BİLGİSAYAR AĞLARI

Wimax

060201024 Enes ÇAĞLAR
060201047 Şeyda

İçindekiler

- Wimax Nedir?
- Wimax Uygulama Alanları
- Wimax Genel Yapısı
- Wimax'in Avantajları
- Wimax'in Sağladığı Faydalar
- Wimax ve WiFi
- IEEE 802.16 iletişim Türleri
- Wimax Katmansal Analiz
    - Fiziksel Katman
    - Mac Katmanı
- 802.16 Güvenlik Standardı
    - WiMAX Güvenlik Altyapısı
    - Veri güvenliği
    - Güvenlik yönetimi
    - WiMAX Ağ(Mesh) Yapısında Güvenlik

2/30

WiMAX (1/2)

- Worldwide Interopability for Microwave Access
- IEEE 802.16-IEEE 802 serisinin 16 nolu kolu
- IEEE 802.16: Telsiz Kentsel alan ağı standardı (Wireless MAN),(1999).
- 802.16 standardını destekleyen uç birimlere telsiz alanda yüksek bandgenişliği (BWA) sağlamayı amaçlayan bir forumun standardı (2001).
- WiFi'nin çok daha büyük ve çok daha güçlü versiyonu
- WiFi gibi yüksek hızda kablosuz internet bağlantısı sunan tenolojidir.

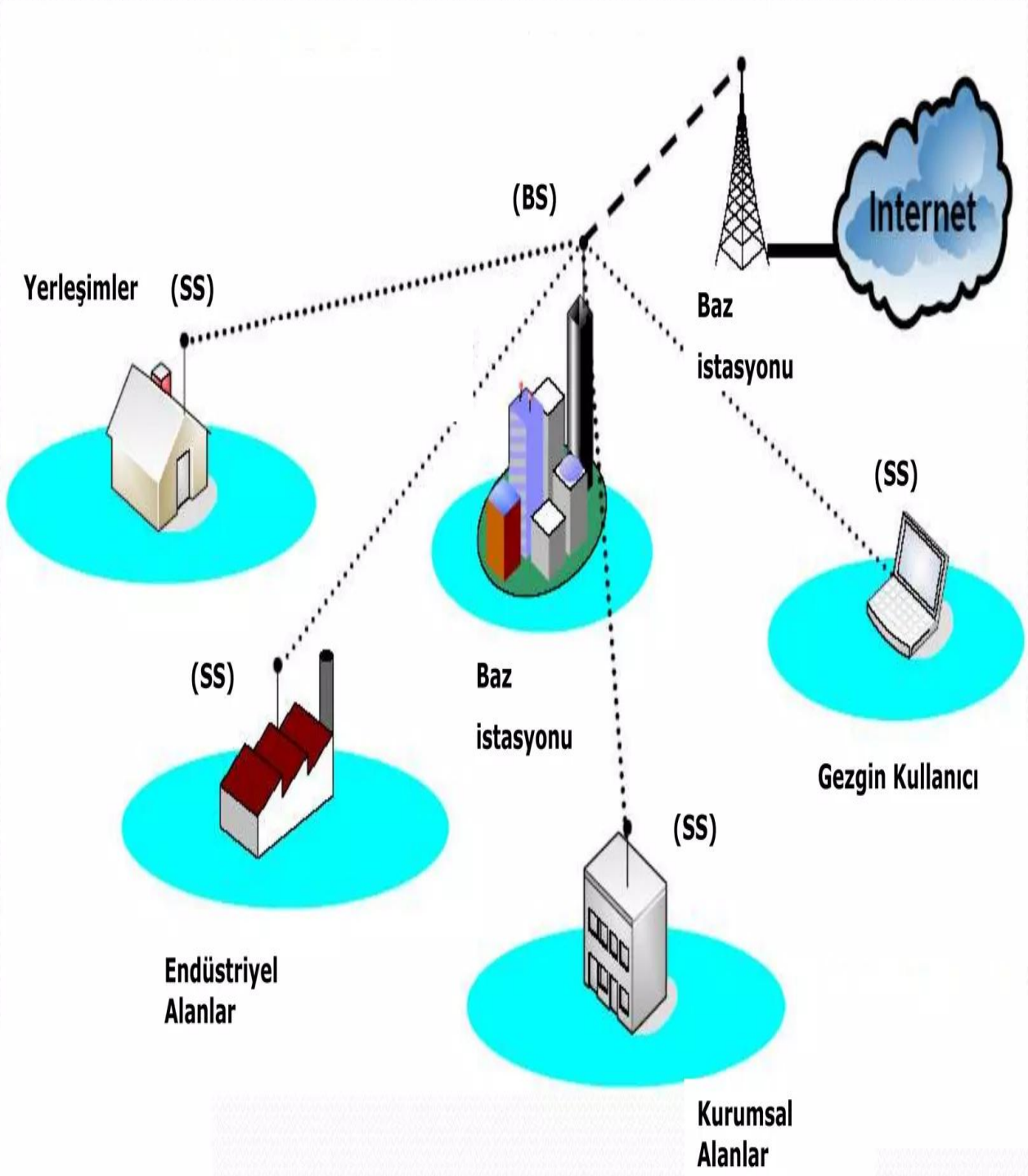
WiMAX(2/2)

