GAZİ ÜNİVERSİTESİ

Gazi

1926

# GNS3 EMÜLASYONU İLE IPV4'TEN IPV6'YA GEÇİŞ: BİR VAKA ÇALIŞMASI OLARAK YEMEN PTE

**Ammar Hamood Saeed QAID**

**YÜKSEK LİSANS TEZİ**
**BİLGİSAYAR BİLİMLERİ ANA BİLİM DALI**

**GAZİ ÜNİVERSİTESİ**
**BİLİŞİM ENSTİTÜSÜ**

**TEMMUZ 2021**

Ammar Hamood Saeed QAID tarafından hazırlanan GNS3 EMÜLASYONU İLE IPV4'TEN IPV6'YA GEÇİŞ: BİR VAKA ÇALIŞMASI OLARAK YEMEN PTE" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi BİLGİSAYAR BİLİMLERİ Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

**Danışman:** Doç. Dr. Özgür ERTUĞ
Elektrik Elektronik Mühendisliği Anabilim Dalı, Gazi Üniversitesi
Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum. ..……

**Başkan:** Prof. Dr. Suat ÖZDEMİR
Bilgisayar Mühendisliği Anabilim Dalı, Hacettepe Üniversitesi
Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum. ……...

**Üye:** Doç. Dr. Ertuğrul AKSOY
Elektrik Elektronik Mühendisliği Anabilim Dalı, Gazi Üniversitesi
Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum. ……...

Tez Savunma Tarihi: 09/07/2021

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

…….…….
Prof. Dr. Aslıhan TÜFEKCİ
Bilişim Enstitüsü Müdürü

## ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Ammar Hamood Saeed QAID

09/07/2021

GNS3 EMÜLASYONU İLE IPV4'TEN IPV6'YA GEÇİŞ: BİR VAKA ÇALIŞMASI OLARAK YEMEN PTE

(Yüksek Lisans Tezi)

Ammar Hamood Saeed QAID

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Temmuz 2021

ÖZET

Son yıllarda teknoloji, giderek daha fazla cihazın İnternete bağlanmasına yol açan, IPv4 adresinin tüketilmesine yol açan hızlı bir gelişmeye tanık oldu. IETF, IPv6'yı uzun vadeli bir çözüm olarak geliştirdi. Ancak farklı IPv4 ve IPv6'nın başlık yapısı nedeniyle, IETF, IPv6 devralmadan önce hem IPv4 hem de IPv6'nın bir süre bir arada bulunmasına izin vermek için bazı geçiş yöntemleri geliştirdi. Bu çalışma, seçilen bazı geçiş yöntemlerinin (İkili Yığın Yöntemi, NAT6-4 Yöntemi, Manuel Tünelleme Yöntemi, Otomatik 6to4 Tünelleme Yöntemi ve Otomatik ISATAP Tünelleme Yöntemi) GNS3 Emulator ile simüle edilerek YPTC'de uygulanabilecek optimal geçiş yöntemini seçmeyi ve ardından Wireshark aracını kullanarak bunları ağ performans metrikleri (Gecikme, Veri Aktarım Hızı ve RTT) ile değerlendirin.

Bilim Kodu : 332100
Anahtar Kelimeler : IPv6, IPv4, İkili Yığın, NAT6-4, Manuel Tünelleme, 6to4, ISATAP.
Sayfa Adedi : 39
Danışman : Doç. Dr. Özgür ERTUĞ

TRANSITION FROM IPV4 TO IPV6 MECHANISMS BY GNS3 EMULATION: YPTC AS A CASE STUDY

(M. Sc. Thesis)

Ammar Hamood Saeed QAID

GAZİ UNIVERSITY

INSTITUTE OF INFORMATICS

July 2021

ABSTRACT

In recent years, technology has witnessed a rapid development, that has led to the connection of more and more devices to the Internet, that has led to consuming the IPv4 Address. IETF developed the IPv6 as a long-term solution. However, due to different IPv4 and IPv6's header structure, IETF developed some transition mechanisms to allow both IPv4 and IPv6 to co-exist for a while before IPv6 take over. This study aims to choose the optimal transition mechanism which can be applied at YPTC by simulating some selected transition mechanisms (Dual Stack Method, NAT6-4 Method, Manual Tunneling Method, Automatic 6to4 Tunneling Method and Automatic ISATAP Tunneling Method) with GNS3 Emulator and then evaluate them with network performance metrics (Delay, Throughput and RTT) by using Wireshark tool.

Science Code : 332100
Key Words : IPv6, IPv4, Dual Stack, NAT6-4, Manual Tunneling, 6to4, ISATAP.
Page Number : 39
Supervisor : Assoc. Prof. Dr. Özgür ERTUĞ

# TEŞEKKÜR

Yüksek lisans eğitimim ve tez çalışmam boyunca bilgisini ve bilimsel desteğini esirgemeyerek, çalışmanın tamamlanmasında fikirleriyle aydınlanmamı sağlayan, öğrencisi olduğum için kendimi her zaman şanslı hissettiğim değerli tez danışmanım Doç. Dr. Özgür ERTUĞ'a kıymetli düşüncelerinden ve ilgisinden dolayı sonsuz teşekkürlerimi sunarım. Kendisinin bu denli bilgisi ve doğru yönlendirmesi olmasa; böyle bir çalışma ve bu çalışmanın çıktısı olabilecek yayınlar olmazdı.

Ayrıca beni hiçbir zaman yalnız bırakmayıp bana güvenmekten hiç vazgeçmeyen kıymetlilerim anneme, babama, kardeşlerime; manevi desteklerini hep hissettiren arkadaşım Mohammed AL-HABARİ'ye teşekkürü borç bilirim.

# İÇİNDEKİLER

**Sayfa**

ÖZET ..... iv
ABSTRACT ..... v
TEŞEKKÜR ..... vi
İÇİNDEKİLER ..... vii
ÇİZELGELERİN LİSTESİ ..... ix
ŞEKİLLERİN LİSTESİ ..... x
SİMGELER VE KISALTMALAR ..... xi
1. GİRİŞ ..... 1
2. IPV6 GEÇİŞ YÖNTEMLERİ ..... 5
2.1. İkili Yığın Yöntemi ..... 5
2.2. Çeviri Yöntemi ..... 6
2.3. Tünelleme Yöntemi ..... 8
2.3.1. Manuel tünelleme yöntemi ..... 8
2.3.2. Otomatik 6to4 tünelleme yöntemi ..... 10
2.3.3. Otomatik ISATAP tünelleme yöntemi ..... 12
3. AĞ TASARIMI ..... 15
3.1. YPTC Şubesi 1 ..... 16
3.2. YPTC Çekirdek ..... 17
3.3. YPTC Şubesi 2 ..... 17
4. SİMÜLASYONLAR ..... 19
4.1. Geçiş Yöntemleri Senaryoları ..... 19
4.1.1. İkili yığın senaryosu ..... 19
4.1.2. Çeviri senaryosu ..... 23
4.1.3. Tünelleme senaryosu ..... 25

**Sayfa**

5. DEĞERLENDİRME VE SONUÇLAR ..... 33
5.1. Gecikme (Delay) ..... 33
5.1.1. 6to4 - ISATAP - manuel tünel gecikmesi ..... 33
5.1.2. İkili yığın - ISATAP - NAT6-4 gecikmesi ..... 34
5.2. Veri Aktarım Hızı (Throughput) ..... 34
5.2.1. 6to4 - ISATAP - manuel tünel veri aktarım hızı ..... 34
5.2.2. İkili yığın - ISATAP - NAT6-4 veri aktarım hızı ..... 35
5.3. RTT ..... 36
KAYNAKLAR ..... 37
ÖZGEÇMİŞ ..... 39

# ÇİZELGELERİN LİSTESİ

**Çizelge** **Sayfa**

Çizelge 3.1. YPTC ağ tasarımı ..... 16

Çizelge 3.2. YPTC şube 1'in arayüz şeması ..... 16

Çizelge 3.3. YPTC çekirdeğinin arayüz şeması..... 17

Çizelge 4.1. İkili yığın yöntemi şube 1'in IP adresleme şeması ..... 20

Çizelge 4.2. İkili yığın yöntemi çekirdeğin IP adresleme şeması..... 21

Çizelge 4.3. İkili yığın yöntemi şube 2'nin IP adresleme şeması ..... 21

Çizelge 4.4. Çeviri yöntemi şube 1'in IP adresleme şeması ..... 24

Çizelge 4.5. çeviri yöntemi çekirdeğin IP adresleme şeması..... 24

Çizelge 4.6. Çeviri yöntemi şube 2'nin IP adresleme şeması ..... 25

Çizelge 4.7. Tünelleme yöntemi şube 1'in IP adresleme şeması ..... 27

Çizelge 4.8. Tünelleme yöntemi çekirdeğin IP adresleme şeması..... 27

Çizelge 4.9. Tünelleme yöntemi şube 2'nin ıp adresleme şeması..... 28

# ŞEKİLLERİN LİSTESİ

**Şekil** **Sayfa**

Şekil 1.1. Coğrafi kapsam ..... 2

Şekil 1.2. Teknolojik kapsam ..... 3

Şekil 2.1. İkili yığın ağların haberleşmesi ..... 5

Şekil 2.2. NAT6-4 yöntemi ağların haberleşmesi ..... 7

Şekil 2.3. Manuel tünelleme yöntemi ağların haberleşmesi ..... 9

Şekil 2.4. 6to4 IPv6 adresinin yapısı ..... 11

Şekil 2.5. 6to4 tünelleme yöntemi ağların haberleşmesi ..... 12

Şekil 2.6. ISATAP IPv6 adres biçimi - yerel bağlantı ..... 13

Şekil 2.7. ISATAP IPv6 adres biçimi - global tek noktaya yayın ..... 13

Şekil 2.8. ISATAP tünelleme yöntemi ağların haberleşmesi ..... 14

Şekil 3.1. YPTC mimarisi ..... 15

Şekil 3.2. YPTC ağ topolojisi ..... 15

Şekil 4.1. İkili yığın senaryosu topolojisi ..... 20

Şekil 4.2. Çeviri senaryosu topolojisi ..... 23

Şekil 4.3. Tünelleme senaryosu topolojisi ..... 26

Şekil 5.1. 6to4 vs ISATAP vs manuel tünel gecikmesi ..... 33

Şekil 5.2. İkili yığın vs ISATAP vs NAT6-4 gecikmesi ..... 34

Şekil 5.3. 6to4 vs ISATAP vs manuel tünel veri aktarım hızı ..... 35

Şekil 5.4. İkili yığın vs ISATAP vs NAT6-4 veri aktarım hızı ..... 35

# SİMGELER VE KISALTMALAR

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

| **Simgeler** | **Açıklamalar** |
|---|---|
| **µSec** | Microsecond |

| **Kısaltmalar** | **Açıklamalar** |
|---|---|
| **DNS** | Alan Adı Sistemi (Domain Name System) |
| **EIGRP** | Gelişmiş İç Ağ Geçidi Yönlendirme Protokolü (Enhanced Interior Gateway Routing Protocol) |
| **GNS3** | Grafiksel Ağ Simülatörü-3 **(**Graphical Network Simulator-3) |
| **IANA** | İnternet Atanmış Numara yetkilisi **(**Internet Assigned Number Authorityinternet) |
| **IETF** | İnternet Mühendisliği Görev Grubu (Internet Engineering Task Force) |
| **IP** | İnternet Protokolü (Internet Protocol) |
| **IPv4** | İnternet Protokolü Sürüm 4 (Internet Protocol version 4) |
| **IPv6** | İnternet Protokolü Sürüm 6 (Internet Protocol version 6) |
| **ISATAP** | Site İçinde Otomatik Tünel Adresleme Protokolü (Intra-Site Automatic Tunnel Adresing Protocol) |
| **ISP** | İnternet Servis Sağlayıcısı (Internet Service Provider) |
| **NSP** | Ağa Özgü Önek **(**Network-Specific Prefix) |
| **OSPF** | İlk Önce En Kısa Yolu Aç (Open Shortest Path First) |
| **OSPF v2** | İlk Önce En Kısa Yolu Aç Sürüm 2 (Open Shortest Path First Version 2) |
| **OSPF v3** | İlk Önce En Kısa Yolu Aç Sürüm 3 (Open Shortest Path First Version 3) |
| **RTT** | Gidiş Dönüş Süresi (Round Trip Time) |
| **WAN** | Geniş Alan Ağı (Wide Area Network) |
| **WKP** | Bilinen Önek **(**Well-Known Prefix**)** |

| **Kısaltmalar** | **Açıklamalar** |
|---|---|
| **YPTC** | Yemen Kamu Telekomünikasyon Kurumu (Yemen Public Telecommunication Corporation) |
| **DNS6-4** | 6to4 Alan Adı Sistemi 6-4 (Domain Name System 6to4) |
| **NAT6**-4 | Ağ Adresi Çevirisi IPv6'dan IPv4'e (Network Address Translation IPv6 to IPv4) |

# 1. GİRİŞ

İnternete bağlanmak için kullandığımız İnternet Protokolü (IP-Internet Protocol) sayesinde, veriler internette bir boğumdan diğerine her bir boğuma benzersiz bir adres verilerek iletilebilir.

1981'de İnternet Protokolü Sürüm 4 (IPv4-Internet Protocol Version 4) internet dünyasında gerçek standart haline geldi. 1980'lerin başında IPv4'ün özellikleri yeterliydi ve bu nedenle internet kullanımın talebi arttı [1].

1980'lerin sonunda İnternet Atanmış Numara Yetkilisi (IANA-Internet Assigned Number Authorityinternet) IPv4 adreslerinin tüketimini tahmin etmeye başladı. IPv4 protokolünün başlangıcında, tasarımcılar internetteki büyümeyi şu an olduğu gibi görselleştirmediler. $2^{32}$ adres alanının geniş olduğunu, yani 4 294 967 296 adresin yeterli olduğunu düşündüler [2].

