinden, karşılaştırılmasından ve bu konudaki yeni nesil teknolojilerin geliştirilmesinden bahsedilecektir. Tezde anlatılan terimler, metotlar ve protokoller IEEE ve Cisco Systems terminolojisini temel almıştır.

Yedeklilik ve yük paylaşımı işlevlerini yürüten metotları iki ayrı başlık altında inceleyebiliriz. Temel teknolojiler ve yeni nesil teknolojiler olarak iki bölüme ayrılmaktadır. Bu teknolojiler bir sonraki bölümde detaylı bir şekilde anlatılacaktır.

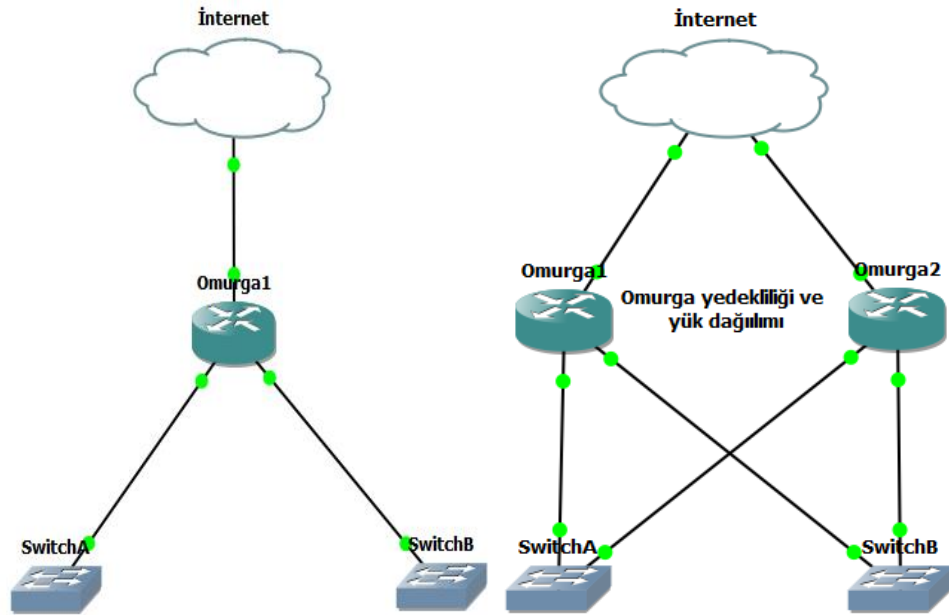
**a) Temel teknolojiler;**

- ✓ Hot Standby Router Protocol (HSRP)
- ✓ Virtual Router Redundancy Protocol (VRRP)
- ✓ Gateway Load Balancing Protocol (GLBP)

**b) Yeni nesil teknolojisi;**

- ✓ Virtual Switching Systems (VSS)

Temel teknolojiler kısmında metotların yedeklilik ve yük paylaşımıyla beraber çalışma mantıkları anlatılıp, konfigürasyon yapılarak uygulamalı olarak performans sonuçları ve topolojik yerleşkeleri açıklanacaktır. Üçüncü bölümde VSS teknolojisinin farklılığı ve yapılandırılması izah edilecektir.



Şekil 1.1: Yedekli olmayan bir ağ altyapısı.

Şekil 1.2: Yedekli bir ağ altyapısı.

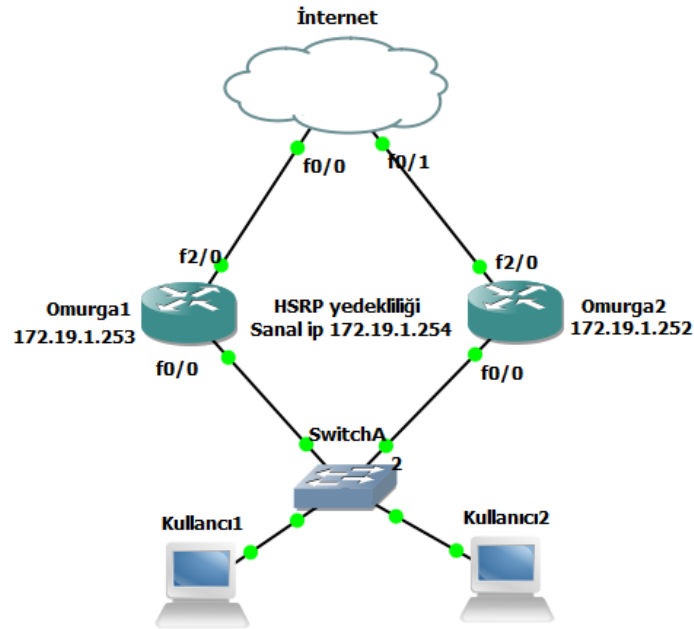
Günümüzde yedekli bir omurga altyapısı olmayan (Şekil 1.1) bir sitem güvenilir olarak tanımlanamaz. Veri akışının kesintisiz devam edebilmesi için yedekli bir topoloji mantığı (Şekil 1.2) şarttır.

## 2.TEMEL TEKNOLOJİLER

Yedeklilik sağlayan bu teknolojiler birden fazla yönlendirici (Routers) ya da üçüncü seviye anahtarlama (Switches) cihazları arasında uygulanır. Yedeklilik için ilk kullanılan teknoloji HSRP (Hot Standby Router Protocol)'dir [7]. Bu bölüm içerisinde daha sonra anlatılacak GLBP (Gateway Load Balancing Protocol) , HSRP den esinlenerek geliştirilmiştir [8]. HSRP ve GLBP cisco teknolojisi standardı olmasına karşın , VRRP (Virtual Router Redundancy Protocol) bir IEEE standardıdır. [9]

### 2.1 Hot Standby Router Protocol (HSRP)

HSRP, birden fazla yönlendiricinin veya üçüncü seviye bir anahtarlayıcının son kullanıcıya tek yönlendirici olarak görünmesini sağlayan protokoldür. Birden fazla yönlendirici arasında bir tanesi aktif yönlendirme işlemlerini yürütürken diğeri yedek olarak beklemekte ve aktif olan yönlendiriciyi takip etmektedir. Bu konu içerisinde HSRP'nin işleyişinden bahsedilecek ve HSRP konfigürasyonunun yönlendiriciler üzerinde nasıl yapıldığı adım adım incelenecektir. Bu bölümdeki konfigürasyonlar GNS3 emülatör ortamında yapılacaktır [10].



Şekil 2.1: HSRP ağ altyapısı.

Şekil 2.1'de görüldüğü gibi kendi fiziksel bağlantıları ve IP adresleri olan iki adet yönlendirici tek bir IP adresi ve fiziksel adresi paylaşan, tek bir sanal yönlendirici gibi hareket etmektedir. Son kullanıcılar HSRP protokolünün oluşturduğu sanal

yönlendiricinin IP adresini bilirler ve bu IP adresini ağ geçidi olarak tanırlar. Bu bölüm içinde HSRP'nin işleyiş kısımlarından bahsedilecek ve simülasyon ortamında yapılan konfigürasyonların gösterimi olacaktır.

HSRP mimarisinde yönlendiricilerden biri "Aktif" (Active) durumda çalışırken, diğerleri "bekleme" (Standby) halde çalışır. HSRP terminolojisinde aktif olarak yönlendirme işlemlerini yapan yönlendirici "Active Router", yedek olarak bekleyen yönlendirici ise "Standby Router" olarak adlandırılır. Standby görevini üstlenen yönlendirici, paket iletimi ile alakalı herhangi bir yönlendirme işlemi yapmaz. HSRP mimarisinde yönlendiriciler yedekliliğin kurulması için aynı grup içerisinde olmak zorundadır. Yönlendiricilere grup numarası ağ yöneticisi tarafından verilir. Eğer bir grup numarası belirtilmez ise 0 olarak kabul edilir ve 255'e kadar numaralar kullanılabilir.

HSRP altyapısında arp isteklerine sadece aktif olan cevap verebilir. Sanal yönlendiricilere ağ yöneticisi tarafından atanan sanal IP adresine gelen ARP (Adres Çözümleme Protokolü) isteklerini aktif yönlendirici cevaplar ve cevap olarak gerçek fiziksel adresi yerine sanal fiziksel adreslerini döner. Sanal fiziksel adresleri ağ yöneticileri tarafından tanımlanmaması durumunda HSRP otomatik olarak sanal bir fiziksel adres üretir.

Burada üretilen sanal fiziksel adresi şu şekildedir;

Üretici kodu (00.00.0C) + HSRP (07.AC) + Grup numarası

Örneğin 1 numaralı HSRP grubu içine sanal fiziksel adresi 0000.0C07.AC01 olacaktır. İstemci bilgisayarların ARP belleklerine bakıldığında sanal IP ve fiziksel adresleri görülecektir.

### **2.1.1 HSRP Durum Evreleri**

Aktif ve yedek yönlendirici 224.0.0.2 multicast IP adresi ve UDP (User Datagram Protocol) 1985 portu üzerinden birbirlerini "Hello" paketi denen paketleri 3 saniye aralıklar ile göndererek haberleşirler [11]. Aktif yönlendirici 3 saniye aralıklar ile gönderdiği Hello paketlerini, örneğin yönlendiricinin yerel tarafa bakan portunda kopma olması gibi bir sebepten dolayı 10 saniye boyunca gönderemez ise yedek yönlendirici, aktif yönlendirici görevini üstlenir ve paket yönlendirmede başrol

oynamaya başlar. Bir HSRP grubuna dâhil edilmiş yönlendiriciler altı ayrı durum sürecinden geçerler. Bu durumlar aşağıdaki özetlenmektedir;

**İlk hal (Initial)** : Yönlendiricilerin ilk durum halidir.

**Öğrenme (Learn)**: HSRP çalışmaya başlamıştır fakat yönlendiriciler henüz aktif ya da yedek durumda değildir. Bu durumda yönlendiriciler henüz sanal IP adresini tanınamışlardır. Yönlendiriciler “**öğrenme**” evresinde “hello” paketlerini beklerler ve paketinin doğruluğunu anlamaya çalışırlar.

**Dinleme (Listen )**: Halen yönlendiriciler aktif ya da bekleme durumuna geçmemiştir. Fakat buldukları grubun sanal IP adresini öğrenmişler, aynı gruptaki diğer yönlendiricilerin “hello” paketlerini dinlemeye başlamışlardır.

**Konuşma (Speak)**: Aktif ve yedek yönlendirici seçimi başlamıştır ve yönlendiriciler bu seçimde yer almak için periyodik “hello” paketlerini göndermeye başlarlar.

**Yedekli Hal (Standby)**: Yönlendirici yedek rolünü üstlenmiştir ve aktif yönlendirici olmak için aday durumundadır. Aktif yönlendiriciden gelen “hello” paketlerini dinleyerek, görevini yerine getirip getirmediğini kontrol eder.

**Aktif Hal (Active)**: Yönlendirici periyodik hello paketlerini göndermeye devam ederken aktif olarak paket yönlendirme ve istemcilerin isteklerine cevap verme işlemlerini de üstlenmiştir.

### **2.1.2 HSRP Aktif – Yedek Seçimi**

HSRP içerisinde kimin aktif yönlendirici rolünü üstleneceğine **priority** değerleri ile karar verilir. İlk durumda priority değeri her yönlendirici için 100’dür. Eğer priority değerleri ağ yönetici tarafından konfigüre edilmemişse fiziksel ip adresi daha büyük olan yönlendirici aktif, diğeri yedek rolünü üstlenecektir. Eğer özellikle bir yönlendiricinin aktif olmasını isteniliyorsa yönlendiricinin priority değeri diğer yönlendiriciden daha yüksek konfigüre edilir. Burada önemli bir husus vardır. Eğer “preempt” aktif edilmemişse sisteme ilk katılan yönlendirici aktif rol alır. Bu adaletli bir seçim olmaz. Bundan dolayı “preempt” aktif edilmelidir. Bu her zaman seçimin adaletli olmasını sağlar. Aktif rolünde olan bir yönlendirici her 3 saniye de bir kendi fiziksel bacağından 224.0.0.2 adresine “hello” paketleri gönderir ve eğer başına bir şey gelir de gönderemeyecek olursa belirli bir süre “hello” paketini alamayan diğer



yönlendirici aktif rolünü üstlenecektir. Bu bölümün uygulaması HSRP konfigürasyon bölümünde yapılmıştır.

### 2.1.3 HSRP Yük Dağılımı

HSRP mimarisinde yük dağılımı temeldir [12]. Topolojide iki adet yönlendirici olduğunu varsayalım. Kullanıcıların yarısı ilk yönlendiriciyi aktif olarak görecektir, kullanıcıların diğer yarısı ise ikinci yönlendiriciyi aktif olarak görecektir. Bu durumda her iki yönlendirici de hem aktif hem yedek rolünde çalışmış olacaktır. Burada yapılması gereken  $N$  adet HSRP grubu oluşturmak ve her grup için sanal IP adresi vermektir. Bu bölümün uygulaması HSRP konfigürasyon bölümünde yapılmıştır.

### 2.1.4 HSRP Konfigürasyonu

HSRP mimarisinin daha iyi anlaşılabilmesi için **Şekil 2.1** topolojisi kullanılacaktır. Şekilde görüldüğü gibi yedeklilik için **Omurga1** ve **Omurga2** isiminde iki adet yönlendirici kullanılıyor. Yönlendiricilerin kullanıcılara bakan interfacerlerinin konfigürasyonlarına bakacak olursak;

```
Omurga1#show running-config interface fastEthernet 0/0
Building configuration...

Current configuration : 124 bytes
!
interface FastEthernet0/0
 ip address 172.19.1.253 255.255.255.0
 duplex auto
 speed auto
 standby 1 ip 172.19.1.254
end
```

**Figür 2.1:** HSRP Omura1 standby konfigürasyonu

“Standby 1 IP 172.19.1.254” buradaki “1” HSRP grup numarası belirtmektedir. “172.19.1.254” ise HSRP sanal IP adresini belirtmektedir.

```
Omurga2#show running-config interface fastEthernet 0/0
Building configuration...

Current configuration : 124 bytes
!
interface FastEthernet0/0
 ip address 172.19.1.252 255.255.255.0
 duplex auto
 speed auto
 standby 1 ip 172.19.1.254
end
```

**Figür 2.2:** HSRP Omura2 standby konfigürasyonu

“Standby 1 IP 172.19.1.254” buradaki “1” HSRP grup numarası belirtmektedir. “172.19.1.254” ise HSRP sanal IP adresini belirtmektedir.

Konfigurasyonlarda görüldüğü gibi iki omurga da HSRP-1 numaralı gruba üyeler ve iki yönlendiriciye de herhangi bir priority değeri verilmemiştir. Bu durumda iki omurganın da priority değeri **HSRP Aktif – Yedek Seçimi** bölümünde anlatıldığı gibi 100’dür. Aktif – yedek yönlendirici seçimi bu durumda fiziksel adrese bakılarak yapılır. Fiziksel adresi yüksek olan yönlendirici aktif olur. Aşağıda gösterilen konfigürasyona bakılarak fiziksel adresi yüksek olan yönlendiricinin aktif durumu ve fiziksel adresi düşük olan yönlendiricinin pasif durumu görülebilir;

```
Omurga1#show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is c205.18c8.0000 (bia c205.18c8.0000)
  Internet address is 172.19.1.253/24
```

**Figür 2.3:** HSRP Omurga1 fiziksel adres gösterim konfigürasyonu

```
Omurga2#show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is c206.18c8.0000 (bia c206.18c8.0000)
  Internet address is 172.19.1.252/24
```

**Figür 2.4:** HSRP Omurga2 fiziksel adres gösterim konfigürasyonu

Omurga2’nin sahip olduğu fiziksel adres Omurga1’in sahip olduğu fiziksel adresten daha büyük olduğundan dolayı Omurga2 aktif yönlendirici olacaktır. Bu durumda, Omurga1 yedek yönlendirici rolünü üstlenecektir. Fiziksel adresler Omurga1 ve Omurga2 konfigürasyonları içerisinde yuvarlak içerisinde belirtilmiştir.

```
Omurga1#show standby
FastEthernet0/0 - Group 1
  State is Standby
    1 state change, last state change 01:16:36
  Virtual IP address is 172.19.1.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.000 secs
  Preemption disabled
  Active router is 172.19.1.252, priority 100 (expires in 9.720 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Fa0/0-1" (default)
```

**Figür 2.5:** HSRP Omurga1 yedeklilik durum gösterimi konfigürasyonu

Yedeklilik durum görüldüğü gibi, yönlendirici yedek (Standby) durumundadır. Sanal fiziksel adrese bakıldığında;

0000.0c07.ac01 = Üretici kodu (00.00.0C) + HSRP (07.AC) + Grup numarası (01)

Priority değeri konfigürasyonda da görüldüğü gibi 100 dür.

```
Omurga2#show standby
FastEthernet0/0 - Group 1
  State is Active
    1 state change, last state change 01:29:49
  Virtual IP address is 172.19.1.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.348 secs
  Preemption disabled
  Active router is local
  Standby router is 172.19.1.253, priority 100 (expires in 8.612 sec)
  Priority 100 (default 100)
  Group name is "hsrp-Fa0/0-1" (default)
Omurga2#
```

**Figür 2.6:** HSRP Omurga2 yedeklilik durum gösterimi konfigürasyonu

Bu konfigürasyon örneğinde Omurga2 'nin yedeklilik durumu yönlendirici aktif (Active) durumundadır. Priority değeri konfigürasyonda da görüldüğü gibi 100 dür.

