

IPv6 SİSTEM GEÇİŞİ

**YÜKSEK LİSANS TEZİ
Müh. Mustafa ŞAHİN
(504031312)**

**Tezin Enstitüye Verildiği Tarih : 8 Mayıs 2006
Tezin Savunulduğu Tarih : 15 Haziran 2006**

**Tez Danışmanı : Prof.Dr. Mine KALKAN
Diğer Jüri Üyeleri: Prof.Dr. Hasan DAĞ (İTÜ)
Doç.Dr. Selçuk PAKER (İTÜ)**

HAZİRAN 2006

ÖNSÖZ

Tez çalışmam sırasında benden yardım ve yönlendirmelerini esirgemeyen değerli hocam ve danışmanım Sayın Prof.Dr. Mine KALKAN'a teşekkürlerimi sunarım. Linux işletim sistemi konusunda yardımcı olan Uzman Emre KARAOĞLU'na ve hayatım boyunca desteğini eksik tutmayan aileme de ayrıca teşekkür etmek isterim.

Mayıs 2006

Müh. Mustafa ŞAHİN

İÇİNDEKİLER

KISALTMALAR	vii
ŞEKİL LİSTESİ	ix
ÖZET	x
SUMMARY	xi
1. GİRİŞ	1
2. TCP/IP YAPISI.....	4
2.1 OSI Referans Modeli	5
2.1.1 Fiziksel katman	5
2.1.2 Veri bağlantı katmanı	6
2.1.3 Ağ katmanı.....	6
2.1.4 İletim katmanı	7
2.1.5 Oturum katmanı	7
2.1.6 Sunum katmanı.....	8
2.1.7 Uygulama katmanı	8
2.2 TCP/IP Ağ Erişim Katmanı	8
2.3 TCP/IP İnternet Katmanı	9
2.3.1 İnternet protokolü	9
2.3.2 ICMP	11
2.3.3 ARP	12
2.3.4 RARP.....	12
2.4 TCP/IP İletim Katmanı.....	13
2.4.1 TCP.....	13
2.4.2 UDP	14
2.5 TCP/IP Uygulama Katmanı	14
3. İNTERNET PROTOKOLÜ VERSİYON 6	16
3.1 IPv6 Adresleri	18
3.1.1 IPv6 adres yapısı	19
3.1.2 IPv6 adres ön ekleri	20
3.1.3 IPv6 adres türleri	20
3.1.4 Unicast Adresleri.....	21
3.1.4.1 Tanımlanmamış unicast adresleri	22
3.1.4.2 Loopback adresi.....	22
3.1.4.3 Global adresler	23
3.1.4.4 Link-local adresleri	23
3.1.4.5 Site-local adresleri	23
3.1.4.6 IPv4 adresi içeren IPv6 adresleri.....	24
3.1.5 Anycast adresleri	24
3.1.6 Multicast adresleri	25

3.1.7 IPv6 düğümünün sahip olması gereken adresler.....	26
3.1.8 EUI arayüz tanımlayıcısı	27
3.2 IPv6 Başlığı	28
3.2.1 Başlık alanları	28
3.2.2 Eklenti başlıkları	29
3.2.3 IPv6 paket boyutu.....	30
3.3 ICMPv6	31
3.3.1 ICMPv6 başlık yapısı	31
3.3.2 ICMPv6 hata mesajları	32
3.3.2.1 Hedef ulaşılamaz hata mesajı.....	32
3.3.2.2 Paket çok büyük mesajı	33
3.3.2.3 Zaman aşımı	33
3.3.2.4 Parametre problemi.....	33
3.3.3 ICMPv6 bilgi mesajları	34
3.3.3.1 Yankı isteği mesajı	34
3.3.3.2 Yankı cevap mesajı.....	34
3.3.4 Multicast dinleyici keşfi	34
3.4 Komşu Keşfi	35
3.4.1 Komşu keşfi mesajları	35
3.4.1.1 Yönlendirici ricası	36
3.4.1.2 Yönlendirici ilanı.....	36
3.4.1.3 Komşu ricası.....	37
3.4.1.4 Komşu ilanı	38
3.4.1.5 Yeniden yönlendirme mesajı.....	38
3.4.2 Komşu keşfi işlemi	39
3.4.2.1 Adres çözümleme	39
3.4.2.2 Yönlendirici Keşfi	40
3.4.2.3 Komşu Erişilemezlik Keşfi	40
3.4.2.4 Yeniden yönlendirme.....	41
3.4.2.5 Adres çakışması tespiti	42
3.5 IPv6 Yönlendirme	42
3.5.1 Yönlendirme çeşitleri	43
3.5.1.1 Statik yönlendirme.....	44
3.5.1.2 Metrik.....	44
3.5.1.3 Uzaklık vektörü	44
3.5.1.4 Yol vektörü.....	45
3.5.1.5 Bağlantı durumu	45
3.5.2 Yönlendirme protokolleri	46
3.5.2.1 RIPv6	46
3.5.2.2 OSPFv3	47
3.5.2.3 Birleştirilmiş IS-IS.....	47
3.5.2.4 BGP-4	48
3.5.2.5 IDRPv2	48
3.6 Alan Adı Sistemi	49
3.7 Otomatik Adres Yapılandırması	50
3.7.1 Sunucusuz otomatik yapılandırma	51
3.7.2 Sunuculu otomatik yapılandırma ve DHCPv6.....	52

3.8 IPv6'ya Geçiş Mekanizmaları	54
3.8.1 Uyumluluk Adresleri	55
3.8.2 Çift yığın yapısı.....	56
3.8.3 IPv4 üzerinden IPv6 tünelleme	57
3.8.4 Tünel çeşitleri.....	58
3.8.4.1 El ile yapılandırılmış tünel.....	58
3.8.4.2 6to4 tüneli.....	58
3.8.4.3 ISATAP.....	60
3.8.4.4 Teredo	61
4. IPV6'YA GEÇİŞ	63
4.1 Ön Hazırlık	64
4.1.1 Planlama	64
4.1.2 İşletim sistemlerinin yapılandırılması	65
4.1.2.1 Debian 3.1 yapılandırması	65
4.1.2.2 Pardus 1.0 yapılandırması	66
4.1.2.3 Windows yapılandırmaları	67
4.2 IPv6 Erişimi Sağlama.....	69
4.2.1 RIPE kaydı	70
4.2.2 SixXS tünel başvurusu.....	70
4.2.3 IPv6 tüneli kurma	71
4.2.4 IPv6 /48 adres aralığı alma	72
4.2.5 IPv6 Tüneli Yapısı.....	73
4.3 IPv6 Adres Dağıtımı.....	74
4.3.1 El ile yapılandırma	75
4.3.2 Sunuculu adres dağıtımı	76
4.3.3 Sunucusuz adres dağıtımı	78
4.4 IPv6 Sunucularının Kurulumu	79
4.4.1 IPv6 isim sunucusu BIND	80
4.4.2 IPv6 Web sunucusu APACHE.....	84
4.4.2.1 Giriş sayfası PHP uygulaması	86
4.4.2.2 Web üzerinden IPv6 uygulaması.....	87
4.4.3 IPv6 e-posta sunucusu ve SQUIRRELMAIL	88
4.4.4 IPv6 dosya transfer sunucusu VSFTP	90
4.4.5 IPv6 sunucularının yedeklenmesi.....	91
4.5 IPv6 ağ servisleri ve uygulamaları.....	92
4.5.1 SNMP	92
4.5.2 MRTG.....	93
4.5.3 Gnomemeeting	95
4.5.4 PuTTY	96
4.5.5 Lynx ve W3M	97
4.5.6 Nmap	98
4.5.7 Iperf ve Netperf	99
4.5.8 Whois.....	101
4.5.9 Sorun giderme uygulamaları.....	101
4.5.9.1 Ping	101

4.5.9.2 Traceroute	101
4.5.9.3 Tracepath.....	102
5. SONUÇLAR.....	104
KAYNAKLAR.....	105
ÖZGEÇMİŞ.....	109

KISALTMALAR

AH	: Authentication Header
API	: Application Programming Interface
ARP	: Address Resolution Protocol
ARPAnet	: Advanced Research Projects Agency Network
ATM	: Asynchronous Transfer Mode
BGP	: Border Gateway Protocol
BIND	: The Berkeley Internet Name Domain
BOOTP	: Bootstrap Protocol
CIDR	: Classless Inter-Domain Routing
CNAME	: Canonical Name
DHCP	: Dynamic Host Configuration Protocol
DNS	: Domain Name System
EGP	: Exterior Gateway Protocol
EIGRP	: Enhanced Interior Gateway Routing Protocol
FDDI	: Fiber Distributed Data Interface
FP	: Format Prefix
FQDN	: Fully Qualified Domain Name
FTP	: File Transfer Protocol
HTML	: Hyper Text Markup Language
HTTP	: Hyper Text Transfer Protocol
IANA	: Internet Assigned Numbers Authority
ICMP	: Internet Control Message Protocol
IDRPv2	: Inter-Domain Routing Protocol Version 2
IGRP	: Interior Gateway Routing Protocol
IEEE	: Institute of Electrical and Electronics Engineers
IETF	: Internet Engineering Task Force
IMAP	: Internet Message Access Protocol
IP	: Internet Protocol
IPsec	: IP Security
IPv4	: Internet Protocol Version 4
IPv6	: Internet Protocol Version 6
ISATAP	: Intra-site Automatic Tunnel Addressing Protocol
ISO	: International Standards Organization
IS-IS	: Intermediate System-to-Intermediate System
LIR	: Local Internet Registry
LSA	: Link State Advertisement
LSP	: Link State Packet
MLD	: Multicast Listener Discovery
MTU	: Maximum Transmission Unit
NAT	: Network Address Translation
ND	: Neighbor Discovery
NNTP	: Network News Transfer Protocol
NTP	: Network Time Protocol
OSPFv3	: Open Shortest Path First Version 3
OUI	: Organization Unique Identifier

PHP	: Personal Home Page
POP	: Point of Presence
POP3	: Post Office Protocol Version 3
PPP	: Point-to-Point Protocol
P2P	: Peer to Peer
RARP	: Reverse Address Resolution Protocol
RFC	: Request for Comments
RIP	: Routing Information Protocol
RIPE NCC	: Réseaux IP Européens Network Coordination Centre
RIPng	: Routing Information Protocol New Generation
RLOGIN	: Remote Login
SLIP	: Serial Line Internet Protocol
SMTP	: Simple Mail Transfer Protocol
SNMP	: Simple Network Management Protocol
SSH	: Secure Shell
SSL	: Secure Socket Layer
ST2	: Stream Protocol Version 2
TCP	: Transmission Control Protocol
TCP/IP	: Transmission Control Protocol/Internet Protocol
UDP	: User Datagram Protocol
WAN	: Wide Area Network
WWW	: World Wide Web

ŞEKİL LİSTESİ

	<u>Sayfa No</u>
Şekil 2.1 : TCP/IP mimarisi	4
Şekil 2.2 : OSI referans modeli	5
Şekil 2.3 : IPv4 başlık yapısı	10
Şekil 3.1 : NAT örneği	17
Şekil 3.2 : IPv6 adres bölümlemesi	21
Şekil 3.3 : Global unicast adres yapısı	23
Şekil 3.4 : Multicast adres yapısı	25
Şekil 3.5 : IPv6 başlık yapısı	28
Şekil 3.6 : Eklenti başlıkları	30
Şekil 3.7 : ICMPv6 mesajının yapısı	31
Şekil 3.8 : Otonom sistem örneği	43
Şekil 3.9 : Çift yığın mimarisi	56
Şekil 3.10 : Tünelleme yapısı	57
Şekil 3.11 : 6to4 tünelleme örneği	59
Şekil 3.12 : 6to4 örneği hedef ve kaynak adresleri	60
Şekil 4.1 : UZEM – SixXS tüneli	73
Şekil 4.2 : Global DNS kaydı	84
Şekil 4.3 : IPv6 Web sitesi	84
Şekil 4.4 : SSL sunucu sertifikası	85
Şekil 4.5 : E-posta istemci yapılandırması	90
Şekil 4.6 : FTP istemci programı	91
Şekil 4.7 : MRTG grafikleri	95
Şekil 4.8 : Gnomemeeting programı	96
Şekil 4.9 : PuTTY istemci arayüzü	97
Şekil 4.10 : W3M Web tarayıcısı	98
Şekil 4.11 : Nmap IPv6 tarama örneği	99
Şekil 4.12 : Iperf sunucu istemci bağlantısı	100
Şekil 4.13 : Netperf sunucu istemci bağlantısı	100
Şekil 4.14 : Traceroute örneği	102
Şekil 4.15 : Tracepath örneği	103

IPv6 SİSTEM GEÇİŞİ

ÖZET

İnternet, askeri amaçla temelleri atılmış olan daha sonra tüm dünyayı saran sanal bir ağıdır. Günümüzde bilgiye en kolay erişim yolu olamasından günlük hayatı kolaylaştırması ve insanlar arası iletişim kurmasına kadar birçok kullanım alanı olan yeri doldurulamaz bir teknoloji halini almıştır.

İnternet Protokolü (IP), İnternet'in temel yapı taşı konumundadır ve İnternet üzerinden haberleşme sırasında çok önemli görevler üstlenmektedir. 1980'li yılların başında geliştirilen IP'nin ilk sürümü olan IPv4 uzun yıllar İnternet'in gelişimine katkıda bulunmuştur. Ancak baş döndürücü bir hızla gelişen İnternet'e bir süre sonra ayak uyduramamış ve ihtiyaçları karşılayamaz hale gelmiştir. Bu sebeple 1995 yılında yeni nesil İnternet Protokolü olan IPv6 geliştirilmiştir. IPv6 ile dağıtılabılır IP adresi sayısı arttırılmış, güvenlik ve servis kalitesi hizmetleri sağlanmış, yönlendirmeler daha verimli hale getirilmiş ve otomatik adres yapılandırması gibi ek özellikler eklenmiştir.

Bu tez çalışmasında, giriş bölümünde İnternet'in ve İnternet Protokolü'nün kısaca geçmişi incelenmiş ve IPv6'ya kadar geçen süreçten bahsedilmiştir. İkinci bölümde OSI referans modeli ve TCP/IP yapısı incelenmiş ve katmanlar hakkında bilgi verilmiştir.

Üçüncü bölümde IPv4'ün eksikliklerinden bahsedilerek neden yeni nesil bir İnternet Protokolü ihtiyacı duyulduğu belirtilmiştir. IPv4'ün eksikliklerini gidermek için geliştirilen diğer teknolojilerden bahsedilmiştir. Daha sonra IPv6 tüm mimarisi ile birlikte detaylı bir şekilde incelenmiştir.

Dördüncü bölümde ise üçüncü bölümde anlatılan teorik bilginin uygulaması olarak bir test laboratuvarı kurulmuştur. Öncelikle laboratuvara IPv6 İnternet bağlantısı sağlanmış, geniş bir IPv6 adres aralığı alınmıştır. Daha sonra bir ağda kesinlikle bulunması gereken önemli sunucular ve ağ yönetimi için kullanılan bazı yazılımlar kurularak test edilmiştir.

Sonuç bölümünde IPv6'nın dünya çapında kullanımı ele alınmıştır. IPv6 sistem geçişinin test laboratuvarı kapsamında sağlandığı belirtilmiş ve sistem geçişi sonuçları özetlenmiştir.

IPv6 SYSTEM MIGRATION

SUMMARY

Internet was firstly invented for military purposes. Since then it has become a virtual network covering the world. Nowadays, it is one of the most important technologies because it is the easiest way for finding information, it makes life easier and it is used for communication between people.

Internet Protocol (IP) is the main structure of Internet and plays very important roles while communicating over Internet. The first version of IP is named as IPv4 and it contributed to the development of Internet for a long time. On the other hand it couldn't keep in step with the rapidly growing Internet and supply the requirements. For this reason, a next generation Internet Protocol, IPv6, is developed in 1995. In IPv6, the number of IP addresses is increased, security and quality of service is supplied, routings become more efficient and some additional properties like automatic address assignment are added.

In this study, the history of Internet and Internet Protocol is shortly examined as an Introduction Chapter and the period till the IPv6 development is explained. In the second chapter, OSI reference model and TCP/IP structure are discussed, and the layers are detailed according to these models.

In Chapter 3, the shortages of IPv4 are mentioned and the reason of the need for a new version Internet Protocol is explained. Later, some technologies to overcome the shortages of IPv4 are mentioned. Finally the IPv6 architecture is examined in a very detailed way.

In Chapter 4, a test laboratory is established, as an application for the theory of IPv6 given in Chapter 3. Firstly the IPv6 Internet connection is established and a wide IPv6 address space is taken. Then the important servers that should be in a network and the network management software are installed and tested in the laboratory.

In the conclusion chapter, the usage of IPv6 in different continents of the World is discussed. It is mentioned that IPv6 system migration is done with the test laboratory. And the results of the system migration are summarized.

1. GİRİŞ

İnternet Protokolü (IP) adından da anlaşılacağı gibi İnternet üzerinden haberleşmek için kullanılan kurallar dizisidir. İnternet diye adlandırılan yapının mimarisini ARPAnet (Advanced Research Projects Agency Network) oluşturmaktadır.

ARPAnet 1957 yılında Rusların Sputnik uydusunu yörüngesine yerleştirmesi ile başlayan, Amerika ile Rusya arasındaki teknoloji ve uzay savaşları yarışının bir başlangıcı olarak kurulmuştur[1]. Sadece askeri amaçlı olmayıp, aynı zamanda araştırma ve geliştirmeye yönelik çalışmalar yapabilmek için kurulmuş bir ağıdır. Dr. Joseph Carl Robnett Licklider ARPAnet'in yöneticisi olarak bu amaçları yerine getirmek üzere görevlendirilmiştir.

ARPAnet geliştirilmeye devam edilmiş, 1968 yılına gelindiği zaman ilk WAN (Wide Area Network) bağlantısı sağlanmıştır. Bu bağlantı Berkeley ve MIT (Massachusetts Institute of Technology) arasında telefon hattı kullanılarak sağlanmıştır[2]. 1969 yılına gelindiğinde ARPAnet Santa Barbara, Utah, UCLA and Stanford uç noktalarını kapsayacak biçimde dörtlü bir ağ haline gelmiştir. 1971'de bu ağ artık yirmi bir düğümden oluşmaktaydı ve insanlar ARPAnet üzerinden haberleşmeye başlamışlardı. 1972'de düğüm sayısı otuz yediye çıkmakla birlikte aynı zamanda ilk elektronik posta denemesi de yapıldı. 1973 yılına gelindiğinde gelişmeler iyice hızlanmıştı. Uluslararası haberleşme kavramı ortaya atıldı, Norveç ve İngiltere ARPAnet'e çevrimiçi olarak dahil oldular.

1974 yılında TCP/IP (Transmission Control Protocol/Internet Protocol) yapısı önerildi ve bu yapı içinde FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), TELNET(Terminal Emulation Protocol) ve HTTP(Hyper Text Transfer Protocol) kural dizinleri tanımlanmıştır. Kullanılan bilgisayarların çok büyük boyutlarda ve çok pahalı olmaları sebebiyle sadece hükümetler, bazı büyük şirketler ve üniversiteler bu bilgisayarları kullanarak ARPAnet'e bağlanabilmekteydiler.

1976'da Kraliçe Elizabeth ilk elektronik postasını göndermiştir. 1980 yılına gelindiğinde bilgisayar sayısı 200, kullanıcı sayısı da 20.000'i geçmiştir. 1982

yılında ilk kez “İnternet” kelimesi telaffuz edilmiş ve TCP/IP yapısı iletim ağına dahil edilmiştir. ARPAnet 1983 yılında askeri amacından tamamen sıyrılarak uluslararası bir haberleşme ağı olarak anılmaya başlanmıştır. 1990 yılında bu büyük ağın isminin İnternet olmasıyla ARPAnet ismi tamamen kullanımdan kalkmıştır. Kullanıcı sayısının iki milyon’u geçmesi ve 600 tane Web sitesi kurulması İnternet isminin resmen kullanılmasından sonra sadece 3 yıl almıştır[2]. İnternet her geçen gün daha da büyümüş ve şimdi tüm dünyayı sanal olarak kapsayan bir ağ haline gelmiştir.

TCP/IP modeli ağ yapısını analiz etmek ve sorun gidermek gibi konularda kolaylık sağlamak için katmanlı bir yapıda inşa edilmiştir. Dört ana katmandan oluşmaktadır. Birinci katman ağ erişim katmanıdır ve fiziksel bağlantıları ifade eder. Kullanılan LAN ve WAN teknolojileri ile ilgilenir. IP, ikinci katman olan İnternet katmanında bulunmaktadır ve o katmandaki en temel protokoldür. IP herhangi bir bilgisayara, herhangi bir yerde ve zamanda hizmet etmek için tasarlanmış evrensel bir protokoldür. Hangi iletim katmanı protokolü veya hangi ağ erişim katmanı yapısı kullanıldığına bakılmaksızın IP görevini hep aynı belirlenmiş kurallar dizini şeklinde yapmaktadır. Üçüncü katman iletim katmanıdır ve burada TCP ve UDP (User Datagram Protocol) bulunmaktadır. Dördüncü ve son katmanda da her gün çok sık kullandığımız uygulamalar bulunmaktadır. Bunlardan bazıları; HTTP, SMTP, TFTP, DNS (Domain Name System), FTP’dir.

IP (İnternet Protokolü), TCP/IP katmanlı yapısı içinde 1981’den itibaren kullanılmaya başlanmıştır. İnternet Protokolünün ilk sürümü, IPv4 (İnternet Protocol Version 4) olarak isimlendirilmiştir. Bu protokol tasarlanırken var olan ihtiyaçlar ve geleceğe yönelik yapılan tahminler çok uzun süre geçerliliğini koruyamamıştır. IPv4 ile ilgili sorunlar 1980’in sonlarına doğru bilim adamlarını düşündürecek şekilde belirmeye başlamıştır. Bu sorunlardan en önemlisi, 32 bit uzunluğunda olan IPv4 adreslerinin sayısının her geçen gün azalması ve bu adreslerin mimarileri dolayısıyla çok verimli kullanılamamasıdır. Bu sebeple 1990’ların başında IETF IPv6 WG (Internet Engineering Task Force IPv6 Work Group) bu soruları çözecek yeni bir adresleme mimarisi üzerinde çalışmaya başlamıştır. IETF İnternet standartlarının belirlendiği, çeşitli çalışma gruplarından oluşan bir organizasyondur. Amerikan Hükümeti tarafından maaşları ödenen çekirdek bir kadro haricinde diğer tüm çalışanlar gönüllülerden oluşmaktadır. Toplam sekiz değişik çalışma alanı vardır.

Bunlar; uygulamalar, kullanıcı servisleri, yönetim, güvenlik, iletim, yönlendirme, İnternet ve operasyon alanlarıdır.[3]

IPv4 adres aralığı sıkıntısı en fazla Uzak Doğu ülkelerinde, özellikle Çin'de görülmektedir. Şu anda Çin mevcut adreslerin 1/7'sini kullanmaktadır. Ancak eğer ülkedeki her öğrenciye (320 milyon) bir adet IP adresi verilmesi gerekirse tüm adreslerin 1/4'ü sadece bu iş için dağıtılması gerekecektir ki bu da imkânsızdır[4].

Yeni protokol tasarımı çalışmalara paralel olarak mevcut protokolü, yani IPv4'ü, daha etkin olarak kullanmak için farklı tasarımlar üzerine de çalışılmıştır. Bu amaçla NAT(Network Address Translation) ve CIDR (Classless Inter-Domain Routing) geliştirilmiştir. Ancak bu teknolojiler de yeni bir İnternet Protokolü ihtiyacını giderememişlerdir.

Bütün bu ihtiyaçları göz önüne alan IETF 1995 yılında yeni versiyon İnternet Protokolünü ilk standartları ile birlikte ortaya çıkarmış ve ismini IPv6 olarak belirlemiştir. İsminin IPv5 olmamasının sebebi, IPv5 isminin RFC 1819'da tanımlanan ve deneysel bir protokol olan ST2'ye (Internet Stream Protocol, Version 2) atanmış olmasıdır. IPv5 hiçbir zaman genel kullanıma açılmamıştır[5].

128 bit adres uzunluğundaki IPv6; gelişmiş ağ fonksiyonları, IPv4'e göre çok daha geniş bir adres aralığı, uçtan uca bağlantı (P2P - Peer to Peer Connection), son noktalar arasındaki güvenlik, otomatik yapılandırma araçları ve diğer protokol geliştirmeleri bakımından bir önceki İnternet Protokolüne göre üstündür.

“Take the Internet where no other network has been before”

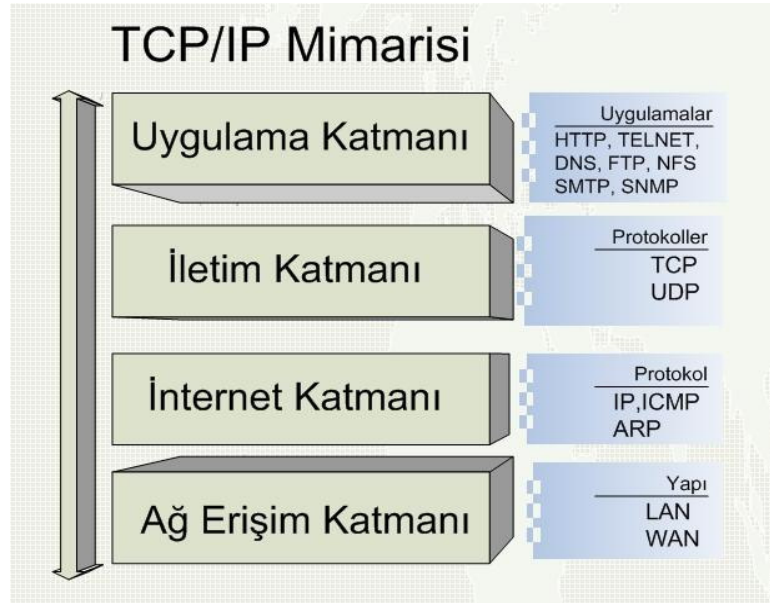
Vint Cerf, IPv6 Forum Honorary Chairman

“İnternet'i, daha önce hiçbir ağın bulunamadığı bir konuma getirin”

Vint Cerf, IPv6 Forumu Onursal Başkanı

2. TCP/IP YAPISI

1983 yılında askeri birimlerin ARPAnet'ten TCP/IP protokol mimarisine geçmesi ile birlikte artık TCP/IP haberleşmedeki birincil protokol olmuş, daha sonra "İnternet" kelimesi sıklıkla kullanılmaya başlanmıştır. İlk zamanlarda İnternet iki bilgisayarın birbirine bağlanmasını ifade etmekteydi. Ancak kısa süre içinde İnternet beklenenden çok daha fazla gelmiştir. Ülkeler, üniversiteler ve firmalar kendi yerel alan ağlarını(LAN), mevcut geniş alan ağlarına bağlamaya başlamışlar, TCP/IP de sağladığı esneklik sayesinde İnternet bağlantısı için bir standart mimari haline gelmiştir.



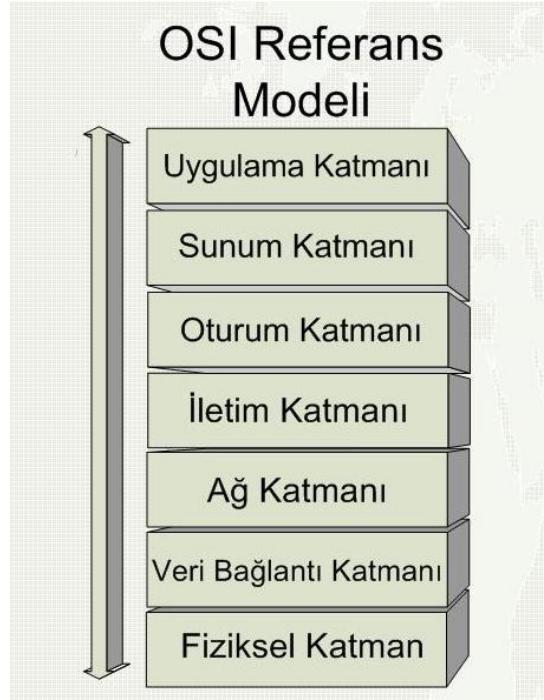
Şekil 2.1: TCP/IP mimarisi

TCP/IP'nin kısa sürede bu kadar kabul görmesinin ana sebebi, dünya çapında veri haberleşmesini sağlayabilecek yapıda olmasıdır. Şekil 2.1'de görüldüğü gibi katmanlı bir mimariye sahiptir ve bu katmanlı mimari ona çok büyük esneklik sağlamaktadır. Kullanılan yazılım ve donanımın ne olduğuna bakılmaksızın, bir üst katman bir alt katmandan bağımsız çalışabilmektedir. Ayrıca standartlaşmış üst seviye protokolleri sayesinde kullanıcılara çok sayıda hizmet sağlamaktadır.

TCP/IP Mimarisini daha iyi anlayabilmek için en iyi yöntem ISO (International Standards Organization) tarafından geliştirilen OSI (Open Systems Interconnection) referans modeli ile karşılaştırmaktır. Bu sayede değişik katmanlarda bulunan her bir protokolün birbiri ile nasıl iletişime geçtiği daha iyi anlaşılmaktadır.

2.1 OSI Referans Modeli

OSI referans modeli yedi katmandan oluşan, her bir katmanına özel bir görev yüklenen ve katmanların birbirine bağımlı olduğu kavramsal bir yapıdır. OSI modeli İnternet üzerinde yapılan herhangi bir işlemi analiz etmek için çok uygun bir modeldir. Mesela bir ağ yazıcısından çıktı alma sırasındaki işlemler, kullanılan mimarinin TCP/IP mi, Novell mimarisi mi olduğundan bağımsız olarak OSI modeli ile incelenebilmektedir. OSI referans modeli şekil 2.2’de görüldüğü gibi birbirini takip eden yedi katmandan oluşmaktadır.



Şekil 2.2: OSI referans modeli

2.1.1 Fiziksel katman

Fizik katman, ağ üzerindeki değişik sistemlerin birbirine bağlandığı fiziksel kablolama yapısı ile ilgilenmektedir. Bitsel iletişimi kablolar, bağlantı noktaları, veri

iletim hızları gibi bazı standartlar ile kontrol altına alır. Bu standartlar sayesinde bir biri ile haberleşecek iki uç noktanın iletim sırasında kullanılacak voltaj, akım ve direnç gibi elektriksel değerleri dikkate almaları gerekmeyecek. Üst katmanlar veriyi gerektiği gibi şekillendirdikten sonra veri fiziksel katmana ulaşacak ve iletim fiziksel ortamda bu katman sayesinde gerçekleştirilecek.

2.1.2 Veri bağlantı katmanı

Verinin iletim ortamında ne şekilde iletildiğinden sorumludur. Aynı zamanda fiziksel katmanın işlevini gerektiği gibi yapıp yapmadığını kontrol etmek zorundadır. İletim sırasında meydana gelen hatalarla ilgilenir ve hata mesajları hazırlayarak bunu ağ katmanına bildirir. Fiziksel adresleme ve fiziksel adres erişimi MAC(Media Access Control) adresi ile bu katmanda sağlanmaktadır. İkinci katman adreslemesi LAN dahilindeki haberleşme için switchler tarafından kullanılmaktadır. Switchler LAN içerisindeki cihazlar arasında anahtarlama işlemi yaparken bu cihazları MAC adresleri sayesinde tanımlayabilmektedirler.

2.1.3 Ağ katmanı

Ağ katmanı sistemler arasındaki haberleşmede kullanılan adresleri belirleyerek veriyi iletim ortamına uygun bir biçimde paketler ve veri bağlantı katmanına iletir. Ağ katmanı iki cihaz arasındaki haberleşmeyi sağlarken iki bilgiye ihtiyaç duymaktadır. Birincisi kaynak ve hedef bilgisayarlara atanan ve o cihazların herhangi bir yerden ulaşılmasını sağlayan kaynak ve hedef adresleri, ikincisi de bu iki cihazı birbirine bağlamak için tercih edilecek yol. Bu bilgiler ağ katmanında kullanılan protokole göre değişmektedir. En yaygın kullanımda olanlar TCP/IP ve IPX (Novell) protokol yığınlarıdır.

TCP/IP mimarisinde kullanılan IP adresi aslında ikinci katmanın yani veri bağlantı katmanının kullandığı MAC adresi ile karşılaştırılabilir. Ancak IP adresi WAN içinde anlamını yitiren MAC adresi yerine kullanılmaktadır. Ağ katmanı üst katmandan kendisine gelen bölümlenmiş veriyi paketlerken bir IP başlığı ekler. Bu başlıkta paketin sistemler arasındaki iletimi sırasında uyacağı kurallar dizini bulunmaktadır.

Birçok ağda, ağ katmanı veri bütünlüğünü kontrol etme görevini üstlenmez. Sadece paketleme ve ağ üzerindeki iletimi ile ilgilenir. Bu çeşit ağlarda veri bütünlüğü ve

verinin karşı tarafa ulaşp ulaşmadığı kontrolü gibi işlerle bir üst katmandaki protokoller ilgilenir. TCP/IP yapısında da bu işi dördüncü katman olan iletim katmanı üstlenmektedir.

2.1.4 İletim katmanı

İletim katmanı hedef ve kaynak cihaz arasındaki uçtan uca bağlantıyı sanal bir şekilde sağlamakla yükümlüdür. Ağ katmanında sunulmayan güvenilirlik hizmetini sağlamaktadır. Ağ katmanının düzgün bir şekilde çalışıp çalışmadığını kontrol edip gerektiği durumlarda verinin yeniden iletilmesini veya bir üst katmana hata mesajı gönderimini yerine getirmektedir.

Güvenilir veri iletimi tamamen uygulamadan uygulamaya değişmektedir. Bazı uygulamalar güvenilir iletim için ayrıca kullanılan bant genişliğini sadece veri iletimi için kullanmak isterler. Ve paketlerin karşı tarafa ulaşp ulaşmadığını kontrol etmek istemezler. Bu sistemlere bir örnek UDP kullanan alan adı sistemidir(DNS).

TCP kullanan uygulamalar güvenilirlik özelliğinden yararlanmak isteyenlerdir. Güvenilir iletim sırasında aşağıdaki işlemler yapılmaktadır:

- İletilen parçaların alındı bilgisi göndericiye bildirilir.
- Eğer parçaların iletimi sırasında alındı bilgisi gelmezse, o parça yeniden gönderilir.
- Parçalar alıcı tarafta göndericinin belirlediği sıraya göre düzgün bir biçimde dizilir.
- Son noktalar arasında akış kontrolü sağlanır.

Ağ katmanı, uygulama katmanından gelen uygulama bilgilerini “Port Numaraları” diye isimlendirilen numaralar sayesinde paketlere eklemektedir. Mesela HTTP servisi kullanılmak isteniyorsa 80 numaralı port, SSH kullanılmak isteniyorsa da 22 numaralı port bilgisi pakete eklenmektedir. Bu bilgiler gene karşı tarafın iletim katmanı tarafından değerlendirilmektedir.

2.1.5 Oturum katmanı

Oturum katmanı sistemler, uygulamalar veya kullanıcılar arasında oturum açma görevini yerine getirmektedir. Üst katmanlardan aldığı oturum açma isteğini, alt katmanları kullanarak yerine getirmektedir. Oturum sağlandığı zaman oturum

katmanı üst katmanlar arasındaki iletişim sağlamaktadır. Üst katmanların işi bittiği zaman bağlantı gene oturum katmanı tarafından sonlandırılır.

2.1.6 Sunum katmanı

Sunum katmanı gönderilen bilginin karşı taraf tarafından anlaşılabilir olması ile ilgilenmektedir. Uygulama katmanından gelen, oturum katmanı tarafından sağlanan bağlantıda kullanılacak, bazı uygulama ve servislere gelişmiş hizmetler sağlamaktadır.

Sunum katmanının sağladığı hizmetlerden biri veri sıkıştırma hizmetidir. Veri sıkıştırma işleminin sunum katmanında yapılması sayesinde, bu servisin uygulamalar tarafından geliştirilmesine gerek kalmaması ve iletim katmanının gerekli olmadığında bu servisi kullanmaması sağlanabilmektedir.

2.1.7 Uygulama katmanı

Uygulama katmanı, ağdaki cihazlara ağ servislerini kullanma olanağı vermektedir. Bu katmanda günlük yaşamda çok sık kullandığımız birçok protokol bulunmaktadır. HTTP, FTP, DNS, SMTP, SNMP, RLOGIN bunlardan bir kısmıdır.

Uygulama katmanı aynı zamanda programların ağı kullanması için bir arayüz oluşturmaktadır. Örnek olarak Microsoft API'leri uygulama katmanında çalışmaktadır. Ağ üzerine program yazan yazılımcılar bu API'leri kullanarak alt katmanlarda neler yapıldığıyla ilgilenmeksizin rahatlıkla program yazabilmektedirler[6].

2.2 TCP/IP Ağ Erişim Katmanı

Ağ erişim katmanı bir IP paketinin ağ ortamına erişebilmesi için ihtiyaç duyacağı tüm işlemlerle ilgilenmektedir. LAN ve WAN teknolojilerinin detaylarının içermekte ve OSI referans modelinde bulunan fiziksel ve veri bağlantı katmanlarının yaptığı görevleri üstlenmektedir. Ağ erişim katmanı, ağ donanımlarının kullanımı ve ağa erişim için tüm kuralları tanımlamaktadır. Modem protokol standartlarından olan SLIP ve PPP modem bağlantısı ile ağ erişimi sağlamaktadırlar. Bu protokoller ağ erişim katmanında bulunmaktadır. Aynı zamanda Ethernet, Fast Ethernet, FDDI, ATM, Frame Relay gibi teknolojiler de bu katmanda yer almaktadırlar.

