İÇİNDEKİLER

TEŞEKKÜR

Tez çalışmalarım sırasında araştırma olanağı veren, aynı zamanda çalışmamın her evresinde bana ilgisini esirgemeyen, önerilerini paylaşan hocam Sayın Yard.Doç.Dr. Rifat Çölkesen'e ve Prof. Dr. Ali Okatan'a teşekkürlerimi sunarım.

Süleyman Özgün SUNAL

İstanbul, MAYIS 2008

ŞEKİL LİSTESİ

TABLO LİSTESİ

. KISALTMA LİSTESİ

. PDU → Protocol Data Unit

. SDU → Service Data Unit

. Protok. → Protokol

. IPv4 → Internet Protokolu Versiyon 4

. IPv6 → Internet Protokolu Versiyon 6

. IPSec → Internet Protokolu Security

. L → Layer(katman)

ÖZET

IPv6 Protokolu, IETF tarafından İnternet'te şu an kullanılan IP Protokolu'nun yerine geçirilmek üzere tasarlanmıştır. Bu çalışmada öncelikle IP Protokolu ve onun, içinde yer aldığı OSI Modeli'ne değinilmekte ve ayrıntıları incelenmektedir. Daha sonra ise esas anlatılmak istenen hareketlilik protokollarına değinilmektedir.

IPv6 için kimi protokol geliştirmeleri sağlanmıştır. Hareketli IPv6 gibi. Örneğin yeni nesil İnternet Protokolu'nun getirmiş olduğu kolaylıklar sayesinde Hareketli IPv6 Protokolu'ndan yararlanılarak IPv6 paketlerinin hareketli cihazlara onların haberi olmaksızın yönlendirmesi (gizli yönlendirme) yapılabilmektedir. Yani, Hareketli IPv6 uygulandığında paket yönlendirme işlemleri konusunda hareketli cihazlar bilgiye sahip olmamaktadır. Üst katman protokolleri, ev aracı ile hareketli cihaz arasındaki veri giydirme işleminin farkına varamamaktadır.

Hareketli IP'de olsun ya da ufak farklılıklar gözeten onun bir sonraki uyarlaması olan hareketli IPv6'da olsun, hareketli her cihaz İnternet'e hangi noktadan bağlanırsa bağlansın ev adresi ile tanımlanmaktadır ve kendisine ulaşılabilmesi de geçici adresle bu ev adresinin ilişkilendirilmesine bağlıdır. Hareketli cihaz ev ağından ayrı iken de o an bulunduğu ağı işaret eden geçici bir adres edinmektedir. Hareketli IPv6'da her cihaz geçici adresi öğrenip değişmez adresle ilişkilendirip saklamakta ve sonra da bu iki adres kullanılarak paketler doğrudan hareketli cihazın geçici adresine gönderilmektedir.

SUMMARY(Abstract)

IP version 6 is being designed within the IETF(İnternet Engineering Task Force) as a replacement for the current version of IP protocol used in the İnternet. In this paper first of all this protocol and the OSI Model is explained that İnternet protocol resides in.

We have designed protocol enhancements for IPv6, known as Mobile IPv6, that allows transparent(invisible) routing of IPv6 packets to mobile nodes, taking advantage of the opportunities made possible by the design of IPv6 the next generation IP. In Mobile IPv6 also similarly in Mobile IPv4, except slight differences among them, each mobile node is identified by its home address all time regardless wherever it connects to the İnternet. While away from its home IP subnet ,a mobile node is also associated with a care-of address, which specifies the current location of the mobile node. In Mobile IPv6, by utilizing Routing header that is one of the extensions, any node is enable to learn and cache the temporary address associated with a mobile node's unchanged address, and then to send packets destined for the mobile node directly to it at this temporary address.

1. GİRİŞ

Son yıllarda İnternet bir hayli büyüdü ve artık neredeyse her eve girmeye başladı. Yalnız İnternet Protokolu'nun dayandığı bir temel vardı ki o da iletişim kurmak isteyen cihazların nadiren hareket edecek oluşu veya hareket etmeksizin bulunduğu yere çakılı kalmasıydı. Yani sisteme göre, cihaz hareket geçtiği anda sistem devre dışı kalacaktı. Bu süre içerisinde hareketli cihazların üretilmesi ve giderek yaygınlaşması artık hareketliliğe çare olacak bir yol arama çalışmalarını da beraberinde getiriyordu. Ve İnternet Protokolu'na hareketlilik özelliği katılması için ona özel bir protokol geliştirildi, adı da Hareketli IPv4'tü.

Bu çalışmada öncelikle protokol kavramına, OSI Modeli'ne, sonrasında IPv4 ve IPv6 Protokolu'na değinilmiştir. Ardından ise Hareketli IPv4 ile yeni nesil hareketlilik protokolu olan Hareketli IPv6 incelenmiş, getirileri sorunları ele alınmıştır. En son olarak da bir çok aksaklığı gideren yeni nesil hareketlilik protokolu ile ne gibi iyileştirmelerin yapılabildiği gösterilmiştir.

2. OSI BAŞVURU MODELİ

Açık sistem ara bağlaşımı (Open Systems Interconnection) (OSI) modeli ISO (Standartlaştırma için uluslararası organizasyon) tarafından geliştirmiştir. Amaç iki bilgisayar arasındaki iletişimin nasıl olacağını tanımlamaktır.

OSI Modeli herhangi bir donanım ya da bilgisayar ağı türüne göre değişiklik göstermemektedir. OSI'nin amacı ağ mimarilerinin ve protokollarının bir ağ ürünü bileşeni gibi kullanılmasını sağlamaktır.

OSI Modeli'nin ele alınmasındaki neden ise asıl konu olan İnternet Protokolu'nun da bu modelin neresinde, kaçıncı katmanda bulunduğunu tanıtmaktır.

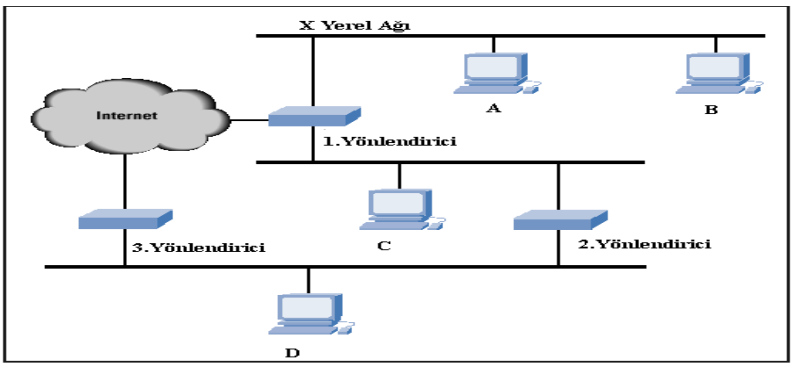
Protokol: Ağ protokolu, iki bilgisayar arasındaki iletişimi sağlamak amacıyla verileri düzenlemeye yarayan, standart olarak kabul edilmiş kurallar dizisidir.[1]

İnternet Protokolu'na Genel bir Bakış (IPv4)

IP (İnternet Protokolu), TCP/IP Protokol kümesinin çekirdeğidir ve 3.katmandaki ana protokoludur. 3.katman genel olarak aynı fiziksel ağdaki cihazlar arasında değil farklı ağlararasındaki paket teslimini yapar. İnternetwork adı verilen kavram da budur yani farklı ağlarda bulunan cihazlar arasındaki iletişimi sağlamak. IP bir mekanizmadır ki TCP/IP ağlarında paketin gönderilmesiyle ilgilenir. IP, 3.katman protokolu olarak TCP/IP yığınında 4.katmana yani bir üste servis sağlar ki 4.katman esasen TCP ve UDP protokollarıyla temsil edilir. Bu servis, TCP ya da UDP'nin paketlediği veriyi almak ve onu işleyip göndermektir. Sözü edilen servis ağlararası paket teslimi (İnternetwork datagram delivery) şeklinde de adlandırılır.

Ağ(Katman) katmanı → Farklı Ağlar

Veri Bağı(Data-link) katmanı → Yerel Ağ



Şekil 2.1 Ağlararası paket teslimi: IP'nin ana görevi

İnternet Protokolu bir cihazdan ağlararasındaki başka bir cihaza paket teslimi için çalışıyor. Örneğe göre uzak istemci ve sunucu, IP paketlerini birbirine bağlı ağlardan geçirerek iletişim kuruyor.

2.1 IP'nin Önemli Özellikleri

IP'nin nasıl çalıştığını öğrenmek için IP'nin tanımlandığı bazı özelliklere göz atmak gerekir.

İnternet Protokolu:

2.1.1 Evrensel adresleme: A noktasından B noktasına paketi gönderebilmek için cihazların B noktasındaki cihazı tanımış olması gerekir. IP, ağ için adresleme mekanizmasını tanımlar ve bu adresleri teslim sırasında kullanır.

2.1.2 Alt katman protokollarından bağımsız: IP, paketin TCP/IP yığınıyla çalışabilecek herhangi bir alt katman ağında da iletimine izin vermek için tasarlanmıştır. Ki bu protokol, Ethernet veya IEEE 802.11 gibi çeşitli düşük seviye protokolları için ön şartları sunar ve bu protokollara kolayca adapte olabilir. IP, PPP gibi özel veri bağı protokollarında da çalışabilir. IP'nin yeteneklerine önemli bir örnek ise geniş ve büyük paket bloklarını küçük olanlarına parçalama, bölmedir. Bu da fiziksel ağın boyutlarının sınırlarıyla eşleşmek zorundadır. Hedef alıcıda ise parçalar yeniden bir araya getirilir ihtiyaç duyulduğu üzere.

2.1.3 Bağlantısız biçimde teslim: IP, bağlantısız bir protokoldur. Bunun anlamı ise eğer A düğümü B'ye paket göndermek isterse, başlangıçta B'ye yönlenecek bir bağlantı kurmaz ve paket gönderilir. Yalnızca, paket üretilir ve gönderilir.

2.1.4 Güvenilmez teslim: IP, güvenilir olmayan bir protokoldur. Güvenilmez denmesindeki kasıt, bir paket A'dan B'ye doğru yola çıkarıldığında A cihazı sadece paketi gönderir ve sonra diğerine geçer. IP, gönderdiği paket için güvenilirlik sağlayamaz. Örneğin akış kontrolü, hata koruması ya da kayıp paketlerin yeniden gönderilmesi gibi bir yeteneğe sahip değildir. Bu sebepten IP bazen, paketin ulaşmasında hıza önem veren protokol olarak bilinir ve

söylenir. Paketi bir yerden alıp başka bir yere iletmek için elinden geleni yapar ama gidip gitmediğinin takibini gerçekleştirmez. Bu konuda garanti vermez.

2.1.5 Aldım cevabı iletilmeksizin teslim: IP, güvenilir olmama durumuna benzer bir biçimde, alındı bilgisi kullanmaz. B cihazı A'dan paketi aldığında ona bir cevap yollamaz. [2]

2.2 IP işlevleri

Daha evvel de belirtildiği gibi IP'nin temel görevi İnternetwork (ağlararası) paket teslimidir. IP'nin yürüttüğü görevler:

2.2.1 Adresleme: Paketlerin teslimi işini gerçekleştirmek için, IP'nin onları nereye teslim edeceğini bilmesi gerekir. Bu nedenden IP, bilgisayar adresleme için bir mekanizma barındırır. IP, ağlararasında işlem yürüttüğünden sistem, cihazların bir diğer cihazın IP adresine benzemeyecek şekilde adreslenmesine imkan tanır. İnternet Protokolu, gerektiğinde paketlerin uzak ağlara yönlendirilmesinde de kolaylık sağlar.

TCP/IP Protokol kümesinin diğer protokolları da IP'den faydalandığından IP'yi kavramak, özümsemek TCP/IP'nin rahatça anlaşılmasına sebep olacaktır ve büyük önem taşır.

2.2.2 Veriyi Giydirme ve Formatlama/Paketleme: TCP/IP'deki ağ protokolu olarak IP, TCP ve UDP taşıma protokollarından veri yükünü kabul eder. Sonra bunu göndermek için, özel bir format kullanarak giydirmeyi yapar.

Veriyi Giydirme(Data Encapsulation):

Protokollar eş düzeyler arası iletişimi kontrol eden kuralları tanımlar. Ki protokollar OSI modelindeki karşılıklı katmanlarda çalışan işlemler arasındaki konuşmalardır. Birinci katman haricinde bu iletişimler 2 veya daha çok cihazdaki karşılıklı yazılım elemanları arasında gönderilen mesaj formunu alır. Protokollar arasında gidip gelen bu mesajlara PDU denir. Her bir

PDU'nun kendine has formatı vardır ve bunlar protokolun özelliklerini ve isteklerini gerçekler.

Herhangi bir katmanda PDU, o katmandaki protokolu uygulayan mesajdır. N.katman PDU eşittir N-1.katman SDU(service data unit) N.katman PDU'su, N-1.katmana verildiğinde, N-1.katman protokolunun servis sunacağı veri yükü olur. N-1.katmanın işi bu SDU'yu nakletmedir. (N.katman PDU'yu kendi PDU formatına yerleştirerek gerekli başlık ve kuyrukları ekler.) İşte buna veriyi giydirme denir.

. Bir protokolun iletişim kurabilmesi için PDU'sunu bir alt katmana iletmesi şarttır. Alt katmanlar üstlerine servis sağlar. Bu servislerden biri üst katmandan alınan veri yükünü yönetmektir.

PDU: Protokol tarafından oluşturulan, o protokolun istediği başlığı ve transfer edilecek paketi barındıran bir yapıdır. Örnek: L7 PDU → L7H + uygulama verisi (6.katmana gelindiğinde bu L6 SDU olur.) **[3]**

2.2.3 Parçalama ve Yeniden Birleştirme: IP paketleri yerel ağda transfer edilmek istendiği zaman 2.katmana verilir. Bununla birlikte IP'yi kullanan fiziksel ağın azami çerçeve boyutu ağdan ağa değişebilir, farklı olabilir. Bu nedenle IP, parçalama yeteneğine sahip olup paketleri bölerek onların yerel ağda taşınmasına olanak sağlar. Alıcı cihaz da paket parçalarını yeniden bir araya getirme işini yapar.

2.2.4 Yönlendirme/Dolaylı Teslim: Doğrudan teslim, paket aynı yerel ağdaki bir hedefe gönderileceği anda alt katman LAN/WLAN/WAN protokolları kullanılarak kolaylıkla yapılır. Ayrıca genellikle(istisnalar dışında) uzak ağdaki bir hedef doğrudan kaynağa bağlı değildir. İşte bu söz konusu ise paket dolaylı biçimde teslim edilir.İşte bu işlem de yönlendirici gibi ara cihazlardan yararlanılarak başarılır. Tabii ki bunları yaparken ICMP ve RIP, BGP gibi yönlendirme protokolları devreye girer. **[4]**

3. IPv6 PAKET GENEL FORMATI

. IPv4'te olduğu gibi IPv6 paketi de başlık ve veri yükünden meydana gelir. Başlık bilgisi yine paketi hedefe gönderebilmek için gerekli iken, payload adı verilen, paketteki taşınan mesaj(eğer ek başlıklar varsa onun da dahil olduğu kısım) da sonuçta ulaştırılmak istenen mesajdır. IPv6 paketi standart veya genişletilmiş formatı kullanabilir. Daha önceden söylendiği gibi IPv6 paketi bilindik bir başlık ve seçenekli olarak da bir veya daha çok uzatma(extension) başlığı içeren yapıya sahiptir. IPv6 ana başlığı her pakette minimumda bulunması istenen kısımdır. Yine adres ve kontrol bilgisi içerir ki bu bilgiler paketin işlenmesinde ve yönlendirilmesinde rol alır.

