WIFI ATTACK AND DEFENSE

Besim ALTINOK
Security Engineer

Kablosuz Ağlar ile ilgili Temel Bilgiler

Önemli Kablosuz Ağ Terimleri

SSID : Kablosuz ağ yayının ismi
BSSID : Kablosuz ağ yayını yapan cihazın MAC adresi
AP : Yayını yapan cihaz (Access Point)
Dbi : Yayın için kullanılan antenin gücü
STA : Erişim noktasına bağlanan cihaz (Client)
Client : Erişim noktasına bağlanan cihaz
Channel : Yayının yapıldığı frekans noktası

Önemli Kablosuz Ağ Terimleri

- **SSID**
  - AP cihazının adıdır.
  - AP cihazında SSID Broadcast özelliği açık ise genelde saniyede 10 defa olmak üzere yayın yaptığı kanalda kendisinin orada olduğunu belirten bir şekilde sinyal gönderir (beacon frame).
  - Bu sayede ağları otomatik olarak bulabiliriz.
  - SSID Broadcast kapatıldığında istemciler AP cihazları otomatik olarak bulamayacaktır.

Önemli Kablosuz Ağ Terimleri

- **MAC**
  - 48 bittir.
  - İlk 24 bit üretici firmayı belirler. (OUI)
  - Benzersizdir.
  - MAC adresinin hangi üretici firmaya ait olduğunu öğrenebilmek için aşağıdaki adresleri kullanabiliriz.

Detaylı bilgi için kullanılabilir.

http://www.macvendorlookup.com/

https://www.wireshark.org/tools/oui-lookup.html

Önemli Kablosuz Ağ Terimleri

Kanal Numaraları

802.11b/g/n Channels

channel	frequency (MHz)	North America [3]	Japan[3]	Most of world[A] [3][4][5][6][7]
1	2412	Yes	Yes	Yes[D]
2	2417	Yes	Yes	Yes[D]
3	2422	Yes	Yes	Yes[D]
4	2427	Yes	Yes	Yes[D]
5	2432	Yes	Yes	Yes
6	2437	Yes	Yes	Yes
7	2442	Yes	Yes	Yes
8	2447	Yes	Yes	Yes
9	2452	Yes	Yes	Yes
10	2457	Yes	Yes	Yes
11	2462	Yes	Yes	Yes
12	2467	No[B]	Yes	Yes
13	2472	No[B]	Yes	Yes
14	2484	No	11b only[C]	No

- Farklı frekanslarda 1-14 arası yayın kanalı vardır,
- AP ve STA bir kanaldan iletişim kurar.
- Örnek olarak AP 12. kanalda yayın yapıyorsa STA' da
- o kanaldan bağlanır. Aynı şekilde AP ve STA' in yaptığı broadcast (*genel*) isteklerde her kanal için ayrı yapılmalıdır.

- **USA** – Uses channels 1 to 11 (2.412 GHz – 2.462 GHz)
- **Europe** – Uses channels 1 to 13 (2.412 GHz – 2.472 GHz)
- **Japan** – Uses channels 1 to 14 (2.412 GHz – 2.484 GHz)

Önemli Kablosuz Ağ Standartları

802.11a

- 5GHz band aralığında yayın yapar
- Daha fazla kanal kapasitesi vardır.
- 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.

Önemli Kablosuz Ağ Standartları

802.11b

- 2.4 GHz frekans bandında çalışmakta ve 11 Mbps veri iletimi hızına çıkabilmektedir.
- Kapsama alanı mesafesi fazladır.
- 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.
- Taşınabilirliğin gerekli olduğu ve orta hızlı ağ bağlantılarına ihtiyaç duyulan alanlarda kullanılır.

Önemli Kablosuz Ağ Standartları

Protocol	Release Date	Frequencies	Rates	Modulation	Channel Width	Notes
Legacy	1997	2.4-2.5GHz	1 or 2Mbit	FHSS/DSSS	1MHz/20MHz	No implementations were made for IR
802.11b	1999	2.4-2.5GHz	1, 2, 5.5, 11Mbit	DSSS	22MHz	Proprietary extension: up to 33Mbit
802.11a	1999	5.15-5.25/5.25-5.35/5.725-5.875GHz	6, 9, 12, 18, 24, 36, 48, 54Mbit	OFDM	20MHz	Proprietary extension: up to 108MBit
802.11g	2003	2.4-2.5GHz	Same as 802.11a and 802.11b	DSSS /OFDM	20MHz/22MHz	Proprietary extensions: up to 180Mbit/125MBit
802.11n	2009	2.4 and/or 5GHz	Up to 600Mbit	DSSS/OFDM	20/20 or 40MHz	

Kablosuz Ağ Çalışma Modları

Master Mod

AP cihazının bulunduğu mod olarak tanımlanır.