- **Amaç:** Evlere ve işletme abonelerine kablosuz yüksek hızlı internet erişimi sağlamak.
- Baz istasyonları (BS) ve kullanıcı istasyonlarını (SS) içerir.
- Çarpışmaları engellemek için merkezi erişim kontrolü yapılır.
- Farklı QoS(Servis Kalitesi) gereksinimleri ile uygulamaları destekler.

WiMAX'in Uygulama Alanları

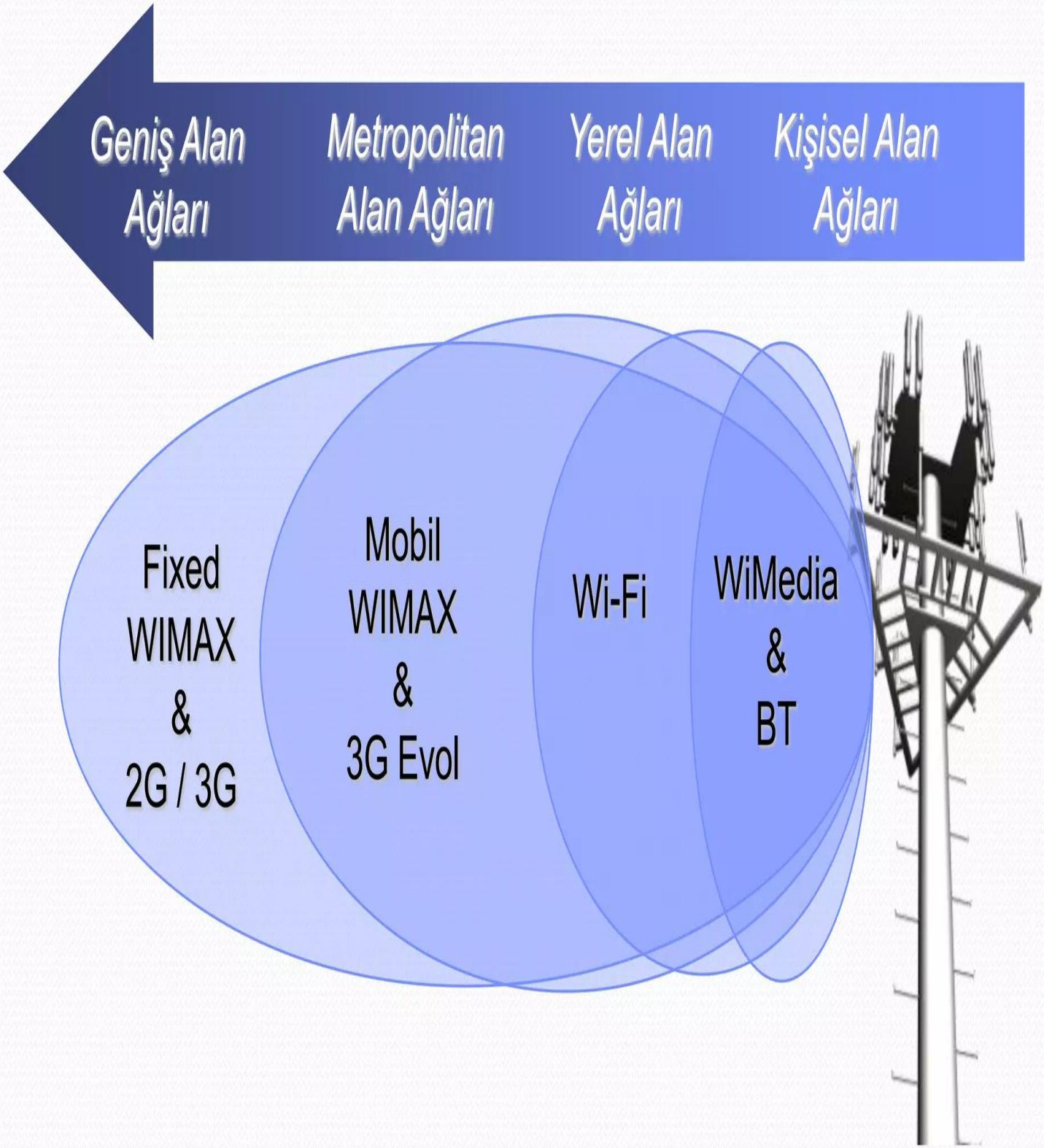
- DSL'e bir kablosuz alternatif olarak uzak mesafelere erişim
- IPTV ve VoIP uygulamalarında
  - VoIP: İnternet veya veri hatları üzerinden ses aktarımı.
- Şehir ve ülkeler arası mobil geniş bant bağlantısı
- Yüksek hızda kesintisiz telsiz iletişim
  - 70 Mbps
  - Kapsama alanı: 50-70 km'ye kadar
  - Veri
  - Ses (isteğe-bağlı)
  - Görüntü (isteğe-bağlı)
  - Videokonferans

