# MUH442 Bilişimde Güvenlik – 2

Prof. Dr. Hasan Hüseyin BALIK

(13. Hafta)

# İçerik

- 4.Ağ güvenliği
  - 4.1. İnternet Güvenlik Protokolleri ve Standartları
  - 4.2.İnternet Kimlik Doğrulama Uygulamaları
  - 4.3. Kablosuz Ağ Güvenliği

# 4.3. Kablosuz Ağ Güvenliği

# 4.3.İçerik

- Kablosuz Ağ Güvenliğene Genel Bakış
- Mobil Cihaz Güvenliği
- IEEE 802.11 Kablosuz LAN'a Genel Bakış
- IEEE 802.11i Kablosuz LAN Güvenliği

# Kablosuz Ağ Güvenliği

- Kablolu ağlara kıyasla kablosuz ağların daha yüksek güvenlik riskine katkıda bulunan temel faktörler şunlardır:
  - **Kanal**
    - Kablosuz ağ, tipik olarak, kablolu ağlara göre dinleme ve parazite karşı çok daha hassas olan yayın iletişimlerini içerir.
    - Kablosuz ağlar ayrıca iletişim protokollerindeki güvenlik açıklarından yararlanan aktif saldırılara karşı daha savunmasızdır.
  - **Hareketlilik**
    - Kablosuz cihazlar çok daha taşınabilir ve mobildir, dolayısıyla bir takım risklere yol açar.
  - **Kaynaklar**
    - Akıllı telefonlar ve tabletler gibi bazı kablosuz cihazlar, gelişmiş işletim sistemlerine sahiptir, ancak hizmet reddi ve kötü amaçlı yazılım da dahil olmak üzere tehditlere karşı koymak için sınırlı bellek ve işlem kaynaklarına sahiptir.
  - **Ulaşılabilirlik**
    - Sensörler ve robotlar gibi bazı kablosuz cihazlar, uzak ve/veya düşmanca konumlarda gözetimsiz bırakılabilir ve böylece fiziksel saldırılara karşı savunmasızlıkları büyük ölçüde artar.

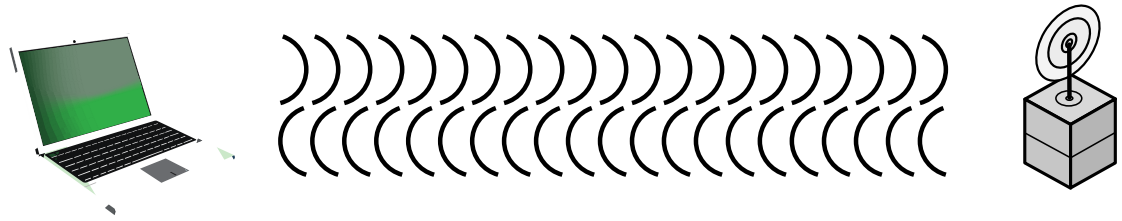



**Figure 24.1 Wireless Networking Components**

# Kablosuz Ağ Tehditleri

- Yanlışlıkla bağlanma
- Kötü niyetli bağlanma
- Ad hoc (Özel) ağlar
- Geleneksel olmayan ağlar
- Kimlik hırsızlığı (MAC sahtekarlığı)
- Ortadaki adam saldırıları
- Hizmet reddi (DoS)
- Ağ enjeksiyonu

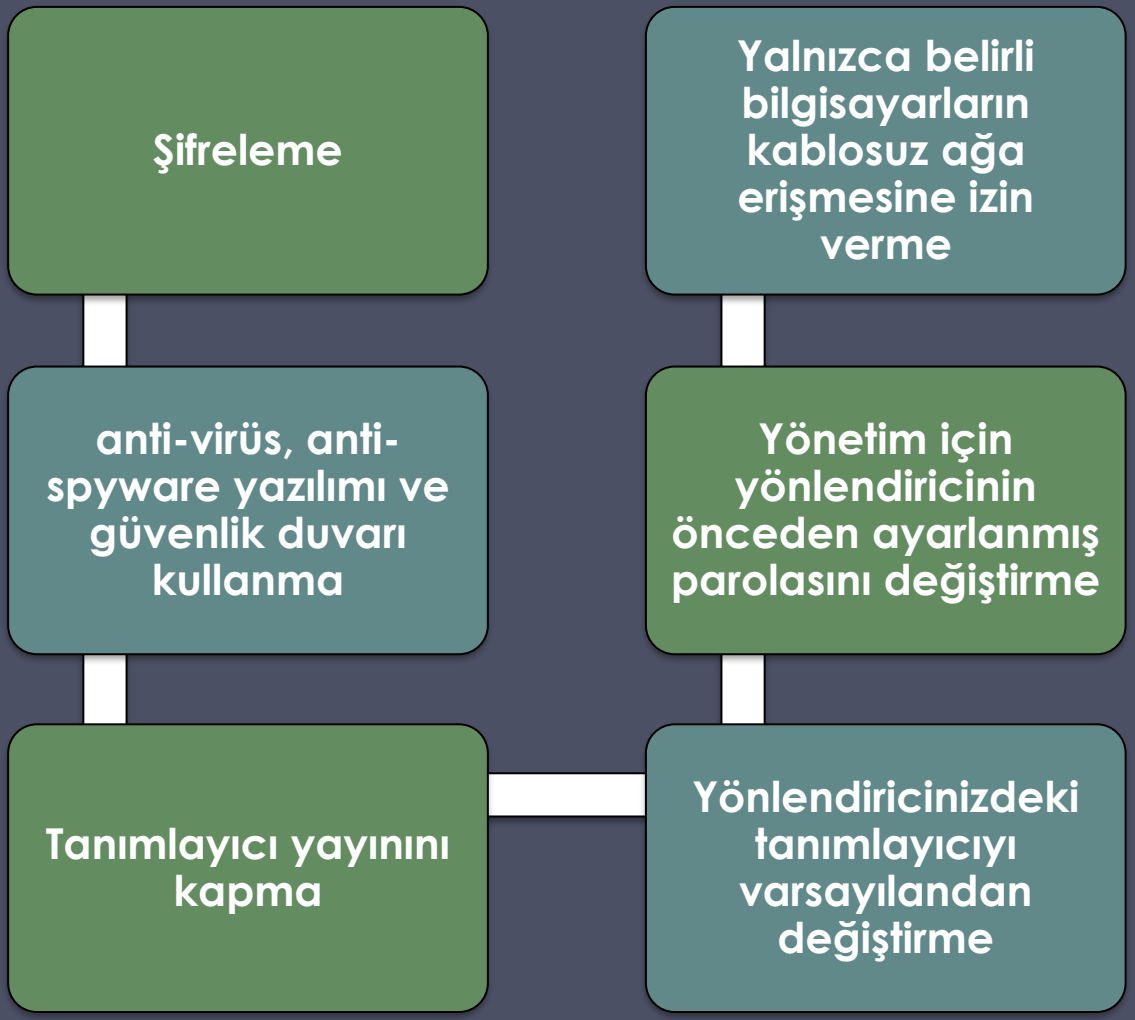
# Kablosuz İletimi Güvenli Hale Getirme

- Başlıca tehditler, gizli dinleme, mesajları değiştirme veya ekleme ve kesintidir.
- Gizli dinleme karşı önlemler:
  - Sinyal gizleme teknikleri
  - şifreleme
- Şifreleme ve kimlik doğrulama protokollerinin kullanılması, iletimleri değiştirme veya ekleme girişimlerine karşı koymanın standart yöntemidir.