2.3 TCP/IP İnternet Katmanı

İnternet katmanının amacı paketlerin ağ içinde iletimi sırasında en iyi yolu bulup oradan paketlerin iletilmesini sağlamaktır. Bu katmandaki en temel protokol İnternet protokolü'dür. IP bir paket ve adresleme yapısı belirler, veriyi İnternet katmanından ağ erişim katmanına geçirir ve paketleri uzaktaki cihaza yönlendirir. İnternet katmanında IP haricinde ICMP, ARP ve RARP protokolleri de işlem görmektedir

2.3.1 İnternet protokolü

İnternet protokolü, tüm kuralları ile birlikte IETF belgelerinden RFC 791'de tamamen anlatılmıştır. RFC 791 Eylül 1981'de Southern California Üniversitesi tarafından hazırlanmıştır. IP'nin tasarım amacı "birbirine bağlı sistemler içinde kullanılmak üzere paket anahtarlama bilgisayar haberleşme ağları oluşturmak" olduğu belirtilmiştir[7].

IP güvenilir olmayan (unreliable) bir protokol olarak geçmektedir. Bunun sebebi iletim işini yerine getirememesinden değil, verilerin aktarılması sırasında son noktalar arasında veya atlama noktalarında herhangi bir onay sistemi ve veri kontrol sistemi bulunmamasındandır. İletim sırasında kaybolan bir paket için yeniden iletim de yapılmamaktadır. Aynı zamanda bir akış kontrolü de bulunmamaktadır. Bu bahsedilen kontroller ve mekanizmalar bir üst katmanda bulunan TCP'ye bırakılmıştır.

Şu anda dünyada yoğun olarak kullanılan İnternet protokolü IPv4'tür. IPv4 adreslerinin uzunluğu 32 bittir. Bu da $2^{32}=4,295$ milyar adet IPv4 adresi atanabileceği anlamına gelmektedir. Ancak bu adresler çok düzensiz paylaşılmıştır. Mesela Amerika'nın Stanford Üniversitesi'nde, Çin'in sahip olduğu tüm IPv4 adres sayısından daha fazla adres vardır. Ayrıca 4,3 milyar adresin %70'i Kuzey Amerika'ya tahsil edilmiştir, yani dünyanın geri kalanına adreslerin %30'u kalmaktadır[8].

IPv4 adresleri 1'ler ve 0'lardan oluşan 32 bitlik bir yapıdır. Okunabilirliği arttırmak ve bazı sistematik düzenlemeler yapabilmek için bu adresler dört tane sekizlik halinde gösterilmektedir. Örnek olarak 160.75.67.1 adresi onluk sayı düzeni ile bu

şekilde gösterilirken, bilgisayar içinde 10100000.01001011.01000011.00000001 şeklinde ikilik sayı düzeninde işlem görmektedir.

Versiyon	IHL	Hizmet Türü	Toplam Uzunluk
(Version)	(IP Header Length)	(Type of Service)	(Total Packet Length)
Tanımlama		Bayraklar	Parça Konumu
(Fragmentation Identifier)		(Flags)	(Fragmentation Offset)
Kalış Süresi	Protokol	Başlık Kontrolü	
(Time-to-Live)	(Protocol ID)	(Header Checksum)	
Kaynak Adresi (Source IP Address)			
Hedef Adresi (Destination IP Address)			
Seçenekler (Options)			Dolgu (Padding)

Şekil 2.3: IPv4 başlık yapısı

Şekil 2.3'te IPv4 başlık yapısı verilmiştir. Bu yapı paketlerin ağ içerisinde doğru ve en hızlı bir şekilde iletilmesini sağlamak üzere geliştirilmiştir. Başlıkta bulunan alanlar:

Versiyon: İnternet protokolünün versiyonunu belirtmektedir. Büyüklüğü dört bittir. IPv4 için değeri 4'tür.

IHL: IP başlık uzunluğunu belirtmektedir. Bu bilgiyi taşımak üzere ayrılan yer dört bittir. En küçük başlık boyutu 20 Byte'tır. Tüm alanlardaki bitlerin kullanılması ile oluşturulacak en büyük başlık boyutu da 60 Byte'tır.

Hizmet Türü: Bazı özel uygulamalar tarafında kullanılabilecek bir alandır. Uzunluğu sekiz bitten oluşmaktadır.

Toplam Uzunluk: Başlık büyüklüğü ve veri boyutunu da sayarak tüm IP paketinin uzunluğunu belirten değerdir. Bu değeri ifade etmek için 16 bit kullanılır.

Tanımlama: Paketlerin ilişkilendirmesini sağlayabilmek için verilen 16 bitlik rastgele bir sayıdır.

Bayrak: Paketlerin parçalara ayrılıp ayrılmadığı bilgisi ve bunların kontrolünü sağlamak için verilen üç bitlik bayrak değeri.

Parça Konumu: IP veri paketinin başlangıç yerini belirten on üç bit ile ifade edilen alandır.

Kalış Süresi: Yönlendirilme sırasında verinin atlayabileceği en fazla düğüm sayısını belirtmektedir. Bu sayı aşılsa paket iletilememiş varsayılır ve yok edilir. Bu bilgi başlıkta sekiz bit olarak tutulur.

Protokol: IP paketinin içerisine gömülmüş daha üst seviyedeki protokolü belirtir. Sekiz bitlik uzunluktadır.

Başlık Kontrolü: Verinin iletim sırasında herhangi bir bozulmaya uğrayıp uğramadığını kontrol etmek için tutulan alandır, sekiz bit uzunluğundadır.

Kaynak Adresi: Veriyi gönderen tarafın IP adresi bilgisini taşıyan alandır. Otuz iki bit uzunluğundadır.

Hedef Adresi: Veriyi alacak olan tarafın IP adresi bilgisini taşıyan alandır. Gene otuz iki bit uzunluğundadır.

Seçenekler: IP başlığına bazı özellikleri eklemek için koyulan bir alandır. Normal halde sıfır bittir ancak istenirse 40 Byte'a kadar çıkabilir.

Dolgu: IP paket başlığının 32 bitin katları şeklinde olmasını sağlayan alandır. Boyutu kullanılan başlığa göre değişmektedir[9].

İki çeşit İnternet adresi bulunmaktadır; global IP adresi, özel (private) IP adresi. İnternet üzerinden haberleşen iki uç noktanın mutlaka kendine ait benzersiz bir IP adresi olması gerekmektedir. Bu adrese global adres denmektedir ve İnternet üzerinde iki tane aynı global adres bulunamamaktadır. Özel adresler ise aynı ağ içinde kullanılabilen ancak dışarı ağa veya İnternet'e yönlendirilemeyen adreslerdir.

IPv4 adreslerinde meydana gelen sayı yetersizliği sorununu çözmek için geliştirilen teknolojilerden bir tanesi ağ adresi çevirme yani NAT'tır. NAT ağ içinde özel adresleri kullanmakta ve sadece ağ dışına çıkarken global adres kullanmaktadır. Bu da sınırlı olan global IP adreslerinin olabildiğince az kullanılmasını sağlar ancak haberleşen iki uç nokta arasına başka cihazların girmesi anlamına gelir ve uçtan uca bağlantıyı sınırladığı için tam bir çözüm olamamaktadır.

2.3.2 ICMP

ICMP, İnternet kontrol mesaj protokolü olarak IP cihazların ağ ve iletimle ilgili problem bilgilerini değiş tokuş etmelerini sağlamaktadır. IP güvenilir olmayan bir protokol olmasına ve iletimle ilgili hiçbir garanti vermemesine rağmen veriyi gönderen tarafa verinin iletilip iletilmediği bilgisini göndermek önemlidir ve ICMP bunu sağlamaktadır.

IP normal çalışma prensiplerine göre veri paketlerinin kaybolması ile ilgilenmez. Eğer bu veri paketleri önemli paketlerse bu görevi daha üst katmanlardan (mesela iletim katmanından TCP veya uygulama katmanından TFTP) bir protokol üstlenmektedir.

Teori bu şekilde iken bazen bir problem yüzünden tüm veri paketlerinin hedef adrese ulaşması engellenebilir. Bu durumda mutlaka göndericiye paketlerin hedefe ulaşmadığı bilgisi gönderilmelidir. Bu şekilde gönderici veri paketlerini göndermeyi bırakabilir veya gönderme şeklini probleme göre değiştirip yeniden gönderebilir. Bu tarz problemlerde göndericiye haber verme görevini ICMP üstlenmektedir[10].

ICMP Hata mesajları:

- Hedef Ulaşılamaz (Destination Unreachable)
- Yeniden Yönlendirme (Redirect)
- Kaynak Yetersizliği (Source Quench)
- Zaman Aşımı (Time Exceeded)
- Parametre Problemi (Parameter Problem)

2.3.3 ARP

ARP, IP tabanlı cihazların kendi yerel ağlarındaki cihazlara donanım adreslerinden erişebilmek için kullandıkları bir protokoldür. IP adresini cihazın daha önceden eşleştirilmiş donanım adresine çevirmektedir. Bu servis yerel ağdaki IP cihazlarının kendi aralarında anlaşabilmesi için mutlaka gerekmektedir. ARP, RFC 826'da tanımlanmış daha sonra RFC 1122 ile güncellenmiştir.

Aynı ağda bulunan iki cihaz aralarında haberleşmek istediklerinde bulundukları özel ortam için tasarlanmış alt seviye protokolleri ve adresleme yapılarını kullanırlar. Mesela ethernet cihazları haberleşmek için ethernet'e özel donanımsal adresler kullanmaktadırlar[11].

2.3.4 RARP

RARP protokolü ARP'ın yaptığı işin tam tersini yapmaktadır. Yani cihazın donanım adresini IP adresine çevirmektedir. RARP genellikle diski olmayan iş istasyonlarında veya IP adresini kaydetmek için yeterli kaynağı olmayan cihazlarda kullanılmaktadır. Bu cihazlar gerektiği zaman bir RARP sunucusuna, RARP isteği yollayarak kendi donanım adresleri ile eşleştirilmiş IP adresini öğrenebilirler.

RARP, IP adresi bilgisini alma konusunda yeteri derecede kullanışlı olsa bile eksik olduğu alanlar vardır. Ağ maskesi ve yönlendirici bilgilerine erişememektedir. Bu yüzden birçok ağda adres atama ve yapılandırma konusunda BOOTP ve DHCP protokolleri kullanılmaktadır[12].

2.4 TCP/IP İletim Katmanı

İletim katmanının birincil görevi kaynaktan hedefe doğru bilginin akışını düzenlemek ve bilgiyi güvenilir ve doğru bir biçimde hedefe iletmektir. İletim katmanında verilen servisler aşağıdaki gibidir:

- Daha üst katmandan gelen uygulama verisini uygun büyüklükte parçalara bölme
- Uç noktalar arası oturumlar kurmak
- Bölümlenmiş parçaların bir uç noktadan diğer bir uç noktaya iletimini sağlamak
- Kayan pencereler yöntemiyle akış kontrolü sağlamak
- Sıra numaraları ve onay bilgileri yardımıyla güvenilir iletişim sağlamak

İletim katmanı verinin transferini sağlarken bir taraftan da veri kaybı olmadığını garanti etmek ister. Alıcı uç eğer gönderilen veriyi gönderildiği hızda işleyemiyorsa alıcı tarafta veri kaybı olacaktır. Çünkü verici uç aynı hızla göndermeye devam ediyordur. Akış kontrolü bu noktada devreye girerek iki ucun belli bir hızda anlaşmasını sağlar. Bu şekilde gönderici taraf alıcının işleyebileceği hızda veri iletimi yapar ve paketler kaybolmamış olur. İletim katmanında iki önemli protokol bulunmaktadır; TCP ve UDP.

2.4.1 TCP

İletim katmanında bulunan TCP bağlantı yönlü (connection-oriented) bir protokoldür. Veri iletimi başlamadan önce TCP iki uç arasında bağlantı kurmaktadır. Böyle bir bağlantının kurulabilmesi için iki uç nokta üç yollu el sıkışma denilen bir yöntemle bazı senkronizasyon numaraları göndererek aralarında anlaşır.

Güvenilir iletimde her veri paketi göndericinin gönderdiği sırada ulaşması gerekmektedir. Aksi takdirde eğer paket kaybolur, hasara uğrar veya değişik sırada alıcıya ulaşır TCP başarısız olmuş demektir. Bu sebeple her iletilen paketten sonra

bir onay bilgisi beklenir ve ondan sonra sıradaki paket iletme başlanır. Bu durum pencere büyüklüğünün bir olduğu durumdur. Pencere büyüklüğü değiştirilerek pencere büyüklüğü sayısı kadar pakette bir onay alınması sağlanabilir. Pencere büyüklüğünün üç olduğu bir durumda gönderici üç adet paketi gönderdikten sonra onay için bekler ve onay gelmeden dördüncü paketi göndermez. TCP'yi kullanan protokollerden bazıları:

- FTP – port 21
- HTTP – port 80
- SMTP – port 25
- Telnet – port 23

2.4.2 UDP

UDP ön bağlantısız (connectionless) bir iletim katmanı protokolüdür. Veriyi herhangi bir sıra numarası veya onay numarası olmadan veri iletim garantisi vermeksizin taşıyan basit bir TCP/IP protokolüdür. Hata analizi ve yeniden iletim prosedürleri üst seviye protokoller tarafından sağlanmalıdır.

UDP'yi kullanan protokoller:

- TFTP – port 69
- SNMP – port 161
- DNS – port 53

2.5 TCP/IP Uygulama Katmanı

OSI referans modelinde ayrı ayrı bulunan oturum, sunum ve uygulama katmanları TCP/IP modelinde tek bir katman olarak uygulama katmanı adını almıştır. Burada amaç son katman üzerinde çalışabilen yazılım geliştiricilere daha fazla esneklik sağlamaktır. Bazı uygulama katmanı protokolleri ve üstlendikleri görevler aşağıda belirtilmiştir:

- NNTP – Ağ haber iletim protokolü: NNTP güvenilir bir iletim ağı üzerinden haberlerin istenilen yerlere iletilmesi görevini yerine getirir. NNTP'nin çalışma yapısına göre haberler merkezi bir veri bankasında toplanır, bu veri bankasına üye kişi tüm haberleri değil sadece istediği haberleri seçip okuyabilir[13].

- SMTP – Basit posta iletim protokolü: SMTP’nin amacı elektronik postaları güvenilir ve verimli bir biçimde iletmektir. E-posta sunucuları aralarında SMTP ile konuşarak mesaj alıp gönderirler. SMTP protokolü elektronik posta mesajlarını TCP’yi kullanarak ASCII formatında gönderirler[14].
- FTP – Dosya transfer protokolünün (FTP) amacı; dosya paylaşımını geliştirmek, uzak bilgisayarlara dolaylı veya direk erişimi arttırmak, kullanıcıyı çeşitli dosya sistemleri karmaşasından kurtarmak ve veriyi güvenilir ve verimli bir şekilde iletmek olarak RFC 765 belgesinde belirtilmiştir.
- HTTP – WWW ile birlikte çalışan ve Web üzerinden bilgiye ulaşmayı sağlayan protokoldür. İnternet’in en hızlı gelişen ve en çok kullanılan parçasıdır. HTTP sunucu istemci tabanlı çalışmaktadır. Bağlanılmak istenen Web sitesi sunucuda yer almakta, istemci de bu siteye bağlanabilmek için bir Web tarayıcısı kullanmaktadır. En popüler iki Web tarayıcısı Firefox ve İnternet Explorer’dır. Web sayfalarının yapıldığı dile de HTML denmektedir.

3. İNTERNET PROTOKOLÜ VERSİYON 6

IPv6, İnternet ve birçok İntranet'in temelini oluşturan İnternet Protokolü'nün yeni versiyonudur. Bu konudaki çalışmalar 1991 yılında başlamış ve 1995 yılına gelindiğinde RFC 1883 ile tamamen standartlaştırılmıştır. Bu süreç içinde IPng (IP new generation) ve IPv7 olarak da adlandırılmış ama IPv6 olarak standartlaşmıştır.

Şu anda yaygın olarak kullanılan İnternet Protokolü olan IPv4 1981 yılında RFC 791 tarafından tanımlanmıştır. IPv4 adresleri 32 bit uzunluğunda bir mimariye sahiptir. Bu uzunluk 4 milyar adresi ifade etmektedir. Dünya üzerinde 4 milyar tane bilgisayar olmamasına rağmen IPv4 adresindeki tükenme ne demek buna açıklık getirmek gerekmektedir.

IPv4 adres aralığı sıkıntısı aslında tüm adreslerin kullanılmasından kaynaklanmamaktadır. Bu adreslerin bilgisayarlara tek tek verilmeyip aslında birer ağ dahilinde dağıtılması, adreslerin verimli kullanımını engellemektedir. Adres dağıtımı yapılan ağlar üç sınıfa ayrılmıştır.

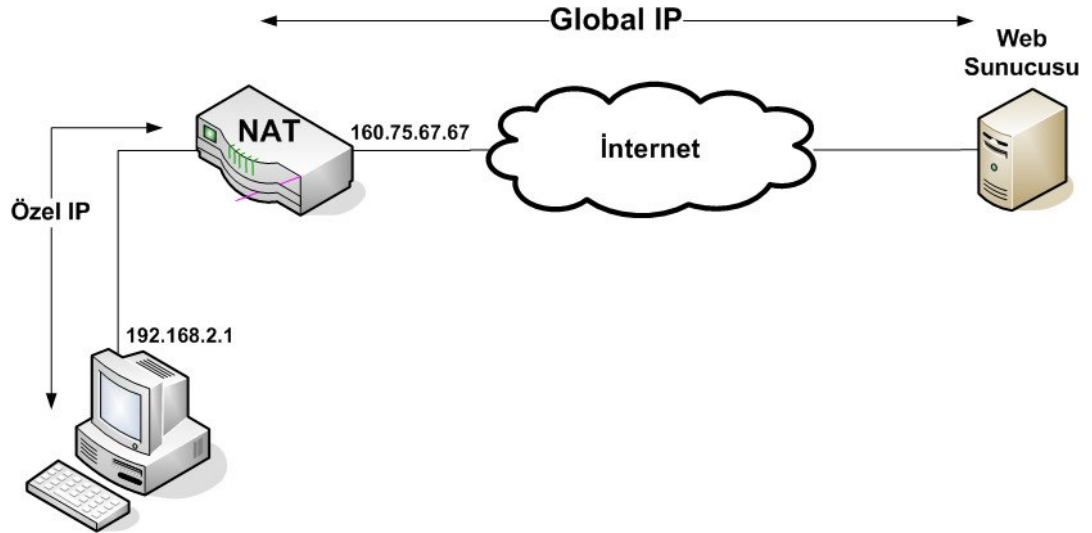
- Sınıf A'da 128 adet ağ, ve her bir ağa 16 milyon adres düşmektedir.
- Sınıf B'de 16.000 adet ağ, ve her ağda 65.000 adet adres bulunmaktadır.
- Sınıf C'de 2 milyon ağ, ve her ağda 254 kullanılabilir adres bulunmaktadır.

Problemin kaynağını bu mimaride aramak gerekmektedir. Mesela B sınıfı bir adres aralığı alan bir firmanın 65.000 adet IP adresine ihtiyacı olmasa bile bu adresler kendisine atanmaktadır. Ve başka bir firma tarafından kullanılamamaktadır. Bu da çok ciddi adres israfına neden olmaktadır.

Bu anlatılan adres darlığının yakın bir süre içinde İnternet için bir problem haline geleceği gerçeği 1991 yılında anlaşılmış ve yeni nesil İnternet Protokolü konusunda çalışmalar başlatılmıştır. Yeni nesil IP çalışmalarına paralel olarak mevcut protokol olan IPv4'ün ömrünün nasıl uzatılabileceği konusu üzerine de yoğun çalışmalar yapılmıştır. Bu çalışmalar sonucunda 1993 yılında İnternet'e yeni bir soluk getirmek amacıyla CIDR (Sınıfsız Alanlar Arası Yönlendirme) haberleşme dünyasına tanıtılmıştır.

CIDR’da asıl amaç sınıfsal adres dağıtımını ortadan kaldırarak mevcut IPv4 adreslerini daha verimli kullanabilmektir. Bu konuda da başarılı olunmuştur. Ancak gerek şimdiye kadar dağıtılmış birçok adres nedeniyle gerekse İnternet’in çok hızlı gelişmesi ve İnternet’e bağlanan cihazların sayısının giderek artması nedeniyle CIDR da tam olarak bir çözüm olamamıştır[15].

IPv4 adres sorununu çözmek için geliştirilen diğer bir yöntem ise NAT (Ağ Adres Çevirimi) olarak adlandırılmış ve RFC 1597 ile RFC 1918’de tanımlanmıştır. NAT’ın çalışma mantığına göre tüm ağların içindeki adresler aynı özel IP adresleri olabilmekte ve bu adresler ağ dışına yönlendirilememektedir. Ancak ağ içindeki cihazlar ağ dışına veya İnternet’e çıkarken global adres ile eşleşmektedirler. Bu şekilde sadece ağ dışına çıkan cihazlara global IPv4 adresi atanmakta ve adres tasarrufu sağlanabilmektedir.



Şekil 3.1: NAT örneği

Şekil 3.1’de özel IP adresi 192.168.2.1 olan bir makinenin İnternet’teki bir Web sunucusu ile haberleşmesi gösterilmektedir. Bu cihazın paketlerinin İnternet ortamında yönlendirilebilmesi için yerel ağ dışına çıkarken, NAT cihazı tarafından global bir IP ile eşleştirilmesi lazımdır. Örnekte eşleştirilen IP adresi 160.75.67.67’dir. Bu adres global bir IP adresidir ve tüm dünyada sadece bir makineye verilebilir. Ancak 192.168.2.1 adresi özel bir IP adresidir ve aynı yerel alan ağı içinde birden fazla kullanılmamak şartıyla değişik ağlarda sayısız bir şekilde tekrarlanabilmektedir.

Özel adresler İnternet adresi otoritesi olan IANA (Internet Assigned Numbers Authority) tarafından 3 blok olarak tanımlanmışlardır[16]:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

İlk blok 24 bitlik, ikinci blok 20 bitlik ve üçüncüsü 16 bitliktir. Bu adreslerden herhangi bir çeşidini kullanmak isteyen bir firma IANA'ya danışmaya gerek olmadan rahatça adres dağıtımı yapabilir. Çünkü özel IP adreslerinin yerel alan ağı dışında hiçbir geçerliliği yoktur ve başka bir firmanın özel IP adresiyle çakışma olasılığı yoktur.

NAT yerel alan ağlarında geniş anlamda kullanım bulmuştur ve IP adres aralığındaki azalmayı yavaşlatmıştır. Ancak uçtan uca (peer-to-peer) bağlantıyı imkânsız kılması nedeniyle özellikle ses ve görüntü servisleri gibi servislerde kullanılamamış ve yeni nesil bir IP ihtiyacını giderememiştir.

Bütün bu gelişmeler göz önüne alınarak IPv6 yapısı, ihtiyaçları en iyi şekilde karşılayabilecek şekilde geliştirilmeye çalışılmıştır. Bu araştırma geliştirme sırasında yeni nesil protokolün aşağıdaki özellikleri sağlaması gerektiğine karar verilmiştir:

- Sağlayacağı adres aralığının hiçbir zaman bitme derdinin olmaması
- IPv4'teki gibi sınıfsal adres dağıtımını kullanmak yerine CIDR kullanmak.
- Şu anda IPv4 ile çok kabarmış olan yönlendirici tablolarının boyutunu düşürmek ve yönlendirmeyi daha verimli hale getirmek.
- İnternet için global IP adresleri, yerel ağ için yerel IP adresleri kullanmak.

IPv4'te eksikliği hissedilen yukarıdaki özellikler doğrultusunda geliştirilen IPv6; IPv6 adres yapısı, IPv6 başlığı ve eklentileri, ICMPv6 protokolü, komşu keşfi mimarisi, IPv6 yönlendirme, IPv6 alan adı sistemi ve IPv6'ya geçiş teknikleri başlıkları altında detaylı bir şekilde incelenecektir.

3.1 IPv6 Adresleri

IPv6'nın geliştirilmesindeki ana neden IPv4 adres aralığının er ya da geç biteceği gerçeğidir. Bu sebeple 32 bit olan IPv4 adresleme yapısı IPv6'da 128 bite genişletilmiştir. 128 bit ile 2^{128} adet adres sağlanabilmektedir. Bu sayı yaklaşık

olarak 10^{38} 'e, tam olarak da 340.282.366.920.938.463.463.374.607.431.768.211.456 adet adrese denk gelmektedir. Dünya yüzeyinin 511.263.971.197.990 metre kare olduğu bilgisi kullanılarak, dünya üzerindeki her metre kare alana yaklaşık $655,5 \times 10^{21}$ adres düşmekte olduğu hesaplanabilmektedir[17]. Bu da inanılmaz bir adres sayısıdır.

3.1.1 IPv6 adres yapısı

IPv4 adresleri 8 bitlik 4 blok halinde ve bloklar arasına nokta işareti koyularak ifade edilmektedir. Örnek adres gösterimi 160.75.67.1 şeklindedir. Aynı şekilde IPv6 adresleri için de tasarım zamanında noktalı bir gösterim seçilebilirdi ancak IPv4 adreslerine göre 4 kat daha uzun oldukları için değişik bir gösterim seçilmiştir. Onluk sayı sistemi yerine onaltılık sayı sistemi kullanılarak IPv6 adresinin daha kısa bir uzunlukla ifade edilmesi sağlanmış ve bloklar arasına iki nokta işareti koyulması uygun görülmüştür. 2001:4BD0:2031:2345:6AE2:FF23:245A:90BB örnek bir IPv6 adresini göstermektedir.

IPv6 adresleri üç değişik şekilde ifade edilmektedirler.

- Tercih edilen gösteriş biçimi x:x:x:x:x:x şeklindedir. Bu gösterimde her bir x onaltılık sayı düzeninde yazılmış 16 bitlik adres parçalarını ifade etmektedir. Örnek olarak 2001:4BD0:2031:2345:6AE2:FF23:245A:90BB adresi verilebilir. Veya 2001:4BD0:2031:0:0:0:1 şeklindeki gibi 16 bitlik sayı parçalarının sol tarafındaki anlamsız 0'ları yazmadan kısaltılmış bir biçimde gösterilebilir.
- Bazı IPv6 adreslerinde birbirini takip eden uzun sıfır dizileri bulunmaktadır. Bu tür adresleri daha kolay ifade edebilmek için bir kısaltma yöntemi geliştirilmiştir. Bu yönteme göre "::" gösterimi bir veya daha çok 16 bitlik sıfır dizisini ifade etmektedir. Örnek olarak belirtilen adresler;

2001:4BD0:2031:0:0:0:1	unicast adresi
FF01:0:0:0:0:0:101	multicast adresi
0:0:0:0:0:0:1	loopback adresi

aşağıdaki şekilde gösterilebilir:

2001:4BD0:2031::1	unicast adresi
FF01::101	multicast adresi
::1	loopback adresi

- Bazı durumlarda IPv4 ve IPv6 protokolleri beraber kullanılmaktadır. Bu gibi durumlarda x:x:x:x:x.d.d.d.d şeklinde bir gösterim kullanılabilmektedir. X'ler 16 bitlik altı adet bloğu onaltılık sayı sisteminde, d'ler de 8 bitlik 4 adet bloğu onluk sayı sisteminde göstermektedir. 2001:4BD0:0:0:0:160.60.67.1 bu tarz gösterime bir örnektir. Bu gösterimde son 32 bit standart IPv4 adresi yapısındadır.

3.1.2 IPv6 adres ön ekleri

IPv6 ön ekleri (prefix) gösterimi IPv4'de kullanılanla aynı şekilde CIDR gösterimine göre ifade edilmektedir. 24 bitlik alt ağ maskesine sahip olan bir IPv4 adresi 192.168.1.0/24 şeklinde gösterilirken, 48 bitlik bir ön eke sahip IPv6 adresi de 2001:0:2310::/48 şeklinde gösterilmektedir. Bu adres için aşağıdaki gösterimlerin tamamı doğrudur:

2001:0000:2310:0000:0000:0000:0000/48
 2001:0:2310:0:0:0:0:0/48
 2001:0:2310::/48

Ancak aşağıdaki gösterimler doğru değildir:

2001:0:231/48	Sağ taraftaki 0'lar ön eke göre gösterilmeyebilir ancak 16 bitlik bloğun içindeki sağda bulunan bir sayıyı takip eden 0'lar atılamaz. Yukarıdaki gösterim 2001:0:2310/48 şeklinde değil de 2001:0:0231/48 şeklinde anlaşılmaktadır
2001::2310/48	Bu adres gösterimi de yukarıdaki adresi ifade etmemektedir. Bu adres 2001:0:0:0:0:0:2310 şeklinde bir adresi belirtmektedir.
2001::2310::/48	Bu gösterim tamamen söz dizimi hatasıdır, "::" ifadesi bir adresin içinde birden fazla kullanılamaz.

Alt ağ maskesi ile uç nokta adresi tek bir şekilde gösterilebilmektedir. Mesela alt ağ maskesi 2001:4BD0:2031::/48 olan bir ağda, bir sunucuya 2001:4BD0:2031::1 adresi verilmiş olsun. Bu sunucunun adresi alt ağ maskesi ile birlikte ifade edilmek istenirse 2001:4BD0:2031::1/48 şeklinde gösterilir.

3.1.3 IPv6 adres türleri

IPv6 adres uzunluğunun 128 bit seçilmesinin amacı hiyerarşik yönlendirmeyi kolaylaştırmaktır. Cihazın ağ arayüzüne atanan 128 bitin 64 biti alt ağ tanımlayıcısı (subnet identifier), diğer 64 biti de arayüz tanımlayıcısıdır (interface identifier).

IPv4'teki sınıflandırmaya benzer şekilde IPv6'da da üst seviye bitler IPv6 adres çeşitlerini belirtmektedir. Bu üst seviye bitlere aynı zamanda FP (format prefix) de denilmektedir. Bazı çok kullanılan adreslerin FP'leri aşağıdaki gibidir[18]:

- Loopback adresi FP= 00...1 (128 bit)
- Global unicast adresinde FP= 001
- Link-local unicast adresinde FP= 1111 1110 10
- Site-local unicast adresinde FP= 1111 1110 11
- Multicast adresinde FP= 1111 1111

Yukarıda verilen FP örneklerinden de anlaşılacağı gibi IPv6'da 3 temel adres çeşidi vardır. Bunlar:

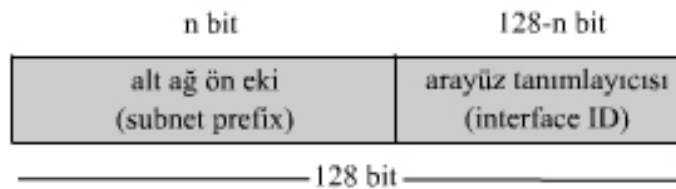
- Unicast Adresi
- Multicast Adresi
- Anycast Adresi

IPv4'te bulunan broadcast adresi IPv6'da tamamen kaldırılmış bu görevi multicast adresi yerine getirmektedir. Ayrıca yeni bir çeşit olan anycast adresi getirilmiştir.

3.1.4 Unicast Adresleri

IPv6 unicast adreslerinin yapısı, uzunluğu hariç CIDR'lı IPv4 adreslerinin yapısına çok benzemektedir. Çok çeşitli unicast adresleri vardır; global, site-local ve link-local bunlardan bazılarıdır. Ayrıca global unicast adreslerinin alt çeşitlerini oluşturan, kodlanmış NSAP ve IPv4 içeren IPv6 adresleri gibi özel amaçlı adresler de vardır.

IPv6 kullanan cihazların bu adreslerin çeşitleri konusundaki bilgileri tamamen ağ içindeki sorumluluklarına göre değişmektedir. Basit bir son nokta cihazı sadece adres uzunluğu bilgisine sahip olup o adresin içyapısı hakkında hiç bilgi taşımayabilir. Biraz daha gelişmiş bir son kullanıcı cihazı alt ağ ön eki ve arayüz tanımlayıcıları hakkında bilgi sahibi olmaktadır. Yönlendiriciler gibi ağ içinde önemli görevler üstlenen cihazlar ise bu adresleri çok daha iyi analiz edebilmelidirler.



Şekil 3.2: IPv6 adres bölümlenmesi

Şekil 3.2’de belirtilen arayüz tanımlayıcıları kendisine atanan cihazı ağ üzerinde tanımlamakla görevlidirler. Benzersiz olmaları gerekmektedir ve aynı ağ içinde birden çok cihaza atanamazlar. Bazı durumlarda arayüz tanımlayıcısı adresi cihazın ikinci katman fiziksel adresinden elde edilmektedir.

Unicast adreslerinin birçok çeşidi vardır. Bunlar; tanımlanmamış adres (unspecified address), loopback adresi, global adres, link-local adresi, site-local adresi, IPv4 adresi içeren IPv6 adresleri, gizlilik ekleri (privacy extensions) ve uyumluluk (compatibility) adresleridir.

3.1.4.1 Tanımlanmamış unicast adresleri

Tüm bitleri sıfır olan adrese tanımlanmamış adres denilmektedir. Kısa gösterimi ile “::” şeklinde yazılabildiği gibi 0000:0000:0000:0000:0000:0000:0000:0000 şeklinde de uzunca ifade edilebilmektedir. Bu adresin var olma amacı herhangi bir düğüme bir adresin atanmadığını ifade etmektir, hiçbir zaman bir son noktaya IP adresi olarak atanmamalıdır. Bu adresin kullanım alanlarından biri, henüz adres tanımlanmamış bir cihazın adresinin verilmesi sırasında o cihaza kaynak adresi olarak atanmaktır. Bu şekilde o cihazın bir adrese ihtiyacı olduğu belirtilmektedir ve cihazın IP yapılandırılması işlemi yerine getirilmektedir.

Tanımlanmamış unicast adresleri asla IPv6 paketlerinin hedef adresi veya yönlendirme başlığı adresi olmamalıdır. Eğer kaynak adresi olarak kullanıyorsa da asla ağ içindeki yönlendirici tarafından ağ dışına gönderilmemelidir.

3.1.4.2 Loopback adresi

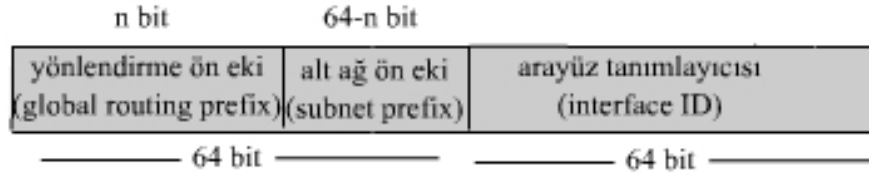
Sadece son biti 1 olan diğer bitleri 0 olan 0000:0000:0000:0000:0000:0000:0000:0001 adresi loopback unicast adresidir. Kısaca ::1 şeklinde de gösterilir. Bu adres cihaz içinde sanal bir arayüze atanarak cihazın kendi kendine IPv6 paketi göndermesini sağlamaktadır. Asla fiziksel arayüzlere atanmaması gerekmektedir.

Loopback adresi hiçbir zaman cihazın dışarıya gönderdiği IPv6 paketlerinin kaynak adresi olamamaktadır. Aynı şekilde hedef adresi loopback adresi olan bir IPv6 paketi ne cihazın dışında bir uç noktaya gönderilebilmekte ne de yönlendiriciler tarafından yönlendirilebilmektedir. Hedef adresi loopback adresi olarak atanmış, başka bir düğümden gelen bir paket kullanılmamakta ve hemen iptal edilmektedir[19].

3.1.4.3 Global adresler

Global unicast adresleri FP 001 değeri ile tanımlanmışlardır. İlk 16 bitlik dizi 2 veya 3 ile başlamaktadır. Bunun nedeni ilk 3 biti 001, bunu takip eden değer 0 veya 1 olabilmektedir. Eğer FP'yi takip eden değer 0 olursa IPv6 adresinin ilk rakamı 2, eğer 1 olursa adresin ilk rakamı 3 olmaktadır.

IPv6 global unicast adresleri aynı IPv4 global unicast adresleri gibi, İnternet'ten herhangi bir yerden erişilebilir ve yönlendiriciler tarafından kaynak adresi olarak kullanılan paketlerin hedef yerlere iletilmesini sağlayabilmektedirler. IETF RFC 1887 dokümanından global unicast adresleri ile ilgili daha detaylı bilgiye erişilebilmektedir. Şekil 3.3'te IPv6 global unicast adres yapısı gösterilmektedir.



Şekil3.3: Global unicast adres yapısı

3.1.4.4 Link-local adresleri

Link-local adresleri 10 bitlik “1111111010” bit dizisi ile başlamaktadır. Bu diziyi takip eden 54 bitlik bir 0 dizisi, sonra da arayüz tanımlayıcısı gelmektedir. Bu sebeple bu tip adreslerin ilk 64 biti FE80:: ile ifade edilmektedir.

Link-local adresler yerel alan ağı içinde kalmak üzere kullanılmakta anahtarlama cihazları tarafından hedeflere iletilmekte ancak asla yönlendiriciler tarafından dış dünyaya yönlendirilememektedir. Otomatik adres yapılandırması ve komşu keşfi gibi mekanizmalarda kullanılmaktadırlar.

3.1.4.5 Site-local adresleri

IPv6 site-local adresleri, IPv4'te kullanılan ve RFC 1597 ve 1918 ile tanımlanmış özel adreslerin yerini almak üzere tasarlanmıştır. IPv4 özel adresleri, alt ağ maskeleri ile birlikte 10.0.0.0/8, 172.16.0.0/12, 192.16.0.0/16 şeklinde ifade edilmektedir.

Site-local adreslerin tasarımı FP=1111111011 olacak şekilde yapılmıştır. FEC0:: şeklinde başlamaktadırlar. Bu adresler link-local adresler gibi otomatik olarak atanmazlar. Kullanıcı veya ağ tarafından ihtiyaç duyulması halinde yapılandırılırlar.

