T.C
FIRAT ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ

IPv6 VE İNTERNETİN GELECEĞİ

BİTİRME ÖDEVİ

HAZIRLAYANLAR

Tamer AYAZOĞLU ve Osman Çağlar ÖZER

Bitirme Yöneticisi :

Yrd.Doç.Dr Hasan Hüseyin BALIK

ELAZIĞ 2005

T.C
FIRAT ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ

IPv6 VE İNTERNETİN GELECEĞİ

BİTİRME ÖDEVİ

HAZIRLAYANLAR

Tamer AYAZOĞLU ve Osman Çağlar ÖZER

Bu tez ,…….tarihinde aşağıda belirtilen jüri tarafından oybirliği / oyçokluğu ile başarılı / başarısız olarak değerlendirilmiştir.

Danışman:

Üye:

TEŞEKKÜR

Bu çalışmanın gerek hazırlanmasında gerekse yürütülmesinde her türlü yardım ve desteğini esirgemeyen Hocamız Yrd.Doç.Dr Hasan Hüseyin BALIK'a ve arkadaşlarımız Erden SAÇAN ve Boğaçhan ER'e teşekkür ederiz.

Tamer AYAZOĞLU ve Osman Çağlar ÖZER

ELAZIĞ 2005

İÇİNDEKİLER

TABLO , ŞEKİL VE RESİMLERİN LİSTESİ

ŞEKİLLER :

TABLOLAR :

RESİMLER :

ÖZET

TCP/IP, bilgisayarların marka ve teknoloji bağımsız çalışabilmelerini sağlayan ve geniş bir kullanım alanı olan bir protokol kümesidir.İnternet TCP/IP'nin kullanıldığı en bilinen uygulamadır.İnternet üzerindeki bilgisayarlar ,TCP/IP 'nin mimarisi gereği kullanıcı/sunucu şeklinde çalışırlar;bilgisayarlardan bir kısmı ve hizmeti sunarken,büyük bir çoğunluğu da bunları kullanır.

TCP/IP,OSI başvuru modeli gibi katmanlı bir yapıya sahiptir;nacak OSI'deki gibi 7 katman değil de 4 katmana sahiptir.Fiziksel katman hariç her katmanın kendi alt protokolleri vardır.Bunlardan TCP ve IP kümenin temel protokolleridir.Adres çözümleme protokolü olan ARP,bir LAN içinde IP adresi bilinen alıcı bilgisayarın fiziksel adresini belli etmek için kullanılan bir protokoldür.

IPv6, TCP/IP'nin yeni nesil yönlendirme katmanı protokolüdür.IPv4'ün üzerine geliştirilmiştir. IPv6 ile IPv4 2de olan birçok kısıtlamalar giderilmeye çalışılmış ve IP başlıklarında çok az kullanılan alanlar kaldırılmıştır.IPv6'da ilk göze çarpan yenilik adresleme alanı genişliğidir.IPv4 de 32 bit olan adresler IPv6'da 128 bit olmuştur. Böylece adres alanı darlığı giderilmiş ve çok daha geniş adres alanı elde edilmiştir.IPv6'nın hayata geçmesinin diğer nedenleri arasında ise güvenlik ve yönlendirme esnekliğinin önem kazanması gösterilebilir.

GİRİŞ

Yapmış olduğumuz bu çalışmada IPv6 teknik özelliklerini,adres yapısını,IPv4 göre üstünlüklerini,IPv6 neden ihtiyaç duyulduğunu ve IPv6 ile birlikte internetin geleceğinin nasıl şekilleneceğini inceledik.

Bunun için yabancı ve Türkçe kaynaklardan faydalanıp,bizim gibi aynı konu üzerinde çalışan birçok kişinin görüş ve önerilerini aldık.Bunu yaparken konumuz olan internetten yararlandık

1 İNTERNET PROTOCOL – IP

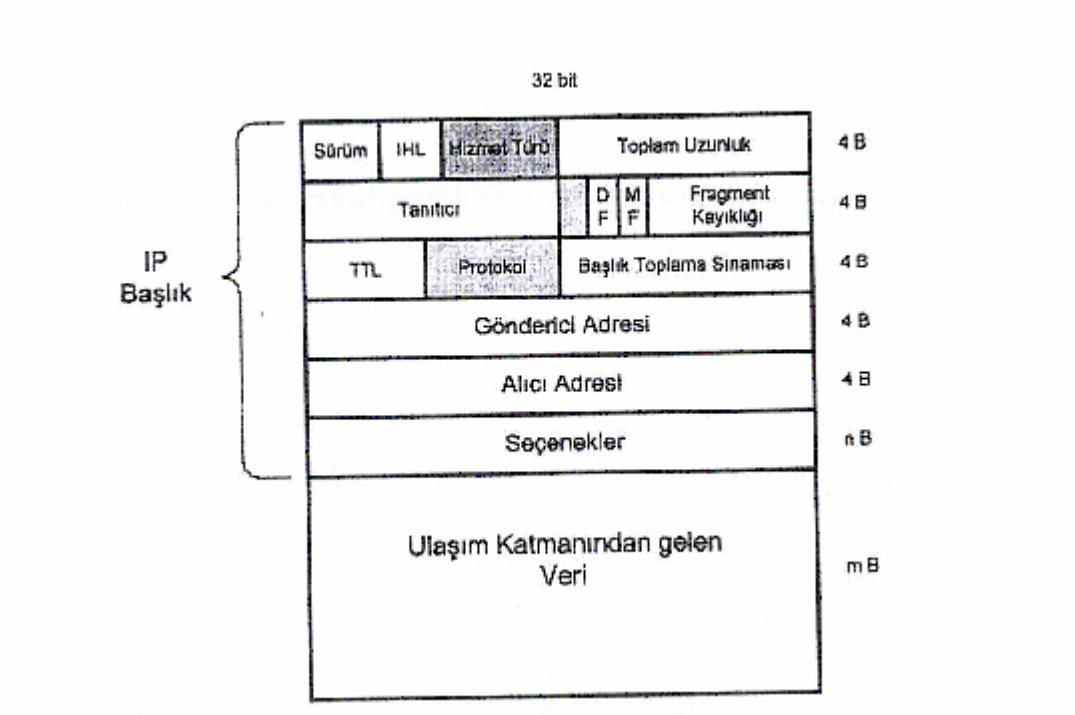
Internet Protocol (IP), insanlığı bilgi çağına taşıyan internet ağının temel yapı taşıdır.internete bağlı herhangi iki bilgisayar arasındaki iletişim bu protokol aracılığı ile sağlanır. İnternet,çok sayıda ağın birbirine bağlı olduğu bir ağlar topluluğudur.Ağ üzerinde yüksek band genişlikli hatlardan ve hızlı yönlendiricilerden oluşan bir dizi omurga bulunmaktadır.Bu omurgalara bölgesel ve ulusal ağlar bağlanmıştır.Bu kocaman ağı birbirine yapıştıran,bir ağ katmanı protokolü olan,internet protokolü IP'dir.Bu açılardan IP'yi internetin ortak lisanı olarak nitelendirebiliriz.IP herhangi bir zaman kısıtlaması olmaksızın ağ kaynaklarının el verdiği ölçüde datagram aktarımını kotarmayı amaçlar.

IP,ağ katmanlarına baktığımızda TCP ve UDP gibi tasıma katmanı protokollerinin altında,Ethernet ve ATM gibi bağ katmanı protokollerinin de üzerinde yer alır.Temel görevi internete bağlı bilgisayarların iletişim amacıyla adreslenebilmesi ve gönderilen veri paketlerinin ağ içerisinde yönlendirilmesidir.

IP'nin üzerindeki ulaşım katmanı üst katmandan gelen veri katarlarını 64 KB uzunluğunu aşmayan datagramlara bölerek IP'ye teslim eder.Datagramlar internet üzerinde yol alırken daha küçük datagramlara (fragment) bölünme durumunda kalabilirler.Son alıcıda fragmentler birleştirilerek orijinal datagram elde edilir ve bu datagram ulaşım katmanına oradan da onun üst katmanına geçirilir.

1.1 İnternet Protokolu Paket Formatı

IP yazılımı,gelen datagramın sürüm (versiyon) alanındaki değer,kendi sürüm değerine eşitse datagramı değerlendirir.aksi halde datagramı çöpe atar.



Şekil 1.1 IP Paket Formatı

IHL (IP Başlık Uzunluğu-IP Header Lenght): Başlık alanının kaç adet 32 bitlik sözcükten oluştuğunu gösterir.(en az 5,en çok 15)

Hizmet Türü: Göndericinin ağdan beklediği güvenilirlik,hız ve gecikmenin düzeyini belirtir.Ancak bu alanı mevcut yönlendiricilerin pek azı değerlendirmektedir.

Toplam Uzunluk: başlık ve veri birlikte datagram uzunluğunu gösterir.

Tanıtıcı: Burada değeri alıcı fragmentleri birleştirmek için kullanır.Aynı datagramın bütün fragmentlerinintanıtıcı değeri birbirinin aynıdır.

DF (Don't Fragment): Yönlendiricilerden datagramı fragmentlere bölmemesini buyuran bir bitlik bir istek alanıdır.Alıcının fragmentleri birleştiremediği durumlarda gereklidir.

MF (More Fragment): Bir datagramın son fragmenti dışındaki tüm fragmentlerinde MF=1 dir.

Fragment Kayıklığı: 8B'lik birimler halinde fragmentin datagram içindeki konumunu gösterir.

TTL (Time To Live): Datagramın alıcısına belirli bir süre içinde ulaşmaması durumunda yok edilmesini sağlayan bir alandır.TTL alanına başlangıçta 255 veya daha küçük bir tam sayı terleştirilir.Her yönlendiricide bu alandaki değer bir eksiltilir.Ayrıca yönlendiricide paket bir bekleme kuyruğuna alınırsa her geçen saniye TTL alanındaki sayı bir eksiltilir.Sayı sıfıra ulaşırsa paket çöpe atılır.Çöpe atan yönlendirici kaynağa bir uyarı paketi gönderir.

Protokol Alanı: IP'nin üst katmanı olan ulaşım katmanında hangi internet protokolünün (TCP,UDP, …) yürütüldüğünü gösterir.

Başlık Toplama Sınaması: Başlıkta bir bozulma olup olmadığını belirlemeye yarar.Her yönlendiricide bu alandaki değer kullanılarak datagramın bozulup bozulmadığı araştırılır.Sonuç olumlu ise paket bir sonraki yönlendiriciye gönderilir.Bu arada başlıktaki bazı değerler ile birlikte (örneğin TTL) bu alandak ideğerde gönderilen pakette yeniden hesaplanır.Yöntem yalnızca başlıktaki hataları açığa çıkardığı için ulaşım katmanının verideki muhtemel bozuklukları yakalayacak önlemler alması gerekebilir.

Gönderici Ve Alıcı Adresleri: 32 bit uzunluğunda adreslerdir.(IPv6 protokolünde 128 bit.)

Seçenekler: Bu alanda güvenlik,izlenecek yörünge,yönlendirici numaralarını ve gerçek zaman saatlerini datagrama eklemeleri için uyarı gibi bazı ek bilgiler bulunmaktadır.

1.2 İnternet Protokolün Gelişimi

IP bundan yaklaşık yirmi yılı aşkın bir süre önce gerçekleştirilmiş bir teknolojidir.İlk amacı çok daha kısıtlı bir boyutta (askeri iletişim amaçlı) kullanım olmasına rağmen,geçtiğimiz on yıl içinde bu teknoloji dünya çapında kullanıma açılmıştır.Özel sektörün bu altyapıyı bir toplu iletişim aracı olara kullanmaya başlaması ve www'in gelişmesi IP'nin hızla yaygınlaşmasını sağlayan faktörler olmuştur.Ama ne yazık ki bu popülerliğin bir yan etkisi de eski protokolun limitlerine ulaşması ve böylesine ağır bir yükün altından kalkamayacak duruma gelmesidir.

İnternetin temellerinin ARPANET adıyla 1960'lı yıllarda atılmasıyla birlikte NCP (Network Control Protocol) üzerinden bağlantılar yürütülüyordu.Bu sözleşmenin yetersiz olması ve olumsuz yanlarının bulunması nedeniyle 1981 yılında TCP/IPv4 sözleşmesi standartlaştırılmıştır.

Günümüz interneti IP protokolünün 4. sürümü (IPv4) üzerine kurulmuştur.IPv4 sınıf (class) sistemine dayalı bir sözleşmedir.

Sınıfların anlamlarını ayrıntılı olarak anlatmak gerekirse :

A-125 ağ,ağ başına yaklaşık 16 milyon adres

B-16382 ağ,ağ başına 65534 adres

C- Yaklaşık 2 milyon ağ,ağ başına 256 adres

D- Multicast kullanım için ayrılmıştır.

E- Gelecekte kullanım için ayrılmıştır

Örneğin ODTÜ 144.122 ile başlayan B sınıfı bir IP bloğuna sahiptir.Bu ODTÜ'ye kurumsal olarak 65534 ayrı adres verebilme olanağı sağlar.IPv4 sistemi kurumsal olarak 4 milyar farklı adrese imkan tanır.Ama sınıf sınıf sistemi nedeniyle bu verimli kullanılamamaktadır.Örneğin bir şirket IP bloğu için başvurduğunda hepsini kullanabilecek kapasitesi olmasa da en az 256 IP'lik bir C sınıfı almak zorundadır.1980'li yıllarda parmakla sayılabilecek internet bilgisayarı olduğu düşünülünce o zamanki en ileri görüşlü insanın bile 4 milyar adresin yetmeyeceğini düşünmesi beklenemezdi.