Manage Mod

AP cihazına bağlanmaya çalışan istemci modu

Monitor Mode

Bu moda geçen cihaz AP cihazı ile iletişim kurmaz

Dinleme moduna geçer

Promiscious Mode ile farkı :

Aynı ağda olmamıza gerek yoktur.

Kablosuz Ağlar İçin Kullanılan Tasarımlar

Infrastructure Network

- Haberleşme için bir kablosuz ağa ihtiyaç vardır.
- İşletim sistemleri varsayılan olarak bu yöntemi kullanırlar
- Basic Service Set (BSS) olarak adlandırılırlar.
- Trafiğin dinlenmemesi için şifreleme kullanılır.

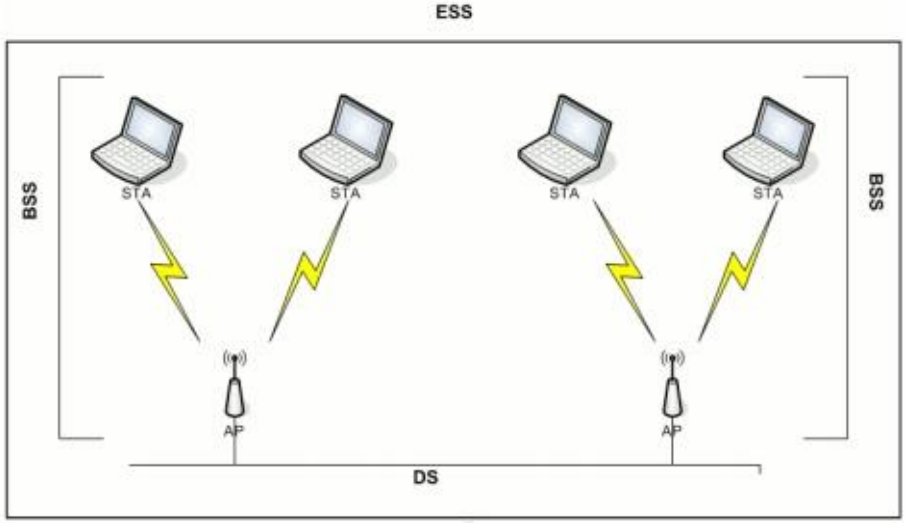


Figure 2-1 - DS, BSS, and ESS Relationships

Kablosuz Ağlar İçin Kullanılan Tasarımlar

Ad-Hoc Network

- Haberleşme için bir kablosuz ağa ihtiyaç yoktur.
- Independent Basic Service Set(IBSS) olarak da bilinir.
- İnternet bağlantısı olmayan bir cihazın internet bağlantısı olan bir cihaz üzerinden internete çıkmasını bu yöntem ile sağlayabiliriz.