3.1 IPv6 Paketi İçindeki Alanlar:

3.1.1 Uyarlama: Paketi üretecek yeni nesil İnternet Protokolu uyarlamasını gösterir. Bu alan IPv4'teki gibi bir işleve sahiptir. 4 bit'tir.

3.1.2 Trafik sınıfı(öncelik): Bir kaynağın, paketin istenen teslim önceliklerini tanımlamasını etkinleştirir, sağlar. Öncelik değerleri aralıklara bölünmüştür. Kaynağın sıkışıklık kontrolü sağladığı ve sağlamadığı trafik. 8 bit'tir. Paketin servis sınıfı(CoS) önceliğini tanımlar. IPv4'teki Servis Türü(Type of Service) alanının yerine geçer.

3.1.3 Akış etiketi(Flow label): Bu geniş ve büyükçe alan gerçek zamanlı paket teslimine ve servis kalitesi özelliklerine ek destek sağlamak amacıyla yaratıldı. Akış, tanım olarak bir kaynaktan tek veya daha çok hedefe gönderilen ardışık paketlerdir. Belli bir akıştaki tüm paketleri teşhis etmek için kullanılır. Bu sayede kaynakla hedef arasındaki yönlendiriciler etiketlenmiş bu paketlerin tümüne aynı muamelede bulunur. Örneğin ses ve video gibi, kendisiyle özel ilgilenilmesi düşünülen paket türleri diğer paket çeşitlerine nazaran daha hassastır. Özellikle düşük gecikmeyle iletilmeleri şarttır. Etiketleme ya da işaretleme dediğimiz olayı kaynak tarafı gerçekleştirir. 20 bit'tir. Hizmet kalitesi yönetimini sağlar.

3.1.4 Paket içinde taşınan mesajın uzunluğu: Paketteki mesajı taşıyan veriyükünün uzunluğudur. 16 bit'tir. Paketin uzunluğu 65,535 Byte'a kadar çıkabilir.

3.1.5 Sonraki başlık(Next header): IPv4'teki protokol alanının yerine kullanılmak üzere oluşturulan alandır. Eğer bir pakette ek(extension) başlıklar var ise bu aynı zamanda ilk ek başlıktır. (Çünkü bir de ana başlık var ve o birinci başlık.) Yok hayır yalnızca ana başlık bulunuyorsa bir başka deyişle ek başlık yoksa IPv4'teki protokol alanıyla hemen hemen aynı işlevi görür. Sadece sayılar farklılık gösterir. İşte bu durumda sonraki başlık, paketin taşıdığı üst katman mesajının başlığıdır. 8 bit'tir. Çok fazla derecede bir kısıtlama olmayıp esneklik olduğundan istenildiği anda istenilen ek özellikler sağlanabilir. Hiç uzatma başlığı yoksa sonraki başlık alanı, ana başlık içinde düşünülür.Bir veya daha çok uzatma başlığı aynı anda varsa önce ana başlık ardından bu sonraki alan içinde "sırayla" aşağıdaki başlık türleri yer alabilir:

- IPv6 başlığı (ana başlık)

-Yönlendiriciden yönlendiriciye seçenekler başlığı

-Hedef seçenekler başlığı(yönlendirme başlık birleşimleri)

-Yönlendirme başlığı

-Parçalama başlığı

-Doğrulama başlığı

-ESP başlığı

-Hedef seçenekler başlığı(son hedefin işlediği seçenekler)

-Üst katman başlığı(TCP, UDP…)

Sonraki Başlık: IPv6 başlığını takip eden başlık türünü tespit eder. IPv4 protokol alanıyla aynı değere sahip.**[5]**

3.2 IPv6 Ek Başlıkları(Extension Headers)

IPv6'da seçenekli İnternet katman bilgisi ayrı başlıklarda kodlanır. Ek başlıklar IPv6 başlığı ile üst katman(upper-layer) başlığı arasına konabilir. Küçük sayıda ek başlık bulunmakta olup her birinin ayrı bir sonraki başlık değeri (next header value) var.

Ek başlıklar hiç olmayabilir de. 1 tane de olabilir daha çok da görülebilir.

Format : IPv6 başlığı + Ek başlıklar + Üst katman başlığı(upper-layer header) (şeklinde bir sıra izler.)

Bir istisna dışında ek başlıklar paket IPv6 başlığın hedef adres alanında belirtilen düğüme ulaşana dek paketin teslim yolundaki hiçbir düğüm tarafından işlenmez.

-Eğer hiç ek başlık yoksa, üst katman başlığı işlenir.

-Ek başlık varsa, ilk ek başlık işlenmek için çağırılır.(yani ek başlık yoksa üst katman başlıkları işlenir eğer varsa ilk ek başlıkla ilgilenilir.)

Az önce bahsedilen istisna yönlendiriciden yönlendiriciye başlığıdır. Bunun anlamına göre bu başlık kaynak ve hedef dahil, paketin teslim yolundaki her düğüm tarafından işlenmesi gereken bilgiyi taşıyor.

Yönlendiriciden yönlendiriciye başlığı eğer varsa IPv6 başlığının hemen ardından gelmelidir. Onun varlığı IPv6 başlığının sonraki başlık alanında sıfır değeriyle belirtilir. IPv6 başlığındaki ek başlıkların sırası şu şekilde olmalıdır:

1- IPv6 başlığı 2- Yönlendiriciden yönlendiriciye seçenekler başlığı (1) 3- Hedef seçenekler başlığı

4- Yönlendirme başlığı 5- Parça başlığı 6- Doğrulama başlığı (2) 7- ESP (2)

8- Hedef seçenekler başlığı (3) 9 – Üst katman başlığı

1)→ IPv6 hedef adres alanında gözüken ilk hedef tarafından işlenecek seçenekler için artı yönlendirme başlığında listelenmiş art arda gelen hedefler tarafından işlenecek seçenekler için.

2)→Ek tavsiyeler (Doğrulanma ve ESP başlığının sırasına bağlı olarak)

3)→ Paketin son hedefi tarafından işlenecek seçenekler için.

Hedef seçenekler başlığı dışında öteki tüm ek başlıklar bir kereliğine kullanılmalı. Eğer aynı pakette birden çok ek başlık kullanılıyorsa sıra yukarıda numaralandırıldığı gibi olacak. Yalnızca yönlendiriciden yönlendiriciye seçenekler başlığı illa ki IPv6 başlığının hemen ardından gelecek. **[6]**

3.3 Ek Başlıkların Özeti

3.3.1 Yönlendiriciden yönlendiriciye seçenekler başlığı: Uzunluğu değişkendir. Kaynaktan hedefe tüm aygıtlar tarafından incelenmesi gereken keyfi seçenekleri tanımlar. Sonraki başlık değeri sıfırdır.

3.3.2 Yönlendirme başlığı: Uzunluğu değişkendir. Bir kaynak aygıtın paket için bir rota belirtmesine imkan tanıyan yöntem tanımlar. Sonraki başlık değeri 43'tür.

3.3.3 Parçalama başlığı: Uzunluğu 8 Byte'dır. Bir orijinal mesajın yalnız bir parçası tutulduğunda bu başlıktan yararlanılır. İçinde ana başlıktan atılmış parça ofset kimliklendirme, daha çok parça alanları bulunur.

3.3.4 ESP başlığı: Uzunluğu değişkendir. Güvenli iletişim için şifrelenmiş veri yükünü taşır.

3.3.5 Doğrulama başlığı: Uzunluğu değişkendir. Şifrelenmiş veri yükünün doğrulanmasıyla ilgili bilgiyi taşır.

3.3.6 Hedef seçenekler başlığı: Uzunluğu değişkendir. Yönlendiriciden yönlendiriciye seçenekler başlığı gibi bir görev üstlenir.

Bunların yanında bir de sözde ek başlıkları var. (no next header) Burada değer ise 59'dur.

(O ek başlıktan sonra hiçbir şey yok demek)

IPv6 Yönlendirme Ek Başlığı

. Kaynak yönlendirmesi yapmak için kullanılır.

Yönlendirme ek başlığı formatı:

-Sonraki başlık: 1 Byte'dır. Yönlendirme başlığından sonraki "sonraki başlığın" protokol numarasını taşır.

- Başlık ek uzunluğu: 1 Byte'dır. 8 Byte'lık birim halinde yönlendirme başlığı uzunluğu.

- Yönlendirme tipi: 1 Byte'dır. Bu alan bir çok yönlendirme tipinin tanımlanmasını yapar. Kullanılan tek değer sıfırdır.

- Kalan segmentler: 1 Byte'dır. Rotada kalan, açıkça isimlendirilmiş düğümlerin sayısını belirtir.

- Ayrılmış: 4 Byte'dır. Kullanılmaz. 0 atanır.

- Adres1….AdresN: Uzunluğu değişkendir.(16'nın katları) Kullanılan rotayı belirten IPv6 adres seti.

IPv6 Parçalama Ek Başlığı

Parçalara ayrılan paketlerde bulunur. (Parçaların bir araya getirilmesinde gerekli bilgiyi sağlamak için.)

Parçalama ek başlığı formatı :

Sonraki başlık: 1 Byte'dır. Parça başlığından sonraki "sonraki başlığın" protokol numarasını içerir.

Ayrılmış: 1 Byte'dır. Kullanılmaz. Sıfır atanır.

Parça ofseti: 13 bit'tir. Mesajdaki 8 Byte'lık birimler halinde belirtilir. (pozisyonu)

Ayrılmış: 2 bit'tir. Kullanılmaz . Sıfır atanır.

M bayrağı (daha çok parça bayrağı): 1 bit. IPv4 başlığındaki aynı isimdeki bayrak sıfıra ayarlandığında mesajdaki son parçayı 1'e ayarlandığında ise daha işlenecek parça olduğunu gösterir.**[7]**

3.4 IPv6 Paket Seçenekleri

IPv4'te tüm ekstra bilgi ki çeşitli amaçlar için istenen, "options(seçenekler)" formu şeklinde pakete yerleştirilir. IPv6'da ek başlıkların yeni şekli ileri sürülür. Bu başlıklar önceden tanımlanmış çoğu IPv4 seçeneklerin yerini alır. Bununla birlikte, seçenekler kavramı hala vardır IPv6'da çok az fark arz eden bir gaye için. Temel IPv6 Protokolu'nun maksimum esneklikle genişlemesi mümkündür artık.

3.5 IPv6 Seçenekler Başlık Türleri

IPv6 seçenekler, ek başlıkları tamamlayıcıdır. Aslında ek başlıklar biçiminde icra edilir. "Options"ı kodlama için 2 farklı tip kullanılır ve aynı formata sahiptirler yalnızca işleyen cihazlarda bir fark söz konusudur.

Hedef seçenekler: Sadece nihai hedef için kastedilen seçenekleri içerir.

Yönlendiriciden yönlendiriciye seçenekler: Kaynak ile hedef arasındaki her cihaz için taşınan bilgiyi içerir.

IPv6 Seçenek formatı:

Bu başlık türlerinin her biri 1 Byte'lık sonraki başlık alanı ve yine 1 Byte'lık başlık ek uzunluğu alanına sahip. Başlığın gerisi bir veya daha fazla seçenek alanı taşıyor.

-Seçenek türü: 1 Byte'dır. Bu alan seçenek türünü gösterir. Bitler aşağıdaki yapıya göre yorumlanır:

Tanınmamış seçenek hareketi: 2 bit. İlk 2 bit, eğer seçeneği işleyen cihaz seçenek tipini bilmiyorsa ne yapılacağını belirtir. 4 değer:

Seçeneği atla. Başlığın gerisini yap.

Paketi çöpe at. Başka bir halt yapma.

Paketi çöpe at, kaynağa ICMP parametresi problemi yolla.

Paketi çöpe at. Üstteki ICMP mesajını yolla. (eğer yalnızca hedef çoklu yayım adresi değilse.)

-Seçenek değiştirme izni verildi bayrağı: 1 bit. Paket yolda iken 1'e ata eğer seçenek verisi değişirse.

-Seçenek türünden arta kalan: 5 bit.

-Seçenek veri yükü uzunluğu: 1 Byte. Kendisinin bir altındaki "seçenek veri yükü" alanının uzunluğunu belirtir. IPv6'da seçenek türü ve seçenek verisi uzunluğu alanının uzunluğunu içermez.

-Seçenek veri yükü: Uzunluğu değişkendir. Seçeneğin parçası olarak gönderilen veri yüküdür.Seçenek türüne hastır.

Ana başlık 40 Byte'dır ve sabittir. (Sonraki başlık alanı(next header) dahil) Duruma göre uzatma başlığı veya başlıkları, ilaveten de veri gelebilir ana başlıktan hemen sonra. Sabit uzunluktaki başlık yönlendiricilerde başlık uzunluğunun algılanması için harcanan zamandan ve işlem gücünden de tasarruf edilmesini sağlamaktadır. IPv6'da adresin 128 bit olması da rasgele değildir. Yönlendirme işlemi sırasında azami hız ve olabildiğince küçük oranda kapasite aşımları yolu açılmaya çalışılmıştır. Yani ana başlık + pakette taşınan mesaj veya ana başlık + uzatma(ek) başlığı + pakette taşınan mesaj ya da ana başlığı + birden fazla ek başlık + pakette taşınan mesaj, şeklinde bir paket yapısı oluşmakta.

3.5.1.1 Hop Sınırı: IPv4'teki TTL yani paketin yaşam süresine benzer bir yapıdadır. 8 bit'tir.

3.5.1.2 Kaynak Adresi: 128 bit'tir. Her zaman için paketin üretildiği ilk kaynağın adresini verir.

3.5.1.3 Hedef Adres: Yine 128 bit değere sahip olup paketin alıcısını belirtir. Yönlendirici adıyla bilinen cihazlar ise her ne kadar paketleri işleyen, elden

geçiren cihazlar biçiminde anılsa da bu alan daima son hedefi anlatmak için-dir.

Not:IPv6'da esas başlık 40 Byte olmak zorundadır. Değişkenlik göstermez. Esneklik mevcuttur ayrıca. Uzatma başlığı adı verilen başlıklara bir boyut sınırlaması yoktur.

