T.C.
MARMARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

IPv6 ADRESLEME SİSTEMİNİN GENEL YAPISI VE GÜVENLİK YENİLİKLERİNİN İNCELENMESİ

Emre DURDAĞI

YÜKSEK LİSANS TEZİ

ELEKTRONİK-BİLGİSAYAR EĞİTİMİ ANABİLİM DALI

ELEKTRONİK-HABERLEŞME EĞİTİMİ PROGRAMI

DANIŞMAN

Yrd. Doç. Dr. Ali BULDU

İSTANBUL 2010

T.C.
MARMARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

IPv6 ADRESLEME SİSTEMİNİN GENEL YAPISI VE GÜVENLİK YENİLİKLERİNİN İNCELENMESİ

Emre DURDAĞI

(141101020050007)

YÜKSEK LİSANS TEZİ

ELEKTRONİK-BİLGİSAYAR EĞİTİMİ ANABİLİM DALI

ELEKTRONİK-HABERLEŞME EĞİTİMİ PROGRAMI

DANIŞMAN

Yrd. Doç. Dr. Ali BULDU

İSTANBUL 2010

TEŞEKKÜR

Çalışmalarım boyunca desteğinden dolayı danışman hocam Yrd. Doç. Dr. Ali BULDU'ya, özveriyle yardımlarından dolayı mesai arkadaşım, değerli büyüğüm Ömer ŞANLI Bey'e ve beni hiçbir zaman yalnız bırakmayan aileme teşekkür ederim.

İÇİNDEKİLER

SAYFA

ÖZET

IPV6 ADRESLEME SİSTEMİNİN GENEL YAPISI VE GÜVENLİK YENLİKLERİNİN İNCELENMESİ

İnternet Protokol versiyon 6 (IPv6), şu anda aktif olarak kullanılan ve ilk uygulanan internet protokolü olan IPv4'ü geliştirmek için dizayn edilmiştir. IPv4 adresleri 32 bitten oluşurlar ve teorik olarak 4.3 milyar adresi destekleyebilirler. Günümüzde teknolojinin hızla ilerlemesiyle internet kullanımı her geçen gün artmakta ve mevcut 4,3 milyar adetlik adres sayısı yetersiz kalmaktadır. IPv4 protokolündeki adres yetersizliğine çözüm olarak CIDR (Classless Inter-Domain Routing) ve NAT (Network Address Translation) gibi yeni teknolojiler geliştirilmiş olsa da uygulamalara getirmiş oldukları zorluklar ve günümüz internet ihtiyaçlarına yetersiz kalmaları nedeniyle istenilen seviyeye gelinememiştir. IPv4 adreslerinin yakın gelecekte tükenecek olması, IPv6 internet protokolünün geliştirilmesinde en önemli faktördür . IPv6, Aralık 1998 tarihinde Internet Engineering Task Force (IETF) tarafından RFC 2460 İnternet Standartı olarak tanımlanmıştır.

IPv6 128 bitlik adres yapısılya 3.4×10^{38} adet gibi tükenmesi çok zor olan ve IPv4'e göre çok daha büyük bir adres kapasitesine sahiptir. Bu adres artışı kullanıcılara adres tahsis etmede ve routing trafiklerinde daha esnek hareket etme şansı getirmiştir. Ticari olmayan kullanım için geliştirilmiş IPv4 yapısına karşın, IPv6 günümüzde çok daha önemli hale gelmiş gerçek zamanlı görüntü-ses aktarımı, mobilite ve güvenlik gibi konuları esas alarak geliştirilmiştir. Bununla birlikte NAT uygulamasına ihtiyaç duyulmayacak olmasından dolayı uçtan uca direk bağlantı kurulabilecek ve IPSec kullanımının yaygınlaşacağı öngörülmektedir.

Bu çalışmada, IPv6 genel yapısı, eski versiyon olan IPv4 ile aralarındaki farklar, getirmiş olduğu yenilikler ve güvenlik konuları incelenmiştir. Güvenlik uygulamalarında IPv4 ile aynı olan saldırı türlerinin yanında ve IPv6 ile birlikte ortaya çıkmış yeni saldırı türleri test edilmiştir. Ayrıca IPv4 ile karşılaştırmalı olarak IPSec uygulamaları yapılmış ve değerlendirilmiştir

Eylül,2010 **Emre DURDAĞI**

ABSTRACT

GENERAL STRUCTURE OF IPv6 ADDRESSING SYSTEM AND EXAMINING SECURITY INNOVATION

Internet Protocol version 6 (IPv6) is an Internet Protocol version which is designed to succeed IPv4, the first implementation which is still in dominant use currently. IPv4 addresses consist of 32 bits and it can support theoretically 4,3 billion addresses. Today's rapid advances in technology, internet usage is increasing every day and 4,3 billion current IPv4 addresses is insufficient. As a solution for lack of IPv4 addresses, some new technologies are developed, such as CIDR and NAT. But because of implementation challenges and inadequate to the needs of today's internet, could not get to exactly the desired level. The main driving force for the redesign of Internet Protocol is the foreseeable IPv4 address exhaustion. IPv6 was defined in December 1998 by the Internet Engineering Task Force (IETF) with the publication of an Internet standard specification, RFC 2460.

According to IPv4, IPv6 with 128 bits address architecture has great address capacity which is difficulty to run out. This expansion provides flexibility in allocating addresses and routing traffic. Although IPv4 that developed for non-commercial use, IPv6 has been designed based on realtime data transfer, mobility and security has become much more important today. In addition to this end to end connection can be established between host without using NAT. So widespread use of IPsec are expected.

In this study, the general structure of IPv6, the differences between the old version IPv4, innovation and safety issues are investigated. In security applications, as well as the same type of attack for IPv4, the new types of attacks that emerged along with IPv6 have been tested and evaluated.

September,2010 **Emre DURDAĞI**

KISALTMALAR

OSI : Open Systems Interconnection
QoS : Quality of Service
IETF : Internet Engineering Task Force
NAT : Network Address Translation
NAT-PT : NAT with Protocol Translator
DOS : Denial of Service
DDOS : Distributed Denial of Service
ICMP : Internet Control Message Protocol
ISP : Internet Service Provider
IP : Internet Protocol
TTL : Time to Live
RFC : Request for Comments
IANA : Internet Assigned Numbers Authority
TLV : Type-Length-Value
MTU : Maximum Transmission Unit
ICV : Integrity Check Value
IPSec : IP Security Protocol - IP Güvenlik Protokolü
MAC : Media Access Control
ARP : Address Resolution Protocol
DHCP : Dynamic Host Configuration Protocol
DNS : Domain Name System
NTP : Network Time Protocol
OSPF : Open Shortest Path First
AH : Authentication Header
ESP : Encapsulating Security Payload
IKE : Internet Key Exchange
ISAKMP : Internet Security Association and Key Management Protocol
IDS : Intrusion Detection System
RAID : Redundant Array of Inexpensive Disks
RH0 : Routing Header Type 0

ŞEKİLLER

SAYFA

TABLOLAR

SAYFA

BÖLÜM I

I. GİRİŞ VE AMAÇ

I.1 GİRİŞ

I.1.1 İnternet Protokolü Versiyon 6 (IPv6)

Internet Protokolü (IP), günümüzün vazgeçilmezi olan İnternet yapısının en temel bileşenidir. İnternet üzerinden haberleşmek isteyen iki bilgisayar arasındaki haberleşme bu protokol vasıtasıyla gerçekleşir. IP, OSI modelinde 3, TCP/IP modelinde ise 2. katmanda yer almakta ve bir ağda uçtan uca (end-to-end) veri yönlendirmesi için kullanılmaktadır. Amaç izlenen yollardan ve ağlardan bağımsız olarak hedef cihaza iletimin sağlanmasıdır. Yol belirleme ve veriyi o yola yönlendirmek için paket anahtarlama bu seviyede yapılmaktadır. Ayrıca bu yapı Internet üzerindeki bir cihaza (bilgisayar ya da yönlendirici ara yüzlerine) mantıksal adres sağlar. IP, 1970'li yılların başında geliştirilmeye başlanmış ve 1981'de tanımlamaları RFC 791 ile yapılmıştır. Önceleri küçük bir araştırma ağında kullanılmaya başlanılan TCP/IP bugün milyonlarca elemanı olan Internet'in temel protokolü haline gelmiştir.

İnternet ve iletişim teknolojilerinin başlangıç noktasından çok farklı yerlere gelmesi nedeniyle IPv4 bugünkü ihtiyaçları karşılayamaz duruma gelmiş ve yeni protokolün tasarlanması kaçınılmaz hale gelmiştir. Bu yüzden IETF (Internet Engineering Task Force) tarafından yürütülen çalışmalar sonucunda 128 bitlik adres yapısına sahip IPv6 (başlarda IP-The Next Generation – IPng olarak adlandırılmıştı) geliştirilmiştir (RFC 2460). IP'nin bu yeni versiyonu birçok yenilik getirmiştir.

Internet Assigned Numbers Authority (IANA), IPv4 adreslerinin 2012 yılında biteceğini öngörmektedir. NASA, Savunma Dairesi gibi Amerikan Kamu Kurumları 2008 ortası itibariyle IPv6'ya geçmeyi planlamışlardır. IP adres sıkıntısı çeken Çin 1998 yılından beri IPv6 geçiş çalışmalarını sürdürmektedir. IPv4 adreslerin ömrünü biraz daha uzatmaya yönelik CIDR ve NAT gibi çalışmalar mevcut olsa bile, bunlar süreyi biraz uzatmaktan öteye gidemeyecek ve kaçınılmazı fazla erteleyemeyecektir.

1970'lerin sonlarında STP (Stream Protocol) adında geliştirilen, servis kalitesi sağlayan, ses ve video iletimini amaçlayan bir protocol geliştirilmişti. 1990'ların

sonlarında tekrar gözden geçirilip bir kaç ticari projede kullanılmıştı. Fakat pratikte çok da fazla yaygınlaşamayan bu protokol IPv5 ismini almıştır. Her hangi bir karışıklığa sebebiyet vermemek için yeni IP versiyonunun adı IPv5 değil de IPv6 olmuştur.

Yeni bir protokole ihtiyaç duyulmasının nedenlerini şu şekilde listeleyebiliriz:

Yetersiz Kalan IP adresleri: Bilindiği gibi IPv4 32 bitlik adresleme kapasitesine sahiptir. Bu da teorik olarak Internet üzerinde 2^{32} adet interface'in adreslenebileceği anlamına gelmektedir. Teorik olarak 2^{32} olan adresleme kapasitesi, uygulamada alt ağlara ayrılma, özellikle A sınıfı dağıtılmış olan IP adreslerinin bir kısmının kullanılmaması gibi nedenlerden dolayı bu sayıdan çok daha düşüktür. Var olan IPv4 adreslerinin %60'ı Amerika Birleşik Devletleri tarafından kullanılırken %40'lık kısım Dünya'nın geri kalanı tarafından paylaşılmaktadır. Yani IPv4 adreslerinin %60'ı, Dünya nüfusunun %5'ine tahsis edilmiştir. Diğer yandan, Çin ve Hindistan gibi nüfusu çok fazla olan ülkelerde IP adresi ihtiyacı hızla artmaktadır. Ayrıca, mobil cihazlara, oyun konsollarına hatta arabalara bile İP adresi verilmesi bir diğer önemli elken olmuştur. 1993 yılında bu sorunu çözmek için IETF tarafından IPng (IP next generation) çalışmaları başlatılmıştır. [1] Türkiye'ye ayrılan adresler ise sadece %0,33'lük bir bölümü oluşturmaktadır. Yine Standfrod ve MIT'nin tek başlarına rezerve ettikleri adres uzayı Çin için rezerve edilen adres uzayından daha fazladır. Her ne kadar NAT (Network Adress Translation) gibi sonradan eklenen sistemler geliştirilse bile IPv4'ün doğal yapısında yer almayan bu tür çözümler uçtan uca direk erişimin sağlanamaması (özellikle P2P uygulamalar, Voice Over IP, IPsec) gibi bir takım problemlere yol açmaktadır.

Performans ve Birlikte Çalışabilirlik Gereksinimleri: IPv4 paketleri, karışık bir başlık yapısına sahiptir. Bu da veri akışı sırasında özelikle yönlendiriciler tarafında bir hız kaybına neden olmaktadır. Ayrıca IPv4 başlıklarının fragmantasyonu ve CRC denetimi hem router'larda performans düşüşüne sebep olmakta hem de güvenlik tarafında bir takım sorunlara sebep olmaktadır. Ayrıca protokolün doğası gereği desteklemediği bazı uygulamalar için sistemler (routers, packet filters, intrusion detection systems) arasında tam bir standardın oturtulamaması nedeniyle bir takım problemler ortaya çıkmaktadır.

Yetersiz Servis Kalitesi (Quality of Services – QoS) desteği: Internet üzerinde artan hız ve bant genişlikleri ile birlikte, ses ve görüntü gibi yüksek büyüklükte verilerin taşınması mümkün hale gelmiştir. Fakat IPv4'ün (Type of Service) yetersiz kalan QoS desteği ile gerçek zamanlı ses ve görüntü aktarımında sorunlar ortaya çıkmaktadır. Ayrıca gelişmiş bir QoS desteği, ağ yöneticilerine, istenmeyen ağ trafiğini en aza indirmeye yardımcı olacak özelliklere de sahiptir. Özellikle ara cihazların (genelde yönlendiricilerin) tümüyle destekleyeceği yeni bir yapıya ihtiyaç duyulmaktadır.

Daha kolay yapılandırma ihtiyacı: Pv4'te IP adres yapılandırılması elle veya DHCP (Domain Host Configuration Protocol) ile yapılmaktadır. Manuel olarak yapılandırılmayan ya da DHCP sunucudan IP adresi alamayan bazı sistemler için APIPA (Automatic Private IP Addressing) gibi mekanizmalar geliştirilmiş olmasına rağmen APIPA tam bir çözüm olmadığı açıktır. Sonuç olarak, IP adreslerinin dağıtımı, otomatik olarak harici bir protokol veya mekanizmaya ihtiyaç duymadan (plug and play) düzgün bir şekilde yapılmasını sağlayan bir protokole ihtiyaç duyulmaktadır.

Mobil kullanıcı desteği: IPv4 ilk çıktığında hareketli kullanıcılar hiç düşünülmemişti. Protokol üzerine giydirilmiş bir takım mekanizmalar ile hareketli kullanıcıların ağa dahil olup iletişim kurmaları sağlanmaktadır. Bu durum özellikle güvenlik sorunlarına yol açmaktadır. Her ne kadar Mobil IPv4 mobil kullanıcılar için bir takım çözümler getirse de doğası gereği hareketli kullanıcıları ve iletişimi destekleyecek bir protokole ihtiyaç duyulmaktaydı.

IP Seviyesinde Güvenlik İhtiyacı: Başlarda sınırlı sayıda kullanıcıya hizmet vermek amacıyla geliştirilen protokol zaman içerisinde, Internet'in hızla gelişimiyle birlikte birçok güvenlik açığı içerir hale gelmiştir. Protokol üzerine IPsec (IP Security) gibi uygulamalar ile veri doğrulama, içerik bütünlüğü ve gizlilik gibi özellikler eklense bile, gerek mekanizmanın protokolün doğası içerisinde olmaması gerekse ara cihazlar (özellikle router'lar) tarafından IPsec'in desteklenmemesi ile, IPsec VPN uygulamasından öteye taşınamamıştır. Ayrıca IPv4 paket header'larının fragmenteye uğraması, IDS'ler (intrusion detection systems) tarafından algılanması

güç ataklara meydan vermektedir. Bunlar birlikte dar IP uzayı nedeniyle hedef network'deki aygıtlara ait bazı bilgilerin (IP adresi, aktif servisler ve aktif port numaraları) toplanması oldukça kolay olmaktadır. Güvenlik özelliklerini kendi bünyesinde barındıran, adresleme yapısıyla istenen ölçüde gizlilik - privacy sağlayan bir protokole ihtiyaç duyulmaktaydı.

I.1.2 Türkiye' deki Durum

IPv6 konusundaki Ar-Ge çalışmalarına 2003 yılı başında başlayan TÜBİTAK - ULAKBİM, Avrupa Akademik Ağı GEANT'a olan İnternet bağlantısındaki hazırlıklarını tamamlayarak 30 Mayıs 2003'te ULAKNET'e bağlı olan tüm üniversitelerin ve araştırma kurumlarının GEANT'a saf IPv6 bağlantısı yapabilmesi için gereken omurga altyapısını oluşturmuş; 2004 yılının başından itibaren talep eden üniversitelere IPv6 adreslerini tahsis edebilecek duruma gelmiş; ve Şubat 2004'te düzenlenen Akademik Bilişim'de tüm üniversitelere IPv6 teknolojisinin tanıtımını yapmıştır. IPv6 protokolünün gelişimini, IPv6'ya geçişte yaşanacak sorunları ve çözüm yollarını, ve dünyadaki IPv6 Ar-Ge çalışmalarını takip eden TÜBİTAK - ULAKBİM, 2006 yılı sonunda 6 üniversitenin de katılımıyla ULAK6NET Görev Gücü'nü oluşturmuştur.

Telekomünikasyon Kurumu tarafından hazırlanan "Mobil IP: Mevcut Düzenlemeler ve Türkiye Önerileri" başlıklı kurum tezinde IPv6 konusu ağırlıklı olarak işlenmiş; tez çalışması kapsamında, İşletmeciler ve ISS'lara 2004 yılında yapılan anket çalışması sonucunda, ISS'ların bir bölümünün IPv6 uyumlu donanım altyapısına sahip oldukları ve geçişe istekli oldukları öğrenilmiştir. Telekomünikasyon Kurumu'nun 2007 iş planında IPv6 ile ilgili stratejik hedefi "IPv6, IPv4'ün yerini alacak olan güvenlik, mobilite ve servis kalitesi gibi yeni servisler için artan talepler ile IP adres kapasitesinin tükenmesi problemlerinin tamamen üstesinden gelebilmek için yeni ağ katmanı protokolüne ülkemizde geçiş sürecini başlatmak, dönüşüm maliyetlerini azaltmak, altyapıda kullanılacak yazılım ve donanımlarda yerli katkı payını yüksek tutmaya yönelik stratejik planın hazırlanması amaçlanmaktadır" şeklinde yer almıştır.

14 Şubat 2007'de Telekomünikasyon Kurumu ile TÜBİTAK - ULAKBİM arasında imzalanan Ar-Ge İşbirliği Protokolü ile yeni nesil teknolojilere geçişin ulusal çapta hız kazanması ve Türkiye'nin teknolojik alanda öncü bir rolü üstlenerek

bilişim ve telekomünikasyon sektörlerinde üretime dayalı bir konumda olması hedefleri bir kez daha vurgulanmıştır.

ULAKBİM, Çanakkale 18 Mart üniversitesi ve Gazi Üniversitesi işbirliği ile TÜBİTAK KAMAG projeleri arasında yer alan "Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi" Şubat 2009'da başlatıldı.

Türkiye'de IPv6 adresi alan üniversiteler ise

Orta Doğu Teknik Üniversitesi (Ocak 2004)
Sabancyı Üniversitesi (Ocak 2004)
Çukurova Üniversitesi (Ocak 2004)
Bahçeşehir Üniversitesi (Mart 2004)
Selçuk Üniversitesi (Nisan 2004)
Dogu Akdeniz Üniversitesi (Mayıs 2004)
Uludağ Üniversitesi (Ocak 2005)
Çanakkale 18 Mart Üniversitesi (Ekim 2005)
Gazi Üniversitesi (Mart 2007)
Marmara Üniversitesi (Nisan 2007)
Celal Bayar Üniversitesi (Nisan 2007)
Bilkent Üniversitesi (Nisan 2007)
Boğaziçi Üniversitesi (Nisan 2007)

I.1.3 Dünya Ülkerlerindeki Durum

1990'lı yılların başından itibaren tüm dünyadaki bilişim teknolojileri bilim insanları IPv4 teknolojisindeki eksiklikler ve sorunların giderilmesi için araştırma ve geliştirme faaliyetlerinde bulunmaktadır. Bu çalışmaların bir ürünü olan Yeni Nesil İnternet teknolojilerinin, var olan hizmetleri kesintiye uğratmadan yaygın olarak kullanılmaya başlanması, üzerindeki yeni nesil uygulamaların kararlılığının ve güvenliğinin sağlanması, sağlam ve güvenilir bir geçiş sisteminin belirlenmesini zorunlu kılmaktadır. Bu yüzden bu konuda yapılmış çok sayıda bilimsel çalışma bulunmaktadır. Çalışmalar arasında belirli bir ülkeye veya bölgeye has geçiş sistemlerini ele alan araştırmalar olduğu gibi, ülkelerin ekonomik ve teknolojik yapısından bağımsız, salt teknoloji odaklı araştırmalar da mevcuttur. Örneğin Japon Gigabit Ağı üzerinde yapılan çalışmada IPv4'ten IPv6'ya geçişte ne tür bir yöntem

izlenmesi gerektiği tartışılmış; öncelikle IPv4 ve IPv6 adres ataması için, ağa bağlı uçların ve yönlendiricilerin güncellenmesi ve/veya konuşlandırılması için, IPv6 destekli DNS'lerin hizmete girmesi için metodolojilerin belirlenmesi, kurumsal düzeyde ve sonrasında tüm İnternet düzeyinde IPv6 uyumluluğunun sağlanabilmesi için geçiş senaryolarının oluşturulması gerekliliği belirtilmiştir. Yine bir başka bilimsel çalışmada, DSL teknolojisinde IPv6'ya geçişin servis kesintisi olmaksızın en iyi şekilde yapilabilmesi için ISS'lerin anahtar bir rolde olduğuna dikkat çekilmiş; Telekom operatörlerinin ve ISS'ların IPv4 ve IPv6 servislerinin şeffaf bir şekilde birlikte çalışabilirliğini ve ileri düzey uygulamaların olgunlaşmış işlevlerini dikkate alan yumuşak bir geçiş stratejisinin benimsenmesi gerektiği savunulmuştur. Ruri Hiromi ve Hideaki Yoshifuji, Japonya'daki WIDE projesinin altında IPv6 konuşlandırması ile ilgili sorunları belirleme amacındaki özel bir araştırma grubu olan IPv6-Fix bünyesindeki çalışmalarında, çift yığın mekanizmasıyla IPv4'ten IPv6'ya geçişte ağ, DNS ve güvenlik duvarında kaynaklanabilek sorunlardan bahsetmiştir. Yine çift yığın mekanizmasını konu alan, ve IPv4 uçların IPv6 uçlara oturum başlatabilmelerini inceleyen çalışma , SIP tabanlı VoIP uygulamaları için iki ayrı geçiş mekanizmasını inceleyen Tayvan'daki çalışma, ve mobil ağların IPv6 uyumlu hale getirilmesi için yapılan araştırmalardan bahsedilen çalışma , IPv6 geçişi ile ilgili araştırmalara örnek olarak gösterilebilir.

Geçiş mekanizmaları ve birlikte çalışabilirlik üzerine yapılan araştırmaların yanısıra, IPv6 ile birlikte gelen yeni uygulamalar ve güvenlik üzerine yapılmış bilimsel çalışmalar da mevcuttur. Örneğin IPv6 yönlendirme başlığındaki güvenlik sorunlarını ele alan bir çalışmada, olası saldırıları engellemek amacıyla güvenlik duvarına eklenecek bir koruma algoritmasının ayrıntıları verilmiştir . Yine güvenlik konusunda yapılan bir çalışma, IPv6 ağlarındaki komşu keşfi protokollerinden kaynaklanan servis dışı bırakma ve dağıtık servis dışı bırakma saldırılarının IPSec ile önlenebileceğini gösteren deneylerden bahsetmiştir.[2]

Ülke veya bölge bazında gerçekleşen yeni nesil internet teknolojilerini araştırma çalışmalarını Uzakdoğu, Avrupa ve ABD olarak gruplamak mümkündür.

I.1.4 Uzakdoğu

Japonya, IPv6 teknolojileri konusunda en çok Ar-Ge yapan ülkelerden biri olma özelliğini taşıyor. Japonya, u-japan projesi ile 2010 yılına kadar "herkes, her zaman ve her yerden her uygulama ile bir ağa erişim sağlayabilir" başlığı altında

Japonya'nın "her yeri kapsayan ağ toplumu" olmasını hedeflemekteydi. Projenin diğer bir hedefi ise Japonya'yı dünyanın en gelişmiş bilgi teknolojileri ülkesi haline getirmektir. Japonya'daki İçişleri ve İletişim Bakanlığı (MIC, Ministry of Internal Affairs and Communication) tarafından oluşturulan plan, devlet kurumlarındaki cihaz alımlarında IPv6 desteği olmasını öngören şekilde tasarlanmıştır. Japon stratejisi, sadece IPv6 geçişinin sorunsuz olmasını sağlamayı değil, IPv6 aracılığı ile Japon şirketlerinin küresel bağlamda ufkunu genişletmeyi ve bu konuda yönetici ve yönlendirici bir konuma gelmeyi de içine alan bir stratejidir. Japonya, ABD'nin IPv4 teknolojisinde üstlendiği rolü IPv6 için üstlenme hedefindedir. Japonya'daki IPv6 Tanıtım Kurulu, İnternet'in geliştirilmesinde uluslararası düzeyde öncü olma, ileri düzey bir bilgi ve telekomünikasyon ağ toplumu ortaya çıkarabilmek için gereken insan kaynağını sağlama, ağ ve terminallerin donanım, yazılım ve servisleri ile ilgili yeni iş alanları yaratma ve destekleme amaçlarını taşımaktadır. Tanıtım kurulu tarafından oluşturulan, Japonya'daki 6 şirketin katılımıyla gerçekleşen, ve 2006 yılının Mart ayında tamamlanan Kame projesi BSD tabanlı işletim sistemleri için IPv6 ve IPSec yığın uygulamalarını geliştirme amacını taşıyordu. Projenin tamamlanması, bu amacın gerçekleştiği anlamına gelmektedir. Bir diğer proje olan USAGI projesi Linux tabanlı işletim sistemleri için benzer bir çalışma ile katkıda bulunmuştur. WIDE projesi ise IPv6'yı PC olmayan ortamlarda hayata geçirme çalışmalarını halen sürdürmektedir. IPv6 Tanıtım Kurulu, IPTV, çoklu dağıtım yayınları ve otomobillerin İnternet bağlantısı yapabilmesini hedefleyen Internetcar gibi IPv6 teknolojisini temel alan projelere destek vermeyi sürdürmektedir. InternetCAR projesi, Japonya'nın "her yeri kapsayan ağ toplumu" hedefi doğrultusunda bir proje olan "Zeki Taşıma Sistemleri"nin bir parçası olarak düşünülebilir. Live-E projesi, sensör ağlarını kullanarak dünya üzerindeki çevresel veriyi bir veritabanında toplamakta ve sensörlerle iletişim standartları geliştirilmesine katkıda bulunmaktadır. Dünyanın IPv6 servislerini veren ilk ISS'sı olma özelliğini taşıyan NTT yüksek kalitede görüntülü telefon, çoklu dağıtım ve broadcast hizmetlerini IPv6 üzerinden vermektedir Freebit şirketi tarafından sağlanan IP telefon hizmeti IPv6 ağı üzerinden verilmektedir; sadece başlangıç ve işletim maliyeti değil, kurulum maliyeti, riski ve zamanı da azaltılmış durumdadır. Japonya, analog TV yayınlarını 2011'de sona erdirecek bir yasayı kabul etmiş durumdadır. Uydu ve karasal sayısal dijital yayın seçeneklerinin yanı sıra, Japon hükümeti doğacak boşluğu doldurmak için IPv6 çoklu dağıtım teknolojisinden de

yararlanmayı planlamaktadır. Toshiba şirketi Japonya'da IPv6 çoklu dağıtımı destekleyen LCD HDTV'ler üretmeye başlamış durumdadır. Japonya'daki tüm bakanlık kuruluşlarının e-devlet kapsamında IPv6 geçiş planlarını Mart 2007'ye kadar bitirmeleri istenmiş durumdadır.

IPv6 Ar-Ge çalışmalarının yoğunlukla yapıldığı bir diğer uzakdoğu ülkesi Çin'dir. Çin Hükümeti, 2002 yılında IPv6 test ağı oluşturulması için 170 milyon dolarlık kaynak ayırmıştır. Bir teknolojinin denenmesi için kullanılan en büyük test ağı olan 6TNet, 3 ayrı IPv6 test yatağının 2.5 Gbps bir bant genişliğiyle birbirine bağlanması ile oluşturulmuştur. Çin, dünyada ülke bazındaki İnternet kullanım sıralamasında 2. sıradadır. Eski IPv4 teknolojisinin adres sayısındaki yetersizliği en erken yaşayan ülke olan Çin'de 8 bakanlık ve devlet kurumu tarafından başlatılan CNGI projesinin hedefi, biri akademik (CERNET), beşi ana telekom operatörleri tarafından olmak üzere toplam altı IPv6 ağının, deneyler ve ticari denemeleri gerçekleştirebilmek amacıyla oluşturulmasıdır. Aynı zamanda Avrupa Birliği ve Japonya gibi yabancı ülkelerle de IPv6 konusunda işbirliği yapılmasını hedefleyen proje, örneğin Japonya ile IPv6-CJ projesinin doğmasına da yol açmıştır. Bu proje kapsamında, Çin ve Japonya'nın yeni nesil İnternet üzerinde birlikte çalışması sağlanmış, ağ testi, sistem yapılandırması, uygulamalar ve standardizasyon konularında başarı sağlanmıştır. Çin Devlet Gelişme ve Reform Komisyonu ve Japonya Ekonomi bakanlığının mali desteğini ortaklaşa sağladığı, omurgadaki bant genişliği 2.5 Gbps ve Japonya'daki uç bağlantıların 45 Mbps olduğu IPv6-CJ projesi , Çin Akademik ağı CERNET ve Japonya İletişim ve Bilgi Ağı Ortaklığı CIAJ tarafından ve her iki ülkeden yirmiden fazla Ar-Ge enstitüsünün de katılımıyla hayata geçirilmiştir. Yaklaşık 20 alt-projeye sahip IPv6-CJ projesi ile Beijing, Shanghai ve Guanghozu arasında yüksek hızda bir deneysel IPv6 ağı oluşturulmuş, Japonya'daki deneysel IPv6 ağı ile bağlantısı sağlanmış, anahtar teknolojilerin, çekirdek sistemlerin ve ilişkili servislerin geliştirilmesi sağlanmıştır. 2002'de yapımına başlanan Çin-Japonya IPv6 ağı, 2005 yılında tamamlanarak faaliyete girmiştir .

Güney Kore de IPv6 konusunda Ar-Ge araştırmaları yapan Uzakdoğu ülkelerine örnek olarak gösterilebilir. Güney Kore'nin iletişim bakanlığı tarafından oluşturulmuş IT839 başlıklı bir platformları ve stratejileri bulunmaktadır. Bu strateji kapsamında 2004 yılında KoreV6 araştırma ağını oluşturmuş durumdalar. Bu ağın odak noktası IPv6'yı popüler hale getirmek ve IPv6 ekipman ve çözümlerinin

işlevselliğinin doğrulanmasıdır. Bu amaca yönelik olarak KoreV6 ağı, İnternet, İstek Üzerine Görüntü (Video on Demand) ve IPv6 üzerinden ses (VoIP) gibi hizmetlerin hayata geçirildiği pilot uygulama ağı olma özelliğini de taşımaktadır. Bu ülkedeki gelişmelerin öncülüğünü Samsung ve LG gibi uluslararası saygınlığı olan şirketler yapmaktadır.

Bir diğer örnek Hindistan'dır. Hindistan Telekomünikasyon Düzenleme Otoritesi TRAI , dünyadaki IPv6 çalışmalarının Hindistan ayağının yürütücülüğünü yapmaktadır. TRAI, Ağustos 2005 yılında IPv6 geçiş aşamaları için önerileri içeren bir bildiri yayınlamış durumda [3]. IPv6'ya geçiş konusunda plan hazırlayan Hindistan'ın, devlet desteğiyle oluşturulmuş IPv6 forumları bulunmaktadır. Cisco, SUN, IBM, Samsung gibi büyük şirketlerin Hindistan'da bulunan Ar-Ge üsleri bu ülkedeki IPv6 geliştirme çalışmalarına destek olmaktadır.

Tayvan'da 7 büyük internet servis sağlayıcısı IPv4-IPv6 geçişi için kurumlara donanım dağıtmış ve IPv6 ile çalışan binlerce VoIP telefonu kamu çalışanlarına verilmiştir. Arabalar, kampüsler ve kişisel elektronik cihazlar için IPv6 teknolojisi kullanılmaya başlanmıştır. Tayvan en detaylı IPv6 projelerinden birini yapmaktadır. [4]

I.1.5 Avrupa

IPv6'yı hayata geçirme konusunda yapılan Ar-Ge çalışmaları Uzakdoğu ile sınırlı değildir. 2001 yılında başlatılan Avrupa IPv6 Görev Gücü ve IPv6 Forum çalışmaları, bu alanda Avrupa'nın önemli bir yol katetmesini sağlamıştır. Avrupa Birliği 6INIT, 6WINIT, 6NET, 6DISS ve Euro6ix gibi projelere son 5 yıl içinde 100 milyon avrodan fazla para aktarmış durumdadır. 6INIT projesi, IPv6 ağlarının birbirleriye ve IPv4 ağlarıyla bağlanabilirliği, IPv6 uygulamalarının birbiriyle bağlanabilirliği, telefon ve çoklu ortam hizmetlerinin hayata geçirilmesi ve yeni IPv6 uygulamalarının geliştirilmesi konularında çalışmak amacıyla başlatılmış bir projedir. 6WINIT projesi benzer çalışmaların kablosuz ve geniş alanlı hücresel ağlarda (örneğin cep telefonu ağları) yapıldığı; buna ek olarak kişisel ve terminal hareketlilik konularının, ve sabit ve hareketli uçların karışık halde bulunduğu geniş ölçekli geçişlerde yetkilendirme, adres çözümü, IPSec dahil olmak üzere uçtan uca güvenlik, mobil IP, hizmet kalitesi, çoklu dağıtım gibi konuların araştırıldığı bir projedir. Kablosuz erişimin önemli olduğu sağlık gibi alanlarda test yataklarının, ve proje ortaklarının diğer projelerinde kullanabileceği bir altyapının oluşturulması da proje dahilinde planlanmış eylemler arasındadır. 6NET projesi kapsamında, IPv6

konuşlandırması ve geçişi konularında deneyimi artırma, yeni IPv6 uygulama ve servislerini deneysel olarak araştırabilmek amacıyla 16 Avrupa ülkesini birbirine bağlayan saf bir IPv6 ağı oluşturulmuştur. 30 Haziran 2005'te tamamlanan 6NET projesinin yaygınlaştırma, eğitim ve destek etkinlikleri 6DISS projesi ile devam ettirilmektedir. Avrupa IST (Information Society Technologies, Bilgi Toplumu Teknolojileri) Programı tarafından fonlanan en büyük proje olan Euro6ix projesi, tüm Avrupa'nın IPv6'ya hızlı geçişine destek olma hedefini taşımaktadır. Bu hedefe yönelik olarak, Euro6ix projesinin ilk amacı, küresel İnternet'in hiyerarşik yapısını izleyen bir IPv6 saf ağının tasarlanması; tasarlanan bu ağın konuşlandırılması; ağın ve ağ üzerindeki ileri düzey hizmetlerin işletilebilmesi için gereken tekniklerin, algoritmanın ve ana protokolün denenmesidir. Euro6ix projesinin ikinci amacı, konuşlandırılan bu ağ üzerinde oluşturulacak test yatağında CoS/QoS, hareketlilik, Anycast and çoklu gönderim, güvenlik, multihoming, renumbering gibi servislerin ve uygulamaların araştırılması, denenmesi ve uygunluklarının doğrulanmasıdır. Aynı test yatağında IPv6 uyumlu uygulamaların geliştirilmesi, taşınması (porting), adaptasyonu ve iyileştirilmesi de sağlanacak araştırma olanakları arasındadır. Euro6ix projesi kapsamında oluşturulan ağ, gelecekteki IPv6 ağlarının performansını ölçmek amacıyla xDSL, kablo, mobil veya eski IPv4 ile bağlanan, veya ticari olmayan IPv6 ileri düzey uygulamaları ve servislerini denemek isteyen belirli kullanıcı gruplarına açık olacaktır. Euro6ix projesinin bir diğer amacı da IETF ve RIPE gibi standard organizasyonları, üçüncü partiler, forumlar, ve GÉANT, 6WINIT ve 6NET gibi ilgili diğer projelerle irtibat ve koordinasyonun sağlanmasıdır.

Avrupa ülkelerinin biraraya gelmesiyle oluşturulan uluslararası bu gibi projelerin yanısıra, bir çok ülke kendi içinde IPv6 ile ilgili AR-GE etkinliklerine devam etmektedir. Avrupa IPv6 Görev Gücü'nün yayınladığı Avrupa IPv6 Yol Haritası belgesinde Avrupa'daki çeşitli ülkelerin IPv6 konusundaki eylemlerine dikkat çekilmiştir. Örneğin Fransadaki IPv6 çalışmaları Fransa IPv6 Görev Gücü gönüllü olarak başlatılmıştır. Görev gücü 2003 yılında IPv6'ya geçiş konusunda önerileri içeren "Fransa'da IPv6 Teknolojilerinin Geliştirilmesi ve Uygulanmasına Yönelik Stratejik Plan İçin Öneriler" başlıklı belgeyi yayınlamıştır. İspanya'da IPv6'ya geçiş çalışmalarının koordinasyonu İspanya hükümeti tarafından desteklenen İspanya IPv6 Görev Gücü tarafından yürütülmektedir Avusturya'da, 2003 yılında sunulan ülke çapında geniş bant politikasındaki eksik parça olarak değerlendirilen IPv6 konusundaki çalışmaları Avusturya hükümeti tarafından desteklenen IPv6

Görev Gücü koordine etmektedir. Almanya'daki IPv6'ya geçiş çalışmaları 2004 yılında Alman Savunma Bakanlığı'nın özellikle üreticiler ve servis sağlayıcılarının desteğini alabilmek amacıyla düzenlediği "Alman IPv6 Zirvesi" ile başlatılmıştır. Kamu aglarınıyepyeni ve güvenilir bir biçimde birbirine baglamak amacıyla "Çevrim içi Almanya"girişimini başlatmış; böylece devletin bilgi teknolojileri altyapısını homojen ve teknolojiye uygun hale getirerek e-Devlet BT kullanımının kalitesinin artırılması ve idari hizmetlerin tümüyle çevrim içi verilmesinin saglanması hedeflenmiş, bu projede IPv4 ve IPv6'nın birlikte kullanılması kararlaştırılmıştır. [5]. Finlandiya Telekomünikasyon düzenleyicisi Ficora, Finlandiya IPv6 Görev Gücü'nün yöneticiliğini yapmaktadır. Portekiz'de IPv6'ya geçiş konusundaki bilinçlendirme ve yaygınlaştırma faaliyetlerini Portekiz IPv6 Görev Gücü yürütmektedir. FCCN tarafından yönetilen RCTS akademik ağı 2003 yılından itibaren Avrupa Akademik Ağı GEANT'a IPv6 bağlantısı sağlayabilmektedir. İrlanda hükümeti, IPv6 çalışmaları konusunda Wattford Teknoloji Enstitüsü'nü merkez olarak belirlemiştir. Anlaşılacağı üzere, bir çok ülkede IPv6 ile ilgili AR-GE faaliyetleri, devlet desteğiyle oluşturulan IPv6 Görev Gücü ekiplerince hal-i hazırda yürütülüyor durumdadır.

I.1.6 ABD

ABD hükümeti tarafından yayınlanan "Memorandum For the Chief Information Officers" başlıklı belgede IPv6 geçiş sürecinde yapılması gerekenler, 15 Kasım 2005 tarihine kadar;

Geçiş planı için bir yönetici atanması ve geçiş aşamasının planlanması,

Kurumun elinde olan yönlendirici, anahtarlama cihazı,güvenlik duruvarı vb cihazlar için enventer çalışması yapılması,

İlk aşamada envantere dahil edilmemiş tüm IP konuşan cihaz ve teknolojilerin envantere dahil edilmesine başlanması

IPv6'ya geçiş sürecinin mali boyutunun araştırılması ve IPv6'ya geçiş aşamasındaki risklerin belirlenmesine başlanması;

Şubat 2006 tarihine kadar kurum için IPv6 geçişi için zaman planının oluşturulması, IPv6 ile ilgili politika ve yaptırım mekanizmalarının geliştirilmesi, kurum paydaşları için eğitim materyali oluşturulması, IPv6 uyumluluk ve birlikte çalışabilirlik için bir test planının oluşturulması, aşamalı IPv6 geçiş planının oluşturulması, ağların kurulması ve izlenmesi, ve IPv6 geçişinin gerektirdiklerinin

devam eden bir süreç şeklinde güncellenmesi; 30 Haziran 2006 tarihine kadar tüm IP konuşan cihaz ve teknoloji envanteri çıkarma ve mali boyutun araştırılarak risk belirleme çalışmalarının tamamlanması; 30 Ağustos 2008 tarihine kadar ise tüm kurum ağlarının omurgalarının çift yığın veya saf IPv6 olarak IPv6 trafiğini taşımaya hazır halde olması olarak belirlenmiştir.

Yine aynı belgede, ilerdeki gereksiz maliyetleri azaltmak için yeni alınacak cihazların IPv6 desteği olmasına azami şekilde dikkat edilmesi gerekliliği vurgulanmıştır. Ayrıca alınacak IPv6 destekli cihazların IPv4 ve IPv6 kullanan diğer sistemlerle sorunsuz çalışabilmesi, satın alındığı sırada desteği yoksa dahi yapılacak bir güncelleme ile Haziran 2008 tarihine kadar destekler hale getirilebilmesi ve IPv6 konusunda teknik destek veren bir üretici/yüklenici tarafından sağlanır olması koşulu getirilmiştir. IPv6 desteklemeyen bir cihaz alınabilmesi gibi bir istisnanın ancak CIO'nun (Chief Information Officer) önceden verilmiş yazılı izni ile mümkün olacağı belirtilmiştir.

ABD'deki Ticaret Departmanı'nın (Department of Commerce) Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) ve Ulusal Telekomünikasyon ve Bilgi İdaresi'nin (NTIA) oluşturduğu görev gücü, ABD için IPv6 geçiş sürecini teknik ve ekonomik açıdan incelemiş ve bulgularını bir rapor halinde yayınlamıştır [29]. IPv6 geçişinin getireceği yararların yanı sıra maliyet, güvenlik, birlikte çalışabilirlik ve geçiş sürecinde hükümetin rolü konularının çok yönlü olarak değerlendirildiği bu raporda, tüm dünyanın açıkça IPv6'ya geçmekte olduğuna ve sadece IPv6 üzerinde veya IPv6'da daha verimli çalışan uygulamaların artmasıyla ABD ekonomisinin uzun vadede rekabetçi konumunda sorunlarla karşılaşabileceği de belirtilmiştir.