Bilgisayarların iletişim sırasında uçtan uca adreslenebilmesini sağlayan IPv4 adresleri sadece 32 bitten ibarettir.32 bitlik adres alanı teoride 4,294,967,296 tane adres yaratabilse de verimsiz adres atama mekanizmalarından dolayı etkin adres sayısı bu noktaya hiçbir zaman ulaşamaz.WWW'nin patlarcasına gelişmesinin yanı sıra son zamanlarda kablosuz erişiminde yaygınlaşmasıyla 32 bitlik adres alanı varolan ihtiyacı karşılamakta yetersiz kalmaya başlamıştır.

Bu problem karşısında IPv4 adres havuzunun etkin kullanımı için çeşitli yöntemler geliştirilmiştir.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 tekniklerde yetersiz kalmaya başlayınca bazı kurumları kullanmadıkları büyük adres bloklarını vermelerine iknaya bile başvurulmuştur.

(Örnek: Stanford Üniversitesi'nin 036/8 adres bloğunu IANA 'ya iadesi). Ne yazık ki sonunda anlaşıldı ki varolan IPv4 mimarisiyle Internete bağlı tüm düğümlere birbiriyle 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 sunmaktadır. Bu bilgisayarlarla Internet arasında bir geçit görevi yapan NAT , Internet mimarinsin en temel prensiplerinden olan uçtan uca adresleme ve paket bütünlüğünü yokeden 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, yönetim zorlukları başlıca problemler arasındadır.

1.3 IPv4 İnternetinde Karşılaşılan Sorunlar

1.3.1 Teknik Veriler Işığında IPv4’ün Güvenlik Açıkları

1) Veri Doğrulama: Alıcı eğer kaynak adresi belli bir IP’den paket alıyorsa gerçekten bu paketin o adresten geldiğine emin olmalıdır.(IP spoff saldırıları)

Çözüm: SA (Security Associations)

- PKI için ortak bir anahtar,güvenlik algoritması ve diğer parametreler konusunda anlaşma sağlanması
- Her protokol kendi Security Association’una sahiptir
-Security Parametreler Index alıcı (receiver) tarafından seçilir
-SPI multicast gruplarında nasıl yaratılıp nasıl dağıtılacağı hala üzerinde çalışılan bir konudur.

2) Data Bütünlüğü: Alıcı bir paket aldığında bunun kaynaktan gelene kadar değişmediğine veya açılmadığına emin olmalıdır

Çözüm: Authentication Header

-Veri doğrulama ve veri bütünlüğü sağlıyor
-Algoritma bağımsız (keyed md5 öneriliyor)
-paket doğrulaması için checksum hesaplanırken yol boyunca değişen TTL/Hop Limit benzeri paket header bilgileri dikkate alınmıyor.

3) Data Şifrelemesi: Alıcının bir paket aldığında yol boyunca bu paketin seyrettiği süre zarfında açılıp okunmadığına emin olmalı.

Çözüm: ESP (Encapsulated Security Payload)

-Gizlilik ve şifreleme sağlıyor
-2 modu var

a) Tünel Modu: tüm datagram şifreleniyor

b) Transport Modu: Sadece payload (TCP,UDP,ICMP)
-DES ve CBS dışında algoritma bağımsız

1.3.2 Hiyerarşik Adresleme Eksikliği

Kullanılmakta olan IPv4 sistemi,internet omurgasına bağlı ağ trafiğini sınıflandırmak için bir adres hiyerarşisi kullanır.Bir adres hiyerarşisi olmadığı taktirde yönlendirme bilgilerinin bütün ağların ulaşabileceği bir yere konması gerekmektedir.İnternetin kullanımının hızla arttığı bir ortamda böyle bir uygulamaya gitmenin imkansız 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 gelişimin engellenmesi için, Internet protokollerinden sorumlu Internet Engineering Task Force (IETF) 1990 yıllarının başında yeni bir çalışma grubu kurdu. O zamanki adıyla IPng (Internet protocol, next generation) çalışma grubu , yeni IP protokolünün geliştirilmesi görevini üstlendi. İnternet mimarisinin temel prensiplerinin korunarak sağlıklı gelişiminin sağlanması ve yeni uygulamaların önünün açılabilmesi için IP protokolünün yeni bir sürümünün geliştirilmesi öngörüldü. Yaklaşık 10 yılı aşkın bir süredir endüstri, akademi, hükümetler ve çeşitli organizasyonların ortak çalışması sonucu IPv6 protokolü doğmuş oldu. ("v5" ,IPv4 'ün uzantısı olarak geliştirilen ve deneysel kullanımın ötesine geçememiş ST protokolüne ayrılmış.)

2. IPV6 (İNTERNET PROTOCOL VERSİYON 6)

2.1 IPv6'nın Teknik Özellikleri

IPv6 protokolü,IETF'in yayınlamış olduğu bir seri RFC dökümanı vasıtasıyla tanımlanmıştır.IPv6'yı IPv4'ten ayıran en temel özelliği 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'dır.Böylesine geniş bir adres alanının şu an yaşadığımız adres sıkıntısını çözmenin yanında internet uygulamalarında yeniliklere de yol açması bekleniyor.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 alır.

128 bitten oluşan IPv6 adreslerinin ilk 64 bitlik kısmı alt ağı adreslemek için kullanılan adres blok bilgisini içerir.Adres bloğu,bir paketin varacağı son bağa kadar olan yolda yönlendirilmesini sağlar.Geriye kalan 64 bit ise bu bağa vardığında paketin son alıcısının tespitinde kullanılır.IPv6 adresleri 16'lık bir düzende ifade edilir.2045:ab28::6cef :85a1:331e:a66f:cdd1 örneğinde olduğu gibi 16 bitlik gruplar birbirlerinden " : " ile ayrılır.Ardarda gelen iki " : " sadece bir kereye mahsus kullanılabilir ve aralarında kalan bütün hanelerin sıfır değerini taşıdığını ifade ederler.

IPv6 adresleri bağ içi (link-local) ve evrensel (global) olmak üzere iki çeşittir.Bunlara ek olarak site içi adreslerde 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,be adresi kullanan birden çok düğümden sadece birine varacak şekilde yönlendirilir.Kullanımda birden çok düğüm aynı adrsi paylaşması açısından çoklu gönderim adreslerine benzemekle birlikte,paketin sonunda sadece tek bir düğüme ulaşması açısından tekil gönderimi andırırlar.

Otomatik adres konfigürasyonu 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 tanır.Temelinde ağdaki yönlendiricilerin gerekli adres bloğunu anons etmeleri ve düğümlerinde bu bloğa kendilerinden 64 bitlik bir değer eklemeleriyle adres oluşturmaları yatar.Bu şekilde oluşturulan adreslerin kullanılmadan önce tekillik testinden geçirilmesi gerekir.Düğümler başkaları tarafından kullanılmadığına kanaat getirdikleri adresi kullanıma alabilir.

IP protokol başlığında ise büyük değişiklikler olmuştur.IPv4'te varolan protokol başlık büyüklüğü,kimlik bilgisi,paket parçası bilgisi,başlık sağlama toplamı kaldırılmış,IPv6 başlığına yeni olarak akış bilgisi eklenmiş.Tipik 20 bayt genişliğindeki IPv4 başlığının yerini 40 baytlık IPv6 başlığı almış.Temel IPv6 başlığına ek olarak,kendince özel amaçlara yönelik yönlendirme,paket bölmesi,şifreleme ve mobil uzantı başlıkları tanımlanmış.Zaman içerisinde ihtiyaç oldukça bunlara yenilerinin eklenmesi de mümkün kılınmıştır.

Yönlendirme alanında temel prensiplerde bir değişiklik olmamakla birlikte varolan RIP,OSPF,IS-IS,MP-BGP,PIM-SM,PIM-SSM gibi protokoller IPv6 adreslerini işleyebilecek şekilde güncellenmiş.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 düzenlenmiş.IPv4 adresleri A tipi kayıtlarda saklanırken,AAAA tipi kayıtlar IPv6 adreslerine tahsis edilmiş.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. 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} 'dir.

19702leirn sonlarında IPv4 dizayn edilirken bir gün yetersiz gelebileceği hayal bile edilemezdi.Ancak teknolojideki gelişmeler 1992 yılında bu yetersizliğin kabulüne yol açtılar.

Geçerli Paylaşım;

IPv4 adresinin ünicast ve muiticast adres gruplarına ayrılması gibi IPv6 adresleri de yüksek değerli bitlerine göre gruplara ayrılır .Aşağıdaki tablodaki belirtildiği üzere;

Table 3-1. **CURRENT ALLOCATION OF THE IPV6 ADDRESS SPACE**

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
Aggregatable 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 Evrensel Unicast Adresinin Yapısı

3.1 IPv6 Adres Düzenleme

32 bitlik IPv4 adresi 8 bitlik 4 gruba ayrılırken 128 bitlik IPv6 16 bitlik 8 gruba ayrılır.Bu gruplar hexadecimal olarak şöyle ifade edilir.

21:DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

Table 3-2. **CONVERTING BETWEEN BINARY, HEXADECIMAL, AND DECIMAL NUMBERS**

Binary	*Hexadecimal*	*Decimal*
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	A	10
1011	B	11
1100	C	12
1101	D	13
1110	E	14
1111	F	15

Tablo 3.2 İkilik,Onluk ve Hex Sayıları Birbirine Çevirme

3.2 IPv6 ADRES TÜRLERİ

3.2.1 ÜNİCAST IPv6 ADRESLERİ

Evrensel adreslerde FP 001 olarak tanımlıdır.Bir evrensel adresin kapsamı tüm IPv6 internetini içine alır.Tablo 3.1 de bir evrensel ünicast adresin yapısı gösterilmiştir.

Bu şekle göre ;

TLA ID:Üst seviye gruplama tanımlayıcısı ,bu bölümün uzunluğu 13 bittir.

Res:TLA veya NLA IP'de ileride meydana gelebilecek ilerlemeler için rezerve esilmiş 8 bittir.

NLA ID:Sonraki seviye gruplama tanımlayıcısı,bu bölüm uzunluğu 24 bittir.

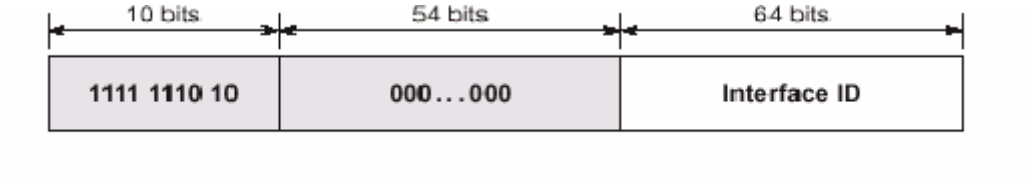
FP,NLA, TLA ve Res 'in oluşturduğu toplam 48 bitlik alan firma bilgisini içerir.

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

Interface ID:Alt ağa ait arayüzüdür.64 bittir.IPv4'deki düğüm ID vey IP'nin karşılığıdır.

3.2.1.1 Yerel Bağlantı Adresleri:

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



Şekil 3.1 Bir Yerel Bağlantı Adresinin Yapısı

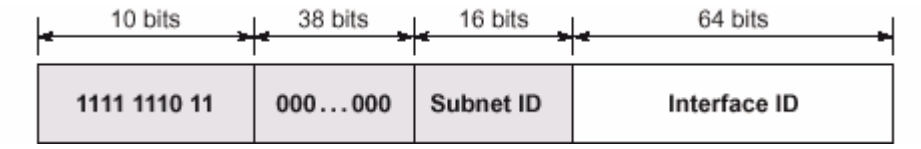
yerel bağlantı adresleri her zaman FE80 ile başlarlar.

3.2.1.2 Yerel Site Adresleri

Yerel site adresleri 111.1110.11 olarak tanımlıdır.IPv4 'teki özel adres alanlarına (10.0.0.0/16)karşılık gelirler.

Evrensel adreslerle çakışma olmadan kullanılabilirler.

Bir yerel site adresin yapısı şeklindeki gibidir;



şekil 3-2 Bir Yerel Site Adresin Yapısı

farklı olarak bu adresler otomatik konfigüre edilemezler,elle atanmaları gerekir.

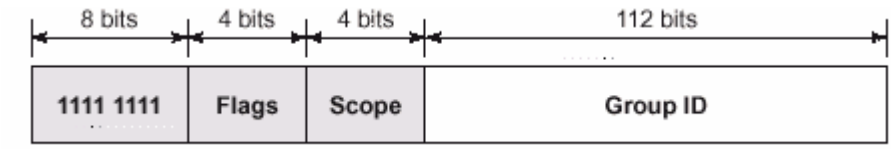
Görüldüğü üzere evrensel adresler ve yerel site adresler ilk 48 bit hariç olmak üzere aynı yapıya sahiptirler.

3.2.2 MULTİCAST IPv6 ADRESLERİ

IPv6'da multicast trafik aynı IPv4'de olduğu şekilde işler.Keyfi yerleştirilmiş IPv6 düğümleri keyfi bir IPv6 multicast adresinde multicast trafiği dinleyebilir.Aynı zamanda IPv6 düğümleri

multicast adreslerini çoğullamada kullanır.Düğümler herhangi bir zamanda multicast gruplarına katılıp ayrılabilir.

