WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)

[Part 1]

Release 1.1.0

July 11, 2007

WiMAX Forum Proprietary

Copyright Notice, Use Restrictions, Disclaimer, and Limitation of Liability.

TABLE OF CONTENTS

TABLE OF FIGURES

1. Introduction and Scope

This document describes the architecture reference model, reference points and protocols and procedures for different end-to-end architecture aspects of WiMAX NWG. The framework is in response to the Stage 1 requirements document.

2. Definitions, and Conventions

2.1 Definitions

2.1.1 AAA

AAA refers to a framework, based on IETF protocols (RADIUS or Diameter), that specifies the protocols and procedures for authentication, authorization, and accounting associated with the user, MS, and subscribed services across different access technologies. For example, AAA includes mechanisms for secure exchange and distribution of authentication credentials and session keys for data encryption.

Location: ASN and CSN

2.1.2 Access Service Network (ASN)

Access Service Network (ASN) is defined as a complete set of network functions needed to provide radio access to a WiMAX subscriber. The ASN provides the following mandatory functions:

- WiMAX Layer-2 (L2) connectivity with WiMAX MS
- Transfer of AAA messages to WiMAX subscriber’s Home Network Service Provider (H-NSP) for authentication, authorization and session accounting for subscriber sessions
- Network discovery and selection of the WiMAX subscriber’s preferred NSP
- Relay functionality for establishing Layer-3 (L3) connectivity with a WiMAX MS (i.e. IP address allocation)
- Radio Resource Management

In addition to the above mandatory functions, for a portable and mobile environment, an ASN SHALL support the following functions:

- ASN anchored mobility
- CSN anchored mobility
- Paging
- ASN-CSN tunneling

ASN comprises network elements such as one or more Base Station(s), and one or more ASN Gateway(s). An ASN MAY be shared by more than one Connectivity Service Networks (CSN)

2.1.3 Accounting Agent

The Account Agent is defined as the functional entity which collects the related accounting information, such as the unsent downlink volume information to the MS and the airlink record information, etc.

Location: ASN

2.1.4 Admission Control

Admission Control is the ability to admit or ability to control admission of a user to a network based on user’s service profile and network performance parameters (for example, load and average delay). If a user requests access to network services but the incremental resources required to provide the grade of service specified in the user’s service profile are not available, the Admission Control function rejects the user’s access request. Note that Admission Control is implemented to ensure service quality and is different from authentication and authorization, which are also used to admit or deny network access.

Location: ASN and CSN

2.1.5 Application Service Provider (ASP)

Application Service Provider (ASP) is a business entity that provides applications or services via V-NSP or H-NSP.

2.1.6 ASN Anchored Mobility

ASN Anchored mobility refers to the set of procedures associated with the movement (handover) of an MS between two Base Stations (referred to in the IEEE 802.16 literature as Serving and Target BS), where the Target BS may belong to the same ASN or a different one, without changing the traffic anchor point for the MS in the serving (anchor) ASN. The associated procedures involve transferring the context of all service flows together with other context from the previous BS to the new BS while attempting to ensure minimal delay and data loss during the transition. ASN Anchored Mobility is mobility within the area of one or more ASNs without FA relocation, i.e. without R3 Mobility. This includes intra-ASN and inter-ASN MM as long as the “ASN R3 reference anchor point” in the NAP, and hence the FA, does not change.

Entities: MS and ASN

2.1.7 ASN Mobility

Same as ASN Anchored Mobility.

2.1.8 Authenticator

Authenticator functionality is defined as per standard EAP 3-party model. An authenticator is an entity at one end of a point-to-point link that facilitates authentication of supplicant (MS) attached to the other end of that link. It enforces authentication before allowing access to services that are accessible to the supplicant. The Authenticator also incorporates AAA client functionality that enables it to communicate with the AAA backend infrastructure (AAA-based Authentication Server) which provides the Authenticator with authentication services over AAA protocols. The Authenticator is always collocated with the Key Distributor and MAY be collocated with the Authentication Relay and Key Receiver functions as defined in Part 2 Section 7.4 – ASN Security Architecture.

2.1.9 Base Station

See Section 6.3.3

2.1.10 Connectivity Service Network (CSN)

Connectivity Service Network (CSN) is defined as a set of network functions that provide IP connectivity services to the WiMAX subscriber(s). A CSN MAY provide the following functions:

- MS IP address and endpoint parameter allocation for user sessions
- Internet access
- AAA proxy or server
- Policy and Admission Control based on user subscription profiles
- ASN-CSN tunneling support,
- WiMAX subscriber billing and inter-operator settlement
- Inter-CSN tunneling for roaming
- Inter-ASN mobility
- WiMAX services such as location based services, connectivity for peer-to-peer services, provisioning, authorization and/or connectivity to IP multimedia services and facilities to support lawful intercept services such as those compliant with Communications Assistance Law Enforcement Act (CALEA) procedures.

CSN MAY comprise network elements such as routers, AAA proxy/servers, user databases, Interworking gateway MSs. A CSN MAY be deployed as part of a Greenfield WiMAX NSP or as part of an incumbent WiMAX NSP.

2.1.11 CSN Anchored Mobility

CSN Anchored mobility refers to a set of procedures for changing the traffic anchor point for the MS from one anchor point to another one in the ASN without changing the CSN anchor. CSN anchored mobility is independent to the .16e handover.

Entities: MS, ASN, CSN

2.1.12 Ethernet Support

Ethernet support refers to a transport that carries encapsulated IPv4 or IPv6 addressing or other payload and encapsulation of end-user data sessions. Ethernet support includes IEEE802.3, IEEE802.1D and IEEE802.1Q. Ethernet MAY be tunneled using MPLS, IPsec, GRE or other tunneling protocols. Ethernet support in WiMAX network MAY operate in two variations:

- End-to-End Ethernet connectivity from the WiMAX SS/MS across WiMAX network (e.g. for connectivity to DSL networks with PPPoE). This option does not support Macro Mobility.
- Ethernet support within the ASN segment only. This support allows Ethernet transport between WiMAX SS/MS and ASN.

Location: MS, ASN, and CSN

2.1.13 Firewall

A firewall provides protection to network elements by enforcing access and filter policies used to monitor and control traffic to and from a network. It can be viewed as a set of rules and policies that determine which traffic should be permitted to go through or blocked. One of its main purposes is to detect and prevent Denial of Service (DoS) attacks on a network.

Location: ASN, CSN, and possibly the ASP Network's infrastructure

2.1.14 Home Network Service Provider (H-NSP)

A home NSP is the operator or business entity that has Service Level Agreements with WiMAX subscribers, authenticates and authorizes subscriber sessions (in-network or roaming scenarios) and services the subscriber's account (charging and billing). To support roaming services, a Home NSP MAY have roaming relationships with other NSPs.

2.1.15 Internet Access

Internet access refers to a gateway that resides at the edge of NAP or NSP network connecting it to Internet. Apart from the IP routing functionality, such gateways MAY include functions such as VPN, Firewall, NAT, layer-4 forwarding, and mobile IPv4 home agent. Alternatively, these functions MAY be implemented in network elements that are either in front of or behind the gateway. Certain deployments MAY also implement functions such as metering and policing as part of Internet Access.

2.1.16 Internetworking Function

An Internetworking Function (IWF) or an Internetworking Unit (IWU) is a network entity that translates one or more communication protocols (data and/or control) from one form to another. An IWU enables integration or interoperability between different types or generations of networks and/or services. For example, an IWU terminating a WiMAX NWG-specified reference point MAY facilitate interoperability between a Greenfield WiMAX network and an incumbent 3G network.

Location: This function resides in the CSN.

2.1.17 IP Header Compression

Header compression is a function to reduce the size of the headers of the packets and increase the overall communication performance between a pair of communication nodes.

Location: MS and ASN

2.1.18 IP Support

IP Support refers to the capability of the WiMAX network to transport IPv4 and IPv6 datagrams as end to end managed session between the WiMAX SS/MS and any IP peer across WiMAX network. IP support does not require any additional L2 encapsulation over the air except for 802.16e and MAY be tunneled in WiMAX network using GRE, MPLS, VLAN or other tunneling protocols.

2.1.19 IPv4 Support

IPv4 support refers to a set of capabilities that enable IPv4 addressing and encapsulation of end-user data sessions. The IPv4 encapsulation MAY directly encapsulate an IPv4-compatible application protocol running over IP transports, such as FTP, SIP, SMTP or HTTP. Alternatively, it MAY encapsulate tunneled end-user data as in the cases of Mobile IP, IPsec or GRE. The end-user IPv4 session MAY in turn be encapsulated within the NAP and NSP networks in an IPv6 tunnel, so long as the IPv6 cladding is removed prior to the delivery of its IPv4 contents. IPv4 Support does not guarantee performance of any particular end-user IPv4 flow, only that the flow will be conveyed between any two nodes in the NAP or NSP networks in a manner logically consistent with IPv4.

Location: MS, ASN, CSN and ASP Network infrastructure

2.1.20 IPv6 Access Router (AR)

The IPv6 AR is the first hop router for an IPv6 MS in the ASN. The IPv6 link exists between the MS and the IPv6 AR and is established via a combination of the transport connection over the air interface (R1) and the GRE tunnel between the BS and ASN-GW functions when implemented in separate physical entities.

2.1.21 IPv6 Support

IPv6 support is a set of capabilities enabling IPv6 addressing and encapsulation of end-user data sessions. The IPv6 encapsulation MAY directly encapsulate an IPv6-compatible application protocol running over IP transports, such as FTP, SIP, SMTP or HTTP. Alternatively, it MAY encapsulate tunneled end-user data as in the case of GRE. The end-user IPv6 session MAY in turn be encapsulated within the NAP and NSP networks in an IPv4 tunnel, so long as the IPv4 cladding is removed prior to the delivery of its IPv6 contents. IPv6 support does not guarantee the performance of any particular end-user IPv6 flow, only that the flow will be conveyed between any two nodes in the NAP or NSP networks in a manner logically consistent with IPv6.

