



Mobile WiMAX: The Blueprint for Future Wireless Technologies


eci
experience




Wireless architecture trends

- **Mobility Management using Mobile IP**
 - Today's 3GPP2 (CDMA) networks use Mobile IP. Mobile WiMAX will use Mobile IP.
 - Today's GPRS uses separate mobility protocols (i.e. GTP), but future LTE networks will use a form of Mobile IP
- **Trend towards OFDMA (WiMAX, 3GPP LTE, IxEV-DO Rev C)**
 - and towards MIMO technologies
- **Move away from closed (proprietary) RAN architectures towards open, interoperable systems**

All rights reserved © 2007, ECI 2




Why WiMAX?




- **Favorable IPR environment**
 - (compared to 3G which is dominated by a few vendors)


- **Leading the wireless broadband industry in adoption of OFDMA**
 - More efficient spectrum usage
 - Scalable-OFDMA allows deployment in a range of spectrum bandwidths
 - Plus Mobile WiMAX supports TDD which is more flexible for asymmetric data services


- **WiMAX Forum leading industry towards all-IP network core**


All rights reserved © 2007, ECI  3





Mobile broadband air interface roadmap

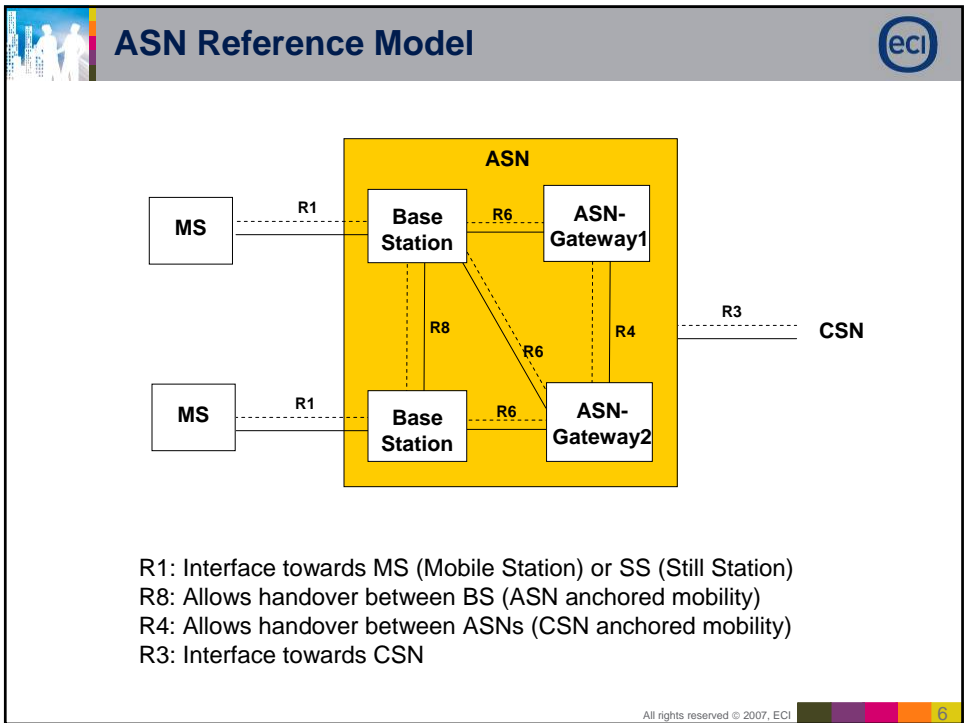
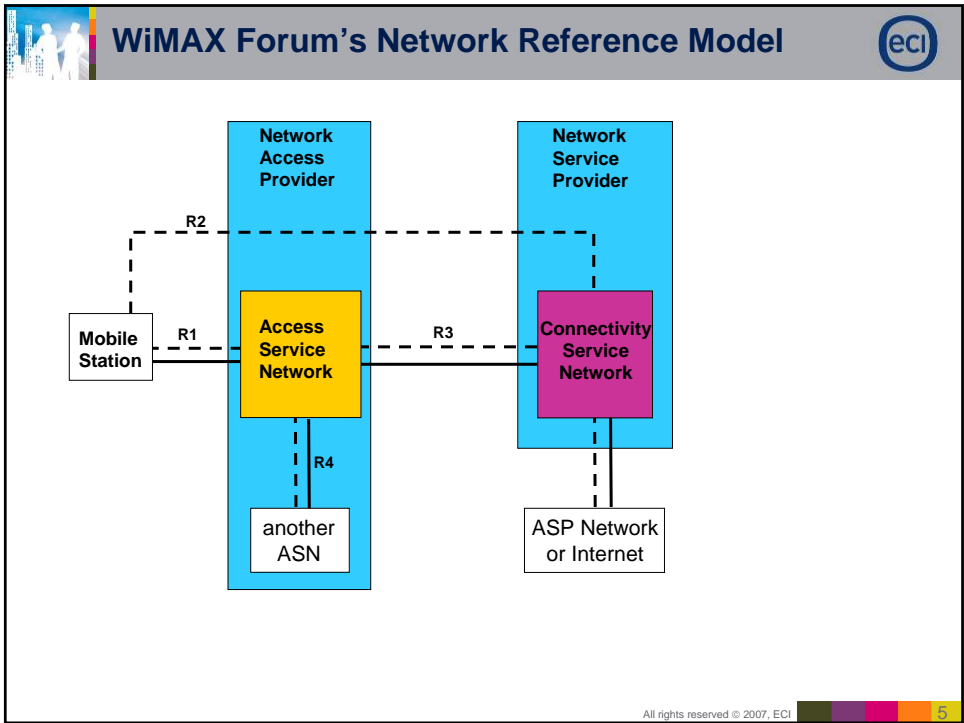