# Kablosuz Ağların Güvenliğini Sağlama

- Kablosuz erişim noktalarına ana tehdit, ağa yetkisiz erişimdir.
- Bu tür erişimi engellemeye yönelik temel yaklaşım, bağlantı noktası tabanlı ağ erişim kontrolü (IEEE 802.1X standardı) kullanmakdır.
  - Standart, bir LAN veya kablosuz ağa bağlanmak isteyen cihazlar için bir kimlik doğrulama mekanizması sunar.
- 802.1X kullanımı, hileli erişim noktalarının ve diğer yetkisiz cihazların güvenli olmayan arka kapılar haline gelmesini önleyebilir

# Kablosuz Ağ Güvenlik Teknikleri



# Mobil Cihaz Güvenliği

- Bir kuruluşun ağları aşağıdakilee uyum sağlamalıdır:
  - **Yeni cihazların artan kullanımı**
    - Çalışanların mobil cihaz kullanımında önemli artış
  - **Bulut tabanlı uygulamalar**
    - Uygulamalar artık yalnızca kurumsal veri merkezlerindeki fiziksel sunucularda çalışmıyor
  - **Çevreyi kaldırma (Deperimeterization)**
    - Yeni cihazların çoğalması, uygulama mobilitesi ve bulut tabanlı tüketici ve kurumsal hizmetler göz önüne alındığında, statik ağ çevresi kavramı neredeyse tamamen ortadan kalktı
    - Kullanıcı rolü, cihaz türü, sunucu sanallaştırma hareketliliği, ağ konumu ve günün saati gibi çeşitli çevresel koşullara uyum sağlamaları gerektiğinden bu çevre ölçüleri dinamik olmalıdır
  - **Harici iş gereksinimleri**
    - Kuruluş ayrıca konuklara, üçüncü taraf yüklenicilere ve iş ortaklarına çok sayıda konumdan çeşitli cihazları kullanarak ağ erişimi sağlamalıdır

# Mobil Cihaz Güvenlik Tehditleri

- Fiziksel güvenlik kontrollerinin olmaması
- Güvenilmeyen ağların kullanımı
- Güvenilmeyen mobil cihazların kullanımı
- Güvenilmeyen uygulamaların kullanımı
- Diğer sistemlerle etkileşim
- Güvenilmeyen içerik kullanımı
- Konum hizmetlerinin kullanımı