Bunların yanında Avustralya, kamu kurumlarında donanım ve yazılımların 2011 sonunda IPv6'ya hazır, 2012 sonunda ise tüm sistemlerin IPv6 destekli olmasını hedeflemektedir.

Ülkelerin yanında birçok organizasyonda IPv6'ya geçiş ve yeni ürünlerin IPv6 protokolü ile uyumlu çalışacak şekilde üretilmesi konusunda açıklamalar yapmışlardır.

Mart 2008'de Google www.ipv6.google.com sitesi üzerinden hizmet vermeye başladı[6,7]

I.2 AMAÇ

Günümüzde mobil teknolojilerin artmasıyla birlikte her geçen gün IP ihtiyacı artmaktadır. Bu artış nedeniyle, aktif olarak kullanılan İnternet protokolu olan IPv4 adres kapasitesi de hızla tükenmektedir. Bununla birlikte IPv4 adreslemenin baslangıçta etkin bir sekilde organize edilememesi ve adaletli dagıtılamaması, sıkıntıyı daha da arttırmakta ve bir çok ülke IPv4 adres ihtiyacını karşılayamamaktadır[8]. Aynı zamanda mevcut IP teknolojinin, gelişmiş internet uygulamalarında yetersiz kalması, IP üzerindeki revizyonu kaçınılmaz hale getirmiş ve IPv6 teknolojisi oluşturulmuştur.

Dünya üzerinde internet kullanımının büyük bir ivmeyle yükselmesi ve hayatın her aşamasında kullanılmasıyla birlikte, güvenlik konusu daha da önem kazanmakta ve öne çıkmaktadır. IPv6 ile birlikte IPv4'te opsiyon olarak sunulan IPSec desteğinin zorunlu tutulması, adres sayısının artırılması, başlık yapısının sadeleştirilmesi, yönlendiricilerde paket parçalanmasına izin vermemesi gibi iyileştirmelerinin yapılması yeni nesil internet protokolünün daha güvenli olarak sunulmasını sağlamıştır[9,10].

Dünya üzerindeki bir çok gelişmiş ülke, bu yeni teknoloji için geçiş hazırlıklarına devam edip plot uygulamalarına başlamışlardır. Ancak bu süreçte, IPv4 ağını kullanarak IPv6 ağına ulaşmak için kullanılan tünelleme tekniklerinde veya birlikte kullanılması durumlarında güvenlik duvarı (firewall) tanımlamaları da oldukça önemli hale gelmektedir. Güncel olmayan ve doğru işletilmeyen güvenlik duvarları (firewall) yetersiz kalacak ve ciddi güvenlik zafiyetleri oluşabilecektir.[11]

Bu çalışma, yakın gelecekte internetin temeli yapısını oluşturacak olan IPv6 teknolojisini ve IPv6 ile birlikte ortaya çıkmış güvenlik riskleri penceresinden incelemeyi amaçlamıştır.

BÖLÜM II

II. GENEL BİLGİLER

II.1 INTERNET PROTOKOL VERSİYON 4

Internet Protokolü (IP), insanlığı bilgi çağına taşıyan Internet ağının temel yapı taşıdır. Internet'e bağlı herhangi iki bilgisayar arasındaki iletişim bu protokol aracılığıyla sağlanır. Bu açıdan IP'yi Internet'in ortak lisanı olarak da nitelendirebiliriz. IP, ağ katmanlarına baktığımızda TCP ve UDP gibi taşıma katmanı protokollerinin altında, Ethernet ve ATM gibi bağ katmanı protokollerinin de üzerinde yer alır. Temel görevi, Internet'e bağlı bilgisayarların iletişim amacıyla adreslenebilmesi ve gönderilen veri paketlerinin ağ içerisinde yönlendirilmesidir. İlk amacı çok daha kısıtlı bir boyutta (askeri iletişim amaçlı) kullanım olmasına rağmen, geçtiğimiz 10 yıl zarfında bu teknoloji dünya çapında kullanıma açılmıştır. Özel sektörün bu altyapıyı bir toplu iletişim aracı olarak kullanmaya başlaması ve Web teknolojisinin gelişmesi IP'nin hızla yaygınlaşmasını sağlayan faktörler olmuştur. Ama ne yazık ki, bu popülerliğin bir yan etkisi de bu eski protokolün limitlerine ulaşması ve böylesine ağır bir yükün altından kalkamayacak duruma gelmesidir. Günümüz Internet'i IP protokolünün 4. sürümü (IPv4) üzerine kurulmuştur. Bilgisayarların iletişim sırasında uçtan uca adreslenebilmesini sağlayan IPv4 adresleri 32 bitten ibarettir.

32 bitlik adres alanı teoride 4,294,967,296 tane adres oluşturabilse de, verimsiz adres atama mekanizmalarından dolayı etkin adres sayısı bu noktaya hiçbir zaman ulaşamaz. Web teknolojisinin gelişmesinin yanı sıra son zamanlarda kablosuz erişimin de yaygınlaşmasıyla 32 bitlik adres alanı varolan ihtiyacı karşılamakta yetersiz kalmaya başlamıştır. Bu problem karşısında IPv4 adres havuzunun etkin kullanımı için çeşitli yöntemler geliştirildi. IPv4 adres bloklarının değişken boyutlarda olmasına izin veren CIDR (Classless Inter-Domain Routing), aynı adresin farklı zamanlarda değişik bilgisayarlarca kullanımına (devre mülk) olanak tanıyan PPP (Point-to-point Protocol) ve DHCP (Dynamic Host Configuration Protocol) bunların başlıcalarıdır. Bu teknikler de yetersiz

kalmaya başlayınca bazı kurumların kullanmadıkları büyük adres bloklarını geri vermelerine iknaya bile başvuruldu (Örnek: Stanford Üniversitesi'nin 036/8 adres bloğunu IANA'ya iadesi).

Ne yazık ki sonunda anlaşıldı ki, varolan IPv4 mimarisiyle Internet'e bağlı tüm düğümlere birbirleriyle çakışmayan adres vermek mümkün değil, aynı anda aynı adresin paylaşımı kaçınılmaz. Sonunda ağ adres çeviricisi (NAT - Network Address Translator) Internet mimarisine girdi. NAT'in amacı, üzerinde barındırdığı bir IPv4 adresini birden çok bilgisayarın Internet'e bağlanırken paylaşımına sunmaktır. Bu bilgisayarlarla Internet arasında bir geçit görevi yapan NAT, Internet mimarisinin en temel prensiplerinden olan uçtan uca adresleme ve paket bütünlüğünü yok eden yegane etkendir. IPv4 adres kıtlığı için ancak bir yama niteliğinde kullanılan NAT teknolojisinin Internet'e faydasından çok zararının olduğu kabul görmüş bir gerçektir. NAT üzerinden istemci-sunucu iletişiminin sadece tek yönlü işleyebilmesi, IPsec bağlantılarının sağlanamaması, ağların sınırlı ölçeklenirliği ve yönetim zorlukları başlıca problemler arasındadır.[12]

TCP ile IP arasında basit bir ilişki vardır. TCP hedef bilgisi bulunan veriyi IP‘ye verir. IP bu veriyi alır ve gönderileceği bilgisayara yönlendirir. IP verileri TCP’den veya UDP(User Datagram Protokolü)’den alır. IP’nin paketler üzerinde çok sınırlı hata kontrolü vardır. IP, 16 bitlik başlık hata kontrolü sağlar. Bu IP paketini alan bilgisayarın IP başlığında bir bozulma oluşup oluşmadığını kontrol etmesini sağlar. IP verinin internet katmanına bozuk ulaştığını değerlendirIP yeniden gönderimi sağlayabilecek fonksiyona sahIP değildir. Bu görev bir üst katmandaki TCP’de yapılır, TCP’nin kullanılmadığı durumlarda daha üst katman protokollerince yerine getirilir. Akış kontrol ve paket sıralama mekanizmaları IP tarafından değil üst katman protokolleri tarafından yapılır.

Şekil II.1: IPv4 Başlık Yapısı

Versiyon: 4 bittir. IP'nin versiyon numarasını belirtir. Değeri 4'tür. Başlıktaki yerleşimi $(0100)_2$ şeklindedir.

Başlık Uzunluğu: IPv4'te seçenekler kısmının değişken olması nedeniyle (0-4 Byte arası) başlık boyutu da değişkendir. Bu nedenle 4 bit başlık uzunluğu bilgisi IP paketinin başlık ve veri kısımlarının ayrılmasını sağlar. Çoğu IP paketi seçenekler içermez. Bu nedenle çoğu durumda başlık uzunluğu standart 20 Byte'tır

Servis Türü: Paketin hangi servisin bilgisini taşıdığını belirtir. Ses iletimi ile yazı dosyası iletimi farklı servislerdir. Farklı servis tIPleri ile uyumlu yönlendiriciler tasarlanarak veri türüne göre iletim tekniği uygulanmasına imkân tanınmıştır .

Datagram Boyutu: IP başlığı ve verinin tamamının ne kadar uzunlukta olduğu bilgisini tutar. 16 bittir. Teorik olarak en uzun IP paketi 64 KiloByte'tır. Ancak fiziksel hatlardaki sınırlar nedeniyle paket uzunluğu hiçbir zaman bu değere ulaşamaz.

Tanımlayıcı, Bayrak, Bölümlendirme Katsayısı: Bu üç değer IPv6 temel başlıkta yoktur. IP çoğunlukla eternet üzerinden çalıştığı için gönderilebilecek paketin maksimum veri boyutu eternetin fiziksel sınırı olan 1500 Byte ile sınırlıdır. Bu durumda 1500 Byte üzerindeki verinin eternet üzerinden yollanması için bölümlendirme ihtiyacı ortaya çıkmıştır. Örneğin 3980 Byte'lık veri ile seçenekleri olmayan IP başlığı (20 Byte) eternet üzerinden yollanırken IP bölümlendirmesi gerekecektir. Veri üç bölmeye ayrılır

1.Bölme	2.Bölme	3.Bölme (Son Paket)
1480 Byte+20 Byte başlık Tanımlayıcı:777 Bayrak :1	1480 Byte+20 Byte başlık Tanımlayıcı:777 Bayrak :1	1020 Byte+20 Byte başlık Tanımlayıcı:777 Bayrak:0

ID=777 o an için gönderici bilgisayar tarafından atanan rasgele değerdir ancak bölmelendirme de her bölmenin hangi ana pakete dahil olduğunu belirtir. Bayrak 1 olunca paketin devamı vardır; bayrak 0 olunca paketin son parçası anlamını taşır

Yaşam Ömrü: Bir başlığın ağ üzerindeki ömrünü belirtir. Bu değer her geçilen bilgisayarda bir azaltılır ve sıfır olunca paket yok edilir.

Protokol: Burada verinin hangi üst seviye protokolden alındığının bilgisi tutulur. IP veriyi TCP veya UDP'den alır. Bu değer TCP için 6 UDP için 17'dir. Bunun belirtilme amacı gönderici ve alıcıda paketin üst katmanlar arasında aynı protokollerden geçme zorunluluğudur .

Başlık Kontrolü: Bir IPv4 başlığının 16 bit bölmeler halinde alt alta toplanması ile elde edilen değerin bire tümleyeni bulunur ve bu değer başlık kontrolü kısmına kaydedilir Bu değer paketin geçeceği yol boyunca yönlendiricilere paket başlığının bozulup bozulmadığının kontrolünü yapabilme imkânı sağlar. Geçilen yol boyunca her yönlendirici paketteki yaşam ömrü değerini bir azaltır ve pakete kendi seçeneklerini ekleyebilir bu nedenle başlık kontrolü değeri geçilen her bilgisayar tarafından yeniden hesaplanıp pakete yerleştirilir. IP de hata kontrolünün yapılma nedeni, sürekli TCP paketleri taşımaması bazen UDP gibi hata kontrolü yapmayan paketleri de taşımasıdır.

Hedef ve Kaynak IP Adresler: 32 bit yapıda IPv4 adresleridir.

Seçenekler: İsteğe bağlı eklemeler için tasarlanmıştır ama çoğunlukla boştur. Boyutu 4 Bytetır. IPv6'da tamamen kaldırılmıştır. Eğer seçenekler sıfır Byte ise bir IPv4 başlığı 20 Byte olur ayrıca 20 Byte TCP başlığı vardır. Bu nedenle seçenek içermeyen bir IP paketi toplam 40 Byte başlık taşır.

Veri: Üst katmanlardan başlıklar da eklenerek gelen sayısal bilgi IP katmanı için veriyi oluşturur. [13]

II.2 INTERNET PROKOL VERSİYON 6

Şekil II.2 : IPv6 Başlık Yapısı

Versiyon: 4 bittir. Değeri 6'dır.Başlıktaki yerleşimi $(0110)_2$ şeklindedir.

Öncelik(Trafik Sınıfı): Paketin taşıdığı verinin tipine göre öncelik verilmesini sağlar. Toplam 8 bittir. İki kısımdan oluşur. Bunlar 6 bit DS (differentiated services) ve 2 bit ECN (Explicit Congestion Notification)'dir. Bu değerler yönlendirmede kullanılan trafik sınıflarını belirler. Trafik sınıfları ile ses ve görüntü iletimi, diğer dosya transferlerinden ayırt edilir ve farklı şekilde iletilir.

Akış Etiketi: Farklı akış tiplerini belirtmek amacıyla 24 bitten oluşur. Performans garantisi isteyen yeni uygulamalar için kullanılacaktır. Bu kısım sayesinde bazı akış etiketleri için özel ağ güzergahları belirlenecek ve özel trafikler özel yollardan geçecektir. Akış etiketi trafik sınıfı ile beraber düşünülmektedir. Ancak trafik sınıfı tipi belirtirken akış etiketi geçilecek yolu belirtir. Bir paket belli istekler ile gönderilecek ve bu nedenle (ses veya video olabilir) bu etiket için bir yol kurulacak ve sonraki paketlerin içeriğine bakılmadan sadece aynı akış etiketi numarası ile gelenler bu yoldan iletilmeye devam edilir. Akış etiketi ayrıca uygulamadan gelen verinin boyutunun çok büyük olduğu

zamanlarda yapılan bölümlendirme işleminde kontrol görevi görür. Bu görev verinin göndericide parçalanıp alıcıda düzgün şekilde birleştirilmesi aşamalarını kapsar.

Akış etiketi değerleri yönlendirici tarafından bir tablo da tutulur. Böylece zaman kazanılır. Bir yönlendiricinin akış etiketi tablosu oluştururken 4 kural vardır:

• Bir akış etiketi bir yönlendirici tarafından desteklenmeyen türde ise, tabloda bu değeri sıfır olarak atamalı ve paketi aynen iletmelidir.

• Aynı akış etiketine sahip paketlerde hedef IP aynı olmalı ve yönlendirici ilk paketi işleyince akış etiketini kaydetmeli böylece sonraki paketlerde zaman kazanmalıdır.

• Akış etiketi 1 ile 2^{20} arasında değişir. Sıfır olarak seçilirse etiket yok demektir.

• Bir akış etiketi numarası çakışma olmaması için gönderilmiş paketin hedefe tahmini ulaşma süresinden önce tekrar kullanılmamalıdır .

Toplam Uzunluk: 16 bittir. Bu kısım temel başlık (40 Byte) hariç tüm genel başlığın boyutunu işaretsiz tamsayı olarak Byte cinsinden belirtir.

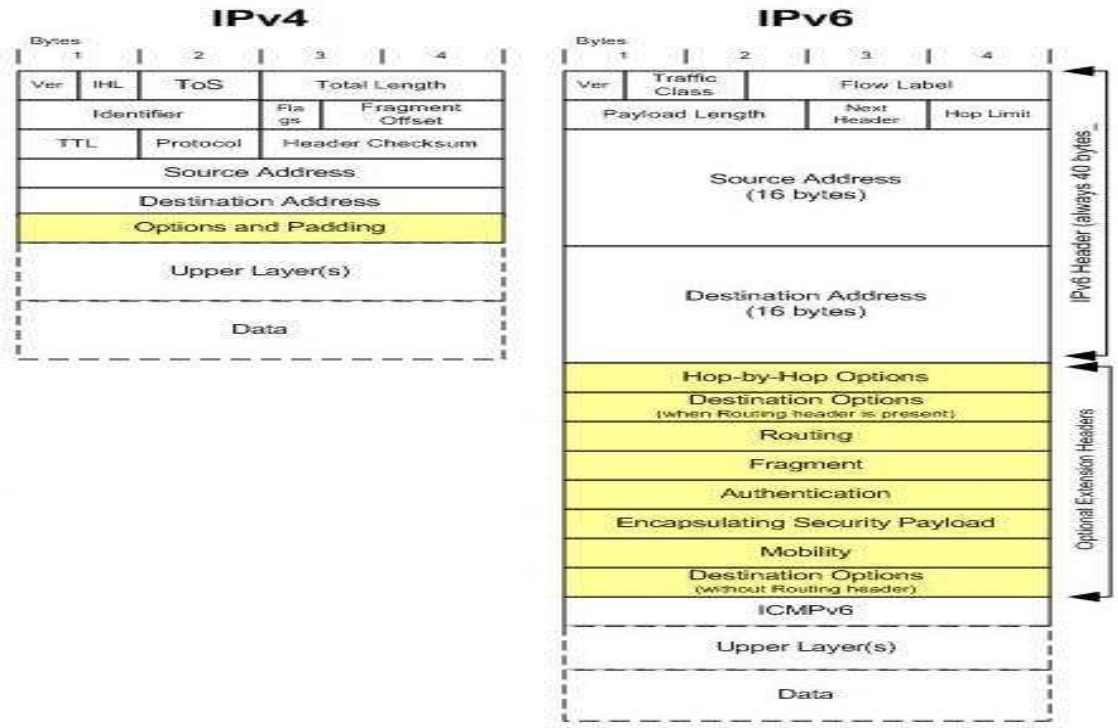
Sonraki Başlık: IP başlığını hangi başlığın takip ettiğini belirtir. Bu kısımda bu başlığı bir ek başlık mı, TCP başlığı mı veya UDP başlığı mı takip eder onun bilgisi tutulur. Mesela bu kısmı eğer bir ek başlık izliyorsa buraya izleyen ek başlığın adı yazılır; TCP ya da UDP izliyorsa bu kısma TCP veya UDP yazılır.

Hop Limit: Bu başlığın en çok kaç hop (bilgisayar, yönlendirici vb.) geçebileceğini belirtir. IP başlığının ağ içerisindeki yasam süresidir. Geçilen her hop bu sayıyı bir azaltır ve sıfıra hangi hopta ulaşılırsa başlık yok edilir. Amaç, internette hedefini bir şekilde bulamamış paketlerin sonsuza dek dolanmasını engellemektir.

Kaynak ve Hedef IP Adresler: RFC 2373'te özellikleri belirlenmiş göndericiyi ve alıcıyı belirleyen 128 bitlik IPv6 adresleridir [13]

Tablo II.1 IPv4 ile IPv6 Arasındaki Temel Farklar

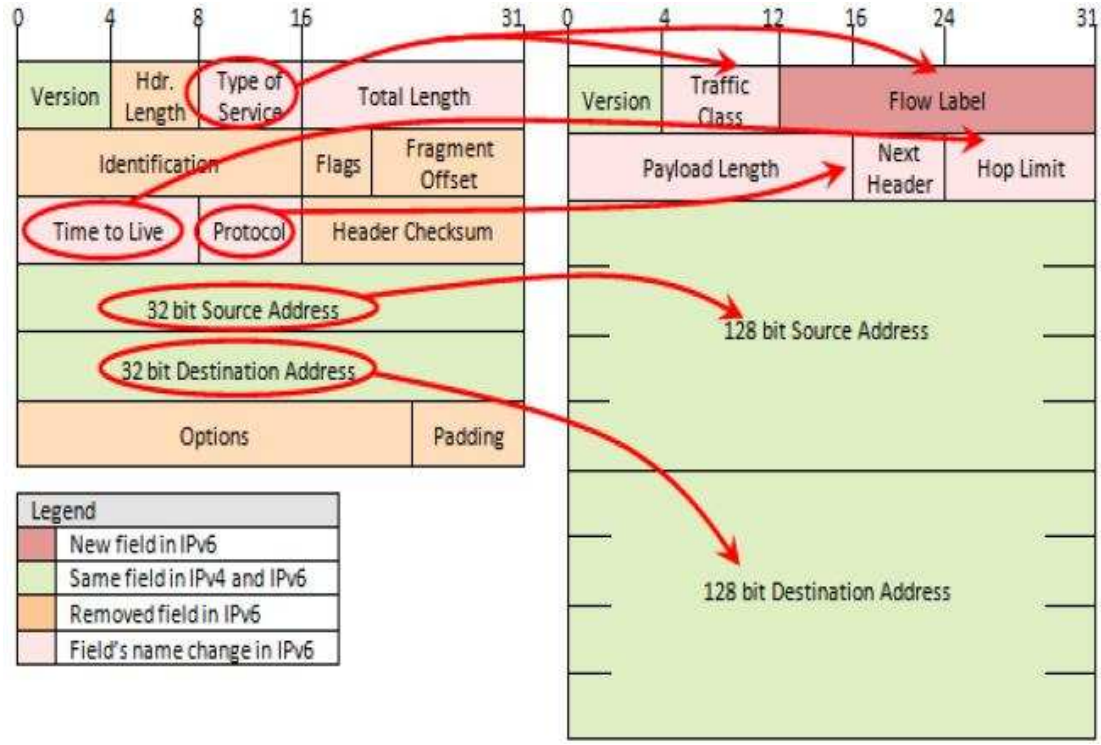
IPv4	IPv6
Adresler 32bit uzunluğundadır.	Adresler 128bit uzunluğundadır
IPsec desteği mecburi değildir.	IPsec desteği mecburidir.
IPv4 başlığında paket akışını tanımlamak için yönlendiricilerin kullanabileceği QoS tanımlamaları yoktur.	IPv6 başlığında bulunan Flow Label alanı yönlendiriciler tarafından paket akışını tanımlamak için kullanılabilir.
Paketin parçalanması (fragmentation) hem yönlendiriciler hem de paketi gönderen istemci tarafından yapılır.	Paketin parçalanması (fragmentation) yönlendiriciler tarafından yapılmaz. Sadece paketi gönderen istemci tarafından yapılır.
Paket başlığı sağlama toplamı (checksum) içerir.	Paket başlığı sağlama toplamı (checksum) içermez.
Paket başlığı sağlama seçenekler (options) alanı içerir.	Tüm seçimli veri IPv6 uzantı başlıklarına (extension headers) taşınmıştır.
Address Resolution Protokolü (ARP), IPv4 adreslerini bağlantı katmanı adreslerine dönüştürmek için ARP Request paketleri kullanır.	ARP Request paketleri multicast Neighbor Solicitation mesajlarıyla değiştirilmiştir.
Lokal subnet grup üyelikleri Internet Group Management Protocol (IGMP)kullanılarak yönetilir.	IGMP'nin yerini Multicast Listener Discovery (MLD) mesajları almıştır.2
En iyi varsayılan ağ geçidini bulmak için ICMP Router Discovery kullanılabilir fakat kullanımı zorunlu değildir.	ICMP Router Discovery yerine ICMPv6 Router Solicitation ve Router Advertisement mesajları kullanılması zorunludur.
Ağdaki tüm düğümlere trafik gönderebilmek için broadcast adresleri kullanılır.	IPv6 broadcast adresi bulunmamaktadır. Bunun yerine link-local scope all-nodes multicast adresi kullanılır.
Yapılandırılması elle veya DHCP kullanılarak yapılır.	Elle veya DHCP kullanmak gerekmeden otomatik olarak yapılandırılabilir.
Bilgisayar isimlerini IPv4 adreslerine çevirmek için DNS sisteminde A kaydı kullanılır.	Bilgisayar isimlerini IPv4 adreslerine çevirmek için DNS sisteminde AAAA kaydı kullanılır.
IPv4 adreslerini bilgisayar isimlerine çevirmek için IN-ADDR.ARPA DNS alanında PTR kaydı kullanılır.	IPv6 adreslerini bilgisayar isimlerine çevirmek için IP6.ARPA DNS alanında PTR kaydı kullanılır.
576-byte uzunluğundaki paket boyutlarını desteklemek zorundadır.	1280-byte uzunluğundaki paket boyutlarını desteklemek zorundadır.



Şekil II.3 IPv4 ve IPv6 Paket Yapıları

II.2.1 Yeni Başlık Yapısı

IPv4 başlık bilgisinin hantal olan yapısı revize edilmiştir. Başarımı yükseltmek için, kullanılması gerekli olmayan ya da görevleri daha üst protokollere devredebilen kısımlar ayıklanmıştır. Günümüz modern bilgisayar ağlarına ve gereksinimlerine uyum sağlayacak şekilde, bazı kısımlar genişletilmiştir (adres bilgisi). Ayrıca IPv6 protokolü, başlık bilgisinde bulunan flow label yardımıyla, başarımı daha yüksek veri akış hızlarına ulaşabilmektedir. Bu iki protokolün başlık yapıları incelenirse fark daha açık bir biçimde anlaşılacaktır.



Şekil II.4 IPv4 ve IPv6 Paketleri Arasındaki Benzerlik ve Farklar

IPv4 başlığında bulunan ve kullanılan adres bilgisinin uzunluğunu belirten 4 bitlik Header Length bölümü IPv6 da kaldırılmıştır, çünkü IPv6 adresleri her zaman 40 baytlık bir uzunluğa sahiptirler.

IPv4 veri paketleri 20 ile 60 bayt arasında değişen, IPv6 veri paketleri ise 40 baytlık sabit uzunluktaki bir başlık bilgisine sahiptir. Sabit uzunluktaki header yönlendiricilerde header uzunluğunun algılanması için harcanan zamandan ve işlem gücünden tasarruf edilmesini sağlamaktadır. IPv4'de 32 bit olan adres verisinin uzunluğu IPv6'da 128-bit olarak rasgele seçilmemiştir. Bu uzunluk seçilirken işlemci mimarileri göz önünde bulundurularak routing işlemi sırasında maksimum hız ve minimum overhead sağlanmaya çalışılmıştır.

IPv6 düğüm noktalarındaki darboğazı aşmak ve daha verimli bir yönlendirme yapabilmek için, sabit başlık bilgisi, tek çevrimde okunan adres bilgisi ve flow label gibi avantajları beraberinde getirmektedir. Hiyerarşik adresleme yapısına sahip IPv6 yol atama çizelgelerinin boyutlarının çok yüksek oranlarda küçülmesini sağlayacaktır. Ayrıca yönlendiricilere ek yük getirmeyen fragmantasyon ve hata kontrolü işlemlerini iki uçtaki ağ elemanlarına bırakan yapısı sayesinde çok daha verimli bir routing işlemine imkân tanımaktadır.

II.2.2 Geniş Adres Alanı

IPv6 128 bitlik bir adresleme yapısına sahiptir. Yani teorik olarak 2^{128} adet IP adresleme kapasitesine sahiptir. Bu da IPv4'e oranla 296 kat fazla IP adresi anlamına gelmektedir. Artık NAT gibi çözümleri kullanmaya gerek kalmayacaktır.

Yani 340.282.366.920.938.463.463.374.607.431.768.211.456 ($3.4X10^{38}$ ya da 340 undecillion) interface adresleme yeteneği vardır.

II.2.3 Etkin ve Hiyerarşik Adresleme ve Yönlendirme

Internet'in çok hızlı bir şekilde gelişmesi ve IPv4'ün flat – hiyerarşik karışımı routing yapısı sonucu Internet bacbone router'ları oldukça büyük routing tabloları ile (85,000'in üzerinde route kaydı) çalışmak zorunda kalmaktadır. "Yeni Başlık Yapısı" kısmında belirtildiği gibi IPv6 global adreslerinin Internet ortamında etkin, hiyerarşik ve özetlenebilir yapısıyla routing işlemini daha düşük overhead ile ve daha hızlı bir şekilde gerçekleşecektir.

II.2.4 Gelişmiş QoS Desteği

IPv4'de bulunan Type of Service kısmının IPv6'daki karşılığı olan Traffic Class her iki başlık için de aynı işleve sahiptir. Öncelik atama ve servis kalitesi (Quality of Service) gibi fonksiyonlar için kullanılmaktadırlar.

IPv6'yla getirilen yeni bir özellik Flow Label kısmıdır. Seçimli olarak kullanılabilen bu bölümle beraber, gerçek zamanlı verilerin bu bölümdeki etiketlere bakılarak hızlı bir şekilde yönlendirilmesi ya da MPLS (Multi Protocol Label Switching) gibi daha alt seviyedeki teknolojilerin daha verimli kullanılması IPv6 ile mümkün olmaktadır.

IP paket payload'u encrypt edilse bile trafik IPv6 header'ında tanımlandığından dolayı QoS desteği yine de sağlanmaktadır.

II.2.5 Yerleşik Güvenlik - IPSec

TCP/IP ilk geliştirildiğinde, ufak ve kapalı bir yapıya sahip olduğundan güvenlik meselesine çok fazla önem verilmemişti. Fakat TCP/IP'nin hızla yayılması ticari uygulamalarda yer alması güvenliği oldukça önemli bir noktaya taşımıstır [14]. IPv6 gerek yeni adresleme yapısı, gerekse protokol içerisine dahil edilmiş IPsec uygulaması, gerekse sadeleştirilmiş ve ara aygıtlarda fragmente olmayan başlık yapısı ile bir çok güvenlik özelliği ile beraber gelmektedir.

Her ne kadar IPv4 içinde IPsec uygulamaları hazırlanmış olsa bile girişte de belirtildiği gibi, gerek ara cihazlarda IPsec'in desteklenmemesi (ya da farklı uygulamaların birlikte çalışabilirliği yönündeki kısıtlar), gerekse IPsec'i protokol'ün üzerinde bir uygulama olarak görmesi nedeniyle bir takım problemlerle karşılaşılmaktaydı. Mesela; IPv4'te adres kısıtı nedeniyle bir çok sistemde kullanımı zorunlu hale gelen NAT, IP header'ındaki adresi değiştirdiği için IPsec'in bütünlüğü bozulmaktadır.

IPv4'te opsiyonel olan IPSec desteğinin IPv6'da zorunlu olmasından dolayı, IPsec kullanımının hızla yaygınlaşacağı ve iletişim güvenliğinin artıracağı tahmin edilmektedir [9,15-18]

II.2.5.1 IPSec

IPSec (İnternet Protokol Güvenliği) kullanıldığında programlar değiştirilmeden güçlübir güvenlik sağlar. Mevcut güvenlik standartlarının bir çoğu uygulama seviyesinde çalışmaktadır. Bu protokoller web,elektronik posta,FTP gibi sınırlı sayıda uygulamayı desteklerken IPSec gibi ağ katmanında çalışan güvenlik protokolleri, IP ağı üzerinden veri iletiminde bilginin gizliliğini,bütünlüğünü ve güvenirliğini sağlar. IPSec, IPSec komşuları denilen iki nokta arasında güvenli haberleşme sağlar. Bu haberleşmede Sas (Güvenlik Kurumları) kümesi kullanılır.Sas hangi güvenlik protokollerinin, parametrelerinin uygulanacağını belirler. İki komşu arasında birden fazla IPSec oturumu kurulabilir ve her IPSec oturum için aynı Sas seti kullanılır.

IPSec üç temel fonksiyonu yerine getirir:

Doğrulama Başlığı (Authentication Header – AH)

Paketin değiştirilmediğinden ve gerçek kaynaktan geldiğinden emin olmak için için kullanılır. [9] Fakat paketin başka kullanıcılar tarafından okunmadığı garanti edilmez. MD5 veya SHA yöntemlerinden biriyle tek yönlü şifrelenmiş hash fonksiyonu ile veri hesaplanarak paketin kaynağının doğru kaynaktan geldiği ve değiştirilmediği tespit edilir[11].

Sarmalıyıcı Güvenlik Yükü (Encapsulation Security Payload – ESP)

Bu protokol yetkilendirme ve verişifrelemesi sağlar. ESP tek başına kullanılacağı gibi AH protokolü ile beraber kullanılabilir. Paket şifrelenerek başka kullanıcılar tarafından okunması engellenir. ESP hem aktarım modda hem tünel modda kullanılabilir.

IKE (Internet Anahtar Değiş-Tokuşu) Protokolü :

(Anahtar değişimi elle de yapılabilir) SAs parametrelerinin tanımlanması IKE tarafından otomatik olarak yapılır. Manual IPSec'te SAs parametreleri ağ yöneticisi tarafından önceden tanımlanır. Böylece konfigürasyona bağımlılık ya da yanlış tanımlamalar gibi sakıncalar doğmaktadır. Ayrıca tanımlanan parametrelerin süresi hiç dolmamaktadır ve böylece güvenlik açığı oluşmaktadır. IKE protokolü elle yapılan IPSec'e göre bir çok avantaj sağlar. Bunlar:

Anahtarların elle tanılanmasına gerek yoktur

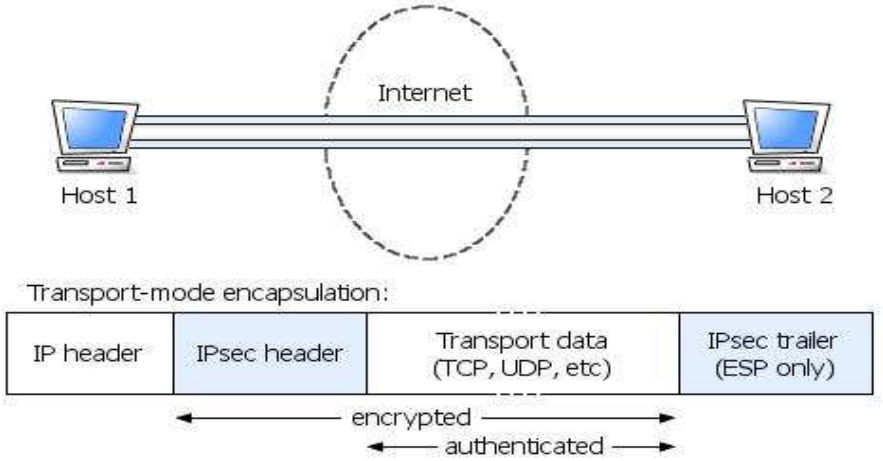
IPSec SAs için hayat süresi belirlenebilir

Şifreleme anahtarlarının IPSec oturumu boyunca değişimine izin verir.

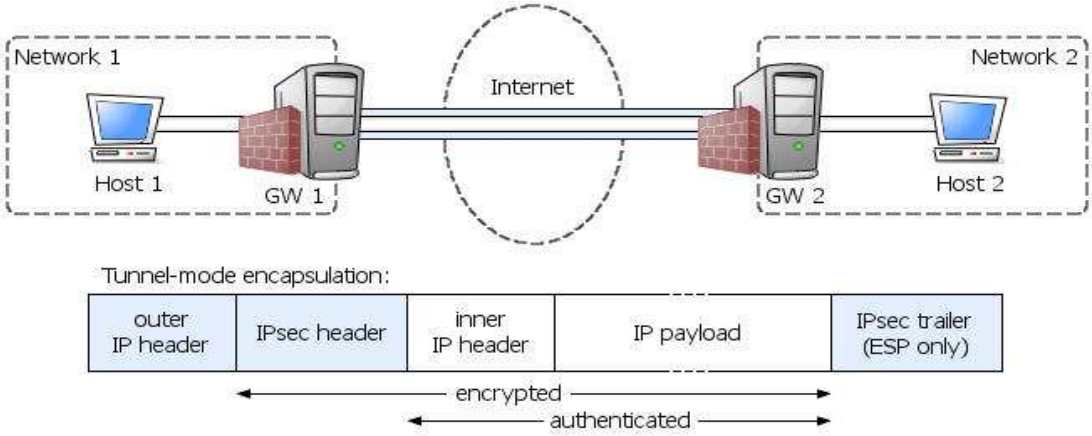
Komşuların dinamik olarak yetkilendirilmesine izin verir.

IPSec göndericinin (veya onun yerine görev yapan geçiş kapısının) her IP paketinin kimlik denetimini yapmasını, şifrelemesini veya her iki fonksiyonu birden pakete uygulamasını sağlar. Bu iki fonksiyonu birbirinden ayırmak IPSec kullanmak için mod denilen iki metodun gelişmesine neden olmuştur. İletim modunda, IP paketinin sadece veri kısmının kimlik denetimi yapılır veya şifrelenir. Bu modun avantajı IP paketine fazla yeni bytelar ilave edilmemesidir. IP paketinin tamamına

kimlik denetimi veya şifreleme yapan öteki yaklaşıma ise tünel modu denir. IPSec iletim modu pek çok alanda faydalı olurken, tünel modu belirli ataklara karşı çok daha iyi koruma ve İnternette oluşacak trafik izlemeyi sağlar.

