INTERNET DRAFT
Category: Informational
Title: <draft-ietf-mobileip-ipm-arch-00.txt>
Date: September 1999

Carey B. Becker
Basvaraj Patil
Emad Qaddoura
Nortel Networks

IP Mobility Architecture Framework

Status of this Memo

Abstract

Today, the wireless network arena is made up of different types of access (TDMA, CDMA, GSM, etc) and core network technologies (IS-41 and MAP over SS7, etc). The heterogeneous nature of today's wireless and wireline packet data networks limits the scope of mobility between these heterogeneous networks. However, as these heterogeneous networks evolve, the mobility management provided by them must evolve to insure seamless roaming between the networks.

With the convergence of voice and data, networks of the future will be built on IP packet switched technology, mostly due to inherent

advantages offered by the technology.

This document identifies several drivers that provide input for an IP Mobility based network and also describes a high level IP Mobility architecture that extends the current third generation IMT2000 wireless architecture and builds on Mobile IP concepts.

1. Introduction

User mobility is an integral part of today's and future wireless and wireline packet data networks. Today, the wireless network arena is made up of different types of access (TDMA, CDMA, GSM, 802.11, etc) and core network technologies (IS-41 and MAP over SS7, etc.). The heterogeneous nature of today's wireless and wireline packet data networks limits the scope of mobility between these heterogeneous networks. However, as these heterogeneous networks evolve, the mobility management provided by them must evolve to ensure seamless roaming between the networks.

With the convergence of voice networks and data networks, networks of the future will be built on IP packet switched technology, mostly due to inherent advantages offered by the technology (the details of which are beyond the scope of this document). The change from the current SS7 based wireless networks to IP centric wireless networks is already in the works. In the very near future, mobile devices that support IP stacks will also proliferate.

The combination of these two concepts, the networks moving to IP packet switched technology and the evolution of mobility management to ensure seamless roaming, defines what we call IP Mobility. There are several drivers that are paving the way for defining an architecture that is IP Mobility enabled. Some of these are:

1. The network should allow for seamless roaming between heterogeneous wireless and wireline networks.

2. The network infrastructure should be access independent.

   As our wireless networks evolve, it will remain a fact of life that we will need to support the multiple types of wireless accesses, e.g., CDMA, TDMA, etc. Users should be able to roam between these different access types via a mobile devices that support access specific PC cards which provide the appropriate 'layer 2' access. However, the current networking protocols that perform the mobility management functions specific to the heterogeneous technologies can evolve into a single protocol.

3. Mobility needs to be based on the users, not the device used by the user.

   GSM already supports the concept of mobility being based on a user via the International Mobile Subscriber Identity (IMSI), although the IMSI is not known by the user. In North American Cellular systems, e.g., TDMA, CDMA, etc, a user is identified via a Mobile Identification Number (MIN) that is specific to the mobile device. This association needs to be separated. Also, both of these concepts are based on users being assigned 'telephony' user IDs, which are solely based on digits. User IDs should not be restricted to digit only identifiers or restricted to the realm of telephony IDs.

4. A roaming user should only need a single subscription to access a home network.

   Within the scope of packet data services being defined for CDMA systems, a user must have a subscription with a cellular provider to gain access to the cellular network. After which the user is authenticated, the user's mobile device is put on a traffic channel to allow the user's mobile IP subscription to be authenticated with the users home network. The multiple subscriptions translate to multiple unwanted registrations and a waste of radio resources for the second registration.

5. The network should support the removal of triangle routes within the network.

   Triangle routes (which contain routing anchor point) can be established at two points, 1) at the home network as defined in mobile IP [2] and 2) at the foreign network as proposed in [4] and [5]. The network needs to support a mechanism, similar to what is defined in [6], which can alleviate the anchor points. The network needs to support policies that allow or disallow triangle routes, e.g., a policy that wants to hide knowledge of where the user is located.

6. Service providers would like to deploy the same network infrastructure in both their wireline and wireless networks.

   One of the major business drivers is to gain economies of scale from deploying the same network infrastructure, e.g., network operation, services platforms, etc, within the service provider's networks that is independent of the access networks. However, mechanisms should be provided that will allow the networks to be optimized on the type of access network.

None of the current packet data technologies, GPRS, Mobile IP and CDPD, support all the concepts depicted in the above drivers. An architecture must be defined that can provide the functions that insure true seamless roaming within a mobility enabled IP network.

2. IP Mobility Architecture

To be able to achieve a mobility enabled IP network that satisfies the drivers stated in the previous section, an enhanced architecture needs to be defined that extends the current third generation IMT2000 wireless architecture and mobile IP. This section defines such an architecture.

