TCP/IP'nin DÜNÜ, BUGÜNÜ, YARINI

Ayhan AKBAL
Fırat Üniversitesi
Mühendsilik Fakültesi
Elektrik-Elektronik Müh.Bölümü
ayhanakbal@gmail.com

Hasan. H. BALIK
Fırat Üniversitesi
Mühendislik Fakültesi
Elektrik-Elektronik Müh. Bölümü
hasanbalik@gmail.com

ÖZET

TCP/IP, bilgisayarların kişi ve kurumlardan bağımsız çalışabilmelerini sağlayan ve geniş bir kullanım alanı olan bir protokol kümesidir. İnternet TCP/IP nin kullanıldığı en bilinen uygulamalarından biridir. Internet gerçek küresel bir ortam haline gelirken, çeşitli servisleri sağlam bir şekilde destekleme yeteneğine sahip bir ağ oluşturmak için yeniliklere ihtiyacı vardır. Bu yayında, bu çerçevede geliştirilen IPv6 standardı, teknik özellikleri, adres yapısı, IPv4 ' e göre üstünlükleri, IPv6 'ya neden ihtiyaç duyulduğu ve bu gelişmeler ile birlikte İnternetin geleceği üzerinde durulmuştur.

ABSTRACT

TCP/IP is a set of protocols by which computers can work indipendant from users. Internet is a most commonand well-known usage of TCP/IP. In this contribution, standarts, technical features, address structure of IPv6 will be explained. In addition advantages of IPv6 againet IPv4 and the feature of internet will be explained.

Anahtar Kelimeler: IPv6, IPv4, İnternet, TCP/IP

1. GİRİŞ

İnternetin kökleri 1962 yılında J.C.R. Licklider' in Amerika'nın en büyük üniversitelerinden biri olan Massachusetts Institute of Technology' de (MIT) tartışmaya açtığı "Galaktik Ağ" kavramı ile ilk olarak ortaya atılmıştır[1]. Licklider, bu kavramla küresel olarak bağlanmış bir sistemde isteyen herkesin herhangi bir yerden veri ve programlara erişebilmesini ifade etmiştir. MIT' de araştırmacı olarak çalışan Lawrence Roberts ile Thomas Merrill, bilgisayarların ilk kez birbirleri ile 'konuşmasını' 1965 yılında gerçekleştirmiştir[1].

1966 yılı sonunda Roberts DARPA' da çalışmaya başlamış ve "ARPANET" isimli proje önerisini yapmıştır. ARPANET çerçevesinde ilk bağlantı 1969 yılında dört merkezle yapılmış ve ana bilgisayarlar arası bağlantılar ile internetin ilk şekli ortaya çıkmıştır. ARPANET' i , University of California at Los Angeles (UCLA), Stanford Research Institute (SRI), University of Utah ve son olarak University of California at Santa Barbara (UCSB) oluşturan ilk dört merkez olmuştur.

Kısa süre içerisinde birçok merkezdeki bilgisayarlar ARPANET ağına bağlanmıştır. 1971 yılında Ağ Kontrol protokolü (NCP-Network Control Protocol) ismi verilen bir protokol ile çalışmaya başlamıştır. 1972 yılı Ekim ayında gerçekleştirilen Uluslararası Bilgisayar İletişim Konferansı (ICCC- International Computer Communications Conference) isimli konferansta, ARPANET 'in NCP ile başarılı bir gösteri gerçekleştirmiştir. Yine aynı yıl içinde elektronik posta (e-mail) ilk defa ARPANET içinde kullanılmaya başlanmıştır. NCP' den daha fazla yeni olanaklar getiren yeni bir protokol, 1 Ocak 1983 tarihinde İletişim Kontrol Protokolü (Transmission Control Protocol/ Internet Protocol - TCP/IP) adıyla ARPANET içinde kullanılmaya başlanmıştır. TCP/IP (IPv4) bugün var olan internet ağının ana halkası olarak yerini almıştır. Günümüz interneti IP protokolünün 4. sürümü (IPv4) üzerine kurulmuştur ve IPv4 sınıf (class) sistemine dayalı bir sözleşmedir.

Sınıf	Ağ Sayısı	Adres Sayısı
A	*125*	*16 miyon*
B	*16382*	*65534*
C	*2milyon*	*256*
D	*Multicast kullanım için ayrılmıştır*	
E	*Gelecekte kullanım için ayrılmıştır*	

Tablo 1. IPv4 Sınıfları

IPv4 sistemi kurumsal olarak 4 milyar farklı adrese imkan tanıyan bir protokol olmasına rağmen sınıf sistemi nedeniyle verimli kullanılamamaktadır. Örneğin bir şirket IP bloğu için başvurduğunda hepsini kullanabilecek kapasitesi olmamasına rağmen en az 256 IP'lik bir C sınıfı almak zorundadır. 1980'li yıllarda 4 milyar adresin yetmeyeceği düşünülmemiştir.