WiMAX Genel Yapısı



SS: Kullanıcı İstasyonu BS: Baz İstasyonu

Geniş Bandlı Kablosuz Teknolojiler



Source: WiMAX Forum

WiMAX'in Avantajları

- *Çoklu yol etkileşimi*
- *Gecikme dağılımı*
- *Sağlamlık*

- Çoklu yol erişimi ve gecikme dağılımı:Kullanıcı istasyonu, baz istasyonunun görüş alanında olmadığı zamanlarda da iyi bir performans gerçekleştirebilir.
- Sağlamlık: Bağlantı tabanlı erişim protokolü değil, erişim talepli erişim protokolü kullanılır. Bu da daha az veri çarpışması demektir.

WiMax'in Sağladığı Faydalar

- ***Ölçeklenebilirlik:*** Esnek kanal bant genişliği için ölçeklenebilir fiziksel katman.
  - Global radyo frekans band dağılım çeşitleri: (e.g.: 1.8, 2.2, 3.5 GHz)
- ***Yüksek veri oranı:***Adaptif modülasyon, genişletilmiş FEC, vb servislerle daha fazlla veri taşınması.
- ***Servis Kalitesi (QoS) :*** Kaynak aktarımı sırasında her servis için ayrı tanımlanır.
- ***Mobilite:*** Hareket halindeyken de internete erişim.
- ***Güvenlik:*** Genişletilebilir kimlik doğrulama protokolü, AES-CCM ile veri şifreleme, CMAC Authentication, X.509 Sertifikalar, Donanım ve kullanıcı Kimlik doğrulaması

Wimax ve WiFi (1/2)

- **WiFi**
  - Tüm kullanıcılar yarış halindedir:bir erişim noktasına aynı anda istek gönderirler.
  - İstekler rasgele sıralanır
  - Erişim noktasına uzak olan istemci sonlarda sıraya girer
    - Uzun beklemeler ve bağlantının sürekli sonlandırılması.
- **WiMAX**
  - Bağlantı noktasına erişmek isteyen istemciler sırayla alınır.
  - Her istemci bir kere yarışa girer.
  - İstemcinin uzaklığına göre belli zaman aralığında erişime izin verilir.
  - Band genişliği daha etkin kullanılır.

Wimax ve WiFi (2/2)

