

# KABLOSUZ AĞ TEKNOLOJİLERİ

## 2011



BİTLİS EREN ÜNİVERSİTESİ  
TATVAN MESLEK YÜKSEKOKULU  
BİLGİSAYAR PROGRAMCILIĞI-2  
GAMZE NAYİR

# ÖNSÖZ

## Kitap Hakkında;

Ağ ve internet teknolojilerinin temeli 1950 ve 1960'larda, nükleer saldırılardan etkilenmeyecek bir askeri komuta kontrol sisteminin tasarlanmasına dayanıyor. O zamana kadar telefon hatları üzerinden yürütülen komuta kontrol işlemleri, telefon hatlarının kilit noktalarına verilecek zararlarla devre dışı bırakılabilirdi, yeni sistem ise ağır hasar olsa bile hasarsız noktalar arasında iletişimi sağlayabilmeliydi. Bunun çözümü olarak iletişim hatlarını merkezi noktalardan çıkartmak yerine; birbiriyle iletişim kuracak uç noktalar, pek çok ara bağlantı ile çok sayıda başka noktaya bağlanacaktı.

Askeri komuta kontrolü sağlamak amacıyla başlayan sistem, dünyanın her köşesiyle iletişim kurmamızı sağlayan ve hayatın her alanını etkileyen bir kavrama dönüşen kablosuz ağ teknolojisini anlatmaya çalıştım.

**Gamze NAYİR**

**Bitlis Eren Üniversitesi**

**Tatvan Meslek Yüksekokulu**

**2011**

# İÇİNDEKİLER

## Sayfa No

|                                                               |    |
|---------------------------------------------------------------|----|
| ÖNSÖZ.....                                                    | i  |
| İÇİNDEKİLER.....                                              | ii |
| 1.KABLOSUZ AĞ TEKNOLOJİSİNİN TARİHÇESİ.....                   | 1  |
| 1.1.Kablosuz Ağ Teknolojisi Nedir?.....                       | 1  |
| 1.2. Kablosuz Ağ Teknolojisi Nasıl Çalışır? .....             | 1  |
| 1.3.Kablosuz Ağa Geçmenin Yararları.....                      | 2  |
| 1.4.Kablosuz Ağın Avantaj ve Dezavantajları.....              | 3  |
| 1.5.Kablosuz Ağ Teknolojisine Neden İhtiyaç Duyarız?.....     | 4  |
| 2.KABLOSUZ AĞ TERİMLERİ.....                                  | 4  |
| 3.KABLOSUZ AĞ STANDARTLARI.....                               | 5  |
| 3.1.Kablosuz Ağ Standartlarının Karşılaştırılması.....        | 7  |
| 4.KABLOSUZ AĞ YAPILARI.....                                   | 8  |
| 5.KABLOSUZ AĞ TEKNOLOJİSİNİN RAHATLIĞI .....                  | 9  |
| 5.1.Kablosuz Ağ İle Neler Yaparsınız?.....                    | 9  |
| 5.2.Kablosuz İletişim Teknolojilerinin Kullanım Alanları..... | 10 |
| 6.KABLOSUZ AĞ YÖNTEMLERİ.....                                 | 10 |
| 7.KABLOSUZ ADRESLEMESİ.....                                   | 12 |
| 8.KABLOSUZ AĞLARDA GÜVENLİK.....                              | 16 |
| 9.KABLOSUZ AĞLARDA KEŞİF.....                                 | 18 |
| 10.KABLOSUZ AĞ KARTINI NEREDEN SATIN ALABİLİRİM?.....         | 21 |

# 1.KABLOSUZ AĞ TEKNOLOJİSİNİN TARİHÇESİ

Bugünkü ağ ve internet teknolojilerinin temeli 1950 ve 1960'larda, nükleer saldırılardan etkilenmeyecek bir askeri komuta kontrol sisteminin tasarlanmasına dayanıyor. O zamana kadar telefon hatları üzerinden yürütülen komuta kontrol işlemleri, telefon hatlarının kilit noktalarına verilecek zararlarla devre dışı bırakılabilirdi, yeni sistem ise ağır hasar olsa bile hasarsız noktalar arasında iletişimi sağlayabilmeliydi. Bunun çözümü olarak iletişim hatlarını merkezi noktalardan çıkartmak yerine; birbiriyle iletişim kuracak uç noktalar, pek çok ara bağlantı ile çok sayıda başka noktaya bağlanacaktı. Ara bağlantı noktalarından bir tanesi bile çalışsa, buradan yola çıkılarak halen çalışan diğer yerlerle iletişim kurulabilecekti. Bu sistemin ilk uygulması Amerika'da, 1969 yılında ARPANET adıyla çalışmaya başladı, ve ilk bağlantı dört üniversite arasında yapıldı ve bağlanan kuruluş sayısı kısa süre içinde arttı. Bu genişleyen ağ 1980'li yıllarda dünya üzerindeki pek çok ülkeyi, akademik kurumları ve ticari şirketleri kapsayan Internet haline geldi. Askeri komuta kontrolü sağlamak amacıyla başlayan sistem, dünyanın her köşesiyle iletişim kurmamızı sağlayan ve hayatın her alanını etkileyen bir kavrama dönüştü.

## 1.1.Kablosuz Ağ Teknolojisi Nedir?

İşiniz kalıcı olarak ofisten konferans salonuna, depo katına, arabaya, eve, havaalanına, otele ve kafeteryaya taşındı. Bu özgürlükten faydalanmak için küçük işletmeler, çalışanları, müşterileri ve iş ortaklarıyla iletişimlerini kesmemek için kablosuz ağları ve WiFi kapsama alanlarını kullanmaktadır. Kablosuz yerel ağ (LAN), bilgisayarlarınızı teller veya kablolar olmadan bağlamanıza olanak tanır.Kablosuz ağ, belirli bir alan içindeki mobil cihazların bağlanmasını ve iletişim kurmasını sağlamak için radyo dalgalarını kullanarak bunu kolaylaştırır.

## 1.2.Nasıl Çalışır?

Kablosuz ağ bağlantı noktaları aslında bildiğimiz router modemlerle aynı şekilde çalışırlar ve küçük radyo dalgaları üreten sistemlerdir. WiFi standartları çeşit ve özelliklerine göre 802.11a, b,g ve n olarak ayrılmışlardır. Bunlardan en yaygın olarak kullanılanı 802.11b'dir ve 2.4Ghz'lik yayılma aralığına sahiptir. Ancak 802.11b ile en fazla 11 Megabit'lik bağlantı kurabilmek mümkündür. Oysa 802.11g ile saniyede 54 Mbit, 802.11n ile 140 Mbit'lik hızlara ulaşmak mümkündür.

Günümüzde dizüstü bilgisayarların tamamına yakını üzerlerinde entegre Wi-Fi alıcıları bulundurulur.Bulunmayanlar ise PCMCIA kartlarla bu özelliği kolayca kazanabilirler.Kablosuz ağ sistemleri radyo frekansları ile çalışmaktadırlar. Radyo dalgaları ile haberleşme üç çeşit olabilmektedir. Bunlar alıcı(receiver), verici(transmitter) ve alıcı-verici(trans-receiver) olarak adlandırılırlar. Bunlardan kısaca bahsetmek gerekirse;

**Alıcılar:** Adından da anlaşılacağı üzere sadece radyo sinyallerini alabilen fakat gönderme özelliği barındırmayan aygıtlardır. Bunlara en basit örnek olarak FM radyoları ve televizyonları gösterebiliriz.

**Vericiler:**Sadece radyo sinyalleri gönderebilen ama alma yetkileri olmayanelektronik devrelerdir. Bunlara örnek olarak radyo verici istasyonları,televizyon vericiistasyonlar vb.sayılabılır

**Alıcı-Vericiler:**Hem alma hem verme özellikleri olan aygıtlardır. Bunlara örnek olarak telsiz röleleri, cep telefonu baz istasyonları, cep telefonları vb. sayılabilir.İletişim anlamında bilinmesi gereken bir diğer konu ise iletim yönüdür. İletim yönleri üçe ayrılır:

**1. Tek Yönlü İletim(Simplex):** Kurulan iletim sistemin de iletimin sadece bir yöne yapılabildiği zaman aldığı addır. Örnek olarak FM radyolar gösterilebilir.

**2. Çift Yönlü Eş Zamansız İletişim(Yarı-Dupleks, Half-Duplex):** Kurulan iletim sisteminde çift yönlü iletim yapılabildiği ancak eş zamanlı olarak sadece bir tarafın gönderim yapabildiği sistemlerdir. Örnek olarak Telsiz uygulamaları gösterilebilir. Bilgi sistemlerinde kullanılan radyo frekansı ile çalışan kablosuz iletişim sistemleri genelde bu tiptedir. Örneğin IEEE 802.11g standardı 54 Mbps’de Yarı-Dupleks iletim imkanı sunar.

**3. Çift Yönlü Eş Zamanlı İletişim (Tam-Dupleks,Full-Duplex):** Hem alıcı hem vericinin eşzamanlı iletim yapabildiği zaman aldığı isimdir. Örnek olarak cep telefonları, telsiztelefonlar gösterilebilir.Şehrin üzerinde bağlantı noktaları arasında kusursuz bir ağ oluşturulur.Busayedetrende,arabada, parkta, cafelerde, restaurantlarda vb. birçok yerde özgürce internete bağlanabilmek mümkündür. Şehirlerde belirli aralıklarla yerleştirilmiş bağlantı noktaları ile kesintisiz sürekli bir bağlantı sağlanır. Bunun için genellikle saniyede 11 Mbit(1.35MB/s) hıza olanak sağlayan ve 2.4 Ghz’lik yayılma aralığına sahip 802.11b sistemi kullanılır.