Location: MS, ASN, CSN and ASP Network infrastructure

2.1.22 Location-Based Service (LBS)

A location-based service (or LBS) is a service provided to a subscriber based on the current geographic location of the WiMAX client MS.

Location: CSN or ASP Network and MS

2.1.23 Media Gateway

A media gateway is an entity that converts media formats in order to provide compatibility between two networks. . For example, a media gateway could terminate bearer channels from a switched circuit network (e.g., DS0s) and media streams from a packet network (e.g., RTP streams in an IP network). A media gateway MAY be capable of processing audio, video and T.120 alone or in any combination, and MAY be capable of full duplex media translations. Additionally, a media gateway MAY also play audio/video messages and support interactive voice response features, or MAY perform media conferencing.

Location: CSN or existing core network in an Interworking scenario

2.1.24 Mobile Station (MS)

Generalized mobile equipment set providing connectivity between subscriber equipment and a base station (BS). The Mobile Station MAY be a host or a CPE type of device that supports multiple hosts..

2.1.25 NAS

The term NAS refers to the grouping of the following functions in the ASN:

* EAP Authenticator

* The Prepaid Client

* Hot-line Device

* AAA client

* Accounting Client

In addition to the above, the NAS maintains and distributes keys received from the AAA infrastructure to various other functions in the ASN and for that reason may also be labeled Anchor Authenticator.

2.1.26 Network Access Provider (NAP)

Network Access Provider (NAP) is a business entity that provides WiMAX radio access infrastructure to one or more WiMAX Network Service Providers (NSPs). A NAP implements this infrastructure using one or more ASNs.

2.1.27 Network Discovery and (Re)selection

Network Discovery and (Re)selection refers to protocols and procedures where the MS detects the existence of one or more NAPs owned by or affiliated with the subscriber's home NSP (directly or through a roaming partner) and selects a NAP based on its local policy to gain access to IP data services.

Location: MS and ASN

2.1.28 Network Management

Network management refers to a variety of tools, applications, and MSs that assist human network managers in monitoring and maintaining networks. The fundamental classes of management operations are typically described as Fault, Configuration, Accounting, Performance and Security (FCAPS).

Most network management architectures use the same basic structure and set of relationships. Managed MSs, such as computer systems and other network MSs, run software (typically referred to as an agent) that enables network managers to query information from agents or be notified when they recognize problems (for example, when one or more user-determined thresholds are exceeded). Upon receiving these alerts, management entities are programmed to react by executing one, several, or a group of actions, including operator notification, event logging, system shutdown, and automatic attempts at system repair.

Location: The ASN, CSN and ASP infrastructure will nominally have independent network management functions. Mechanisms to query and process the management information bases MAY be centralized or distributed.

2.1.29 Network Service Provider (NSP)

Network Service Provider (NSP) is a business entity that provides IP connectivity and WiMAX services to WiMAX subscribers compliant with the Service Level Agreement it establishes with WiMAX subscribers. To provide these services, an NSP establishes contractual agreements with one or more NAPs. Additionally, an NSP MAY also establish roaming agreements with other NSPs and contractual agreements with third-party application providers (e.g., ASP or ISPs) for providing WiMAX services to subscribers.

From a WiMAX subscriber standpoint, an NSP MAY be classified as Home NSP (H-NSP) or Visited NSP (V-NSP).

2.1.30 Paging

Paging refers to procedures used by the network to seek an MS in idle mode in the coverage area of a predefined set of Base Station(s) identified by a Paging Group (as per IEEE 802.16e specification). In addition, Paging Update refers to procedures to obtain location update or network entry from an MS in idle mode. Paging procedures are implemented using Paging MAC message exchanges between MS and BS, under the control of a higher-layer paging management functions.

Location: ASN and MS

2.1.31 Payload Compression

Payload compression is a function to reduce the size of datagram payloads and increase the overall communication performance between a pair of communication nodes. Examples of payload compression protocols include the use of [37] over IP transport.

Location: The payload compression function and its protocol SHALL be running between two communicating peers.

2.1.32 Peer-to-Peer Service

Peer-to-peer or point-to-point services are IP services delivered to MS using a point-to-point IP-connectivity bearer channel. The correspondent node to MS for such services MAY be another MS or a network server. Examples of such services include peer-to-peer file-sharing, VoIP, gaming, etc.

Location: MS, CSN, or ASP Network

2.1.33 Point of Attachment Address (PoA)

A Point of Attachment (PoA) address refers to the IP address, routable in CSN domain that is allocated to MS for the purpose of data connectivity. For fixed, nomadic and PMIP-based access, the PoA address is delivered to MS using DHCP. For CMIPv4-based mobile SS/MSs, the PoA address is delivered using MIP-based procedures. For MIPv4-based access, a PoA address refers to Home Address. For MIPv6 based access, a PoA may refer to the CoA or HoA

2.1.34 Power Management

There are two aspects of power management:

- **MS platform power management** – This refers to efficient allocation of Sleep and Idle modes to an MS with the intention of maximizing battery life while minimizing disruption to communication flows between an MS and the network. Sleep and Idle modes are described in the 802.16e specification.
- **MS transmit power management** – This refers to the management of MS transmit power based on one or more factors with the intent to conserve battery resources while not impacting communication flows between an MS and the network.

Location: MS and ASN

2.1.35 QoS Enforcement and Admission Control

QoS enforcement and admission control refers to procedures that ensure QoS in the ASN infrastructure comprising infrastructure provided by more than one Service Provider or third-party carrier. These functions include QoS profile authorization, QoS admission control, Policy Enforcement Point (PEP), Policy Decision Functions (PDF), policing and monitoring, QoS parameter mapping across different QoS domains, etc. These procedures MAY reside within a network or distributed across networks.

Location: MS, ASN, CSN, and ASP Network

2.1.36 Radio Resource Management (RRM)

Radio Resource Management refers to *measurement*, *exchange*, and *control* of radio resource-related indicators (e.g., current subchannel allocations to service flows) in a wireless network.

Measurement refers to determining values of standardized radio resource indicators that measure or assist in estimation of available radio resources.

Exchange refers to procedures and primitives between functional entities used for requesting and reporting such measurements or estimations. The resulting information from exchange MAY be made available within the measuring station (using proprietary procedures and primitives), or, to a remote functional entity (using standardized procedures and primitives).

Control refers to decisions made by the measuring station or remote entity to adjust (i.e., allocate, reallocate or deallocate) radio resources based on the reported measurements, other information, or using proprietary algorithms, and communicating such adjustments to network entities using standardized primitives. Such control MAY be local and remote from the measuring station.

Location: MS and ASN

2.1.37 Reference Point

A reference point (RP) is a conceptual link that connects two groups of functions that reside in different functional entities of an ASN, CSN, or MS. It is not necessarily a physical interface. A reference point only becomes a physical interface when the functional entities on either side of it are contained in different physical MSs.

2.1.38 Roaming

Roaming is the capability of wireless networks via which a wireless subscriber obtains network services using a "visited network" operator's coverage area. At the most basic level, roaming typically requires the ability to reuse authentication credentials provided/provisioned by the home operator in visited networks, successful user/MS authentication by the home operator, and a mechanism for billing reconciliation and optionally access to services available over the Internet services. A key benefit of roaming is to provide a wider coverage and access to subscribers of an operator with consolidated/common billing.

Location: MS, ASN, and CSN

2.1.39 Service Level Agreement (SLA)

A Service Level Agreement (SLA), as defined in [8] is "a contract between a network's provider and user or between network providers that defines the service level which a user will see or an operator can obtain and the cost associate with that level of service".

2.1.40 Session Management

At a fundamental level, a session refers to link-layer, IP-layer, or, higher layer connectivity established between one or more MS and a network element in order to exchange link-level frames or packets. Additionally, a session MAY have certain well-defined properties associated with it such as traffic characteristics (e.g., traffic type, policy, encryption), mobility support (e.g., re-authentication, re-keying, routing), and robustness (e.g., state management, persistence). Session management generically refers to the set of procedures implemented in MS and the network that support all such properties associated with an active session.

Location: MS and ASN or CSN or ASP Network

2.1.41 SLA Management

SLA management refers to procedures that translate a Service Level Agreement into a set of QoS parameters and their values, which together define the service offered.

Location: This function MAY be located between ASN and CSN, CSN and ASP's infrastructure, or between CSNs of two NSPs.

2.1.42 MS IP Address Management

IP address assignment is typically done after the MS is authenticated and authorized to the network. The IP address allocated to an MS may be public or private, and may either be a point-of-attachment IP address or an inner-tunnel IP address. For the basic-connectivity IP service, the IP address is assigned by the CSN (incumbent or reference). For IP services accessible over an inner-tunnel, the network that terminates the tunnel allocates the IP address.

Location: MS and CSN

2.1.43 Subscriber Station

Generalized stationary equipment set providing connectivity between subscriber equipment and a base station (BS). The Subscriber Station may be a host or support multiple hosts.

2.1.44 Tunneling

Tunneling refers to the capability that enables two packet networks to exchange data or packets via intermediate networks, while hiding the protocol details from the intermediate networks. Tunneling is generically implemented by encapsulating an end-to-end network protocol within packets that are natively carried over the intermediate networks. For example, Point-to-Point Tunneling Protocol (PPTP) is a technology that enables organizations to use the Internet to transmit private data across a VPN. It does this by embedding its own network protocol within the TCP/IP packets carried by the Internet. Tunneling is alternately referred to as encapsulation.

Location: MS and CSN and/or ASP's infrastructure.

2.1.45 Visited Network Service Provider (V-NSP)

A visited NSP is defined from a roaming WiMAX subscriber standpoint. A roaming subscriber uses the visited NSP's coverage area for access to WiMAX services. A visited NSP may have roaming relationship with subscriber's home NSP. The visited NSP provides AAA traffic routing to home NSP. Depending on WiMAX services requested and the roaming agreement between home NSP and visited NSP, the visited NSP MAY provide some/all WiMAX services to roaming WiMAX subscriber or provide data/control traffic routing to home NSP.

2.2 Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [10].

3. References

[1] IEEE 802.16-2004 October 2004, Air Interface for Fixed and Mobile Broadband Wireless Access Systems — Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, August 2004.