Priority değerlerinin eşit olmasına rağmen Omurga2 yönlendiricisinin aktif olmasının nedeni, Omurga2 yönlendiricisinin gerçek fiziksel adresinin Omurga1'in fiziksel adresinden büyük olmasıdır. Bu topolojide aktif yönlendiricinin Omurga1 olması isteniyorsa, Omurga1 yönlendiricisinin HSRP priority değerinin yükseltilmesi gerekmektedir. Lakin bu durum yeterli değildir. Çünkü priority değeri yükseldikten sonra tekrar seçim yapılabilmesi için preempt özelliğinin aktif edilmesi gerekmektedir. Bu özelliğin aktif olabilmesi için yapılan işlemlerin konfigürasyonları aşağıdaki gibidir. Preempt , yönlendiriciler arası aktif-pasif seçiminin periyodik olarak sürekli yapılmasını sağlar.

```
Omurga1(config)#interface fastEthernet 0/0
Omurga1(config-if)#standby 1 priority ?
    <0-255> Priority value

Omurga1(config-if)#standby 1 priority 150
Omurga1(config-if)#standby 1 pre
Omurga1(config-if)#standby 1 preempt
Omurga1(config-if)#
*Mar  1 02:52:18.943: %HSRP-5-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active
Omurga1(config-if)#
```

**Figür 2.7:** HSRP Omurga1 preempt konfigürasyonu

Yukarıdaki konfigürasyonda görüldüğü gibi Omurga1'in HSRP priority değeri 150 değerine yükseltilmiştir ve preempt özelliğinin aktif edilmesiyle HSRP durumu yedekten aktife geçmiştir.

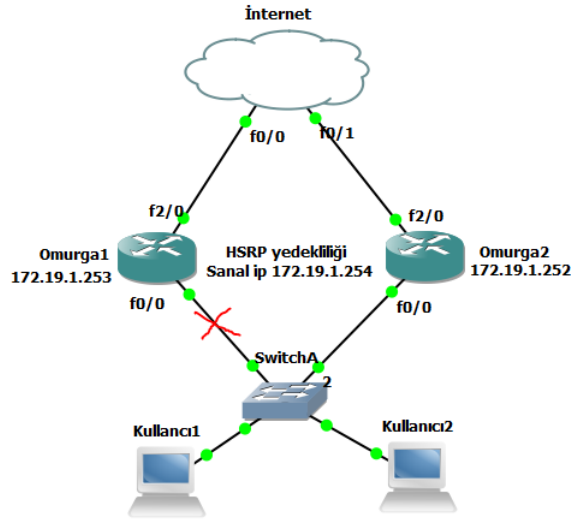
```

Omurga1#show standby
FastEthernet0/0 - Group 1
  State is Active
    2 state changes, last state change 00:03:39
  Virtual IP address is 172.19.1.254
  Active virtual MAC address is 0000.0c07.ac01
  Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 2.228 secs
  Preemption enabled
  Active router is local
  Standby router is 172.19.1.252, priority 100 (expires in 7.304 sec)
  Priority 150 (configured 150)
  Group name is "hsrp-Fa0/0-1" (default)

```

**Figür 2.8:** HSRP Omurga1 yedeklilik durum gösterimi konfigürasyonu

Yönlendiricilerden herhangi birinin zarar görmesi veya yönlendiricilerin kullanıcılarla olan iletişim kablolarının kopması gibi önemli durumlarda yedeklilik işlemi yapılmalıdır. Bu işlem aşağıdaki gösterildiği gibi yapılmalıdır.



**Şekil 2.2 :** HSRP yedeklilik işleyişi.

Şekil 2.2’de görüldüğü gibi omurga1 yönlendiricinin yerel bacağındaki kablonun kopmasıyla ya da yönlendiricinin zarar görmesi gibi durumlarda Omurga2 aktif rolünü üzerine alacaktır. Simülasyon ortamında bu işleyişi görebilmek için Omurga1’in **fastEthernert 0/0** portunu devre dışı bırakalım. Bu işlev porta “**shutdown**” komutunu girerek yapılır.

```

Omurga1(config)#interface fastEthernet 0/0
Omurga1(config-if)#shu
Omurga1(config-if)#shutdown
Omurga1(config-if)#
*Mar 1 03:42:39.843: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
*Mar 1 03:42:40.843: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
Omurga1(config-if)#

```

**Figür 2.9:** HSRP Omurga1 interface shut etme konfigürasyonu

```

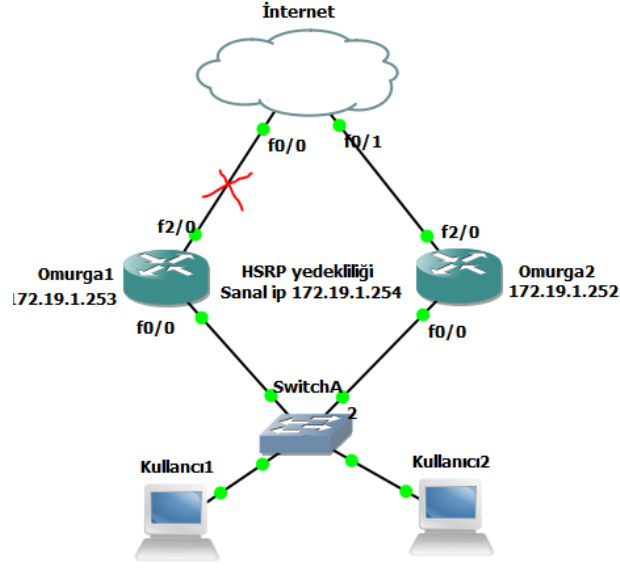
Omurga2#
*Mar 1 03:44:51.595: HSRP: Fa0/0 Grp 1 Hello in 172.19.1.253 Active pri 150 vIP 172.19.1.254
*Mar 1 03:44:52.571: HSRP: Fa0/0 Grp 1 Hello in 172.19.1.253 Active pri 150 vIP 172.19.1.254
Omurga2#
*Mar 1 03:44:52.715: HSRP: Fa0/0 Grp 1 Hello out 172.19.1.252 Standby pri 100 vIP 172.19.1.254
Omurga2#
*Mar 1 03:44:54.187: HSRP: Fa0/0 Interface adv out, Passive, active 0 passive 1
*Mar 1 03:44:54.659: HSRP: Fa0/0 Grp 1 Hello in 172.19.1.253 Active pri 150 vIP 172.19.1.254
Omurga2#
*Mar 1 03:44:55.719: HSRP: Fa0/0 Grp 1 Hello out 172.19.1.252 Standby pri 100 vIP 172.19.1.254
Omurga2#
*Mar 1 03:44:57.627: HSRP: Fa0/0 Grp 1 Resign in 172.19.1.253 Active pri 150 vIP 172.19.1.254
*Mar 1 03:44:57.627: HSRP: Fa0/0 Grp 1 Standby: i/Resign rcvd (150/172.19.1.253)
*Mar 1 03:44:57.631: HSRP: Fa0/0 Grp 1 Active router is local, was 172.19.1.253
*Mar 1 03:44:57.635: HSRP: Fa0/0 Nbr 172.19.1.253 no longer active for group 1 (Standby)
*Mar 1 03:44:57.635: HSRP: Fa0/0 Nbr 172.19.1.253 Was active or standby - start passive holddown
*Mar 1 03:44:57.639: HSRP: Fa0/0 Grp 1 Standby router is unknown, was local
*Mar 1 03:44:57.643: HSRP: Fa0/0 Grp 1 Standby -> Active
*Mar 1 03:44:57.643: %HSRP-5-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active
Omurga2#
*Mar 1 03:44:57.643: HSRP: Fa0/0 Interface adv out, Active, active 1 passive 0
*Mar 1 03:44:57.643: HSRP: Fa0/0 Grp 1 Redundancy "hsrp-Fa0/0-1" state Standby -> Active
*Mar 1 03:44:57.647: HSRP: Fa0/0 Grp 1 Hello out 172.19.1.252 Active pri 100 vIP 172.19.1.254
*Mar 1 03:44:57.651: HSRP: Fa0/0 Grp 1 Activating MAC 0000.0c07.ac01
*Mar 1 03:44:57.651: HSRP: Fa0/0 Grp 1 Adding 0000.0c07.ac01 to MAC address filter
*Mar 1 03:44:57.655: HSRP: Fa0/0 IP Redundancy "hsrp-Fa0/0-1" standby, local -> unknown
*Mar 1 03:44:57.659: HSRP: Fa0/0 IP Redundancy "hsrp-Fa0/0-1" update, Standby -> Active
Omurga2#
*Mar 1 03:45:00.647: HSRP: Fa0/0 Grp 1 Hello out 172.19.1.252 Active pri 100 vIP 172.19.1.254
*Mar 1 03:45:00.651: HSRP: Fa0/0 IP Redundancy "hsrp-Fa0/0-1" update, Active -> Active
Omurga2#
*Mar 1 03:45:03.651: HSRP: Fa0/0 Grp 1 Hello out 172.19.1.252 Active pri 100 vIP 172.19.1.254
Omurga2#
*Mar 1 03:45:06.655: HSRP: Fa0/0 Grp 1 Hello out 172.19.1.252 Active pri 100 vIP 172.19.1.254
*Mar 1 03:45:07.323: HSRP: Fa0/0 Grp 1 Hello out 172.19.1.252 Active pri 100 vIP 172.19.1.254

```

**Figür 2.10:** HSRP Omurga2 debug gösterim konfigürasyonu

HSRP mimarisinde yönlendiriciler her 3 saniyede birbirlerine “hello” paketi gönderirler. Omurga 2 ‘nin konfigürasyon çıktısına baktığımızda fas0/0 portuna giren ve çıkan “hello” paketlerini gözlemleyebiliriz. Omurga1’den artık hello paketi gelmediğinde ilk olarak Omurga2 kendini aktif olarak duyurur. Eğer ortamda priority değeri daha yüksek bir yönlendirici yoksa Omurga2 HSRP durum tablosunda aktif olarak rol alır.

Şu an kadar yönlendiricilerin kenar switch’lere bakan tarafındaki yedeklilik durumlarına bakıldı. Peki yönlendiricilerin internete bakan bacağında bir problem olursa durum nasıl olur? İnternete ulaşım kesilse bile, yönlendirici halen çalıştığı için ve kullanıcı tarafına bakan tarafta da herhangi bir problem olmadığı için aktif yönlendirici “hello” paketlerini göndermeye devam edecek ve yedeklilik durumunda bir değişiklik oluşmayacaktır. Bu problemin çözümü için “**tracking**” metodunu kullanacağız. Yönlendiricinin eğer internet tarafındaki portuna zarar gelirse (kablo kopması, interface yanması vs.) priority değerinin düşürülmesi sağlanır. Böylece diğer yönlendiricinin priority değeri daha yüksek olacağı için aktif yönlendirici değişmiş olur ve trafik aksamadan devam eder.



Şekil 2.3 : HSRP tracking işlemi.

```

Omurgal#show running-config interface fastEthernet 0/0
Building configuration...

Current configuration : 220 bytes
!
interface FastEthernet0/0
 ip address 172.19.1.253 255.255.255.0
 duplex auto
 speed auto
 standby 0 preempt
 standby 1 ip 172.19.1.1
 standby 1 priority 150
 standby 1 preempt
 standby 1 track FastEthernet2/0 60
end

```

Figür 2.11: HSRP Omurga1 track konfigürasyonu

“standby 1 track FastEthernet 2/0 60” komutunda eğer fastEthernet2/0 bacağına down olursa priority değerinin 60’a düşürülmesi istenmiştir. Böylece priority değeri  $150 - 60 = 90$  olacaktır. Omurga2 ‘nin priority değeri 100 olduğu için ve bu değer Omurga1 ‘in yeni priority değerinden büyük olduğu için , aktif rolünü Omurga2 üstlenecektir.

Aşağıdaki konfigürasyonda Omurga1 ‘ in Fas2/0 portun çalışır halindeki yedeklilik durumu gösterilmektedir.

```

Omurgal#show standby
FastEthernet0/0 - Group 1
State is Active
  2 state changes, last state change 03:40:43
Virtual IP address is 172.19.1.1
Active virtual MAC address is 0000.0c07.ac01
  Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 2.588 secs
Preemption enabled
Active router is local
Standby router is 172.19.1.252, priority 100 (expires in 7.564 sec)
Priority 150 (configured 150)
  Track interface FastEthernet2/0 state Up decrement 60
Group name is "hsrp-Fa0/0-1" (default)

```

**Figür 2.12:** HSRP Omura1 yedeklilik track öncesi durum gösterim konfigürasyonu

Aşağıdaki konfigürasyonda Omurgal ‘ in Fas2/0 portu down olma halindeki yedeklilik durumu gösterilmektedir.

```

Omurgal#show standby
FastEthernet0/0 - Group 1
State is Standby
  2 state changes, last state change 03:42:21
Virtual IP address is 172.19.1.1
Active virtual MAC address is 0000.0c07.ac01
  Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 1.520 secs
Preemption enabled
Active router is 172.19.1.252, priority 100 (expires in 7.580 sec)
Standby router is local
Priority 90 (configured 150)
  Track interface FastEthernet2/0 state Down decrement 60
Group name is "hsrp-Fa0/0-1" (default)

```

**Figür 2.13:** HSRP Omura1 yedeklilik track sonrası durum gösterim konfigürasyonu

Görüldüğü gibi priority değeri 60’a kadar düşürülmüş ve yönlendirici aktif rolden yedek role geçmiştir.

HSRP mimarisinde yedeklilik işleyişi anlatıldı. Yük dağılımı konfigürasyonunda **HSRP Yük Dağılımı** bölümünde anlatıldığı gibi birden fazla grup oluşturularak yapılabilir.

```

Omurgal#show running-config interface fastEthernet 0/0
Building configuration...

Current configuration : 228 bytes
!
interface FastEthernet0/0
 ip address 172.19.1.253 255.255.255.0
 duplex auto
 speed auto
 standby 0 preempt
 standby 1 ip 172.19.1.1
 standby 1 priority 150
 standby 1 preempt
 standby 2 ip 172.19.1.2
 standby 2 preempt
end

```

**Figür 2.14:** HSRP Omura1 yük dağılımı konfigürasyonu

```
Omurga2#show running-config interface fastEthernet 0/0
Building configuration...

Current configuration : 209 bytes
!
interface FastEthernet0/0
 ip address 172.19.1.252 255.255.255.0
 duplex auto
 speed auto
 standby 1 ip 172.19.1.1
 standby 1 preempt
 standby 2 ip 172.19.1.2
 standby 2 priority 150
 standby 2 preempt
end
```

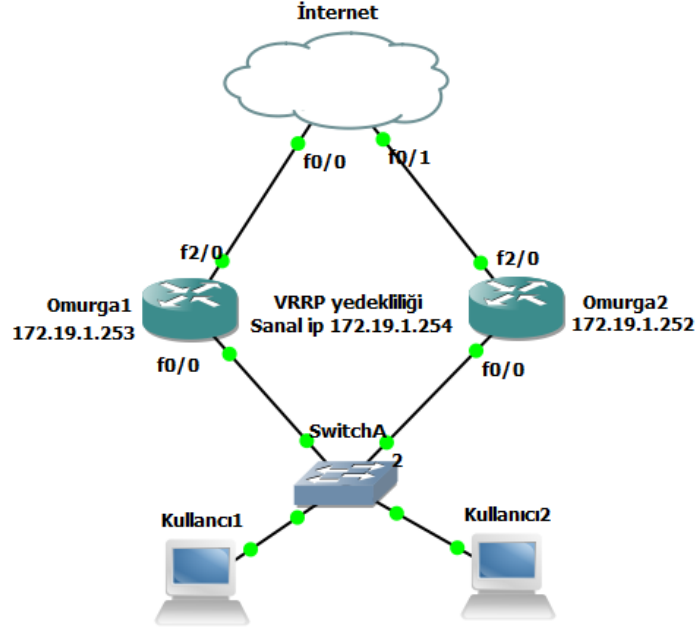
**Figür 2.15:** HSRP Omurga2 yük dağılımı konfigürasyonu

Konfigürasyonlarda görüldüğü gibi 1 ve 2 numaralı iki adet grup oluşturulmuştur. Grup 1 de Omurga1'in priority değeri daha yüksek olduğu için aktif rolünü üstlenecektir. Grup 2'de ise Omurga2'nin priority değeri daha yüksek olduğu için Omurga1 yedek rolünü üstlenecektir. Böylece ağ trafiğinin yarısı Omurga 1'in üzerinden, diğer yarısı ise Omurga 2'nin üzerinden geçecektir. Bu durumda yük dağılımı oranı %50 olur. HSRP de yük dağılımı kontrolü esnek değildir. Vlan bazlı ya da yönlendiricilerin isteğe bağlı olarak herhangi bir oranda yük dağılımı yapması mümkün değildir.

