Mobile IP

Internet, bilgiye erişim için küresel bir yöntemi sunmasına rağmen çoğunlukla bu erişim sabit bir telefon hattı veya kurumsal bir bağlantı üzerinden sabit bir bilgisayar kullanılarak sağlanmaktadır. Günümüzde kablosuz olarak Internet'e erişimi sağlayacak teknolojiler hızlı bir şekilde gelişmekte ancak aynı hızlı yaygınlaşmamaktadırlar.

Kablosuz ağ teknolojileri, WAP, GPRS, UMTS, 802.11b-a gibi, daha şimdiden pek çok seçenek sunmasına rağmen, maliyet problemleri bir yana, yaygınlaşabilmeleri için çözülmesi gereken birçok soruna sahiptirler. Güvenlik, doğrulama, dolaşım *(Roaming)* gibi konular bu sorunların başında yer almaktadır.

IP protokolüne dayanan Internet, iletim s›ras nda sabit IP adreslerine sahip uçlar arasında veri alışverişine olanak tanır. Kablosuz ağ teknolojileri kullanılarak gerçekleştirilen bir Internet bağlantısında, bağlanılan ağdan çıkılıp yeni bir etki alanına girildiğinde, mobil ucun IP adresinin değişmesi söz konusu olacaktır. Bu durum ister istemez veri iletiminin kesilmesine sebep olacaktır. Dolaşım sırasında yaşanacak söz konusu problemin çözümü için bir IETF çalışma grubu tarafından Mobile IP *(RFC 2002)* önerilmiştir. Önerilen, mobil bir ucun, biri sabit *(Home Address)*, diğeri ise dolaşım sırasında, dahil olunan ağa göre değişen yardımcı bir IP adresinin *(Care-of Address)* kullan›lmas›na dayan r.

IP protokolü bir kaynaktan gelen veri paketlerini alıcısına, yöneltilmiş olduğu alıcı adresine bakarak yönlendirir. Yönlendirme işlemi, yönlendirici *(Router)* ad verilen cihazlarda, veri paketinin yönlendirilmiş olduğu alıcı adresinden türetilen ağ adresine göre yap›l r. Tipik olarak bir yönlendiricide veri paketlerinin hangi fiziksel arayüz üzerinden gönderileceğinin tanımlandığı yönlendirme tabloları tutulur. IP paketlerinin kaynaktan alıcısına ulaştırılmasından sorumlu TCP ayrıca veri oturumlarının kurulması ve çözülmesi işlevini üstlenmiştir. Her bir TCP bağlantısı karşılıklı uçlarda bağlantı için ayrılmış port numaraları ve karşılıklı IP adreslerini içeren dört bölümlü bir etiketle birbirinden ayr›l r.

Aşağıda DOS komut satırında çalıştırılan `netstat` komutu ile listelenen TCP oturumları gösterilmektedir. Her bir bağlantı diğerinden, oturumun gerçekleştirildiği IP adresleri ve karşılıklı olarak bağlantıların sağlandıkları port numaralar› ile ayr lmaktadırlar. Bu bilgilerden herhangi birinin, etkin bir oturum sırasında değiştirilmesi bağlantının kesilmesine sebep olacaktır. Mobil bir ucun ağlar arasında dolaşımı sıras›nda bu maalesef kaç›n lmaz ve çözülmesi gereken bir sorundur.

```
C:\>netstat -n -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:3011         127.0.0.1:4146         ESTABLISHED
  TCP    127.0.0.1:4146         127.0.0.1:3011         ESTABLISHED
  TCP    192.168.10.148:4097    192.168.10.23:139      ESTABLISHED
  TCP    192.168.10.148:4125    192.168.10.1:1056      ESTABLISHED
  TCP    192.168.10.148:4129    192.168.10.1:1067      ESTABLISHED
  TCP    192.168.10.148:4147    213.194.65.26:25       ESTABLISHED
```