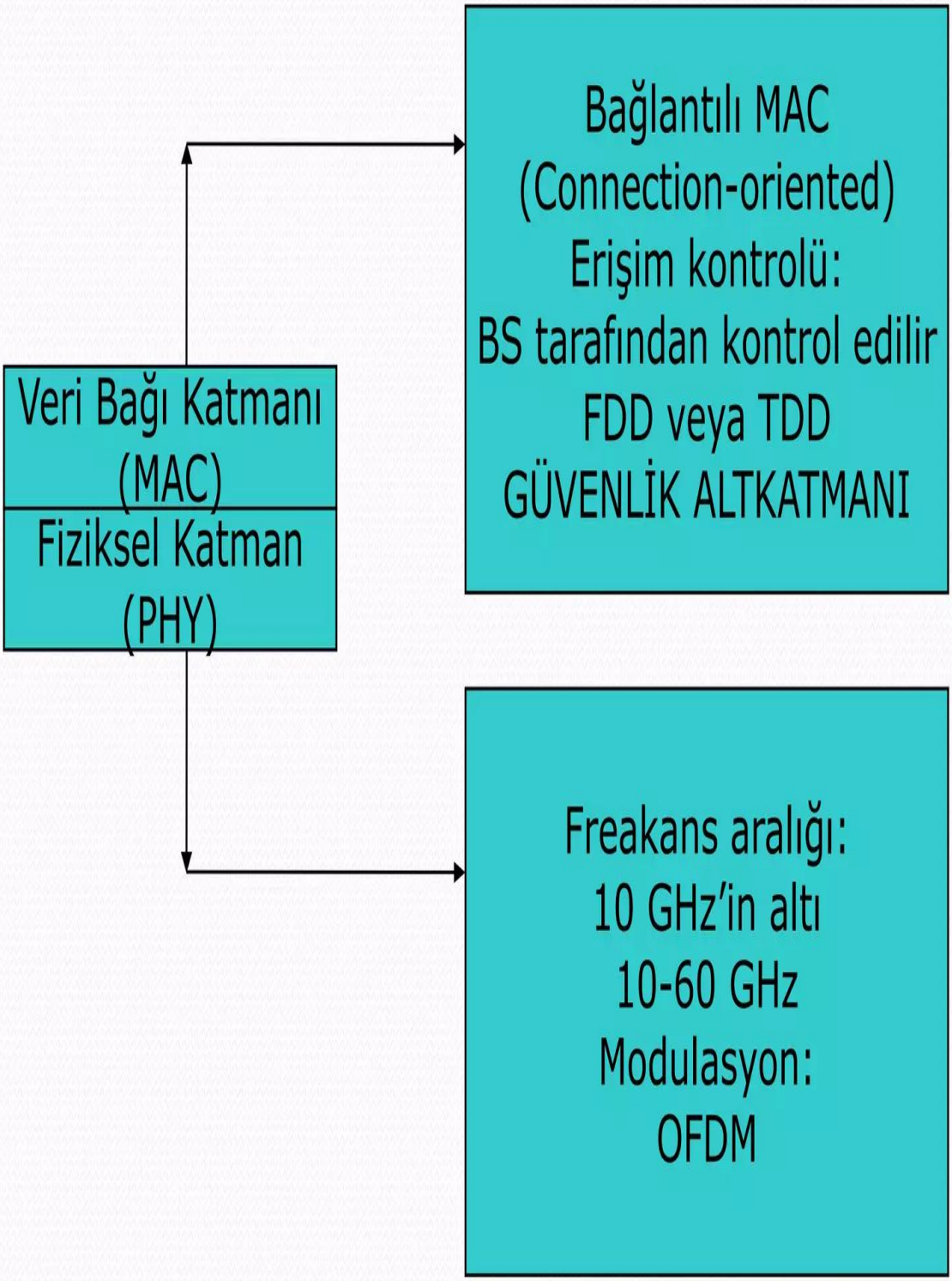
- WiFi
  - En hızlı Wifi bağlantısı 54Mbps
  - Wifi'nin menzili 30 metre
- WiMAX
  - En hızlı Wimax bağlantısı 70 Mbps
  - Wimax'in menzili 50 km
    - Kapsama alanı ortam koşullarına göre artmakta ya da azalmaktadır.

IEEE 802.16 İletişim Türleri

- İletişim Türleri:
  - Baz istasyonu(BS)□ Kullanıcı İstasyonu(SS): Downlink
  - Kullanıcı İstasyonu(SS)□ Baz İstasyonu(BS): Uplink
  - Baz İstasyonu(BS)-kullanıcı İstasyonları (SS) arası
    - Tek noktadan Çok noktaya (PMP)
  - Kullanıcı İstasyonları arası
    - Ağ (mesh) yapısı

12/30

WiMAX Katmansal Analiz



13/30

Fiziksel Katman

- Yönlü antenlerin kullanımına imkan sağlar
- İki farklı çoklama sağlar:
  - Frekans Bölme Çoklama (FDD)
  - Zaman Bölme Çoklama(FDD)
- Tam ve yarı çift yönlü istasyonları destekler
- Veri kayıplarına uyumlu profil
  - İletme parametreleri (örn: Modulasyon, FEC)
  - Profiller "Interval Usage Code" tarafından tanımlanır.
    - Interval Usage Code: Aralık kullanım kodu.