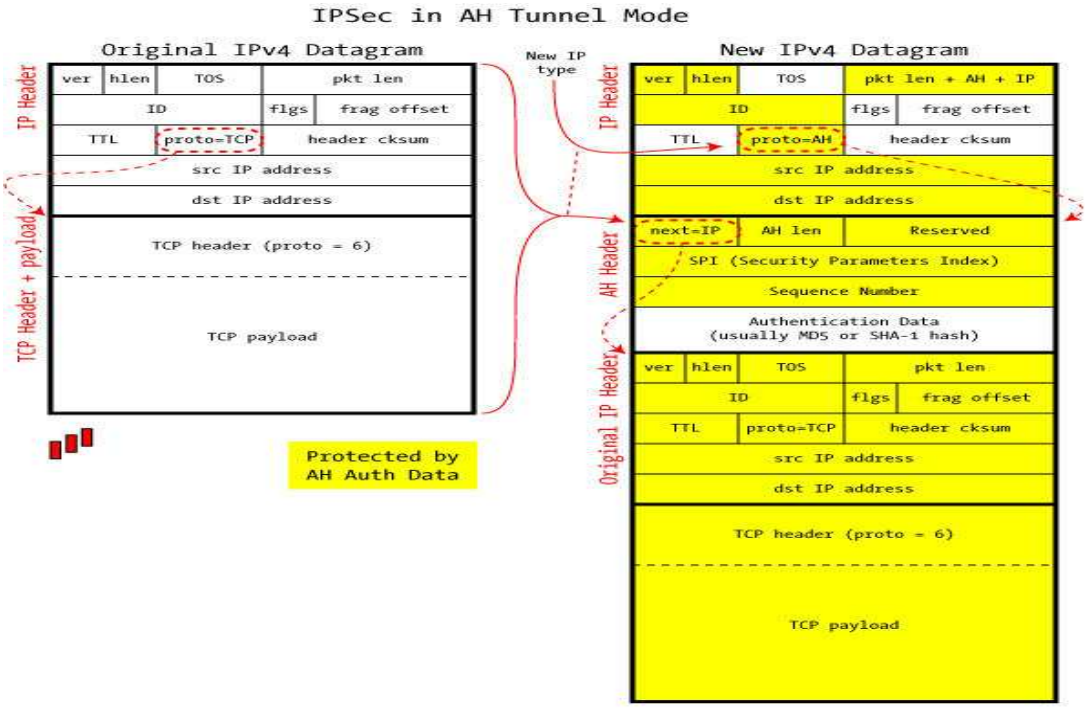


Şekil II.5 :IPSec İletim Modu

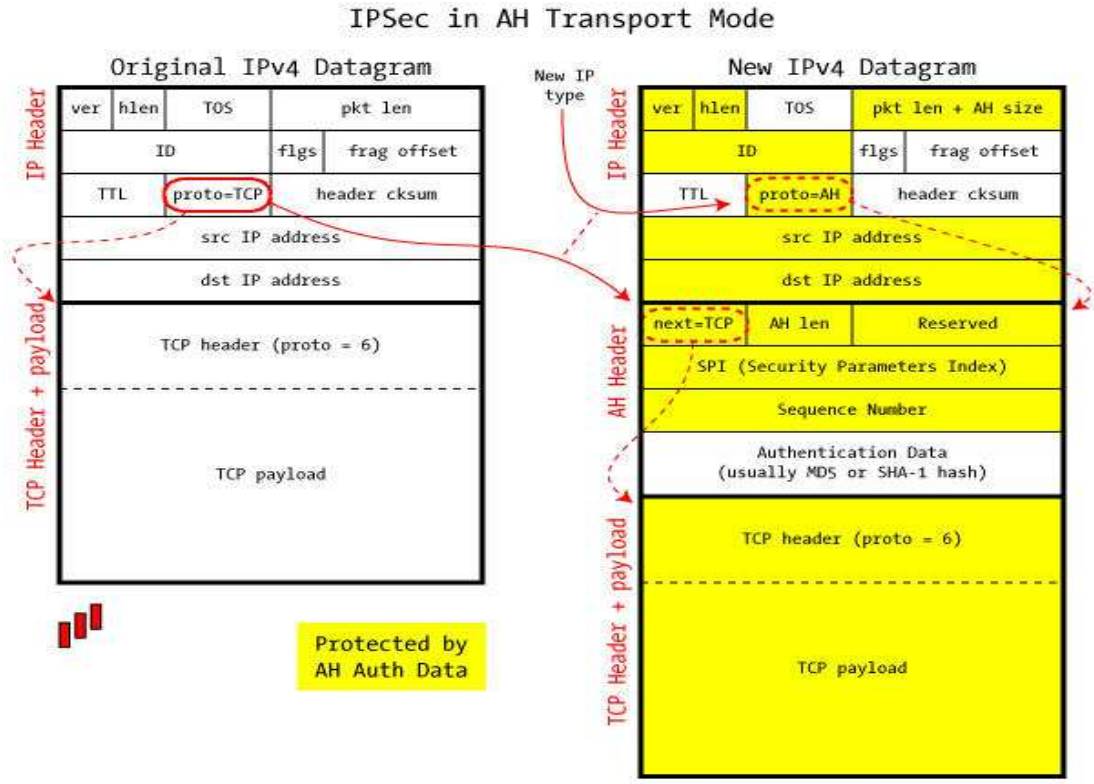


Şekil II.6 : IPSecTünel Modu

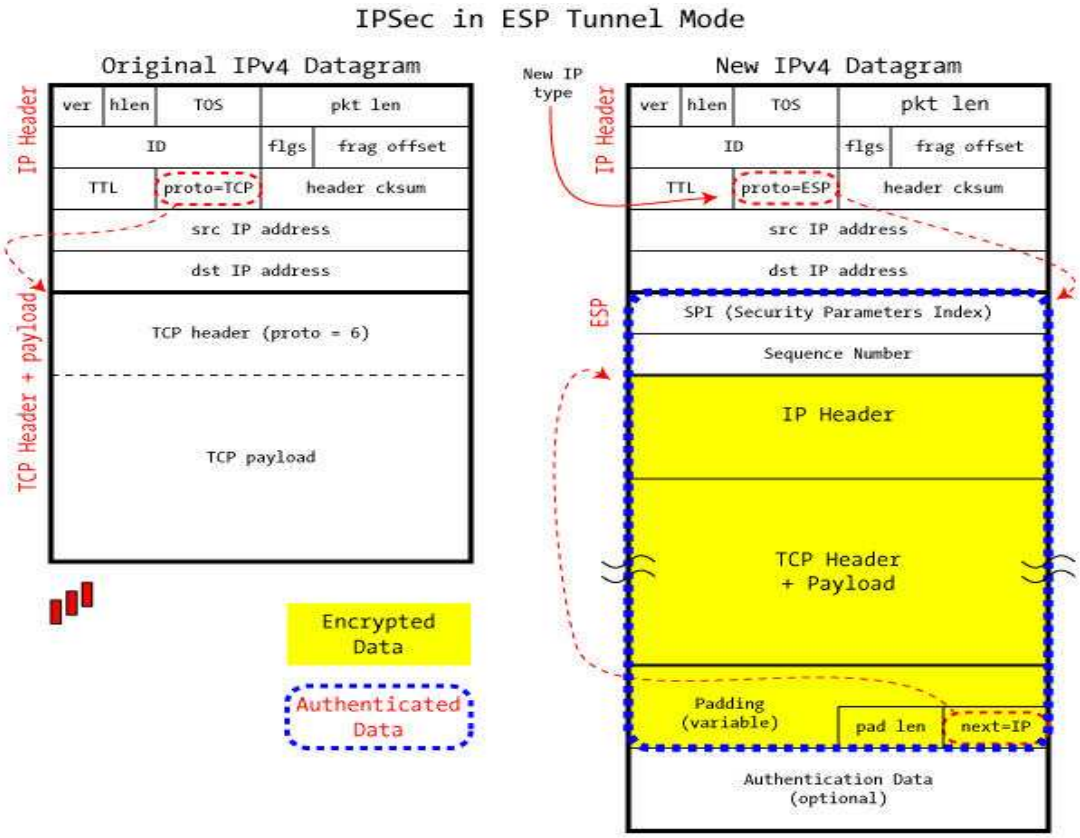
IPSec güvenliği,gizliliği ve bütünlüğü tüm sistemde sağlamak için birkaç değişik güvenlik teknolojilerini birlikte kullanır. Şifreleme için DES,bütünlük için SHA(ki bu özet fonksiyonunu baz alır) ve yetkilendirme için ise IKE farklı metodları destekler. [19]



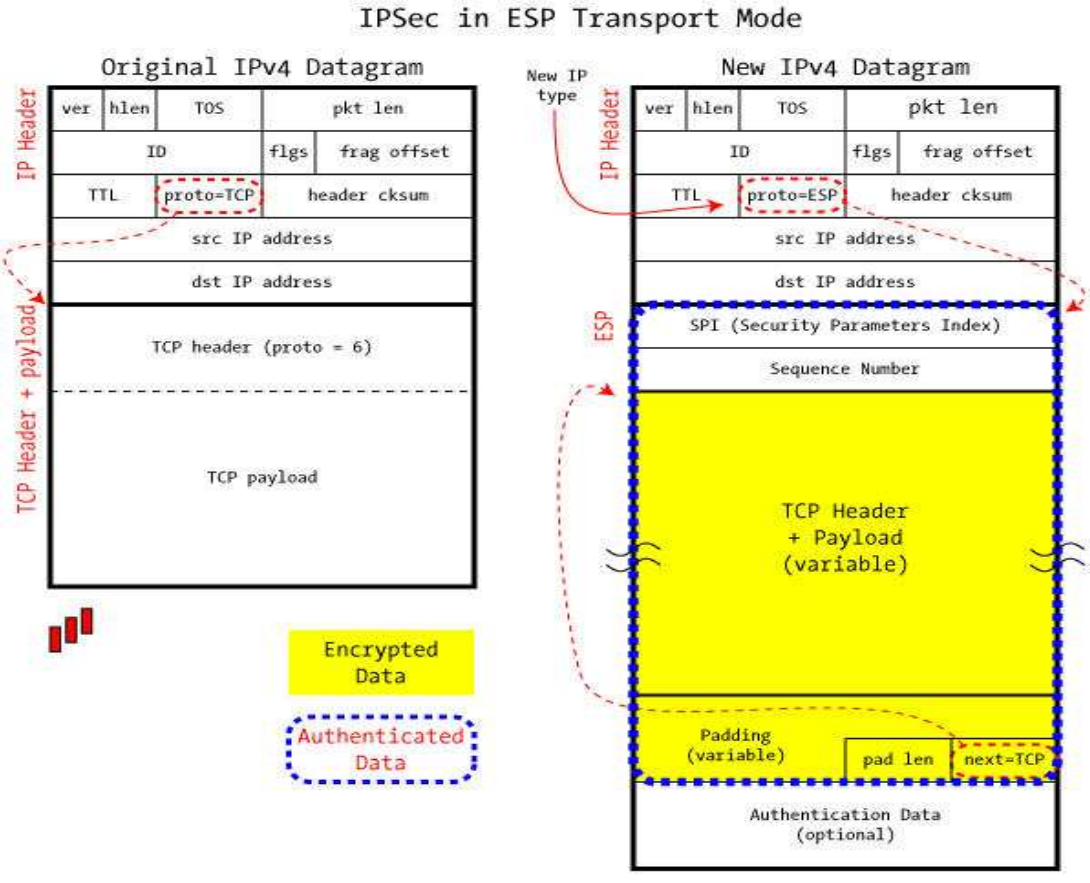
Şekil II.7: AH -Tunel Modu



Şekil II.8 : AH – İletim Modu



Şekil II.9 : ESP – Tunel Modu



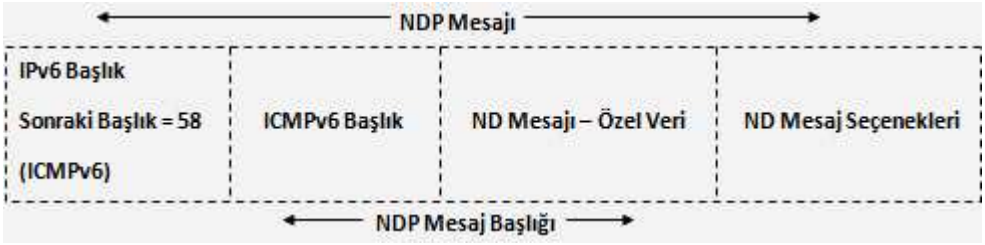
Şekil II.10: ESP – İletim Modu

II.2.6 Yeni Protokoller -Komşu Saptama Protokolu (Neighbor Discovery)

Komşu Saptama İletişim Kuralı (Neighbor Discovery Protocol (NDP)) IPv6 ile kullanılan internet iletişim kuralları dizisinde bir protokoldur. Bağlantı katmanında çalışır ve bağlantıdaki diğer düğümleri bulmak, diğer düğümlerin MAC adreslerine karar vermek, uygun routerlar bulmak ve diğer aktif komşu düğümlere yollar hakkında erişilebilirlik bilgisi sağlamakla yükümlüdür.

NDP, Adres Çözümleme Protokolü (ARP) ve ICMP Yönlendrici Keşif ve Yönlendirici Yeniden Yönlendirme protokollerinin IPv4 için yaptığını IPv6 için yapar. Bununla birlikte, IPv4'deki karşılıklarına göre daha fazla gelişme içerir. (bkz RFC 4861, bölüm 3.1) Örneğin başarısız yönlendirici ya da bağlantıların varlığında paket sağlamlığını sağlayan Komşu Erişilememezlik Tespiti(Neighbor Unreachability Detection (NUD))'ni içerir.

ND protokolü RFC 1970 ile 1996 da tanımlanmıştır, sonrasında 1998'de değiştirilip RFC 2461deki halini almıştır. Eylül 2007 tarihinde ise RFC 4861 ile son halini almıştır.



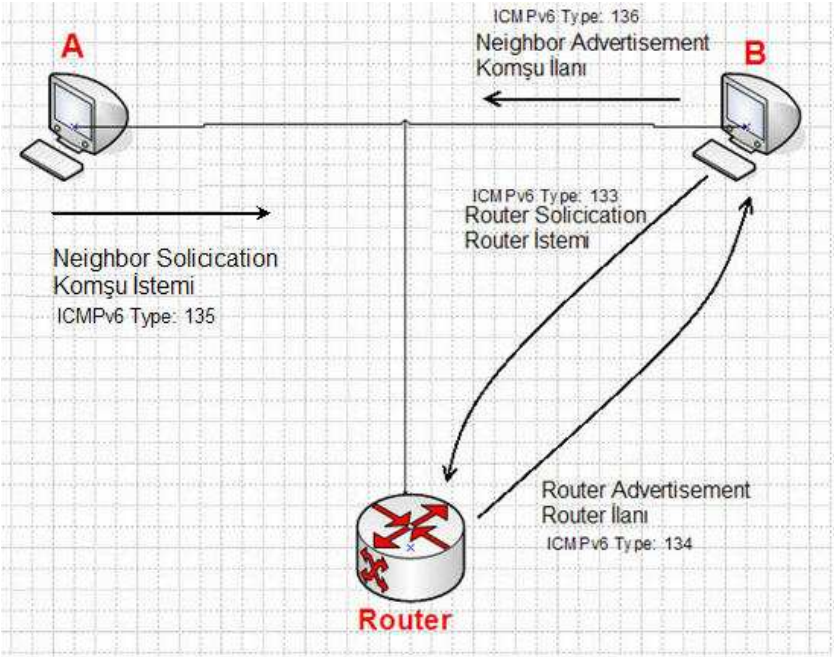
Şekil II.11 : Komşu Saptama Protokolü Başlığı

ND protokolünün en önemli beş işlemi ICMPv6 control mesajları ile yapılmaktadır.

- Yönlendirici İstemi(Router Solicitation)
- Yönlendirici İlanı(Router Advertisement)
- Komşu İstemi (Neighbor Solicication)
- Komşu İlanı (Neighbor Advertisement)
- Yeniden Yönlendirme

Neighbor discovery:		
133	Router Solicitation	RFC 2461 (rfc section 4.1)
134	Router Advertisement	RFC 2461 (rfc section 4.2)
135	Neighbor Solicitation	RFC 2461 (rfc section 4.3)
136	Neighbor Advertisement	RFC 2461 (rfc section 4.4)
137	Redirect	RFC 2461 (rfc section 4.5)

Şekil II.12 : ICMPv6 Paket Tanımları

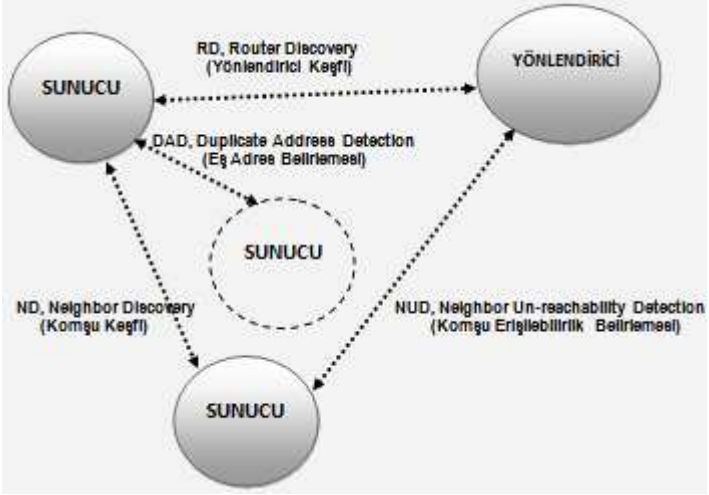


Şekil II.13 : Neighbor Discovery

Örnekle açıklayacak olursak;

A bilgisayarının B bilgisayarı ile iletişime geçebilmesi için, B bilgisayarının MAC adres bilgisini öğrenmesi gerekir. Bu uygulama IPv4'te, A bilgisayarının ARP paketini broadcast yayın yapmasıyla gerçekleşmekteydi. Şimdi ise bağlantı kurmak isteyen A bilgisayarı, kaynak ip adresini kendi IP adresi yapar. Hedef ip adresi iletişim kurulmak istenen IPv6 adresine karşılık gelen İstemli-Birim Multicast adresi (Solicited-Node Multicast) adresidir ve B bilgisayarının MAC adresini sorgular. Kendi MAC adresinin sorgulandığını anlayan B bilgisayarı ise Router Advertisement paketiyle MAC adresini A bilgisayarına gönderir. Bu sayede haberleşme başlar.

Aynı şekilde B bilgisayarı bütün routerlara FF02::2 multicast adresi üzerinden Router Solicication mesajı yayınlar. Bunun üzerine router, Router Advertisement mesajını gönderir. Bu paket B bilgisayarının ön ek adresini(prefix), link konfigürasyon parametrelerini, global adres atamalarında durumlu(statefull) yada durumsuz(stateless) metodların kullanılıp kullanılmayacağını ve DHCPv6 kullanarak ilave network konfigürasyon parametlerini içerir



Şekil II.14 : Neighbor Discovery Fonksiyonları

Komşu Saptama İletişim Kuralı şu işlevsellikleri sağlamak için gerekli olan mekanizmayı tanımlar:

- Yönlendirici Keşfi: hostlar bitişik bağlantılardaki yönlendiricilerin yerini belirleyebilir.
- Önek Keşfi: hostlar bitişik bağlantılar için bağlı olan(on-link) adres öneklerini bulabilir.
- Parametre Keşfi: hostlar internet parametrelerini bulabilir (MTU gibi).
- Adres Otomatik Yapılandırması: bir arayüz için adreslerin yersiz(stateless) yapılandırması.
- Adres Çözümlemesi: IP adreslerinin bağlantı-katmanı(link-layer) adresine eşlenmesi.
- Sonraki-Durak(next-hop) Kararı: hostlar bir hedef için sonraki-durak yönlendiricileri bulabilirler.
- Komşu Erişilememezlik Tespiti (Neighbor Unreachability Detection (NUD)): bağlantıdaki bir komşunun artık erişilemez olduğuna karar verir.
- Çoklu Adres Tespiti (Duplicate Address Detection (DAD)): düğümler bir adresin kullanımda olup olmadığını kontrol edebilir.
- Yeniden Yönlendrime: yönlendirici düğümü daha iyi ilk-durak(first-hop) hakkında bilgilendirebilir

II.2.7 Daha Basit IP Yapılandırması

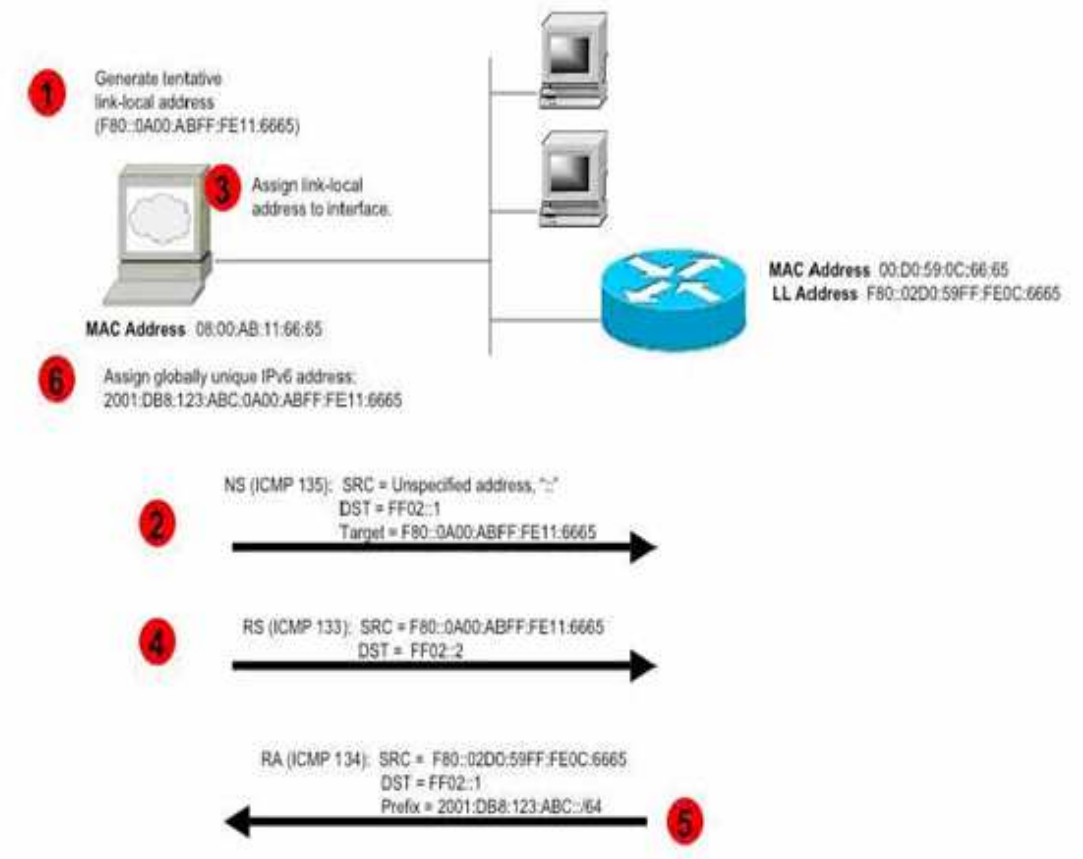
IPv6 ile birlikte, IP adres yapılandırma işlemi protokol içine entegre edilmiş ve ara yüzler IP adres konfigürasyonunu otomatik olarak harici bir protokol veya mekanizma kullanılmadan yapabilir hale gelmiştir. IPv6 adres yapılandırması için iki yöntem sunulmaktadır.

II.2.7.1 Durum Denetimli Yapılandırma (Stateful Autoconfiguration):

Bu yapılandırma biçiminde IPv6 adresinin yapılandırılabilmesi için harici bir sunucu kullanımına gerek vardır. Ancak adres yapılandırılması genelde DHCPv6 kullanılarak yapılmaktadır.

II.2.7.2 Durumsuz Otomatik Yapılandırma (Stateless Autoconfiguration):

Bu yapılandırma biçiminde harici bir sunucu olmadan IPv6 adresi yapılandırılabilmektedir. IPv6 adresinin son 64 biti (privacy extension) network kartından türetilip, ilk 64 biti router tarafından istenen durumda sağlanmaktadır. Bu mekanizma tarafından yaratılan link yerel adres, yerel ağda bilgisayarların birbiri ile iletişim sağlamaları için yeterlidir.



Şekil II.15 : Durumusuz Otomatik Yapılandırma

1. Ipv6 host networke ilk bağlandığı zaman otomatik olarak, MAC adres tabanlı, geçiçi bir bir link-local IP adresi oluşturur.
2. Host IP adresini kendine tahsis etmeden önce, DAD ile network içinde tek olduğunu ve aynı IP adresinin başka hostlar tarafından kullanılmadığından emin olması gerekir. Bunun için öncelikle kendi geçiçi link –local IP adresini kullanarak, bütün hostlara FF02::1 multicast adresi üzerinden NS mesajı yayınlar.
3. Komşu hostlar bu NS mesajını alırlar ve şayet gelen adres kullanılıyorsa bu adresin kullanılamayacağını ifade eden bir NA mesajı dönerler. Bu NA mesajı nedeniyle host bu adresi kendisine tahsis edemez. Bu örneğimizde komşu hostlardan dönen herhangi bir NA mesajı olmadğı farzedildi. Busayede host, ürettiği link-lokal adresin tek ve kullanılabilir olduğunu algılar ve bu adresi kendisine tahsis eder.
4. Host şimdi bütün routerlara FF02::2 multicast adresi üzerinden RS mesajı yayınlar. Bu adım ihmal edilebilir.
5. Routerdan dönen RA mesajı ön ek adresini(prefix), link konfigürasyon parametrelerini, global adres atamalarında durumlu(statefull) yada durumsuz(stateless) metodların kullanılıp kullanılmayacağını ve DHCPv6 kullanarak ilave network konfigürasyon parametlerini içerir.
6. Burada adres konfigürasyonu için durumsuz otomatik yapılandırmanın kullanıldığı farzedildi. Host burada kendi Ipv6 adresini şekillendirmek için routerın anons ettiği 64 bitlik prefix bilgisini, EUI-64 link-local formatındaki adresine ekleyerek Ipv6 adresini oluşturur. Statefull bir adres yapılandırması söz konusu olsaydı adresler DHCPv6 tarafından konfigüre edilecekti

Komşu Saptama (Neighbor Discovery) aleyhinde, IPv6 ND Trust Models and Threats [RFC 3756] dahilinde bahsedilen birçok güvenlik tehditi olmasına karşın, durumsuz otomatik yapılandırma ve komşu saptama ile alakalı birçok güvenlik sorunu aşağıdaki tehditlerle ilgilidir :

Neighbor Solicitation (NS) veya Neighbor Advertisement (NA) spoof edilerek lokal linke ulaşılır ve öyleki kötü niyetli host local linkteki diğer hostlara ulaşılabilir.

Spoof edilmiş global adres oluşturmak için Local linke erişilmesi ve RA mesajının alınması networkün diğer kısımlarına yetkisiz erişim imkanı sağlar.

Kötü niyetli kullanıcı sahte RA paketleri üretip yeni bir route oluşturabilir. Giden bütün paketleri istediği networkten geçirip paketleri yakalar ve sonra tekrar gitmesi gereken hedef noktasına yönlendirebilir (Redirect)

DAD atakları gibi DOS atakları da hiçbir kullanıcının networke bağlanmasına izin vermezler. Aynı şekilde çoğunlukla spoof edilmiş NS ve NA mesajlarından kaynaklanan varyanslar da kullanıcıların networke bağlanmalarına izin vermezler.

Yukarıda anlatılan tehditlerden IPSec ile korunabilir. Fakat IPSec'in kurulum problemlerinden dolayı devamlı olarak kulanılabilen bir güvenlik seçeneği değildir. Bu duruma daha pratik bir çözüm olarak Güvenilir Komşu Saptama - Secure Neighbor Discovery (SeND) geliştirilmiştir.

II.2.8 Güvenilir Komşu Saptama (SeND)

Güvenilir komşu saptama, ipsec kullanmaksızın güvenilir biçimde komşu saptaması için dizayn edilmiş bir mekanizmadır. Mevcut IPv6 standartları komşu saptaması ve otomatik adres konfigürasyonu mekanizmalarını IPSec AH ile korumaya imkan sağlasa da manuel ön konfigürasyonunun büyük ölçekli firmalarda kabul edilemez olduğundan daha pratik ve kullanılabilir olan SeND geliştirildi. IPv6 Neighbor Discovery Trust Models and Threats [RFC 3756] güvenli komşu saptaması için gerekenleri ele alarak SeND protokolünün oluştrulmasına sebep olmuştur.

SeND protokolü için iki yeni ICMPv6 opsiyonu tanımlanmıştır; RSA imza opsiyonu ve CGA Cryptographically Generated Address opsiyonu. Komşu saptama RSA public key imzası tüm mesajları korumak için kullanılır. Mesaj içeriğinin bütünlüğünü ve göndericinin kimliği için doğrulama sağlar. Public key otoritesi, dijital sertifika kullanarak otoritenin delagasyonu ile devam eder. Adres sahipliği kanıtlama mekanizması CGA tarafından sağlanır.

SeND, değiştirilmiş mesajlar kullanarak komşu önbelleğinde yanlış girdiler oluşturulması, komşu ulaşılamaz tespiti hatası, kopya adres kullanarak Dos atakları, router talep ve anons atakları, tekrarlama atakları ve komşu saptama dos atakları gibi saldırılara karşı koruma sağlar.

Bilinen hiçbir SeND uygulaması sevkiyatı olmamasına rağmen,bir kaç üretici işlemi kendi ürünlerine uygulamaktadır. CGA protokolünün IPR (Intellectual

Property Right)'ın hak talep ettiği protokolleri temel almasından dolayı bazı telif hakkı endişeleri mevcuttur. Bu da lisans kullanımı gerektirmektedir ki geniş çaplı yayılımı engellemektedir.

II.2.8.1 Güvenilir Komşu Saptaması İçin Ipsec Kullanımı.

İletişim halindeki hostlar arasında bir güven ilişkisinin olduğu çevrelerde güvenilir komşu saptaması için IPsec protokolü de kullanılabilir. Örneğin hostlar arasında öntanımlı anahtarlar veya PKI sertifkalarının tanımlı olduğu networklerde IPSec kullanılabilir. Bu durumda hostlar geçici IPv6 adresleri kullanarak IPSec güvenlik tesisini başlatabilirler ve daha sonra IPSec iletişimiyle gerçek IPv6 adresi alabilirler. Geçerli IPv6 adresler alındıktan sonra yeni IPSec güvenlik tesisi yeni IPv6 adreslerini kullanılarak daha sonraki iletişim için oluşturulur. Başlangıç olarak IPSec SA tesisi yeteneğine istinaden güvenilir bir birimle iletişim yapıldığını varsayılır. Bu senaryo zararlı bir cihazın networkte trafiğe kaynak olmasına veya geçerli bir IPv6 adresi elde etmeye çalışmasına engel olmaz [20]

II.2.9 IPv6 Adres Biçimi ve Türleri

IPv6 adresleri 8 adet 16 bitlik bloklardan oluşur ve 128 bittir. 16 bitlik bloklar, ":"işareti ile birbirlerinden ayrılmışlardır. Onaltılık sayı sistemini (Hexadecimal) kullanırlar ve bu sistemde büyük küçük karakter ayrımı yoktur. Mesela ;

2001: 09C0:130F:0000:0000:0000:876A:130B

IPv4 adreslerine daha uzun olduklarından kullanımı kolaylaştırmak bazı kısaltmalar oluşturulmuştur. Bunlar ;

-16 bitlik blokların başlarında yer alan 0'lar yazılmayabilir. Mesela; 2001:9C0:130F:0:0:0:876A:130B

- Çoklu 0'lar yerine " :: " ifadesi kullanılabilir. Mesela;
2001:9C0:130F::876A:130B
Fakat aynı adreste iki farklı "::" kısaltması kullanılamaz.

- IPv6 Ön Ekleri (Prefix) ondalık sayılardan oluşurlar. Baştan kaç bitin ağ adresine ait olduğunu belirlerler ve sadece bit sayısı ile ifade edilirler.

2001: 09C0:130F:0::/64 ya da 2001: 09C0:130F:0/64 şeklinde yazılabilir.

Ağ adresi : 2001:09C0:130F:0000:0000:0000:0000:0000
Ağ maskesi : FFFF: FFFF: FFFF: FFFF: 0000:0000:0000:0000

IPv6'da da IPv4 'teki gibi alt ağ kavramı vardır. FE80::2A0:D2FF:FEA5:E9F5/64 ile ilk 64 bitin ağı son 64 bitin bilgisayarları gösterdiği belirlenir. Standart IPv6'da ilk 48 bit ağı, sonraki 16 bit alt ağları en son 64 bit bilgisayarları belirtir. Bir ağda en çok 2^{16} adet (65536) alt ağ kadar bulunur. Her alt ağda 2^{64} adet bilgisayarlar bulunabilir. [13]

IPv6 adres türleri aşağıdaki tablo ile özetlenebilir.[11,21]

Tablo 1 IPv6 Adres Türleri

Adres Türü	İkilik Başlangıcı Öneki	Onaltılık Gösterimi
Yerel Bağlantı Unicast adresi	1111 1110 10	FE80::/10
Global Unicast Adres	001x	2xxx, 3xxx
Döngü adresi (loopback)	00..1 (128 bit)	::1/128
Belirsiz adres	00..0 (128 bit)	::/128
Multicast	1111 1111	FF00::/8

Şekil II.16 IPv6 Adres Türleri

- Tekli Yayın (Unicast) adresler,
- Anycast adresler,
- Çoklu Yayın (Multicast) adresler.

II.2.9.1 Tekli Yayın (Unicast) adresler

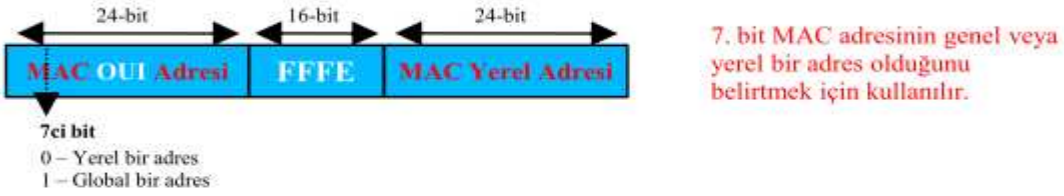
Bir bilgisayarı belirten adreslerdir. Bir paket böyle bir adrese yollanınca en kısa yoldan bu adresin belirttiği bilgisayara iletilir.

- Global Unicast Adres
- Site-Local Unicast Adres
- Link-Local Unicast Adres
- IPv4 uyumlu IPv6 adres **(**IPv4-Compatible Address**)**
- IPv4 bağlantılı IPv6 Adres **(**IPv4-Mapped Address)
- Belirsiz IP Adresi (Unspecified Address)
- Döngü Adresi (Loopback Address)

Global Unicast Adres

Bu adreslerin ilk 3 biti 001'dir ve IPv6 'da bu adresler 2000::/3 ile gösterilirler. İlk 3 bit ardından gelen 45 bit ile birlikte adresin nereye ait olduğunu gösterir. Toplam IPv6 adres toplamının 1/8!ini oluşturur. Yönlendiricilerde paketlerin iletimi bu 48 bite göre yapılır. Bundan sonra gelen 16 bit ise alt ağlar oluşturmaya yarar. Kalan 64 bit ise kullanılan arayüzü ifade eder. Arayüz numarası ise organizasyonların kendi yerel adres hiyerarşisini oluşturması içindir. EUI-64-bit metodu ile 48 bitlik MAC adresinin tam ortasına 16 bitlik FFFE değeri eklenerek eşsiz bir arayüz oluşturulur. Bu kısım otomatik olarak hesaplanır. Genel IPv6 adres bloğunun sekizde birini bu adres bloğu (2000::/3) oluşturuyor. 2001::/16 adres bloğu IANA (Internet Assigned Numbers Authority) tarafından İnternet Servis Sağlayıcılara (ISP) dağıtılmaktadır.

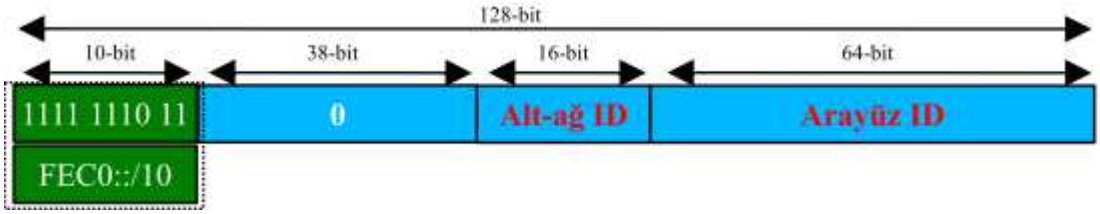
Şekil II.17: Global Unicast Adres Yapısı



Şekil II.18 : EUI-64 Arayüz Adres Yapısı

Site-Local Unicast Adres

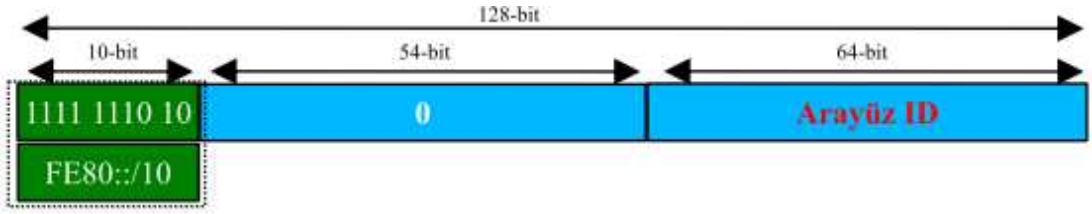
IPv4'teki private (özel) adreslere denk gelir. Bu adresler FEC0::/10 ön ekine sahiptir. Bu adresler yönlendiriciler tarafından site dışına anons edilmez ve kabul edilmezler. Eğer ileride genel ağa bağlanmak isterlerse global unicast ön-ek kullanılır. Bu işlem ön-ek değiştirmek dışında bir değişiklik gerektirmez. Yaşanan yönlendirme problemlerinden dolayı yerlerini Unique Local Unicast Adreslere bırakmışlardır. Bu adres tipi intranet trafiği için geliştirilimiştir fakat günümüzde kullanılmamaktadır.



Şekil II.19: Site-Local Unicast Adres Yapısı

Link-Local Unicast Adres

Bu adresler sadece bir arabirim bağlantısı üzerinde geçerli olacak özel adreslerdir. Link-Local ön-eki ve EUI-64 arayüz ID'si kullanılarak otomatik olarak atanır. Eğer hedef adresi olarak kullanılırsa paketler yönlendiriciyi asla geçemez. Bu adresler FE80::/64 ön ekine sahiptir. Yerel bağlantılarda, global bağlantı gerekmeyen durumlarda kullanılır.



Şekil II.20: Link-Local Unicast Adres Yapısı

IPv4 Uyumlu Adres (IPv4-Compatible Address)

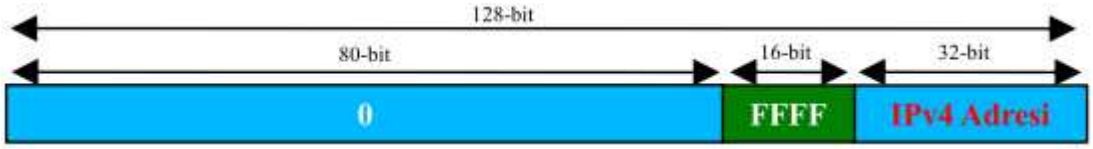
Bu adresler otomatik tünelleme yapmak için kullanılmaktadır. 0:0:0:0:0:0:A:B:C:D veya ::A:B:C:D şeklinde gösterilir. Burada A:B:C:D IPv4 adresinin onluk düzendeki karşılığıdır. IPv4 adresi son 32-bit içerisine yerleştirilmiş olarak saklanır. IPv4 uyumlu bir adres IPv6 hedefi olarak kullanılırsa, IPv6 trafiği otomatik olarak IPv4 başlığı ile kapsüllenir ve IPv4 altyapısı kullanılarak hedefe gönderilir.

Şekil II.21: IPv4 Uyumlu Unicast Adres Yapısı

IPv4 Bağlantılı Unicast Adres (IPv4-Mapped Address)

Sadece IPv4 adresine sahip bir düğümü IPv6 adresine sahip düğüme bağlamakta kullanılır. 0:0:0:0:0:FFFF:A:B:C:D veya :FFFF:A:B:C:D şeklinde ifade edilir. IPv4 adresi son 32-bit içerisine yerleştirilmiş olarak saklanır. Bu yalnızca

dahili tanıtım amaçlı kullanılır. IPv4 eşlemeli adres hiçbir zaman IPv6 paketinin bir kaynak veya hedef adresi olarak kullanılmaz.



Şekil II.22: IPv4 Bağlantılı Unicast Adres Yapısı

Belirsiz IP Adresi (Unspecified Adresses)

0:0:0:0:0:0:0:0 veya ::/128 olarak ifade edilir. Kesinlikle her hangi bir düğüme atanmamalıdır. Düğüm bir adrese sahip olmadığı zaman bu adresi kullanılır. Kendi Ip adresini öğrenmeden önce kullanıcı tarafından gönderilen IPv6 paketinin kaynak kısmında yer alır. Hiçbir zaman hedef adres olarak kullanılmamalı ve yönlendiriciyle iletilmemelidir.

Döngü Adresi (Loopback Address)

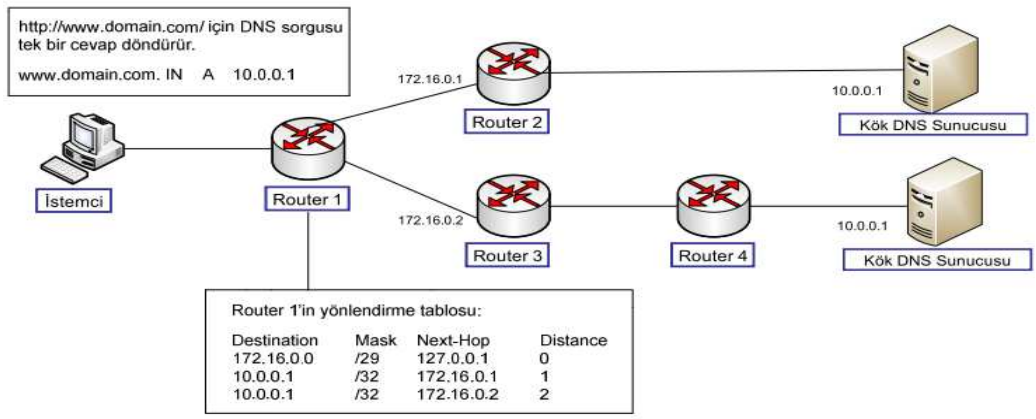
0:0:0:0:0:0:0:1 veya ::1 ile ifade edilir. IPv4'teki 127.0.0.1 adresinin karşılığıdır. Br düğümün kendisine paketler göndermesini sağlamak için kullanılırlar. Döngü adresine gönderilen paketler hiçbir zaman bir bağlantı üzerinden gönderilmemeli veya bir yönlendiriciyle iletilmemelidir**.** [21-23]

II.2.9.2 Anycast Adresler

Günümüzde gerek giriş seviyesinde gerek ileri seviyedeki IPv6 dökümanlarının çoğunda anycast adreslerden bahsedilir. Anycast IPv6 ile gelen bir yenilik değil, ilk kez 1993 yılında tanımlanmış bir tekniktir. Aynı IP adresinin genellikle farklı coğrafi konumlardaki birden fazla sunucuya ya da cihaza atanması ile mevcut yönlendirme protokollerinin isteklerin hangi sunucuya ya da cihaza iletileceğine karar verdiği bir tekniktir. Anycast 1993 yılında tanımlanmasına karşın geniş bir kullanım alanına ve bilinilirliğe sahip değildir. En yaygın ve verimli olarak Kök DNS sunucuları tarafından kullanılmaktadır. 13 Kök DNS sunucusundan 7 tanesi anycast teknolojisi kullanmaktadır**.**

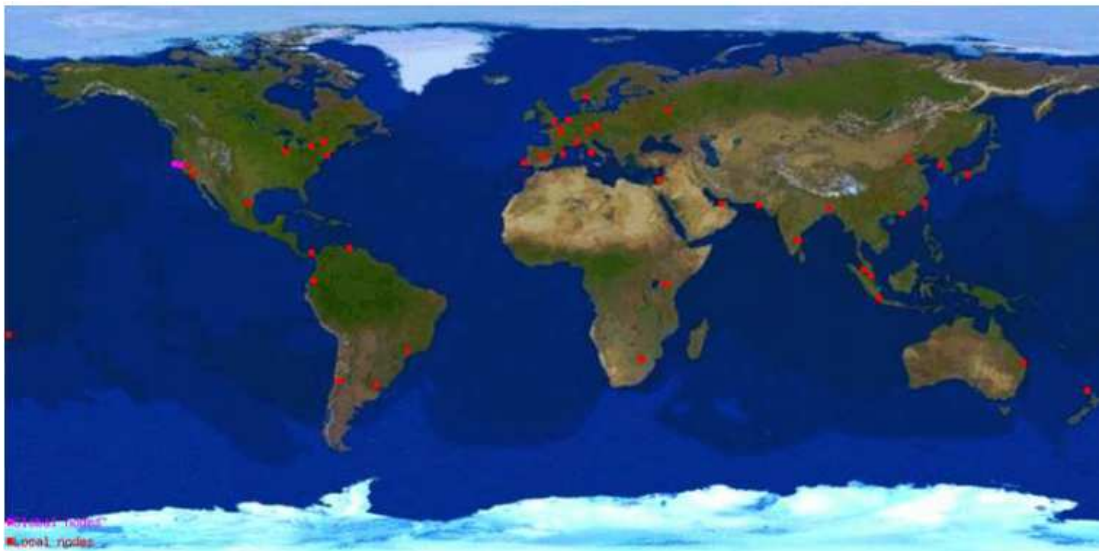
Anycast tekniğinde aynı IP adresi genellikle farklı coğrafi konumlardaki birden fazla sunucuya ya da cihaza atanır. Yönlendirme protokolleri bu IP hedefli istekleri kendi çalışma prensiplerine göre en iyi rotada bulunan sunucuya iletir. Şekil II.23'de

görüldüğü gibi istemcinin DNS sorgusu Router 1 tarafından Router 2'ye yönlendirilir.



Şekil II.23: Anycast Adres Çalışma Yapısı

Internet Systems Consortium(ISC) tarafından sunulan F Kök DNS sunucusu hizmeti 192.5.5.241 IPv4 adresi ve 2001:500:2f::f IPv6 adresi ile verilmektedir. Şekil[24]'de Dünya çapında konumlandırılmış F Kök DNS sunucularının konumları yeralmaktadır.[24]

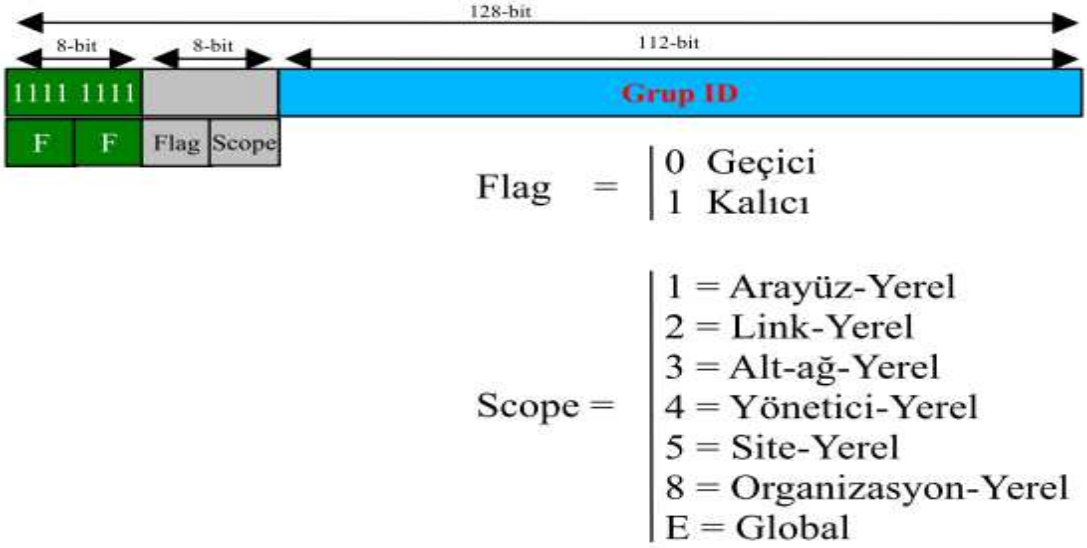


Şekil II.24: Dünya üzerindeki F Kök DNS sunucularının konumları

II.2.9.3 Çoklu-Yayın (Multicast) Adresler

Bu adresler birden fazla arayüze verilir. Gönderilen paket bu arayüzlerin hepsine ulaşır. Yapılan en büyük değişikliklerden biri de IPv4′de bulunan genel-yayın (broadcast) adresinin, IPv6'da kaldırılmış olmasıdır. Bunun yerine bir çok alana özgü yeni çoklu-yayın adresleri tanımlanmıştır. Her arayüze paketler gönderileceğine sadece belli bir gruba paketler gönderir. Örneğin yerel ağdaki tüm

aryayüzler, tüm yönlendiriciler veya tüm DHCP sunucular gibi yeni multicast adresler üretilmiştir. Böylece CPU'dan kazanç sağlanırken yerel ağdaki gereksiz trafik de önlenir. Genel olarak FF00::/8 ile ifade edilir. Flag biti (4-bit) adres ömrünü belirlerken Scope biti (4-bit) adresin tipini ve yayın kapsamını belirler.