Mobil IP bu problemi, mobil uca iki adresinin atanması ile çözmeye çalışır. Mobil IP'de merkez adresi *(Home Address)* sabittir ve TCP bağlantılarının sürekli olması için kullanır. Yardımcı adres ise mobil ucun, merkez ağa göre konumunun belirlenmesi için kulla ›lır ve mobil uç dolaştıkça bağlantı kurduğu ağa göre değişir. Merkez adresi, mobil ucun, bu adresi üzerinde muhafaza eden merkezdeki bir arac uç aracılığı ile *(Home Agent)*, dolaşım halinde iken, diğer IP ağlarındaki uçlar ile sürekli bir veri iletiminde bulunabilmesini sağlar. Merkez ağda yerleşik olan bu aracı Mobil IP'nin en gerekli bileşenlerinden biridir; mobil uç merkez ağda olmadığı zaman, harici bir ağa bağlandığında *(Foreign Network)*, paketler merkez ağdaki aracı uç aracılığı ile Mobil uca ulaştır›l r.

Mobil uç dolaşımda bulunduğu sürece aldığı yeni yardımcı adresini merkez aracı üzerine kay›t eder. Merkez arac Mobil uca gelen veri paketlerini bu adrese yönlendirir. Bu yönlendirme, asıl pakete merkez aracının yeni bir başlık eklemesi ile gerçekleştirilir. Yeni başlıkta alıcı adresi olarak yardımcı adresi belirlenir. İşlemin tersi mobil uç tarafından paket alındığında tekrarlanır; pakette alıcı adresi, mobil ucun merkez adresi ile değiştirilir. Bu işlem tünelleme olarak adlandırılır. Mobil IP'de işletim üç ayrı başlık altında toplanabilir:

- Yardımcı adresin keşfedilmesi
- Yard›mc adresin kaydedilmesi
- Yardımcı adrese tünellemenin gerçekleştirilmesi

1. Yardımcın Adresin Keşfedilmesi

Mobil IP'de keşif işlemi RFC 1256'da tanımlanan Yönlendirici Duyuru Protokolü *(Router Advertisement)* üzerine inşa edilmiştir. Mobil IP söz konusu protokolde, yönlendirici duyurusu mesajlarının iletildiği paketlerin yapısında bir değişiklik yapmaz; ancak mobil işletim için gerekli sahaları ekler. Mobil IP'de bu duyurular, arac duyurular *(Agent Advertisement)* olarak adland›r›l›r. Merkez ve uzak arac lar belirli aral klarla *(Örneğin saniyede bir)* bu duyurular› yay nlarlar. Duyuru beklemek istemeyen bir Mobil uç, Broadcast veya Multicast ile, yard›mc IP adresi talebinde bulunabilir. Genel olarak aracı duyuruları aşağıdaki işlevleri sağlar:

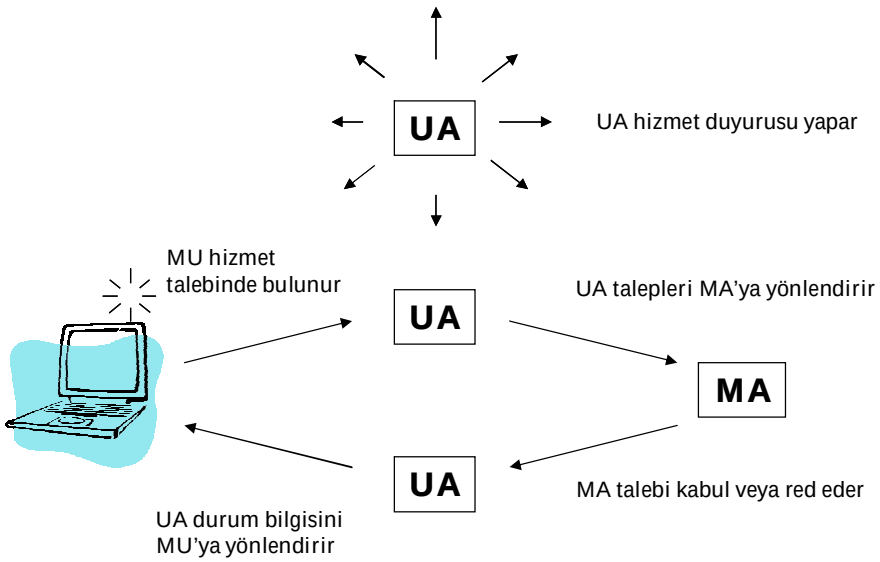
- Aracı uçların tespitine olanak sağlamak.
- Kullan›labilir yard›mc adresleri bildirmek.