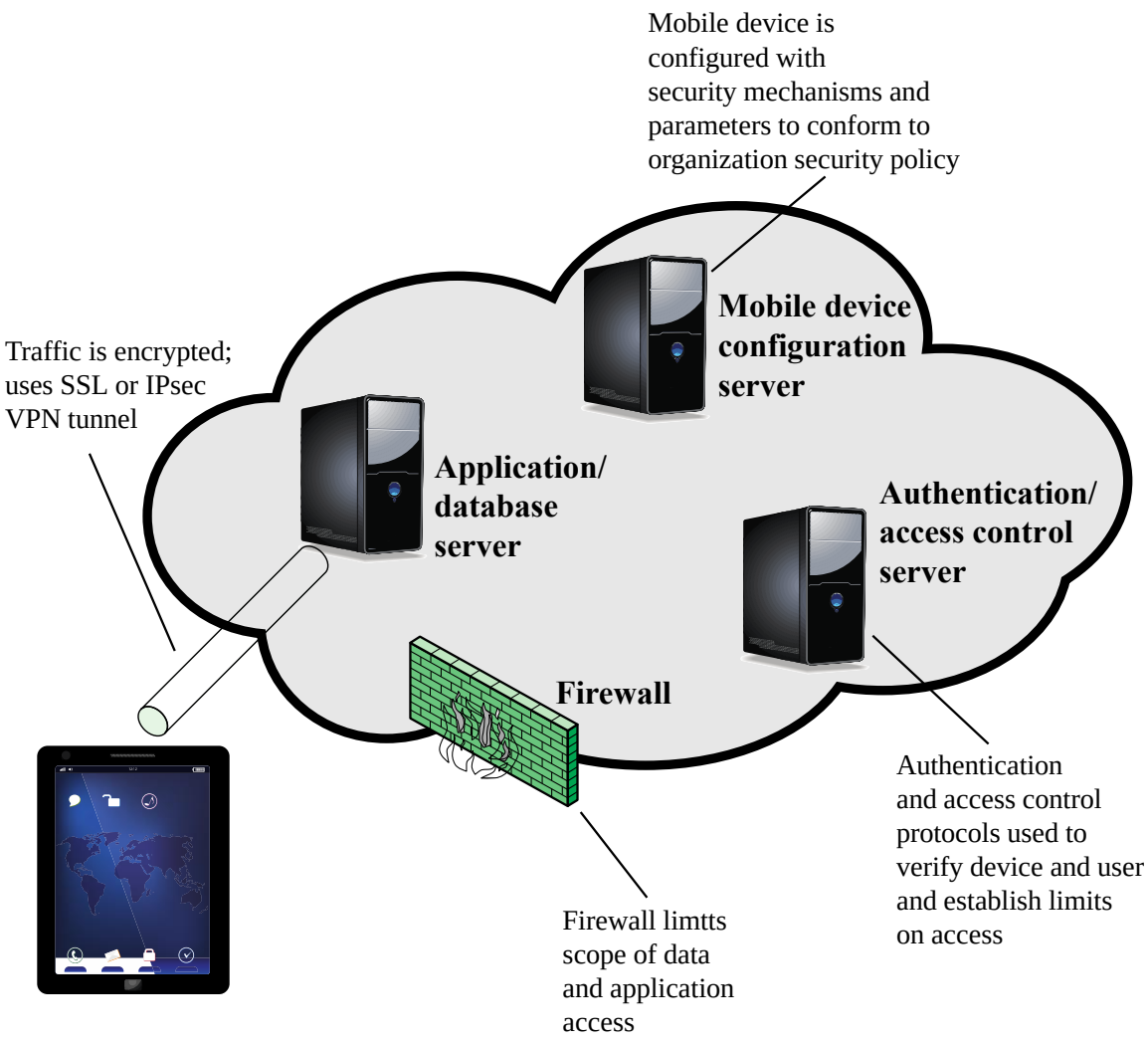



**Figure 24.2 Mobile Device Security Elements**

# IEEE 802.11 Terminoloji

| | |
|---|---|
| Erişim noktası (AP) | İstasyon işlevselliğine sahip olan ve ilişkili istasyonlar için kablosuz ortam aracılığıyla dağıtım sistemine erişim sağlayan herhangi bir varlık |
| Temel hizmet seti (BSS) | Tek bir koordinasyon işlevi tarafından kontrol edilen bir dizi istasyon |
| Koordinasyon işlevi | Bir BSS içinde çalışan bir istasyonun PDU'ları iletmesine ve almasına ne zaman izin verileceğini belirleyen mantıksal işlev |
| Dağıtım sistemi (DS) | Bir ESS oluşturmak için bir dizi BSS'yi ve entegre LAN'ları birbirine bağlamak için kullanılan bir sistem |
| Genişletilmiş hizmet seti (ESS) | Bu BSS'lerden biriyle ilişkili herhangi bir istasyonda LLC katmanına tek bir BSS olarak görünen bir veya daha fazla birbirine bağlı BSS'ler ve entegre LAN'lar kümesi |
| MAC protokolü veri birimi (MPDU) | Fiziksel katmanın hizmetlerini kullanarak iki eş MAC varlığı arasında değiş tokuş edilen veri birimi |
| MAC servis veri birimi (MSDU) | MAC kullanıcıları arasında bir birim olarak iletilen bilgiler |
| İstasyon | IEEE 802.11 uyumlu MAC ve fiziksel katman içeren herhangi bir cihaz |

# Kablosuz Uygunluk Birliği (Wireless Fidelity-Wi-Fi Alliance)

- 802.11b
  - Sektörde geniş kabul gören ilk 802.11 standardıdır
- Kablosuz Ethernet Uyumluluk Birliği (WECA)
  - 1999'da, farklı satıcılardan gelen ürünlerin başarılı bir şekilde birlikte çalışması endişesini gidermek için kurulan endüstri konsorsiyumudur
  - Daha sonra Wi-Fi Alliance olarak yeniden adlandırılmıştır
- Sertifikalı 802.11b ürünleri için kullanılan terim:*Wi-Fi*
  - 802.11g ürünlerini içerecek şekilde genişletildi
- Wi-Fi Korumalı Erişim (WPA)
  - IEEE802.11 güvenlik standartları için Wi-Fi Alliance sertifika prosedürleridir
  - WPA2, IEEE802.11i WLAN güvenlik özelliğinin tüm spefikasyonlarını içerir

