

# WLAN Kavramları ve Konfigürasyon Rehberi

Hazırlayan: Furkan Yaşar [in](#) LinkedIn

Bu rehber, kablosuz ağ teknolojileri, standartları, güvenlik mekanizmaları ve konfigürasyonları hakkında temel bilgiler içermektedir.



Kablosuz  
Teknolojiler



Güvenlik



Ağ Bileşenleri



Konfigürasyon

## 1. Kablosuz Ağlara Giriş

**ÖNEMLİ:** Kablosuz LAN (WLAN), ev, ofis ve kampüs ortamlarında yaygın olarak kullanılan bir kablosuz ağ türüdür.

### Kablosuz Ağ Türleri

Ağ Türü	Kapsam	Standart	Örnekler
WPAN	1-100m	IEEE 802.15	Bluetooth, Zigbee
WLAN	~100 metre	IEEE 802.11	Wi-Fi
WMAN	Şehir/District	IEEE 802.16	WiMAX
WWAN	Ülke/Küresel	-	Cellular (4G/5G)

### Kablosuz Teknolojiler

- Bluetooth:** Sınıfına göre menzil:
  - Class 1: ~100m
  - Class 2: ~10m (en yaygın)
  - Class 3: ~1m
- WiMAX:** Alternatif geniş bant internet (50km mesafe)
- Cellular Broadband:** GSM (global), CDMA (ABD)
- Satellite Broadband:** Kırsal alanlarda kullanım

## 2. IEEE 802.11 Standartları

**UYARI:** Farklı standartlar birbiriyle uyumlu olmayabilir (ör. 802.11a, 802.11b/g ile uyumsuzdur).

Standart	Frekans	Maksimum Hız	Özellikler
802.11	2.4 GHz	2 Mb/s	İlk standart
802.11a	5 GHz	54 Mb/s	802.11b/g ile uyumsuz
802.11b	2.4 GHz	11 Mb/s	Daha uzun mesafe
802.11g	2.4 GHz	54 Mb/s	802.11b ile uyumlu
802.11n	2.4/5 GHz	600 Mb/s	MIMO teknolojisi
802.11ac	5 GHz	1.3 Gb/s	8 antene kadar destek
802.11ax (Wi-Fi 6)	2.4/5/6 GHz	9.6 Gb/s	Yüksek Verimlilik Kablosuz
802.11be (Wi-Fi 7)	2.4/5/6 GHz	46 Gb/s	Ultra yüksek verimlilik

### Frekans Bantları

- **2.4 GHz:** 802.11b/g/n/ax (daha geniş kapsama)
- **5 GHz:** 802.11a/n/ac/ax (daha yüksek hız)
- **6 GHz:** 802.11ax (Wi-Fi 6E) ve 802.11be (Wi-Fi 7)

## 3. WLAN Bileşenleri

Kablosuz ağların temel bileşenleri: kablosuz NIC'ler, erişim noktaları (AP), antenler ve kablosuz kontrolcülerdir.

### Erişim Noktası (AP) Türleri

AP Türü	Yönetim	Özellikler
Otonom AP	Bağımsız	Manuel konfigürasyon, CLI/GUI
Lightweight AP	Merkezi (WLC)	CAPWAP/LWAPP protokolü

### Anten Türleri

- **Omni-directional:** 360° kapsama (ev/ofis)
- **Directional:** Belirli yönde sinyal (Yagi, parabolik)
- **MIMO:** Çoklu anten (8'e kadar) ile bant genişliği artışı

### CAPWAP Konfigürasyonu

```
WLC(config)# capwap ap controller ip address 192.168.1.10
WLC(config)# capwap dtls enable # DTLS şifrelemeyi aktifleştir
AP(config)# capwap ap controller ip address 192.168.1.10
AP(config)# capwap dtls enable
```

## 4. WLAN Operasyonu

**KRİTİK BİLGİ:** WLAN'lar yarı çift yönlüdür ve çarpışma tespit edilemez. CSMA/CA protokolü kullanılır.

### Kablosuz Topoloji Modları

Mod	Açıklama
Ad hoc	AP olmadan eşler arası iletişim
Infrastructure	AP kullanarak ağa bağlanma
Tethering	Mobil cihazın kişisel hotspot olması
Mesh	Çoklu AP'lerin otomatik ağ oluşturması

### CSMA/CA Süreci

- Kanal boş mu kontrol et
- RTS (Göndermeye Hazır) mesajı gönder
- CTS (Gönderebilirsin) mesajını bekle
- Veriyi gönder
- ACK alındı onayı

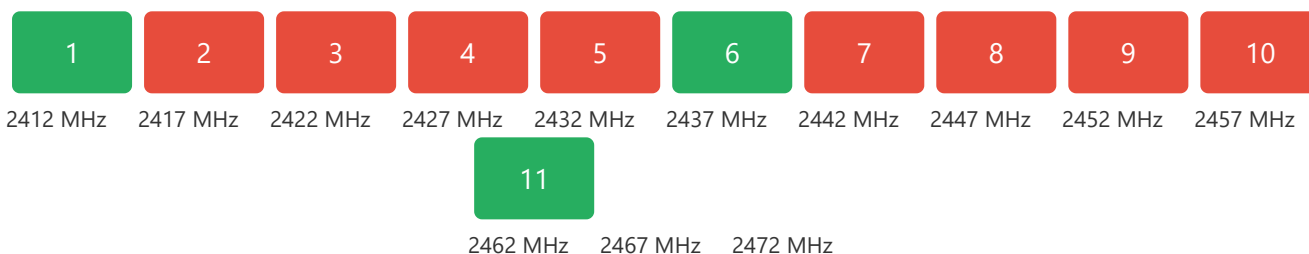
### Band Steering Konfigürasyonu

```
WLC(config)# band-select enable # Band Steering aktifleştir
WLC(config)# band-select probe-cycle 2 # Prob sayısı
WLC(config)# band-select expiry 60 # Zaman aşımı (saniye)
```