[2] IEEE 802.16-2005 and IEEE 802.16-2004/Cor 1-2005, Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, February 2006

[3] Public EtherType Field Listings, http://www.iana.org/assignments/ethernet-numbers

[4] RFC792 - Internet Control Message Protocol (ICMP), J. Postel, September 1981,

[5] RFC826 - An Ethernet Address Resolution Protocol (ARP), David C. Plummer, November 1982.

[6] RFC1027 - Using ARP to Implement Transparent Subnet Gateways, Smoot Carl-Mitchell and John S. Quarterman, October 1987

[7] RFC1349 – Type of Service in the Internet Protocol Suite, P. Almquist, July 1992.

[8] RFC1678 - IPng Requirements of Large Corporate Networks, E. Britton and J. Tavs, August 1994, Informational

[9] RFC1701 - Generic Routing Encapsulation (GRE), S. Hanks, et al., October 1994, Informational

[10] RFC2119 – Key words for use in RFCs to Indicate Requirement Levels, S. Bradley, March 1997, Best Current Practice

[11] RFC2131 – Dynamic Host Configuration Protocol (DHCP), R. Droms, March 1997, Standards Track

[12] RFC2132 – DHCP Options and BOOTP Vendor Extensions, S. Alexander and R. Droms, March 1997, Standards track

[13] RFC2205 – Resource ReSerVation Protocol (RSVP), R. Braden, et al., September 1997, Standards track

[14] RFC2327 – SDP: Session Description Protocol, M. Handley and V. Jacobson, April 1998, Standards Track

[15] RFC2461 – Simpson, Neighbor Discovery for IP Version 6 (IPv6), Narten and Nordmark, December 1998, Standards Track

[16] RFC2462 – IPv6 Stateless Address Auto-configuration, Thomson and Narten, December 1998, Standards Track

[17] RFC2474 – Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers, K. Nichols, et al., December 1998, Standards Track

[18] RFC2475 – Architecture for Differentiated Services, S. Blake, et al., December 1998, informational

[19] RFC2597 – Assured Forwarding PHB Group, J. Heinanen, et al., June 1999, Standards Track

[20] RFC2598 – Expedited Forwarding PHB Group, V. Jacobson, et al., June 1999, Standards Track

[21] RFC2748 – The COPS (Common Open Policy Service) Protocol, D. Durham, et al., January 2000, Standards Track

[22] RFC2794 – Mobile IP Network Access Identifier Extension for IPv4, P. Calhoun and C. Perkins, March 2000, Standards Track

[23] RFC2865 – Remote Authentication Dial In User Service (RADIUS), C. Rigney, et al., June 2000, Standards Track

[24] RFC2866 – RADIUS Accounting, C Rigney and Livingston, June 2000, Informational

[25] RFC2904 – AAA Authorization Framework, J. Vollbrecht, et al., August 2000, Informational

[26] RFC2905 – AAA Authorization Application Examples, J. Vollbrecht, et al., August 2000, Informational

[27] RFC2906 – AAA Authorization Requirements, S. Farrell, et al., August 2000, Informational

[28] RFC3012 – Mobile IPv4 Challenge/Response Extensions, C. Perkins and P. Calhoun, November 2000, Standards Track

[29] RFC 3024 – Reverse Tunneling for Mobile IP, revised, G. Montenegro, January 2001, Standards track

[30] RFC3041 – Privacy Extensions for Stateless Address Autoconfiguration in IPv6, Narten, Draves, January 2001, Standards Track

[31] RFC3046 – DHCP Relay Agent Information Option, M. Patrick, January 2001, Standards Track

[32] RFC3084 – COPS Usage for Policy Provisioning (COPS-PR), K. Chan, et al., March 2001, Standards Track

[33] RFC3115 – Mobile IP Vendor/Organization-specific extensions, G. Dommety and K. Leung, April 2001, Standards Track

[34] RFC3118 – Authentication for DHCP Messages, R. Droms and W. Arbaugh, June 2001, Standards Track

[35] RFC3159 – Structure of Policy Provisioning Information (SPPI) K. McCloghrie, et al., August 2001, Standards Track

[36] RFC3162 - RADIUS and IPv6, B. Aboba, et al., August 2001, Standards Track

[37] RFC3173 - IP Payload Compression Protocol (IPComp), A. Shacham, et al., September 2001, Standards Track

[38] RFC3203 – DHCP Reconfigure Extension, Y. T'Joens, et al., December 2001, Standards Track

[39] RFC3264 – An Offer/Answer Model with the Session Description Protocol (SDP), J. Rosenberg and H. Schulzrinne, June 2002, Standards Track

[40] RFC3312 – Integration of Resource Management and Session Initiated Protocol, G. Camarillo, et al., October 2002, Standards Track

[41] RFC3313 – Private Session Initiation Protocol (SIP) Extensions for Media Authorization, W. Marshall, January 2003, Informational

[42] RFC3315 – Dynamic Host Configuration Protocol for IPv6 (DHCPv6, R. Droms, et al., July 2003, Standards Track

[43] RFC3344 – Mobile IP support for IPv4, C. Perkins, August 2002, Standards Track

[44] RFC3520 – Session Authorization Policy Element, L-N. Hamer, et al., April 2003, Standards Track

[45] RFC3543 - Registration Revocation in Mobile IPv4, S. Glass and M. Chandra, August 2003, Standards Track

[46] RFC3556 – Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth, S. Casner, July 2003, Standards Track

[47] RFC3565 - Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS), J. Schaad, July 2003, Standards Track

[48] RFC3576 - Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), M. Chiba, et al., July 2003, Informational

[49] RFC3579 – RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP), B. Aboba and P. Calhoun, September 2003, Informational

[50] RFC3588 – Diameter Base Protocol, P. Calhoun, et al., September 2003, Standards Track

[51] RFC3736 – Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6, R. Droms, April 2004, Standards Track

[52] RFC3748 – Extensible Authentication Protocol, B. Aboba, et al., June 2004, Standards Track

[53] RFC3775 – Mobility Support in IPv6, D. Johnson, C. Perkins, J. Arkko, June 2004, Standards Track

[54] RFC3776 – Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents, J. Arkko, V. Devarapalli, F. Dupont, June 2004, Standards Track

[55] RFC3957 – Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4, C. Perkins and P. Calhoun, March 2005, Standards Track

[56] RFCaaaa – draft-adrangi-eap-network-discovery-14.txt, Network Discovery and Selection within the EAP Framework, F. Adrangi, et al., August 2005, Informational (RFC Editor's Queue)

[57] draft-ietf-eap-netsel-problem-05.txt

[58] RFC4285 –Authentication Protocol for Mobile IPv6, A. Patel, et al., January 2006, Informational

[59] RFC4283 –Mobile Node Identifier Option for MIPv6, A. Patel, et al., November 2005, Standards Track

[60] RFC4282 –The Network Access Identifier, B. Aboba, et al., December 2005, Standards Track

[61] draft-ohba-eap-aaakey-binding-01.txt

[62] TR-025 – DSL Forum, "Core Network Architecture for Access to Legacy Data Network over ADSL", Nov-1999

[63] TR-044 – DSL Forum , "Auto-Config for Basic Internet (IP-based) Services, " Nov-2001

[64] TR-059 – DSL Forum, "DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services," Sept-2003

[65] 3GPP TR 22.934 V6.2.0 (2003-09) "Feasibility Study on 3GPP system to Wireless Local Area Network (WLAN) interworking (Release 6)"

[66] 3GPP TR 23.981 V6.3.0 (2005-03) "Interworking aspects and migration scenarios for IPv4 based IMS Implementations"

[67] 3GPP TS 23.002 V6.9.0 (2005-10) "Technical Specification Group Services and Systems Aspects; Network architecture (Release 6)"

[68] 3GPP TS 23.234 V6.5.0 (2005-06) "3GPP system to Wireless Local Area Network (WLAN) interworking; System description (Release 6)"

[69] 3GPP TS 23.207 V6.6.0 (2005-10) "End-to-end Quality of Service (QoS) concept and architecture (Release 6)"

[70] 3GPP TS 23.228 V6.10.0 (2005-06) "IP Multimedia Subsystem (IMS); Stage 2, (Release 6)"

[71] 3GPP TS 24.229 V6.8.0 (2005-10) "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 6)"

[72] 3GPP TS 24.234 V6.3.0 (2005-06) "3GPP System to Wireless Local Area Network (WLAN) interworking; User Equipment (UE) to network protocols; Stage 3 (Release 6)"

[73] 3GPP TS 29.234 V6.4.0 (2005-10) "3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3"

[74] 3GPP TS 33.234 V6.5.1 (2005-06) "Wireless Local Area Network (WLAN) interworking security (Release 6)"

[75] TR-101 - DSL Forum, "Migration to Ethernet-Based DSL Aggregation", Apr-2006

[76] 3GPP2 X.S0013-000-0 v2.0 "All-IP Core Network Multimedia Domain – Overview," Aug-2005

[77] 3GPP2 X.S0013.00200 v1.0 "All-IP Core Network Multimedia Domain: IP Multimedia Subsystem Stage 2," Feb-2004

[78] 3GPP2 X.S0013-004-0 v1.0 "All-IP Core Network Multimedia Domain: IP Multimedia Call Control Protocol Based on SIP and SDP Stage 3," Feb-2004

[79] WiMAX Service Provider Working Group Requirements Document, "SPWG_Requirements_10182005," Most Current Version

[80] IEEE 802.16g /D9, April 2007.

[81] RFC 4017 – EAP Method Requirements for Wireless LAN, D. Stanley, J. Walker, B. Aboba, March 2005, Informational.

4. Identifiers

4.1 Identifiers Used in Stage-2 document

4.1.1 Introduction

This section provides at one place a list of various identifiers used in a WiMAX network. The following table is an exhaustive list of those identifiers. Each identifier is accompanied with a few key attributes (like scope, size, etc.) and a short description on its usage.

