IPv6-GO Test Ağı Kurulumu

Onur Bektaş[1] *Emre Yüce*[2] *Neşe Kaptan Koç*[3] *İlknur Gürcan*[4]
Serkan Orcan[5] *Murat Soysal*[6] *Gökhan Eryol*[7] *Yusuf Öztürk*[8] *Yavuz Gökırmak*[9]

TÜBİTAK ULAKBİM, Ankara

[1]e-posta: onur@ulakbim.gov.tr [2]e-posta: emre@ulakbim.gov.tr [3]e-posta: nese@ulakbim.gov.tr
[4]e-posta: ilknur@ulakbim.gov.tr [5]e-posta: serkan@ulakbim.gov.tr [6]e-posta: msoysal@ulakbim.gov.tr
[7]e-posta: eryol@ulakbim.gov.tr [8]e-posta: yusuf.ozturk@ulakbim.gov.tr [9]e-posta: yavuzg@ulakbim.gov.tr

Özet

Tüm dünyada yeni nesil internet protokolüne (IPv6) geçiş konusunda çalışmalar yapılmaktadır. IPv6 geçişinin katma değer yaratacak yeni servisler yaratacak şekilde yapılabilmesinin temel gereksinimlerinden birisi IPv6 destekli araştırma ağlarına sahip olunmasıdır. Bu nedenle, özellikle geleceğin internetinde kendine yer edinmeyi amaçlayan ülkelerde üniversiteler, araştırma kurumları ve/veya sanayi organizasyonların bir araya gelerek IPv6 araştırma ve test ağlarının oluşturulmaktadır. Bu makalede bu amaç doğrultusunda "Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi" kapsamında TÜBİTAK ULAKBİM, Gazi Üniversitesi ve Çanakkale Onsekiz Mart Üniversitesine konuşlandırılan IPv6-GO (IPv6 Geliştirme Ortamı) test laboratuarların tasarım ve kurulum süreçleri ile ilgili olarak gerçekleştirilen çalışmalar irdelenecektir.

Anahtar Kelimeler: IPv6, geliştirme ortamı, test laboratuarı, test yatağı, IPv6-GO

1. GİRİŞ

Teknolojinin hızla gelişmesi ile birlikte kullanıcı sayısı ve ihtiyaçlarının beklentilerin ötesinde artması, yeni hizmet ve servislerin ihtiyaçlarının farklılaşması, 30 seneye yaklaşan kullanım süresi ile internetin temel protokolü olan IPv4'ün yeni nesil internet hizmetlerin verildiği alanlarda teknik olarak yetersiz kalmasına neden olmuştur. IPv4'te yaşanan problemler göz önüne alınarak tasarlanan IPv6, dolaşılabilirlik, çoklu gönderim, servis kalitesi, IP seviyesinde şifreleme ve kimlik doğrulama benzeri özellikleri tasarımında barındırmaktadır.

IPv6'nın içerdiği özelliklerin yazılım ve donanım desteği ile uygulanabilirliği, yeni nesil internet protokolüne geçiş için önerilen yöntemlerin performans, güvenlik ve tüm bu süreçlerin getireceği maliyetin belirlenebilmesi için gerek akademik gerekse ticari firmalar tarafından birçok çalışma yapılmaktadır.

Bu çalışmalarda temel amaç IPv6'nın vaat ettiği özelliklerin uygulanabilirliğinin denemesi, farklı ticari firmalar tarafından geliştirilen IPv6 destekli cihazların uyumluluk ve uygunluk testlerinin yapılabilmesi, IPv6 geçişinde yaşanacak ön görülmeyen problemlerin test edilerek çözüm üretilmesi, geçiş sırasında karşılaşılabilecek güvenlik problemlerin araştırılmasıdır.

Türkiye'nin IPv6 geçiş aşamasındaki yol haritasının belirlenmesi amaçlayan ve TÜBİTAK Kamu Kurumları Araştırma Ve Geliştirme Projelerini Destekleme Programı tarafından desteklenen "Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi" 'de TÜBİTAK ULAKBIM yönetici kurum, GAZİ Üniversitesi, Çanakkale Onsekiz Mart Üniversitesi yürütücü kurum olarak yer almaktadır. Bilgi Teknolojileri ve İletişim Kurumu (BTK) projede müşteri kurumdur. Proje Şubat 2009'da başlamıştır ve 24 ay sürmesi planlanmaktadır.