3.6 IPv4'ten IPv6'ya Geçiş ve İkisi Arasındaki Farklar

Bilindiği gibi IP, OSI modeline göre TCP/IP Protokol kümesi içinde 3.katmana karşılık gelmekte ve bir ağda uçtan uca veri yönlendirmesi için kullanılmaktadır. İnternet ve iletişim teknolojilerinin başlangıç noktasından çok farklı yerlere gelmesi nedeniyle IPv4 bugünkü ihtiyaçları karşılayamaz duruma gelmiş ve yeni protokolun tasarlanması kaçınılmaz olmuştur. Bu yüzden IETF (İnternet Mühendislik İş Gücü) tarafından yürütülen çalışmalar sonucunda 128 bit'lik adres yapısına sahip IPv6(Başlarda IP- Yeni Nesil – IPng olarak adlandırılmıştı) geliştirilmiştir.(RFC 2460) Ayrıca özetle IPv6'daki yenilikler :

-Sadeleşmiş standart başlık ve uygulamaya yönelik ek başlıklar

-Paket anahtarlamalı ağ üzerinde devre anahtarlama desteği

-Ek başlık yapısı içerisinde desteklenen IPSec güvenlik özelliği

-Hizmet kalitesi desteğinin artırılmış olması

-Komşu düğümlerle daha yakın işbirliği; yeni bir protokol

-Hiyerarşik adresleme mekanizması ve yönlendirme

-IP adresinin 128-bit olması nedeniyle genişlemiş IP adres aralığı

-Mobil IP uygulamalarına destek

-Ölçeklenebilirliğin göz önüne alınmış olması

IPv6'ya Geçiş → a- Çift-protokol kümesine sahip düğümler

b- Tünelleme : IPv4 paketlerine IPv6 paketi bindirilmesi

c- IPv4-IPv6 dönüşümü : Çift-protokol kümesine sahip sistemler IPv4 ile IPv6 arasında geçiş cihazı gibi kullanılır.Böylece IPv4'ten gelen paketler IPv6'ya dönüştürülüp öyle gönderilir; veya tersi olarak IPv6 paketleri IPv4'e dönüştürülür.

3.7 IPv6'nın Geliştirilmesi Nedenleri:

3.7.1 Yetersiz kalan IP adresleri: IPv4 32 bit'lik adresleme gerçekleştiriyordu. NAT ve alt ağlara ayırma yöntemleriyle zamanında düzensiz dağıtılan IP adreslerinin tüketimi hızı düşürülmeye çalışıldı. NAT da sonradan eklenmiştir. Ancak NAT IPv4'ün doğal yapısında bulunmadığından uçtan uca direk erişim isteyen VoIP, P2P gibi uygulamalarda sıkıntı yaratmaya başladı.

3.7.2 Performans ve birlikte çalışabilirlik gereksinimleri: IPv4 paketleri, karışık bir başlık yapısına sahipti. Bu kadar karmaşık olduğundan yönlendiricilerin paketi işlemesi de gecikiyordu o nedenle IPv4'te bulunan bir çok alan atıldı. Ayrıca güvenlik sorunları yaşanıyordu yine doğası gereği destek bulunmadığından işin içinden çıkılamıyordu.

3.7.3 Yetersiz servis kalitesi desteği: İnternet üzerinde artan hız ve bant genişlikleri ile birlikte, ses ve görüntü gibi yüksek büyüklükte paketlerin taşınması mümkün hale gelmiştir. Fakat IPv4'ün yetersiz kalan QoS desteği ile gerçek zamanlı ses ve görüntü aktarımında sorunlar ortaya çıkıyordu. Ayrıca gelişmiş bir QoS desteği, ağ yöneticilerine, istenmeyen ağ trafiğini en aza indirmeye yardımcı olacak özelliklere de sahiptir. Ki IPv4'te yönlendirici gibi ara cihazlar da QoS desteğini verememektedir.

3.7.4 Daha kolay yapılandırma ihtiyacı: IPv4'te IP adres yapılandırması elle ya da DHCP ile yapılmaktadır. Elle uygulanmayan veya DHCP sunucudan IP adresi alamayan bazı sistemler için APIPA(Otomatik Özel IP Adresleme) gibi mekanizmalar geliştirilmiş olmasına rağmen APIPA'nın tam bir çözüm olmadığı açıktır. Sonuç olarak IP adreslerinin dağıtımı otomatik olarak ha-

rici bir protokol veya sisteme ihtiyaç duymadan düzgün bir şekilde yapılmasına imkan tanıyan bir protokola gerek vardır.

3.7.5 Hareketli kullanıcı desteği: IPv4 ilk çıktığında hareketli kullanıcılar hiç düşünülmemişti. Hareketli cihazlar sonraki yıllarda yaygınlaştı o nedenle artık İnternet Protokolu'na hareketlilik yeteneği de verilmeliydi. Protokol üzerine giydirilmiş bir takım mekanizmalar(Mobility Agent Advertisement Extension, Mobile-Home Extension gibi) ile şimdi hareketli kullanıcıların ağa dahil olup iletişim kurmaları sağlanabiliyor. Ancak bu durum da özellikle güvenlik sorunlarını beraberinde getiriyor.

3.7.6 IP seviyesinde güvenlik ihtiyacı: Başlarda sınırlı sayıda, küçük çapta bir kitleye hitap eden protokol zaman içerisinde, İnternet'in hızla büyümesi ve gelişimiyle güvenlik açıkları doğurur hale gelmiştir. Protokol üzerine IPSec (IP security) gibi uygulamalar ile veri doğrulama (authentication), içerik bütünlüğü (data integrity) ve gizlilik(privacy) gibi özellikler eklense bile, gerek mekanizmanın protokolun doğası içerisinde olmaması (gerekse yönlendirici gibi ara cihazlar tarafından IPSec'in desteklenmeyişi ile, IPSec VPN uygulamasından öteye taşınamamıştır. Güvenlik özelliklerini kendi bünyesinde barındıran,adresleme yapısıyla istenen ölçüde gizlilik sağlayan bir protokola ihtiyaç duyulunca bu özellikler IPv6 adı verilmiş yeni nesil İnternet Protokolu'nda kullanılmadı. **[8]**

3.8 IPv4 ile IPv6'nın Karşılaştırılması

-IPv4 32'şer bit adreslemeyi içerir. (kaynak ve hedef) IPv6'da ise bu 128'er bit'tir.

Geniş adres alanı: 2 üssü 128 adet IP adresleme kapasitesiyle adeta bir çığır açılmakta IPv6 ile ancak bir durumu da göz ardı etmemeliyiz ki o da artık yalnızca ağ cihazları ya da bilgisayarlar haricindeki günlük cihazların da mesela telefon mesela buzdolabının da IP adresi alabilmesidir. Artık NAT gibi çözümlere gerek kalmayacaktır.

-IPv4'te IPSec seçeneklidir ve protokol alanında doğrulama ve şifreleme başlığıyla taşınır, IPv6'da ise yine bu protokol alanına benzer yapıdaki ek başlıklar kısmında yerini alır.

- IPSec: Yani IP Security bir ki her bir paketin şifrelenmesi ve doğrulanması yoluyla İnternet Protokolu iletişimlerini güvenlik altına almak için kullanılan bir protokol kümesidir. IPSec Protokolu OSI modelinin 3.katmanı olan ağ katmanında çalışır. SSL, SSH gibi benzer protokollar ise daha üst katmanlarda görevini yerine getirir. IPSec tasarlanmasındaki niyetlerden biri paket trafiğinin taşıma modu (uçtan uca) güvenliğini sağlamak ki bu işlem son kullanıcıların güvenlik işlemini yaptığı ortamda gerçekleştirilir. "Yalnızca transfer ettiğimiz veriyükü" şifrelenir ya/ya da doğrulanır. Diğeri tünel modudur. Bunda ise iletişim güvenliğinin bir düğüm tarafından birçok düğüme sağlandığı görülür. IP paketinin bütünü(başlık + veriyükü) şifrelenir ve/veya doğrulanır.

3.9 Teknik Ayrıntılar:

İki protokol, paket seviyesinde hem IPv4 hem IPv6 için güvenlik sağlamak amacıyla geliştirildi.

- IP Doğrulama Başlığı: Bütünlük ve doğrulama kontrolu yapar.

- IP ESP: Bütünlük korumasına ilaveten güvenilirlik sağlar.

IPv4'te yönlendiricilerde QoS desteği yetersizdir IPv6'da ise İnternet Protokolu'na entegre(tümleşik) olduğundan iyi bir destek sunulmaktadır. (özellikle akış etiketi ile)

QoS : Quality of Service isminden de anlaşılacağı üzere sunulan hizmet kalitesi demektir. QoS hizmeti değişik yapılarda farklı işlevlere sahiptir. Şöyle bir örnek verilebilir. VoIP destekli bir ağda hattınız yoğun ise VoIP paketlerini gönderemiyorsunuz ya da gecikmeli gönderiyorsunuz. Burada hatırlamamız gereken bir ayrıntı VoIP paketlerinin en basitinden Web istekleri gibi

beklemeye çok fazla tahammülünün olmadığıdır.(düşünsenize biriyle telefonda konuşurken seslerin 10 saniye sonra geldiğini). Bu nedenle VoIP ve e-posta trafiği gibi önceliğe sahip paketleri bir şekilde belirtip bunlarla alakalı bir paket geldiğinde üstünlük durumuna göre paketlerin gönderilmesi gerekir.

Gelişmiş QoS desteği: IPv4'te bulunan Servis türü kısmının IPv6'daki karşılığı olan Trafik sınıfı her iki başlık için de aynı işleve sahiptir. Öncelik atama ve servis kalitesi (Servis kalitesi)gibi fonksiyonlar için kullanılmaktadır. IPv6 ile getirilen yeni bir özellik akış etiketi kısmıdır. Gerçek zamanlı paketler örneğin ses, video. Bu etiketlere bakılarak daha hızlı bir şekilde yönlendirilebilir bu sayede ağ trafiği daha akıcı hale ulaşır.

-IPv4'te gönderici tarafında ve ayrıca yönlendiricilerde parçalama mevcutken IPv6'da ise yalnızca göndericilerde bu işlem yapılmaktadır.

-IPv4'te başlık kontrolu alanı var iken özellikle günümüz ağlarında İnternet Protokol'unun gelişmiş olması nedeniyle çok önemli boyutlarda hatalarla karşılaşılmadığından bu alana IPv6'da gerek duyulmamıştır. Ki IPv4teki bu kontrol yalnızca başlığın bozulup bozulmadığına bakarken IPv6'da bu alan atılmıştır. Ancak "tüm paketin" bütünlüğünün sorunlu olup olmadığını IPv6'da sonraki başlık alanına belli başlıklar ekleyerek yapabilmek mümkündür.

-IPv4'te ana başlık(main header), seçenekler alanına sahipken IPv6'da bu alan kaldırılmış ve eğer sonradan bir özellik eklenip protokol geliştirilecekse sonraki başlık alanına ilavelerle bu sağlanacaktır.

-Genişletilebilirlik: İnternet ve özellikle mobil teknolojiler çok hızlı ve öngörülemeyen bir şekilde gelişmektedir. IPv6, ek başlıkları ile yeni ihtiyaçlara kolayca genişletilebilir. Bu seçenek IPv4 başlığında 40 Byte ile sınırlıyken (options) IPv6'da IPv6 paketi boyutudur.

-Uzantılar ve Seçenekler için Artırılmış Destek:

Değişiklik sayesinde daha verimli iletim, seçenek uzunluğunda az derecede sınırlama ve gelecekteki yeni seçenekler için önemli sayılabilecek bir esneklik gerçekleşiyor.

- IPv4'te ARP(Adres çözümleme protokolu) ARP istek çerçevelerinin yayını ile IPv4 adreslerin veri bağı katmanı adreslerinin çözümünde kullanılıyor. IPv6'da ise bunların yerini komşuya istekte bulunmak için çok alıcıya gönderilen mesajlar almış.

Komşu keşfi denen şey çok alıcıya gönderilen ve tek alıcıya gönderilen mesajlarla daha verimli bir ağ iletişimi sağlar.

-IPv4'te yayın var. IPv6'da yok. Bu, yerel trafiği hızlandırıyor, tıkanıklığı aşmamızı sağlıyor.

-IPv4'te elle ya da DHCP adres ayarına ihtiyaç var. IPv6'da ise elle vermek ya da DHCP zorunlu değil.

-Bilgisayar adı/IPv4 adresleri ikilileri için DNS'te A kaydı tutuluyor. IPv6'da ise AAAA kaydı. Nedeni ise IPv4'te 32 bit IPv6'da ise bunun 4 katı 128 bit olması.

-IPv4 576 Byte'lık paket boyutunu desteklerken IPv6'da bu 1280 Byte'dır minimumda.**[9]**

-Akış Etiketleme Becerisi

IPv6'da rastladığımız, yeni bir özellik. Göndericinin özel bir işleme tabi tutulmasını istediği (gerçek zamanlı hizmet) belirli bir trafiğe ait paketlerin etiketlenmesi.

IPv4 başlık içeriği: Versiyon(uyarlama), İnternet başlık uzunluğu, servis türü, toplam uzunluk, kimliğini belirleme (identification), bayraklar, parça ofseti, paket yaşam süresi, protokol, başlık kontrolü (header checksum), kaynak adresi, hedef adres, seçenekler.

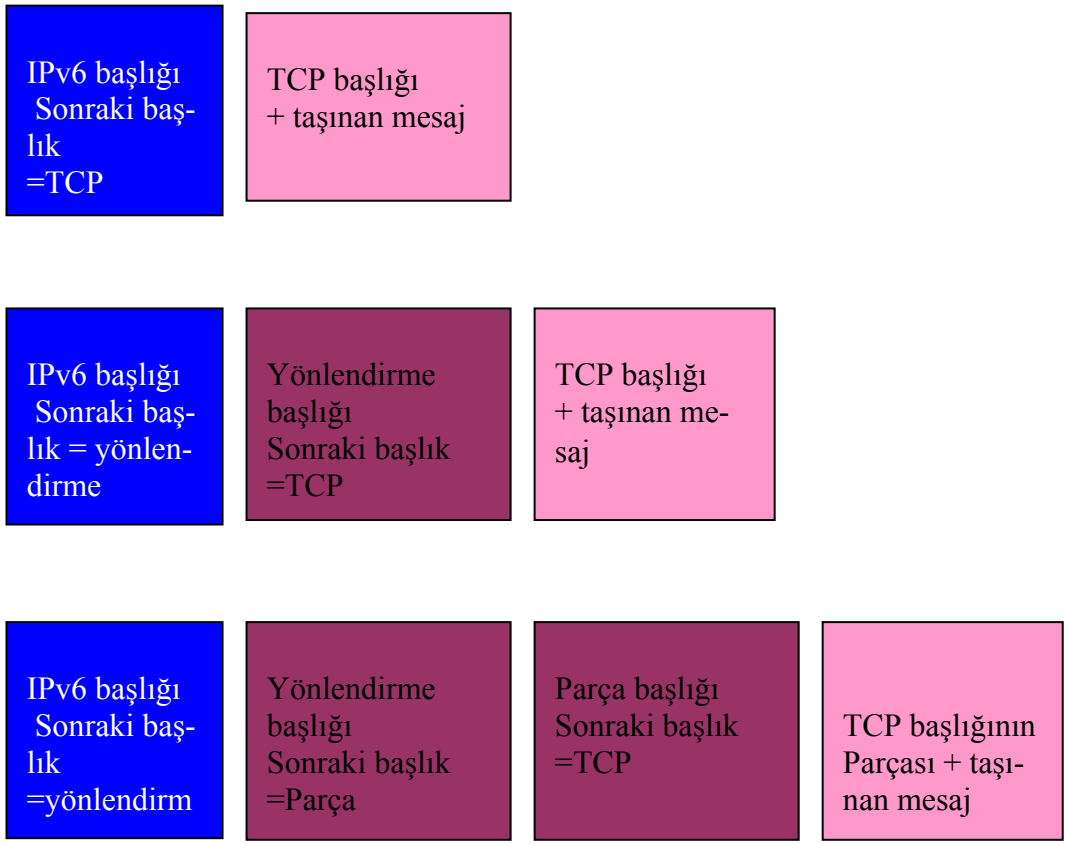
IPv6 başlık içeriği: Uyarlama, trafik sınıfı, akış etiketi, (ek başlık varsa taşınan mesaj + ek başlık uzunluğu, yoksa taşınan mesaj uzunluğu), sonraki başlık, hop sınırı, kaynak adres, hedef adres.