1990'larda internet yetkilileri, uzun vadeli çözüm olarak bir gün IPv4 protokolünü devralmak için İnternet Protokolü Sürüm 6 (IPv6-Internet Protocol Version 6) adlı yeni bir IP sürümü geliştirmeye başladılar [3]. 128 bit adresli IPv6 protokolü, yani IPv6 protokolü $2^{128}$ yaklaşık 340 282 366 920 938 463 463 374 607 431 768 211 456 adres üretebilir [4].

IPv4'ten IPv6'ya geçiş büyük bir zorluktur ve hemen uygulanamaz. IPv6'nın IPv4 ile uyumsuz olması nedeniyle, IPv6'ya sorunsuz bir geçiş yoktur.

Çözüm olarak, İnternet Mühendisliği Görev Gücü (IETF-Internet Engineering Task Force) bu sorunu gidermek için birçok geçiş yöntemi oluşturmuştur. Bu yöntemler, IPv4 ağlarının IPv6 ağları ile paralel olarak bir arada bulunmasına ve sorunsuz iletişim kurmasına izin verir. Çeşitli geçiş yöntemleri, İkili Yığın Yöntemi, Çeviri Yöntemi ve Tünelleme Yöntemi olmak üzere üç kategoriye ayrılabilir [5].

Günümüzde pek çok ülke IPv6'ya geçmeyi planlamaktadır. Diğer yandan, henüz hiçbir ülke IPv6'ya tam olarak geçiş yapmadı. Google IPv6 Benimseme İstatistikleri sitesine göre Nisan 2021'de, IPv6 trafiğinin yüzdesi yüzde 30,72. Bu da son beş yılda yüzde 25 artış anlamına geliyor. Dünyada yalnızca dört ülkede IPv6'nın benimsenme oranı %50'den fazladır; Hindistan%57,48, Belçika%56,98, Almanya%51,70 ve Malezya%51,09. Öte yandan, IPv6

benimseme oranının sadece%0,35'ine sahip olan Çin gibi birçok ülke bu alanda hala çok geç kalmıştır. İspanya, İran ve Hırvatistan sırasıyla%2,86, %1,88 ve%1,1'dir, Yemen 0,52 ile küçük bir değere sahiptir. Kuzey Kore, Türkiye ve diğer birçok ülke başlamadı; IPv6 benimseme oranı%0'dır [6].

Çalışma kapsamı

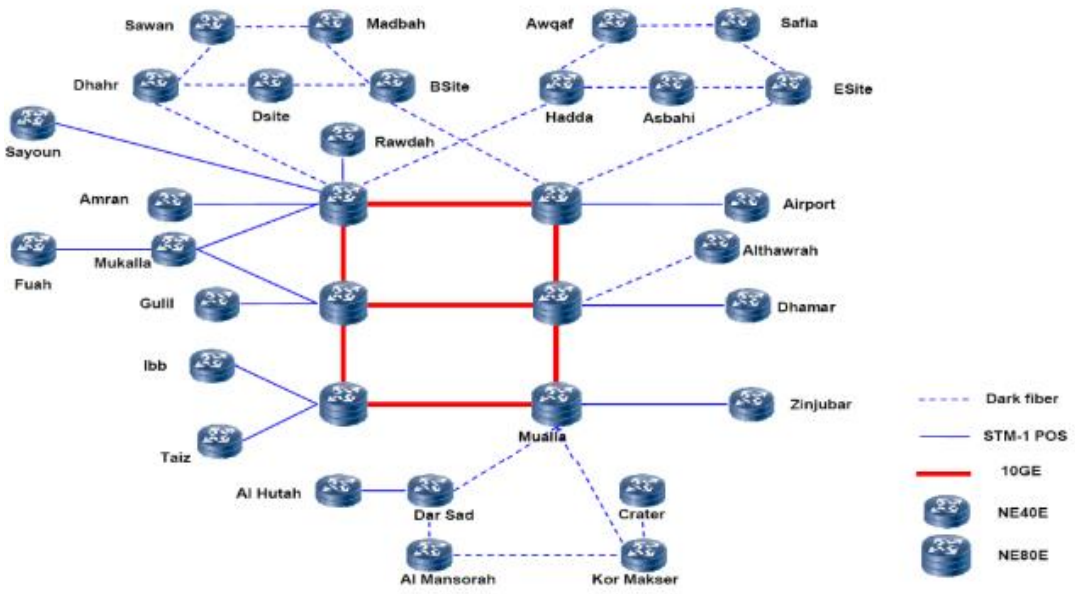
*Bu çalışmanın iki kapsamı var:*

*Coğrafi kapsam*

Yemen Kamu Telekomünikasyon Kurumu (YPTC-Yemen Public Telecommunication Corporation), telekomünikasyon sektöründe genel hükümet hedeflerine ulaşmak için 1981 yılında kurulmuş, Yemen hükümetine ait bir kamu kuruluşudur.

Yemen'in 22 Mayıs 1990'da birleşmesinin ardından, Sanaa'daki Kamu Telekom Şirketi, Yemen Cumhuriyeti'ndeki tüm telekomünikasyon hizmetlerinden sorumlu olacak YPTC'yi oluşturmak için Aden'deki Telekom Otoritesi ile tamamen birleştirildi.

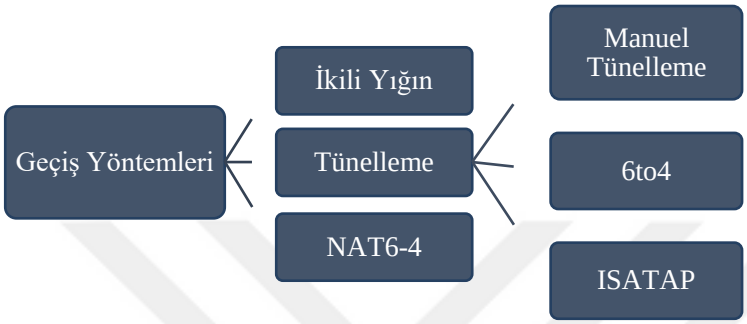
YPTC, Yemen'in tek İnternet Servis Sağlayıcısı (ISP-Internet Service Provider) olduğundan YPTC, Yemen internet ağ geçididir [13]. Şekil 1.1. YPTE diyagramını göstermektedir.




Şekil 1.1. Coğrafi kapsam

*Teknolojik kapsam*

Teknolojik kapsam, YPTE'de internet gelişimini sağlamak için IPv4 ve IPv6 bir arada yaşama döneminde kullanılması beklenen geçiş yöntemlerinden seçilmiş gruptur, şekil 1.2’de teknolojik kapsamın gösterimi yapılmıştır.




Şekil 1.2. Teknolojik kapsam

Bu çalışmanın temel amacı, Grafiksel Ağ Simülatörü-3 (GNS3-Graphical Network Simulator-3) Öykünücüsü kullanılarak üç senaryoda seçilen geçiş yöntemlerini taklit ederek YPTC ağı için en uygun yöntemi seçmektir. Ağdaki tüm arabirim trafiğini izlemek için Wireshark gibi bazı araçları kullanarak her senaryodaki ağ performansını değerlendirmek a minimum gecikmeye (Delay) ve maksimum trafik hacmine (Throughput) sahip olan ve aynı zamanda en düşük Gidiş Dönüş Süresine (RTT-Round Trip Time) sahip olan optimum yöntemi seçmek.

Bu çalışma beş bölümden oluşmaktadır. Bölüm 1'de konuya kısa bir giriş verilmiştir. Bölüm 2'de geçiş yöntemlerinin analitik bir çalışmasını içerir. Bölüm 3’te YTPC'nin ağ tasarımı. Bölüm 4'de geçiş yöntemleri simüle edilmektedir. Bölüm 5'te simüle edilen yöntemlerin performansının analizi ve çalışmanın sonuçları içerir.

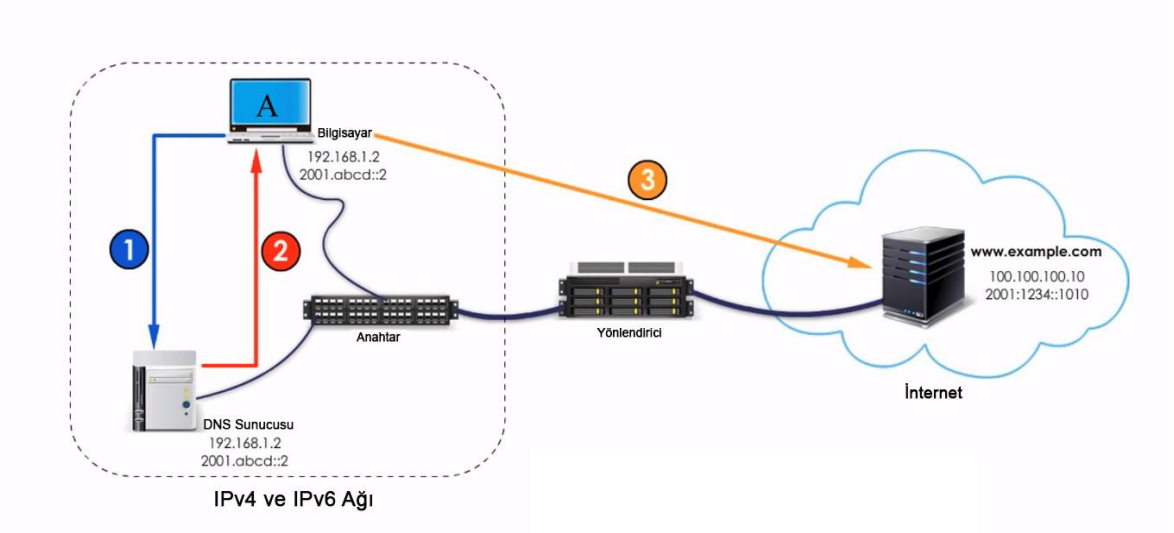
# 2. IPV6 GEÇİŞ YÖNTEMLERİ

IETF, IPv4 ağlarının IPv6 ağlarıyla paralel olarak bir arada bulunmasına ve sorunsuz bir şekilde iletişim kurmasına izin vermek için birçok geçiş yöntemi geliştirmiştir. Çeşitli geçiş yöntemleri üç kategoriye ayrılabilir: İkili Yığın Yöntemi (Dual Stack Method), Çeviri Yöntemi (Translation Method) ve Tünelleme Yöntemi (Tunelling Method).

Tünelleme yöntemi, manuel tünelleme veya otomatik tünelleme olabilir. Otomatik tünelleme: Site İçinde Otomatik Tünel Adresleme Protokolü (ISATAP-Intra-Site Automatic Tunnel Adresing Protocol) Tünelleme ve 6to4 Tünelleme olabilir [7].

## 2.1. İkili Yığın Yöntemi

İkili yığın yöntemi, en yaygın kullanılan geçiş yöntemidir çünkü basitçe uygulanır ve çoğu işletim sistemi tarafından desteklenir. Adından da anlaşılacağı gibi, her ağ düğümü iki protokol yığınını korur ve her düğüm hem IPv4 hem de IPv6 iletişim yetenekleriyle yapılandırıldığı için bunları aynı düğüm üzerinde paralel olarak çalıştırır [8]. İkili yığın yönlendirici her iki protokolü de destekler ve iki yönlendirme tablosunu yan yana yönetebilmek için yüksek işlem gücüne sahip bir yönlendirici ve bellek gerekir; biri IPv4 ve diğeri IPv6 [7].




Şekil 2.1. İkili yığın ağların haberleşmesi

Şekil 2.1'den, ana bilgisayar A ikili yığınlı bir cihazdır ve example.com'daki uzak sunucuyla aşağıdaki gibi iletişim kurmak ister:

***Adım 1:*** Ana bilgisayar A, Alan Adı Sistemi (DNS-c) Sunucusuyla bağlantı kurarak example.com'un tüm mevcut IP adreslerini sorar.

***Adım 2:*** DNS Sunucusu isteği alır ve hem IPv4 hem de IPv6 adresleriyle yanıt verir ve ana bilgisayar A, kullanılacak IPv4 veya IPv6'yı seçecektir. Çoğu durumda, IPv6 varsayılan olarak seçilir.

***Adım 3:*** IPv6 oturumu kuruldu.

IPv6'nın example.com'daki sunucuyla çalışmaması durumunda, istemci IPv4'ü kullanarak iletişimi yeniden kurmayı deneyeceğinden, istemci biraz gecikme yaşayabilir. Böylece, müşteri sunucuya iki deney yapacaktır.

## 2.2. Çeviri Yöntemi

Çeviri Yöntemi, IPv6 ağı içindeki düğümlerin başka bir ağdaki IPv4 düğümlerine erişmesi gerektiğinde kullanılır. Çeviri yönteminde aktarım için temel yapı taşı, sınırlanmış yönlendiricidir (Çeviri Yönlendirici). Çeviri yönlendiricinin ağ adreslerini ve protokollerini IPv6'dan IPv4'e ve tersi yönde çevirmek için görev aldığı yerde [9].

Geçiş sürecinde, IPv4'ün IPv6 ile bir arada bulunmasına izin veren birkaç çeviri yöntemi vardır. Bu yöntemlerden bir tanesi Ağ Adresi Çevirisi IPv6'dan IPv4'e (NAT6-4-Network Address Translation IPv6 to IPv4) yöntemidir ve bu yöntem, NAT6-4 Öneki, DNS6-4 Sunucusu (DNS6-4 Domain Name System 6to4) ve NAT6-4 Yönlendirici olmak üzere uç bileşen içermektedir [18].

*1. NAT6-4 Öneki*

NAT6-4 Öneki, ağa özgü bir önek (NSP-Network-Specific Prefix ) veya iyi bilinen bir önek (WKP-Well-Known Prefix) olabilir.

