WiMAX Overview

Parviz Yegani

Cisco Systems

pyegani@cisco.com

IETF-64

Nov. 7-11, 2005

Vancouver, Canada

Outline

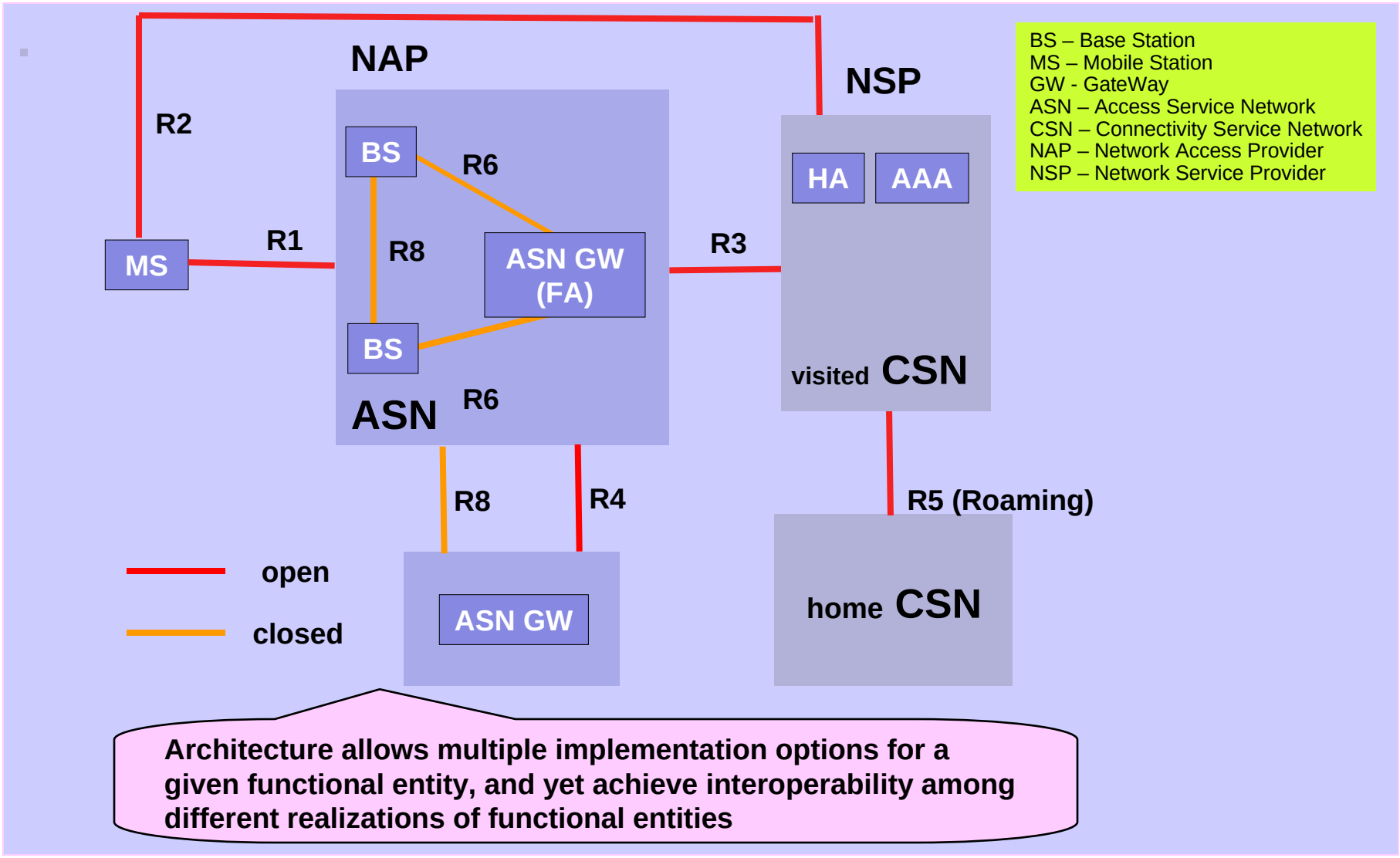
- WiMAX NWG Goals
- Network Reference Model
- Reference Points and Interfaces
- NWG Release 1 Features
- Implementation Scenarios
- Usage Modes (Fixed, Nomadic, Mobile)
- Quality of Service (QoS)
- Mobility Management (MM)
- Security
- Next Steps

WiMAX NWG Goals

Network WG was formed to create an open end-to-end framework for interoperable WiMAX networks.