IPv6 multicast adresleri 11111111 lik FP'ye sahiptirler.Bundan dolayı bir IPv6 multicast adresi her zaman FF ile başlar.Multicast adresleri kaynak adresleri yada yönlendirme başlığındaki orta derece hedefler olarak kullanamazlar.FP'nin ardından multicast adresleri bayrakları onların sahalarını ve multicast gruplarını tanımlayan ilave yapılar içerirler.Aşağıdaki şekil IPv6 multicast adresinin yapısını gösterir.



şekil 3.3 IPv6 Multicast Adresin Yapısı

3.2.2.1 Multicast Adresteki Alanlar ;

Bayraklar: İşaretçiler multicast adreste ayarlanmıştır.Bu alan 4 bittir.RFC 2373 de olduğu gibi tek tanımlı bayrak,bayrak alanın düşük seviye bitini kullanan Transient (T) bayrağıdır.T bayrağı 0'a ayarlandığı zaman multicast adresin IANA tarafından tahsis edildiği gibi kalıcı olarak atanmış(iyi bilinen) multicast adres olduğunu belirtir.

T bayrağı 1'e ayarlandığı zaman ise multicast adresin geçici (sürekli atanmamış) multicast adres olduğunu belirtir.

Saha: IPv6 ağ sahasının hangi multicast adresine verildiğini belirtir.Bu alanın boyutu 4 bittir.Multicast routing protokolleri tarafından sağlanan bilgiye ilave olarak routerler multicast sahasını,multicast trafiğin iletilip iletilmediğini tanımlamada kullanılır.

Table 3-3. **DEFINED VALUES FOR THE SCOPE FIELD**

Scope Field Value	*Scope*
0	Reserved
1	Node-local scope
2	Link-local scope
5	Site-local scope
8	Organization-local scope
E	Global scope
F	Reserved

Tablo 3.3----------

Örneğin: FF02::2 multicast trafik yerel bağlı sahaya sahiptir.Bir IPv6 router hiçbir zaman bu trafiği yerel bağın ardına iletmez.

Grup ID: Multicast grubu tanımlar ve sahaya bağlı olarak benzersizdir.Bu alanın boyutu 112 bittir.Sürekli atanmış grup ID'leri sahadan bağımsızdır.Geçici grup ID'leri sadece özel alanlaruygundur.FF01:: den FF0F:: e doğru olan multicast adresleri ayrılmıştır.İyi bilinen adreslerdir.

Tüm yerel düğüm ve yerel bağ sahası düğümlerini tanımlamak için aşağıdaki adresler belirtilmiştir.

- FF01:: (tüm düğümlerin yerel düğüm saha multicast adresi)
- FF02::1 (tüm düğümlerin yerel düğüm saha multicast adresi)

Tüm routerler için yerel düğüm,yerel bağ ve yerel taraf sahası tanımlamak için aşağıdaki adresler belirtilmiştir.

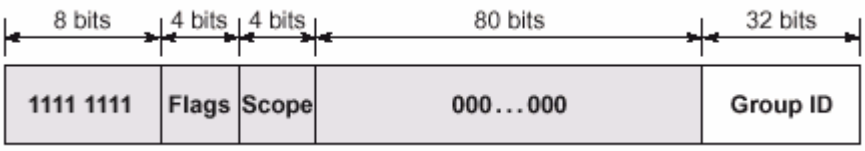
- FF01::2 (tüm routerlerin yerel düğüm saha multicast adresi)
- FF02::2 (tüm routerlerin yerel bağ saha multicast adresi)
- FF05::2 (tüm routerlerin yerel taraf saha multicast adresi)

IPv6 multicast adresleri IPv4 yayın adreslerinin tüm şekillerinin yerini almıştır.IPv4 ağ yayını alt ağ yayın ve sınırlı yayın adresleri IPv6 'daki tüm düğümlerin yerel bağ saha multicast adresi ile yer değiştirmiştir.

3.2.2.2 Önerilen Multicast IPv6 Adresleri:

Grup ID alanındaki 112 bitlik 2^{112} tane grup ID'si tanımlamak mümkündür.IPv6 adreslerinin multicast MAC adreslemesi ethernete haritalanma biçiminden dolayı,RFC 1373 IPv6 multicast adresinin düşük seviye 32 bitli Grup ID'sinden atanmasını ve kalan orijinal Grup ID alanı bitlerini sıfıra ayarlamayı önerir.Sadece düşük seviyeli 32 biti kullanarak her Grup ID'si benzersiz bir multicast MAC adresini haritalar.

Aşağıdaki şekil önerilen yapıdaki IPv6 multicast adresini gösterir.



Şekil 3.4 Önerilen Yapıdaki IPv6 Multicast Adresini Gösterir

3.2.2.3 İstenen Düğüm Adresi

İstenen düğüm adresleri network düğümlerinin etkin sıralanmaması sırasında bağ hat adresi çözünürlüğü bilinen bir IPv6 adresin bağ katman adresi çözümünde kolaylık sağlar.IPv4'de ARP'u tek tek çerçevesi MAC seviye yayına ağ katmanındaki tüm düğümlere dağıtılarak gönderilir ve bu IPv4'de işlemez.IPv6 bağ katman adres çözünürlüğü icar etmek için komşu rica mesajını kullanır.Her nasılsa komşu rica mesajı hedefi için tüm düğümlerin yerel bağ saha multicast adresi yerine istenen doğru multicast adresi kullanılır.İstenen düğüm adresi FF02::1:FF00:0/104 öneki ve bir ünicast IPv6 adresinin son 24 bitinden oluşturulur.

Örneğin ;A düğümü FE80:2AA:FF:FE28:9C5A 'nin yerel bağ adresi olarak atanır ve ayrıca FF02::1:FF28:9C5A'nin uygun istenen düğüm multicast adresi dinlemektedir.(altı çizili son 6 hexa digit uzunluğu işaret eder) Yerel hattaki B düğümü A düğümünün yerel hat adresi FE80::2AA:FF:FE28:9C5A 'yı uygun yerel hat adresine çözebilmelidir.B düğümü FF02:1:FF28:9C5A'nın istenen düğüm multicast adresine bir komşu rica mesajı gönderir.A düğümü bu multicast adresini dinler çünkü komşu,rica mesajını işler ve bir ünicast komşu reklam mesajını cevaben gönderir.İstenen düğüm multicast adresini kullanmanın sonucunda bağ katman adresi çözünürlüğü hatta alışıla gelmiş bir olaydır.Tüm ağ düğümlerini rahatsız etmeyen bir yapı kullanır.İstenen düğüm adreslerini kullanarak adres çözümleme esnasında çok az düğüm rahatsız edilir.Pratik de bağ katman MAC adresi,IPv6 arayüz ID'si ve istenen düğüm adresi arasındaki ilişkiye bağlı olarak istenen düğüm adresi çok etkin adres çözümleme için sahte ünicast adres gibi davranır.

3.2.3 ANYCAST IPv6 ADRESLERİ

Bir anycast adres multicast arayüzleri çoğullamak için atanmıştır.Bir anycast adrese gönderilen paketler anycast adresin atandığı en yakın arayüze yönlendirici alt yapı tarafından iletilir.Teslimatı kolaylaştırmak amacıyla yönlendirici ölçülerdeki hata mesafe terimlerine sahip arayüzlerin farkına varmalıdır.

Örneğin;3FFE:2900:D005:6187:2AA:FF:FE89:6B9A anycast adresi için sağlayacağı yönlendirmeleri organizasyonun atadığı 48 bit 3FFE:2900:D005::/48 öneki ynlendirici arayüzden yayılır.Bu anycast adresin atadığı bir düğüm organizasyonun intranetinde herhangi bir yere yerleştirilebildiğinden dolayı hedef yönlendirmelerinde bütün düğümler için atanmış bu anycast adreslerine organizasyondaki tüm routerlerin yönlendirme tablolarında ihtiyaç duyulur.

Organizasyonun dışında bu anycast adresleri organizasyona atanmış olan 3FFE:2900:D005::/48 öneki ile özetlenebilir.bundan dolayı sağlayıcı yönlendirmeler. IPv6 internetin

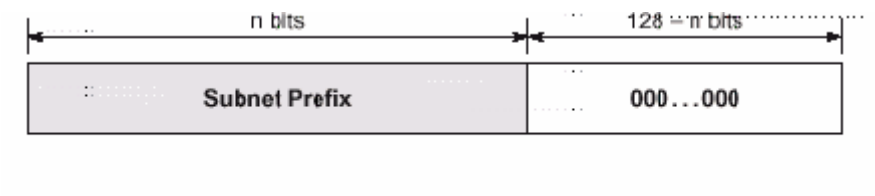
yönlendirici arayüzüne ihtiyaç duymayan bir organizasyonun intranetindeki en yakın anycast grup üyesine IPv6 paketlerini ulaştırmak zorundadır.

RFC 2373 'e göre anycast adresleri sadece hedef adresleri olarak kullanılabilir ve sadece routerlere atanırlar.Anycast adresler ünicast adres boşluklarının dışında atanırlar ve anycast adresin atandığı tipteki ünicast adresin sahası olan bir anycast adresin sahasıdır.

Eğer verilen hedef ünicast adres aynı zamanda bir anycast adresi ise tanımlamak mümkün değildir.Bunun farkında olan yegane düğümler kaynak yönlendirmelerini,anycast trafiği en yakın anycast grup üyesine aktarmak için kullanılır ve anycast grup üyelerinin kendilerinin olduğu routerlerdir.

3.2.3.1 Alt Ağ Router Anycast Adresleri:

Alt ağ router anycast adresi RFC 2373 de tanımlanmıştır ve gereklidir.Verilen bir arayüzün alt ağ önekinden türetilmiştir.Alt ağ router anycast adresi yapıldığı zaman alt ağ önekindeki bitleri yaklaşık değerlerine getirebilir ve kalan bitler sıfır yapılır.Aşağıdaki şekil alt ağ router anycast adresin yapısını gösterir.



Şekil 3.5 Alt Ağ Router Anycast Adresin Yapısı

Bir alt ağa eklenmiş tüm router arayüzleri bu alt ağ için atanmış alt ağ router anycast adresleridir.Alt ağ router anycast adresleri belirtilmiş bir alt ağa bağlanmış en yakın routerik haberleşmede kullanılır.

3.3 Bir Kaynak İçin IPv6 Adresleri

Tekli ağ uyarlayıcısına sahip IPv4 kaynağı tipik olarak bir uyarlayıcıya atanmış tekbir IPv4 adresine sahiptir.Her nasılsa bir IPv6 kaynağı her uyarlayıcı atanmış çoklu IPv6 adreslerine sahiptir.Tipik bir IPv6 kaynağı üstündeki arayüzlere aşağıdaki ünicast adresleri atanmıştır.

- Her arayüz için bir yerel bağ adresi

- Her arayüz için ilave ünicast adresleri (yerel taraf adresleri tekli yada çoklu global adresleri olabilir.)
- Geri döngü arayüzü için geri döngü adresi (::1)

Tipik IPv6 kaynakları her zaman için lojik olarak çoklu adreslenmiştir.Çünkü her zaman paketleri ileten en az iki adrese sahiptir.Yerel bir bağ trafiği için bir yerel bağ adresi ve yönlendiriciler yerel taraf yada global adres.
İlaveten bir IPv6 kaynak üzerindeki her arayüz aşağıdaki multicast adresleri için trafiği dinler:

- Tüm düğümleri yerel düğüm saha multicast adresi (FF01::1)
- Tüm düğümleri yerel bağ saha multicast (FF02::1)
- Her ünicast adres için istenen düğüm adresi
- Katılınan grupların multicast adresleri

3.4 Bir Router için IPv6 Adresleri

Bir IPv6 router üzerindeki arayüzlere aşağıdaki ünicast adresler atanmıştır.

- Her arayüz için bir yerel bağ adresi
- Her arayüz için ilave ünicast adresleri (yerel taraf adresleri ve tekli yada çoklu global adresleri olabilir)
- Geri dögü arayüzü için geri döngü arayüz için geri döngü adresi (::1)

İlaveten bir IPv6 router üzerindeki arayüzler aşağıdaki multicast adresleri için trafiği dinler.

- Tüm düğümlerin yerel düğüm saha multicast adresi (FF01::1)
- Tüm routerlerin yerel düğüm saha multicast adresi (FF01::2)
- Tüm düğümlerin yerel bağ saha multicast adresi (FF02::1)
- Tüm routerlerin yerel bağ saha multicast adresi (FF02::2)
- Tüm routerlerin yerel taraf saha multicast adresi (FF05::2)
- Her ünicast adres için istenen düğüm adresi
- Katılınan grupların multicast adresleri

3.5 IPv6 Adres Boşluğunun Alt Ağlanması

Ipv4 de olduğu gibi IPv6 adres boşluğu da alt ağlanmış ağ önekleri oluşturmaya yarayan sabitlenmiş değerli yüksek seviye bitleri kullanılarak bölünebilir.Bunlar hem yönlendirme yada adresleme hiyerarşisindeki (64'den kısa önekli) bir seviyeyi özetlemede hem de özel bir alt ağı yada

alt katmanını (64 bitlik öneke sahip) tanımlamada kullanılır.IPv4 alt ağlaması adresin kaynak ID kısmının tanımlanmasında IPv6 dan farklılıklar gösterir.IPv4 de alt ağlama şemasına bağlı olarak kaynak ID'si değişik uzunluklarda olabilir.Şimdiki tanımlaması ile ünicast IPv6 adreslerinde kaynak ID'si, IPv6 ünicast adresi arayüz ID kısmıdır ve her zaman 64 bite sabitlenmiştir.