Şekil II.25: Multicast Adres Yapısı

ff02::1 Yerel Ağdaki Tüm düğümler

ff02::2 Yerel Ağdaki Tüm Routerlar

ff05::1:3 Yerel Ağdaki Tüm DHCP Serverlar

ff02::101 Tüm Network Time Protocol (NTP) Serverlar gibi birçok Multicast adres tanımlanmıştır.[25]

Unicast Önek Tabanlı Multicast Adresleri

Bu tür çoklu-yayın adresleri sadece belirtilen ağ üzerindeki belirtilen düğümlere yayın yapılmak istendiğinde kullanılır. Bu yapıya göre örnek olarak 2001:0db8:1234::/48 ağındaki tüm dhcp sunucularına yayın yapılmak isteniyorsa kullanılması gereken adres:

ff35:0030:2001:0db8:1234:0000:0001:0003

olacaktır. Burada ikinci bloktaki son 8 bitlik alandaki 30 değeri onaltılık düzendedir ve onluk 48 değerinin eşitidir. Sonra gelen 64 bitte ağ adresi belirtilmiş ve son 32 bit ise dhcp sunucuları için gereken ID no belirtilmiştir.[11]

IPv6 İstemli-Birim Multicast Adresi (Solicited-Node Multicast Address) ve Üretilmesi

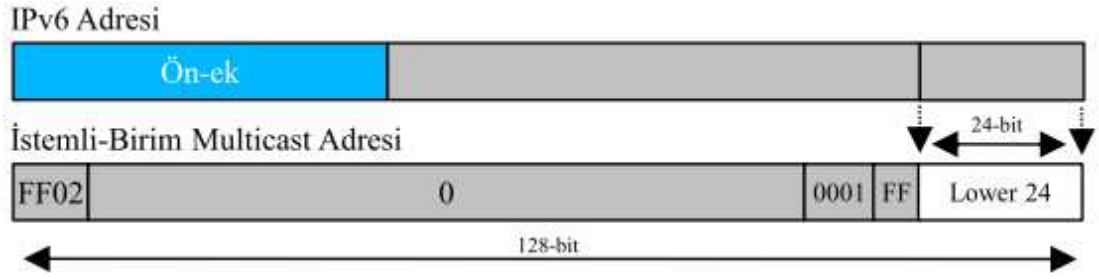
Normal multicast adreslerinin yanı sıra IPv6'da her unicast adresin solicited-node address olarak adlandırılan multicast adresi vardır. Bu multicast adresi cihazın unicast adresinden özel bir şekilde üretilir. Solicited-Node Multicas adresi IPv6 Neighbor Discovery protokolünde kullanılır. Temel olarak IPv4 te kullanılan ARP tekniğinin IPv6'ya uyarlanmasını sağlar.

Tüm solicited-node adreslerinde T flag 0, scope ID 2 dir. Yani "FF02" şeklinde başlarlar.

Unicast IPv6 Adresinden Solicited-Node IPv6 Adresi Üretilmesi

FF02::1:FF00:0 adresinin son 24 bit'i ile unicast ip adresi matematiksel "veya" işlemine tabi tutulurlar, bu işlem sonucunda Solicited-Node Multicast Addresses adresine ulaşılır. Daha kolay bir şekilde açıklayacak olursak;

Solicited-Node Multicast Adres = FF02:0:0:0:0:1:FF + Unicast adresin son 24 biti



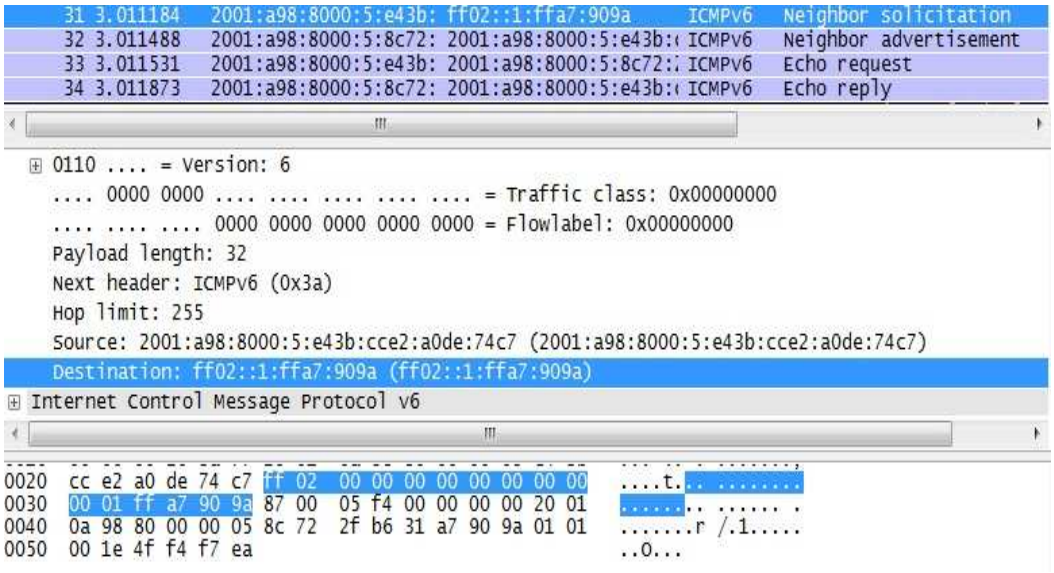
Şekil II.26: İstemli-Birim Multicast adresi

Bu bilgiler ışığında IPv6 adresi 2001:a98:8000:5:78e0:5830:820:5a9e olan bir cihaz aynı yerel ağdaki hedef 2001:a98:8000:5:8c72:2fb6:31a7:909a adresini pinglemek istiyor. Bu durumda beklentimiz kaynak makinenin ulaşmak istediği unicast adresininden oluşturacağı Solicited-Node Multicast adresine paket yollamasıdır.

Hedef Unicast adres : 2001:a98:8000:5:8c72:2fb6:31a7:909a

FF02:0:0:0:0:1:FF adresine unicast adresinin son 24 biti olan A7:909A'i eklersek FF02::1:FFA7:909A adresini elde ederiz yani yukarıdaki unicast adresine aynı yerel

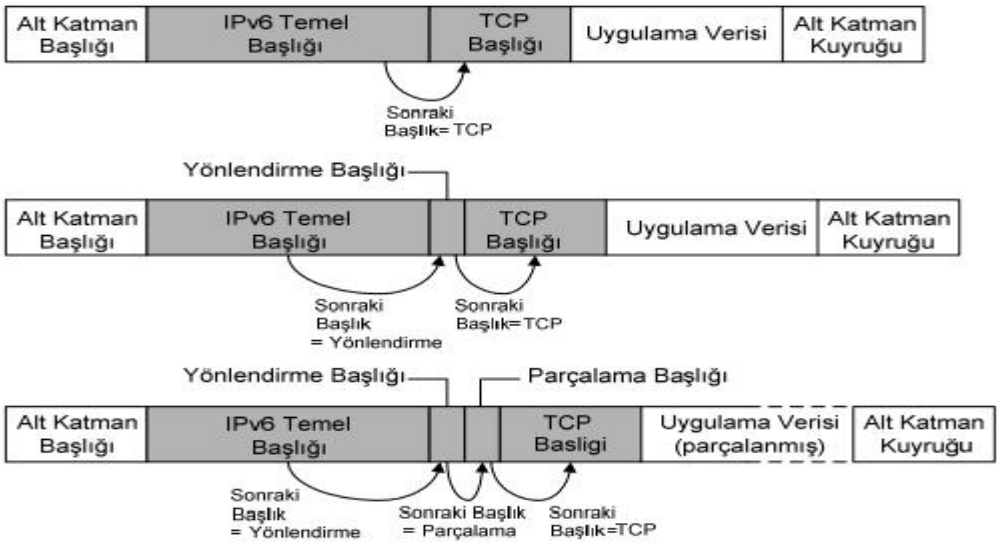
ağdan ulaşmak isteyen bir cihaz mac adresini öğrenmek için bu ip adresine ICMPv6 Neighbor solicitation mesajı yollar. Bu işlem sırasında Wireshark ile iletişim kurmak isteyen cihazın yolladığı paketler aşağıda görülmektedir [26]



Şekil II.27: İstemli-Birim Multicast adresi WireShark görüntüsü

II.2.10 Genişletilebilirlik - IPv6 Ek Başlıkları

IPv6'nın getirdiği en büyük değişimlerden birisi ise ek-başlık (extension header) yapısıdır. Temel IP başlığına ek olarak bu alan içerisindeki "sonraki başlık" (next header) kısmı sayesinde ilave edilmek istenen ve değişik özellikleri barındıran ek-başlıklar, IP başlığına ilave edilebilir.



Şekil II.28: IPv6 Ek-Başlık Kullanımı

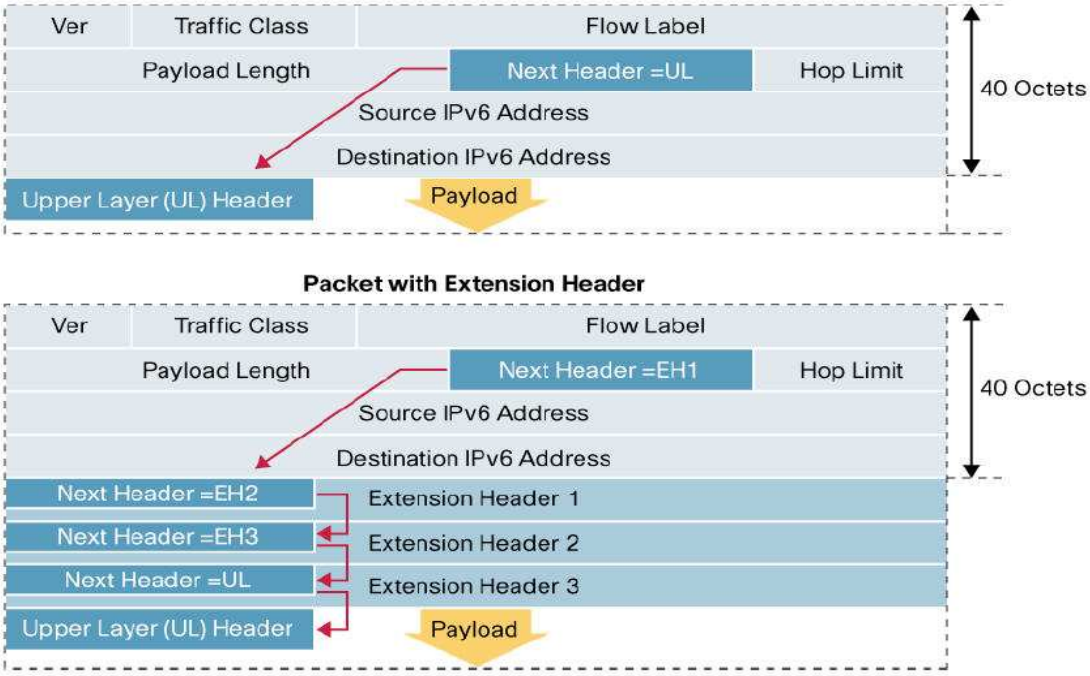
Tablo II.2: Ek-Başlık Kodları

Order	Header Type	Next Header Code
1	Basic IPv6 Header	–
2	Hop-by-Hop Options	0
3	Destination Options (with Routing Options)	60
4	Routing Header	43
5	Fragment Header	44
6	Authentication Header	51
7	Encapsulation Security Payload Header	50
8	Destination Options	60
9	Mobility Header	135
	No next header	59
Upper Layer	TCP	6
Upper Layer	UDP	17
Upper Layer	ICMPv6	58

Eğer IPv6 başlığında bir fazla uzantı başlığı aynı paket içerisinde kullanılacak ise, başlıklar yukarıdaki sıraya göre sıralanacaktır.[27]

Her uzantı başlığın bir 8 bit uzunluğunda tam sayı değeri vardır. Hangi başlığın geleceği hem IPv6 başlığındaki hem de uzantı başlığındaki "Sonraki

Başlık' değerine göre belirlenir. Uygulamalarda karşımıza sıklıkla yukarıdaki uzantı başlıkları gelmektedir.

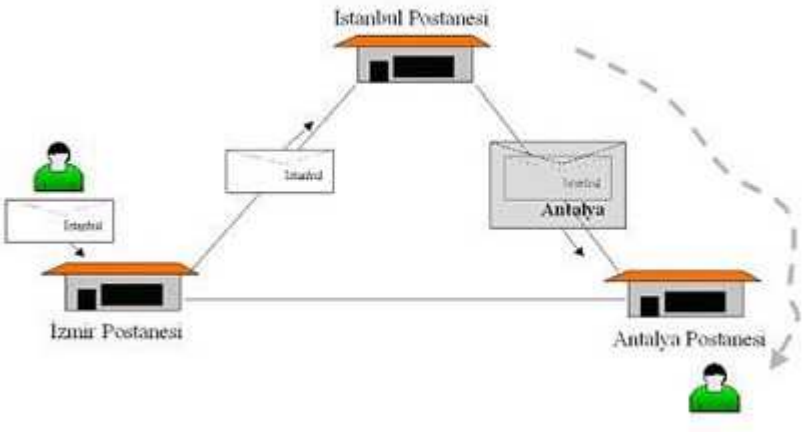


Şekil II.29: IPv6 Çoklu Ek-Başlık Kullanımı

II.2.11 Gelişmiş Mobilite

Mobil IP, mobil bilgisayarların şebekeye bağlantı noktaları değiştiğinde, IP adresi değişmeksizin İnternete bağlı kalmasını olanaklı kılan ve TCP gibi daha yüksek protokollere açık, İnternet protokolü üzerine inşa edilen bir standart protokoldür. Günümüzde kullanılan IPv4 protokolü ve yeni nesil IP diye adlandırılan IPv6 protokolünün her ikisi de Mobil IP'yi desteklemektedir. Ancak mobilite destek verimliliği için daha çok birçok özellikler ile gelişmiş ağ güvenliği desteği sağlayan IPv6'ya yönelinmektedir. Mobil IP, mobil sunuculara açık şebeke bağlantısı sağlayan bir mekanizma ve kullanıcılara mobil cihazları ile farklı IP adresine sahip başka bir şebekede olduğu zaman, İnternet bağlantılarını sürdürmeleri için IP adreslerinin şebeke ile birleşmesine izin veren bir standarttır. Böylece Mobil IP, servis sunucu şebekelerine otomatik olarak uygun IP tabanlı bağlantıları sağlayarak, şebekeler boyunca dolaşıma açık mobil cihazları (mobil düğüm noktalarını) olanaklı kılmaktadır. Bu durumda, mobil düğüm noktası, şebekenin farklı bölgesinde işletildiği zaman, cihazın IP adresinin değişme zorunluluğu ortadan kalkmaktadır[30]

Mobil IP protokolünün çalışma prensibini hayattan bir örnekle açıklayalım. Posta servisini düşünürsek, bir vatandaş olarak sizin bir posta adresiniz (mesela İstanbul'da) ve kullandığınız postaneniz var. İzmir'deki arkadaşınız size bir mektup attığında, bu mektup yerel postane üzerinden sizin adresinize ulaştırılmakta. Ta ki geçici bir süre için bile olsa siz o adresten çıkana kadar. Mesela o yaz tatil için Antalya'ya gittiniz. Normalde hiçbir şey yapmazsanız mektubunuz İstanbul'a gelecek ve orada kalacaktır. Eğer sizin İstanbul adresinize yollanan mektupların Antalya adresinizde elinize ulaşmasını istiyorsanız, o zaman yeni adresinizi İstanbul'daki postaneye bildirmeniz gerekecektir. Bunda sonra, İstanbul postanesi size yollanan mektubu, üzerine Antalya'daki adresinizin yazılı olduğu bir başka zarfa koyarak size yollayabilir. Siz de, elinize İstanbul postanesinden gelen zarfları açtığınızda içinden sizin İstanbul adresine yollanan orijinal mektubunuzu bulacaksınız. Daha sonra eğer Antalya'dan Side'ye geçerseniz yine İstanbul postanesine durumu bildirmek suretiyle mektuplarınız yeni adresinizde elinize ulaşacaktır. Görüldüğü gibi basit bir mekanizmayla, sürekli yer değiştirmenize rağmen sanki hala orijinal adresinizdeymişçesine iletişim kurabilirsiniz.



Şekil II.30: Mobil IP

Bu mekanizmayı birebir IP'ye uygularsak karşımıza çıkan protokolün adı Mobil IP oluyor. Ev adresiniz cihazınızın sabit IP adresi (home address), tatilde gittiğiniz yerlerdeki adresleriniz geçici IP adresi (care-of address), İstanbul'daki postane sizin her zaman konum bilginizden haberdar olan yuva sunucusu (home agent), ve zarfı bir başka zarfın içine koyup yollamak da IP tünellemesi oluyor.

Cihazınız evdeyken kullandığı sabit adres içinde bulunduğu ağın bir parçası olduğu için kendisine yollanan paketlere ulaşabilecektir. Internet'teki yönlendiriciler

bu adrese yollanmış bir paketin fiziksel olarak hangi ağda olduğunu bilirler (BGP ve RIP sayesinde). Ne zaman ki sizin cihazınız yuva ağından (home network) ayrılır, o zaman kendisine yollanan paketler ulaşmamaya başlar. Nitekim bu paketler hala yuva ağına gitmekte ve orada sahipsiz kalmaktadırlar. Cihazınızın ilk olarak yapması gereken yeni bağlandığı ağı keşfetmesidir (movement detection, router discovery). Daha sonra, PPP veya DHCP gibi protokolleri kullanarak bir geçici adres edinir. Bu geçici adres bağlandığı ağdan bir adrestir. Bu topolojisi doğru (topologically correct) adrese yollanan paketler cihazımıza ulaşacaktır. Şimdi geriye kalan, cihazımızın bu geçici adresi yuva sunucusuna bildirmesidir. Bu da kayıt (registration) paketinin yollanmasıyla olur. Bu kayıt paketini alan yuva sunucusu artık cihazın evde olmadığını bilir ve cihazın ev adresine yollanan paketleri onun adına almaya başlar. Her yakaladığı paketi kendi hazırladığı başka bir IP paketinin içine koyar. Bu yeni paketin varış adresine de cihazımızın geçici adresini yazar. Böylece cihazımızın iletişim içinde bulunduğu herhangi bir karşı tarafın yolladığı paketler, hiç değiştirilmeden IP tünellemesiyle cihazımızın yeni bulunduğu ağa yollanır. Cihazımız her ağ değişikliğinde bu protokolü takip ederek kendisini "erişilebilir" (reachable) konumda tutar.

II.2.12 Fragmantasyon

IPv6'nın adres başlık yapısındaki en önemli değişiklerinden biri de yönlendirici gibi ara elemanlarda parçalama (Fragmentation) ve hata kontrolü yapılmamasıdır. Bu görevler bir üst seviyedeki protokol olan TCP'ye yani iletişimdeki uç noktalara bırakılmıştır. Bu değişiklik sayesinde bu işlevleri yerine getirmekte kullanılan Fragment Offset ve Header Checksum bölümleri IPv6'da yer almamaktadır.

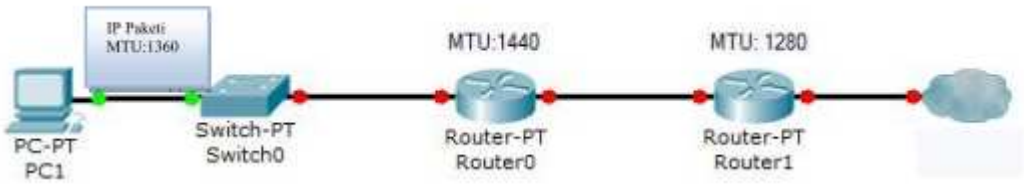
Örnek şema ile madde madde açıklanırsa;

1. Aşağıdaki şekilde verilen örnekte görüldüğü gibi PC1'den çıkan paketin uzunluğu1360 byte olsun.
2. Router0 işleyebileceği maksimum iletim birimi (MTU) boyutundan düşük bupaketi Router1'e aktaracaktır.
3. Ancak işleyebileceği MTU boyutu 1280 olan Router1 (IPv6) bu paketi

fragmante etmeyecektir ve bu paketi düşürecektir.

4. Bununla birlikte ICMPv6 olarak Paket Çok Büyük (Packet Too Big) mesajı kaynağa yollanacaktır.

5. Kaynak, paketi uygun boyuta fragmante edip (parçalayıp)fragmantasyon başlıkları eklenmiş halde tekrar yollayarak başarılı bir iletişim gerçekleştirilir.



Bu örnek senaryoda görüldüğü gibi bu şekilde iletişim aksamalarının önüne geçmek için "iletişim yolunun MTU'su" (Path MTU) olarak adlandırılan, belirli bir hedefe gönderilebilecek maksimum paket büyüklüğünü hesaplamaya yönelik olarak RFC1981'de tanımlanan "iletişim yolu MTU'su bulma" (path MTU Discovery) süreci tanımlanmıştır. IPv6 düğümlerinin "iletişim yolu MTU'su bulmayı kullanmaları şart değildir; ancak bunu kullanmayacaklarsa, izin verilen minimum IPv6 MTU olan 1280 byte'tan daha büyük paket yollamamaları tavsiye edilir.[11]

II.3 IPv4'TEN IPv6'YA GEÇİŞ SÜRECİ

IPv6'ya geçiş son yıllarda özellikle Asya ve Avrupa'da artmıştır. IPv6'ya geçişte en kolay ve etkili yol, hâlihazırda var olan IPv4 ağlarına IPv6 ile çalışan cihazlar eklemek ve zaman geçtikçe IPv6 ağırlığını artırarak nihayetinde bütün ağların IPv6 ile çalışır hale gelmesini sağlamaktır. Yani IPv4 ağlardan tamamen IPv6 ağlara geçiş keskin bir zaman aralığı değil, uzun vadeli bir süreç olacaktır.

IPv4'ten IPv6'ya geçiş keskin bir zaman diliminde değil uzun vadeli bir süreç içinde gerçekleşecektir. Dünya üzerindeki organizasyonlar en sorunsuz bir şekilde bu geçişi sağlayabilmek için çalışmalar yapmakta ve geçiş teknolojileri geliştirmektedirler. Genel olarak bu teknolojiler [4] :

II.3.1 Geçiş Teknolojileri

İkili Yığın (Dual Stack): Ağ cihazlarında hem IPv4, hem de IPv6'nın birlikte çalışması

Tünelleme: IPv6 paketlerin IPv4 paket formatına dönüştürülerek, IPv4 ağ üzerinden gönderilmesi

Dönüştürücü: Ağ geçidi veya yönlendirici tarafından yapılan adres ve port dönüşümü

II.3.1.1 İkili Yığın

İkili yığın teknolojisinde, ağ cihazlarında hem IPv4 hem de IPv6 desteklenmektedir. Böylece IPv4-IPv4 iletişimler ve IPv6-IPv6 iletişimler aynı ağ üzerinden gerçekleşmektedir. Bu teknolojinin uygulanabilmesi için yönlendirici gibi ağ katmanında çalışan ağ cihazları ve son kullanıcı bilgisayarları hem IPv4 hem de IPv6 teknolojisini desteklemelidir. Bu cihazlarda hem IPv4 hem de IPv6 adresi ayarlanabilmektedir. Örneğin bir ağ yöneticisi IPv4 adreslerin, IPv4 ile çalışan DHCP üzerinden dağıtımını sağlayabilir. Aynı zamanda IPv6 adreslerin otomatik olarak ayarlanması gerçekleştirilebilir.

Ortak bir ağ altyapısında çalışan IPv4 ve IPv6 teknolojisinin ikili yığınla çalışan cihazlarda uygulanması, hem IPv4 hem de IPv6'nın aynı fiziksel bağlantılardan iletilmesini gerektirmektedir. Dolayısıyla ethernet ve ikinci katmanda çalışan diğer teknolojiler hem IPv4 hem de IPv6'yı desteklemelidir. IPv4 ve IPv6'yı destekleyen cihazların her iki teknolojiyle de çalışabilmesi için bu tür fiziksel bağlantıları da desteklemesi gerekmektedir.

Bu mimariyi gerçekleştirebilmek için yönlendiricilerin IPv6'yı desteklemesine yönelik sürüm yükseltme işlemlerinin yapılması gerekir. RFC 4554, yönlendiricilerde yapılması gereken bu sürüm yükseltme işlemi yapılmadan VLAN kullanılarak IPv6'nın nasıl uygulanabileceğini tanımlamaktadır. Bu tanımlamaya göre ikinci katmanda çalışan anahtarlar IPv6 paketlerini yönlendiricilere gönderebilmektedir. IPv6'yı destekleyen bir yönlendirici ile anahtarın birlikte çalışabilmesi için anahtarda IPv6 VLAN ayarlanabilmektedir. IPv6 veya ikili yığınla çalışan diğer cihazlar daha sonra bu VLAN'a atanabilir.

II.3.1.2 Tünelleme

IPv4 üzerinden IPv6 paketlerini veya IPv6 üzerinden IPv4 paketlerini iletmek için kullanılabilecek pek çok tünelleme teknolojisi bulunmaktadır. Bu teknolojiler genel olarak ayarlanmış ve otomatik gibi iki şekilde ifade edilebilir. Ayarlanmış tüneller önceden tanımlıdır.

Genel olarak IPv6 paketlerinin IPv4 ağı üzerinden tünellenmesi, her bir IPv6 paketin başına IPv4 başlığı eklenmesiyle gerçekleştirilir. Bu işlemle birlikte tünellenmiş IPv6 paketlerinin IPv4 cihazlar tarafından iletilmesi sağlanır. Tünelin başlangıç ve bitiş noktaları yönlendirici veya son kullanıcı olabilir. Kaynak IPv4 adresi olarak tünel başlangıcındaki cihazın IPv4 adresi, hedef IPv4 adresi olarak da tünel bitişindeki cihazın IPv4 adresi verilir. IPv4 başlığın protokol numarası kısmı ikili düzende 41 olarak ayarlanır. Bu sayı IPv6 tünellemeyi ifade etmektedir. Tünelin çıkış noktası IPv4 başlığını açarak IPv6 paketi ortaya çıkarır ve gerekli yönlendirmeleri yaparak bu paketin hedefine ulaşmasını sağlar.

II.3.1.3 Dönüştürücü

IPv6 paketleri, IPv4 paketlere veya IPv4 paketleri IPv6 paketlere dönüştürerek iletmek mümkündür. Bu dönüşümler Ağ Adres Dönüşümü ve Port Dönüşümü (PT) ile yapılır.

İkili yığın yöntemi kullanımı kolay ve esnek bir çözümdür. Ancak bu yöntem IPv4 ve IPv6 yığınlarını bir arada çalıştırmak zorundadır. Bu yüzden daha çok hafıza ve işlemci gücü gerektirmektedir. Ayrıca bu yöntemde kullanılan uygulamaların, bilgisayarların IPv4'le mi yoksa IPv6'yla mı çalıştığını tespit edebilmesi gerekir.

Tünelleme yöntemi, herhangi bir ISS desteği olmadan ve kullanılan ISS IPv6 protokolünü desteklemiyorsa bile, IPv6 protokolüyle iletişim yapılabilmesini sağlar. Bütün bir ağda sadece iki bilgisayar IPv6 teknolojisi içeriyorsa, IPv4 ağı üzerinden bu iki bilgisayarın IPv6 ile haberleşebilmesi tünelleme yöntemiyle mümkündür. Bu yöntemin olumsuzlukları, diğer tünelleme mekanizmalarında olduğu gibi, tünel giriş ve çıkış noktalarında çalışan cihazların fazladan iş yapması ve tekil arıza noktaları içermesidir.

Dönüşüm yöntemleri ise sadece özel ihtiyaçlar halinde kullanılır. Bu yöntem, IPv6 teknolojisiyle gelen bazı özelliklerin kullanılamamasına sebep olmaktadır.

Her bir dönüşüm yöntemi çeşitli artılar ve eksilere sahip olmasına karşın uygulanacak ağın durumu hangi yöntemin seçileceğinde önemli bir rol oynamaktadır. Etkin bir geçiş yöntemi için ağ analiz edilmeli, ihtiyaçlar belirlenmeli ve ona uygun bir geçiş yöntemi seçilmelidir.

Tablo II.3 IPv4-IPv6 arası geçiş mekanizmaları [13]

İSİM	BAĞLANTI	TİP
İKİLİ YIĞIN	4'TEN 4'E , 6'DAN 6'YA	İKİLİ YIĞIN
SIIT	6'DAN 4'E 4'TEN 6'YA	DÖNÜŞTÜRÜCÜ
BIS	4'TEN 6'YA	DÖNÜŞTÜRÜCÜ
BIA	4'TEN 6'YA	DÖNÜŞTÜRÜCÜ
NAT-PT	6'DAN 4'E 4'TEN 6'YA	DÖNÜŞTÜRÜCÜ
MTP	6'DAN 4'E 4'TEN 6'YA	DÖNÜŞTÜRÜCÜ
TRT	6'DAN 4'E	DÖNÜŞTÜRÜCÜ
SOCKS64	6'DAN 4'E 4'TEN 6'YA	DÖNÜŞTÜRÜCÜ
4 ÜZERİNDEN 6	4 ÜZERİNDEN 6'DAN 6'YA	TÜNEL
ISATAP	4 ÜZERİNDEN 6'DAN 6'YA	TÜNEL
DSTM	6'DAN 6'YA , 4'TEN 4'E	TÜNEL
İP İÇİNDE İP	6'DAN 6'YA , 4'TEN 4'E	TÜNEL
DİNAMİK TÜNEL	6 ÜZERİNDEN 4'TEN 4'E	TÜNEL
6'DAN 4'E OTOMATİK	4 ÜZERİNDEN 6'DAN 6'YA	TÜNEL

II.4 GÜVENLİK

Günümüzde, dünyada 400 milyon civarında İnternet'e bağlı bilgisayar, 1 milyarı aşkın İnternet kullanıcısı, 100 milyona yakın web sitesi olduğu tahmin ediliyor. Türkiye'de ise bu rakam 15 milyona ulaşmış durumdadır. Bu platformda yapılan elektronik ticaret gibi gerçek zamanlı ve para transferinin söz konusu olduğu işlerde; askeri güvenlik uygulamalarında performansın, doğruluğun ve güvenliğin en üst düzeyde olması gerekir. İnternet uluslar arası veya ulusal arenada bir firmanın varlığını rekabetçi olarak sürdürebilmesi için yenilikleri takip, bilgi edinme, bilgi paylaşım, haberleşme, pazar araştırması ve benzeri konularda en büyük yardımcısıdır. Ancak aynı zamanda firmanın tüm dünyaya açık, savunmasız bir penceresidir. Şirketlerin de kendilerine ait çok özel ve önemli sırları ve bilgileri mevcuttur. Şirket yerel alan ağlarının internet bağlantılarında güvenliğin sağlanması belki de şirketin var olması kadar önemlidir. Ancak bu noktayı çok iyi dengelemek ve internet ortamından gelecek zararlardan cok faydalarını ön plana çıkarabilecek bir güvenlik organizasyonunun oluşturulması gerekmektedir.

Firmaların kendi içlerinde tuttukları verilere saldırı olabildiği ve korunması gerektiği gibi cok basit bir şekilde firmaların kendi tanıtımlarını yaptıkları web sitelerine yapılabilecek bir saldırıda cok büyük maliyetlere yol açabilmektedir. Bunu

basit bir hesaplamayla incelediğimizde; genellikle bankacılık sektörünün sitelerinin yüksek güvenlik içerdiği ve maliyet açısından büyük yatırımlar yapıldığı ancak onun haricinde diğer firmaların kendi sitelerine bu derece maliyetli yatırımları fazla gördükleri gözlenmiştir. Basit bir örnek olarak Borsada hisseleri işlem gören bir firmanın kendi tanıtım sitesine yapılan bir saldırıda sitenin ekran penceresinde kayan haber hattına firmanın bu yıl zarar açıkladığı ve yönetim kurulunun istifa ettiği bilgisinin kötü niyetli kişiler tarafından saldırı yapılarak yazılması 10.000 $ lık güvenlik yatırımından kaçınan firmanın haberi fark edip düzeltinceye kadar 1 milyon $ lık bir kayba uğramasına neden olmaktadır.

Bir diğer örnek ise internet üzerindeki en iyi performansa sahip sitelerden biri olan YaHOO!'ya 1999 yılında düzenlenen saldırıdır. . Bir internet analiz servisi olan Keynote Sysyems ' e göre Yahoo normalde % 99.3 'lük erişim oranına sahipti. Fakat saldırı sırasında YAHOO portalı 3 saat boyunca neredeyse erişilmez hale geldi. Bu zaman aralığındaki erişim oranı sadece % 0 ile % 10 aralığındaydı.New York' taki Wit Capital Group'tan Jordan E. Rohan Yahoo 'nun erişilemediği süre boyunca 100milyon gibi çok sayıda sayfa görüntüsünü kaybetmiş olabileceğini ve muhtemel reklam ve elektronik ticaret geliri kaybının yaklaşık olarak 500.000 $ olduğunu belirtti. Günümüzdeki rekabet koşullarında kurumların ülkelerin ve organizasyonların varlıklarının temeli olan stratejik bilgilerin üretildiği, işlendiği, saklandığı iletildiği ve işlem yapıldığı bilişim sistemleri bu bilgi ile çıkar, rant ekonomik avantaj ve rekabet gücü sağlayacak kişi kurum ve hatta ülkeler tarafından potansiyel hedef olarak değerlendirilmektedir. İnternet kullanan şirketlerin % 50 sinden fazlası güvenlik saldırılarına uğramakta ve saldırıya uğrayanların da % 60 'ı güvenlikle ilgili karşılaştığı saldırı ve bilgi sızmalarının farkına bile varmamaktadır.[31] Bu nedenlerle güvenlik zaaflarına karşı etkin tedbirlerin alınması oldukça önemlidir. Fakat bununla birlikte güvenlik önlemlerinin hiçbir zaman mükemmel olamayacağı ve her güvenlik önleminin bazı zayıflıkları olduğu gerçeği de unutulmamalıdır.

Yerel ağda alınabilecek temel önlemler aşağıda sıralanmıştır.[32]

Cihazların OSI'nin hangi seviyesinde çalışma yeteneğine sahip olduğuna göre L2 ve L3 cihazlar olarak tanımlanmıştır. Ağda alınabilecek önlemleri dört ana başlıkta sınıflamak mümkündür:

- L2 Cihazlar ile Alınabilecek Önlemler
- L3 Cihazlar ile Alınabilecek Önlemler
- Güvenlik Cihazları ile Alınabilecek Önlemler
- Diğer Sistemler ile Alınabilecek Önlemler

II.4.1 L2 Cihazlar ile Alınabilecek Önlemler

OSI'nin 2. katmanında çalışan yerel ağ cihazlarında alınabilecek önlemler aşağıdaki gibidir:

- MAC Adresi Bazında Güvenlik
- 802.1x Tabanlı Kimlik Tanımlama
- Broadcast/Multicast Sınırlandırması

II.4.1.1 MAC Adresi Bazında Güvenlik

Switch'lerde port bazında MAC adresi güvenliği uygulaması zor bir çözümdür. Böyle bir işleme gidebilmek için önce bütün kullanıcıların MAC adresleri toplanmalı ve bu bilgiler sürekli güncel tutulmalıdır. Kaldı ki, günümüzde MAC adresi çok kolay değiştirilebilmektedir. Yani o porttan, switch'de izin verilen MAC adresini giren başka bir kullanıcı da erişebilecektir. Günümüzde zararlı yazılımlar bulaştıkları bilgisayarların tespitini zorlaştırmak için IP adreslerini ve MAC adreslerini bile değiştirebilmektedirler.

MAC adresi güvenliğinin cihazlarda uygulanması durumunda aşağıdakiler sağlanabilecektir:

- Ağa kontrolsüz bilgisayar erişimi ve MAC adres değiştirme durumunda bağlantı engellenecek,
- MAC flood saldırısı ile switch'in MAC adresi tablosu doldurulup Hub gibi çalışması engellenecek,
- Bu tür durumlar loglanacak ve bilgisayarın yeri tespit edilecektir.

Birçok markanın yönetilebilir anahtarlama cihazları ile bu önlemler alınabilmektedir. Aşağıda Cisco marka anahtar cihazlarında uygulanabilecek komutlar verilmiştir:

- Portta MAC adres güvenliğinin açılması:

```
switch(config)#Interface <int adı> <int.no>
switch(config-if)# switchport port-security
```

- Switch'in o portundan erişimine izin verilen MAC adresinin tanımlanması:

```
switch(config-if)# switchport port-security mac-address <PC'nin MAC
adresi>
```

- Porttan bağlanması istenen maksimum PC sayısının belirlenmesi

```
switch(config-if)# switchport port-security maximum <toplam PC sayısı>
```

- Belirtilen MAC adresi dışında bir PC'nin porta dahil olması veya belirtilenden daha fazla PC'nin porta dahil olması durumunda uygulanacak işlemin tanımlanması. Bu işlemler ayrıntılı olarak aşağıdaki tabloda belirtilmiştir

```
switch(config-if)# switchport port-security violation <protect | restrict
| shutdown>
```

Cisco marka anahtar cihazları için örnek konfigürasyon aşağıda gösterilmiştir.

```
switch(config)#Interface fastethernet 0/0
switch(config-if)# switchport port-security
switch(config-if)# switchport port-security maximum 2
switch(config-if)# switchport port-security violation restrict
switch(config-if)# switchport port-security mac-address 1010.1010.1010
switch(config-if)# switchport port-security mac-address 2020.2020.2010
```

II.4.1.2 802.1x Tabanlı Kimlik Tanımlama

IEEE 802.1X, port tabanlı ağ erişim kontrol standardıdır. Kullanıcı bilgileri (kullanıcı adı, parola ve bazı özel durumlarda MAC adresi) yardımı ile ağa ağlanılmasına izin verilmesini sağlar. Kullanıcı doğrulama sırasında EAP extensible authentication protocol-RFC2284) yöntemi kullanılır. 802.1x için ağ

altyapısındaki yönetilebilir (switch, kablosuz ağ cihazı gibi) cihazlarda gerekli ayarlar yapılmalı ve kullanıcı bilgilerini denetleyip gerekli düzenlemeleri yapacak bir sunucu bulundurulmalıdır.

Bu protokol sayesinde, sadece kurumun kullanıcıları izin verilen ağlara bağlanılacaktır. Güvenlik açısından, misafir bilgisayarların ayrı bir VLAN'a bağlanması ile yetkileri, ulaşabilecekleri ağlar ve kullanacakları iletişim kapıları kısıtlanabilecektir. Bu da zararlı yazılımların dağılmasını kısıtlayabilecektir. Kullanıcının bu tür bir yöntemle sisteme bağlanması anında, kişisel antivirüs yazılımını ve imza güncelliğini denetleyen ticari sistemler de bulunmaktadır. Böylece kullanıcı, kurumun antivirüs yazılımını kurana ve/veya güncel imzaya sahip olana kadar, sistem tarafından ayrı bir sanal ağa alınacaktır. Ancak gerekli yüklemeler gerçekleştikten Kurumsal Ağlarda Zararlı Yazılımlarla Mücadele Kılavuzu sonra kendi ağına bağlanabilecektir. Bu da, zararlı yazılımların etkin olmasını engelleyecek yöntemlerden birisidir.

Cisco marka anahtar cihazları için örnek konfigürasyon aşağıda verilmiştir:

```
dot1x mac-auth-bypass eap
dot1x pae authenticator
dot1x port-control auto
dot1x timeout quiet-period 1
dot1x timeout tx-period 1
dot1x max-req 1
```

II.4.1.3 Broadcast/Multicast Sınırlandırması

DoS veya DDoS saldırılarının bir kısmı broadcast (genel yayın) adresi üzerinden yapılmaktadır. Bu tür saldırıların etkisinin azaltılması için broadcast sınırlaması yapılmalıdır. Broadcast düşünülürken, kullanılan protokol dikkate alınmalıdır. En yaygın olanları Ethernet ve IP'dir.

Broadcast/multicast/unicast trafiğinin 1 saniyede belirli bir yüzdeyi aşması durumuna, Broadcast/multicast/unicast fırtınası (storm) denilmektedir. anahtarlama cihazlarında yapılan ayarlama, 1 sn içinde interface'in toplam bant genişliğinin belirlenen yüzdeyi geçmesi veya belirlenen paket sayısını aşaması durumunda eşik değerinin üstündeki trafiğin bloklanmasıdır. Kullanılan cihaza ve odüle bağlı olarak broadcast, multicast ve unicast trafik kontrol edilebilir. Örneğin cisco cihazlarda bu kontrol donanım seviyesinde yapılmaktadır.

Yapılabilecek bazı denetimler ve çalışma şekli aşağıdaki gibidir:

- Tek başına Broadcast Traffic Storm Control özelliğinin açılması: 1sn içinde eşik değeri aşılırsa eşik değeri üstündeki bütün broadcast trafiği bloklanır.
- Multicast ve Unicast Traffic Storm Control aynı anda açılması:
- Multicast ve broadcast trafiği toplam eşik değerini aşarsa, o birim zamandaki bütün aşan multicast ve broadcast trafiği bloklanır.
- Sadece broadcast trafiği toplam eşik değerini aşarsa, o birim zamandaki bütün aşan multicast ve broadcast trafiği bloklanır.
- Sadece multicast trafiği toplam eşik değerini aşarsa, o birim zamandaki bütün aşan multicast ve broadcast trafiğini bloklanır.

Cisco marka cihazlarda bu düzenlemelerin yapılması durumunda, aşağıdaki özellikler dikkate alınmalıdır:

- BPDU paketleri bazı cihazlarda multicast trafiğinden sayılır ve eşik değeri aşılırsa BPDU paketleri de bloklanır. Bazı modeller BPDU trafiğini storm kontrolü dışında tutabilmektedir. Eşik değeri aşılsa bile bu cihazlarda BPDU trafiği bloklanmaz.
- Eşik değeri 0 yapılırsa bütün trafik bloklanır
- Eşik değeri 100 yapılırsa hiç bloklanma yapılmaz.
- Default'ta bütün traffic storm control özellikleri kapalıdır.
- EtherChannel interface'lerinde storm control açılabilir. Ancak konfigürasyon, fiziksel interface'lerde değil sadece mantıksal port channel interface'inde uygulanmalıdır.