Günümüzde halen internet protokolü olarak kullanılan IPv4, bilgisayarların iletişim sırasında uçtan uca adreslenebilmesini sağlamaktadır. IPv4 adresleri 32 bit ve teorik olarak 4.294.967.296 adet dir. Ancak pratikte verimsiz adres atama mekanizmalarından dolayı etkin adres sayısı bu sayıya hiçbir zaman ulaşamamaktadır. 1990 lı yıllarda patlayan internetteki host sayısındaki ve web sayfalarındaki artış nedeniyle IPv4, ihtiyacı karşılamakta yetersiz kalmaya

başlamıştır. Bu problemler karşısında IPv4 adreslerinin etkin kullanımı için çeşitli yöntemler geliştirilmiştir. İnternet üzerindeki IP'lerin standardını sağlayan CIDR (Classless Inter Domain Routing), IPv4 adres bloklarının değişken boyutlarda olmasına izin vermesiyle aynı adresin farklı zamanlarda farklı bilgisayarlarca kullanımına olanaklar sağlayan DHCP(Dynamic Host Configuration Protocol) v.b. tekniklerin gelişmesini sağlamıştır. Bu tekniklerde yetersiz gelmeye başlayınca değişik çözümler aranmış ve en sonunda IPv4' e bir yama yapılarak sistemin günümüzde ayakta kalması sağlanmıştır. Bu yama NAT (Network Address Translator) adı ile internet mimarisine bütünleşmiştir. NAT' ın amacı, üzerinde barındırdığı bir IPv4 adresini birden çok bilgisayarın paylaşımına sunmaktadır. Bu bilgisayarlar ile internet arasında bir geçit görevi yapan NAT, İnternet mimarisinin en temel prensiplerinden olan uçtan uca adresleme ve paket bütünlüğünü ortadan kaldırmıştır. IPv4 adres sayısının azlığı ancak bu yama ile geçici olarak çözülmüştür. Ancak bu yöntemin yarardan çok zarar getirdiği kısa zamanda anlaşılmıştır. NAT üzerinden istemci-sunucu (server-client) iletişiminin sadece tek yönlü işleyebilmesi, IPsec gibi güvenlik bağlantılarının sağlanamaması ağların sınırlı ölçeklenirliği, yönetim zorlukları gibi problemler ortaya çıkmıştır.

Bu nedenle 1981 yılından beri kullanılan IPv4 'ün artık çeşitli yamalar ile iyileştirilemeyeceği açıkça görülmüş ve IPv6 adı ile tamamen yeni bir altyapı protokolü ortaya çıkmıştır

2. IPv4' ün İHTİYAÇLARI

İnternetin yaygınlaşması, IPv4' ünde yaygınlaşmasını beraberinde getirdi. Kullanıldıkça IPv4' ün eksikleri ve yeni ihtiyaçlar ortaya çıkmaya başlamıştır. Ortaya çıkan bu durumların başlıcalar aşağıda sıralanmış ve çözüm yolları belirtilmiştir.

- *Veri Doğrulama:* Alıcı eğer kaynak adresi belli bir IP'den paket alıyorsa gerçekten bu paketin o adresten geldiğine emin olmalıdır (IPspoff saldırıları).
  Çözüm: SA (Security Associations)

- *Data Bütünlüğü*: Alıcı bir paket aldığında bunun kaynaktan gelene kadar değişmediğine veya açılmadığına emin olmalıdır
  Çözüm: Authentication Header

- *Data Şifrelemesi:* Alıcının bir paket aldığında yol boyunca bu paketin seyrettiği süre zarfında açılıp okunmadığına emin olmalıdır.
  Çözüm: : ESP (Encapsulated Security Payload)

- *Hiyerarşik Adresleme Eksikliği:* Kullanılmakta olan IPv4 sistemi, internet omurgasına bağlı ağ trafiğini sınıflandırmak için bir adres hiyerarşisi kullanmaktadır. Bir adres hiyerarşisi olmadığı takdirde yönlendirme bilgilerinin bütün ağların ulaşabileceği bir yere konması gerekmektedir. İnternetin kullanımının hızla arttığı bir ortamda böyle bir uygulamaya gitmenin imkânsız olduğu açıktır. Adres hiyerarşisi kullanılarak omurga yönlendiricileri, IP adresi eklerini kullanarak trafiğin geçişini yönlendirebilmektedirler. Ancak kullanılmakta olan hiyerarşi sisteminin tek çeşit olmaması ve IPv4 adreslerinin dikkatli dağılma gereksinimi, internet adresleme ve yönlendirmesini gittikçe zorlaştırmaktadır. Bunun yanı sıra IPv4 sitelerinin yeniden numaralanması da pratik olmayan ve maliyeti artıran bir uygulamadır. Sonuç olarak internet'in hızla büyüyen adres kıtlığı problemi ve NAT yüzünden girmiş olduğu sağlıksız gelişim.
  Çözüm: : *IPv6* → (Internet Protocol version 6)

3. IPv6 PROTOKOLÜ

Internet protokollerinden sorumlu Internet Engineering Task Force (IETF) 1990 yıllarının başında yeni bir çalışma grubu kurulmuş ve o zamanki adıyla IPng (Internet protocol, next generation) çalışma grubu , yeni IP protokolünün geliştirilmesi görevini üstlenmiştir. İnternet mimarisinin temel prensiplerinin korunarak sağlıklı gelişiminin sağlanması ve yeni uygulamaların önünün açılabilmesi için IP protokolünün yeni bir sürümünün geliştirilmesi öngörülmüştür. Yaklaşık 10 yılı aşkın bir süredir endüstri, akademi, hükümetler ve çeşitli organizasyonların ortak çalışması sonucu IPv6 protokolü oluşmuştur.