3.6 NLA ID'ler için Alt Ağlama

Eğer bir ISP iseniz IPv6 adres boşluğunun alt ağlanması global adresinin NLA ID kısmının bölünmesi için kullanılan alt ağlama tekniklerinden ibarettir ve bu yönlendirme özetlemesi ile farklı müşteriler yada sizin ağınızı yükleme sağlayıcıları için farklı kısımların kalan adres boşluklarının bir araya getirir.Global adres bir en üst seviye toparlayıcı ile bir müşteri taraf arasındaki değişik ISP seviyelerini kullanabilecek 24 bitlik NLA ID alanına sahiptir.

En üst seviye bir toparlayıcıya ayrılmış bir global adres için adresin 16 biti sabitlenmiştir ve FP (001'ayarlı) ile TLA ID (13 bit uzunlukta)'yi karşılar.TLA ID önceden 8 biti sıfırlanmış Res kısmı tarafından talep edilir.Bundan dolayı bir global adresin NLA ID kısmı alt ağlanırken ilk 24 bit sabitlenmiştir.Bir global adreste IPv6 kalan hexa gösterimindeki yol göstericisi sıfırların bastırılmasından ötürü Res bitler hiçbir zaman gösterilmez.Bir global adresin NLA ID kısmının alt ağlanması 2 adımda gerçekleştirilir.

1. Alt ağlama için gerekli olan bit sayısının belirlenmesi
2. Yeni alt ağlama ağ öneklerinin birer birer sayılması

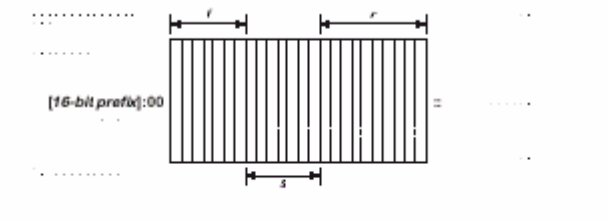
Burada tanımlanan alt ağlama tekniğinde NLA ID 'nin adres boşluğuna bölünmesiyle alt ağlama yapıldığı varsayılmıştır.Bu yapılırken NLA ID deki yüksek seviye bitlerin sabit değerli olmadığı kabul edilmiştir.Bu yapı hiyerarşik adresleme ile yönlendirmeyi iletirken gerekli değildir.Örneğin; NLA ID için alt ağları 0 dan 16,777,215'e kadar numaralandırarak kesin bir adresleme boşluğu oluşturmak da mümkündür.

3.6.1 Adım 1: Alt Ağlama Bit Sayısını Tespit Etmek

Alt ağlama bit sayısını belirlerken ağın coğrafik olarak veya müşteri bölümlemesi gibi bölümlemelere ayrılması durumunda ortaya çıkabilecek olası alt ağ örneklerini göz önünde bulundurmak gerekir.Hiyerarşik bir yönlendirme yapısında ne kadar ağ öneki,ne kadar bit ve kaç seviyelik bir hiyerarşiye ihtiyaç duyulacağının belirlenmesi gerekir.Bit sayısını yükseltirseniz hiyerarşi seviyesi seçeceğiniz,az seçerseniz numaralandırabileceğiniz alt ağ sayınız artar.Hiyerarşinin son seviyesi müşteri sitelerine 48 bitlik önekler atamak için kullanılır.

Örneğin;büyük bir ISP'nin dizayn edicisi 8 bitlik coğrafik seviyeye ve 8 bitlik müşteri seviyesine sahip iki katlı bir hiyerarşi kullanmaya karar veriyor diyelim.Bu durum her coğrafik bölgedeki müşteri bölümünün 8 bitlik alt ağlama alanına sahip olduğu anlamına gelir.(24-8-8)Bu aynı zamanda 256 tane 48 bitlik önek anlamına gelir.

Herhangi bir hiyerarşi de bir sonraki hiyerarşi seviyesi tarafından sabitlenmiş bit sayısına (f),geçerli hiyerarşi seviyesinde alt ağlama için kullanılan bit sayısına (s) ve bir alt seviye hiyerarşi seviyesi için elde kalan bit sayısına (r) sahipsinizdir.Her durumda f +s+r=24'tür.bu ilişik şekil 3.8'da gösterilmiştir.



Şekil 3.6

3.6.2 Adım 2: Alt Ağlama Ağ Öneklerini Numaralandırma

Alt ağlama için gerekli bit sayısına bağlı olarak yeni alt-ağlanmış ağ öneklerini listelemeliyiz.İki ana yaklaşım vardır:

- **Hexadecimal:** NLA ID'nin hexadecimal karşılığını kullanarak yeni alt ağlanmış ağ önekleri numaralandırır ve arttırırız
- **Decimal:** NLA ID'nin decimal karşılığını kullanarak yeni alt ağlanmış ağ önekleri numaralandırır ve arttırırız.Decimal alt ağlama tekniği sayılarla uğraşırken daha rahat bir yöntemdir.

Her iki yöntem de aynı sonucu verir.

3.6.2.1 Hexadecimal Yöntem Kullanarak Alt Öneklerinin Numaralandırılmış Bir Listesini Oluşturmak:

1. s'e bağlı olarak (alt ağlama için seçili bit sayısı), m (önek uzunluğu) ve m (alt ağlanmış ağ öneklerinin sabit uzunluğu) şu şekilde hesaplanır:

f=m-24

f sabitlenmiş NLA ID'lerdeki bit sayısıdır.

n=25

n; ağ öneki sayısı:

$i = 2^{24-(f+s)}$

i her başarılı NLA ID 'nin hexadecimal karşılığındaki artış miktarı:

ℓ:24+f+s

ℓ yeni alt ağlanmış ağ öneklerinin sabit uzunluğu

2. n girişli 3 sütunlu bir tablo oluşturun.ilk sütun ağ öneki sayısıdır. (1 ile başlar).İkinci sütun F'in değeridir.(NLA ID'nin hexadecimal karşılığı) ve üçüncü sütun alt ağlanmış ağ önek sayısı.

3. İlk giriş tablosunda NLA ID sütun girişi F ve alt ağlanmış ağ öneki ise orijinal ağ önekidir.(sabit uzunluklu) F'i elde etmek için son iki hexadecimal basamağı (ikinci hexadecimal bloğun) üçüncü hexadecimal bloğun dört hexadecimal basamağı ile birleştiririz.Örneğin 3000:4D:C00::/38 global adres öneki için F 0*4D0C002dır.

4. Sonraki tablo girişinde ,NLA ID sütunu için F, i kadar arttırılır.Örneğin ikinci tablo da NLA ID, F+i 'dir.

5. Alt ağlanmış ağ öneki sütunu için NLA ID 'yi iki ayrı 16 bitlik blok haline getiririz ve yeni alt ağlanmış ağ önekini elde etmek için 16-bitlik önekten sonra yerleştiririz.

6. 4. ve 5. adımların tablo tamamlanana kadar tekrar ederiz.

Örneğin;3 bitlik alt ağlanmış evrensel ağ öneki 3000:4D:C00::/38 elde etmek için öncelikle önek sayısı değeri,artışı ve yeni önek uzunluğunu hesaplarız.Başlangıç değerlerimiz:

F:0*4DC00, s=3 ve f=38-24=14 'dür.önek sayısı 8'dir. ($n=2^3$) Artış

$0x80\ (i = 2^{24-(14+3)} = 128 = 0x80)$ yeni önek uzunluğu 41'dir. $(l = 38 + 3).$

Daha sonra 8 girişli bir tablo hazırlayalım.Alt ağlanmış ağ öneki 3000:4D:C00::/41'dir.diğer girişler NLA ID 'nin arttırılması ile elde edilmiştir.

Table 3-4. **THE HEXADECIMAL SUBNETTING TECHNIQUE FOR NETWORK PREFIX 3000:4D:C00::/38**

Network Prefix Number	*NLA ID (hexadecimal)*	*Subnetted Network Prefix*
1	4D0C00	3000:4D:C00::/41
2	4D0C80	3000:4D:C80::/41
3	4D0D00	3000:4D:D00::/41
4	4D0D80	3000:4D:D80::/41
5	4D0E00	3000:4D:E00::/41
6	4D0E80	3000:4D:E80::/41
7	4D0F00	3000:4D:F00::/41
8	4D0F80	3000:4D:F80::/41

Tablo 3.4 ----------

3.6.2.2 Onluk Sistem Kullanarak Ağ Sabitlerinin Numaralanmış Listesini Oluşturmak:

1. s (ağ için seçili bitlerin sayısı) ve m (ağ sabitlerinin uzunluğu)'e bağlı olarak ve F (NLA ID 'nin hexadecimal değeri), aşağıdakiler hesaplanır.

$$f = m - 24$$

f , NLA ID 'de daha önceden sabitlenmiş bitlerin sayısı

$$n = 2^s$$

n , elde edilmiş network(ağ) sabitleri sayısı

$$i = 2^{24-(f+s)}$$

i , onluk forma çevrilmiş her başarılı NLA ID arasındaki artan değerdir.

$$l = 24 + f + s$$

l , yeni ağ sabitlerinin sabit uzunluğudur.

D: F'nin onluk sunumu

2. n tane dört sütunlu bir tablo oluşturalım.ilk sütun network sabiti sayısıdır (1 ile başlar),ikinci sütun NLA ID bölümünün (yeni ağ sabitine ait) onluk sunumu,üçüncü sütun NLA ID'nin hexadecimal sunumu,üçüncü sütun NLA ID 'nin hexadecimal sunumu,dördüncü sütun ise yeni alt ağ sabiti sayısıdır.

3. ilk girilen tablo da NLA ID ‘nin onluk sunumu D,hexadecimal sunumu F,alt ağ network sabiti sayısı ise orijinal ağ sabiti sayısının yeni değeridir.

4. Sonraki tabloyu hazırlarken ,ikinci sütun için NLA ID’nin onluk değerini i kadar arttırın.örnek olarak ikinci tablo girişinde ID’nin onluk sunum değeri D+i olacaktır

5. Üçüncü sütunda NLA ID’nin onluk değerini hexadecimale çevirin.

6. Dördüncü sütun da NLA ID’yi iki ayrı 16 bitlik bloğa ayırarak (hexadecimal halde)yeni alt ağın 16 bitlik sabitinden hemen sonra yerleştirin.Örnek olarak ikinci tablo için yeni alt ağ sabiti: [16 bitlik sabit] : [F+i (hexadecimal değeri)]::/ l.

7. 4’ten 6’ya kadar olan maddeleri tablo tamamlanana kadar sürdürün.

Örnek olarak 3 bitlik alt ağı olan bir evrensel ağ öneki 3000:4D:C00::/38,öncelikle ağın önek sayısı hesaplanır,daha sonra artış ve yeni önek uzunluğu hesaplanır.Başlangıç değerlerimiz:

F=0*4D0C00, s=3 ve f=38-24=14’dür.önek sayısı=8 (2^3).Artış ise

$128\ (i = 2^{24-(14+3)} = 128)$.

Yeni önek uzunluğu =41 (l=38+3).

Başlangıç NLA ID’nin onluk karşılığı =5049344 (D=0*4D0C00)

Daha sonra 8 girişli bir tablo yapacağız.Alt ağ öneki ,1 için 3000:4D:C00::/41.Tablodaki ek girişler NLA ID ‘nin i kadar arttırılmış halleri içindir.tablo 3-5’de gösterilmiştir.

Table 3-5. **THE DECIMAL SUBNETTING TECHNIQUE FOR NETWORK PREFIX 3000:4D:C00::/38**

Network Prefix Number	*Decimal Representation of NLA ID*	*Hexadecimal Representation of NLA ID*	*Subnetted Network Prefix*
1	5049344	4D0C00	3000:4D:C00::/41
2	5049472	4D0C80	3000:4D:C80::/41
3	5049600	4D0D00	3000:4D:D00::/41
4	5049728	4D0D80	3000:4D:D80::/41
5	5049856	4D0E00	3000:4D:E00::/41
6	5049984	4D0E80	3000:4D:E80::/41
7	5050112	4D0F00	3000:4D:F00::/41
8	5050240	4D0F80	3000:4D:F80::/41

Tablo 3.5

3.7 SLA ID LER VE ALT AĞ ID'LER;

Bir firmadaki çoğu sistem yöneticileri için IPv6 adresleme alanı, SLA ID'yi paylaştırma (evrensel adres için) veya yerel ağ adresinin alt ağ bölümü için (yönlendirme özeti için yetkilendirme amacıyla)gereklidir.

Evrensel adres firmaların sitelerinde kullanmaları için 16-bitlik bir SLA ID alanına sahiptir.sitenin yerel adresi 16 bitlik bir alt ağ ID'ye sahiptir.

Her durumda adresin ilk 48 bitlik bölümü sabittir.Evrensel adres için ilk 48 bit sabittir ve bir ISP tarafından tahsis edilmiştir.Site yerel adresi için ilk 48 bit FECO::/48'e sabitlenmiştir.

Evrensel veya yerel bir sitenin adres alanını alt ağlamak için iki adımlık bir prosedürü gerektirir.