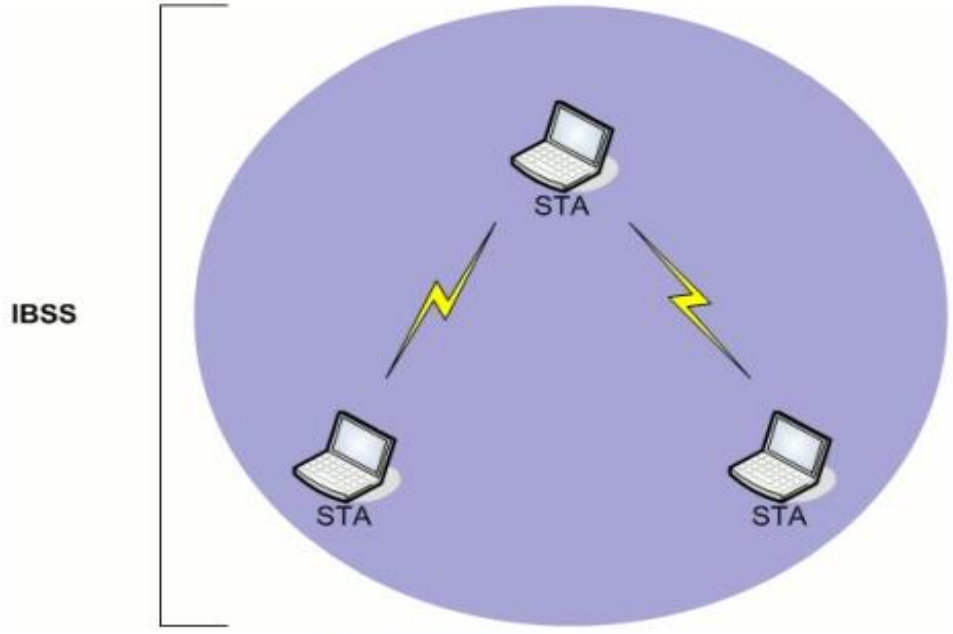


Figure 2-2 - Ad-Hoc Network Diagram

Kablosuz Ağ Testlerinde Ağ Adaptörü ve Anten Seçimleri

Testlerde Kullanılabilecek Ağ Adaptörleri

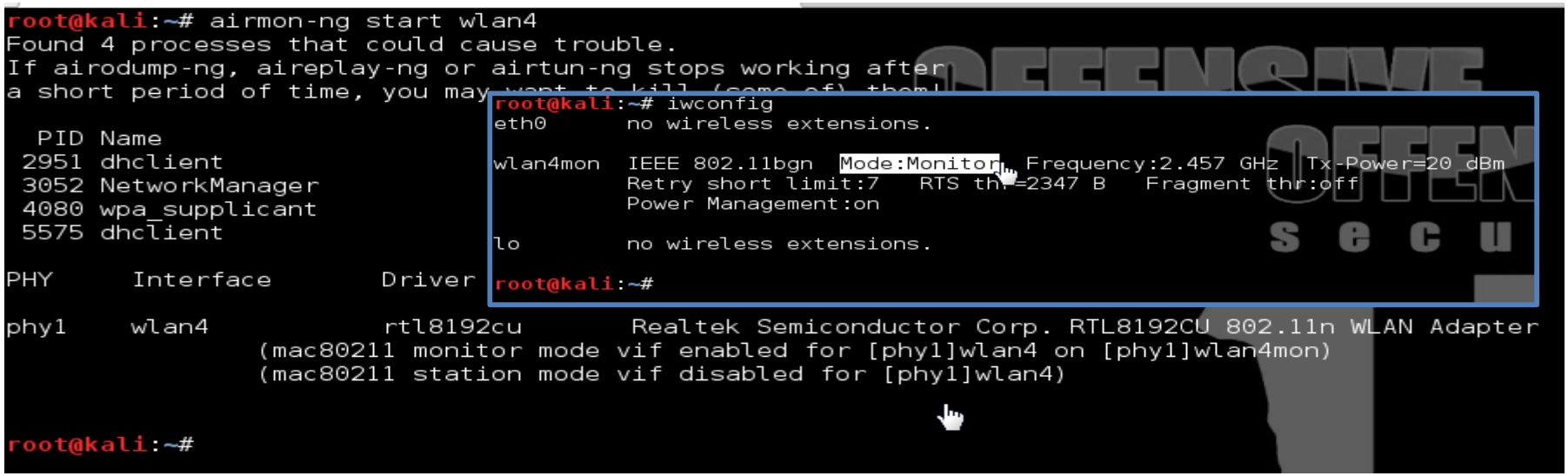
- Atheros (AR5XXX, AR9XXX)
- Broadcom (B43XX Family)
- Intel Pro Wireless and Intel Wifi Link (Centrino)
- Ralink (RT2X00)
- Realtek (RTL8187)

Kablosuz Ağ Testlerinde Ağ Adaptörü ve Anten Seçimleri

- Kullanılabilecek Anten Tipleri
  - Kablosuz ağ testlerinde çekim alanımızı artırmak için farklı tipte antenler kullanma ihtiyacımız olabilir.
  - **Omni-Directional Antenler**
    - Bu antenler tek yönlü değildirler aynı anda her yönde alanı genişletebilirler.
  - **Directional Antenler**
    - Eğer hedef tespit edildi ve tek yönlü sinyal güçlendirme gerçekleştirilmek isteniyorsa bu tip anten kullanılabilir.

Kablosuz Ağ Kartımızı Monitör Moda Almak

- Bir önceki işlemi gerçekleştirdikten sonra ,
  - **Airmon-ng start wlan0** komutunu yazarak ağ kartımızı monitör moda alıyoruz.



Kablosuz Ağ Kartımızı Yapılandırmak