## 2.2 Virtual Router Redundancy Protocol (VRRP)

VRRP teknolojisi IEEE temel alınarak geliştirilmiştir.[13] VRRP, HSRP gibi teknolojilerde olduğu gibi birden fazla yönlendiricinin veya üçüncü seviye bir anahtarlayıcının son kullanıcıya bir tek yönlendirici olarak görünmesi sağlanır. Birden fazla yönlendirici arasında bir tanesi aktif yönlendirme işlemlerini yürütürken diğeri yedek olarak beklemekte ve aktif olan yönlendiriciyi takip etmektedir. Bu konu içerisinde VRRP'nin işleyişinden bahsedildikten sonra, VRRP konfigürasyonunun yönlendiriciler üzerinde nasıl yapıldığı adım adım incelenecektir. Bu bölüm'deki konfigürasyonlar GNS3 simülasyon ortamında yapılmıştır [10]





Şekil 2.4 : VRRP ağ altyapısı.

Şekil 2.4’de görüldüğü gibi bir ağ’ın kendi fiziksel bağlantıları ve ip adresleri olan iki adet yönlendirici tek bir ip adresi ve fiziksel adresi paylaşan, tek bir sanal yönlendirici gibi hareket etmektedir. Son kullanıcılar VRRP protokolünün oluşturduğu sanal yönlendiricinin ip adresini bilirler ve bu ip adresini ağ geçidi olarak tanırlar. Bu bölüm içerisinde VRRP’nin işleyiş kısımlarından bahsedilecek ve emulasyon ortamında yapılan konfigürasyonların gösterimi ve anlatımı yapılacaktır.

VRRP mimarisinde yönlendiricilerden biri “Aktif” (MASTER) durumda çalışırken, diğerleri “yedek” (BACKUP) halde çalışır. VRRP terminolojisinde aktif olarak yönlendirme işlemlerini yapan yönlendirici “Master Router”, yedek olarak bekleyen yönlendirici ise “Backup Router” olarak adlandırılır. Backup görevini üstlenen yönlendirici, paket iletimi ile alakalı herhangi bir yönlendirme işlemi yapmaz. VRRP mimarisinde yönlendiriciler yedekliliğin kurulması için aynı grup içerisinde olmak zorundadır. Yönlendiricilere, grup numarası ağ yöneticisi tarafından verilir. Eğer bir grup numarası belirtilmez ise 0 olarak kabul edilir ve 255’e kadar farklı numaralar verilebilir.

VRRP altyapısında ,HSRP de olduğu gibi arp isteklerine sadece aktif olan cevap verebilir. Yönlendiriciler için belirlenen sanal ip adresine gelen ARP (Adres çözümleme protokolü) isteklerini aktif yönlendirici cevaplar ve gerçek fiziksel adresi

yerine sanal fiziksel adreslerini döner. Sanal fiziksel adresleri ağ yöneticileri tarafından tanımlanmaması durumunda VRRP otomatik olarak sanal bir fiziksel adres üretir. Burada üretilen sanal fiziksel adresi şu şekildedir;

Üretici kodu (00.00.5E) + VRRP (00.01) + Grup numarası

Örneğin, 1 numaralı VRRP grubu içinde sanal fiziksel adres 0000.5E00.0101 olacaktır. İstemci bilgisayarların ARP belleklerine bakıldığında sanal ip ve fiziksel adresleri görülecektir.

Aktif ve yedek yönlendirici 224.0.0.18 multicast ip adresi ve UDP 8888 portu üzerinden birbirlerini “hello” paketlerini 1 saniye aralıklar ile göndererek haberleşirler. Aktif yönlendirici 1 saniye aralıklar ile gönderdiği hello paketlerini, örneğin yönlendiricinin yerel tarafa bakan bacağında kopma olması gibi bir sebepten dolayı 3 saniye boyunca paket gönderemez ise yedek yönlendirici, aktif yönlendirici görevini üstlenir ve paket yönlendirmede başrol oynamaya başlar. Bu nedenden dolayı VRRP teknolojisi, HSRP teknolojisine göre daha hızlı ve daha sağlam yedeklilik sağlar.[13]

### **2.2.1 VRRP Aktif – Yedek Seçimi**

VRRP içerisinde kimin aktif yönlendirici rolünü üstleneceğine **priority** değerleri ile karar verilir. İlk durumda priority değeri her yönlendirici için 100’dür. Eğer priority değerleri ağ yönetici tarafından konfigüre edilmemişse fiziksel ip adresi daha büyük olan yönlendirici aktif, diğeri yedek rolünü üstlenecektir. Eğer özellikle bir yönlendiricinin aktif olması isteniyorsa yönlendiricin priority değeri diğeri yönlendiriciden daha yüksek konfigüre edilir. VRRP’de preempt özelliği, HSRP’de olan preempt özelliğinin aksine başlangıçta açıktır. Aktif rolünde olan bir yönlendirici her saniyede bir kendi fiziksel portundan 224.0.0.18 adresine “hello” paketleri gönderir ve eğer başına bir şey gelme durumunda paket gönderemeyecek olursa belirli bir süre “hello” paketini alamayan diğeri yönlendirici aktif rolünü üstlenecektir. Bu bölümün uygulaması VRRP konfigürasyon bölümünde yapılmıştır.

### **2.2.2 VRRP Yük Dağılımı**

VRRP mimarisinde yük dağılımı, HSRP’deki gibi statiktir [14]. Kullanıcıların yarısı ilk yönlendiriciyi aktif olarak görecektir, kullanıcıların diğeri yarısı ise ikinci yönlendiriciyi aktif olarak görecektir. Bu durumda her iki yönlendirici de hem aktif hem de yedek rolünde çalışmış olacaktır. Burada yapılması gereken X adet VRRP

grubu oluşturmak ve her grup için sanal ip adresi vermektir. Bu bölümün uygulaması VRRP konfigürasyon bölümünde yapılmıştır.

### 2.2.3 VRRP Konfigürasyonu

VRRP mimarisinin daha iyi anlaşılabilmesi için **Şekil 2.2.1** topolojisi kullanılacaktır. Şekilde görüldüğü gibi yedeklilik için **Omurga1** ve **Omurga2** isiminde iki adet yönlendirici kullanılıyor. Yönlendiricilerin kullanıcılara bakan bacalarının konfigürasyonlarına bakacak olursak;

```
Omurga1#show running-config interface fastEthernet 0/0
Building configuration...

Current configuration : 119 bytes
!
interface FastEthernet0/0
 ip address 172.19.1.253 255.255.255.0
 duplex auto
 speed auto
 vrrp 1 ip 172.19.1.1
end
```

**Figür 2.16:** VRRP Omurga1 konfigürasyonu

“vrrp 1 ip 172.19.1.1” buradaki “1” VRRP grup numarası belirtmektedir. “172.19.1.1” ise VRRP sanal ip adresini belirtmektedir.

```
Omurga2#show running-config interface fastEthernet 0/0
Building configuration...

Current configuration : 119 bytes
!
interface FastEthernet0/0
 ip address 172.19.1.254 255.255.255.0
 duplex auto
 speed auto
 vrrp 1 ip 172.19.1.1
end
```

**Figür 2.17:** VRRP Omurga2 konfigürasyonu

“vrrp 1 ip 172.19.1.1” buradaki “1” VRRP grup numarası belirtmektedir. “172.19.1.1” ise VRRP sanal ip adresini belirtmektedir.

Konfigürasyonlarda görüldüğü gibi iki omurga da VRRP 1 numaralı gruba üyelerdir. İki yönlendiriciye de herhangi bir **priority** değeri verilmemiştir. Bu durumda iki omurganın da priority değeri **VRRP Aktif – Yedek Seçimi** bölümünde anlatıldığı gibi 100 dür. Aktif – yedek yönlendirici seçimi bu durumda fiziksel adrese bakılarak yapılır. Fiziksel adresi yüksek olan yönlendirici aktif olur. Aşağıda gösterilen konfigürasyona bakılırsa;

```
Omurga1#show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
Hardware is Gt96k FE, address is c205.18c8.0000 (bia c205.18c8.0000)
Internet address is 172.19.1.253/24
```

**Figür 2.18:** VRRP Omura1 fiziksel adres gösterim konfigurasyonu

```
Omurga2#show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
Hardware is Gt96k FE, address is c206.18c8.0000 (bia c206.18c8.0000)
Internet address is 172.19.1.254/24
```

**Figür 2.19:** VRRP Omura2 fiziksel adres gösterim konfigurasyonu

Omurga2 yönlendiricisinin sahip olduğu fiziksel adres daha büyük olduğundan aktif yönlendirici kendisi olacaktır. Omurga1 ise yedek yönlendirici rolünü üstlenecektir.

```
Omurga1#show vrrp
FastEthernet0/0 - Group 1
State is Backup
Virtual IP address is 172.19.1.1
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 100
Master Router is 172.19.1.254, priority is 100
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec (expires in 2.769 sec)
```

**Figür 2.20:** VRRP Omura1 yedeklilik durum gösterimi konfigurasyonu

Yedeklilik durumu görüldüğü gibi, yönlendirici yedek (Backup) durumundadır. Sanal fiziksel adrese baktığımızda ;

0000.5e00.0101 = Üretici kodu (00.00.5E) + VRRP (00.01) + Grup numarası (01)

Priority değeri konfigürasyonda da görüldüğü gibi 100'dür.

```
Omurga2#show vrrp
FastEthernet0/0 - Group 1
State is Master
Virtual IP address is 172.19.1.1
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 100
Master Router is 172.19.1.254 (local), priority is 100
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec
```

**Figür 2.21:** VRRP Omura1 yedeklilik durum gösterimi konfigurasyonu

Yedeklilik durumu görüldüğü gibi, yönlendirici aktif (Master) durumdadır. Priority değeri konfigürasyonda da görüldüğü gibi 100 dür.

Priority değerlerinin eşit olmasına rağmen Omurga2 yönlendiricisinin aktif olmasının nedeni, Omurga2 yönlendiricisinin gerçek fiziksel adresinin Omurga1'in fiziksel adresinden büyük olmasıdır. Bu topoloji'de aktif yönlendiricinin Omurga1 olması

isteniyorsa, Omurgal yönlendiricisinin VRRP priority değerinin yükseltilmesi gerekmektedir. Bu işlemlerin konfigürasyonları aşağıdaki gibidir.

```
Omurgal(config)#interface fas 0/0
Omurgal(config-if)#vr
Omurgal(config-if)#vrrp 1 pr
Omurgal(config-if)#vrrp 1 pri
Omurgal(config-if)#vrrp 1 priority 150
Omurgal(config-if)#
*Mar 4 08:52:31.255: %VRRP-6-STATECHANGE: Fa0/0 Grp 1 state Backup -> Master
Omurgal(config-if)#
```

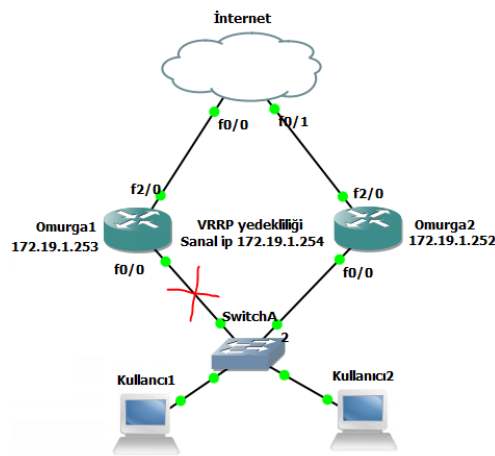
**Figür 2.22:** VRRP Omura1 priority değerini değiştirme konfigürasyonu

VRRP de preempt default da uygulanmış olduğundan herhangi bir priority değişikliğinde yönlendiriciler aktif-pasif seçim sürecini başlatırlar. Yukarıdaki konfigürasyonda görüldüğü gibi Omurgal'in HSRP priority değeri 150 değerine yükseltilmesiyle VRRP durumu yedekten aktife geçmiştir.

```
Omurgal#show vrrp
FastEthernet0/0 - Group 1
  State is Master
  Virtual IP address is 172.19.1.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 150
  Master Router is 172.19.1.253 (local), priority is 150
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.414 sec
```

**Figür 2.23:** VRRP Omura1 yedeklilik durum gösterimi konfigürasyonu

Yönlendiricilerden herhangi birinin zarar görmesi ya da yönlendiricilerin kullanıcılara bakan iletişim kablosunun kopması gibi durumlarda yedekliliğin işleyişi aşağıdaki gibi olmalıdır.



**Şekil 2.5:** VRRP yedeklilik işleyişi.

Şekil 2.5’de görüldüğü gibi aktif yönlendiricinin yerel bacağındaki iletişim kablosunun kopması ya da yönlendiricinin zarar görmesi gibi olumsuz durumlarda Omurga2 aktif rolünü üzerine alacaktır. Emulator ortamında bu işleyişi görebilmek için Omurga1’in **fastEthernet 0/0** bacağını kapalı duruma getirelim. **FastEthernet 0/0** portu shut olduğunda yönlendiricinin bağlantısı kopacağından diğer yönlendirici aktif rolünü üstlenecektir.

```
Omurga1(config)#interface fastEthernet 0/0
Omurga1(config-if)#shu
Omurga1(config-if)#shutdown
Omurga1(config-if)#
*Mar 1 03:42:39.843: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
*Mar 1 03:42:40.843: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
Omurga1(config-if)#
```

**Figür 2.24:** VRRP Omurga1 interface shut etme konfigürasyonu

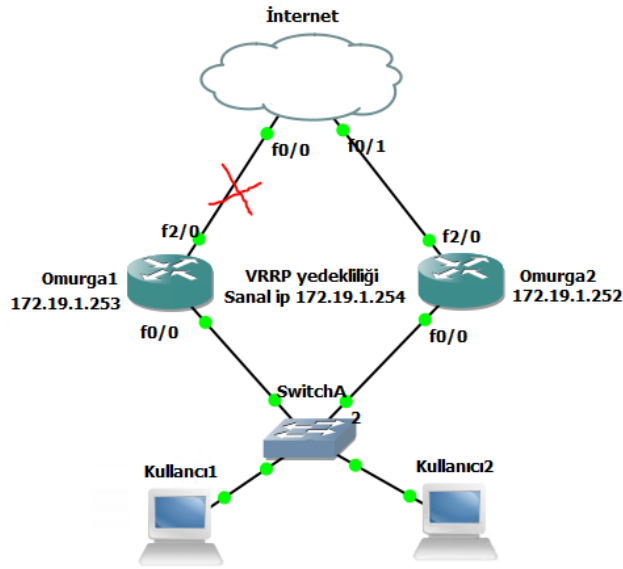
```
Omurga2#
*Mar 4 09:31:42.279: VRRP: Grp 1 Advertisement priority 150, ipaddr 172.19.1.253
*Mar 4 09:31:42.283: VRRP: Grp 1 Event - Advert higher or equal priority
*Mar 4 09:31:43.075: VRRP: Grp 1 Advertisement priority 150, ipaddr 172.19.1.253
*Mar 4 09:31:43.079: VRRP: Grp 1 Event - Advert higher or equal priority
Omurga2#
*Mar 4 09:31:43.763: VRRP: Grp 1 Advertisement priority 0, ipaddr 172.19.1.253
*Mar 4 09:31:43.767: VRRP: Grp 1 Event - Advert priority 0
*Mar 4 09:31:44.383: VRRP: Grp 1 Event - Master down timer expired
*Mar 4 09:31:44.383: %VRRP-6-STATECHANGE: Fa0/0 Grp 1 state Backup -> Master
Omurga2#
*Mar 4 09:31:44.391: VRRP: Grp 1 sending Advertisement checksum CDE7
*Mar 4 09:31:45.355: VRRP: Grp 1 sending Advertisement checksum CDE7
Omurga2#
*Mar 4 09:31:46.199: VRRP: Grp 1 sending Advertisement checksum CDE7
*Mar 4 09:31:47.151: VRRP: Grp 1 sending Advertisement checksum CDE7
Omurga2#
```

**Figür 2.25:** VRRP Omurga2 debug gösterimi konfigürasyonu

VRRP mimarisinde yönlendiriciler her saniyede birbirlerini “hello” paketi gönderirler [15]. Omurga 2’nin konfigürasyon çıktısına baktığımızda fas0/0 bacağına giren ve çıkan hello paketlerini gözlemleyebiliriz. Omurga1’den artık hello paketi gelmediğinde ilk olarak Omurga2 kendini aktif olarak duyurur. Eğer ortamda priority değeri daha yüksek bir yönlendirici yoksa Omurga2 VRRP durum tablosunda aktif olarak rol alır.

