Understanding WiMAX (Chapter 10)
ENE 490
MON 13:30-16:30
Asst. Prof. Dr. Suwat Pattaramalai
Understanding WiMAX

- WiMAX Network Architecture
  - End-to-end network system architecture, three stages development
  - Stage 1: the use case scenarios and service requirements are listed
  - Stage 2: the architecture that meet the service requirements is developed
  - Stage 3: the details of the protocols associated with the architecture are specified
  - This chapter will focuses mostly on the stage 2
  - WiMAX network reference model, end-to-end protocol layering, network selection and discovery, IP address allocation, functional architecture and processes associated with security, QoS, and mobility management
Understanding WiMAX

- General Design Principles of the Architecture
  - Functional decomposition: Features are decomposed into functional entities without specific implementation assumptions about physical network entities
  - Deployment modularity and flexibility: enough to not preclude a broad range of implementation and deployment options
  - Support for variety of usage models: support the coexistence of fixed, nomadic, portable, and mobile usage model
  - Decoupling of access and connectivity services: unbundling of access infrastructure from IP connectivity services
  - Support for a variety of business models: logical separation between (1) network access provider, NAP; own and/or operates the access network, (2) network service provider, NSP; owns the subscriber and provides broadband service, (3) application service providers, ASP;
  - Extensive use of IETF protocols: Internet Engineering Task Force
Understanding WiMAX

- General Design Principles of the Architecture
  - Support for access to incumbent operator services: through interworking functions
- Network Reference Model

*Figure 10.1 Network reference model*
Understanding WiMAX

- Network Reference Model (NRM)
  - (1) mobile stations used by the subscriber to access network
  - (2) access service network (ASN) owned by NAP
  - (3) connectivity service network (CSN) owned by NSP

- ASN Functions, Decompositions, and Profiles

The ASN performs the following functions:

- IEEE 802.16e–based layer 2 connectivity with the MS
- Network discovery and selection of the subscriber’s preferred CSN/NSP
- AAA proxy: transfer of device, user, and service credentials to selected NSP AAA and temporary storage of user’s profiles
- Relay functionality for establishing IP connectivity between the MS and the CSN
- Radio resource management (RRM) and allocation based on the QoS policy and/or request from the NSP or the ASP
- Mobility-related functions, such as handover, location management, and paging within the ASN, including support for mobile IP with foreign-agent functionality
Understanding WiMAX

- ASN gateway: location management and paging; acts as a server for network session and mobility management; performs admission control and temporary caching of subscriber profiles and encryption keys; acts as an authenticator and AAA; client/proxy, provides mobility tunnel establishment and management with BS; performs service flow authorization (SFA); provides foreign-agent functionality; performs routing (IPv4 and IPv6) to selected CSNs
### Understanding WiMAX