Media Acces Control (MAC)

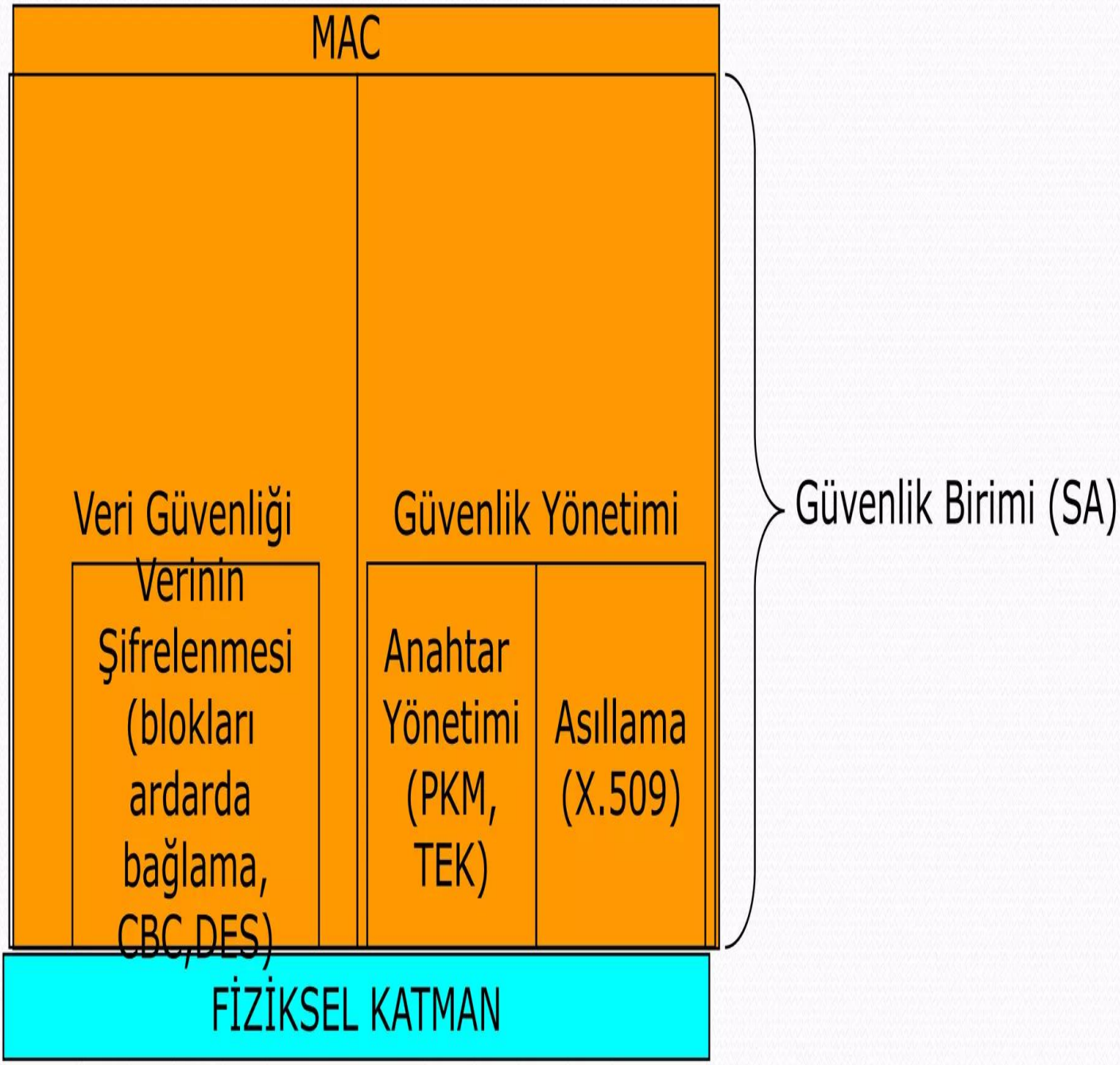
- Bağlantı Yönelimli
  - Connection ID (CID), Service Flows
- Kanal Erişimi: Baz istasyonu tarafından karar verilir.
  - UL-MAP
    - Uplink kanal erişimini tanımlar.
    - Uplink veri burst profillerini tanımlar.
  - DL-MAP
    - Downlink veri burst profillerini tanımlar.
- UL-MAP ve DL-MAP'in her ikisi de her downlink altçerçeve iletiminin başlangıcında iletilirler.