Omurga yönlendiricilerin local taraftaki yedekliliğinin VRRP de nasıl sağlandığı anlatıldı. Tam yedekliliğin sağlanması için hem local taraftaki hem Wan taraftaki olumsuz durumlara karşı önlem alınması gerekiyor. VRRP de yönlendiricilerin internete bakan bacağında bir problem olsa bile, yani internete ulaşım kesilse bile, omurga yönlendirici çalışmaya devam ettiği için local tarafına bakan portundan “hello” paketlerini göndermeye devam edecektir. Bu durumda yedeklilik durumunda herhangi bir aktif-pasif değişikliği oluşmayacaktır ve bu ağ trafiğinde probleme yol

açacaktır. Bunu önlemek için HSRP’de de kullandığımız “**tracking**” metodunu kullanacağız. Omurga yönlendiricilere eğer Wan tarafına bakan portlarına erişim kesilirse otomatik olarak priority değerini düşürecek ayarlamalar yapılır. Bu değer diğer yönlendiricinin priority değerinden daha düşük olacak şekilde ayarlanır. Yönlendiriciler priority değeri değiştiği için aktif-pasif seçimi yaparlar ve aktif yönlendirici değişmiş olur. Bu işlemin yapılması trafik herhangi bir kesintiye uğramadan devam etmesini sağlar.



Şekil 2.6: VRRP tracking işlemi.

```
Omurgal(config)#track 1 interface fastEthernet 2/0 li
Omurgal(config)#track 1 interface fastEthernet 2/0 line-protocol
Omurgal(config-track)#exit
Omurgal(config)#inter
Omurgal(config)#interface as
Omurgal(config)#interface fas
Omurgal(config)#interface fastEthernet 0/0
Omurgal(config-if)#vr
Omurgal(config-if)#vrrp 1 tr
Omurgal(config-if)#vrrp 1 track 1 de
Omurgal(config-if)#vrrp 1 track 1 decrement 60
Omurgal(config-if)#end
```

Figür 2.26: VRRP Omura1 track işlemi konfigürasyonu

“vrrp 1 track 1 decrement 60” komutunda eğer fastEthernet2/0 bacağına down olursa priority değerinin 60’a düşürülmesi istenmiştir. Böylece priority değeri 150-60 = 90 olacaktır.

Fas2/0 çalışır durumunda olduğunda ağ konfigürasyonu aşağıdaki gibidir.

```

Omurgal#show vrrp
FastEthernet0/0 - Group 1
  State is Master
  Virtual IP address is 172.19.1.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 150
    Track object 1 state Up decrement 60
  Master Router is 172.19.1.253 (local), priority is 150
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.414 sec

```

**Figür 2.27:** VRRP Omura1 track öncesi yedeklilik durum gösterimi konfigürasyonu Fas2/0 bağlantısı koptuğunda;

```

Omurgal(config-if)#
*Mar 4 09:58:38.899: VRRP: Grp 1 sending Advertisement checksum 9BE7
*Mar 4 09:58:39.059: %TRACKING-5-STATE: 1 interface Fa2/0 line-protocol Up->Down
Omurgal(config-if)#
*Mar 4 09:58:39.783: VRRP: Grp 1 sending Advertisement checksum D7E7
*Mar 4 09:58:40.643: VRRP: Grp 1 sending Advertisement checksum D7E7
Omurgal(config-if)#

```

**Figür 2.28:** VRRP Omura1 interface shut olma debug gösterimi konfigürasyonu

```

Omurgal#show vrrp
FastEthernet0/0 - Group 1
  State is Backup
  Virtual IP address is 172.19.1.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 90 (cfgd 150)
    Track object 1 state Down decrement 60
  Master Router is 172.19.1.254, priority is 100
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.414 sec (expires in 2.782 sec)

```

**Figür 2.29:** VRRP Omura1 track sonrası yedeklilik durum gösterimi konfigürasyonu Görüldüğü gibi priority değeri 60'a kadar düşürülmüş ve yönlendirici aktif rolden yedek role geçmiştir.

VRRP mimarisinde yedeklilik işleyişi anlatıldı. Yük dağılımı konfigürasyonunda **VRRP Yük Dağılımı** bölümünde anlatıldığı gibi birden fazla grup oluşturarak yapılabilir.



```
Omurga1#show running-config interface fastEthernet 0/0
Building configuration...

Current configuration : 162 bytes
!
interface FastEthernet0/0
 ip address 172.19.1.253 255.255.255.0
 duplex auto
 speed auto
 vrrp 1 ip 172.19.1.1
 vrrp 1 priority 150
 vrrp 2 ip 172.19.1.2
end
```

**Figür 2.30:** VRRP Omura1 yük dağılımı gösterimi konfigürasyonu

```
Omurga2#show running-config interface fastEthernet 0/0
Building configuration...

Current configuration : 162 bytes
!
interface FastEthernet0/0
 ip address 172.19.1.254 255.255.255.0
 duplex auto
 speed auto
 vrrp 1 ip 172.19.1.1
 vrrp 2 ip 172.19.1.2
 vrrp 2 priority 150
end
```

**Figür 2.31:** VRRP Omura2 yük dağılımı gösterimi konfigürasyonu

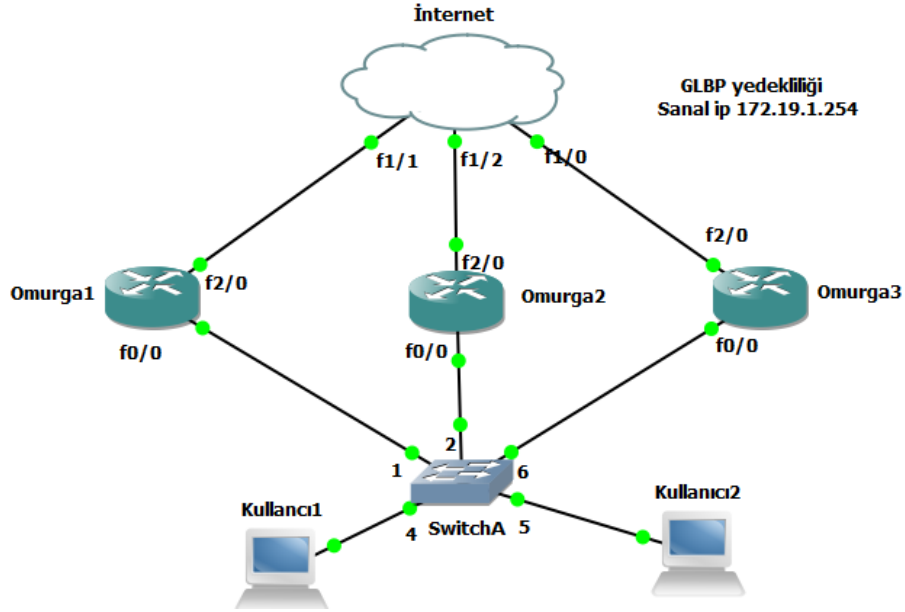
Konfigürasyonlarda görüldüğü gibi 1 ve 2 numaralı iki adet grup oluşturulmuştur. Grup 1’de Omurga1’in priority değeri daha yüksek olduğu için aktif rolünü üstlenecektir. Grup 2’de ise Omurga2’nin priority değeri daha yüksek olduğu için yedek rolünü üstlenecektir. Böylece trafiğin yarısı Omurga 1’in üzerinden, diğer yarısı ise Omurga 2’nin üzerinden geçecektir. %50 yük dağılımı söz konusudur. VRRP’de, HSRP’de olduğu gibi yük dağılımı kontrolü esnek değildir. Vlan bazlı ya da yönlendiricilerin isteğe bağlı olarak herhangi bir oranda yük dağılımı yapmak mümkün değildir.

## 2.3 Gateway Load Balancing Protocol (GLBP)

GLBP, diğer protokollere göre (HSRP,VRRP) daha verimli ve etkilidir [16]. HSRP ve VRRP teknolojilerinde yönlendiriciler yedeklilik açısından aktif-pasif rollerini yaparken, GLBP aktif-aktif olarak çalışabilir .

GLBP, diğer iki protokol gibi birden fazla yönlendiricinin veya üçüncü seviye bir anahtarlayıcının son kullanıcıya bir tek yönlendirici olarak görünmesini sağlar, lakin çalışma stratejisi diğer protokollere göre birçok açıdan farklılık gösterir. HSRP ve VRRP teknolojilerinde birden fazla yönlendirici arasında bir tanesi aktif yönlendirme işlemlerini yürütürken diğeri yedek olarak beklemekte ve aktif olan yönlendiriciyi takip etmekteyken bu durum GLBP’de daha farklıdır. Omurgadaki bütün

yönlendiriciler aktif-aktif olarak çalışabilmektedir. Bu konu içerisinde GLBP'nin işleyişinden bahsedildikten sonra, GLBP konfigürasyonunun yönlendiriciler üzerinde nasıl yapıldığını adım adım inceleyeceğiz. Bu bölümdeki konfigürasyonlar GNS3 emülatör ortamında yapılmıştır [10].



Şekil 2.7: GLBP ağ altyapısı.

Şekil 2.7'de görüldüğü gibi kendi fiziksel bağlantıları ve ip adresleri olan üç adet yönlendirici tek bir yönlendirici gibi hareket etmektedir. Diğer protokollerde olduğu gibi GLBP de aynı şekilde sanal (virtual) ip adres mantığı ile hareket etmektedir. Yönlendiricilerin kendine ait bir ip adresi olmasına rağmen kullanıcılarla sanal ip adresleri ile haberleşirler. Son kullanıcılar GLBP protokolünün oluşturduğu sanal yönlendiricinin ip adresini bilirler ve bu ip adresini ağ geçidi olarak tanırlar. HSRP ve VRRP'de bir adet sanal fiziksel adres olurken, GLBP'de bu durum farklıdır. GLBP'de yönlendirici sayısı kadar sanal ip adres oluşturulur ve her yönlendirici kendi sanal fiziksel ip adresiyle arp paketlerine cevap döner. Sanal fiziksel adreslerin oluşması ve haberleşme mimarisi ileriki bölümlerde anlatılacaktır. Bu bölüm içerisinde GLBP'nin işleyiş kısımlarından bahsedilecek ve emülatör ortamında yapılan konfigürasyonların gösterimi anlatılacaktır.

GLBP mimarisinde diğer teknolojilerde olduğu gibi yönlendiricilerin üye olduğu gruplar vardır. GLBP'de 1024 adet grup oluşturulabilir. Her grup içerisinde "Aktif Sanal Ağ Geçiti" **AVG** seçilir. Dışardan gelen istekler ilk olarak AVG olan yönlendiriciye gelir. AVG olan yönlendirici grubun yöneticisi konumundadır. AVG

rolünü üsteleneen yönlendirici üç adet sanal fiziksel adres oluşturur (Topolojimizde üç adet yönlendirici olduğu için üç adet kullanıldı.) Toplamda en fazla 4 adet sanal fiziksel adres oluşturulabilir. Gruptaki diğer yönlendiricilere “Aktif Sanal Yönlendiriciler” **AVF** denir. AVG de aynı zamanda bir AVF’dir. Oluşturulan sanal fiziksel adresler bu AVF’lere atanır. Bu AVF’ler kendilerine atanan sanal fiziksel adreslere gelen paketlere cevap verirler. Üst limit olarak dört adet sanal fiziksel adres oluşturulabildiği için AVG dâhil, grupta en fazla dört adet aktif olarak çalışan yönlendirici olabilir. Eğer grupta dörtten fazla yönlendirici mevcut ise AVF olmayan yönlendiriciler yedek durumda beklerler ve gelen paketlere herhangi bir cevap dönmezler. Her bir AVF kendisine atanan sanal fiziksel adres için birinci öncelikli sanal yönlendirici (Primary Virtual Forwarder)’dir. Bu yönlendirici aynı GLBP grubu içerisindeki diğer yönlendiricilere bu sanal fiziksel adres için kendisinin cevap vereceğini duyurur. Bu sanal fiziksel adres için ikinci öncelikli sanal yönlendirici (Secondary Virtual Forwarder) vardır ve yönlendirici birinci öncelikli olarak sanal yönlendiriciye ulaşamazsa onun yerine cevap verir.

GLBP mimarisinde yönlendiriciler yedekliliğin kurulması için aynı grup içerisinde olmak zorundadır [17]. Yönlendiricilere grup numarası ağ yöneticisi tarafından verilir. Eğer bir grup numarası belirtilmez ise 0 olarak kabul edilir ve 1024’e kadar numaralar kullanılır.

Sanal yönlendiricilere ağ yöneticisi tarafından atanan sanal ip adresine gelen ARP (Adres çözümüleme protokolü) isteklerini AVG cevaplar ve cevap olarak gerçek fiziksel adresi yerine oluşturulan üç adet sanal fiziksel adresten birini döner. Sanal fiziksel adresleri ağ yöneticileri tarafından tanımlanmaması durumunda GLBP otomatik olarak sanal bir fiziksel adres üretir.

Burada üretilen GLBP sanal fiziksel adresi şu şekildedir;

Üretici kodu (00.07.B4) + GLBP (00) + Grup numarası + AVF no

Örneğin 1 numaralı GBPP grubu için AVG’nin sanal fiziksel adresi 0007.B400.0101 olacaktır. Diğer AVF’ler için 0007.B400.0102 ve 0007.B400.0103 olur. AVF’ler için oluşturulan sanal fiziksel adresler yönlendiricilerin aynı zamanda kimlik numaraları olur. İstemci bilgisayarların ARP belleklerine bakıldığında sanal ip ve fiziksel adresleri görülecektir.

Aktif ve yedek yönlendirici 224.0.0.102 multicast ip adresi ve UDP 3222 portu üzerinden birbirlerini “hello” paketlerini 1 saniye aralıklar ile göndererek haberleşirler. Aktif yönlendiriciler üç saniye aralıklar ile gönderdiği hello paketlerini, örneğin yönlendiricinin yerel tarafa bakan iletişim bacağının kopması durumunda ve 10 saniye boyunca yerel tarafa paket gönderemez ise yedek yönlendiriciler, aktif yönlendiricinin görevini üstlenir. Bu durum için, GLBP teknolojisi, HSRP ve VRRP ye göre daha hızlı ve daha sağlam yedeklilik sağlar [18].