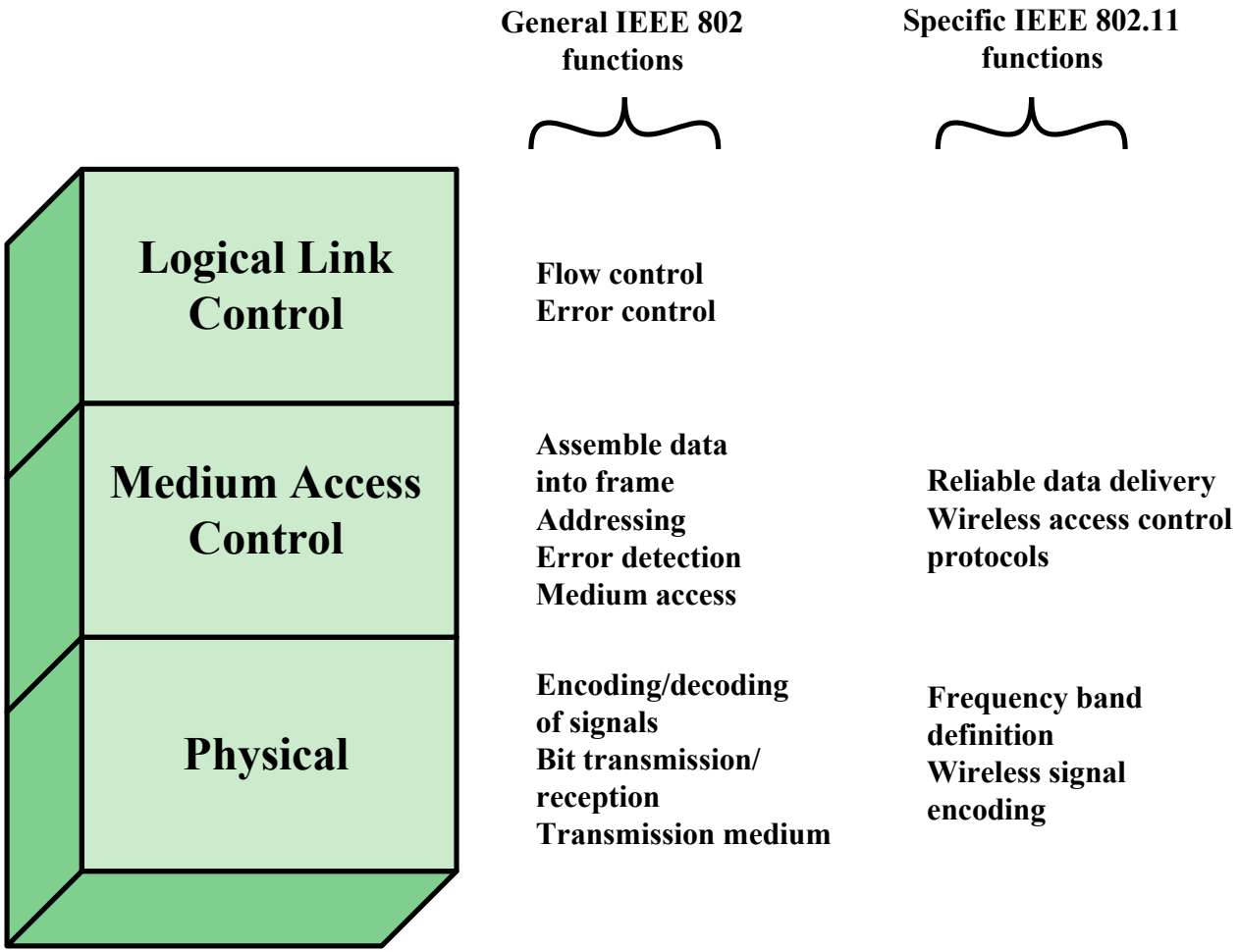



**Figure 24.3 IEEE 802.11 Protocol Stack**


**Figure 24.4 General IEEE 802 MPDU Format**

MPDU: MAC protokolü veri birimi

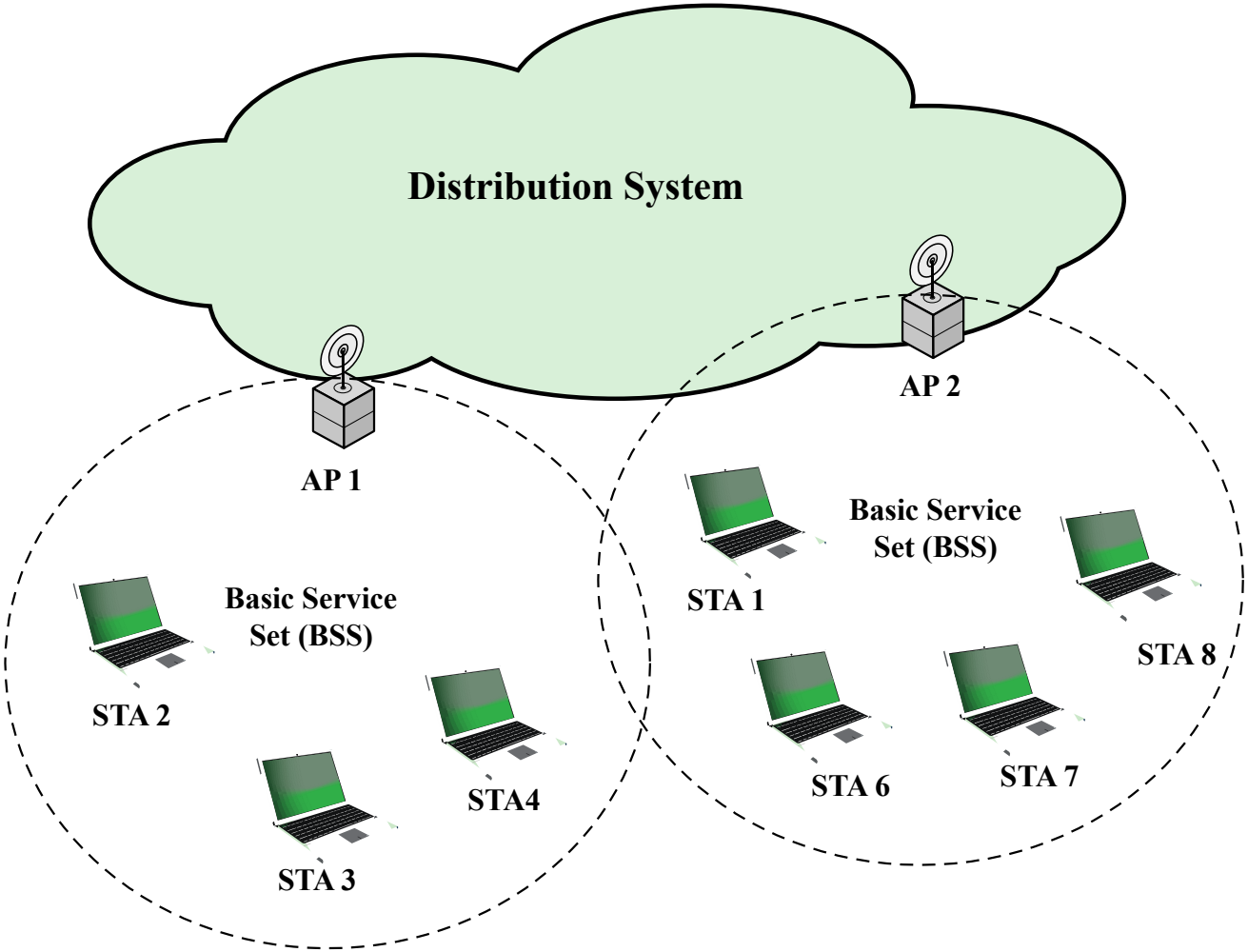



**Figure 24.5 IEEE 802.11 Extended Service Set**

# IEEE 802.11 Servisleri

| Servis | Sağlayıcı | Destek için Kullanım |
|---|---|---|
| İlişkilendirme | Dağıtım sistemi | MSDU dağıtımı |
| Kimlik doğrulama | İstasyon | LAN erişimi ve güvenliği |
| Yetkisizlendirme | İstasyon | LAN erişimi ve güvenliği |
| Ayrışma | Dağıtım sistemi | MSDU dağıtımı |
| Dağitim | Dağıtım sistemi | MSDU dağıtımı |
| Entegrasyon | Dağıtım sistemi | MSDU dağıtımı |
| MSDU dağıtımı | İstasyon | MSDU dağıtımı |
| Gizlilik | İstasyon | LAN erişimi ve güvenliği |
| Yeniden ilişkilendirme | Dağıtım sistemi | MSDU dağıtımı |

# Mesajların DS İçinde Dağıtımı

- Bir DS içindeki mesajların dağıtımıyla ilgili iki hizmet şunlardır:
  - Dağıtım
  - Entegrasyon

## Dağıtım

- MPDU'ların bir BSS'deki bir istasyondan başka bir BSS'deki bir istasyona gitmek için DS'yi geçmesi gerektiğinde MPDU'ları değiş tokuş etmek için istasyonlar tarafından kullanılan birincil hizmettir

## Entegrasyon

- IEEE 802.11 LAN üzerindeki bir istasyon ile entegre IEEE 802x LAN üzerindeki bir istasyon arasında veri aktarımı sağlar
- Hizmet, IEEE 802.11 LAN üzerindeki bir istasyon ile entegre IEEE 802.x LAN üzerindeki bir istasyon arasında veri aktarımı sağlar

# Bağlantı ile ilişkili Servisler

- Hareketliliğe dayalı geçiş türleri:
  - Geçiş yok
    - Bu tür bir istasyon ya durağandır ya da yalnızca tek bir BSS'nin iletişim kuran istasyonlarının doğrudan iletişim menzili içinde hareket eder.
  - BSS geçişi
    - Aynı ESS içinde bir BSS'den başka bir BSS'ye istasyon hareketi; Verilerin istasyona teslimi, adresleme yeteneğinin istasyonun yeni konumunu tanıyabilmesini gerektirir
  - ESS geçişi
    - Bir ESS'deki BSS'den başka bir ESS içindeki BSS'ye istasyon hareketi; 802.11 tarafından desteklenen üst katman bağlantılarının bakımı garanti edilemez

# Hizmetler

**Bağlantı**

- Bir istasyon ve bir AP arasında bir başlangıç ilişkisi kurar

**Yeniden bağlantı**

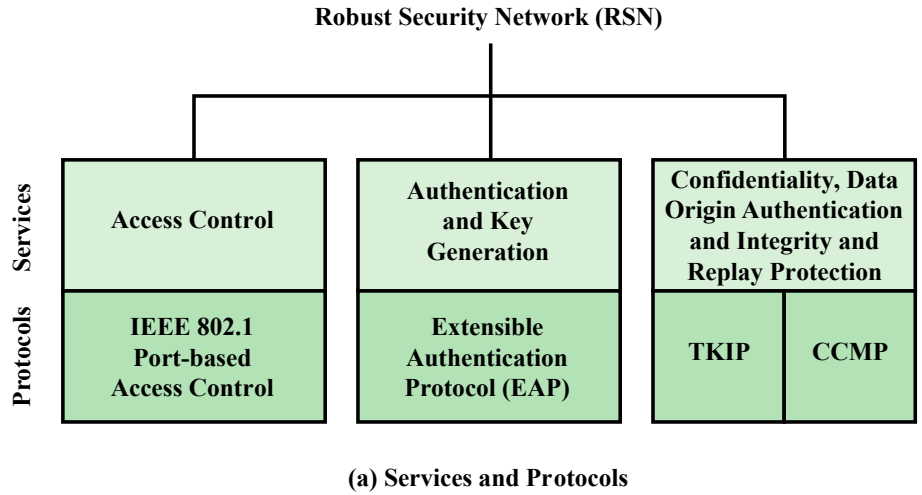
- Yerleşik bir ilişkinin bir AP'den diğerine aktarılmasını sağlayarak bir mobil istasyonun bir BSS'den diğerine geçmesine izin verir