1. Alt ağlamak için kullanılacak bit sayısını belirleyin.
2. Yeni alt ağ sabitlerini numaralandırın.

Burada alt ağlama tekniği tanımlanırken,alt ağlamanın 16 bitlik adres alanını alt ağdaki üst sıra bitleri kullanılarak elde edildiği varsayılmıştır.her ne kadar bu yöntem hiyerarşik adresleme ve yönlendirmeyi bir üst sınıfa taşısa da çok gerekli değildir.

Örnek olarak az sayıda alt ağa sahip küçük bir firmada bir düz adresleme alanı yaratarak alt ağ kimliklerini 0'dan başlayarak numaralandırabiliriz.

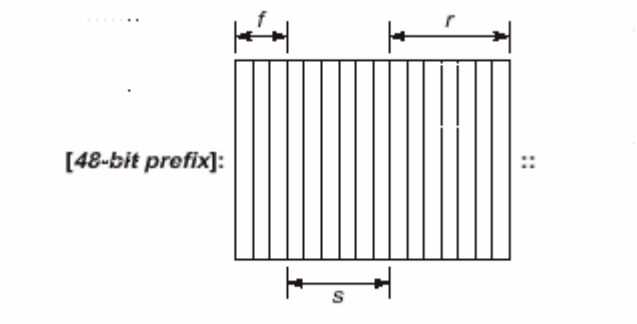
"Yerel kullanım ünicast adresleme" bölümün de açıklandığı üzere aynı alt ağlama şemasını hem yerel hem global ağ öneklerini adreslerken kullanabiliriz.

3.7.1 Adım 1: Alt Ağlama Bit Sayısını Tespit Etmek

Alt ağlama bitleri sayısını tespit ederken coğrafik veya departmantal bölünme durumlarındaki olası alt ağ öneki sayısı göz önüne alınır.Hiyerarşik bir yönlendirmede ne kadar ağ öneki ve ne kadar bite gereksinim duyulacağı belirlenmelidir.

Örnek olarak bir ağ yöneticisi bir coğrafik veya departmansal bölünme sonucu iki seviyeli bir hiyerarşi kurmak istiyor ve coğrafik seviye için 4 bit, departmantal seviye için 6 bit kullanılıyor.Böylece (16-6-4=6) » Her departman için sadece $64 (= 2^6)$ alt ağ kullanılıyor.

Verilen herhangi bir hiyerarşide elinizde sabit sayıda bit olacaktır.Bir üst seviye tarfından sabitlenen bit sayısı 'f ', geçerli seviye hiyerarşisi tarafından kullanılan bir sayısı 's' ve bir seviye alt ağlama için kalan bit sayısı 'r' =>f + s + r =16'dır.



Şekil 3.7 f,s,r Arasındaki İlişkiyi Gösterir

3.7.2 Adım 2: Alt Ağlama Ağ öneklerini Numaralandırma;

Alt ağlama için gerekli bit sayısına bağlı olarak yeni alt ağlanmış ağ öneklerini listelemeliyiz.İki ana yaklaşım vardır;

1. **hexadecimal:** Alt ağ kimliklerine ait yeni ağ önekleri hexadecimale çevrilir ve arttırılır.
2. **decimal:**Alt ağ kimliklerine ait yeni ağ önekleri decimale çevrilir ve arttırılır.

İki metoda aynı sonucu verir

3.7.2.1 Hexadecimal Yöntem Kullanarak Alt Öneklerinin Numaralandırılmış Bir Listesini Oluşturmak:

1. s'e bağlı olarak (alt ağlama için seçili bit sayısı), m (önek uzunluğu) ve F (alt ağ sayısının hexadecimal değeri)ise;

f=m-48

f sabitlenmiş alt ağ ID'lerdeki bit sayısıdır.

$$n = 2^s$$

n; ağ öneki sayısı

$$i = 2^{16-(f+s)}$$

i , her başarılı alt ağ ID'sinin hexadecimal karşılığındaki artış miktarı

$$l = 48 + f + s$$

l, yeni alt ağlanmış ağ öneklerinin uzunluğu

2. İki sütunlu ,n girişli bir tablo oluşturun.İlk sütun ağ öneki numarasıdır (1 ile başlar) ve ikinci sütun yeni alt ağlanmış ağ önekidir.

3. İlk tablo girişinde F'e bağlı olarak ,(alt ağlanan ID'nin hexadecimal değeri),alt ağlanan değeri,alt ağ öneki; [48-bit önek] : F+i: :/ ℓ.

4. Sonraki tablo girişinde ,yerel site veya evrensel adrese ait alt ağ Id değerini i kadar arttırın.Örneğin; ikinci tablo girişinde alt ağlanan önek; [48 bit önek]: F+ i ::/ ℓ

5. Tablo tamamlanan kadar adım 4'ü tekrarlayın.

Örneğin; 3 bit alt ağlanmış yerel site ağ öneki FEC0:0:0:C000::/51 için ,öncelikle önek sayısını,artışı ve yeni önek uzunluğu hesaplamalıyız.Başlangıç değerlerimiz ;

F=0*C000 , s=3 ve f=51-48=3.

Önek sayısı =>($n=2^3=8$).

Artış;

$$0x400\ (i = 2^{16-(3+3)} = 1024 = 0x400).$$

Yeni önek uzunluğu=>54 (ℓ=48+3+3)

Daha sonra 8 girişli bir tablo yapalım.Ağ öneki 1 için giriş FEC0:0:0:C00::/54.Ek girişler ağ önekinin i kadar artırımıyla sağlanır.Tablo 3-6'da gösterilmiştir…

Table 3-6. THE HEXADECIMAL SUBNETTING TECHNIQUE FOR NETWORK PREFIX FEC0:0:0:C000::/51

Network Prefix Number	*Subnetted Network Prefix*
1	FEC0:0:0:C000::/54
2	FEC0:0:0:C400::/54
3	FEC0:0:0:C800::/54
4	FEC0:0:0:CC00::/54
5	FEC0:0:0:D000::/54
6	FEC0:0:0:D400::/54
7	FEC0:0:0:D800::/54
8	FEC0:0:0:DC00::/54

Tablo 3.6

3.7.2.2 Decimal Metod Kullanarak Alt Ağ Öneklerinin Numaralandırılmış Bir Listesini Oluşturmak

1. s 'ye bağlı olarak (alt ağlama için seçili bit sayısı) , m (önek uzunluğu) ve F (alt ağ sayısının hexadecimal değeri) ise;

f =m- 48

f ;sabitlenmiş alt ağ ID'lerdeki bit sayısıdır.

$$n = 2^s$$

n; ağ öneki sayısı

$$i = 2^{16-(f+s)}$$

i , her başarılı alt ağ ID'sinin değerinin artış miktarı

$$l = 48 + f + s$$

l, yeni alt ağlanmış ağ öneklerinin uzunluğu

D=F'in decimal karşılığı

2. n girişli 3 sütunlu bir tablo oluşturun.İlk sütun ağ önek numarasıdır.(1 ile başlar) İkinci sütunda yeni ağ önekinin alt ağ kimliğinin decimal karşılığı yer alır.
3. İlk tablo girişte alt ağ ID'nin decimal karşılığı D ve ağ öneki [48 bit önek]:F::/*l*.
4. Sonraki giriş ikinci sütun için alt ağ ID'sinin decimal değeri 'i 'kadar arttırın.Örneğin ikinci tablo da 'D' yerine 'D+i' kullanılıyor .
5. üçüncü sütun için alt ağ ID'sinin onluk karşılığını hexadecimale çevirin ve önek için; [48 bit önek]:[alt ağ ID]::/ *l*.

Örneğin ikinci tablo girişinde alt ağ önek için;

[48-bit önek]:[D+i (hexadecimale çevrilmiş)]::/*l*…

6. 4. ve 5. adımları tablo tamamlanan kadar tekrarlayınız.

Örneğin; 3-bit alt ağlanmış yerel site öneki; FEC0:0:0:C000::/51 ise önek sayısı değerini, artışı, yeni önek uzunluğunu ve başlangıç alt ağ ID'si decimal karşılığını hesaplamalıyız.

Başlangıç değerlerimiz=> F=0*C000, s=3 ve f =51-48=3

Önek sayısı=> 8($n=2^3$)

Artış;

$1024\ (i = 2^{16-(3+3)})$.

Yeni önek uzunluğu 54 (*l*=48+3+3).

Başlangıç alt ağ ID'si onluk karşılığı 49152 (D=0*C000=49152)

Daha sonra 8 girişli bir tablo hazırlayacağız.Ağ önek: 1 için giriş 49152 ve FEC0:0:0:C000::/54. Tablodaki ek girişler ağ önekinin 'i' kadar arttırılması ile elde edilir.Tablo 3-7'de gösterildiği gibi;

Table 3-7. THE DECIMAL SUBNETTING TECHNIQUE FOR NETWORK PREFIX FEC0:0:0:C000::/51

Network Prefix Number	*Decimal Representation of Subnet ID*	*Subnetted Network Prefix*
1	49152	FEC0:0:0:C000::/54
2	50176	FEC0:0:0:C400::/54
3	51200	FEC0:0:0:C800::/54
4	52224	FEC0:0:0:CC00::/54
5	53248	FEC0:0:0:D000::/54
6	54272	FEC0:0:0:D400::/54
7	55296	FEC0:0:0:D800::/54
8	56320	FEC0:0:0:DC00::/54

Tablo 3.7

3.8 IPv6 ARAYÜZ BELİRLEYİCİLERİ

Bir IPv6 ünicast adresinin tanımlanan son 64 biti,IPv6 adresinin benzersiz olarak tanımlanmış 64 bitlik önekinin arayüzüdür.IPv4'de sunucu ve düğüm,IPv4 alt ağın arayüzünün mantıksal tanımlayıcılarıdır.IPv4 sunucu ID'leri alt ağ şemsındaki değişken uzunlukları ve verilmiş alt ağda ne kadar arayüze izin verileceğinize bağlıdır.Örneğin;8-bitlik sunucu ID'sinde $2^8 - 2$ =254 olası yönetici ID'si vardır.

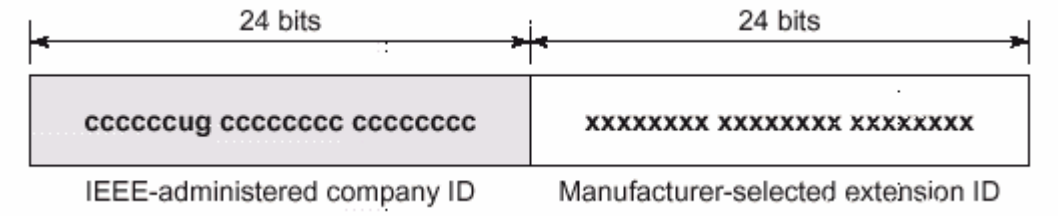
IPv6'da arayüz ID'sinin uzunluğu sabittir.Uzunluk 64 bite sınırlı değildir ve aynı alt ağda 2^{64} olası sunucuya kadar çıkabilir.Ayrıca IPv6 arayüz ID'si 64 bit uzunluğundadır.Böylece hali hazırdaki 48 bit MAC adreslerini(en çok kullanılan LAN teknolojisi) ve 64 bit MAC adreslerini (IEEE 1394 veya FireWirw) ve gelecekteki teknolojileri karşılayabilir.

3.8.1 EUI 64-Adres Bazlı Arayüz Tanımlayıcıları

Bir IPv6 arayüz tanımlayıcısının elde edilmesi için en yaygın yolu MAC adresinin ağ kartları için yeni bir türü olan EUI-64 adresidir.EUI-64 adresini anlamak için MAC adresinin IEEE 802 olarak bilinen formatını incelemek yeterlidir.

3.8.2 IEEE 802 Adresleri

Jetonlu halka,Ağ,Fiber Data Dağıtım Arayüzü (FDDI) gibi 48 bit adresleme,kullanılan yaygın Ağ Teknolojileri için kullanılan ağ kartları IEEE 802 olarak bilinir.24-bitlik üretici ID'si ve 24 bitlik uzatılmış ID içerir.Üretici ID'sinin kombinasyonu her üretici tarafından benzersiz olarak atanır ve evrensel olarak benzersiz bir 48 bitlik bir adres oluşturur.Buna MAC ADRESİ denir



Şekil 3.8 MAC Adresi

3.8.3 Evrensel / Yerel (U/L)

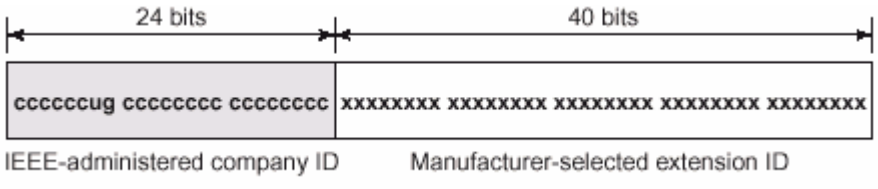
En düşük değerli bitten sonra gelen bit (ilk byte'ta)adresin evrensel veya yerel yönetimini gösterir.Eğer U/L biti 0!a ayarlanmışsa adresi IEEE yönetiyor demektir.U/L biti 1!e ayarlanmışsa adres yerel olarak yönetiliyor demektir.Bu durumda ağ yöneticisi üretici adresi üzerine farklı bir adres tanımlamış demektir.Bu durum yukarıdaki şekilde gösterilmiştir.

3.8.4 Bireysel / Grup (I /G)

İlk byte'ın düşük değerli biti adresin bireysel adres mi olduğunu (ünicast), grup adresi(multicast) mi olduğunu belirler.0'a ayarlanmışsa adres ünicast adres, 1'e ayarlanmışsa multicast adresidir.tipik 802.x ağlarında U/L ve I/G bitleri genelde 0'a ayarlıdır.