## 5. Kanal Yönetimi

**KANAL ÇAKIŞMASI:** Komşu kanalların üst üste binmesi performans düşüşüne neden olur.

### 2.4 GHz Kanal Planlaması



**Önerilen kanallar:** 1, 6, 11 (veya bölgeye göre 13)

### 5 GHz Kanal Planlaması



## Kanal Geniřlięi Ayarlama

```
AP(config)# interface Dot11Radio0
AP(config-if)# channel 36 # Kanal numarası
AP(config-if)# channel width 80 # 80 MHz genişlik (802.11ac)
AP(config-if)# power local 12 # Güç seviyesi (dBm)
```

## 6. WLAN Güvenlięi

**GÜVENLİK UYARISI:** WEP artık güvenli kabul edilmiyor, WPA3 kullanılması önerilir.

### Kimlik Doğrulama Yöntemleri

Yöntem	Güvenlik	Öneri
WEP	Çok düşük	Kullanmayın
WPA	Düşük	TKIP şifreleme
WPA2	Yüksek	AES şifreleme
WPA3	Çok yüksek	SAE kimlik doğrulama

### WPA2/WPA3 Konfigürasyonu

```
AP(config)# dot11 ssid SECURE-NET
AP(config-ssid)# authentication wpa2 psk aes # WPA2-PSK AES
AP(config-ssid)# wpa-psk ascii STR0ngP@ssw0rd # Paylaşılan anahtar

# WPA3 için:
AP(config-ssid)# authentication wpa3 psk
AP(config-ssid)# wpa3 sae
```

### Kurumsal Güvenlik

```
AP(config)# aaa new-model
AP(config)# aaa authentication login default group radius
AP(config)# radius-server host 192.168.1.50
AP(config)# radius-server key SECR3T-K3Y
```

## 7. WLAN Tehditleri ve Korunma

**TEHDİT:** Rogue AP'ler (yetkisiz erişim noktaları) ağ güvenlięi için büyük risk oluşturur.

## Yaygın Tehditler

- **Veri Ele Geçirme:** Şifrelenmemiş trafiğin dinlenmesi
- **Kablosuz Sızma:** Yetkisiz erişim
- **Hizmet Engelleme (DoS):** Kanal hataları veya kasıtlı saldırılar
- **Rogue AP:** Yetkisiz erişim noktaları
- **Ortadaki Adam (MITM):** "Evil Twin" AP saldırıları

## Korunma Yöntemleri

Tehdit	Korunma
Veri Ele Geçirme	WPA3/AES şifreleme
Kablosuz Sızma	802.1X kimlik doğrulama
DoS Saldırıları	Cihaz güvenliği, güncellemeler
Rogue AP	Rogue AP politikaları, izleme
MITM Saldırıları	Kimlik doğrulama, anormal trafik izleme

## Rogue AP Tespiti

```
WLC(config)# wids rogue ap detect # Rogue AP tespitini aktifleştir
WLC(config)# wids rogue ap alert # Alarm ayarla
WLC# show wids rogue ap # Tespit edilen Rogue AP'leri göster
```

## 8. İleri WLAN Özellikleri

### Wi-Fi 6E (6 GHz Bandı)

- 1200 MHz ek spektrum
- 59 yeni kanal (20 MHz genişlikte)
- Düşük gecikme, yüksek kapasite
- Otomatik Frekans Koordinasyonu (AFC)

## Mesh Ağ Konfigürasyonu

```
AP(config)# dot11 mesh-backhaul
AP(config)# mesh root # Root AP tanımlama
AP(config)# mesh parent 1 # Parent AP belirleme
```

## QoS ve Trafik Şekillendirme

```
AP(config)# priority-queue out # Öncelik kuyruğu
AP(config)# wlan qos silver # QoS profili ata
AP(config)# bandwidth 5000 # Bant genişliği sınırı (Kbps)
```

## 9. IoT Güvenliđi ve Cihaz Onboarding

IoT cihazları için DPP (Device Provisioning Protocol), WPS'nin güvenlik açıklarını giderir.

### IoT Onboarding Süreci

1. Cihaz QR kodunu gösterir
2. Mobil uygulama QR kodu okur
3. Wi-Fi ağ bilgileri cihaza aktarılır
4. Cihaz ağa güvenli şekilde bağlanır

### WPA3 IoT Özellikleri

- **WPA3-Personal:** SAE ile brute-force saldırılarına karşı koruma
- **WPA3-Enterprise:** 192-bit kriptografik paket
- **Açık Ağlar:** OWE ile tüm trafiğin şifrlenmesi
- **IoT Onboarding:** DPP ile hızlı entegrasyon

**SON UYARI:** Tüm kablosuz ağlarda WPA3 kullanın, WEP ve WPA'dan kaçının. Düzenli güvenlik denetimleri yapın.