Bu sistem hem fazla güç tüketmediklerinden hem 2.4 Ghz gibi birçok yerde kullanılan(modemler, oyun kumandaları vs.) standart bir yayılma aralığına sahip olduklarından ve insanlara zarar vermediği ifade edilen radyo frekansı ile haberleştiğinden şehir kullanımında tercih edilmektedir.Günümüzde adından bahsedilen yeni kablosuz ağ teknolojisi ise WiMAX’tir. Çalışma prensibi standart kablosuz ağ sistemleriyle aynıdır fakat çok güçlü mikrodalga iletimiyle sinyalleri daha uzak mesafelere taşıyabilmek mümkündür. Bu sayede birim metrekarelik alan için gereken kablosuz ağ noktası maliyeti düşmekle beraber sinyal kalitesi de arttırılmış olmaktadır.

### 1.3.Kablosuz Ağa Geçmenin Yararları

Kablosuz ağların kısa ve uzun vadeli yararları şunlardır:

- **Kolaylık:** Günümüzde tüm dizüstü bilgisayarlarda ve birçok cep telefonunda, bir kablosuz LAN'ye doğrudan bağlanmak için gereken WiFi teknolojisi bulunmaktadır. Çalışanlar, kapsama alanınızdaki herhangi bir yerden ağ kaynaklarınıza güvenli bir şekilde erişebilir. Kapsama alanı genellikle sizin tesisinizdir, ancak birden fazla binayı içerecek şekilde genişletilebilir.

- **Mobilite:** Çalışanlar, masalarında olmadıklarında dahi ağınıza bağlı kalabilir. Toplantıdakiler belgelere ve uygulamalara erişebilir. Satış bölümündekiler, herhangi bir yerden ağdaki önemli bilgileri kontrol edebilir.
- **Verimlilik:** Bilgilere ve şirketinizin önemli uygulamalarına erişim, çalışanlarınızın işlerini yapmalarına yardımcı olur ve işbirliğini özendirir. Ziyaretçiler için (örneğin müşteriler, yükleniciler veya satıcılar), Internet ve iş verilerine güvenli konuk erişimi sağlanabilir.
- **Kurulum kolaylığı:** Bir yerden fiziksel olarak kablolar geçirmeniz gerekmediğinde, kurulum hem hızlı hem de düşük maliyetli olur. Kablosuz LAN'ler de ağ bağlantısını, depo veya üretim katı gibi ulaşılması zor yerlere kolayca ulaştırır.
- **Ölçeklenebilirlik:** İşle ilgili işlemlerinizi büyüdükçe, ağınıza hızla genişletmeniz gerekebilir. Kablosuz ağlar, genellikle mevcut ekipmanla genişleyebilir; bununla birlikte, kablolu bir ağ için ek kablolar gerekebilir.
- **Güvenlik:** Kablosuz ağınızın başarılı olmasında erişimin denetlenmesi ve yönetilmesi önem taşır. WiFi teknolojisindeki gelişmeler, verilerinize yalnızca izin verdiğiniz kişilerin kolayca erişmesini sağlayacak, güçlü güvenlik korumaları sağlamaktadır.
- **Maliyet:** Ofis taşınmaları, yeniden yapılandırmalar veya genişletmeler sırasında kablolu maliyetlerini ortadan kaldırdığı veya azalttığı için bir kablosuz LAN'nin işletim maliyeti daha düşüktür.

#### 1.4.Kablosuz Ağın Avantaj Ve Dezavantajları

##### Avantajları:

- 1-)Bilgi transfer hızı küçük ölçekli yerel ağlar için yeterlidir.(802.11b için 11 mbit/ saniye).
- 2-)Hata giderici algoritmalar sayesinde güvenilir haberleşme sağlar.
- 3-)Şifreleme tekniği kullanarak haberleşmeleriniz gizliliğini sağlayabilirsiniz.
- 4-)Açık alanda 300 metreye kapalı alanda ise 120 metreye kadar bilgi gönderebilirsiniz.
- 5-)Kablosuz ağ erişim noktalarını mevcut ağınıza eklemek çok kolaydır.

##### Dezavantajları:

- 1-)Kablosuz ağ donanımları geleneksel ağ donanımlarından daha pahalıdır.
- 2-)Kurulum işlemi geleneksel ağlardan daha zordur.
- 3-)Oda duvarları sinyal kalitesinin büyük miktarda düşmesine yol açar.
- 4-)Kablosuz ağ kartı taşıyan bilgisayarların yeri değiştirildiğinde veri aktarımı hızında olumsuzluklar yaşanabilir.

## 1.5.Kablosuz Ağ Teknolojisine Neden İhtiyaç Duyarız?

Her ne kadar bu teknoloji taşınabilir bilgisayarlarla yaygınlaşmış olsa da illa onlar için ve onlarla beraber kullanılmasına gerek yok. Ev içindeki kablo karmaşasına son vermek veya en başından hiç ağ için kablo döşeme işine bulaşmamak için kablosuz ağ kullanabilirsiniz. Kablosuz ağ ile iki bilgisayarı birbirine bağlayabileceğiniz gibi bir erişim noktası kullanarak genişlemeye müsait tam anlamıyla bir yerel ağ oluşturabilirsiniz. Bu şekilde bilgisayarlarınız belirli sınırlar dahilinde nerede olursa olsun yerel ağ ve İnternet'ten faydalanabilir. Bu iş için de kablo çekmeniz veya bilgisayarı özel olarak biryere yerleştirmeniz gerekmez. Diğer taraftan yerel ağdan yüksek başarımla üstün ve sabit iletim hızı bekliyorsanız, kablosuz ağ kötü bir tercih olacaktır. Merak etmeyin, ağ üzerinden bir kaç kişi Quake, Unreal, WarCraft veya Counter-Strike gibi oyunlar oynayabilirsiniz ve çok büyük engeller olmadığı ve sağlıklı bir iletim hızında olduğunuz sürece ağınızda gecikme süreleri konusunda bir sıkıntı olmaz.

## 2.KABLOSUZ AĞ TERİMLERİ

**Frame:** İki kablosuz ağ cihazı arasında gidip gelen veri.

**WEP :** Kablosuz ağlarda sık kullanılan şifreleme protokolü. Wired Equivalent Privacy...kablosuz ağlarda kullanılan şifreleme yöntemidir. Şu an itibariyle birçok açığı bulunmuş ve yerine wpa'ya bırakmıştır. Kimlik doğrulaması sırasında; AP'ye bir bağlantı isteği gönderir. AP bağlantı isteğini alıp 128 bitlik bir metni geri gönderir. kablosuz cihazımız bu 128 bitlik metni alıp kendi içindeki WEP şifresi ile şifreleyip geri gönderir. AP'de bu şifrelenmiş metnin doğruluğunu onaylar.

WEP hem 64 bit hemde 40 bit seviyesinde belirtilebilir. Bunun sebebi 24-bit "Initialization Vector" (başlatma vektörü) nün 40 bit üzerine eklenerek 64 bit'e çekilmesidir. Aynı şekilde 128 bit WEP de 104 bit secret key kullanır, bunun 24 bit'i başlatma vektörüdür.

**WPA :** WEP'de çıkan güvenlik açıklarının giderilmesi ve yeni özelliklerin eklenmesi ile çıkarılmış güvenlik protokolü. Wi-Fi Protected Access...WEP'in yetersizlikleri üzerine çıkarılan güvenlik protokolü. Tüm 802.11 cihazlarla uyum sağlamaktadır. WEP dene en büyük farkı ise statik keyler yerine dinamik keyler kullanmasıdır.

**Access Point:** Kablosuz ağ cihazlarının bağlanarak bir ağ oluşturduğu merkezi cihaz. Bu cihaz bir donanım olabileceği gibi özelleştirilmiş bir Linux dağıtımı da olabilir.

**SSID:** AccessPoint(ErişimNoktası)'nın tanımlayıcı adı.

**802.11x :** IEEE tarafından tanımlanmış ve kablosuz ağ cihazlarının nasıl çalışacağını belirttiği standartlardır.

•**802.11**\_2.4 GHz aralığında - Max bant genişliği 11Mbps - 30-75m arası

•**802.11a**\_5GHz aralığında yayın yapar - Max bant genişliği 54Mbps - 25-50m **civarında**

•**802.11g**\_2.4 GHz aralığında - 54 Mbps'e kadar çıkan hız kapasitesi

•**802.11i**\_Güvenli WLAN kullanımı - 802.11a ve 802.11b WLAN'lari arasındaki iletişimin şifrelenmesini belirler - AES TKIP(temporary key integrity protocol) kullanılır.