### 2.3.1 GLBP Aktif – Yedek Seçimi

GLBP mimarisinde diğer protokollerde olduğu gibi rol seçimi **priority** değerleri ile karar verilir [17]. İlk durumda priority değeri her yönlendirici için 100’dür. Eğer priority değerleri ağ yöneticisi tarafından konfigüre edilmemişse fiziksel ip adresi daha büyük olan yönlendirici AVG, diğeri yedek rolünü üstlenecektir. Eğer özellikle bir yönlendiricinin AVG olmasını isteniyorsa yönlendiricin priority değeri diğer yönlendiriciden daha yüksek bir değer olarak konfigüre edilir. Burada önemli bir husus vardır. Eğer “preemt” aktif edilmemişse sisteme ilk katılan yönlendirici aktif rol alır. Bu adaletli bir seçim olmaz. Bundan dolayı “preemt” aktif edilmelidir. Bu her zaman seçimin adaletli olmasını sağlar. Aktif rolünde olan bir yönlendirici her üç saniyede bir kendi fiziksel bacağında 224.0.0.102 adresine “hello” paketlerini gönderir ve eğer başına bir şey gelir de gönderemeyecek olursa belirli bir süre “hello” paketini alamayan diğer yönlendirici aktif rolünü üstlenecektir. AVG grupta bulunan diğer yönlendiricileri kendisi de dâhil sanal kimlik fiziksel adresleri üretir ve bu AVF rolünü üstlenen yönlendiricilerin her biri kendi sanal fiziksel kimlik adresleri için aktif olarak çalışır. GLBP grubu içinde en fazla dört adet AVF olabilir. Diğer yönlendiriciler yedek durumunda çalışır ve AVF’lerin durumunu takip eder. Grup içerisinde bir AVF’nin down olması halinde AVG 600 saniye (redirect time) içerisinde secondary virtual router’a görev değişikliğini iletir. İkinci süreç ise “secondary hold timer”dır. Bu süre default olarak 14.400 saniyedir ve bu süre dolduğunda AVG down olan AVF’ye ait sanal kimlik fiziksel adresinin artık olmadığını duyurur. Bu bölümün uygulaması GLBP konfigürasyon bölümünde yapılmıştır.

### 2.3.2 GLBP Yük Dağılımı

GLBP mimarisinde yük dağılımı dinamiktir ve 3 farklı yöntem vardır [16] Bu yöntemleri sırayla inceleyim;

- **Round Robin** : Default olan yöntemdir. Protokol olarak HSRP ve VRRP gibi çalışır. Gelen paketler sırasıyla AVF'lere dağıtılır. [16]
- **Host Depented** : Host – yönlendirici bazlı çalışır. Kullanıcılar AVF'lere atanır. Belli bir host hep aynı AVF'nin sanal fiziksel adresini tanır. Küçük ağlarda tavsiye edilmez. [16]
- **Weighted** : Dinamik olan bir metottur. Bu yöntemde AVF'ye ne kadar yük taşınması gerektiği söylenebilir. Böylece güçlü olan AVF'ler daha fazla yük taşıyabilirler. [16]

Bu bölümün uygulaması GLBP konfigürasyon bölümünde yapılmıştır.

### 2.3.3 GLBP Konfigürasyonu

GLBP mimarisinin daha iyi anlaşılabilmesi için **Şekil 3.2.1** topolojisi kullanılacaktır. Şekilde görüldüğü gibi yedeklilik için **Omurga1, Omurga2** ve **Omurga3** isminde üç adet yönlendirici kullanılıyor. Yönlendiricilerin kullanıcılara bakan bacalarının konfigürasyonlarına bakacak olursak;

```
Omurga1#show running-config interface fastEthernet 0/0
Building configuration...

Current configuration : 260 bytes
!
interface FastEthernet0/0
 ip address 172.19.1.1 255.255.255.0
 duplex auto
 speed auto
 glbp 1 ip 172.19.1.254
 glbp 1 priority 110
 glbp 1 preempt
 glbp 1 weighting 70
 glbp 1 load-balancing weighted
 glbp 1 authentication md5 key-string numankarakas
end
```

**Figür 2.32:** GLBP Omura1 konfigürasyonu

“glbp 1 ip 172.19.1.254” buradaki “1” GLBP grup numarasını belirtmektedir. “172.19.1.254” ise GLBP sanal ip adresini belirtmektedir.

“**glbp 1 priority 110**” burada priority değeri 110 olarak manuel belirlendi.

“**glbp 1 preempt**” burada seçimin olmasını aktif olarak girildi.

“**glbp 1 load balancing weighted**” burada load balancing seçiminin weighted stratejisiyle olması istendi.

“**glbp 1 weighting 70**” burada weighting değerini 70 olarak belirtildi.

“**glbp 1 authentication md5 key-string numankarakas**” burada authentication şifresi olarak “numankarakas” belirlendi.

```
Omurga2#show running-config interface fastEthernet 0/0
Building configuration...

Current configuration : 239 bytes
!
interface FastEthernet0/0
 ip address 172.19.1.2 255.255.255.0
 duplex auto
 speed auto
 glbp 1 ip 172.19.1.254
 glbp 1 preempt
 glbp 1 weighting 20
 glbp 1 load-balancing weighted
 glbp 1 authentication md5 key-string numankarakas
end
```

**Figür 2.33:** GLBP Omura2 konfigürasyonu

“**glbp 1 ip 172.19.1.254**” buradaki “1” GLBP grup numarasını belirtmektedir. “172.19.1.254” ise GLBP sanal ip adresini belirtmektedir.

Priority değerini belirtilmediği için default olarak 100 atanır.

“**glbp 1 preempt**” burada seçimin olması aktif yapıldı.

“**glbp 1 load balancing weighted**” burada load balancing seçiminin weighted stratejisiyle olması istendi.

“**glbp 1 weighting 20**” burada weighting değerini 20 olarak belirtildi.

“**glbp 1 authentication md5 key-string numankarakas**” burada authentication şifresi olarak “numankarakas” belirlendi.

```
Omurga3#show running-config interface fastEthernet 0/0
Building configuration...

Current configuration : 259 bytes
!
interface FastEthernet0/0
 ip address 172.19.1.3 255.255.255.0
 duplex auto
 speed auto
 glbp 1 ip 172.19.1.254
 glbp 1 priority 90
 glbp 1 preempt
 glbp 1 weighting 10
 glbp 1 load-balancing weighted
 glbp 1 authentication md5 key-string numankarakas
end
```

**Figür 2.34:** GLBP Omura3 konfigürasyonu

“**glbp 1 ip 172.19.1.254**” buradaki “**1**” GLBP grup numarası belirtmektedir. “**172.19.1.254**” ise GLBP sanal ip adresini belirtmektedir.

“**glbp 1 priority 90**” burada priority değerini 90 olarak manuel olarak belirlendi.

“**glbp 1 preempt**” burada seçimin olması aktif yapıldı.

“**glbp 1 load balancing weighted**” burada load balancing seçiminin weighted stratejisiyle olması istendi.

“**glbp 1 weighting 10**” burada weighting değerini 10 olarak belirtildi.

“**glbp 1 authentication md5 key-string numankarakas**” burada authentication şifresi olarak “numankarakas” belirlendi.

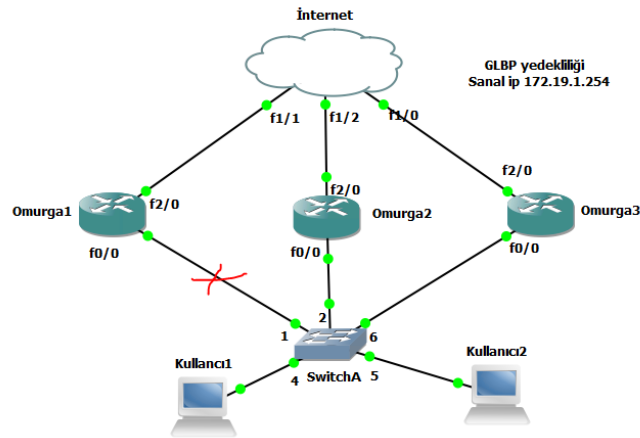
Konfigürasyonlara bakıldığında 3 yönlendirici de GLBP 1 numaralı grubuna üyeler ve sanal ip adresi olarak 172.19.1.254 ayarlanmış. Kullanıcılar ağ geçidi olarak 172.19.1.254 ip adresini tanırlar. Priority değerlerini bakıldığında Omurga1 yönlendiricisinin en yüksek değere sahip olduğu görülür ve bu durumda AVG rolünü Omurga1 yürütür. AVG de aynı zamanda AVF rolünde olduğu için 3 yönlendirici de aktif olarak trafiği AVF olarak iletir. AVG nin yedek durumuna bakıldığında bu rolü Omurga2 üstelenir. Rol durumları aşağıdaki gibidir;

Omurga	AVG	Yedek AVG	AVF
Omurga1	+		+
Omurga2		+	+
Omurga3			+

**Tablo 2.1:** GLBP topolojisinde rol paylaşımları

Yukarıdaki tabloda **Şekil 2.1** deki GLBP ağ altyapısında yönlendiricilerin rolleri gösterilmiştir. Omurga1 AVG ve AVF olarak çalışmakta , Omurga2 yedek AVG ve AVF olarak çalışmakta ve Omurga3 sadece AVF olarak çalışmaktadır.

Yönlendiricilerden herhangi birinin zarar görmesi ya da yönlendiricilerin kullanıcılara bakan kablusunun kopması gibi durumlarda yedekliliğin işleyişi aşağıdaki gibidir.



**Şekil 2.8:** GLBP yedeklilik işleyişi.

**Şekil 2.8**'de görüldüğü gibi AVG yönlendiricisinin yerel bacağındaki kablonun kopmasıyla ya da yönlendiricinin kendisinin zarar görmesi durumlarında Omurga2 priority değeri olarak Omurga3'den büyük olduğu için aktif rolünü üzerine alacaktır. Emulator ortamında bu işleyişi görebilmek için Omurga1'in **fastEthernet 0/0** portunun erişimini keselim. Bu işlemi **fastEthernet 0/0** interface 'inin altında "**shutdown**" komutuyla yapabiliriz.

```

Omurga1(config)#interface fastEthernet 0/0
Omurga1(config-if)#shu
Omurga1(config-if)#shutdown
Omurga1(config-if)#
*Mar 17 06:08:02.863: %GLBP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Active -> Init
Omurga1(config-if)#
*Mar 17 06:08:04.859: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
*Mar 17 06:08:05.859: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down

```

**Figür 2.35:** GLBP Omurga1 interface shut etme konfigürasyonu



```

Omurga2#undebg all
*Mar 17 06:20:01.011: GLBP: Fa0/0 Grp 1 Hello in VG Active pri 110 vIP 172.19.1.254 hello 3000, hold 10000 VF 2 Active pri 167 vMAC 0007.b400.0102
*Mar 17 06:20:01.903: GLBP: Fa0/0 Grp 1 Hello in VG Listen pri 90 vIP 172.19.1.254 hello 3000, hold 10000 VF 1 Active pri 167 vMAC 0007.b400.0101
*Mar 17 06:20:02.007: GLBP: Fa0/0 Grp 1 Hello out VG Standby pri 100 vIP 172.19.1.254 hello 3000, hold 10000 VF 3 Active pri 167 vMAC 0007.b400.0103
Omurga2#undebg all
All possible debugging has been turned off
Omurga2#debug glbp events
GLBP Events debugging is on
Omurga2#
*Mar 17 06:20:23.015: GLBP: Fa0/0 1 Standby: g/Active timer expired (172.19.1.1)
*Mar 17 06:20:23.019: GLBP: Fa0/0 1 Active router IP is local, was 172.19.1.1
*Mar 17 06:20:23.023: GLBP: Fa0/0 1 Standby router is unknown, was local
*Mar 17 06:20:23.023: GLBP: Fa0/0 1 Standby -> Active
*Mar 17 06:20:23.023: %GLBP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active
*Mar 17 06:20:23.031: GLBP: Fa0/0 1.2 Listen: g/Active timer expired
*Mar 17 06:20:23.031: GLBP: Fa0/0 1.2 Listen -> Active
*Mar 17 06:20:23.035: %GLBP-6-FWDSTATECHANGE: FastEthernet0/0 Grp 1 Fwd 2 state Listen -> Active
*Mar 17 06:20:23.051: GLBP: Fa0/0 1.2 Active: i/Hello rcvd from higher pri Active router (135/172.19.1.3)
*Mar 17 06:20:23.051: GLBP: Fa0/0 1.2 Active -> Listen
*Mar 17 06:20:23.055: %GLBP-6-FWDSTATECHANGE: FastEthernet0/0 Grp 1 Fwd 2 state Active -> Listen
Omurga2#
*Mar 17 06:20:23.059: GLBP: Fa0/0 API MAC address update
Omurga2#
*Mar 17 06:20:43.059: GLBP: Fa0/0 1 Standby router is 172.19.1.3

```

**Figür 2.36:** GLBP Omurga2 debug gösterim konfigürasyonu

```

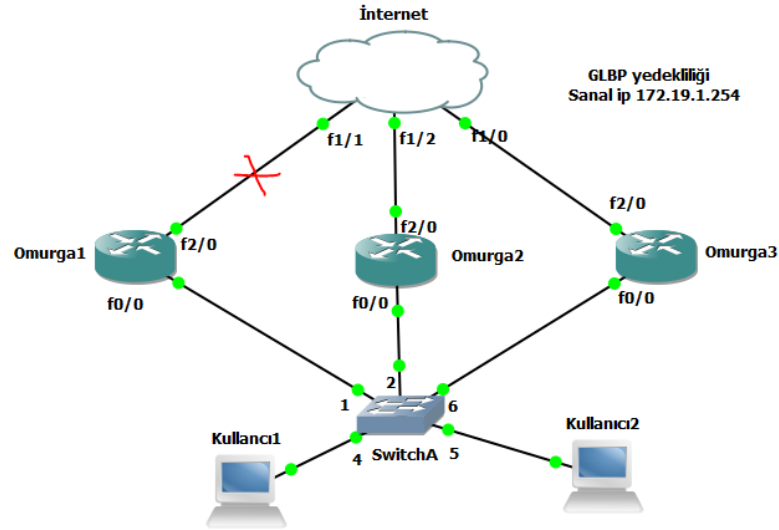
Omurga3#debug glbp packets
GLBP Packets debugging is on
Omurga3#debug glbp events
*Mar 8 11:25:38.251: GLBP: Fa0/0 Grp 1 Hello in VG Standby pri 100 vIP 172.19.1.254 hello 3000, hold 10000 VF 3 Active
*Mar 8 11:25:39.139: GLBP: Fa0/0 Grp 1 Hello out VG Listen pri 90 vIP 172.19.1.254 hello 3000, hold 10000 VF 1 Active
Omurga3#undebg all
All possible debugging has been turned off
Omurga3#
*Mar 8 11:25:40.175: GLBP: Fa0/0 Grp 1 Hello in VG Active pri 110 vIP 172.19.1.254 hello 3000, hold 10000 VF 2 Active
Omurga3#debug glbp events
GLBP Events debugging is on
Omurga3#
*Mar 8 11:25:59.187: GLBP: Fa0/0 1 Listen: g/Active timer expired (172.19.1.1)
*Mar 8 11:25:59.187: GLBP: Fa0/0 1 Active router IP is unknown, was 172.19.1.1
*Mar 8 11:25:59.187: GLBP: Fa0/0 1 Listen -> Speak
*Mar 8 11:25:59.191: GLBP: Fa0/0 1.2 Listen: g/Active timer expired
*Mar 8 11:25:59.191: GLBP: Fa0/0 1.2 Listen -> Active
*Mar 8 11:25:59.191: %GLBP-6-FWDSTATECHANGE: FastEthernet0/0 Grp 1 Fwd 2 state Listen -> Active
Omurga3#
*Mar 8 11:25:59.255: GLBP: Fa0/0 1 Active router IP is 172.19.1.2
*Mar 8 11:25:59.255: GLBP: Fa0/0 1 Standby router is unknown, was 172.19.1.2
*Mar 8 11:25:59.259: GLBP: Fa0/0 1.2 Active: j/Hello rcvd from lower pri Active router (135/172.19.1.2)
Omurga3#
*Mar 8 11:26:09.187: GLBP: Fa0/0 1 Speak: f/Standby timer expired (unknown)
*Mar 8 11:26:09.187: GLBP: Fa0/0 1 Standby router is local
*Mar 8 11:26:09.187: GLBP: Fa0/0 1 Speak -> Standby
Omurga3#

```

**Figür 2.37:** GLBP Omurga3 debug gösterim konfigürasyonu

Konfigürasyonlarda görüldüğü gibi GLBP mimarisinde yönlendiriciler her üç saniyede birbirlerine “hello” paketi gönderirler. Omurga1, Omurga2 ve Omurga3’un konfigürasyon çıktıklarına baktığımızda fas0/0 bacağına giren ve çıkan hello paketlerini gözlemleyebiliriz. Omurga1’den artık hello paketi gelmediğinde ilk olarak Omurga2 ve Omurga3 yönlendiricileri yeni rolleri için paket alışverişinde bulunur ve Omurga2’nin priority değeri daha büyük olmasından dolayı (100>90), Omurga2 kendini aktif olarak otomatik atar. Omurga3 ise standby görevini üstlenir.