Projede yol haritasının belirlenebilmesi temel amacı çerçevesinde, Türkiye'de IPv6 geçiş yöntemlerinin hangisinin daha verimli olacağı, yönetim bilimi/yöneylem araştırması teknikleri kullanılarak oluşturulacak bir karar destek sistemi ile değerlendirilecek; geçiş aşamaları planlanacak ve geçiş takvimi oluşturulacak; geçiş aşamasında yaşanması muhtemel problemler belirlenecek ve çözüm önerileri geliştirilecek; geçiş süresinde ve sonrasında oluşabilecek güvenlik sorunları araştırılacak; maliyet analizi yapılacaktır.

Proje süresince yukarıda belirtilen çalışmaların gerçekleştirilmesine temel oluşturacak "Türkiye IPv6 Test Yatağı ve Geliştirme Ortamı (IPv6-GO)" proje başlangıcını takip eden 8 aylık süre içinde kurulmuştur. Makalenin bundan sonraki ikinci bölümünde IPv6-GO kurulum süreçleri hakkında bilgi verilecektir. Üçüncü bölümde benzeri araştırma ağı ve test yatakları konusunda bilgi verilecektir. İkinci bölümde IPv6-GO kurulum bilgisi üçüncü bölümde test senaryolarının nasıl uygulandığı anlatılacak ve son bölümde IPv6-GO'nun diğer İnternet Servis Sağlayıcılar ile olan bağlantılar yer almaktadır.

2. IPV6-GO KURULUMU

2.1. IPv6 -GO ihtiyaç analizi

Türkiye IPv6 Test Yatağı ve Geliştirme Ortamı (IPv6-GO) 'nın kurulma amaçları: geçiş yöntemleri güvenlik incelemesi yapılabilmesi; IPv6 ileri seviye özelliklerinin test edilebilmesi ve IPv6 tabanlı geliştirilen uygulamaların testlerinin yapılabilmesi için bir ortam sağlanmasıdır. Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi kapsamında yapılacak olan çalışmalar doğrulusunda, çeşitli olay örneklerini teşkil eden topolojiler oluşturulmakta ve bu topolojiler IPv6-GO laboratuarında gerçeklenmektedir. IPv6-GO test yatağı aşağıda belirtilen ihtiyaçlara cevap verecek şekilde tasarlanmıştır.

2.1.1. Farklı Test Senaryolarının Uygulanabilmesi

IPv6-GO tasarımı farklı test senaryolarının aynı anda uygulanabilmesine uygun olmalıdır.

2.1.2. Uzaktan Erişilebilirlik ve Yönetilebilirlik

IPv6-GO farklı kullanıcıların birbirlerinde izole olarak testlerini yapabilmeleri için uzaktan erişim sağlamalıdır. Bununla birlikte kullanıcıların test ağına fiziksel erişimlerinin olmadığı durumda dahi test ağı uygulanmak istenilen senaryoya göre uzaktan yapılandırılabilmelidir.

2.1.3. Donanım ve Yazılım Çeşitliliği

IPv6-GO tek bir üreticinin ürünlerinin yeteneğinden bağımsız olunabilmesi için açık kaynak kodlu ve ticari ürünleri barındıracak şekilde donanım ve yazılım çeşitliğine sahip olmalıdır.

2.1.4. Farklı Geçiş Yöntemlerinin Denenebilmesi

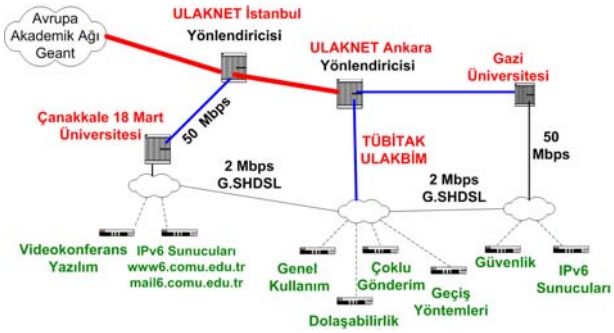
IPv6-GO yalın IPv6, tünelleme ve çevirici kullanımı geçiş yöntemlerinin test edilebilmesine imkan verecek şekilde, bu yöntemlerin oluşturulabileceği yazılım ve donanımı içermelidir.