The intent of defining this architecture is to stimulate discussion on the merits of its components. The transition strategies required by the packet data technologies to evolve to this architecture are outside the scope of this document. However, it is an important item that should be addressed as part of the work group discussions.

The architecture described in this draft is not complete. It does not include some necessary concepts; one example being brokers/proxies as described in [7] and [8]. However, it does contain a substantial subset of what is needed to provide mobility within IP networks.

2.1. Network Reference Model

The following figure depicts the logical view of the proposed network architecture.

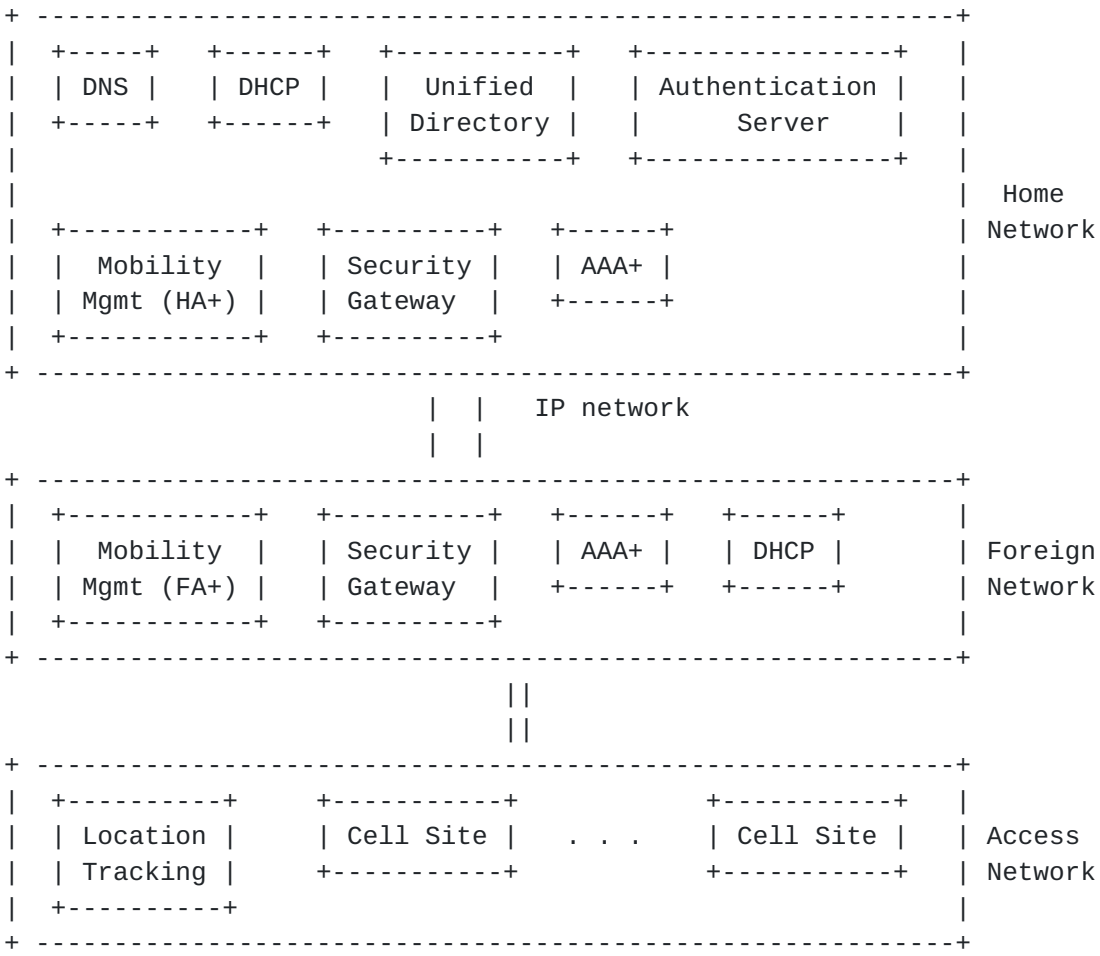

Figure 1: Network Reference Model

The following sections describe the functionality of the components of the network reference model.

2.2. Home Network

The Home Network is very similar in concept to the home network defined in [2[and the home network defined in the wireless networks. Basically, the Home network is a combination of the two with some extensions.

Some of the relevant functions of the Home Network as they relate to mobility are:

* It is the home network that 'owns' the mobile user's subscription.

* Maintains the mobile user's subscription and associated subscriber profile.