GLBP de yönlendiricilerin local portlarının ve ya cihazların kendilerinin kesintiye uğraması durumunda yedekliliğin işleyişi anlatıldı. Yedekliliğin tam verimli şekilde sağlanması için yönlendiricilerin Wan portlarının da kesintiye uğraması durumunda yedeklilik durumlarını kontrol etmesi gerekmektedir. Yönlendiricilerin internete bakan portunda bir problem olursa internete ulaşım kesilse bile, yönlendirici halen çalıştığı için ve kullanıcı tarafına bakan tarafta da herhangi bir problem olmadığı için aktif yönlendirici “hello” paketlerini göndermeye devam edecek ve yedeklilik durumunda bir değişiklik oluşmayacaktır. Bu problemin çözümü için HSRP ve VRRP de olduğu gibi “**tracking**” metodunu kullanacağız. HSRP ve VRRP de, yönlendiriciye eğer internet tarafındaki bacağına zarar gelirse (kablo kopması, interface yanması vs.) priority değeri düşür denilirdi. Lakin GLBP de bu durum farklıdır. Böyle durumla karşılaşıldığında priority değeriyle ilgili bir değişiklik olmaz. Bunun yerine weight değerinin üzerinde değişiklik yapılır. Böylece yönlendiriciler arasında rol değişikliği olmasına gerek kalmaz. Yeni weight değerlerine göre yük dağılımı hesaplanır ve trafik kesintiye uğramaz.



Şekil 2.9: GLBP tracking işleyişi

```
Omurga1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Omurga1(config)#track 1 interface fastEthernet 2/0 line-protocol
```

Figür 2.38: GLBP Omura1 track işlemi konfigürasyonu

Burada track 1'in fastEthernet2/0 izlemesini sağladık. Ayrıca GLBP de aynı anda 500 adet interface izleyebilir. Bunu sağlamak için de her bir interface için track nesnesi oluşturmamız gerekir. Bu interface aşağıdaki gibi oluşturulur;

```
Omurgal(config)#
Omurgal(config)#interface fastEthernet 0/0
Omurgal(config-if)#glbp 1 weighting track 1 decrement 70
```

**Figür 2.39:** GLBP Omurga1 weighting track işlemi konfigürasyonu

Burada track 1 nesnesini omurgal yönlendiricisinin local tarafındaki interface'ine uyguladık. Bu konfigürasyon içerisinde eğer Omurgal'in internet tarafındaki interface'ine bir zarar gelirse weight değerini 70 azaltmasını sağlar. Böylece weight değeri 70 olan omurgal'in yeni weight değeri  $70-70 = 0$  olur. Burada dikkat edilmesi gereken bir husus var. Omurgal'in priority değeri değişmiyor yani AVG rolüne devam ediyor ama weight değeri 0 olduğu için AVF rolünü yapamadığı için üzerinden paket trafiği geçmiyor. Böylece herhangi bir veri kaybı olmadan ağ veya paket trafiği kesintisiz olarak devam ediyor.

Bu senaryoyu emulator ortamında aşağıdaki gibi gösterirsek;

```
Omurgal(config)#interface fastEthernet 2/0
Omurgal(config-if)#shu
Omurgal(config-if)#shutdown
Omurgal(config-if)#
*Apr 10 20:40:17.644: %TRACKING-5-STATE: 1 interface Fa2/0 line-protocol Up->Down
Omurgal(config-if)#
*Apr 10 20:40:17.648: GLBP: Fa0/0 1 Track 1 object changed, state Up -> Down
*Apr 10 20:40:17.648: GLBP: Fa0/0 1 Weighting 70 -> 0
```

**Figür 2.40:** GLBP Omurga1 interface shut etme konfigürasyonu

Görüldüğü gibi FastEthernet2/0'ın bağlantısı kopması durumunda Omurgal'in yeni weight değeri 70 azalarak 0 oluyor.

```
Omurgal#show glbp
FastEthernet0/0 - Group 1
  State is Active
    16 state changes, last state change 00:35:23
  Virtual IP address is 172.19.1.254
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.168 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Authentication MD5, key-string "numankarakas"
  Preemption enabled, min delay 0 sec
  Active is local
  Standby is 172.19.1.2, priority 100 (expires in 8.908 sec)
  Priority 110 (configured)
  Weighting 0, low (configured 70), thresholds: lower 1, upper 70
  Track object 1 state Down decrement 70
  Load balancing: weighted
```

**Figür 2.41:** GLBP Omurga1 track işlemi sonrası yedeklilik gösterim konfigürasyonu

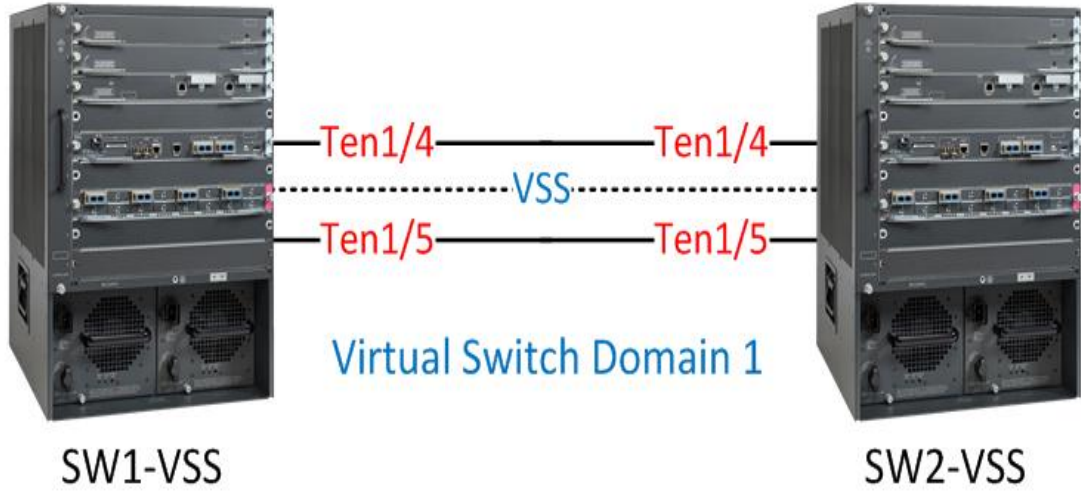
Konfigurasyon'da görüldüğü gibi Omurgal Aktif (AVG) olarak devam ediyor. FastEthernet2/0'ın bağlantısının kopması AVF rolünü kaybettiriyor. Omurgal'in sorumlu olduğu sanal fiziksel adrese gelen isteklere ise Redirect Timer süresince başka yönlendirici cevap verecektir.

## **3.YENİ NESİL TEKNOLOJİLER**

Veri merkezlerinde, ağ cihazları ve bağlantılarını çift yapılandırarak ağ güvenilirliği artırılabilir. [19] Yedekli ağ elemanları ve bağlantıları arttıkça network kablolu ve yapı karmaşıklığı da artar [20] Bunu önlemek amaçlı yeni teknolojiler geliştirilmiştir. Bu teknolojiler sanal anahtarlama şebeke elemanlarının sayısını azaltarak ve gereksiz anahtarları ve bağlantıları yönetme karmaşıklığını gizleyerek ağ yapısını ve haberleşmeyi kolaylaştırır ve kenar anahtarlamalarda herhangi bir sonsuz döngü olmasına müsaade etmeden bütün uplink portlarının aktif olarak çalışmasını sağlar.

### **3.1 VIRTUAL SWITCHING SYSTEM (VSS)**

VSS teknolojisi önceki teknolojilerde olduğu gibi birden fazla yönlendiricinin veya üçüncü seviye bir anahtarlayıcının son kullanıcıya bir tek yönlendirici olarak görünmesini sağlar [21]. Lakin buradaki işlevsellik çok farklıdır. VSS'de birden farklı yönlendirici sanal olarak değil, gerçek anlamda tek bir yönlendirici haline gelir ve bu stack bağlantı metodu ile sağlanır. [22] Bu konu içerisinde VSS'nin işleyişinden bahsedildikten sonra, VSS konfigürasyonunun yönlendiriciler üzerinde nasıl yapıldığını adım adım inceleyeceğiz. Bu bölümdeki konfigürasyonlar gerçek ortamda yapılmıştır.



Şekil 3.1: VSS ağ altyapısı.

Şekil 3.1 de görüldüğü gibi iki ayrı yönlendiricinin birbirlerine TenGig modül ile bağlanması sonucu tek bir yönlendirici haline gelmesi sürecini adım adım inceleyeceğiz. Öncelikle omurgada konum alan yönlendiricileri inceleyelim.

Omurga yönlendiricileri data-plane ve control-plane olmak üzere ikiye ayrılır [23];

**Control-Plane:** Cihaz üzerindeki yönetimin, paket yol belirlenmesinin ve konfigürasyonun yapıldığı yerdir. Bu rolü üstlenen modüle supervisor denir.

**Data-Plane :** Cihaz üzerinde paket trafiğinin taşındığı ve iletiildiği kısımdır. Bu rolü üstlenen modüllere line-card denir. Bunlar GigaEthernet veya TenGigaEthernet line-cardları olabilir.

İki cihaz birbirlerine 2 x 10Gig ile bağlanır ve tek bir cihaz haline getirilir. VSS data plane kısmında aktif-aktif ama control plane kısmında ise aktif-pasif olarak çalışır. Cihazların VSS olma süreci bittiğinde line-card'lardaki port numaraları değişir. Örneklemek gerekirse;

- VSS öncesi ilk yönlendiricinin TenGig 2/5 portu (2. Slot daki 5. Port demek)
- VSS sonrasında TenGig 1/2/5 olur (1. Yönlendiricinin 2. Slotundaki 5. Portu )

VSS sürecini anlatırken ürün olarak Cisco 6504 Catalyst switchlerini 720-10G supervisor modülleri ile kullanacağız.

### 3.1.1 VSS Konfigurasyonu

Standalone halinde çalışan iki adet yönlendiricinin VSS konfigürasyon süreci aşağıdaki gibidir;

- Her iki omurga yönlendiricisinde virtual switch domain oluşturulur ve bu domain altında yönlendiriciler “switch1” ve “switch2” olarak numaralandırılır.
- Virtual switch linkler oluşturulur.
- Conversion komutu girilerek yönlendiriciler baştan başlatılır.

VSS konfigürasyonu yapılmadan önce her iki cihazın IOS versiyonlarına bakılır ve her iki versiyonun da aynı olduğundan emin olunur. İki versiyonun da aynı olmaması durumunda hazırlanan konfigürasyon çalışmayacaktır. Kullandığımız her iki yönlendiricinin software ve hardware modellerinin VSS yapısını desteklediğini aşağıdaki konfigürasyonda görülür.

```
SW1-VSS#show module
Mod Ports Card Type Model Serial No.
-----
 1    5 Supervisor Engine 2T 10GE w/ CTS (Acti VS-SUP2T-10G SAL11111111
 2    4 CEF720 4 port 10-Gigabit Ethernet WS-X6704-10GE SAL11111111
 3   48 CEF720 48 port 10/100/1000mb Ethernet WS-X6748-GE-TX SAL11111111

Mod MAC addresses Hw Fw Sw Status
-----
 1 588d.09e6.d0b9 to 588d.09e6.d0c0 1.3 12.2(50r)SYS 15.0(1)SY2 Ok
 2 001a.a10e.833c to 001a.a10e.833f 2.5 12.2(14r)S5 15.0(1)SY2 Ok
 3 0002.fcc1.1bd0 to 0002.fcc1.1bff 1.2 12.2(14r)S5 15.0(1)SY2 Ok

Mod Sub-Module Model Serial Hw Status
-----
 1 Policy Feature Card 4 VS-F6K-PFC4 SAL11111111 1.2 Ok
 1 CPU Daughterboard VS-F6K-MSFC5 SAL11111111 1.4 Ok
 2 Centralized Forwarding Card WS-F6700-CFC SAD11111111 3.1 Ok
 3 Centralized Forwarding Card WS-F6700-CFC SAD11111111 1.1 Ok

Mod Online Diag Status
-----
 1 Pass
 2 Pass
 3 Pass
```

**Figür 3.1:** SW1 module gösterim konfigürasyonu

Switch2'nin konfigürasyon çıktısına bakıldığında ;

```
SW2-VSS#show module
*Aug 13 18:37:25.727: %SYS-5-CONFIG_I: Configured from console by console
Mod Ports Card Type                               Model                               Serial No.
-----
 1    5 Supervisor Engine 2T 10GE w/ CTS (Acti VS-SUP2T-10G       SAL22222222
 2    4 CEF720 4 port 10-Gigabit Ethernet      WS-X6704-10GE       SAL22222222
 3   48 CEF720 48 port 10/100/1000mb Ethernet WS-X6748-GE-TX      SAD22222222

Mod MAC addresses                               Hw   Fw       Sw       Status
-----
 1 588d.09e6.cc7d to 588d.09e6.cc84  1.3  12.2(50r)SYS 15.0(1)SY1 Ok
 2 001a.6c68.73e0 to 001a.6c68.73e3  2.5  12.2(14r)S5  15.0(1)SY1 Ok
 3 000d.6551.041a to 000d.6551.0449  1.2  12.2(14r)S5  15.0(1)SY1 Ok

Mod Sub-Module                               Model                               Serial   Hw   Status
-----
 1 Policy Feature Card 4                      VS-F6K-PFC4                      SAL22222222 1.2  Ok
 1 CPU Daughterboard                          VS-F6K-MSFC5                      SAL22222222 1.4  Ok
 2 Centralized Forwarding Card WS-F6700-CFC                      SAL22222222 3.1  Ok
 3 Centralized Forwarding Card WS-F6700-CFC                      SAD22222222 1.1  Ok

Mod Online Diag Status
-----
 1 Pass
 2 Pass
 3 Pass
```

**Figür 3.2:** SW2 module gösterim konfigürasyonu

Her iki yönlendirici de VSS teknolojisini destekleyen VS-SUP2T-10g supervisorlarını kullanıyorlar. Yönlendiricilerin hardware modülleri VSS uyumlu olduğu gibi software versiyonları da uyumlu olmalıdır.

```
SW1-VSS#show version
Cisco IOS Software, s2t54 Software (s2t54-ADVENTERPRISEK9-M), Version 15.0(1)SY2,
RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
```

**Figür 3.3:** SW1 version gösterim konfigürasyonu

Diğer yönlendiricinin software versiyonu

```
SW2-VSS#show version
Cisco IOS Software, s2t54 Software (s2t54-ADVENTERPRISEK9-M), Version 15.0(1)SY2,
RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
```

**Figür 3.4:** SW2 version gösterim konfigürasyonu

Her iki yönlendiricinin de software versiyonları IOS 15.0(1)SY2 olup VSS teknolojisine uygun oldukları konfigürasyon çıktılarında görülmektedir. Bu durumda VSS konfigürasyon yapılandırılmasına geçilebilir.