- **Normative use of protocols based on existing IEEE and IETF standards**
- **Protocols are defined for different capabilities supported by the network**
- **Profiles are defined to allow interoperability for different usage modes and service models**

Network Reference Architecture



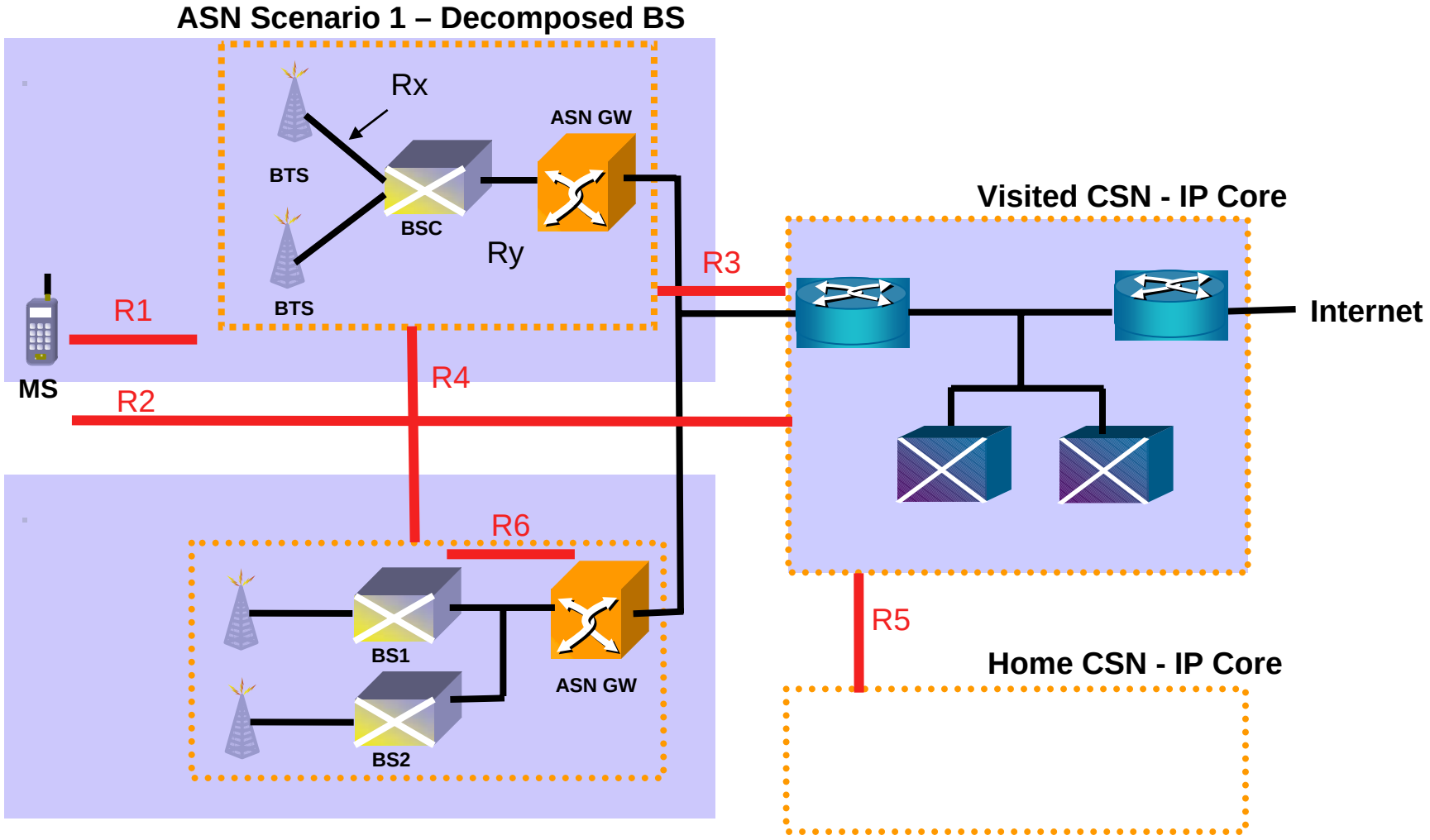
Interoperability Framework

- **Main goals:**
  - Maximize vendors access to the market
  - Maximize revenue opportunity for operators
- **Reference Points (RPs)**
  - Network Entities on either side of an RP represent a collection of control protocols and bearer end-points
  - Interoperability will be verified based only on protocols & procedures exposed across an RP
  - For a supported capability, NWG will specify the normative use of protocols over an RP