3.8.5 IEEE EUI-64 Adresleri

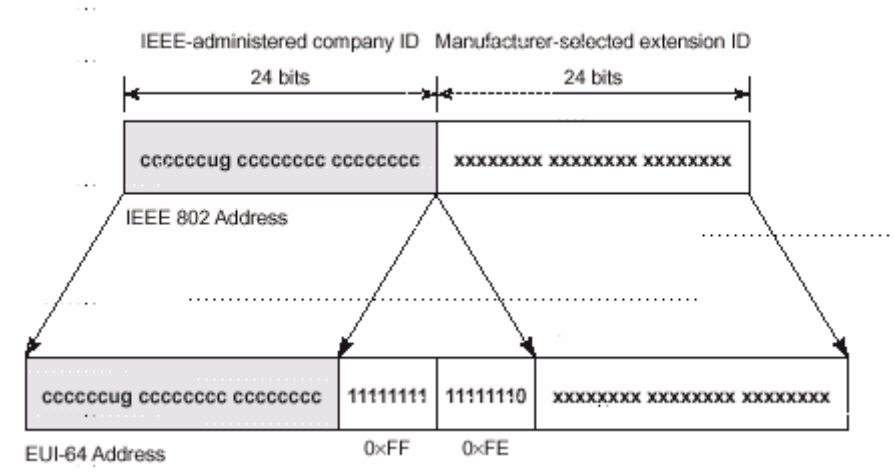
IEEE EUI-64 adresi ağ arayüzleri adreslemesine yeni standartlar getirir.Üretici ID'si yine 24 bit uzunluğunda olmakla beraber uzatılmış ID 40 bite çıkmıştır.EUI adresleri U/L ve I/G bitlerini IEEE 802'deki gibi kullanılır.



Şekil 3.9 IEEE EUI-64 Adres Yapısı

3.8.6 IEEE 802 Adreslerini EUI-64 Adreslerine Dönüştürmek

Bir IEEE 802adresinden EUI 64 adresi oluşturmak için 16 bitlik 1111111111111110 (0xFFFE) değeri IEEE 802 adresinde üretici ID'si ve uzatılmış ID arasına yerleştirilir.



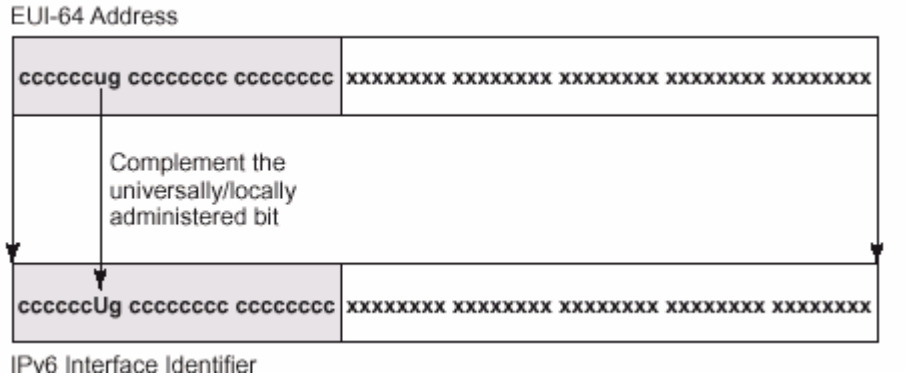
Şekil 3.12 IEEE 802 Adreslerini EUI-64 Adreslerine Dönüştürme Şekli

3.8.7 IPv6 Adresleri İçin Arayüz Tanımlayıcıları Oluşturmak;

IPv6 ünicast adresleri için 64 bit arayüz tanımlayıcısı oluştururken EUI-64 adresindeki U/L biti terslenir.(0 ise 1, 1 ise 0 yapılır)

Bu biti terslemekteki asıl amaç yerel olarak yönetilen EUI-64'ün sıkıştırılabilirliliğini arttırmaktır.Bu yerel yönetilen adresleri numaralandırmada kullanılan yaygın bir

yoldur.Örneğin;noktadan noktaya bağlantıda bağlantının bir yüzüne 02-00-00-00-00-00-01 adresini atarken diğer yüzüne 02-00-00-00-00-00-02 atanabilir.U/L biti terslenmemişse bu kez yerel bağlantı adresleri FE80::200:0:0:1 ve FE80:200:0:0:2 haline gelir.Ancak terslenirse FE80::1 ve FE80::2 olur.

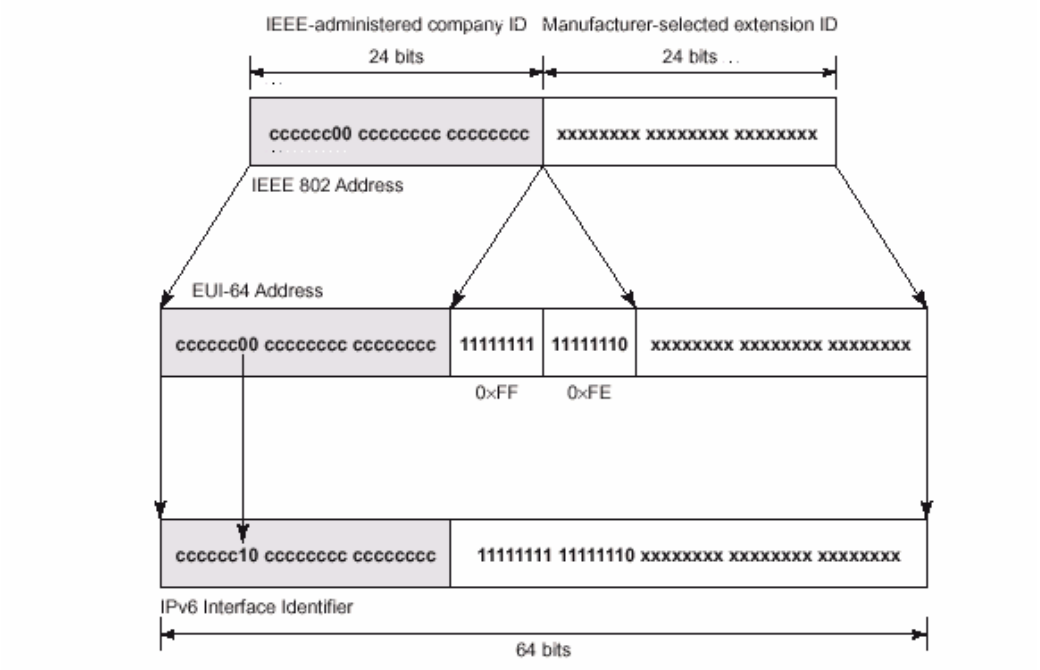


Şekil 3.13 IPv6 Adresleri İçin Arayüz Tanımlayıcıları

NOT: Eğer IPv6 arayüz tanımlayıcısının 7.biti 0 olarak tanımlanmışsa adres yerel,1 olarak tanımlanmışsa evrensel olarak yönetilmektedir.

3.8.8 IEEE 802 Adreslerini IPv6 Arayüz Tanımlayıcılarına Dönüştürmek

Bir IEEE 802 adresinden IPv6 arayüz tanımlayıcısı elde etmek için öncelikle IEEE 802 adresini bir EUI 64 adresine yönlendirmek daha sonrada U/L bitini terslemek gerekir.Aşağıdaki şekil evrensel yönetilen ünicast bir adresin dönüştürülmesini göstermektedir.



Şekil 3.14 IEEE 802 Adreslerini IPv6 Arayüz Tanımlayıcılarına Dönüştürmek

3.8.9 IEEE 802 Adres Dönüştürme Örneği;

A sunucusu 00-AA-00-3F-2A-1C MAC adresine sahip olsun Öncelikle bu adresi 3. ve 4. byte'larının arasına FF-FE ekleyerek EUI-64 formatına çevirmeliyiz.Böylece 00-AA-00-FF-FE-3F-2A-1C haline gelir.Daha sonra U/L bitini yani ilk byte'ın 7. bitini terslemeliyiz.Böylece 00000000 olan ilk byte 00000010 (0x02) haline gelir.Sonuç olarak 02-AA-00FF-FE-3F-2A-1C haline gelen adres kalan hexadecimal formuna çevrilirse 2A:FF:FE3F:2A1C arayüz tanımlayıcısı elde edilir.

4. IPv6'ya GEÇİŞ SÜRECİ

4.1 Zamanlama Sorunları

ACM'in (Association for Computing Machinery) 1999'daki SIG (Special Interest Group) konferansında (SIGCOMM99), AT#&T'nin bilimsel araştırmalar yöneticilerinden Sandy Fraser, Internet mimarisine ilişkin endişelerini dile getirmişti. Ölçeklenebilir mi? Niye hâlâ IPv4'ten IPv6'ya geçmedik? Çok övülen Internet Engineering Task Force (IETF) neden bir şey yapmıyor?

IPv6 tartışmasındaki problemlerden biri, tüm IPv4 adreslerinin tam olarak ne zaman tükeneceğinin bilinmemesidir. İyimser olanlar IPv4'ün birkaç on yıl daha idare edeceğini söylerken, kötümser olanlar sadece birkaç yıl kaldığını iddia ediyorlar. Yine de IPv6'ya geçiş için büyük bir baskı var. Çin ve Japonya gibi ülkeler (fazla IPv4 adresi almadılar), gelişmekte olan endüstrilerle birlikte bunun en önemli destekçileri konumundalar. Yeni nesil mobil dijital sesli görüşme sağlayıcıları ve ağa bağlı aygıtlar üreten firmalar da, milyonlarca cihaz için IP adreslerine ihtiyaç duyacaklarına dikkat çekiyorlar.

IETF tarafında da çalışmalar yapılıyor. Ekibin yeni nesil Internet protokolü (IP next generation–IPng) çalışma grubu, IPv6 spesifikasyonları ve yeni kurulan IPv6 Forumu üzerinde yoğun bir şekilde çalışıyor. Amaç, yeni Internet'i kurmak için yeni IP protokolünü geliştirmek.

4.2 Harekete Geçmek

Vint Cerf, "Uygulama yapan çoğu kişi IP adres boşluğunun neye benzediğini bilmiyor. Buna dikkat göstermesi gereken birileri varsa bu ISS'lerdir. Bunlar yakın vadede NAT (Network Address Translation–Ağ Adres Dönüşümü) sistemine güveniyorlar" şeklinde konuşuyor.

Uzun vadeli zaman aralığının IPv6 kararlarını ertelemelerine izin verdiğini düşünen ağ yöneticileri bunu bir kez daha düşünmeliler. IPv6 ağlarını planlama, kurma ve test etmek için çok erken sayılmaz. Geçişi ertelemek yerine şimdiden hazırlanarak, sağlam bir bilgi tabanı oluşturabilirler ve 2000 yılı (Y2K) programlama çabalarına benzer bir kargaşaya düşmeden bu işi halledebilirler.

4.3 Adresleme ve Yönlendirme

IPv6, şu anda kuruluşların içinde ve aralarında bulunan birkaç problemi çözmeye yardım ediyor. IPv6 küresel ölçekte, Internet omurga tasarımcılarının esnek ve genişletilebilir bir küresel yönlendirme hiyerarşisi oluşturmalarına izin verecek. Internet omurgası (büyük işletmeler ve ISP şebekelerinin birleştiği yer), ulusal ve uluslararası telefon sistemlerindeki yapıya benzeyen bir hiyerarşik adresleme sisteminin korunmasına bağlıdır. Örneğin, büyük ve merkezi ofis telefon anahtarları, uzun mesafeli bir telefon çağrısını doğru yerel noktaya bağlamak için yalnızca üç rakamlı bir ulusal alan koduna ihtiyaç duyar.

Mevcut IPv4 sistemi, Internet omurgasına bağlı şebekelerin trafiğini sınıflandırmak için de bir adres hiyerarşisi kullanır. Bir adres hiyerarşisi olmazsa, omurga yönlendiricilerinin yönlendirme tablosu bilgilerini dünyadaki tüm şebekelerin erişebileceği bir yerde saklaması gerekir. 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 başladı. CIDR, Internet hiyerarşisinin çeşitli seviyelerinde "yön kümelemeye" izin veriyor. Böylece, omurga yönlendiricilerinin pek çok alt seviye şebekeye ulaşmak için kullanılabilen tek bir yön tablosu girişini saklaması yeterli oluyor.

CIDR'ın bir dezavantajı, etkili ve ölçeklenebilir bir hiyerarşiyi garanti etmiyor olması. 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 (özetlenmelidir). CIDR öncesinden gelen eski IPv4 adres atamaları ve mevcut erişim sağlayıcı hiyerarşisi, genellikle özetleme işini kolaylaştırmaz. 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 etkiliyor. Ayrıca, IPv4 sitelerinin yeniden numaralanması

da (örneğin, bir kullanıcının bir ISS'den başkasına geçmesi ya da bir adrese bakım yapılırken değiştirilmesi ya da rotaların birleşmesi) gereksiz derecede karışık ve dolayısıyla IPv6'dan daha pahalı.

4.4 Geçiş Mimarisi

IPv6'nın IPv4'le birlikte çalışması (ya da içinden geçmesi–tunneling) kaçınılmaz bir durumdur. İyi haber ise, IPv6 sıra bağımlılıkları oluşturmuyor: Şebeke mimarları önce host'ları sonra yönlendiricileri ya da önce yönlendiricileri sonra host'ları terfi edebilirler. Hatta bazı host ve yönlendiricileri terfi edip kalanları sonraya bırakabilirler. "Üç birlikte çalışma mekanizmasından (tüneller, çevirme ya da iki yığın) hangisinin hakim olacağı" sorusu henüz cevap bulmuş değil.