Yapı bakımından global unicast adreslerine çok benzerler. Global adreslerle birlikte kullanılabilirler. Yapısı ile ilgili bilgiler RFC 3513'te belirtilmiştir.

RFC 4219'da belirtildiği üzere bu adresler yeni uygulamalarda kullanılmayacak, ancak eski uygulamalar desteklemeye devam edebileceklerdir. Yeni uygulamalar bu ön ekli adresi global unicast adresi olarak algılayacaklardır.

3.1.4.6 IPv4 adresi içeren IPv6 adresleri

IPv4 adreslerini IPv6 adresinin en düşük anlamlı 32 bitinde taşıyan iki çeşit adres bulunmaktadır. Bunlar, IPv4 uyumlu (IPv4-compatible) adresler ve IPv4'le eşlenmiş (IPv4-mapped) adreslerdir.

IPv4 uyumlu adresler 0:0:0:0:0:m.n.k.l veya ::m.n.k.l şeklinde ifade edilmektedir. Adreste bulunan m.n.k.l 32 bitlik IPv4 adresidir ve daha anlamlı 96 bit "0" ile doldurularak 128 bitlik bir IPv6 adresi elde edilmektedir. Burada kullanılan IPv4 adresi global bir adres olmalıdır. Bu adres türü artık desteklenmemektedir çünkü mevcut IPv6 geçiş mekanizmalarının hiçbirisi bu adresi kullanmamaktadır. Bu sebeple yeni uygulamalar veya güncellemeler bu adresi desteklemek zorunda değildir.

IPv4'le eşlenmiş adresler 0:0:0:0:0:FFFF:m.n.k.l veya ::FFFF:m.n.k.l şeklinde ifade edilmektedir. Bu adres türü IPv4 düğümlerini IPv6 adresleri olarak tanımlayabilmek için kullanılmaktadır. En büyük avantajı bu adres çeşidini kullanan programlar tek adresi alarak hem IPv4 hem IPv6 adresini elde etmiş olurlar. Bu adres türünde son 32 bit ile ifade edilen IPv4 adresi onluk sayı düzeninde yazıldığı gibi istenirse onaltılık sayı düzeninde de yazılabilmektedir. RFC 4038 bu adresi türünün kullanımı hakkında detaylı bilgi vermektedir.

3.1.5 Anycast adresleri

Anycast adresleri IPv4'te bulunmayan ve IPv6 için geliştirilen bir adres çeşididir. Kendisine ait bir FP'si bulunmamaktadır. Aslında yapısal olarak bir unicast adresinin tamamen aynısıdır, ancak kullanım alanı farklıdır. Bir anycast adresi bir unicast adresinin birden çok düğüme verilmesi ile oluşmaktadır. Bu düğümlere atanan adresin anycast adresi olduğunu belirtmek gerekmektedir çünkü yapısal olarak bu adresleri unicast adresinden ayırmak mümkün değildir.

Bir grup ağ cihazına verilen anycast adresi o gruptaki cihazların herhangi birine ulaşmak için kullanılır. Yani unicastteki gibi birebir haberleşme veya multicastteki

gibi grubun tamamı ile haberleşme yapılmamaktadır. Anycast adresleri ile ilgili doğabilecek bazı sorunları engellemek için RFC 1884 ile bu adreslere bazı sınırlamalar getirilmiştir.

- Anycast adresleri IPv6 paketlerinin kaynak adresi olarak kullanılmamalı
- Anycast adresleri son noktalara atanmamalıdır. Bu da bu adreslerin IPv6 yönlendiricilerine atanabileceği anlamına geliyor.

Bu adreslerin kullanım alanına yönelik bir örnek, bir firmanın yönlendirme işlevini yerine getiren cihazlara anycast adresleri atanması olabilir. Bu yönlendiriciler firmanın İnternet bağlantısını sağlıyor olsunlar. Herhangi bir son nokta aynı anycast adresi kullanan bu yönlendiricilerden herhangi birini kullanarak İnternet'e çıkabiliyor olacaktır. Bu sayede her bir yönlendiricinin adresini tek tek bilmesi gerekmeyecektir[20]. Henüz çok fazla kullanım alanı bulamış olmalarına rağmen, IPv6 konusunda ağ tecrübeleri arttıkça anycast adresleri de TCP/IP yapısı içindeki yerini alacaktır.

3.1.6 Multicast adresleri

Multicast adresleri ile veri taşıma olanağı 1988 yılında IPv4 adresleri ile sağlanmıştır. Bu adresler genelde bir sunucu birden çok uç noktaya veri transfer edeceği zaman kullanılmaktadır. IPv4'te bulunan broadcast adresi IPv6'da kaldırılmış ve bu görev de multicast adreslerine yüklenmiştir.

Multicast adreslerinin ilk 8 biti 1'lerden oluşmaktadır, bu söz dizimi adresin çeşidini belirtmektedir. Şekil 3.4'te görülebileceği gibi ilk 8 bitten sonra flgs, scop ve grup ID bölümleri vardır.



Şekil 3.4: Multicast adres yapısı

Flgs bölümü bayrak (flag) bitlerinden oluşmakta ve 4 bitlik bir yapıdadır. Bu 4 bitlik bayrak yapısında en anlamlı bite her zaman 0 değeri atanmaktadır. Daha sonraki bayrak isimleri de R, P ve T olarak adlandırılmaktadır. R ve P daha sonraki kullanımlar için ayrılmış ve şu anda 0 değerini almaktadırlar. R hakkında detaylı bilgiye RFC 3306'dan, P hakkındaki bilgiye de RFC 3956'dan ulaşılabilmektedir. T

bayrağının değeri 1 ise bu adres sürekli olarak IANA tarafından atanmış bir multicast adresi anlamına gelmektedir. Eğer değer T değeri 0 ise bu adres geçici veya dinamik atanmış bir multicast adresini ifade etmektedir. Scop değeri de multicast adresinin kullanım kapsamını belirten 4 bitlik bir alandır. Alabileceği değerler ve anlamları aşağıdaki gibidir:

- 0 Reserve edilmiş
- 1 Arayüze özel
- 2 Link-local
- 3 Reserve edilmiş
- 4 Yöneticiye özel
- 5 Site-local
- 6 (atanmamış)
- 7 (atanmamış)
- 8 Organizasyona özel
- 9 (atanmamış)
- A (atanmamış)
- B (atanmamış)
- C (atanmamış)
- D (atanmamış)
- E Global
- F Reserve edilmiş

Multicast adresleri hiçbir zaman herhangi bir paketin kaynak adresi olarak veya bir yönlendirme başlığında kullanılmamalıdır. Multicast adresleri yukarıda anlatılan şekilde oluşturulabildiği gibi bir de önceden tanımlanmış çeşitleri bulunmaktadır. Tüm düğümleri kapsayan adresler; FF01:0:0:0:0:0:1 ve FF01:0:0:0:0:0:2'den oluşmaktadır. Aynı şekilde tüm yönlendiricileri kapsayan adresler de FF01:0:0:0:0:0:2, FF02:0:0:0:0:0:2 ve FF05:0:0:0:0:0:2'den oluşmaktadır.

3.1.7 IPv6 düğümünün sahip olması gereken adresler

IPv6 adresleme yapısını iyi anlayabilmek için, bir IPv6 düğümünde hangi çeşit adreslerin bulunması gerektiğini bilmek gerekmektedir. IPv4 adresleme yapısında düğüme tek bir IPv4 adresi atanmakta ve ağ ile ilgili tüm işler bu adres ile sağlanmaktaydı. IPv6'da ise düğüm kendisini tanımlayabilmesi için aşağıdaki adreslere ihtiyaç duymaktadır:

- Her ağ arayüzü için bir adet link-local adresi

- Herhangi anycast veya unicast, adres veya adresleri (bir arayüze birden fazla unicast adres atanabilmektedir.)
- Her bir düğüm için bir adet loopback adresi
- Bir adet tüm düğümleri belirten multicast adresi (IPv4'teki karşılığı broadcast adresidir.)
- Kendisinin de üye olduğu multicast gruplarının adresleri

Yönlendiriciler bir düğümde bulunması gereken tüm adresleri algılayabilmekte ve ayrıca ek olarak aşağıdaki adreslere ihtiyaç duymaktadırlar:

- Yönlendirici olarak davranacak tüm arayüzlerine atanacak alt ağ yönlendirici unicast adresleri
- Yönlendiricinin yapılandırıldığı tüm diğer anycast adresleri
- Tüm yönlendiricileri belirten multicast adresi
- Tüm düğümleri belirten multicast adresi

3.1.8 EUI arayüz tanımlayıcısı

IPv6 adres çeşitleri incelendiğinde site-local, link-local ve global adres gibi unicast adreslerin birçoğunda 64 bitlik bir arayüz tanımlayıcısı bölümü, bir de ön ek bölümü vardır. Bu 64 bitlik arayüz tanımlayıcısı ağ içinde adresin atandığı arayüze özel bir bilgidir ve adres atanan arayüzleri birbirinden ayırmaya yarayan benzersiz(unique) bir değerdir. Bu bölüm değişik şekillerde oluşturulabilir. Sunuculu (stateful) ve sunucusuz (stateless) adres atamalarındaki gibi rastgele veya belli bir aralıkta atanabildiği gibi MAC adresine göre oluşturulan arayüz tanımlayıcıları da bulunmaktadır.

IEEE, 64 bit uzunluğunda EUI-64 ismi verilen yeni bir fiziksel adres(MAC) çeşidi geliştirmiştir. Şu anda kullanılan MAC adresleri 48 bit uzunluğundadır ve 24 biti IEEE tarafından atanan kuruluşa özel ve OUI (Organization Unique Identifier) diye adlandırılan bir değer, diğer 24 bit kuruluş tarafından atanan kendi ürünlerini ayırmaya yarayan değerdir. IEEE'nin yeni geliştirilen MAC adresine göre kuruluş 24 bitlik adresi IEEE'den aldıktan sonra kendisine özel değeri 40 bit olarak verebilmekte ve böylelikle EUI-64 standardını destekleyebilmektedir.

Ayrıca EUI-64 adresi eski 48 bitlik adreslerin belli kurallara göre genişletilmesi ile de oluşturulabilmektedir. Bu konuda çeşitli kurallar bulunmaktadır, Düğümler için

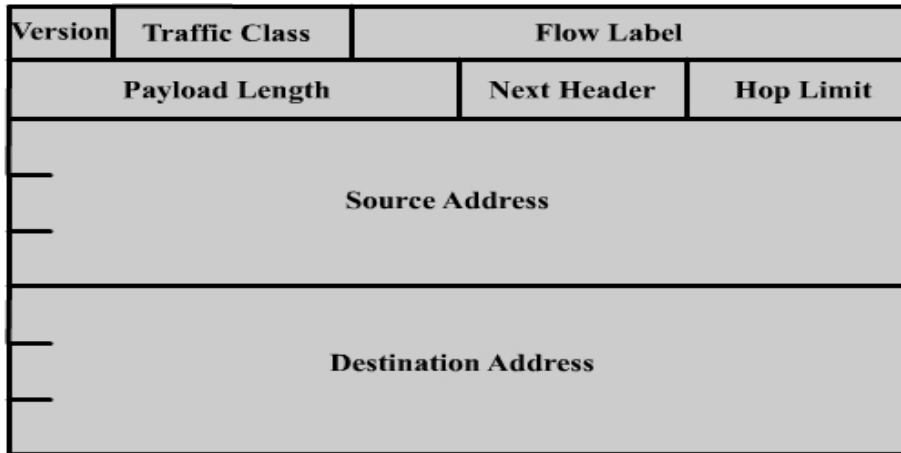
kullanılan EUI-64 adresleri için MAC adresi içindeki 7. bit adresin evrensel olarak geçerli mi yoksa yerel olarak mı oluşturulduğuna göre 0 veya 1 değerini alır. 48 bitlik adres içindeki 24 bitlik iki bölüm birbirinden ayrılıp araya onaltılık sayı düzeninde FFFE değeri eklenmektedir. Bu şekilde yeni adresi 64 bitlik EUI-64 adresi halinde gelmektedir[21]. Örnek olarak MAC adresi 0012:F0E0:B6F5 olan bir cihazın EUI-64 adresi 0212:F0EF:FFE0:B6F5 olmaktadır. Site-local adresleri otomatik olarak bu değere göre oluşturulmaktadır.

3.2 IPv6 Başlığı

Bölüm 3.1’de bahsedildiği gibi IPv6 mimarisinde adres uzunluğu 128 bite çıkarılmış yani IPv4’e göre uzunluk bakımından dört kat büyümüştür. Adresteki bu büyüme aynı zamanda IPv6 paketinin başlığına da yansımaktadır çünkü başlık içinde hem hedef hem kaynak adresleri bulunmaktadır. Meydana gelen bu büyümeden dolayı ve IPv4 başlığında fark edilen bazı eksiklikleri gidermek amacıyla IPv6 için yeni bir paket başlığı tasarımına gidilmiştir.

3.2.1 Başlık alanları

Bu yeni tasarlanan başlıkta IPv4’te bulunan ve çok verimli kullanılmayan bazı alanlar tamamen kaldırılmış bazı alanlar seçime bağlı yapılmıştır. Ayrıca IPv6 başlığı için daha verimli iletimi sağlayacak yeni alanlar da eklenmiştir. IPv4 başlık uzunluğu 20 byte standart olmak üzere 60 byte’a kadar çıkıyordu. IPv6 da ise 40 byte’lık sabit bir başlık var, istenilirse bu başlık eklenti başlıkları ile genişletilebiliyor. IPv4 başlık yapısı şekil 2.3’te belirtilmişti, şekil 3.5’te de IPv6 paket başlığı görünmektedir[22].



Şekil 3.5: IPv6 başlık yapısı

IPv6 paket başlığında sırası ile aşağıdaki alanlar bulunmaktadır:

Versiyon (version): Bu alan IPv4'teki versiyon alanı ile aynı uzunlukta yani 4 bit uzunluğundadır ve İnternet protokolünün hangi versiyon olduğunu belirtmektedir. IPv6 için 6 değerini almaktadır.

Trafik sınıfı (traffic class): 8 bitlik bir alandır. IPv4'teki hizmet tipi alanı yerine getirilmiştir. IPv6 paketleri arasındaki değişik sınıf ve öncelikleri belirtme görevini üstlenmektedir.

Akış etiketi (flow label): 20 bit uzunluğundaki akış etiketi bölümü değişik akış yolları çizen paket dizilerini etiketlemek için kullanılmaktadır. Bu etiketleme genellikle servis çeşitlerine göre yapılmaktadır. Akış etiketini desteklemeyen bir düğüm eğer paketi yaratıyorsa bu alana sıfır değeri yerleştirir, paketi yönlendiriyorsa bu alanı hiç değiştirmeden paketi yönlendirir, eğer paketi alan tarafısa bu alandaki değeri hiç dikkate almaz.

Yük uzunluğu (payload length): IPv6 başlığını takip eden tüm paketin uzunluğunu 16 bitlik bir alanda ifade etmektedir. Eğer pakette bir veya birden fazla eklenti başlığı varsa onlarda bu uzunluğa dahil edilir. IPv4 başlığındaki karşılığı toplam uzunluk alanıdır.

Sonraki başlık (next header): 8 bitlik bu alanda IPv6 başlığından hemen sonra gelen başlık çeşidi belirtilmektedir. Bu herhangi bir eklenti başlığı olabilir veya TCP, UDP gibi daha üst seviyelerden bir protokol olabilir. IPv4'te protokol alanı adıyla geçmektedir.

Atlama limiti (hop limit): 8 bitlik bir değerle ifade edilmektedir. Paket her bir düğümden geçtikçe atlama limiti sayısı bir eksiltilmektedir. Bu sayı sıfır olduğu zaman paket atılmaktadır. IPv4'teki karşılığı TTL alanıdır.

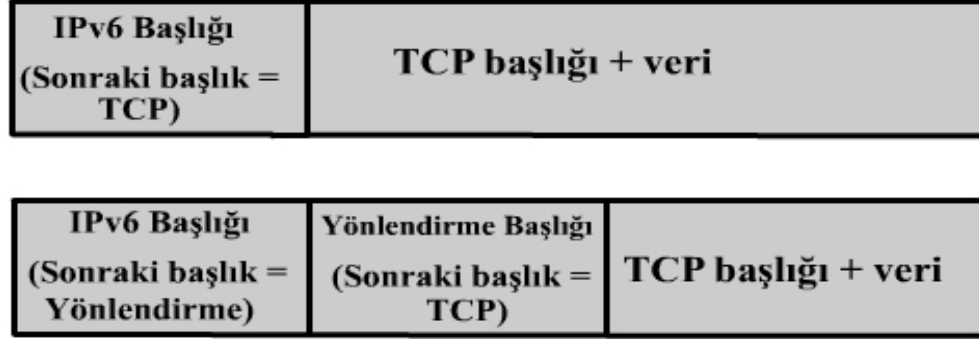
Kaynak adresi (source address): 128 bitlik paketin kaynak adresini belirten alandır. Bölüm 3.1'de IPv6 adresleme yapısı detaylı olarak anlatılmıştır.

Hedef adresi (destination address): 128 bitlik paketin hedef adresini belirten alandır. Eğer yönlendirici başlığı varsa, hedef adres bu sefer en son alıcının adresi değildir.

3.2.2 Eklenti başlıkları

IPv4'te seçime bağlı alanlar için yerler ayrılmıştır. Yani o alan kullanılmasa da o yer vardır ve bu alanlar her yönlendirici tarafından tek tek incelenmektedir. Kullanılmayan yerler hem paket boyutunu arttırmakta, hem de yönlendiricinin işini zorlaştırmaktadır.

IPv6’da İnternet katmanı bilgisi seçeneğe bağlı olarak ayrı başlıklar halinde pakete eklenebilmektedir. Ve bu eklenen bölüm IPv6 başlığı ile daha üst seviye protokol başlığının arasında olmaktadır. IPv6 paketi içinde bir, iki veya daha fazla eklenti başlığı olabildiği gibi hiç eklenti başlığı olmayabilir de. Eğer eklenti başlığı varsa bu sonraki başlık alanında bir önceki başlıkta ifade edilmektedir.



Şekil 3.6: Eklenti başlıkları

Şekilde birinci durumda IPv6 başlığından hemen sonra TCP başlığının gelmektedir yani eklenti başlığı kullanılmamaktadır. İkinci durumda ise IPv6 başlığı ile TCP başlığı arasında bir yönlendirme başlığı kullanılmıştır. Eklenti başlıkları incelenirken başlık içerikleri bir sonraki eklenti başlığının incelenip incelenmeyeceğini belirtir. Bu sebepten dolayı eklenti başlıkları her zaman bir sıraya göre eklenmelidir. Kullanılabilecek altı çeşit eklenti başlığı kullanım sırasına göre aşağıda belirtilmektedir:

- Atlama noktası seçenekleri (RFC2460)
- Hedef seçenekleri (RFC 2460)
- Yönlendirme (RFC 2460)
- Parçalara ayırma (RFC 2460)
- Kimlik doğrulaması (RFC 2406)
- Güvenlik başlığı (RFC 2406)

Hedef seçenekleri eklenti başlığı ara düğümleri belirtmeyip sadece son noktayı belirtiyorsa, bu eklenti başlığı ikinci sıraya değil en son sıraya yerleştirilmelidir.

3.2.3 IPv6 paket boyutu

İnternet içindeki her ortamın en büyük iletim biriminin (MTU) en az 576 byte olması gerekmektedir. Bu paket büyüklüğünü taşıyamayan veya iletemeyen düğümler

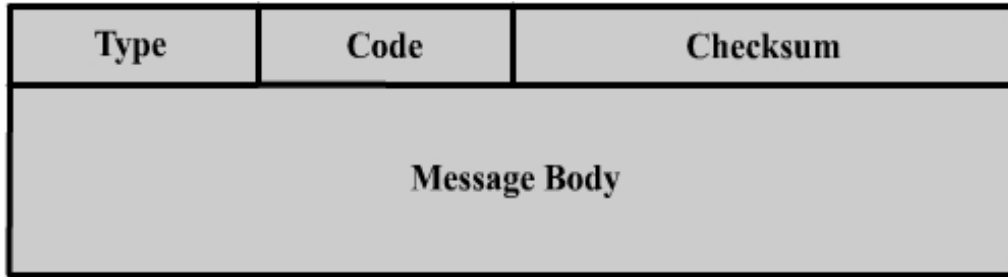
IPv6'nın altında OSI referans modeline göre ikinci katman olan veri bağlantı katmanında parçalara ayırma işlemi yapmak zorundadırlar. RFC 1883 belgesinde bu konu açıkça belirtilmektedir.

3.3 ICMPv6

İnternet protokolü (IP), basit yapısı gereği sadece verinin iletimi işini yerine getirmektedir. Veri iletimi sırasında meydana gelen hatalarla ilgili herhangi bir bilgilendirme yapmamaktadır. Bu görevi İnternet kontrol mesaj protokolü (ICMP) yerine getirmektedir. ICMPv6, IPv4'te kullanılan ICMP'nin IPv6'ya uyarlanmış halidir. IPv6'nın ayrılmaz bir parçasıdır ve her IPv6 düğümü tarafından tamamen tanınması gerekmektedir. ICMPv6 birçok amaca yönelik kullanılan bir protokoldür. Paketlerin işlenmesi sırasında ortaya çıkan hataları bildirmek, sistem kontrolleri gerçekleştirmek, komşu keşfi yapmak ve multicast üyeliklerini bildirmek gibi değişik hizmetler sağlamaktadır. Bu sebeple de hata ve bilgi mesajları diye iki sınıfa ayrılmıştır.

3.3.1 ICMPv6 başlık yapısı

ICMPv6 başlığı, IPv6 paket yapısındaki sonraki başlık bölümünde bir önceki başlık tarafından 58 değeri ile belirtilir. Şekil 3.7'de ICMPv6 mesajının yapısı belirtilmektedir.



Şekil 3.7: ICMPv6 mesajının yapısı

ICMPv6 mesajı tür (type), kod (code), toplam kontrolü (checksum) ve mesaj gövdesinden (message body) oluşmaktadır[23].

Tür: ICMPv6 mesajının türünü belirtmektedir. 8 bitlik alanda ifade edilmektedir. ICMPv6 hata mesajlarında en anlamlı bit "0", ICMPv6 bilgi mesajlarında en anlamlı bit "1" değerini almaktadır.

Kod: Aynı tür mesajlar için ayırma faktörü olarak kullanılmaktadır. 8 bit uzunluğunda bir alandır. Aynı türde olan mesajlardan ilk mesajın kod alanındaki değer sıfırdır.

Toplam kontrolü: ICMPv6 mesajlarının toplam kontrolünü sağlamaktadır. 16 bitlik bir alanda yer almaktadır. IPv6 ve ICMPv6 mesajlarındaki hataları ortaya çıkarmaktadır.

Mesaj gövdesi: ICMPv6 mesajına yönelik verileri taşımaktadır.

3.3.2 ICMPv6 hata mesajları

ICMPv6 hata mesajları ICMP(v4) hata mesajlarına çok benzemektedir. Dört değişik hata mesajından oluşmaktadır. Bunlar; hedef ulaşılamaz (destination unreachable), paket çok büyük (packet too big), zaman aşımı (time exceeded) ve parametre problemleridir (parameter problems).

3.3.2.1 Hedef ulaşılamaz hata mesajı

Eğer bir paket herhangi bir sebepten dolayı hedefe ulaşılamıyorsa paketi gönderen tarafa bu bilgi hata mesajları ile bildirilmektedir. ICMPv6 hata mesajı oluşturulurken hedef adres, ulaştırılamayan paketin kaynak adresi olmaktadır. Tür değeri için 1 verilmekte ve kod değeri ile beş değişik durum ifade edilmektedir.

- Kod 0 hedefe yönlendirme yok mesajını belirtmektedir. Bu mesaj bir yönlendirici yönlendirme tablosunda ilgili hedef adresi ile ilgili uyuşan bir yol bulamadığı ve dolayısıyla paketi yönlendiremediği zamanlarda kaynak tarafa iletilmektedir.
- Kod 1 hedef adres ile iletişim yönetsel olarak yasaklanmıştır bilgisini kaynak cihaza iletmektedir. Paket bir şekilde ateş duvarından (firewall) hedef adrese ulaşamamış veya bazı kurallar tanımlanmış olan yönlendiriciden geçememiş olabilmektedir. Bu sınırlamalar genellikle yönetsel olarak güvenliği sağlamaya yönelik yapılan ayarlardan oluşmaktadır.
- Kod 2 değerine hiçbir bilgi atanmamıştır. Kod kısmına bu değer atanmamakta çünkü alıcı için hiçbir şey ifade etmemektedir.
- Kod 3 adres ulaşılamaz hata mesajını bildirmektedir. Meydana gelen bir arayüz hatasından veya ikinci katman adreslemelerinden kaynaklanan bir hatadan dolayı paketin hedefe ulaşamadığı hatasını ifade eder.

- Kod 4 port ulaşılamaz hatasıdır. Paket hedefe ulaşmıştır ancak hedefte dördüncü katman protokollerinden birine gönderilen paket için ilgili port dinlemede değildir. Örnek olarak bir Web isteği olarak gönderilen paket, ulaştığı hedef adreste eğer TCP 80 portu kullanımda değilse, ICMPv6 kod 4 hata mesajı ile geri dönmektedir.

3.3.2.2 Paket çok büyük mesajı

Paket çok büyük hata mesajı, ağda iletilecek paketin MTU'dan büyük olması durumunda yaratılan bir hata mesajıdır. ICMPv6 paketinin hedef adresi boyutu MTU'dan büyük olduğu için düşürülen paketin kaynak adresinden oluşmaktadır. Tür değeri 2 olmakta ve kod değeri her zaman 0 değerini almaktadır. Kod değerine 0 değeri gönderici tarafından atanır, alıcı tarafından bu değer dikkate alınmaz. Bu hata mesajında bir de MTU alanı vardır. Bu alan da paketin düşürülmesine sebep olan MTU'yu göndericiye belirtmektedir bu sayede gönderici paketlerini o MTU değerinden daha büyük oluşturmamaktadır. Paket çok büyük mesajı alan bir gönderici bu mesajı daha üst katmanlara işlem görmek üzere göndermesi gerekmektedir.

3.3.2.3 Zaman aşımı

Zaman aşımı hata mesajı iki durumda oluşmaktadır. IPv6 paketinin atlama limiti (hop limit) değeri sıfıra düşmüş olabilir veya IPv6 paketinin yeniden oluşturulması zaman aşımına uğramıştır. ICMPv6 hata mesajı oluşturulurken tür değeri 3, kod değeri de 0 veya 1 olmaktadır.

Kod değerinin 0 olması iletim sırasında atlama limitinin aşıldığını göstermektedir. Bu atlama limiti değerini küçük seçilmesinden kaynaklanabildiği gibi paketin sonsuz döngüye girmesinden dolayı da kaynaklanabilmektedir. Kod değerinin 1 olması paket için parça yeniden oluşturma zaman aşımı nedeniyle yapılamadığını belirtmektedir.

3.3.2.4 Parametre problemi

Parametre problemi hata mesajı IPv6 paketi başlığında veya eklenti başlığında bir hata bulunduğunda yaratılan bir mesajdır ve bu iki sebepten birinden dolayı düşürüldüğünü göndericiye bildirmek için iletilmektedir.

Tür değeri 4 olmaktadır. Kod bölümü ise üç değişik değeri alabilmektedir. Hatalı başlık alanı ile karşılaşıldığı durumda 0, tanınmayan bir sonraki başlık çeşidi ile karşılaşırsa 1, tanınmayan bir IPv6 seçeneği ile karşılaşırsa 2 değerini almaktadır. Bir de işaretçi (pointer) bölümü bulunmaktadır. Bu değeri de hatanın paketin neresinde bulunduğunu bildirmektedir.

3.3.3 ICMPv6 bilgi mesajları

ICMPv6 bilgi mesajları genellikle sorun giderme işlemlerinde kullanılmaktadır. Yankı isteği (echo request) ve yankı cevabı (echo reply) mesajlarından oluşmaktadır. Yankı cevabı mesajı yankı isteğine verilen karşılıktır.

3.3.3.1 Yankı isteği mesajı

Yankı isteği mesajının hedef adresi herhangi kullanımda olan bir IPv6 adresi olabilmektedir. Tür değeri 128, kod değeri ise 0 olmaktadır. Tanımlayıcı alanı isimli yeni bir alan içermektedir. Bu alanda yankı isteklerine karşılık gönderilen yankı cevaplarının eşleştirilmesi yapılmaktadır ve 0 değeri alabilmektedir. Hata mesajlarında bulunmayıp bilgi mesajlarına eklenen yeni alanlardan bir tanesi de sıra numarasıdır. Bu alan da yankı istek ve cevaplarının eşleştirilmesine yardımcı olmaktadır. Son olarak veri alanı isteğe göre veri ile doldurulan bir alandır.

IPv6 destekleyen her düğüm yankı isteği alabilecek ve aldığı yankı isteğine karşı yankı cevabı gönderebilecek yapıda olması gerekmektedir. Ayrıca düğümlerden en az bir tanesinin kontrol amaçlı kullanılmak üzere yankı isteği gönderecek uygulama katmanı arayüzü bulundurması gerekmektedir.

3.3.3.2 Yankı cevap mesajı

Yankı cevap mesajının hedef adresi, yankı isteği mesajının kaynak adresinden kopyalanmaktadır. Tür değeri 129, kod değeri ise 0 olmaktadır. Tanımlayıcı, sıra numarası ve veri alanları yankı isteği mesajının aynısı olmaktadır. ICMPv6 yankı isteği mesajı ile alınan veri tamamen ve hiçbir değişikliğe uğramadan yankı cevabı ile geri gönderilmektedir.

3.3.4 Multicast dinleyici keşfi

Multicast dinleyici keşfi (multicast listener discovery - MLD) ICMPv6 mesaj çeşitlerinden bir tanesidir. Yönlendiricilerin multicast adresleri dinleyen grupları

keşfetmesini sağlamaktadır. MLD, sonraki başlık alanında 58 değeri ile ifade edilmektedir. Tüm MLD mesajları kaynak adresi olarak link-local IPv6 adresleri kullanmakta ve atlama limiti olarak 1 değerini atamaktadırlar.

Üç çeşit MLD bulunmaktadır, bunlar: multicast dinleyici sorgusu (listener query), multicast dinleyici raporu (listener report) ve multicast dinleyici bitti (listener done) mesajlarıdır. Tür alanına dinleyici sorgusu için 130, dinleyici raporu için 131 ve dinleyici bitti mesajı için 132 yazılmaktadır. Kod alanına gönderici tarafından 0 atanmakta ve alıcı tarafından bu değer dikkate alınmamaktadır. MLD konusu RFC 2710 belgesinde çok detaylı olarak incelenmektedir.

3.4 Komşu Keşfi

IPv6 komşu keşfi (ND) protokolü, IPv6 ile birlikte gelen büyük yeniliklerden biridir. IPv4'te bulunan ARP, ICMP yönlendirici keşfi ve ICMP mesaj yeniden yönlendirme protokollerinin yerine geçmekte ve aynı zamanda IPv4'te bulunmayan yeni özellikler eklemektedir. ND aşağıda belirtilen görevleri yerine getirmektedir:

- Ağda bulunan çakışan adresleri bulma
- Komşu yönlendiricileri bulma
- Komşuların erişilip erişilmediği kontrolü
- Adres yapılandırması için ön ek ve adres bilgilerini öğrenme
- İkinci katman adresleri ile IPv6 adresleri arasında ilişki kurarak adres oto yapılandırmasını sağlamak
- Yeniden yönlendirme yapmak

3.4.1 Komşu keşfi mesajları

Komşu keşfi mesajları ICMPv6 mesajına komşu keşfi başlığı eklenerek oluşturulmaktadır. İstendiği zaman komşu keşfi mesaj seçenekleri de eklenebilmektedir. Beş adet komşu keşfi mesaj çeşidi tanımlamaktadır. Bunlar yönlendirici ricası (router solicitation), yönlendirici ilanı (router advertisement), komşu ricası (neighbor solicitation), komşu ilanı ve yeniden yönlendirme mesajıdır (redirect message).

3.4.1.1 Yönlendirici ricası

Bir cihazın ağ arayüzü aktif hale geldiği zaman, cihaz yönlendirici ricası mesajı üretmektedir. Bu mesaj yönlendiricilerin normalde planlanmış zaman haricinde bu mesajı alır almaz yönlendirici ilanı üretmelerini sağlamaktadır.

Kaynak adresi olarak mevcut arayüze atanmış bir IP adresi kullanılmakta eğer arayüze herhangi bir adres atanmamışsa tanımlanmamış unicast adresi (::) belirtilmektedir. Hedef adresi ise tüm yönlendiricileri belirten multicast adresi (FF02::2) olarak tanımlanmaktadır. Atlama limiti değeri 255 olarak verilmektedir. Gönderici ile alıcı arasında eğer güvenliğe yönelik kimlik denetimi mevcutsa pakete bir de kimlik denetimi başlığı eklenmektedir. ICMPv6 başlığı alanları doldurulurken tür değeri 133, kod değeri 0 verilmektedir.

3.4.1.2 Yönlendirici ilanı

Yönlendiriciler ağ üzerindeki varlıklarını bildirmek için periyodik olarak veya bir yönlendirici ricasına cevaben yönlendirici ilanı yayınlamaktadırlar. Multicaste uygun ağlarda yönlendiriciler düzenli olarak multicast şeklinde yönlendirici ilanı yollarlar. Ağdaki tüm yönlendiricilerden bu mesajı alan uç noktalar bir yönlendirici listesi oluşturmaktadır.

Yönlendirici ilanları, yönlendiricilerin uç noktalara adres yapılandırmasını nasıl gerçekleştireceklerini bildirmelerini sağlamaktadır. Örneğin uç noktaların DHCPv6 kullanıp kullanmayacakları bu mesajlarla iletilebilir. Aynı zamanda yönlendirici ilanları atlama limiti gibi İnternetle ilgili parametreleri ve MTU gibi ağ üzerinde iletim değeri bilgilerini de içermektedir. Bu özellik bazı önemli parametrelerin yönetiminin yönlendirici tarafından yapılması ve uç noktaların bu bilgiyi tek bir yönetim merkezinden almalarını sağlamaktadır.

Yönlendirici ilanı mesajlarının kaynak adresi paketin gönderileceği ağ arayüzünün link-local adresi olmak zorundadır. Hedef adresi ise tüm düğümleri kapsayan multicast adresi veya yönlendirici ricası gönderen yönlendiricinin adresi olmaktadır.

Yönlendirici ilanında bulunan ICMP paketi alanları aşağıdaki gibidir:

- Tür değeri 134
- Kod değeri 0
- Toplam kontrolü

- Mevcut atlama limiti – yönlendirici ilanı alan uç noktaların gönderdiği paketlere vereceği atlama limiti değerini belirtmektedir. 8 bitlik bir değerdir.
- Rezerv alanı – gönderici tarafından 0 değeri verilmeli ve alıcı tarafından dikkate alınmamalıdır.
- Yönlendirici ömrü – 16 bitlik bir değerle ifade edilmektedir. Zaman birimi olarak saniye şeklinde yönlendiricinin ömrünü belirtmektedir ve verilebilecek en büyük zaman uzunluğu 18.2 saate denk gelmektedir. Eğer bu alanın değeri 0 ise, bu mesajı alan uç nokta bu yönlendiriciyi yönlendirici listesine eklememelidir.
- Erişilebilirlik süresi – 32 bitlik bir tam sayıda tutulmaktadır. Bir komşudan erişilebilirlik onayı aldıktan sonra mili saniye zaman dilimi içinde komşunun ne kadar süre tanınacağını belirtmektedir.
- Yeniden iletim zamanı – 32 bitlik tam sayı ile ifade edilen, mili saniye olarak ne kadar süre sonra komşu ricası mesajının yeniden iletileceğini belirtmektedir.
- MTU – değişken MTU değerlerine sahip olunan durumlarda bu değer belirtilmelidir. Seçeneğe bağlıdır.
- Veri bağlantı katmanı adresi - yönlendirici ilanı gönderen arayüzün OSI ikinci katman adresi seçeneğe bağlı olarak eklenebilmektedir.
- Ön ek bilgisi - Gerekli görüldüğünde kullanılmak üzere tasarlanmıştır. Ön eki tanımlamakta ve adresin otomatik yapılandırılmasında kullanılmaktadır.

3.4.1.3 Komşu ricası

Komşu ricası mesajı bir komşunun ikinci katman adresini öğrenmek veya eldeki listedeki ikinci katman adresi ile komşunun halen erişilip erişilemediğini belirlemek için kullanılmaktadır. Düğümler adres çözümleme işlemini multicast olarak komşu ricası göndererek yaparlar. Bu mesajı alan hedef düğümler de istenen bilgiyi unicast olarak mesajı gönderen düğüme iletirler.

Aynı zamanda ağ üzerinde yinelenen bir adres olup olmadığını belirleyebilmektedir. Eğer birden fazla düğüme aynı unicast adresi atanmışsa bu ağ üzerinde aynı adresin tekrarlanması anlamına gelmektedir ve sorun yaratmaktadır. Bu sorun komşu ricası mesajı ile fark edilmektedir ve sorun için çözüm aranmaktadır.

IP alanı kaynak adresi düğümün mesajı gönderen arayüzünün adresi, hedef adresi ricanın gönderileceği düğümlerin multicast adresi veya tek bir hedefin unicast adresi, atlama limiti 255 olarak belirtilir. Eğer gönderici ile alıcı arasından herhangi bir güvenlik ilişkilendirilmesi varsa bu durumda ilgili pakete kimlik denetimi başlığının da eklenmesi gerekmektedir. ICMP alanları ise, tür 135, kod 0, hedef adres olarak paketin gönderileceği adres belirtilecek şekilde doldurulmaktadır.