IPv4'ten IPv6'ya önemli değişimlerden biri adres atamada büyük bir esneklik sağlayacak derecede geniş bir adres aralığına geçiştir. Bu durum IPv6 tasarımcılarının kastı olmayıp her bireysel cihaza ve bilgisayara benzersiz IP vermek de. Adres aralığının bu derece büyümesi NAT denilen ağ adres çevrimi mekanizmasına da artık gereksinim duyulmadığını göstermektedir. Ağ adres çevrimi mekanizmasından IPv4'te yararlanılmasındaki en mühim neden, zamanında IPv4 adreslerinin düzensiz dağıtılmasından dolayı tükenmesinin giderek hızlanması ve ağ adres çevrimiyle de bunun yavaşlatılmak istenmesidir. Ağ adres çevriminin elimine edilmesi ile uçtan uca iletim de tam anlamıyla gerçekleşmiş oluyor. IPv4'te ağ adres çevrimi uygulanıp kaynak adresi değiştirildiğinden uçtan uca iletim tam manasıyla gerçekleştirilemiyordu. Bu durum IPSec gibi bazı uygulamalarda sorun yaratıyordu.

IPv4 adres tükenmesinin yavaşlatılması amacıyla kullanılan bir diğer olay subnetting yani büyük bir ağı alt ağlara bölerek o ağda ihtiyaç hissedildiği kadar adres atanmasıydı aksi takdirde israf meydana geliyordu. IPv6'da yeterince hatta haddinden fazla IP adresi sağlandığından artık alt ağlara ayırma , bölme gereği de anlamsız kalıyor.

IPv6 adres aralığı IPv4'e göre hayli hayli büyük ki IPv4 $2^{32} \cong$ 4milyon IP adresi sunarken bu durum IPv6'da 3.4 * 10 üssü 38'dir. IPv6'nın öteki bir ismi de yeni nesil İnternet Protokolu'dur(IPng).

IPv6 başlık seçenekler



Şekil 3.1 IPv6 başlık seçenekler

Şekildeki sıralama kafamıza estiği gibi yapılmamıştır. Birden çok başlık aynı anda bulunduğunda sıra ne ise ona göre dizilmiştir.

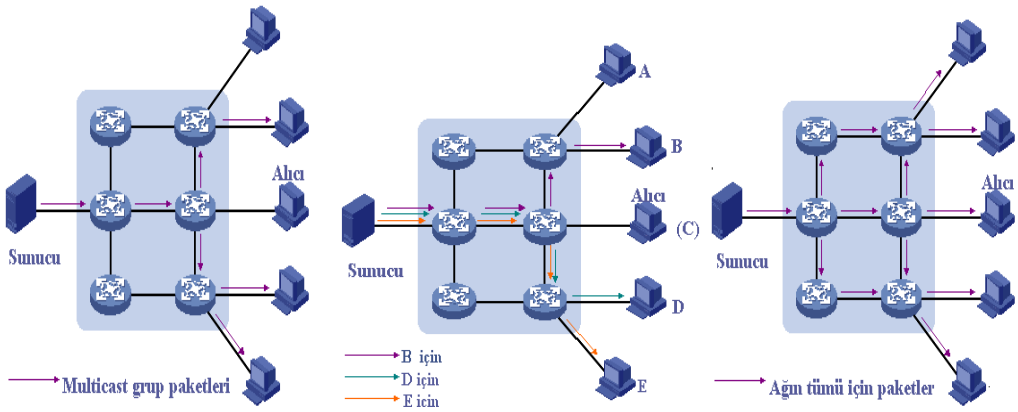
IPv6 paketi minimumda 1280 Byte'dır ancak link katmanı esnek bir MTU boyutu desteği sağlarsa bu 1500 Byte'a çıkabilir. Sıra şu şekildedir: IPv6 Header (main header), Hop-by-hop options header, Destination options header(routing header association), Routing header, Fragment header, Authentication header, ESP header, Destination options header(options processed by final destination), Upper-layer header.

3.10 IPv4 Adres Türleri: unicast, multicast, broadcast olmak üzere 3'e ayrılır.

3.10.1 Bire bir (Unicast Address)→ Tek bir bilgisayarı (yönlendirici dışındaki cihaz) temsil etmek, göstermek amaçlı kullanılır. Bir diğer nokta ise eğer bir paket bir kaynaktan tek bir hedefe gönderiliyorsa ve o şekilde yorumlanıyorsa buna bire bir iletim denir.

3.10.2 Bir göndericiden birden fazla alıcıya yönlenen (Multicast Address) → Burada ise yine bir kaynaktan bu sefer birden fazla hedefe gönderilme gerçekleşiyorsa bu adı alır. Bu birden çok hedef belli bir grup adresi işaret eder.

3.10.3 Bir göndericiden o yerel ağdaki tüm alıcılara yönlenen (Broadcast Address)→ Tüm bilgisayarları temsil eder. Bu, çoklu yayıma benzer ancak bu durumda ilgili paket hedeflenen o ağdaki tüm alıcılara gönderilir. Yani örneğin bir ağda bir kaynak o ağdaki diğer tüm bilgisayarlara mesaj atarsa paket o ağ içindeki diğer tüm bilgisayarlara ulaştırılır.



Şekil 3.2 Bir göndericiden çok alıcıya yönlenen, bir-e-bir ve tüm alıcılara yönlenen adresler **[10]**

Herkese Açık, izinsiz ve izinli özel IP Adresleri

.Herkese açık adresler: Bir bilgisayarın İnternet'te görülebilir hale gelmesi için herkese açık IP adresi yoluyla kendisine ulaşılabilmesi şarttır. IANA adı konmuş yönetim planı organizasyonlara belli aralıklarda herkese açık IP adresleri atar ki bu organizasyonlar da daha sonra bireysel bilgisayarlara o aralıklarda IP adresleri atayacaktır. Bu durum, bir çok bilgisayarın aynı, herkese açık IP adresine kavuşması problemini engelleyecektir. Genellikle ISP'ler tarafından sağlanır.

Yetkili(izinli) Özel Adresler: IANA, İnternet'te hiçbir zaman kullanılmayacak belli sayıda IP adreslerini ayırdı. Bu tür IP adresleri doğrudan İnternet'e bağlantı istememekle beraber IP bağlanabilirliğine ihtiyaç duyuyordu. Örneğin bir kullanıcı o ev ağı içindeki diğer bilgisayarlara bağlanmak istediğinde otomatik özel IP adresleme (APIPA) yönteminden istifade edebilir. Bu özelliğe göre her bir bilgisayar kendine otomatik bir şekilde IP adresi verebilir.İşte bu durumda kullanıcı tek tek her bilgisayara IP adresi vermek zorunda kalmayacak yada bunun için DHCP sunucusu da devreye girmeyecektir.APIPA adres aralığı ise 169.254.1.0'dan başlayıp 169.254.254.255'e kadar gitmektedir az önce de söylediğim üzere eğer başka hiçbir adres atama yolu mevcut değilse bu izlenir. İzinli özel adrese sahip bilgisayarlar vekil sunucu veya NAT mekanizmaları aracılığıyla İnternet'e bağlanır.

İzinsiz özel adres: Eğer ağımızın hiçbir şekilde İnternet'e erişemeyeceği kesinse izinsiz özel adres seçeneği kullanılabilir.**[11]**

3.11 IPv6 Adres Yapısı

IPv4'ten IPv6'ya en köklü değişiklik ağ adreslerinin uzunluğu konusunda meydana geldi. IPv6 adresleri 128 bit'tir ki IPv4 adresleri 32 bit'ti. IPv6 adresleri iki mantıksal bölümden oluşur. Bunlardan bir tanesi 64 bit'lik (alt ağ önek (prefix) öbürü ise 64 bit'lik, o bilgisayarı ilgilendiren bölümüdür. Görüldüğü üzere toplam 128 bit'lik bir adres yapısı mevcut. Bu bölüm sıralı olarak atanır veya arayüzün MAC adresinden üretilir.

Gösterim: IPv6 adresleri normalde 4 tane, 16'lık tabanda sayı grubu 8 bölüm halinde yazılır. Mesela 2001:0db8:85a3:08d3 :1319:8a2e:0370:7334 geçerli bir IPv6 adresine örnektir.

Bir ya da daha çok 4'lü sayı grubu 0000 ise sıfırlar hiçe sayılıp,atılıp bunun yerine :: konulup devam edilebilir.Yani örneğin 2001:0db8:0000:0000:0000:0000:1428:57ab biçimindeki bir IPv6 adresi 2001:0db8::1428:57abye kısaltılabilir.Bu kuralı takip ederek, peşi sıra gelen 0000 grupları ::ye kısaltılabilir, küçültülebilir.(adreste tek bir ikili kolon kullanıldıkça) Aşağıdaki şu adres biçimleri geçerli ve doğru kullanıma sahip olup aynı anlamı taşımaktadır.

İkili kolon → :

2001:0db8:0000:0000:0000:0000:1428:57ab

2001:0db8:0000:0000:0000::1428:57ab

2001:0db8:0:0:0:0:1428:57ab

2001:0db8:0:0::1428:57ab

2001:0db8::1428:57ab

2001:db8::1428:57ab

Bir IPv6 adresinde birden fazla ikili kolon bulunması geçersizdir ve kullanım açısından yanlıştır. Nedeni ise bu durumda adresin neresinde 0 grubu

olduğu açığa çıkamaması Örnek verirsek 2001::FFD3::57ab kullanılamaz bir adrestir.

CIDR prensibi → önek/önek uzunluğu

x:x:x:x:x:x:x:x → 16 bit'lik alan

son 64 bit arayüz kimliği olarak kullanılır. İkili kolon bir kez kullanılabilir.

3.12 IPv6 Adres Türleri: 3 kategoriye ayrılır.

-Bir-e-bir (Unicast Addresses)

-Bir göndericiden çok alıcıya (Multicast Addresses)

- IPv6da yeni gelen bir adres çeşidi Bir göndericiden çıkıp iletilmesi istenen alıcılardan yönlendiriciye en yakın olanına (Anycast Addresses)

Yalnız IPv4'ten farklı olarak burada tekli yayım adresler de birkaç tanedir. Bunlar

-Tek alıcıya yönlenen (Global Unicast Addresses)

-Bağ-içi Adresler (Link-local)

-Site-içi Adresler (Site-local)

-Özel Adresler

3.12.1 Unicast Address: Tek bir ağ arayüzünü ifade eder. Tekli yayım adresine gönderilen bir paket o spesifik bilgisayara teslim edilir.

3.12.2 Multicast Address: Yegane düğümün yerine farklı düğümlere ait olan arayüz setini tanımlar. Bir paket bir çoklu yayım adresine iletildiğinde protokol o paketi o adresin tanıladığı tüm arayüzlere gönderir.

3.12.3 Anycast Address: IPv6'da gelen bir adres türü olup farklı düğümlere ait birden çok arayüze atanır. Ancak herhangi birine gönderim adresine gönderilecek paket bu arayüzlerden yalnızca bir tanesine iletilir. Muhtemelen yön-

lendirme protokolunun uzaklık düşüncesine dayanarak en yakın arayüze. Yani işaret edilen arayüz fazla ancak gönderilme bunlardan sadece birine yapılıyor.

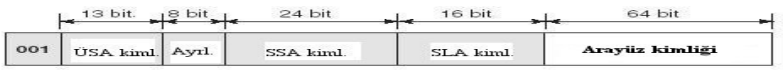
Link-local(Bağ-içi): Kapsama alanı yerel linktir(Aynı alt ağdaki düğümler)

Site-içi: Kapsama alanı organizasyondur. (Özel site adresleme)

Global: Kapsama alanı globaldir. (IPv6 İnternet Adresi)

Tek alıcıya yönlenen IPv6 adresleri

Tek alıcıya yönlenen global adresler: Bu adres türü IPv4'teki herkese açık adreslere benzer ve global olarak yönlendirilebilirler.



Şekil 3.3 Tek alıcıya yönlenen global adresler

001: Bunun bir IPv6 bir-e-bir adres olduğunun işaretidir.

Üst seviye birleştirme kimliği: Yönlendirme hiyerarşisindeki en üst düzeyi tanır. TLA kimliklerini IANA tarafından yönetilir ki IANA bu kimlikleri yerel İnternet kayıtçılarına tahsis eder. Bu İnternet kayıtçıları da sonra TLA'leri global ISP'ye tahsis eder.

Ayrılmış: Gelecekte kullanılmak üzere ayrılmış .

Sonraki seviye birleştirme kimliği: Belirli bir müşteri sitesini tanır.

Site düzeyi birleştirme kimliği: Bir organizasyon sitesi içinde 65.536 civarında alt ağ kimliği etkinleştirir, olanak tanır. Site içerisinde atanır ve ISP buna dokunamaz.

Arayüz kimliği(Interface ID): Belirli bir alt ağdaki düğümlerin arayüzünü işaret eder.

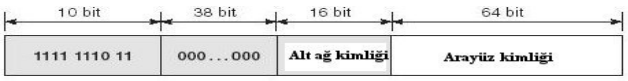
1- Tek alıcıya yönlenen site-içi adresi: IPv4 özel adreslerine benzerlik gösterir. Bunun kapsama alanı organizasyon sitesi içindeki ağdır(hem global hem de site içi adresleri kendi ağımız içinde kullanabiliriz.)

(IPv4'teki 10.0.x.x, 172.16.x.x, 192.168.x.x yerel ağ

Prefix: önek (hangi tür adres olduğunu işaret eden kavram.)

Site içi için önek → FEC0::/48'dir. 48 olma nedeni aşağıdaki şekilde görüldüğü gibi alt ağ kimliğine kadar olan kısmı almamızdır.

Adres yapısı



Şekil 3.4 Tek alıcıya yönlenen site-içi adresi

Başlangıçtaki sabit 48 bit'i 16 bit'lik alt ağ kimliği alanı takip ediyor. Bu alan sayesinde düz bir alt ağ yapısında 65.536 civarında alt ağ elde edilebiliyor. Alternatif olarak, alt ağ kimliği alanının yüksek sıra bitlerini alt katmanlara bölerek hiyerarşik bir yönlendirme yapısı yakalanabilir.

Not: İlk 48 bit'ten sonraki kısım global ve site-içinde aynıdır. Global adresteki 16 bit'lik kısım olan SLA kimliği de, site-içindeki yine 16 bit'lik alt ağ kimliği kısmının her ikisi de organizasyon sitesinin alt ağlarını ifade eder.

2- Tek alıcıya yönlenen bağ-içi adresi: IPv6 unicast bağ-içi adresleri IPv4 APIPA adresleri gibidir. Aynı link veya alt ağdaki bilgisayarlar birbirleriyle iletişim sağlamak için bu otomatik ayarlama adresleri kullanır. Neighbor

Discovery adı verilen komşu keşfi yöntemiyle adres çözümlemesi yapılır. Bağ-içi adresi için Önek FE80::/64'tür.

16lık taban = FE80 + MAC adresin değiştirilmiş şekli .

MAC adresi mesela 11-22-33-44-55-66 ise 11-22-33 ile 44-55-66 arasına FF FE'yi koyarsak bu durumda 64 bit'e çıkar ve 11-22-33-FF-FE-44-55-66 sonucuna ulaşılır.