  - If the vendor claims support for the capability and exposes the RP, then the implementation must comply with the NWG definition
  - Avoids the situation where a protocol entity can reside on either end of an RP or replication of identical procedures across multiple RPs

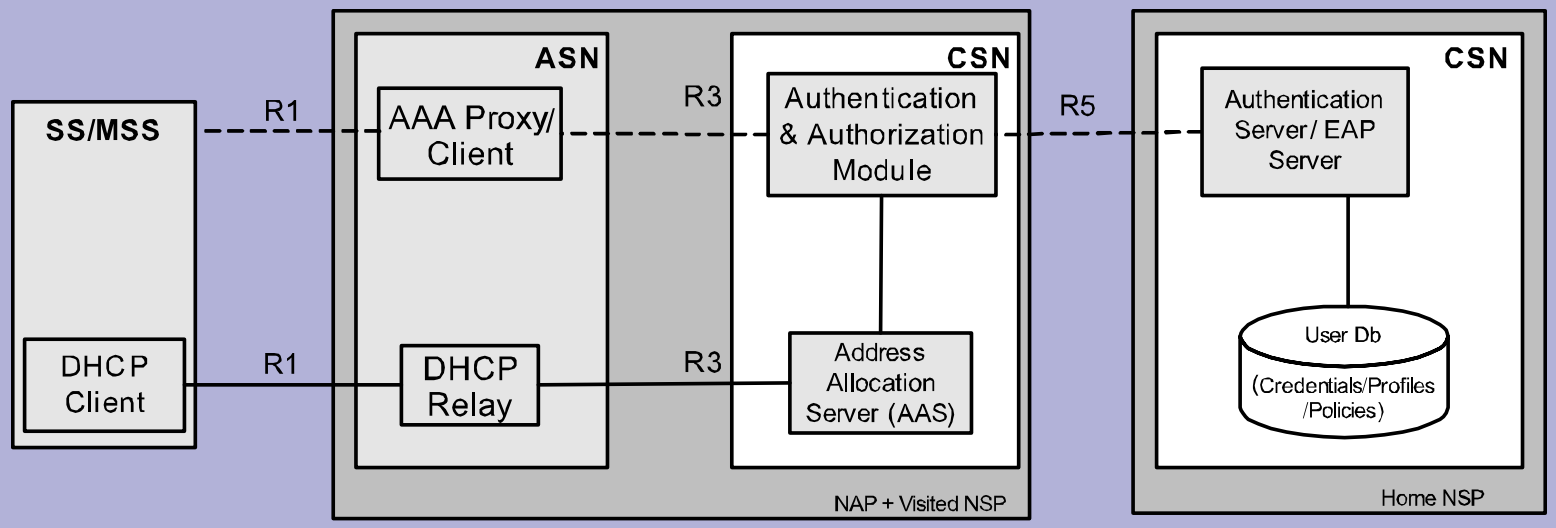
NWG Release 1 Features

- NWG Release 1 enforces interoperability across R1, R2, R3, R4 and R5 for all ASN implementation profiles
- Convergence sub-layer considerations/choices
- IP Address Assignment (Stateless/Stateful)
- Network Discovery and Selection
- PKMv2 based end-to-end security
- Accounting support for multi-operator roaming (RADIUS only)
- QoS, Admission Control and Service Flow Management
- Layer 2/3 Mobility Management
- Radio Resource Management