3.4.1.4 Komşu ilanı

Komşu rica mesajına verilen cevaptır. Bir düğüm aynı zamanda bir rica mesajı almadan da ikinci katman adresi değişikliğine dair komşu ilanı mesajı gönderebilmektedir. Komşu ilanlarında paketin kaynak adresi ilanı gönderen düğümün mesajı gönderdiği ağ arayüzü adresi olmaktadır. Hedef adresi de ricaya karşılık gönderilen mesajlarda ricanın sahibinin adresi, rica sahibinin adresi yoksa tüm düğümler multicast adresi olarak belirlenmektedir. Atlama limiti olarak 255 değeri atanmaktadır.

ICMP alanları doldurulurken türe 136, koda 0 değerleri verilmektedir. Komşu ilanı mesajlarında R, S ve O ile gösterilen üç yeni alan bulunmaktadır:

- Yönlendirici bayrağı (router flag) – R harfi ifade edilmekte ve eğer bir değer atanmışsa mesaj göndericinin bir yönlendirici olduğunu ifade etmektedir.
- Rica bayrağı (solicited flag) – S harfi ifade edilmekte ve eğer bir değer atanmışsa ilanın bir ricaya karşılık gönderildiğini ifade etmektedir.
- Yenileme bayrağı (override flag) - O harfi ifade edilmekte ve eğer bu değer atanmışsa yeni gelen bilginin eski bilgilerin üzerine yazılacağını ve eski bilgilerin yenileneceğini ifade etmektedir. Eğer bu alana atama yapılmamışsa mevcut ikinci katman adresi bilgisi yeni gelen bilgi ile değiştirilmemekte, ancak eğer alıcıda mesaj gönderen düğümle ilgili hiçbir bilgi yoksa o durumda yeni gelen bilgi listeye eklenmektedir.

3.4.1.5 Yeniden yönlendirme mesajı

Yönlendiriciler tarafından uç noktalara daha iyi bir hedef yol belirlemek için kullanılmaktadır. Yeniden yönlendirme mesajları unicast olarak sadece ilgili uç noktaya gönderilmektedir. ICMP alanında tür değeri 137 olmaktadır. Atlama noktası

255, kaynak adresi yönlendirici unicast adresi, hedef adresi uç noktanın unicast adresi olmaktadır.

3.4.2 Komşu keşfi işlemi

Komşu keşfi işlemini yerine getirebilmek için her düğümün sahip olmak zorunda olduğu bazı veri yapıları vardır. Bunlar:

- Komşu önbelleği (neighbor cache)
- Hedef önbelleği (destination cache)
- Ön ek listesi (prefix list)
- Varsayılan yönlendirici listesi (default router list)

Komşu önbelleği, komşuların IPv6 adreslerine karşı gelen ikinci katman adreslerini tutmaktadır. Aynı zamanda komşunun erişilebilirlik bilgisini de tutmaktadır. IPv4'te bu görevi ARP belleği üstlenmektedir.

Hedef önbelleği, en son paket gönderilen hedefler için bir sonraki atlama noktası üzerindeki bilgileri tutmaktadır. Hedef önbelleğindeki her bir giriş hedef düğümün IP adresini, bir sonraki atlama noktası IP adresini ve hedef için yol MTU değerinin içermektedir.

Ön ek listesi, aynı alt ağda bulunan ve yönlendirmeye ihtiyaç olmadan doğrudan haberleşilecek düğümlerin listesidir. Yönlendirici tarafından, yönlendirici ilanı mesajları ile iletilen bilgiler doğrultusunda bu liste oluşturulmaktadır.

Varsayılan yönlendirici listesi, yönlendirici ilanı gönderen yönlendiricilerin tutulduğu listedir. Bu listedeki yönlendiriciler kaynak düğüm tarafından varsayılan yönlendirici olarak seçilmeye aday yönlendiricilerdir[26].

3.4.2.1 Adres çözümleme

Adres çözümleme (address resolution) işlemi komşu ricası ve komşu ilanı mesajlarının ağ içinde değiş tokuş edilmesi ile yapılmaktadır. Buradaki amaç hedefe giden yoldaki bir sonraki atlama noktasının ikinci katman adresini bulmaktır. Kaynak düğüm multicast olarak bir komşu ricası mesajı göndermektedir. Kendi ikinci katman adresini de bu mesaj içinde bildirmektedir.

Hedef düğüm komşu ricası mesajını aldığı zaman kendi komşu önbelleğini bu mesaja göre güncellemektedir. Daha sonra da mesajı aldığı kaynak düğüme, kendi ikinci katman adresini içeren komşu ilanı mesajını unicast olarak göndermektedir.

Adres çözümleme işlemini başlatan düğüm, hedef düğümden komşu ilanı mesajını aldıktan sonra kendi komşu önbelleğini gelen komşu ilanı mesajına göre güncellemektedir. Bundan sonra bu iki düğüm arasında unicast veri trafiği sağlanabilmektedir.

3.4.2.2 Yönlendirici Keşfi

Yönlendirici keşfi, aynı alt ağda bulunan düğümlerin ağ üzerindeki yönlendiricilerin hangilerinin aktif olduklarını bulmak için kullandıkları yöntemdir. IPv4'teki ICMP yönlendirici keşfi yapısına çok benzer bir şekilde çalışmaktadır. IPv4'te yönlendirici keşfi ile düğümler varsayılan yönlendiriciyi kullanıyorlar ve bu yönlendirici erişilemez olduğunda yeni bir yönlendiriciyi varsayılan olarak atamaktadırlar.

IPv4'te yönlendiricinin erişilebilir sayıldığı belli bir süre vardır, buna yönlendirici ömrü denmektedir. Bir yönlendiricinin erişilemez olduğu ancak bu süre bittikten sonra anlaşılabilir. IPv6'da ise yönlendirici ömrüne ek olarak komşu erişilemezlik keşfi (neighbor unreachability detection) mesajı kullanılmaktadır. Bu sayede yönlendirici ömrü dolmadan erişilemez olan yönlendiriciler bu mesaj sayesinde hemen keşfedilmekte ve varsayılan yönlendirici listesinden yeni bir yönlendirici seçilmektedir[27].

3.4.2.3 Komşu Erişilemezlik Keşfi

Bir düğümün erişilebilir varsayılması için o düğümden erişilir olduğuna dair onay mesajı alınması gerekmektedir. Bir düğümün erişilebilir olup olmadığını öğrenmenin bir yolu o düğüme komşu ricası mesajı yollamaktır. Bu mesaja cevaben eğer komşu ilanı mesajı alınıyorsa bu durumda ilgili düğüme erişilebilmektedir. Burada dikkat edilmesi gereken yer komşu ricası alan düğüm mesajı gönderen düğümü erişilebilir varsaymamaktadır. Bir düğüm komşu ilanı gönderdiği zaman erişilebilirliğini ispatlamaktadır.

Erişilebilirlik keşfinin diğer bir yöntemi de üst seviye protokollerin kurduğu oturumları kontrol etmektir. Eğer TCP gibi dördüncü katman protokolü veri alış veriş için bir oturum kurduysa bağlantı kurulan hedef düğüm erişilebilirdir

denmektedir. Yine dördüncü katman protokolü olan UDP bu amaçla kullanılamamaktadır. Çünkü UDP kullanan uygulamalar paket göndermek için kaynak ile hedef düğüm arasında bir oturum kurulmasına bakmazlar ve paket gönderimine dair bir kontrol mekanizmaları yoktur.

Komşu önbelleğine eklenen bir giriş değişik durumlarda bulunabilmektedir.

- Tamamlanmamış: Adres çözümleme henüz tamamlanmamıştır.
- Erişilebilir: Komşu şu anda erişilebilir bir durumdadır.
- Durgun(stale): Yönlendirici ilanındaki yönlendirici erişilebilirlik zamanı dolmuş ise önbellekteki giriş durgun hale geçer. Düğümünden yeni bir komşu ilanı mesajı gelince giriş tekrar erişilebilir durumuna geçer.
- Geciktirme (delay): Üst katman protokollerin bilgi verebilmesi için düğüm komşu rica mesajı göndermeden önce bir süre geciktirme durumuna geçer.
- İnceleme (probe): Bu durumda komşu erişilemez kabul edilmektedir. Bu sebeple komşu ricası incelemesi başlatılmaktadır.

3.4.2.4 Yeniden yönlendirme

Yeniden yönlendirme mesajları yönlendiriciler tarafından bir uç noktaya, hedefe ulaşabilmesi için kullanılabileceği en iyi yönlendiriciyi bildirmek için kullanılmaktadır. Veya uç noktaya ulaşmak istenen hedef noktanın aslında bir komşu olduğu mesajı iletilmektedir.

Bir yönlendirici tüm komşu yönlendiricilerin ikinci katman adreslerini bilmek zorundadır. Bu sayede yeniden yönlendirme mesajındaki hedef adresin ikinci katman adresine göre kendi komşusu olup olmadığını belirleyebilmektedir. Statik yönlendirici yapılandırmasında bir sonraki atlama noktasındaki yönlendiricinin adresi ikinci katman adreslemesi kullanarak belirtilmelidir. Dinamik yönlendirme yapılandırmasında ise tüm IPv6 yönlendirme protokollerinin komşu yönlendirici ikinci katman adreslerini değişik tokuş etmeleri gerekmektedir[25].

Yeniden yönlendirme mesajı gönderen yönlendirici, kaynak düğümün bu mesajı doğrulama yapılmadığı için dikkate almaması veya doğru bir şekilde cevap verememesi durumunda, mesaj gönderme oranını düşürmektedir. Bu şekilde bant genişliği ve işlemci kaynak kullanımını sınırlamaktadır. Bir yönlendiricinin, aldığı

yeniden yönlendirme mesajına göre asla mevcut yönlendirme tablosunu güncellememesi gerekmektedir.

Yönlendirici mesajı alan bir uç nokta hedef önbellegini bu mesaja göre güncellemektedir. Eğer herhangi bir hedef önbellegi yoksa da bunu oluşturmaktadır. Uç nokta IP doğrulama başlığı olmayan yeniden yönlendirme mesajlarını kabul etmeyecek şekilde yapılandırılabilir. Ayrıca bir uç noktanın hiçbir zaman yeniden yönlendirme mesajı göndermemesi gerekmektedir[25].

3.4.2.5 Adres çakışması tespiti

Adres çakışması tespiti (duplicate address detection) adresin otomatik mi yoksa el ile mi yapılandırıldığına bakılmaksızın tüm unicast adreslere uygulanabilmektedir. Ancak multicast ve anycast adresleri için kullanılmaması gerekmektedir.

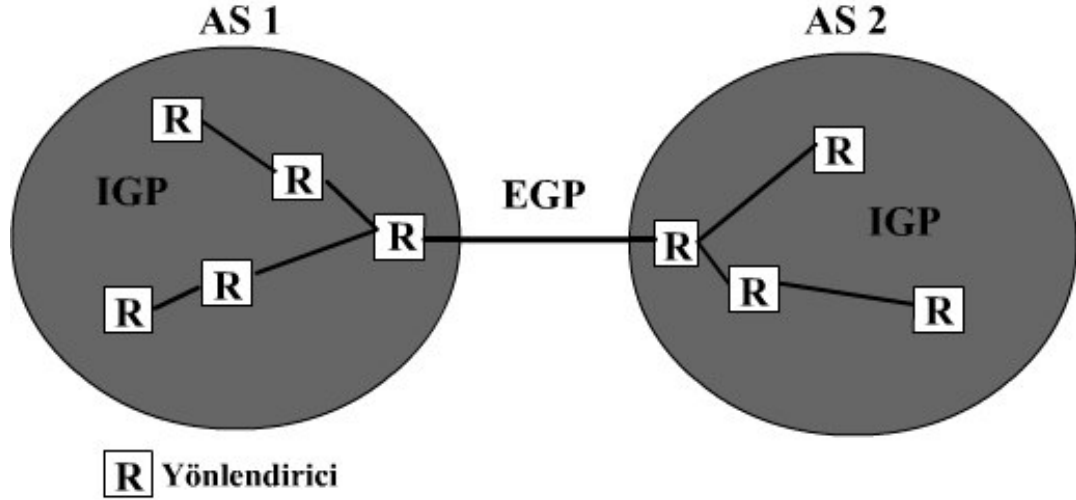
Adres çakışması testi, kontrol edilecek adrese bir komşu rica mesajı göndererek yapılmaktadır. Eğer bu mesaja cevaben bir komşu ilanı mesajı gönderilirse bu durumda o adres ağ üzerinde kullanılıyor demektir ve başka bir cihaz tarafından kullanılmamalıdır. Eğer komşu ricası mesajına herhangi bir cevap gelmezse o adresin herhangi bir düğüm atanmamış olması sonucu çıkarılmaktadır. Varsayılan yapılandırmaya göre aynı anda sadece bir adet komşu rica mesajı gönderilebilir ve bu mesaj bir saniye süre ile komşu ilanı cevabı beklemektedir[17].

3.5 IPv6 Yönlendirme

IPv6'daki yönlendirme bazı yenilikler hariç IPv4'e göre çok büyük değişikliğe uğramamıştır. Paket yönlendirme alt ağdan başlamaktadır. Bir düğüm bir paketi aynı alt ağdaki başka bir düğüme direk gönderebildiği gibi bir yönlendiriciye ileterek paketin hedefe en iyi yoldan iletilmesini sağlayabilmektedir. Yönlendirici paketi iletmek için kendi yönlendirme tablosundaki en uygun girişi seçmekte ve bu girişe göre paketi hedefe yönlendirmektedir.

Alt ağlar belli özelliklerine göre bir otonom sistem (autonomous system - AS) altında gruplandırılmaktadır. Aynı otonom sistemde bulunan yönlendiriciler aynı yönetim politikalarına göre çalışmaktadırlar. Bu yönlendiricilere dahili yönlendiriciler (interior routers) denmektedir. Değişik otonom sistemleri arasında haberleşen yönlendiricilere de harici yönlendiriciler (exterior routers) denmektedir. Dahili

yönlendiriciler dahili geçit protokolleri (interior gateway protocol - IGP), harici yönlendiriciler ise harici geçit protokolleri(exterior gateway protocol - EGP) kullanmaktadır. Aynı AS içindeki yönlendiriciler genellikle aynı IGP'yi kullanarak haberleşmektedirler. Şekil 3.8'de örnek iki tane otonom sistem görünmektedir.



Şekil 3.8: Otonom sistem örneği

3.5.1 Yönlendirme çeşitleri

Yönlendiriciler dahili de harici de olsa kendi içinde tuttıkları yönlendirici tablosuna göre işlem yapmaktadırlar. Yönlendirme tablosu ağ yöneticileri tarafından yaratılabilmekte ve bu tarz yönlendirmeye statik yönlendirme denilmektedir. Eğer bu tablo belirli algoritmalar doğrultusunda otomatik olarak oluşturuluyorsa bu tarz yönlendirme dinamik yönlendirme olarak adlandırılmaktadır. Dinamik yönlendirmede yönlendiriciler tablolarının birbirlerinden aldıkları mesajlar doğrultusunda oluşturmaktadırlar[17].

Bir ağ içinde dinamik ve statik yönlendirmeler beraber kullanılabilir. Statik yönlendirmeler genellikle basit ağ yapılarında kullanılmakta ve yönlendiricilerin ayarlarında çok fazla değişiklik olmadığı varsayımı altında yararlı olmaktadır. Sürekli yapılandırma değiştirmek zorunda kalınan ağlarda dinamik yönlendirme seçilmelidir. Bu şekilde ağ yapısı değişse de yönlendirme tabloları yeni ağ yapısına göre otomatik oluşacaktır. Dinamik yönlendirmelerde kullanılan üç çeşit yönlendirme algoritması bulunmaktadır. Bunlar; uzaklık vektörü (distance vector), bağlantı durumu (link state), ve yol vektörüdür (path vector).

3.5.1.1 Statik yönlendirme

Statik yönlendirme, yönlendirme tablosunun bir ağ yöneticisi tarafından oluşturulması ile yapılmaktadır. Tüm paket akışı yöneticinin elindedir. Ancak ağda meydana gelen küçük bir değişiklik tüm yönlendirme yapısını bozabilmektedir. Genellikle küçük ağlarda tüm paketlerin belli bir yönlendiriciye yönlendirilmesi şeklinde kullanılır. Daha karmaşık ağlarda yöneticinin tüm yönlendirme tablosunu oluşturması oldukça zorlaşmaktadır. Ve yapılandırmada bir değişiklik yapmak istediğinde bu değişikliği tek tek tüm yönlendiricilere uygulamak durumunda kalacaktır.

Burada dikkat edilmesi gereken şey uç düğümler için IPv6'da varsayılan yönlendiriciyi tanıtmaya gerek yoktur. Bu işlev komşu keşfi mesajları doğrultusunda yapılmaktadır. Ancak IPv4 yapılandırılmasında kesinlikle varsayılan yönlendirici belirtilmelidir, aksi durumda paketler ağ dışına çıkamamaktadırlar.

3.5.1.2 Metrik

Dinamik yönlendirme bazı algoritmalar yardımı ile sağlanmaktadır ve bu algoritmaların çalışmasında metrik değeri çok önemli görev yapmaktadır. Birçok alternatif yol içinde seçilecek yol metrik değerine bağlı olarak seçilmektedir. İki tane metrik parametresi vardır. Birincisi atlama noktası sayısıdır ve bu sayı bir paketin hedefe ulaşana kadar kaç yönlendiriciden geçeceğini belirtmektedir. Diğer metrik parametresi de maliyet (cost) değeridir. Maliyet yol üzerindeki tüm yönlendiricilerin maliyetlerinin toplamını ifade etmektedir.

Maliyet ve atlama noktası parametreleri ters değerli olarak ifade edilmektedir. Yani metrik değeri yüksek olan yolun seçilme olasılığı düşük olmaktadır. Çünkü maliyeti büyük olan bir yolun sağlayabildiği bant genişliği düşük demektir. Aynı şekilde eğer atlama noktası sayısı fazla ise paket hedefe gidene kadar o kadar çok yönlendiriciden geçecektir. Bu da gecikmelere neden olmaktadır.

3.5.1.3 Uzaklık vektörü

Uzaklık vektörü algoritması dinamik yönlendirme algoritmalarından bir tanesidir. Her yönlendirici uzaklık vektörü veri yapısı adı altında bir tablo tutmaktadır. Ve kendi tablolarını düzenli olarak komşu yönlendiricilerle paylaşmaktadırlar. Bir yönlendirici kendisine gelen tabloyu inceleyerek kendi tablosunu güncellemekte ve

oradaki deęerleri bir arttırarak tabloyu gönderen hariç dięer yönlendiricilere iletmektedir.

Bir paket yönlendirileceęi zaman seçme kriteri olarak tablodaki metrik deęerleri kullanılmaktadır. Ve en düşük metriklı yolun en verimli olacaęı varsayımı altında paket hedefe doęru iletilmektedir. Bazı yönlendirme protokolleri belli aralıklarla kendi tablosunu dięer yönlendiricilere göndermektedirler. Yönlendirme bilgi protokolü RIP uzaklık vektörü tablosunu gönderme işini 30 saniyede bir yapmaktadır.

Bu algoritmanın yararı uygulama kolaylığındadır. Tüm tablo deęişimleri otomatik olmakta ve aę yöneticisine ilk yapılandırmadan sonra fazla iş düşmemektedir. Ancak belli sayıdan fazla yönlendiricinin bulunduğu bir otonom sistemde tablo iletim trafięi çok fazla ve karışık olacaęından bu algoritma çok verimli çalışmamaktadır[17].

3.5.1.4 Yol vektörü

Yol vektörü algoritmasının yapısı, uzaklık vektörü algoritmasına çok benzemektedir. Bu algoritmada metrikler yerine otonom sistemlerin listesi deęiş tokuş edilmektedir. Bu da sistemi uzaklık vektörüne göre çok daha basit bir yapıya kavuşturmaktadır. Aynı zamanda sonuz döngüler daha kolay fark edilebilmektedir. Harici geçit protokolleri (EGP) yönlendirme yapmak için bu algoritmayı kullanmaktadırlar.

3.5.1.5 Bağlantı durumu

Baęlantı durumu algoritması dięerlerine göre daha sonradan geliştirilen bir yapıdır. Bu algoritmaya göre tüm yönlendiriciler bir biri ile iletişime geçerek bulundukları aęın bir haritasını çıkarırlar. Her yönlendirici elindeki bilgileri kullanarak bir harita oluşturmakta daha sonra bir kısım hesaplamalar yapmaktadır. Hesaplamalar sonucunda kendi yönlendirme tablolarını oluşturmaktadırlar.

Yönlendiriciler bilgi alış verişini baęlantı durumu paketleri (LSP) ile yapmaktadırlar ve bu paketler yardımıyla bir LSP veri bankası oluşturmaktadırlar. LSP'ler yönlendiricilerin aę haritasını çıkarmalarını ve tüm yönlendiricilerde aynı haritanın oluşmasını sağlamaktadırlar.

Uzaklık vektörü algoritmasında yönlendiriciler mesajları sadece komşu yönlendiricilere göndermekte ve aynı alt aęda olup olmadıklarına bakmamaktadırlar.

Bağlantı durumu mesajlaşmasında ise yönlendiriciler aynı alt ağdaki tüm yönlendiricilere LSP'leri göndermektedirler.

Bağlantı durumu algoritması ile çok fazla yönlendiriciden oluşan ağlar kolaylıkla yönetilebilmektedir. Bir yönlendiricide meydana gelen bir değişiklik çok hızlı bir şekilde diğerleri tarafından fark edilmekte ve ona göre yönlendirici tabloları düzeltilmektedir. Bu algoritma IS-IS ve OSPF protokolleri tarafından kullanılmaktadır.

3.5.2 Yönlendirme protokolleri

IPv4'te kullanılan yönlendirme protokollerinin ana yapısı değiştirilmeden bu protokoller IPv6'ya uyarlanmışlardır. IPv6 yönlendirme yapmak için kullanılan protokoller RIPv6, OSPFv3, IS-IS, BGP4, IDRPv2'dir. Hiçbir protokol IPv4'teki ile aynı şekilde kullanılamamakta çünkü 128bitlik IPv6 adreslerinin iletimini sağlayamamaktadırlar[17].

3.5.2.1 RIPv6

RIPv6 aynı zamanda RIPng (yeni nesil RIP) olarak da adlandırılmaktadır. RIP uzaklık vektörü algoritması kullanan bir IGP protokolüdür. Bu protokolün düzgün çalışabilmesi için aynı otonom sistemde bulunan tüm yönlendiriciler RIP ile yapılandırılmalıdır.

RIP kullanan her bir yönlendirici kendi komşu yönlendiricilerine her 30 saniyede bir uzaklık vektörü mesajları göndermektedir. Bu mesajları alan yönlendiriciler mesaj içeriklerine göre yönlendirici tablolarını oluşturmaktadırlar. Tablo içinde her bir hedef için yalnızca bir adet seçenek bulunmaktadır. Bu seçenek de metrik değeri en düşük olan yol olacaktır. RIP'le ilgili en önemli sorun 15 olan atlama noktası sınırıdır. Atlama noktası 15 i geçtiği an paket çöpe atılmakta ve hedef ulaşılamaz hatası alınmaktadır.

RIPv6'da yukarıda bahsedilen sınırlama için herhangi bir geliştirilmeye gidilmemiştir. Sadece 128 bitlik adresleri destekleyecek yapıya dönüştürülmüş, yeni bir özellik eklenmemiştir. İstek ve cevap olmak üzere iki çeşit mesaj ile haberleşme sağlanmaktadır. Bu paketler UDP kullanılarak iletilmektedir.

İstek mesajı gönderilen yönlendiricinin tüm yönlendirme tablosu veya tablonun bir kısmı istenmektedir. Cevap mesajı da bir isteğe bağlı olarak gönderilebildiği gibi belirli aralıklarla da gönderilebilmektedir[28].

3.5.2.2 OSPFv3

OSPF bağlantı durumu algoritması kullanan bir dahili geçit protokolüdür(IGP). Çalışma mekanizması RIP'e göre biraz daha karmaşık ancak büyük ağlar için çalışma performansı çok daha iyidir. Hiyerarşik bir yapısı vardır ve bu sayede büyük ağları parçalara ayırıp daha kolay yönetilmesini sağlamaktadır.

Aynı otonom sistem içindeki yönlendiriciler belli özelliklere göre alanlara ayrılmaktadırlar. Ve her alan için bir seçilen yönlendirici (designated router) bir de yedek seçilen yönlendirici (backup designated router) belirlenmektedir. Bir alan içindeki seçilen yönlendirici o alandaki tüm yönlendirici bilgilerini toplamakta ve yönlendirici tablosunu diğer yönlendiricilere bildirmektedir. Herhangi bir sebepten dolayı seçilen yönlendirici devre dışı kalırsa yedek seçilen yönlendirici devreye girmekte ve onun yerine yeni bir yedek seçilen yönlendirici belirlenmektedir. Bu seçimler ve komşuluk ilişkilerini belirleme işleri OSPF merhaba (OSPF hello) paketleri ile yapılmaktadır. Bu protokolde en uygun yol seçilirken bant genişliği, gecikme gibi maliyetler göz önüne alınır ve SPF (en kısa yol ilk önce) algoritması çalıştırılır. Bu algoritmaya göre yönlendirme tablosu oluşturulmaktadır[29].

IPv6 destekleyen OSPFv3'te OSPFv2'ye göre aşağıdaki değişiklikler yapılmıştır[26]:

- OSPF paketlerinin yapısı IPv6 adresleme mimarisini de destekleyecek şekilde geliştirilmiştir.
- IPv6 adres ve ön eklerini taşıyabilecek yeni bağlantı durumu ilanları (LSA) tanımlanmıştır.
- LSA'lar gönderilen ağın kapsamında bazı değişikliklere gidilmiştir.
- OSPFv3, OSPFv2'nin aksine kimlik denetimi yapmamaktadır. Bunun yerine OSPF, AH kimlik denetimi başlığına ve ESP başlığına güvenmektedir.

3.5.2.3 Birleştirilmiş IS-IS

Birleştirilmiş IS-IS (integrated IS-IS) hem TCP/IP'yi yem OSI'yi destekleyebilen, verimli yönlendirme sağlayabilen ve kimlik doğrulama mekanizmaları sunan bir

yönlendirme protokolüdür. Bağlantı durumu algoritması kullanarak dahili geçit protokolü IGP olarak görev yapmaktadır. Yapı olarak OSPF'e çok benzemektedir ve Uluslararası Standartlar Organizasyonu (ISO) dokümanı olarak ISO 10589'da tanımlanmıştır. Ayrıca RFC 1195'te de protokol mimarisi ve kullanımı detaylı olarak açıklanmaktadır.

IS-IS'e IPv6 desteği sağlarken yapılan büyük değişikliklerden biri IPv4 için bulunan "IP dahili erişilebilirlik" ve "IP harici erişilebilirlik" alanları yerine "IPv6 erişilebilirliği" ve "IPv6 arayüz adresi" alanları eklenmiştir. IPv6 erişilebilirlik alanının türü 236 ve IPv6 arayüz adresinin türü 232 değeri verilerek ifade edilmektedir. Ayrıca diğer yönlendirme protokollerinde olduğu gibi IS-IS de IPv6 adresleme yapısının destekleyebilecek yapıya getirilmiştir[30].

3.5.2.4 BGP-4

Sınır geçit protokolü (BGP) RFC 1771 belgesinde tanımlanmış bir yol vektörü yönlendirme protokolüdür. RIP ve OSPF'in yaptığı gibi otonom sistemler içindeki yönlendirmeyi değil de otonom sistemler arasındaki yönlendirme işini yapmaktadır. Bu sebeple harici geçit protokolleri (EGP) arasında yer almaktadır. Yol vektörü algoritmasının çalışma yapısı gereği sanal yollar belirleyip o yollara göre yönlendirme tablosu hazırlamaktadır. BGP-4 mesajları 179 numaralı TCP portundan iletilmektedir[26].

BGP-4 için IPv6 desteği RFC 2545 ve RFC 2858 belgelerinde detaylı olarak anlatılmaktadır. BGP yönlendirme bilgisi bakımından IPv4 ile IPv6 arasındaki en önemli değişiklik IPv6'nın yeni getirdiği unicast adresleri ve belli durumlar için belli bir adres aralığının kullanılması gerekliliğidir. Taşıma katmanı protokolü olarak IPv6 TCP kullanılmaktadır. IPv4'e göre yeni güvenlik özellikleri getirilmemiştir.

3.5.2.5 IDRPv2

IDRP, BGP-4 gibi yol vektörü algoritması kullanmakta ve otonom sistemler arasındaki yönlendirmeyi sağlamaktadır. ISO 10747 belgesinde tanımlanmıştır. IDRPv2 bu protokolün IPv6 desteği sağlayan yeni sürümüdür. IPv6 yönlendirme bakımından BGP'ye göre üstündür çünkü yeni otonom sistem tanımlayıcıları yerine IPv6 adres ön eklerini kullanmaktadır[26].

3.6 Alan Adı Sistemi

IPv6 ile birlikte alan adı sistemi eskisine göre çok daha fazla önem kazanmıştır. 32 bit olan IPv4 adreslerini kullanmak bazı uygulamalarda uzun alan isimleri kullanmaktan daha kolay olsa da, 128 bitlik IPv6 adreslerinde durum böyle olmamaktadır. IPv6 adreslerini öğrenmeye çalışmak ve işlemleri bu adresler ile yapmak bir sistem yöneticisi için zorunlu durumlarda nadir olarak kullanılacak bir yöntem olabilmekte ancak bir son kullanıcı için neredeyse imkânsız gözükmektedir.

Alan adı sisteminin IPv6 yapısını desteklemesi için yeni bir kayıt türü geliştirilmiştir. IPv4'te "A" olarak geçen kayıt türü IPv6'da "AAAA" (quad-A) olarak geliştirilmiştir. Burada dört "A" kullanılmasının sebebi IPv6 adresinin IPv4 adresine göre 4 kat uzun olmasıdır. AAAA kaydının tür değeri 28 olarak belirlenmiştir[32].

IPv6 adreslerinin isim kayıtlarının tutulabilmesi için, var olan yazılımlarla uyumlu çalışabilecek, aşağıdaki geliştirmeler yapılmıştır:

- Alan adını IPv6 adresi ile eşleştiren yeni bir kayıt türü geliştirilmiştir.
- Bu tür adreslerle yapılan aramaları desteklemek için yeni bir alan tanımlanmıştır.
- IPv4 adreslerini konumlandırmak için yapılan sorgular, IPv6'yı da destekleyecek şekilde genişletilmiştir.

Kayıt türleri tamamen nitelikli alan ismi (FQDN) adres türü ve adresin kendisinden oluşmaktadır. Aşağıda aynı alan isminin hem IPv4 hem IPv6 adres kayıtları örnek olarak verilmiştir. Herhangi bir isim sorgusunda sorgulayan düğüme bağlı olarak bu iki adresten biri veya ikisi de cevap olarak geri dönmektedir.

<i>İsim</i>	<i>IN</i>	<i>A/AAAA</i>	<i>Adres</i>
<i>ns.mustafa.ipv6</i>	<i>IN</i>	<i>A</i>	<i>160.75.67.1</i>
<i>ns.mustafa.ipv6</i>	<i>IN</i>	<i>AAAA</i>	<i>2001:4BD0:2031::10</i>

Ters sorgularda (reverse query) "ip6.arpa." alanı kullanılmaktadır. İlk zamanlarda "ip6.init." de kullanılmış ancak yavaş yavaş devre dışı kalmaktadır. Tersten sorgu kayıtları işaretçi kaydı (pointer record) olarak geçmekte ve PTR ile ifade edilmektedir. IPv6 adresi 2001:4BD0:2031::1 olan bir cihazın PTR kaydı aşağıdaki gibi tutulmaktadır.

"1.0.1.3.0.2.0.D.B.4.1.0.0.2 IN PTR ns.mustafa.ipv6"

Yukarıdaki örneklerden de görüldüğü gibi IPv6 alan adı sisteminde çalışma prensipleri ve yapılandırma bakımından bazı değişikliklere gidilmiş ve ek geliştirmeler yapılmıştır. IPv6 adres uzunluğu ile önemi bir kat daha artan alan adı sisteminde yapılan bu değişiklikler son kullanıcı tarafından fark edilmemektedir. Yani son kullanıcı aynen IPv4'te olduğu gibi alan adını kullanmakta, bu alan adı ile birlikte dönen adresin IPv4 mü, IPv6 mı olduğu veya hangi çeşit adres olduğu (global, site-local vb.) detayları ile uğraşmak zorunda kalmamaktadır.

3.7 Otomatik Adres Yapılandırması

IPv6'nın en yararlı özelliklerinden bir tanesi, herhangi bir sunucu olmadan da kendi adresini otomatik olarak yapılandırabilmesidir. IPv6 yapısını destekleyen bir uç nokta her arayüzü için bir adet link-local adresi otomatik olarak yapılandırmış bulunmaktadır. Ayrıca komşu keşfi mekanizması ile yönlendirici adreslerini ve diğer ağ yapılandırmalarını alabilmektedir.

Alan adı sistemi gibi otomatik adres yapılandırması sistemi de IPv6 için kritik öneme sahiptir. Çünkü bu derece uzun adreslerin tek tek uç noktalara el ile yapılandırılması oldukça güç bir iştir. Aynı zamanda böyle bir yapılandırmada hata olasılığı çok yüksek olmaktadır. IPv4'teki gibi sunucu adreslerinin el ile yapılandırılması gerekmektedir çünkü bu adreslerin bir kere verildikten sonra bir daha değişmemesi gerekmektedir.

İki çeşit otomatik adres yapılandırması bulunmaktadır. Bir tanesi sunucusuz otomatik adres yapılandırması (stateless autoconfiguration) diğeri de sunuculu otomatik adres yapılandırmasıdır (stateful autoconfiguration). Sunucusuz yapılandırma IPv6 ile yeni gelen bir özelliktir. IPv4'te bulunmamaktadır. Uç noktalarda herhangi bir ayar yapılmamakta ve bir sunucu kullanılmamaktadır. Sadece yönlendirici tarafında küçük bir ayar ile sunucusuz otomatik yapılandırma kullanılabilmektedir. Sunuculu yapılandırma ise adresin ve bazı ağ ile ilgili bilgilerin bir sunucu yardımı ile dağıtıldığı, IPV4 ve IPv6'da kullanılabilen bir yapılandırma çeşididir. Sunuculu ve sunucusuz iki yapılandırmanın birlikte kullanıldığı ağlar da bulunmaktadır.

3.7.1 Sunucusuz otomatik yapılandırma

Sunucusuz otomatik adres yapılandırması bir uç noktanın kendi elindeki bilgiler ve yönlendiricinin ilan ettiği bilgileri kullanarak ağ arayüzünü yapılandırmasını sağlamaktadır. Bir sunucu kullanılması gerekmemesi ve yönlendiricide yapılan ayarın çok az olması dolayısıyla otomatik yapılandırma işlemini çok basitleştirmektedir.

IPv6 adresleri arayüzlere belli bir zaman aralığı için atanmaktadır. Her adresin bir ömrü vardır ve o ömür bittiği zaman bu adres yeniden atanmak üzere serbest bırakılmaktadır. Bu mekanizma sırasında bir adres iki durumda olabilmektedir. Tercih edilen (preferred) durumda ise bu adres istenen şekilde herhangi bir sınır olamadan kullanılabilir. Eğer adres reddedilmiş (deprecated) konumda ise adres kısa süre içinde kullanılmaz olacaktır ve bu adres ile yeni bağlantılar kurulmamalıdır. Yeni bağlantılar tercih edilmiş adres atanınca kurulmalıdır[26].

Burada anlatılan otomatik adres yapılandırması uç noktalar içindir yönlendiriciler için değildir. Yönlendiricilerin sadece link-local adresleri otomatik yapılandırılmaktadır. Sunucusuz otomatik yapılandırma aşağıdaki amaçları yerine getirebilmek için tasarlanmıştır[33]:

- Uç noktaları ağa bağlamadan önce el ile herhangi bir ayar yapılmamalıdır. Otomatik yapılandırma her düğümün kendine özel bir tanımlayıcı sağlayabileceğini varsaymaktadır. En basit durumda da bu tanımlayıcı ağ arayüzünün ikinci katman adresidir.
- Birkaç tane düğümden oluşan küçük ağlarda ağ içi haberleşme için herhangi bir adres sunucusuna veya yönlendiriciye ihtiyaç duyulmamalıdır. Link-local adresleri bu işi yerine getirebilmelidir.
- Büyük bir ağda uç noktalar ve yönlendiriciler bir adres dağıtım sunucusuna ihtiyaç duymamalıdır. Link-local adreslere ek olarak site-local ve global adresler de otomatik yapılandırılmalıdır.
- Bir cihaz bir ağdan tamamen ayrı başka bir ağa taşınmak zorunda kaldığı zaman daha önce kullanmış olduğu adresler otomatik olarak devre dışı kalmalı ve yeni ağın özelliklerine uygun yeni adres yapılandırılması gene otomatik olarak yapılandırılmalıdır.

- Sistem yöneticileri yönlendirici ilanları ile hangi çeşit adres yapılandırmasının kullanacağını bildirebilmelidirler. Uç noktalar sunuculu veya sunucusuz yapılandırma kullanacaklarını bu şekilde anlayabilmelidirler.

Bir uç noktaya link-local adresi atanmadan ve kullanılmadan önce bu geçici (tentative) adresin aynı ağdaki başka bir düğüm tarafından kullanılmadığının kontrol edilmesi gerekmektedir. Bu kontrol komşu ricası mesajı ile yapılmaktadır. Kontrol edilmek istenen link-local adresi komşu ricası mesajının hedef adresi olarak atanmaktadır. Eğer komşu cevabı mesajı alınırsa bu durumda ilgili adresin ağda tekil olmadığı sonucuna varılmaktadır. Eğer bir düğüm geçici adresinin tekil olmadığını fark ederse otomatik yapılandırma sona ermektedir ve yeni bir adresin el ile yapılandırılması gerekmektedir.