802.16 Güvenlik Standardı

- 5 kavrama dayalı bir yapı
  - Veri Şifreleme
    - MAC başlığı dışındaki kısma uygulanıyor
  - Anahtar Yönetimi
    - PKM
  - "Güvenlik Birimi" nin oluşturulması
    - Birimler arasında saydam bir iletişim kontrolü
  - Bağlantıların güvenlik birimine iletilmesi
  - Kriptografik süreç
    - Güvenlik biriminin veri şifrelemesi, asıllama ve anahtar alışverişi sırasında uyguladığı metodlarve girdiği durumlar

16/30

WiMAX Güvenlik Altkatmanı(1/2)

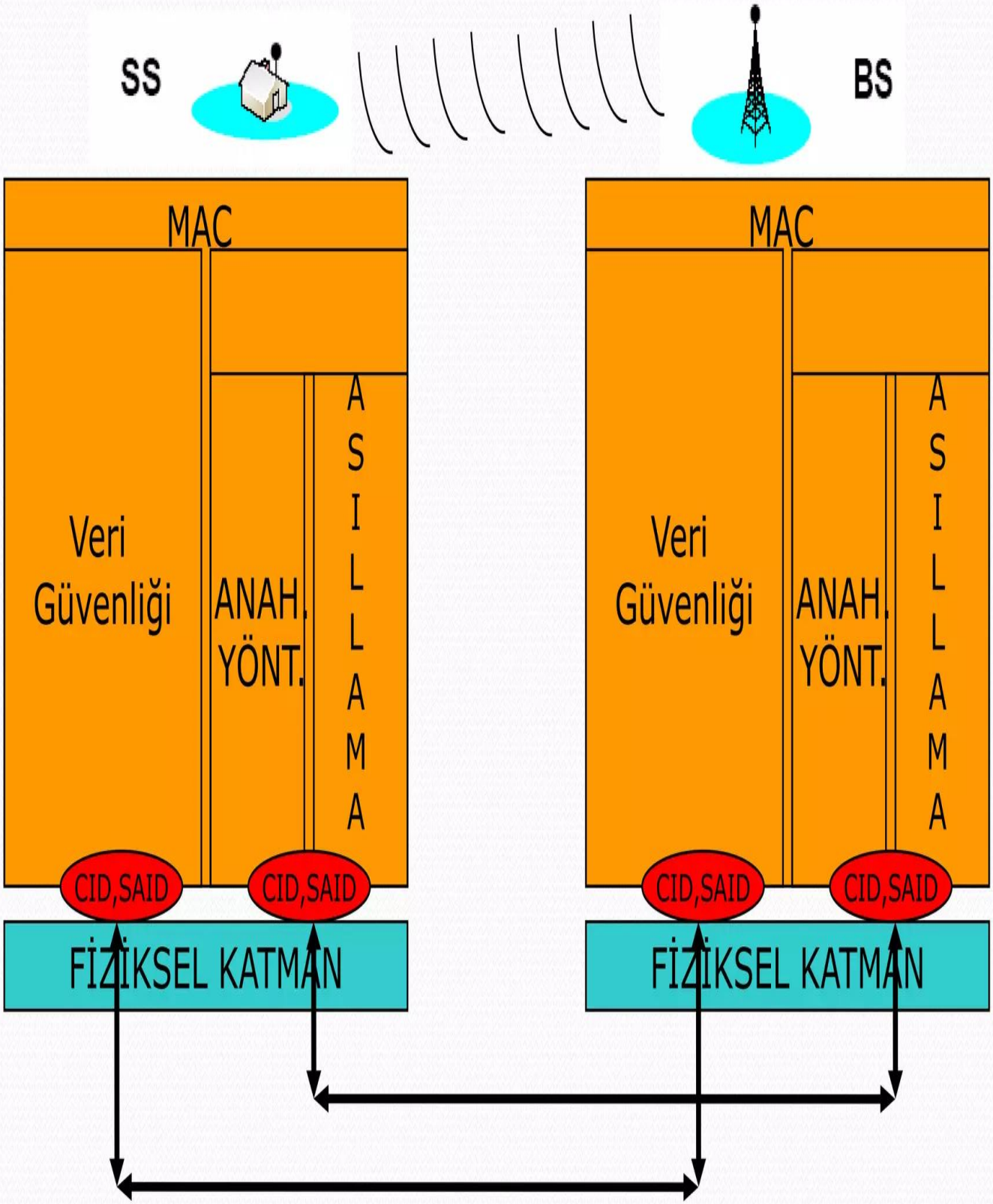


WiMAX Güvenlik Altkatmanı(2/2)

- Güvenlik Birimi (SA):
  - BS-SS arasındaki her türlü güvenlik bağlantısını sağlar.
  - 16-bitlik bir belirteci vardır (SAIP).
  - Tutulan parametler:
    - Her düzey için bir bağlantı ID'si(CID).
    - Kriptografik bilgiler(CBC, DES vs)
    - Güvenlik Bilgileri(Anahtar, IV)