Implementation Scenarios

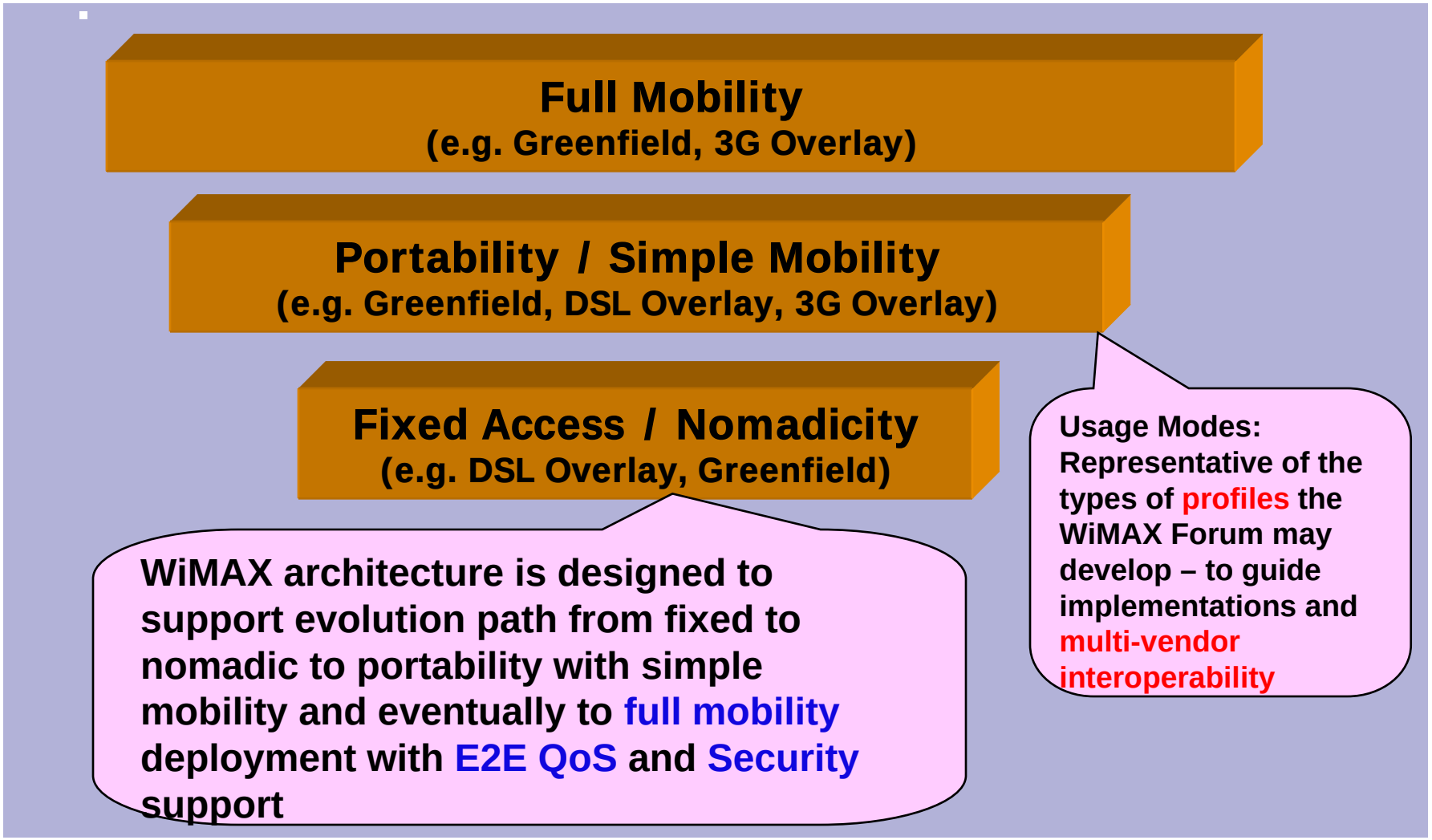


Access Scenarios

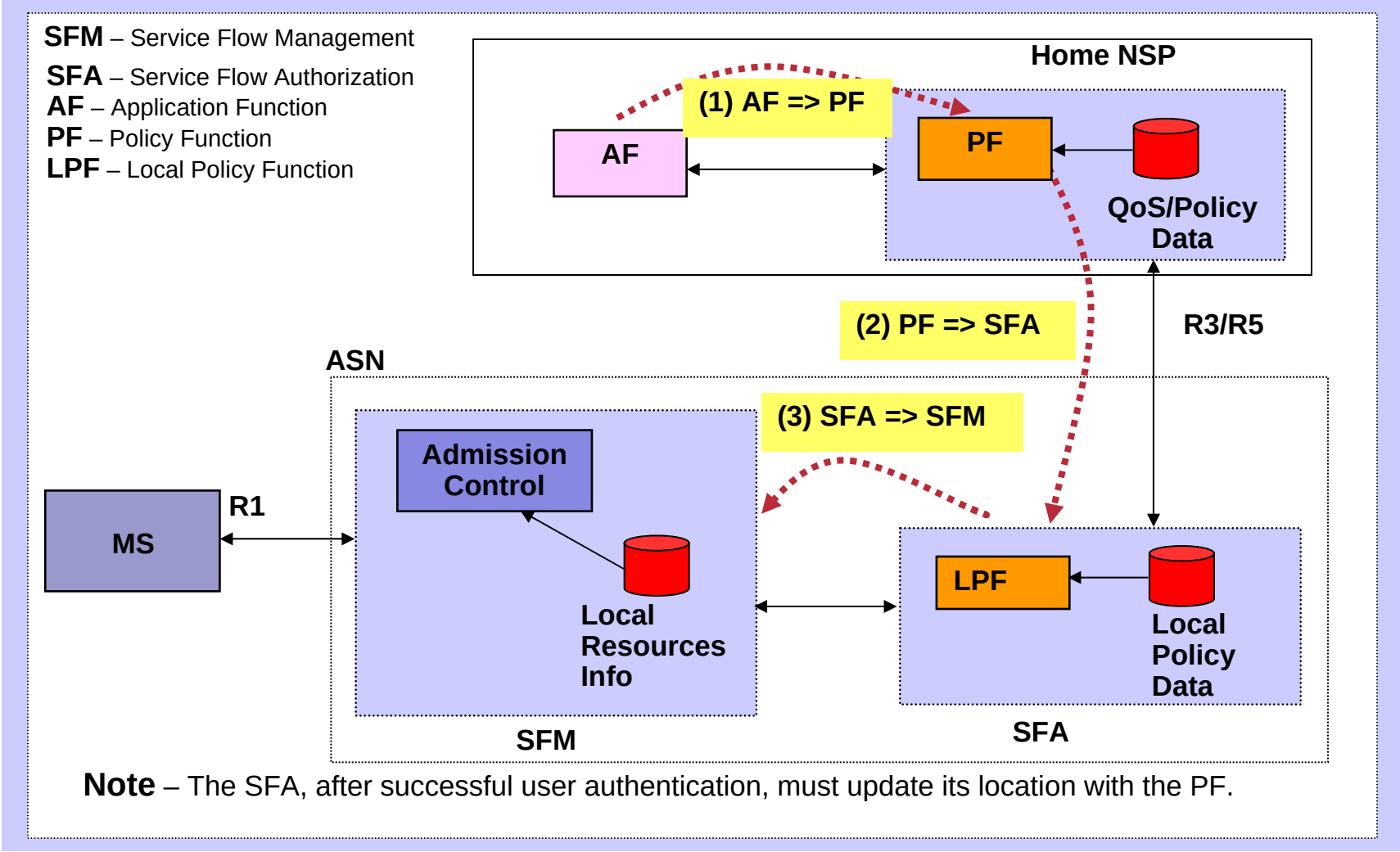


Stateful auto-configuration based on DHCPv6 [RFC3315]. The DHCP server is in the serving CSN and a DHCP relay must exist in the network path to the CSN.
Stateless auto-configuration as defined in RFC2462 and privacy extensions in RFC3041.