IPv6 protokolü, IETF' in yayınlamış olduğu bir seri RFC dokümanı vasıtasıyla tanımlanmıştır. IPv6'yı IPv4'ten ayıran en temel özellik 128 bitlik genişletilmiş adres alanıdır. Bu genişlemenin sağlamış olduğu teorik adreslenebilir düğüm sayısı 340.282.366.920.938.463.463.374.607.431.768.211.456 adettir. Böylesine geniş bir adres alanının şu an yaşadığımız adres sıkıntısını çözmenin yanında internet uygulamalarında yeniliklere de yol açması beklenmektedir. Öte yandan, IP üzerinde yapılan değişiklikler sadece bununla da kalmayıp, protokolün tam anlamıyla tekrar gözden geçirilmesi ve yenilenmesi de söz konusu olmuştur. Bunlar arasında basitleştirilmiş ve 64 bitlik işlemcilere göre düzenlenmiş paket başlığı paket bölünmesinin sadece uç noktalarda yapılacak olması yönlendiricilerin veri trafiğini daha seri bir şekilde işleyebilmesi için yapılan değişikliklerdir. Temel IP başlığının yanı sıra ihtiyaca göre eklenebilir uzantı başlıklarının tanımlanabilmesi protokolün esnekliğini artıran bir faktör olmuştur. Güvenlik için IPsec (IP Security protocol) şartı da IPv6 ile gelen özellikler arasında yer almaktadır.

128 bitten oluşan IPv6 adreslerinin ilk 64 bitlik kısmı alt ağı adreslemek için kullanılan adres blok bilgisini içermektedir. Adres bloğu, bir paketin varacağı son

bağa kadar olan yolda yönlendirilmesini sağlamaktadır. Geriye kalan 64 bit ise bu bağa vardığında paketin son alıcısının tespitinde kullanılmaktadır. IPv6 adresleri 16'lık bir düzende aşağıdaki gibi ifade edilir.

2045:ab28::6cef :85a1:331e:a66f:cdd1

6 bitlik gruplar birbirlerinden " : " ile ayrılır. Ardı ardına gelen iki " : " sadece bir kereye mahsus kullanılabilir ve aralarında kalan bütün hanelerin sıfır değerini taşıdığını ifade etmektedir. IPv6 adresleri bağ içi (link-local) ve evrensel (global) olmak üzere iki çeşittir. Bunlara ek olarak site içi adresler de tanımlanmış olmasına rağmen, IPv6 çalışma grubu bu adresleri mimariden çıkarma kararı almıştır. Bağ içi adresler sadece özel amaçlarla kullanılır ve bu adresleri taşıyan paketler yönlendiriciler tarafından asla diğer bağlara iletilmezler. IPv4'te sıkça kullanılan herkese gönderim (Broadcast) adresleri, görevleri çoklu gönderim (Multicast) adresleri tarafından üstlenildiği için IPv6 mimarisinde yer almaz. Herhangi birine gönderim adresleri (anycast) IPv6'nın getirmiş olduğu yenilikler arasındadır. Bu tip adreslere gönderilen paketler, birden çok düğümden sadece birine varacak şekilde yönlendirilmektedir. Kullanımda birden çok düğüm aynı adresi paylaşması açısından çoklu gönderim adreslerine benzemekle birlikte, paketin sonunda sadece tek bir düğüme ulaşması açısından tekil gönderime benzemektedir[2].

Otomatik adres yapılandırması, IPv6'nın getirmiş olduğu önemli yeniliklerdendir. Ağ üzerindeki adres atama görevini üstlenmiş bir DHCP ya da PPP sunucusu olmaksızın ağa bağlı düğümlerin kendilerince adres edinmelerine olanak tanımaktadır. Otomatik IP alma işlemi ağdaki yönlendiricilerin gerekli adres bloğunu anons etmeleri ve düğümlerinde bu bloğa kendilerinden 64 bitlik bir değer eklemeleriyle oluşmaktadır. Bu şekilde oluşturulan adreslerin kullanılmadan önce tekillik testinden geçirilmesi gerekmektedir. Düğümler başkaları tarafından kullanılmadığından emin oldukları adresi kullanabilirler.

IP protokol başlığında ise büyük değişiklikler olmuştur. IPv4'te var olan protokol başlık büyüklüğü, kimlik bilgisi, paket parçası bilgisi, başlık sağlama toplamı bilgileri kaldırılmıştır. IPv6 başlığına yeni olarak akış bilgisi eklenmiş, tipik 20 bayt genişliğindeki IPv4 başlığının yerini 40 baytlık IPv6 başlığı almıştır. Temel IPv6 başlığına ek olarak, özel amaçlara yönelik yönlendirme, paket bölmesi, şifreleme ve mobil uzantı başlıkları tanımlanmıştır. Zaman içerisinde ihtiyaç oldukça bunlara yenilerinin eklenmesi de mümkün kılınmıştır. Yönlendirme alanında temel prensiplerde bir değişiklik olmamakla birlikte var olan RIP, OSPF, IS-IS, MP-BGP, PIM-SM, PIM-SSM gibi protokoller IPv6 adreslerini işleyebilecek şekilde güncellenmiştir[2].