### 3.KABLOSUZ AĞ STANDARTLARI

Kablosuz ağ standartları 1997 yılından itibaren Elektrik-Elektronik Mühendisleri Enstitüsü, IEEE (Institute of Electrical and Electronics Engineers), tarafından geliştirilmeye başlanmıştır. Geliştirilen bu standardın genel adı IEEE 802.11'dir. 802.11 standardı kablosuz yerel ağ, WLAN (Wireless Local Area Network ), üzerinden iletişim kurarken kullanılan kuralları temsil eder. IEEE 2,4 GHz frekansında çalışan, maksimum 75 metreyi kapsayan, 1-2 Mbps aralığında veri iletimi hızı sunan bu standardın teknolojik gelişmeler sonucunda yetersiz hale gelmesiyle, 802.11x adı verilen standartlar serisini geliştirmeye başlamıştır. Arada farklar olmasına rağmen temel olarak 802.11 ailesi aynı iletişim kurallarını kullanır. 802.11a, 802.11b, 802.11g ve yeni geliştirilen 802.11n bu standartlardan en çok kullanılanlardır.

#### 802.11a

802.11 standardının yetersiz hale gelmesiyle, 1999 yılında ortaya çıkan ilk geliştirilmiş sürümdür. Bu standart temelde 802.11 ile benzer olmasına karşın 5 GHz frekansında çalışmaktadır. 54 Mbps veri iletim hızı sunan bu standart, açık alanlarda maksimum 100 metreyi kapsayacak şekilde çalışabilmektedir. 802.11a'yı diğer kablosuz ağ standartlarından ayıran temel avantajı daha fazla kapasiteye (throughput) destek vermesi ve daha fazla kanal kapasitesi olmasıdır, böylelikle daha fazla bant genişliği kullanımına olanak sağlamaktadır. Diğer standartların aksine 802.11a'nın 5 GHz frekansında çalışması bu standardda çeşitli avantajlar ve dezavantajlar sağlamıştır. Bu frekansta yayın yapmanın olumlu yanı, bluetooth, mikrodalga fırın ve kablosuz telefon gibi diğer elektronik cihazlarının farklı frekans aralığını kullanmasından dolayı kanal kapasitesi artar ve veri iletim hızı daha yüksek olur. Son olarak, bu teknoloji yüksek veri iletim hızına ihtiyaç duyan kullanıcılar ve video dağılım sistemlerinde aktif olarak kullanılmaktadır. Daha pahalı cihazlarda bulunmasına rağmen iş hayatında kurumsal kullanıcılar tarafından tercih edilmektedir.

#### 802.11b

802.11b standardı 802.11a ile beraber 1999 yılında piyasaya sürülmüştür. Ancak 802.11a'ya göre çok daha kısa bir sürede yaygınlaşarak bütün dünyada kullanılmaya başlanmıştır. 802.11b, 802.11 gibi 2.4 GHz frekans bandında çalışmakta ve 11 Mbps veri iletimi hızına çıkabilmektedir. İlk çıktığında 802.11b erişebildiği veri iletim hızının etkisiyle ethernet teknolojisine rakip hale gelmiş ve kablosuz ağ kullanımının yaygınlaşmasında büyük rol oynamıştır. 802.11b'nin sağladığı en önemli avantaj kapsama alanı mesafesinin fazla olmasıdır. 2.4 Ghz frekansında yayın yapmasından dolayı kapalı alanlarda yaklaşık olarak 38 metre, açık alanlarda ise 150 metreyi aşacak şekilde alanı kapsayabilmektedir. Ayrıca maliyet açısından da diğer standartlara göre oldukça uygundur. Bununla birlikte bluetooth, mikrodalga fırın ve kablosuz telefon gibi farklı elektronik cihazlar ile aynı frekansta çalışmasından dolayı işaretler birbiriyle karışmaktadır. Bunun sonucunda veri iletim hızı ve bant genişliği 802.11a'ya göre daha düşüktür.

Sonuç olarak, 802.11b genellikle ofis ortamları, hastaneler, depolar ve fabrikalar gibi ortamlarda kullanılmaya oldukça uygundur. Özellikle konferans salonları, çalışma alanları ve kablo çekmenin tehlikeli olduğu noktalarda ağ bağlantısı sağlanması için uygun bir teknolojidir. Kısaca 802.11b, taşınabilirliğin gerekli olduğu ve orta hızlı ağ bağlantılarına ihtiyaç duyulan alanlarda kullanılır.

## **802.11g**

2003 yılında IEEE tarafından kablosuz ağ standartlarında geliştirilen 3. nesil teknolojidir. 802.11b'de olduğu gibi 2.4 GHz frekansında çalışmaktadır. 802.11g standardı temel olarak 802.11b standardının bir uzantısıdır, fakat veri iletim hızı ve kullanılan bant genişliğinde önemli ölçüde gelişme sağlanmıştır. Bu açıdan bakılırsa 802.11g için 802.11a ve 802.11b'nin daha etkin olduğu özelliklerinin birleştirilmiş hali olduğu söylenebilir.

802.11g'nin sahip olduğu en önemli özellik 802.11b ile ulaşılan kapsama alanını koruyarak, (açık alanlarda 38 metre, kapalı alanlarda 150 metre) veri iletim hızını ortalama 22 Mbps'a ulaştırmasıdır. Bu hız 802.11a'da olduğu gibi maksimum 54 Mbps'a ulaşabilmektedir. Bu standardın zaman zaman 802.11b ile çalışan cihazlarla uyum sorunu yaşamasından dolayı kullanımı çok fazla yaygınlaşmamıştır. Bununla birlikte fiyatının 802.11b'den yüksek olması da tercih edilebilirliğini azaltmaktadır. Son olarak, yüksek hız gerektiren video ve çoklu ortam uygulamalarında hızı ve kapsadığı alanın genişliği nedeniyle 802.11g standardı oldukça uygundur.

## **802.11n**

Zaman içerisinde kullanıcı sayısının artması ve kullanıcıların farklı uygulamaları kullanmak istemesi daha fazla bant genişliği, daha fazla erişilebilirlik ve daha geniş kapsama alanı gibi talepleri artırmıştır. Bu amaçla IEEE 2003 yılından beri 802.11n standardını geliştirmek üzere çalışmaya başlamıştır. 802.11n, Çoklu Giriş / Çoklu Çıkış, MIMO (Multiple Input / Multiple Output), adı verilen bir protokol sayesinde 2,4 GHz ve 5 GHz frekanslarının her ikisini de aynı anda kullanabilmektedir. MIMO teknolojisi, iletilecek bir bilginin parçalara ayrılıp farklı antenler üzerinden karşı tarafa gönderilmesini sağlar. Diğer standartlarla çalışan cihazlar bir anten üzerinden bir yayın yaparken, 802.11n teknolojisine sahip ağ cihazları gönderi tarafında 2 veya daha fazla yayın yaparken, alım tarafında birden fazla anten kullanır.

Gönderilen veriler duvarlardan, kapılardan ve diğer eşyalardan yansıyarak ve farklı rotalar takip ederek alıcı antene farklı zamanlarda ve birden fazla kere varır. MIMO teknolojisi bu durumu kendi lehine kullanarak işaretin güçlenmesini ve daha uzaklara iletilmesini sağlar. 802.11n standardına göre veri iletim hızı ortalama 130 Mbps seviyelerinde olacaktır. Hatta teorik olarak bu hız 600 Mbps'ye kadar ulaşabilir ve kapsama alanı kapalı alanlarda 70 metre, açık alanlarda ise 250 metre kadar olabilir. Bu teknolojinin en önemli özelliklerinden birisi de eski standartlarla uyumlu bir şekilde çalışabilmesidir. Sonuç olarak, 802.11n henüz tam olarak tamamlanmamış bir standart olmasına rağmen vadettiği veri hızı, güvenilirlik ve olması beklenen yüksek fiyatı ile İnternet telefonu, müzik ve video yayını, IPTV gibi daha fazla bant genişliği isteyen uygulamalar için oldukça yeterli olacaktır.

### 3.1.Kablosuz Ağ Standartlarının Karşılaştırılması

| Kategori /Standart          | Max. Veri Oranı (Data Rate) | Frekans (Hz)   | Mesafe (Bina İçi) | Mesafe (Bina Dışı) |
|-----------------------------|-----------------------------|----------------|-------------------|--------------------|
| IEEE 802.11 (1997)          | 2 Mbps                      | 2.4GHz         | 20 m              | 100 m              |
| IEEE 802.11a (Wi-Fi)        | 54 Mbps                     | 5.2GHz         | 35 m              | 120 m              |
| IEEE 802.11b (Wi-Fi)        | 11 Mbps                     | 2.4GHz         | 38 m              | 140 m              |
| IEEE 802.11g (Wi-Fi)        | 54 Mbps                     | 2.4GHz         | 38 m              | 140 m              |
| IEEE 802.11n (Haziran 2009) | 248 Mbps                    | 2.4GHz, 5.2GHz | 70 m              | 250 m              |
| IEEE 802.11y (Haziran 2008) | 54 Mbps                     | 3.7GHz         | 50 m              | 5000 m             |
| IEEE 802.16 (WiMAX)         | 70 Mbps                     | 10-66 Ghz      | ?                 | 50 000 m           |
| IEEE 802.16a (WiMAX)        | 70 Mbps                     | 2-11 Ghz       | ?                 | ?                  |
| HiperLAN1                   | 20 Mbps                     | 5.2GHz         | ?                 | ?                  |
| HiperLAN2                   | 54 Mbps                     | 5.2GHz         | ?                 | ?                  |
| HomeRF                      | 10 Mbps                     | 2.4 Ghz        | 45 m              | -                  |
| Bluetooth                   | 1 Mbps                      | 2.4 Ghz        | 10 m              | -                  |

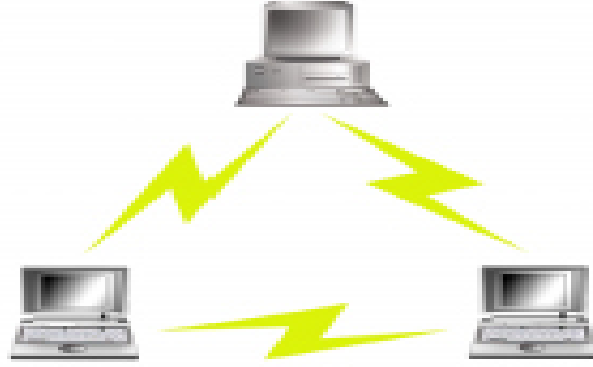
## 4.KABLOSUZ AĞ YAPILARI

İki tip kablosuz ağ yapısı vardır ;

### Ad-Hoc veya Peer to Peer

- Her biri kablosuz ağ kartına sahip bilgisayarlardan oluşur.
- Her bilgisayar direkt olarak istediği bir başka kablosuz donanıma sahip bilgisayarla haberleşerek bu yolla dosya ve yazıcı paylaşımını sağlarlar.