İkilik Önek → 1111 1110 1000 0000 (169.254.x.x APIPA'yı düşün) **[15]**

Komşu Keşfi

IPv6 ND birbirine komşu düğümler arasındaki ilişkileri belirleyen işlem ve mesajlar setidir. IPv4'teki ARP, ICMP yönlendirici keşfi ve ICMP yeniden gönderme yerine geçmiş olup ek işlevler de sağlamaktadır.

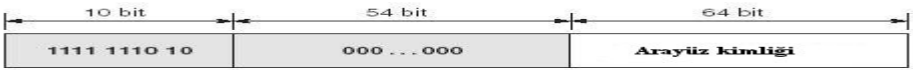
Bir link üzerinde düğümden düğüme iletişimi gerçekleştiren ICMPv6 mesajları setidir. Yönlendiriciler, bilgisayarlar ve düğümler bunu nasıl kullanıyor görelim.

-Bilgisayarlar ND'yi komşu yönlendiricileri, adresleri, adres öneklerini ve diğer parametreleri bulmak, keşfetmek için kullanıyor.

-Yönlendiriciler varlıklarını ilan etmek, duyurmak için; bilgisayarın alacağı parametrelerini yaymak için kullanıyor. Bunun yanında bilgisayardan gelen paketler hedefe iletirken daha iyi bir hop adresinden yararlanmalarında uyarabiliyor.

-Düğümler, paketin iletileceği komşu düğümlerin veri bağı katmanı adreslerini çözümlemede kullanıyor. Ki eğer komşu düğümün veri bağı katmanı adresi değiştiyse de bunu yine ND sayesinde öğrenebiliyoruz. **[16]**

Adres Yapısı



Şekil 3.5 Tek alıcıya yönlenen bağ-içi adres

Neden 64 ? Arayüz kimliğine kadar olan kısım 64 bit de ondan.

4- Tekli yayım geri çevrim adresi: Bu adres, IPv4'teki 127.0.0.1'e eşit değerdedir. Buradaki gösterimi ise 0:0:0:0:0:0:0:1'dir bir başka biçimde ::/1'dir.

5- Tekli yayım 6to4 adresleri: IPv6 6to4 adreslerini IPv4 İnternet'i üzerindeki iki farklı IPv6/IPV4 düğümünün haberleşmesini sağlamak için kullanır. Bu tip adresler herkese açık 32 bit'lik IPv4 adresiyle 2002::/16 önekinin birleşiminden oluşmuştur. Böylece 48 bit'lik bir önek elde edilir. 2002 : wwxx : yyzz :: /48 gibi .

wwxx:yyzz, w.x.y.z(herkese açık IP adresi)nin 16'lık tabandaki karşılığıdır. Ayrıca IPv4 adresi şu şekilde olabilir : 157.60.91.123 ve bu adres 2002 : 9D3C : 5B7B :: /48'e (6to4 adresi) çevrilebilir. **[17]**

Colon-hexadecimal(16'lık tabanda)

9D3C 5B 7B

Dotted-decimal(10'luk tabanda)

157 60 91 123

Çoklu yayım için 16'lık tabanda → FF00'dır. (önek) Global tekli yayım için 16'lık tabanda→ 2000(önek)

ÖRN : FEC0:bbbb:cccc:dddd:eeee:ffff:1111:2222 = site-içi tekli yayım FF00:0:0:0:0:0:0:1000 = çoklu yayım adresine bir örnektir.

IPv6'da iki çeşit yerel adres bulunmakta. Bunlar bağ-içi ve site içidir. Site içi olanı aynı organizasyon yada site içinde yer alan cihazların paket takası yapmasına olanak verir.Bu adresler İnternet bilgisayarlarına erişimde kullanılamaz. Bağ-içi ise site-içine nazaran daha küçük kapsama alanını işaret eder. Fiziksel linke yerelliği temsil eder. Ayrıca bu adres türü paketi iletmede de kullanılamaz. Ancak ND amacıyla yararlanılabilir.

Bağ-içi adreslerde esas amaç komşu keşfi(o alt ağdaki) ve kendi cihazının otomatik biçimde kendi kendine IP adresi alması.

IPv6'nın uygulamalara etkisi ise şu cümlelerle açıklanabilir : Yeni nesil İnternet protokolu olan IPv6, sonuçta bir 3.katman protokoludur. Bu katman TCP/IP protokol kümesinin 2.katmanıdır; bu protokol ile oluşan değişiklikler 4.katmanda bulunan uygulama protokollarına nasıl yansıyacaktır? Başka bir açıdan, IPv6 ile gelen değişiklikler kullanıcılara ve uygulama programlarına nasıl yansıyacaktır? Bunun görülebilmesi için IPv4 iyi bilinmelidir, daha sonra IPv6'nın ek başlık yapısı, adresleme yapısı incelenmelidir. Yüzeysel olarak, IPv6'nın fazla bir getirisi olmadığı sanılsa da, teknik açıdan bir çok şeyin değiştiği görülür.

3.13 IPv6 Adres Atama Yöntemleri

IPv6'daki en ilgi uyandıran ve değerli sayılabilecek özellik şüphesiz ki cihazların kendilerini bağımsızca ayarlayabilmelerini imkan tanıyan özelliktir. IPv4'te bilgisayarlar ilk zamanlarda elle (kişi tarafından adres atanmak suretiyle) ayarlanabiliyordu. Daha sonraları DHCP adı verilen bilgisayar adresi ayarlama protokoluna sahip sunucular ağa katılmış bilgisayarlara IP adreslerini tahsis etmeye başladı. IPv6 ise bu durumu bir adım öteye götürerek yeni bir yöntem tanımlamasına gidiyor. Bu yönteme göre bazı cihazlar, sunucuların yardımı olmaksızın kendi IP adreslerini ve öteki parametreleri

otomatik olarak ayarlayabilecek. Bu aynı zamanda ağdaki IP adreslerinin aralıklı olarak değiştirilebileceği anlamına gelen yeniden numaralama (renumbering) yöntemini de sunuyor.

Kendini başka cihazlardan bağımsızca ayarlayabilecek işte bu deyimsel tabiriyle "stateless" adını alıyor ki DHCPv6 kullanılarak yapılan "stateful"(bir yere bağlı)ın tam zıttı bir yöntem sergiliyor.

İki tür otomatik ayarlama mevcuttur IPv6'da. Bunlar bir yerden bağımsızca ve bir yere bağlı biçimde olan ayarlama.

3.13.1 Bir yerden bağımsızca otomatik ayarlama (Stateless Autoconfiguration): Başka bir cihazdan yardım almadan bilgisayarların kendine ayar çekmelerine yarar. Bu ayarlama türü bağ-içi adresleri, çoklu yayım yapmayı, ND Protokolu'nu ve 2.katman adresinden arayüz kimliği üretme yeteneğini barındırır.

Genel düşünce bir cihaz o ağın karakteristiğini öğrenene kadar kullanılacak geçici bir adres oluşturup daha sonra kalıcı hale getirmedir.

Not: Interface ID: Adresin hangi arayüze atanacağını işaret eder.

Adımlar:

1- Bağ-içi Adres üretimi: Cihaz bağ-içi adresi üretir. Bu adresler ilk 10 bit'te 1111 1110 10'a sahiptir. Üretilen adres bu 10 biti kullanır, takiben 54 sıfır ve sonrasında da 64bit'lik arayüz kimliği vardır.(Arayüz kimliği, 2.katman adresinden üretilir.) Bu üretim nasıl gerçekleşiyor?

Şekil 3-6 Bağ-içi adres

IPv6 arayüz kimliği 48 bit'lik MAC adresinden ortaya çıkarmak için:

a – 16'lık tabandaki sayı grubu 0xFF-FE, MAC adresindeki 3.ve 4. Byte arasına yerleştirilir.

b- Global/yerel bit, MAC adresin ikinci düşük sıra biti tümlendirilir. Eğer 1 ise 0'a ayarlanır 0 ise 1'e .Örnek verirsek MAC adresi 00-60-08-52-F9-D8 olsun.- 3.Byte 0x08 ile 4.Byte 0x52 arasına 0xFF-FE 16'lık tabandaki sayı grupları konur böylece 00-60-08-FF-FE-52-F9-D8'lik 64 bit şeklini alır. İlk bit olan 0x00'ın 2. düşük sıra biti tümlendirilir. Yani oradaki x 1 ise 0100'dan 0x00'dan 0x02 olur. Sonuç olarak Ethernet MAC adresine(00-60-08-52-F9-D8) karşılık gelen IPv6 arayüz kimliği 02-60-08-FF-FE-52-F9-D8 oluyor. Düğümün bağ-içi adresi FE80::/64 önekiyle 64-bit'lik arayüz kimliğinin birleşiminden oluşur. Bu örneğe bakarsak sonuç FE80::260:8FF:FE52:F9D8 elde edilir.

Not → :: koymamızın nedeni geri kalan 52 bit'in 0 olması.

2- Bağ-içi Adres Eşsizlik Testi: Düğüm, adresin ağda daha önceden alınıp alınmadığını kontrol eder. Düğüm komşuya davet mesajını ND Protokolu kullanarak yollar. Sonra başka bir düğümün o adresi kullandığını işaret eden "komşudan ilan" mesajını bekler. Eğer böyleyse ya yeni bir adres üretilecek veya adresin otomatik ayarlaması düşecek ve başka bir yöntem uygulanacak. (Eğer aynı adresten iki tane var mı tespiti başarısız olursa)

.3- Bağ-içi Adres Ataması: Aynı adresten iki tane var mı tespitinden başarıyla geçilirse ilgili arayüze atanır.

Adresin otomatik ayarlaması şöyle devam eder: (yönlendirici keşif aşaması)

a- Bilgisayar, yönlendiriciye davet mesajı gönderir.

b- Yönlendiriciden ilan mesajı alınmıyorsa, sonra bilgisayar adres ve diğer ayarlama parametrelerini elde etmek için bir yere bağlı biçimde adres ayarlama protokolu kullanır. (yani etrafta o bilgisayara cevap verebilecek yönlendirici bulunamazsa MECBUREN bir yere bağlı biçimdeki adresleme için ayar yapılır.)

c- Eğer ki yönlendiriciden ilan mesajı alınıyorsa mesajın içindeki ayarlama. bilgileri o bilgisayarda ayarlanır.

d- x) Adres öneki ve uygun 64-bit'lik arayüz ID, geçici bir adres oluşturmada kullanılır.

y) Aynı adresten iki tane var mı tespiti ise geçici adresin benzersizliğini doğrulamada kullanılır. Geçici adres daha evvel atanmışsa arayüzde başlatılmaz. **[19]**

Not:Bir yere bağlı biçimdeki adreslemenin yapılıp yapılmayacağı da tamamen Yönlendiriciden ilan mesajında belirtilir. Bağ-içi adres ayarlaması illa ki gerçekleştiriliyor. İstenirse yönlendirici keşfine çıkılıyor diğer parametreleri almak için. Bir yerden bağımsızca ayarlamayı yalnızca bilgisayarlar(yönlendirici dışındaki cihazlar) yapabilir. Yönlendirici ve öbür ara cihazlar elle ayarlanmalıdır.

Bilgisayarlar → Bir yerden bağımsızca ayarlama, elle, DHCP yönlendirici → Elle, DHCP

Yönlendiriciden ilan mesajları içinde bir yerden bağımsız adres türü için önekler ve bir yere bağlı biçimde adresleme için işleyen protokol varsa bilgisayar bir yerden bağımsızca adreslemeye, tam tersi ise bir yere bağlı olacak biçimde adreslemeye tabi tutulur.

Durumlar:

Bağ-içi benzersiz(tek) çıktı ve çevrede yönlendirici bulunamadı diyelim hatta DHCP de yok işte bu durumda elle ayar çekilir. Bağ-içi benzersiz çıkmazsa otomatikman elle, Bağ-içi benzersiz çıktı ve yönlendiriciden ilan da geldi o zaman bir yerden bağımsızca adresleme .Bağ-içi benzersiz çıktı ancak çevrede yönlendirici bulunamadı (yönlendiriciden ilan gelmedi bilgisayara) o zaman bir yere bağlı kalınarak adresleme (yani DHCPv6 ile ayarlama.)

3.13.2 Bir yere bağlı biçimde otomatik ayarlama (Stateful Autoconfiguration): Ayarlama bilgisinin bir sunucu tarafından sağlandığı tekniktir. DHCPv6 Protokolu ile gerçekleştirilir. Eğer istemci, IP adresine

sahipse diğer ayarlama bilgilerini almak için bundan yararlanılır. Yok IP adresi de taşımıyorsa o zaman IP adresi de bu tür sunuculardan elde edilir.

4. Hareketli IP

Taşınabilir cihazlarla ilgili hesaplamanın önemi gün geçtikçe artmaktadır. Bunun birkaç nedeni bulunmaktadır:

-Taşınabilir(hareketli)cihazların sayısının giderek yükselmesi

- O düğüm her nerede olursa olsun İnternet'e bağlanabilirliğin sağlanması.

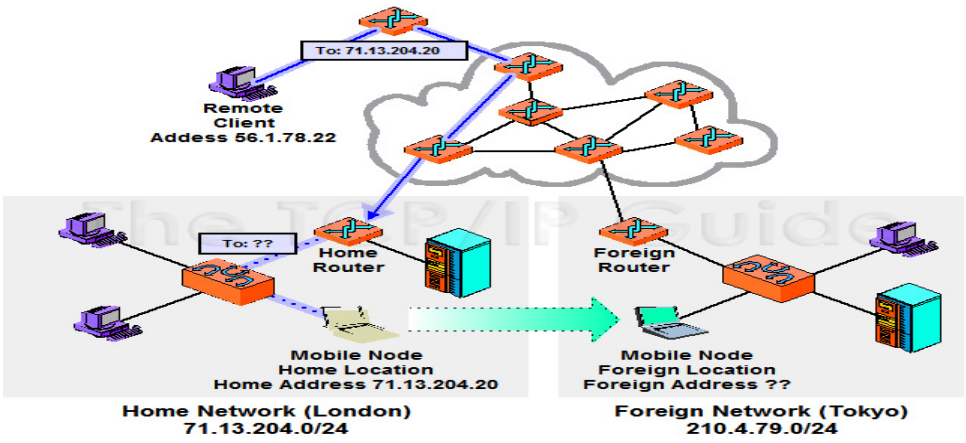
- İnternet Protokolu'nun, ağ cihazlarının bir yerde sabitlenmiş veya nadiren az hareketli olduğu varsayılarak geliştirilmesi.