**Ayrışma**

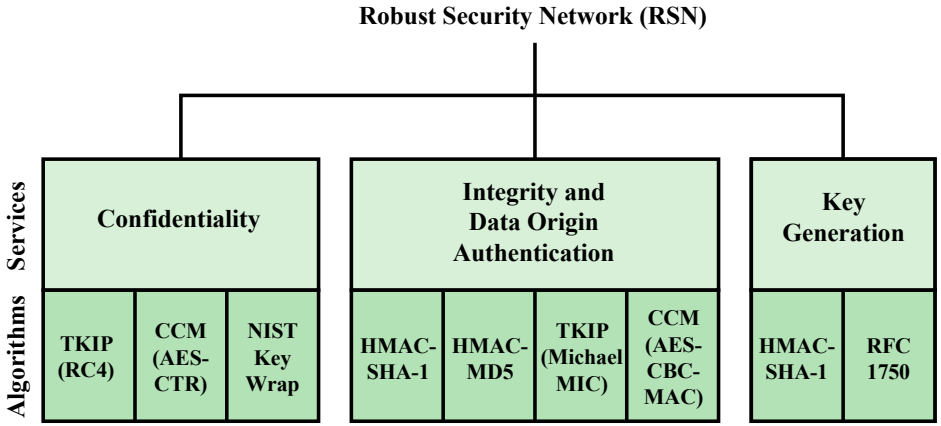
- Bir istasyondan veya bir AP'den mevcut bir ilişkinin sonlandırıldığına dair bir bildirimdir

# Kablosuz LAN Güvenliği

- Kabloluya Eşdeğer Gizlilik (Wired Equivalent Privacy - WEP) algoritması
  - 802.11 gizliliği
- Wi-Fi Korumalı Erişim (WPA)
  - 802.11 güvenlik sorunlarının çoğunu ortadan kaldıran ve 802.11i standardının mevcut durumunu temel alan bir dizi güvenlik mekanizması
- Güçlü Güvenlik Ağı (RSN)
  - 802.11i standardının son halidir
- Wi-Fi Alliance, satıcıları WPA2 programı kapsamında tam 802.11i spesifikasyonuna uygun olarak onaylar




(a) Services and Protocols




(b) Cryptographic Algorithms

CBC-MAC = Cipher Block Block Chaining Message Authentication Code (MAC)
CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol