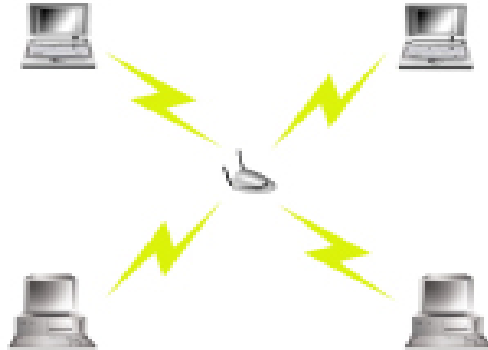
#### Ad-Hoc Yapısı



### Access Point Donanımlı Yapı

- Bu teknolojiye, bir kablosuz ağ merkez bir istasyon kullanarak haberleşebilir.
- Bu tip yapıda Access point, kablosuz bilgisayarların iletimini sağlayarak bir hub gibi hareket eder.
- Diğer adı Infrastructure dır.

#### AP Donanımlı Yapısı(Erişim Cihazı)



## Dikkat Edilecek Özellikleri:

- **Standartlar:** Cihazın desteklediği kablosuz LAN standartları.
- **Modülasyon:** Cihazın desteklediği modülasyon yöntemleri (OFDM).
- **Veri transfer değerleri:** Veri transferi yapabildiği hız değerleri.
- **Ağ bağlantısı tipi:** Desteklediği ağ bağlantı tipi (Infrastructure ve Ad-hoc).
- **Çalışma modları:** Çalışabildiği kablosuz bağlantı modları (Erişim Noktası, AP-to-AP Bridge, Point-to-MultiPoint Bridge, Wireless Client)
- **Frekans bandı:** Cihazın çalıştığı frekans aralığı (MHz olarak).
- **Verici çıkış gücü:** Cihazın verici gücü (db olarak).
- **Alıcı hassasiyeti:** Cihazın alıcı hassasiyeti (db olarak).
- **Dış anten tipi:** Cihazın takılabilen anten tipi.
- **Ağ desteği:** Cihazın kullanılabileceği ağlar ( server and Client)
- **Güvenlik:** Cihazın desteklediği güvenlik modları (64-bit, 128-bit 152-bit WEP şifreleme, WPA, 802.x vb.)
- **Çalışma menzili:** Cihazın iletişim kurabildiği menzili (Kapalı alanda,Açık alanda)

## 5.KABLOSUZ AĞ TEKNOLOJİSİNİN RAHATLIĞI NEDİR?

Kablosuz ortam size bağlanabilirliğinizden ödün vermeden kablosuz olarak çalışma özgürlüğü verir. Yer ve zaman kısıtlamalarını ortadan kaldırdığı için işyeriniz fiilen herhangi bir yer olabilir. Diğer kablosuz cihazlara bağlanan cihazlar mobil çalışanlara daha kesintisiz çalışma yöntemleri sağlar. İşyeri içi uygulamaları da ağıınızı rahatlatmaya yardımcı olur. Kablosuz ortam işinizin daha becerili ve verimli hale gelmesi demektir. Çalışanlarınız teknolojik engellerle boğuşmak zorunda olmadan en iyi yaptıkları işleri yapabilirler.

### 5.1.Kablosuz Ağ İle Neler Yaparsınız?

- İnternet’i tarama veya dosya gönderme,
- Wi-Fi 50-100 metre menzile sahiptir,
- Ofisinize veya e-posta istemcinize bağlantı,
- Telefonunuz ve ofis takviminin senkronizasyonu,
- Ofis internetine bağlantı,
- word, sheet veya ppt dosyalarını gönderme/alma,
- Şebeke bağlantısı gerektiren gelişmiş konferans çağrısı teknolojilerinden faydalanma,
- Çevrimiçi oyun oynama,
- Telefonunuzda hızlı mesajlaşmayı kullanarak sohbet.
- Aldığı sinyaller doğrultusunda kablosuz bağlanabilme .

## 5.2.Kablosuz İletişim Teknolojilerinin Kullanım Alanları

- 1.Telekomünikasyon
- 2.Tıp ve sağlık
- 3.Savunma sanayi
- 4.Endüstriyel üretim
- 5.Radyo,televizyon ve eğlence
- 6.Ulaşım

## 6.KABLOSUZ AĞ YÖNTEMLERİ

- Kızılötesi Teknolojisi
- Bluetooth Teknolojisi
- Wİ-Fİ Teknolojisi
- GPRS Teknolojisi
- 3G Teknolojisi

### KIZILÖTESİ TEKNOLOJİSİ

Kızılötesi teknolojisini elektromanyetik spektrumunda gözle görülebilen ışığın altındaki frekansları ( $3 \times 10^{14}$  kHz / 850-950 nm) veri iletiminde kullanan bir teknolojidir. Alıcı ile verici cihaz arasında açık görüş hattının bulunduğu ortamlarda ve kısa mesafeler için çok uygundur. Kızılötesi teknolojisini iki tür kullanmak mümkündür. Birincisi görüş hattı (direct beam, line of sight), ikincisi ise yansıma (diffused beam) yöntemidir [2, 52]. Doğal olarak görüş hattı yöntemi diğerine oranla daha fazla veri iletişimi sağlamaktadır. Ancak uygulamada geniş alan kaplamak ya da çok kullanıcıya ulaşabilmek için yansıma yöntemi tercih edilmektedir.

Profesyonel olarak kızılötesi teknolojisini geçici ağ kurma ihtiyacı duyulan toplantılarda veya gezici satış elamanları tarafından kullanılmaktadır. Bu tür kullanımda yerel kablolu ağ ile bağlantı kurarak bilgi alış verişinde bulunmak ve sunucuya bağlı faks ve yazıcı gibi cihazlardan faydalanmak mümkündür. Aynı ortamda çalışan bir grubun yazıcı, faks ve benzeri donanımları ortaklaşa kullanabilmeleri için bir ağ oluşturmaları da mümkündür.

Kısa mesafe iletişim için uygun olan kızılötesi teknolojisinin iletişim mesafesinin kısıllığı ve fiziksel engellerin ötesine ulaşamaması nedeniyle kablosuz yerel ağlarda çok az kullanılmaktadır. WLAN pazarında %14 oranında kullanıldığı ve bu oranının giderek azaldığı belirtilmektedir [53].

Kızılötesi teknolojisini kısa mesafe (10 m) kablosuz iletişim için uygun ve ucuzdur. Ancak mobil kullanım için uygun olmadığından FHSS ve DSSS kadar yaygın değildir [52]. Kızılötesi teknolojisini WPAN'larda kullanılmakta olup; en yaygın kullanımı ise Bluetooth'da görülmektedir.

## BLUETOOTH TEKNOLOJİSİ

En çok on metre uzaklıkta bulunan Bluetooth® özelliği etkinleştirilmiş cihazları birbirine bağlayan, tüm dünyada kullanılan bir radyo frekansıdır. Bu özellikle dizüstü veya avuçi bilgisayarınızı başka dizüstü bilgisayarlara, cep telefonlarına, kameralara, yazıcılara, klavyelere, hoparlörlere ve bilgisayar faresine bağlayabilirsiniz.

### Size Ne Sağlar?

Hızlı ve kolay erişim sağlar. Bluetooth® özelliğinin eşler arası ağı kullanmak sabit veya kablosuz ağa bağlanmanıza gerek kalmadan ani toplantılarda kolaylıkla dosya alışverişi yapmanızı, belgeleri yazdırarak zaman kazanmanızı sağlar. Örneğin, bir müşterinizin işyerindeki toplantıyı henüz bitirdiğinizi ve hemen eyleme geçmek için durum raporunu yazdırmanız gerektiğini düşünelim. Bluetooth® kullanarak dizüstü bilgisayarınızdaki raporu kapsama alanındaki herhangi bir Bluetooth® özelliği etkinleştirilmiş yazıcıdan yazdırabilirsiniz.