İnternet altyapısı, TCP/IP Protokol kümesi adı verilen protokollar bütünü üzerine inşa edilmiştir. İsminde de geçtiği üzere TCP ve IP protokolları çekirdektir. IP, İnternet'e bağlı herhangi bir bilgisayarın benzersiz bir IP adresi taşımasını şart koşar. Bu durum, hareketlilikte çok önemli bir sorunu beraberinde getirir. Çünkü bir bilgisayar(hareketli), başka bir fiziksel bölgeye yol aldığında IP adresini yenisiyle değiştirmesi gerekir. Bununla birlikte, üst katman protokolları bağlantıların saptanması için bilgisayarın IP adresinin değişmezliği felsefesine göre çalışır. Hareketli IP, İnternet Protokolu'na bu problemi ortadan kaldırmak için bir uzantı, bir ek özellik kazandırma şeklinde düşünülmüştür.**[20]**

4.1 TCP/IP'de Hareketli Cihazlarla İlgili Problemler

Bilindiği üzere IP adresi iki bölümden oluşur. Bunlardan biri ağ kimliği öbürü ise bilgisayar kimliğidir. Ağ kimliği, bir veya birçok bilgisayarın hangi ağda bulunduğunu gösterir. Bilgisayar kimliği de doğrudan ilgili bilgisayarı tanımlar. Ağ kimliği, paketlerin yönlendirilmesi sırasında gereklidir. Bu durum çoğu ağ cihazı için sorun teşkil etmese bile esas sıkıntıyı hareketli diye nitelendirdiğimiz cihazlarda yaşatmaktadır. Hareketli bir cihaz kendi ev

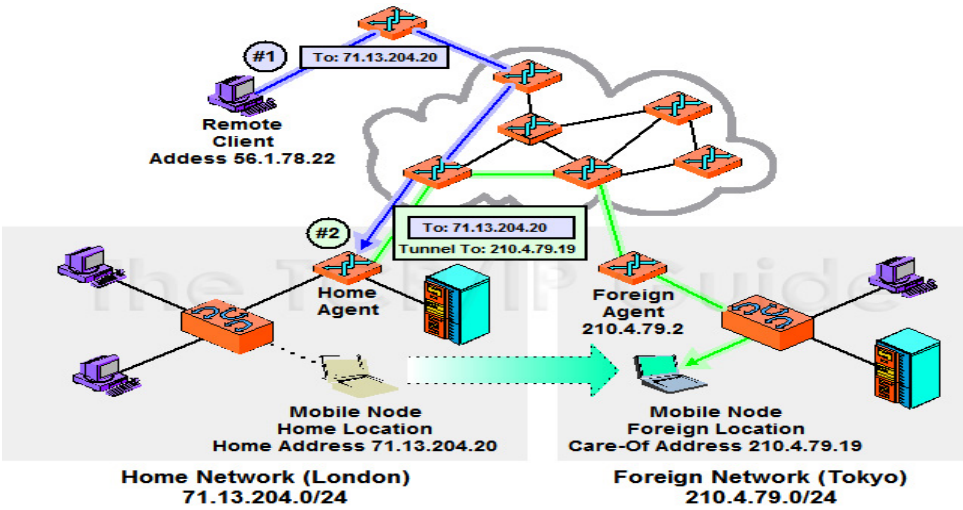
ağından ayrılıp yer değiştirdiğinde IP sistemi bozulmaktadır. Yaşanan bu sıkıntı aşağıdaki şekilde gösterilmektedir.



Şekil 4.1 Hareketli IP Protok.Uygulanmazken Ortaya Çıkan Sorun

Şekle bakıldığında ev ağında bulunan hareketli cihaza uzaktan erişim sağlamak isteyen bir istemci var. Ki o istemci, hareketli cihazın daima ev ağında kaldığını varsayarak bir paket yollamakta. Ancak temel sorun da işte bu aşamada ortaya çıkıyor. Ev ağındaki hareketli cihaz, başka bir ağa gittiğinde, istemcinin paketi kendisine ulaşamayacaktır. Nedeni ise artık o hareketli cihaz ev ağından çıkıp başka bir ağa gittiğinden ve bu konuda ev ağındaki yönlendiricinin de bilgisi olmadığından paketi iletemeyecek oluşudur. Hareketli cihaz şu anda Tokyo'dadır ama bundan ev ağı yönlendiricisinin bile haberi yoktur. İşte hareketli IP adı konulan bir protokol sayesinde bunun üstesinden gelinmekte, hareketli cihazlara ve yönlendiricilere paketi sevk etme yeteneği kazandırılmaktadır.

Eğer hareketli cihaz her nerede olursa olsun kendisine gelen paketlerin alınması isteniyorsa paket sevkine başvurulmalıdır. İşte bu paket sevki olayının nasıl gerçekleştiği de bir örnek ile görülebilir.



Şekil 4.2 Hareketli IP Protokolu'nun çalışması

4.2 Hareketli IP Protokolu'nun Çalışması

Yine aynı istemci ile aynı hareketli düğüme paket gönderiminde bulunuluyor. Fakat bu sefer, Hareketli IP Protokolu uygulandığından ileti sevki kullanılarak paket istenen yere ulaştırılabilecektir. Çünkü bu kez ev ağından başka ağa yer değiştiren hareketli cihaz, hareket ettiği sırada ev ağındaki yönlendiriciye kendisinin nereye gittiğini söylemektedir. Ve ne zaman hareketli cihaza bir ileti gönderilmek istense, o ileti önce ev ağına kadar gelecektir daha sonra ise ev ağındaki yönlendirici bu iletileri şu anda hareketli cihaz ev ağında bulunmadığı için yakalayacak ve hareketli cihaz hangi ağı ziyarete gittiyse oraya yönlendirecektir. Bu yönlendirme de iki türlüdür. Hemen bir üstteki şemadaki gibi ya doğrudan yabancı ağdaki hareketli cihaza, ya da yabancı ağdaki yönlendiriciye olmak üzere.

Yukarıdaki şemadaki sistemin bazı getirileri vardır: Öncelikle anlaması ve uygulaması kolaydır. Bunun dışında, nereye gidilirse gidilsin ileti alınmaktadır ayrıca hareketli cihazın yer değiştirmesiyle ilgili işlere yalnızca ev ağındaki, bazen de yabancı ağdaki yönlendirici bakmakta, iletiyi gönderenin bu işlemlerden haberi olmamaktadır.

Bunun yanında götürüleri de vardır: Ev ağında bulunan yönlendirici bu işi bedavaya yapıyor olsa da işlemin sürekli yinelenmesiyle bir süre sonra yıpranacak ve dolacaktır. Ayrıca ziyaret edilen her ağla ilgili özel bir anlaşmaya ve hareketli cihaz hareket ettiği her an ev ağındaki yönlendiriciyle iletişim kurmaya gerek duyulmaktadır. Belki de en önemli sorun ise paketin önce ev ağına uğraması daha sonra da yabancı ağa iletilmesiyle iletinin ağlardan iki kez geçmesi ve gereksiz trafik yaratmasıdır. Gereksiz trafik de ağlardaki trafik akışını yavaşlatmaktadır.

4.3 Hareketli IP Protokolu'na İlişkin, Şekillerde de Geçen Bazı Kavramlar

.4.3.1 Ev Adresi(Home Address): Hareketli cihaz, ev ağına tutturulduğunda kendisine atanan adres. Ayrıca bu adres sayesinde, hareketli cihaz nereye gitmiş olursa olsun kendisiyle iletişim sağlanabilmektedir. TCP ve üst katmanların kullandığı, hareketli düğümün değişmez adresi. Uçtan uca bağlantıları sürdürebilmek için gerekli adres.

4.3.2 Ev ağı(Home network): Hareketli cihazın ev ağı.

4.3.3 Ev aracı(Home agent,home router): Hareketlilik ile ilgili bir tablo tutan, hareketli cihaz başka ağlara gittiğinde oradaki adreslerini ve kayıtlarını not alan aracı. Tablo şu şekildedir:

Ev adresi	Ilgili adres	Yaşam süresi
131.193.171.4	128.172.23.78	200
131.193.171.2	119.123.56.78	150

Tablo 4.3 Hareketlilik bilgileri tablosu

.4.3.4 Yabancı ağ(Foreign network): Hareketli cihazın ağı olmayan , ziyaret ettiği ağ.

.4.3.5 Yabancı aracı(Foreign agent, foreign router): Hareketli cihazın bulunduğu yabancı ağdaki aracı. Hareketli cihaza hizmet sunan bir aracı. Bu aracı da bir tablo tutar ki adı da ziyaretçi listesi tablosudur. O anda ağa kim uğramışsa onların listesini tutar.

Ev adresi	Ev ajanı adresi	MAC adresi	Yaşam süresi
131 193 44 14	131 193 44 7	00 60 08 95 66 F1	150
131.193.33.19	131.193.33.1	00-60-08-68-A2-56	200

Tablo 4.4 Ziyaretçi listesi tablosu

.4.3.6 Geçici adres (Care-of address): Şu anda hareketli cihaz hangi ağdan bağlı ise İnternet'e, orada aldığı IP adresi.IP yönlendirmesine göre cihaz hangi ağda İnternet'e erişmek istiyorsa o ağa uygun IP adresi almalıdır yani yenisiyle değiştirmelidir.

.4.3.7 Hareketli cihaz (Mobile node): İnternet'e o andaki tutturulma noktasını değiştiren cihaz. Bir tane ev adresi bir de geçici olmak üzere iki adrese sahiptir.

.4.3.8 Hareketli cihazla iletişime geçen hareketli veya sabit cihaz (correspondent node)

Kısaca, hareketli IP uygulandığında paketler hareketli cihazın ev adresi vasıtasıyla o ev ağına ulaştırılır ve olağan durumda ev aracıdan geçerek yine ev ağındaki hareketli cihaza iletilir. Eğer hareketli cihaz başka ağa taşınırsa işte burada ev aracı paketleri tutar ve hareketli cihazın o an bulunduğu ağda aldığı adrese tüneller.[23]

Not: Ev aracı ve yabancı aracı keşfi Hareketli IP Protokolu'nda tanımlanmıştır.

.4.4 Hareketli IP Protokolu'nun Çalışması Sırasında Gerçekleşen İşlemler

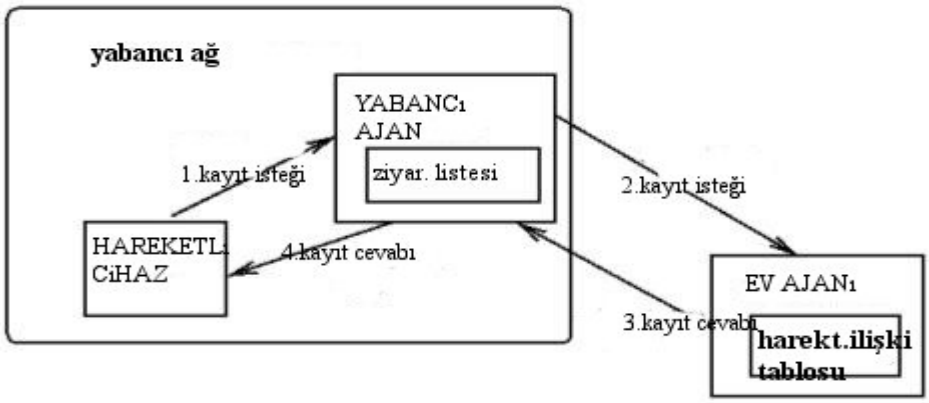
.4.4.1 Aracı Keşfi(Agent Discovery): Hareketli IP protokolunun yürütülmesinde ilk gerekli aşama aracı keşfidir. Bu aracı denilen cihazlar aslında yönlendiricilerdir. Biri ev aracı iken öbürü de yabancı aracıdır. Bunların keşfedilmesinin nedeni ise belli sorumluluklar üstlenmeleridir. IPv4'te aracı keşfi ev aracı ve yabancı aracının bulundukları ağ içinde varlıklarını duyurmaları ile gerçekleşir. Hareketli IPv4'te bir göndericiden(aracılar) o yerel ağdaki tüm alıcılara yönlenecek biçimde duyuru yapılır. Duyuruları hareketli cihaz(lar)dinler. Daha sonra bu duyuruları alan hareketli cihaz artık ilgili aracılardan haberdardır ve kayıt işlemini başlatır.

Not : Eğer hareketli cihaz başka ağa taşınmışsa, geçici bir adres edinmesi gerekir. Yalnız bu geçici adres de ikiye ayrılır:

a- Yabancı aracıdan alınan geçici adres (Foreign agent care-of address)

b- Hareketli cihazın DHCP'den edindiği geçici adres(Co-located care-of address)

4.4.2 Kayıt: Bu işlemin yürütülebilmesi için öncelikle, hareketli cihazın kendi ağından ayrı bir yabancı ağda bulunması şarttır. Kayıt isteği ve kayıt cevabı adı verilen iletilerle gerçekleştirilir. Önce, hareketli cihaz hangi ağda konaklıyorsa bunu kendi ev aracıya bildirmelidir. Kayıt işlemi şu şekilde yapılır: Kayıt isteği yabancı aracıdan geçerek ev aracıya iletilir ve ev aracı da hareketli cihazı geçici adresi ile birlikte hareketlilik tablosuna kaydedip cevabı hareketli cihaza gönderir. Bu hizmetin belirli bir yaşam süresi vardır. Bu yaşam süresi, hareketli cihazın yabancı bir ağdan yeni bir ağa geçişi arasındaki zaman dilimidir.



Şekil 4.5 Kayıt Süreci

Aracıların keşfedilmesi ve hareketli cihazın da kendini ev aracıya kaydetmesi işlemi tamamlanır. Böylece hareketli cihazla iletişim kurmak isteyen cihazın paketleri ev aracı tarafından tutulur ve o anda hareketli cihaz hangi ağa yerleşmişse oraya sevk edilir. Ev aracı, hareketli cihaza erişmek isteyen cihaza kendisini hareketli cihaz gibi gösterir.

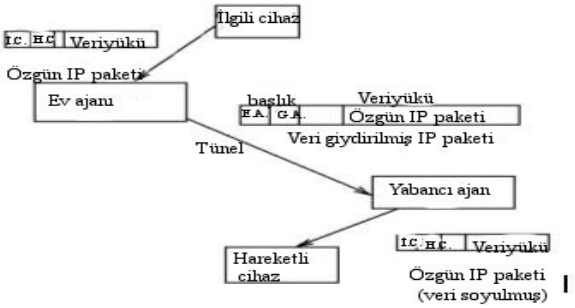
Not: Eğer hareketli cihaz kendi ev ağına dönerse kayıt işlemini iptal ettirmelidir. Çünkü o durumda bir yabancı ağda yer almadığından kayda da gerek yoktur.

.4.4.3 Tünel açma(Tunneling)

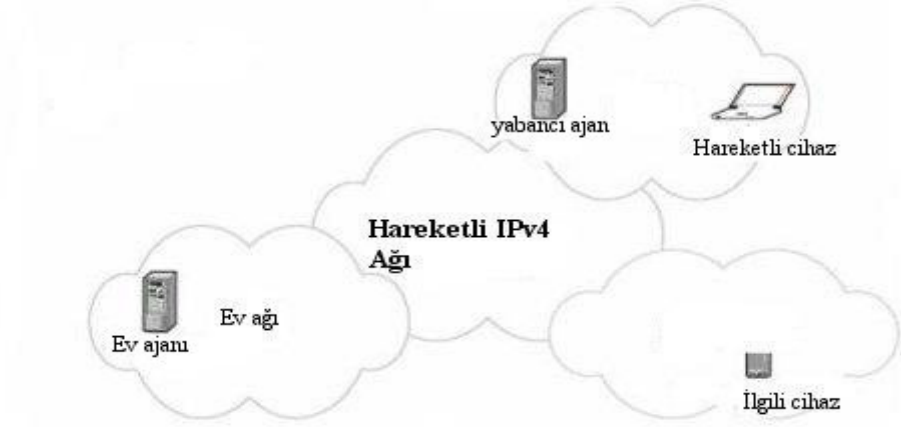
Geçici adres, ev aracıya ev adresiyle birlikte kaydettirildikten sonra hareketli cihazın ev adresine gönderilmesi tasarlanan paketleri, ev aracı yakalayıp hareketli cihazın geçici adresine bir tünelden bırakarak iletecektir. Bu tünel ya yabancı aracı da ya da hareketli cihazın kendisinde son bulacaktır. Tünel yabancı aracıda bittiğinde, yabancı aracı ile hareketli cihaz arasındaki iletişim 2.katman seviyesinde gerçekleşir ve yabancı aracı özgün paketi tünelden kaldırır sonra da hareketli cihaza teslim eder.