4.1.2 List of Identifiers

<table>
<tr><th>Identifier</th><th>Type</th><th>Size</th><th>Definition (Stage-2 section or reference to external source)</th><th>Scope (area of validity)</th></tr>
<tr><td rowspan="2">MS ID</td><td>binary</td><td>48 bit</td><td>IEEE 802.16-2004 and IEEE 802.16e-2005 [1] and [2]</td><td>Global</td></tr>
<tr><td colspan="4">Each WiMAX subscriber station is provisioned with a unique 48-bit MAC address by the manufacturer. It is used in 802.16 management messages to address the MS prior to allocation of CIDs. It is transferred as part of context during handover.</td></tr>
<tr><td rowspan="2">NAI</td><td>character</td><td>variable up to 253 bytes</td><td>RFC 4282 [60]</td><td>Global</td></tr>
<tr><td colspan="4">NAI is allocated to a WiMAX subscriber by its home operator and serves as primary ID for AAA purposes. WiMAX networks use NAI as defined in [60] instead of RFC2486 because the draft allows for decorated NAIs which are necessary for roaming. Although actually separate name space, NAIs are administered together with FQDNs.</td></tr>
<tr><td rowspan="2">HoA</td><td>binary</td><td>4 octets / 16 octets</td><td>Section 2.1.33</td><td>Global / NSP</td></tr>
<tr><td colspan="4">HoA belongs to the address range allocated to the NSP. It is either a globally valid IPv4 or IPv6 address or allocated from the private address space range. In the second case its scope is CSN. HoA's primary use is to route MS's IP packets from internet to home or visited CSN. The CSN uses tunneling to deliver packets to ASN. HoA is also used for classifications to determine the tunnel tag.</td></tr>
<tr><td rowspan="2">Flow ID</td><td>binary</td><td>variable</td><td>Part 2 Section 7.4</td><td>MS</td></tr>
<tr><td colspan="4">Used by the accounting framework to identify IP flows in primitives between CSN and ASN. Packet Data Flow ID always identifies a single unidirectional or bidirectional flow. A unidirectional Packet Data Flow ID maps to a single SFID while bidirectional Packet Data Flow ID maps to exactly two SFIDs. Packet Data Flow ID is always allocated by AAA server.</td></tr>
<tr><td rowspan="2">Service flow ID (SFID)</td><td>binary</td><td>32 bit</td><td>IEEE 802.16-2004 and IEEE 802.16e-2005 [1] and [2]</td><td>MS</td></tr>
<tr><td colspan="4">Each service flow represents a single unidirectional WiMAX radio interface connection with guaranteed QoS parameters. Service flows could be pre-provisioned or dynamically created. SFID doesn't change during Intra-NAP handover. Note that Service Flows according 802.16 should not be confused with Service Flows as used in QoS Framework of IETF.</td></tr>
</table>

Identifier	Type	Size	Definition (Stage-2 section or reference to external source)	Scope (area of validity)
Connection ID (CID)	binary	16 bit	IEEE 802.16-2004 and IEEE 802.16e-2005 [1] and [2]	BS
	CID represents a unidirectional connection between BS and MS and it is used to address the MS when it is attached to a BS.			
Data Path ID	binary	variable	7.7	NAP
	Data Path ID is used to identify the tunnel carrying MS traffic between ASN gateways or between the ASN gateway and base station. This specification allows only for GRE key to be used as data path ID.			
HO ID	binary	8 bit	IEEE 802.16-2004 and IEEE 802.16e-2005 [1] and [2]	Target BS
	Allocated by target BS and used instead of MS MAC to send the RNG_REQ during network re-entry for non-contention based ranging. Used for R6/R8 and R4 MM.			
Paging Controller ID	binary	48 bit	IEEE 802.16-2004 and IEEE 802.16e-2005 [1] and [2]	NAP
	Paging controller ID is a unique identity of a network entity which retains the MS state and operational parameters while MS is in idle mode. The Paging Controller ID parameter is signaled by MS during network re-entry and location update procedures.			
PG ID	binary	16 bits	IEEE 802.16-2004 and IEEE 802.16e-2005 [1] and [2]	NAP
	Base stations are organized into paging groups, and each group is assigned a paging group ID. When the subscriber is paged, it is paged in all base stations belonging to its current paging group.			
BS ID	binary	48 bit	IEEE 802.16-2004 and IEEE 802.16e-2005 [1] and [2]	Global
	BS ID is a global unique identifier for a WiMAX base station, as defined in the IEEE 802.16-2004 and IEEE 802.16-2005 standard represents one logical instance of a PHY and MAC function providing 802.16 radio connectivity services to an SS/MS (equivalent to a single frequency sector of a physical base station). The upper 24 bits contain unique identifier of a NAP (NAP ID), while lower 24 bits are used to differentiate between NAP's base stations. BS ID is programmable and is regularly broadcasted by the PHY/MAC in the DL-MAP message. Note that a physical multi-sector cell site implementation SHALL include multiple BS IDs.			
Operator ID	binary	24-bit	IEEE 802.16-2004 and IEEE 802.16e-2005 [1] and [2]	Global
	Operator ID is a globally unique identifier of WiMAX network access provider, and is alternatively termed NAP ID. The upper 24 bits of BS ID always contain operator ID of the NAP.			

<table>
<tr><th>Identifier</th><th>Type</th><th>Size</th><th>Definition (Stage-2 section or reference to external source)</th><th>Scope (area of validity)</th></tr>
<tr><td rowspan="2">NSP ID</td><td>binary</td><td>24 bit</td><td>Part 2 Section 7.1.4.2</td><td>Global</td></tr>
<tr><td colspan="4">NSP ID is a globally unique identifier of a WiMAX network service provider. NSP ID(s) is broadcasted on a regular basis by a base station, and it can be also solicited by the MS.</td></tr>
<tr><td rowspan="2">Anchor Data Path FunctionID</td><td>binary</td><td>4 /6 / 16 octets</td><td>7.7</td><td>NAP</td></tr>
<tr><td colspan="4">Uniquely identifies the ASN GW to which the CSN sends the downlink user plane traffic.</td></tr>
<tr><td rowspan="2">Authenticator ID</td><td>binary</td><td>4 /6 / 16 octets</td><td>Delivered in Intra ASN primitives (e.g. micro mobility, paging)</td><td>NAP/NSP</td></tr>
<tr><td colspan="4">IP address or other ID for the Authenticator.</td></tr>
</table>

4.2 Network Addressable Identifiers for Inter-ASN Communications

When several ASNs are engaged in communication, they may use the following four Identifiers in order to address the network entities located within the communicating ASNs:

1. Base Station ID
2. Authenticator ID
3. Anchor Data Path Function ID (Anchor ASN GW ID in profiles A&C and ASN ID in profile B)
4. Paging Controller ID

These Identifiers are referred to as Network Addressable Identifiers. Network Addressable Identifier is a generic term. It can take form of 6-octet IEEE 802.16e Identifier (e.g. BS ID, PC ID), IPv4 Address or IPv6 Address.

5. Tenets for WiMAX Network Systems Architecture

The tenets presented in this section are independent of particular releases of the WiMAX Network Systems Architecture.

5.1 General

a. The architecture framework and Network Reference Model (NRM) SHALL accommodate all WiMAX-based usage models as defined in the Stage 1 requirements specification [79].

b. The WiMAX architecture, based on a packet-switched framework, SHALL be based on the IEEE 802.16 standard and its amendments and use appropriate IETF RFCs and IEEE Ethernet standards. In the event that currently defined IETF protocols do not satisfy a solution requirement, extensions (some possibly unique to WiMAX) MAY be specified.

c. The architecture framework SHALL permit decoupling of access architecture (and supported topologies) from connectivity IP services and consider network elements of the connectivity serving network (CSN) agnostic to the IEEE 802.16 radio specifics.

d. The WiMAX network architecture framework SHALL be based on functional decomposition principles (i.e. decomposition of features into functional entities across interoperability reference points, without specific implementation assumptions including the notion of network entities and interfaces). Such a framework SHALL be modular and flexible enough to accommodate a broad range of deployment options such as:

   - Small-scale to large-scale (sparse to dense radio coverage and capacity) WiMAX networks
   - Urban, suburban and rural radio propagation environments
   - Licensed and/or licensed exempt frequency bands
   - Hierarchical, flat, or mesh topologies, and their variants
   - Co-existence of fixed, nomadic, portable and mobile usage models

e. The WiMAX architecture SHALL employ use of native IEEE 802.16 procedures and logical separation between such procedures and IP addressing, routing and connectivity management procedures and protocols to enable use of the access architecture primitives in standalone and interworking deployment scenarios.

f. The architecture SHALL support sharing of a NAP's ASN(s) by multiple NSPs.

g. The architecture SHALL support a single NSP providing service over multiple ASN(s) – managed by one or more NAPs.

h. The architecture SHALL support the discovery and selection of accessible NSPs by an MS.

i. The architecture SHALL support NAPs that employ one or more ASN topologies.

j. The architecture SHALL support access to incumbent operator services through internetworking functions as needed.

k. The architecture SHALL specify open, published and accepted standards based and well-defined reference points between various groups of network functional entities (within an ASN, between ASNs, between an ASN and a CSN, and between CSNs), and in particular between an MS, ASN and CSN to enable multi-vendor interoperability.

l. The architecture SHOULD be flexible so it is likely that it accommodates future enhancements to the IEEE802.16 suite of standards

m. The architecture SHOULD be able to accommodate documented geo-specific constraints.

n. The architecture SHOULD support evolution paths between the various usage models subject to reasonable technical assumptions and constraints.

o. The architecture SHALL not preclude different vendor implementations based on different combinations of functional entities on physical network entities, as long as these implementations comply with the normative protocols and procedures across applicable reference points, as defined in this specification.

p. The architecture SHALL support the most trivial scenario of a single operator deploying an ASN together with a limited set of CSN functions, so that the operator can offer basic Internet access service without consideration for roaming or interworking.