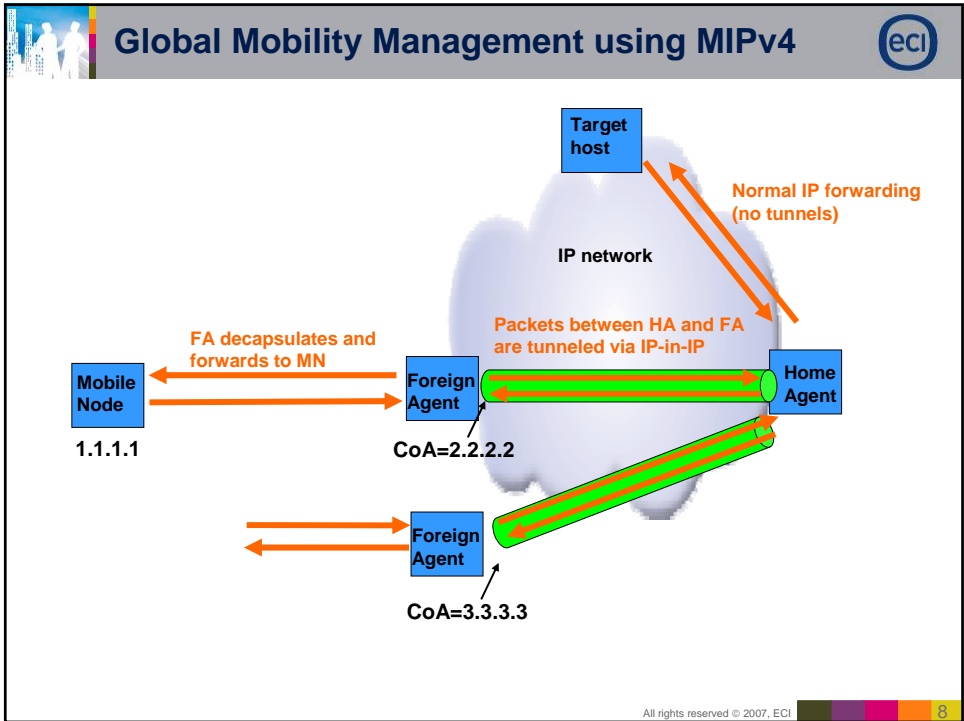
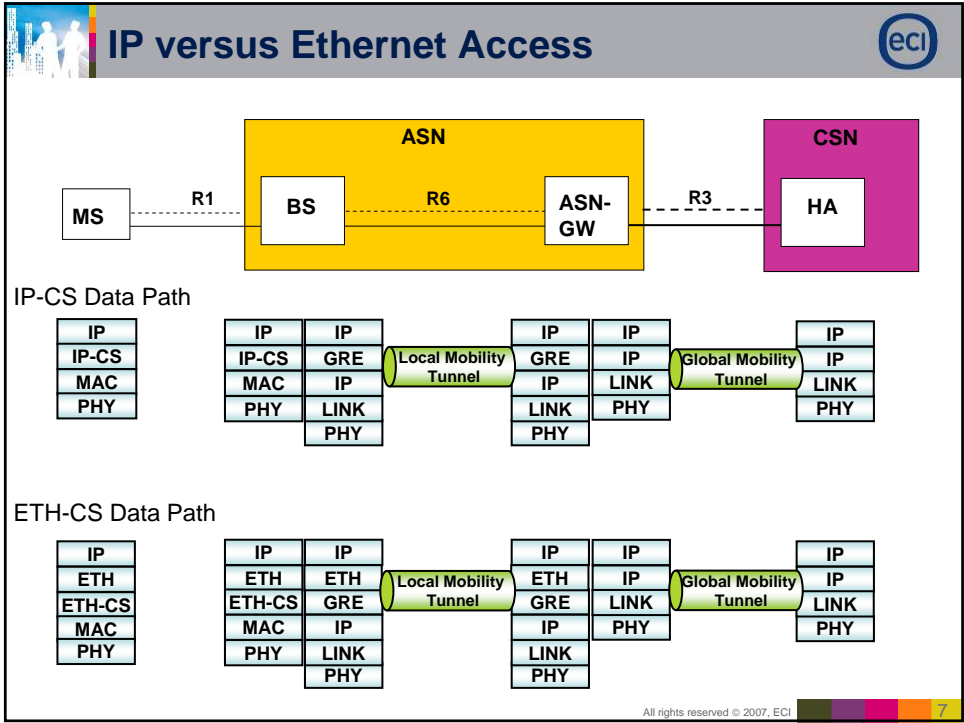
- **CDMA2000 1xEV-DO**
 - 1xEV-DO Rev. 0 (2004) 2.4Mbps downlink (1.25MHz)
 - 1xEV-DO Rev. A (2007) 3.1Mbps downlink
 - 1xEV-DO Rev. B (2007/2008) 4.9Mbps downlink
 - 1xEV-DO Rev. C (2009)  OFDMA