Aşağıda Cisco marka cihazlarda "storm control" komutları açıklanmıştır. Bu komutlarda, "Level" değeri ile belirtilen yüzde veya paket değerinin aşılması durumda aşan trafik bloklanmaktadır. "Level-low" ise seçimlidir ve "Level" ile belirtilen değerin aşılmasından sonra, trafiğin hangi değer altına inmesi durumunda tekrar bloklanmanın kaldırılacağı belirtilmektedir. Temel komutlar:

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# storm-control broadcast level <level:Yüzde.Küsüratı
şeklinde> {level-low Yüzde.Küsüratı şeklinde}
Switch(config-if)# storm-control multicast level <level:Yüzde.Küsüratı
şeklinde> {level-low Yüzde.Küsüratı şeklinde}
Switch(config-if)# storm-control unicast level <level:Yüzde.Küsüratı
şeklinde> {level-low Yüzde.Küsüratı şeklinde}
Switch(config-if)# storm-control broadcast level pps <level:pps şeklinde>
{level-low pps şeklinde}
Switch(config-if)# storm-control multicast level pps <level:pps şeklinde>
{level-low pps şeklinde}
Switch(config-if)# storm-control unicast level pps <level:pps şeklinde>
{level-low pps şeklinde}
```

Varsayılan olarak, eşik değeri aşılan trafik bloklanacak ve bir uyarı yollanmayacaktır. Eşik değeri aşılınca SNMP trap yollayacak şekilde de ayarlanabilir. Ayrıca "shutdown" parametresi ile interface "err-disable" durumuna da getirilebilir.

```
Switch(config-if)# storm-control action <shutdown | trap>
```

Cisco marka anahtar cihazları için örnek konfigürasyon aşağıda verilmiştir:

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# storm-control multicast level 80.0 50
Switch(config-if)# storm-control broadcast level pps 200 100
storm-control action shutdown
```

II.4.2 L3 Cihazlar ile Alınabilecek Önlemler

OSI'nin 3. katmanında çalışan cihazlarda alınabilecek önlemler aşağıdaki gibidir:

- Vlan Tabanlı Güvenlik Çözümleri
- Erişim Listeleri ile Alınabilecek Çözümler
- QoS ile Kişi Başına Bant Genişliği Sınırlaması
- Yeni Nesil Güvenlik Çözümleri

II.4.2.1 VLAN Tabanlı Güvenlik Çözümleri

Üçüncü katman ağ cihazlarında yapılacak ayarlamalar ile kötü amaçlı yazılımların ağ üzerindeki etkileri azaltılabilir. Aşağıda Cisco marka cihazlarda vlan bazında uygulanabilecek ayarlar ve açıklamaları bulunmaktadır. Konfigürasyon genel olarak kullanılması tavsiye edilen ayarları içermektedir, ancak kullanmadan önce uygulanacak ağın ihtiyaçları da göz önüne alınmalıdır.

II.4.2.2 Erişim Listeleri ile Alınabilecek Çözümler

Erişim listelerini kullanılıp yönlendiricilerde aşağıdaki önlemler alınarak kötü amaçlı yazılımların ağ üzerindeki yükü azaltılabileceği gibi kendilerini yaymaları da engellenebilir. Temel önlemler aşağıdaki gibi özetlenebilir:

• Yönlendiriciye gelen paketlerdeki kaynak IP adresleri kontrol edilmelidir. Dış ağdan iç ağa gelen paketlerde, gelen paketlerdeki kaynak ip'lerin kontrolüne giriş (ingress) filtreleme denmektedir. İç ağdan dış ağa giden paketlerde, gelen paketlerdeki kaynak ip'lerin kontrolüne çıkış (egress) filtreleme denmektedir. Bu RFC 3704'de tarif edildiği gibi kaynağı olmayan 0.0.0.0/8, 10.0.0.0/8, 192.168.0.0/16, 127.0.0.0/8 ve 169.254.0.0/16 adresleri bloklanmalıdır. Ayrıca kurumun IP adresi aralığını, kaynak IP adresi olarak kullanarak yapılabilecek saldırıları engellemek için dışarıdan kurumun IP adresi kaynaklı trafik yasaklanmalıdır. Güvenlik açıklarının kullandığı bilinen bazı portların kapatılması veya kısıtlanmasıdır. Bunlara örnek olarak şu portları belirtmek mümkündür: TCP 135, 137, 139, 445 UDP: 137, 138, 161, 162

• SMTP trafiğinin sadece iç mail sunuculara doğru açılmalı, diğer SMTP trafiğinin bloklanmalıdır.

• ICMP trafiğinde "packet-too-big", "time-exceeded", "echo-reply", "echo" ya izin vermek, geriye kalan ICMP türlerini bloklamaktır.

• Erişimi engellenen trafik loglanarak saldırgan bilgisayarın kimliği de tespit edilebilir. Ancak bunun çok sistem kaynağı tüketme riski de vardır.

Cisco marka yönlendiricilerde kullanılabilecek ve dışarıdan gelecek trafiği filtreleyecek örnek erişim listesi aşağıda gösterilmiştir. Örneklerde, VLAN'in kendi IP adresi aralığı ve wildcard maskesi, İçAğTanımı değişkeni ile gösterilecektir. Sunucuların bulunduğu ağ, SunucuAltAğı değişkeni ile gösterilecektir.

```
ip access-list Vlan_disardan
remark ******* icmp **********
permit icmp any any packet-too-big
permit icmp any any time-exceeded
permit icmp any any echo-reply
permit icmp any any echo
deny icmp any any
remark * bloklanacak portlar *
deny tcp any any eq 445
deny tcp any any range 135 139
deny udp any any range 135 139
deny udp any any range 161 162
...
remark * bloklanacak IPler *
deny ip 10.0.0.0 0.255.255.255 any
deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip 127.0.0.0 0.255.255.255 any
deny ip 169.254.0.0 0.0.255.255 any
deny ip İçAğTanımı any  # dışarıdan iç ağa ait IP adresli paket gelemez
permit ip any any
```

II.4.2.3 QoS ile Kişi Başına Bant Genişliği Sınırlaması

Birim kullanıcının dışarı veya içeri doğru kullanabileceği trafik miktarı QoS teknikleri ile kısıtlanabilir. Bu şekilde kötü bir yazılım bulaşmış bir bilgisayarın ağ kaynaklarını sömürmesi engellenir.

II.4.2.4 Yeni Nesil Güvenlik Çözümleri

Kötü amaçlı yazılımların IP adreslerini değiştirmelerini, DHCP ve ARP zehirleme saldırıları yapamalarını engellemek için L3 anahtarlama cihazlarında çeşitli çözümler bulunmaktadır. Cisco marka anahtar cihazlarında bu amaçlarla DHCP Snooping, Dynamic ARP Inspection, IP Source Guard çözümleri vardır.
Aşağıda bu çözümler için örnek konfigürasyon bulunmaktadır.

```
ip dhcp snooping
ip dhcp snooping vlan <vlan no>
ip arp inspection vlan <vlan no>
!
interface <int adı> <int.no>
description Istemci bilgisayar portu
ip verify source port-security
!
interface <int adı> <int.no>
description DHCP sunucusunun portu veya Uplink portu
ip dhcp snooping trust
ip arp inspection trust
```

II.4.3 Güvenlik Cihazları ile Alınabilecek Önlemler

Ağ üzerinde güvenlik amaçlı kurulacak sistemlerle alınabilecek önlemler aşağıdaki gibidir:

- Güvenlik Duvarları (Firewall)
- Antivirüs Geçitleri
- IDS/IPS Sistemleri

II.4.3.1 Güvenlik Duvarları (Firewall)

Güvenlik duvarları, durum korumalı (statefull) çalıştıkları için, düzgün ayarlanmaları durumunda zararlı yazılım aktivitesi içeren birçok bağlantıyı engelleyebilecektir. Servis sağlayan sunucuların belirli portları hariç, bütün portlar kurum dışından içeri doğru erişime kapatılmalıdır. 4.2.2'de

Erişim kural listeleri ile alınacak bütün çözümler güvenlik duvarlarında da alınmalıdır. Güvenlik duvarının en basit kural tablosunun mantığı aşağıdaki gibi olmaldır.

II.4.3.2 Antivirüs Geçitleri

Geçen trafiği zararlı içeriğe göre kontrol eden sistemlerdir. Özellikle büyük ağlarda sadece eposta trafiği için bu tür çözümler kullanılmaktadır. Kötü amaçlı yazılımların kendilerini bulaştırmak için en sık kullandığı tekniklerden biri eposta olduğundan, kullanılması ciddi bir fayda sağlamaktadır.

II.4.3.3 IDS/IPS Sistemleri

Günümüzde güvenlik duvarları bütünleşik olarak IDS/IPS mekanizmalarına sahip oldukları gibi, bu sistemler ayrı olarak da kurulabilmektedir. İyi yapılandırılmış bir IDS/IPS sistemi; ağı pek çok kötü yazılımdan izole edebileceği gibi, sorunun kaynağını tespitini de hızlandırmaktadır. Ancak bu sistemlerin iyi bir şekilde ayarlanmaması ve devamlı takip edilmemesi, yanlış tespitler sonucu sorununu da çıkarabilmektedir. Bu sistemler için, ticari çözümler kullanabileceği gibi Snort gibi açık kaynak koduna sahip çözümler de kullanılabilir. Snort için http://www.bleedingsnort.com/ adresinde bulunan bleeding-malware.rules" dosyasındaki güncel zararlı yazılım imzaları kullanılmalı ve sistem sorumluları gözlemledikleri yeni saldırılara ait imzaları da kendileri eklemelidir.

II.4.4 Diğer Sistemler ile Alınabilecek Önlemler

Alınabilecek önlemler aşağıdaki gibidir:

- Saldırgan Tuzağı Ağları (Honeynet)
- Trafik Akış Analizi Sunucuları

II.4.4.1 Saldırgan Tuzağı Ağları (Honeynet)

Zararlı yazılım ve saldırganların saldırılarını saptamak için tuzak sistemleri (honeypot) kullanılabilir. Tuzak ağı (honeynet), tuzak sistemlerinden oluşan bir ağdır. Açık kaynak kodlu yazılımlarla bu tür sistemler kurmak ve yenilerini geliştirmek mümkündür. Saldırgan tuzağı ağı (honeynet), kurum tarafından kullanılmayan bir alt ağı kullanacak şekilde ayarlanmalıdır. Güvenlik

duvarından, bu ağa gelen bütün trafiğe izin verilmelidir. Bu ağ, normalde dışarı hiç trafik oluşturmadığı için, bu ağa gelen bütün trafik incelenilmesi gereken ağ trafiğidir. Bu trafik, saldırı trafiği olmaktadır.

Çeşitli bilinen zayıflıkları simüle eden, virüs ve worm etkinliğini yakalama amaçlı kurulan sistemlere örnek olarak "Nepenthes" ve "Amun" yazılımları verilebilir. Bunun yanı sıra, "Honeyd" yazılımı ile bir makine üzerinde farklı işletim sistemlerini simüle eden sanal makineler, sanal yönlendiriciler ve sanal ağlar oluşturulabilir. Burada amaçlanan, bu makinelere saldırganların veya zararlı yazılımların erişimlerini takip etmektir. Ayrıca transparan olarak çalışan "Honeywall" yazılımı çalışan sistem, üzerinden geçen trafiği analiz etmekte, düzgün ayarlanması durumunda alt ağdaki tuzak sistem makinelerinin ele geçirilmesini ve buradan dışarı saldırı yapılmasını engelleyebilmektedir.

II.4.4.2 Trafik Akış Analizi Sunucuları

Bilmediğimiz saldırı türleri olabilir. Bilinmeyen ve saldırı saptama sistemleri tarafından saptanamayan saldırılar için trafik çözümleme süreçleri kullanılmalıdır. Kurum ağı trafiği ve özellikle saldırgan tuzağı ağına gelen trafik, ayrıntılı olarak incelenmelidir. Trafik akış ile bahsedilen, iki makine arasındaki iletişimin özetlenmesidir. İletişime ilişkin yön, adres, ağ kapısı ve trafik büyüklüğü gibi bilgilerin çözümlenme için elde edilmesidir. Ağ trafiği çözümlenerek ağın normal davranışını modellemek olasıdır. Haftanın herhangi bir günü için, çeşitli zaman aralıklarında trafiğin özelliğini belirtecek veriler elde edilebilir. Trafik bilgisinde, incelenmesi ve saptanması gerekenlere örnek olarak aşağıdakilerden söz edilebilir:

- O an çalışmayan makinelere/alt IP ağlarına giden trafik
- Yüksek ağ kapılarına giden/gelen servis isteği trafiği
- Yüksek bağlantı oranları
- Yüksek paket oranları
- İzlenmeyi engellemek için veriyi başka veri akışlarında saklayarak yapılan saldırılar (Covert channels)

Elde edilen ortalama değerlerden yaşanan sapmalar, kurum ağında farklı bir etkinliğin gerçekleştiği konusunda bize ipucu verecektir. Özellikle servis aksatma saldırıları, güvenlik açığı tarama girişimleri veya saldırı sonrasında sunucuların farklı amaçlar için kullanılması gibi saldırılar bu şekilde saptanabilir.

Bunun yanı sıra, saldırının boyutu, saldırganın başka hangi sunucu ve servislere erişim kurduğu/kurmaya çalıştığı da incelenebilecektir.

Ağ cihazlarının bize sağladığı monitor port özellikleri ile trafik bir bilgisayara yönlendirebilir ve trafik bu bilgisayardaki programlarla analiz edilebilir. Aşağıda Cisco marka anahtarlama cihazlarında monitor özelliğini devreye almak için kullanılacak komutlar bulunmaktadır.

```
monitor session 2 source interface <kaynak interface adı> <kaynak
interface no>
monitor session 2 destination interface <hedef interface adı> <hedef
interface no>
```

Geleneksel yöntemlere göre, ağ trafiği tcpdump programı ile pcap biçiminde kaydedilecek ve sistem yöneticisi bu dosyayı Ethereal/Wireshark programları ile çözümlemeye çalışacaktır. Küçük miktarda veri trafiği için bu yöntem geçerli olmakla beraber, günümüzün artan veri trafiğini çözümlemek için daha ayrıntılı süreçlere gereksinim duyulmaktadır. Bu süreçler için ticari ürünler kullanılabileceği gibi açık kaynak kodlu yazılımlar da kullanılabilir. Örneğin, kaydedilen trafik bilgisi Argus biçimine dönüştürülerek ayrıntılı olarak incelenebilir. Argus, ağ cihazı firmasından bağımsız bir yazılım olduğu için birçok ortamda kullanılabilecektir. Argus yazılımı ile birlikte çeşitli ağ trafiği akış çözümleme programları (ra, racluster, ragraph, ragrep, racount, rahosts …) gelmektedir.

Tcpdump ile interface üzerinden paket yakalamak ve kaydetmek için:

```
tcpdump -i eth0 -w argus_dosyasi
```

Pcap dosyasından trafik akış bilgisini oluşturarak argus biçimine dönüştürme komutu aşağıda verilmiştir:

```
argus -r tcpdump_dosyasi.pcap -w argus_dosyasi.arg
```

Oluşturulan dosyadan, en fazla trafik yaratan 20 makinayı (kaynak adres, kaynak paket sayısı, hedef paket sayısı, trafik) çıkarmak için aşağıdaki komut kulanılabilir:

```
racluster -n -r argus_dosyası.arg -M rmon -m saddr -w - - ip | rasort -m
bytes -w -| ra -N 20 -s saddr spkts dpkts bytes
```

Ağ cihazları, üzerlerinden geçen trafik akış (flow) bilgisini, incelenmesi ve normal dışı davranışlar belirlenmesi için harici bir sunucuya yollayabilir. Cisco yönlendiricilerden trafik akış bilgisi (netflow) alınabilmektedir. Aşağıdaki örnekte, Ethernet1 arayüzünden geçen ağ verisine ait trafik akış bilgisi, FlowSunucuIPAdresi ile belirtilen sunucunun 3737 numaralı ağ kapısına gönderilmektedir.

Cisco cihazlarda devreye almak icin kullanılacak komutlar aşağıdaki gibidir. Flow-export versiyon numarası (Örneğin 1, 5, 9 gibi) , sunucuda kullanılan analiz yazılımın desteğine göre girilmelidir. Bunun yanı sıra, akış bilgisinin gönderileceği sunucu adresi ve port numarası da girilmelidir. Hangi arayüzden dinleme yapılacağı da belirtilmelidir.

```
router(Config)# ip flow-export version  <netflow VersiyonNumarası>

router(Config)# ip flow-export destination <Flow sunucusunu IP adresi>
<Sunucun flow dinlemek icin kullandigi UDP port numarasi>

router(Config)# ip flow-export source <Dinlenecek Arayüz Adi>
```

Akış bilgisinin alınacağı interface'e girilir ve akış bilgisinin alınacağı tanımlanır. Eger kullanılan cihaz 7200,7500 gibi güçlü bir cihaz ise WAN veya LAN interface'inde aşağıdaki komutlar girilir:

```
router(Config-if)# ip flow ingress
router(Config-if)# ip flow egress
```

Eğer küçük bir yönlendirici ise (Örn: 2800), komut sadece in yönünde uygulanabilir. Eğer bu cihazda hem "download" hem de" upload" trafiğini dinlemek istiyorsan, hem WAN hemde LAN interface'ine girip aşağıdaki komut yazılmalıdır.

```
router(Config-if)# ip route-cache flow
```

Gönderilen akış bilgisi çeşitli yazılımlarla incelenebilir. Scrutinizer yazılımının ücretsiz sürümü, kurulum ve kullanım açısından etkin bir çözümdür.

Yukarıdaki önlemlerin yanında networkte bulunan verilerin şifrelenmesi de güvenlik açısandan oldukça önem taşımaktadır.

II.4.5 IPv6 Güvenlik ve Saldırı Türleri

Genel olarak güvenlik konusu 3 başlık altında incelenebilir.

- IPv6 protokolunde güvenlik [35-39]
- Geçiş yapılarınında güvenlik [40,41,47,11]
- IPv6 protokolünün uygulanmasıyla birlikte ortaya çıkacak olan güvenlik

Bu çalışmada salt IPv6 protokolünün güvenlik durumu incelenmiştir. Geçiş yapılarındaki güvenlik durumu bir sonraki çalışmada detaylı olarak incelenecektir.

IPv6 protokolunde uygulanabilecek saldırı türleri aşağıda sıralanmaktadır: [29]

- Keşif (reconnaissance)
- Başlıkta oynama ve parçalama işlemi
- 3. veya ve 4. katman seviyesinde aldatma (3. and 4. layer spoofing)
- ARP ve DHCP atakları (ARP and DHCP attacks)
- Yayınla saldırıya maruz bırakma (Broadcast amplification attacks-smurf)
- Yönlendirme atakları (Routing attacks)
- Paket gözleme (Sniffing)
- Uygulama katmanı saldırıları
- Sahte cihazlar
- Ortadaki adam saldırısı (Man in the middle)
- Paket seli (Flooding)

II.4.5.1 Keşif Atakları

• Adres çokluğundan dolayı port tarama işlemi zorlaşacaktır. IPv4'de varsayılan alt ağ büyüklüğü 2^8 iken IPv6'da varsayılan alt ağ büyüklüğü 2^{64} olmaktadır. Bir alt ağ içerisinde çok fazla sayıda adres kullanabileceğimizi düşünürsek bu ağüzerinde düğüm veya uçbirim arama işlemi bugünkü mimariye göre çok daha uzun bir süre alacaktır.

• TCP katmanında değişiklik olmadığından dolayı port tarama işleminde bir değişiklik olmayacaktır.

• Uygulama ve uygulama açıkları taraması ile ilgili bir değişiklik beklenmemektedir. Çünkü bunlar üst katman protokollerini ilgilendirmektedirler.

• IPv6 protokolünde multicast iletişim daha yaygın olacak ve bu iletişim türünü ağ içerisinde kullanan bazı önemli düğümlerin (yönlendirici ve NTP gibi) bulunması daha kolay olacaktır (yönlendirici keşif işlemi).

II.4.5.2 Başlıkta Oynama ve Parçalama İşlemi

• Sözce (string) imza denetimi konusunda IPv6'nın ek bir getirisi söz konusu olmamaktadır. Dolayısıyla bu tehditlere yönelik ağ yöneticilerinin kendi önlemlerini almamaları durumunda bu tehdit gelecekte de var olacaktır.

• RFC2460'da tanımlanan minimum MTU değeri 1280 oktet'dir. Bu noktada ağ yöneticilerinin minimum MTU değerinden düşük olan paketleri ağ cihazları üzerinden engellemesi tavsiye edilir. Eğer bu yapılmazsa söz konusu ağ'a bir çok sayıda küçük paketle saldırı yapılması ve bunun sonucunda ağın trafiğinin oldukça yavaşlaması veya tamamen durması söz konusu olabilir.

II.4.5.3 Aldatma Saldırıları

4'üncü katmanda yapılan aldatma saldırısı ile oturum çalma işleminde bir değişiklik söz konusu olmamaktadır. Bu saldırının temeli düşünüldüğünde saldırıda suistimal edilen protokol esas olarak TCP protokolü ve bunun bünyesinde bulunan üç yollu el sıkışma tekniğidir. Yeni nesil İnternet Protokolü ile birlikte TCP protokolünde bir değişim öngörülmediğinden bu sorunun gelecekte de yaşanması beklenmektedir. Fakat IPSec desteğinin aktif bir şekilde yeni nesil protokolde kullanılması,kesin güvenlik sağlamamakla birlikte, optimum bir güvenlik seviyesinin sağlanmasını gerçekleştirebilecektir.

II.4.5.4 ARP ve DHCP Atakları

IPv6'nın kendi doğasında DHCP veya ARP'yi güvenli kılacak bir özellik yoktur. Birçok durumda bağlantısız otomatik konfigürasyon özelliği ile DHCP'ye benzer bir hizmet sağlanabilmektedir. Günümüzdeki birçok işletim sistemi ile gelen DHCP sunucularında IPv6 desteği bulunmamaktadır. Yeni nesil DCHPv6 sunucularda DNS sunucusu, zaman sunucusu, IP telefon hizmeti sunucusu gibi ek konfigürasyon parametreleri hizmeti verilebilir. Dolayısıyla DHCP seviyesinde hala bir güvenlik ihtiyacı söz konusu olmaktadır. Maalesef bağlantısız oto konfigürasyon mesajları taklit edilebilir ve bu işlem cihaza erişilememesine neden olabilir. Bunu engellemeye yönelik yönlendirici-duyuru mesajı ile güvenilir bir port konsepti birlikte kullanılabilir.

- ARP açısından bakacak olursak, IPv6 da ARP'nin yerine yeni bir çözüm olan komşu keşfetme işlemi getirilmiştir. Bu paketler IP paketleri olduğundan güvenlik açısından ARP'tan daha güvenli bir yapıya sahip olabilirler. Bu protokolde kullanılan komşu-duyuru ve keşfetme mesajları taklit edilebilir ve komşu keşfetme protokolünce kullanılan geçici bellekte olan bilginin üstüne yazılabilir. Buna örnek olarak taklit edilmiş bir yönlendirici keşfetme paketi içerisine sahte yönlendirici bilgisi yerleştirilebilir ve böylece uçbirimlerin trafiğinin bu sahte yönlendirici üzerinden akması sağlanabilir. Bunun sonucunda da trafik bu yönlendiricide kayıt edilebilir.

- DHCPv6 ile ilgili güvenlik çalışmaları sürmektedir.

II.4.5.5 Yayınla Saldırıya Maruz Bırakma (Smurf)

IPv6'da yayın türü trafik kaldırılmıştır ve saldırı riskini azaltmak için yeni bazı teknikler geliştirilmiştir. Örneğin hedef olarak multicast, link-layer multicast veya link-layer broadcast adresleri kullanan paketlere cevap verilmesi engellenmiştir.

II.4.5.6 Yönlendirme Atakları

Birçok protokolün güvenlik mekanizması IPv4'den IPv6'ya geçişle birlikte henüz değişmemiştir. Domainler arası yönlendirme bilgilerinin taşınması için BGP protokolü kullanılmaya devam etmektedir. Bununla birlikte BGP protokolü TCP katmanında kimlik doğrulaması için MD5 kullanmaya devam etmektedir. OSPFv3 protokolünde kimlik doğrulama başlığı kaldırılmıştır. RIPng (Routing Information

Protocol Next-Generation) protokolünde de kimlik doğrulama özelliği yoktur. Bu iki protokol bilgileri aktarırken güvenlik kısmında IPSec AH ve ESP başlıklarına güvenmektedirler. Dolayısıyla IPSec protokolünün güvenirliği bu noktada da önem taşımaktadır.

II.4.5.7 Paket Gözleme

Trafiğin dinlenilmesi saldırısına karşılık IPv6 protokolünün kendi içerisinde IPSec desteklemesi bir çözüm olarak gözükmektedir. Fakat IPSec ve güvenlik birliğinin kurulmasında kullanılan IKE ve ISAKMP protokolleri ayrı protokollerdir ve bunlar için geçerli güvenlik sorunları devam ettikçe IPv6'da da paket gözleme türü saldırıların gerçekleştirilebilmesi mümkün olacaktır.

II.4.5.8 Uygulama Katmanı Saldırıları

Bu saldırılar İnternet Protokolü'nün uygulandığı ağ katmanına yönelik olmadığı için bu saldırıların aynen geçerli olması beklenmektedir. IPv6'nın kendi içerisinde IPSec desteklemesi aradaki iletişimin şifrelenmesine yönelik destek verecektir. Ancak bu, saldırıların kesilmesini sağlamaz. Bu tarz saldırılar şifrelenmiş kanallardan geçerek hedeflerine ulaşıp aynı zararı verebilirler. Fakat bunun getirisi olaraksaldırının kaynağının keşfine yönelik geri izleme işlemi daha kolaylaşacaktır. Yeni nesil protokolün de IPSec desteklemesi ile birlikte uç cihazlarda bu protokol uygulanırsa güvenlik gereksinimleri biraz daha azalacaktır çünkü firewall veya IDS'lerşifreli trafiği görmektedirler fakat içeriğini okuyamadıkları için veri hakkında karar verememektedirler.

II.4.5.9 Sahte Cihazlar

Bu saldırı IPv4 sistemlerde oldukça kullanılmaktadır ve maalesef IPv6'da yeterince değişmemiştir. Eğer IPSec IPv6'da daha çok yönlü bir şekilde kullanılırsa cihaz doğrulanması ile ilgili saldırıların önemli ölçüde azalması beklenmektedir.

II.4.5.10 Ortadaki Adam Saldırısı

IPv6'nın bu saldırıya karşı etkinliği tamamen IPSec protokol kümesinin, özellikle de IKE protokolünün zaafları oranında olabilmektedir. Bilindiği üzere IPSec uygulanmadığı durumda IPv6'nın bu tarz bir saldırıda IPv4'den farkı

olmamaktadır. Bu saldırıya karşı etkinliği IPSec protokol kümesi sağlamaktadır fakat bu protokolün de çeşitli zaafları mevuttur.

II.4.5.11 Paket Seli Saldırısı

Temel ilke olarak bu atak IPv6'da da değişmemektedir. Yerel veya dağıtık DoS saldırıları yine kaynakları tüketme yolunda en basit saldırılardan biri olma özelliğini korumaktadırlar. Bu konuda saldırı tespiti ve geri izleme teknikleri IPv4'de olduğu gibi IPv6'da da uygulanabilmektedir.

II.5 SANALLAŞTIRMA TEKNOLOJİSİ

Sanallaştırma, bilişim kaynaklarının (işlemci, depolama, ağ, bellek, platform, sunucu, masaüstü, uygulama vb.) soyutlanarak, yani gerçekte var olan kaynağın değil de, gerçek kaynağa dayandırılarak tanımlanmış olan soyut halinin, ilgili bilişim kaynağının kullanıcılarına sunulması olarak tanımlanabilir. Böylece, gerçek kaynak ile kullanıcısı arasındaki bağ gevşetilebilmekte ve var olan gerçek kaynak, göreceli olarak daha az kapasiteli çok sayıda sanal kaynak olarak kullandırılabilmektedir. Daha basit olarak ifade edecek olursak, fiziksel bir makine içinde birden fazla sanal makinenin çalışması olarak ifade edebiliriz.

Sanallaştırmanın ilk temelleri Oxford Üniversitesinde atılmış ve ilk olarak 1966 yılında IBM tarafından tam sanallaştırma (full virtualization) gerçekleştirilmiştir. 1990'lı yılların sonunda ekonomik gelişmeler, maliyetlerin gözden geçirilmesini ve kaynakların daha verimli kullanılması ihtiyacını doğurdu ve sanallaştırma tekrar gündeme geldi. Bu kapsamda 1998'de sanallaştırma yazılımı odaklı VMware şirketi kuruldu ve ilk ürünü olan VMware Workstation 1999'da pazara sunuldu. Sunucu pazarına ise 2001 yılında VMware GSX Server ve VMware ESX Server ürünleri ile girdi. 2003'de VMware Virtual Center ve VMotion and Virtual SMP teknolojileri geldi. Windows ve Linux ortamında çalışan VMware'e, 2006'da Mac OS desteği de geldi. Ayrıca, Intel ve AMD 2005-2006 yıllarında sanallaştırmayı destekleyecek ek donanım sunmaya başladılar. Yaygın kullanılan Intel IA-32 mimarisinin sanallaştırma konusundaki eksiklerinin tamamlanması, bu mimarideki uygulamaların sanallaştırılmasını da hızlandırdı. Aynı yıllarda, daha sonra tamamen açık kaynak olan Xen yazılımı, bir araştırma projesi olarak Cambridge Universitesi'nde

geliştirildi. Xen'in ilk ürünü 2003'de pazara sunuldu. 2007'de Citrix Systems, Xen'i satın aldı ve Xensource ürünleri olarak isimlendirdi. 2007'de bu sektörün öncülerinden Citrix, IBM, Intel, Hewlett-Packard, Novell, Red Hat, Sun Microsystems ve Oracle'ın katılımıyla Xen Projesi Danışma Kurulunu oluşturdu.

Sanallaştırma teknolojilerini kullanılarak birçok yarar sağlanabilmektedir. Bunlardan bazıları aşağıda sıralanmıştır:

- Fiziksel sunucuların sayısını azaltma.
- Veri merkezi için gerekli olan altyapı ihtiyacını azaltma (enerji, soğutma, alan, yedekleme, ağ geçiş bağlantı noktaları, KVM bağlantı noktaları).
- Sunucular tek bir merkezden yönetilebildiği için yönetimsel ek yükü azaltma.
- Yeni sunucuları kolayca mevcut ortama ekleme kabiliyeti. Yeni bir fiziksel sunucuyu eklemek günler hatta haftalar sürerken, sanallaştırma teknolojileri ile yeni bir sanal sunucu oluşturmak sadece birkaç dakika alabilmektedir.
- Sanal sunucuların donanım bağımsızlığı. Diğer bir ifade ile, sanal sunucular donanım bağımsız herhangi bir sunucu üzerinde çalışabilmesi.

Bilişim hizmeti veren kurumlar ve firmalar, sanallaştırma teknolojilerinin kullanımı ile birçok farklı alanlarda masraflarda azalma anlamında kazançlar sağlayabilmektedir. Örneğin, BT sektöründe faaliyet gösteren büyük firmalardan birinin, kendi BT altyapısına ilişkin olarak yürüttüğü sanallaştırma çalışmalarının sonucu olarak, 3 bini aşkın dağıtık sunucu sayısını 30 kadar yüksek kapasiteli sunucuya indirmeyi, veri merkezi için gerekli alan miktarını %85 azaltmayı ve 5 yıl içinde 4 Milyar Doların üzerinde tasarruf sağlamayı başarmış olduğu bilinmektedir.[34]

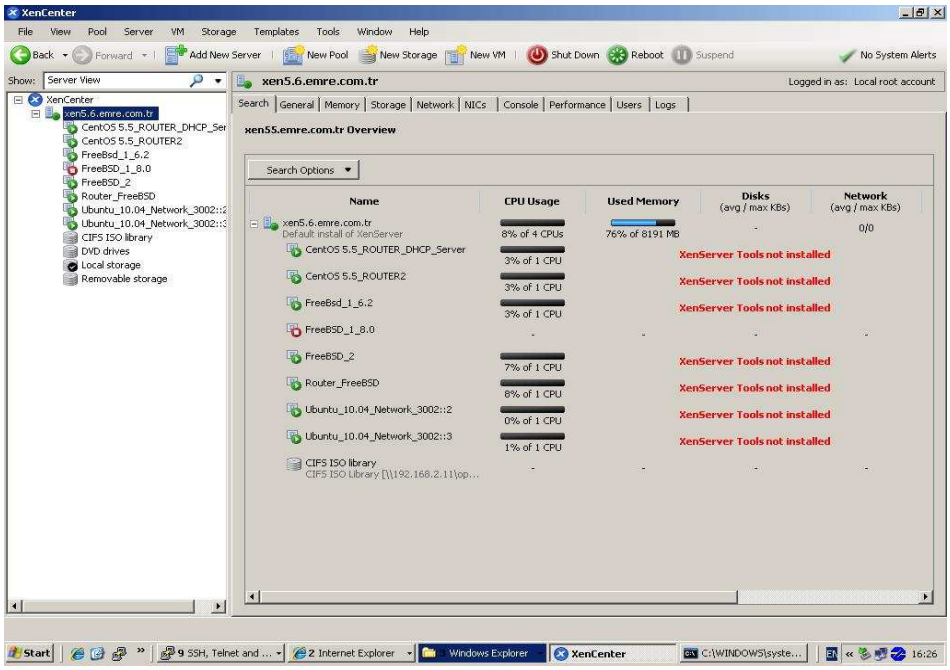
BÖLÜM III

III. IPv6 GÜVENLİK DENEYLERİ

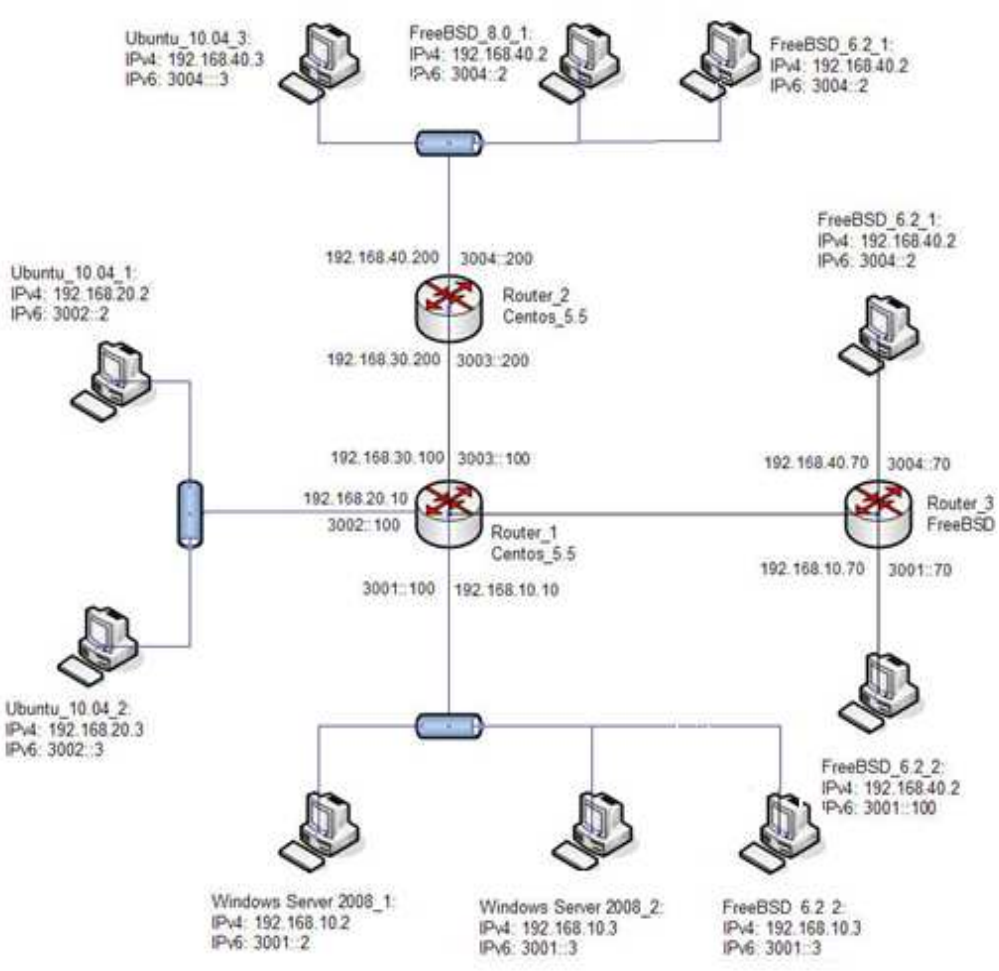
İlk olarak sanallaştırılmış ortamda bulunan bulunan bilgisayarlar üzerinde IPv4 ve IPv6 paketleri için IPSec güvenlik protokolü çeşitlemeleri uygulanmış ve her biri için ayrı ayrı bant genişlikleri ölçülmüş ve incelenmiştir. Ardından sanal ortamda kurulmuş olan network topoloji dahilinde IPv6 için çeşitli atak türleri denenmiş ve değerlendirilmiştir. Son olarakta, testlerin yapıldığı tarihte son versiyon olan farklı işletim sistemleri (FreeBSD , Ubuntu ve Windows) üzerinde, IPv6 ile birlikte gelen ve güvenlik açısından büyük bir zaafiyet olarak öne çıkarılan Routing Header (Yönlendirme Başlığı) ek başlığı ile ilgili güvenlik testleri yapılmıştır.

III.1 DENEY ORTAMI

Deneyler, üzerinde RAID-1 olarak konfigure edilmiş 200 GB Serial Attached SCSI (SAS) Harddisk ve 8 GbRam olan 4 çekirdek 1.86 GHz Intel Xeon işlemcili IBM System x3650 Server üzerinde oluşturulmuş sanal makinelerde gerçekleştirilmiştir. Sanallaştırma programı olarak Citrix XenServer seçilmiştir. Xen donanımsal tabanlı (Hypervision - Hardware-Level Virtualization) bir sanallaştırma sistemidir (Virtual Dedicated Server) ve iki kısımdan oluşmaktadır. Birincisi IBM 3650 server üzerinde sanal makinelerin oluşturulmasını sağlayan işletim sistemi Citrix XenServer Host , ikincisi ise Xen Serverın yönetim konsolu olan ve Windows ortamında çalıştırılması gereken Citrix Xen Center. Citrix Xen Server Express, Standart, Enterprise ve Platinum olmak üzere 4 sürümden oluşur. Platinum Hariç diğer sürümler tamamen ücretsizdir. Bu çalışmamızda, tezin yazıldığı tarihte en versiyon olan Citrix Xen Server 5.6 Enterprise sürümü kullanılmıştır. Ayrıca Xen Server üzerinde Linux tabanlı sanal makineler oluşturabilmek için Linux Pack dosyasını da yüklemeniz gerekmektedir. Yukarıda bahsedilen üç program **http://www.citrix.com/lang/English/lp/lp_1688615.asp** adresinden indirilebilmektedir.



Şekil III.1 : Xen Center Ekran Görüntüsü



Şekil III.2 : Deney Topolojisi

Windows Server 2008'lerde, IPSec güvenlik protokolü testleri için bant genişliği ölçümleri açık kaynak kodlu Iperf programı kullanılarak yapılmıştır. Program **www.noc.ucf.edu/Tools/Iperf/** adresinden indirilebilmektedir.

IPv6'da çeşitli saldırı türlerini deneyebilmek için, açık kaynak kodlu THC atak toolu kullanılmıştır . Program **http://freeworld.thc.org/thc-ipv6/** adresinden indirilebilmektedir.

Yönlendirme Ek Başlığı (Routing Header) saldırılarında gerekli paketleri oluşturabilmek içinse Scapy programı kullanılmıştır. Scapy, Python dili ile yazılmış komut satırından çalışan açık kaynak kodlu bir yazılımdır. Kullanım amacı TCP/IP ağlar için özelleştirilmiş paketler üretmektir. Program **http://www.secdev.org/projects/scapy/** adresinden indirilebilir.

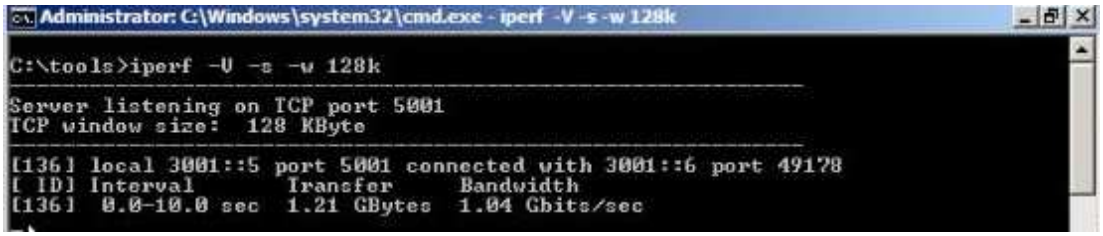
Topoloji oluşturulurken kullanıcılara otomatik IP dağıtılması için DHCPv6 kurulmuş ve adres havuzları oluşturulmuştur. Routing işlemlerinin stabil bir şekilde yapılabilmesi için RadVD deamen kullanılmıştır. Ayrıca sanal ortamda oluşturulmuş olan topoloji dahilindeki Centos, Ubuntu, FreeBSD ve Windows tabanlı işletim sistemlerinin, IPv6 network ve routing konfigurasyonları için çeşitli kaynaklardan faydalanılabilir [11,42]

III.2 DENEYLER

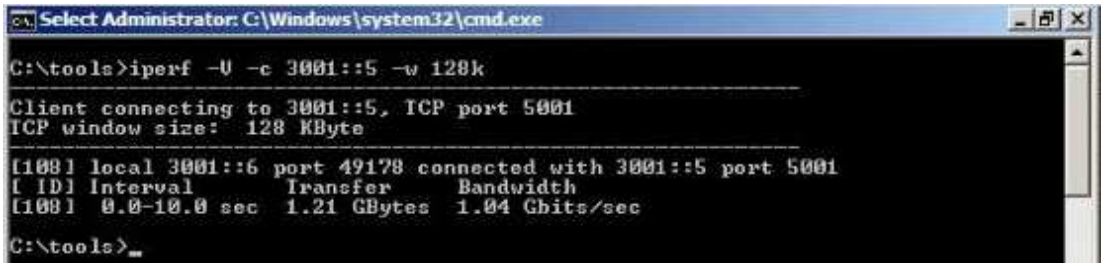
III.2.1 IPSec Güvenlik Protokolü ve Bant Genişliğ Deneyi

Bu deneyde Xen Server üzerinde sanallaştırılmış, aynı network üzerinde bulunan 2 adet Windows Server 2008 bilgisayar kullanılmıştır. Her iki bilgisayar içinde Xen Server üzerinden 1GB Ram ve 1 adet CPU rezerve edilmiştir.