5.2 Services and Applications

a. The architecture SHALL be capable of supporting voice, multimedia services and other mandated regulatory services such as emergency services and lawful interception.

b. The architecture SHALL be agnostic to and support access to a variety of independent Application Service Provider (ASP) networks.

c. The architecture SHALL support mobile telephony communications using VoIP and, in applicable roaming scenarios, SHALL support inter-operator policy definition, distribution and enforcement as needed for voice communications. The following capabilities SHALL apply (subject to specific services offered and provisioned):

  - The architecture SHALL support SLA-based resource management for subscribers
  - The architecture SHALL support more than one voice session (when applicable) to the particular subscriber
  - The architecture SHALL support simultaneous voice and data sessions.
  - The architecture SHALL support prioritization (including pre-emption) for emergency voice calls and high priority data sessions

d. The architecture SHALL support interfacing with various interworking and media gateways permitting delivery of incumbent/legacy services translated over IP (for example, SMS over IP, MMS, WAP) to WiMAX access networks.

e. The architecture SHALL support delivery of IP Broadcast and Multicast services over WiMAX access networks.

5.3 Security

a. The WiMAX security framework SHALL be agnostic to the operator type and ASN topology and apply consistently across Greenfield and internetworking deployment models and usage scenarios (where possible).

b. The architecture SHALL accommodate support for strong mutual MS authentication between an MS and the WiMAX network, based on the IEEE 802.16 security frameworks.

c. An MS SHOULD be able to support all commonly deployed authentication mechanisms and authentication in home and visited operator network scenarios based on a consistent and extensible authentication framework. An MS SHOULD be able to select between various authentication method(s) based on NSP type.

d. The architecture SHALL support data integrity, replay protection, confidentiality and non-repudiation using applicable key lengths within the WiMAX Access Network.

e. The architecture SHALL accommodate the use of MS initiated/terminated security mechanisms such as Virtual Private Networks (VPNs) [ref].

f. The architecture SHALL accommodate standard secure IP address management mechanisms between the MS and its home or visited NSP [ref].

g. Unless explicitly permitted, the architecture SHOULD ensure MS and host's specific states such as – authentication state, IP Host configuration, service provisioning and service authorization are not inadvertently shared with other users/SS/MSs.

h. As required and specified in IEEE 802.16 and applicable IETF IP protocol specifications [ref], group communications SHALL be restricted to authorized group membership.

5.4 Mobility and Handovers

a. The architecture SHALL NOT preclude inter-technology handovers— e.g., to Wi-Fi, 3GPP, 3GPP2, DSL/MSO – when such capability is enabled in multi-mode MS.

b. The architecture SHALL accommodate IPv4 or IPv6 based mobility management. Within this framework, and as applicable, the architecture SHALL accommodate MS with multiple IP addresses and simultaneous IPv4 and IPv6 connections.

c. The architecture SHALL NOT preclude roaming between NSPs. The architecture SHOULD allow a single NAP to serve multiple MSs using different private and public IP domains owned by different NSPs (except where solutions become technically infeasible). The NSP MAY be one operator or a group of operators (e.g., Visited Operator MAY be different from the Home Operator and the Home Operator MAY delegate mobility unrelated service aspects to third party ISPs).

d. The architecture SHALL support mechanisms to support seamless handovers at up to vehicular speeds—satisfying bounds of service disruption as specified in Stage 1.

e. The architecture SHALL support dynamic and static home address configurations.

f. The architecture SHALL allow for dynamic assignment of the Home Agent in the service provider network as a form of route optimization, as well as in the home IP network as a form of load balancing.

g. The architecture SHALL allow for dynamic assignment of the Home Agent in H-CSN or V-CSN based on policies

5.5 Quality of Service

a. To flexibly support simultaneous use of a diverse set of IP services, the architecture framework SHALL support:

- Differentiated levels of QoS – coarse-grained (per user/SS/MS) and/or fine-grained (per service flow per user/SS/MS)
- Admission control
- Bandwidth management

b. The architecture SHALL support the means to implement policies as defined by various operators for QoS based on their SLAs, which MAY require policy enforcement per user and user group as well as factors such as location, time of day, etc. QoS policies MAY be synchronized between operators depending on subscriber SLAs, accommodating for the fact that not all operators MAY implement the same policies.

c. The architecture SHALL use standard IETF mechanisms for managing policy definition and policy enforcement between operators.

5.6 Scalability, Extensibility, Coverage and Operator Selection

a. The WiMAX Access Service Network (ASN) architecture SHALL enable a user to manually or automatically select from available NAPs and NSPs.

b. The architecture SHALL enable ASN and CSN system designs that easily scale upward and downward – in terms of coverage, range or capacity.

c. The architecture SHALL accommodate a variety of ASN topologies— including hub-and-spoke, hierarchical, flat, and/or multi-hop interconnects.

d. The architecture SHALL accommodate a variety of backhaul links, both wireline and wireless with different latency and throughput characteristics.

e. The architecture SHALL support incremental infrastructure deployment.

f. The architecture SHALL support phased introduction of IP services that in turn scale with increasing number of active users and concurrent IP services per user.

g. The architecture SHALL support the integration of base stations of varying coverage and capacity— for example, pico, micro, and macro base stations.

h. The architecture SHALL support flexible decomposition and integration of ASN functions in ASN network deployments in order to enable use of load balancing schemes for efficient use of radio spectrum and network resources.

5.7 Interworking and Roaming

a. The architecture SHALL support loosely-coupled interworking with existing wireless networks (for example, 3GPP, 3GPP2) or wireline networks (for example DSL). In all such interworking instances, the interworking interface(s) SHALL be based on standard IETF and IEEE suite of protocols.

b. The architecture SHALL support global roaming across WiMAX operator networks, including support for credential reuse, consistent use of AAA for accounting and charging, and consolidated/common billing and settlement.

c. The architecture SHALL support a variety of user authentication credential formats such as username/password, digital certificates, Subscriber Identity Module (SIM), Universal SIM (USIM), and Removable User Identify Module (RUIM).

5.8 Manageability

a. The architecture SHALL accommodate a variety of online and offline client provisioning, enrollment, and management schemes based on open, broadly deployable, industry standards.

b. The architecture SHALL accommodate Over-The-Air (OTA) services for MS SS/MS provisioning and software upgrades.

5.9 Performance

a. The architecture SHALL accommodate use of header compression/suppression and/or payload compression for efficient use of the WiMAX radio resources.

b. The architecture SHALL support mechanisms that enable maximum possible enforcement and fast re-establishment of established QoS SLAs due to handover impairments.

5.10 Multi-vendor Interoperability

a. The architecture SHOULD support interoperability between equipment from different manufacturers within an ASN and across ASNs. Such interoperability SHALL include:

   - Interoperability between BS and backhaul equipment within an ASN.
   - Interoperability between various ASN elements (possibly from different vendors) and CSN, with minimal or no degradation in functionality or capability of the ASN.

5.11 Convergence Sublayers (CS)

a. The IEEE 802.16 standard defines multiple convergence sub layers. The network architecture framework SHALL support the following CS types:

   - Ethernet CS and IPv4/IPv6 over Ethernet CS
   - IPv4 CS

- IPv6 CS

6. Network Reference Model

6.1 Overview

The Network Reference Model (NRM) is a logical representation of the network architecture. The NRM identifies functional entities and reference points over which interoperability is achieved between functional entities. Figure 6-1 illustrates the NRM, consisting of the following logical entities: MS, ASN, and CSN, whose definitions were given in Section 2.1. The figure depicts the normative reference points R1-R5.

Each of the entities, MS, ASN and CSN represent a grouping of functional entities. Each of these functions MAY be realized in a single physical functional entity or MAY be distributed over multiple physical functional entities. While the grouping and distribution of functions into physical devices within the ASN is an implementation choice, the NWG Release 1.0.0 specification defines three ASN interoperability profiles - Profiles A, B and C (see chapter 8). Infrastructure manufacturers MAY choose one or more of these ASN profiles in their physical implementations of the ASN to satisfy network interoperability requirements as detailed in other parts of the specification**.**

The intent of the NRM is to allow multiple implementation options for a given functional entity, and yet achieve interoperability among different realizations of functional entities. Interoperability is based on the definition of communication protocols and data plane treatment between functional entities to achieve an overall end-to-end function, for example, security or mobility management. Thus, the functional entities on either side of RP represent a collection of control and Bearer Plane end-points. In this setting, interoperability will be verified based only on protocols exposed across an RP, which would depend on the end-to-end function or capability realized (based on the usage scenarios supported by the overall network).

This document specifies the normative use of protocols over an RP for such a supported capability. If an implementation claims support for the capability and exposes the RP, then the implementation SHALL comply with this specification. This avoids the situation where a protocol entity can reside on either side of an RP or the replication of identical procedures across multiple RPs for a given capability.