Çoklu gönderim için kullanılan IGMP'nin yerini yeni geliştirilen MLD almıştır. Alan adlarının kaydından sorumlu DNS, artık IPv4 adreslerinin yanı sıra IPv6 adreslerini de barındıracak şekilde düzenlenmiştir. IPv4 adresleri A tipi kayıtlarda saklanırken, AAAA tipi kayıtlar IPv6 adreslerine tahsis edilmiştir. IPv6'yı destekleyen bir DNS sunucusu üzerinde bir alan adı aynı zamanda hem IPv4 hem de IPv6 adreslerine atanabilmektedir.

IPv4'ün hareketlilik protokolü Mobil IPv4'e karşılık olarak Mobil IPv6 geliştirilmiştir. Aralarında uygulamada öne çıkan farklılıklar olmasına rağmen bu iki protokol ana hatlarıyla birbirine benzemektedir.

3.1. IPv6 ADRES UZAYI

IPv6'nın getirdiği en büyük yenilik daha kapsamlı adreslemedir. 128 bitlik IPv6 adresleme 32 bitlik IPv4 adresinin 4 katı daha uzundur. IPv4 de 2^{32} olası adres varken IPv6 'da bu rakam 2^{128} dır. 1970 lerin sonlarında IPv4 tasarlanırken bir gün yetersiz gelebileceği hayal bile edilememiştir. Ancak teknolojideki gelişmeler sonucunda 1992 yılında bu yetersizlik kabul edilmiştir. Geçerli paylaşım; IPv4 adresinin Unicast ve Multicast adres gruplarına ayrılması gibi IPv6 adresleri de yüksek değerli bitlerine göre gruplara ayrılır. 32 bitlik IPv4 adresi 8 bitlik 4 gruba ayrılırken 128 bitlik IPv6 16 bitlik 8 gruba ayrılır. Bu gruplar hexadecimal olarak ifade edilir.

3.2. IPv6 ADRES TİPLERİ

3.2.1 ÜNİCAST IPv6 ADRESLERİ

Evrensel adreslerde FP*(Format Prefix*) 001 olarak tanımlanmaktadır. Bir evrensel adresin kapsamı tüm IPv6 internetini içine almaktadır. Tablo 3.1 de bir evrensel unicast adresin yapısı gösterilmiştir.

TLA ID: Üst seviye gruplama tanımlayıcısı, bu bölümün uzunluğu 13 bittir.
Res: TLA veya NLA IP'de ileride meydana gelebilecek ilerlemeler için rezerve edilmiş 8 bittir.
NLA ID: Sonraki seviye gruplama tanımlayıcısı, bu bölüm uzunluğu 24 bittir.

FP, NLA, TLA ve Res 'in oluşturduğu toplam 48 bitlik alan firma bilgisini içerir.

SLA ID: Site seviyesi gruplama tanımlayıcısı; bu bölüm 16 bitliktir. Alt ağlama bilgisi içerir.

Interface ID: Alt ağa ait ara yüzüdür, 64 bittir. IPv4'deki düğüm ID veya IP'nin karşılığıdır.

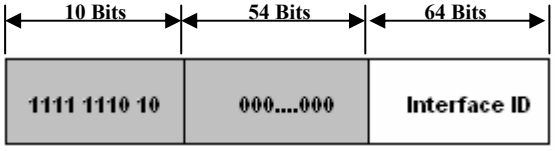
Allocation	Format Prefix (FP)	Fraction of the Address Space
Reserved	0000 0000	1 / 256
Unassigned	0000 0001	1 / 256

Reserved for Network Service Access Point (NSAP) allocation	0000 001	1 / 128
Unassigned	0000 010	1 / 128
Unassigned	0000 011	1 / 128
Unassigned	0000 1	1 / 32
Unassigned	0001	1 / 16
Aggregatbale global unicast addresses	001	1 / 8
Unassigned	010	1 / 8
Unassigned	011	1 / 8
Unassigned	100	1 / 8
Unassigned	101	1 / 8
Unassigned	110	1 / 8
Unassigned	1110	1 / 16
Unassigned	1111 0	1 / 32
Unassigned	1111 10	1 / 64
Unassigned	1111 110	1 / 128
Unassigned	1111 1110 0	1 / 512
Link Local unicast Addresses	1111 1110 10	1 / 1024
Site Local unicast Addresses	1111 1110 11	1 / 1024
Multicast Addresses	1111 1111	1 / 256

Tablo 3.1: IPv6 Adres Uzayı

3.2.1.1 Yerel Bağlantı Adresleri:

Bu adreslerde FP 1111 1110 10 olarak tanımlıdır ve aynı bağlantı üstündeki komşu düğümler için kullanılmaktadır. Bir yerel bağlantı adresinin yapısı aşağıdaki şekildeki gibidir.



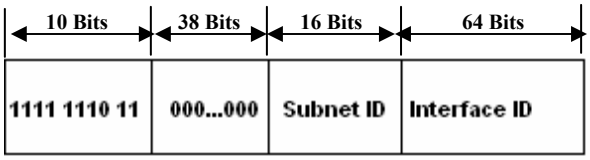
Şekil 3.1 Bir Yerel Bağlantı Adresinin Yapısı

Yerel bağlantı adresleri her zaman FE80 ile başlarlar.