2.1.5. IPv6 İleri Seviye Özelliklerinin Desteklenmesi

IPv6-GO dolaşılabilirlik, çoklu gönderim ve servis kalitesi gibi IPv6 ileri seviye özelliklerinin denenebileceği ve uygulanabileceği yazılımı ve donanımları içermelidir.

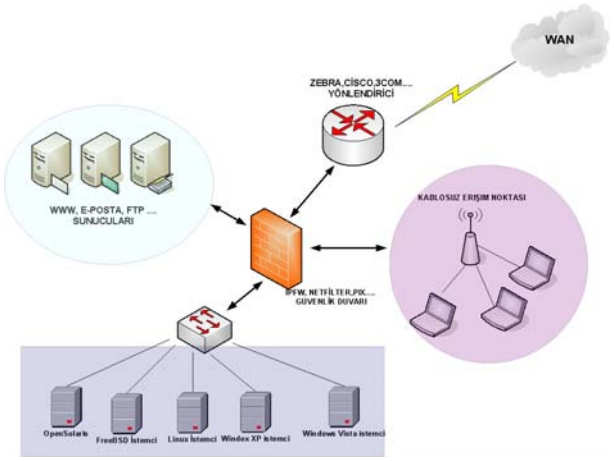
2.2. IPv6-GO Genel Topolojisi

IPv6-GO ULAKBİM, Gazi Üniversitesi ve Çanakkale Onsekiz Mart Üniversitesine konuşlandırılmıştır. Bu üç yerleşkedeki test laboratuvarları sırası ile 1000 Mbit/s, 50 Mbit/s ve 200 Mbit/s hızlar ile Ulusal Akdemik Ağ (ULAKNET) [1] omurgası üzerinden birbirlerine bağlıdır. Bununla birlikte trafiğin ağdan izole edilebimesi ve yalın IPv6 bağlantısı için ULAKBİM-Gazi Üniversitesi ve ULAKBİM- Çanakkale Onsekiz Mart Üniversitesi arasında 2 Mbit/s hızında G.SHDSL bağlantısı bulunmaktadır. IPv6-GO genel bağlanyı topolojisi Şekil 1' de verilmiştir.



Şekil 1IPv6-GO Genel Bağlantı Topolojisi

Üç yerleşkede konuşlanan test laboratuarları için örnek topoloji Şekil 2'de verilmiştir.



Şekil 2 IPv6-GO Örnek Laboratuar Topolojisi

2.3. IPv6-GO Donanımı

IPv6-GO test yatağındaki donanımlar bilgisayarlar (istemci ve sunucular), yönlendiriciler ve anahtarlama cihazı olmak üzere 3 başlıkta incelenebilir.

2.3.1. Bilgisayarlar

IPv6 araştırma laboratuarında farklı işletim sistemlerinin IPv6 yapılandırılması ve performanslarının incelenmesi hedeflenmiştir. Bu sebeple laboratuardaki bilgisayarlara farklı işletim sistemleri kurulmuştur. Test laboratuarlarında kullanılmak üzere Pentium 4 2.66 Ghz işlemci, 80 Gbayt Sabit disk ve 1 Gbayt bellek donanıma sahip 100

adet bilgisayar bulunmaktadır. ULAKBİM bünyesindeki IPv6-GO test laboratuarındaki ilk 13 bilgisayarın bilgileri örnek olarak Tablo 1'de belirtilmiştir.