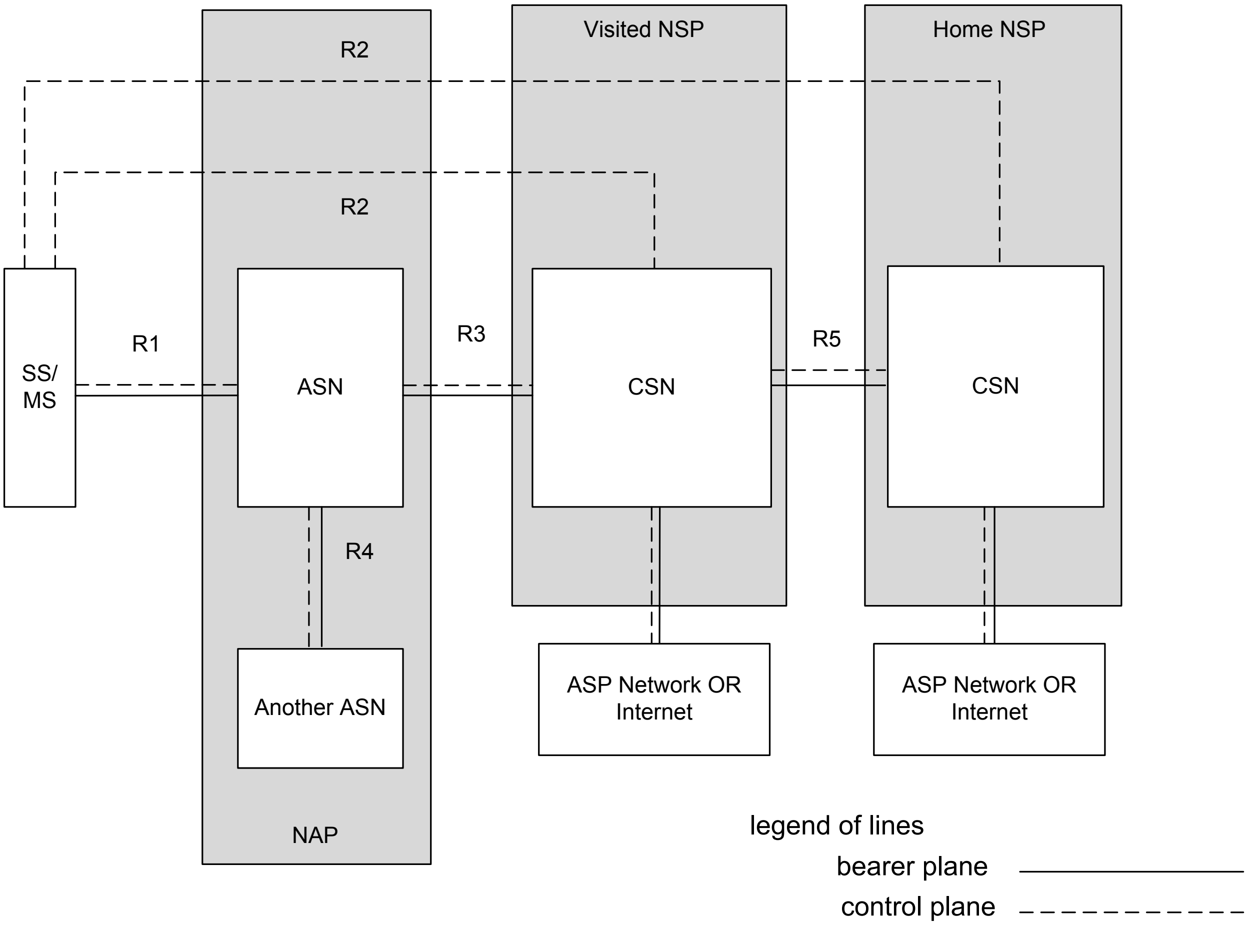

Figure 6-1—Network Reference Model[1]

6.2 Reference Points

Figure 6-1 introduces several interoperability reference points. A reference point is a conceptual point between two groups of functions that resides in different functional entities on either side of it. These functions expose various protocols associated with an RP. All protocols associated with a RP MAY not always terminate in the same functional entity i.e., two protocols associated with a RP SHALL be able to originate and terminate in different functional entities. The normative reference points between the major functional entities are in the following subsections.

6.2.1 Reference Point R1

Reference Point R1 consists of the protocols and procedures between MS and ASN as per the air interface (PHY and MAC) specifications (IEEE P802.16e-2005 [2], IEEE P802.16-2004 [1] and IEEE 802.16g). Reference point R1 MAY include additional protocols related to the management plane.

6.2.2 Reference Point R2

Reference Point R2 consists of protocols and procedures between the MS and CSN associated with Authentication, Services Authorization and IP Host Configuration management.

This reference point is logical in that it does not reflect a direct protocol interface between MS and CSN. The authentication part of reference point R2 runs between the MS and the CSN operated by the home NSP, however the

---

[1] Dashed/Dotted line represents the Control Plane, Normal line represents Bearer Plane

ASN and CSN operated by the visited NSP MAY partially process the aforementioned procedures and mechanisms. Reference Point R2 might support IP Host Configuration Management running between the MS and the CSN (operated by either the home NSP or the visited NSP).

6.2.3 Reference Point R3

Reference Point R3 consists of the set of Control Plane protocols 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 user data between the ASN and the CSN.

6.2.4 Reference Point R4

Reference Point R4 consists of the set of Control and Bearer Plane protocols originating/terminating in various functional entities of an ASN that coordinate MS mobility between ASNs and ASN-GWs. R4 is the only interoperable RP between similar or heterogeneous ASNs.

6.2.5 Reference Point R5

Reference Point R5 consists of the set of Control Plane and Bearer Plane protocols for internetworking between the CSN operated by the home NSP and that operated by a visited NSP.

6.3 ASN Reference Model

6.3.1 ASN Definition

The ASN defines a logical boundary and represents a convenient way to describe aggregation of functional entities and corresponding message flows associated with the access services. The ASN represents a boundary for functional interoperability with WiMAX clients, WiMAX connectivity service functions and aggregation of functions embodied by different vendors. Mapping of functional entities to logical entities within ASNs as depicted in the NRM is informational.

6.3.2 ASN Decomposition

The ASN reference model is illustrated in Figure 6-2 and Figure 6-3.

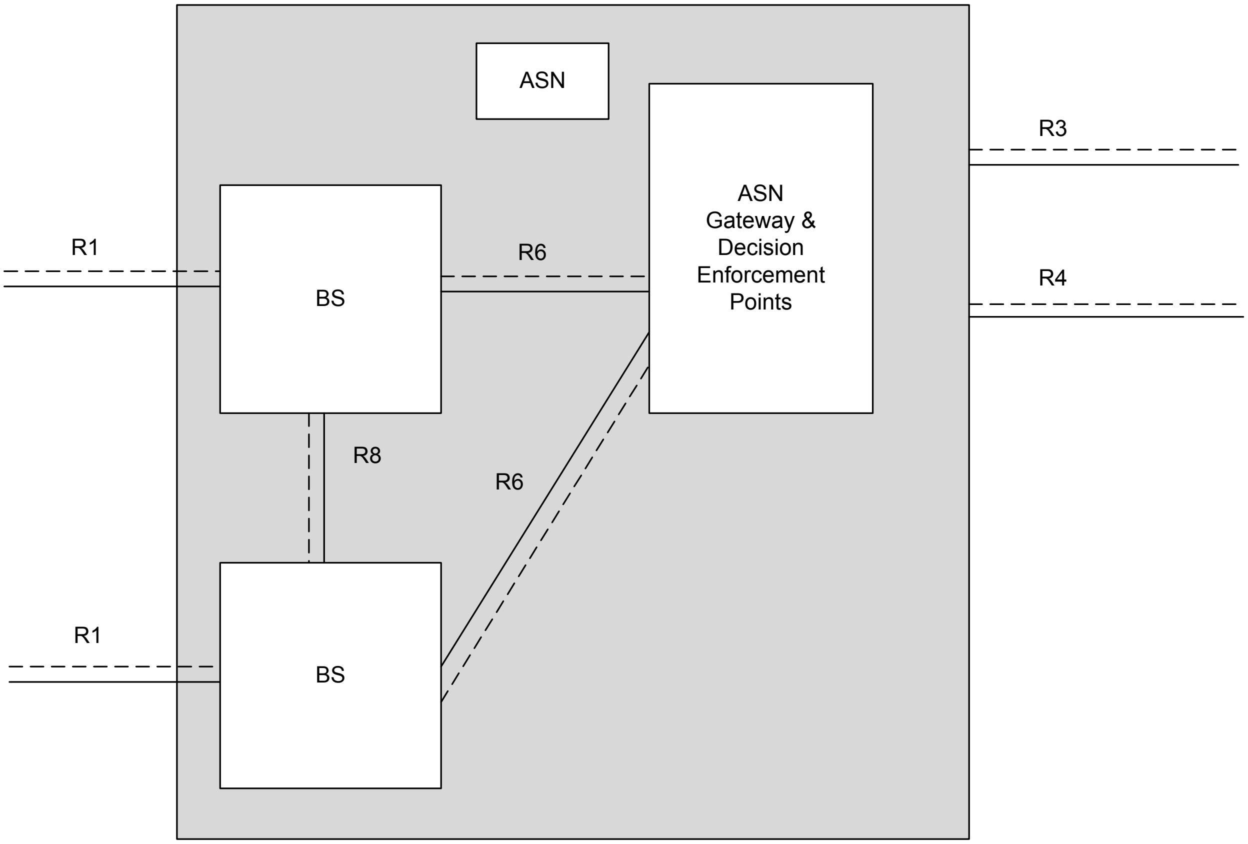

Figure 6-2—ASN Reference Model containing a single ASN-GW

An ASN shares R1 reference point (RP) with an MS, R3 RP with a CSN and R4 RP with another ASN. The ASN consists of at least one instance of a Base Stations (BS) and at least one instance of an ASN Gateway (ASN-GW). A BS is logically connected to one or more ASN Gateways (Figure 6-3)

The R4 reference point is the only RP for Control and Bearer Planes for interoperability between similar or heterogeneous ASNs. Interoperability between any types of ASNs is feasible with the specified protocols and primitives exposed across R1, R3 and R4 Reference Points.

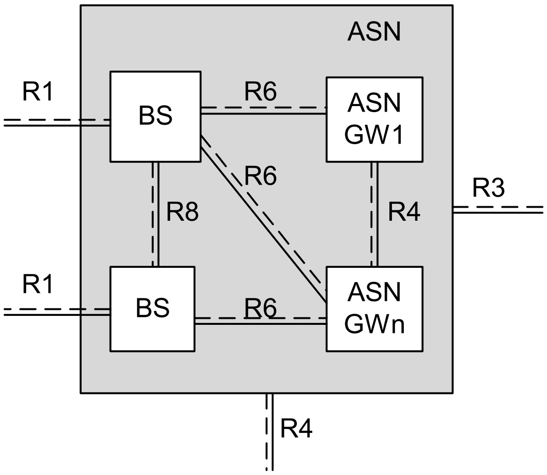

Figure 6-3—ASN Reference Model containing multiple ASN-GW

When ASN is composed of *n* ASN-GWs (where *n* > 1), Intra ASN mobility MAY involve R4 control messages and Bearer Plane establishment. For all applicable protocols and procedures, the Intra-ASN reference point R4 SHALL be fully compatible with the Inter-ASN equivalent.

6.3.3 BS Definition

The WiMAX Base Station (BS) is a logical entity that embodies a full instance of the WiMAX MAC and PHY in compliance with the IEEE 802.16 suite of applicable standards and MAY host one or more access functions. A BS instance represents one sector with one frequency assignment. It incorporates scheduler functions for uplink and downlink resources, which will be left for vendor implementation and is outside the scope of this document. Connectivity (i.e. reachability) of a single BS to more than one ASN-GW MAY be required for load balancing or a redundancy option. BS is logical entity and one physical implementation of BS can have multiple BSs.