Otomatik yapılandırmanın bir sonraki aşaması bir yönlendirici ilan almak veya ağda herhangi bir yönlendirici bulunmadığını keşfetmek olmaktadır. Eğer ortamda yönlendirici varsa yönlendirici ilanları gönderilecektir. Yönlendiricinin olmadığı durumlarda sunuculu yapılandırılma kullanılması gerekmektedir.

Yönlendirici ilanlarında sunuculu ve sunucusuz yapılandırma bilgileri bir birinden bağımsız olarak işlenmekte bu sebeple bir düğüm ikisini de aynı anda kullanabilmektedir. Aynı zamanda kullanılan adresin ömrü de bildirilmektedir[33].

3.7.2 Sunuculu otomatik yapılandırma ve DHCPv6

Sunuculu adres otomatik yapılandırması orta ve büyük ölçekli ağlar içinde kullanılması yararlı olan, bir sunucu yardımıyla IP adresinin ve diğer parametrelerin dağıtılabildiği bir sistemdir. İleride geliştirilecek olan yeni seçenekleri de taşıyabilecek şekilde genişletilebilir bir yapıya sahiptir. Şu anda en çok kullanılan dinamik yapılandırma protokolü DHCP'dir

DHCP'nin eski sürümü DHCPv4 olarak adlandırılmaktadır. DHCP'ye IPv6 desteği DHCPv6 ile birlikte sağlanmıştır. Adres ve istenen diğer parametrelerin dağıtımı DHCP sunucusu ile yapılmaktadır. Büyük ve karmaşık ağlarda her bir alt ağ için bir DHCP sunucusu kurmak çok verimli olmamaktadır. Bu sebeple DHCP rölesi (DHCP relay) terimi ortaya atılmıştır. DHCP rölesi sunucu ile istemci arasında DHCP paketlerinin iletilmesini sağlamaktadır. Adres yapılandırma bilgilerinin birden çok DHCP sunucusunda tutulması, ağın güvenilirliğini ve performansını arttıracaktır.

İstemci ve sunucular aralarındaki DHCP mesaj değişimini UDP kullanarak link-local adresler aracılığıyla yapmaktadırlar. Sunucular, istemcilerden gelen mesajları reserve edilmiş link-multicast adreslerinden almaktadırlar. Bu sebeple de istemcilere DHCP sunucusunun adresinin bildirilmesine gerek kalmamaktadır. İstemci bir kere DHCP sunucusun adresini öğrendikten sonra artık unicast olarak mesaj gönderebilmektedir[34].

İstemci sunucunun kendisine bir IP adresi atamasını istemeyip, DNS sunucusunun ve ağ zaman protokolü NTP sunucusunun adresleri gibi başka bazı bilgileri istiyor olabilmektedir. Bu durumda istemci ile sunucu haberleşmesi iki mesajlı bir yapı ile sağlanmaktadır. İstemci tüm DHCP röle ve sunucularını ifade eden multicast adrese bir bilgi isteği mesajı göndermektedir. Sunucular da bu mesaja istenen bilgilerin eklendiği bir cevap mesajı ile geri dönmektedirler. Eğer sunucuda bir istemci için ayrılmış IPv6 adres/adresleri ve diğer yapılandırma bilgileri bulunuyorsa bu haberleşme gene iki mesajlı yapı ile sağlanmaktadır.

Bir istemci adres atamasının ve ağ ile bilgilerin bir DHCP sunucu tarafından verilmesini istiyorsa dört mesajlı bir haberleşme yapısı kullanmaktadır. İstemci, erişilebilir DHCP sunucuları bulabilmek için tüm DHCP röle ve sunucularına bir rica mesajı göndermektedir. İstemcinin isteklerini karşılayabilecek herhangi bir DHCP sunucu istemciye ilan mesajı göndermektedir. Daha sonra istemci sunucular arasından bir tanesini seçerek ona istek mesajı göndermektedir. Seçilen sunucu gerekli bilgiler cevap mesajı ile sağlamaktadır. İstemciye atanan her adresin sunucu tarafından belirlenmiş bir ömrü bulunmaktadır. Bu ömrü uzatmak için istemci sunucuya yenileme mesajı göndermekte, sunucu da cevap mesajında o adreslerin geçerli olacağı yeni zaman aralığını bildirmektedir[35].

DHCPv6 geliştirilirken IPv6'ya özel olan düğümlerin kendi link-local adreslerini yaratabilmesi ve her düğümün multicast adreslerini destekleme gerekliliği özellikleri kullanılmıştır. IPv6'nın bu iki avantajı sayesinde sunuculu otomatik adres yapılandırması yapmak isteyen bir istemci iletişim için kendi yarattığı link-local adresini kullanabilmekte ve multicast adresleri sayesinde ilgili DHCP röle veya sunucu ile haberleşebilmektedir.

DHCPv6 ile kullanıma geçen iki önemli multicast adresi bulunmaktadır. Bunlar; tüm DHCP röle ve sunucuları ifade eden FF02::1:2 multicast adresi ve tüm DHCP sunucuları ifade eden FF05::1:3 multicast adresidir. FF02::1:2 adresi istemcinin

komşu röle ve sunucularla iletişime geçtiği adrestir. Aynı linkteki tüm sunucular ve röleler bu adresin bir üyesidir. FF05::1:3 adresi ise röle ajanlarının (relay agent) DHCP sunucuları ile iletişime geçtikler adrestir. Ağdaki tüm sunucular bu multicast grubun bir üyesidirler. Haberleşme sırasında istemciler DHCP mesajlarını UDP 546 portundan, sunucu ve röle ajanları UDP 547 portundan dinlemektedirler[34].

3.8 IPv6'ya Geçiş Mekanizmaları

Yeni bir teknolojinin mevcut sisteme başarılı adaptasyonu, sistemin kolay kurulumu ve mevcut altyapı üzerinde çalışan servislerde önemli bir kesintiye sebep olmaması ile sağlanabilmektedir. İnternet'te şu anda yüz binlerce IPv4 ağı ve milyonlarca da IPv4 düğümü bulunmaktadır. Şirketlerin İnternet'e ve ağ içi servislere olan bağımlılıkları o kadar fazladır ki en ufak bir kesintiye bile tahammülleri bulunmamaktadır. Bu sebeple böyle geniş kullanıma sahip bir protokolden yeni nesil bir protokole çok hızlı bir şekilde geçebilmek imkânsızdır. Burada en önemli iki kavram geçişin olabildiğince saydam bir şekilde olması ve çalışan sistemin bu geçişten olabildiğince az etkilenmesidir.

Ağ tasarımcıları IPv6'ya geçişin ağ içindeki küçük bir alandan başlamasının ve yavaşça ağ merkezine doğru yaklaşmasının en uygun geçiş yöntemi olacağını düşünüyorlar. Böyle bir küçük alandan başlamanın stratejik yanı, bu alan dışındaki IPv6 trafiğinin IPv4 üzerinden akması, aynı alan içindeki düğümlerin aralarında sadece IPv6 ile haberleşmesidir. Bu alanda sağlanan başarılı iletimden sonra alan genişletilebilmekte, en son amaç olarak da IPv6 geçişinin tüm ağı kapsayan şekilde gerçekleştirilmesi sağlanmaktadır[36].

Yukarıda bahsedilen sebeplerden dolayı IPv4'ün tamamen kullanımdan kalkıp tüm dünyanın IPv6 kullandığı bir zaman belirtmek oldukça zordur. Bu geçiş yavaş gerçekleşecektir. Ancak birçok şirket teknolojide önderlik kavramını vurgulamak adına geçiş için önemli ölçüde bütçe ve insan gücü ayırmaktadır. Büyük şirketler er ya da geç IPv6 göçünün (migration) olacağını farkında olarak, bu geçişi en kısa sürede gerçekleştirmek istemektedirler.

Bir düğüm beş çeşitten bir tanesi olmak durumundadır[37]:

- *Sadece IPv4 düğümü* (IPv4-only node) - Sadece IPv4 adresi olan ve IPv6 destekleyemeyen düğümdür. Şu anda dünyadaki birçok yönlendirici ve uç nokta sadece IPv4 düğümüdür.
- *Sadece IPv6 düğümü* (IPv6-only node) - Sadece IPv6 adresi olan ve IPv4 destekleyemeyen düğümdür. Şu anda bu tarz düğümler çok fazla değildir. Daha çok IPv6 destekli cep telefonlarında ve el bilgisayarlarında görülmektedir.
- *IPv6/IPv4 düğümü* - Hem IPv6'yı hem de IPv4'ü destekleyebilen düğümdür. IPv6 göçünün tamamlanabilmesi sırasında bir süre bu düğümler yoğun olarak kullanılacaktır.
- *IPv4 düğümü* - IPv4 destekleyebilen bir düğümden bahsedilmektedir. Sadece IPv4 düğümü veya IPv6/IPv4 düğümü olabilmektedir.
- *IPv6 düğümü* - IPv6 destekleyebilen bir düğümden bahsedilmektedir. Sadece IPv6 düğümü veya IPv6/IPv4 düğümü olabilmektedir.

3.8.1 Uyumluluk Adresleri

Uyumluluk adresleri, IPv6 ve IPv4 düğümlerinin bir arada bulunabilmeleri ve aralarında iletişimde kurabilmeleri için geliştirilmiştir.

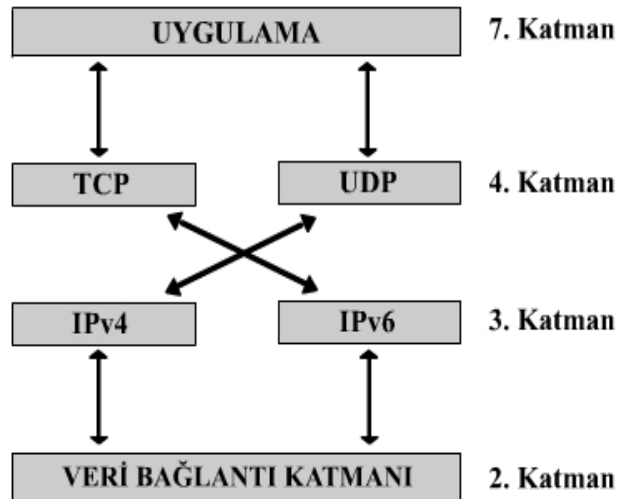
- *IPv4 uyumluluk adresi* - IPv4 uyumlu adresler 0:0:0:0:0:m.n.k.l veya ::m.n.k.l şeklinde ifade edilmektedir. Burada m.n.k.l 32 bitlik IPv4 adresidir ve bu IPv4 adresi global olmak zorundadır.
- *IPv4'le eşlenmiş adresler* - 0:0:0:0:FFFF:m.n.k.l veya ::FFFF:m.n.k.l şeklinde ifade edilmektedir. Bu adres türü IPv4 düğümlerini IPv6 adresleri olarak tanımlayabilmek için kullanılmaktadır. En büyük avantajı bu adres çeşidini kullanan programlar tek adresi alarak hem IPv4 hem IPv6 adresini elde etmiş olurlar.
- *6over4 adresleri* - 6over4 adresleri ::XXYY:WWZZ şeklinde gösterilmektedir. Buradaki XXYY:WWZZ bölümü m.n.k.l IPv4 adresinin onaltılık sayı düzeninde ifadesidir. Örnek olarak 160.75.67.1 IPv4 adresi ::A04B:4301 6over4 adresi şeklinde ifade edilmektedir.

- *6to4 adresler* – 2002:XXYY:WWZZ::/48 ön ekinden oluşan adreslerdir. Burada bulunan XXYY:WWZZ bölümü global bir IPv4 adresinin onaltılık sistemde ifadesidir.
- *ISATAP adresleri* – 64 bitlik ön ek ve 64 bitlik arayüz tanımlayıcısından oluşmakta ve ::5EFE:m.n.k.l şeklinde ifade edilmektedir. Link-local ISATAP adresine bir örnek olarak FE80::5EFE:160.75.67.1 verilebilir.
- *Teredo adresleri* – Teredo adresleri 3FFE:831F::/32 ön ekini kullanmaktadır. Teredo mekanizması NAT kullanan sistemlere IPv6 desteği sağlamak üzere geliştirilmiştir[26].

3.8.2 Çift yığın yapısı

Çift yığın (dual stack) yapısı, düğümlerde hem IPv6 hem de IPv4 protokol yığınlarının kullanılabilmesini sağlamaktadır. Çift IP katmanı (dual IP layer) olarak da isimlendirilmektedir. Tünelleme mekanizması kullanan bir düğümün mutlaka çift IP katmanına sahip olması gerekmektedir.

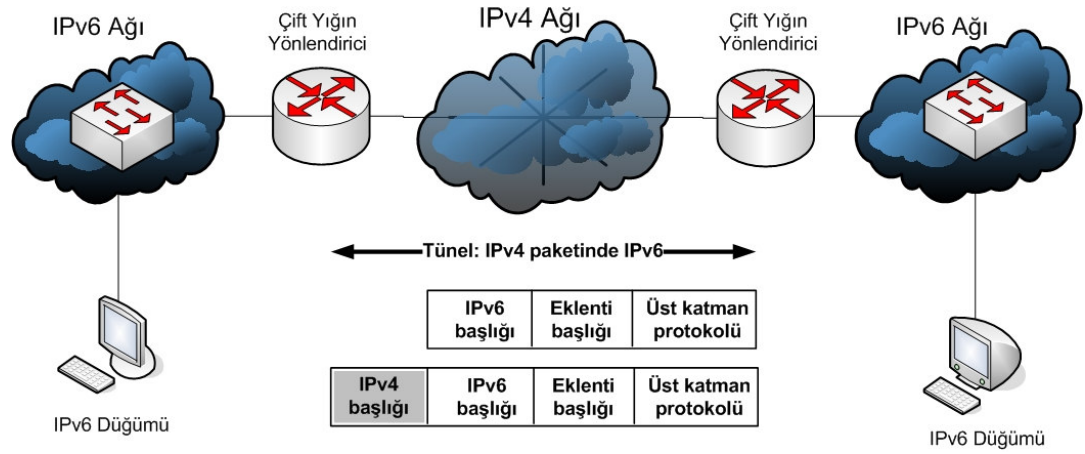
Bir düğümün haberleşeceği adres eğer IPv4 adresi ise düğüm içinde IPv4 protokol yığını, IPv6 ise IPv6 protokol yığını kullanılmaktadır. Genellikle çiftli IP katmanı kullanan uygulamaların ilk tercihi IPv6 kullanarak işlemleri yerine getirmektir ancak bu ayarlar uygulamadan uygulamaya değişmektedir. Mesela DNS isteği ile geri dönen adreslerden Web uygulaması için öncelikle IPv6 adresi tercih edilmektedir[38]. Şekil 3.9’da çift yığın mimarisi gösterilmektedir.



Şekil 3.9: Çift yığın mimarisi

3.8.3 IPv4 üzerinden IPv6 tünelleme

IPv4 üzerinden IPv6 tünelleme, IPv6 paketlerinin iletilmediği ortamlarda bu paketlere IPv4 başlıkları ekleyerek iletilmesini sağlayan yöntemdir. Şu anda İnternet'in çok büyük bir kısmı IPv4 olduğu için tünelleme mekanizmaları çok yoğun olarak kullanılmaktadır. Şekil 3.10'da birbirinden IPv4 ağı ile ayrılmış iki IPv6 ağının içindeki düğümlerin arasında IPv6 anlaşabilmelerini sağlayan tünelleme yapısı gösterilmektedir.



Şekil 3.10: Tünelleme yapısı

Dört çeşit tünelleme yapısı bulunmaktadır[38]:

- *Yönlendiriciden yönlendiriciye* (router-to-router) – Çift yığın destekli yönlendiricilerin arasında eğer IPv4 ağı varsa yönlendiriciden yönlendiriciye tünel kurulmaktadır. Bu yolla IPv6 paketleri IPv4 ağı içerisinde hedefe iletebilmektedir. Şekil 3.10'daki belirtilen yapı bu tip tünellemeye örnektir.
- *Uç noktadan yönlendiriciye* (host-to-router) – İsminden de anlaşıldığı üzere IPv6/IPv4 bir uç nokta IPv6 paketleri iletebilmek için IPv6/IPv4 bir yönlendiriciye tünel kurmaktadır.
- *Uç noktadan uç noktaya* (host-to-host) – Bu durumda iki uç nokta arasında tünel kurulmaktadır. Yani uçtan uca bir tünel bağlantısı sağlanmaktadır. Dikkat edilmesi gereken konu iki noktanın da çift yığın yapısında olması gerektiğidir.

- *Yönlendiriciden uç noktaya (router-to-host) – Çift IP katmanlı bir yönlendiricinin çift IP katmanlı bir uç nokta cihazına tünel kurması gerekebilmektedir. Bu durumda yönlendiriciden uç noktaya diye adlandırılan tünel yapısı kullanılmaktadır.*

3.8.4 Tünel çeşitleri

Ağ yapılarının çok çeşitli olması ve ihtiyaçların bu ağ yapılarına göre değişmesi nedeniyle çok sayıda tünel çeşitleri geliştirilmiştir. Ağ yöneticileri kendi ağlarına tünelleme ile IPv6 desteği kazandırmadan önce tünelleme mekanizmalarını çok iyi incelemeleri ve kendilerine en uygun mekanizmayı seçmeleri gerekmektedir.

Şu anda dünya yüzeyindeki mevcut ağların çok büyük bir bölümünün IPv4 olmasından dolayı tünellemenin asıl kullanım amacı IPv6 erişimi sağlamak olmaktadır. IPv6'ya geçişin uzun dönemdeki aşamalarından bir tanesi de tam tersine olan tünellemeyi kullanmaktır. Yani dünyada IPv6 kullanımı baskın hale geldiğinde geriye kalan az miktardaki IPv4 ağı için IPv6 üzerinden tünellemeler yapılacaktır. Burada anlatılacak mekanizmalar IPv6 erişimi sağlamak için kullanılanlardır.

3.8.4.1 El ile yapılandırılmış tünel

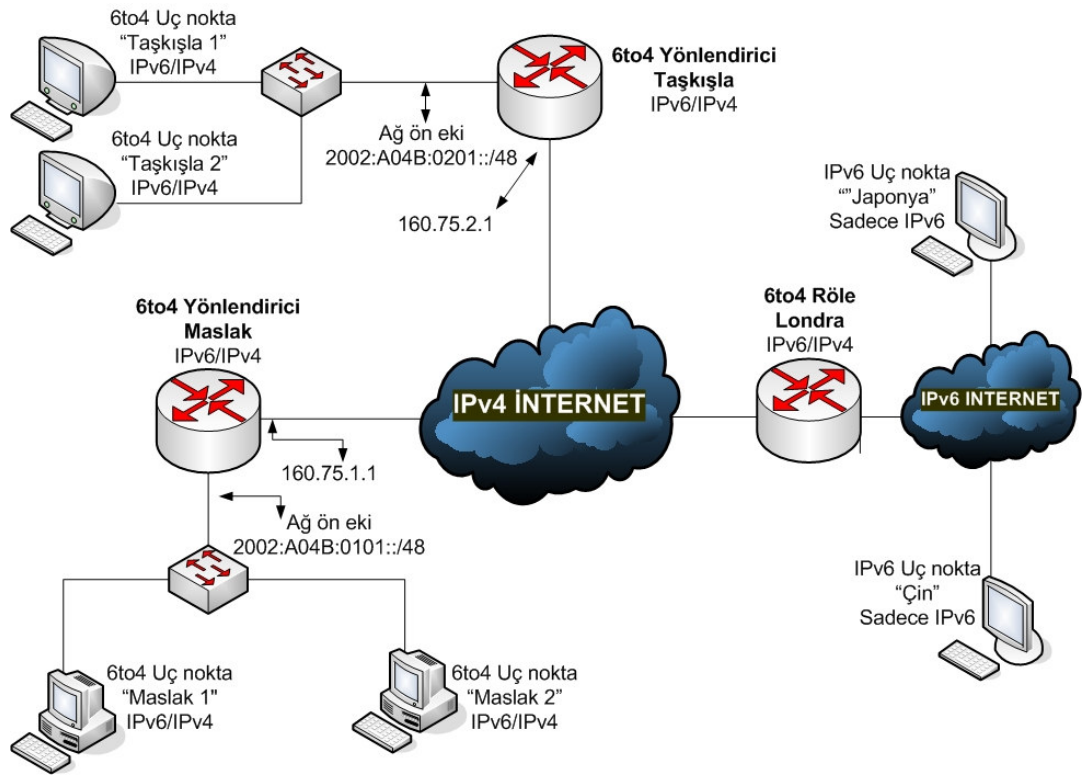
Bir ağ yöneticisi IPv6 tünelini kendi ağı ile ilgili bazı nedenlerden dolayı el ile yapılandırmak isteyebilir. Bu durumda kullandığı tünel mekanizmasına ve yönlendiriciye göre bazı komutlar girmesi gerekmektedir. Tünel sayısı arttığı zaman tünel yapılandırması zorlaşmakta veya tünel uç noktalarından herhangi birinde bir değişiklik olduğu zaman iki tarafta da yeni yapılandırma yapılması gerekmektedir. Bundan sonraki anlatılacak mekanizmalar otomatik yapılandırma çeşitleridir.

3.8.4.2 6to4 tüneli

6to4 tüneli çift yığınlı yönlendiriciler arasında kurulan ve yönlendiricilerin bulundukları ağlar arasında IPv6 bağlantısı sağlamayı amaçlayan bir tüneldir. 2002:WWXX:YYZZ::/48 ön ekine sahip 6to4 adresleri kullanılarak haberleşme sağlanmaktadır. Burada WWXX:YYZZ, m.n.k.l şeklindeki IPv4 adresinin onaltılık sayı düzenindeki ifadesidir.

Ağda 6to4 adresleri üç çeşit düğüme atanmaktadır[39]:

- *6to4 yönlendirici* – 6to4 tüneli kurulan yönlendiriciyi ifade etmektedir. Genellikle tünelin bir uç noktasını oluşturmakta ve IPv4 ile IPv6 ağının arasında yer almaktadır.
- *6to4 rölesi* – Normal IPv6 adresleri ile 6to4 adresleri arasındaki geçiş yönlendirmesini yapmaktadır.
- *6to4 uç noktası* – En azından bir adet 6to4 adresi ile yapılandırılan bir uç noktayı ifade etmektedir. Diğer tüm özellikleri ile IPv6 destekleyen standart bir uç noktadır.



Şekil 3.11: 6to4 tünelleme örneği

Şekil 3.11’de 6to4 tünel yapısı kullanılarak sağlanan IPv6 bağlantısı örneklenmiştir. 6to4 yönlendiriciler 2002:WWXX:YYZZ:SubnetID::/64 şeklinde bir ön ek oluşturmakta ve bu ön ek kullanımı ile uç noktalar kendilerine 6to4 adresleri yapılandırmaktadırlar. Buradaki WWXX:YYZZ yönlendiricinin tünel tarafındaki IPv4 adresinin on altılık sistemde gösterilişi, SubnetID de yönlendiricinin alt ağlar için verdiği 16 bitlik bir değerdir. Maslak yönlendiricisi 160.75.1.1 olan tünel ucundaki IPv4 adresini kullanarak 48 bitlik “2002:A04B:0101” şeklinde bir ön ek

oluşturmuştur. Aynı ağ içinde oluşturulan 64 bitlik ön eklerle uyuşmayan hedef adresler 6to4 yönlendiriciye iletilmektedir. 6to4 yönlendiricisi de 2002::/16 şeklindeki hedef adresleri diğer 6to4 yönlendirici veya düğümlere, bunun dışındaki adresleri ::/0 varsayılan yönlendirme olarak 6to4 rölesine göndermektedir[26].

Şekil 3.11’de verilen örnekte Maslak 1 ve Maslak 2 uç noktaları aynı ağda bulundukları için aralarında direk haberleşebilmektedirler. Maslak 1 bilgisayar, Taşkışla 1 bilgisayarına paket göndermek istediği zaman paketi IPv6 şeklinde Maslak 6to4 yönlendiricisine göndermektedir. Bu paketi alan yönlendirici IPv6 paketini IPv4 başlığı ile bir daha paketlemekte ve sonra yönlendirici tablosuna göre Taşkışla 6yo4 yönlendiricisine paketi iletmektedir. Taşkışla yönlendiricisi öncelikle IPv4 başlığını atmakta sonra kendi yönlendirme tablosuna göre IPv6 paketini Taşkışla 1 bilgisayarına iletmektedir.

Yukarıdaki örnekte Maslak 1 bilgisayarının arayüz tanımlayıcısını A1, Maslak alt ağ tanımlayıcısını 1, Taşkışla 1 bilgisayarının arayüz tanımlayıcısını B1 ve Taşkışla alt ağ tanımlayıcısını da 2 olarak ele alalım. Bu durumda Maslak 1 bilgisayar ile Taşkışla 1 bilgisayar arasındaki 6to4 haberleşme sırasında IPv4, IPv6 hedef ve kaynak adresleri Şekil 3.12’deki gibidir.

ALAN	DEĞER
IPv4 Kaynak Adresi	160.75.1.1
IPv6 Kaynak Adresi	2002:A04B:0101:1::A1
IPv4 Hedef Adresi	160.75.2.1
IPv6 Hedef Adresi	2002:A04B:0201:2::B1

Şekil 3.12: 6to4 örneği hedef ve kaynak adresleri

3.8.4.3 ISATAP

ISATAP IPv6 uç noktalarının IPv4 ağı üzerinden haberleşmelerini sağlayan tünelleme mekanizmalarından bir tanesidir. Uç noktaların haberleşmesi sırasında ISATAP adresleri kullanılmaktadır. Bu adresler 6to4, 6over4 ve IPv4 uyumlu adresleri gibi IPv6 adresin içerisinde IPv4 adresi içermektedirler. IPv4 adresinin global olması gerekmemektedir. ISATAP adresleri 64 bitlik ön ek ve 64 bitlik arayüz tanımlayıcısından oluşmakta ve ::5EFE:m.n.k.l şeklinde ifade edilmektedir. ISATAP arayüz tanımlayıcısı 64 bitlik herhangi bir IPv6 ön eki birleştirilebilmektedir. Link-

local ISATAP adresine bir örnek olarak FE80::5EFE:160.75.67.200 verilebilmektedir.

IPv6 desteği sunan Microsoft işletim sistemlerinde (Windows XP, 2K3 ve Vista) link-local ISATAP adresi otomatik olarak yapılandırılmaktadır. IPv4 bir ağ içerisinde ISATAP yapılandırılması yapılan iki bilgisayar aralarında IPv6 haberleşebilmektedirler. Bir ağda IPv4 adresleri 160.75.67.20 ve 160.75.67.21 olan iki bilgisayar olsun ve bunlar ISATAP adresi ile yapılandırılmış olsunlar. ISATAP link-local adresleri FE80::5EFE:160.75.67.20 ve FE80::5EFE:160.75.67.21 olmaktadır. Bu arayüzleri kullanarak birbirlerine IPv6 paketi gönderebilmektedirler[37].

Bir ISATAP uç noktası ağ dışında bir nokta ile IPv6 haberleşmesi sağlamak istiyorsa paketlerin ağ dışına yönlendirilmesi gerekmektedir. Bu işi ISATAP yönlendiricisi yapmaktadır. ISATAP yönlendiricisi ISATAP uç noktası ile diğer ağdaki uç nokta arasındaki paketleri iletmektedir. ISATAP uç noktalar için varsayılan yönlendirici olmakta ve adres ön eklerini ilan etmektedir.

3.8.4.4 Teredo

Teredo tüneli, IPv4 NAT sistemi arkasında bulunan uç noktalara IPv6 bağlantısı sağlayabilmek için geliştirilmiştir. NAT içerisindeki IPv6 tünellemesi UDP paketleri kullanılarak yapılmaktadır. Teredo servisi NAT cihazlarının IPv6 yönlendirme yapamadıkları, 6to4 yönlendirici olamadıkları ve protokol 41 dönüşümü yapamadıkları durumlar için tanımlanmışlardır.

Teredo tünel yapısında aşağıdaki düğümler bulunmaktadır[40]:

- *Teredo sunucusu* – IPv6/IPv4 düğümüdür ve Teredo istemcilerinin Teredo adres yapılandırmasını sağlamaktadır. Teredo istemcilerinin kendi aralarında veya IPv6 düğümleriyle iletişimde ilk haberleşmeyi başlatmaktadır.
- *Teredo istemcisi* – IPv6/IPv4 düğümüdür. Teredo rölesi sayesinde gerçekleştirilen IPv6 paketlerinin iletimi sırasında Teredo arayüzlerini kullanılmaktadırlar.
- *Teredo rölesi* – IPv6/IPv4 yapısına sahip bir yönlendiricidir. Görevi Teredo istemcileri arasındaki veya Teredo istemcisi ve IPv6 düğümü arasındaki paket iletimini sağlamaktır.

- *Teredo uç nokta rölesi* (host specific relay) – IPv6/IPv4 olan bir düğümdür ve hem IPv6 hem IPv4 İnternet’e bağlantısı bulunmaktadır. Bu sayede Teredo istemcileri ile herhangi bir Teredo rölesi olmadan haberleşebilmektedir.

Teredo çok fazla kullanılan bir tünelleme mekanizması değildir. Eğer ortamda doğrudan IPv6 bağlantısı yoksa, 6to4 ve ISATAP tünellemeleri kullanılmıyorsa bu durumda Teredo kullanılmaktadır. Her geçen gün NAT sistemindeki protokol 41 desteği arttıkça Teredo tüneli sistemi kullanılmasına gerek kalmamaktadır.

4. IPV6'YA GEÇİŞ

Üçüncü bölümde IPv6 protokolü detaylı bir şekilde anlatılmıştır. Ancak burada anlatılan teorik bilgiyi daha iyi anlamak ve analiz edebilmek için IPv6 uygulamaları yapmak gerekmektedir. Yeni nesil protokolün her geçen gün daha da yaygınlaşmasıyla, sadece donanım geliştirenler değil yazılım geliştiricileri de bu konuda yoğun çalışmalara başlamışlardır. Yazılımcılar mevcut yazılımlarını IPv6'yı da destekleyecek şekilde güncellemektedirler.

IPv6 destekleyen uygulamalara bakıldığı zaman büyük bölümünün açık kaynak kodlu uygulamalar olduğunu görmekteyiz. Bu da çok şaşırtıcı değildir çünkü diğer yazılımlar ticari amaçlıdır, zorunda kalmadıkça bir güncellemeye gitmezler ve bu konuda masraf yapmak istemezler. Açık kaynak programcıları büyük oranda gönüllülerden oluşmaktadır ve programlar ticari kaygılar yerine insanların ihtiyaçları doğrultusunda geliştirilmektedir.

Test laboratuvarı kurmaktaki amacım orta ölçekli bir ağda bulunabilecek tüm servisleri IPv6'ya geçirip bu servisleri küçük bir ağda toplamaktır. Bu testin sonucu şu anda IPv6'ya geçişe ne kadar hazırlıklıyız onu belirleyecektir. Aynı zamanda üçüncü bölümde teorik olarak bahsedilen konuların uygulaması yapılmış olacaktır. Dünya çapında kabul edilen ve uygulanan yöntem, bir ağı IPv6'ya geçirmeden önce daha küçük ölçekli bir IPv6 test laboratuvarı kurmak ve ağdaki servisleri tek tek bu laboratuvarı denemektir. Bu şekilde denenen ve başarılı olunan servisler asıl servislerle yer değiştirmekte ve geçiş ağ hizmetlerini engellemeyerek son kullanıcı için son derece saydam bir şekilde olmaktadır.

IPv6'ya geçiş sürecini test eden bu laboratuvarı öncelikle altyapı olarak işletim sistemlerinin geçişi yapılmış, daha sonra IPv6 İnternet bağlantısı için başvurular gerçekleştirilmiştir. IPv6 bağlantısı sağlandıktan sonra sunucu servisleri kurulmuş ve IPv6 destekleyen birçok program test edilmiştir.

4.1 Ön Hazırlık

IPv6'ya geiş iin bir test laboratuvarı kurmaya karar verdikten sonra yapılması gereken ön hazırlıklar iyi bir planlama ve kullanılacak işletim sistemlerinin IPv6 desteğinin sağlanmasıdır. Bazı işletim sistemleri hiçbir ek yapılandırma yapmadan yeni nesil İnternet protokolünü desteklerken bazıları iin ek komutlar vermek gerekmektedir. Bu laboratuvarda özellikle istemci düzeyinde olabildiğince çeşitli işletim sistemi denenmeye çalışılmıştır.

4.1.1 Planlama

Planlama aşaması en önemli safhalardan bir tanesini oluşturmaktadır. Başlangıta yapılan plan doğrultusunda kurulumlar gerçekleşeceği iin bu aşamaya vakit ayırmakta fayda bulunmaktadır.

Çalışma sırasında karar verilmesi gereken konulardan bir tanesi hangi işletim sistemlerinin kullanılacağı ve istemci, sunucu bilgisayarlarının neye göre seçileceği idi. Öncelikle kullanılmak istenen işletim sistemleri seçildi. Bunlar; Windows XP, Windows 2003, beta aşamasında olan Windows Vista, Debian Sarge ve Tübitak'ın geliştirdiği ilk ulusal Linux işletim sistemi olan Pardus olarak belirlendi.

Daha sonra sıra sunucu işletim sistemlerini seçmeye geldi. Sunucuların Linux mu Windows mu olacağı sorusunun cevabı birçok denemeden sonra belirlendi. Sunucular iin bir GNU/Linux sürümü olan Debian Sarge (Debian 3.1) seçilmiştir. İstemci bilgisayarlar ve uygulama testleri iin de Windows sürümleri ve Pardus kullanılmıştır.

Planlamanın diğeri bir aşaması da IPv6 adres kaydı yaptırmak ve bu adreslerin sunuculara ve istemcilere nasıl dağıtılacağının belirlenmesidir. Bu aşamada IPv6 adres aralığı iin RIPE başvurusu yapılmıştır. RIPE Türkiye'nin de iinde bulunduğu bir alan dahilinde İnternet kayıtlarını tutan kuruluştur. Daha sonra SixXS IPv6 tüneli iin bu RIPE kaydı kullanılmaktadır. IPv6 tünel kaydı tamamlandıktan sonra /48'lik bir adres aralığı alınabilmektedir. Sunucu, istemci bilgisayarlarının IPv6 desteğinin sağlanması ve IPv6 tünelinin kurulması ile artık global bir IPv6 erişimi sağlanabilmektedir. En son olarak ağı ii servisleri kurmakta ve IPv6 destekleyen programları denenmektedir.

4.1.2 İşletim sistemlerinin yapılandırılması

Bir ağa IPv6 desteği sağlayabilmek için yapılan çalışmalarda işletim sistemleri yapılandırması çok önemli bir yer tutmaktadır. Çünkü IPv6'yı kullanacak olan kullanıcılar bunu işletim sistemi arayüzü ile yapacaklardır. Test laboratuvarı için seçilen işletim sistemleri GNU/Linux (Debian ve Pardus) ve Windows (XP, 2K3, Vista) sistemleridir.

4.1.2.1 Debian 3.1 yapılandırması

Bir GNU/Linux işletim sistemi olan Debian'ın en son kararlı (stable) sürümü 3.1'dir ve Sarge adı ile anılmaktadır. Linux işletim sistemi üç durumda olabilmektedir; kararlı (stable), test aşamasında (testing), kararsız (unstable). Bir program geliştirildiği zaman önce kararsız duruma girmektedir. Daha sonra belirli bir süre sonra test aşamasına alınmakta ve eğer testlerden başarı ile geçerse kararlı duruma geçmektedir. Sunucular için tavsiye edilen kararlı durum yüklemesi yapmaktır. Kararlı durumda programların sürümleri, kararsız ve test aşaması durumlarına göre daha eski olmaktadır ancak birçok denemeden geçtiği için sunucu gibi önemli konumlarda denenmiş sürümlerin kullanılması tavsiye edilmektedir.

Debian Sarge yüklemesi yaparken ilk aşamada linux26 komutu ile 2.6x çekirdek kurulumu yapılmıştır. Linux'larda 2.4x çekirdeğinden itibaren IPv6 desteği tam olarak gelmektedir. Ancak 2.4x çekirdekler bazı gelişmiş IPv6 özelliklerini sağlamamaktadırlar bu yüzden kurulumlar 2.6x çekirdek ile yapılmıştır.

Debian sunucularından bir tanesi IPv6 yönlendirici, bir tanesi Web sunucusu ve DNS sunucusu ve bir tanesi de e-posta sunucusu olarak kullanılmıştır. Otomatik yapılandırılan link-local adresini görmek için ifconfig komutu verilmektedir.

```
debian:~ # ifconfig
```

```
eth0    Link encap:Ethernet HWaddr 00:0D:60:65:E4:17
        inet addr:160.75.67.1 Bcast:160.75.x.255 Mask:255.255.255.0
        inet6 addr: fe80::20d:60ff:fe4b:f0a1/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:161060 errors:0 dropped:0 overruns:0 frame:0
        TX packets:17503 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:12835273 (12.2 MiB) TX bytes:1609340 (1.5 MiB)
        Interrupt:20 Base address:0x2000 Memory:e8100000-e8100038
```

```
lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING MTU:16436 Metric:1
        RX packets:982 errors:0 dropped:0 overruns:0 frame:0
        TX packets:982 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:103337 (100.9 KiB) TX bytes:103337 (100.9 KiB)
```

Şimdi “*ping6 ::1*” komutu vererek loopback adresine yankı isteği (echo request) göndermekteyiz. Bu şekilde IPv6 yapısının çalışıp çalışmadığı kontrol edilmektedir. Eğer yankı cevabı (echo reply) geliyorsa sistem içindeki IPv6 yapısı çalışıyor demektir. Debian yapılandırılması sunucu kurulumlarında daha detaylı olarak incelenecektir.