Usage Modes


Full Mobility
(e.g. Greenfield, 3G Overlay)
Portability / Simple Mobility
(e.g. Greenfield, DSL Overlay, 3G Overlay)
Fixed Access / Nomadicity
(e.g. DSL Overlay, Greenfield)
WiMAX architecture is designed to support evolution path from fixed to nomadic to portability with simple mobility and eventually to full mobility deployment with E2E QoS and Security support
Usage Modes: Representative of the types of profiles the WiMAX Forum may develop – to guide implementations and multi-vendor interoperability

QoS Framework



Note – The SFA, after successful user authentication, must update its location with the PF.

Mobility & Handover

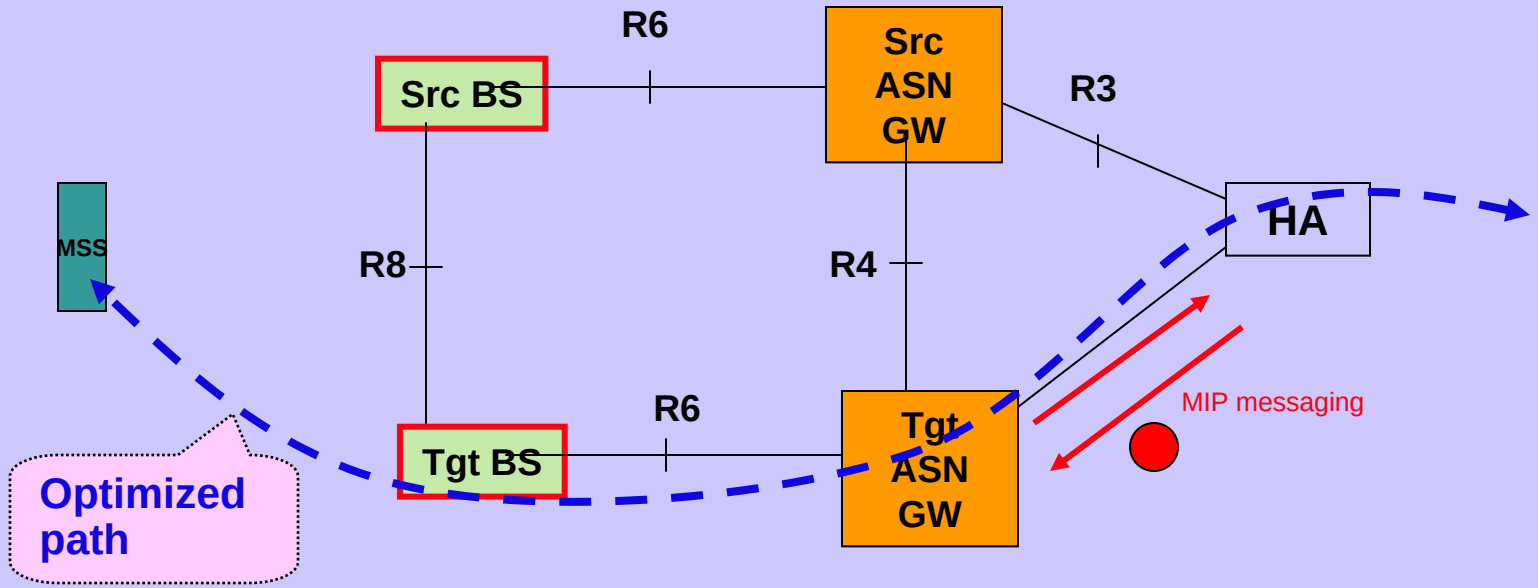
- The architecture must support intra-ASN micro-mobility
  - R6 Mobility
  - R8 Mobility (inter-BS handover)
- The architecture must support inter-ASN macro-mobility
  - R3 Mobility
  - R4 Mobility
- Intra/inter-ASN Mobility is to ensure minimal delay and data loss during the transition/handover from serving ASN to target ASN. This is done via transferring context (mobility, security, …) and all active service flows when handover occurs.