Bu test esnasında ilk olarak yalın IPv4 ve IPv6 paketlerinin, XenServerda bulunan donanımsal ve sanal arayüzler üzerindeki bant genişliği ölçümleri yapılmış ve her geçen daha da yaygınlaşan sanal arayüzlerin, donanımsal arayüzlere göre performans analizlerinin yapılması amaçlanmıştır. Ardından XenServerdaki sanal arayüzler üzerinde, IPv4 ve IPv6 paketleri için IPSec güvenlik protokolü kombinasyonları uygulanmış ve bant genişliği performansları incelenmiştir. Bant genişliği ölçümleri için açık kaynak kodlu iperf programı kullanılmıştır. Sonuçların daha önce donanımsal arayüzler üzerinde yapılan testlerle [11] mukayese edilebilmesi açısından her deney 40 defa tekrarlanmış ve paket büyüklüğü 128k olarak sabitlenmiştir.



Şekil III.3 : Iperf ile Bant Genişliği Ölçümü - Server



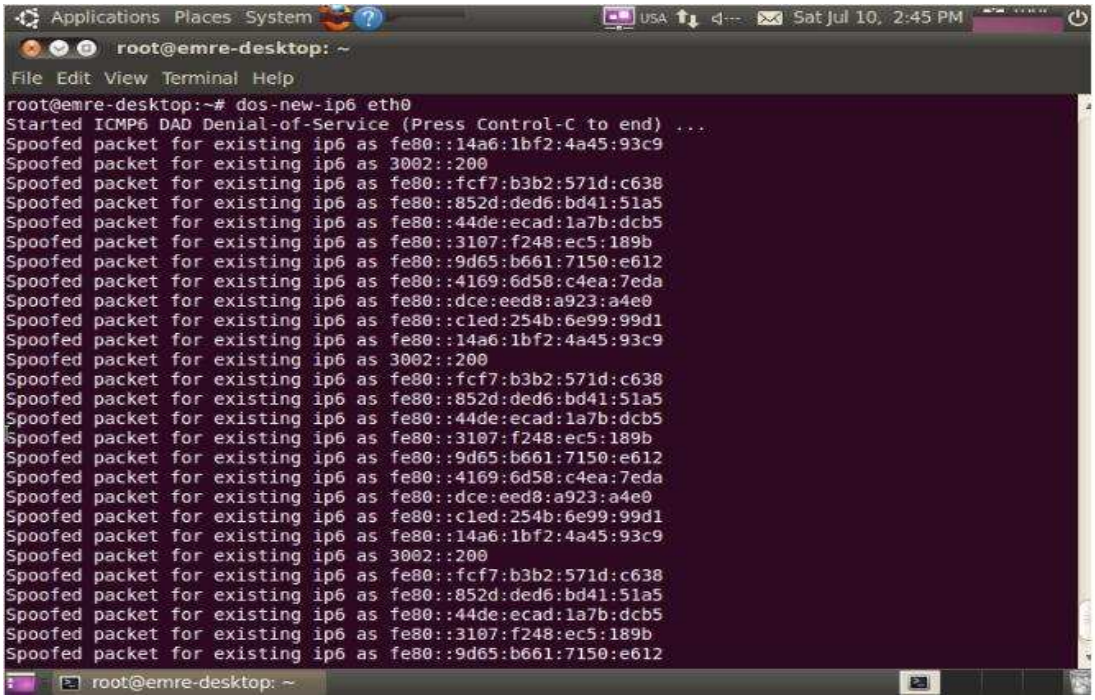
Şekil III.4 : Iperf ile Bant Genişliği Ölçümü - Client

III.2.2 Bazı Saldırı Türlerinin IPv6 üzerinde denenmesi

Saldırı deneylerinde THC programı dahilindeki toollar kullanılmıştır.

III.2.2.1 Dos-new-ip6

IPv6 protokolünde bir host, ip bilgisini kendisine tahsis etmeden önce, adres çakışmasını engellemek için, bu adresin yerel ağ dahilinde başka kullanıcılar tarafından kullanılıp kullanılmadığını kontrol eder. Bunu da yerel ağdaki bütün hostlara NS mesajları göndererek yapar. Komşu hostlar bu mesajı alırlar ve şayet gelen adres kullanılıyorsa bu adresin kullanılamayacağını ifade eden bir NA mesajı dönerler. Saldırgan bu yapıdan faydalanarak, networke yeni bir hostun bağlanıp ip çakışmasını kontrol etmek için gönderdiği paketlere, bu adres kullanılıyor mesajı döner ve hostun ip almasını engeller.



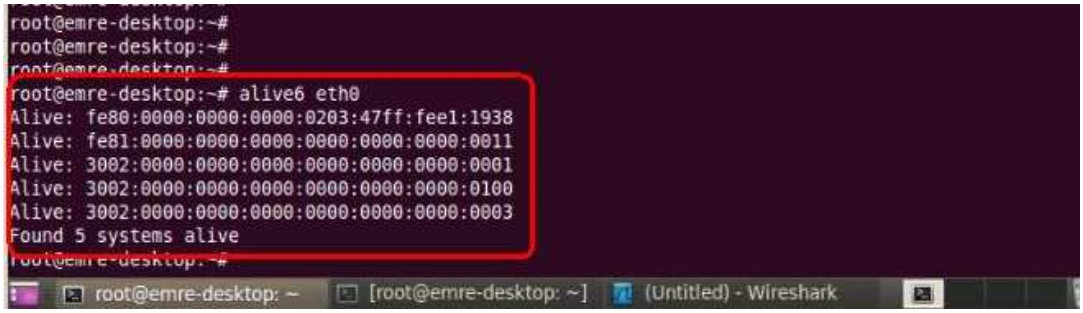
Şekil III.5: Sadırıyı yapan 3002::2 bilgisayarının Dos-new-ip6 ekran görüntüsü

Şekil III.6 Saldırıya maruz kalan 3002::1 bilgisayarının Dos-new-ip6 ekran görüntüsü

Yukarıdaki şekilde, networke bağlanmak isteyen bilgisayar, saldırıdan dolayı IP çakışması olduğunu sanıyor ve IP alamıyor.

III.2.2.2 Alive6

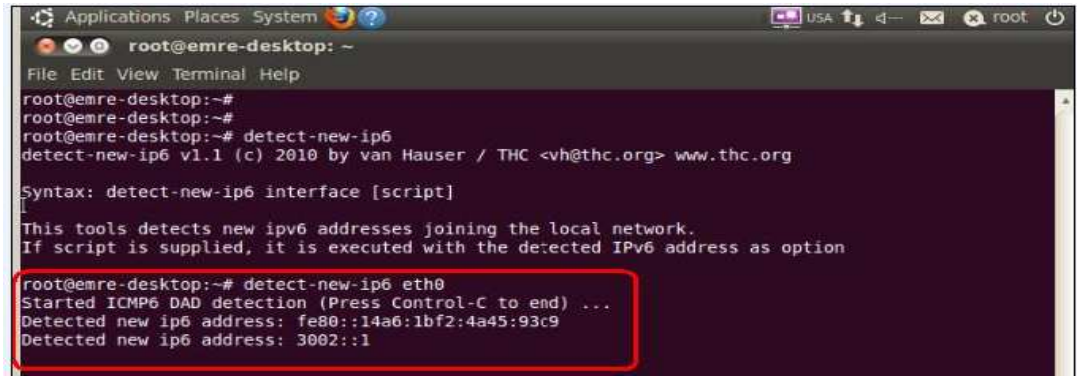
Ağ dahilinde akfif olan cihazları bulmak için kullanılır.



Şekil III.7: Ağdaki bilgisayarların ip bilgileri

III.2.2.3 Detect-new-ip6

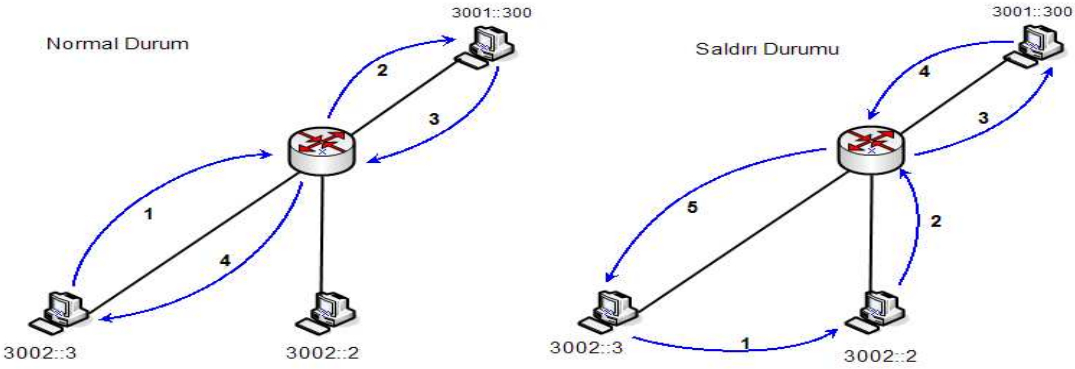
Ağa yeni bir hostun bağlandığını ve bağlanan hostun IP bilgilerini tespit eder.



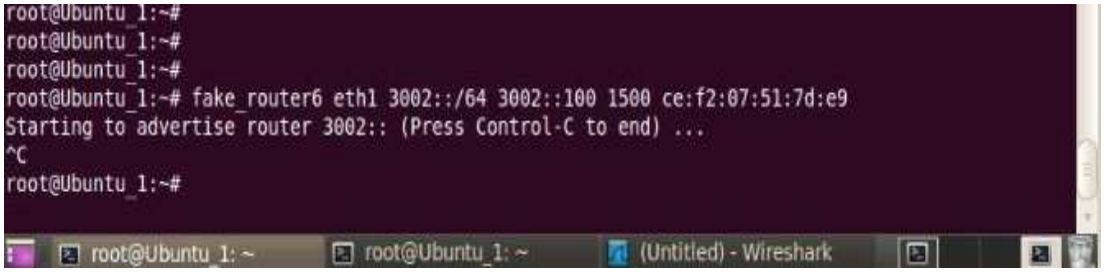
Şekil III.8: Ağa yeni bağlanan host ve ip bilgileri

III.2.2.4 Fake_router6

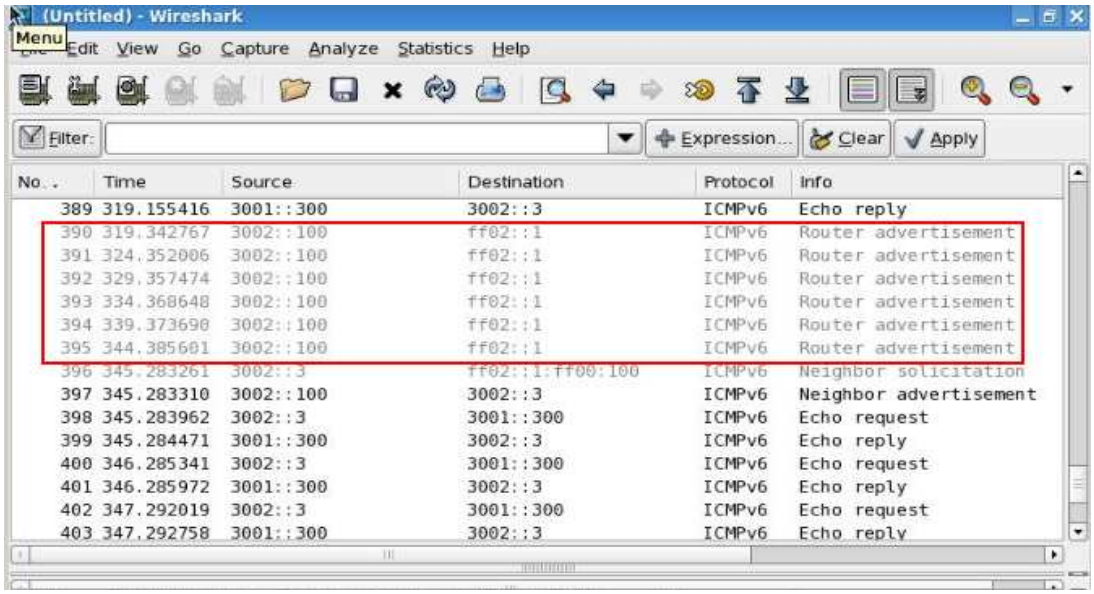
Bu saldırı şeklinde saldırgan kendini yüsksek öncelikli router olarak anons eder. Bu sayede paketler önce saldırganın bilgisayarına oradan gerçek routera oradan da hedef bilgisayara ulaşmaktadır. Bu sayede saldırgan bütün paketleri kendi üzerinden geçirebilmektedir. Saldırgan dönen paketleri de üzerinden geçirmek isterse Router için poisining mesajları oluşturabilir.



Şekil III.9: Sahte Router Saldırısı

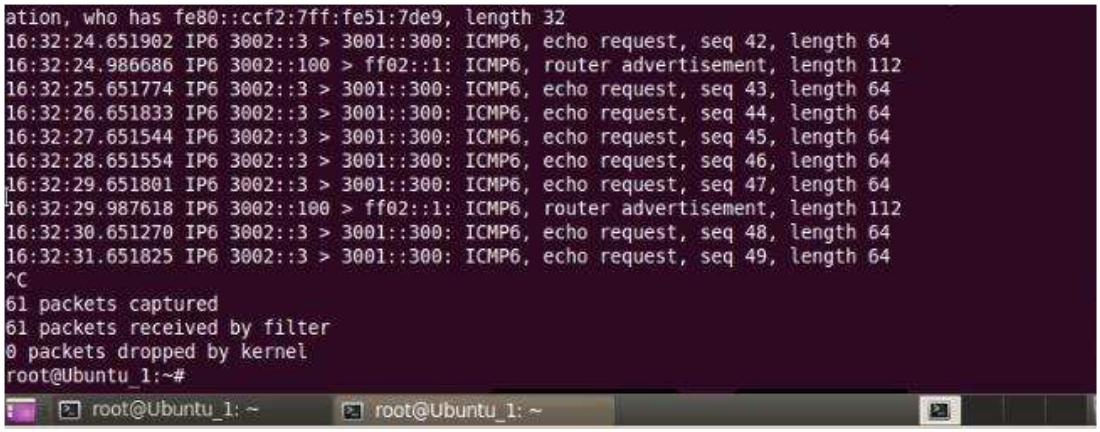


Şekil III.10: Sadırıyı yapan 3002::2 bilgisayarının Fake_router6 ekran görüntüsü



Şekil III.11: Saldırıya maruz kalan 3002::1 bilgisayarının Fake_router6 WireShark çıktısı

Yukarıdaki şekildede görüldüğü gibi saldırı başlatıldığı anda networke sahte Router Advertisement paketleri sayısı artmıştır.

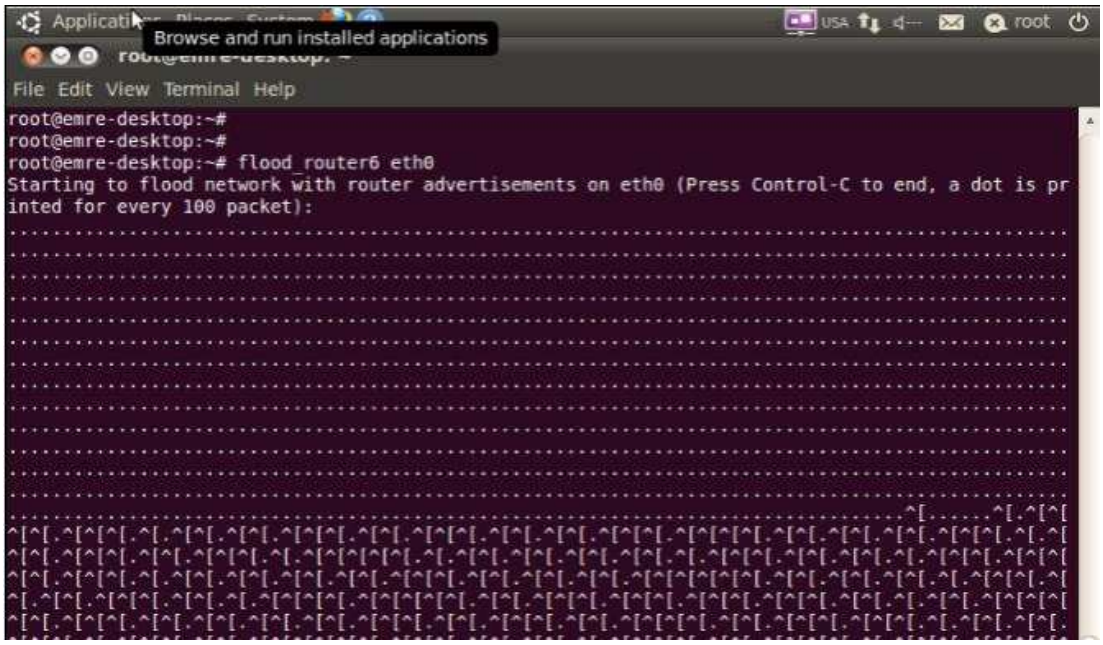


Şekil III.12: Sadırıyı yapan 3002::2 bilgisayarının Fake_router6 Tcpdump çıktısı

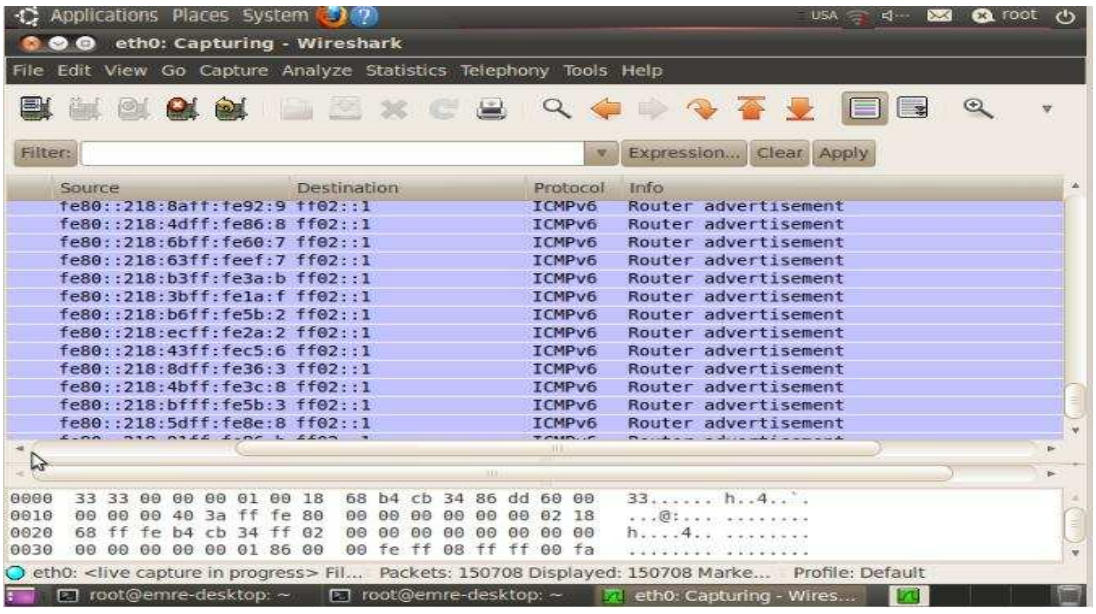
Yukarıdaki şekilde görüldüğü gibi Echo Request paketleri saldırganın üzerinden geçmektedir. Fakat cevap olarak gelen Echo Reply paketleri direkt olarak 3002::3 bilgisayarına döndüğünden saldırgan dönen paketlere ulaşamamaktadır.

III.2.2.5 Flood_Router6

Saldırgan bilgisayar, hedef aldığı bilgisayara rastgele oluşturduğu çok sayıda Router Advertisement paketleri göndererek hedef bilgisayarı etkisiz bırakmayı amaçlamaktadır.



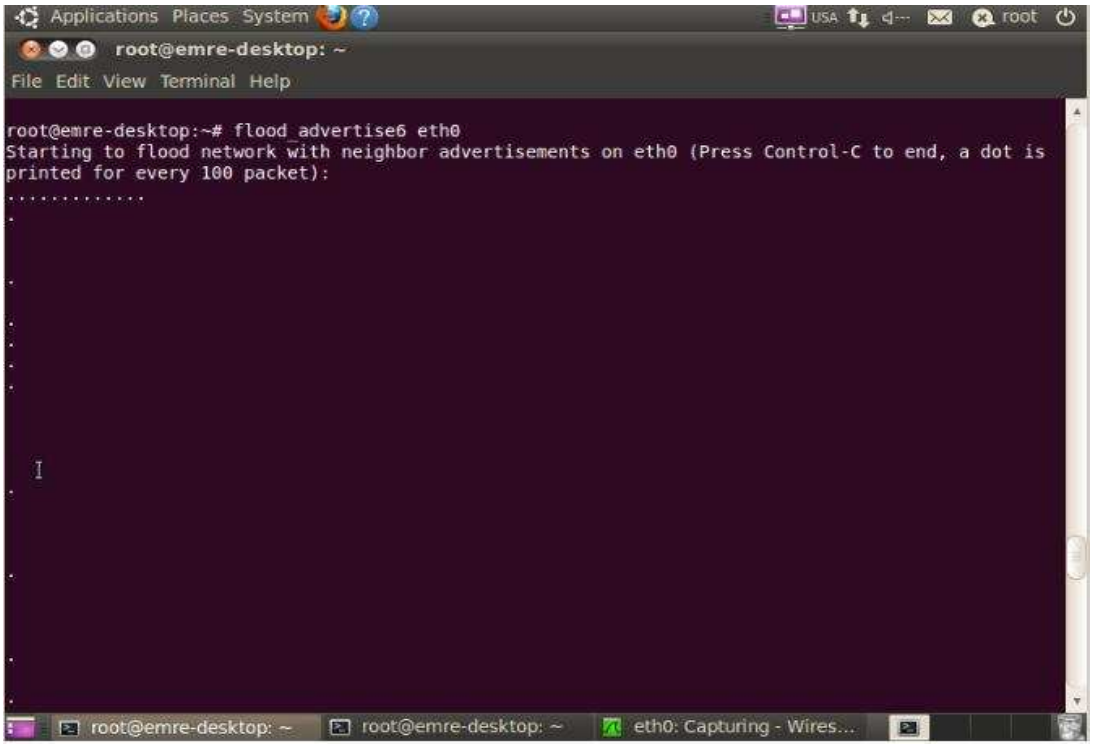
Şekil III.13: Sadırıyı yapan 3002::2 bilgisayarının ekran görüntüsü



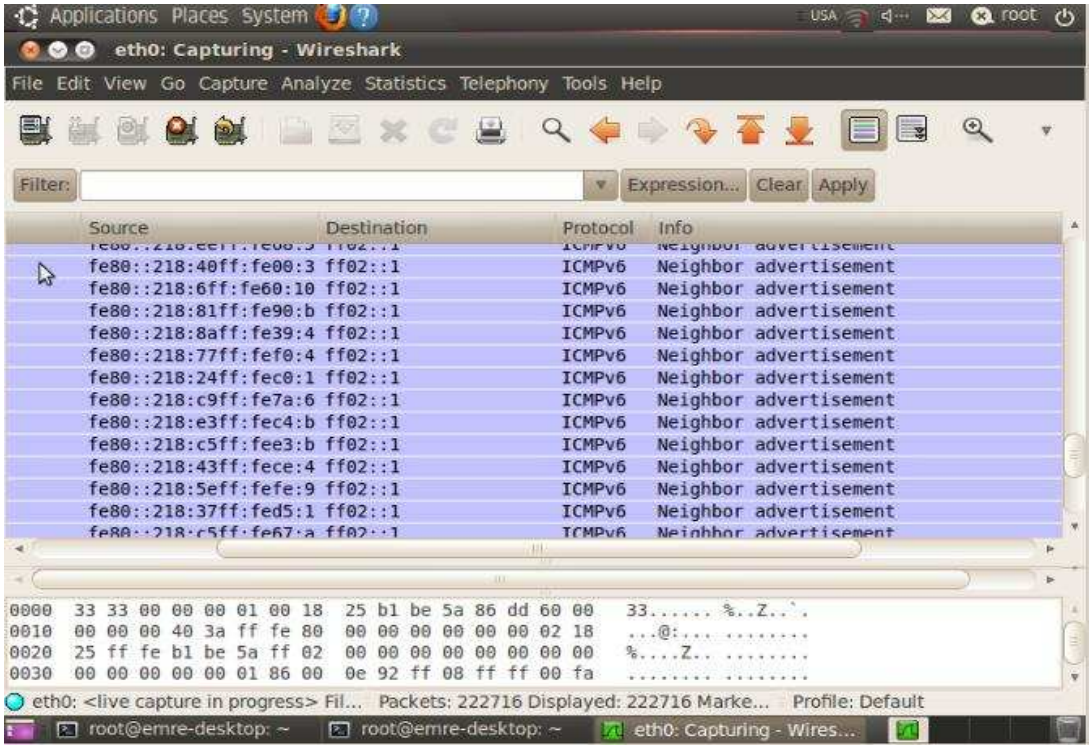
Şekil III.14: Saldırıya maruz kalan 3002::1 bilgisayarının WireShark çıktısı

III.2.2.6 Flood_advertise6

Saldırgan bilgisayar, hedef aldığı bilgisayara rastgele oluşturduğu çok sayıda Neighbor Advertisement paketleri göndererek hedef bilgisayarı etkisiz bırakmayı amaçlamaktadır.



Şekil III.15: Sadırıyı yapan 3002::2 bilgisayarının Flood_advertise6 ekran görüntüsü

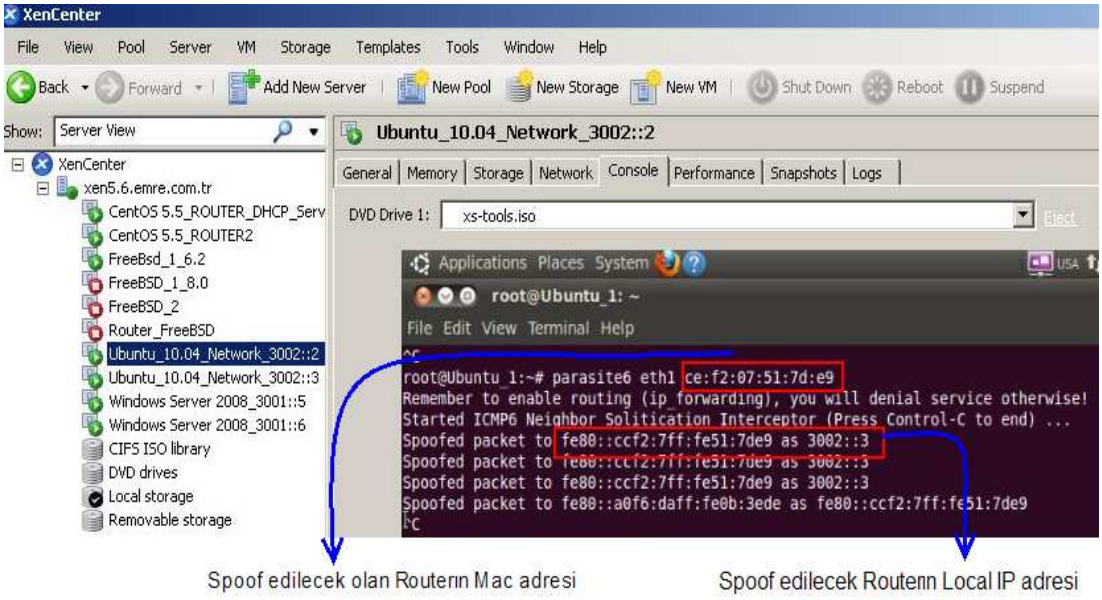


Şekil III.16: Saldırıya maruz kalan 3002::1 bilgisayarının Flood_advertise6 çıktısı

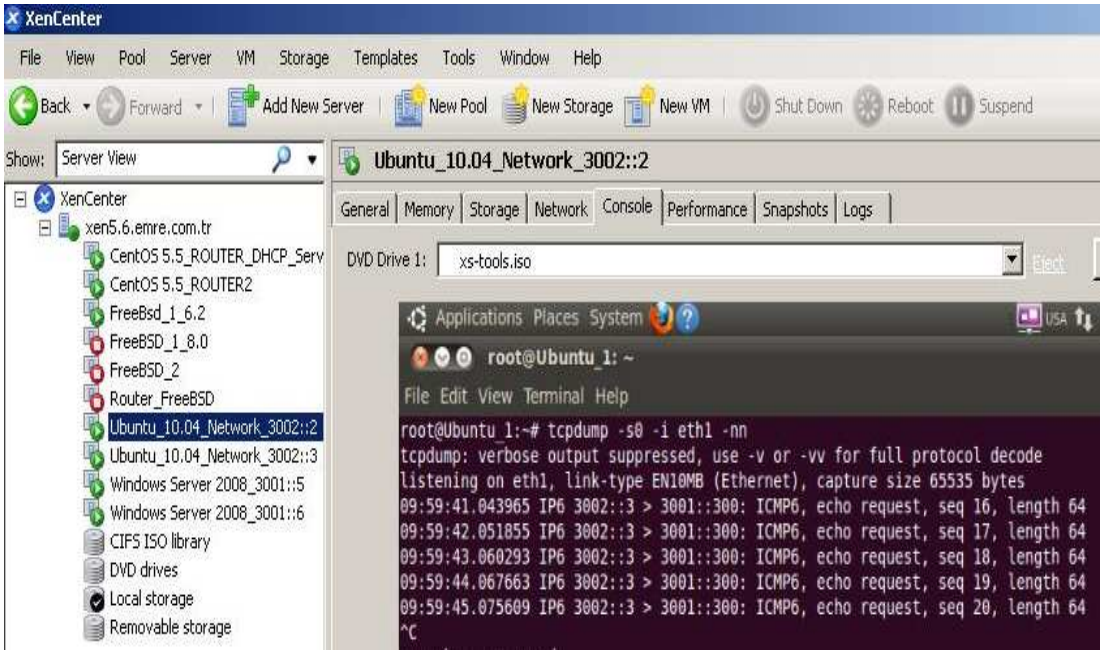
III.2.2.7 Parasite6

IPv4'teki ARP spoofer saldırının IPv6 versiyonudur. Burada saldırgan, sahte Neighbor Solicitation ve Advertisement paketleri üreterek, lokal networkte router

üzerinden geçmesi gereken tüm trafiği üzerine alır. Ardından da üzerine aldığı paketleri, saldırıya maruz kalan bilgisayarlardan geliyormuş gibi sahte IP paketleri üreterek routera gönderir. Bu sayede lokal networkten routera giden bütün trafiği dinlemiş olur.



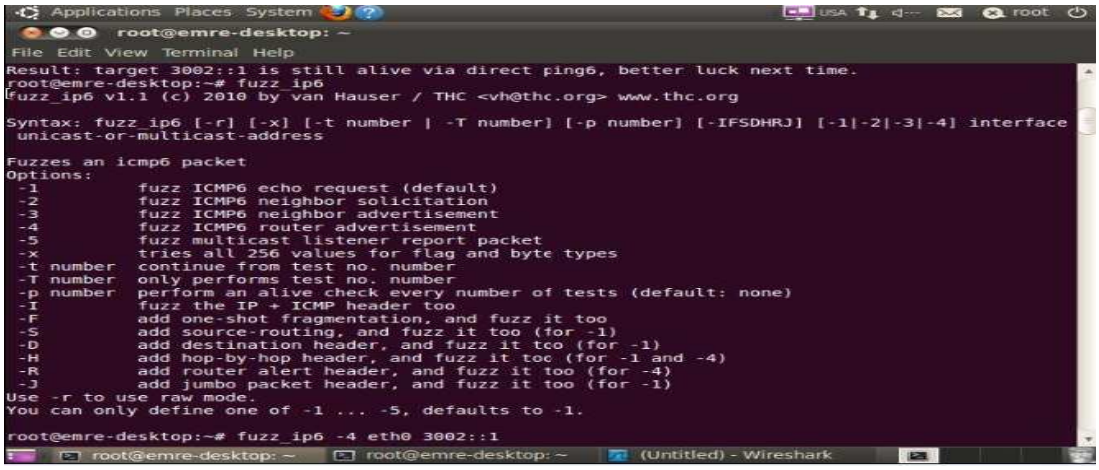
Şekil III.17: Sadırıyı yapan 3002::2 bilgisayarının Parasite6 ekran görüntüsü



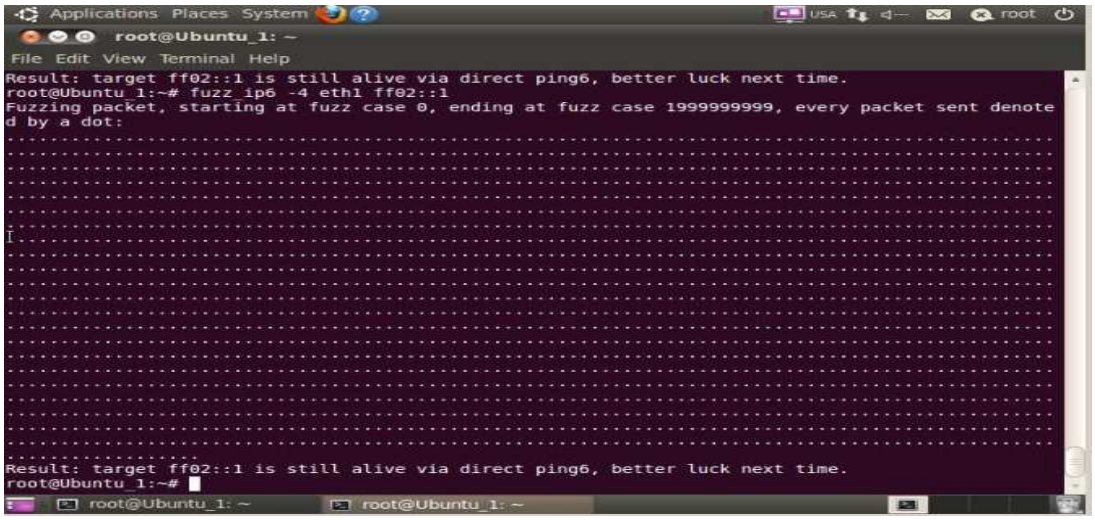
Şekil III.18:Sadırıyı yapan 3002::2 bilgisayarının Parasite6 Tcpdump ekran çıktısı

III.2.2.8 Fuzz_ip6

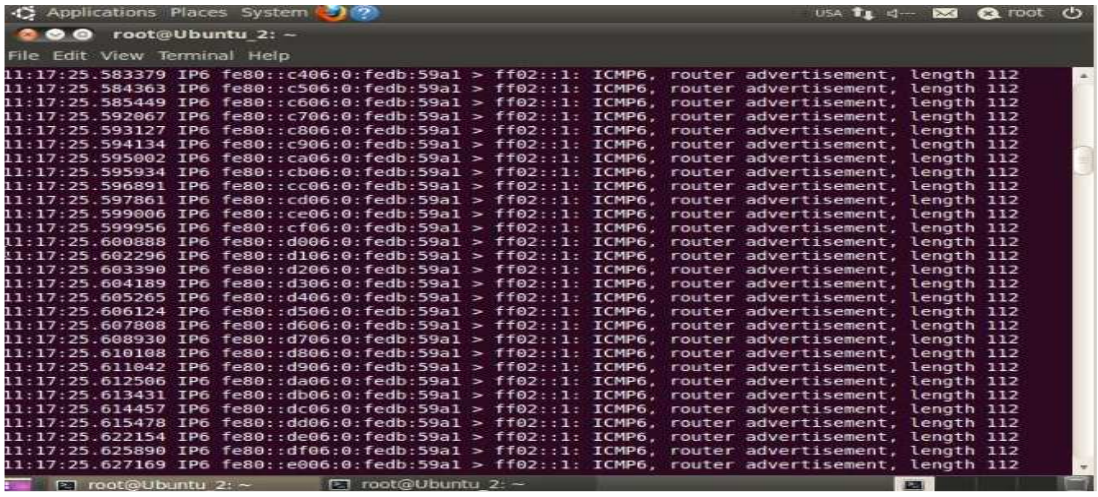
Burada saldırgan networkteki tüm hostlara rastgele adreslerden gelen ve istenilen özelliklere sahip çok sayıda paket göndermektedir.



Şekil III.19: Fuzz_ip6 paket seçenekleri



Şekil III.20 Fuzz_ip6 ile Router Advertisement paketleri oluşturma

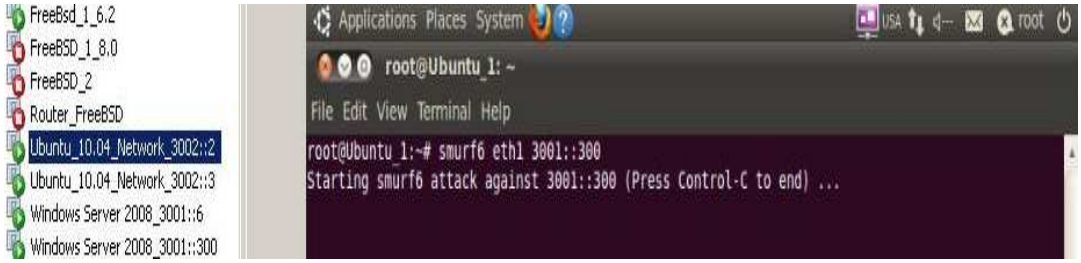


Şekil III.21: Saldırıya maruz kalan 3002::1 bilgisayarının Fuzz_ip6 Tcpdump çıktısı

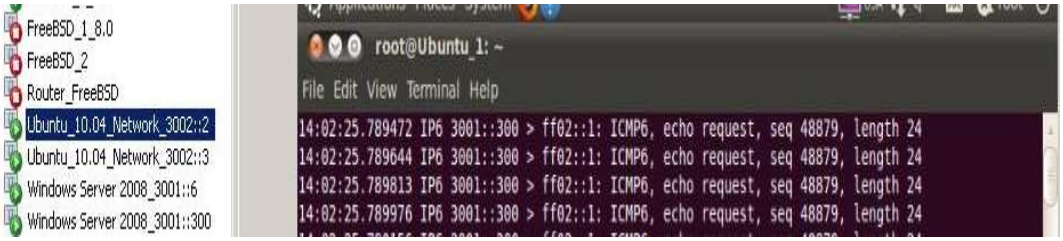
III.2.2.9 Smurf6

Bu saldırı tooluyla saldırgan, kaynak adresi hedef aldığı bilgisayar olan bir Echo request paketi oluşturur ve bu paketi networkteki tüm hostlara gönderir.

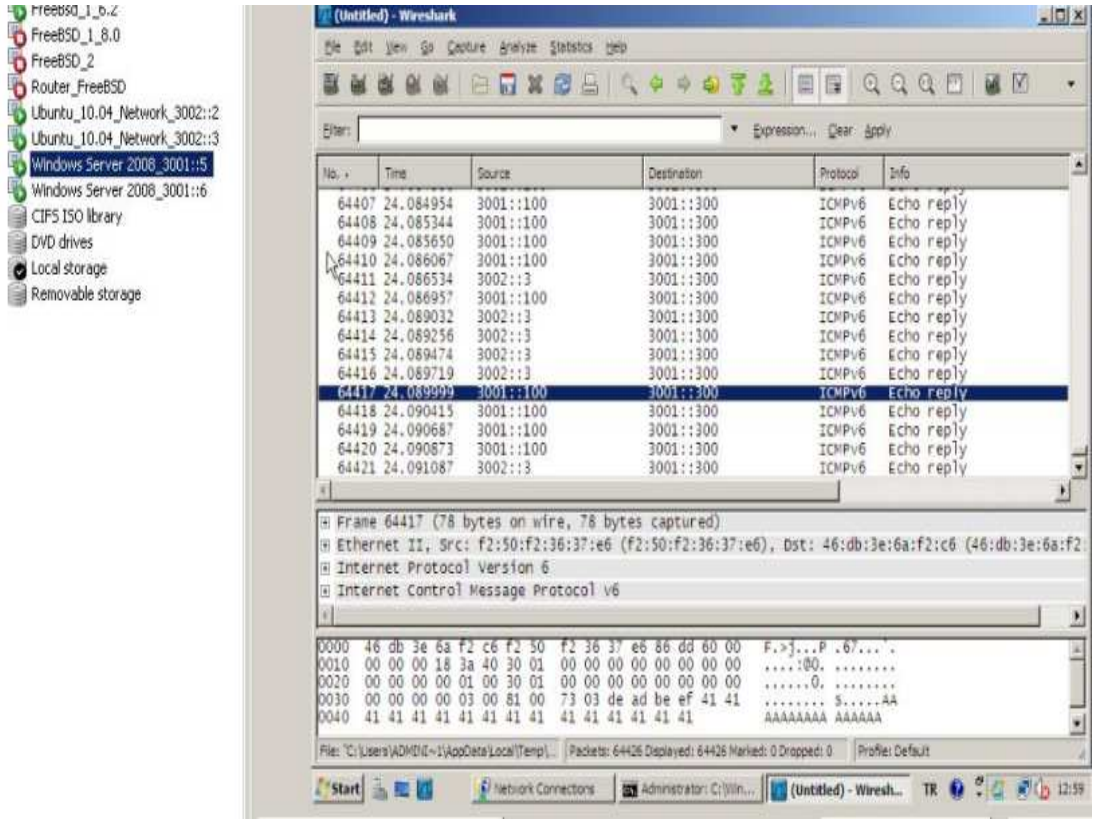
Kaynak adresi, hedef bilgisayar olarak oluşturulmuş echo request paketini alan networkteki hostlar ise echo reply paketlerini döndürürler. Bu sayede hedef alınan 3001::300 bilgisayarına DOS saldırısı yapılmış olur.