#### Table 10.1 Functional Decomposition of the ASN in Various Release 1 Profiles

<table>
<thead>
<tr>
<th>Functional Category</th>
<th>Function</th>
<th>ASN Entity Name</th>
<th>Profile A</th>
<th>Profile B</th>
<th>Profile C</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security</strong></td>
<td>Authenticator</td>
<td>ASN-GW</td>
<td>ASN-GW</td>
<td>ASN-GW</td>
<td>BS</td>
</tr>
<tr>
<td></td>
<td>Authentication relay</td>
<td>BS</td>
<td>ASN</td>
<td>BS</td>
<td>BS</td>
</tr>
<tr>
<td></td>
<td>Key distributor</td>
<td>ASN-GW</td>
<td>ASN</td>
<td>ASN-GW</td>
<td>BS</td>
</tr>
<tr>
<td></td>
<td>Key receiver</td>
<td>BS</td>
<td>ASN</td>
<td>BS</td>
<td>BS</td>
</tr>
<tr>
<td><strong>Mobility</strong></td>
<td>Data path function</td>
<td>ASN-GW and BS</td>
<td>ASN</td>
<td>ASN-GW and BS</td>
<td>BS</td>
</tr>
<tr>
<td></td>
<td>Handover control</td>
<td>ASN-GW</td>
<td>ASN</td>
<td>BS</td>
<td>BS</td>
</tr>
<tr>
<td></td>
<td>Context server and client</td>
<td>ASN-GW and BS</td>
<td>ASN</td>
<td>ASN-GW and BS</td>
<td>BS</td>
</tr>
<tr>
<td></td>
<td>MIP foreign agent</td>
<td>ASN-GW</td>
<td>ASN</td>
<td>ASN-GW</td>
<td>BS</td>
</tr>
<tr>
<td><strong>Radio resource management</strong></td>
<td>Radio resource controller</td>
<td>ASN-GW</td>
<td>ASN</td>
<td>BS</td>
<td>BS</td>
</tr>
<tr>
<td></td>
<td>Radio resource agent</td>
<td>BS</td>
<td>ASN</td>
<td>BS</td>
<td>BS</td>
</tr>
<tr>
<td><strong>Paging</strong></td>
<td>Paging agent</td>
<td>BS</td>
<td>ASN</td>
<td>BS</td>
<td>BS</td>
</tr>
<tr>
<td></td>
<td>Paging controller</td>
<td>ASN-GW</td>
<td>ASN</td>
<td>ASN-GW</td>
<td>BS</td>
</tr>
<tr>
<td><strong>QoS</strong></td>
<td>Service flow authorization</td>
<td>ASN-GW</td>
<td>ASN</td>
<td>ASN-GW</td>
<td>BS</td>
</tr>
<tr>
<td></td>
<td>Service flow manager</td>
<td>BS</td>
<td>ASN</td>
<td>BS</td>
<td>BS</td>
</tr>
</tbody>
</table>
Understanding WiMAX

CSN Functions:

The CSN provides the following functions:

- IP address allocation to the MS for user sessions.
- AAA proxy or server for user, device and services authentication, authorization, and accounting (AAA).
- Policy and QoS management based on the SLA/contract with the user. The CSN of the home NSP distributes the subscriber profile to the NAP directly or via the visited NSP.
- Subscriber billing and interoperator settlement.
- Inter-CSN tunneling to support roaming between NSPs.
- Inter-ASN mobility management and mobile IP home agent functionality.
- Connectivity infrastructure and policy control for such services as Internet access, access to other IP networks, ASPs, location-based services, peer-to-peer, VPN, IP multimedia services, law enforcement, and messaging.
**Understanding WiMAX**

Reference Points: a conceptual link that connects two groups of functions that reside in different functional entities of the ASN, CSN, or MS.

<table>
<thead>
<tr>
<th>Reference Point</th>
<th>End Points</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>MS and ASN</td>
<td>Implements the air-interface (IEEE 802.16e) specifications. R1 may additionally include protocols related to the management plane.</td>
</tr>
<tr>
<td>R2</td>
<td>MS and CSN</td>
<td>For authentication, authorization, IP host configuration management, and mobility management. Only a logical interface and not a direct protocol interface between MS and CSN.</td>
</tr>
<tr>
<td>R3</td>
<td>ASN and CSN</td>
<td>Supports AAA, policy enforcement, and mobility-management capabilities. R3 also encompasses the bearer plane methods (e.g., tunneled) to transfer IP data between the ASN and the CSN.</td>
</tr>
<tr>
<td>R4</td>
<td>ASN and ASN</td>
<td>A set of control and bearer plane protocols originating/terminating in various entities within the ASN that coordinate MS mobility between ASNs. In Release 1, R4 is the only interoperable interface between heterogeneous or dissimilar ASNs.</td>
</tr>
<tr>
<td>R5</td>
<td>CSN and CSN</td>
<td>A set of control and bearer plane protocols for interworking between the home and visited network.</td>
</tr>
<tr>
<td>R6</td>
<td>BS and ASN-GW</td>
<td>A set of control and bearer plane protocols for communication between the BS and the ASN-GW. The bearer plane consists of intra-ASN data path or inter-ASN tunnels between the BS and the ASN-GW. The control plane includes protocols for mobility tunnel management (establish, modify, and release) based on MS mobility events. R6 may also serve as a conduit for exchange of MAC states information between neighboring BSs.</td>
</tr>
<tr>
<td>R7</td>
<td>ASN-GW-DP and ASN-GW-EP</td>
<td>An optional set of control plane protocols for coordination between the two groups of functions identified in R6.</td>
</tr>
<tr>
<td>R8</td>
<td>BS and BS</td>
<td>A set of control plane message flows and, possibly, bearer plane data flows between BSs to ensure fast and seamless handover. The bearer plane consists of protocols that allow the data transfer between BSs involved in handover of a certain MS. The control plane consists of the inter-BS communication protocol defined in IEEE 802.16e and additional protocols that allow controlling the data transfer between the BS involved in handover of a certain MS.</td>
</tr>
</tbody>
</table>
Understanding WiMAX