3.2.1.2 Yerel Site Adresleri

Yerel site adresleri 111.1110.11 olarak tanımlanmaktadır. IPv4 'teki özel adres alanlarına (10.0.0.0/16)karşılık gelmektedir. Evrensel adreslerle çakışma olmadan kullanılabilmektedir. Bir yerel site adresin yapısı Şekil 3–2 deki gibidir;

Farklı olarak bu adresler otomatik düzenlenmemektedir, elle atanmaları gerekmektedir.



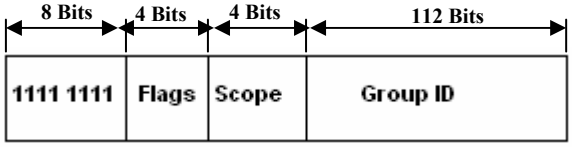
Şekil 3-2 Bir Yerel Site Adresin Yapısı

Görüldüğü üzere evrensel adresler ve yerel site adresler ilk 48 bit hariç olmak üzere aynı yapıya sahiptirler.

3.2.2 MULTİCAST IPv6 ADRESLERİ

IPv6'da Multicast trafik aynı IPv4'de olduğu şekilde işlemektedir. Keyfi yerleştirilmiş IPv6 düğümleri keyfi bir IPv6 Multicast adresinde Multicast trafiği dinleyebilmektedir. Aynı zamanda IPv6 düğümleri Multicast adreslerini çoğullamada kullanılmaktadır. Düğümler herhangi bir zamanda Multicast gruplarına katılıp ayrılabilmektedir.

IPv6 Multicast adresleri 11111111 lik FP'ye sahiptirler. Bundan dolayı bir IPv6 Multicast Adresi her zaman FF ile başlar. Multicast adresleri kaynak adresleri ya da yönlendirme başlığındaki orta derece hedefler olarak kullanılmamaktadır. FP'nin ardından Multicast adresleri bayrakları onların sahalarını ve Multicast gruplarını tanımlayan ilave yapılar içermektedir. Aşağıdaki şekil IPv6 Multicast adresinin yapısı gösterilmektedir.

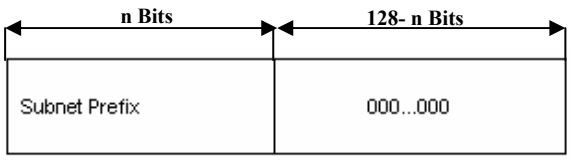


Şekil 3.3 IPv6 Multicast Adresin Yapısı

3.2.3 ANYCAST IPv6 ADRESLERİ

IPv6 ile birlikte ortaya çıkan bu kavram, multicast ara yüzleri çoğullamak için kullanılmaktadır. Bir anycast adrese gönderilen paketler anycast adresin atandığı en yakın ara yüze yönlendirici tarafından iletilmektedir.

3FFE:2900:D005:6187:2AA:FF:FE89:6B9A anycast adresi için sağlayacağı yönlendirmeleri organizasyonun atadığı 48 bit 3FFE:2900:D005::/48 öneki yönlendirici ara yüzden yayılmaktadır. Bu anycast adresin atadığı bir düğüm organizasyonun intranetinde herhangi bir yere yerleştirilebildiğinden, hedef yönlendirmelerinde bütün düğümler için atanmış bu anycast adreslerine organizasyondaki tüm routerlerin yönlendirme tablolarında bulunmalıdır. IPv6 internetin yönlendirici ara yüzüne ihtiyaç duymayan bir organizasyonun intranetindeki en yakın anycast grup üyesine IPv6 paketlerini ulaştırmak zorundadır. Anycast adresleri sadece hedef adresleri olarak kullanılabilir ve sadece routerlere atanmaktadır[3]. Anycast adresler unicast adres boşluklarının dışında atanırlar ve anycast adresin atandığı tipteki unicast adresin sahası, bir anycast adresin sahasıdır. Eğer verilen hedef unicast adres aynı zamanda bir anycast adresi ise tanımlamak mümkün değildir. Bunun farkında olan düğümler kaynak yönlendirmelerini, anycast trafiği en yakın anycast grup üyesine aktarmak için kullanılmaktadır.