Bir NSP, bir kuruluş tarafından atanır veya belirlenir.

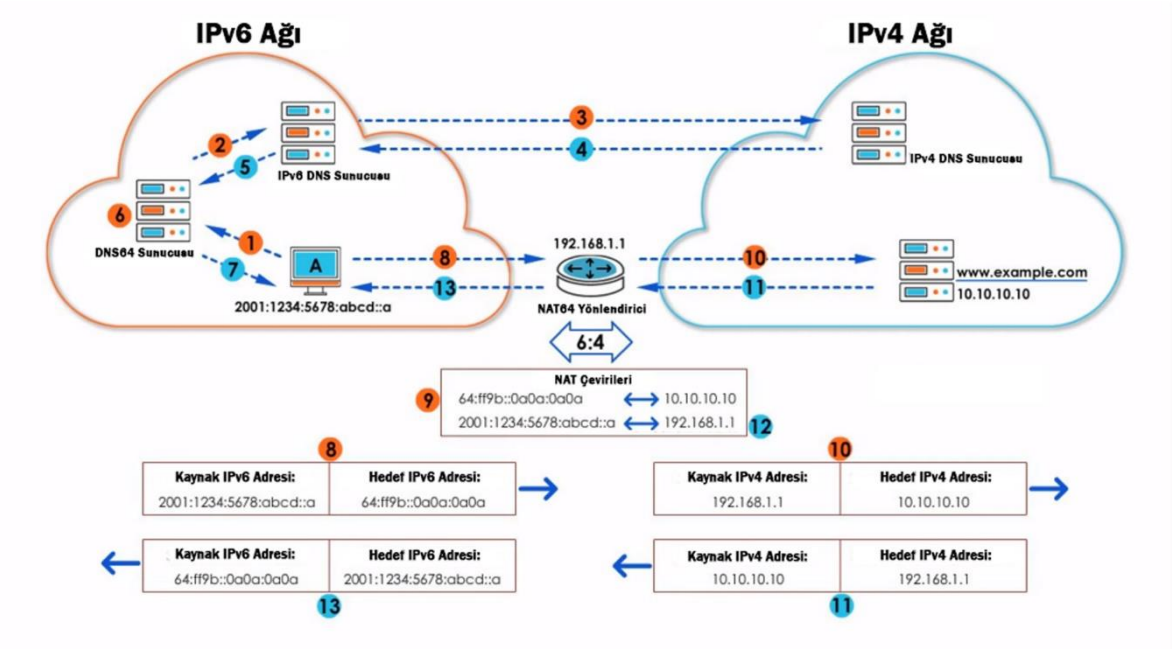
NAT6-4 için WKP 64: FF9B::/ 96'dır.

*2. DNS6-4 Sunucusu*

DNS6-4 Sunucusu, süreçteki önemli bir bileşendir. Hem IPv6 hem de IPv4 için DNS sunucusudur.

*3. NAT6-4 Yönlendirici*

NAT6-4 önekini yalnızca IPv6 ağına tanıtır ve yalnızca IPv6 ile yalnızca IPv4 ağları arasında çeviriyi gerçekleştirir.




Şekil 2.2. NAT6-4 yöntemi ağların haberleşmesi

Şekil 2.2'den, ana bilgisayar A yalnızca IPv6 cihazdır ve example.com'daki uzak sunucuyla aşağıdaki gibi iletişim kurmak ister:

***Adım 1:*** Ana Bilgisayar A, DNS6-4 Sunucusuyla bağlantı kurarak example.com sunucusu için ipv6 adresini sorar.

***Adım 2:*** DNS6-4 sunucusu böyle bir kayıt içermez, bu durumda DNS6-4 sunucusu IPv6 DNS sunucusuna sorar.

***Adım 3:*** IPv6 DNS sunucusu "example.com'un IPv6 adresini bulamadım ancak IPv4 adresini isteyebilirim" diye yanıtını verir.

***Adım 4:*** IPv4 DNS sunucusu, example.com 10.10.10.10 IPv4 adresiyle yanıt verir.

***Adım 5:*** example.com 10.10.10.10'un IPv4 adresi DNS64 sunucusuna iletilir.

***Adım 6:*** DNS6-4 sunucusu, onaltılık sayılarda IPv4 adresine 64: FF9B::/96 önekini ekleyerek example.com sunucusu için bir NAT6-4 adresi oluşturur, 0A0A:0A0A, bu da example.com için NAT6-4 adresinin tamamı 64'tür. :FF9B::0A0A:0A0A

***Adım 7:*** DNS6-4 sunucusu, A ana bilgisayarına 64: FF9B::0A0A:0A0A adresi verir.

***Adım 8:*** Ana Bilgisayar A, example.com için hedef IPv6 adresi olarak 64:FF9B:: 0A0A:0A0A adresini kullanır

***Adım 9:*** NAT6-4 yönlendirici, IPv6 ve IPv4 başlığı arasında çeviri yapar.

***Adım 10:*** NAT6-4 çevirisinden sonra çevrilen IPv4 paketi example.com'a iletilir.

***Adım 11:*** example.com sunucusu IPv4 paketiyle NAT6-4 yönlendiricisine yanıt verir.

***Adım 12:*** NAT6-4 yönlendirici, Ipv4 paketini ipv6 paketine çevirir.

***Adım 13:*** Çeviriden sonra IPv6 paketi A ana bilgisayarına iletilir.

### 2.3. Tünelleme Yöntemi

Tünelleme yöntemi, doğrudan bağlı olmayan IPv6 ya da IPv4 ağlarının bağlanmaya gerektiğinde kullanılır. Bir IPv6 paketi bir IPv4 tünelinde aktarıldığında veya bunun tersi olduğunda, orijinal paketin başlığı ve yükü, IPv4 altyapıları üzerinden taşınmasına izin vermek için IPv4 başlığında kapsüllendiğinden değiştirilmez. Tünelin her iki ucunda, aktarılan IPv6 paketi kapsüllenir ve kapsüllenir. Bu nedenle, tünel yönlendiricisinin her iki ucu hem IPv4 hem de IPv6'yı desteklemelidir [10].

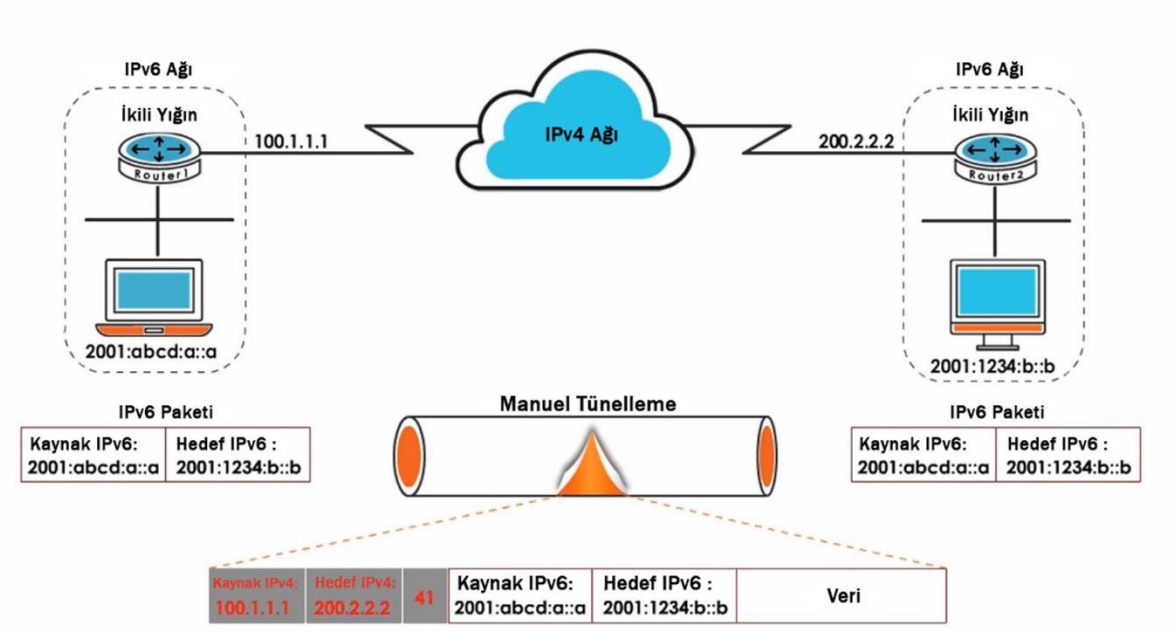
Genel olarak, Tünelleme yöntemi manuel tünelleme ve otomatik tünelleme (6to4 ve ISATAP) kategorilerine ayrılmıştır [11].

#### 2.3.1. Manuel tünelleme yöntemi

Manuel Tünelleme, yönlendiriciler arasında noktadan noktaya bir bağlantıdır. Tüm ana bilgisayarların yapılandırmaya ihtiyacı yoktur çünkü sınır yönlendiricileri o işi yapar.

Uygulanması basittir, ancak bu yöntem iyi ölçeklenemez çünkü eğer yeni bir yönlendirici ağa eklenmesi gerekiyorsa tüm mevcut yönlendiricilerde yeni bir tünelin yapılandırılması gerekir.

Bazı küçük kuruluşlar için birkaç manuel tünellemeyi yönetmek kabul edilebilirken, diğerleri daha ölçeklenebilir bir çözüm isteyebilir [20].




Şekil 2.3. Manuel tünelleme yöntemi ağların haberleşmesi

Şekil 2.3'ten, ana bilgisayar A ve ana bilgisayar B iki farklı IPv6 ağındadır, yalnızca IPv4 ağı ile ayrılırlar. Sınır yönlendiricileri, noktadan noktaya bağlantı için ikili yığınlıdır.

Ana Bilgisayar A, ana bilgisayar B'ye bir IPv6 paketi göndererek ana bilgisayar B ile iletişim kurmak istiyor.

IPv6 paketi, ana bilgisayar A'dan sol uçtaki yönlendirici 1'e gönderilir, yönlendirici 1, paketi tünel yoluyla yönlendirici 2'ye gönderir ve paket, yönlendirici 2'den sağ uçtaki ana bilgisayar B'ye gönderilir.

Tünelin içinde

Ana bilgisayar A bir IPv6 paketi gönderdiğinde, yönlendirici 1 bunu yeni bir IPv4 paketine dönüştürmek için fazladan IPv4 başlık bilgisi ekler; orijinal IPv6 paketi, yeni IPv4 paketinin yüküdür. Yalnızca bu şekilde, paket IPv4 ağından geçebilir.

Yönlendirici 2, paketi aldığında yönlendirici 2 IPv4 başlığını kaldırır ve orijinal IPv6 paketini geri yükler ve ardından bunu B bilgisayarına teslim eder.

### 2.3.2. Otomatik 6to4 tünelleme yöntemi

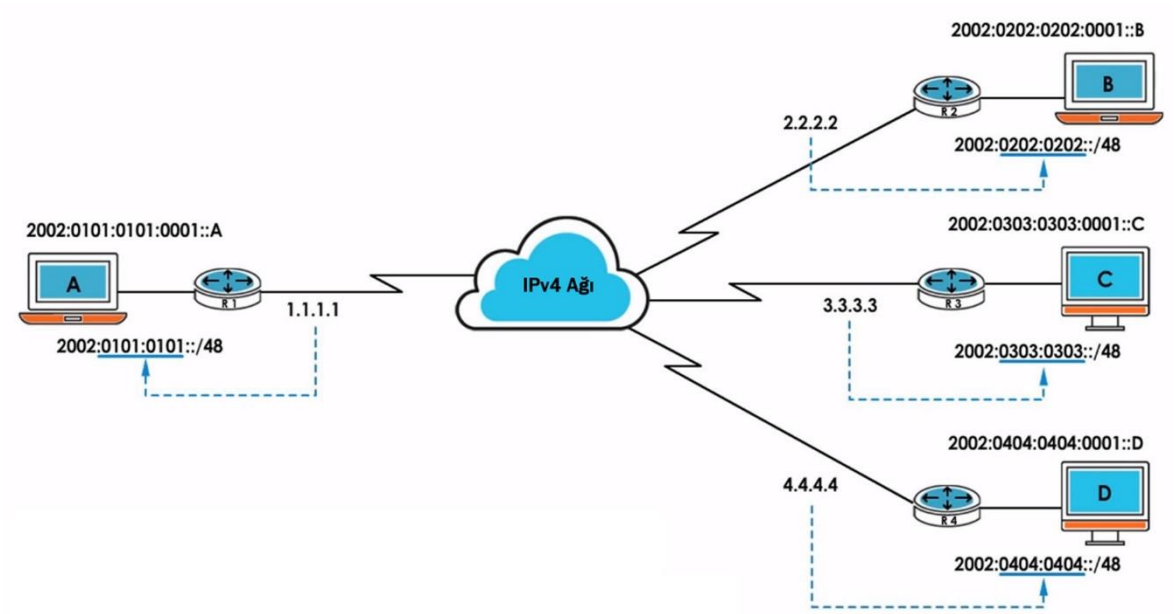
6to4 tünelleme, tek bir tünel üzerinden birden çok IPv6 ağına otomatik olarak bağlanmak için oluşturulur ve birden çok bağlantıya işaret eder.

Başka bir deyişle, Şekil 2.4'te gösterildiği gibi tek bir 6to4 tüneli, yalnızca IPv4 ağı üzerinden herhangi bir sayıda IPv6 ağı için kullanılabilir.

6to4 tünelleme, temel olarak IPv6 paketlerini yalnızca IPv4 ağından geçebilmeleri için sarmak için IPv4 başlıklarını kullanır.

Manuel tünelleme ile karşılaştırıldığında, 6to4 tünelleme daha ölçeklenebilir, çünkü mevcut 6to4 ağlarına daha fazla yönlendirici eklemek manuel tünelden daha kolaydır [19].