Bilgisayar Adı	İşletim Sistemi
R1BSD	FreeBSD 7.1
H1BSD	FreeBSD 7.1
H2LINUX	Debian 4.0
H3NETBSD	NetBSD 5.0
H4LINUX	Debian 4.0
H5LINUX	Debian 4.0
H6OPENBSD	OpenBSD 4.4
H7SOLARIS	OpenSolaris 2008.11
H8XP	MS Windows XP SP3
H9XP	MS Windows XP SP3
H10PARDUS	Pardus 2008.2
H11SERVER2008	MS Windows Server 2008
H12SERVER2003	MS Windows Server 2003
H13BSD	FreeBSD 7.1

Tablo 1 ULAKBİM IPv6-GO Bilgisayar Listesi

Sunucu seçiminde en son teknolojik özelliklere sahip olması, yedekli çalışabilmesi göz önünde bulundurulmuştur. Sunucu 2U yüksekliğindedir ve fanları ve güç kaynağı yedeklidir. Disklerin yedekli olarak çalışabilmesi için RAID 1, 1+0, 5 ve 6 destekleyen 512 Mbayt belleğe sahip olan RAID denetleyicisi eklenmiştir. Bunun yanında sanallaştırma uygulamaların yüksek bellek ihtiyacı göz önünde bulundurularak sunucu belleği 36 Gbayt olarak alınmıştır. Sunucu işlemcilerin Intel'in en son sunucu ailesi işlemcisi olan Nahalem tabanlıdır. Alınan sunucunun teknik özellikleri Tablo 2'de belirtilmiştir.

Özellik	
İşlemci	Intel Xeon W5580
Bellek	36 Gbyte DDR3
Disk kapasitesi	2 x 160 Gbyte 15.000 RPM SAS + 2 x 1 Tbyte 72000 RPM SATA
RAID denetleyicisi	LSI Megaraid 512 Mbyte

Tablo 2 IPv6-GO sunucu teknik özellikleri

2.3.2. Yönlendiriciler

IPv6-GO test laboratuarında 5 tane Cisco 2620, 1 tane 2621, 2 tane 2611XM ve 1 tane 2600 model yönlendirici bulunmaktadır. Tüm yönlendiricilerin ağ üzerinden iletişimi için gerekli yapılandırmalar uygulanmıştır.

2620 model yönlendiricilerin IPv6 destekli IOS sürümlerini yükleyebilmeleri için bellekleri yükseltilmiş ve üzerlerindeki işletim sistemleri (IOS) IPv6 destekli sürüme yükseltilmiştir.

Bununla birlikte, yönlendiriciler üzerinde yapılacak denemelerde esneklik sağlanabilmesi ve üretici bağımsız deneylerin yürütülebilmesi için, IPv6-GO üzerine açık kaynak kodlu Quagga [2] yönlendiricileri konuşlandırılmıştır.

2.3.3. Anahtarlama Cihazları

IPv6-GO ana bağlantısı noktasını oluşturacak anahtarlama cihazının seçimi sırasında cihazında aşağıdaki özelliklerin olmasına dikkat edilmiştir.

- Yüksek kapasiteli tıkanmasız (non-blocking) anahtarlama kapasitesi
- Yeni nesil yüksek hızlı (10 Gbps) arabirimlere sahip olma
- OSI ağ katmanı 3 seviye çalışabilme (L3 Switch)
- Yönlendirme protokollerini IPv4 ve IPv6 olarak desteklenmesi (OSPF, EIGRP, BGPv4 , OSPFv3 EIGRPv6)
- İleri Seviye IPv6 özelliklerini desteklemesi (Çoklu gönderim, QOS, IPSec vb)
- 24 adet veya daha fazla sayıda arabirime sahip olma

2.4. Güvenlik Yapılandırması

IPv6-GO test yatağının güvenliğinin sağlanabilmesi için aşağıdaki önlemler alınmıştır.

2.4.1. Fiziksel Güvenlik

IPv6-GO ULAKBİM laboratuarı 7/24 kamera ile takip edilen ve yetkili personelinin giriş kartlarını kullanarak girebildiği sistem odasına kurulmuştur. Ayrıca sistem odasına giriş çıkış yapan kişiler kart bazlı takip edilmektedir. Benzer şekilde Gazi ve Çanakkale 18 Mart Üniversitesi'nde bulunan IPv6-GO laboratuarları da giriş/çıkışlar sadece yetkili kişiler tarafından yapılacak şekilde düzenlenmiştir.