## Wİ-Fİ TEKNOLOJİSİ

Kablosuz Yerel Ağ ( ), kablo yerine , veya radyo frekansı kullanan ve çeşitli kablosuz Internet bağlantıları sağlayan orta boyutta bir BT ağıdır. Wi-Fi veya WLAN ağının olduğu yeri biliyorsanız, web içinde gezebilir, e-posta gönderip alabilir ve özel şirket ağınıza erişebilirsiniz. Bu ağ "yol savaşçısı" durumundaki mobil çalışanları için idealdir.

### Size Ne Sağlar?

Wi-Fi olan her yerde bir bilgi ve iletişim portalı vardır. İşyerinde WLAN olması geleneksel çalışma ortamınızın çok yönlü olmasını sağlayarak daha serbest çalışmanıza olanak verir. Cafe, restoran, otel ve hava alanı gibi yerlerde giderek daha çok WLAN kurulmaya başladığından bu özellikler yalnızca işyeri ile sınırlı kalmaz, ihtiyacınız olan bilgilere buralardan da erişmenizi sağlar. Uçağınızı mı kaçırdınız? Bütün o e-postaları ve faturaları gönderebilirsiniz. En son envanteri bulmanız gerekiyor, ama depoda kimse yok. Şirket ağınıza ulaşın ve programınıza göre, ihtiyacınız olan yanıtları alın. Wi-Fi Internet'ten çok daha fazla yararlanmanızı sağlar.

## GPRS TEKNOLOJİSİ

General Packet Radio Services (Genel Paket Radyo Servisleri ) tanımının kısaltmasıdır. Genellikle dijital cep telefonu teknolojisinin ikinci (2G ) ve üçüncü (3G ) nesillerini belirten "2.5 G" olarak tanımlanır. Cep telefonu şebekeleri üzerinden iletilir ve 114 Kbps'ye kadar veri aktarımı sağlar. Cep telefonunuz ve cep bilgisayarınız, GPRS ile Internet'te sörf yapabilir, e-posta gönderip alabilir, karşıdan veri ve ortam yükleyebilir. Ayrıca, nerede olursanız olun, iş arkadaşlarınızla video konferansı gerçekleştirmenize veya anlık iletilerle ailenizle ya da arkadaşlarınızla sohbet etmenize olanak verecek kadar hızlıdır. Bunların yanı sıra, dizüstü bilgisayarınız veya diğer mobil aygıtlarla bağlantı kurmanızı sağlar.

### 3G TEKNOLOJİSİ

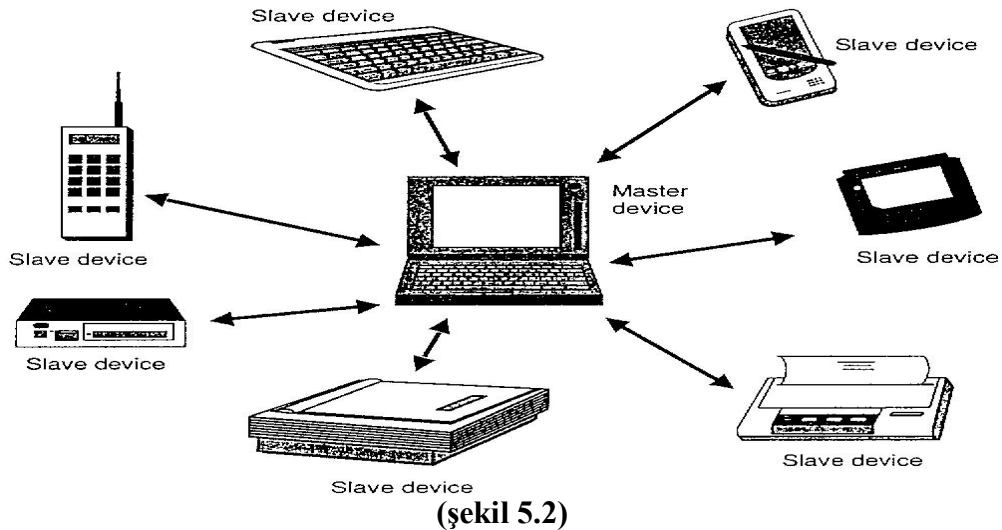
GPRS gibi, de (üçüncü esil kablosuz teknoloji ) bir kablosuz iletişim hizmetidir ve cep telefonunuz, cep bilgisayarınız, tablet PC'niz veya dizüstü bilgisayarınız üzerinden Internet'e 'her zaman açık' (sürekli ) bir bağlantı sağlar. 3G teknolojisi, daha yüksek güvenilirlik ve kalite, daha hızlı veri iletimi ve daha fazla bant genişliği vaat etmektedir (multimedya uygulamaları gönderme olanağı dahil ). 384kbps'ye ulaşabilen veri iletim hızları ile, standart çevirmeli bağlantıya göre yedi kat daha hızlıdır. GPRS ve 3G kullanıcılarından, Internet'e her zaman bağlı olduklarından "her zaman açık" olarak bahsedilmektedir. Arazide çalışanlar, kısa metin mesajlarıyla çalışmalarının ilerleme durumunu bildirebilir ve destek isteyebilirler. Seyahate çıkan yöneticiler şirket e-postalarına ulaşabilir, satış temsilcileri stok durumunu uzaktan denetleyebilirler. Evinizi veya işyerinizi GPRS ve 3G aygıtlarıyla otomatikleştirebilir ve yatırımlarınızı izleyebilirsiniz. GPRS'yi dizüstü bilgisayarınızla kullanarak dosya aktarımı gerçekleştirebilir, uzaktan işbirliği yapabilirsiniz. Her zaman ödeme gerektirmeyen "her zaman açık" bağlantı: Arama süresine göre değil, aktarılan veri miktarına göre ücretlendirme yapılır.

## 7.KABLOSUZ ADRESLEMESİ

### Kablosuz kişisel alan ağları adreslemesi

Tek bir "Bluetooth WPAN" maksimum sekiz aktif aygıt içerebilir. Bu tip ağlar genelde "piconet" olarak açıklanır.

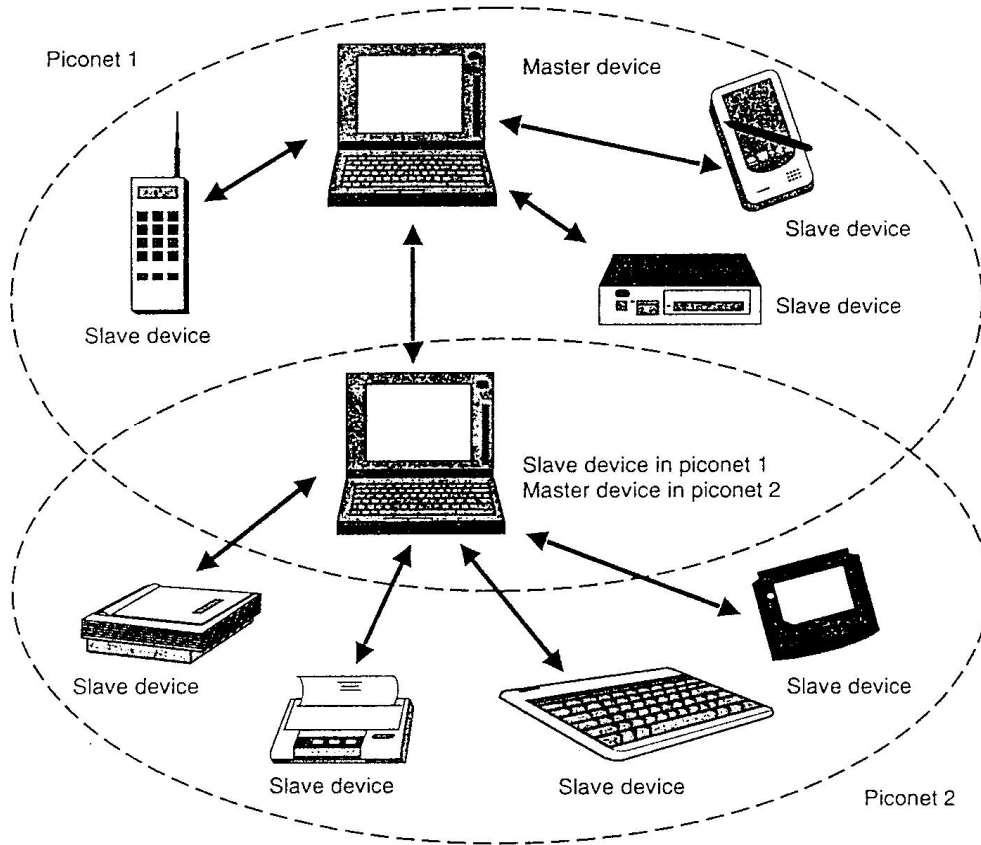
"Piconet" içindeki bir aygıt "master" olmak için tasarlanır, diğer aygıtlar ise "slave" olarak tanımlanır. Herhangi "Bluetooth" aygıtı "master" ya da "slave" olabilir. Genel "piconet" üzerine tasarlanmış aygıtlar "master" olarak belirlenir. "Master" aygıtın gerçek rolü aygıtlar arası senkronizasyon sağlamak ve kontrol etmektir. (bakınız şekil 5.2)



48-bit adresleme her bir “Bluetooth” aygıt üreticisi tarafından tekil olarak verilmektedir. Bu nedenle “piconet” üzerinde maksimum sekiz aktif aygıt olabilir ve sadece adresleme için 3 bit yeterlidir ( $2^3=8$ ). “Master” aygıt her bir “slave” aygıtı 1 den 7 ye kadar numara verir. “Broadcast” mesajı için “0” değerinin gönderilmesi yeterli olacaktır. “Piconet” üzerinden “broadcast” mesajı sadece “master” aygıt üzerinden olabilir.