18/30

WiMAX Güvenlik Altyapısı



Veri Güvenliği (1/2)

- Şifreleme
  - Kullanılan Algoritma
    - DES
      - 56 bit anahtar
      - 64 bitlik bloklar
  - Kullanılan Şifreleme Kipi
    - "Şifreleme Bloklarını ardarda Bağlama Kipi" (Cipher Block Chaining,CBC)
    - CBC-IV: başlama vektörü TEK anahtar değiştokuşu sırasında öğrenilir
    - XOR: Çerçevedeki senkronizasyon alanında belirtilir.

20/30

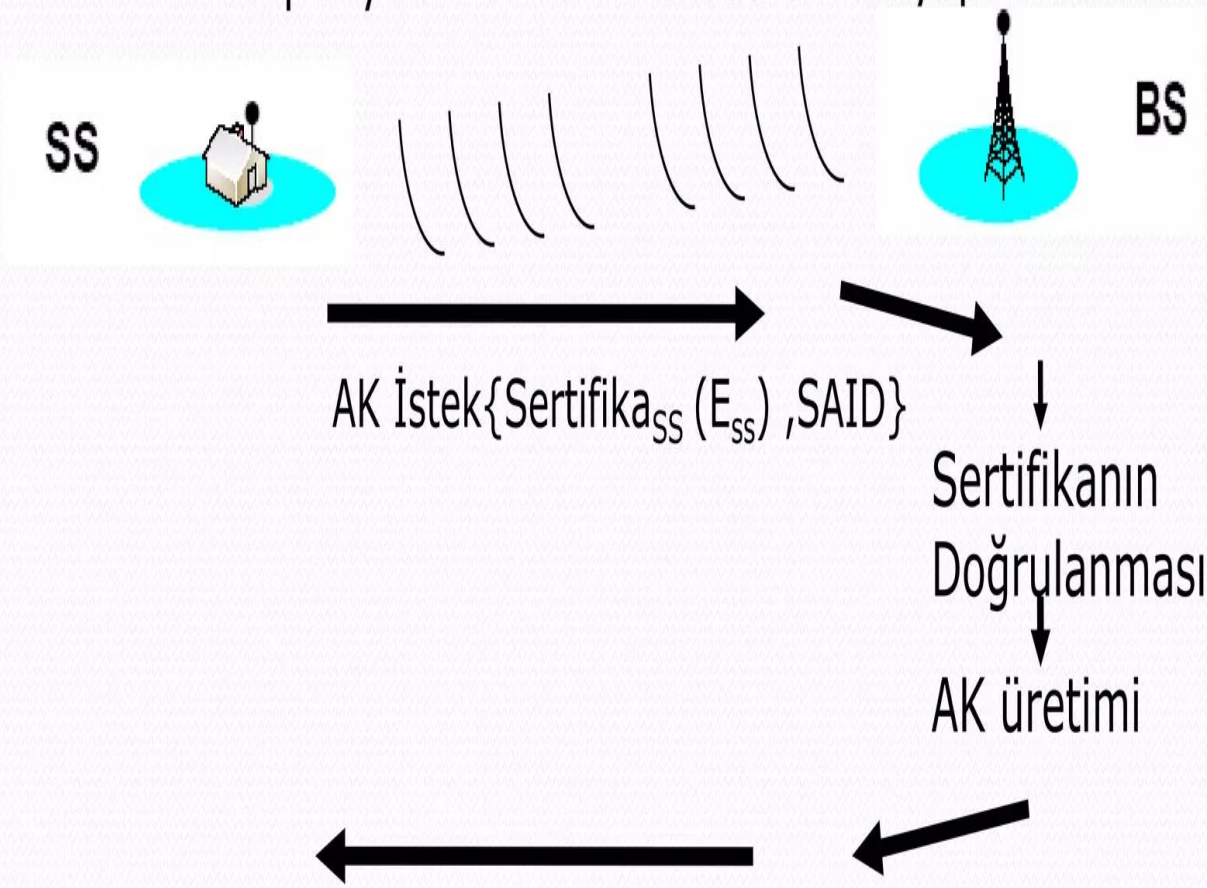
Güvenlik Yönetimi(1/2)