2.4.2. Yönlendirici güvenlik yapılandırılması

Yönlendiricilerde konsoldan ve telnet ile uzaktan erişim için şifre uygulaması aktif hale getirilmiştir. Bununla birlikte erişim listesi (access list) tanımları yapılarak yönlendiricilere sadece IPv6-GO kullanıcılarına ait IP adreslerinden erişim yapılabilmesi için filtreler tanımlanmıştır. Cisco yönlendiricilerde tutulan parolaların yapılandırma dosyasında daha güçlü şifreleme algoritmaları ile saklanması için tüm yönlendiricilerde "service password-encryption" komutu kullanılmıştır.

2.4.3. İşletim sistemleri yama yönetimi

BSD tabanlı işletim sistemleri "cvsup" ve "portaudit" araçları kullanılarak güncellenmiş ve yüklü paketler güvenlik açıklarına karşı kontrol edilmiştir. Debian işletim sistemi yüklü bilgisayarlar "apt-get" paket yöneticisi kullanılarak güncellenmiştir. OpenSolaris yüklü bilgisayar "pfexec" komutu kullanılarak güncellenmiştir. Windows versiyonları yüklü işletim sistemlerinde otomatik güncelleme özelliği aktif hale getirilmiştir.

2.4.4. Güvenlik duvarı ve erişim kontrolü yapılandırması

IPv6-GO laboratuarı bünyesinde, kullanılmayan test bilgisayarlarının tutulduğu "test5" adlı sanal ağın ön tanımlı ağ geçidi olarak kullanılan R1BSD adlı bilgisayar üzerine "pf" [3] ateş duvarı uygulaması kurulmuştur. Ayrıca saldırı senaryoları denenmesi sürecinde kullanılan güvenlik açığı içeren bilgisayarların kontrol altında tutulabilmesi için "pf" ateş duvarı kullanılmıştır. Windows işletim sistemine yapılan saldırıları engellemek ama aynı zamanda otomatik güncelleştirmelere izin vermek amacıyla özel ateş duvarı kuralları yazılmıştır.

2.4.5. Saldırı Tespit sistemi yapılandırması

Açık kaynak kodlu BRO [4] ve Snort [5] saldırı tespit sistemlerinin kurulumu IPv6-GO'da gerçekleştirilmiştir.

2.4.6. Günlük izleme ve yönetim mekanizması

Günlük dosyalarının ortak bir sunucuda toplanması amacı ile "syslog-ng" programı kullanılmıştır.

2.4.7. Rootkit yakalama

Unix tabanlı bilgisayarlara bulaşacak rootkitlerin yakalanabilmesi için sunuculara "chkrootkit" [6], "rkhunter" [7] ve "lynis" [8] rootkit tarama programları kurularak düzenli olarak sistemlerin taranması sağlanmıştır.

2.4.8. Dosya bütünlük doğrulama

Kritik işletim sistemi dosyalarında yapılacak olan değişikliklerin sistem yöneticilerine iletilebilmesi için betikler yazılarak sunuculara yüklenmiştir.

3. IPV6-GO TEST SENARYOSU YAPILANDIRMASI

3.1.1. İsimlendirme

Bilgisayarların belli bir düzen dâhilinde kullanılabilmesi için laboratuar kapsamında standart bir isimlendirme kullanılmıştır. Bu amaçla bilgisayarlara verilen isimler 3 bölümden oluşmaktadır. Birinci bölüm, ilk harf (R veya H), test bilgisayarının yönlendirici olup olmadığını - işletim sisteminde paket yönlendirme özelliğinin açık olup olmadığını - belirtmektedir. R (Router) bilgisayarın yönlendirme özelliğinin olduğunu, H (Host) ise bilgisayarın sadece istemci olduğunu göstermektedir. İkinci bölüm numaralandırmadır. Her eklenen bilgisayar ile birlikte sayı 1 artırılmıştır. Son bölüm ise bilgisayarda kurulu işletim sistemi hakkında bilgi vermektedir. Örneğin, R1BSD üzerinde FreeBSD işletim sistemi bulunan bir yönlendirici iken H3NETBSD üzerinde NetBSD işletim sistemi kurulu bir istemcidir.