4.1.2.2 Pardus 1.0 yapılandırması

Ulusal işletim sistemi projesi 2003 yılının yazında ortaya çıkan bir fikirdir. Geliştiriciler Tübitak UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) bünyesinde toplanarak bu proje için ilk adımları atmışlardır. 1 Şubat 2005 tarihinde ilk çalışan CD, 26 Aralık 2005 tarihinde de ilk kurulabilir CD, Pardus 1.0 sürümü ile kullanıma açılmıştır.

Bu test laboratuvarında Pardus kullanılmasının ana sebebi açık kaynak kodlu işletim sistemlerinin dağıtım isminden bağımsız olarak IPv6 desteği sunabilirliğini test etmektir. Test için Pardus 1.0 kurulabilir sürüm 2.4x çekirdek kullanılmıştır.

Pardus işletim sistemi standart bir şekilde yüklendikten sonra “*ifconfig*” komutu ile IPv6 yığınının olup olmadığı kontrol edildi. Loopback arayüzü olarak *::1* ve her bir ethernet kartı için bir adet link-local adresi atanmışsa bu durumda IPv6 desteği vardır. Bu kontrol “*lsmod | grep ipv6*” komutu ile de yapılabilmektedir. Eğer *ipv6* ile başlayan bir satır varsa, çekirdekte *ipv6* desteği vardır denir. Pardus 1.0 sürümü 2.4x çekirdek ile IPv6 desteğinin gelmediği görüldü. Son olarak modül yapısında olabileceği ve sadece çağırıldığında yüklenebileceği varsayımı ile “*modprobe ipv6*” komutu verildi. Ancak böyle bir modül bulunmadığı sonucu ile karşılaşıldı.

Pardus’a IPv6 yığını yükleyebilmek için çekirdek derlenmesine karar verildi. Bu sebeple çekirdek sürüm 2.6.14.4-15 indirildi. Çekirdek ayarlarında bir program için üç seçenek bulunmaktadır. Bunlar; yüklensin, yüklenmesin veya modül olarak yüklensin seçenekleridir. Yeni çekirdek derlemesi için “*make menuconfig*” komutu

ile IPv6 yığını tamamen yüklenmek üzere seçildi. Daha sonra aşağıdaki komutlarla çekirdek derleme işlemi tamamlandı.

```
pardusAtUzem:~# make bzImage  
pardusAtUzem:~# make modules  
pardusAtUzem:~# make modules_install  
pardusAtUzem:~# cp /usr/src/linux-2.6.14.4-15/arch/i386/boot/bzImage /boot/kernel2.6-  
ipv6
```

Son olarak çekirdek imajı “/boot/grub/menu.list” dosyasına eklenmiştir ve bilgisayar yeniden başlatılmıştır. Açılış ekranında karşımıza çıkan grub penceresinden yeni çekirdek seçilerek bilgisayar başlatılacaktır. Son olarak,

```
pardusAtUzem:~# ifconfig eth0 add 2001:4BD0:2031::3/64
```

komutu ile IPv6 adresi eklenmekte ve test için “ping6 ::1” komutu verilmektedir. Yankı cevabının başarıyla geldiği gözlenecektir.

4.1.2.3 Windows yapılandırmaları

Laboratuvarda istemci olarak Windows XP (SP2’li), 2003 ve Vista işletim sistemleri test edilmiştir. Windows XP ve 2003 sonradan servis paketleri ile IPv6 desteği kazanmakta ve komut satırından “*ipv6 install*” veya “*netsh interface ipv6 install*” komutları verilerek IPv6 protokolünün yüklenmesi sağlanmaktadır. Bu işletim sistemlerinde ağ bağlantı özelliklerine bakıldığı zaman hem TCP/IP yığını hem de TCP/IPv6 yığını görülmektedir. Ayrı ayrı yer almasının sebebi IPv6 yapısının sonradan eklenmesidir.

Windows Vista Microsoft’un uzun süredir çıkaracağını duyurduğu ve ertelediği yeni nesil işletim sistemidir. Şu anda beta sürümleri bilişim uzmanları tarafından test edilmekte, asıl sürümü piyasada bulunmamaktadır. Bu laboratuvarda da önce Vista Beta 1 denenmiş sonra da Beta 2’ye yükseltilmiştir. Vista’da IPv4 ve IPv6 tek bir protokol yığını olarak TCP/IP başlığı ile görünmektedir. Microsoft’un IPv6’yı tam destekleyen işletim sistemi olarak lanse edilmiştir. En önemli özelliklerinden biri de IPv6 yapılandırması için komut satırının yanında görsel arayüzün de kullanılabilmesidir. Aynen IPv4’teki gibi IPv6 adresi, varsayılan geçit ve isim sunucusu bir arayüz ile yapılandırılabilir.

Windows Vista'daki geliřtirmelerden bir tanesi de Teredo tnelinin varsayılan olarak gelmesidir. Teredo, XP ve 2003'te aktif edilmiř durumda deęildir. Ayrıca Vista hem IPv4 hem de IPv6'yı destekleyen ateř duvarı (firewall) ile birlikte gelmektedir[41].

Windows XP, 2003 ve Vista iin el ile yapılandırma komutları ařaęıdaki gibidir[42]:

- *ipconfig /all*
Bilgisayardaki tm IP adresi yapılandırmasını arayzlerin fiziksel adresleri ile birlikte detaylı bir biimde gstermektedir.
- *netsh interface ipv6 show address*
Bilgisayardaki aę arayzlerine atanmıř tm IPv6 adreslerini ve trlerini gstermektedir.
- *netsh interface ipv6 set address "Local Area Connection" "ip adresi"*
"Local Area Connection" isimli aę arayzne IPv6 adresi atamak iin kullanılmaktadır.
- *netsh interface ipv6 add dns "Local Area Connection" 2001:4BD0:2031::10*
"Local Area Connection" arayz iin dns sunucusu belirtilmektedir.
- *netsh interface ipv6 show neighbors*
Komřu dęmleri gstermektedir.
- *netsh interface ipv6 show routes*
Bilgisayarın ynlendirme tablosunu gstermektedir.
- *netsh interface ipv6 add route ::/0 "Local Area Connection" 2001:4BD0:2031::1*
Bu komutta ::/0 ynlendirme listesinde olmayan dięer tm baęlantıları ifade etmektedir. 2001:4BD0:2031::1 adresi de ipv6 aę geidi(gateway) adresini belirtmektedir. Aynı řekilde "add" yerine "delete" komutu ile o kayıt ynlendirme tablosundan silinebilir.
- *netsh interface ipv6 set interface interface="Local Area Connection" firewall=enabled*
IPv6 arayz iin ateř duvarını aktifleřtirmek iin kullanılmaktadır. Ateř duvarını kapatmak iin "enabled" yerine "disabled" yazılması gerekmektedir.

4.2 IPv6 Eriřimi Saęlama

IPv6 eriřimi saęlamanın iki yolu bulunmaktadır. Bir İnternet servis saęlayıcı (ISP – Internet service provider) yardımıyla doęrudan IPv6 baęlantısı saęlanabildięi gibi tünel hizmeti sunan bir řirketin baęlantısını kullanarak da ile IPv6 eriřimi saęlanabilmektedir. Bu iki yöntemin birbirine göre avantaj ve dezavantajları bulunmaktadır.

Doęrudan saęlanan IPv6 baęlantıları tünelleme mekanizmalarına göre daha büyük bant geniřlięi saęlamaktadırlar. Özellikle tünel son noktası tünel bařlangıç noktasına göre çok uzakta ise baęlantı hızı o ölçüde düşük olmaktadır. Ancak doęrudan IPv6 baęlantısı kurmak bazı durumlarda zor olabilmektedir. Tüm alt aę yapısının ve yerel alan aęındaki yönlendiricilerin IPv6 destekleyecek řekilde güncellenmesi gerekmektedir. Tünel mekanizmasında ise tünel kuracak yönlendirici bir alt aęa kurulduktan sonra, hiyerarřik olarak daha üst yönlendiricilerin IPv6 desteęi sunması gerekmemektedir. Bu řekilde yazılım geliřtiriciler, sistem yöneticileri ve donanım test edenler için daha masrafsız ve kurulması daha kolay bir IPv6 eriřimi saęlanmış olmaktadır.

Burada bahsedilen test laboratuvarı kapsamında yukarıdaki iki yöntem üstünde iyice düşünölmüş ve daha sonra tünel mekanizması kurulmasına karar verilmiştir. Bunun sebebi doęrudan IPv6 baęlantısı saęlayabilmek için İstanbul Teknik Üniversitesi'nin (İTÜ), Ulusal Akademik Aę'dan (UlakNet) IPv6 baęlantısı isteęinde bulunması ve adres aralıęı talep etmesi gerekmektedir. Ayrıca İTÜ aęında bulunan birçok donanımın ve yazılımın güncellenmesi gibi yoğun bir çalışma gerektirmektedir. İTÜ aęının yönetiminin Bilgi İşlem Daire Başkanlıęı'nda (BİDB) olması ve sadece IPv6 baęlantısı saęlayabilmek ařamasında birçok deęişik güncelleme ile uğrařılmak zorunda kalınacaęı sebebiyle bu yöntem seçilmemiřtir.

Tünel mekanizması kullanılmasına karar verildikten sonra Uzaktan Eęitim Merkezi'nde (UZEM) bir tane bilgisayara Debian Sarge işletim sistemi yüklenmiş ve bu bilgisayar UZEM aęını IPv6 İnternet'e çıkaran yönlendirici olarak belirlenmiştir. Yapılandırmaların UZEM yerel alan aęı içinde yapılması İTÜ BİDB'ye olan baęımlılıęın azalmasını ve hareket esneklięini saęlamıştır. BİDB'den sadece Debian yönlendirici ile ilgili bir eriřim ayarı yapılması istenmiştir.

4.2.1 RIPE kaydı

RIPE NCC (Réseaux IP Européens Network Coordination Centre) İnternet kayıtlarını tutan bölgesel dört tane kuruluştan bir tanesidir. RIPE NCC teknik koordinasyon sağlayarak İnternet altyapısını destekleyen, kar amacı olmayan bağımsız bir organizasyondur. En yoğun kullanılan hizmeti kendi bölgesinde bulunan üyelere IPv4, IPv6 ve AS numaraları konularında bölgesel İnternet kayıtları sunmasıdır. Üyeler genellikle İnternet servis sağlayıcıları, telekomünikasyon kurumları ve büyük şirketlerden oluşmaktadır. Hizmet verdiği alanlar Avrupa, Orta Doğu ve Asya'nın bazı bölümleridir[43].

IPv6'ya geçiş aşamalarından bir tanesi IPv6 adres aralığı edinmektir. Bu adres aralığını alabilmek için Türkiye'nin içinde bulunduğu alana hizmet sunan RIPE NCC'nin Whois veri yapısına kayıt olmak gerekmektedir. Bu adres aralığında bulunan adreslerden herhangi bir tanesi Whois veri bankasında sorgulandığı zaman, bu adresin yönetiminin benim tarafımdan sağlandığı ve iletişim bilgilerim bulunmaktadır.

RIPE NCC'den “*nic-hdl: MS11188-RIPE*” kodlu bir kayıt oluşturuldu. Bu kayıt oluşturulurken “*mnt-by*” ve “*auth*” gibi veriler girilirken biraz zorlanılmış ve bu konularda araştırma yapılmak zorunda kalınmıştır. Oluşturulan kayıt Whois veri yapısında aşağıdaki şekilde tutulmaktadır.

person :	Mustafa Sahin
address:	dereboyu cad. 63/65
address:	istanbul/Turkey
mnt-by:	MUSTAFA-MNT
e-mail:	mustafa@uzem.itu.edu.tr
phone:	+902122853024
nic-hdl:	MS11188-RIPE
source:	RIPE # Filtered

4.2.2 SixXS tünel başvurusu

SixXS (Six Access), yerel İnternet kayıtları (LIR) için ücretsiz hizmet sunmaktadır. En önemli hedefi firmalara altyapılarında çok büyük değişiklikler yapmadan IPv6 erişimi sağlamak ve bu şekilde IPv6'nın gelişimine katkıda bulunmaktır. Sunulan tünel servisi aynı zamanda araştırma ve geliştirme amaçlı olarak da çok yoğun olarak kullanılmaktadır.

SixXS başvurusu yapmak için RIPE NCC'den alınan MS11188-RIPE kaydı kullanılmıştır. Başvuru nedeni detaylı bir şekilde ilgili kişiye anlatıldıktan sonra başvuru kabul edilirse verilen nic-hdl'a karşılık bir şifre gönderilmektedir. Bu şifre ile SixXS Web sitesine giriş yapılmakta ve bir tünel isteği gönderilmektedir. İki çeşit tünel mekanizması bulunmaktadır. Dinamik veya statik tünel seçilebilmektedir. Dinamik tünelin kurulması daha kolaydır ve tünel kullanılmadığı zaman otomatik kapanmaktadır. Statik tünel ise statik bir IP adresine ihtiyaç duymakta ve yönlendiricinin hiçbir zaman kapanmamasını gerektirmektedir. Test laboratuvarında daha kararlı bir yapı ve uç noktaları inceleme olanağının bulunması açısından statik tünel kullanımı seçilmiştir.

4.2.3 IPv6 tüneli kurma

Şimdi sıra yönlendirici için seçilen Debian Sarge için yönlendirici yazılımını yüklemek ve yapılandırmasını yapmaya geldi. "http://www.sixxs.net/archive/sixxs/aiccu/debian/unstable/aiccu_current.deb" adresinden indirilen Debian paketi "*dpkg -i*" komutu ile yüklenmektedir. Yapılandırma için "*/etc/aiccu.conf*" dosyası kullanılmaktadır. Yapılandırmada önemli satırlar aşağıda belirtildiği gibi oluşturulmak zorundadır.

```
# AICCU Configuration/Yapılandırması
# Login information/ Oturum açma bilgisi
username MS11188-RIPE
password *****

# Interface names to use/ Kullanılacak ağ arayüzleri
ipv4_interface eth1
ipv6_interface sixxs

# Be verbose?
verbose false
```

Bu yapılandırma dosyasında "#" ile başlayan satırlar yorum veya açıklama satırları, diğer satırlar komut satırlarıdır. RIPE NCC kaydı ve SixXS tarafından bu kayıt ile eşleştirilen şifre doğru girilmelidir yoksa bağlantı kurulmayacaktır. Yapılandırma dosyasındaki en önemli alan arayüz belirtme ayarıdır. Yönlendiriciler yapısı gereği en az iki ağ arayüzünden oluşurlar. Bir arayüzden aldıkları paketleri diğer arayüze aktarmaktadırlar.

Kurmakta olduğumuz yönlendiricide de iki tane ağ arayüzü bulunmaktadır. Bir tanesi UZEM IPv6 ağına bağlı ve ismi eth0 diğeri de tünel bağlantısında kullanılmakta ve eth1 olarak isimlendirilmektedir. Aiccu programı ile birlikte bir de sanal sixxs

arayüzü oluşmuştur. Yani iki adet fiziksel arayüz ve loopback dahil iki adet de sanal arayüz oluşmuştur. Yukarıdaki yapılandırma dosyasında tünelin IPv4 arayüzü olarak eth1, IPv6 arayüzü olarak da sixxs arayüzü belirtildi.

Tünel kurulurken seçilmesi gereken özelliklerden birisi de POP noktasıdır. Tünel kurulacak yerle POP arasındaki en hızlı bağlantıya sahip yer tünelin son noktası olarak seçilmelidir. Bu seçimde kullanılan yöntem tüm POP noktalarına ping atmak ve geri dönen cevaplara bakarak en kısa süreli yankı cevabının bulunduğu noktayı POP olarak seçmek olmuştur. Yönlendiriciden yapılan testler sonucunda Londra'daki gblon01 POP noktası tünel son noktası olarak seçilmiş ve İstanbul ile Londra arasında bir tünel kurulmuştur. Tünel bilgileri aşağıdaki gibidir:

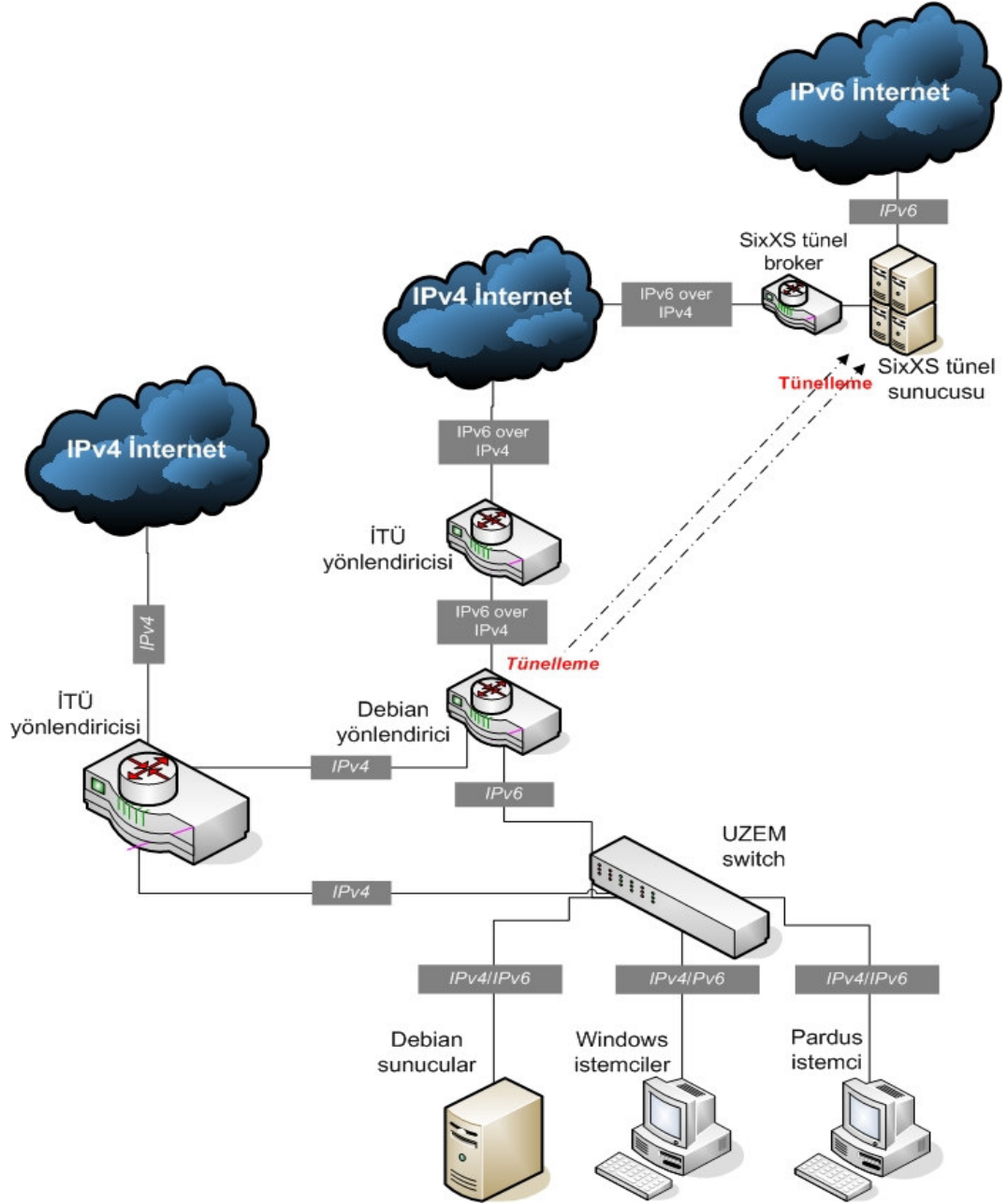
PoP ismi	gblon01
PoP son nokta	Londra, İngiltere 
PoP IPv4	85.116.5.101
Yönlendirici yeri	İstanbul, Türkiye 
Yönlendirici IPv4	160.75.67.89
IPv6 ön eki	2001:4BD0:2000:7a::1/64
PoP IPv6	2001:4BD0:2000:7a::1
Yönlendirici IPv6	2001:4BD0:2000:7a::2

Tüneli test etmek için POP IPv6'ya ping atılabilir. “*ping6 2001:4BD0:2000:7a::1*” komutunu verdikten sonra ping cevabı geliyorsa tünel çalışıyor demektir. Daha sonra yönlendiricinin IPv6 İnternet'e çıkışını test etmek için “*ping6 www.kame.net*” cevabına bakılabilir. Kame, IPv6 Web sitesi olan Unix sistemlere IPv6 desteği kazandırmak için geliştirilen bir projedir. Kame sayfasına girildiğinde eğer IPv6 kullanılıyorsa hareketli bir kaplumbağa görülmekte, IPv4 ile bağlanıldıysa kaplumbağa resmi hareket etmemektedir.

4.2.4 IPv6 /48 adres aralığı alma

RIPE NCC ve SixXS kayıtları yapıldıktan ve yönlendirici yazılımı kurulup, yapılandırıldıktan sonra sıra SixXS tüneli IPv6 adres aralığı başvurusuna geldi. Bu başvuruda /32 ve /48 seçenekleri bulunmaktadır. /48 ön eki 2^{16} adet alt ağ ve her alt ağda 2^{64} adet IPv6 adresi anlamına gelmektedir. Test laboratuvarı için /48 ön eki fazlasıyla yeterli görülmüştür. Alt ağ başvurusu ile birlikte 2001:4BD0:2031::/48 adres aralığı belirtilen tünel için ayrılmıştır. IPv6 adresleri ağ içindeki diğer düğümlerin de IPv6 İnternet'e çıkabilmeleri için sunuculara el ile, istemcilere de otomatik olarak atanmak üzere artık hazırdır.

4.2.5 IPv6 Tüneli Yapısı



Şekil 4.1: UZEM - SixXS tüneli

UZEM (Uzaktan Eğitim Merkezi) ile SixXS tünel broker arasında kurulan tünelin yapısı şekil 4.1’de gösterildiği gibidir. UZEM ağında bulunan düğümler IPv4/IPv6 çift IP katmanlı yapıda olup, kendi aralarında istenildiği zaman IPv6, istenildiği zaman IPv4 haberleşmektedirler. IPv4 İnternet’e geleneksel yoldan yani varsayılan

geçit olan İTÜ yönlendiricisinden çıkmaktadırlar. Aynı şekilde Debian yönlendirici de çift IP katmanlı yapıdadır ve IPv4 İnternet'e İTÜ yönlendiricisinden çıkmaktadır.

Yukarıdaki mimari tünel broker (TB) tarafından incelendiğinde tünel istemcisi Debian yönlendirici olmaktadır. Tünel kurulacağı zaman TB, kimlik doğrulama ve yetkilendirme yapabilmek için istemciye bazı kimlik bilgilerine ihtiyaç duymaktadır. İstemci, yetkilendirme tamamlandıktan sonra şu bilgileri sağlaması gerekmektedir: tünel tarafındaki IPv4 adresi, DNS kaydı için bir isim ve istemci türü (yönlendirici veya uç nokta).

Eğer kurulan tünelde istemci makine bir yönlendirici ise ve IPv6 bağlantısını bir dizi uç noktaya sağlamak amaçlı ise, istemci TB'ye kullanacağı adres aralığını belirtmek zorundadır. Bu sayede TB istemcinin ihtiyaçları doğrultusunda tünel için atayacağı adres aralığını belirlemekte. Test laboratuvarı için kurulan tünelde uç noktalara dağıtılmak üzere alınan adres aralığı 2001:4BD0:2031::/48'dir.

Tünel kurma başlangıcında TB, tünel son noktası olarak bir tane tünel sunucusu belirlemektedir. İstemciye atanacak IPv6 adres aralığını belirlemekte, bu bilgiyi sunucu ve istemciye bildirmektedir. Tünel uç nokta adreslerinin DNS kaydının otomatik olarak yapmaktadır. Sunucu tarafının yapılandırmasını tamamlamakta ve son olarak tünelle ilgili tüm bilgileri istemci tarafa iletmektedir[44].

4.3 IPv6 Adres Dağıtımı

IPv6 tünelinin kurulması ile tünelin UZEM ucundaki yönlendirici IPv6 İnternet'e erişmeye başlamış olmaktadır. Bundan sonraki amaç tüm UZEM ağının IPv6 İnternet'e erişmesidir. Bunu sağlamak için uç noktaların çift IP katmanlı yapıda olması ve IPv6 adresi, yönlendirme bilgileri gibi bazı ayarların yapılandırılması gerekmektedir. Tüm uç noktalar Debian yönlendiricisi üzerinden IPv6 İnternet'e erişecekleri için IPv6 için varsayılan geçitleri bu yönlendirici olacaktır.

Düğümlere IPv6 adres dağıtımı için kullanılabilecek üç yöntem bulunmaktadır. Adresler işletim sistemine bağlı olarak değişen komutlar yardımıyla komut satırından el ile girilebildiği gibi sunuculu veya sunucusuz otomatik adres dağıtımı da kullanılabilmektedir. El ile yapılandırma çok zor olmasa da orta ve büyük ölçekli ağlarda uç nokta sayısına bağlı olarak yönetimsel bir zorluk yaratmaktadır.

Genellikle sunucu cihazları ve yönlendiriciler el ile yapılandırılmakta, istemciler otomatik olarak yapılandırılmaktadır.

4.3.1 El ile yapılandırma

Ağ yöneticisi eğer bir bilgisayara adres planlamasına göre belirlediği bir IP adresini atamak istiyorsa bu adresi el ile yapılandırmaktadır. El ile yapılandırmaya statik yapılandırma da denilmektedir çünkü atanan IP adresi statik olmakta ve hiçbir zaman değişmemektedir. Sunucuların DNS kayıtları tutulduğu için, yönlendiricilerin de varsayılan geçit (default gateway) görevi görmeleri nedeniyle adres atamaları statik yapılmaktadır. Ayrıca bu adreslerin bir kere kayıtları tutulduktan sonra hiç değiştirilmemesi beklenmektedir.

Windows işletim sistemlerinde en temel adres yapılandırması için aşağıdaki komutlar kullanılmaktadır. Birinci komut “*Local Areal Connection*” ağ arayüzüne IPv6 adresi eklemek, ikinci komut aynı arayüz için IPv6 DNS sunucusunu tanımlamak ve üçüncü komut da IPv6 İnternet’e çıkabilmek için kullanılacak yönlendiriciyi belirtmek için kullanılmaktadır.

```
netsh interface ipv6 set address "Local Area Connection"
2001:4BD0:2031::10
netsh interface ipv6 add dns "Local Area Connection" 2001:4BD0:2031::10
netsh interface ipv6 add route ::/0 "Local Area Connection"
2001:4BD0:2031::1
```

Windows’un en son sürümü Vista’da bu ayarları yapmak için görsel bir arayüz sunulmaktadır. Bu arayüz sayesinde ilgili boşluklara sadece IPv6 adresleri girilmekte böylelikle bu uzun komutlar kullanılmak zorunda kalınmamaktadır. Windows XP ve 2K3’te böyle bir arayüz bulunmamaktadır.

Debian ve Pardus GNU/Linux işletim sistemleri için adres atanacak ağ arayüzünün eth0 ile isimlendirildiği varsayımı altında verilmesi gereken komut, “*ifconfig eth0 add 2001:4BD0:2031::10/64*” veya “*ip addr add 2001:4BD0:2031::10/64 dev eth0*” şeklindedir. Eth0 arayüzünden IPv6 adresini silmek için aynı komutta “*add*” yerine “*del*” yazılmaktadır. IPv6 için varsayılan geçidi ayarlayarak İnternet’e çıkabilmek için verilecek komut “*route -A inet6 add default gw 2001:4BD0:2031::1*” şeklindedir.

Uç noktanın yönlendirme tablosunu görmek için Linux işletim sistemlerinde “*ip -6 route*” komutunu vermek yeterlidir.

```
2001:4bd0:2031::/48 dev eth0 proto kernel metric 256 expires 2109251sec mtu
1500 advmss 1440 hoplimit 4294967295
fe80::/64 dev eth0 metric 256 expires 21263230sec mtu 1500 advmss 1440
hoplimit 4294967295
ff00::/8 dev eth0 metric 256 expires 21263230sec mtu 1500 advmss 1440 hoplimit
4294967295
default via 2001:4bd0:2031::1 dev eth0 metric 1 expires 21263354sec mtu 1500
advmss 1440 hoplimit 4294967295
default dev eth0 metric 256 expires 21263345sec mtu 1500 advmss 1440 hoplimit
4294967295
```

Varsayılan (default) çıkışları ağ içinde bulunmayan bir adrese ulaşmak için kullanılmaktadır. En alt iki satırda belirtildiği gibi ağ dışına (İnternet’e) çıkmak için varsayılan geçidin IPv6 adresi olan 2001:4BD0:2031::1 kullanılmaktadır.

Tünelin UZEM son noktasını oluşturan yönlendiricinin iki ağ arayüzü vardır. Bir tanesi tünel kurmak için kullandığı IPv4 arayüzü, diğeri de UZEM test laboratuvarındaki ağa bağlı arayüzünün IPv6 adresi. Bu IPv6 adresi 2001:4BD0:2031::1’dir ve UZEM içindeki uç noktalar IPv6 çıkışı için varsayılan yönlendirici tanımlarken bu adresi kullanmaktadırlar.

Son olarak DNS sunucusunu el ile ayarlamak için laboratuvarında kullanılan GNU/Linux işletim sistemlerinde /etc/resolve.conf dosyasında değişiklik yapılması gerekmektedir. Belirtilen dosyada en başa “*nameserver 2001:4bd0:2031::10*” satırı eklenmelidir. Burada 2001:4bd0:2031::10 adresi birazdan kurulumu anlatılacak olan IPv6 DNS sunucusun adresidir.

4.3.2 Sunuculu adres dağıtımı

Sunuculu (stateful) IP adresi dağıtımı hem IPv6 hem de IPv4 için çok kullanılan bir yöntemdir. IPv4 için el ile yapılandırma yapmak istenmiyorsa geriye kalan tek IP dağıtım yöntemidir. Genellikle orta ve büyük ölçekli ağlarda tercih edilmektedir. IP adresi dağıtımı bir sunucu kontrolünde ve belirli bir düzene göre yapılmaktadır. Sunuculu yöntemde adres dağıtımı haricinde birçok yapılandırma parametresi de istemcilere dağıtılabilmekte bu da ağ yöneticilerinin işini büyük ölçüde kolaylaştırmaktadır.

Sunuculu adres dağıtımı için dinamik uç nokta yapılandırma protokolü DHCP kullanılmaktadır. DHCPv6 bu protokolün IPv6 için geliştirilen yeni sürümüdür. İstemci ve sunucu arasında değiş tokuş edilen DHCP mesajları UDP kullanılmaktadır.

Sunuculu adres yapılandırması ve DHCPv6 bölüm 3.7.2’de detaylı olarak anlatılmıştır.

Test laboratuvarında hem sunuculu hem de sunucusuz adres yapılandırılması denenmek istenmiştir. DHCPv6 sunucusu için işletim sistemi olarak Windows XP, program olarak Dibbler sunucusu kullanılmıştır. Dibbler hem Linux hem de Windows işletim sistemlerinde çalışabilen kolay uygulanabilen bir DHCPv6 uygulamasıdır. İstemciler için de Dibbler istemci programı kullanılmıştır. Sunucu için “<http://klub.com.pl/dhcpv6>” Web adresinden Windows XP sunucu programı indirilmiş ve yüklemesi yapılmıştır. İstemciler için de gene aynı adresten uygun işletim sistemi yazılımları indirilmiş ve yüklenmiştir.

Windows XP’ye yüklenen Dibbler server programının yapılandırması server.conf dosyasından yapılmaktadır.

```
log-level 7
log-mode short

iface "IPv6 Dhcp Sunucusu"{
    T1 1800
    T2 2000
    preferred-lifetime 3600
    valid-lifetime 7200

    class {
        pool 2001:4BD0:2031::30 - 2001:4BD0:2031::ff
    }
    option dns-server 2001:4BD0:2031::10
    option domain mustafa.ipv6
    option ntp-server 2001:4BD0:2031::9
}
```

“*Log-level*” gerçekleşen olayların kayıtlarının tutulması ile ilgili bir komuttur. Değerinin 7 olması hata düzeltme kayıtlarının tutulmaması ayarını ifade etmektedir. T1 değeri saniye olarak istemcinin sunucuya ne kadar süre sonra adres yenileme mesajı göndereceğini bildirmekte, T2 ise istemcinin o adresi yeniden kullandığına dair mesaj gönderme aralığını ifade etmektedir.

Yapılandırma dosyasında en önemli parametre pool’dur. Pool ile adres havuzu belirlenmekte ve adres dağıtımı bu havuz içinde yapılmaktadır. Test laboratuvarında son 8 biti 30 ile 255 arasında olan 225 adet adres dağıtımı uygun görülmüştür. Daha

sonra isteğe bağılı olarak isim sunucusu, zaman sunucusu gibi yapılandırma verileri de “*option*” komutu ile istemcilere gönderilebilmektedir.

Dibbler üç adet programla gelmektedir. Dibbler sunucusu yapının ana bileşenidir. Dibbler rölesi aynı link içinde olamayan uç noktalara aynı sunucu ile adres yapılandırılmasını sağlamaktadır. Dibbler istemcisi de sunucunun gönderdiği yapılandırma bilgilerini alarak adresleri ilgili arayüzlere atamaktadır. Windows’ta Dibbler’i başlatmak için `dibbler-server.exe` ve `dibbler-client.exe` programları çalıştırılmalıdır. Ayrıca WinXP (SP2’li) sunucuda DHCPv6 UDP paketlerinin geçebilmesi için “*netsh firewall set adapter “IPv6 Dhcp Sunucusu” filter=disable*” komutu verilmektedir. Linux işletim sistemi için `dibbler-client` (`dibbler-server/dibbler-relay`) start/stop komutu verilmektedir.

İstemci yapılandırma dosyası sunucuya göre oldukça basittir. Sadece hangi ağ arayüzünün kullanılacağı seçilmektedir, geriye kalan işlemler sunucu tarafında belirlenmiştir.

Dibbler programı ile birlikte aynı zamanda birde DHCPv6 rölesi gelmektedir. Eğer tek bir DHCP sunucusu aynı linkte bulunmayan istemciler için kullanılacaksa o istemcilerin bulunduğu yere bir röle kurulmaktadır. Röle DHCP sunucusu ile istemcisi arasındaki iletişimi sağlamaktadır.

Dibbler DHCPv6 sunucusu ağ üzerinde başarılı bir şekilde çalışmıştır. Daha geniş ağlar için daha detaylı yapılandırmalar yapılabilmekte ve ağ yöneticisinin yapılandırma zamanını çok kısaltmaktadır. Dikkat edilmesi gereken konu sunuculara atanan statik adresler asla DHCP havuzu içinde olmamalıdır. Yoksa adres çakışması yaşanacaktır.

4.3.3 Sunucusuz adres dağıtımı

Sunucusuz otomatik (stateless) adres yapılandırması IPv6’nın IPv4’e göre getirdiği yeniliklerden bir tanesidir. Küçük ve orta büyüklükteki ağlar için çok kullanışlıdır. Bu tarz adres yapılandırması için herhangi bir sunucu kullanılmamakta sadece yönlendiricide bazı ayarlar yapılmaktadır. İstemcide ise hiçbir ayar yapılmamaktadır. Detaylı açıklama bölüm 3.7.1’de yapılmıştır.

Test laboratuvarında yönlendirici Debian işletim sistemi üzerinde olduğu için sunucusuz adres dağıtımı da bu bilgisayar üzerinden yapılacaktır. Debian program

deposunda bu işi yapmak için RADVD (Router ADVERTISEMENT Daemon) programı bulunmaktadır. Debian “*apt-get install radvd*” komutu ile RADVD yönlendiriciye yüklenmiştir. Daha sonra yapılacak tek işlem /etc/radvd.conf dosyasında bulunan yapılandırma dosyasına dağıtılmak istenen adres ön ekinin belirtilmesidir.

```
interface eth0 {
    AdvSendAdvert on;

    prefix 2001:4bd0:2031:aaaa::/64 {
        AdvPreferredLifetime 3600;
        AdvValidLifetime 7200;
        AdvSourceLLAddr on;
    };
};
```

“*AdvSendAdvert on*” komutu RADVD’nin yönlendirici ilanı (RA) göndermesini sağlamaktadır. Bu değer “*off*” yapılırsa RADVD çalışmayacaktır. “Prefix” komutundan sonraki küme parantezi içine “*AdvOnLink*” ve “*AdvAutonomous*” parametreleri girilebilmektedir. Varsayılan olarak ikisi de “*on*” değerini almaktadır. Bu sebeple yapılandırma dosyasında ayrıca belirtilmemiştir. “*AdvOnLink*” yönlendiriciden RA alan bir istemcinin aynı ön eke sahip tüm uç noktalara yönlendiricinin bulunduğu ağ arayüzünden erişebileceğini varsaymasını sağlamaktadır. “*AdvAutonomous*” belirtilen ön ekin otomatik adres yapılandırılmasında kullanılabileceğini ifade etmektedir[45].

Sunucusuz adres yapılandırması test edilmek için laboratuvarında kullanılmıştır. Herhangi bir işletim sistemine IPv6 desteği sağlandıktan sonra istemcinin belirtilen ön eke göre IPv6 adresi ve yönlendirme bilgilerini aldığı gözlemlenmiştir.

4.4 IPv6 Sunucularının Kurulumu

Bir ağda en önemli bileşenlerden bir tanesi de sunuculardır. Ağ içinde ve dışında kullanıcılara hizmet veren sunucular artık İnternet ve İntranet’in vazgeçilmez birleşenleri haline gelmiştir. Test laboratuvarında IPv6 İnternet bağlantısını tüm uç noktalara sağladıktan sonra sıra sunucuların ağ içine ve ağ dışına IPv6 hizmeti sunacak şekilde kurulmasına ve yapılandırılmasına gelmiştir.