Tünel açma bir diğer adıyla IP içinde IP giydirmesi olayı aşağıdaki şekilde verilmiştir. IP içinde IP giydirmesinde amaç uçtan uca bağlantıyı sağlayarak yaptığımız işlemin hareketli cihaza ve onunla iletişim kurmak isteyen cihaza

karşı şeffaflığını sağlamaktır. Eğer tünel hareketli cihazda biterse o durumda o cihaz özgün paketi tünelden kaldırma sorumluluğu taşır.



Şekil 4.6 IP Tünel açma

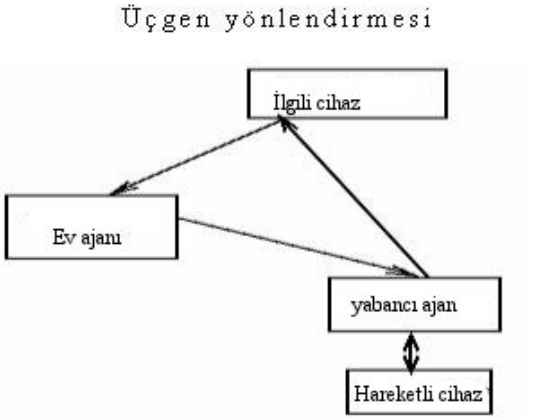


Şekil 4.7 Hareketli IP Protokolu çalışması[24]

.4.5 Hareketli IP Protokolu'nda Karşılaşılan Sorunlar ve Çözüm Öneriler

4.5.1 Üçgen yönlendirme(Triangle routing): Üçgen yönlendirmesine göre, hareketli cihazla iletişim kurma düşüncesindeki cihaz, paketleri ev ağına gönderir sonra paketleri ev aracı tutar ve hareketli cihaza yönlendirir.Bu esnada yabancı aracı giydirilmiş paketin kılıfını çeker çıkarır ve hareketli cihaza verir. Daha sonrasında da hareketli cihaz artık ilgili cihaza cevap mesajı yollar. İşte bu durum bir üçgen yönlendirmesidir. Paketler ağda dönüp du-

rur. Üçgen yönlendirmesinde sorun, hareketli cihaz ve ona erişmek isteyen cihaz birbirine ev aracıdan olduklarından daha yakınsa ortaya çıkar.



Şekil 4.8 Üçgen yönlendirmesi

İlgili cihaz hareketli cihazla irtibata geçmek istediğinde illa ki ev aracıyla meşgul olunacaktır. Bu da uzun süreli bir gecikmeye ve ağda gereksiz yüke yol açacaktır.

Olası çözüm: Ev aracıyla zaman kaybedilmeden ilgili cihazın paketlerinin doğrudan hareketli cihaza iletilmesidir. Bu da hareketli cihazın geçici adresinin ilgili cihaza anlatılmasıyla gerçekleşecek ve ilgili cihaz yabancı aracıya kendi tünelini kurarak paketleri doğrudan hareketli cihaza iletecektir. Hareketli IP Protokolu, ilgili cihazla yabancı aracı arasına izlenecek yolu depolayan bir önbellek koyabilir ve eğer ilgili cihaz, hareketli cihaza ait girdileri tutan bir önbelleğe sahip olursa paketler ev aracı meşgul edilmeden doğrudan geçici adrese tünel edilebilir.

Not: Hareketli IP Protokolu'nun ev aracı ile hareketli cihazın geçici adresi arasında tünel açmasının sebebi, o aralıktaki diğer yönlendiricilerin, hareketli cihazın ev adresini öğrenmesini engellemek. Çünkü iki gizli ağın iletişimi İnternet yani açık ağ üzerinden sağlanıyor.

.4.5.2 Güvenlik sorunu(Güvenlik duvarları)

Güvenlik duvarları bir sorun teşkil etmekte çünkü belli bir kritere uymayan ve o ağa gelen paketleri keser. Zaten güvenlik duvarlarının görevi güvenilir,gizli ağlarla İnternet gibi herkese açık ağlararasına set çekmektir. Bu her ne kadar İnternet'e iç ağdan erişmek isteyen kullanıcıyı yönetmek için uygun görünse de, ev ağındaki hareketli cihazların birbiriyle iletişime geçmesini önlemektedir.

4.5.3 Hareketli IP'ye yönelik güvenlik tehditleri

4.5.3.1 İçeriden birisinin saldırısı(Insider attacks)

Örnek: Bir şirkette çalışan bir kişi mahrem verilere erişip dışarıdaki bir kaynağa aktarabilir.

Olası çözüm: İlgili kişinin kesin kontrolu sağlanıp şirket içindeki kişi ve bilgisayarların doğrulanması, kaynaktan hedefe giden paketin şifrelenmesi.

4.5.3.2 Hizmeti yürütülemez hale sokma(Denial of Service)

Örnek: Bir kullanıcının ağ trafiğine sıkıntı verecek biçimde, paketleri salması ve kullanıcıların bundan dolayı görevlerini yapamaması

Olası çözüm: Sağlayıcılarla, kaynak adresinin sahiciliğinden emin olmak için yönlendiricilerinde paket iletilmeden önce filtreleme yapılabilir.

4.5.3.3 Tekrar saldırıları(Replay Attacks)

Örnek: Bir saldırgan kayıt isteğinin bir kopyasını alır sonra onu depolayıp yeniden kullanır. Bu yolla yapay bir geçici adres elde edilebilir.

Olası çözüm: Hareketli cihaz kayıt için olan art arda gelen her girişimde eşsiz bir kimlik alanı üretiyor. Bu kimlik alanı, ev aracının, takip eden değerin ne olabileceğini anlamasına olanak tanıyor. Saldırgan bu durumdan zararlı çıkıyor çünkü saldırgandaki kayıt isteği ev aracıya göre tarihi geçmiş görülebilir.

4.5.3.4 Bilgi hırsızlığı: Etkisiz kulak misafirliği(Passive eavesdropping)

Örnek: Saldırgan, bilginin mahremiyetine göz dikebilir

Olası çözüm: 1- Uçtan uca şifreleme 2- 2.katman şifrelemesi

4.5.4 Ev aracı ve yabancı aracı adı verilen yönlendiricilerde NAT kullanılması

NAT uygulanan ağlarda içteki kaynak adresi ve port numarası değiştirilip içteki bilgisayarı dış tehditlerden korumak için sanki paketler NAT kurulmuş cihazlardan çıkıyor görünüyor. Bu da bazı uygulamaların tam verimle çalışamaması anlamına geliyor. Örneğin uçtan uca şifreleme mantığına sahip IPSec Protokolu çalışabilme için ana kaynak adresi ve porta ihtiyaç duyuyor.

4.5.5 İnternet'in iki kez dolaşılması

İlgili cihazdan hareketli cihaza paket akışı sırasında önce ev aracıya gidilirken İnternet'ten geçilir. Daha sonra da ev aracıdan hareketli cihaza tünel açılırken gerçekleşir.

4.5.6 NAT yüzünden şifrelemenin yetersiz kalması ve ayrıca IPv4 başlığında hareketlilik üzerine istenilen yerin olmaması[25]

5. Hareketli IPv6

Hareketli IP Protokolu'nun yeni uyarlamasına verilmiş ad Hareketli IPv6'dır. Hareketliliğe özel ve yeni bir protokola adım atılmasında en başta İnternet Protokolu'nun değişimi yatmaktadır. Özellikle IP adresi konusunda ciddi sıkıntıların baş gösterdiği ve temelinde özellikle uzak ağlararasında paket teslimi bir göreve sahip olan İnternet Protokolu evrim geçirme zorundaydı. Tabii IP adres yetersizliği olunca ki günümüzde kullanılabilir IP adres sayısı % 19'larda seyrederken, Bazı uygulamaların yine bazı mekanizmalardan kaynaklanan engellemelerinden dolayı tam verimli ve doğru bir şekilde çalışamaması da önemli nedenler arasındadır.

.5.1 Neden Hareketli IPv6'ya Geçildi?

Bilindiği üzere, hareketli IPv4 hareketli cihaz başına iki adres kullanımını şart koşuyordu ve IPv4 adresleri hızla tükeniyordu. Kimi durumlardan dolayı da herkese eşsiz ve aynı zamanda İnternet'e erişim sağlayabileceği türden yani halka açık adres vermek imkansız gibi bir şeydi. Bunun haricinde, hareketli IP'nin yararlandığı tünel açma yöntemi yüksek maliyetli bir biçimde bant genişliği kullanımına dayanıyordu. Yine, IP adres sıkıntısı çekildiğinden IP başlığında hareketlilik bilgisine istenildiği ölçüde yer verilemiyordu.

Tüm bunların yanında Hareketli IP adı konulan protokol ilk geliştirilen ve cihazların konum olarak ya sbt ya da nadiren değiştiği bir yapıya sahip İnternet Protokolu'nun ana mayasında bulunmayıp sonradan hareketli cihazların giderek yaygınlaşması sonucu bir eklenti biçiminde getirildiği için yüksek başarım gösteremiyordu. Özellikle bu tür nedenlere dayanılarak Hareketli IPv6'ya geçiş gerçekleşti.

5.2 Hareketli IPv6'nın Getirdiği Kazanımlar ve Yenilikler

1- Geniş adres aralığı sayesinde ek başlıklar kullanarak daha esneklik sağlanması

2- Özgün yeni nesil İnternet Protokolu'nun bir parçası olması, IPv4'teki gibi, bir eklenti olmaması

3- Ev aracı kullanılması ancak yabancı aracıya gerek duyulmaması

4- Gelişmiş güvenlik için IPSec desteği

5- NAT gibi, son kullanıcılar için güvenlik sağlasa da IP adresi ve portlarda değişikliğe gidildiği için aksaklıklara yol açan mekanizmaların artık uygulanmayacak oluşu

6- Hareketli IP'de verimsiz bir yönlendirme olan üçgen yönlendirmesinin burada olmayışı

7-.IPv6'daki otomatik adres ayarlaması (autoconfiguration) özelliğiyle hareketli cihazın geçici adres alabilmesi

.a- DHCP ile veya ziyaret edilen ağın öneki + arayüz kimliği(MAC adresi + 16'lık FF-FE bitleri)

b- Ev aracıyı bulmak için ev ağında, göndericiden çıkıp iletilmesi istenen alıcılardan yönlendiriciye en yakın olanına teslim edilen(anycast) paket kullanılması

c- Arayüz başına bir çok adrese sahip olabilme(Ev adresi + geçici adres)

Hareketli IPv6'da hareket tespiti ve geçici adres edinme

Hareketli bir cihaz yeni ağa taşındığında hareket tespitini yönlendirici(aracı)lerin duyuru iletilerinden yapar. Hareketli cihaz, yönlendirici keşfi iletisi yollayarak yönlendirici duyuru iletilerinin kendisine gönderimini de sağlayabilir. Yeni bir duyuru iletisi alındığında hareketli cihaz yeni bir geçici adres alabilir.(yönlendirici varlık duyurusundaki öneke dayanarak) Bu yüzden bir IPv6 hareketli cihazı mevki yenilediği an, yönlendirici keşfinden yararlanıp hareketin saptayabilir. Ayrıca IPv6'daki otomatik adres ayarlamasına başvurarak yeni geçici adresini edinebilir.

Burada Hareketli IP'ye göre farklardan biri o ağ içindeki istisnasız her cihaza gönderilen ve ağı yoran adres türünün(broadcast) kullanılmayışı ve aracıların kendi varlıklarını duyurması beklenmeden hareketli cihazın onları bulabilmesi ve kendine otomatik bir biçimde adres atayabilecek oluşudur.

İzlenecek yolu iyileştirme(Üçgen yönlendirmesinden kurtuluş)

Hareketli IPv4'te ilgili cihazdan başlayıp ev aracının aracılığıyla yolun uzayıp hareketli cihazda sonlandığı verimsiz üçgen yönlendirmesi ile karşılaşılıyordu. Bu üçgen yönlendirmesi yöntemiyle paketler her şekilde hareketli cihaza ulaşıyordu. Ancak gecikme,ağ trafiğinin yavaşlaması sorunları yeni ve daha sorunsuz bir yola gerekliliği de gösteriyordu. İşte bu yüzden izlenecek yolu iyileştirme daha bir üst aşamaya çekildi.

İzlenecek yolu iyileştirme(route optimization) IPv4'te tüm cihazlar için seçenekli iken hareketli IPv6 uygulanan cihazlar bu yetenekle donatılacak şekilde tasarlanmıştır. Yenilenmeye göre, hareketli cihaz ev aracıdan tünelden geçerek gelen bir paket aldığında, kendine özgün paketi yollayan ilgili ciha-

zın, şu anda bulunduğu yerden habersiz olduğunu bilir. Bu nedenle, üçgen yönlendirmesinden kaçınılması için ev adresi ve geçici adresin ilişkilendirilmesinin güncellenmesini(binding update) kullanarak ilgili cihazın paketleri doğrudan hareketli cihaza iletimini sağlayabilir. Geçici adresini ilgili cihaza bildirerek.

Ev adresi ve geçici adresin ilişkilendirilmesinin güncellenmesi(Binding update)

a- Geçici adres, ev adresi, yaşam süresi

b- Ev aracı ve ilgili cihaza gönderilebilir.

c-Önceki ilişkilendirmeleri silmek için de kullanılabilir.

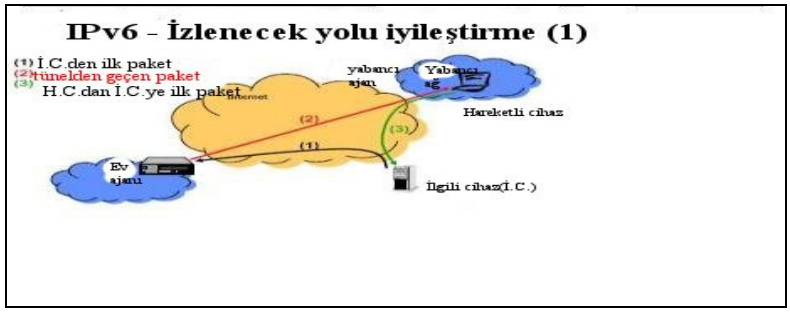
Ev adresi ve geçici adresin ilişkilendirilmesine dayanan aldım cevabı(Binding ack)

Eğer doğrulama başarısız olursa, ilişkilendirme reddedilebilir.