**Figure 24.6 Elements of IEEE 802.11i**

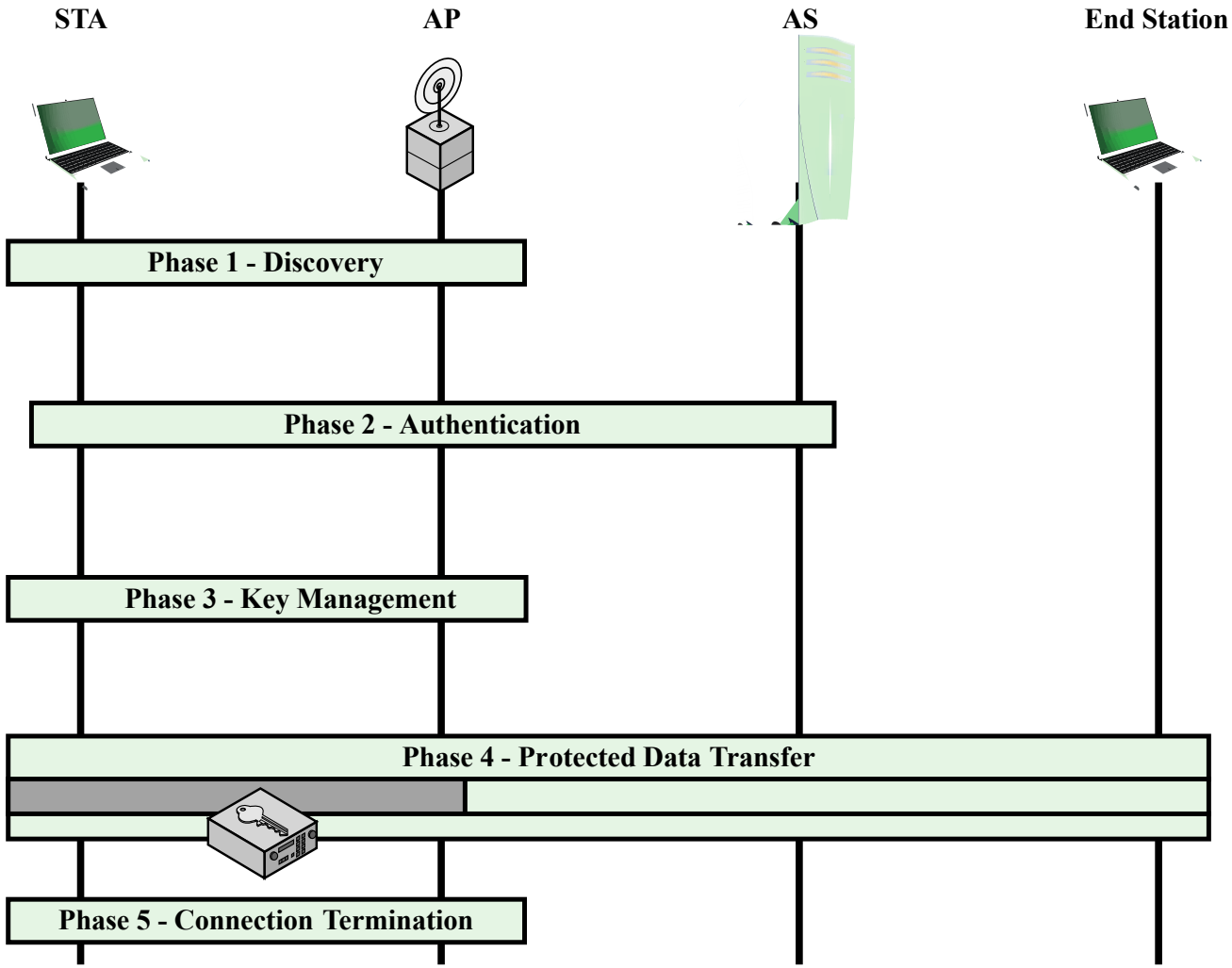



**Figure 24.7 IEEE 802.11i Phases of Operation**

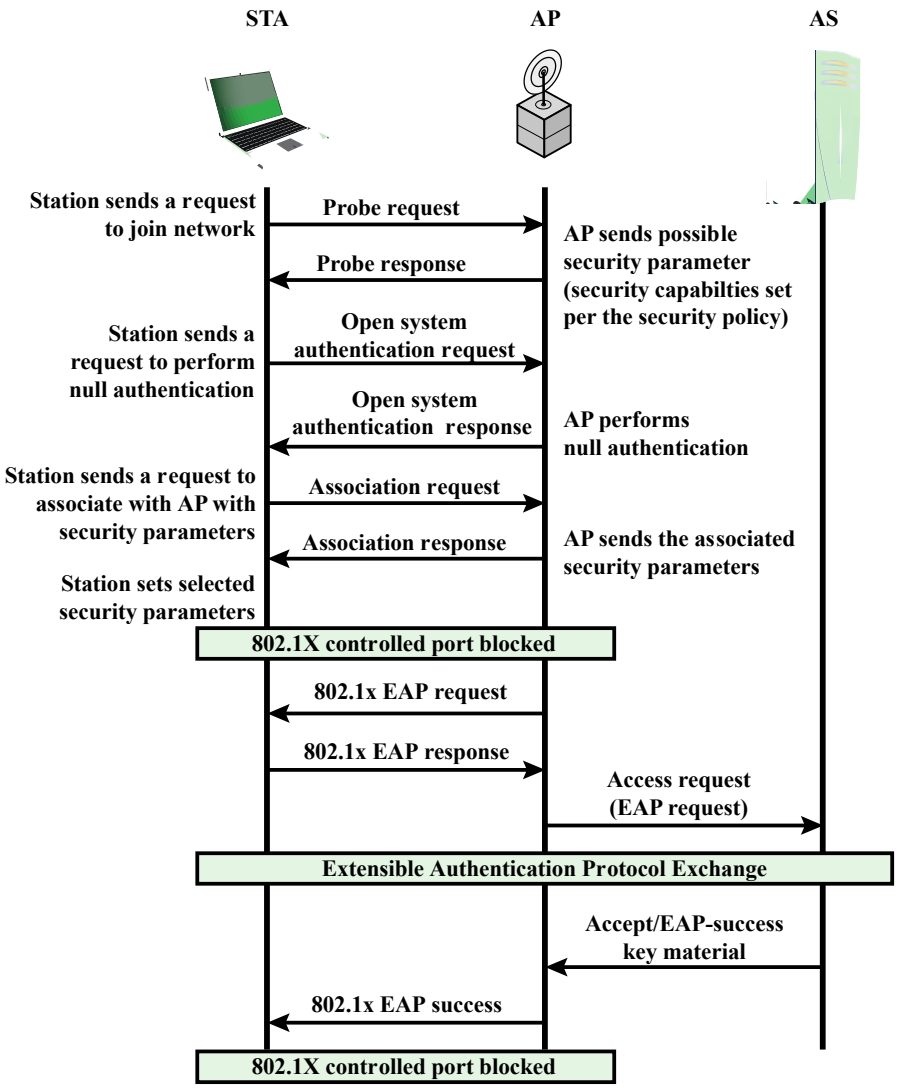



**Figure 24.8 IEEE 802.11i Phases of Operation: Capability Discovery, Authentication, and Association**

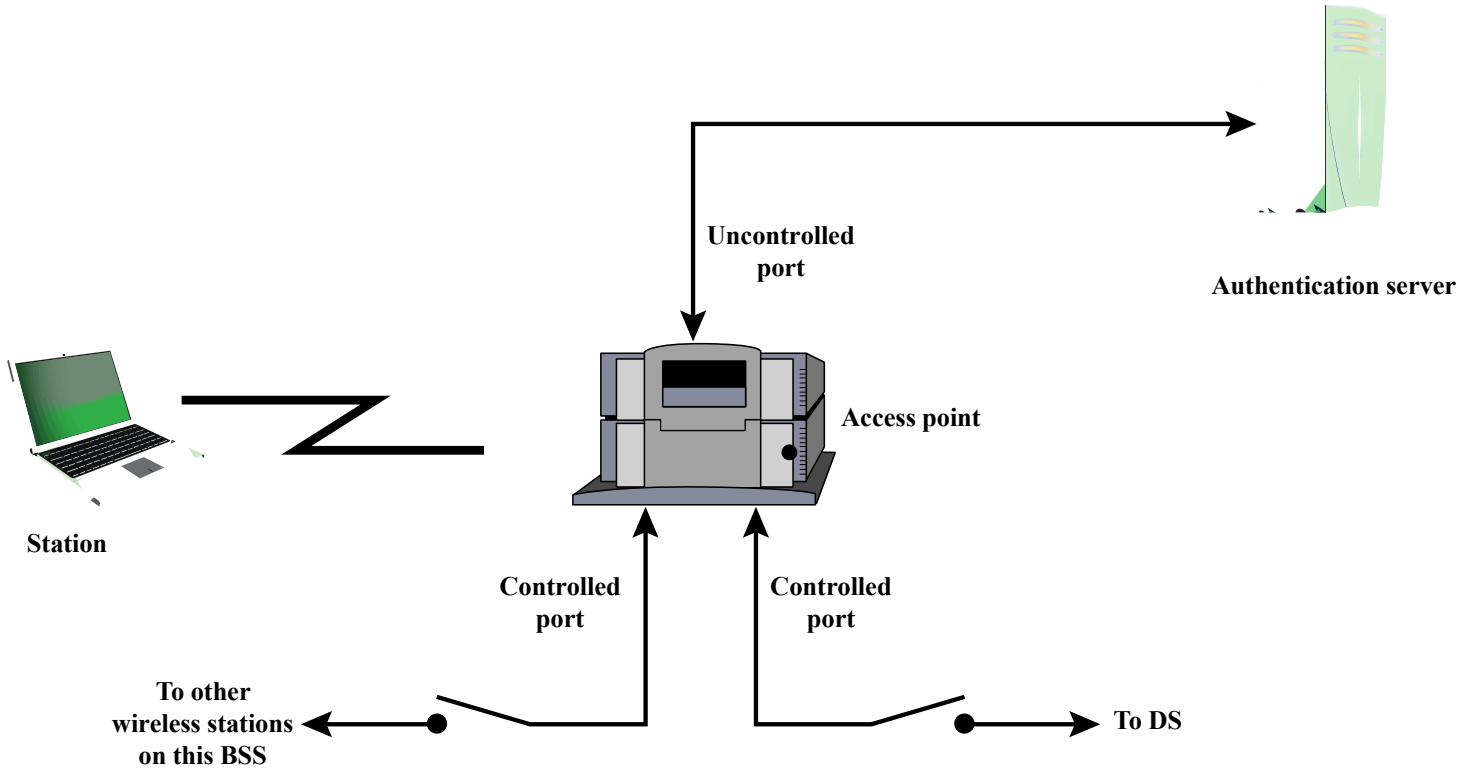
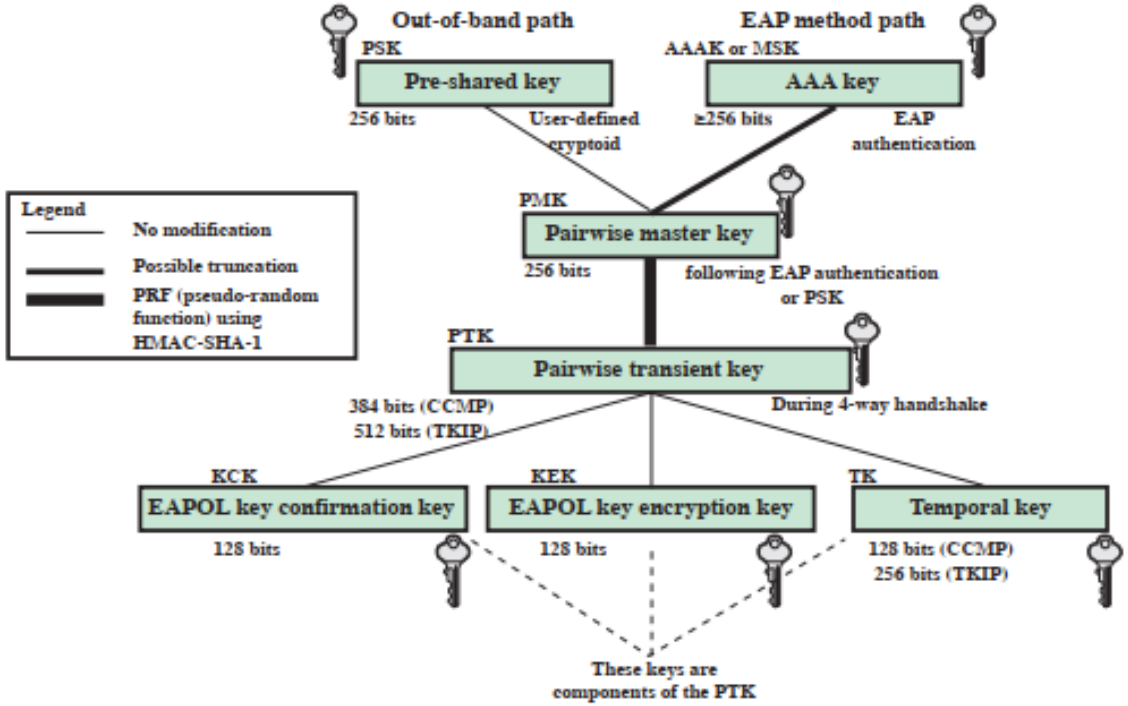