VSS yapılandırılma sürecinde ilk adım olan Virtual Switch Domain Id, 1 ile 255 arasında grup numarası olarak verilebilir. 6500 serisi “SW1-VSS” ve “SW2-VSS” isimli cihazlarımızdan her ikisini de aynı virtual switch domain id altında konfigür etmemiz gerekiyor.

```
SW1-VSS(config)#switch virtual domain 1
Domain ID 1 config will take effect only
after the exec command 'switch convert mode virtual' is issued

SW1-VSS(config-vs-domain)#switch 1
```

```
SW2-VSS(config)#switch virtual domain 1
Domain ID 1 config will take effect only
after the exec command 'switch convert mode virtual' is issued

SW2-VSS(config-vs-domain)#switch 2
```

**Figür 3.5:** SW1 ve SW2 virtual domain konfigürasyonu

Yukarıdaki konfigürasyonlarda görüldüğü gibi her iki yönlendirici de aynı virtual switch domain altındalar. Bu sistem içerisinde SW1-VSS, “switch1” ve SW2-VSS “switch2” olarak ayarlandılar. Sonraki adım yönlendiricilere aktif-pasif seçimi için priority değeri atamak olarak belirlenir.

```
SW1-VSS(config-vs-domain)#switch 1 priority 110
SW1-VSS(config-vs-domain)#switch 2 priority 100
```

```
SW2-VSS(config-vs-domain)#switch 1 priority 110
SW2-VSS(config-vs-domain)#switch 2 priority 100
```

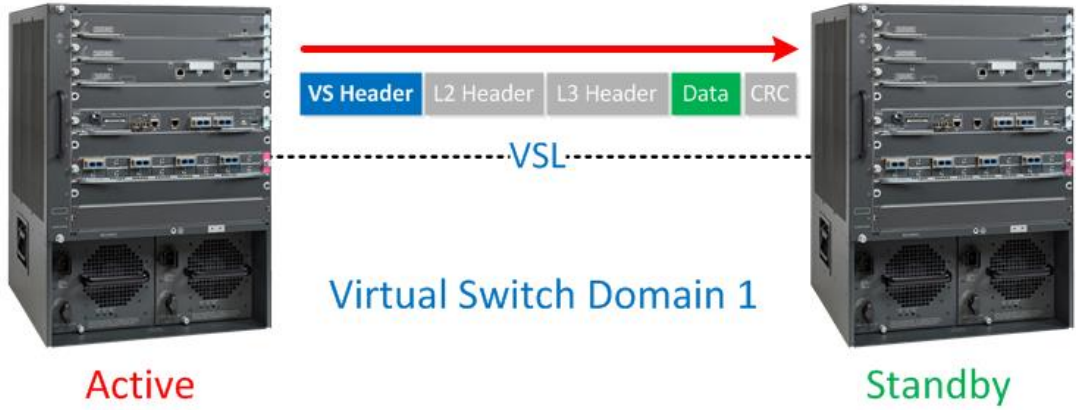
**Figür 3.6:** SW1 ve SW2 , VSS priority değeri konfigürasyonu

Priority değeri yüksek olan yönlendirici aktif rol alır. Buradaki aktif rolden kastı supervisor rolü içindir. Bu durumda Switch1’in priority değeri daha yüksek olduğu için SW1-VSS aktif yönlendirici olur. SW2-VSS ise beklemede yani standby



durumunda kalır. Buradaki roller control-plane içindir. Her iki yönlendiricide de data-plane aktif olarak rol alır.

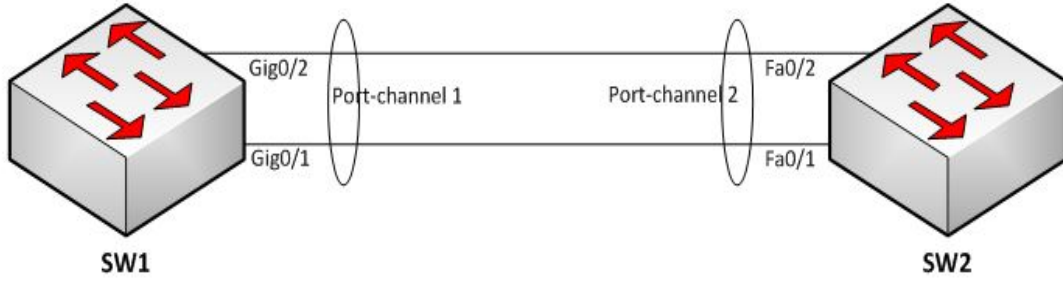
VSS teknolojisinde yönlendiriciler arasında konfigürasyon deęişikliği ve durum bilgisi güncellemeleri **virtual switch link** üzerinden yapılır [22]. VSS bağlantısı için virtual switch link olarak fiziksel port ya da yedeklilik için etherchannel kullanılabilir. VSL, link üzerinden gönderilen her bir paket frame ine “virtual switch header” ekler. Bu süreç **şekil 3.2**'deki gibidir.



Şekil 3.2: VSS Vsl Header.

Yönlendiricilerin üzerindeki fiziksel portların hepsi VSS teknolojisini desteklemez. Bu tezde VSS bağlantısı kurulurken supervisor üzerindeki Ten Gigabit interfaceler kullanıldı. VSS kurulurken yedekli bağlantı için etherchannel kullanıldı. Etherchannel konfigürasyonuna geçmeden önce etherchannel, link aggregation konusuna hakim olunması gerekiyor.

**Etherchannel** teknolojisi sayesinde paralel hatlar birleştirilerek tek bir mantıksal hat gibi kullanılabilirler [24]. Buna göre en az iki, en fazla sekiz FastEthernet, GigabitEthernet veya 10-Gigabit Ethernet hat birleştirilebilir ve Fast Etherchannel, Gigabit Etherchannel ve 10-Gigabit Etherchannel oluşturabilirler. Bu durumda full-duplex olarak en fazla 1600 Mbps (8 FastEthernet hattın birleştirilmesiyle), 16 Gbps (8 Gigabit Ethernet hattın birleştirilmesiyle) ve 160 Gbps (8 10-Gigabit Ethernet hattın birleştirilmesiyle) hızlarına ulaşılabilir. Bu da iki switch arasındaki hat kapasitemizi arttırabilmemiz anlamına gelmektedir ki ihtiyaç durumunda bizler için önemli bir avantaj sağlamaktadır. Çünkü normal şartlarda switchler arası paralel hatlardan biri dışındaki diğerleri loop oluşmaması için STP(Spanning Tree Protocol) tarafından engellenmektedir.



Şekil 3.3: Etherchannel.

Konfigurasyon yapılmadan önce Etherchannel'a dahil olan portların Spanning-Tree özelliklerinin aynı olmasına dikkat edilmelidir. Ayrıca Etherchannel'ı oluşturan portlar aynı vlan'de olmalıdırlar veya trunk görevi göreceklere native vlan'leri geçmesine izin verdikleri vlan'ler aynı olacak biçimde trunk modunda konfigüre edilmelidirler.

Etherchannel'ı oluşturan hatlar arasında network trafiğinin dağılımı bir algoritmaya göre yapılır ve bu trafik hatlara eşit dağıtılmak zorunda değildir. Bu yüzden yukarıda bahsettiğimiz hızlara ulaşamayabilir. Etherchannel'ı oluşturan hatlardan herhangi birisi çalışamaz duruma gelirse onun trafiği otomatik olarak Etherchannel içindeki başka bir hatta yönlendirilir. Algoritma, trafiği hatlar arasında dağıtırken kaynak IP, hedef IP, kaynak MAC, hedef MAC adreslerini veya port numaralarını temel alabilir. İki hattın birleştirilmesinden oluşan bir Etherchannel'da karar için 1 bitlik bilgiye ihtiyacımız vardır. Buna göre, trafiği dağıtmak için eğer bu 1 bitlik bilgi 0 ise hat 0, 1 ise hat 1 seçilebilir. Bu seçim için kullanılan bir yöntem, adreslerin son bitlerinin XOR'lanmasıdır. Bir örnek verecek olursak 192.168.2.1 adresinden 172.31.68.46 adresine gönderilen bir paket için trafiğin akacağı hat seçimi şu şekilde yapılır; Eğer iki hattın birleştirilmesiyle oluşturulmuş bir Etherchannel varsa IP adreslerinin son 1 biti üzerinde XOR işlemi uygulanarak  $1 \text{ XOR } 0=1$ , bu trafik için hat 1'in kullanılacağına karar verilir. Eğer dört hattın birleştirilmesiyle oluşturulmuş bir Etherchannel varsa IP adreslerinin son 2 biti üzerinde XOR işlemi uygulanarak  $01 \text{ XOR } 10=11$ , bu trafik için hat 3'ün kullanılacağına karar verilir. Son olarak sekiz hattın birleştirilmesiyle oluşturulmuş bir Etherchannel varsa IP adreslerinin son 3 biti üzerinde XOR işlemi uygulanarak  $001 \text{ XOR } 110 = 111$ , bu trafik için hat 7'nin kullanılacağına karar verilir.

Etherchannel port numaraları	Yük dağılımı
8	1:1:1:1:1:1:1:1
7	2:1:1:1:1:1:1:1
6	2:2:1:1:1:1:1:1
5	2:2:2:1:1:1:1:1
4	2:2:2:2:1:1:1:1
3	3:3:2:1:1:1:1:1
2	4:4:1:1:1:1:1:1

**Tablo 3.1:** Etherchannel 8 bitlik HASH algoritması

Yukarıdaki yöntem, hatlar arasında trafiğin dağıtımında adaletsizliğe yol açabilir. Bazen hatlardan biri fazla yük taşırken diğeri çok daha az yük taşır konuma gelebilir. Bunu dengelemek için TCP ve UDP portları trafik dağıtımında kullanılabilir. VSS bağlantımızın yedekli olması için yönlendiricilerin supervisor modülleri üzerindeki Ten 1/4 ve Ten 1/5 interfaceleri kullanıldı.

```
SW1-VSS(config)#interface port-channel 1
SW1-VSS(config-if)#no shutdown
SW1-VSS(config-if)#switch virtual link 1
SW1-VSS(config-if)#exit
SW1-VSS(config)#int range ten 1/4 - 5
SW1-VSS(config-if-range)#channel-group 1 mode on
SW1-VSS(config-if-range)#no shut
```

**Figür 3.7:** SW1 virtual link konfigürasyonu

```
SW2-VSS(config)#interface port-channel 2
SW2-VSS(config-if)#no shutdown
SW2-VSS(config-if)#switch virtual link 2
SW2-VSS(config-if)#exit
SW2-VSS(config)#int range ten 1/4 - 5
SW2-VSS(config-if-range)#channel-group 2 mode on
SW2-VSS(config-if-range)#no shutdown
```

**Figür 3.8:** SW2 virtual link konfigürasyonu

Yukarıdaki konfigürasyonlarda iki yönlendiricin birbirleriyle bağlantısı için etherchannel yapılmış ve supervisorlar üzerindeki TenGig interfaceler bu oluşturulan etherchannel'lara üye edilmiştir. Ayrıca her bir yönlendirici için etherchannel'lar "virtual switch link" olarak belirlenmiştir. Etherchannel durumlarını görmek için;

```
SW1-VSS#show etherchannel summary | incl Po1
1      Po1(RU)          -      Te1/4(P)      Te1/5(P)
```

```
SW2-VSS#show etherchannel summary | incl Po2
2      Po2(RU)          -      Te1/4(P)      Te1/5(P)
```

**Figür 3.9:** SW1 ve SW2 etherchannel durum gösterim konfigürasyonu

Yapılan adımlar tek tek incelendi. Yönlendiriciler VSS oluşumu için hazırlar. Son adım olarak VSS dönüşümünü gerçekleştirdikten sonra switchler üç süreçten geçer.

- Her iki switch'in konfigürasyonları tek bir konfigürasyon haline gelir.
- İnterface numaraları slot/port düzeninden switch-numarası/slot/port olarak değişir.
- Switch'lerin aktif-pasif rollerinin belirlenme süreci

VSS oluşumunu başlatmak için aşağıdaki konfigürasyonlar yapılır;

```
SW1-VSS#switch convert mode virtual

This command will convert all interface names
to naming convention "interface-type switch-number/slot/port",
save the running config to startup-config and
reload the switch.

NOTE: Make sure to configure one or more dual-active detection methods
once the conversion is complete and the switches have come up in VSS mode.

Do you want to proceed? [yes/no]: yes
Converting interface names
Building configuration...
```

**Figür 3.10:** SW1 virtual convert konfigürasyonu

Aynı işlem diğer switch için de yapılır ve bu işlemin her iki switch için aynı zamanda yapılması gerekir.

```
SW2-VSS#switch convert mode virtual

This command will convert all interface names
to naming convention "interface-type switch-number/slot/port",
save the running config to startup-config and
reload the switch.

NOTE: Make sure to configure one or more dual-active detection methods
once the conversion is complete and the switches have come up in VSS mode.

Do you want to proceed? [yes/no]: yes
Converting interface names
Building configuration...
```

**Figür 3.11:** SW2 virtual convert konfigurasyonu

Yukarıda görülen işlemler yapıldıktan sonra switch'ler baştan başlar ve süreç console arayüzünden aşağıdaki gibi görülür;

```
SW1-VSS#
System detected Virtual Switch configuration...
Interface TenGigabitEthernet 1/1/4 is member of PortChannel 1
Interface TenGigabitEthernet 1/1/5 is member of PortChannel 1
```

**Figür 3.12:** SW1 VSS başlangıç süreci gösterim konfigurasyonu

```
SW2-VSS#
System detected Virtual Switch configuration...
Interface TenGigabitEthernet 2/1/4 is member of PortChannel 2
Interface TenGigabitEthernet 2/1/5 is member of PortChannel 2
```

**Figür 3.13:** SW2 VSS başlangıç süreci gösterim konfigurasyonu

Bu adımda switch'lerin aktif-pasif seçimleri görülür;

```
SW1-VSS#
%PFREDUN-6-ACTIVE: Initializing as ACTIVE processor for this switch

%VSL_BRINGUP-6-MODULE_UP: VSL module in slot 1 switch 1 brought up
%VSLP-5-RRP_ROLE_RESOLVED: Role resolved as ACTIVE by VSLP
%VSL-5-VSL_CNTRL_LINK: New VSL Control Link 1/1/4
```

```
SW2-VSS#
%PFREDUN-6-ACTIVE: Initializing as ACTIVE processor for this switch

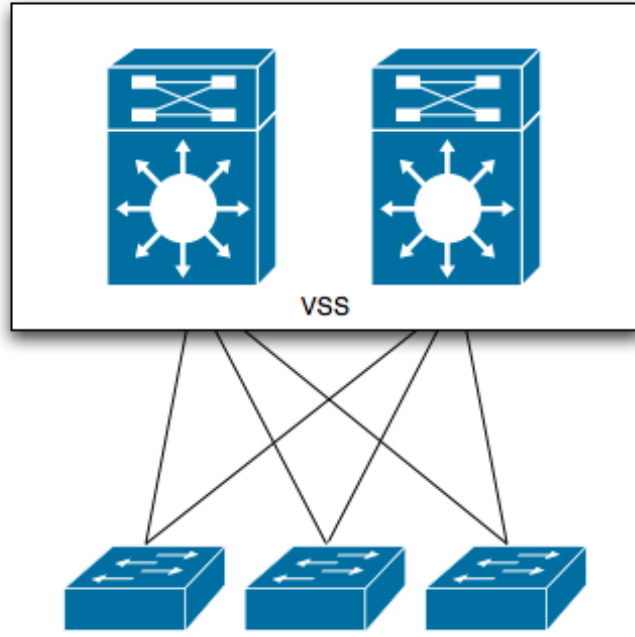
%VSL_BRINGUP-6-MODULE_UP: VSL module in slot 1 switch 2 brought up
%VSLP-5-RRP_ROLE_RESOLVED: Role resolved as STANDBY by VSLP
%VSL-5-VSL_CNTRL_LINK: New VSL Control Link 2/1/4
```

**Figür 3.14:** SW1 ve SW2 VSS aktif-pasif seçim süreci gösterim konfigürasyonu

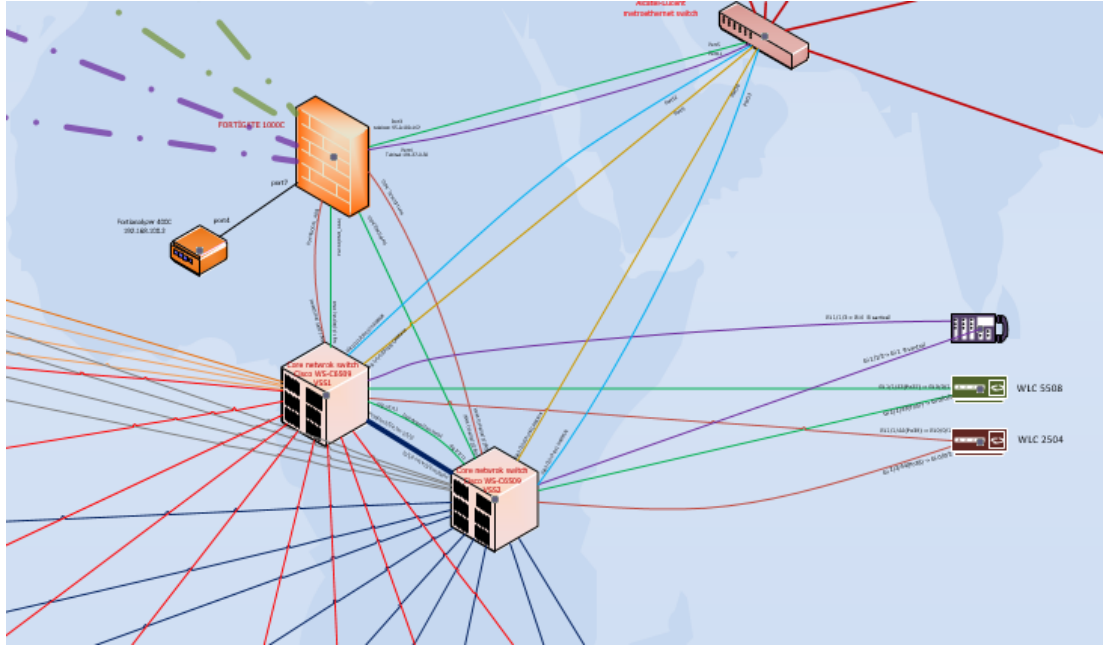
Her iki switch’inde baştan başlarken boot olma sürecinde VSS bağlantısı olma sürecinde fiziksel portları “virtual switch link” olarak görülür ve kendi aralarında aktif-pasif seçimini yaparlar. Bizim senaryomuzda SW1-VSS aktif olarak seçilmiştir. SW2-VSS artık konfigürasyon için devre dışı bırakılmıştır. Bu seçim olduktan sonra bütün konfigürasyonlar SW1-VSS üzerinden yapılır ve eş zamanlı olarak SW2-VSS ile paylaşılır.