* Provides mobility to subscribers on a 'larger' scale. It is responsible for maintaining the current location of the mobile user.

* Allocation of mobile node IP addresses

* Supports a 'unified' directory for subscriber profiles independent of the access network type.

* Stores policies and profiles associated with mobile users.

* Provides Authorization functions associated with the mobile user.

* May provide the Authentication functions required to authenticate the mobile users.

* Support Service Level Agreements (SLA) with all Foreign Networks it wants its users to roam in.

* Support a policy that allows 'hiding' the user's location. This policy will mandate that the home be an anchor point for datagrams sent to it's users while they are roaming.

2.2.1. Home Network Mobility Components

The following describes some functions associated with the components of the Home network.

* Mobility Management (MM)

  Mobility management is comprised of two high level concepts, 1) mobile user location tracking and 2) performing routing update functions for mobile nodes. These functions are very similar to what Home Agents do in [2] and what Home Location Registers do in wireless networks, with some enhancements. The location tracking function of the MM expects to receive a single mobile user registration message from the foreign

networks that is independent of the access network used at the foreign network. This is true for all messages sent from the foreign networks to the home networks. The architecture supports the concept of a centralized location tracking function for the home network. However, the architecture does not preclude the idea of having a distributed location tracking function.

* AAA+

  The protocol used to send messages between a foreign network and a home network is the AAA protocol, with extensions to support mobility management (hence AAA+). Another important concept used within the AAA+ framework is that the AAA+ between a foreign network and a home network. This single security association can be used to alleviate the need for security associations between mobile IP FA and HA components and dynamic session key establishment as suggested in [2] and [4]. It is suggested that the security framework be based on IPSec.

* Authentication Server

  The authentication server is a combination of certificate authority, key management system, and digital signature verification server. The authentication server receives roaming mobile user authentication requests via the AAA+ and authenticates the user.

* Unified Directory

  The Unified Directory is the database that contains all the home user's subscriber profiles, network policies, and any other data that needs to be stored at the Home Network. The subscriber profiles in the directory are independent of the access network association. Access to data in the Unified Directory from other components within the network is via a single protocol, LDAP.

* DHCP

  In the Home Network, the DHCP server may be used to assign IP addresses to roaming mobile stations that do not have a permanently configured IP.

* DNS

  In the home network, Dynamic DNS is the protocol used to

update DNS with a roaming user's mobile node allocated IP address. If the home network is responsible for allocating the IP address, DNS is updated by DHCP. If the foreign network is responsible for allocating the IP address, the home network mobility manager will update DNS.

* Security gateway

  The security gateway performs all the necessary 'firewall' functions.

2.3. Foreign Network

The Foreign Network is very similar in concept to the foreign network defined in [2] and the foreign network defined in the wireless networks. Basically, the Foreign Network is a combination of the two with some extensions.

Some of the relevant functions of the Foreign Network as they relate to mobility are:

* It is the serving area network for one or more access networks.

* It can support multiple Access Networks, where each AN is associated with a different technology, e.g. one AN may be a CDMA RAN, another AN may be GSM RAN.

* Provides mobility management for mobility within the access networks that it serves.

* Provides local services.

* Routes data to the mobile user via the access link that the mobile node is currently attached to.

* Routes data that is sent by the mobile user.

* Allocates IP address to be used by the mobile nodes if allowed by policy.

* Support for the establishment of Service Level Agreements (SLA) with all Home Networks that want to allow their user to roam within the foreign network.

* Support for user authentication to be provided by at the foreign network after the user initially registers.

2.3.1. Foreign Network Mobility Components

The following describes some functions associated with the components of the Foreign Network.

* Mobility Management (MM)

  Foreign Network's mobility management is comprised to three high level concepts, mobile user location tracking within the foreign network, handoffs between foreign networks, and performing routing update functions for datagram delivery to the access network/mobile node. These functions are very similar to what Foreign Agents do in [2], with some enhancements. The location tracking function of the MM expects to receive the same formatted mobile user registration message from each of the heterogeneous access network. The architecture supports the concept of a centralized location tracking function within for the foreign network. However, the architecture does not preclude the idea of having a distributed location tracking function.

* AAA+

  The protocol used to send messages between a foreign network and a home network is the AAA protocol, with extensions to support mobility management (hence AAA+). Another important concept used within the AAA+ framework is that the AAA+ between a foreign network and a home network. This single security association can be used to alleviate the need for security associations between mobile IP FA and HA components and dynamic session key establishment. It is suggested that the security framework be based on IPSec.