Şekil 3.4 Bir Alt Ağ Router Anycast Adres Yapısı

4. IPv6'ya NE ZAMAN GEÇİLMELİ

4.1 IPv6 Geçiş Süreci

ACM'in (Association for Computing Machinery), SIG (Special Interest Group) konferansında (SIGCOMM99), AT&T'nin bilimsel araştırmalar yöneticilerinden Sandy Fraser, Internet mimarisine ilişkin endişelerini dile getirmiş, ölçeklenebilir mi? Niye hâlâ IPv4'ten IPv6'ya geçmedik? Çok övülen Internet Engineering Task Force (IETF) neden bir şey yapmıyor? gibi sorular sormuştur. IPv6 tartışmasındaki problemlerden bir diğeri de tüm IPv4 adreslerinin tam olarak ne zaman tükeneceğinin bilinmemesidir. İyimser tahminler IPv4'ün birkaç on yıl daha idare edeceği iken, kötümser tahminler sadece birkaç yıl kaldığıdır. Çin ve Japonya gibi ülkeler fazla IPv4 adresi almadıklarından, gelişmekte olan endüstrilerle birlikte IPv6'ya geçiş için büyük bir baskı kurmakta ve IPv6' ya geçişin en önemli destekçileri konumundadırlar. Yeni nesil mobil dijital sesli görüşme sağlayıcıları ve ağa bağlı aygıtlar, milyonlarca cihaz için IP adreslerine ihtiyaç duyacaklardır. IETF ekibi, yeni nesil Internet protokolü (IP next generation–IPng) çalışma grubu, IPv6 spesifikasyonları ve yeni kurulan IPv6 Forumu üzerinde yoğun bir şekilde çalışmaktadırlar. Amaç, yeni Internet'i kurmak için yeni IP protokolünü geliştirmektir.

4.2 Adresleme ve Yönlendirme

IPv6, şu anda kuruluşların içinde ve aralarında bulunan birkaç problemi çözmeye yardım etmektedir. IPv6 küresel ölçekte, Internet omurga tasarımcılarının esnek ve genişletilebilir bir küresel yönlendirme hiyerarşisi oluşturmalarına izin vermektedir. Internet omurgası, ulusal ve uluslararası telefon sistemlerindeki yapıya benzeyen bir hiyerarşik adresleme sisteminin korunmasına bağlıdır.

Mevcut IPv4 sistemi, Internet omurgasına bağlı şebekelerin trafiğini sınıflandırmak için de bir adres hiyerarşisi kullanılmaktadır. Adres hiyerarşisi olmaması durumunda, omurga yönlendiricilerinin yönlendirme tablosu bilgilerini dünyadaki tüm şebekelerin erişebileceği bir yerde saklaması gerekmektedir. Açıkça görülüyor ki, dünya üzerindeki IP alt-ağlarının sayısı ve internet'in büyüme hızı düşünüldüğünde, böyle bir yön tablosunun güncellenmesi ve yönetimi mümkün değildir. Adres hiyerarşisi sayesinde omurga yönlendiricileri, IP adresi eklerini kullanarak trafiğin omurgadan nasıl geçmesi gerektiğini belirleyebilirler. Geçtiğimiz yıllarda IPv4, alanlar arası sınıfsız yönlendirme (classless interdomain routing–CIDR) adı verilen ve bit maskelerini kullanarak 32 bit IPv4 adresinin değişken kısmını bir şebeke, alt şebeke ya da noktaya tahsis eden bir tekniği kullanmaya başlamıştır. CIDR, Internet hiyerarşisinin çeşitli seviyelerinde "yön kümelemeye" izin vermektedir. Böylece, omurga yönlendiricilerinin pek çok alt seviye şebekeye ulaşmak için kullanılabilen tek bir yön tablosu girişini saklaması yeterli olmaktadır.

CIDR'ın bir dezavantajı, etkili ve ölçeklenebilir bir hiyerarşiyi garanti etmemektedir. Her bir yön için ayrı bir kayıt tutmamak için, yönlendirme hiyerarşisinin alt seviyelerindeki yönler (daha uzun eklere sahiptirler), yönlendirme hiyerarşisinin üst seviyelerinde daha az sayıda ve daha az özel bir grup şeklinde toplanmış olarak bulunmalıdır. CIDR öncesinden gelen eski IPv4 adres atamaları ve mevcut erişim sağlayıcı hiyerarşisi, genellikle özetleme işini kolaylaştırmamaktadır. Mevcut hiyerarşi sisteminin tek çeşit olmaması ve IPv4 adreslerinin dikkatli dağıtılma gereksinimi, Internet adresleme ve yönlendirmesini büyük ölçüde güçleştirmektedir. Bu konular üst düzey servis sağlayıcıları ve dolayısıyla son kullanıcıları etkilemektedir. Ayrıca, IPv4 sitelerinin yeniden numaralanması da gereksiz derecede karışık ve dolayısıyla IPv6'dan daha maliyetlidir.

4.3 IPv4 den IPv6 ya geçiş

Servis sağlayıcılar IPv6 omurgalarını kurup, tamamen IPv6 servisleri hizmete girene kadar geçen sürede, noktadan noktaya IPv6 uygulamalarının IPv4 ağları üzerinden geçirmeleri gerekecektir. Bu, bir IPv6 paketinin bir IPv4 paketinin içerisine sokulmasıyla sağlanılmaktadır. Bir IPv6 düğümünden çıkan IPv6 paketleri, IPv4 içine yerleştirilir ve IPv4 şebekesi üzerinden iletilirler. Tünelin öbür ucundaki düğüm, IPv4 paketini ayrıştırır ve hedef düğüme gönderilmeye hazır olan IPv6 paketini ortaya çıkartır.