6.3.4 ASN Gateway Definition

The ASN Gateway (ASN-GW) is a logical entity that represents an aggregation of Control Plane functional entities that are either paired with a corresponding function in the ASN (e.g. BS instance), a resident function in the CSN or a function in another ASN. The ASN-GW MAY also perform Bearer Plane routing or bridging function.

ASN-GW implementation MAY include redundancy and load-balancing among several ASN-GWs. The implementation details are out of scope for this document.

For every MS, a BS is associated with exactly one default ASN GW. However, ASN-GW functions for every MS may be distributed among multiple ASN-GWs located in one or more ASN(s).

6.3.5 ASN-GW Decomposition

The ASN functions hosted in an ASN-GW MAY optionally be viewed as consisting of two groups of functions, namely, the Decision Point (DP) and the Enforcement Point (EP). The EP includes bearer-plane functions and the DP includes non-bearer-plane functions. For implementation purposes, the decomposition of ASN functions into these two groups is optional.

If decomposed as DP and EP, the EP includes bearer-plane and the DP MAY include non-bearer-plane function – for example, Radio Resource Management Controller.

As indicated above, the aggregated ASN-GW MAY optionally be decomposed into the DP and the EP, separated by Reference Point R7, as shown in Figure 6-4 below. In an aggregated ASN-GW, the R7 RP will not be exposed. An ASN-GW DP MAY be associated with one or more ASN-GW.

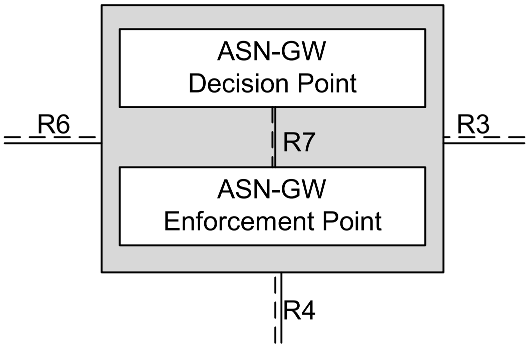

Figure 6-4—ASN-GW Decomposition Reference Diagram

ASN-GW decomposition is associated with ASN-GW reference points decomposing (e.g., R3, R4, R6) as shown in Figure 6-4..

Further decomposition of R6, R4 and R3 are out of scope for this document.

6.3.6 ASN Reference Points

In addition to the normative Reference Points R1, R2, R3, R4 and R5, the following intra-ASN informative Reference Points are identified:

6.3.6.1 Reference Point R6

Reference point R6 consists of the set of control and Bearer Plane protocols for communication between the BS and the ASN-GW. The Bearer Plane consists of intra-ASN datapath between the BS and ASN gateway. The Control Plane includes protocols for datapath establishment, modification, and release control in accordance with the MS mobility events. However, when protocols and primitives over R8 are defined, MAC states will not be exchanged over R6.

6.3.6.2 Reference Point R7

Reference Point R7 consists of the optional set of Control Plane protocols e.g., for AAA and Policy coordination in the ASN gateway as well as other protocols for co-ordination between the two groups of functions identified in R6. The decomposition of the ASN functions using the R7 protocols is optional.

6.3.6.3 Reference Point R8

Reference Point R8 consists of the set of Control Plane message flows and optionally Bearer Plane data flows between the base stations to ensure fast and seamless handover. The Bearer Plane consists of protocols that allow the data transfer between Base Stations involved in handover of a certain MS. The Control Plane consists of the inter-BS communication protocol in line with IEEE 802.16e-2005, March 2006 [2] and 802.16g [80] (802.16g is under development in the IEEE.) and additional set of protocols that allow controlling the data transfer between the Base Stations involved in handover of a certain MS. Messages and protocols shall be informatively specified for applicable ASN profiles in Release 1.0.0.

6.4 Core to Access Network Internetworking Relationships

The following figures show a couple of particular internetworking relationships between ASN and CSN for

- sharing an ASN by multiple CSN,
- providing service to roaming MS with mobility anchor in the visited CSN
- providing service to roaming MS with mobility anchor in the home CSN,
- providing a stationary service without inter-ASN mobility and
- enabling service access in the client MIPv6 case over the CoA as well as over the HoA and enabling services in the client MIPv4 case over HoA.

ASN decomposition is only shown as example for illustrative purposes.

6.4.1 NAP Sharing

Several ASNs might be connected to a single CSN and vice-versa i.e., several CSNs might share the same ASN. Figure 6-5 depicts an instance of ASN-CSN inter-connection wherein multiple CSNs share the same group of ASNs. In this scenario, ASN and MS will exchange information so that the ASN can determine which CSN an MS SHOULD be connected to. ASN and CSN may be owned by the same operator or may belong to different operators.

The case where multiple operators share the same ASN constitutes an example of unbundled access networking.

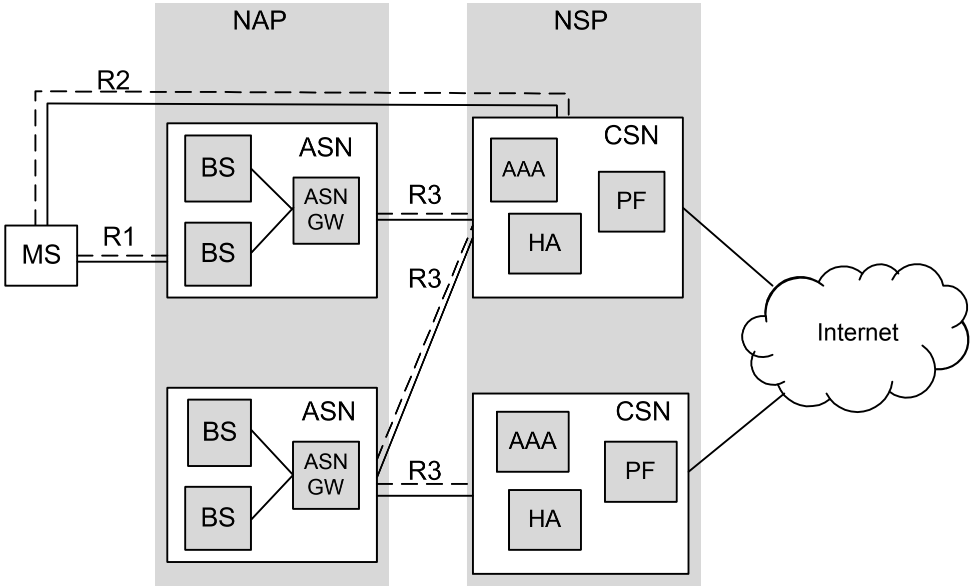

Figure 6-5: Multiple ASN to Multiple CSN Connectivity

6.4.2 Roaming with HA located in the visited NSP

The Figure 6-6 shows the reference architecture for providing service to roaming MS with usage of the HA in the visited CSN. Authentication, authorization as well as policy information is provided from the home CSN to the visited CSN over the reference point R5. Accounting information is forwarded from the visited CSN to the home CSN over R5, and access to services in the home CSN may also provided over R5 whereas Internet access is usually established directly out of the visited CSN.

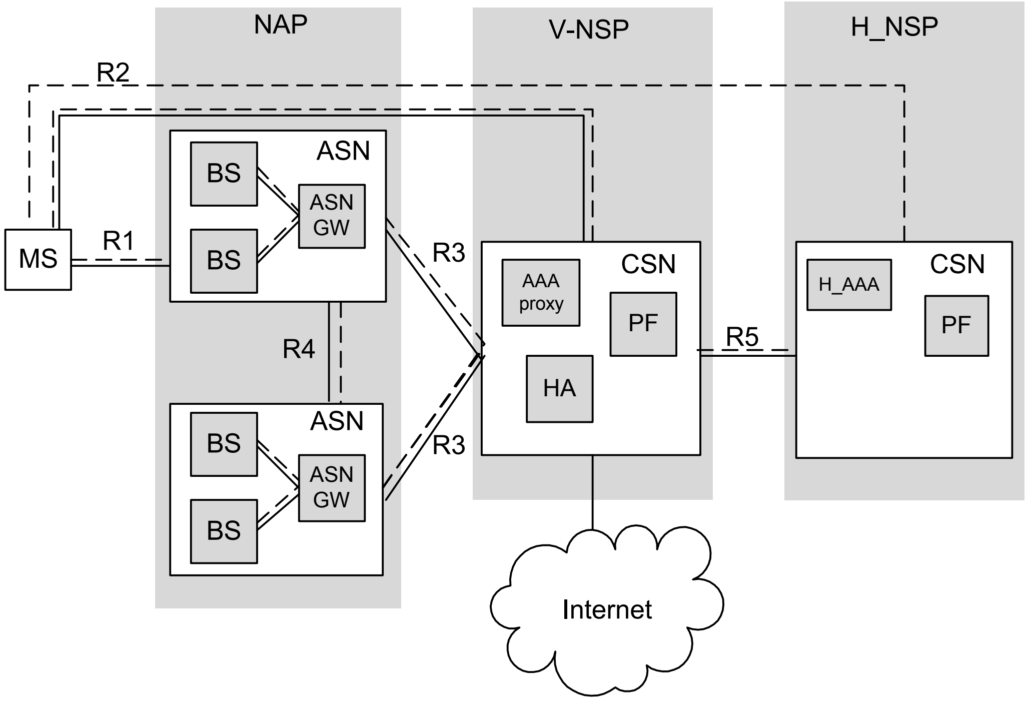

Figure 6–6: Roaming model with HA in visited NSP

6.4.3 Roaming with HA located in the home NSP

The Figure 6-7 shows the reference architecture for providing service to roaming MS with usage of the HA in the home CSN. In this case the visited CSN becomes a kind of proxy for R3. The home CSN is connected to the visited CSN over an R3 reference point with Mobile IP passing through the visited CSN and terminating in the HA in the home CSN.