6to4 IPv6 adresinin yapısı




Şekil 2.4. 6to4 IPv6 adresinin yapısı

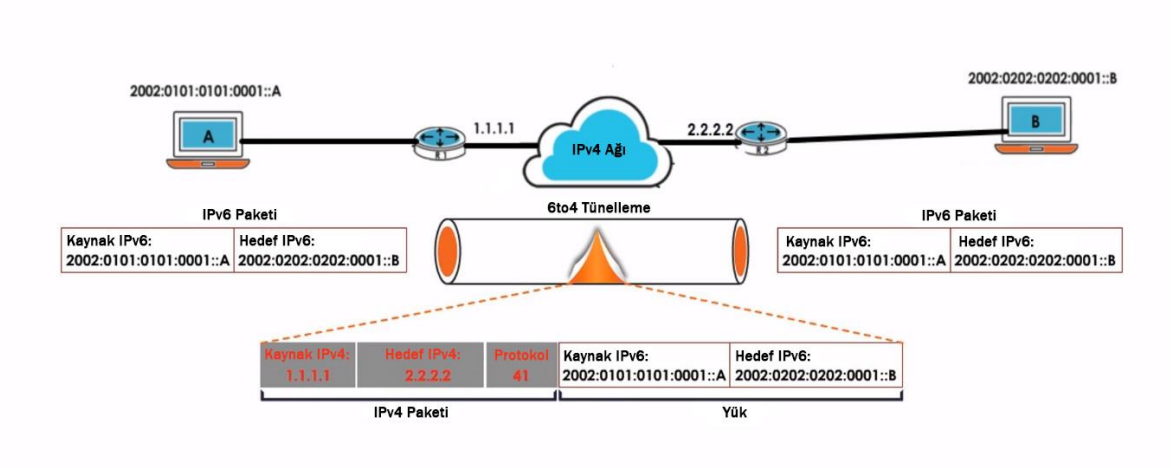
6to4 tünelleme kullanan tüm cihazların özel bir IPv6 adresine ihtiyacı vardır. Şekil 2.4'ten, ana bilgisayar A 6to4 IP adresi 2002:0101:0101::/48'dir. İlk 16-bitlik önek, 6to4 özel öneki 2002'dir ve ardından sınır yönlendiricisinin geniş alan ağı (WAN-Wide Area Network) arabiriminin sınır yönlendiricilerinin 1.1.1.1 32-bitlik IPv4 adresinden dönüştürülen 32 bit uzunluğunda bir onaltılık sayı, ardından alt ağ kimliği ve kendi 64 bit arayüz kimliği [19].

*Aynı ilke B, C ve D ana bilgisayarları için de geçerlidir.*

Otomatik 6to4 tünelleme nasıl çalışır?

Ana bilgisayar A, ana bilgisayar B ile iletişim kurmak istediğini, ana bilgisayar A bir paket göndererek ana bilgisayar B ile iletişim kurmaya başladığını varsayalım.

Ana Bilgisayar A, kaynak IP adresi olarak 6to4 IP adresini ve hedef IP adresi olarak ana bilgisayar B 6to4 IP adresini kullanır. Ana bilgisayar A ve ana bilgisayar B arasında, iletişim IPv6'dan IPv6'ya kadardır, ancak tünel içinde iletişimler IPv4'ten IPv4'e kadardır, çünkü bunlar Şekil 2.5'te gösterildiği gibi yalnızca IPv4 ağıyla ayrılmıştır.




Şekil 2.5. 6to4 tünelleme yöntemi ağların haberleşmesi

*Tünelin içinde*

Paketin kaynak adresi, yönlendirici 1'in IPv4 adresi olan 1.1.1.1'dir ve hedef adresi, yönlendirici 2'nin IPv4 adresi olan 2.2.2.2'dir.

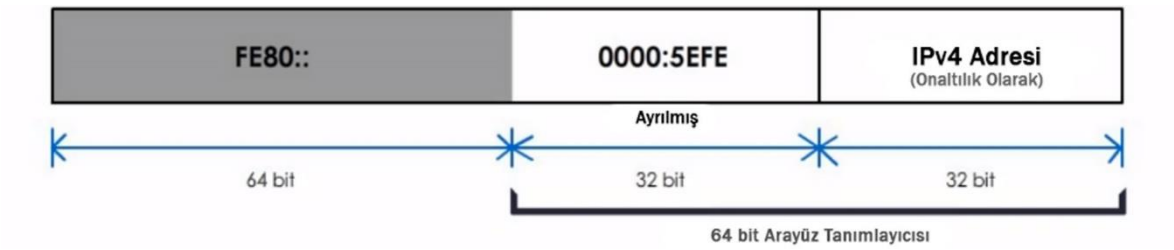
6to4 IP paketi, paketin IPv4 ağından geçebilmesi için IPv4 başlığı tarafından kapsüllenir.

Yönlendirici 2, paketi aldığında yönlendirici 2 IPv4 başlığını kaldırır ve orijinal IPv6 paketini geri yükler ve ardından bunu B bilgisayarına teslim eder.

### 2.3.3. Otomatik ISATAP tünelleme yöntemi

ISATAP, çoğunlukla ana bilgisayarlar ve yönlendiriciler veya Katman 3 anahtarları arasında kullanılan başka bir otomatik tünel oluşturma yöntemidir, ancak yönlendiriciler arasında manuel tüneller kullanılır. ISATAP tüneli, ana bilgisayarın ve yönlendiricinin IPv4 adresleri kullanılarak oluşturulur. ISATAP tüneli, ana bilgisayara ihtiyaç duyduğunda otomatik olarak oluşturulur [12].

ISATAP IPv6 adres biçimi - yerel bağlantı



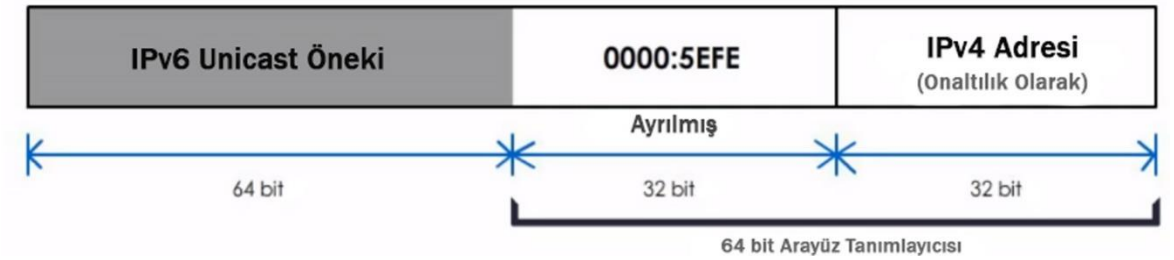

Şekil 2.6. ISATAP IPv6 adres biçimi - yerel bağlantı

ISATAP IPv6 adres bağlantısı yerel, Şekil 2.6'da gösterildiği gibi üç bölümden oluşur [21]:

- İlk 64-bit FE80: , ardından özel ayrılmış kimlik ve ardından IPv4 adresinden dönüştürülmüş 32-bit uzunluğunda onaltılık bir sayı gelir.

- İkinci ve üçüncü kısım birlikte arayüz tanımlayıcıdır.

ISATAP IPv6 adres biçimi - global tek noktaya (Unicast) yayın




Şekil 2.7. ISATAP IPv6 adres biçimi - global tek noktaya yayın

ISATAP IPv6 adresi global tek noktaya yayın da Şekil 2.7'de gösterildiği gibi üç bölümden oluşur:

- İlk bölüm 64 bitlik tek noktaya yayın önekidir, ardından özel ayrılmış kimlik ve ardından IPv4 adresinden dönüştürülmüş 32 bit uzunluğunda onaltılık bir sayı gelir.

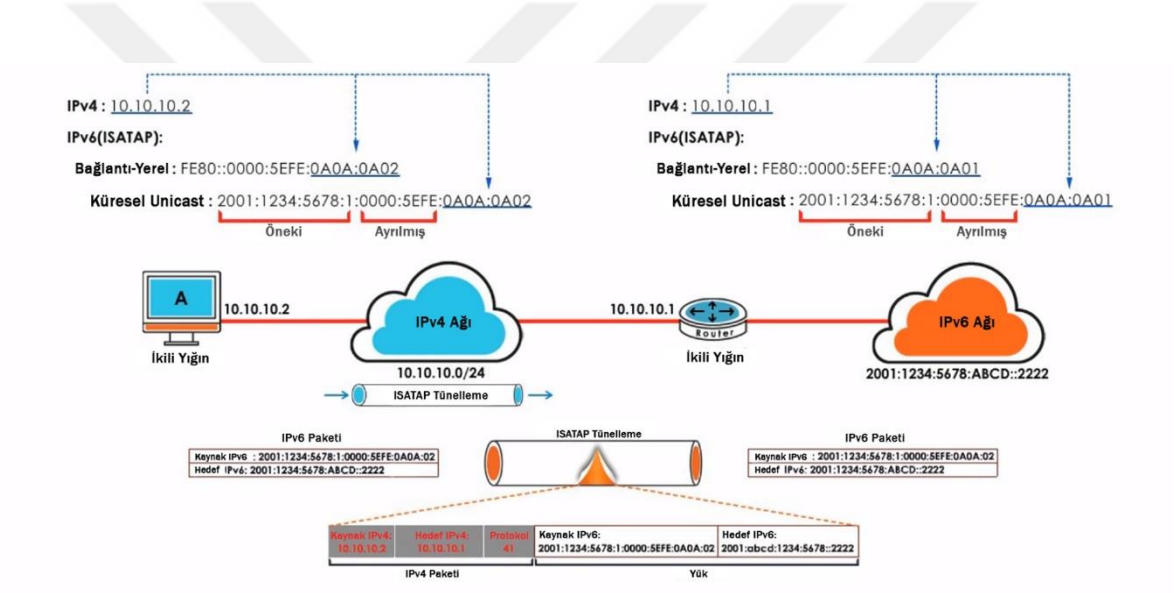
- İkinci ve üçüncü bölümler 64 bit arayüz tanımlayıcıdır.

*Otomatik ISATAP tünelleme nasıl çalışır?*

Diğer tünel oluşturma yöntemleri gibi, herhangi iki İkili yığınlı aygıt arasında, ana bilgisayardan yönlendiriciye veya ana bilgisayardan ana makineye bir ISATAP tüneli olabilir.

Ancak, ISATAP tünellemenin ana özelliği, yalnızca IPv4 ağı üzerinden IPv6 ağına ikili yığınlı ana bilgisayarlara erişim sağlamaktır.

Şekil 2.8'den, ana bilgisayar A, IPv4 ağında oturuyor, ancak ikili yığınlı cihaz olarak yapılandırılıyor [12].




Şekil 2.8. ISATAP tünelleme yöntemi ağların haberleşmesi

Sağ tarafta, yönlendirici bir ISATAP yönlendiricisi olarak yapılandırılmıştır, IPv6 bağlantısı yerel ve genel tek noktaya yayını, ana bilgisayar A ile aynı şekilde yapılandırılır.

Bu nedenle, ana bilgisayar A, yalnızca sağdaki IPv6 ağındaki herhangi bir ana bilgisayara bir paket gönderirken, önce yönlendiriciyle IPv4 protokolleriyle iletişim kurar.

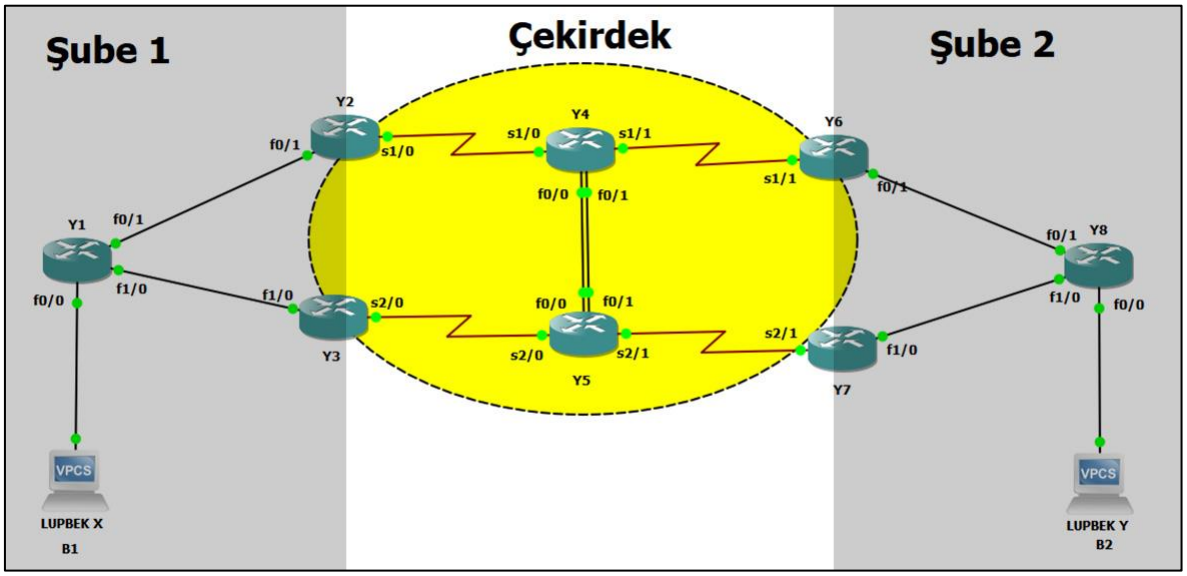
ISATAP yönlendiricisi IPv4 paketini aldığında, IPv4 başlığını çıkarır ve IPv6 paketini yalnızca Ipv6 ağındaki ana bilgisayara teslim eder.

# 3. AĞ TASARIMI

Bu bölüm, Şekil 3.1'de gösterildiği gibi çekirdeğe bağlı iki YPTE Şubesinin tasarımını içerir. YPTE Çekirdeği, uçta diğer dağıtım yönlendiricileriyle birlikte esas olarak altı yönlendiriciye sahiptir. Şekil 3.2, YPTE'nin iki kolunu birbirine bağlayan çekirdeği göstermektedir.