3.1.2. Test Senaryosu Yapılandırması

IPv6-GO laboratuarında farklı senaryoların uygulanabilmeleri için bilgisayar, yönlendirici, anahtarlama cihazı ve sunucuların yapılandırmalarının otomatik olarak gerçekleştirilebileceği bir yapı oluşturulmuştur. İlk aşamda, IPv6-GO ekipmanlarının tümü standart olarak yapılandırılmış ve bu yapılandırma ayarları ".ori" uzantılı açılış dosyalarına kaydedilmiştir.

Sunucu ve Bilgisayarlar.
BSD ve LINUX yüklü makinelerde işletim sisteminin yüklenmesi sırasında açışışta başlatılacak servisler, ağ arabirimlerin yapılandırmaları ve benzeri temel ayarlar "rc.conf" ve "rc.local" dosyalarında saklanmaktadır. Bilgisayarların standart yapılandırmaları sırasıyla "rc.conf.ori" ve "rc.local.ori" dosyalarına yedeklenmiştir. Yeni bir test senaryosu oluşturulurken, öncelikle bu senaryoda yer alcak donanımlarda ilgili yapılandırmalar gerçekleştilmektedir. Daha sonra tüm donanımlardaki yapılandırma ayar dosyaları "ayar_dosyası_adı.senaryo_adı" şeklinde yedeklenerek aynı senaryonun tekrar edilmesi gerektiğinde hızlıca bu senaryoya dönüş sağlanmaktadır. Örneğin, test laboratuarında daha önceden denenmiş olan saldırı1 senaryosuna tekrar ihtiyaç duyulduğunda rc.local.saldırı1 ve rc.conf.saldırı1 dosyalarını orjinal yerlerine kopyalayıp cihazları yeniden başlatmak yeterli olmaktadır.

Anahtarlama Cihazları ve Yönlendiriciler
Benzer bir şekilde, bu modüler yapılandırma anahtarlama cihazında ve yönlendiricilerde de uygulanmaktadır. Yönlendirici ve anahtarlama cihazlarının yapılandırmaları senaryo ismi uzantısı ile tftp sunucusunda saklanmaktadır. Senaryo tekrar deneneceği zaman tftp sunucusundan senaryonun yapılandırma dosyası yönlendircinin açılış dosyasına kopyalanmaktadır.

Sanal Ağ (Vlan) Yapılandırması
Anahtarlama cihazında 5 adet sanal ağ (VLAN) oluşturulmuştur. Herhangi bir teste dahil olmayan ekipmanlar test5 sanal ağında bulunmaktadır. Labaratuarda bulunan tüm cihazların anahtarlama cihazında bağlı bulundukları fiziksel port bilgisi bir tabloda tutulmaktadır. Herhangi cihazın test senaryosu

için yeni bir ağa dahil edimesi gerektiğinde fiziksel olarak anahtarlama cihazındaki bağlı bulunduğu portun değiştirilmesi yerine, o portun ait olduğu sanal ağ numarası değiştirilmektedir.

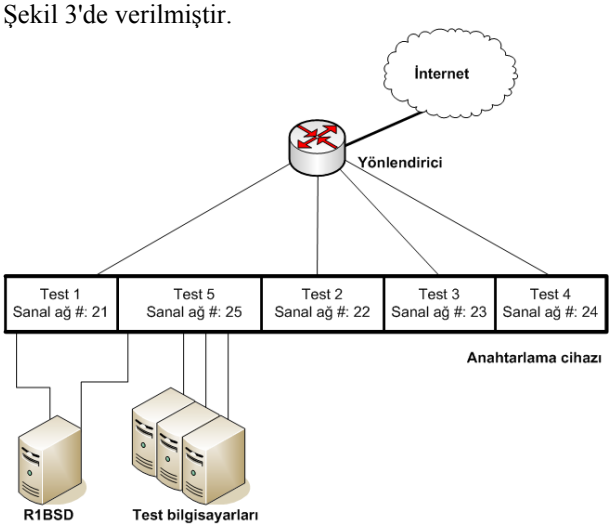
3.1.3. Uzaktan Erişim

IPv6-GO kapsamında kurulan test laboratuarları herhangi bir güvenlik açığına yol açmadan uzaktan erişilebilir olmalıdır. Bu amaçla Unix tabanlı işletim sistemlerinde SSH ile uzaktan erişim aktif hale getirilmiştir. Test ortamına bağlanacak kullanıcıların her bilgisayar için farklı şifre kullanma zorluğunun önüne geçebilmek için kullanıcı doğrulaması açık anahtar altyapısı ile yapılmıştır. Windows tabanlı işletim sistemlerinde de uzaktan erişim aktif hale getirilmiştir. Windows sistemlerin erişime açılması Windows işletim sistemi ile birlikte gelen ve RDP protokolü kullanan uzak masaüstü ile gerçekleştirilmiştir.