L3 Mobility – Anchored ASN

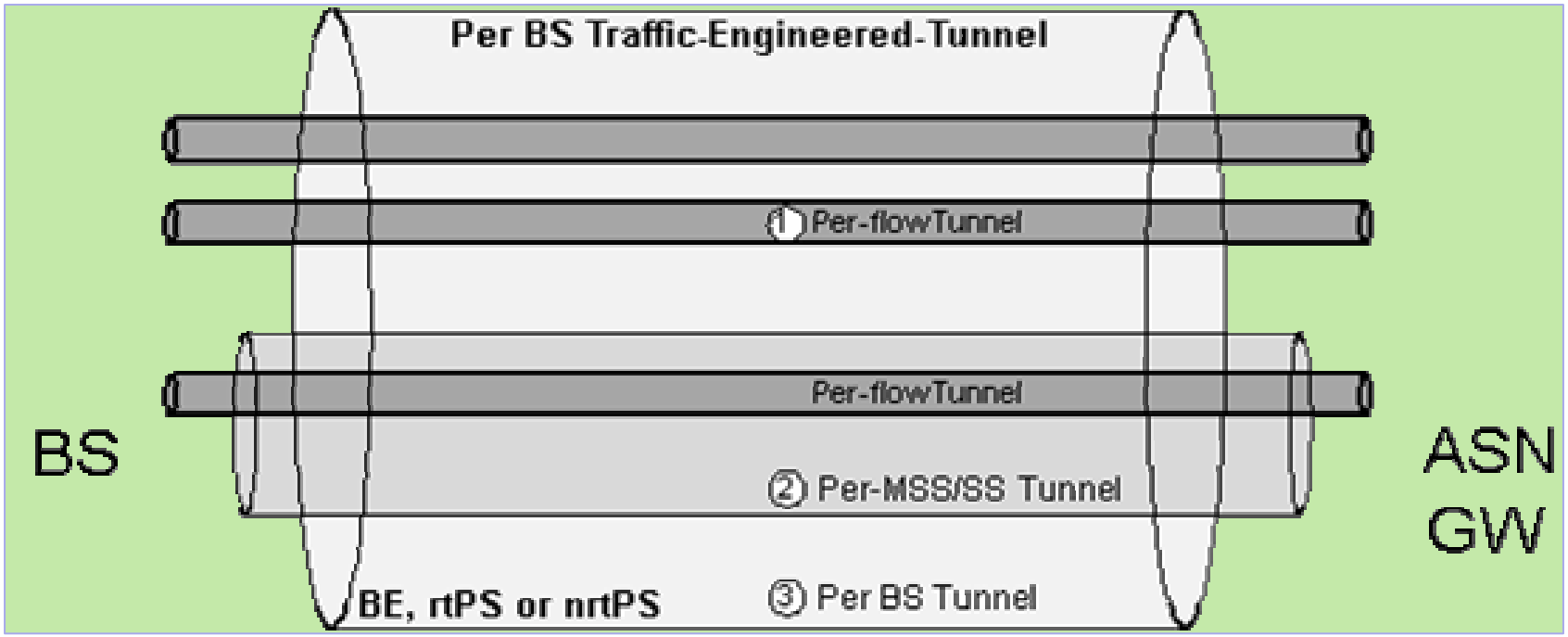
- **Proxy MIP (PMIP) - does not involve a change in the point of attachment address when the user moves. There is no need for the terminal to implement a client MIP stack.**
- **Client MIP (CMIP) - with a FA based CoA, the CoA point of attachment IP address can change with the Foreign Agent. Foreign Agent change can be detected by Agent Advertisement. For ASN mobility using client MIPv6 in a Co-located CoA mode (CoCoA), the point of attachment CoA changes when subnet changes.**
- **PMIP and CMIP can coexist in the network.**
- **MS should support either Mobile IP with CMIP or simple IP with PMIP.**
- **Network should support both CMIP and PMIP for coexistence**
- **R3 mobility is established between ASN and CSN that are in the same or different administrative domains.**
- **R4 mobility should allow for keeping an existing anchor ASN GW or re-anchoring at the target ASN GW.**

L3 Mobility - FA Migration

- Initiated by policy (e.g. for path optimization)
- Triggered by MIP Agent Advertisement
- MIP registration to new FA (ASN GW) – for PMIP and CMIP



R6 Mobility



R6 mobility should take into account different level of Data Path granularities: per-flow, user, and per-BS Data Paths. The Data Path is identified via the classification operation based on a set of classification criteria such as MS IP address.