IPv6 şebekesini işletmenin maliyeti, aynı ölçekteki bir IPv4 şebekesinden daha düşüktür. Bunun nedeni, IPv6'nın IPv4'ten daha akıllı olmasıdır. Örneğin, IPv6 düğümleri, doğru dinamik host yapılandırma protokolü sürümü ile kendilerini otomatik olarak konfigüre edebilmektedir. Bunun yanında, komşu tespit işlevi sayesinde, bir IPv6 düğümü herhangi bir şebekeye eklenebilir ve bir insanın müdahalesine gerek olmadan bağımsız bir oto yapılandırma sunucusuna bağlanıp uyumlu bir şekilde konfügre edilebilmektedir. Bu özellikler gerçek tak ve çalıştır şebeke erişimi sağlamaktadır. Komşu tespitini

kullanarak, düğümler bağlantıları arasındaki hangi yönlendiricilerin mevcut ve erişilebilir durumda olduğunu otomatik olarak tespit edebilmektedir. IP adreslerinin atanması işlemi kurumsal seviyede basitleştirilmiştir.

IPv6'nın sınırları genel şebeke bağlanabilirliğini etkilemeden IPv6 adacıkları oluşturabilmektedir. Dışarıdan içeriye doğru geçiş yaparken, kurumlar IPv6 yönlendiricilerini network sınırlarına yerleştirerek IPv6 ağlarına ve onların aracılığıyla bağlanabilirliğe izin verebilmektedir. Bu senaryoda kurumlar, IPv6 omurgalarına bağlanırlar ve IPv4 trafiğini onların içinden geçirirler.

4.4 IPv6 mı? NAT mı?

Elbette herkesin IPv6'yı desteklemesi beklenemez. Karşı görüşte olanlar, adres atanması ve yönlendirme problemlerinin başka mekanizmalarla kontrol edilebileceğini iddia etmektedirler. Bu tür mekanizmalar içerisinde özellikle şebeke adres çevirimi tartışılmakta. NAT'ı destekleyenler, onun IPv4 adres problemleri için kesin çözüm olduğunu iddia etmektedir. Karşı olanlar ise, gerçek noktadan noktaya bağlanabilirliği (güvenlik açısından) ortadan kaldıran NAT'ı, ortak çalışmaya aktif olarak zarar veren bir pürüz olarak görmektedirler (NAT şebekesinden geçen tüm verilerin dönüştürülmesi gerekir, bu da iletişimi şifrelemek ya da imzalamak için IP güvenliği mimarisi (IPsec) protokollerinin kullanımını imkansız hale getirir). Öte yandan, NAT'ın kullanımı tüm bir ağın tek bir IP adresi arkasına gizlemeyi sağlar, dolayısıyla onunda kendine has bir güvenliği mevcuttur.

5. IPv6 ve İNTERNETİN GELECEĞİ

Internet ve elektronik ticaretin geleceğini şimdiden tahmin etmek, oldukça güçtür. Basitçe, Internet'in gelecekte nerelerde kullanılacağını ve tam etkisinin ne olacağını bilinmemekle birlikte internet'in iş, eğitim ve eğlence sektörlerini değiştirdiği bilinmektedir ve internet hızlandıkça daha çok amaca hizmet edeceği ve daha büyük değişiklikleri meydana getireceği düşünülmektedir. Gelecek Internet'e ilişkin tariflerin çoğu bant genişliği üzerinde yoğunlaşmaktadır. Fakat yeni nesil Internet, yüksek hızlı ağlardan öte bir uygulamadır. Problem teknolojinin neler yapabileceği değil, bizlerin neler yapabileceğidir.

5.1 Gizlilik ve Güvenlik

IPv6' nın tüm potansiyelini ortaya çıkarmak için, son kullanıcıların on-line bilgilere ve işlemlere, daha önce kâğıttaki belgelere olduğu kadar güvenmeleri gerekmektedir. Sayısal bilgi önemli bir ürün haline geldiğinde, korunması ve gerçeklenmesi gerekmektedir. Veriler kontrol edebilmeli ve gizliliğini korunabilmelidir. Bunun için kolay kullanılan, ucuz, değişmez güvenlik ve gerçekleme mekanizmaları gerekmektedir.

5.2 Servis Kalitesi

Çoğu Internet kullanıcısı, on-line geçen vaktinin büyük bölümünde, web sitesine bağlanmak için, sayfaların yüklenmesini, yazılımın download edilmesini beklemektedir. Yeni nesil Internet ihtiyaç duyulan hızı sunacaktır.

IPv4 bir ayrıcalıklı servisler (differantiated services–DS) byte'ı taşır ve IPv6'da aynı iş için bir trafik sınıfı (traffic class–TC) byte'ı bulunmaktadır[2]. Bunlar basit farklı servisleri desteklemek için düşünülmüştür. IPv4 ve IPv6, daha karmaşık QoS uygulamaları için kaynak ayırma protokolünü (resource reservation protocol–RRP) desteklemektedir. IPv6 paket formatı yeni bir 24 bit'lik trafik akışı tanımlama sahası içermektedir ve bu da servis kalitesiyle ilgili ağ işlevlerini uygulayan üreticilere büyük fayda sağlamaktadır. Bu ürünler henüz planlama aşamasında olsalar da, IPv6 gerekli temeli hazırlayarak geniş QoS fonksiyonlarının açık ve birlikte çalışabilir bir şekilde sunulmasına imkan vermektedir. IPv6'daki QoS' in diğer bir faydası da, yönlendirmenin optimize edilmesi için bir akış etiketi (IPv6 başlığı içinde bulunur) kullanılarak trafik akışlarının ayırt edilebilmesidir. Akış etiketi içerik şifreliyken dahi akışın niteliğini belirlemek için kullanılabilmektedir.