- Uzak aracıları sağladığı özel işlevlerin mobil uca bildirilmesi; kullanılabilecek farkl kapsülleme yöntemleri gibi.
- Mobil ucun ağ adresi ve Internet bağlantısının durumunun belirlemesine olanak sağlamak.
- Mobil ucun arac›n›n bir uzak veya merkez arac *(veya her ikisi birden)* olup olmadığını belirlemesine ve dolayısıyla kendi merkez ağında mı yoksa uzak bir ağda mı olup olmadığını belirlemesine olanak sağlamak.

Mobil uçlar bağlı olduğu noktada etkin olan aracıların durumunda herhangi bir değişiklik olup olmadığını tespit etmek için RFC 1256'da tanımlanan yönlendirici taleplerini kullan rlar *(Arac Talebi - Agent Solicitation)*. Eğer bir uzak aracıdan gelen duyurular art›k mobil uç taraf ndan tespit edilemiyorsa, mobil uç kendini söz konusu aracının menzilinden çıkmış varsayacaktır. Bu durumda mobil uç, ya yeni bir aracı duyurusunu bekleyecek veya bir yard›m › adres için bir talepte bulunacakt r.

2. Yard›mc Adresin Kaydedilmesi

Bir mobil uç yard›mc› bir adres ald›ktan sonra, merkez arac›n›n bu adres hakk nda bilgilendirilmesi gerekir. Aşağıdaki şekilde mobil ucun yardımcı adresinin merkez arac›da nas l kaydedildiği gösterilmektedir. Yardımcı adresini alan mobil uç, seçime bağlı olarak uzak aracının yardımıyla, bir kayıt talebini merkez aracısına gönderir. Bu talebi alan merkez arac›s , kendi yönlendirme tablosunu günceller ve geriye bir onay mesaj gönderir.



Şekil 1. Mobil IP'de kayıt işlemleri. UA, Uzak Arac *(Foreign Agent)*, MA, Merkez Arac *(Home Agent)* ve MU, Mobil Uca karşılık gelmektedir.

Kayıt talebi, merkez aracısının veri paketlerini yardımcı adrese içinden ulaştıracağı tünelin oluşturulması için gereken parametreleri içerir. Tünellerin nasıl kurulduğu bir sonraki bölümde anlat›lmaktad›r. Merkez arac› talebi ald ktan sonra, mobil ucun merkez adresi ve bildirmiş olduğu yardımcı adresi arasında bir ilişki kurar ve bunu kay t geçerlilik süresince *(Registration Lifetime)* tutar. Merkez adresi, yard›mc adres ve kayıt geçerlilik süresinden oluşan üç sahalı bilgi mobil uç için bir ilişkilendirme *(Binding)* olarak adland›r›l›r. Mobil uç taraf ndan gönderilen bir kay t talebi, bir ilişkilendirme güncellemesi olarak düşünülebilir.

Kayıt işleminde doğrulama çok önemlidir. Zira Internet üzerindeki başka bir uç kendini söz konusu mobil uç gibi göstererek, sahte bir yard›mc› adres ile as l mobil ucun ulaşılamaz hale gelmesine sebep olabilir. Bu yüzden merkez arac›n›n kay t talebinin gerçekten mobil uçtan geldiğinden emin olması gerekir. Mimari gereği her mobil ucun kay t talepleri için128 bitlik anahtarlar ile MD5 *(RFC 1321)* değiştirilemez say›sal imzalar kullanabilmesi ve bir güvenlik grubunu *(Security Association, SA)* paylaşması gereklidir. Sayısal imza, MD5'in tek yönlü karıştırma algoritması ile, imzadan önce gelen kayıt mesajı başlığındaki ve uzantılarındaki veri üzerinden hesaplan r.