Ofis gibi çoklu kullanıcı ortamlarında birden fazla “piconet” aktif olabilir. “Scatternet” kavramı 2 veya daha fazla “piconet” in aynı ortamdaki topluluğunu anlatır. Bu tür durumlarda tek bir “Bluetooth” aygıtı birden fazla “piconet” üzerinde “master” ya da “slave” olarak aktif olabilir. (bakınız şekil 5.3)

“Scatternet” üzerinde 48-bit aygıt adreslemesi her bir “piconet”i tekil olarak tanımlamada “access code” türetmek için kullanılır. “Access code”ların kombinasyonu ve 3 adresleme bit’i bağımsız mesaj alıcılarının okumasını ve verilen mesajı işlemesini sağlar.



(şekil 5.3)

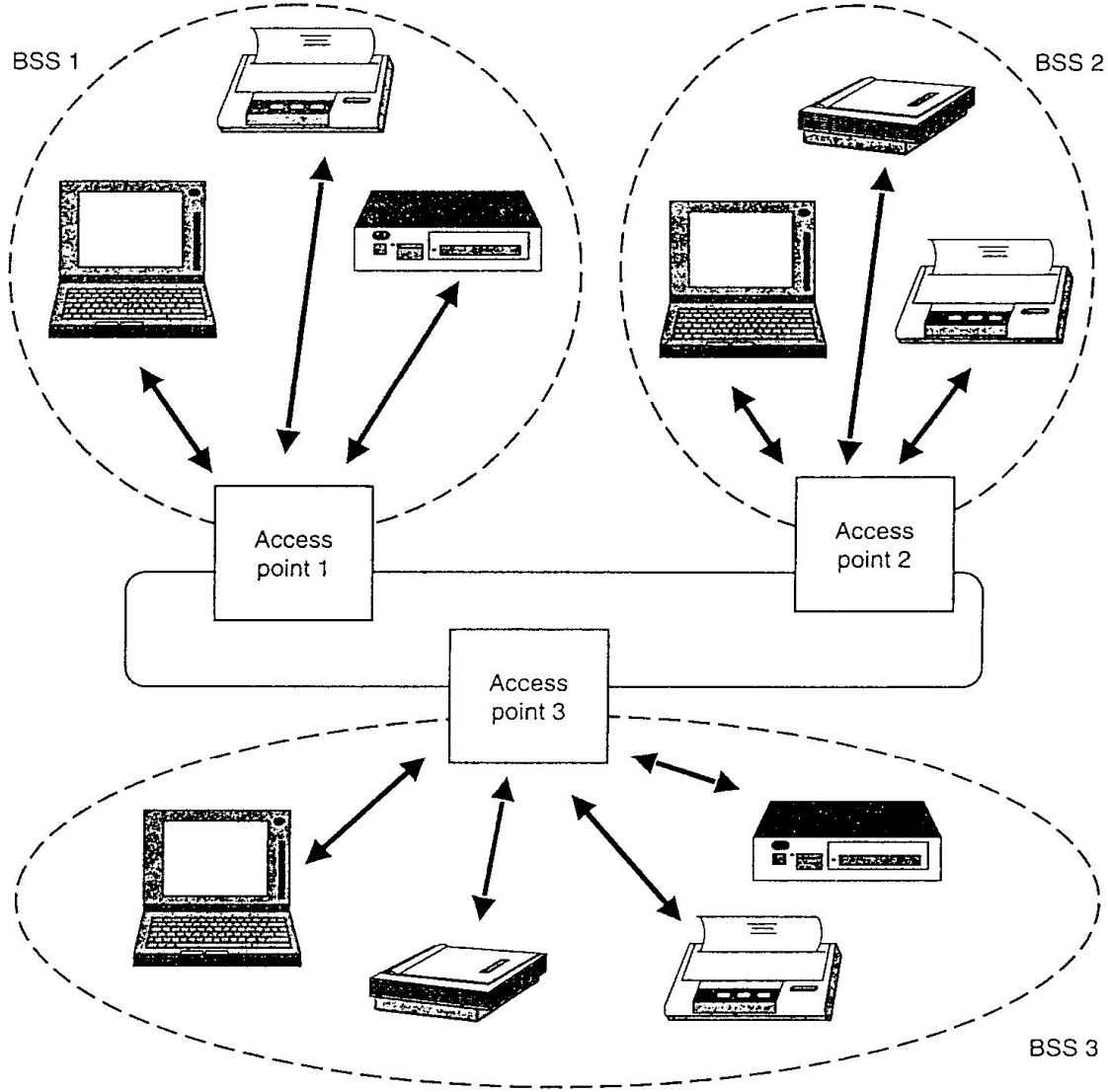
## Kablosuz yerel alan ağı adreslemesi

Bir “IEEE 802.11 WLAN” bir veya birden fazla “APs” içerebilir ki bunlarlar da geleneksel kablolu “LANs” için kullanılan “hub” ve “concentrator” lara eş değerdir. “APs” kullanıldığında, ağ mesajları heriki istasyondan da kaynaklanabilir.

Verilen bir mesaj aşağıda verilen yönlerden birini izleyebilir:

- Kaynak aygıttan hedef aygıt
- Kaynak aygıttan hedef “AP” e
- Bir “AP”ten başka bir “AP” e
- Kaynak aygıttan bir veya birden fazla ilave edilmiş “AP”a ve oranda hedef aygıt

Bu yönler üzerinde dağıtımı sağlamak için “IEEE 802.11” ağı üzerindeki her bir mesaj dört 48-bit adresinden fazlasını içerebilir. Çoklu “APs” üzerinden mesaj transferine ihtiyaç duyulurken “APs” adreslerinin düzeltilebilmesinde hedef ve kaynak aygıt adreslerinin her zaman uygun olmasını sağlar. (bakınız şekil 5.4)



BSS = Basic service set

(şekil 5.4)

Aşağıda “WLAN” adreslemesiyle ilgili birkaç terim açıklaması yer almaktadır.

### **Aygıt Adresi**

“WLAN” üzerinde bulunan her bir aygıtı veya “AP”i tanımlamak için kullanılan 48-bit sıralı adreslemedir. Bir aygıt ya da “AP” adresinin mesajın kaynak adres kısmında gözlenmesinde, aygıt ya da “AP” mesajı okur ve işler. Aşağıdaki terimler genelde “device address” için kullanılır

- Donanım adresi (Hardware address)
- Fiziksel adres (Physical address)
- Bireysel adres (Individual address)
- Bilgi aktarma katman adresi (Data link layer address)
- MAC adresi (MAC address)
- NIC adresi (NIC address)
- Yerel alan ağ adresi (LAN address)
- Katman 2 adresi (Layer 2 address)

### **Evrensel yönetimli adresleme**

Üretici firmalar tarafından “WLAN” arayüzlerine “device address” atanmasıdır. Bu adresin tekil olması garantidir. Başka hiçbir üretici tarafından bu adres kullanılamaz. Birçok “WLAN” üzerinde 48-bit adresleme kabul edilmiş ve aygıtın içerdiği arayüzü tanımlamada kullanılmıştır. Adresin ilk 24-bit’i arayüz üreticisini tanımlar. Bu “organization unique identifier (OUI)” olarak adlandırılır. “IEEE” üreticilerin “OUI” larını tutmakla sorumludur.

“Globally administered addressing” bazen “Universal addressing” diye de kullanılır.

### **Yerel yönetimli adresleme**

“Locally administered addressing” ile aygıtların “globally administered address”i ağ tasarımcıların seçilen adresleri ile yer değiştirilmiştir. “Locally administered addressing” genelde kullanılmaz çünkü ağ sorumlusunun her atanmış adresin izini saklamasını gerekli kılar. Bu durum adres tekrarlanmasının oluşturduğu ağ hatalarından kaçınmayı gerektirir.

### **Grup yayım adresi**

Aynı ağa bağlı olan tüm aygıtların mesajı okumasını ve işlemesini göstermek için kullanılır. “WLANs” üzerinde “broadcast” adresi 48-bit’tir.

**Not:** Genelde 48-bit “WLAN” adresleri “hexadecimal” şeklinde görülür. “Broadcast” adreslerinin “hex” görünümü “FF-FF-FF-FF-FF-FF” şeklindedir. Buradaki her bir “F” dört çifti gösterir.

### **Çoklu grup adresi**

Aynı ağa bağlı iki ya da ikiden fazla aygıtın mesajı okumasını ve işlemesini göstermek için kullanılır.

**Not:** “Multicast group” içine dahil edilmiş aygıtlar “higher layer processes-software operating above the OSI Data Link layer” tarafından seçilir.

### **Temel servis atama tanımlaması**

“AP” tarafından kontrol edilen ağın bir parçasını tanımlamak için 48-bit adresleme kullanılır. Çoklu “AP”li “WLAN” üzerinde her bir “AP”e tekil “BSSID” verilir. Bir aygıt başka bir aygıtla mesaj göndereceği “AP”i tanımak için “BSSID”ı kullanılır.