IPv6 akış etiketleri sayesinde, şebeke özel ilgi isteyen paket akımlarını tespit edebilmektedir. Akış tabanlı yönlendirme, Internet sistemlerine, bağlantı merkezli anahtarlama teknolojisi ve sanal devrelerde bulunan bazı karakteristikleri verebilmektedir. Örneğin, masaüstü video ya da ses akımları, kontrollü bir noktadan noktaya gecikmenin gerekli olduğunu yönlendiricilere bildiren bir akış etiketine bağlanabilmektedir. Akış etiketleri bundan başka, trafik akışlarına özel güvenlik seviyesi, yayılma gecikmesi ya da maliyet vermek için kullanılabilmektedir. Standart dışı IPv4 QoS uygulamaları ile yapılan deneysel çalışmalarda, çeşitli özelliklerdeki ağ katmanlarından ses ve hareketli görüntü iletiminin fazla bir kayıp olmadan yapılabileceği gösterilmiştir[4]. IPv6 bu tür bir üretim uygulamasının yolunu açmaktadır.

5.3 Taşınabilirlik

Bazı nedenlerden ötürü, IPv4'ün mobil bilgisayarda kullanımında güçlükler mevcuttur: Mobil bilgisayarlar, Internet'e girdikleri her nokta için bir aktarım (forwarding) adresine ihtiyaç duyarlar. IPv4'te bu adresi almak her zaman kolay olmaz.

IPv4 düğümlerinde yaygın olarak bulunan iyi gerçekleme sistemleri, yönlendirme altyapısındaki tüm aracılara mobil düğümün yeni yerini bildirmek zorundadırlar. IPv4'te, mobil düğümlerin aynı şebekeye bağlı olup olmadıklarını anlaması zor olabilmektedir. IPv4'te mobil düğümler, iletişim partnerlerine yer değişikliklerini bildirememektedir.

IPv6 protokolünün tasarımındaki birkaç nokta, mobil bilgi işlem için dial-up desteğini direkt olarak sağlamakta ve ötesine de geçmektedir. Hedef seçenekleri, otomatik yapılandırma, yönlendirme başlıkları, paketleme, güvenlik ve anycast adreslerin gelişmiş kullanımı, IPv6'nın mobil tasarımına katkıda bulunmaktadır. IPv6'nın mobil olma avantajı, mobil düğümlere daha iyi servis kalitesi veren akış etiketi yönetiminin ilavesiyle daha da ön plana çıkmaktadır.

6. SONUÇ

Veriler mobil hale gelecek ve hücresel telefonlar, akıllı telefonlar, sayısal kişisel yardımcılar (personal digital assistant–PDA), elektronik kitaplar ve kağıt gibi çeşitli cihazlardan geçebilecek. Kullanıcılar, bulundukları yerden bağımsız olarak kesintisiz bir şekilde bir kampüs LAN'ına bağlı kalabileceklerdir. Kullanıcılar fiziksel olarak kampus bölgesinden ayrıldıklarında, bağlantıları kesilmeden WAN' aktarılacaktır.

Internet gerçek küresel bir ortam haline gelirken, çeşitli servisleri sağlam bir şekilde destekleme yeteneğine sahip bir ağ oluşturmak için yeniliklere ve kişilerin çalışmalarına ihtiyaç duyulmaktadır.
Özetle;

- Internet üzerinden gönderilen verinin gizliliğini sağlayan,
- Gizli verinin gizli kaldığını ispatlayan,
- Bir mesajın düzgün bir şekilde gönderilip alındığını doğrulayan,
- Web üzerinde şahısların ve bilgilerin gerçek olduğunu ispatlayan,
- Birinin bir elektronik belgeyi imzaladığını kanıtlayan ve
- Bir işlemin belli bir zamanda yapıldığını onaylayan
- Hatalara karşı güvenli

Yeni bir protokol olan IPv6 yakın zamanda tüm ağlarda kullanılmaya başlayacaktır.

KAYNAKLAR

[1] J. C. R. Licklider, "Man-Computer Partnership," *International Science and Technology,* May, 1965.
[2] R. Hinden, S. Deering, RFC 2460 Internet Protocol version 6 (IPv6) Specification
[3] Huitema, C. An anycast prefix for 6to4 relay routers. IETF Proposed Standard RFC3068, June 2001
[4] A. Conta, S. Deering "Request for Comments: 2473", 1998
[5] Tsuchiya, K. et al., An IPv6/IPv4 Multicast Translator based on IGMP/MLD Proxying. http://www.ietf.org/ internet-drafts/draft-ietf-ngtrans-mtp-01.txt, work-in-progress, February 2002.
[6] S. Kent, R. Atkinson, RFC 2402 IP Authentication Header (AH)
[7] S. Kent, R. Atkinson, RFC 2406 IP Encapsulation Security Payload (ESP)
[8] R. Hinden, S. Deering, RFC 3513 Internet protocol Version 6 (IPv6) Addres Architecture
[9] http://www.ip6forum.org.uk/navbar/links/v6porting.htm
[10] http://www.6bone.net/
[11]http://www.caida.org/analysis/geopolitical/bgp2country/ipv6.xml