Kay›t talebinin güvenlik alt›na al›nabilmesi için, her talebin farkl veriyi içermesi ve böylelikle pratik olarak farklı iki talebin aynı MD5 şifresini kullanmaması gerekir. Aksi takdirde kötü niyetli bir uç, bu talepleri kaydedip daha sonra bunlar kullanarak, asıl uç yerine geçmeye çalışabilir *(Replay Attack)*. Bunu engellemek için Mobil IP'de, her kayıt mesajında, her kayıt talebinde değeri değiştirilen bir kimlik sahası bulunmaktadır. Bu sahanın değerinin benzersiz olması için temel olarak iki teknik kullanılır. İlki bir zaman damgasını *(Time Stamp)* kullan›lmas›d r. Böylelikle sonraki kayıt taleplerinde zamana bağlı olarak farklı kimlik değerleri kullanılacaktır. Diğer teknik ise rasgeleliliği yeterince sağlayacak bit sayısı ile kimlik değerine rasgele değerler atanmasıdır. Rasgele değerlerin kullanılması, mobil uç ve merkez arac arasında eşzamanlamanın bozulması durumda *(NTP problemleri yaşandığında örneğin)*, kötü niyetli bir ucun gelecekteki bir zaman damgas›n kullanarak araya girmesini önleyecektir.

Kimlik sahas› ayr›ca uzak arac›lar taraf ndan bekleyen, kay t taleplerine gelen kay t cevaplarını eşlemesi için kullanılır. Uzak aracı ayrıca bekleyen kayıt talepleri için başka bilgileri de depolar; mobil ucun merkez adresi, mobil ucun MAC adresi, mobil uçtan gelen kay›t talebinin kaynak port numaras›, mobil uç taraf ndan önerilen kay›t geçerlilik süresi ve merkez arac›n›n adresi gibi. Uzak arac›, kendi arac duyurularına yerleştirebileceği bir değerde kayıt geçerlilik süresini ayarlanabilir bir şekilde s›n›rland›rabilir. Merkez arac›da kendi kay t talebi cevab n n bir parça olarak kay›t geçerlilik süresini azaltabilir ancak art ramaz.

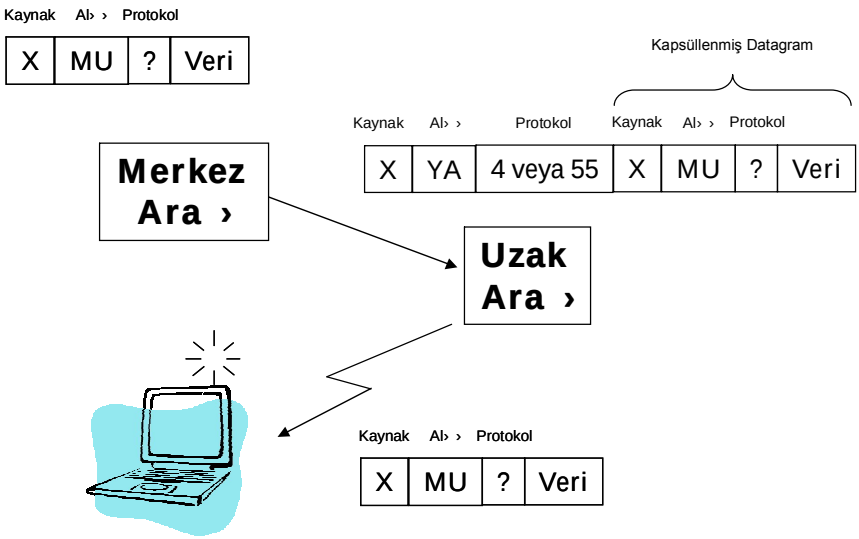
Yukarıdaki şekilde gösterildiği gibi uzak aracılar çoğu kez pasif davranırlar; merkez aracı ve mobil uç arasında, kayıt talepleri ve cevaplarının geçişini sağlarlar ve genellikle ne talimat verilirse onu yerine getirirler. Uzak arac› ayr›ca merkez arac dan gelen trafiğin başlığını ayrıştırıp asıl trafiği mobil uca iletir. Burada dikkat edilmesi gereken, uzak aracının mobil uca veya merkez aracıya kendisini doğrulatmamasıdır.

Bu durumda sahte bir uzak arac›, as›l uzak arac›n›n yerine geçerek, merkez arac dan, mobil uca doğru olan paketleri üzerine alarak trafiği bölebilir. Ancak sonuç, geçerli geçidin, doğrulama olmadan yönlendirici duyuru protokolünün kullanımı sırasında bu mümkündür; yerine bir sahtesinin yer almasında yaşanacak durumdan daha kötü olmayacakt r.