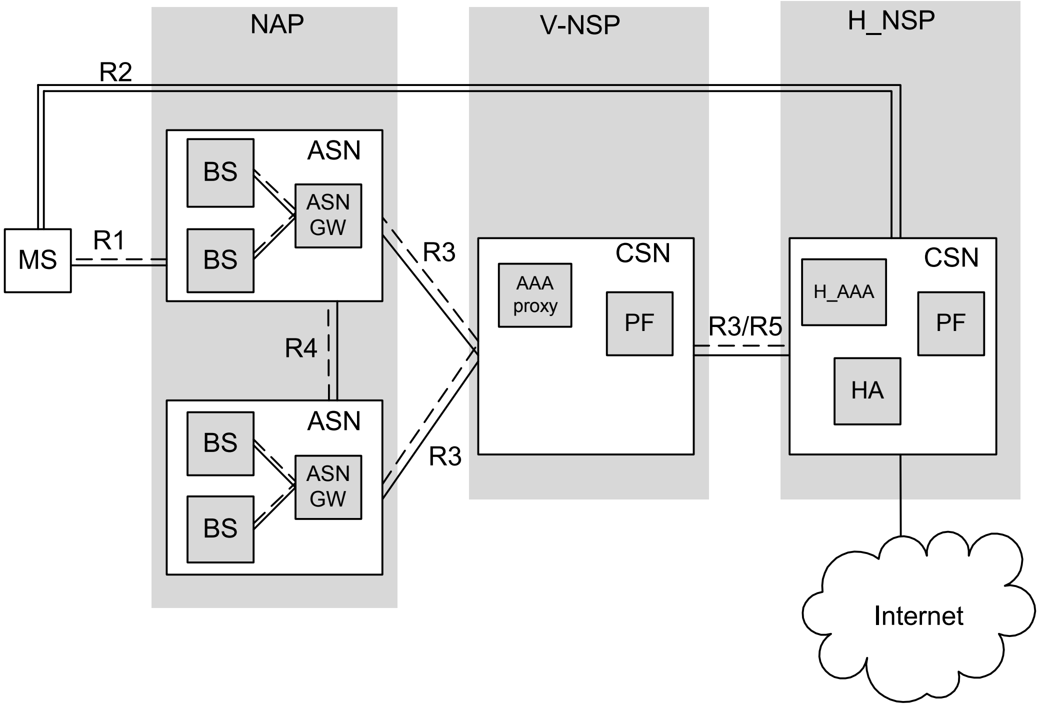

Figure 6-7: Roaming model with HA in home NSP

6.4.4 Stationary Network

When CSN-anchored mobility management is not required and a single ASN is connected with a single CSN the reference point R3 may not to be exposed. In this case it is possible to attach directly the CSN to the ASN and remove in the combined ASN/CSN all the functions not being visible on any of the remaining reference points. When serving only PMIP terminals, even the FA and the HA can be removed in the model, as these entities do not have any impact on any of the remaining reference points.

Such a simplified model is well suitable for stationary applications, as there is no need for Mobile IP based mobility management. Figure 6-8 shows the derived stationary network reference model with support for roaming MS. For roaming MS the authentication, authorization, accounting and policy control are provided by the home NSP over the reference point R5.

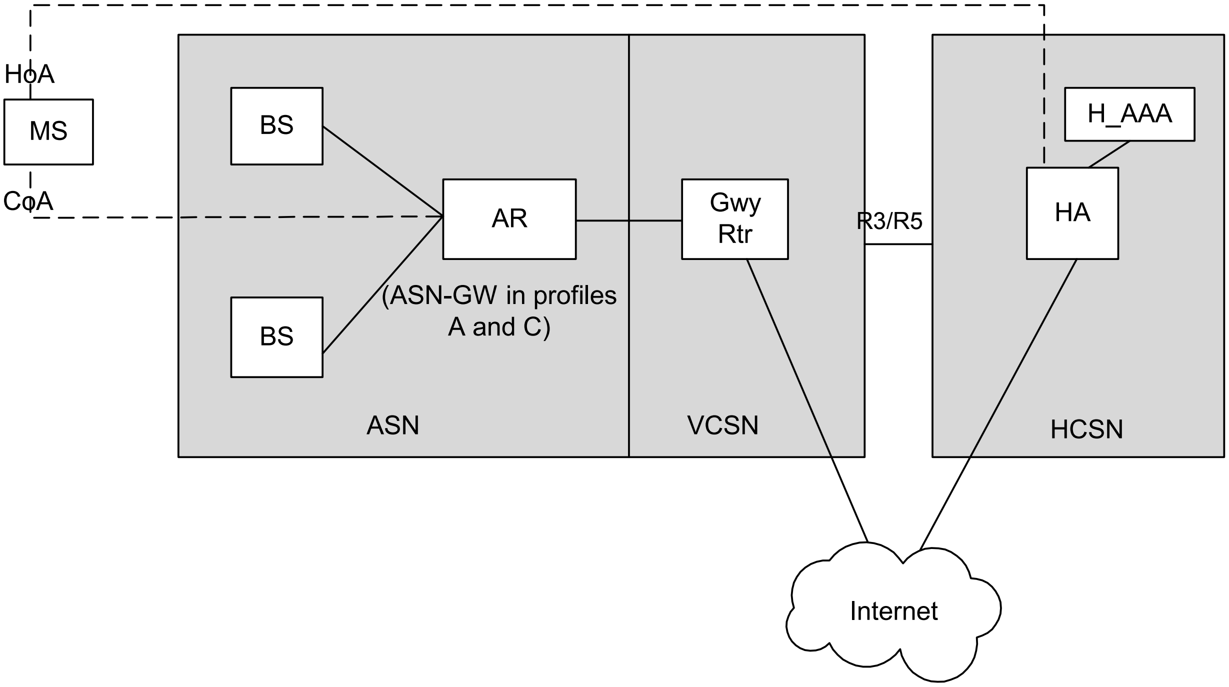

Figure 6-8 Stationary network model

6.4.5 Client MIPv6 network with service connectivity on the CoA as well as on the HoA

Terminals with client MIPv6 have been assigned two addresses: the Care-of-Address (CoA) for establishing the transport connection to the HA, and the Home Address (HoA) for providing mobile service connectivity by the HA in the home CSN. In addition to the mobile services over the HoA, the CoA can be used for stationary access to services and for route optimization between mobile terminals. Making use of the CoA for access to services requires the extension of the ASN to stationary network by directly attaching a CSN to the ASN to provide all the necessary control for service access. While route optimization and stationary services are provided by the directly attached CSN, mobile IPv6 runs over R2 from the MS to the HA in the home NSP. Authentication, authorization and accounting information as well as policy control are handled by the home NSP over an R5 reference point.

Figure 6-9 shows the network reference model for client Mobile IPv6 with support of route optimization and stationary services on the CoA.

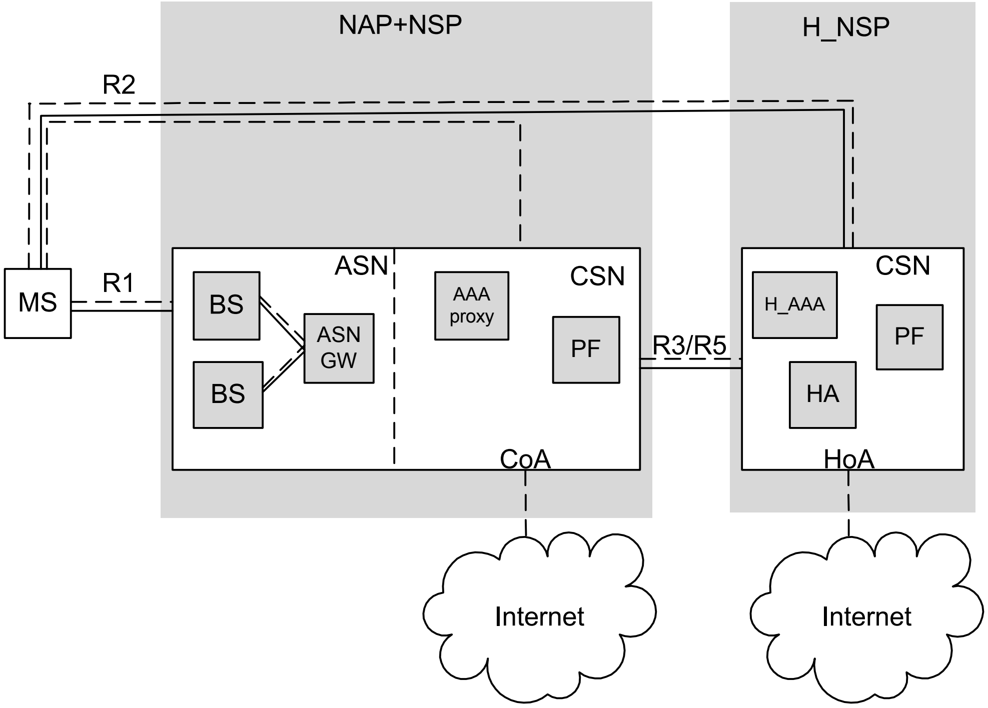

Figure 6-9 Mobile IPv6 with service over CoA and HoA

.

6.5 Release 1.0.0 Interoperability Scope

6.5.1 Reference Points

Supported capabilities across reference points R1–R5 (based on usage scenarios), and the normative definition of interoperable protocols/procedures for each supported capability is within the scope of Release 1.0.0 specification. Control Plane definition message flows and Bearer Plane data flows for interoperable R6 reference points are within the normative scope of the Release 1.0.0 specification and R7-R8 is informative for particular ASN profiles exposing the reference points.

6.5.2 ASN Functions

The normative definition of protocols, messages, and procedures to support ASN functions and capabilities, independent of specific grouping of these capabilities into physical realizations, is within the scope of Release 1.0.0 specification. The functional decomposition is the preferred methodology of Release 1.0.0 without specific reference to any logical or physical network entities. Additionally, 3 ASN Profiles (Profile A, B and C) have been defined in scope of Release 1.0.0.

6.6 CSN Reference Model

CSN internal reference points are out of scope of this specification.