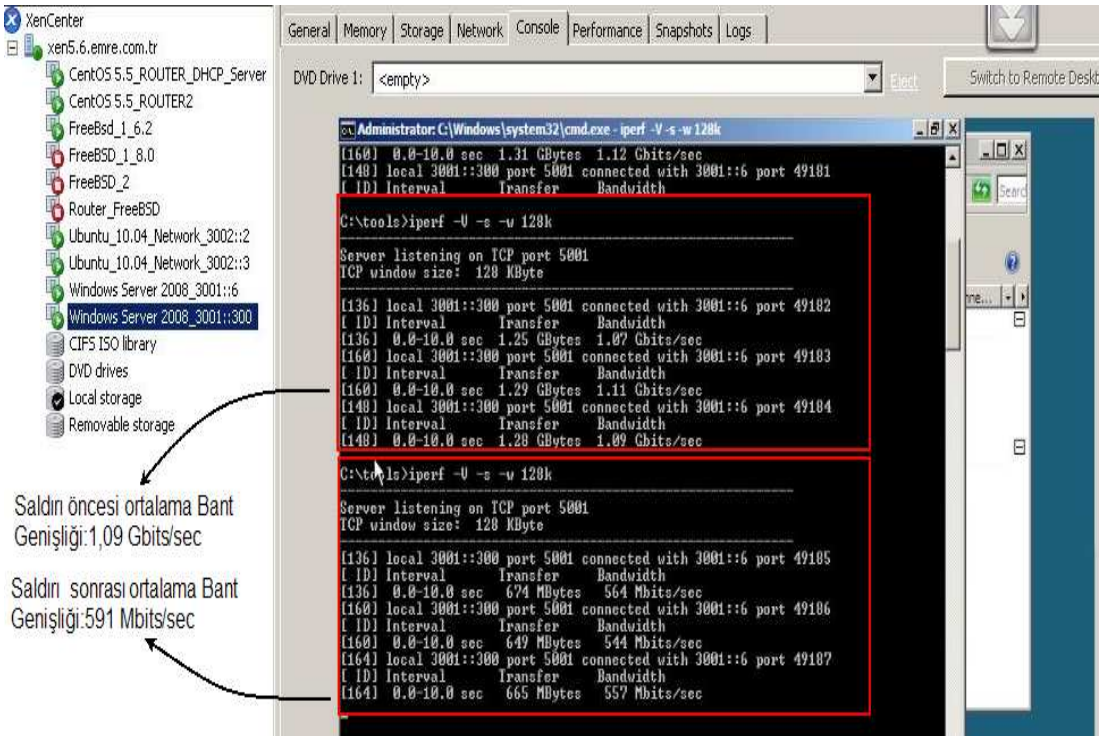
Şekil III.22: Sadırıyı yapan 3002::2 bilgisayarının Smurf6 ekran çıktısı



Şekil III.23: Sadırıyı yapan 3002::2 bilgisayarının Smurf6 Tcpdump çıktısı



Şekil III.24: Saldırıya maruz kalan 3001::300 bilgisayarının Smurf6 Wireshark çıktısı



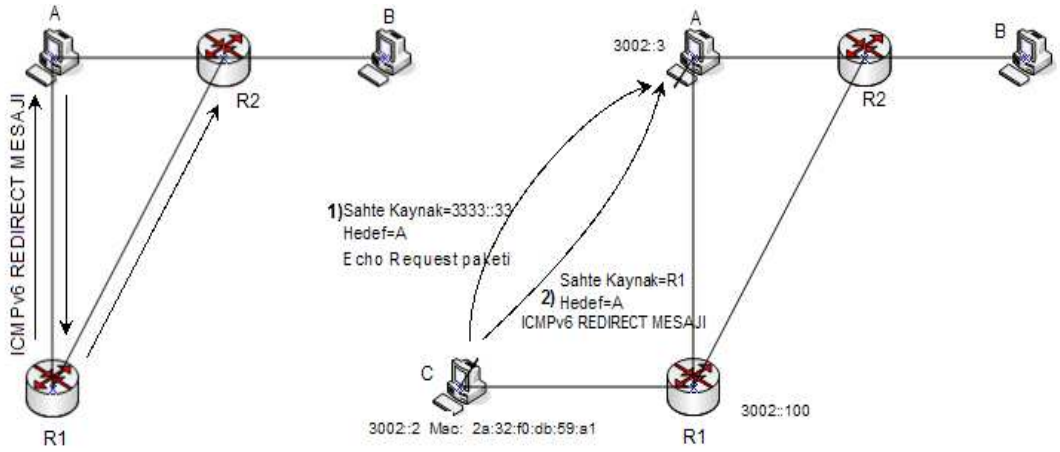
Şekil III.25: Smurf6 saldırı sonrası Bant genişliği ölçümü

Yukarıdaki şekilden de anlaşılacağı gibi saldırı sonrasında band genişliği neredeyse yarı yarıya düşmektedir.

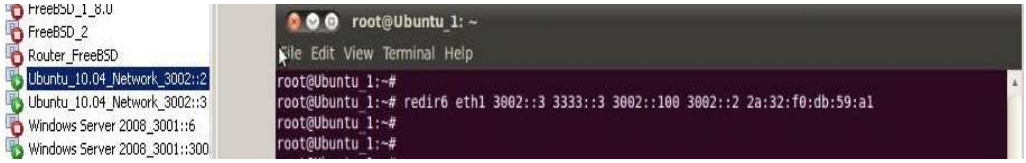
III.2.2.10 Redir6

A bilgisayarından B bilgisayarına bir paket gönderilmek istediğini düşünelim. A bilgisayarı önce kendi Route Tablosunda B bilgisayarına ait bir route olup olmadığına kontrol eder. Bu örneğimizde route olmadığını farzedelim. Bu nedenle A bilgisayarı, paketi Varsayılan Ağ geçidi (Default Gateway) olarak ayarlanmış R1 routerına gönderecektir. R1 routerı ise paketi B bilgisayarına ulaşması için R2 routerına teslim edecektir. Ardından da A bilgisayarına bir ICMP Redirect mesajı yollayarak B hedefine daha kısa yoldan gidebilmesi için paketlerini R2 routerına göndermesi bilgisini gönderir. Bu ICMP mesajını alan A bilgisayarı ise kendi route tablosuna B bilgisayarı için yeni route bilgisini ekler ve bundan sonra B bilgisayarına olan mesajlarını direk olarak R2 routerı üzerinden gönderir. Fakat bu durum bazı güvenlik zaafiyetlerini de beraberinde getirmektedir. Öncelikle saldırgan C bilgisayarı aynı networkte olduğu A bilgisayarına, kendi route tablosunda olmayan bir kaynak olan 3333::3 adresinden geliyormuş gibi sahte bir Echo Request paketi gönderir. Ardından da R1 router adresinden geliyormuş gibi bir ICMPv6 Redirect Mesajı gönderir.[43] Bu mesajın içeriğinde ise 3333::3 adresi için C bilgisayarına

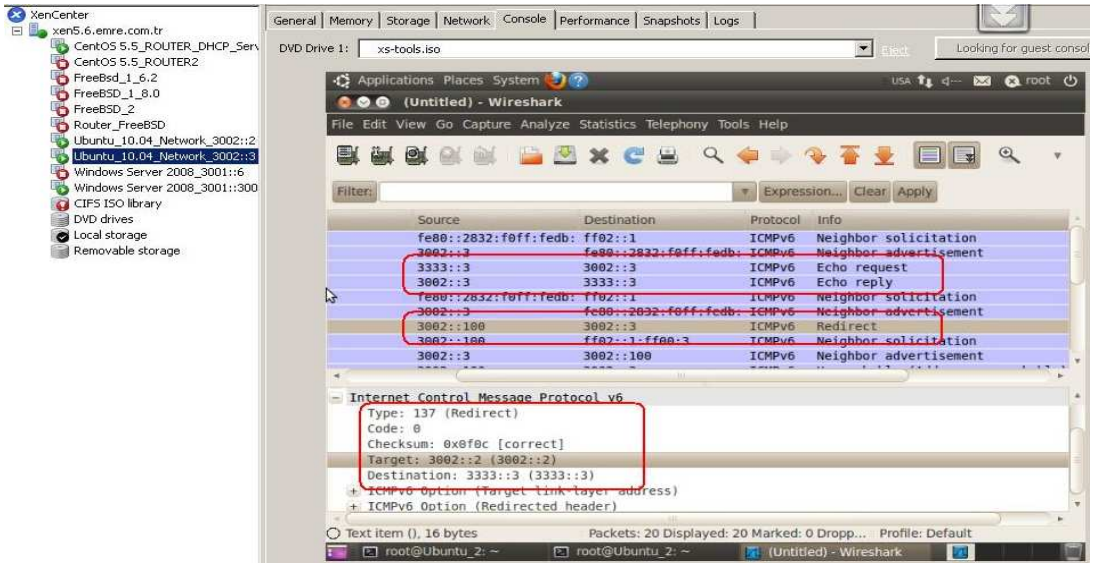
route bilgisi vardır. Bu mesajı alan A bilgisayarı route tablosuna C bilgisayarını ekler ve bundan sonraki paketler C bilgisayarına gönderilir. Bu sayede C bilgisayarı paketleri kendi üzerinden geçirmiş ve paketleri dinlemiş olur.



Şekil III.26: ICMPv6 Redirect Mesaj saldırısı



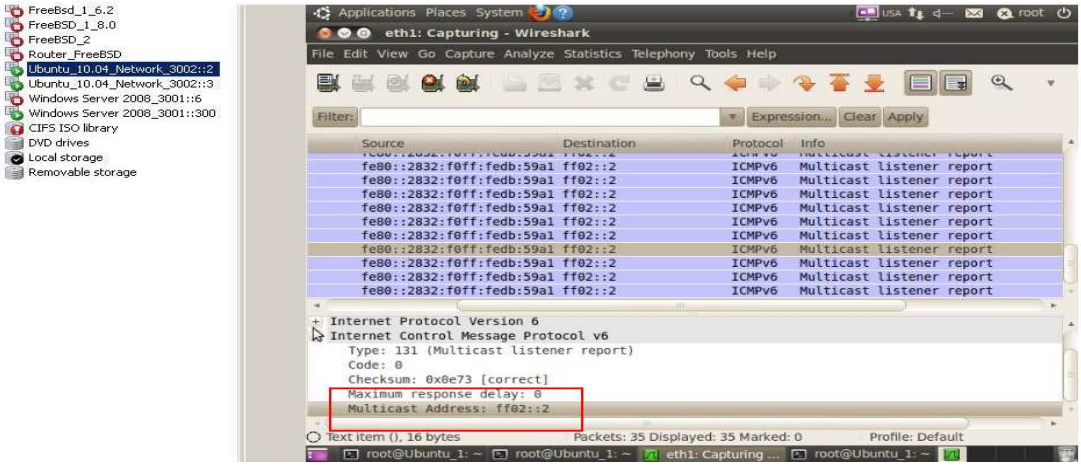
Şekil III.27: ICMPv6 Redirect Saldırısı



Şekil III.28: ICMPv6 Redirect Saldırısına maruz kalan bilgisayar

III.2.2.11 Fake_mld6

Burada kendinizi veya istediğiniz başka birini, seçmiş olduğunuz bir multicast gruba dahil edebilirsiniz.



Şekil III.29: Fake_mld6 wireshark çıktısı

III.2.3 Routing Header (Yönlendirme Başlığı) Ek Başlığı Güvenlik Testleri

Yönlendirme başlığı, paketin hedef düğüme ulaşırken üzerinden geçmesi istenilen diğer düğümlerin adres bilgisilerini taşır. Yani paket kaynak noktasından gönderilirken ilerlelemesi istenilen yol rotası da belirlemiş olur (Source Routing). "Sonraki başlık" değeri 43'tür.

Şekil III.30: Routing Header

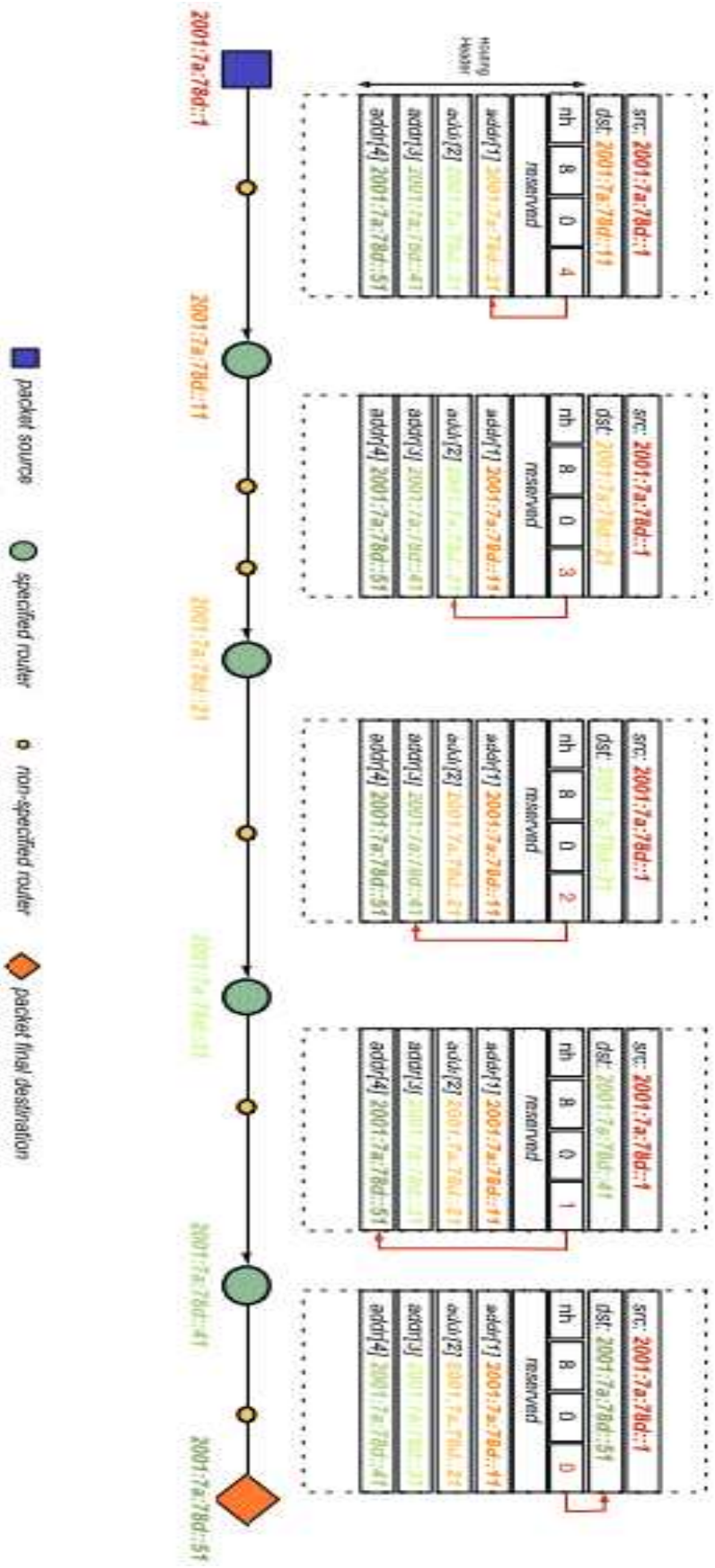
Sonraki Başlık: 8 bit uzunluğundadır. Bir sonraki başlığın tür bilgisini içerir.

Başlık Genişleme Uzunluğu: Yönlendirme türü değerinin 0 olduğu durumda başlık genişleme uzunluğu değeri, başlık içerisinde listelenen adres sayısının iki katına eşittir.

Yönlendirme Türü: Routing Header Type bilgisi burada tutulur. Varsayılan olarak 0 değerini alır.

Kalan Segment: Paketin alıcı düğüme ulaşmadan önce geçmesi gereken düğüm sayısını gösterir.

Türe Özel Veri: Yönlendirme Türüne bağlı olarak değişken uzunluktadır. Kalan segment alanından sonraki tüm kısmı kapsar.



Şekil III.31: Yönlendirme Türünün 0 olması durumunda Yönlendirme [46]

Bu testleri gerçekleştirmek için öncelikle Extension Header içeren paketler oluşturmamız gerekiyor. Bunun içinse Scapy programı kullanılmıştır.

III.2.3.1 Scapy ile paket oluşturma [44]

- ICMPv6 EchoRequest paketi oluşturma:

```
root@Ubuntu_1:~# scapy
Welcome to Scapy (2.0.1)
>>> destination="3002::3"
>>> packet=IPv6(dst=destination)/ICMPv6EchoRequest()
>>> sr1(packet)
```

Bu paket daha kısa şekliyle aşağıdaki şekliyle oluşturulabilir.

```
>>> sr1(IPv6(dst=3002::3)/ ICMPv6EchoRequest())
```

veya

```
>>> send(IPv6(dst=3002::3)/ ICMPv6EchoRequest())
```

- 10 adet ICMPv6EchoRequest paketi oluşturulup gönderilmek isteniyorsa;

```
>>> send(IPv6(dst=3002::3)/ ICMPv6EchoRequest()*10)
```

10 adet ICMPv6 EchoRequest paketi oluşturulup 3002::3 adresine gönderildi.

- İstenilen türde sahte paketler oluşturma [45]:

```
>>> spoofsource="3010::10"
>>> destination="3002::3"
>>> spoofpacket=IPv6(src=spoofsource,dst=destination)/ICMPv6EchoRequest()
>>> sr1(spoofpacket)
```

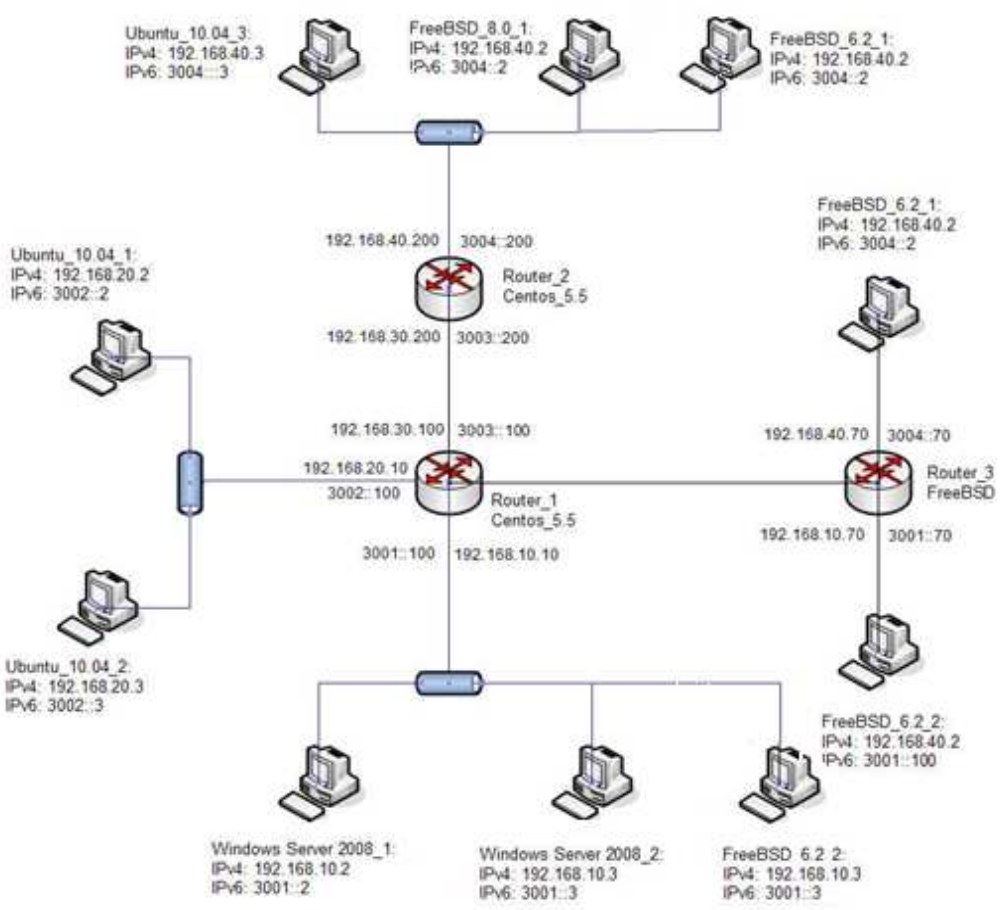
3010::10 adresinden geliyormuş gibi ICMPv6 EchoRequest paketi oluşturulup 3002::3 adresine gönderildi.

- RoutingHeader Type:0 (RH0) içeren ICMPv6 EchoRequest paketi oluşturma:

```
>>> hope1="3005::1"
>>> hope2="3006::1"
>>> hope3="3007::1"
>>>sr1(IPv6(dst=3002::3)/IPv6ExtHdrRouting(addresses=[hope1,hope2,hope3])/
ICMPv6EchoRequest())
```

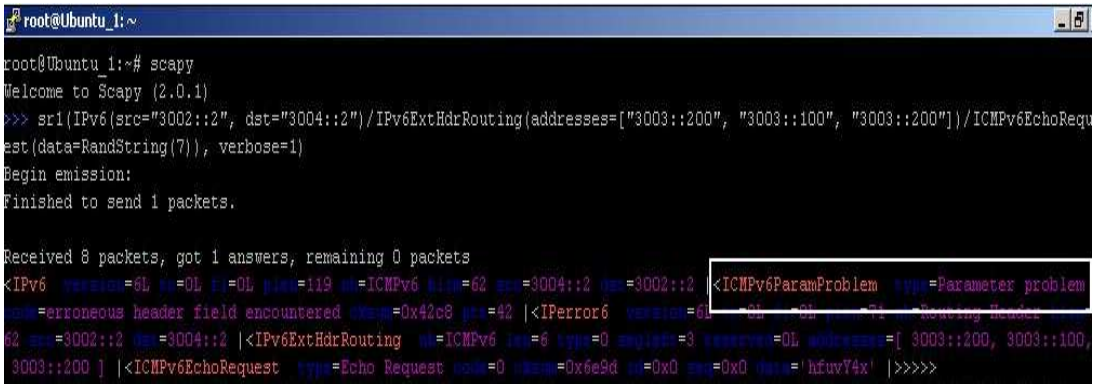
III.2.3.2 Testler

Bu testler sırasında Ubuntu 10.04, Centos 5.5, Windows Server 2008, FreeBSD 8.0 ve FreeBSD 6.2 işletim sistemleri kullanılmış ve her birinin Routing Header ek başlığı saldırılarına karşı durumları gözlemlenmiştir.



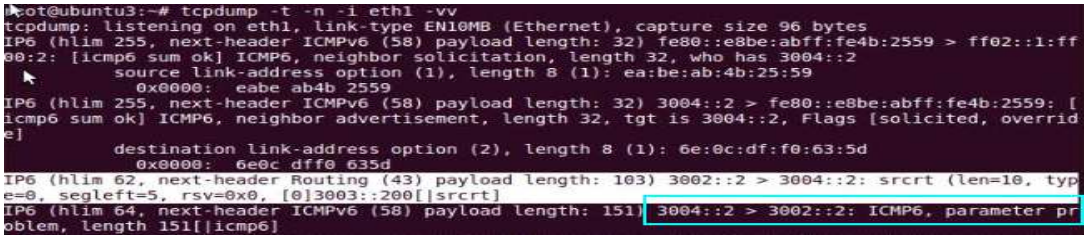
Şekil III.2 : Deney Topolojisi

İlk olarak Ubuntu_1 bilgisayarında birden fazla hedef IPv6 adres taşıyan ICMPv6 EchoRequest paketi oluşturulmuş ve Ubuntu_3 bilgisayarına gönderilmiştir.



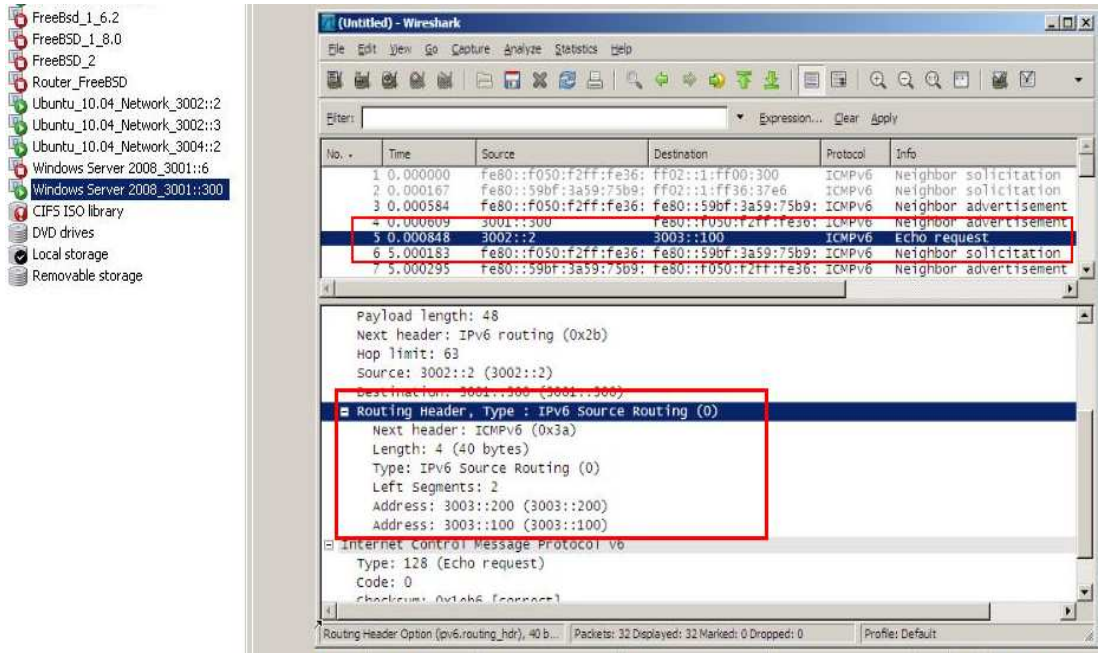
Şekil III.32 : Ubuntu_1 Parametre Problemi

Fakat Şekil III.30 'da görüldüğü gibi Ubuntu_3 bilgisayarı RH0 içeren pakete Prameter Problem hata mesajı dönmüştür.



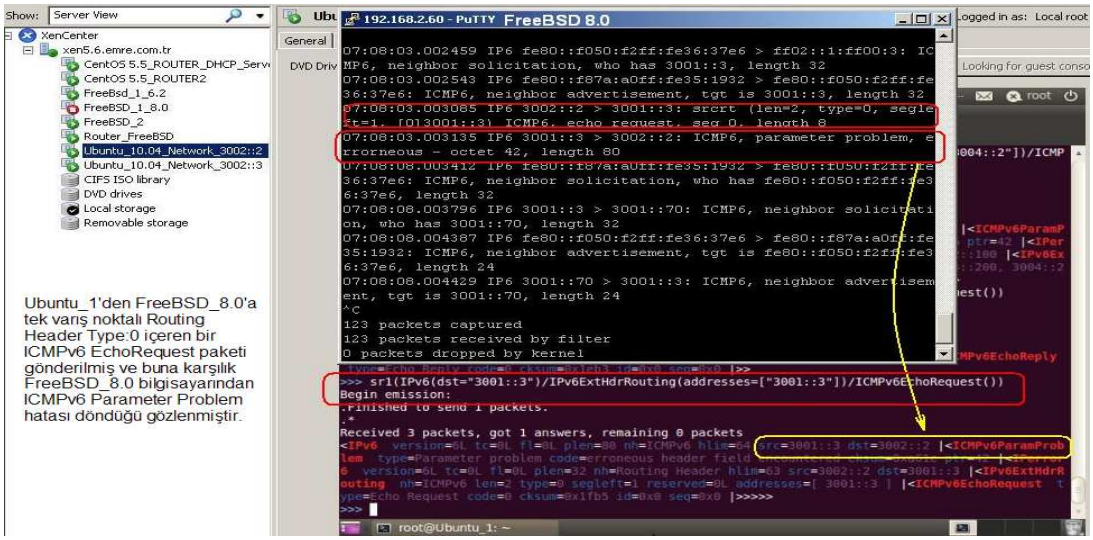
Şekil III.33: Ubuntu_3 ICMPv6 Parametre Problemi

Ardından Ubuntu_1 bilgisayarından Windows_1 bilgisayarına aynı test uygulanmış, Ubuntu_1'den Router_1'e gelen Routing Header paketi incelenmiştir. Fakat Windows_1 adresine gelen her hangi bir Routing Header paketi gözlemlenmemiştir.



Şekil III.34: Windows_1 Routing Header paketi

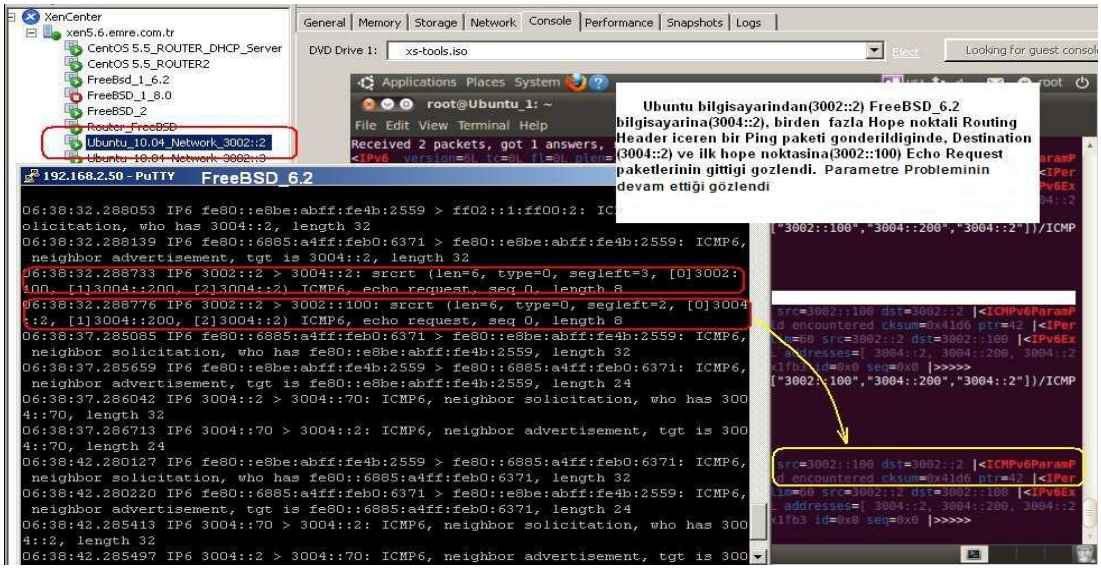
Sonrasında aynı test FreeBSD_8.0 bilgisayarı için yapılmıştır. Ubuntu_1 bilgisayarından FreeBSD_8.0 bilgisayarına, tek IPv6 adres taşıyan RH0 içeren ICMPv6 EchoRequest paketi gönderilmiştir. Bu pakete karşılık FreeBSD_8.0 bilgisayarından ICMPv6 Parameter Problem Hatasının döndüğü gözlemlenmiştir.



Şekil III.35 : FreeBSD_8.0 ICMPv6 Parametre Problemi

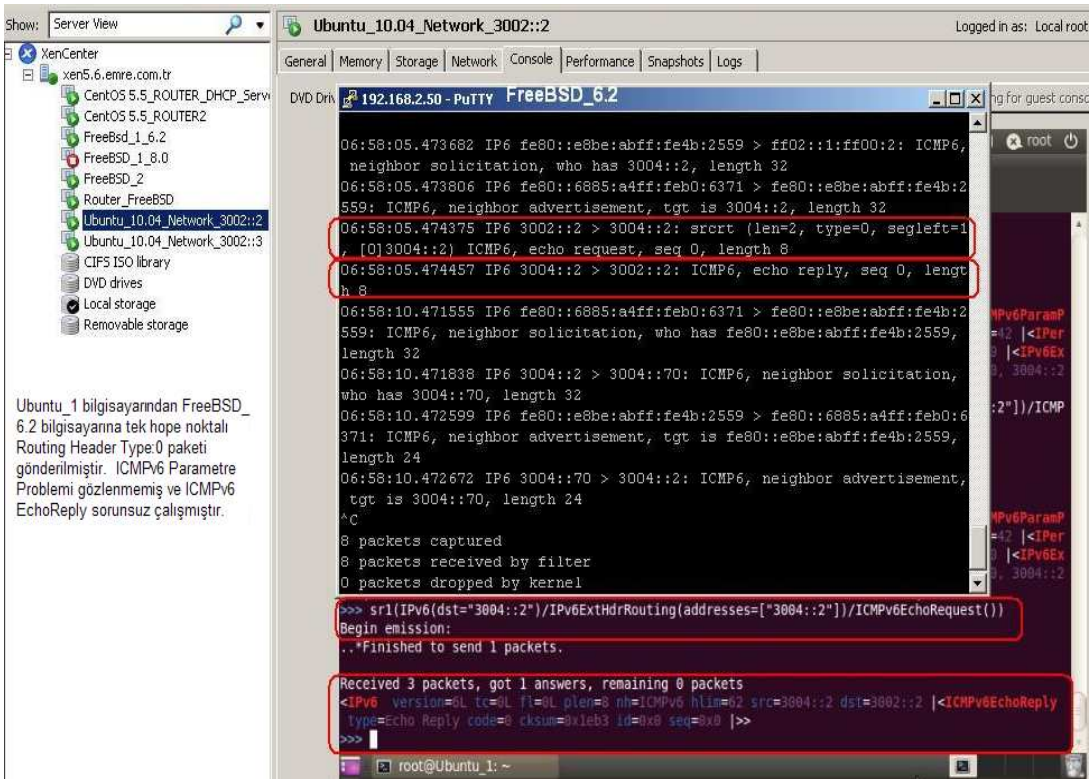
Son olarak FreeBSD_6.2 bilgisayarı teste tabi tutulmuştur. FreeBSD_6.2 bilgisayarı 2 farklı şekilde test edilmiştir.

Birincisinde Ubuntu_1 bilgisayarından FreeBSD_6.2 bilgisayarına birden fazla IPv6 adres taşıyan RH0 paketi içeren ICMPv6 EchoRequest paketi gönderilmiştir. Bu test sonunda diğer testlerde olduğu gibi FreeBSD_6.2 bilgisayarından ICMPv6 Parameter Problem Hatasının döndüğü gözlemlenmiştir



Şekil III.36 : FreeBSD_6.2 ICMPv6 Parametre Problemi

FreeBSD_6.2 bilgisayarını tabi tuttuğumuz ikinci testte ise sadece tek IPv6 adres taşıyan RH0 paketi içeren ICMPv6 EchoRequest paketi gönderilmiştir. Bu test sonunda her hangi bir ICMPv6 Parametre Problemine rastlanmamıştır. Ubuntu_1 bilgisayarından gönderilen ICMPv6 EchoRequest paketine cevaben FreeBSD_6.2 bilgisayarından ICMPv6 EchoReply paketinin geldiği gözlemlenmiştir.

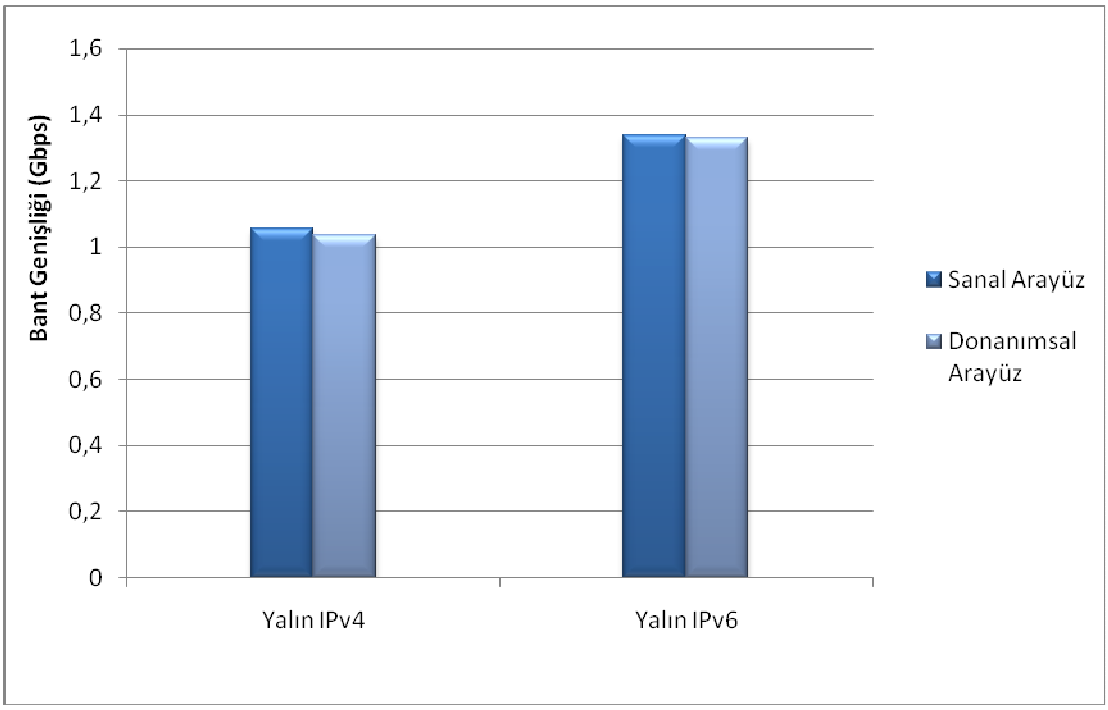


Şekil III.37 : FreeBSD_6.2 Routing Header

BÖLÜM IV

IV. SONUÇLAR VE TARTIŞMALAR

Şekil III.2'deki Xen Server üzerinde oluşturulmuş deney topolojinde yer alan Window Server 2008 bilgisayarlar arasında, yalın IP paketlerinin Sanal ve Donanımsal arayüzler üzerindeki performansları test edilmiş ve Şekil IV.1' deki grafik elde edilmiştir.



Şekil IV.1: Sanal ve Donanımsal Arayüzlerin Bant Genişliği Performansları

Bu ölçümler sonucunda Sanal arayüzler üzerindeki Bant geniliği değerlerinin Donanımsal arayüzler üzerindeki değerlere kıyasla çok az oranla daha iyi olduğu gözlenmiştir.

Tablo IV.1 Sanal ve Donanımsal Arayüzlerin Bant Genişliği Performansları

Bant Genişliği	Sanal-Donanımsal Arayüz (+%)
IPv6	0,53%
IPv4	1,59%

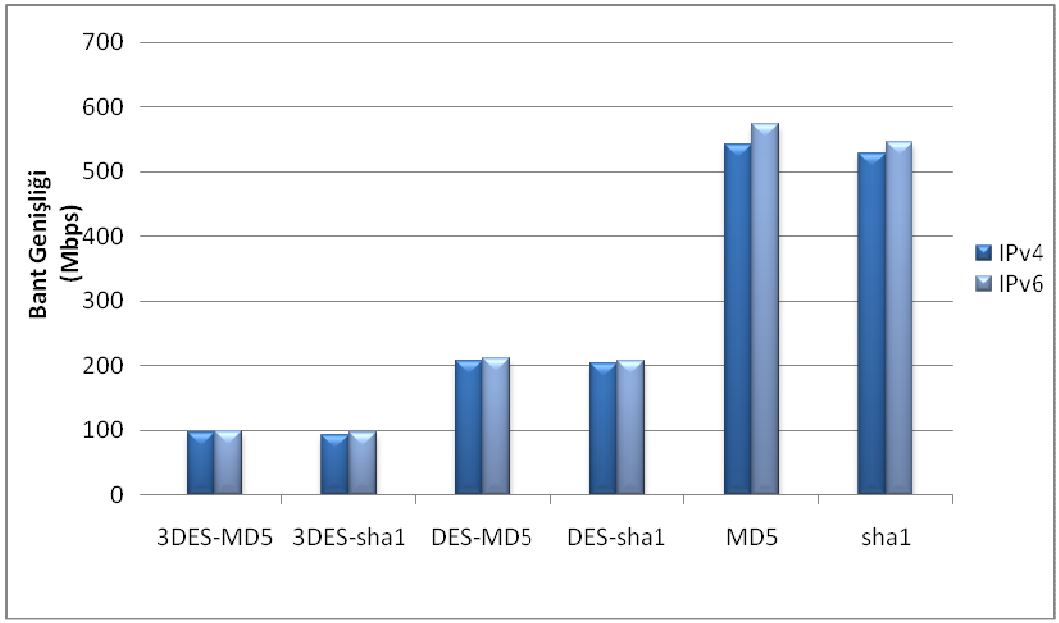
Tablo IV.1 üzerinde de görüldüğü gibi IPv4 ve IPv6 adresleme sistemlerinde sanal arayüzlerin bant genişliklerinin donanımsal arayüzlere oranla daha iyi olduğu saptanmıştır.

Tablo IV.2 IPv6 ve IPv4 Paketlerinin Bant Genişliği Performansları

Bant Genişliği	IPv6-IPv4 karşılaştırması (+%)
Sanal arayüz	26,74%
Donanımsal Arayüz	28,08%

Tablo IV.2 'ten anlaşılacağı üzere IPv6 paketleri, sade başlık yapısı vb. nedenlerle sanal ve donımsal arayüzler üzerinde IPv4 paketlere oranla daha iyi bant genişiliği performansına sahip olduğu gözlemlenmiştir.

IPSec güvenlik protokolünü oluşturan AH ve ESP fonksiyonlarının farklı kombinasyonları hem IPv4 için hem de IPv6 için sanal arayüzler üzerinde ayrı ayrı denenmiş ve Şekil IV.1' deki grafik elde edilmiştir. IPv4'te olduğu gibi IPv6 içinde IPSec uygulamaları büyük oranda Bant Genişliği azalmalarına sebep olmaktadır.



Şekil IV.2 : IPSec Kombinasyonlarına ait Bant Genişlikleri

Sadece AH Doğrulama Başlıklarının kullanılması, sadece ESP Şifreleme Başlıklarının kullanımına göre çok daha düşük bir yük getirmiş ve bant genişlik değerleri yüksek çıkmıştır. ESP Şifreleme Başlıklarını oluşturan 3DES algoritması

DES algoritmasına kıyasla çok daha büyük bir yük getirmiş ve bu nedenle bant genişliği değerleri daha düşük çıkmıştır.

Tablo IV.3 IPSec Türevlerinin IPv6-IPv4 Bant Genişliği Performansları

Bant Genişliği	IPv6-IPv4 karşılaştırması (+%)
3DES-MD5	0,84%
3DES-sha1	3,93%
DES-MD5	2,18%
DES-sha1	1,99%
MD5	6,05%
sha1	3,08%

Tablo IV.3 verilerinden de anlaşılacağı gibi sanal arayüzler üzerinde uygulanan IPSec Türevlerinin hepsinde IPv6 bant genişliği performansının IPv4 bant genişliği değerlerine göre, donanımsal arayüzler üzerinde yapılan [11] çalışmasından farklı olarak, çok ufak oranlarla daha iyi olduğu ölçülmüştür.

Aynı zamanda mukayese edilen [11] çalışmasında, AH Doğrulama Başlığında kullanılan hash algoritmalarından olan sha1 bant genişliği değerinin MD5 bant genişliği değerinden %50 civarında az olduğu görülmüştür. Fakat sanal arayüzlerde testlerin defalarca tekrarlanmasına karşın sha1 bant genişliği değerinin MD5 bant genişliği değerinden %5 civarında düşük olduğu bilgisi elde edilmiştir.

. Bant genişliği değerlerinin donanımsal arayüzlere kıyasla daha yüksek çıkmasının nedeninin testlerin sanal ortamda gerçekleştirildiğinden yani paketlerin layer2 ethernet katmanına inmeden direk olarak uygulama katmanında işlenmesinden kaynaklandığı düşünülmektedir.