İlk kurulacak sunucu IPv6 için önemi büyük olan alan adı sistemi (DNS) sunucusudur. IPv6 adreslerinin IPv4’e göre dört kat uzun olması ve bu sebeple akılda tutulmasının neredeyse imkânsız olması nedeniyle DNS bir IPv6 ağı için bu kadar

önemli olmaktadır. Daha sonra test laboratuvarı için IPv6 Web, e-posta, FTP sunucuları kurulacak ve bu sunucuların yedeklemesi yapılacaktır.

4.4.1 IPv6 isim sunucusu BIND

Alan adı sistemi (DNS) İnternet'in vazgeçilmez servislerinden biri haline gelmiştir. İnternet tarayıcısına yazılan her İnternet adresine karşılık düşen bir IP adresi vardır ve veri iletimi bu IP adresleri sayesinde olmaktadır. Dolayısıyla İnternet adreslerini IP adreslerine çevirecek bir sisteme ihtiyaç duyulmaktadır. Bu ihtiyacı DNS sunucuları gidermektedir. DNS sadece isimleri IP adreslerine çevirmekle kalmayıp aynı zamanda e-posta yönlendirmesi ve dosya transfer protokolü (FTP) erişimi gibi diğer bazı hizmetleri de sağlamaktadır. DNS, UDP ve TCP 53 portlarını kullanmaktadır.

Bu laboratuvarıda IPv6 desteği olması ve Debian deposunda paketinin bulunması sebebiyle DNS sunucusu olarak BIND9 (The Berkeley Internet Name Domain) seçilmiştir. Debian Sarge işletim sisteminde “*apt-get install bind9*” komutu ile yüklenmiştir.

Web tarayıcısına herhangi bir İnternet sitesi adresi girildiği zaman işletim sisteminde tanımlı DNS sunucusuna o adresin ilişkilendirildiği A kaydı (A record) sorulmaktadır. A kayıtları IPv4 adresleri ile isimleri eşleştirmektedir. DNS'te IPv6 desteği için öncelikle 32 bitlik IPv4 adreslerini tutan A kayıtları, 128 bitlik IPv6 adresini tutan AAAA (quad-A) kayıtları şeklinde değiştirilmiştir. Aynı isme ait hem A hem de AAAA kaydı tutulabilmektedir. Bu isim DNS sunucunda sorgulandığı zaman sunucu hem IPv4 hem IPv6 adresini istemciye göndermekte, istemci de bazı kurallara göre tercih ettiği adresi kullanmaktadır.

BIND isim sunucusu yüklendikten sonra ağ ile ilgili birçok yapılandırma yapılması gerekmektedir. Gerekli yapılandırmanın yapılabilmesi için de ağdaki tüm sunucuların görevlerinin ve IP adreslerinin belirlenmiş olması gerekmektedir. Ayrıca eğer istemcilere de isim kaydı sağlanmak isteniyorsa onlara ilişkin isim IP adresi eşleştirilmesi de tamamlanmalıdır.

BIND yapılandırma dosyaları “*/etc/bind*” dizininde bulunmaktadır. “*named.conf*” dosyası BIND'in ana yapılandırma dosyasıdır ve alt dosyalara ihtiyaç duymaktadır. DNS yapılandırması sırasında bu alt dosyalar tek tek hazırlanmaktadır. DNS iki çeşit kayıt tutmaktadır; adresten IP'ye çeviren kayıtlar ve ters kayıtlar (reverse records).

“named.conf” dosyası içeriğinin bir kısmı aşağıdaki şekildedir.

“*named.conf*” dosyası içinde zone “.” ifadesi ile “*db.root*” kök sunucuları tanımlanmıştır. Ayrıca “*db.local*” dosyası ile ters loopback kaydı tanımlanmış ve ağda bulunan düğümlerin ters kayıtlarının “*db.reverse6*” dosyasında bulunduğu belirtilmiştir. En alt satırda da “*named.conf.local*” dosyasının çağırılma komutu verilmiştir. Bu dosya isim kayıtlarının olduğu “*db.mustafa.ipv6*” dosyasını belirtmektedir. “*db.mustafa.ipv6*” dosyasının içeriği aşağıdaki gibidir.

81

mustafa	A	160.75.67.71
ns	AAAA	2001:4bd0:2031::10
ns	A	160.75.67.88
posta	AAAA	2001:4bd0:2031::11
posta	A	160.75.67.86
ftp	AAAA	2001:4bd0:2031::9
ftp	A	160.75.67.93
wwws	AAAA	2001:4bd0:2031::9
wwws	A	160.75.67.93
vista	AAAA	2001:4bd0:2031::5
vista	A	160.75.67.94
pardus	AAAA	2001:4bd0:2031::3
pardus	A	160.75.67.92
videokonferans1	AAAA	2001:4bd0:2031::20
videokonferans1	A	160.75.67.183
videokonferans2	AAAA	2001:4bd0:2031::21
videokonferans2	A	160.75.67.90
www	CNAME	ns
mail	CNAME	posta

Bu dosyada ilk olarak NS (Name Server) olarak ns.mustafa.ipv6 isim sunucunun ve MX (Mail eXchange) olarak da mail.mustafa.ipv6 e-posta sunucusunun kullanılacağı belirtilmektedir. Bazı zaman parametrelerinden sonra isim kayıtları bölümü gelmektedir.

“\$ORIGIN mustafa.ipv6.” komutu aşağısındaki tabloda her bir isimden sonra alan isminin tekrar bildirilmesi gerekliliğinden kurtarmaktadır. Aksi durumda tüm isim kayıtlarına “.mustafa.ipv6” ifadesi eklenmek zorunda kalınırdı. Yapılandırma dosyasında tüm düğümler için hem IPv6 adresi hem de IPv4 adresi olacak şekilde iki kayıt oluşturulmuştur. CNAME komutu ile ns.mustafa.ipv6 makinesinin bir Web sunucusu (www) ve posta.mustafa.ipv6 makinesinin de bir e-posta (mail) sunucu olacağı belirtilmiştir.

Yapılandırma dosyalarından bir tanesi de “named.conf.options” dosyasıdır. Bu dosyada istenilen yönetim ve çalışma seçenekleri belirtilmektedir. “listen-on-v6 { any; };” satırı sayesinde IPv6 alan ismi isteklerine de cevap verebilmektedir. “acl” komutu ile iki tane erişim listesi (access list) oluşturulmuş ve “allow-query” komutu ile bu erişim listelerinde belirtilen uç noktalarından gelen isteklere cevap verilmesi sağlanmıştır. Dahili erişim listesi sunucunun kendi isteklerine cevap verebilmesi için loopback adreslerini içermekte ayrıca UZEM ağının sahip olduğu IPv4 ve IPv6 adres aralığını belirtmektedir. Harici erişim listesi Türk Telekom ADSL ağının IPv4

```
options {
    directory "/var/cache/bind";
    listen-on-v6 { any; };
    allow-transfer { DahiliErisimListesi; };
    allow-query { DahiliErisimListesi; HariciErisimListesi; };
};
acl DahiliErisimListesi {
    127.0.0.1; ::1/128;
    2001:4bd0:2031::/64;
    160.75.67.0/24;
};
acl HariciErisimListesi {
    85.105.0.0/16;
};
```

[illegible]

Alan adı seçilirken “*mustafa.ipv6*” seçilmiştir, ve bu alan adı global olarak erişilememektedir. Ancak DNS sunucusu olarak burada yapılandırılan sunucu belirtilirse bu kayıtlara erişilebilmektedir. IPv6 Web sitesinin global olarak erişilebilmesi için Sitelutions isimli bir şirketten (<http://sitelutions.com>) ücretsiz IPv6 DNS kaydı hizmeti alındı. Yerel ağdan <http://www.mustafa.ipv6> adresi ile erişilebilen IPv6 Web sitesi, global olarak <http://ipv6uzem.rr.nu> adresinden

erişilebilmektedir. Alan uzantısı çok anlamlı olmadığı için diğer sunucuların bu alan üzerinden global DNS kaydı yapılmadı. Şekil 4.2’de yapılan global isim kaydının yönetim ekranı görünmektedir.

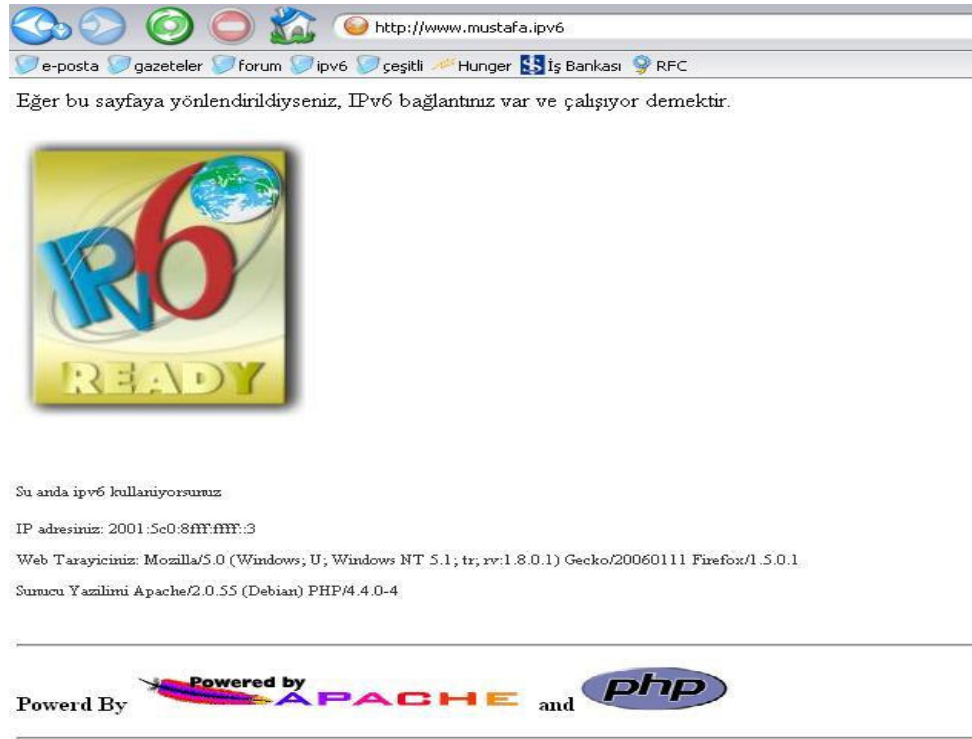
A Records (Point to IP Addresses or Sitelutions Space)				
Destination (IP or Sitelutions Space)	TTL	Edit	Delete	DynDNS
160.75.67.88	3600	[edit]	[delete]	[Dynamic DNS]

AAAA(IP version 6) Records				
Destination (IPv6 address)	TTL	Edit	Delete	
2001:4bd0:2031:0000:0000:0000:0010	3600	[edit]	[delete]	
[Add Record]				

Şekil 4.2: Global DNS kaydı

4.4.2 IPv6 Web sunucusu APACHE

Web sunucuları için açık kaynak kodlu olan Apache yazılımı kullanılmıştır. Debian işletim sistemi deposunda Apache2 yazılımı bulunduğu için “*apt-get install apache2*” komutu ile Web sunucu programını yüklemiş olmaktadır. Web sitesi ve alan adı sistemi sunucusu laboratuvarında aynı bilgisayara kurulmuştur. Şekil 4.3’te hazırlanan Web sayfası görülmektedir.



Şekil 4.3: IPv6 Web sitesi

Apache ön tanımlı olarak IPv6'yı desteklemektedir. Bu sebeple IPv6 ile ilgili ek bir ayar yapılmasına gerek kalmamıştır. Web sitesi için `"/etc/apache2/sites-available/default"` dizininde bulunan dosyada `"RedirectMatch ^/$ /apache2-default/"` satırı bulunarak silinmekte, bu sayede herhangi başka bir yere yönlendirme yapılmadan `"/var/www/"` dizini Web sitesi dosyaları için varsayılan dizin olarak kabul edilmektedir. Bu dizine ilgili HTML sayfaları yükledikten sonra Web sitesine `http://[2001:4BD0:2031::10]` adresinden veya `http://www.mustafa.ipv6` adresinden erişilebilmektedir.

İnternet'te güvenli haberleşme için bazı şifreleme yöntemleri kullanılmaktadır. İnternette iletilen bilgilerin güvenliği için SSL (Secure Socket Layer) kullanılmaktadır. Şifreli Web siteleri genellikle bankaları veya üyelik isteyen yerlerde kullanılmasına rağmen IPv6 alanında test edebilmek için laboratuvarında bir sunucuya Apache-SSL kurulmuştur. Sunucu işletim sistemi olarak Debian Sarge seçilmiş ve `"apt-get install apache-ssl"` komutu kullanılmıştır. Gerekli yüklemelerden sonra oluşturulacak sertifika ile ilgili görsel arayüzlü bir ekran çıkmakta ve girilen bilgiler kullanılarak bir RSA (Rivest Shamir Adelman) anahtarı oluşturulmaktadır. RSA kendisini bulan kişilerin isimlerinden oluşan, bugün çok sık kullanılan matematiksel bir şifreleme algoritmasıdır.



Şekil 4.4: SSL sunucu sertifikası

Bu güvenli Web sitesinin isim kaydı <https://www.mustafa.ipv6> şeklinde yapılmıştır. Şekil 4.4'te bu siteye girildiği zaman istemci tarafa gönderilen sertifika görünmektedir.

IPv6 üzerinden çalışan Web ve güvenli Web sitelerinin kurulumundan sonra birinci Web sitesi üzerinde çalışacak bir takım PHP uygulaması geliştirilmiştir. PHP kodunun sunucu üzerinde çalışabilmesi için Debian işletim sisteminde “*apt-get install php4*” komutu verilmiştir.

4.4.2.1 Giriş sayfası PHP uygulaması

IPv6 Web sunucusuna PHP desteği verdikten sonra yazılan PHP kodunda yapılmak istenen eğer kullanıcı IPv6 bağlantısı ile siteye bağlanıyorsa farklı bir site, IPv4 ile bağlanıyorsa farklı bir siteye erişmesidir. Ayrıca bağlandığı sitenin en altında da kendi IPv4 veya IPv6 adresi, kullandığı Web tarayıcısı, sunucu yazılımı gibi bilgiler sunmaktır. Web sitesini ziyaret eden istemcinin adresi “*REMOTE_ADDR*” değişkeni ile alınmakta ve adresin yapısına göre IPv6 mı IPv4 mü olduğu belirlenmektedir. Bu belirleme sonucu uygun sayfaya yönlendirme yapılmaktadır.

```
<?php
    if (ereg(':',$_SERVER['REMOTE_ADDR'])) {
        header("Location: http://ipv6guzem.rr.nu/indexv6.php");
        die();
    } else {
        header("Location: http://ipv6guzem.rr.nu/indexv4.php");
        die();
    } ?>
```

Kullanıcı iki siteden birine yönlendirildikten sonra bu sitenin en altında kendi ile ilgili bilgiler görmektedir. Bu bilgiler hangi İnternet Protokolünü kullandığı, kendi IP adresi, belirtilen siteye bağlanmak için kullandığı Web tarayıcı ismi ve bağlandığı Web ve PHP sunucularının sürümleridir. Bu iş için aşağıdaki PHP kodu yazılmış ve ilgili sayfalara eklenmiştir.

```
<?php
    if (ereg(':',$_SERVER['REMOTE_ADDR'])) {
        echo "Su anda ipv6 kullaniyorsunuz";
    } else {
        echo "Su anda ipv4 kullaniyorsunuz";
    }

?>

<?php echo "IP adresiniz: " .$_SERVER['REMOTE_ADDR']; ?>
<?php echo "Web Tarayiciniz: " .$_SERVER['HTTP_USER_AGENT']; ?>
<?php echo "Sunucu Yazilimi " .$_SERVER['SERVER_SOFTWARE']; ?>
```

4.4.2.2 Web üzerinden IPv6 uygulaması

Yazılan uygulamalardan ilk iki tanesinin temeli, herhangi bir bilgisayardan (IPv6 desteklemesi gerekmiyor) bir IPv6 adresinin veya IPv6 Web sitesinin cevap verip vermediğini test etmek için ping atmaya dayanmaktadır. Ping ICMP yankı isteği ve cevabı mesajları ile çalışmaktadır. Ping atılan bir bilgisayardan cevap geliyorsa bu o bilgisayarın İnternet üzerinde ve aktif olduğunu göstermektedir.

İlk PHP kodu ping atılacak IPv6 adresini istemektedir. Bazı kontroller yapıldıktan sonra adrese 4 adet ICMP paketi gönderilip cevap beklenmektedir. Gelen cevap ekrana yazdırılmaktadır.

```
<?php
if (!empty($_POST['adres_r'])) {
    if (ereg(['^0-9a-fA-F:.'], $_POST['adres_r'])) {
        die('hatali ip girildi');
    }
    $komut=((strpos($_POST['adres_r'], ':')!==false)?'ping6':'ping');
    $sonuc=shell_exec(sprintf("%s %s -c 4", $komut, $_POST['adres_r']));
    echo "<b>SONUC:</b><pre>";
    echo $sonuc."<br><br>";
}

echo 'Ping Atılacak IPv6 Adresi: <form action="ping.php" method="post"><input
type="text" name="adres_r"> <input type="submit"></form>';
?>
```

Aşağıdaki PHP kodunda ise giriş olarak ping atılacak İnternet adresi istenmektedir. Gene aynı şekilde gelen cevap ekrana yazdırılmaktadır. Burada dikkat edilmesi gereken bir nokta bazı sunucular güvenlik sebebiyle ping'e kapatılmaktadırlar. Yani bir bilgisayardan ICMP cevabı geliyorsa o bilgisayar kesinlikle erişilebilirdir, ancak ICMP cevabı gelmiyorsa erişilebilir olabilir de olmayabilir de.

```
<?php
if (!empty($_POST['adres'])) {
    $_POST['adres']=trim($_POST['adres']);
    if (ereg(['^a-zA-Z0-9_\.'], $_POST['adres'])) {
        echo "gecersiz adres.<br>";
    } else {
        $komut=('ping6');
        $sonuc=shell_exec(sprintf("%s %s -c 6", $komut, $_POST['adres']));
        echo "<b>SONUC:</b><pre>";
        echo $sonuc."<br><br>";
    }
}
```

```
echo 'Ping Atılacak Internet Adresi: <form action="pingname.php" method="post"><input
type="text" name="adres"> <input type="submit"></form>';
?>
```

Son olarak Peter Bieringer tarafından geliştirilen IPV6CALC isimli program kullanılarak giriş yapılan bir IPv6 adresinin türü, kaydının yapıldığı organizasyon gibi veriler sunulmaktadır. Web sunucusunun bulunduğu işletim sisteminde “*apt-get install ipv6calc*” komutu ile program yüklenmiş ve bu programı kullanan PHP kodu hazırlanmıştır. Burada sadece adresi analiz etmek için kullanılan komut belirtilecektir. Daha sonra adres bilgileri ekrana yazdırılmaktadır.

Analiz edilmek istenen adres 2001:0200::8002:0203:47ff:fea5:3085 ise verilecek komut “*ipv6calc --showinfo -i -m 2001:0200::8002:0203:47ff:fea5:3085*” şeklinde olmaktadır. Bu program çalıştırıldığı zaman aşağıdaki gibi bir çıktı vermektedir.

```
IPV6=2001:0200:0000:8002:0203:47ff:fea5:3085
TYPE=unicast,global-unicast,productive
SLA=8002
IPV6_REGISTRY=APNIC
IID=0203:47ff:fea5:3085
EUI48=00:03:47:a5:30:85
EUI48_SCOPE=global
EUI48_TYPE=unicast
OUI="Intel Corporation"
```

4.4.3 IPv6 e-posta sunucusu ve SQUIRRELMAIL

Bir ağda en önemli hizmetlerden bir tanesi de e-posta hizmetidir. Test laboratuvarına kurulan sistem, yüzlerce kullanıcıyı destekleyecek, POP3, IMAP ve Web arayüzünden erişim desteği verecek aynı zamanda IPv6 üzerinden çalışacak şekilde yapılandırılmıştır. E-posta sunucusunda IPv6 ile ilgili çok fazla ayar yapılmasına gerek olmamaktadır ancak alan adı sisteminin kayıtlarının düzgün bir şekilde oluşturulmuş olması gerekmektedir.

E-posta sunucusunun kurulumu çok uzun sürdüğü ve IPv6 ile ilgili ayarları içermediği için kısaca anlatılacaktır. Öncelikle e-posta sunucusunun isim kaydı kontrol edilmelidir. “*posta.mustafa.ipv6*” isim kaydı 2001:4bd0:2031::11 ve 160.75.67.86 adresleri ile yapılmıştır. Alan adı kaydında “*mail CNAME posta*” satırı ile e-posta sunucusunun adresinin “*mail.mustafa.ipv6*” olacağı ve ağda “*posta.mustafa.ipv6*” olarak isimlendirildiği belirtilmektedir.

E-posta sunucusu altyapısı olarak Apache2, PHP4, mysql sunucusu kurulmaktadır. Daha sonra SMTP sunusu olarak kullanılmak üzere qmail kaynak paketi ilgili adresten indirilmekte ve kurulumu yapılmaktadır. Burada dikkat edilmesi gereken özellik ya paket smtp-auth destekleyecek şekilde yamanmış olacaktır veya bu iki program ayrı ayrı indirilip kurulacaktır. SMTP 25 numaralı porttan çalıştığı için eğer qmail düzgün olarak kurulduysa “telnet localhost 25” komutuna “Connected to localhost” cevabı gelmelidir. Qmail programı POP kullanımına izin verilecek şekilde yapılandırılmalıdır.

E-posta alanını yönetmek için Vpopmail programı kurulmalıdır. Vpopmail kullanıcı kayıtları için mysql veri tabanını kullanacaktır. Bu sebeple “mysql> create database vpopmail;” komutu ile yeni bir veri tabanı oluşturulmaktadır. Son olarak IMAP desteği için Courier-IMAP yazılımı kurulmalıdır. Tüm kurulumlar bittikten sonra “telnet localhost 110” komutu ile POP3 desteği, “telnet localhost 143” komutu ile de IMAP desteği test edilebilmektedir.

E-posta sunucusuna “mustafa.ipv6” alanını eklemek için “~vpopmail/bin/vaddomain mustafa.ipv6 yönetici_sifresi” komutu verilmelidir. Oluşturulan yeni e-posta alanına kullanıcı eklemek için “~vpopmail/bin/vadduser test@mustafa.ipv6 kullanıcı_sifresi” komutu yerine getirilmelidir.

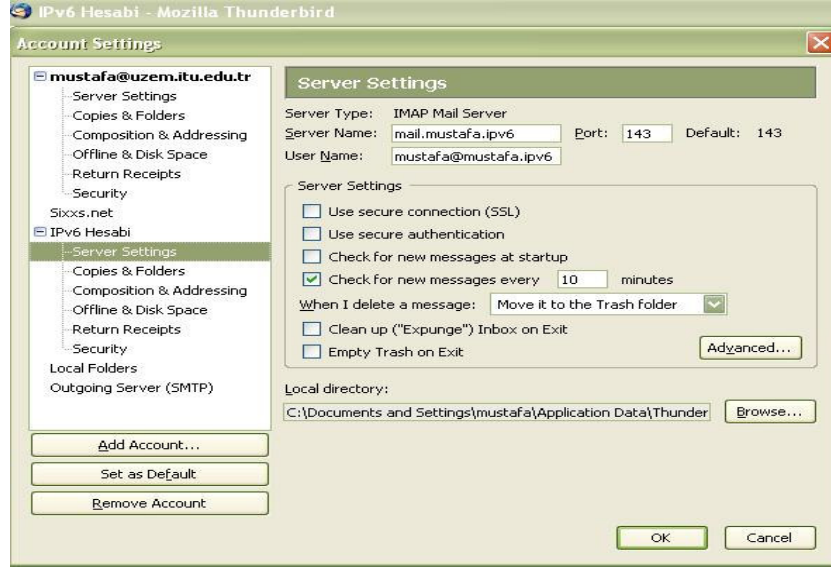
Yukarıda bahsedilen ayarların yapılmasından sonra, kullanıcıların e-postalarına Web arayüzünden de erişebilmeleri için Squirrelmail programı yüklenmektedir. Squirrelmail ile ilgili yapılacak tek yapılandırma “/etc/squirrelmail/apache.conf” dosyası içine IPv6 alan adını belirten bir yönlendirme paragrafı yazmak.

```
<VirtualHost mail.mustafa.ipv6 >  
    DocumentRoot /usr/share/squirrelmail  
    ServerName mail.mustafa.ipv6  
</VirtualHost>
```

Yukarıda belirtilen paragraf sayesinde “http://mail.mustafa.ipv6” adresini Web tarayıcısına giren kullanıcı e-postalarına Web arayüzünden ulaşabilecek.

E-postalarına bir e-posta istemcisi ile erişmek isteyen bir kullanıcı bazı ayarlar yapmalıdır. Öncelikle erişim protokolü olarak POP3 mü yoksa IMAP mi kullanacağına karar vermelidir. Burada kurulumu yapılan IPv6 e-posta sunusu her iki protokolü de desteklemektedir. Kullanıcının, gerekli protokolü seçtikten sonra kullandığı istemciye göre bazı sunucu ayarları yapması gerekmektedir. Şekil 3.17’de

Mozilla Thunderbird programı için “*mustafa@mustafa.ipv6*” e-posta adresine özel IMAP ayarları belirtilmiştir. POP3 kullanılacağı zaman ayarlarda sadece port numarası 110 olarak değişmektedir. IMAP’ın POP3’ten farklı özelliği herhangi bir istemciden veya Web arayüzünden okunan mesajlar sunucuda okunmuş olarak işaretlenmektedir. Aynı şekilde bir mesajı bir kere silmek, o mesajın sunucudan silinmesi anlamına gelmektedir. POP3’te ise istemci mesajı kendi diskine çekmekte ve sunucu ile herhangi bir mesaj eşlemesi yapmamaktadır.



Şekil 4.5: E-posta istemci yapılandırması

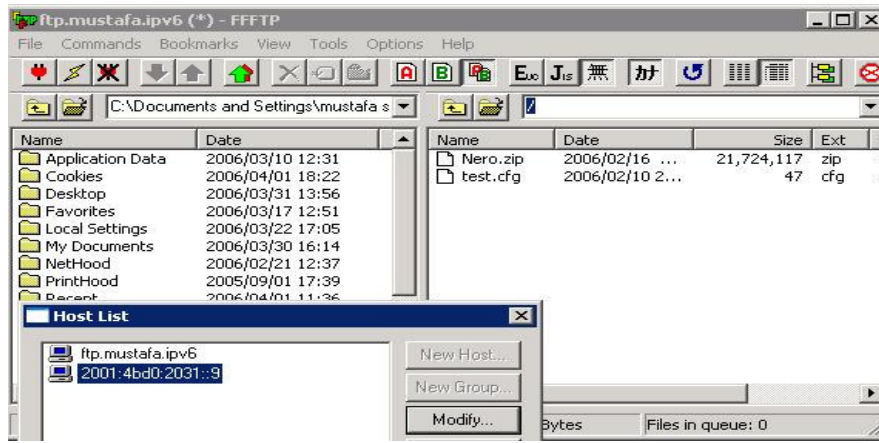
4.4.4 IPv6 dosya transfer sunucusu VSFTP

FTP, dosya transfer protokolüdür ve ağ içinde veya İnternette dosya paylaşmak için FTP sunucusu kurulmaktadır. FTP sunucusu olarak VSFTPD seçilmiştir çünkü bu yazılım açık kaynak dünyasında sıkça kullanılan, Redhat, Suse, OpenBSD, Debian, FreeBSD işletim sistemlerinin dosya dağıtımı için kullandığı bir yazılımdır. Bu laboratuvarıda kullanılmak üzere seçilmesinin en önemli sebebi sağladığı IPv6 desteğidir.

FTP sunucusu güvenli Web sunucusunun bulunduğu bilgisayara yüklenmiştir. VSFTPD yazılımı Debian Sarge deposunda bulunduğu için “*apt-get install vsftpd*” komutu bu programın kurulması için yeterlidir. Yapılandırma için “*/etc/vsftpd.conf*” dosyası incelenmiştir. Burada IPv6 desteği için iki komut bulunmaktadır. Birincisi “*listen_ipv6*” satırı, buradaki ifade “*listen_ipv6=YES*” yapılmalıdır. Diğer komut “*listen_address6*” buraya da FTP sorgularını hangi adresten dinlenmesi isteniyorsa o

adres belirtilmelidir. Böyle bir adres belirlenmesine gerek duyulmadığı için o ifade varsayılan şekliyle boş olarak bırakılmıştır.

İsim kaydı bölüm 4.4.1’de belirtildiği gibi yapıldı ve ftp://ftp.mustafa.ipv6 adresi 2001:4bd0:2031::9 IPv6 adresi ve 160.75.67.93 IPv4 adresi ile eşleştirildi. IPv6 adresi kullanılarak erişilmek istenirse ftp://[2001:4BD0:2031::9] yazmak yeterlidir. FTP dosyalarına erişmek için Web tarayıcısı kullanılabilirdiği gibi Windows işletim sistemleri için IPv6 destekleyen şekil 4.6’da gösterilen FFFTP programı da kullanılabilir. FFFTP programı Jun Sota isimli bir Japon tarafından Windows ortamında kullanılmak üzere geliştirilmiş ücretsiz bir yazılımdır.



Şekil 4.6: FTP istemci programı

4.4.5 IPv6 sunucularının yedeklenmesi

Laboratuvarda kurulumu yapılan sunuculardan DHCP sunucusu hariç diğerleri ve de IPv6 yönlendiricisi hep Linux işletim sistemleri üzerine kurulmuştur. Bu sebeple Linux sistemler için bir yedekleme stratejisinin ihtiyacı hissedilmiştir. GNU/Linux işletim sistemlerinde gerekli bazı yapılandırma dosyalarını ve kullanıcı ayarlarını kaydetmek tüm işletim sistemini yedeklemek için yeterli olmaktadır. Yedekleme yapmak için kullanılan komut “tar -cpf /tmp/sistem_yedek21.01.06.tar bin/ boot/ etc/ home/ initrd intrd.img lib/ root/ sbin/ sys/ usr/ var/ vmlinuz 2> /tmp/sistem_yedek21.01.06.err > /tmp/sistem_yedek21.01.06.log” şeklindedir. Burada belirtilen dosya ve klasörler tmp dizini içine “sistem_yedek21.01.06.tar” dosyası şeklinde birleştirilmekte, hatalar “sistem_yedek21.01.06.err” şeklinde, işlem kayıtları da “sistem_yedek21.01.06.log” şeklinde tutulmaktadır.

Herhangi bir sebeple 21.01.06 tarihinde yedeklenen bu yapılandırmaya geri dönmek istenirse yapılması gereken tek şey “*tar -xf /tmp/sistem_yedek21.01.06.tar/*” komutunu vermektir. Arşivlenmiş olan “*sistem_yedek21.01.06.tar*” dosyası tekrar açılmakta ve dosyalar kök dizin altına yerleştirilmektedir.

4.5 IPv6 ağ servisleri ve uygulamaları

IPv6'ya geçiş test laboratuvarında tüm ilgili düğümler çift IP katmanlı yapıya getirildi, IPv6 tüneli kuruldu, Debian yönlendirici sayesinde ağa IPv6 bağlantısı sağlandı, IPv6 adres aralığı alındı ve orta ölçekli bir ağda bulunabilecek tüm sunucular kuruldu. En son olarak kurulan IPv6 destekli ağda bazı servis ve uygulamalar kurulup çalıştırılarak test edilecektir. Bu uygulamalar; SNMP, MRTG, Gnomemeeting, Putty, Lynx, W3M, Nmap, Iperf, Netperf, Whois, Ping, Traceroute, Tracepath yazılımlarıdır.

4.5.1 SNMP

Yalın Ağ Yönetimi Protokolü (SNMP), uygulama katmanında çalışarak ağ cihazları arasında ağ yönetimine ait bilgiler taşımaktadır. Ağ yöneticilerinin band genişliği, performans ve sunucuların durumu gibi bilgileri edinebildiği ve sorun giderme aşamalarında sıkça kullandığı bir uygulama olmaktadır.

Üç çeşit SNMP sürümü geliştirilmiştir. Bunlar SNMP versiyon 1 (SNMPv1), SNMP versiyon 2 (SNMPv2) ve SNMP versiyon 3'tür (SNMPv3). SNMPv1 1988 yılında RFC 1065, 1066, 1067 belgeleri ile tanımlanmıştır. Birinci sürüm güvenlik eksiklikleri konusunda sıkça eleştirilmiştir. Kimlik denetimi bir tek topluluk alanında yapılmakta ve şifre açık metin olarak iletilmektedir[46].

SNMPv2p, RFC 1441 ve 1452 belgelerinde tanımlanmıştır. Performans, güvenlik, gizlilik gibi konularda SNMPv1'e göre yenilikler getirilmiştir. Daha sonra RFC 1901 ve 1908 ise SNMPv2c geliştirilmiş SNMPv2p'nin tartışılan kısımları bu sürümle değiştirilmiştir. Ancak SNMPv2'nin karmaşık yapısı bir problem olmaya devam etmiş ve SNMPv2u RFC 1909 ve 1910 ile kullanıcı tabanlı olarak geliştirilmiştir.

SNMPv3, RFC 3411 ve 3418 ile tanımlanmış en son sürümdür. IETF, SNMP standart versiyonu olarak SNMPv3'ü tanımlamaktadır. Ancak sürümler arasında

geriye doğru uyumluluk bulunmakta ve iki değişik sürüm beraber kullanılabilmektedir[47].

Test laboratuvarında hangi sürüm olduğuna dikkat edilmeden IPv6 ile ilgili bölümler daha ağırlıklı incelenmiştir. Öncelikle SNMP sunucusu olarak seçilen Web ve DNS'in bulunduğu sunucuya ve e-posta sunucusuna “*apt-get install snmpd*” komutu ile gerekli sunucu yazılımı kurulmuştur. Bu sunucuların gözlemleneceği bilgisayarlara da “*apt-get install snmp*” komutu ile snmp istemcisi kurulmuştur.

SNMP sunucusunun IPv6 adresinden de dinleme yapabilmesi için “/etc/default/snmpd” dosyasındaki ilgili satırın, “*SNMPDOPTS='-Lsd -Lf /dev/null -p/var/run/snmpd.pid udp6:161 udp:161'*” şeklinde değiştirilmesi gerekmektedir. Snmp buradaki yapılandırmadan da görülebileceği gibi UDP 161 portundan çalışmaktadır. Ayrıca “/etc/snmp/snmpd.conf” yapılandırma dosyasına “*rwcommunity6 public*” satırı eklenmelidir.

Gerekli ayarlar yapıldıktan sonra örnek olarak “*snmpget -v 1 -c public udp6:[2001:4bd0:2031::10] SNMPv2-MIB::sysUpTime.0*” komutu verilerek Web sunucusunun ne kadar süredir aktif olduğu “*SNMPv2-MIB::sysUpTime.0 = Timeticks: (56281) 0:09:22.81*” cevabı ile öğrenilebilmektedir. Web sunucusundan alınabilecek tüm verileri görebilmek için “*snmpwalk -v 2c -c public udp6:[2001:4bd0:2031::10]*” komutu verilmektedir.

4.5.2 MRTG

SNMP bilgileri, snmpget ve snmpwalk komutları ile kullanılabildiği gibi bazı programlar tarafından analiz edilerek, sonuçları görsel bir arayüzle sunulmak üzere de kullanılabilmektedir. SNMP verilerini kullanan programlardan bir tanesi MRTG'dir (Multi Router Traffic Grapher). MRTG, yapılandırıldığı SNMP bilgilerinin değişimini belirtilen zaman aralıklarında kontrol ederek bunu grafiksel bir arayüzle sunmaktadır.

MRTG ilk olarak yönlendiriciler için geliştirilmiştir. Bu sebeple isminde yönlendirici trafiğinden bahsedilmektedir. Ancak zamanla çok geniş kullanım alanı bulmuş ve sunucuların da kontrolünün yapıldığı bir yazılım halini almıştır. MRTG ile sunucuların işlemci kullanımı, hafıza kontrolü, diskindeki boşluk oranı ve trafik giriş çıkışı gibi bir çok özelliği grafiksel olarak izlenebilmekte ve günlük, haftalık, aylık, yıllık istatistikler kontrol edilebilmektedir.