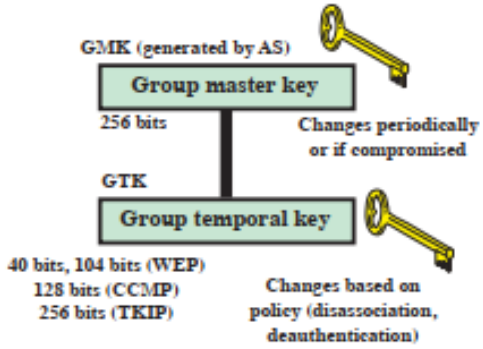

**Figure 24.9 802.1X Access Control**

# MPDU Değişimi

- Kimlik doğrulama fazı üç aşamadan oluşur:
  - AS'ye bağlantı
    - STA, AP'sine AS'ye bağlantı için bir ilişkisi olduğu yönünde bir istek gönderir; AP bu talebi kabul eder ve AS'ye bir erişim talebi gönderir.
  - EAP (Extensible Authentication Protocol) değişimi
    - STA ve AS'yi birbirlerine doğrular
  - Güvenli anahtar teslimi
    - Kimlik doğrulama sağlandıktan sonra, AS bir ana oturum anahtarı oluşturur ve bunu STA'ya gönderir.




(a) Pairwise key hierarchy




(b) Group key hierarchy

**Figure 24.10 IEEE 802.11i Key Hierarchies**

# Veri Gizliliği ve Bütünlük Protokolleri için IEEE 802.11i Anahtarları (1/2)

| Kısaltma | İsim | Açıklama/Amaç | Boyut (bit) | Tip |
|---|---|---|---|---|
| AAAKey | Kimlik Doğrulama, Hesaplama ve Yetkilendirme Anahtarı | PMK'yı türetmek için kullanılır. IEEE 802.1X kimlik doğrulaması ve anahtar yönetimi yaklaşımıyla kullanılır. MMSK ile aynı | ≥256 | Anahtar oluşturma anahtarı, kök anahtar |
| PSK | Ön Paylaşımlı Anahtar | Önceden paylaşılan anahtar ortamlarda PMK olur | 256 | Anahtar oluşturma anahtarı, kök anahtar |
| PMK | İkili Ana Anahtar | PTK'yı türetmek için diğer girişlerle birlikte kullanılır | 256 | Anahtar oluşturma anahtarı |
| GMK | Grup Ana Anahtarı | GTK'yı türetmek için diğer girişlerle birlikte kullanılır | 128 | Anahtar oluşturma anahtarı |
| PTK | İkili Geçiş Anahtarı | PMK'dan türetilmiştir. EAPOL-KCK, EAPOL-KEK ve TK ve (TKIP için) MIC anahtarından oluşur | 512 (TKIP) 384 (CCMP) | Bileşik anahtar |

# Veri Gizliliği ve Bütünlük Protokolleri için IEEE 802.11i Anahtarları (2/2)

| Kısaltma | İsim | Açıklama/Amaç | Boyut (bit) | Tip |
|---|---|---|---|---|
| TK | Geçici Anahtar | Tek noktaya yayın kullanıcı trafiği için gizlilik ve bütünlük koruması sağlamak üzere TKIP veya CCMP ile birlikte kullanılır | 256 (TKIP) 128 (CCMP) | Trafik anahtarı |
| GTK | Grup Geçici Anahtarı | GMK'dan türetilmiştir. Çok noktaya yayın/yayın kullanıcı trafiği için gizlilik ve bütünlük koruması sağlamak için kullanılır | 256 (TKIP) 128 (CCMP) 40,104 (WEP) | Trafik anahtarı |
| MIC Key | Mesaj Bütünlüğü Kod Anahtarı | Mesajların bütünlük koruması sağlamak için TKIP'nin Michael MIC'si tarafından kullanılır | 64 | Mesaj bütünlüğü anahtarı |
| EAPOL-KCK | EAPOL Anahtarı Onay Anahtarı | 4'lü el sıkışma sırasında dağıtılan temel malzeme için bütünlük koruması sağlamak için kullanılır. | 128 | Mesaj bütünlüğü anahtarı |
| EAPOL-KEK | EAPOL Anahtarı Şifreleme Anahtarı | 4'lü el sıkışmada GTK ve diğer anahtar materyallerin gizliliğini sağlamak için kullanılır | 128 | Trafik anahtarı/ anahtar şifreleme anahtarı |
| WEP Key | Kablolu Eşdeğer Gizlilik Anahtarı | WEP ile kullanılır | 10,104 | Trafik anahtarı |