THC saldırı programı ile yapılan güvenlik testleri sonuçlarına göre IPv6 için IPv4'e nazaran her hangi bir güvenlik üstünlüğünün ya da zafiyetinin olmadığı sonucu çıkarılmıştır. IPv6 protokolü ile saldırı türlerinde kısmi farklılıklar meydana gelmiştir. IPv4 protokolünde yer alan bazı atak türleri yok olurken literatüre yeni saldırı türlerinin girdiği gözlemlenmiştir.

Yönlendirme Ek Başlığı (Routing Extension Header) testleri için oluşturululan ICMPv6 paketlerinde yer alan Routing Header paketlerinin varsayılan olarak Type:0 özelliği taşıdığı gözlenmiştir.

Eğer kalan segment değeri sıfır ise, düğüm yönlendirme başlığını önemsemez, bu başlık içerisindeki sonraki başlık kısmında işaret edilen bir sonraki başlığa geçilir. Eğer kalan segment değeri sıfırdan farklı ise, düğüm paketi çöpe atar ve paketin kaynak adresi kısmındaki adrese ICMP Parametre Problemi, kod 0, tanınmayan yönlendirme türü hatasını işaret eden bir mesaj yollar.

Farklı işletim sistemleri üzerinde yapılan RH0 ek başlığı içeren paket testleri sonucunda, tüm güncel işletim sistemlerinin DOS saldırılarını engelleyebilmek için bu paketlere kernel seviyesinde ve giriş aşamasında filtre (ingress filtering) uyguladığı doğrulanmıştır [48-49]. Güncel versiyon işletim sistemlerinin paketi filtrelemesi sonucunda FreeBSD_6.2 işletim sisteminin Routing Header içeren paketleri filtrelemediği bilgisine ulaşılmış [46] ve beraberinde Ubuntu_1 bilgisayarından FreeBSD_6.2 bilgisayarına doğru birden fazla IPv6 adresi taşıyan RH0 paketi gönderilmiştir. Fakat paketler FreeBSD_6.2 tarafından filtrelenmiş ve tekrar ICMPv6 Parameter Problem hatası alınmıştır. Aynı test tek IPv6 adresli RH0 paketi içeren ICMPv6 EchoRequest paketiyle tekrar denenmiş ve herhangi bir Parametre hatası alınmadan ICMPv6 EchoReply paketi gözlemlenmiştir. Bu bağlamda FreeBSD_6.2 versiyonunun [46] çalışmasında bahsedildiği gibi RH0 paketlerini filtrelemeden, tam olarak işlediği bilgisinin eksik olduğu ve sadece tek IPv6 adres taşıyan RH0 paketlerini filtrelemeyip işlediği bilgisine ulaşılmıştır.

Sonuç olarak IPv6 açısından önemli bir güvenlik açığı olarak öne çıkmış olan RH0, işletim sistemleri tarafından filtrelenmekte ve bu güvenlik zafiyeti ortadan kaldırılmaktadır.

Bununla birlikte Mobil IPv6 uygulamaları için gerekli olan Routing Header ek başlıkları, Type:2 olarak kullanılmaktadır. Type:2, Routing Header içerisinde taşınacak adres sayısını 1 olarak sınırlandırmıştır. Bu nedenle herhangi bir güvenlik zafiyeti oluşturmamaktadır. Mobil IPv6 teknolojisinin gelişebilmesi için, Router ve FireWall gibi cihazların farklı Routing Header tiplerini analiz edip, analiz sonuçlarına göre aksiyon almaları gerekmektedir. Bu sayede güvenlik açığı olarak algılanıp filtrelenen Type:0 Routing Headerlar, Type:2 üzerinden iletilen Mobil IPv6 trafiğini sınırlandırmayacak ve uygulamalarının yaygınlaşmasında sorun teşkil etmeyecektir [50]

BÖLÜM V

V. SON DEĞERLENDİRMELER ve ÖNERİLER

IPv6 adresleme sistemini ve güvenlik yeniliklerini incelemek için Citrix XenServer sanallaştırma teknolojisi kullanılarak bir network topolojisi oluşturulmuştur. Oluşturulan sanal network üzerinde IPv6 adresleme sistemi kullanılmış ve güvenlik konusu irdelenmiştir. Bunun için IPv6 ve IPv4 için IPSec ve türevlerinde bant genişlikleri incelenmiştir. Beraberinde farklı işletim sistemlerinde IPv6 saldırı toolları kullanılarak güvenlik zafiyetleri araştırılmıştır. Son olarak ta RH0 paketleriyle oluşturulabilecek güvenlik açıklıkları analiz edilmiştir. Sanallaştırma teknolojisi ile istenildiği anda kolaylıkla host ve arayüz ekleme özelliği sayesinde, test ortamları için oldukça verimli bir kullanış sunmaktadır.

Sanallaştırmanın yapılacağı ve sanal bilgisayarların kurulacağı makine seçilirken Server olarak ifade ettiğimiz, PC'lere göre daha performanslı, daha stabil ve uzun süreli çalışmalar için geliştirilmiş makinelerin kullanılması, edinilen tecrübelere dayanılarak tavsiye edilmektedir. Öncelikle kullanılacak olan işlemcinin sanallaştırma teknolojisini desteklemesi gerekmektedir. Eğer PC kullanılacak ise ilk aşama olan XenServer işletim sisteminin kurulum aşamasında daha fazla zorluklarla karşılaşılabilir. Sanallaştırma programlarının seçimi aşamasında farklı sanallaştırma programları denenmiş fakat lisans, performans ve üzerinde çalışacak olan Linux-Unix tabanlı işletim sistemlerin performans değerleri açısından XenServer tercih edilmiştir.

Bunlarla birlikte oluşturulan sanal makineler, donanımsal makineler kadar sorunsuz ve stabil çalışmamakta ve daha fazla uğraştırıcı olabilmektedirler.

İşletim sistemleri üzerinde yapılan deneyler sırasında, FreeBSD işletim sisteminin diğer işletim sistemlerine göre daha performanslı ve stabil çalıştığı gözlemlenmiştir.

IPv6 ile önemi ve kullanımı daha da artacak olan IPSec ve bant genişliği üzerine testler yapılmış ve IPv4 ile aralarında çok küçük oranlarda fark olduğu bulgusuna ulaşılmıştır.

Native IPv6 desteği olan saldırı programları vasıtasıyla güvenlik konusu incelenmiş bu konuda da IPv4 ile aralarında bir üstünlük olmadığı anlaşılmıştır. Fakat bu testler native IPv6 desteği olan programların artması ve IPv6'nın daha yaygın kullanılmasıyla birlikte daha net veriler ortaya koyabilecektir.

Yapılan çalışma neticesinde, Yönlendirme Ek Başlığından kaynaklanabilecek güvenlik zaafiyetlerinin İşletim sistemlerinde Kernel seviyesinde engellendiği gözlenmiştir.

NAT yapısının ortadan kalkmasıyla birlikte kullanıcılar routerdan aldıkları network bilgileri ile kendi IP adreslerini oluşturur ve internet ortamına çıkarlar. Bu nedenle kullanıcının IP adres bilgisinden ait olduğu network bilgisine ulaşılabilecektir. Bu güvenlik açığını engelleyebilmek için oluşturulan ve en genel ifadeyle network bilgisini gizleme işlemini yapan RFC 4864 " Local Network Protection " etkili olacaktır.

Geçiş aşamasında, paketlerin tünellemiş olarak gönderilmesi ve enkapsüle edilmiş paketlerin güvenlik cihazları tarafından algılanamamış olması, çok daha ciddi güvenlik zafiyetlerini ortaya çıkarabilecektir. Bu nedenle geçiş süreci güvenliği oldukça önemli bir hal almaktadır.

KAYNAKLAR

[1] Çalışkan, B.: "Teredo; Güvenlik ve Performans Analizi", 4.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Mayıs, **(2010)**

[2]http://www.ipv6.net.tr/index.php?option=com_content&view=article&id=61%3Aduenyada-ve-tuerkiye-ipv6nn-durumu&catid=41%3Aipv6-tarihi&Itemid=67 **(30.07.2010)**

[3] Orcan, S.: "Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi**" ,** IPv6 Bilgilendirme Toplantısı , Ankara, Mayıs **(2009)**

[4] Kara, M.: "IPv4 Protokolünden IPv6 Protokolüne Geçiş", TÜBİTAK-UEKAE, **(2009)**

[5] Aktaş, M.: " IPv6'ya Geçiş Sürecinde Yaşananlar" , IPv6 Çalıştayı, 4. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, ODTÜ Ankara, Mayıs **(2010)**

[6] Marin, E.: " IPv6 Security " , 6Net, Zagreb, **(2003)**

[7] Akbal, A.; Balık, H.H.: " TCP/IP'nin Dünü, Bugünü, Yarını ", Fırat Ünivertisesi,

[8] Bolat, A.; Ve Ark. "Ulusal IPv6'ya Geçiş ve Stratejileri " **(2007)**
.

[9] Sotillo, S: "IPv6 Security Issues." **(2006).**
www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf

[10] Sağıroğlu, Ş.; Bektaş, O.: "Güvenlik Penceresinden IPv4/IPv6 Karşılaştırılması" , Aralık, **(2008)**

[11] Boztoprak, Ö.T. : " IPv4'ten IPv6'ya Geçiş Süreci ", Marmara Üniversitesi, Şubat, **(2009).**

[12] Kadayıf, İ.; Kabal, O.: "IPv4 ağlarının IPv6 Ağlarına Entegrasyonu", Çanakkale Onsekiz Mart Üniversitesi Bilimsel Araştırma Projeleri Komisyonu, Aralık, **(2006)**

[13] Erdoğan, K. : " IPv4'ten IPv6'ya Geçiş Süreci İçin IPv6 Tünel ve Sanal Hedef Ip Teknikleri ", Gazi Üniversitesi, Haziran**,(2007)**

[14] Buckley, R.: " IPv6: Improvements and Security" , **(2005)**

[15] Sailan, M. K.; Hassan, R.; Patel, A.: " A Comparative Review of IPv4 and IPv6 for Research Test Bed " , International Conference on Electrical Engineering and Informatics, Selangor, Malaysia, August, **(2009)**

[16] The Government of the Hong Kong Special Administrative Region: "IPv6 Security" , **(2008)**

[17] Gadong, J.: "IPv6-to-IPv4 Transition And Security Issues" , Information Technology Protective Security Services, February, **(2008)**

[18] Radwan, A.M.: "Using IPSec in IPv6 Security". **(2005).** http://www.uop.edu.jo/csit2006/vol2%20pdf/pg471.pdf

[19] Yüksel, Z.: "Ağ Güvenliği ve Güvenlik Duvarında VPN ve NAT Uygulamaları", İstanbul, **(2007)**

[20] North American IPv6 Task Force (NAv6TF) Technology Report: "IPv6 Security Technology Paper" ,Version 1.0, July 22, **(2006)**

[21] Deering, S.; Hinden, R.: "IP Version 6 Addressing Architecture", RFC 4291, February, **(2006)**

[22] Demir, H.: "IPv6" , Ortadoğu Teknik Üniversitesi, **(2008)**

[23] **http://technet.microsoft.com/tr-tr/library/cc755011(WS.10).aspx (30.07.2010)**

[24] Ketenci, S.; Akın, G.: "Anycast ve IPv6'da Anycast Kullanımı" , İTÜ Bilgi İşlem Daire Başkanlığı , **(2009)**

[25] Deering, S.; Hinden, R.: "IPv6 Multicast Address Assignments", RFC 2375, July, **(1998)**

[26] Uncu,A.:"Solicited-node-multicast-addresses" , **(2009)** **http://www.agciyiz.net/index.php/servis-ve-**uygulamalar//

[27] Sümer, O.; Kipman, E.: "IPv6 Adresleme ve Başlık Yapısı"

[28] Pul, A.: " IPv6 ve Getirdikleri ", Karadeniz Teknik Üniversitesi, Haziran, **(2004).**

[29] Efe, A. : " IPv6 Güvenlik Riskleri ve Olası Çözümleri" , Beykent Üniversitesi, **(2006)**

[30] Bolat, A.: " Mobil Ip" Haberleşme Teknolojileri ve Uygulamaları Sempozyumu, Kasım, **(2007)**

[31] Ural, Ö.: "Yerel Alan Ağların İnternet Bağlantılarında Güvenliğin Sağlanmasında Kısısıtlar Teorisinin Düşünce Süreçlerinin Kullanılması" , **(2007).**

[32] Karaaslan, E.; Akın, G.; Fetah, V.: " Kurumsal Ağlarda Zararlı Yazılımlarla Mücadele Kılavuzu " , Nisan, **(2008)**

[33] Güvensan, M. A.: "Linux İşletim Sitemi Çekirdeği ile Bütünleşik Bir Kriptografik Sistemin Tasarımı ve Gerçeklenmesi " , **(2006)**

[34] Türkiye Bilişim Derneği : "Sanallaştırma " , Kamu Bilişim Platformu XII , Nisan, **(2010)**

[35] Majstor, F.: "Does IPv6 protocol solve all security problems of IPv4? " **(2003)**

[36] Oh, H.; ve Ark. : "Comparisons analysis of Security Vulnerabilities for Security Enforcement in IPv4/IPv6" , Womans University, Korea, **(2006)**

[37] Hogg, S.; Vyncke, E.: "IPv6 Security" , **(2009)**

[38] Zagar, D.; Grgic, K.; Rimac S.: "Security Aspects in IPv6 networks – implementation and testing", Faculty of Electrical Engineering, J.J. Strossmayer University of Osijek, July 12**, (2007)**

[39] Zagar, D.; Grgic, K.: "IPv6 Security Threats and Possible Solutions." Automation Congress, WAC '06. World, 1-7. **(2006).**

[40] Yüce, E.: "A Case Study On The Security Of IPv6 Transitions Methods" , **(2009)**

[41] Lancaster, T.: "IPv6 & IPv4 Threat Review with Dual-Stack Considerations", University of Southampton, Department of Electronics and Computer Science, **(2006)**

[42] Bieringer, P.: " Linux IPv6 Howto" , **(2009)**

[43] Hauser, v.: "Attacking the IPv6 Protocol Suite" The Hackers Choice, (2008) http://freeworld.thc.org/papers/vh_thc-ipv6_attack.pdf **(25.03.2010)**

[44] **http://secdev.org/projects/scap (17.03.2010)**

[45] Yüce, E.; Gökırmak, Y.: "IPv6 Saldırı Araçları ve IPv6-GO Uygulamaları" **(2010)**

[46] Biondi, P.; Ebalard, A.: " IPv6 Routing Header Security " , Fransa, **(2007)**

[47] Yüce, E.; Gökırmak, Y.; Bektaş, O.; Orcan. S.: "IPv6 Geçiş Yöntemleri Güvenlik Analizi " , TÜBİTAK ULAKBİM, ANKARA, **(2010)**

[48] Abley, J.; Savola, P.: "Deprecation of Type 0 Routing Headers in IPv6 ", RFC 5094, December, **(2007)**

[49] Ferguson, P.; Senie, D.: " Network Ingress Filtering: Defeating Defeating Denial of Service Attacks which employ IP Source Address Spoofing ", RFC 2267, May, **(2000)**

[50] Johnson, D.; Perkins, C.: "Mobility Support in IPv6 ", RFC 3775, June, **(2004)**

EK I. 1 IPSec Test Sonuçları

Yalın IPv4 : Sanal Arayüz		Yalın IPv6 : Sanal Arayüz		Yalın IPv4 : Donanımsal Arayüz		Yalın IPv6 : Donanımsal Arayüz	
Transfer	Bandwidth	Transfer	Bandwidth	Transfer	Bandwidth	Transfer	Bandwidth
1,24GBytes	1,07Gbits/sec	1,54GBytes	1,32Gbits/sec	1,2GBytes	1,03Gbits/sec	1,55GBytes	1,33Gbits/sec
1,24GBytes	1,07Gbits/sec	1,55GBytes	1,33Gbits/sec	1,21GBytes	1,04Gbits/sec	1,57GBytes	1,35Gbits/sec
1,24GBytes	1,06Gbits/sec	1,52GBytes	1,31Gbits/sec	1,23GBytes	1,06Gbits/sec	1,56GBytes	1,33Gbits/sec
1,23GBytes	1,05Gbits/sec	1,56GBytes	1,34Gbits/sec	1,21GBytes	1,04Gbits/sec	1,59GBytes	1,36Gbits/sec
1,24GBytes	1,06Gbits/sec	1,55GBytes	1,33Gbits/sec	1,22GBytes	1,04Gbits/sec	1,55GBytes	1,33Gbits/sec
1,24GBytes	1,07Gbits/sec	1,55GBytes	1,33Gbits/sec	1,22GBytes	1,05Gbits/sec	1,53GBytes	1,31Gbits/sec
1,25GBytes	1,07Gbits/sec	1,54GBytes	1,32Gbits/sec	1,21GBytes	1,04Gbits/sec	1,54GBytes	1,32Gbits/sec
1,23GBytes	1,05Gbits/sec	1,58GBytes	1,35Gbits/sec	1,23GBytes	1,06Gbits/sec	1,57GBytes	1,35Gbits/sec
1,23GBytes	1,05Gbits/sec	1,53GBytes	1,31Gbits/sec	1,19GBytes	1,02Gbits/sec	1,54GBytes	1,32Gbits/sec
1,19GBytes	1,02Gbits/sec	1,59GBytes	1,36Gbits/sec	1,21GBytes	1,04Gbits/sec	1,53GBytes	1,32Gbits/sec
1,24GBytes	1,06Gbits/sec	1,58GBytes	1,35Gbits/sec	1,22GBytes	1,04Gbits/sec	1,58GBytes	1,35Gbits/sec
1,24GBytes	1,06Gbits/sec	1,57GBytes	1,35Gbits/sec	1,22GBytes	1,04Gbits/sec	1,55GBytes	1,33Gbits/sec
1,22GBytes	1,05Gbits/sec	1,54GBytes	1,32Gbits/sec	1,2GBytes	1,03Gbits/sec	1,54GBytes	1,32Gbits/sec
1,25GBytes	1,07Gbits/sec	1,57GBytes	1,34Gbits/sec	1,22GBytes	1,05Gbits/sec	1,55GBytes	1,33Gbits/sec
1,24GBytes	1,06Gbits/sec	1,53GBytes	1,32Gbits/sec	1,2GBytes	1,02Gbits/sec	1,57GBytes	1,35Gbits/sec
1,2GBytes	1,03Gbits/sec	1,57GBytes	1,35Gbits/sec	1,21GBytes	1,04Gbits/sec	1,57GBytes	1,34Gbits/sec
1,24GBytes	1,06Gbits/sec	1,54GBytes	1,32Gbits/sec	1,18GBytes	1,01Gbits/sec	1,53GBytes	1,31Gbits/sec
1,25GBytes	1,07Gbits/sec	1,57GBytes	1,35Gbits/sec	1,21GBytes	1,04Gbits/sec	1,55GBytes	1,33Gbits/sec
1,2GBytes	1,03Gbits/sec	1,55GBytes	1,33Gbits/sec	1,22GBytes	1,05Gbits/sec	1,55GBytes	1,33Gbits/sec
1,23GBytes	1,06Gbits/sec	1,57GBytes	1,35Gbits/sec	1,22GBytes	1,04Gbits/sec	1,58GBytes	1,35Gbits/sec
1,24GBytes	1,06Gbits/sec	1,52GBytes	1,3Gbits/sec	1,18GBytes	1,01Gbits/sec	1,56GBytes	1,34Gbits/sec
1,23GBytes	1,06Gbits/sec	1,59GBytes	1,37Gbits/sec	1,19GBytes	1,02Gbits/sec	1,58GBytes	1,36Gbits/sec
1,24GBytes	1,06Gbits/sec	1,59GBytes	1,36Gbits/sec	1,21GBytes	1,04Gbits/sec	1,52GBytes	1,3Gbits/sec
1,22GBytes	1,04Gbits/sec	1,59GBytes	1,36Gbits/sec	1,21GBytes	1,04Gbits/sec	1,53GBytes	1,31Gbits/sec
1,23GBytes	1,06Gbits/sec	1,56GBytes	1,34Gbits/sec	1,21GBytes	1,04Gbits/sec	1,57GBytes	1,35Gbits/sec
1,24GBytes	1,07Gbits/sec	1,58GBytes	1,35Gbits/sec	1,21GBytes	1,04Gbits/sec	1,54GBytes	1,32Gbits/sec
1,22GBytes	1,04Gbits/sec	1,54GBytes	1,32Gbits/sec	1,22GBytes	1,05Gbits/sec	1,52GBytes	1,3Gbits/sec
1,22GBytes	1,05Gbits/sec	1,55GBytes	1,33Gbits/sec	1,19GBytes	1,02Gbits/sec	1,56GBytes	1,34Gbits/sec
1,23GBytes	1,06Gbits/sec	1,52GBytes	1,31Gbits/sec	1,23GBytes	1,05Gbits/sec	1,51GBytes	1,3Gbits/sec
1,24GBytes	1,06Gbits/sec	1,58GBytes	1,35Gbits/sec	1,21GBytes	1,04Gbits/sec	1,58GBytes	1,35Gbits/sec
1,22GBytes	1,05Gbits/sec	1,55GBytes	1,33Gbits/sec	1,21GBytes	1,04Gbits/sec	1,55GBytes	1,33Gbits/sec
1,19GBytes	1,02Gbits/sec	1,55GBytes	1,33Gbits/sec	1,19GBytes	1,02Gbits/sec	1,55GBytes	1,33Gbits/sec
1,21GBytes	1,04Gbits/sec	1,6GBytes	1,37Gbits/sec	1,2GBytes	1,03Gbits/sec	1,53GBytes	1,31Gbits/sec
1,21GBytes	1,04Gbits/sec	1,51GBytes	1,3Gbits/sec	1,23GBytes	1,05Gbits/sec	1,51GBytes	1,29Gbits/sec
1,23GBytes	1,06Gbits/sec	1,58GBytes	1,35Gbits/sec	1,19GBytes	1,02Gbits/sec	1,54GBytes	1,32Gbits/sec
1,25GBytes	1,07Gbits/sec	1,59GBytes	1,36Gbits/sec	1,21GBytes	1,04Gbits/sec	1,55GBytes	1,33Gbits/sec
1,21GBytes	1,04Gbits/sec	1,55GBytes	1,33Gbits/sec	1,22GBytes	1,04Gbits/sec	1,53GBytes	1,31Gbits/sec
1,22GBytes	1,04Gbits/sec	1,55GBytes	1,33Gbits/sec	1,21GBytes	1,04Gbits/sec	1,55GBytes	1,33Gbits/sec
1,22GBytes	1,05Gbits/sec	1,55GBytes	1,33Gbits/sec	1,21GBytes	1,04Gbits/sec	1,53GBytes	1,32Gbits/sec
1,23GBytes	1,06Gbits/sec	1,54GBytes	1,32Gbits/sec	1,21GBytes	1,04Gbits/sec	1,56GBytes	1,34Gbits/sec
Ortalama		Ortalama		Ortalama		Ortalama	
1,2285GBytes	1,05375	1,55725	1,3355	1,20925	1,03725	1,54925	1,3285

EK I. 2 IPSec Test Sonuçları

3DES-MD5 : IPv4		3DES-MD5 : IPv6		3DES-sha1 : IPv4		3DES-sha1 : IPv6	
Transfer	Bandwidth	Transfer	Bandwidth	Transfer	Bandwidth	Transfer	Bandwidth
116MBytes	97,3Mbits/sec	116MBytes	97,3Mbits/sec	114MBytes	95,6Mbits/sec	115MBytes	96,3Mbits/sec
116MBytes	97Mbits/sec	117MBytes	97,9Mbits/sec	114MBytes	95,3Mbits/sec	115MBytes	96,6Mbits/sec
117MBytes	97,8Mbits/sec	116MBytes	97Mbits/sec	98,8MBytes	82,7Mbits/sec	115MBytes	96,4Mbits/sec
115MBytes	96Mbits/sec	117MBytes	98,3Mbits/sec	109MBytes	91,3Mbits/sec	115MBytes	96,1Mbits/sec
115MBytes	96Mbits/sec	117MBytes	97,9Mbits/sec	106MBytes	89,2Mbits/sec	116MBytes	96,9Mbits/sec
115MBytes	95,9Mbits/sec	116MBytes	97,5Mbits/sec	103MBytes	86,2Mbits/sec	115MBytes	96,6Mbits/sec
115MBytes	96,1Mbits/sec	116MBytes	97,3Mbits/sec	99,3MBytes	83,2Mbits/sec	115MBytes	96,1Mbits/sec
115MBytes	96,2Mbits/sec	115MBytes	96,2Mbits/sec	114MBytes	95,3Mbits/sec	116MBytes	96,9Mbits/sec
115MBytes	96,6Mbits/sec	116MBytes	96,8Mbits/sec	113MBytes	94,9Mbits/sec	116MBytes	96,7Mbits/sec
115MBytes	96,5Mbits/sec	116MBytes	97,4Mbits/sec	115MBytes	96,1Mbits/sec	117MBytes	98Mbits/sec
117MBytes	97,8Mbits/sec	115MBytes	96,6Mbits/sec	114MBytes	95,2Mbits/sec	115MBytes	96,4Mbits/sec
117MBytes	98,4Mbits/sec	116MBytes	96,8Mbits/sec	115MBytes	96Mbits/sec	115MBytes	96,7Mbits/sec
115MBytes	96,5Mbits/sec	116MBytes	97Mbits/sec	115MBytes	96,1Mbits/sec	115MBytes	96,7Mbits/sec
114MBytes	95,6Mbits/sec	115MBytes	96,5Mbits/sec	115MBytes	96,1Mbits/sec	115MBytes	96,6Mbits/sec
115MBytes	96Mbits/sec	116MBytes	96,8Mbits/sec	114MBytes	95Mbits/sec	117MBytes	98,2Mbits/sec
115MBytes	96,1Mbits/sec	116MBytes	97,5Mbits/sec	114MBytes	95,8Mbits/sec	116MBytes	97,2Mbits/sec
115MBytes	96,5Mbits/sec	115MBytes	96,6Mbits/sec	115MBytes	96,2Mbits/sec	116MBytes	97,2Mbits/sec
116MBytes	96,8Mbits/sec	115MBytes	96,4Mbits/sec	113MBytes	94,9Mbits/sec	118MBytes	98,6Mbits/sec
116MBytes	97,5Mbits/sec	118MBytes	98,4Mbits/sec	113MBytes	94.5Mbits/sec	116MBytes	97,5Mbits/sec
114MBytes	95,4Mbits/sec	117MBytes	98,2Mbits/sec	113MBytes	94.7Mbits/sec	115MBytes	96,5Mbits/sec
115MBytes	96,3Mbits/sec	117MBytes	97,7Mbits/sec	113MBytes	94.7Mbits/sec	114MBytes	95,3Mbits/sec
114MBytes	95,7Mbits/sec	116MBytes	96,9Mbits/sec	114MBytes	95.2Mbits/sec	115MBytes	96Mbits/sec
116MBytes	96,8Mbits/sec	117MBytes	98Mbits/sec	113MBytes	94.7Mbits/sec	115MBytes	96,3Mbits/sec
115MBytes	96,3Mbits/sec	116MBytes	97,2Mbits/sec	114MBytes	95.2Mbits/sec	116MBytes	97,1Mbits/sec
115MBytes	95,9Mbits/sec	118MBytes	98,6Mbits/sec	114MBytes	95.1Mbits/sec	116MBytes	97Mbits/sec
115MBytes	96,4Mbits/sec	117MBytes	97,9Mbits/sec	114MBytes	95.3Mbits/sec	117MBytes	98Mbits/sec
116MBytes	97,2Mbits/sec	117MBytes	98,1Mbits/sec	116MBytes	96.8Mbits/sec	115MBytes	96,4Mbits/sec
115MBytes	96,3Mbits/sec	115MBytes	96,6Mbits/sec	114MBytes	95.3Mbits/sec	116MBytes	97,5Mbits/sec
114MBytes	95,7Mbits/sec	116MBytes	97,6Mbits/sec	114MBytes	95.1Mbits/sec	116MBytes	97,5Mbits/sec
116MBytes	97Mbits/sec	116MBytes	97,1Mbits/sec	115MBytes	96.3Mbits/sec	116MBytes	97,5Mbits/sec
116MBytes	97,3Mbits/sec	117MBytes	97,7Mbits/sec	116MBytes	97.1Mbits/sec	116MBytes	97,1Mbits/sec
115MBytes	96,6Mbits/sec	116MBytes	97,6Mbits/sec	114MBytes	95,3Mbits/sec	117MBytes	98,2Mbits/sec
116MBytes	97,5Mbits/sec	116MBytes	97,3Mbits/sec	103MBytes	86,2Mbits/sec	116MBytes	97,1Mbits/sec
114MBytes	96Mbits/sec	116MBytes	97,1Mbits/sec	114MBytes	95,2Mbits/sec	114MBytes	95,8Mbits/sec
117MBytes	98Mbits/sec	117MBytes	97,6Mbits/sec	114MBytes	95,8Mbits/sec	114MBytes	95,9Mbits/sec
116MBytes	96,9Mbits/sec	116MBytes	97,1Mbits/sec	113MBytes	94.7Mbits/sec	115MBytes	96,7Mbits/sec
114MBytes	95,7Mbits/sec	115MBytes	96,4Mbits/sec	114MBytes	95.1Mbits/sec	115MBytes	96,7Mbits/sec
115MBytes	96Mbits/sec	116MBytes	97,2Mbits/sec	113MBytes	94.7Mbits/sec	116MBytes	96,9Mbits/sec
115MBytes	95,9Mbits/sec	116MBytes	97,1Mbits/sec	116MBytes	97.1Mbits/sec	115MBytes	96,5Mbits/sec
114MBytes	95,6Mbits/sec	118MBytes	98,4Mbits/sec	115MBytes	96,1Mbits/sec	116MBytes	96,9Mbits/sec
Ortalama		Ortalama		Ortalama		Ortalama	
115,275MBytes	96,5275	116,225	97,34	112,5025	93,2043478260869	115,575	96,865

EK I. 3 IPSec Test Sonuçları

DES-MD5 : IPv4		DES-MD5 : IPv6		DES-sha1 : IPv4		DES-sha1 : IPv6	
Transfer	Bandwidth	Transfer	Bandwidth	Transfer	Bandwidth	Transfer	Bandwidth
244MBytes	204Mbits/sec	251MBytes	210Mbits/sec	242MBytes	203Mbits/sec	246MBytes	206Mbits/sec
250MBytes	210Mbits/sec	253MBytes	212Mbits/sec	241MBytes	202Mbits/sec	250MBytes	209Mbits/sec
244MBytes	205Mbits/sec	251MBytes	210Mbits/sec	241MBytes	202Mbits/sec	254MBytes	213Mbits/sec
248MBytes	208Mbits/sec	250MBytes	209Mbits/sec	244MBytes	204Mbits/sec	248MBytes	208Mbits/sec
245MBytes	205Mbits/sec	250MBytes	210Mbits/sec	245MBytes	205Mbits/sec	246MBytes	206Mbits/sec
243MBytes	204Mbits/sec	253MBytes	212Mbits/sec	245MBytes	205Mbits/sec	249MBytes	208Mbits/sec
248MBytes	208Mbits/sec	253MBytes	212Mbits/sec	241MBytes	202Mbits/sec	249MBytes	209Mbits/sec
248MBytes	208Mbits/sec	251MBytes	210Mbits/sec	241MBytes	202Mbits/sec	248MBytes	208Mbits/sec
248MBytes	208Mbits/sec	254MBytes	213Mbits/sec	243MBytes	203Mbits/sec	244MBytes	204Mbits/sec
245MBytes	206Mbits/sec	253MBytes	212Mbits/sec	244MBytes	205Mbits/sec	247MBytes	207Mbits/sec
248MBytes	207Mbits/sec	252MBytes	211Mbits/sec	246MBytes	206Mbits/sec	250MBytes	210Mbits/sec
246MBytes	206Mbits/sec	253MBytes	212Mbits/sec	242MBytes	202Mbits/sec	251MBytes	210Mbits/sec
246MBytes	206Mbits/sec	249MBytes	209Mbits/sec	246MBytes	206Mbits/sec	252MBytes	211Mbits/sec
245MBytes	206Mbits/sec	252MBytes	211Mbits/sec	242MBytes	202Mbits/sec	250MBytes	209Mbits/sec
245MBytes	205Mbits/sec	251MBytes	210Mbits/sec	247MBytes	207Mbits/sec	247MBytes	207Mbits/sec
248MBytes	208Mbits/sec	251MBytes	210Mbits/sec	243MBytes	204Mbits/sec	250MBytes	209Mbits/sec
247MBytes	207Mbits/sec	251MBytes	210Mbits/sec	240MBytes	201Mbits/sec	246MBytes	206Mbits/sec
247MBytes	207Mbits/sec	248MBytes	208Mbits/sec	243MBytes	204Mbits/sec	243MBytes	204Mbits/sec
246MBytes	206Mbits/sec	252MBytes	211Mbits/sec	242MBytes	203Mbits/sec	246MBytes	206Mbits/sec
246MBytes	206Mbits/sec	259MBytes	217Mbits/sec	242MBytes	203Mbits/sec	245MBytes	205Mbits/sec
247MBytes	207Mbits/sec	250MBytes	209Mbits/sec	242MBytes	203Mbits/sec	249MBytes	209Mbits/sec
248MBytes	208Mbits/sec	251MBytes	210Mbits/sec	241MBytes	202Mbits/sec	250MBytes	210Mbits/sec
243MBytes	204Mbits/sec	251MBytes	211Mbits/sec	250MBytes	210Mbits/sec	249MBytes	209Mbits/sec
241MBytes	202Mbits/sec	251MBytes	210Mbits/sec	244MBytes	204Mbits/sec	250MBytes	210Mbits/sec
248MBytes	208Mbits/sec	250MBytes	210Mbits/sec	244MBytes	204Mbits/sec	246MBytes	206Mbits/sec
247MBytes	207Mbits/sec	251MBytes	210Mbits/sec	243MBytes	204Mbits/sec	249MBytes	209Mbits/sec
247MBytes	207Mbits/sec	255MBytes	213Mbits/sec	244MBytes	204Mbits/sec	244MBytes	205Mbits/sec
245MBytes	206Mbits/sec	252MBytes	211Mbits/sec	242MBytes	203Mbits/sec	250MBytes	209Mbits/sec
244MBytes	204Mbits/sec	253MBytes	212Mbits/sec	245MBytes	205Mbits/sec	247MBytes	207Mbits/sec
250MBytes	209Mbits/sec	254MBytes	213Mbits/sec	242MBytes	203Mbits/sec	245MBytes	206Mbits/sec
246MBytes	206Mbits/sec	251MBytes	211Mbits/sec	245MBytes	205Mbits/sec	250MBytes	209Mbits/sec
245MBytes	205Mbits/sec	255MBytes	214Mbits/sec	242MBytes	203Mbits/sec	252MBytes	211Mbits/sec
248MBytes	207Mbits/sec	252MBytes	211Mbits/sec	242MBytes	203Mbits/sec	250MBytes	210Mbits/sec
245MBytes	205Mbits/sec	254MBytes	213Mbits/sec	245MBytes	206Mbits/sec	247MBytes	207Mbits/sec
248MBytes	208Mbits/sec	253MBytes	212Mbits/sec	244MBytes	204Mbits/sec	249MBytes	209Mbits/sec
249MBytes	209Mbits/sec	249MBytes	209Mbits/sec	247MBytes	207Mbits/sec	250MBytes	209Mbits/sec
243MBytes	203Mbits/sec	251MBytes	210Mbits/sec	243MBytes	204Mbits/sec	247MBytes	207Mbits/sec
247MBytes	207Mbits/sec	251MBytes	211Mbits/sec	247MBytes	206Mbits/sec	249MBytes	209Mbits/sec
245MBytes	205Mbits/sec	247MBytes	207Mbits/sec	244MBytes	205Mbits/sec	249MBytes	209Mbits/sec
248MBytes	208Mbits/sec	249MBytes	209Mbits/sec	243MBytes	204Mbits/sec	247MBytes	207Mbits/sec
Ortalama		Ortalama		Ortalama		Ortalama	
246,275	206,375	251,675	210,875	243,475	204	248,25	208,05

EK I. 4 IPSec Test Sonuçları

MD5 : IPv4		MD5 : IPv6		sha1 : IPv4		sha1 : IPv6	
Transfer	Bandwidth	Transfer	Bandwidth	Transfer	Bandwidth	Transfer	Bandwidth
652MBytes	546Mbits/sec	656MBytes	550Mbits/sec	628MBytes	526Mbits/sec	644MBytes	539Mbits/sec
646MBytes	541Mbits/sec	692MBytes	580Mbits/sec	631MBytes	528Mbits/sec	640MBytes	536Mbits/sec
635MBytes	532Mbits/sec	687MBytes	576Mbits/sec	619MBytes	519Mbits/sec	645MBytes	540Mbits/sec
659MBytes	552Mbits/sec	689MBytes	577Mbits/sec	627MBytes	525Mbits/sec	653MBytes	547Mbits/sec
643MBytes	539Mbits/sec	693MBytes	580Mbits/sec	637MBytes	533Mbits/sec	658MBytes	551Mbits/sec
646MBytes	541Mbits/sec	668MBytes	560Mbits/sec	623MBytes	522Mbits/sec	643MBytes	538Mbits/sec
653MBytes	547Mbits/sec	691MBytes	579Mbits/sec	635MBytes	532Mbits/sec	655MBytes	549Mbits/sec
661MBytes	554Mbits/sec	699MBytes	586Mbits/sec	634MBytes	531Mbits/sec	659MBytes	552Mbits/sec
635MBytes	532Mbits/sec	693MBytes	581Mbits/sec	631MBytes	528Mbits/sec	649MBytes	544Mbits/sec
647MBytes	543Mbits/sec	670MBytes	562Mbits/sec	646MBytes	541Mbits/sec	659MBytes	552Mbits/sec
645MBytes	540Mbits/sec	682MBytes	572Mbits/sec	638MBytes	534Mbits/sec	653MBytes	547Mbits/sec
637MBytes	534Mbits/sec	675MBytes	566Mbits/sec	645MBytes	541Mbits/sec	655MBytes	549Mbits/sec
640MBytes	536Mbits/sec	685MBytes	575Mbits/sec	630MBytes	528Mbits/sec	662MBytes	555Mbits/sec
643MBytes	538Mbits/sec	693MBytes	582Mbits/sec	634MBytes	532Mbits/sec	639MBytes	535Mbits/sec
655MBytes	549Mbits/sec	681MBytes	570Mbits/sec	634MBytes	531Mbits/sec	641MBytes	537Mbits/sec
657MBytes	550Mbits/sec	690MBytes	579Mbits/sec	642MBytes	539Mbits/sec	651MBytes	546Mbits/sec
655MBytes	549Mbits/sec	681MBytes	571Mbits/sec	613MBytes	514Mbits/sec	638MBytes	534Mbits/sec
644MBytes	539Mbits/sec	684MBytes	574Mbits/sec	616MBytes	516Mbits/sec	650MBytes	544Mbits/sec
652MBytes	546Mbits/sec	694MBytes	582Mbits/sec	631MBytes	528Mbits/sec	659MBytes	552Mbits/sec
653MBytes	547Mbits/sec	685MBytes	574Mbits/sec	624MBytes	522Mbits/sec	647MBytes	542Mbits/sec
649MBytes	543Mbits/sec	698MBytes	584Mbits/sec	629MBytes	527Mbits/sec	643MBytes	538Mbits/sec
646MBytes	541Mbits/sec	687MBytes	577Mbits/sec	626MBytes	525Mbits/sec	652MBytes	546Mbits/sec
630MBytes	528Mbits/sec	684MBytes	574Mbits/sec	638MBytes	534Mbits/sec	657MBytes	551Mbits/sec
653MBytes	547Mbits/sec	689MBytes	578Mbits/sec	649MBytes	544Mbits/sec	659MBytes	552Mbits/sec
634MBytes	531Mbits/sec	693MBytes	581Mbits/sec	642MBytes	538Mbits/sec	647MBytes	542Mbits/sec
652MBytes	546Mbits/sec	701MBytes	588Mbits/sec	628MBytes	526Mbits/sec	654MBytes	548Mbits/sec
647MBytes	542Mbits/sec	697MBytes	584Mbits/sec	643MBytes	539Mbits/sec	656MBytes	550Mbits/sec
650MBytes	544Mbits/sec	696MBytes	583Mbits/sec	636MBytes	533Mbits/sec	672MBytes	563Mbits/sec
650MBytes	544Mbits/sec	695MBytes	583Mbits/sec	626MBytes	525Mbits/sec	636MBytes	533Mbits/sec
633MBytes	530Mbits/sec	690MBytes	579Mbits/sec	634MBytes	531Mbits/sec	651MBytes	545Mbits/sec
655MBytes	549Mbits/sec	680MBytes	571Mbits/sec	632MBytes	530Mbits/sec	656MBytes	550Mbits/sec
650MBytes	545Mbits/sec	682MBytes	572Mbits/sec	621MBytes	520Mbits/sec	657MBytes	551Mbits/sec
656MBytes	550Mbits/sec	689MBytes	577Mbits/sec	637MBytes	533Mbits/sec	646MBytes	541Mbits/sec
637MBytes	534Mbits/sec	686MBytes	575Mbits/sec	625MBytes	523Mbits/sec	648MBytes	543Mbits/sec
643MBytes	538Mbits/sec	677MBytes	568Mbits/sec	633MBytes	530Mbits/sec	662MBytes	555Mbits/sec
660MBytes	553Mbits/sec	686MBytes	575Mbits/sec	637MBytes	534Mbits/sec	657MBytes	550Mbits/sec
646MBytes	541Mbits/sec	674MBytes	565Mbits/sec	630MBytes	528Mbits/sec	644MBytes	539Mbits/sec
645MBytes	540Mbits/sec	676MBytes	567Mbits/sec	618MBytes	518Mbits/sec	646MBytes	542Mbits/sec
635MBytes	532Mbits/sec	673MBytes	564Mbits/sec	638MBytes	534Mbits/sec	650MBytes	546Mbits/sec
649MBytes	543Mbits/sec	677MBytes	567Mbits/sec	631MBytes	528Mbits/sec	655MBytes	549Mbits/sec
Ortalama		Ortalama		Ortalama		Ortalama	
646,95	541,9	685,45	574,7	631,775	529,25	651,2	545,575

ÖZGEÇMİŞ

DURDAĞI, Emre ,1982 Çıldır / ARDAHAN doğumlu.

Ortaöğrenimini Haydarpaşa Anadolu Teknik Lisesinde 2001 yılında tamamladı. Yüksek öğrenimini Marmara Üniversitesi Teknik Eğitim Fakültesi , Elektronik ve Haberleşme Eğitimi Anabilim Dalı'nda 2005 yılında tamamladı. Halen özel bir kuruluşta Network & Güvenlik Departmanında çalışmaktadır.