- Protocol Layering Across a WiMAX Network
Understanding WiMAX

- Protocol Layering Across a WiMAX Network

Figure 10.3 Protocol stack for Ethernet convergence sublayer with routed ASN
Understanding WiMAX

- Protocol Layering Across a WiMAX Network
Understanding WiMAX

- **Network Discovery and Selection: 4 procedures**
  - NAP discovery: MS discover all available NAPs within a coverage area
  - NSP discovery: MS discover all NSPs that provide service over given ASN
  - NSP enumeration and selection: MS make a selection from the list of available NSPs by using an appropriate algorithm (auto or manual)
  - ASN attachment: MS indicates NSP selection by attaching to an ASN associated with the selected NSP and by providing its identity and home NSP domain in the form of a network access identifier

- **IP Address Assignment**
  - Dynamic Host Control Protocol (DHCP): primary mechanism to allocate a dynamic point-of-attachment (PoA) IP address to the MS
  - To support IPv6, the ASN includes and IPv6 access router (AP), for mobile IPv6, MS obtains the care-of-address (CoA) from the ASN, and a home address (HoA) from the home CSN
Understanding WiMAX

- **Authentication and Security Architecture**
  - AAA framework should meet following:

  - Support for device, user, and mutual authentication between MS/SS and the NSP, based on Privacy Key Management Version 2 (PKMv2) as defined in IEEE 820.16e-2005.
  - Support for authentication mechanisms, using a variety of credentials, including shared secrets, subscriber identity module (SIM) cards, universal SIM (USIM), universal integrated circuit card (UICC), removable user identity module (RUIM), and X.509 certificates, as long as they are suitable for EAP methods satisfying RFC 4017.
  - Support for global roaming between home and visited NSPs in a mobile scenario, including support for credential reuse and consistent use of authorization and accounting through the use of RADIUS in the ASN and the CSN. The AAA framework shall also allow the home CSN to obtain information, such as visited network identity, from the ASN or the visited CSN that may be needed during AAA.
  - Accommodation of mobile IPv4 and IPv6 security associations (SA) management.
  - Support for policy provisioning at the ASN or the CSN by allowing for transfer of policy-related information from the AAA server to the ASN or the CSN.
**Understanding WiMAX**

- **AAA Architecture Framework: pull model 4 steps**

1. The supplicant MS sends a request to the network access server (NAS) function in the ASN.
2. The NAS in the ASN forwards the request to the service provider’s AAA server. The NAS acts as an AAA client on behalf of the user.
3. The AAA server evaluates the request and returns an appropriate response to the NAS.
4. The NAS sets up the service and tells the MS that it is ready.