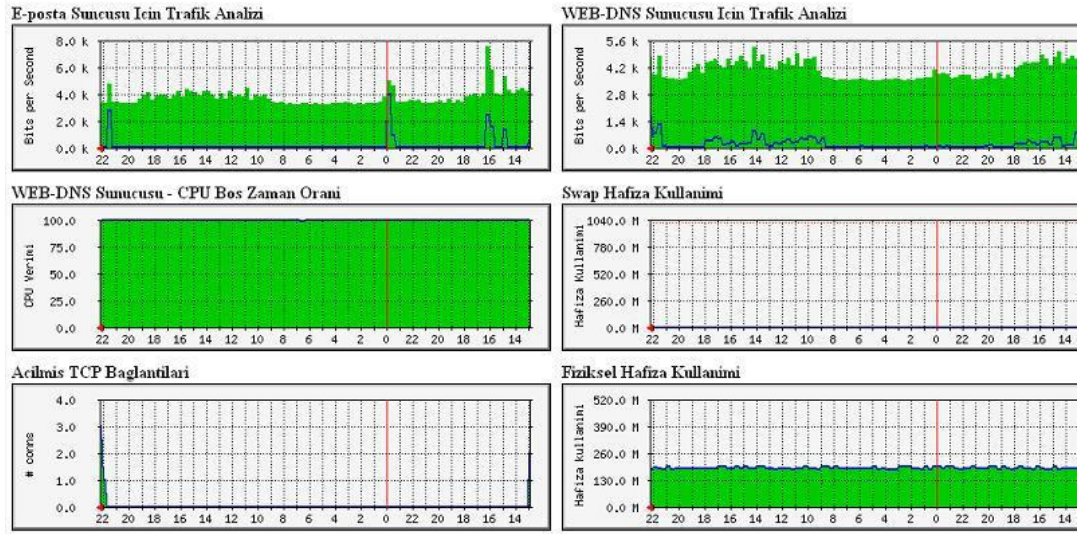
MRTG kurulumu için Debian sunucularda “*apt-get install mrtg*” komutu verilmektedir. Ayrıca IPv6 desteği için “*libsocket6-perl*” ve “*libio-socket-inet6-perl*” kütüphane dosyaları yüklenmelidir. Son olarak yapılandırma dosyasında her bir hedef grafik için sadece “*Enable IPv6: yes*” satırı eklenmelidir. Bu işlemten sonra yapılandırma dosyası SNMP verileri ile hazırlanıp, bir ağ arayüzünden geçen IPv6 trafiği rahatlıkla izlenebilmektedir. E-posta sunucusunun IPv6 trafiğini izleyen örnek bir yapılandırma dosyası aşağıdaki gibidir[48].

```
Target[mailserver]: 2:public@posta.mustafa.ipv6:161
SetEnv[mailserver]: MRTG_INT_IP="2001:4bd0:2031::11"
                    MRTG_INT_DESCR="eth0"
MaxBytes[mailserver]: 12500000
Title[mailserver]: E-posta Suncusu Icin Trafik Analizi
PageTop[mailserver]: <H1> E-posta Suncusu Icin Trafik Analizi </H1>
Options[mailserver]: bits
EnableIPv6: yes
```

Bu yapılandırmada “*Target*” komutunda “2” ile SNMP sürümü, “*public*” ile de topluluk belirtilmiştir. Hedef sunucunun *posta.mustafa.ipv6* makinesi olduğu gene “*Target*” ile ifade edilmektedir. İzlenecek sunucunun IP adresi ve arayüzü “*SetEnv*” komutu ile ifade edilmekte ve “*MaxBytes*” ile 12.5MB yani 100 mega bitlik bir ethernet arayüzü belirtilmiştir. Test laboratuvarı için izlenmek istenen 6 adet özellik grafik oluşturulacak şekilde “*ns.mustafa.ipv6.cfg*” isimli yapılandırma dosyasına kaydedilmiştir. Daha sonra bu grafikler için bir HTML sayfası oluşturulacaktır. Bu iş için MRTG ile birlikte gelen *indexmaker* programı kullanılmıştır. “*indexmaker --title="MRTG Sunucu" -output=/var/www/mrtg/index.html /etc/mrtg/ns.mustafa.ipv6.cfg*” komutu verilerek hazırlanacak HTML sayfasının hangi yapılandırma dosyasından bilgileri okuyacağı ve hazırlanan sayfanın başlığının ne olacağı belirtilmektedir.

Bu grafikler sırasıyla, e-posta ve Web sunucularının trafik grafikleri, Web sunucusunun CPU boş zaman oranı, swap hafıza kullanımı, sunucuda açılmış TCP bağlantı sayısı ve sunucunun fiziksel hafıza kullanımı grafikleridir. Bu grafiklerin üstüne tıklandığı zaman günlük, haftalık, aylık ve yıllık istatistik grafikleri detaylı olarak izlenebilmektedir. En son olarak “*/etc/crontab*” dosyasına “**/10 * * * * root /usr/bin/mrtg /etc/ns.mustafa.ipv6.cfg*” satırı eklenmekte ve MRTG grafikleri çizimi her 10 dakikada bir yenilenmektedir. Bu zaman dilimi isteğe göre değiştirilebilmektedir.

MRTG Sunucu İzleme Sayfası



Şekil 4.7: MRTG grafikleri

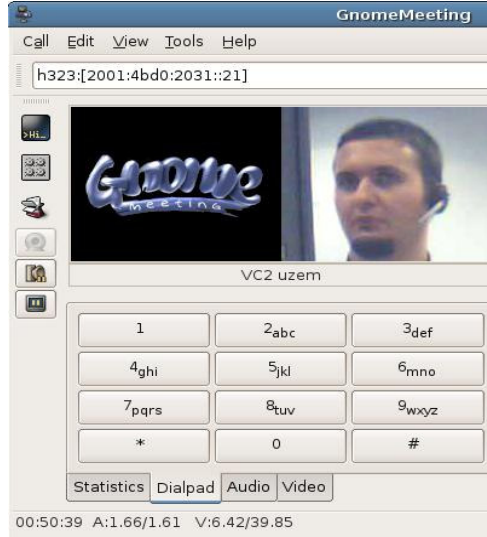
Şekil 4.7’de oluşturulan grafikler görülmektedir. MRTG grafikleri ile hem IPv6 trafikleri kontrol edilebilmekte hem de IPv6 sunucularının performansları izlenebilmektedir. MRTG grafikleri sistem ve ağ yöneticileri için son derece önemli bir izleme metodudur. Bu sebeple IPv6 desteği ile birlikte bu test laboratuvarında kurulumu yapılmıştır.

4.5.3 Gnomemeeting

Gnomemeeting, IP üzerinden ses ve görüntü (VOIP ve video-over IP) iletimini sağlayan açık kaynaklı bir yazılımdır. Hem H323 hem de SIP protokollerini desteklemektedir. Açık kaynak dünyası tarafından çok benimsenmiş ve bir çok Linux dağıtımı için paketleri hazırlanmıştır. Gnomemeeting yazılımının IPv6 desteği bulunmasından dolayı test laboratuvarında yüklenerek IPv6 videokonferans uygulamaları yapılmıştır.

Gnomemeeting yazılımı standart Debian kurulumu ile birlikte gelmekte ve IPv6’yı ek bir ayar yapılmadan desteklemektedir. Test yapmak için iki tane Debian istemci bilgisayarı kullanılmış ve 2001:4bd0:2031::20 ile 2001:4bd0:2031::21 IP adresleri arasında video konferans oluşturulmuştur. Bu bilgisayarların isim kayıtları videokonferans1.mustafa.ipv6 ve videokonferans2.mustafa.ipv6 şeklinde yapılmıştır. Arama isim kaydına göre yapılabildiği gibi h323:[2001:4bd0:2031::21] şeklinde

IPv6 adresini kullanarak da yapılabilir. Şekil 4.8’de bir konferans sırasındaki Gnomemeeting arayüzü görülmektedir.



Şekil 4.8: Gnomemeeting programı

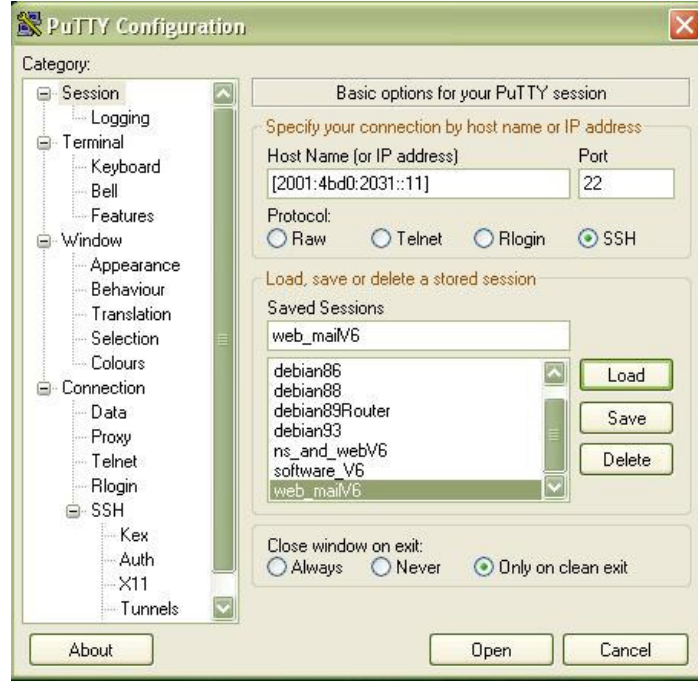
IPv6 video konferans uygulaması test edilirken aynı zamanda Uzem’de bulunan Polycom markalı video konferans sistemlerinin IPv6 desteği de araştırılmıştır. Ancak mevcut cihazların şu an itibariyle IPv6 desteği sağlayamadığı firma tarafından bildirilmiştir. Bu da açık kaynak kodlu yazılımların, ticari yazılımlara göre IPv6 ve yeni teknolojiler konusundaki önderliklerini bir kere daha göstermiştir.

4.5.4 PuTTY

SSH bir bilgisayara uzaktan TCP 22 portu kullanılarak bağlanmaya yarayan bir telnet ve rlogin benzeri bir protokoldür. SSH ile uzaktan herhangi bir bilgisayarın komut satırına bağlanıp bağlanılan kullanıcının yetkisine göre ayarlar yapılabilir. SSH’ta iletişim tamamen çok güçlü bir kriptoyla şifrelenmiş bir şekilde yapıldığı için açık metin olarak iletişim sağlayan Telnet yerine tercih edilmektedir. Bir çok yazılım SSH ile tünellenerek şifrelenmiş iletişim sağlanabilmektedir.

SSH’ın başka bir yararlı özelliği sunucuya otomatik bağlanmayı sağlayıp, bir takım önceden tanımlı komutları koşturabilmesi ve sonra da bağlantıyı sonlandırabilmesidir. Ayrıca gerekli ayarlar yapıldığı zaman şifre girilmesi zorunluluğu bulunmamaktadır.

PuTTY Telnet ve SSH bağlantısı sağlamak için hem Windows hem Unix/Linux platformunda kullanılabilen açık kaynaklı bir yazılımdır. IPv6 destekleyen ayrı bir sürümü çıkarılmıştır. Şekil 4.9’da PuTTY istemci arayüzü görülmektedir.



Şekil 4.9: PuTTY istemci arayüzü

Linux komut satırından “*ssh yonlendirici.mustafa.ipv6*” veya “*ssh 2001:4bd0:2031::1*” komutları ile de SSH sunucusuna bağlantı kurulabilmektedir.

4.5.5 Lynx ve W3M

Lynx ve W3M, IPv6 desteği sunan komut satırı ekranında çalışan Web tarayıcılarıdır. Linux sunucularda genellikle performansı arttırmak açısından X-masaüstü ortamı kurulmamaktadır. Çünkü görsel ekranın ciddi hafıza gereksinimleri bulunmaktadır. Bir sistem yöneticisi böyle bir sunucuda komut satırından çalışırken eğer bir Web sitesine girmesi gerekirse Lynx ve W3M kullanabilmektedir. Bu Web tarayıcıları resimleri göstermeseler de bazen sorun giderme prosedürlerinde işe yaramaktadırlar.

Komut satırından “*lynx www.mustafa.ipv6*”, “*lynx http://[2001:4bd0:2031::10]*”, “*w3m www.mustafa.ipv6*” veya “*w3m http://[2001:4bd0:2031::10]*” komutlarından bir tanesi verilerek IPv6 Web bağlantısı sağlanabilmektedir. Şekil 4.10’da W3M tarayıcısı ile yapılan bir Web sitesi bağlantısı gösterilmektedir.

```
KAME Project

[kame-anime]
dancing kame by atelier monochrome

KAME Project is a joint effort of six companies in Japan
to provide a free IPv6 and IPsec (for both IPv4 and IPv6) stack for BSD
variants to the world.

* 7th Nov. 2005: An announcement of conclusion of the KAME project
+ An announcement from the NIDE project
+ An announcement from the KINE project
* Newsflash! New!
+ Mar 31, 2006 Newsletter: "Obtained IPv6 Ready Logo (Phase2 Core) on
KAME-FreeBSD!"
+ Mar 4, 2006 NIDE-DHCPv6 project will maintain/develop/release our
DHCPv6 programs. (Please see this mail for further detail)
+ Jan 31, 2006: ipv6style released articles regarding the conclusion of
KAME:
o Special Interview with Dr. Jun Nishii
o The history and success of the KINE project by Kazuhiko Yamamoto
o Comments from the core members
+ Nov 17, 2005: KAME snap releases will not follow *BSD releases toward
the project conclusion (Please see this message for further detail)
+ Fast newsflash

-----
KAME banner $Date: 2006/03/31 07:42:50 $
you are using IPv6, from 2001:4bd0:2031:0:20d:60ff:fe66:c7c5
the server room's temperature is 24.9C°at 19:09:30 on 4/7JST. Powered by
Internet noodle.
<=UpDn Viewing <Webpage of Kame Project>
```

Şekil 4.10: W3M Web tarayıcısı

4.5.6 Nmap

Nmap (Network Mapper), ağ keşfi yaparak güvenlik eksikliklerini bulmak üzere geliştirilmiş açık kaynak kodlu bir yazılımdır. Büyük ağları taramak amacıyla geliştirilse de günümüzde tek bir uç nokta hakkında bilgi edinmek için de sıkça kullanılmaktadır. Nmap ile bir ağda bulunan düğümlerin bulunuş sebepleri, sundukları hizmetler ve kullandıkları uygulamalar, işletim sistemleri, ağda bulunan güvenlik mekanizmaları gibi birçok bilgi edinilebilmektedir. Nmap birçok işletim sisteminde grafiksel arayüzden ve komut satırından çalışabilmektedir.

Nmap sistem yöneticilerinin kendi sunucularını ve ağlarını güvenlik taramasından geçirerek kontrol etmelerini sağlamak üzere geliştirilmiştir. Çok fazla benimsendiği için tüm işletim sistemleri için sürümleri çıkartılmıştır ve özellikleri gelişen teknolojilere göre sürekli yenilenmektedir. Bu sebeple nmap programına IPv6 desteği en kısa sürede eklenmiştir. Nmap ile tarama yaparken “-6” parametresini ekleyerek bir IPv6 düğümü taranabilmektedir.

```
#nmap -6 -v -sT www.mustafa.ipv6

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-04-07 13:43 EEST
Machine 2001:4bd0:2031::10 MIGHT actually be listening on probe port 80
Initiating Connect() Scan against ns.mustafa.ipv6 (2001:4bd0:2031::10) [1663 ports] at
13:43
Discovered open port 22/tcp on 2001:4bd0:2031::10
Discovered open port 53/tcp on 2001:4bd0:2031::10
Discovered open port 80/tcp on 2001:4bd0:2031::10

The Connect() Scan took 0.04s to scan 1663 total ports.
Host ns.mustafa.ipv6 (2001:4bd0:2031::10) appears to be up ...
good. Interesting ports on ns.mustafa.ipv6 (2001:4bd0:2031::10):
(The 1660 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http

Nmap finished: 1 IP address (1 host up) scanned in 0.154 seconds
```

Şekil 4.11: Nmap IPv6 tarama örneği

Şekil 4.11’de IPv6 Web sitesinin bulunduğu sunucuya güvenlik taraması yapılmaktadır. Parametrelerden “-6” IPv6 adresinin kullanılması, “-v” detaylı sonuç gösterimi ve “-sT” TCP paket taraması için kullanılmıştır. Sonuç olarak 22(ssh), 53(dns) ve 80(http) portlarının açık olduğu belirtilmektedir. Taranan sunucunun Web ve DNS sunucusu olduğu bu sonuçtan anlaşılabilmektedir.

4.5.7 Iperf ve Netperf

Iperf, TCP ve UDP band genişliğini ölçerek ağ performansını izlemeye yarayan bir yazılımdır. Band genişliği haricinde paket kaybı ve ağdaki gecikme bilgisine ulaşmak için de kullanılmaktadır. Test laboratuvarında Iperf 2.0.2 sürümü IPv6 desteği ile birlikte denenmiştir.

Iperf sunucu ve istemci mantığıyla çalışmaktadır. Aradaki band genişliği ölçülecek iki düğümden bir tanesi sunucu bir tanesi istemci olmaktadır. Sunucu olan düğümde (Linux) “*iperf -V -s*” komutu, istemci olan düğümde de “*iperf -V -c <Sunucu IPv6 adresi>*” komutu verilmektedir. “-V” komutu IPv6 protokolü kullanılarak bağlantının yapılacağını belirtmektedir. Şekil 4.12’de örnek bir band genişliği testi gösterilmektedir. Laboratuvardaki FTP sunucusu ile e-posta sunucusu arasında kurulan IPv6 bağlantısından sonra 111MB veri iletilmiş ve 92Mb/sn’lik band genişliğine ulaşılmıştır.

```
# iperf -V -s
-----
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
-----
[ 4] local 2001:4bd0:2031::11 port 5001 connected with 2001:4bd0:2031::9 port 40209
[ 4] 0.0-10.0 sec 111 MBytes 92.8 Mb/s/sec

# iperf -V -c 2001:4bd0:2031::11
-----
Client connecting to 2001:4bd0:2031::11, TCP port 5001
TCP window size: 16.0 KByte (default)
-----
[ 3] local 2001:4bd0:2031::9 port 40209 connected with 2001:4bd0:2031::11 port 5001
[ 3] 0.0-10.0 sec 111 MBytes 92.9 Mb/s/sec
```

Şekil 4.12: Iperf sunucu istemci bağlantısı

IPv6'ya uyarlanmış ağ performans uygulamalarından bir tanesi de Netperf yazılımıdır. Netperf de, Iperf gibi TCP veya UDP üzerinden paket göndermekte ve iki düğüm arasındaki ağ özelliklerini ölçmektedir. Komut söz dizimi biraz farklılık göstermektedir. Şekil 4.13'te Netperf bağlantı örneği belirtilmektedir.

```
# netserver -6 -p 123
Starting netserver at port 123
Starting netserver at hostname ::0 port 123 and family AF_INET6

# netperf -H ftp.mustafa.ipv6 -6 -p 123
TCP STREAM TEST from ::0 (::) port 0 AF_INET6 to ftp.mustafa.ipv6
(2001:4bd0:2031::9) port 0 AF_INET6
Recv  Send  Send
Socket Socket Message Elapsed
Size  Size  Size   Time   Throughput
bytes bytes bytes  secs.  10^6bits/sec
87380 16384 16384 10.00 92.82
```

Şekil 4.13: Netperf sunucu istemci bağlantısı

Sunucuya “netserver” komutu verilmekte, “-6” ile IPv6 bağlantısı “-p” ile de bağlantı kurulacak port numarası belirtilmektedir. İstemci tarafında “netperf -H <sunucu>” komutu verilmektedir. Dikkat edilmesi gereken nokta sunucuda belirtilen bağlantı portu ile istemcide belirtilen port aynı olmalıdır.

4.5.8 Whois

Whois, bir veri tabanından IP adresine, alan adı kaydına veya otonom sistem numarasına göre arama yapmaya yarayan programdır. Aranılan verinin kaydının kimin üzerine yapıldığını belirtmektedir. IPv6 adreslerinin de kayıtlarını kontrol edebilmekte ve bu adreslerin kimin üstüne olduğunu bildirmektedir.

Linux işletim sistemlerinde komut satırından “*whois <IP adresi>*” şeklinde sorgulama yapılabileceği gibi whois Web siteleri kullanılarak da sorgulama yapılabilmektedir. Laboratuvarında bulunan Debian işletim sistemli bilgisayarlardan herhangi birinde “*whois 2001:4bd0:2031::1*” komutu verilerek, test için alınmış olan 2001:4bd0:2031/48 IPv6 aralığının RIPE ve SixXS kayıtları görülebilmektedir. Bu aralıktaki herhangi bir IP adresi arandığı zaman iletişim kurulacak kişi olarak ben gözükmekteyim.

4.5.9 Sorun giderme uygulamaları

Bir ağda çıkan bağlantı sorununu gidermek için kullanılan bazı basit uygulamalar vardır. Bunlardan bazıları ping, tracepath ve traceroute uygulamalarıdır. Bu uygulamaların tamamı IPv6 desteği sunmaktadırlar.

4.5.9.1 Ping

Ping uygulaması, hedef bir düğüme ICMP bilgi mesajları kapsamındaki yankı isteği mesajı gönderilmesine dayanmaktadır. Eğer yankı isteğine, yankı cevabı ile karşılık verilirse karşıdaki düğüm canlıdır ve ağ bağlantısı çalışıyordur sonucu çıkarılmaktadır.

Bu uygulamanın IPv6 desteği Linux işletim sistemlerinde “*ping6*” komutu ile sağlanmaktadır. Windows işletim sistemlerinde ise “*ping*” komutu hem IPv4 için hem de IPv6 için kullanılmaktadır. Yazılan adrese göre sistem nasıl bir paket göndereceğine karar vermektedir. Ping uygulamasında ayrıca gönderilen paketlerin başarı oranına ve iletim süresine göre istatistikler çıkarılmaktadır.

4.5.9.2 Traceroute

Traceroute, iki düğüm arasında bir bağlantı kopukluğu olduğu zaman, kopmanın nereden kaynaklandığını bulabilmek için kullanılmaktadır. Hedef adrese paketler

gönderilmektedir. İlk paketin TTL değeri bir olmakta, yani birinci yönlendiriciden geçtikten sonra paket iptal edilmektedir. Eğer birinci yönlendiriciden başarı mesajı gelirse bu sefere TTL değeri iki olan paket gönderilmektedir. Bu şekilde TTL değeri arttırılarak hedef düğüme erişilmekte ve bu erişim sırasında izlenen yol belirtilmektedir. Ancak IP iletişiminde tüm paketlerin aynı yoldan gitmesi garanti edilememektedir.

Linux işletim sistemlerinde IPv6 analizi için “*tracert6 <hedef IPv6 adresi>*” komutu, Windows’ta ise “*tracert <hedef IPv6 adresi>*” komutu verilmektedir. Şekil 4.14’te UZEM test laboratuvarından SixXS Web sunucusuna ulaşırken geçilen yönlendiriciler isim kayıtları ve IPv6 adresleri ile birlikte görünmektedir.

```
tracert6 www.sixxs.net

tracert6 to noc.sixxs.net (2001:838:1:1:210:dcff:fe20:7c7c) from
2001:4bd0:2031::9, 30 hops max, 16 byte packets
 1 yonlendirici.mustafa.ipv6 (2001:4bd0:2031::1) 0.14 ms 0.114 ms 0.107 ms
 2 gw-123.lon-01.gb.sixxs.net (2001:4bd0:2000:7a::1) 74.784 ms 74.869 ms
 82.489 ms
 3 fa0-0.712-IPv6-necromancer.sov.kewlio.net.uk
 (2001:4bd0:d10:1234:260:f5ff:fe06:dfe) 78.866 ms 330.221 ms 276.869 ms
 4 2001:7f8:5::704b:1 (2001:7f8:5::704b:1) 81.532 ms 130.833 ms 138.644 ms
 5 ge0-0-44.br0.nlams1.realroute.net (2001:1598:a:3::1) 163.22 ms 157.093 ms
 140.305 ms
 6 ams-ix.ipv6.concepts.nl (2001:7f8:1::a501:2871:1) 126.526 ms * 130.328 ms
 7 se1.breda.ipv6.concepts-ict.net (2001:838:0:10::2) 136.124 ms 140.195 ms *
 8 noc.sixxs.net (2001:838:1:1:210:dcff:fe20:7c7c) 176.559 ms 179.566 ms
 178.861 ms
```

Şekil 4.14: Traceroute örneği

4.5.9.3 Tracepath

Tracepath programı, traceroute uygulamasına çok benzer çalışmaktadır. Traceroute gibi detaylı parametreleri bulunmamaktadır. Hedefe ulaşılıncaya kadar izlenen yönlendiricilerin sadece isim kayıtları gösterilmekte IP adresleri ekran çıktısında belirtilmemektedir.

Tracepath’in bir ek özelliği yol üzerindeki MTU değerini de belirtmektedir. İletim sırasında UDP portu kullanılmaktadır. Tracepath uygulaması sadece Linux işletim sistemlerinde bulunmaktadır. Windows için de bu işi yapacak değişik uygulamalar geliştirilmiştir. Şekil 4.15’te bir tracepath örneği gösterilmektedir.

```
debianSoftware:~# tracepath6 www.sixxs.net
1: [LOCALHOST] pmtu 1500
1: yonlendirici.mustafa.ipv6 0.746ms
2: yonlendirici.mustafa.ipv6 asymm 1 0.608ms pmtu 1280
2: gw-123.lon-01.gb.sixxs.net 217.661ms
3: fa0-0.712-IPv6-necromancer.sov.kewlio.net.uk 226.440ms
4: 2001:7f8:5::704b:1 asymm 5 217.352ms
5: ge0-2-0-32.br0.bebru1.realroute.net asymm 6 288.10ms
6: ge2-0-0-32.br1.nlams1.realroute.net asymm 7 281.727ms
7: ams-ix.ipv6.concepts.nl asymm 8 306.490ms
8: se1.breda.ipv6.concepts-ict.net asymm 9 303.632ms
9: noc.sixxs.net 307.642ms reached
Resume: pmtu 1280 hops 9 back 9
```

Şekil 4.15: Tracepath örneği

5. SONUÇLAR

İnternet kullanımındaki ve TCP/IP kullanan cihaz sayısındaki öngörülemeyen artış 1981 yılında geliştirilen İnternet Protokolü'nde bir takım değişiklikler yapılmasını zorunlu kılmıştır. Uzun süren toplantılar sonucunda mevcut IPv4 yapısını değiştirmek yerine adres aralığı sorununu tamamen ortadan kaldıracak ve görülen diğer eksiklikleri giderecek yeni bir protokol geliştirilmesine karar verilmiştir. 1995 yılında yeni protokol IPv6 adı ile standartlaştırılmış ve 128 bit adres uzunluğu ile çok geniş bir adres aralığı sunulmuştur. Ayrıca yönlendirici tablolarındaki şişmeleri engelleyecek ve işlemci zamanını azaltacak paket yapısı ve paket eklenti başlıkları geliştirilmiştir. IPv6 ile otomatik yapılandırma sağlanmış, güvenlik ve servis kalitesi özellikleri geliştirilmiştir.

IPv6'nın şu andaki önceliği ülkeden ülkeye değişmektedir. Uzak Doğu ülkeleri hızlı bir şekilde IPv6 bağlantıları kurmakta ve yeni yazılım ve donanımlar geliştirmektedir. Avrupa ülkeleri araştırma ortamlarında ve üniversitelerde bu yapıyı test etmektedir. A.B.D.'de ise, IPv4 adres aralığı uzun süre yetecek olmasına rağmen, teknolojiden geride kalmamak amacıyla yeni nesil İnternet Protokolü çalışmaları hükümetin de desteğiyle bir çok ortamda yapılmaktadır. IPv6'ya dünya çapında tamamen geçişin 10 yıl içinde tamamlanacağı hesaplanmaktadır.

Bu çalışmanın uygulaması kapsamında öncelikle Londra ile kurulan tünel mekanizması ile IPv6 İnternet bağlantısı sağlanmış ve RIPE NCC'den /48'lik bir adres aralığı alınmıştır. Bu adres aralığı ile 2^{16} adet ağa, her bir ağda 2^{64} adet uç nokta olacak şekilde IPv6 adresi verilebilmektedir. Yani 2^{80} adet uç nokta desteklenebilmektedir.

Daha sonra orta ölçekli bir ağda bulunması gereken Web, DNS, FTP, E-posta gibi sunucular kurulmuş ve IPv6 destekleyecek yapıya getirilmiştir. Ayrıca Web üzerinden çalışan IPv6 PHP uygulamaları yazılmıştır. Son olarak da ağ yönetiminde kullanılacak yazılımların IPv6 destekleri test edilmiştir.

Açık kaynak kodlu yazılımların diğer ticari yazılımlara göre IPv6 konusunda çok daha önde olduğu görülmüştür. Bunun nedeni açık kaynak kodlu yazılımların herhangi bir kar amacı gütmeyen dünya çapındaki gereksinimler doğrultusunda ortaya çıkmasıdır. IPv6 dünyası genişledikçe yeni nesil protokolü destekleyen yazılım ve donanım sayısı artacak, sistem geçişi yavaş yavaş son kullanıcılara hissettirilmeden gerçekleşecektir.

Kurulan laboratuvar ve yapılan bu testler sonucunda IPv6 sistem geçişinin mevcut bir çok servis ve uygulama için gerçekleştirilebildiği görülmüştür. Ayrıca sistemin sadece IPv6 kullanılacak yapıya ulaşana kadar geçecek sürede IPv4 ile de uyumlu bir şekilde çalışabilirliği de test edilmiştir. Ancak yeni protokolün yapısının karmaşık olmasından ve geçişin sadece IP'nin bulunduğu Ağ Katmanını değil diğer birçok katmanı da etkilemesinden dolayı geçişin dünya çapında çok hızlı bir şekilde gerçekleştirilemediği fark edilmiştir. IPv6'nın daha fazla yaygınlaşabilmesi için ağ uzmanlarının, yazılım ve donanım geliştiricileri birlikte çalışmaları gerekmektedir.

Test laboratuvarında kazanılan tecrübeler ve IPv6 konusundaki teorik bilgi sayesinde, artık IPv6 sistem geçişinin bir ağ içinde tamamlanması sağlanabilmektedir. Test laboratuvarı kurulumu sonrasında, IPv6 ile ilgili tüm ağ, uygulama ve donanım testleri yapılabilmekte ve IPv6 protokolünün yaygınlaşmasına da katkıda bulunulabilmektedir. Ancak IPv6'nın donanımsal ve yazılımsal olarak daha kullanışlı hale getirilmesi gerekmektedir. IPv6'ya olan talep arttıkça arz da aynı oranda artacaktır.

Bundan sonra sistem performans ölçümü ve iyileştirmesi üzerine çalışılabilir. IPv6, sistem geçişi için çok büyük oranda hazır olmasına rağmen protokol performansı alanında yapılması gereken çok fazla iş bulunmaktadır. Şu anda daha çok tünel mekanizmaları kullanılmaktadır. Yeni nesil protokolün yaygınlığı az olduğu için IPv6 performansı tam olarak IPv4 ile karşılaştırılamamaktadır. Performans konusunda iyileştirmeler yapılması gerekmektedir. Bir diğer konu olarak, IPv4'te de çok fazla önemli olan, güvenlik konusu üzerinde çalışılabilir. NAT'ı ortadan kaldırmayı amaçlayan IPv6 için daha fazla güvenlik uygulamaları geliştirilmelidir. IPsec protokolü kullanan yazılımlarla iletim veya tünel şifreleme mekanizmaları sayesinde güvenlik artırımı sağlanabilir.

KAYNAKLAR

- [1] **Hauben, M.**, “History of ARPANET”, <<http://www.dei.isep.ipp.pt/docs/arpa--1.html>>.
- [2] **Griffiths, R.T.**, 2002. “From ARPANET to World Wide Web”, <<http://www.let.leidenuniv.nl/history/ivh/chap2.htm> >.
- [3] **Huitema, C.**, 1995. “Routing in the Internet”, Prentic-Hall, New Jersey.
- [4] **Cisco Systems**, 2005. “IPv6 Tutorial”, South Asian Network Operators Group <<http://www.sanog.org/resources/sanog5-pfs-ipv6-tutorial.pdf>>
- [5] **RFC 1819**, 1995. “Internet Stream Protocol Version 2 (ST2)”, IETF RFC Belgesi.
- [6] **McQuerry, S.**, 2004. “CCNA Self-Study, Interconnecting Cisco Network Devices (ICND)”, Cisco Pres, Indianapolis.
- [7] **RFC 791**, 1981. “Internet Protocol”, IETF RFC Belgesi.
- [8] **Bolat, A.**, 2004. “Mobil IP: Mevcut Düzenlemeler ve Türkiye Önerileri”, Uzmanlık Tezi, Telekomünikasyon Kurumu.
- [9] **A.Hall, E.**, 2000. “Internet Core Protocols”, O’Reilly, California.
- [10] **RFC 1122**, 1989. “Requirements for Internet Hosts -- Communication Layers”, IETF RFC.
- [11] **RFC 826**, 1982. “An Ethernet Address Resolution Protocol”, IETF RFC Belgesi.
- [12] **RFC 903**, 1984. “A Reverse Address Resolution Protocol”, IETF RFC Belgesi.
- [13] **RFC 977**, 1986. “Network News Transfer Protocol”, IETF RFC Belgesi.
- [14] **RFC 821**, 1982. “Simple Mail Transfer Protocol”, IETF RFC Belgesi.
- [15] **RFC 1519**, 1993. “Classless Inter-Domain Routing”, IETF RFC Belgesi.
- [16] **RFC 1597**, 1994. “Address Allocation for Private Internets”, IETF RFC Belgesi.
- [17] **Gai, S.**, 1998. “Internetworking IPv6 with Cisco Routers” McGraw-Hill.

- [18] **RFC 3513**, 2003. “Internet Protocol Version 6 (IPv6) Addressing Architecture”, IETF RFC Belgesi.
- [19] **RFC 4291**, 2006. “IP Version 6 Addressing Architecture”, IETF RFC Belgesi.
- [20] **RFC 1546**, 1993. “Host Anycasting Service”, IETF RFC Belgesi.
- [21] **IEEE Standards Tutorials**, “Guidelines for 64 Bit Global Identifier Registration Authority”,
<<http://standards.ieee.org/regauth/oui/tutorials/EUI64.html>>
- [22] **RFC 2460**, 1998. “Internet Protocol, Version 6 (IPv6) Specification”, IETF RFC Belgesi.
- [23] **RFC 2463**, 1998. “Internet Control Message Protocol (ICMPv6)”, IETF RFC Belgesi.
- [24] **RFC 2710**, 1999. “Multicast Listener Discovery (MLD) for IPv6”, IETF RFC Belgesi.
- [25] **RFC 2461**, 1998. “Neighbor Discovery for IP Version 6 (IPv6)”, IETF RFC Belgesi.
- [26] **Davies, J.**, 2003. “Understanding IPv6”, Microsoft Press, Washington.
- [27] **RFC 1256**, 1991. “ICMP Router Discovery Messages”, IETF RFC Belgesi.
- [28] **RFC 2080**, 1997. “RIPng for IPv6”, IETF RFC Belgesi.
- [29] **RFC 2740**, 1999. “OSPF for IPv6”, IETF RFC Belgesi.
- [30] **Hopps, C.E.**, 2005. “Routing IPv6 with IS-IS”. IETF Internet Draft,
<<http://www.ietf.org/internet-drafts/draft-ietf-isis-ipv6-06.txt>>.
- [31] **RFC 2545**, 1999. “Use of BGP-4 Multiprotocol Extensions for IPv6 Inter Domain Routing”, IETF RFC Belgesi.
- [32] **RFC 1886**, 1995. “DNS Extensions to Support IP Version 6”, IETF RFC Belgesi.
- [33] **RFC 2462**, 1998. “IPv6 Stateless Address Autoconfiguration”, IETF RFC Belgesi.
- [34] **RFC 3315**, 2003. “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, IETF RFC Belgesi.
- [35] **Stolze, A.**, 2005. “DHCPv6 Implementation and Test Report Version 3”, 6NET,
<<http://www.6net.org/publications/deliverables/D3.2.3v3.pdf>>.

- [36] **Cisco IOS Learning**, 2002. "The ABCs of IPv6", Understanding the Essentials Series, <http://www.cisco.com/application/pdf/en/us/guest/products/iosswrel/c1127/cdccont_0900aecd8018e369.pdf>.
- [37] **Microsoft White Paper**, 2005. "IPv6 Transition Technologies", <<http://download.microsoft.com/download/7/4/1/741daf62-02d6-40f3-b082-701b5acc56d6/IPv6Trans.doc>>.
- [38] **RFC 2893**, 2000. "Transition Mechanisms for IPv6 Hosts and Routers", IETF RFC Belgesi.
- [39] **RFC 3056**, 2001. "Connection of IPv6 Domains via IPv4 Clouds", IETF RFC Belgesi.
- [40] **RFC 4380**, 2006. "Teredo: Tunneling IPv6 over UDP", IETF RFC Belgesi.
- [41] **Microsoft TechNet**, 2005. "Changes to IPv6 in Windows Vista and Windows Server Longhorn", <<http://www.microsoft.com/technet/community/columns/cableguy/cg1005.mspx>>.
- [42] **Microsoft TechNet**, 2005. "Troubleshooting IPv6", <<http://www.microsoft.com/technet/community/columns/cableguy/cg0305.mspx>>.
- [43] **RIPE NCC**, 2006. "About the RIPE NCC", <<http://www.ripe.net/info/ncc/index.html>>.
- [44] **RFC 3053**, 2001. "IPv6 Tunnel Broker", IETF RFC Belgesi.
- [45] **Linux Reviews**, 2001. "Configuration File of Router Advertisement Daemon", <<http://linuxreviews.org/man/radvd.conf>>.
- [46] **Cisco Documentation**, "Simple Network Management Protocol", <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid1>.
- [47] **RFC 3584**, 2003. "Coexistence between Version 1, Version 2, and Version 3 of the Internet-Standard Network Management Framework", IETF RFC Belgesi.
- [48] **Colitti, L.**, 2006. "MRTG – IPv6", <<http://oss.oetiker.ch/mrtg/doc/mrtg-ipv6.en.html>>.

ÖZGEÇMİŞ

Mustafa Şahin, 1981 yılında Konya’da doğmuştur. İlkokul öğrenimini Çankaya İlkokulu’nda, ortaokul ve lise öğrenimini Mersin Anadolu Lisesi’nde tamamlamıştır. 1999 yılında İstanbul Teknik Üniversitesi (İTÜ) Elektronik ve Haberleşme Mühendisliği bölümü lisans programına, 2003 yılında da İTÜ Telekomünikasyon Mühendisliği bölümü yüksek lisans programına başlamıştır.

2000-2003 yılları arasında İTÜ Uzaktan Eğitim Merkezi’nde (UZEM) yarı zamanlı asistan olarak çalışmıştır. 2003 yılında uzman kadrosunda çalışmaya başlamıştır. Halen UZEM’de uzman olarak çalışmaktadır.