## 8.KABLOSUZ AĞLARDA GÜVENLİK

Güvenlik, kablolu veya kablosuz her türlü ağ için en önemli konudur. Klasik bir kablolu ağ üzerinden iletişim, fiziksel kablolar üzerinden sağlanır ve güvenlik, genellikle fiziksel altyapıda dahili olarak bulunur. WLAN'lar radyo sinyalleri üzerinden çalışır ve bu nedenle aynı güvenlik önlemlerinin uygulanması gerekmez. Kablosuz verilerin benzersiz niteliği için, bir WLAN kullanıcısı bilgisayar korsanlarının saldırılarına, vandalizm saldırılarına ve hatta kurumsal casusluğa karşı ağın daha güvenli hale getirilmesi için çeşitli güvenlik özelliklerinden yararlanabilir.

### **Wi-Fi Korumalı Erişim 2 (WPA2)/802.11i**

Wi-Fi Korumalı Erişim 2 (WPA2), IEEE 802.11i standardına dayanır ve Gelişmiş Şifreleme Standardı -Karşı Mod ile Şifre Bloğu Zincirleme Mesaj Kimlik Denetimi Kodu Protokolü (AES-CCMP) kullanarak bir şifreleme mekanizması sağlar. Bu sayede, birçok kuruluşun ihtiyacı olan veri gizliliği seviyesi sağlanmış olur. WPA2/802.11i ayrıca sinyal gecikmesini ve dolanım sırasında ses içerisindeki kaybolmasını önleyerek, kablosuz ses iletimi için en güncel kod ayarını ve desteğini sunar. WPA2 iki modda çalışabilir: WPA2 kurumsal ve WPA2 bireysel. WPA2 kurumsal modu, 802.1 x/EAP tabanlı kimlik denetimi için gerekli tüm WPA 2 özelliklerini ve desteğini içerirken, WPA2 bireysel modu, özellikle daha az karmaşık temel yönetim şemaları gerektiren küçük işletme ve ev ortamları için kullanılır. WPA2/802.11i, Wi-Fi Korumalı Erişim (WPA) ile geriye dönük olarak tam uyumludur.

### **Wi-Fi Korumalı Erişim (Wi-Fi Protected Access ) (WPA)**

Wi-Fi Korumalı Erişim, (WPA) birçok yönden WPA2/802.11i ile benzerdir. WPA ve WPA2 arasındaki temel fark, kullanılan şifrelemedir. WPA için RC4/TKIP ve WPA2 için AES-CCMP. WPA ve WPA2, 802.11i standardından türetilmiş olup, WPA2 bu ikisi arasında en yeni sürümdür. WPA, kurumsal modda çalışan istemcinin bilgi işlem oturumu için bir 'çiftler arası' anahtar yaratmak için 802.1x ağ kimlik denetimi ve Geçici Anahtar Bütünlüğü Protokolü (TKIP) şifreleme önlemleri kullanır; veya ev modu oturumları için kullanıcılar kablosuz ağdaki her bir AP ve PC'ye bir ana anahtar girer. Çiftler arası anahtar daha sonra istemciye AP'ye dağıtılır.

Kimlik denetiminin başarılı olmasının ardından, TKIP tekli statik 40-bit WEP güvenlik anahtarını çoklu dinamik 128-bit güvenlik anahtarlarına dönüştürür. İşin özünde TKIP, arka arkaya kullanılan tek bir WEP anahtarını, yaklaşık 500 trilyon adet başka olası anahtarla değiştirir. Yeni nesil ürün ailelerinde, maksimum güvenlik ve başka kablosuz cihazlarla daha yüksek düzeyde birlikte çalışabilirlik sağlamak amacıyla hem WPA2 ve hem de WPA bulunmaktadır.

## **802.1x Ağ Kimlik Denetimi**

802.1x, bir WLAN erişim noktasında (AP) oturum açmak isteyen bireysel bir istemciyi (dizüstü ya da masaüstü bilgisayar), AP'ye Genişletilebilir Kimlik Denetimi Protokolü (EAP) başlatma mesajı göndererek, onaylanmamış bir duruma geçiren bir kimlik denetimi yöntemidir. 802.1x ağ kimlik denetimi, 802.11g kablosuz standardının bir parçasıdır ve tüm 802.11g uyumlu kablosuz standardlı ürünlerde yer alır.

## **Kablolu Eşdeğeri Gizlilik (WEP)**

Kablolu Eşdeğeri Gizlilik (WEP) 64 ve 128-bit şifreleme kullanır ve 802.11a, 802.11b ve 802.11g ağlarında kullanım için belirlenen şifre şemasıdır. WEP bir WLAN üzerinden iletilen verileri şifreleyerek, istemci ve erişim noktası arasındaki hassas iletişimi korur. Klasik güvenlik önlemleriyle (şifre koruması, kimlik denetimi, şifreleme, sanal özel ağlar) karşılaştırıldığında, WEP son derece etkili olabilir. Tüm kablosuz ağ ürünlerinde 64 ve 128-bit WEP şifreleme mevcuttur.

## **SSID Yayını Devre Dışı Bırakma**

Bir Servis Seti Tanımlayıcısı (SSID), tamamen özel olarak atanmış bir alfanümerik ad 1 - 32 bayt arası olup, bir WLAN ağını tanımlamak için kullanılır ve kapalı, çakışan bir ortam içinde birden fazla WLAN ağı kullanıldığında, kablosuz cihazların uygun WLAN ağına başlanmasını sağlar. Bu tanımlayıcı yayınlanır ve bu nedenle kapsama alanı içindeki kablosuz istemciler tarafından görülebilir. WLAN Erişim Noktası (AP), bu tanımlayıcıyı engelleyerek birçok rasgele kablosuz aygıt tarafından görülmez olmasını sağlayan SSID Yayını Devre Dışı Bırakma ayarı ile gelir. İstemcilerin tipik olarak belirli bir SSID ile "ilişkilendirilmesi" gerektiğinden, bu sayede başka bir kablosuz koruma seviyesi sağlanmış olur.

## **MAC Adresi Kimlik Denetimi**

Bazı erişim noktaları (veya erişim noktası içeren kablosuz yönelticiler) kullanıcıların tam olarak hangi Ortam Erişim Denetimi (MAC) adreslerinin ağla iletişim kurabileceğini tanımlamasına olanak sağlar. Bir MAC adresi, bir ağın her bir düğümünü ayrı ayrı tanımlayan bir donanım adresidir. Dünyadaki her bir ağ adaptörünün, kendine has bir MAC adresi vardır. Sadece bir ağa bağlanabilecek MAC adreslerini tam olarak belirleyerek, yetkisiz kullanıcılar devre dışı bırakılabilir. MAC adresi kimlik denetimi bunu sağlar. Ağın baz istasyonu (erişim noktası), yetkili MAC adreslerinin bir veritabanını tutar. Sadece yetkili MAC adresine sahip cihazların ağa erişimine izin verilir.

## 9.KABLOSUZ AĞLARDA KEŞİF

Kablosuz ağlarda keşif civar çevrede bulunan erişim noktalarının tespitidir. İşi abartıp WLAN araçlarını arabalarına alarak yol boyunca etrafta bulunan kablosuz ağları keşetmeye yönelik durumlara Wardriving, erişim noktalarının özelliklerine göre(şifreleme desteği var mı? Hangi kanalda çalışıyor vs) bulundukları yerlere çeşitli işaretlerin çizilmesine ise WarChalking deniyor. Ülkemizde henüz yaygınlaşmasa da, Amerika gibi kablosuz ağların çok yoğun olduğu ülkelerde sık karşılaşılabilecek durumlardır. War driving için çeşitli programlar kullanılabilir fakat bunlardan en önemlileri ve iş yapar durumda olanları Windows sistemler için Netstumbler , Linux sistemler için Kismet'dir. Kismet aynı zamanda Windows işletim sisteminde de çalışabilmektedir.

Kablosuz ağlarda keşif, Pasif ve aktif olmak üzere ikiye ayrılır. Adından da anlaşılacağı gibi aktif keşiflerde keşif yapan kendisini belirtir ve aktif cihazları aradığını anons eder. Pasif keşif türünde ise tam tersi bir durum söz konusudur. Pasif keşif gerçekleştiren cihaz kesinlikle ortama herhangi birşey anons etmez, sadece ortamdaki anonsları dinleyerek aktif cihazları belirlemeye çalışır.

Aktif keşif araçlarına en iyi örnek NetStumbler verilebilir. Ücretsiz olarak kullanılabilen Netstumbler çalıştırıldığında kapsama alanındaki tüm aktif cihazları bularak bunları raporlar. Netstumblerin çalışması ya da bir erişim noktasını keşfetmesi için erişim noktasının kendisini anons etmesi lazımdır. Yani basit güvenlik önlemi olarak aldığımız SSID saklama işlemi Netstumbler'i şaşırtacaktır. ,

Pasif keşif aracı olarak kullanılabilen Kismet ise Netstumbler'a göre oldukça fazla özellik içerir ve kötü niyetli birinin elinde tam donanımlı gizli bir silaha dönüşebilir.