### 3.1.2 Virtual System Switching de Yük Dağılımı ve Yedeklilik

VSS topolojisinde yedeklilik ve yük dağılımı tam verimle çalışır [22] Her bir kenar switch’den omurga yönlendiriciye iki bağlantı kablosu gider. Bu kablolardan biri SW1-VSS e giderken diğeri SW2-VSS e gider. Daha önce anlatıldığı gibi VSS’nin çalışma mantığında control-plane aktif-pasif çalışırken data-plane aktif-aktif çalışır. Kenar switch’den omurga yönlendiricilere giden iki kabloda etherchannel teknolojisi kullanılarak her iki kablonun aktif bir şekilde trafiği iletmesi sağlanır. Aynı şekilde omurga yönlendiricisine gelen iki kabloda da etherchannel teknolojisi kullanılır. Bu yük dağılımını sağlar. Bu kablolarda biri olan SW1-VSS yönlendiricisinin data-plane modülüne giderken, diğeri kablo olan SW2-VSS yönlendiricisinin data-plane modülüne gider. Böylece yedeklilik de sağlanmış olur.



Şekil 3.4: VSS Yedeklilik ve Yük dağılımı.

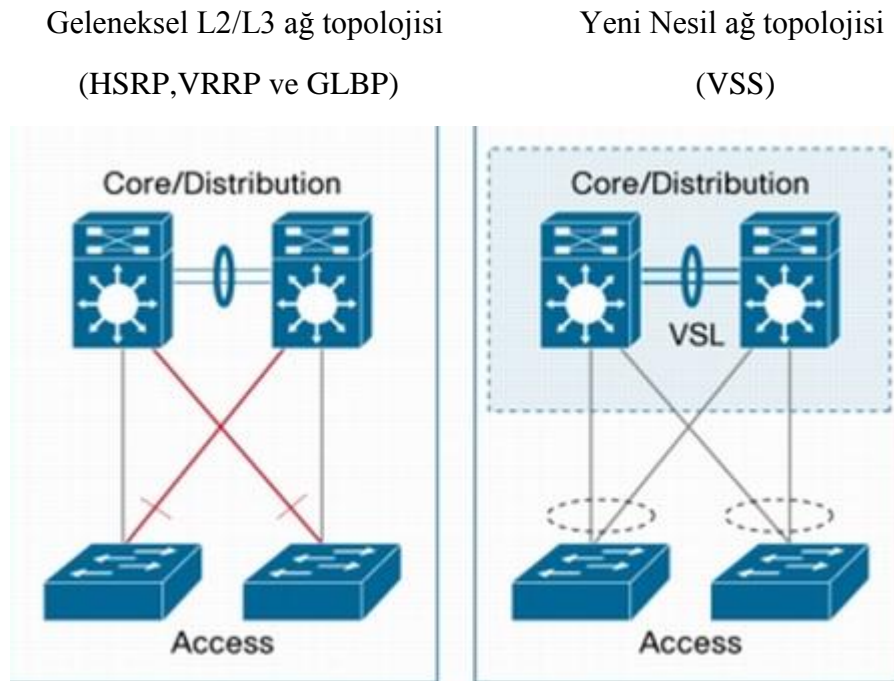


Şekil 3.5: Gediz Üniversitesi VSS ağ altyapısı

## 4.SONUÇ

Veri merkezlerinde yönlendirme hizmetinin önemi göz önüne alındığında, bu hizmetin güvenliliğinin önemi iyice anlaşılacaktır. Yedekleme ve yük dağılımı protokolleri oluşabilecek yönlendirici sorunlarını önlemek amacıyla geliştirilmiştir. Yüksek güvenilirlikte bir çalışma beklenen ortamlarda bu tür yedekleme ve yük dağılımı şarttır.

Bu tezde yukarıda bahsedilen protokol ve teknolojiler anlatıldı. Bu teknolojiler iki kısım olarak ayrıldı. İlk kısım'da anlatılan HSRP, VRRP ve GLBP gibi teknolojileri geleneksel ikinci ve üçüncü seviye ağ teknolojileri olarak adlandırabiliriz. VSS gibi virtual chassis yapıda olanlar ise yeni nesil teknolojiler olarak adlandırılabilir.



Şekil 4.1: Geleneksel ve yeni nesil teknolojilerinin yedeklilik ve yük dağılımı karşılaştırması.

Şekil 4.1'de görüldüğü gibi geleneksel teknolojilerde döngü iletişimini önlemek amacıyla spanning-tree protokolü devreye alınarak portlardan biri kapalı duruma getirilir. Lakin yeni nesil teknoloji VSS, L2 seviyesinde çalıştığı için ve iki fiziksel cihazı tek bir logical cihaza dönüştürdüğü için bütün portları aktif olarak kullanır. Yeni nesil teknolojisi virtual switching software, geleneksel teknolojilere (HSRP, VRRP ve GLBP) göre daha verimli ve stabil olarak çalışmaktadır.[22]



Yeni nesil teknolojilerinden VSS, geleneksel teknolojilere göre daha fazla avantajı vardır [22]. Bu avantajları 3 ana kategoriye ayırabiliriz;

1. VSS en az yüzde 50 oranında anahtarlama (switching) yönetim yükünü azaltarak ve ağ topolojisini sadeleştirerek operasyonel verimliliği artırır.
  - Yönlendiricilerin yönetimi için tek bir konfigürasyon kolaylığı sağlar. VSS, geleneksel L2/L3 teknolojilerinde olan yedeklilik için iki defa konfigürasyon yapma ihtiyacını da ortadan kaldırır.
  - Geleneksel L2/L3 teknolojilerinde her bir vlan için ağ geçidi tanımlanırken 3 adet (2 fiziksel ve bir sanal) IP adresi kullanılır. Yeni nesil teknolojilerinden VSS’de ise ağ geçidi tanımlanırken her vlan için tek IP adresi kullanılır. Bu durum IP yönetimini kolaylaştırmayı sağlar.
  - VSS, L2 seviyesinde birden fazla yol belirlemede loop-free topolojisini sağlayan MultiChassis EtherChannel (MEC) teknolojisini kullanarak spanning-tree bazlı yapılacak yanlış konfigürasyonlara karşı korumayı aktif hale getirir.
  - Esnek dağıtım seçenekleri sağlar. Supervisor’ların yedekliliği 10Giga fiber ile sağlanır ve bu fiberler 40 km iletim sağlar. Bu esneklik ayrıca lokasyon bazlı yedeklilik de sağlamış olur.
2. VSS kesintisiz iletişimi artırır.
  - VSS teknolojisinin mimarisi firmware upgrade yapılırken herhangi bir kesinti olmayacak şekilde geliştirilmiştir. Bu özellik geleneksel L2/L3 teknolojilerinde (HRSP, VRRP ve GLBP) yoktur.
  - NAT(Network Address Translation) , ARP tablosu, netflow gibi ağ durum bilgileri gerektiren protokollerin sorunsuz bir şekilde çalışmasını sağlar.
3. VSS trafik kapasitesi olarak 1.4 Tbps band genişliği destekler.
  - 10 Gigabit Ethernet portlarının kullanımını maksimum seviyeye çıkarır.
  - EtherChannel protokolü sayesinde kenar switchlerden 20 (2 x 10) Gigabit Ethernet bandwidth genişliği sağlar.

Protokoller ve Teknolojiler	HSRP (Hot Standby Router Protocol)	VRRP (Virtual Redundancy Router Protocol)	GLBP (Gateway Load Balancing Protocol)	VSS (Virtual Switching System )
Yönlendirici rolleri	1 aktif yönlendirici ve 1 pasif yönlendirici ya da dinleyici durumdaki yönlendiriciler	1 aktif yönlendirici ve 1 pasif (yedek) yönlendirici	1 adet AVG yönlendirici. Maksimum 4 adet AVF yönlendirici	Control plane olarak aktif-pasif Data plane olarak Aktif-aktif
Standart	Cisco Standardı	IEEE standardı	Cisco Standardı	Cisco Standardı
Seçim	En yüksek Priority değeri, En yüksek ip adresine sahiplik	En yüksek Priority değeri, En yüksek ip adresine sahiplik	En yüksek Priority değeri, En yüksek ip adresine sahiplik	Seçime bağlı priority değeri
Optimizasyon özellikleri	Tracking,Preempt	Tracking,Preempt	Tracking,Preempt	Logical
Trafik biçimi	224.0.0.2 udp 1985 portu	224.0.0.18 8888 udp portu	224.0.0.102 udp 3222 portu	Fast Hello Dual Active
Paket zamanlamaları	3 saniye	1 saniye	3 saniye	1 saniyeden düşük
Yük dağılımı fonksiyonları	Her bir kaynak ip adresi için ağ geçidi paylaşımı	Her bir kaynak ip adresi için ağ geçidi paylaşımı	Kaynak paketler ARP isteklerini yük dengeleme algoritmasına göre günceller	Tam verimli yük dengeleme vardır.

**Tablo 4.1:** Geleneksel ve yeni nesil teknolojilerin yedeklilik ve yük dağılımı karşılaştırılması

# KAYNAKLAR

- [1] **Wendell Odom, David Hucaby, Kevin Wallace**, 2010, “*CCNP Routing and Switching Official Certification Guide*”, Cisco Pres.
- [2] **Corporate Headquarters** , 2010, “*Data Center High Availability Clusters Design*”, Cisco Press.
- [3] **Santosh Mahapatra, Xin Yuan** , 2010, “*Load Balancing Mechanisms in Data Center Networks*”, Department of Computer Science, Florida State University, Tallahassee [Tez].
- [4] **Robin Taylor** , 2013, “*Importance of Today’s World*”, [www.selfgrowth.com](http://www.selfgrowth.com)
- [5] **Matthew Desantis, US-CERT**, 2010, “*Understanding Voice Over IP*”  
[www.us-cert.gov](http://www.us-cert.gov)
- [6] **Wikipedia**, 2012, “*Load Balancing and Clustering in Backbone Internet*”,
- [7] **Cisco Resmi Kaynaklar** , 2010, “*Hot Standby Router Protocol Features and Functionality*”, Document ID: 9234 , Cisco Press
- [8] **Cisco Resmi Kaynaklar** , 2010, “*GLBP Gateway Load Balancing Protocol*”, Document ID: 9249 , Cisco Press
- [9] **R. Hinden, Ed.** , 2004, “*Virtual Router Redundancy Protocol (VRRP)*”, IEEE, ACM  
DL Digital Library
- [10] **GNS3 resmi web sitesi** , 2010, “*Graphical Network Simulator*”,  
[www.gns3.com](http://www.gns3.com)
- [11] **Cisco Resmi Kaynaklar** , 2010, “*Configuring HSRP*”, [www.cisco.com](http://www.cisco.com).
- [12] **Cisco Resmi Kaynaklar** , 2010, “*Load Sharing with HSRP*”, [www.cisco.com](http://www.cisco.com).
- [13] **Jen-Hao Kuo, Pang-Ting Liao, Chun-Ying Huang** , 2005, “An evaluation of the virtual router redundancy protocol extension with load balancing”, 11th Pacific Rim International Symposium on Dependable Computing, pp. 1-7.
- [14] **Joe Wilson**, 2011, “*Comparing HSRP Versus VRRP*”, [www.routerfreak.com](http://www.routerfreak.com)
- [15] **Nikhil Hemant Bhagat**, 2011, “Virtual Router Redundancy Protocol-A Best OpenStandard Protocol in Maintaining Redundancy”, Proceedings published by International Journal of Computer Applications (IJCA).

- [16] **Sian Wilkins**, 2013, “Introduction to the Cisco Gateway Load Balance Protocol (GLBP)”, Person.
- [17] **Cisco Resmi Kaynaklar**, 2011, “*Configuring GLBP*”, www.cisco.com
- [18] **Paul Matwaet, T eknopankaj**, 2011, “*Comparing and Differences between HSRP, VRRP and GLBP*”, cisoctec.
- [19] **Junming Xu**, 2010, “*Topological Structure and Analysis of Interconnection Networks*”, Springer Publishing Company, Incorporated.
- [20] **Radhika Niranjana Mysore, Andreas Pamboris, Nelson Huang** 2010, “*A Scalable fault-tolerant layer2 data center network fabric*”, University of California, San Diego
- [21] **Tim Clegg**, 2011, “*Cisco Virtual Switching System 1140*”, Global Technology Resource.
- [22] **Cisco resmi kaynaklar**, 2011, “*Cisco Catalyst 6500 Series Virtual Switching Supervisor Engine 720 with 10 Gigabit Ethernet Uplinks*”, Datasheet.
- [22] **Cisco resmi kaynaklar**, 2013, “*Campus 3.0 Virtual Switching System Design Guide*”, Datasheet
- [23] **Cisco resmi kaynaklar**, 2012, “*Cisco Catalyst 6500 Series Virtual Switching Supervisor Engine 720 with 10 Gigabit Ethernet Uplinks*”, Datasheet.
- [24] **Peter K. Craft, Clive M. Philbrick, Daryl D. Starr** 2006, “*Port aggregation for network connections that are offloaded to network interface devices*”, Alacritech. Inc. pp . 2-4
- [23] **Cisco resmi kaynaklar**, 2012, “*Cisco Catalyst 6500 Series Virtual Switching Supervisor Engine 720 with 10 Gigabit Ethernet Uplinks*”, Datasheet.

## ÖZGEÇMİŞ



**Ad Soyad:** NUMAN FARUK KARAKAŞ

**Doğum Yeri ve Tarihi:** AKSARAY / 1989

**Adres:** GEDİZ ÜNİVERSİTESİ

**E-Posta:** nfkarakas@gmail.com

**Lisans:** ELEKTRONİK VE HABERLEŞME MÜHENDİSLİĞİ / YILDIZ TEKNİK ÜNİVERSİTESİ

**Yüksek Lisans :** SİSTEM MÜHENDİSLİĞİ / GEDİZ ÜNİVERSİTESİ

### Mesleki Deneyim ve Sertifikalar:

CCNP - Cisco Certified Networking Professional

CCNA - Cisco Certified Networking Associate

BNT PRO Juniper srx

RZK Fortigate Firmware

7.Ulaknetce (TUBITAK) certificate

3CX Voip Certification

IP ROUTING TECNOLOGY

EIGRP TECNOLOGY

OSPF TECNOLOGY

BGP TECNOLOGY

RIP TECNOLOGY

REDISTRIBUTION TECNOLOGY

POLICY-BASED ROUTING TECNOLOGY

IPV6 , CAMPUS NETWORK DESIGN

LAYER 2 SWITCHING

VLANS , TRUNKING , INTER-VLAN ROUTING

DTP AND VTP TECNOLOGY

STP FEATURES

ETHERCHANNEL , LAYER2 SECURITY

WIRELESS

VPN TECNOLOGY , USER AUTHENTICATION

FAILOVER, REDUNDANT NETWORK SYSTEM DESIGN (HSRP,VRRF,GLBP,VSS)

P2P, INTERNET VPN, METROETHERNET,L2 TUNNELLING

NETWORK MONITORING (PRTG , SOLARWINDS)

SECURTY (802.1X,CAPTURE PORTAL)

NAC (NETWORK ACCESS CONTROL)

VOIP TECNOLOGY

CISCO vPC (VIRTUAL PORT-CHANNEL)  
SDN (SOFTWARE DESIGNED NETWORK)  
VRF TECHNOLOGY  
MPLS TECHNOLOGY