Şekil 3.1. YPTC mimarisi

Şekil 3.2, kenar yönlendiricilerine bağlı bir erişim yönlendiricisini kullanarak iki şubeli çekirdek üzerinden bağlamak için gerekli yönlendiricilerin dağıtımını çizen öykünme diyagramını açıklar.




Şekil 3.2. YPTC ağ topolojisi

Çizelge 3.1, Şube 1 ve Şube 2’deki yönlendiricilerin, kısa bir mesafede daha iyi iletişim kurmak için hızlı ethernet bağlantıları kullandığını göstermektedir. Öte yandan, hem kollar hem de çekirdek yönlendiriciler arasındaki bağlantı, uzun mesafeli bağlantılar için kullanılan seridir. Çekirdek yönlendiricilerin, çekirdek binada oldukları için hızlı ethernet ile bağlandığına dikkat edin. Çekirdek ağda iki ana yönlendirici (Y4, Y5) bulunur, ayrıca kenar yönlendiricileri (Y2, Y3, Y6, Y7) çekirdek ve erişim yönlendiricileri arasında paylaşılır.

Çizelge 3.1. YPTC ağ tasarımı

| Yönlendirici | Şube 1 | Şube 2 | Çekirdek |
|---|---|---|---|
| Giriş | Y1,B1 | Y6,B2 | |
| Dağıtım kenarı | Y3,Y2 | Y6,Y7 | |
| Çekirdek | | | Y4,Y5,Y2,Y3,Y6,Y7 |

### 3.1. YPTC Şubesi 1

Şekil 3.2'den, Yönlendiriciler (Y1, Y2 ve Y3), Şube 1'in çekirdeğe çıkması için ağ geçidini oluşturur. Kenar yönlendiriciler (Y2, Y3) istemcisi (B1) ile bağlı erişim yönlendiricisi (Y1). Çizelge 3.2, Şube 1'in arayüzlerini göstermektedir.

Çizelge 3.2. YPTC şube 1'in arayüz şeması

| Yönlendirici | Arayüzler | Komşular | Komşu Arayüzleri |
|---|---|---|---|
| Y1 | Hızlı Ethernet 0/0 | B1 | LUPBEK X |
| | Hızlı Ethernet 0/1 | Y2 | Hızlı Ethernet 0/1 |
| | Hızlı Ethernet 1/0 | Y3 | Hızlı Ethernet 1/0 |
| Y2 | Hızlı Ethernet 0/1 | Y1 | Hızlı Ethernet 0/1 |
| | Seri Arayüz 1/0 | Y4 | Seri Arayüz 1/0 |
| Y3 | Hızlı Ethernet 1/0 | Y1 | Hızlı Ethernet 1/0 |
| | Seri Arayüz 2/0 | Y5 | Seri Arayüz 2/0 |
| B1 | LUPBEK X | Y1 | Hızlı Ethernet 0/0 |

### 3.2. YPTC Çekirdek

Şekil 3.2'den, Yönlendiriciler (Y2, Y3, Y4, Y5, Y6 ve Y7), her iki şubeli birbirine bağlayan YPTC Çekirdek Ağını oluşturur. Çizelge 3.3, YPTC çekirdeğinin arayüzlerini göstermektedir.

Çizelge 3.3. YPTC çekirdeğinin arayüz şeması

| Yönlendirici | Arayüzler | Komşular | Komşu Arayüzleri |
|---|---|---|---|
| Y4 | Hızlı Ethernet 0/0 | Y5 | Hızlı Ethernet 0/0 |
| | Hızlı Ethernet 0/1 | | Hızlı Ethernet 0/1 |
| | Seri Arayüz 1/0 | Y2 | Seri Arayüz 1/0 |
| | Seri Arayüz 1/1 | Y6 | Seri Arayüz 1/1 |
| Y5 | Hızlı Ethernet 0/0 | Y4 | Hızlı Ethernet 0/0 |
| | Hızlı Ethernet 0/1 | | Hızlı Ethernet 0/1 |
| | Seri Arayüz 2/0 | Y3 | Seri Arayüz 1/0 |
| | Seri Arayüz 2/1 | Y7 | Seri Arayüz 1/1 |

### 3.3. YPTC Şubesi 2

Şekil 3.2'den, Yönlendiriciler (Y6, Y7 ve Y8), Şube 2'nin çekirdeğe çıkması için ağ geçidini oluşturur. Erişim Yönlendiricisi (Y8) ile uç yönlendiriciler (Y6, Y7) ve istemci (B2) bağlıdır. Çizelge 3.4, Şube 2'nin arayüzlerini göstermektedir.

Çizelge 3.4. YPTC şube 2'nin arayüz şeması

| Yönlendirici | Arayüzler | Komşular | Komşu Arayüzleri |
|---|---|---|---|
| Y6 | Seri Arayüz 1/1 | Y4 | Seri Arayüz 1/1 |
| | Hızlı Ethernet 0/1 | Y8 | Hızlı Ethernet 0/1 |
| Y7 | Seri Arayüz 2/1 | Y5 | Seri Arayüz 2/1 |
| | Hızlı Ethernet 1/0 | Y8 | Hızlı Ethernet 1/0 |
| Y8 | Hızlı Ethernet 0/0 | B2 | LUPBEK Y |
| | Hızlı Ethernet 0/1 | Y6 | Hızlı Ethernet 0/1 |
| | Hızlı Ethernet 1/0 | Y7 | Hızlı Ethernet 1/0 |
| B2 | LUPBEK Y | Y8 | Hızlı Ethernet 0/0 |

# 4. SİMÜLASYONLAR

Bu bölüm tezin uygulama bölümünü içerir GNS3 öykünücüsünü kullanarak YPTC'nin iki şubesi arasında simüle ederek üç senaryo üzerinden YPTC ağ topolojisi için en uygun yöntemi seçmek üzere tezde önerilen geçiş yöntemlerini simüle eder.

Aşağıda listelenen üç senaryo altında uygulanmıştır:

1- İkili Yığın Senaryosu.

2- Çeviri Senaryosu.

3- Tünelleme Senaryosu.

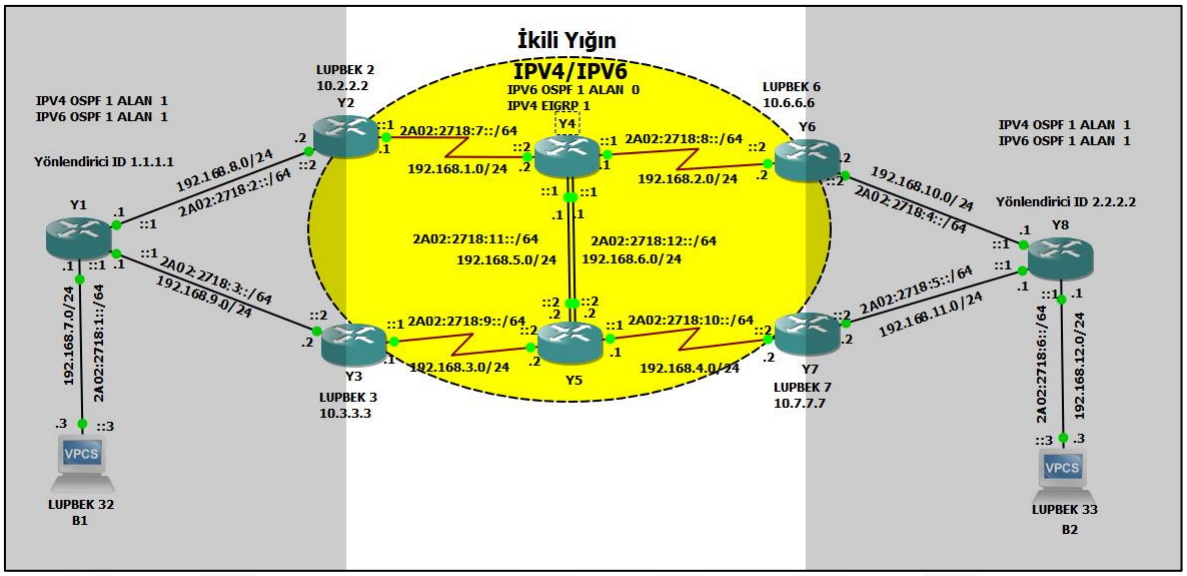
## 4.1. Geçiş Yöntemleri Senaryoları

Simülasyonlar senaryoları IPv6 adresleme şeması için aralığı (2A02:2718::/29) kullanırken, IPv4 adreslerinde özel adresleme şemasını (192.168.0.0/24) ve ayrıca geri döngü adresleme şeması için (10.2.2.2) kullandı.

### 4.1.1. İkili yığın senaryosu

Bu yöntemin temel yapı taşı, IPv6 paketini IPv4 paketine kapsüllemekten sorumlu olan tünel yönlendiricisidir ve bunun tersi, Şekil 3.4'teki Y4 ve Y5 tünel yönlendiricileri olarak yapılandırılmıştır.

Manuel Tünelleme, 6to4 Tünelleme ve ISATAP Tünelleme, her yöntemle orantılı yönlendirici ayarları ile bu tasarımda üç farklı senaryoda uygulanmıştır.




Şekil 4.1. İkili yığın senaryosu topolojisi

• <u>Şube 1</u>

Şekil 4.1'den, Yönlendiriciler (Y1, Y2 ve Y3), Çizelge 4.1'de gösterildiği gibi belirli bir IP adresleme şeması aracılığıyla şubesi 1 oluşturur.

Çizelge 4.1. İkili yığın yöntemi şube 1'in IP adresleme şeması

| Yönlendirici | Arayüzler | IP Adres |
|---|---|---|
| Y1 | Hızlı Ethernet 0/0 | 2A02:2718:1::1/64<br>192.168.7.1/24 |
| | Hızlı Ethernet 0/1 | 2A02:2718:2::1/64<br>192.168.8.1/24 |
| | Hızlı Ethernet 1/0 | 2A02:2718:3::1/64<br>192.168.9.1/24 |
| Y2 | Hızlı Ethernet 0/1 | 2A02:2718:2::2/64<br>192.168.8.2/24 |
| | Seri Arayüz 1/0 | 2A02:2718:7::1/64<br>192.168.1.1/24 |
| | LUPBEK 2 | 10.2.2.2/24 |
| Y3 | Hızlı Ethernet 1/0 | 2A02:2718:3::2/64<br>192.168.9.2/24 |
| | Seri Arayüz 2/0 | 2A02:2718:9::1/64<br>192.168.3.1/24 |
| | LUPBEK 3 | 10.3.3.3/24 |
| B1 | LUPBEK 34 | 2A02:2718:1::3/64<br>192.168.7.3 |

• *Çekirdek*

Şekil 4.1'den, Yönlendiriciler (Y2, Y3, Y4, Y5, Y6 ve Y7) her iki şubesi birbirine bağlayan çekirdeği oluşturur. Çizelge 4.2 çekirdeğin IP adresleme şeması gösterilmektedir.

Çizelge 4.2. İkili yığın yöntemi çekirdeğin IP adresleme şeması

| Yönlendirici | Arayüzler | IP Adres |
|---|---|---|
| Y4 | Hızlı Ethernet 0/0 | 2A02:2718:11::1/64<br>192.168.5.1/24 |
| | Hızlı Ethernet 0/1 | 2A02:2718:12::1/64<br>192.168.6.1/24 |
| | Seri Arayüz 1/0 | 2A02:2718:7::2/64<br>192.168.1.2/24 |
| | Seri Arayüz 1/1 | 2A02:2718:8::1/64<br>192.168.2.1/24 |
| Y5 | Hızlı Ethernet 0/0 | 2A02:2718:11::1/64<br>192.168.5.1/24 |
| | Hızlı Ethernet 0/1 | 2A02:2718:12::1/64<br>192.168.6.1/24 |
| | Seri Arayüz 1/0 | 2A02:2718:7::2/64<br>192.168.1.2/24 |
| | Seri Arayüz 1/1 | 2A02:2718:8::1/64<br>192.168.2.1/24 |

• <u>Şube 2</u>

Şekil 4.1'den, Yönlendiriciler (Y6, Y7 ve Y8), Çizelge 4.4'te gösterildiği gibi belirli bir IP adresleme şeması aracılığıyla şubesi 2 oluşturur.

Çizelge 4.3. İkili yığın yöntemi şube 2'nin IP adresleme şeması

| Yönlendirici | Arayüzler | IP Adres |
|---|---|---|
| Y6 | Seri Arayüz 1/1 | 2A02:2718:8::2/64<br>192.168.2.2/24 |
| | Hızlı Ethernet 0/1 | 2A02:2718:4::2/64<br>192.168.10.2/24 |
| | LUPBEK 6 | 10.6.6.6/24 |
| Y7 | Seri Arayüz 2/1 | 2A02:2718:10::2/64<br>192.168.4.2/24 |
| | Hızlı Ethernet 1/0 | 2A02:2718:5::2/64<br>192.168.11.2/24 |
| | LUPBEK 7 | 10.7.7.7/24 |

Çizelge 4.3. (devam) İkili yığın yöntemi şube 2'nin IP adresleme şeması

| | | |
|---|---|---|
| Y8 | Hızlı Ethernet 0/0 | 2A02:2718:4::2/64<br>192.168.10.2/24 |
| | Hızlı Ethernet 0/1 | 2A02:2718:4::1/64<br>192.168.10.1/24 |
| | Hızlı Ethernet 1/0 | 2A02:2718:5::1/64<br>192.168.11.1/24 |
| B2 | LUPBEK 33 | 2A02:2718:6::3/64<br>192.168.12.3/24 |

Her bir etkin boğumda IPv4 ve IPv6 yapılandırıldıktan sonra, ana bilgisayar B1'den ana bilgisayar B2'ye iletişimi mümkün kılmak için tüm yönlendiricilerdeki ağları tanımlamak için yönlendirme protokollerine ihtiyaç duyar, tüm yönlendiricilerde yönlendirme protokolleri oluşturulmalıdır. Bunu başarmak için, bir ağda iki tür protokol kullanıldı, hem IPv4 hem de IPv6'da OSPF (OSPF- Open Shortest Path First) yönlendirme protokolü ve çekirdek ağda IPv4'te EIGRP (EIGRP-Enhanced Interior Gateway Routing Protocol) yönlendirme protokolü de kullanıldı.