### Kablosuz Ağları Dinleme

Kablosuz ağlarda veriler havada uçtuğu için dinleme yapmak kablolu ağlara göre daha kolaydır. Amaca uygun kullanılan bir dinleme aracı ile bir kablosuz ağdaki trafik ağa dahil olmadan rahatlıkla izlenebilir. Linux sistemlerde kablosuz ağ trafiği dinlemek için Kismet adlı program tercih edilir. Kismet, monitoring (rfmon) mod destekleyen kablosuz ağ arabirimleri için düşünülmüş 802.11b, 802.11a ve 802.11g protokolü ile çalışan kablosuz ağlarda pasif dinleme yapmaya yarayan bir araçtır. Aynı zamanda kablosuz ağlar için pasif keşif aracı olarak da kullanılabilir.

Kismet ile dinleme yapılırken etraftaki erişim noktaları ya da istemciler rahatsız edilmez. Tamamen pasif modda bir dinleme yapıldığı için kablosuz ağları korumaya yönelik saldırı tespit sistemleri kolaylıkla aldatılmış olur. Özellikle şifresiz bir iletişim yöntemi tercih edilmişse Kismet bu noktada kablosuz ağdaki tüm herşeyi görebilir. Ekte bu seneki Linux şenliklerinde sunum için hazırladığım Kismet'in ekran görüntüsünü görebilirsiniz: ağa dahil olmadan çevre civardaki erişim noktalarını ve bu erişim noktasına bağlı tüm kablosuz ağ istemcilerinin MAC ve IP bilgilerinin kismet tarafından rapor edilmiş hali.

Kismet ve ek bir iki araç kullanılarak MAC adres tabanlı güvenlik önlemi alınmış kablosuz ağlara kolaylıkla giriş yapılabilir.

Kismet aynı zamanda kablosuz ağlarda izinsiz giriş tespiti içinde kullanılabilir. Ağa erişim izni olmayıp da giriş deneyiminde bulunan kullanıcılar Kismet tarafından rahatlıkla belirlenerek raporlanacaktır.

Yine kismet aracı tarafından kaydedilmiş trafiğin Ethereal( Trafik Analiz aracı) ile analiz edilmiş haline bakacak olursak hiç yetkimiz olmadığı halde kablosuz ağdaki istemcilerin nerelere eriştiğini ve neler yaptığını görmemiz zor değildir.

## **Nasıl Korunacağız?**

Özellikle kablosuz ağlarda tehlike oluşturabilecek potsansiyelleri belirleyerek işe girişelim. Kablosuz ağlarda risk oluşturan kullanıcı kitlesini üçe ayırabiliriz;

- Meraklı Bilgisayar kullanıcıları
- Band genişliği hırsızları
- Hackerlar**

Meraklı bilgisayar kullanıcıları,hiçbir şekilde kurtulamayacağımız, aslında görüldüğü kadar da tehlikeli olmayan kısmı oluşturur. Konu hakkında teorik bilgileri olmadığı için yapmak istedikleri işleri otomatize araçlara havale ederler ve bunların çıktıları ile yetinirler. Bu kullanıcı grubunu oluşturan kimliklerden korunmak için SSID saklama, MAC adres tabanlı erişim denetimi gibi temel güvenlik önlemlerini almanız yeterli olacaktır. Diğer bir kullanıcı kitlesi de şifrelenmemiş ya da eksik yapılandırılmış kablosuz ağları kullanan “bant genişliği hırsızları “olarak da adlandırabileceğimiz zararsız kullanıcılardır. Bunların tek amacı varolan kablosuz ağı kullanmaktır. Kablosuz ağdan kendileri de yararlandıkları için zarar vermezler. Ağınızda yavaşlıktan şikayet ediyorsanız ilk düşünülecek kategorideki kimliklerdir.

Hackerlar, bu tip kimlikler bilgi seviyelerine göre değişecektir. Bazıları için ileri düzey güvenlik önlemleri almadan korunmanız imkansızdır. Yine de WEP/WPA gibi protokolleri kullanırsanız bu tip kimliklerden gelecek saldırı riski azalacaktır. Bir nevi caydırma politikası olarak da düşünebiliriz.

## **Ev Kullanıcıları için Tavsiyeler**

Evinde kablosuz ağ kullananlar için temel seviyede güvenlik önlemi almak yeterli olacaktır. İlk olarak Kullandığımız erişim noktası cihazının adını(SSID) değiştirmeliyiz. Zira erişim noktasının adını varsayılan olarak bırakmamız cihazın yazılımında çıkacak bir güvenlik açığının ilk bizim donanımımızda denenmesi demektir. Yine benzer şekilde cihaz markası ve modelini bilen kötü niyetli birileri cihazın yönetim arabirimine ulaşarak varsayılan kullanıcı adı ve parolalarını deneyecektir. Bu sebeple alınan cihazların varsayılan değerleri – özellikle yönetim arabirimine giriş için kullanılan hesap bilgileri- mutlaka değiştirilmelidir. Cihaz destekliyorsa SSID yayını da kesebiliriz. Sadece kendi belirlediğimiz istemcilere cihazın adını vererek bağlantı kurmasını sağlamak da iyi bir önlem olacaktır.

## **Şirket Ağları için tavsiyeler**

Şirket ağlarında kullanılan erişim cihazları kesinlikle yerel ağla direkt haberleştirilmemelidir. Araya bir güvenlik duvarı konularak kablosuz ağ istemcilerinin yerel ağa girişleri sınırlandırılarak olası saldırı girişimlerinde iç ağıımızın etkilenmesini önlemiş oluruz.

Mac adresi tabanlı güvenlik kontrolü şirket ağlarından da alınması gereken temel güvenlik önlemlerindendir. Fakat sadece mac adresi tabanlı denetim yapıp bırakmak bir işe yaramayacaktır. Ağımızdaki MAC-IP değişikliklerini izleyen ve raporlayan bir araç da güvenliğin kontrolünü sağlamada önemli bir adım olarak karşımıza çıkıyor. En basitinden ağa yeni eklenen ve ağda IP, MAC adreslerini değiştiren cihazlar uygun bir yazılım ile kontrol edilmelidir. Linux ve UNIX sistemlerde arpwatc yazılımı bu işi oldukça iyi yapmaktadır. Aynı yazılımın Windows versiyonu(winarpwatc) da ücretsiz olarak kullanılabilir.

Kablosuz ağlar için tasarlanmış saldırı tespit yazılımları kullanılabilir. Fakat bu tip yazılımların yönetimi ve ağa uygulanması zaman alacaktır. Erişim noktası cihazınız destekliyorsa WPA kullanımı iyi bir seçim olacaktır. Şirket ağlarında kesinlikle WEP kullanımı tercih edilmemelidir. Erişim noktası cihazının özelliklerine bağlı olarak EAP olarak adlandırılan ve çeşitli şekillerde kimlik doğrulama özelliği sağlayan protokollerde kullanılmalıdır.

## **Halka Açık Kablosuz Ağlardaki Tehlikeler**

Kablosuz ağların belki de en işe yarar olduğu durumlar halka açık olanlarıdır. Hemen hemen tüm büyük alışveriş merkezlerinde bu tip ağlara rastlayabiliriz. Bazıları erişim için kullanıcı adı / parola istese de yukarıda anlattığım yöntemler kullanılarak bu tip ağlar rahatlıkla kandırılabilir. Gelelim bu tip ağlardaki risklere; Öncelikle aynı erişim noktasına bağlı tüm istemcilerin trafiği şifrelenmemiş bir şekilde havada dolaşacaktır. Bunun içinde MSN görüşmeleriniz, e-postalarınız ve ziyaret ettiğiniz siteler de dahil. Hemen kafamızda minik bir senaryo kuralım: Herkese açık bir kablosuz ağ ortamına gelen kötü niyetli bir kullanıcı diz üstü bilgisayarını açarak ortama dahil oluyor ve kablolu ağlarda da kullanılabilen trafik dinleme ve değiştirme araçlarını kullanmaya başlıyor. Beş dakika sonra tüm trafiği erişim noktası üzerinden değil de kendisi üzerinden geçirmeyi başarıyor ve istediği işlemleri bu trafik üzerinde yapıyor. Mesela bir istemci [www.galatasaray.org](http://www.galatasaray.org) adresine girmek isterken onun isteğini [www.antu.com](http://www.antu.com)'a yönlendirebilir ve daha niceleri. Burada kurduğumuz senaryo oldukça zor gözükmesine rağmen işini bilen kötü niyetli biri tarafından kolaylıkla başarılabilir. Peki o zaman ne yapacağız? Böyle bir nimetten faydalanmayacağız mı dediğinizi duyar gibiyim. Kullanım riskini bildikten sonra kullanmamanız için hiçbir sebep yok. Ama eğer güvenli bir iletişim istiyorsanız ya VPNi kullanmanızı ya da benzeri bir özellik sağlayan TOR aracını kullanmanızı öneririm.

## **10.KABLOSUZ AĞ KARTINI NEREDEN SATIN ALABİLİRİM?**

Bilgisayar ve teknoloji ürünleri satan mağazalardan yada;  
<http://www.koc.net/adsl/adsl.shtml> sayfasından  
<http://www.artnet.net.tr/> sayfasından  
<http://www.telekomadsl.com> sayfasından  
<http://www.hepsiburada.com> sayfasından  
[www.ofislog.com.tr](http://www.ofislog.com.tr) gibi internet sayfalarından alabilirsiniz.