4.5 Akıllı Düğümler

Servis sağlayıcılar IPv6 omurgalarını kurana ve IPv6 servislerini sunana dek, noktadan noktaya IPv6 uygulamalarının IPv4 ağları üzerinden geçmesi (tünelleme–tunneling) gerekecek. Bu, bir IPv6 paketinin bir IPv4 paketinin içerisine sokulmasıyla sağlanır. Bir IPv6 düğümünden çıkan IPv6 paketleri, IPv4 içine yerleştirilir ve IPv4 şebekesi üzerinden iletilir. Tünelin öbür ucundaki düğüm, IPv4 paketini ayrıştırır ve hedef düğüme gönderilmeye hazır olan IPv6 paketini ortaya çıkarır.

4.6 Geçiş Stratejileri

IPv6'ya geçiş stratejileri çok çeşitli. Bazı durumlarda, IPv4 okyanusları ile çevrili küçük IPv6 adacıkları oluşturacak şekilde şebekeler bütün olarak terfi edilebilir. Böyle olduğunda, IPv6 şebekeleri içindeki düğümlerin IPv4 desteğine sahip olması gerekmez. Bununla birlikte, harici uyumluluğu desteklemek için şebeke sınırlarındaki cihazların IPv4'ü desteklemesi gerekir. Dahili IPv6 düğümleri, kendi aralarında direkt olarak ve diğer IPv6 şebekeleriyle de ikili IP yönlendiricileri arasındaki tünelleri kullanarak haberleşebilirler.

Alternatif olarak, düğümleri ayrı ayrı IPv4 ve IPv6 destekleyecek şekilde terfi ederek, operatörler bir çeşit "üzümlü kek" mimarisi oluşturabilirler. Burada düğümler, aynı bağlantı üzerindeki bir başka düğümle direkt olarak haberleşirken, uzak IPv6/IPv4 düğümleriyle de tüneller yoluyla haberleşirler. Bu yaklaşım, kurumların, düğümleri uzak IPv6 düğümleri ve şebekelerine erişime teker teker terfi etmesine izin verir. Öte yandan, IPv6 kaynaklarına erişim için tünellerin elle konfigürasyonunu gerektirdiğinden işleri biraz güçleştirir.

4.7 IPv6 Altyapısı

IETF, IPv6 protokollerinin gelişimde kendine düşeni yaptı. Internet Corporation for Assigned Names and Numbers (ICAAN), IPv6 adres tahsisi ve atanması ile ilgili dokümanını yayınladı (www.arin.net adresine bakınız). 1996'dan bu yana, 40'tan fazla ülkede 400 civarında şebeke 6bone (www.6bone.net) IPv6 ağına bağlandı.

4.8 Perde Arkasındakiler

İlk uygulayıcıların, şebekelerine IPv6 desteğini eklemek için pek çok seçeneği olacak. Çok sayıda yönlendirici üreticisi IPv6'yı destekliyor: 3Com (ABD), Ericsson Telebit (Danimarka), Hitachi Ltd. (Japonya), Nokia Telecommunications (Finlandiya) ve Northern Telecom Ltd. (Kanada). Linux kerneli de IPv6 desteğine sahip. Microsoft şu an için, Windows NT ile ve Windows 2000'in beta versiyonuyla çalıştığı bildirilen deneysel bir IPv6 yığınının alfa versiyonunu sunuyor.

4.9 Geçişle Başa Çıkmak

Ağ ürünleri imalatçıları eninde sonunda tüm ürünlerine IPv6 desteğini ekleyecekler, tıpkı şu an IPv4'ü destekledikleri gibi. Bazı uzmanlar, uygulama maliyetlerinin yeni bir işletim sistemi sürümü kurmanın maliyetiyle kıyaslanabileceğini söylüyorlar. Gerçekte, IPv6'nı desteklenmesi neticede para tasarrufu sağlayacaktır. IPv6'ya geçiş, yığılı (nested) NAT'lara (ISS kendi NAT adres boşluğunu kullanır fakat müşterilerinin paketlerini, kendi benzersiz NAT adres boşluğunu kullanan bir omurga içinde yönlendirir) geçiş kadar masraflı değildir.

Toplamda, bir 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 konfigürasyon protokolü (dynamic host configuration protocol–DHCPv6) versiyonu ile kendilerini otomatik olarak konfigüre edebilirler. Bunun yanında, komşu tespit işlevi sayesinde, bir IPv6 düğümü herhangi bir şebekeye eklenebilir ve bir insanın müdahalesine gerek olmadan bağımsız bir otokonfigürasyon sunucusuna bağlanıp uyumlu bir şekilde konfigüre edilebilir. Bu özellikler gerçek tak ve çalıştır şebeke erişimi sağlıyor. Komşu tespitini kullanarak, düğümler bağlantıları arasındaki hangi yönlendiricilerin mevcut ve erişilebilir durumda olduğunu otomatik olarak tespit edebilirler. Dahası, IP adreslerinin atanması işlemi kurumsal seviyede basitleştirilmiş olur.

Peki IPv6'nın sınırlarını test etmenin en iyi yolu nedir? İlk uygulayıcılar, genel şebeke bağlanabilirliğini etkilemeden IPv6 adacıkları oluşturabilirler. Araştırma grupları IPv6'yı genellikle bu şekilde destekliyorlar. Diğer gruplar da, ihtiyaçların zorladığı şekilde IPv6 desteği branşları ekleyebilirler. Dışarıdan içeriye doğru geçiş yaparken, kurumlar IPv6 yönlendiricilerini network sınırlarına yerleştirerek IPv6 ağlarına ve onların aracılığıyla bağlanabilirliğe izin verebilirler. Bu senaryoda kurumlar, IPv6 omurgalarına bağlanırlar ve IPv4 trafiğini onların içinden geçirirler.

4.10 IPv6: Evet! NAT: Hayır?

Elbette herkesin IPv6'yı desteklemesi beklenemez. Karşı görüşte olanlar, adres atanması ve yönlendirme problemlerinin başka mekanizmalarla kontrol edilebileceğini iddia ediyorlar. Bu tür mekanizmalar içerisinde özellikle şebeke adres çevirimi tartışılıyor. NAT'ı destekleyenler, onun IPv4 adres problemleri için kesin çözüm olduğunu iddia ediyorlar. Rakipleri ise, gerçek noktadan noktaya bağlanabilirliği (güvenlik açısından önemlidir) ortadan kaldıran NAT'ı, ortak çalışmaya aktif olarak zarar veren bir pürüz olarak görüyorlar (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, Birinci Dünya Savaşında çift kanatlı uçak kullanan bir pilotun büyük jetleri ve modern havaalanlarını tahmin etmesi kadar güçtür. Basitçe, Internet'in gelecekte nerelerde kullanılacağını ve tam etkisinin ne olacağını bilemeyiz.

Yine de, Internet'in iş, eğitim ve eğlenceyi değiştirdiğini biliyoruz (neredeyse yaşamımızın tüm yönleri). Dahası, Internet hızlandıkça, sağlamlaştıkça ve daha çok amaca hizmet etmeye başladıkça, daha da büyük değişikliklerin meydana geleceğini biliyoruz.

Gelecek Internet'e ilişkin tariflerin çoğu bant genişliği üzerinde yoğunlaşıyor. Fakat yeni nesil Internet, yüksek hızlı ağlardan öte bir şey. Esasen her şey uygulama. Problem teknolojinin neler yapabileceği değil, bizim onunla neler yapabileceğimiz.

5.1 İş İçin IPv6 (Noktadan Noktaya Servis Kalitesi)

İş dünyasındaki, interaktif multimedya ve yüksek bant genişliği isteyen ağ uygulamaları gereksinimlerini sürekli arttığı düşünülürse, IPv6, şirket Internet çalışmalarının ve büyük ölçekte de açık Internet'in varlığını sürdürebilmesi için çok önemlidir. Bu öneme ve ağ endüstrisindeki en parlak zekaların çabalarına rağmen, IPv6'nın doğumuyla birlikte, ileri dönük ağ stratejisi geliştirmeye çalışan ağ sahiplerini kolayca yanıltabilecek söylenti ve tarifler de ortada dolaşmaya başladı. Mevcut küresel Internet altyapımızı güncelleştirilmiş bir protokole taşımak için gereken işlerin çokluğu karşısında biraz bulanıklık zaten beklenir. Fakat, IPv6 ile ilgili söylentiler bu şekilde sürüp giderse, gelişmiş ağ servisleri için son kullanıcı ve ticari gereksinimler katlanarak artarken, Internet 20 yaşındaki protokol bileşenleriyle tıkanabilir. Şimdi yolu açma zamanı.

Resim 1. Internet'in geleceğini anlatan tanımların çoğu bant genişliğini öne çıkarıyor. Fakat yeni nesil Internet, yüksek hızlı ağlardan çok daha fazlasına sahip. Problem teknolojinin neler yapabileceği değil, bizim onunla neler yapabileceğimiz.

5.2 Güvenilirlik ve Ölçeklenebilirlik

Günümüz Internet'i ve yeni Internet arasındaki en büyük fark, yeni Internet'e güvenebilmemizdir: Internet kullanmak istediğimizde hazır olacak. Son kullanıcılar sürekli on-line olacak ve şimdiki dial-up bağlantı ve sisteme giriş aşamalarından geçmeden Internet'i kullanmaya başlayabilecekler. Ve her zaman her yerden erişilebilecek (yani durum sadece son kullanıcıların Internet'e anında bağlanması değil, kullanmak istedikleri siteler ve uygulamalar da erişilebilir olacak ve ağdaki yük değişimleriyle birlikte görünüp tekrar kaybolmayacak).

5.3 Gizlilik ve Güvenlik

Yeni Internet'in tüm potansiyelini ortaya çıkarmak için, son kullanıcıların on-line bilgilere ve işlemlere, daha önce kağıttaki belgelere olduğu kadar güvenmeleri gerekiyor. Sayısal bilgi önemli bir ürün haline geldiğinde, korunması ve gerçeklenmesi gereklidir. Bizim gördüğümüz, gönderilen ve bize gelenle aynı şey olmalıdır. Siber uzayda verilerimizi kontrol edebilmeli ve gizliliğimizi koruyabilmeliyiz. Bunun için kolay kullanılan, ucuz, değişmez güvenlik ve gerçekleme mekanizmaları gerekir. 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 araçlara ihtiyacımız var.

5.4 Servis Kalitesi: Hızlı ve Farklı Servisler

Günümüzde çoğu Internet kullanıcısı, on-line geçen vaktinin büyük bölümünde sadece bekliyor (web sitesine bağlanmak için bekliyor, sayfaların yüklenmesini bekliyor, yazılımın download edilmesini bekliyor). Yeni nesil Internet bize ihtiyacımız olan hızı sunacak.

IPv4 bir ayrıcalıklı servisler (differantiated services–DS) byte'ı taşır ve IPv6'da aynı iş için bir trafik sınıfı (traffic class–TC) byte'ı bulunur. Bunlar basit farklı servisleri desteklemek için düşünülmüştür. IPv4 ve IPv6, daha kompleks QoS uygulamaları için kaynak ayırma protokolünü (resource reservation protocol–RRP) destekliyorlar. IPv6 paket formatı yeni bir 24 bit'lik trafik akışı tanımlama sahası içeriyor ve bu da servis kalitesiyle ilgili ağ işlevlerini uygulayan üreticilere büyük fayda sağlayacak. Bu ürünler henüz planlama aşamasında olsalar da, IPv6 gerekli temeli hazırlayarak geniş QoS fonksiyonlarının (bant genişliyi rezervasyonu ve gecikme sınırları dahil) açık ve birlikte çalışabilir bir şekilde sunulmasına imkan veriyor. IPv6'daki QoS'in diğer bir faydası da, yönlendirmenin optimize edilmesi, için bir akış etiketi (IPv6 başlığı içinde bulunur) kullanılarak trafik akışlarının ayırt edilebilmesidir. Dahası, akış etiketi içerik şifreliyken dahi (mesela port numaraları gizli olduğunda), akışın niteliğini belirlemek için kullanılabilir.

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

5.5 Her Yerde Erişim

Günümüzde bir ev ya da ofise girdiğimizde tipik olarak bir ya da birkaç bilgisayar görürüz. Bir eve girdiğinizi ve karşınıza yüzlerce bilgisayar, PDA ve diğer cihazların çıktığını düşünün (hepsi Internet'e bağlı). 10-20 doların üstündeki her şeyin (buzdolabı, gömlek ya da bir bisiklet) Internet'e kablosuz olarak bağlandığı bir dünya düşünün. Böyle bir dünyada, bağlanabilirlik hava kadar olağan sayılacaktır (saatlerimiz, ağaçlar ve hatta köpeklerimiz veri yayacaktır). Kol saatiniz çağrı cihazı görevi görebilir. Bir evin çevresindeki ağaçlardaki alıcılar, ağaçların sulanması gerektiğini bize ya da bir sulama sistemine haber verebilir. Bir köpeğin tasması, nerede olduğunu bildirebilir. En iyisi de, yanlış arabaya takılan anahtarlar da nerede olduklarını Internet'te duyurabilecekler.