OSPF yönlendirme protokolü, hem IPv4 hem de IPv6 ağları için her iki şubede, şube 1 ve şube 2'de yapılandırılırken, çekirdek ağ, IPv6 için OSPF yönlendirme protokolü ve IPv4 için EIGRP yönlendirme protokolüne sahiptir.

Tüm ağı yalnızca bir yönlendirme protokolüyle yapılandırmak kolaydır, ancak IPv4 ağları için ağ, her iki şubede iki farklı yönlendirme protokolü OSPF ve çekirdekte EIGRP ile çalışır.

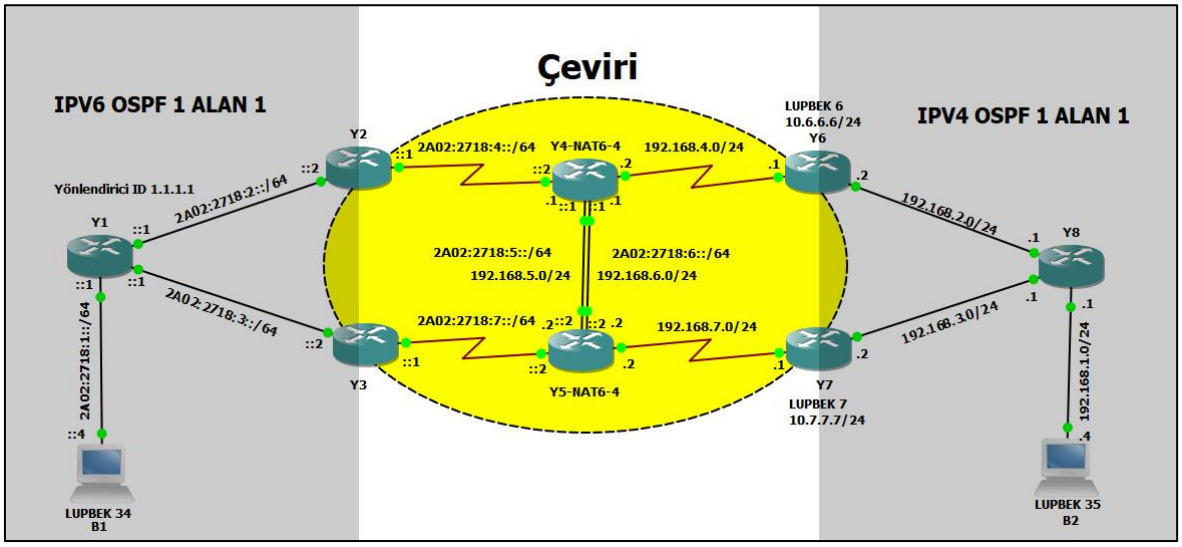
IP yönlendirme protokollerinin iki farklı sürümü arasındaki uyumluluk için, IPv4 ağlarının tümünde tam yakınsamasını sağlamak için, uç yönlendiricilerdeki (Y2, Y3, Y6 ve Y7) OSPF ve EIGRP arasında yeniden dağıtım sürecini kurmalıdır, sonunda uçtan uca bağlantıya yol açan yönlendiriciler.

Yapılandırma komutları Ek 1'de yer almaktadır.

### 4.1.2. Çeviri senaryosu

Bölüm 2'de bahsedildiği gibi, bu yöntemin temel yapı taşı, IPv6'dan IPv4 adreslerine çevirmekten sorumlu olan NAT6-4 yönlendiricidir ve bunun tersi, yalnızca IPv6 aygıtlarının yalnızca IPv4 aygıtlarıyla iletişim kurmasına olanak tanır.

Bu yöntem ikili yığın veya Tünellemenin yerini almaz; sadece IPv4 ve IPv6 ana bilgisayarları ve cihazları arasında doğrudan bağlantı istendiğinde uygulanır.




Şekil 4.2. Çeviri senaryosu topolojisi

• <u>Şube 1</u>

Şekil 4.3'ten, Yönlendiriciler (Y1, Y2 ve Y3), Çizelge 4.7'de gösterildiği gibi belirli bir IP adresleme şeması aracılığıyla şubesi 1 oluşturur.

Çizelge 4.4. Çeviri yöntemi şube 1'in IP adresleme şeması

| Yönlendirici | Arayüzler | IP Adres |
|---|---|---|
| Y1 | Hızlı Ethernet 0/0 | 2A02:2718:1::1/64 |
| | Hızlı Ethernet 0/1 | 2A02:2718:2::1/64 |
| | Hızlı Ethernet 1/0 | 2A02:2718:3::1/64 |
| Y2 | Hızlı Ethernet 0/1 | 2A02:2718:2::2/64 |
| | Seri Arayüz 1/0 | 2A02:2718:4::1/64 |
| Y3 | Hızlı Ethernet 1/0 | 2A02:2718:3::2/64 |
| | Seri Arayüz 2/0 | 2A02:2718:7::1/64 |
| B1 | LUPBEK 34 | 2A02:2718:1::4/64 |

- *Çekirdek*

Şekil 4.3'ten Yönlendiriciler (Y2, Y3, Y4, Y5, Y6 ve Y7) her iki şubesi birbirine bağlayan çekirdeği oluşturur. Çekirdek için IP adresleme şeması Çizelge 4.8'de gösterilmektedir.

Çizelge 4.5. çeviri yöntemi çekirdeğin IP adresleme şeması

| Yönlendirici | Arayüzler | IP Adres |
|---|---|---|
| Y4 | Hızlı Ethernet 0/0 | 2A02:2718:5::1/64<br>192.168.5.1/24 |
| | Hızlı Ethernet 0/1 | 2A02:2718:6::1/64<br>192.168.6.1/24 |
| | Seri Arayüz 1/0 | 2A02:2718:4::2/64 |
| | Seri Arayüz 1/1 | 192.168.4.2/24 |
| Y5 | Hızlı Ethernet 0/0 | 2A02:2718:5::2/64<br>192.168.5.2/24 |
| | Hızlı Ethernet 0/1 | 2A02:2718:6::2/64<br>192.168.6.2/24 |
| | Seri Arayüz 2/0 | 2A02:2718:7::2/64 |
| | Seri Arayüz 2/1 | 192.168.7.2/24 |

- <u>Şube 2</u>

Şekil 4.3'ten, Yönlendiriciler (Y6, Y7 ve Y8), Çizelge 3.9'da gösterildiği gibi belirli bir IP adresleme şeması aracılığıyla şubesi 2 oluşturur.

Çizelge 4.6. Çeviri yöntemi şube 2'nin IP adresleme şeması

| Yönlendirici | Arayüzler | IP Adres |
|---|---|---|
| Y6 | Seri Arayüz 1/1 | 192.168.4.1/24 |
| | Hızlı Ethernet 0/1 | 192.168.2.2/24 |
| | LUPBEK 6 | 10.6.6.6/24 |
| Y7 | Seri Arayüz 2/1 | 192.168.7.1/24 |
| | Hızlı Ethernet 1/0 | 192.168.3.2/24 |
| | LUPBEK 7 | 10.7.7.7/24 |
| Y8 | Hızlı Ethernet 0/0 | 192.168.1.1/24 |
| | Hızlı Ethernet 0/1 | 192.168.2.1/24 |
| | Hızlı Ethernet 1/0 | 192.168.3.1/24 |
| B2 | LUPBEK 35 | 192.168.1.4/24 |

Her bir etkin boğumda IP'yi yapılandırdıktan sonra, ağdaki tüm IPv6 arabirimleri için (topolojinin sol bölümü) OSPF v3 yönlendirme protokolü, ayrıca IPv4 ağları (topolojinin sağ bölümü) OSPF v2 işlemi ile yapılandırılmıştır.

NAT6-4 yöntemi yapılandırmaları, çekirdek yönlendiricilerde (Y4, Y5) yalnızca hem IPv4 hem de IPv6 ağlarına bağlı yönlendiricilerin arabirimlerinde çeviri işlemi etkinleştirilerek uygulanmıştır.

IPv4 adresleri 2A02:2718::/96 önekine çevrilirken, IPv6 adresleri adreslere çevrilirken, 192.168.4.0/24 olan Y4 ile doğrudan bağlanan ilk IPv4 ağına aittir.

Yapılandırma komutları Ek 2'de yer almaktadır.

### 4.1.3. Tünelleme senaryosu

Bölüm 2'de bahsedildiği gibi, bu yöntemin temel yapı taşı, IPv6 paketini IPv4 paketine kapsüllemekten sorumlu olan tünel yönlendiricidir ve bunun tersi de geçerlidir.

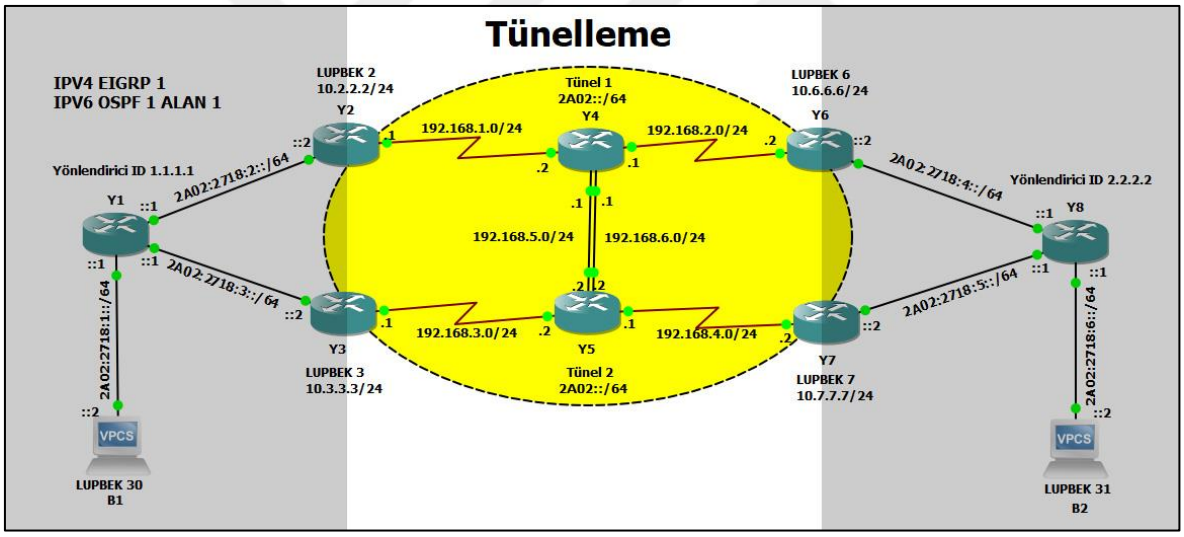
Tünelleme yöntemi yapılandırması

1. IPv6 tek noktaya yayın yönlendirmesi, IPv6 kullanan her yönlendiricide etkinleştirilmelidir.

2. IPv6 ayrıca tünellerin içinde ve ayrıca her iki Şubenin, Şube 1 ve Şube 2'nin Yönlendiricilerindeki IPv6 arabirimlerinin içinde etkinleştirilmelidir.

3. Topolojinin ana yönlendirme altyapısı, ağdaki tüm IPv6 arayüzleri için OSPF süreci kullanılarak uygulanırken, tüm IPv4 ağları için EIGRP süreci oluşturulmuştur.

Manuel Tünelleme, 6to4 Tünelleme ve ISATAP Tünelleme, her yöntemle orantılı yönlendirici ayarları ile bu tasarımda üç farklı senaryoda uygulanmıştır.




Şekil 4.3. Tünelleme senaryosu topolojisi

• Şube 1

Şekil 4.2'den, Yönlendiriciler (Y1, Y2 ve Y3), Çizelge 4.4'te gösterildiği gibi belirli bir IP adresleme şeması aracılığıyla şubesi 1 oluşturur.

Çizelge 4.7. Tünelleme yöntemi şube 1'in IP adresleme şeması

| Yönlendirici | Arayüzler | IP Adres |
|---|---|---|
| Y1 | Hızlı Ethernet 0/0 | 2A02:2718:1::1/64 |
| | Hızlı Ethernet 0/1 | 2A02:2718:2::1/64 |
| | Hızlı Ethernet 1/0 | 2A02:2718:3::1/64 |
| Y2 | Hızlı Ethernet 0/1 | 2A02:2718:2::2/64 |
| | Seri Arayüz 1/0 | 192.168.1.1/24 |
| Y3 | Hızlı Ethernet 1/0 | 2A02:2718:3::2/64 |
| | Seri Arayüz 2/0 | 192.168.3.1/24 |
| B1 | LUPBEK 30 | 2A02:2718:1::4/64 |

- *Çekirdek*

Şekil 4.2'den, Yönlendiriciler (Y2, Y3, Y4, Y5, Y6 ve Y7) her iki şubesi birbirine bağlayan çekirdeği oluşturur. Çekirdek için IP adresleme şeması Çizelge 4.5'te gösterilmektedir:

Çizelge 4.8. Tünelleme yöntemi çekirdeğin IP adresleme şeması

| Yönlendirici | Arayüzler | IP Adres |
|---|---|---|
| Y4 | Hızlı Ethernet 0/0 | 192.168.5.1/24 |
| | Hızlı Ethernet 0/1 | 192.168.6.1/24 |
| | Seri Arayüz 1/0 | 192.168.1.2/24 |
| | Seri Arayüz 1/1 | 192.168.2.1/24 |
| Y5 | Hızlı Ethernet 0/0 | 192.168.5.2/24 |
| | Hızlı Ethernet 0/1 | 192.168.6.2/24 |
| | Seri Arayüz 2/0 | 192.168.3.2/24 |
| | Seri Arayüz 2/1 | 192.168.4.1/24 |

• Şube 2

Şekil 4.2'den Yönlendiriciler (Y6, Y7 ve Y8), Çizelge 4.6'da gösterildiği gibi belirli bir IP adresleme şeması aracılığıyla şubesi 2 oluşturur.