Mobil uç merkez aracısı ile temasa geçemediğinde, mobil ucun başka bir merkez aracısına kendini kayıt edebilmesini sağlayan bir mekanizma devreye girer. Bu otomatik merkez aracı keşfi yöntemi, kay t talebi için hedef IP adresi olarak merkez arac›n›n IP adresi yerine bir yay n *(Broadcast)* IP adresi kullanılarak çalışır. Bu mesaj merkez ağdaki aracılara ulaştığında kendi adreslerini içeren bir red mesajı geri döndürülür. Bu IP adresleri yeni bir kay›t talebinde kullan›labilir. Bu yay n, Internet çapında bir yayın işlemi değildir; sadece merkez ağdaki IP uçlarına yönlendirilmiş bir yay›nd r *(Directed Broadcast)*.

3. Yardımcı Adrese Doğru Tünelleme

Aşağıdaki şekilde Mobil IP'deki tünelleme işlemleri gösterilmektedir. Tüm arac lar taraf ndan desteklenmesi gereken geçerli kapsülleme yöntemi IP-in-IP'dir. IP-in-IP ile merkez aracı, bu durumda tünel kaynağı *(Tunnel Source)*, mobil ucun merkez adresine yönlendirilmiş her datagrama yeni bir başlık ekler *(Tunnel Header, Tünel Başlığı)*. Tünel başlığı alıcı adresi olarak mobil ucun yardımcı adresini kullanır *(Tunnel Destination)*. Tünel kaynak adresi merkez arac›n›n IP adresidir ve tünel başlığında, üst seviye protokol numarası olarak bir sonraki protokol başlığının yine bir IP başlığı olduğunu belirtmek için 4 kullanılır. IP-in-IP'de, veri yükünün ilk parças olarak asıl IP başlığı muhafaza edilir; uzak aracı mobil uca paketi ulaştırmak için yalnızca tünel başlığını kaldırır.



Şekil 28.2. Mobil IP'de Tünelleme

Yukarıdaki şekilde ayrıca tünel başlığının bazen iç başlık için protokol numarasını 55 olarak kullandığı gösterilmektedir. Bu, merkez aracının IP-in-IP yerine asgari kapsülleme *(Minimal Encapsulation)* kullandığında gerçekleşir. Asgari kapsülleme başlığının işlenmesi, IP-in-IP yöntemi ile karşılaştırıldığında biraz daha karmaşıktır; zira tünel başlığındaki bilginin bir kısmı ile iç asgari kapsülleme başlığındaki bilgi, asıl IP başlığını oluşturmak için birleştirilir. Öte yandan başlık fazlalığı *(Overhead)* azaltılmış olur.

4. **Mobil IP ve IPv6**

IPv6 mobil işletim için birçok yeniliği beraberinde getirmektedir. Stateless Address Autoconfiguration ve Neighbor Discovery ile mobil uçlar Uzak Arac lara ihtiyaç duymaks›z›n yard›mc› adreslerini yap landabileceklerdir. IPv6-in-IPv6 da ta ›mlanmış durumdadır. Ayrıca IPv6'nın dahili güvenlik özellikleri Mobil IP protokolünün de basitleştirilmesine olanak tanımaktadır.

5. **Özet**

Aslen kablosuz ağlar için tasarlanan mobil IP, özellikle kamusal kablosuz ağların yavaş bir şekilde gelişmesinden ötürü yaygınlaşamamaktadır. Öte yandan L2TP ve PPTP, mobil IP için rakip protokoller olarak görünmektedirler. Ayr ca mimariden kaynaklanan ve çözümlenmeye çalışan problemlerde bulunmaktadır. Örneğin birçok yönlendirici, dışarı doğru giden bir paket, dahili ağdan bir kaynak IP adresine sahip değilse paketi göz ardı etmektedir. Benzeri problemlerin, önerilmiş çözümleri bulunmaktadır ancak mobil IP'nin yıldızı IPv6'nın kullanımının yaygınlaşmasıyla parlayacakt r.

6. **Sorular**

1. Mobil IP'nin temel bileşenleri nelerdir?
2. Mobil IP'de Uzak Aracının işlevini açıklayınız.
3. Mobil IP'de mesaj alıç verişinde güvenlik nasıl sağlanmaktadır?
4. Mobil IP'de ne türde kapsülleme kullan›lmaktad r?