5.6 Taşınabilirlik

Bazı nedenlerden ötürü, IPv4'ün mobil bilgisayarda kullanımında güçlükler mevcut:

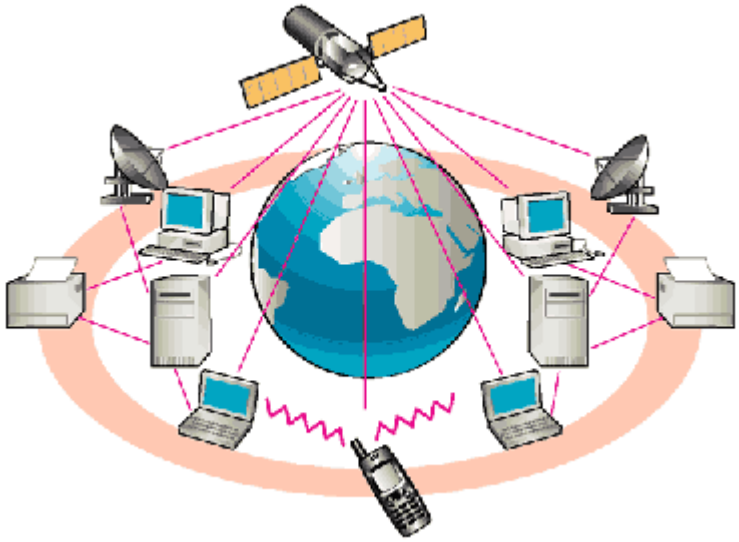
- Mobil bilgisayarlar, Internet'e girdikleri her nokta için bir aktarım (forwarding) adresine ihtiyaç duyarlar. IPv4'te bu adresi almak her zaman kolay olmaz.
- IPv4 düğümlerinde yaygın olarak bulunan iyi gerçekleme sistemleri, yönlendirme altyapısındaki tüm aracılara mobil düğümün yeni yerini bildirmek zorundadırlar.
- IPv4'te, mobil düğümlerin aynı şebekeye bağlı olup olmadıklarını anlaması zor olabilir.
- IPv4'te mobil düğümler, iletişim partnerlerine yer değişikliklerini bildiremezler.

IPv6 protokolünün tasarımındaki birkaç nokta, mobil bilgi işlem için dial-up desteğini direkt olarak sağlıyor ve ötesine de geçiyor. Hedef seçenekleri, otokonfigürasyon, yönlendirme başlıkları, paketleme, güvenlik ve anycast adreslerin gelişmiş kullanımı, IPv6'nın mobil tasarımına katkıda bulunuyor. (Anycast, bir gönderici ile alıcı grubu içinde göndericiye en yakın konumda bulunan alıcı arasındaki iletişimdir.) IPv6'nın mobil olma avantajı, mobil düğümlere daha iyi servis kalitesi veren akış etiketi yönetiminin ilavesiyle daha da ön plana çıkabilir.

5.7 Multicast ve Anycast

Internet sistemlerinde en hızlı büyüyen iş gereksinimlerinden biri de, video, ses, haberler, ekonomi bilgileri ve diğer zamana bağlı bilgilerin, benzer işlevli fakat coğrafi konumları farklı uç noktalardan oluşan bir gruba gönderilebilmesi becerisidir. Bu en iyi şekilde şebeke multicast teknikleriyle yapılabilir. Tipik olarak, bir sunucu multimedya ya da zamana duyarlı bilgi akımını başlatır. Sonra, multicast yetenekli bir ağ bu sunucunu paketlerini çoğaltır ve multicast grubundaki her bir aboneye verimli bir yoldan gönderir. Yönlendiriciler, grubun her üyesini multicast sunucusuna bağlayan bir paket dağıtım "ağacını" dinamik olarak oluşturmak için, Distance Vector Multicast Routing Protocol (DVMRP) ve Multicast Open Shortest Path First (MOSPF) gibi multicast protokollerini kullanırlar.

Yeni üyeler, yakındaki bir yönlendiriciye "katıl" mesajını göndererek multicast grubuna katılırlar. Dağıtım ağacı yeni rotayı içerecek şekilde ayarlanır. Multicast servislerinde, bir sunucu tek bir paket gönderebilir ve bu sonradan çoğaltılıp multicast grubuna ihtiyaca göre Internet altyapısı üzerinden gönderilir. Bu yöntemde sunucu ve ağ kaynakları tutumlu kullanıldığından, unicast ve broadcast çözümlerinden üstündür. (Unicast, ağ üzerinde tek bir alıcı ile tek bir gönderici arasındaki iletişimdir.) IPv4 için de multicast uygulamaları geliştiriliyor fakat IPv6 sağladığı çok geniş multicast adres boşluğu ve multicast yönlendirme bilgisinin bir sistemde yayılma derecesini kısıtlamak için kullanılabilen bir kapsama belirleyicisi ile, IP multicast becerilerini büyük ölçüde artırır. IPv6'nın multicast'i, unicast ve broadcast işlevlerini destekleyerek IPv4'ün broadcast özelliğinin yerini alan önemli bir IPv6 özelliğidir.



Resim 2. IPv6; hedef seçenekleri, otokonfigürasyon, yönlendirme başlıkları, paketleme, güvenlik ve anycast adresleri konularında üstün özelliklere sahip.

Anycast servisi de, IPv4'te bulunmayan başka bir IPv6 yeniliğidir. Anycast kavram olarak unicast ve multicast arasında bir yerdedir: İstenen sayıdaki düğüm üzerindeki bir veya daha fazla arabirim bir anycast grubu olarak gösterilebilir. Grubun anycast adresine gönderilen bir paket, gruptaki arabirimlerden sadece birine ulaşır ve tipik olarak bu, mevcut protokol ölçüleri içerisinde gruptaki "en yakın" arabirimdir. Bu, paketleri multicast grubundaki her bir üyeye gönderen multicast servislerinin zıddıdır. Bir anycast grubundaki düğümler özel olarak, unicast adres boşluğundan çekilen anycast adreslerini tanıyacak şekilde konfigüre edilmiştir.

5.8 Birlikte Çalışma ve Görüşme

Günümüz Internet'i, iletişim için güçlü bir ortamdır (bire bir, birden çoğa ve çoklu iletişim için). Gelecekte yeni uygulamalar ve arabirimler, kişilerin siber uzayda daha kolay ve sezgisel bir biçimde birlikte çalışmalarını sağlayacak. Yeni medya teknolojileri ile kullanıcılar;

- İş toplantısı için kilometrelerce ötedeki bir odaya "yürüyerek" girebilecek
- Bir "sanal galeriyi" ziyaret edip bir satış temsilcisinden almak istedikleri arabanın üç boyutlu bir modeli üzerinde bilgi alabilecek ya da
- 360 derece panoramik bir ekranın içine girip Kaliforniya'da bir kayalık gezintisine çıkabilecekler. Bu yeni iletişim araçları sayesinde kullanıcılar, en az karşılıklı görüşme kadar etkili bir şekilde iletişim kurabilecekler.

5.9 Mobil İletişim Dünyası

Bir takvim ve adres listesini, tüy kadar hafif ve katlanabilen bir elektronik kağıtta taşıdığınızı ya da kapıdan çıkarken bilgisayarınıza "Rakiplerimizin stratejileri hakkında bir rapor hazırla" diyebildiğinizi düşünün. Peki bir toplantıdayken "sanal kendinizi" başka bir toplantıya yollamaya ne dersiniz? Bu aslında iki yerde birden olmak değil midir?

Bu kişisel bilgi işlem hayalleri beş yıldan daha kısa bir sürede gerçekleşebilir. Compaq, Ericsson, IBM ve Hewlett-Packard, işleme gücünün üretilmiş hemen her üründe (alarmlı saatlerden kahve fincanlarına dek) bulunduğu yaygın ve şeffaf bir bilgi işlem dünyasının oluşturulmasını mümkün kılacak teknolojiler üzerinde çalışıyorlar. Dahası, bu cihazlar kablosuz ve kesintisiz bir şekilde bağlı olacaklar.

Sonunda teknoloji geliştiğinde, artık bunlara dikkat etmeyeceğiz ve düşünmeyeceğiz. Veriler mobil hale gelecek ve hücresel telefonlar, akıllı telefonlar, sayısal kişisel yardımcılar (personal digital assistant–PDA), elektronik kitaplar ve kağıt gibi çeşitli cihazlardan geçebilecek.

Kablosuz bant genişliğindeki ferahlık, bu cihazların çoğalmasını mümkün kılacak. Kablosuz veri iletişimindeki dar boğazlar, UMTS ve Bluetooth tabanlı yeni kablosuz teknolojiler sayesinde birkaç sene içerisinde ortadan kalkacak. Örneğin, 384 Kbps iletim hızına sahip üçüncü nesil hücresel şebekeler 2001'de Avrupa'da ve 2002 ya da 2003'te de ABD'de hizmete girecek.

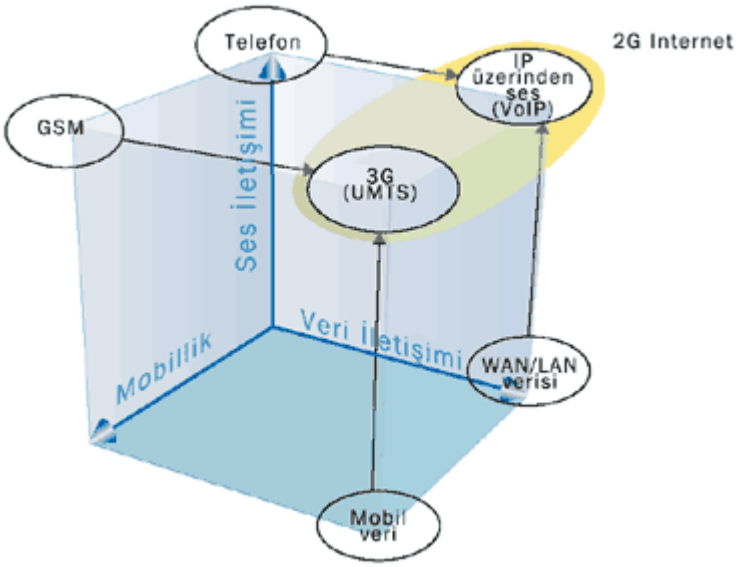
Çok uzak olmayan bir gelecekte, 802.11 kablosuz teknolojisinin (11 Mbps hızında çalışıyor ve saniyede 54 Mbit veri taşıması bekleniyor), geniş alan şebekesine (wide area network–WAN) şeffaf olarak entegrasyonuyla birlikte ağlar tamamen şeffaf bir hale gelecek. Bu sayede kullanıcılar, bulundukları yerden bağımsız olarak kesintisiz bir şekilde bir kampüs LAN'ına bağlı kalabilecekler. Kullanıcılar fiziksel olarak kampüs bölgesinden ayrıldıklarında, bağlantıları kesilmeden WAN'a aktarılacak.

2003 yılında, Internet'te ticaret hacmi 3,2 milyar dolara ulaşabilir ve bu da dünya ekonomisinin yüzde 10'u demektir. Fakat Internet buna hazır mı? Büyük yatırım siteleri (ör. Charles Schwab #& Co.) ve tüketici müzayede sitelerinin (ör. eBay) mevcut on-line aktiviteye yetişmeye çalıştığı düşünüldüğünde, Internet ve iş adamlarının günün her saatinde gerçekleşen milyonlarca ve belki milyarlarca işlemi idare edebilmek için daha çok yol almaları lazım.

Merak etmeyin yardım yolda. Yedekli, sağlam ve kendisini düzelten ağlar, yeni bir Internet iletişim protokolü ve daha iyi güvenlik geliyor (elektronik ticaret siteleri yüz milyonlarca müşteriye hizmet vermenin dışında bir de hacker ve elektronik korsanlarla baş etmek zorunda olacaklar).

6. SONUÇ

Uçsuz bucaksız adres boşluğuyla IPv6 çözümü, çok seviyeli hiyerarşik bir küresel yönlendirme mimarisi tanımlıyor. CIDR tarzı ekleri kullanarak, IPv6 adres boşluğu, yönlendirme özetlemeyi kolaylaştıracak ve omurga yönlendiricilerindeki yön tablolarının genişlemesini kontrol edecek bir şekilde tahsis edilebilir. IPv6 adreslerinin bolluğu, özel adres boşluklarına duyulan ihtiyacı ortadan kaldırıyor. ISS'ler, Internet'ten tam olarak yararlanmak için küresel ölçekte benzersiz adresler isteyen küçük şirketler ve dial-in kullanıcılara atamak için bol miktarda adrese sahip olacaklar. Kalabalık telefon şebekelerinden örnek verecek olursak, IPv6, aramaları yönlendirecek bir operatöre (otomatik ya da değil) gerek olmaksızın her ofise direk iletişim hatları sağlayarak paralel hat ihtiyacını ortadan kaldırıyor.



Resim 3. IPv6, Yeni Telekom Dünyası'nın anahtar bileşenidir.

Internet gerçek küresel bir ortam haline gelirken, çeşitli servisleri sağlam bir şekilde destekleme yeteneğine sahip bir ağ oluşturmak için yeniliklere ve kişilerin sebatkar çalışmalarına ihtiyacımız olacak. Metcalf Yasasına göre, bir ağın değeri, onu kullanan insanların karesine eşittir.

Şöyle düşünün: Bir ağa katıldığınızda sadece ondan faydalanmış olmuyorsunuz, başkaları için de ağın kıymetini artırıyorsunuz.