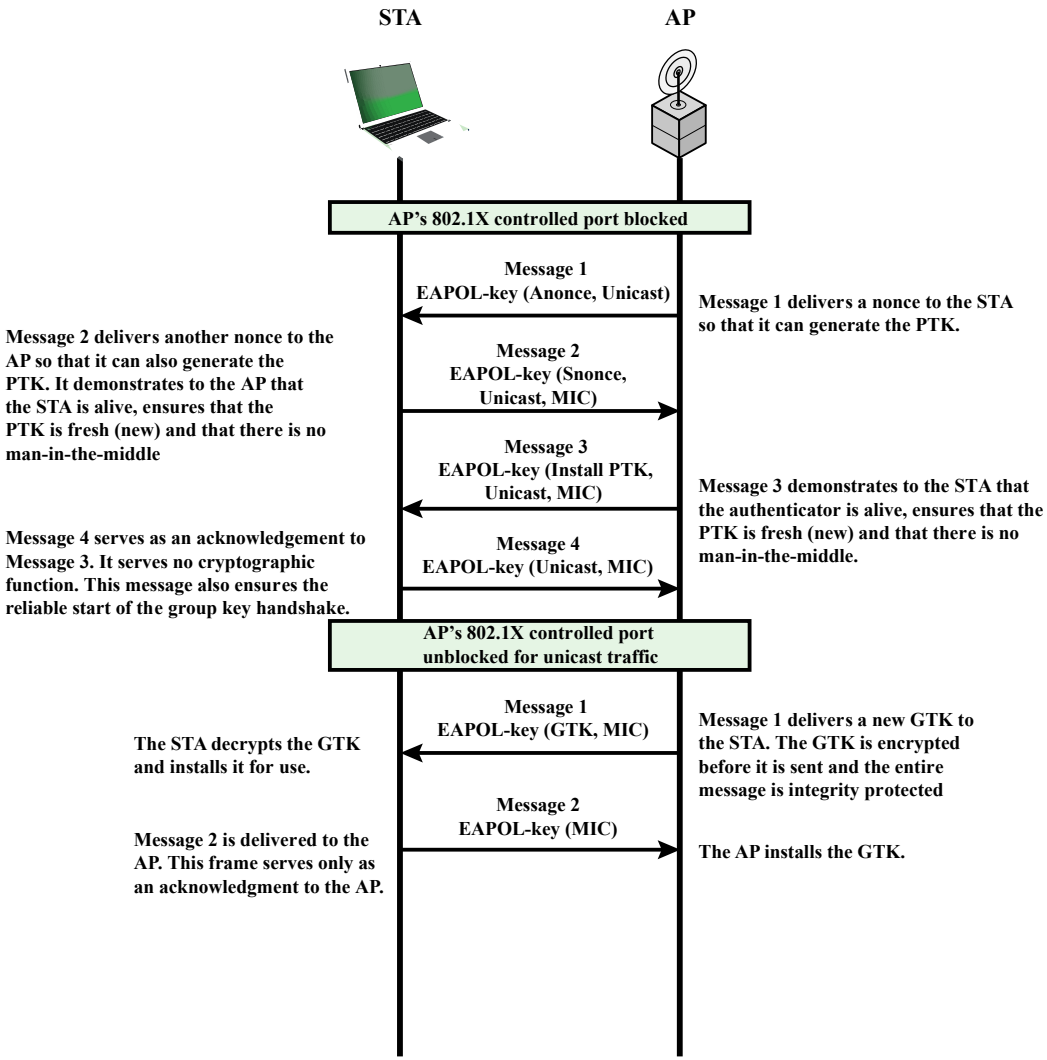



**Figure 24.11 IEEE 802.11i Phases of Operation: Four-Way Handshake and Group Key Handshake**

# Geçici Anahtar Bütünlüğü Protokolü (TKIP)

- Cihazlarda yalnızca WEP adı verilen eski kablosuz LAN güvenlik yaklaşımıyla uygulanan yazılım değişikliklerini gerektirecek şekilde tasarlanmıştır
- İki hizmet sunar:

**Mesaj bütünlüğü**

Veri alanından sonra 802.11 MAC framine bir mesaj bütünlük kodu ekler

**Veri gizliliği**

MPDU şifrelenerek sağlanır

# Sayaç Modu-CBC MAC Protokolü (CCMP)

- Bu şemayı destekleyecek donanıma sahip daha yeni IEEE 802.11 aygıtları için tasarlanmıştır

- İki hizmet sunar:

**Mesaj bütünlüğü**

Blok zincir şifreleme mesaj kimlik doğrulama kodunu (CBC-MAC) kullanır

**Veri gizliliği**

Şifreleme için AES ile CTR blok şifreleme çalışma modunu kullanır

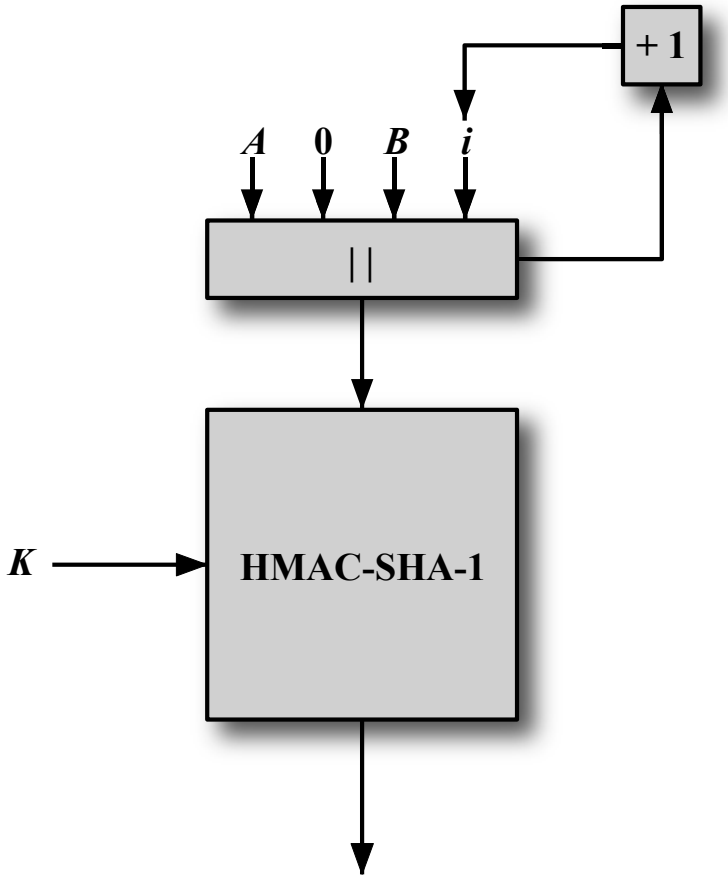



**Figure 24.12 IEEE 802.11i Pseudorandom Function**