3.2. IPv6-GO Örnek Test Senaryosu

Bu bölümde IPv6 kullanılarak gerçekleştirilen uygulama düzeyinde bir saldırının gerçekleştirilmesi ve saldırı aşamalarının takip edilmesi için oluşturulan topolojiye yer verilmiştir. Önceki bölümlerde anlatılan sanal ağ yapısı ve bilgisayarlarda kullanılan isimlendirme gibi bileşenlerle oluşturulan modüler yapının bir uygulaması sunulmaktadır.

Anahtarlama cihazında oluşturulan sanal ağ yapısı Şekil 3'de verilmiştir.

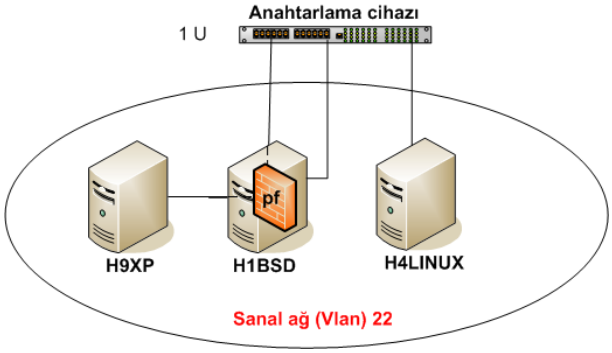


Şekil 3 IPv6-GO sanal ağ yapısı

Bu yapı ve eşleşme bilgisi kullanılarak istenilen test için gerekli olan topoloji kısa sürede hazırlanabilmektedir. Gerekli olan topolojiyi kurmak için aşağıdaki işlemler gerçekleştirilmektedir.

1. Bilgisayarlar üzerindeki ilgili ağ ayarlarını içeren dosyalar (.ori uzantılı dosyalar korunarak) değiştirilmektedir.
2. Kullanılacak bilgisayarların bağlı olduğu portlar, topoloji için kullanılacak olan sanal ağa dâhil edilmektedir.

IPv6 üzerinde uygulama seviyesinde saldırı testi için düzenlenen senaryonun detayları ise Şekil 4'te verilmiştir.



Şekil 4 IPv6-GO test senaryo topolojisi

Bu senaryoda H9XP (Windows XP), H4LINUX (Debian) ve H1BSD (FreeBSD) adlı bilgisayarlar kullanılmıştır. H9XP'ye gelen trafik, H1BSD adlı bilgisayar tarafından izlenmiş ve bu bilgisayar üzerinde kurulu pf ateş duvarı ile kontrol edilmiştir. Saldırı H4LINUX adlı bilgisayardan gerçekleştirilmiştir. Senaryoda kullanılan bilgisayarlar 22 numaralı sanal ağa geçirilmiş ve ilgili ayar dosyaları .saldiri1 uzantısı ile kayıt edilmiştir. Bu senaryo tekrar gerçeklenmek istenildiğinde bu ayar dosyasını kullanmak yeterli olmaktadır.

4. DİĞER İSS'LER İLE BAĞLANTILAR VE IPV6-DN (DEĞİŞİM NOKTASI)

IPv6-GO test laboratuarının bir amacı da Türkiye'de IPv6 kullanımını yaygınlaştırmak ve deneme amaçlı IPv6 ağına bağlanmayı talep eden kurumlara yardımcı olmaktır. Bu amaç doğrultusunda diğer İnternet Servis Sağlayıcılar (İSS) ile bağlantı sağlanabilmesi için "IPv6 Üzerinden İnternet Trafiği Değişim Noktasına Bağlantı Protokolü" hazırlanmış ve bu protokolü imzalayan aşağıdaki İnternet Servis Sağlayıcılar ile IPv6 bağlantısı sağlanmıştır.