* DHCP

  In the Foreign Network, the DHCP server may be used to 1) assign co-located care of addresses to private network mobile nodes and 2) if policies indicate, assign IP addresses to roaming mobile stations that do not have a permanently configured IP.

* Security Gateway

  The security gateway performs all the necessary 'firewall' functions. It supports ESP IPSec security associations with other network security gateways.

2.4. Access Network

The Access Network defines the 'layer 2' access technology used by a user to gain access to a Foreign Network. The access network can be one of several types:

* North American Cellular and GSM radio access networks (and their evolution to 3rd generation)

* 802.11 wireless LAN access

* 802.3 wireline LAN access

* Dial-up network access

Figure 1 above only depicts an access network associated with a wireless network.

2.5. IP Network

The IP network provides the routing of datagrams between Home Networks and Foreign Networks. The IP network can be the public Internet or a closed network such as those defined in IMT2000 standards.

2.6. Mobile Nodes

It can be argued that all nodes in the future will be mobile, or at least have the potential to be mobile. Stationary nodes, generally called correspondent nodes in [2], will only have to be equipped with the appropriate access specific PC card(s) and software that can perform the network registration functions.

The mobile node's PC cards provide the 'layer 2' interface to the specific access network. For each of the access network types, there is a layer 2 address associated with the PC card so the access network and mobile node are able to uniquely address each other. Mobile node software will need to determine when and which access networks are available and perform the appropriate registration functions.

Both types of nodes will have to support tunneling, e.g., IP in IP encapsulation [9], to a roaming mobile node's care-of addresses. This will help alleviate the triangle routing (anchor points) issue.

2.7. User Identification

The architecture suggests user identities be based the Network Access Identifier (NAI) as defined in [1]. The NAI allows for a highly flexible definition of a user which does not restrict user identities to digits only.

3. Conclusion

The architecture defined in this document provides a foundation that will allow true seamless roaming within a mobility enabled IP network.

Some of the advantages provided by the architecture are:

* A user may have a single subscription with a home network that allows for roaming within all foreign networks that have service level agreements with the home network.

* Mobility being based on the user, not the device used by the user.

* A single control plane network protocol based on AAA that can be deployed in a provider's network independent of the access network.

* A single security framework based on IPSec and used by the AAA+ server to minimize other security associations and the use of dynamic session keys.

* The ability to alleviate routing anchor points and support for policies that allow the hiding of users by allowing routing anchor points.

* Users to truly roam seamlessly between heterogeneous access networks.

4. References

[1] B. Aboba, M. Beadles, "The Network Access Identifier" RFC 2486, January 1999.

[2] C. Perkins, "IP Mobility Support", RFC 2002, October 1996.

[3] P. Calhoun, C. Perkins, "Mobile IP Dynamic Home Address Allocation Extension", draft-ietf-mobileip-home-addr-alloc-00.txt, November 1998.

[4] P. Calhoun P, C. Perkins, "Mobile IP Foreign Agent Challenge/Response Extension", draft-ietf-mobileip-challenge-00.txt, November 1998.

[5] P. Calhoun, G. Zorn, P. Pan, "DIAMETER Framework", Internet-Draft, draft- calhoun-diameter-framework-01.txt, August 1998

[6] C. Perkins, D. Johnson, "Route Optimization in Mobile IP", Internet Draft, ietf- mobileip-optim-07.txt, November 1997.

[7] B. Aboba, et al, "Review of Roaming Implementations", RFC 2194, September 1997.

[8] P. Calhoun, W. Bulley, "DIAMETER User Authentication Extensions", Internet- Draft, draft-calhoun-diameter-authent-04.txt, July 1998

[9] W. Simpson, "IP in IP Tunneling", RFC 1853, October 1995.

5. Acknowledgements

The authors would like to thank Russ Coffin, Mary Barnes, and Lachu Aravamudham of Nortel Networks and John Myhre of ATT Wireless Services for their useful discussion.

6. Authors' Addresses

Carey B. Becker
Nortel Networks Inc.
2201 Lakeside Blvd.
Richardson, TX. 75082-4399

Phone: 972-685-0560
email: becker@nortelnetworks.com

Basavaraj Patil
Nortel Networks Inc.
2201 Lakeside Blvd.
Richardson, TX. 75082-4399

Phone: 972-684-1489
email: bpatil@nortelnetworks.com

Emad Qaddoura
Nortel Networks Inc.
2201 Lakeside Blvd.
Richardson, TX. 75082-4399

Phone: 972-684-2705
email: emadq@nortelnetworks.com