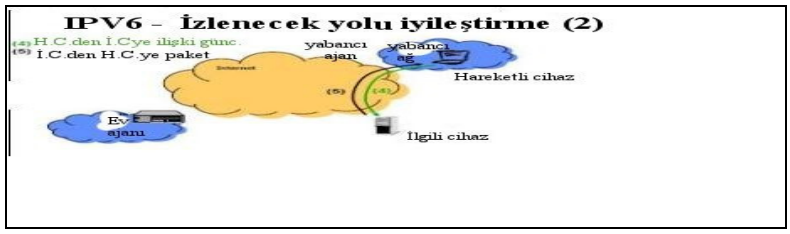
Ev adresi ve geçici adresin ilişkilendirmesinde yeni istek(Binding request)

a- Yaşam süresi dolduğunda ilişkilendirmeyi tazelemek içindir.

b- Hareketli cihazın yeni bir geçici adres alması ve yaşam süresini de yenilemesi isteği



Şekil 5.1 IPv6-İzlenecek yolu iyileştirme



Şekil 5.2 IPv6-İzlenecek yolu iyileştirme 2

İlk şekil hareketli IPv4'teki olayın aynısı iken, ikinci şekilde hareketli cihaz ile, ilgili cihaz arasında çift yönlü iletişim söz konusu. Ancak bu, güvenlik açısından sıkıntı yaratabileceği için şifreleme gerekmekte

Ev aracıyla hareketli cihaz arasında da güvenlik sağlanması için IPSec tüneli sorunsuzca kurulur. İlgili cihaz, hareketli cihazdan bir paket aldığında önbelleğinde hareketli cihazın geçici adresiyle ilgili bir bilgiye sahipse onu kontrol eder, tersi durumda ise ilgili cihaz paketleri hareketli cihazın ev adresine yollar. Hareketli cihaz ev ağını terk etmişse, ev aracı paketleri alır ve hareketli cihazın geçici adresine tünel açarak iletir. Ki bu durum zaten bir evvelki hareketlilik protokolu ile aynıdır. Hareketli cihazın ev aracı rahatsız edilmeden doğrudan ilgili cihazla iletişim kurması için, öncelikle ev aracıdan ve hareketli cihazdan ilgili cihaza bağlantı yolu güvenli hale getirilmelidir.Bu, dönüş yönlendirilebilirliği (return routability) adı verilen yordamla gerçekleştirilir.

-Yabancı aracı gibi özel bir yapıya sahip yönlendiricilere hareketli IPv6'da gerek duyulmadı. Hareketli IPv6 yerel yönlendiriciden gelecek özel bir desteğe gerek duymaksızın her yerde çalışabilir.

- Hareketli IPv6, ARP yerine IPv6 komşu keşfini kullanır. Bu da protokolun dayanıklılığını artırır.

- Hareketli IPv6, IPv6 Protokolu'nun genişletilebilirliğini kullanır. Bunu da yeni komşu keşfi mesajlarını türlerini, yönlendirici başlığını tanımlayarak ve IPv6 paketinde hedef seçeneği taşımayla gerçekleştirir. IPv4'te bunlar yer almaz.

-Evinden ayrı olan hareketli cihaza gönderilen IP paketlerinin çoğu, hareketli IPv4'te ağa nefes aldırmayan veri giydirme yerine yönlendirme başlığı ile gönderilmektedir.

-Hareketli IPv6'da yabancı aracı yerine 3 tür adres olayı söz konusu. Şimdiki geçici adres, eski geçici adres ve yeni geçici adres. Bu 3 servis sayesinde ev aracıyla iletişim kurulmakta, paketlerin doğru işlenmesi garanti altına alınmakta ve izlenecek yolun iyileştirilmesi daha iyi hale getirilmektedir.

5.3 Hareketli IPv6 Çalışması

Aşamalar:

1- Yönlendirici, hareketli cihaza o cihazın yerini ve ev aracı IP adresini duyurur, hareketli cihaz onu tutar.

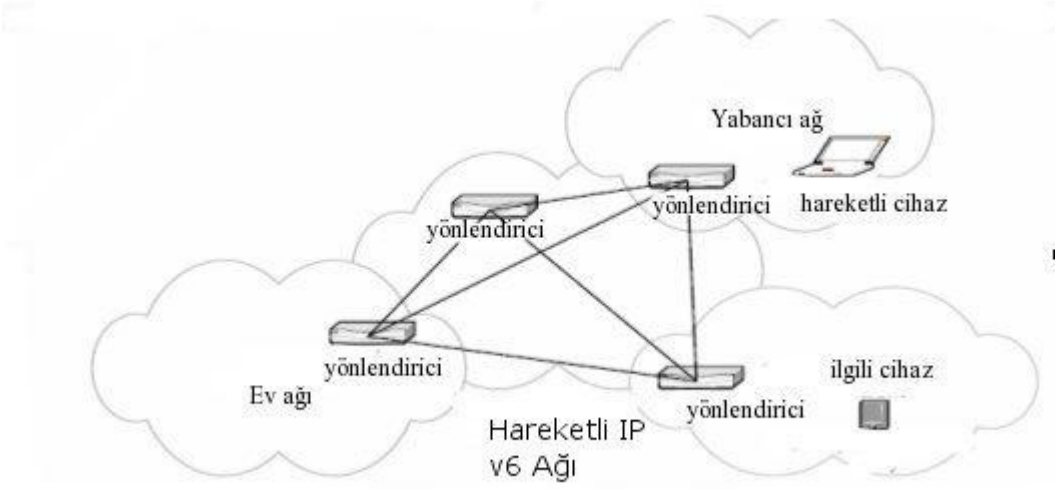
2- Hareketli cihaz, yeni bir ağa taşındığında yeni bir yönlendirici duyurusu alır. Otomatik adres ayarlaması ile yeni bir adres alır ve yönlendiriciden şimdiki geçici adres edinir. Sonra bunu depolar.

3- Daha sonra hareketli cihaz ev aracıya ev adresiyle geçici adresin ilişkilendirilmesinin güncellemesini yollar ve cevap alır. Ev aracı ayrıca hareketli cihaza ARP cevabı yollar.

4- İlgili cihaz hareketli cihazla temas girişiminde bulunduğunda bağlantı başlatır. Uzak cihaz, ev aracının MAC adresiyle, hareketli cihazın IP adresine yollar.

5- Ev aracı, paketleri bir kılıfa sokar ve hareketli cihaza ulaştırmak üzere tünelden geçirir. Hareketli cihaz, yönlendirici yoluyla uzak cihaza cevabı gönderir.

6- Hareketli cihaz, ev ağına döndüğünde yönlendirici duyuru su alır ve ilişkilendirmeyle ilgili güncellemeyi ev aracı ve ilgili cihaza iletir. Ayrıca eski geçici adrese de bu güncellemeyi yollar.



Şekil 5.3 Hareketli IPv6 çalışması

Uzak cihaz denilen cihaz, orta ağdaki yönlendiricidir.**[26]**

5.4 Hareketli IPv6'daki Güvenlik Problemleri

Hareketli IPv6'yı tasarlamanın önemli nedenlerinden biri de şüphesiz IPv6'yı hareketli hale getirip güvenliği de en az Hareketli IPv4'teki gibi yapmaktı. Halbuki yeni nesil Hareketlilik Protokolu'nun da güvenlik açısından açıkları bulunmakta. Bunlardan en büyüğü de ilişkilendirme güncellemelerinin yetkilendirilmesidir.

İzlenecek yolun iyileştirilmesi olayı hareketli IPv4'teki gibi bir eklenti olmayıp IPv6 içinde yer alıyor ve üçgen yönlendirmesi yok edilerek yönlendirmenin verimliliği artırılıyor. Her ne kadar verim artsa da bununla beraber gidip gelen güncelleme paketlerinin artış göstermesi de yüksek bir risk anlamına geliyor. Kötü niyetli ve yetki verilmemiş güncelleme paketleri ilgili ağı bir çok saldırıya açık hale getiriyor.

Ev aracı ile Hareketli cihaz arasında ilişki güncellemesi

Ev aracıyla hareketli cihaz arasındaki mesajların takası IPSec Protokolu ile olmaktadır. Bu aralıkta başka hiç bir güvenlik mekanizmasına gerek yoktur. Zorunlu IPSec doğrulama başlığı kullanımı bunun yanında ESP ve şifre yönetimi mekanizması, ilişkilendirme güncellemesinin bütünlüğünü garanti altına alır.

.6.SONUÇ

Bilindiği üzere paketlerin ağlararası teslimi İnternet Protokolu ile sağlanmaktadır. Bunun ilk uyarlamasının bazı yetersizlikleri ki özellikle adres aralığı konusunda,sıkıntılar yaşandığından kimi geliştirmelere gidilip yenisi olan IPv6 tasarlanmıştır. Bu konudaki çalışmalar ise sürmektedir. Bunun yanında, IP yönlendirme mekanizması da IP ilk tasarlandığında yalnızca sabit cihazların birbirleriyle iletişim kurmasına olanak tanımıştır. Zaman içerisinde hareketlilik özelliğine sahip kimi cihazlar ortaya çıkmış ve bunlara duyulan ihtiyaç da hızla artış göstermiştir. Ancak sabit cihazlarla yapılan İnternet bağlantılarının her an her yerde gerçekleştirilebilmesi nedeniyle buna has bir protokola gerek hissedilmiş ve Hareketli IP ile tanışılmıştır. Hareketli IP'nin eksik olduğu yönleri iyileştirilmiş ve onun da yeni nesil türü çıkmıştır. Böylelikle, hareket ederken bile kesintisiz İnternet bağlantısı daha performanslı daha sorunsuz bir biçimde yapılmaktadır.

Bu çalışmada İnternet protokollarına, hareketlilik protokollarına değinilmiş, baş gösteren sorunlar eksikler ele alınarak çözüm önerileri sunulmuştur.

Kaynaklar

[1] J.B.Postel, editor. İnternet Protocol. İnternet Request
For Comments RFC 791, September 1981

[2] J.B.Postel, editor. İnternet Protocol. İnternet Request
For Comments RFC 791, September 1981

[3] Charles Perkins, IP Encapsulation within IP, RFC 2003, IBM, September 1996.

[4] J.B.Postel, editor. İnternet Protocol. İnternet Request
For Comments RFC 791, September 1981

[5] Stephen E.Deering ve Robert M.Hinden, İnternet Protocol version 6(IPv6 specification). İnternet Request For Comments RFC 1883, December 1995.

[6] D.Borman ve Robert M.Hinden, İnternet Protocol version 6(IPv6 specification). İnternet Request For Comments RFC 2460, December 1998.

[7] Philippe Biondi & Arnaud Ebelard, IPv6 Routing Header Security. EADS Innovation Works, 2007

[8] Thomas Narten, Routing and Addressing: Differences Between IPv4&IPv6. ARIN XVI, October 2005

[9] Seiji Ariga, IPv6 Operation and Transition. NTT Communications, 1997

[10] S.Bradner & V.Paxson, IANA Allocation Guidelines For Values In the İnternet Protocol and Related Headers. IANA Assignments, March 2000

[11] Y.Rekhter, B.Moskowitz, D.Karrenberg, Address Allocation for Private İnternets. BCP 5, RFC 1918, February 1996.

[12] R.Hinden & S.Deering, İnternet Protocol Version 6 (IPv6) Addressing Architecture. İnternet Request For Comments RFC 3513, April 2003

[13] R.Hinden & S.Deering, İnternet Protocol Version 6 (IPv6) Addressing Architecture. İnternet Request For Comments RFC 2373, July 1998

[14] R.Hinden & S.Deering, İnternet Protocol Version 6 (IPv6) Addressing Architecture. İnternet Request For Comments RFC 2373, July 1998

[15] R.Hinden & S.Deering, İnternet Protocol Version 6 (IPv6) Addressing Architecture. İnternet Request For Comments RFC 2373, July 1998

[16] R. Hinden, Nokia, IP Version 6 Addressing Architecture. RFC 4291, February 2006.

[17] R. Hinden, Nokia, IP Version 6 Addressing Architecture. RFC 4291, February 2006.

[18] R. Hinden, Nokia, IP Version 6 Addressing Architecture. RFC 4291, February 2006.

[19] S.Thomson & T.Narten, IPv6 Stateless Address Autoconfiguration. RFC 2462, December 1998.

[20] Charles Perkins, editor. IP mobility support. Intemet-Draft, draft-ietf-mobileip-protocol-17.txt, May 1996. Work in progress.

[21] J.Solomon, Motorola, Applicability Statements for IP Mobility Support. RFC 2005, October 1996

[22] J.Solomon, Motorola, Applicability Statements for IP Mobility Support. RFC 2005, October 1996

[23] Charles Perkins, editor. IP Mobility Support for IPv4. RFC 3220, January 2002

[24] G. Montenegro, editor. Reverse Tunneling for Mobile IP RFC 2344, May 1998

[25] G. Montenegro, editor. Reverse Tunneling for Mobile IP revised RFC 3024, January 2001

[26] Fumio Teraoka, Mobility Support in IPv6. İnternet Draft draft-teraoka-ipv6-mobility-sup-03.txt, April 1996. Work in progress.

Diğer kaynaklar

1- http://www.tcpipguide.com/free/t_IPOverviewandKey OperationalCharacteristics.htm

2- http://www.tcpipguide.com/free/t_IPOverviewandKey OperationalCharacteristics.htm

3- http://www.tcpipguide.com/free/t_DataEncapsulationProtocol DataUnitsPDUsandServiceDa.htm

4- http://www.tcpipguide.com/free/t_IPFunctions.htm

5- http://www.tcpipguide.com/free/t_IPv6DatagramMainHeaderFor mat.htm

6- http://www.tcpipguide.com/free/t_IPv6DatagramExtension Headers.htm

7-http://www.tcpipguide.com/free/t_IPv6DatagramExtension Headers-4.htm

8- http://www.cyber-warrior.org

9- http://www.cyber-warrior.org

10- http://www.tcpipguide.com/free/t_MessageAddressing andTransmissionMethodsUnicastBroa.htm

11- http://technet.microsoft.com/en-us/library/bb457118.aspx

12- http://en.wikipedia.org/wiki/ IPv6

13- http://msdn2.microsoft.com/en-us/library/ms885359.aspx

14- http://msdn2.microsoft.com/en-us/library/ms885359.aspx

15- http://msdn2.microsoft.com/en-us/library/ms885359.aspx

16- http://msdn2.microsoft.com/en-us/library/ms883129.aspx

17- http://msdn2.microsoft.com/en-us/library/aa450092.aspx

18- http://msdn2.microsoft.com/en-us/library/aa916865.aspx

19- http://msdn2.microsoft.com/en-us/library/aa450078.aspx

20- http://www.acm.org/crossroads/xrds7-2/mobileip.html

21- http://www.tcpipguide.com/free/t_MobileIPOverviewHistoryandMotivation.htm

22- http://www.tcpipguide.com/free/t_MobileIPConceptsandGeneralOperation.htm

23- http://www.tcpipguide.com/free/t_MobileIPConceptsandGeneralOperation.htm

24- http://www.acm.org/crossroads/xrds7-2/mobileip.html

25- http://www.acm.org/crossroads/xrds7-2/mobileip.html

ÖZGEÇMİŞ

Adı Soyadı : Süleyman Özgün Sunal

Doğum Yeri ve Tarihi : Safranbolu / 15-05-1984

Adresi(Okul) : Haliç Üniversitesi Fen Bilimleri Fakültesi , Bilgisayar Müh. Bölümü , BÜYÜKDERE CAD NO:101, 34394 MECİDİYEKÖY - İSTANBUL

Tel : (0212) 275 20 20 - (0212) 44 HALİÇ - (0212) (444 25 42)
Fax : (0212) 274 81

Cep : (0533) 253 53 95

E-posta : ozgunsunal@hotmail.com

Eğitim

Lisans : (2002-2006) Haliç Üniversitesi Bilgisayar Müh. Bölümü

Lise : (1998-2002) Şehremini Süper Lisesi(Y.D.A.)