Çizelge 4.9. Tünelleme yöntemi şube 2'nin ıp adresleme şeması

| Yönlendirici | Arayüzler | IP Adres |
|---|---|---|
| Y6 | Seri Arayüz 1/1 | 192.168.2.2/24 |
| | Hızlı Ethernet 0/1 | 2A02:2718:4::2/64 |
| | LUPBEK 6 | 10.6.6.6/24 |
| Y7 | Seri Arayüz 2/1 | 192.168.4.2/24 |
| | Hızlı Ethernet 1/0 | 2A02:2718:5::2/64 |
| | LUPBEK 7 | 10.7.7.7/24 |
| Y8 | Hızlı Ethernet 0/0 | 2A02:2718:6::1/64 |
| | Hızlı Ethernet 0/1 | 2A02:2718:4::1/64 |
| | Hızlı Ethernet 1/0 | 2A02:2718:5::1/64 |
| B2 | LUPBEK 31 | 2A02:2718:6::2/64 |

Manuel tünelleme senaryosu

Manuel tüneller yontemin yapılandırılması basittir, bu nedenle az sayıda site için kullanışlıdır. Tünellerin sona erdiği kenar yönlendiricilerinin, internet protokolünün her iki sürümünü de çalıştırabilmeleri gerektiğinden, ikili yığınlanmış olmaları gerekir.

Manuel Tünel Yapılandırma Adımları:

***Adım 1:*** Bir tünel tanımlama ve tünel numarasını atama,

*Router (config)# interface Tunnel {number}*

***Adım 2:*** Tünel arayüzünde IPv4'ün devre dışı bırakılması,

*Router (config-if)# no ip Adres*

***Adım 3:*** Tünel arayüzünde IPv6'nın etkinleştirilmesi,

*Router (config-if)# ipv6 enable*

IPv6 etkinken, dinamik olarak verildiği için tünele bir IPv6 adresi verilmesi gerekli değildir veya manuel olarak verilebilir:

*Router (config-if)# ipv6 Adres {IPv6 Adres with prefix}*

***Adım 4:*** Tünele bir kaynak atayın,

*Router(config-if)# tunnel source LUPBEK {IPv4 LUPBEK }*

Geri döngü adı veya IPv4 adresi olabilen tünel kaynağının fiziksel arayüzü seçilebilir.

***Adım 5:*** Tünele bir hedef atayın.

*Router(config-if)# tunnel destination LUPBEK {IPv4 LUPBEK }*

Geri döngü adı veya IPv4 adresi olabilen tünelin hedefinin fiziksel arabirimi seçilebilir.

***Adım 6:*** Tünel tipinin Manuel Tünel olarak tanımlanması,

*Router(config-if)# tunnel mode {ipv6ip}*

Bu komut, Tünel arabiriminin yolcu protokolü olarak IPv6'yı ve hem kapsülleme hem de taşıma protokolü olarak IPv4'ü kullanması için kapsülleme modunu ayarlar.

Manuel Tünel yapılandırmasından sonra, ana bilgisayar B1, ana bilgisayar B1'den ana bilgisayar B2'ye ping komutunu uygulayarak yapılandırılmış tünel aracılığıyla ana bilgisayar B2'ye bağlanabilir.

Yapılandırma komutları Ek 3'te yer almaktadır.

<u>6to4 tünelleme senaryosu</u>

Manuel tünel, çok sayıda tünel için istikrarlı bir teknik değildir, bu nedenle tünel sayısını azaltmak için otomatik 6to4 tünel tekniği geliştirilmiştir.

*6to4 tünel yapılandırma adımları*

***Adım 1:*** Bir tünel tanımlama ve tünel numarasını atama,

*Router (config)# interface Tunnel {number}*

***Adım 2:*** Tünel arayüzünde IPv4'ün devre dışı bırakılması,

*Router (config-if)# no ip Adres*

***Adım 3:*** Tünel arayüzünde IPv6'nın etkinleştirilmesi,

*Router (config-if)# ipv6 enable*

IPv6 etkinken, dinamik olarak verildiği için tünele bir IPv6 adresi verilmesi gerekli değildir veya manuel olarak verilebilir:

*Router (config-if)# ipv6 Adres {IPv6 Adres with prefix}*

***Adım 4:*** Tünele bir kaynak atayın,

*Router(config-if)# tunnel source LUPBEK {IPv4 LUPBEK }*

Geri döngü adı veya IPv4 adresi olabilen tünel kaynağının fiziksel arayüzü seçilebilir.

***Adım 5:*** Tünel tipini 6to4 tünel olarak tanımlama.

*Router(config-if)# tunnel mode ipv6ip 6to4*

***Adım 6:*** Statik rotalar kullanarak her iki uçtaki tünelleri tanımlama

*Router(config)# ipv6 route 2A02::/16 Tunnel 1*

6to4 tünel yapılandırmasından sonra, ana bilgisayar B1, ana bilgisayar B1'den ana bilgisayar B2'ye ping komutunu uygulayarak yapılandırılmış tünel aracılığıyla ana bilgisayar B2'ye bağlanabilir.

Yapılandırma komutlarının tamamı Ek 4'te yer almaktadır.

ISATAP tünelleme senaryosu

ISATAP tüneli, 6to4 tünele çok benzer. IPv6 etki alanlarını bir IPv4 ağı üzerinden bağlamak için kullanılır. ISATAP'ın amacı, yalnızca IPv4 erişim ağı üzerinden IPv6 ana bilgisayarları için merkezi bir IPv6 yönlendiricisine bağlantı sağlamaktır.

Bu yöntemde, yalnızca bir tünel kaynağı tanımlanır ve hedef yapılandırılmaz. Bu nedenle, her yönlendiricide yalnızca bir tünel oluşturulur, çünkü bu tür bir tünel, çok noktalı tüneli işaret eder.

ISATAP Tüneli yapılandırma adımları:

***Adım 1:*** Bir tünel tanımlama ve tünel numarasını atama,

*Router (config)# interface Tunnel {number}*

***Adım 2:*** Tünel arayüzünde IPv4'ün devre dışı bırakılması,

*Router (config-if)# no ip Adres*

***Adım 3:*** Tünel arayüzünde IPv6'nın etkinleştirilmesi,

*Router (config-if)# ipv6 enable*

IPv6 etkinken, dinamik olarak verildiği için tünele bir IPv6 adresi verilmesi gerekli değildir veya manuel olarak verilebilir:

*Router (config-if)# ipv6 Adres {IPv6 Adres with prefix}*

***Adım 4:*** Tünele bir kaynak atayın,

*Router(config-if)# tunnel source LUPBEK {IPv4 LUPBEK }*

Geri döngü adı veya IPv4 adresi olabilen tünel kaynağının fiziksel arayüzü seçilebilir.

***Adım 5:*** Tünelin türünü ISATAP tüneli olarak tanımlama.

*Router(config-if)#  tunnel mode ipv6ip ISATAP*

***Adım 6:*** Statik rotalar kullanarak her iki uçtaki tünelleri tanımlama

*Router(config)# ipv6 route 2A02::/16 Tunnel 1*

ISATAP tüneli yapılandırmasından sonra, ana bilgisayar B1, ana bilgisayar B1'den ana bilgisayar B2.z'ye ping komutunu uygulayarak yapılandırılmış tünel aracılığıyla ana bilgisayar B2'ye bağlanabilir.

Yapılandırma komutlarının tamamı Ek 5'te yer almaktadır.

# 5. DEĞERLENDİRME VE SONUÇLAR

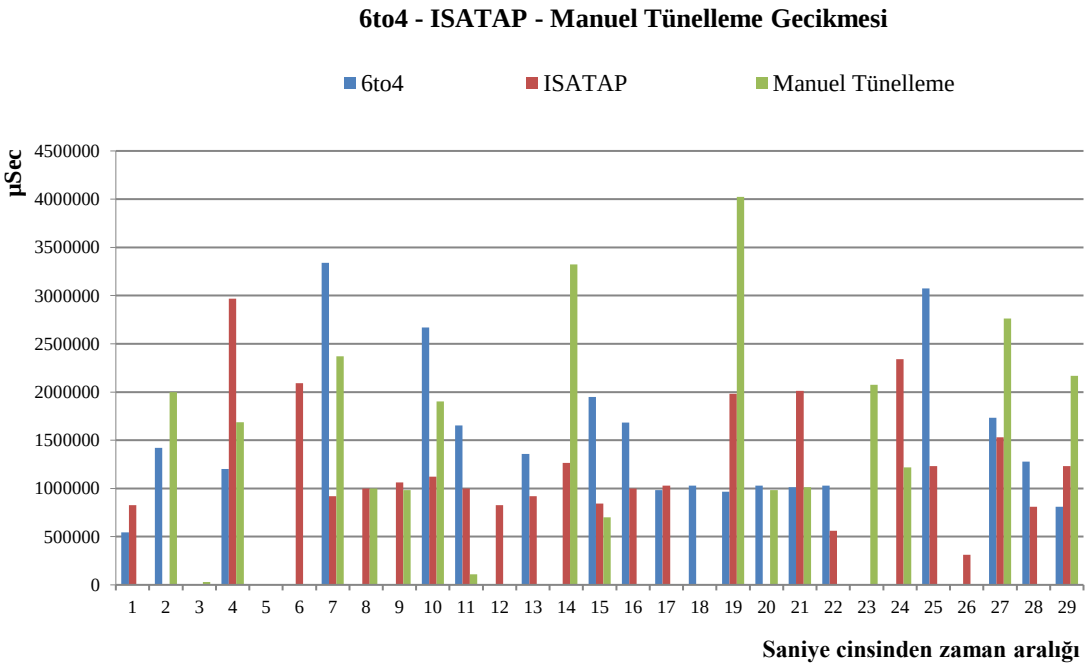
Bu bölümde, Wireshark aracı kullanılarak ağ performans ölçütleri ile beş öykünme senaryosu değerlendirilerek minimum gecikmeye ve maksimum trafik hacmine ve ayrıca en düşük Gidiş Dönüş Süresine sahip optimum yöntem seçilmiştir.

## 5.1. Gecikme (Delay)

Gecikme, ağın performansını ölçmek için ana parametrelerden biridir, ilk bitin kaynak ile hedef arasındaki bir bağlantı üzerinden geçmesi için bir süre belirtir [14].

### 5.1.1. 6to4 - ISATAP - manuel tünel gecikmesi

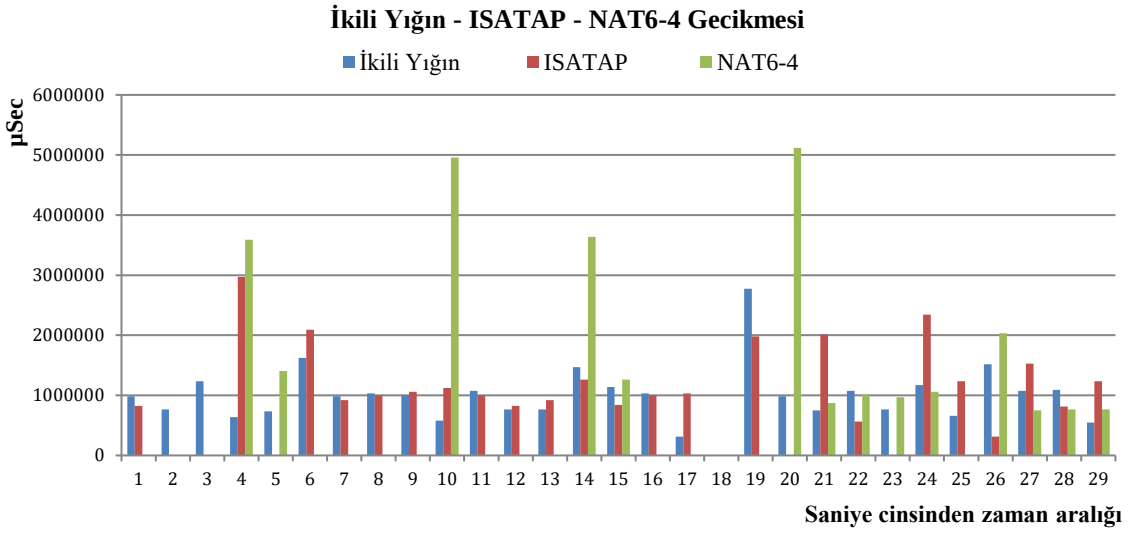
Aşağıdaki şekilden, Y ekseni µSec cinsinden ölçülen gecikmeyi gösterir ve X ekseni bu zaman aralığını saniye cinsinden gösterir, çünkü ISATAP tünelinin 6to4 tünelden ve manuel tünelden daha iyi olduğunu gösterir, çünkü Birçok zaman aralığında ISATAP'ın ortalama gecikmesi 6to4'ün aksine 2 000 000 µSec'in altındadır ve manuel tünellemede ortalama gecikme 2 000 000 µSec'in üzerindedir ki bu daha fazladır.