Koç-Net ile ULAKNET arasında, Koç-NET tarafında G.SHDSL, ULAKNET tarafında Metro Ethernet

teknolojisi ile sonlandırılmak üzere bir devre tesis edilmiştir. Bu devre üzerinden tünelleme yöntemi kullanılarak IPv6 bağlantısı yapılmıştır.

Meteksan-Net ile IPv6 bağlantısı her iki tarafta Ethernet arayüzlerinde sonlandırılan doğrudan fiber bağlantısı üzerinden, "dual stack" yöntemi ile gerçekleştirilmiştir.
Bağlantı üzerinde kurulan iki ayrı BGP oturumu aracılığıyla IPv4 ve IPv6 rotalarının karşılıklı olarak değişimi sağlanmaktadır

Superonline-Net ile IPv6 bağlantısı Superonline ile ULAKNET İstanbul omurga yönlendiricisi arasında tesis edilen doğrudan fiber-optik bağlantı üzerinden yalın IPv6 yöntemi ile gerçekleştirilmiştir. Devre üzerinde IPv6 için BGP oturumu kurulmuş olup Superonline rotalarının GEANT aracılığı ile Global IPv6 ağına anons edilmesine başlanmıştır.

ULAKNET ile ADA-NET arasında IPv6 Trafik Değişimi Protokolü karşılıklı olarak imzalanmış olup devresin tesisi için Türk Telekom'a gerekli başvurular yapılmıştır. Devrenin kurulumunun kısa süre içinde tamamlanması beklenmektedir.

5. SONUÇ

"Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi" kapsamında, Türkiye'de IPv6 kullanımını yaygınlaştırmak, IPv6 geçiş yöntemleri ile ilgili test ve güvenlik analizleri yapmak ve IPv6 tabanlı uygulamaların testlerini gerçekleştirmek amacıyla TÜBİTAK ULAKBİM, Gazi Üniversitesi ve Çanakkale 18 Mart Üniversitesi bünyesinde IPv6-GO test laboratuarları kurulmuştur. Bu test laboratuarlarının kurulması ile oluşacak bilgi birikimi ile üniversiteler, araştırma kurumları ve sanayi kuruluşlarındaki ar-ge faaliyetlerinin desteklenmesi hedeflenmektedir. Bu çalışmada IPv6-GO test laboratuarı kurulumu ve kullanımı ile ilgili elde edilen tecrübeler paylaşılmıştır. Proje kapsamında halen geçiş senaryolarının ve IPv6 ileri seviye özelliklerinin test uygulamaları devam etmektedir.

Teşekkür

Bu çalışma Türkiye çapında IPv6 altyapısı oluşturmak ve Türkiye'nin IPv6 protokolüne geçişini planlamak amacıyla TÜBİTAK – ULAKBİM'in yönetici, Gazi Üniversitesi ve Çanakkale 18 Mart Üniversitesi'nin yürütücü, Bilgi Teknolojileri ve İletişim Kurumu'nun müşteri kurum olarak katıldığı "Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi" kapsamında gerçekleştirilmiştir. [9] Bu proje TÜBİTAK tarafından desteklenmektedir.

6. KAYNAKÇA

[1] Ulusal Akademik Ağ (ULAKNET), http://www.ulakbim.gov.tr/ulaknet/
[2] Quagga, http://www.quagga.net/
[3] PF (Packet Filter) ateş duvarı, http://www.openbsd.org/faq/pf/
[4] Bro Saldırı Tespit Sistemi, http://www.bro-ids.org/
[5] Snort Saldırı Tespit Sistemi, http://www.snort.org/
[6] Chkrootkit rootkit tarama betiği, http://www.chkrootkit.org/
[7] Rkhunter rootkit tarama betiği, http://rkhunter.sourceforge.net/
[8] Lynis rootkit tarama betiği, http://www.rootkit.nl/projects/lynis.html
[9] TÜBİTAK - ULAKBİM, Gazi Üniversitesi ve Çanakkale 18 Mart Üniversitesi, Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi, http://www.ipv6.net.tr/