- Asıllama
  - Açık anahtarlı kriptografi kullanılır.
  - SS ile BS arasında SAID alışverişi
  - SS için kullanılan yöntem: X.509 sertifikalama
    - Üretici Sertifikası
      - Kendi kendine veya üçüncü kişi tarafından
      - Üretici bilgileri(WiMAX forumuna uygunluk)
    - SS sertifikası
      - Üretici tarafından
      - SS'in Seri numarası
      - SS'in MAC adresi
    - SS'ler açık-gizli anahtar çiftleri ile donatılmıştır
      - RSA tabanlı bir algoritma ile
      - Herhangi bir lokal algoritmayla dinamik olarak

21/30

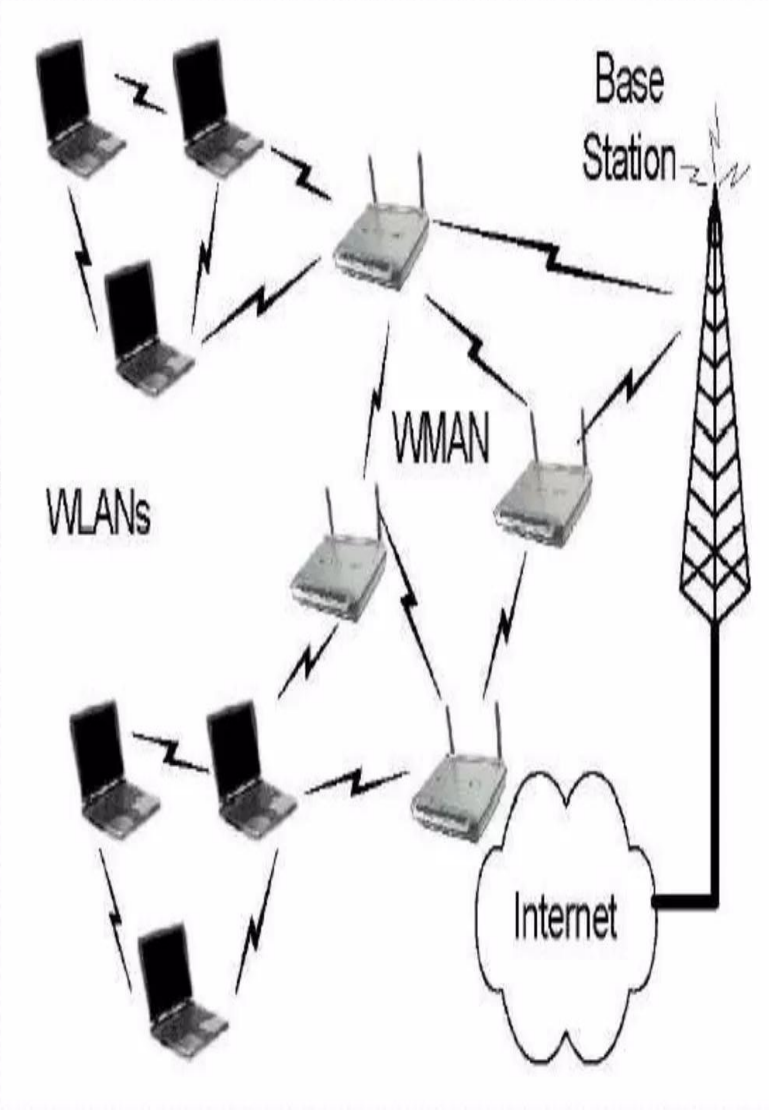
Güvenlik Yönetimi(2/2)

- Asıllama anahtarı(AK,128-bit) alışverişi yapılır
  - Açık anahtar ile şifreli olarak gönderilir.
  - BS ve SS AK'yı elde ettikten sonra asıllama tamamlanmış olur.
  - SS periyodik olarak AK tazelemesi yapar.



WiMAX Ağ(Mesh) Yapısında Güvenlik

- SS'ler BS olmadan birbirleriyle haberleşebilir→Mesh yapının en önemli özelliği
- BS'nin kapsama alanında artış olur
- Ağda bir düğüm çöktüğünde yada BS çöktüğünde tüm iletişim kesilmez.



23/30

Sonuç

- 802.16 standardındaki 2 düzeyli yapı,802.11'e göre geliştirilmeye daha elverişli bir altyapı oluşturmakta.
- Sertifika otoriteleri hakkında daha açık bilgiler verilmeli.
- Veri şifreleme yöntemi:DES yetersiz
- Tek taraflı bir asıllama söz konusu
  - Geliştirilmesi gereken bir nokta
  - EAP kullanılabilir
- Anahtar üretiminde problemler var
  - Tekrar saldırıların engellenebilmesi için rastgele sayıların üretilmesi gerekiyor.

24/30