- **WCDMA HSPA**
 - HSDPA (2005/2006) 14Mbps downlink (5MHz)
 - HDUPA (2007/2008)
 - UTRAN LTE (2009)  OFDMA

-  **WiMAX uses Scalable OFDMA and MIMO now**

All rights reserved © 2007, ECI  4







Extensible Authentication Protocol (EAP) eci

Mobile Station

Authenticator

Authentication Server

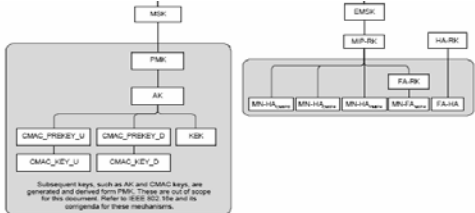
- Mobile authentication method commonly use EAP
- EAP enables “tunneling” of authentication methods so that the “authenticator” remains simple
 - Concept started with CHAP and distribution of CHAP-Challenges to backend RADIUS server
- EAP methods used for WiMAX device and user authentication
 - 802.1x (EAP over LAN) used in Wi-Fi networks

All rights reserved © 2007, ECI

Key Management & Encryption eci

- Mobile broadband network generally use encryption on the air interface
- Handover presents additional difficulties
- Keys are derived from a set of root keys produced via the EAP exchange
 - Mobile WiMAX encryption performed on BS which is not involved in EAP
 - Key derivation must produce “cryptographically separate” keys



Subsequent keys, such as AK and CMAC keys, are generated and derived from PMK. These are out of scope for this document. Refer to 3GPP R2-02, 5th and its corrigenda for these mechanisms.

Example key hierarchy from WiMAX Forum All rights reserved © 2007, ECI



Thank You

Jeremy.Brayley@ecitele.com