Security

- WiMAX architecture must comply with the security and trust architecture defined in the IEEE 802.16 specification and IETF EAP RFCs.
- Authenticator is anchored during HO (e.g., in the ASN GW)
- Session is anchored at the first GW through which the MS connects to the network
- HA and Anchor GW have trust relationship with Home AAA
- Anchor GW and HA are in different administrative domains
- Trust relationship needs to be set up before signalling
- Home AAA distributes keys to Authenticator and HA
- Authenticator distributes AKs to the BSs
- HA has to authorize setup of forwarding path for MS to Anchor GW
- Signaling between HA and Anchor GW needs to be secure
- EAP packets carried between the EAP Relay (BS) and the Authenticator to populate channel binding attributes in the Authenticator
  - ASN is treated as a single NAS

What's Next?

- NWG Release 1 Schedule
  - Stage 2 is near completion
  - Stage 3 just started (Oct. 2005)
- Release 2 (tentative) Schedule
  - Stage 1 2Q06
  - Stage 2&3 4Q06
  - New Features
    - Legal Intercept
    - VoIP (full support)
    - IPv6 Mobility
    - IMS
    - BCMCS
    - Other features as requested by SPWG.

Backup Slides

Interfaces …

- **R1 – the interface between the MS and the ASN as per the air interface (PHY and MAC) specifications (IEEE P802.16d/e). R1 may include additional protocols related to the management plane.**
- **R2 – the interface between the MS and CSN associated with Authentication, Services Authorization, IP Host Configuration management, and mobility management. This is a logical interface thus does not reflect a direct protocol interface between MS and CSN.**
- **R3 – the interface between the ASN and the CSN to support AAA, policy enforcement and mobility management capabilities. It also encompasses the bearer plane methods (e.g., tunneling) to transfer IP data between the ASN and the CSN.**

Interfaces …

- **R4 – consists of 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.**
- **R5 – consists of a set of control plane and bearer plane protocols for internetworking between CSNs operated by either the home or visited NSP.**
- **R6 – consists of 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 ASN GW.**
  - **The control plane includes protocols for IP tunnel management (establish, modify, and release) in accordance with the MS mobility events. R6 may also serve as a conduit for exchange of MAC states information between neighboring BSs.**

Interfaces

- **R8 – consists of a set of control plane message flows and, in some situations, bearer plane data flows between the base stations to ensure fast and seamless handover.**
  - **bearer plane consists of protocols that allow the data transfer between Base Stations involved in handover of a certain MS.**
  - **control plane consists of the inter-BS communication protocol defined in IEEE 802.16 and additional set of protocols that allow controlling the data transfer between the Base Stations involved in handover of a certain MS.**

Quality of Service (QoS)

- IEEE QoS Framework
  - Deals with radio link (802.16) QoS
  - Connection-oriented service
  - Five QoS classes are defined
    - UGS: Unsolicited Grant Service
    - rtPS: real-time Polling Service
    - ertPS: enhanced real-time Polling Service
    - nrtPS: non-real-time Polling Service
    - BE: Best-Effort
  - Provisioned QoS profile for permitted flows per subscriber
  - Admission policies for new service flows
- NWG QoS Framework
  - Extends the 802.16 QoS framework to NWG NRM
  - Deals with WiMax QoS only (see next slide)
  - QoS control entities are placed either in the BS or ASN GW

QoS Models in Release 1

Push or Pull

- **Pre-Provisioned Service Flow - Static Push Model (steps 1-2)**
- **Dynamic Service Flow - triggered Push Model (or Push/Pull)**
- **Subscribed QoS profile is provisioned either in AAA DB or a policy server**
- **User priority may be used to enforce relative precedence for admitting new flows when radio resources are tight**

Triggers:

- **L2 User-initiated via IEEE 802.16 signaling**
- **L3 User-initiated on-path QoS signaling (e.g., RSVP)**
- **Network-initiated - Application Triggered (e.g., SIP proxy)**
- **Network-initiated - Administratively Triggered (e.g., SNMP)**