![Generic AAA roaming model](image)
Understanding WiMAX

- Authentication Protocols and Procedure

![Diagram of WiMAX Authentication Protocols and Procedure](image-url)

*Figure 10.6 Protocol stack for user authentication in WiMAX*
Understanding WiMAX

- Authentication Protocols and Procedure

![Diagram of WiMAX Authentication Protocols](image-url)

- Supplicant MS
- BS ASN
- Authenticator (NAS) ASN
- AAA Proxy(s)
- AAA Server Home CSN

1. 802.16e Linkup → Link Activation
   - EAP Request/Identity
2. EAP Response/Identity
   - EAP Method (EAP-AKA, PEAP, EAP-TLS, etc.)
   - EAP over RADIUS
3. MSK and EMSK Established in MS and AAA Server
   - Transfer MSK
4. PMK Generated in MS and Authenticator
5. AK Generated in MS and Authenticator
6. SA-TEK Challenge
   - SA-TEK Request
   - SA-TEK Response
7. Key Request
   - Key Reply
8. Flow Creation (DSX Exchange)

*Figure 10.7 PKMv2 procedures*
Understanding WiMAX

- ASN Security Architecture
  - (1) authenticator defined in EAP specifications
  - (2) authentication relay is the functional entity in a BS
  - (3) key distributor holds the keys generated during EAP exchange
  - (4) key receiver hold the authentication key

---

![ ASN security architecture and deployment models: (a) integrated deployment model and (b) stand-alone deployment model ](image)
Understanding WiMAX

- Quality-of-Service Architecture
  - Dynamic service flow follows three generic steps

1. For each subscriber, the allowed service flows and associated QoS parameters are provisioned via the management plane.
2. A service flow request initiated by the MS or the BS is evaluated against the provisioned information, and the service flow is created, if permissible.
3. Once a service flow is created, it is admitted by the BS, based on resource availability: if admitted, the service flow becomes active when resources are assigned.
Understanding WiMAX

- Quality-of-Service Architecture

![Diagram of QoS functional architecture](image-url)
Understanding WiMAX

- Mobility management

  - Minimize packet loss and handoff latency and maintain packet ordering to support seamless handover even at vehicular speeds
  - Comply with the security and trust architecture of IEEE 802.16 and IETF EAP RFCs during mobility events
  - Supporting macro diversity handover (MOHO) as well as fast base station switching (FBSS)\(^7\)

  - Minimize the number of round-trips of signaling to execute handover
  - Keep handover control and data path control separate
  - Support multiple deployment scenarios and be agnostic to ASN decomposition
  - Support both IPv4- and IPv6-based mobility management and accommodate mobiles with multiple IP addresses and simultaneous IPv4 and IPv6 connections
  - Maintain the possibility of vertical or intertechnology handovers and roaming between NSPs
  - Allow a single NAP to serve multiple MSs using different private and public IP domains owned by different NSPs
  - Support both static and dynamic home address configuration
  - Allow for policy-based and dynamic assignment of home agents to facilitate such features as route optimization and load balancing
Understanding WiMAX

- Mobility

**Figure 10.10** Handover scenarios supported in WiMAX
Understanding WiMAX

- Mobility
Understanding WiMAX

- Mobility

*Figure 10.12* Mobility event triggering a network-initiated R3 reanchoring (PMIP)
Understanding WiMAX

- Radio Resource Management

Figure 10.13 Generic reference models for RRM: (a) split RRM and (b) integrated RRM
Understanding WiMAX

- Paging and Idle-Mode Operation

![Diagram of WiMAX paging network reference model](image-url)
Understanding WiMAX

Summary and Conclusions

- The WiMAX Forum NWG has developed a network reference model that provides flexibility for implementation while at the same time providing a mechanism for interoperability.
- The network architecture provides a unified model for fixed, nomadic, and mobile usage scenarios.
- The security architecture of WiMAX supports the IEEE 802.16e MAC privacy services, using an-EAP based AAA framework that supports global roaming.
- The WiMAX architecture defines various QoS-related functional entities and mechanisms to implement the QoS features supported by IEEE 802.16e.
- The WiMAX architecture supports both layer 2 and layer 3 mobility. Layer 3 mobility is based on mobile IP and can be implemented without the need for a mobile IP client.
- The WiMAX architecture defines two generic reference models for radio resource management: one with and the other without an external controller for managing the BS resources.
- The network architecture supports paging and idle-mode operation of mobile stations.