Şekil 5.1. 6to4 vs ISATAP vs manuel tünel gecikmesi

### 5.1.2. İkili yığın - ISATAP - NAT6-4 gecikmesi

Aşağıdaki şekilden, Y ekseni µSec cinsinden ölçülen gecikmeyi gösterir ve X ekseni, bu zaman aralığı yaklaşık 30 saniye boyunca ölçülen zaman aralığını saniye cinsinden gösterir, İkili Yığın en iyisidir, çünkü birçok zaman aralığında İkili Yığın ortalama gecikmesinin 2 000 000 µSec'in altında olduğuna işaret eder, aksine ISATAP tüneli ve NAT6-4 bunların ortalama gecikmesi 2 000 000 µSec'in üzerindedir ki bu daha fazladır.



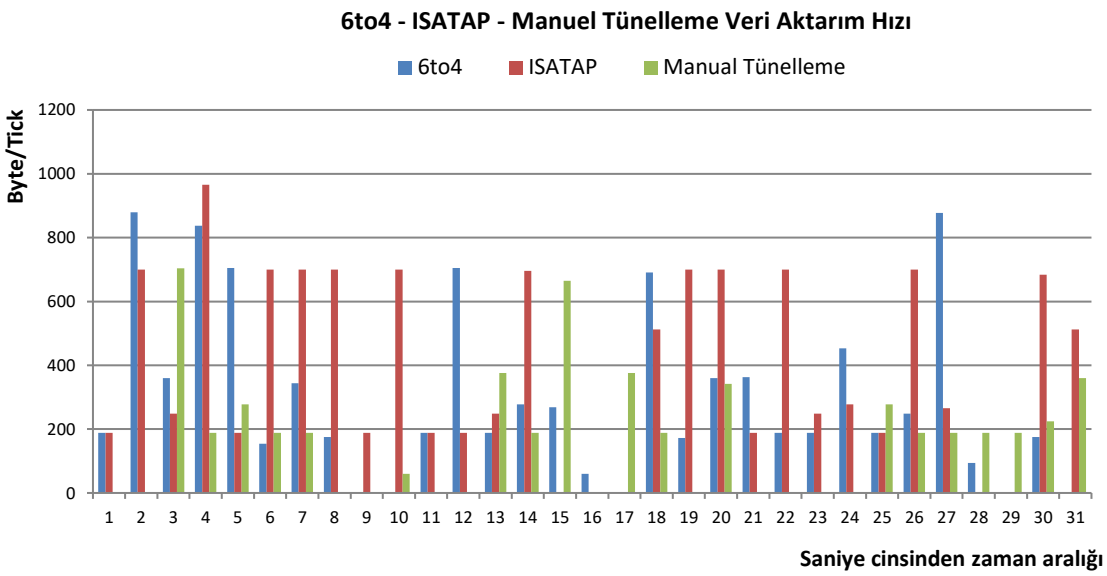

Şekil 5.2. İkili yığın vs ISATAP vs NAT6-4 gecikmesi

## 5.2. Veri Aktarım Hızı (Throughput)

Veri Aktarım Hızı, ağ üzerinden belirli bir süre içinde bir noktadan diğerine aktarılabilen veri miktarıdır [15].

### 5.2.1. 6to4 - ISATAP - manuel tünel veri aktarım hızı

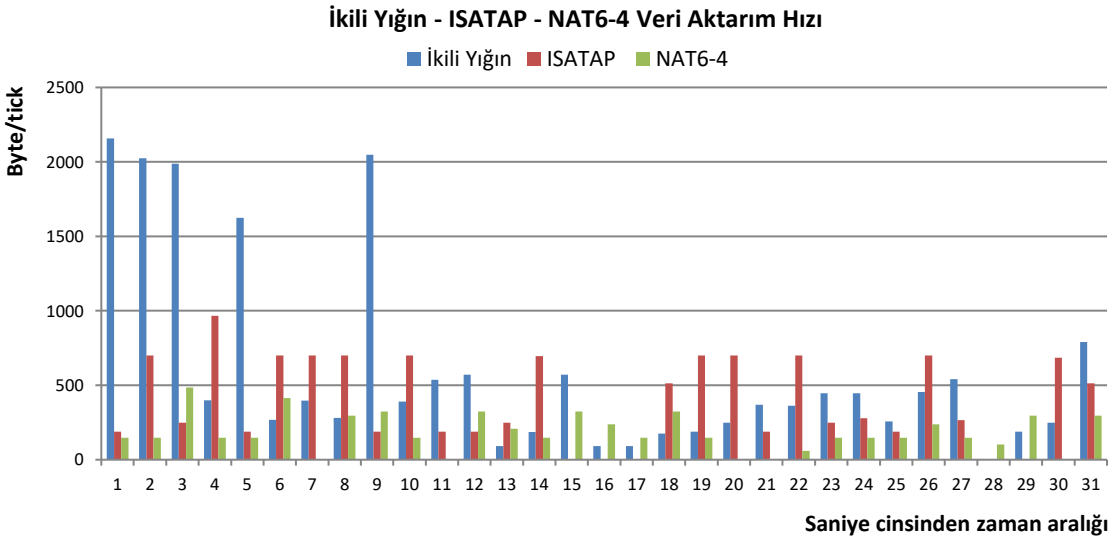
Aşağıdaki şekilden, Y ekseni bayt / tik olarak ölçülen verimi gösterir ve X ekseni, ISATAP tünelinin 6to4 ve manuel tünelden daha iyi olduğunu gösterdiği için bu zaman aralığının yaklaşık 30 saniye boyunca ölçülen zaman aralığını saniye cinsinden gösterir. Çünkü birçok zaman aralığında ISATAP'ın ortalama verimi 6to4'ün tersine 600 bayttan fazladır ve manüel tünellemenin ortalama verimi 600 bayt / işaretten daha azdır, bu da daha az verimdir.




Şekil 5.3. 6to4 vs ISATAP vs manuel tünel veri aktarım hızı

### 5.2.2. İkili yığın - ISATAP - NAT6-4 veri aktarım hızı

Aşağıdaki şekilden, Y ekseni bayt / tik olarak ölçülen verimi gösterir ve X ekseni, bu zaman aralığı yaklaşık 30 saniye boyunca ölçülen zaman aralığını saniye cinsinden gösterir. Bu, İkili Yığının en iyisi olduğunu gösterir, çünkü çoğu zaman aralıklar, İkili Yığın ortalama veriminin 1 000 bayttan fazla olduğuna işaret eder, ISATAP ve NAT6-4'ün aksine, bunların ortalama iş hacmi 1 000 bayttan daha azdır ve bu daha az verimdir.




Şekil 5.4. İkili yığın vs ISATAP vs NAT6-4 veri aktarım hızı

## 5.3. RTT

RTT, kaynaktan hedefe gönderilen bir paketin ve yanıtın kaynağa geri dönmesinin ne kadar zaman alır [16].

Çizelge 5.1, IPv6 için geçiş yöntemleri arasındaki bir gecikme karşılaştırmasının sonuçlarını göstermektedir. Test sonuçları, ikili yığın yaklaşımının en düşük RTT'ye sahip olduğu için daha iyi performans gösterdiğini göstermektedir. Görüldüğü gibi, diğer yöntemler, çeşitli ağ adresleri için çoklu işlemlerinden dolayı büyük bir gecikmeye sahiptir.

Çizelge 5.1. Geçiş yöntemlerinde 100 ping komutu uygulaması

| Yöntem / Parametre | Gönderilen Paketler | Alınan Paketler | Kayıp Paketler | Ortalama RTT (ms) |
|---|---|---|---|---|
| İkili Yığın | 100 | 97 | 3% | 215 |
| Manual Tünelleme | 100 | 90 | 10% | 231 |
| ISATAP Tünelleme | 100 | 87 | 13% | 295 |
| 6to4 Tünelleme | 100 | 89 | 11% | 317 |
| NAT6-4 | 100 | 93 | 7% | 223 |

<u>Sonuçlar</u>

Tüm bu tekniklerin performans analizinden İkili yığın yaklaşımı, YPTC için IPv4'ten IPv6'ya geçiş için en uygun olanıdır. İkili Yığın en iyi yöntemdir, esnektir çünkü yönlendiricilerde aynı anda hem IPv4 hem de IPv6 kullanır ve kullanımı kolaydır. Geçiş sürecinde NAT6-4 yönlendiricilerine aksilik olursa tüm ağlar çökeceği için çeviri yöntemi ağı savunmasız hale getirir. Tünel oluşturma, ağ yönetimine daha fazla karmaşıklık ekleyerek tünel yönlendiricilerinde daha fazla gecikmeye neden olur.

# KAYNAKLAR


1. Yadav, A., Abad, P., Shah, H., and Kaul, A. (2012). *IPv6 protocol adoption in the US: Why is it so slow. Capstone paper, University of Colorado,* 4.

2. Sookun, Y., and Bassoo, V. (2016). *Performance analysis of IPv4/IPv6 transition techniques. In 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)* IEEE, 188-193.

3. Colitti, L., Di Battista, G., and Patrignani, M. (2004). *IPv6-in-IPv4 tunnel discovery: methods and experimental results. IEEE Transactions on Network and Service Management* IEEE, 1(1), 30-38.

4. Araji, B., and Gurkan, D. (2014). *Embedding switch number, port number, and MAC Adres (ESPM) within the IPv6 Adres. In 2014 Third GENI Research and Educational Experiment Workshop* IEEE, 69-70.

5. Ali, M. S., and Yahiya, T. A. (2018). *Performance Analysis of Native Ipv4/Ipv6 Networks Compared to 6to4 Tunnelling Mechanism. In 2018 International Conference on Advanced Science and Engineering (ICOASE)* IEEE, 250-255.

6. İnternet: Google IPv6 (Per-Country IPv6 adoption) URL: https://www.google.com/intl/en/ipv6/statistics.html , Son Erişim Tarihi: 07.04.2021.

7. Sookun, Y., and Bassoo, V. (2016). *Performance analysis of IPv4/IPv6 transition techniques. In 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)* IEEE, 188-193.

8. Savita, S. (2013). *Comparison analysis of various transition mechanisms from ipv4 to ipv6. International Journal Of Engineering And Computer Science,* 2(6), 1-6.

9. Dawadi, B. R., Joshi, S. R., and Khanal, A. R. (2015). *Service provider IPv4 to IPv6 network migration strategies. Journal of Emerging Trends in Computing and Information Sciences,* 1-10.

10. Sha, F., Chen, X., Ye, R., Wu, M., Zhang, Z., and Cai, W. (2017). *A communication method between IPv4 server and IPv6 network in virtual machine environment. In 2017 IEEE/ACIS 16th International Conference on Computer and Information Science (ICIS)* IEEE, 885-888.

11. Dawadi, B. R., Joshi, S. R., and Khanal, A. R. (2015). *Service provider IPv4 to IPv6 network migration strategies. Journal of Emerging Trends in Computing and Information Sciences,* 6(10).

12. Govil, J., Govil, J., Kaur, N., and Kaur, H. (2008). *An examination of IPv4 and IPv6 networks: Constraints and various transition mechanisms. In IEEE SoutheastCon 2008* IEEE, 178-185.

13. İnternet: Public Telecommunication Corporation URL: http://ptc.gov.ye/en/Home.aspx, Son Erişim Tarihi: 07.04.2021.

14. El Khadiri, K., Labouidya, O., Elkamoun, N., and Hilal, R. (2018). Performance evaluation of IPv4/IPv6 transition mechanisms for real-time applications using OPNET modeler. Performance Evaluation, 9(4).

15. Siddika, F., Hossen, M. A., and Saha, S. (2017). *Transition from IPv4 to IPv6 in Bangladesh: The competent and enhanced way to follow. In 2017 International Conference on Networking, Systems and Security (NSysS)* IEEE, 174-179.

16. Gu, K., Zhang, L., Wang, Z., and Kong, Y. (2017). *Comparative studies of IPv6 tunnel security. In 2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)* IEEE, 2799-2804.

17. Manimozhi, S., and Jayanthi, J. G. (2020). *A Literature Survey on Transition Mechanisms in IPv4 and IPv6 Networks. In 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)* IEEE, 12-18.

18. Hunek, M., and Pliva, Z. (2018). *DNSSEC in the networks with a NAT64/DNS64. In 2018 International Conference on Applied Electronics (AE)* IEEE, 1-4.

19. Suleiman, M. F., and Cordry, J. (2017). *Analysis of organizations IPv6 deployment strategies in Nigeria and evaluating suitable transition mechanisms. In 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)* IEEE, 695-704.

20. Goyal, H. (2019). *IPv4 to IPv6 Migration and Performance Analysis using GNS3 and Wireshark. In 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking* (ViTECoN) IEEE, 1-6.

21. Kurniawan, D. E., Kushardianto, N. C., and Thohari, A. H. (2019). *Simulation and Analysis Network Performance of IPv4, IPv6 and ISATAP Tunneling on Polibatam Network Laboratory. In 2019 2nd International Conference on Applied Engineering (ICAE)* IEEE, 1-4.

# ÖZGEÇMİŞ

## Kişisel Bilgiler

Soyadı, adı : Ammar, QAID

Uyruğu : Yemen

## Eğitim

| Derece | Eğitim Birimi | Mezuniyet Tarihi |
|---|---|---|
| Yüksek lisans | Gazi Üniversitesi Bilgisayar Bilimleri | Devam ediyor |
| Lisans | Yemen Bilim ve Teknoloji Üniversitesi Bilgisayar Ağları | 2016 |
| Lise | Taiz Lisesi | 2011 |

## Yabancı Dil

İngilizce, Türkçe

## Yayınlar

1. Qaid, A., ve Ertuğ Ö., (2021). Transition from IPv4 to IPv6 Mechanisms by GNS3 Emulation: YPTC as a Case Study, *2021 International Symposium on Networks, Computers and Communications* (ISNCC'21).

## Hobiler

Futbol, Yüzme, Karikatür çizimi, Haberleşme ve bilgisayar teknolojileri

*GAZİLİ OLMAK AYRICALIKTIR…*