International Journal of Multimedia and Ubiquitous Engineering
Vol. 2, No. 2, April, 2007

A Review on Mobile IP Connectivity and its QoS

Adrian Stoica

Senior Research Scientist, Principal MTS
Supervisor, Advanced Robotic Controls
Mobility and Robotic Systems, Autonomous Systems Division
NASA Jet Propulsion Laboratory
MS 198-219, 4800 Oak Grove Drive, Pasadena, CA 91109
adrian.stoica@jpl.nasa.gov

Abstract

Mobile IP (or IP mobility) is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address. The Mobile IP protocol allows location-independent routing of IP datagrams on the Internet. Each mobile node is identified by its home address disregarding its current location in the Internet. While away from its home network, a mobile node is associated with a care-of address which identifies its current location and its home address is associated with the local endpoint of a tunnel to its home agent. Mobile IP specifies how a mobile node registers with its home agent and how the home agent routes datagrams to the mobile node through the tunnel.In this paper, we review IP mobility and its components. And also, we review current technologies related to IP mobility

Keywords: *IP Mobility, MIPv4, MIPv6, Mobile Network*

1. Introduction

When IP routing was originally defined, mobility of hosts was not considered to be an issue. Routing methods were built for static networks, where the hosts were unlikely to move from one subnet to another. Routing takes advantage of a “network number“contained in every IP address. Thus, the IP address encodes the computer’s physical location, and - by default - the location is fixed. [1]

Mobile IP defines protocols and procedures by which packets can be routed to a mobile node, regardless of its current point-of-attachment to the Internet, and without changing its IP address. [1]

Mobile IP provides an efficient, scalable mechanism for roaming within the Internet. Using Mobile IP, nodes may change their point-of-attachment to the Internet without changing their home IP address. This allows them to maintain transport and higher-layer connections while roaming. Node mobility is realized without the need to propagate host-specific routes throughout the Internet routing fabric. [2]

2. IP Mobility

Mobile IP is most often found in wired and wireless environments where users need to carry their mobile devices across multiple LAN subnets. It may for example be used in roaming between overlapping wireless systems, for example IP over DVB, WLAN, WiMAX and BWA. Currently, Mobile IP is not required within cellular systems such as 3G, to provide transparency when Internet users migrate between cellular towers, since these systems provide their own data link layer handover and roaming mechanisms. However, it is often used in 3G systems to allow seamless IP mobility between different Packet Data Serving Node (PDSN) domains. In many applications (e.g., VPN, VoIP), sudden changes in network connectivity and IP address can cause problems.

A mobile node can have two addresses - a permanent home address and a care of address (CoA), which is associated with the network the mobile node is visiting. There are two kinds of entities in Mobile IP:

- A home agent stores information about mobile nodes whose permanent home address is in the home agent's network.
- A foreign agent stores information about mobile nodes visiting its network. Foreign agents also advertise care-of addresses, which are used by Mobile IP.

A node wanting to communicate with the mobile node uses the permanent home address of the mobile node as the destination address to send packets to. Because the home address logically belongs to the network associated with the home agent, normal IP routing mechanisms forward these packets to the home agent. Instead of forwarding these packets to a destination that is physically in the same network as the home agent, the home agent redirects these packets towards the foreign agent through an IP tunnel by encapsulating the datagram with a new IP header using the care of address of the mobile node.

When acting as transmitter, a mobile node sends packets directly to the other communicating node through the foreign agent, without sending the packets through the home agent, using its permanent home address as the source address for the IP packets. This is known as triangular routing. If needed, the foreign agent could employ reverse tunneling by tunneling the mobile node's packets to the home agent, which in turn forwards them to the communicating node. This is needed in networks whose gateway routers have ingress filtering enabled and hence the source IP address of the mobile host would need to belong to the subnet of the foreign network or else the packets will be discarded by the router.The Mobile IP protocol defines the following:

- an authenticated registration procedure by which a mobile node informs its home agent(s) of its care-of-address"(es);
- an extension to ICMP Router Discovery, which allows mobile nodes to discover prospective home agents and foreign agents; and
- the rules for routing packets to and from mobile nodes, including the specification of one mandatory tunneling mechanism and several optional tunneling mechanisms.

3. Proxy Mobile IP

Proxy Mobile IP (or PMIP, or Proxy Mobile IPv6) is a new standard currently (2008) being worked on at Internet Engineering Task Force (IETF). Sometimes referred to as Network-based mobility management, it provides similar functionality to that of Mobile IP, however it does not require any modifications to the mobile host's network stack, i.e. the mobility is taken care of by the network. [3]

Network-based mobility management enables the same functionality as Mobile IP, without any modifications to the host's TCP/IP Protocol stack. With PMIP the host can change its point-of-attachment to the Internet without changing its IP address. Contrary to Mobile IP approach, this functionality is implemented by the network, which is responsible for tracking the movements of the host and initiating the required mobility signalling on its behalf. However in case the mobility involves different network interfaces, the host needs modifications similar to Mobile IP in order to maintain the same IP address across different interfaces.

The standard defines two network entities which are involved in the process - Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). Mobile Access Gateway is a function on an access router that manages the mobility related signalling for a mobile host that is attached to its access link. Local Mobility Anchor is the home agent for the mobile host in a Proxy Mobile IP domain. The protocol works as follows: [3]

- A mobile host enters a PMIP domain
- A Mobile Access Gateway on that link checks host authorization
- A mobile host obtains an IP address
- A Mobile Access Gateway updates a Local Mobility Anchor about the current location of a host
- Both MAG and LMA create a bi-directional tunnel

3. IEEE 802.21

IEEE 802.21-2008, also known as Media-Independent Handover Services, features a broad set of properties that meet the requirements of effective heterogeneous handovers. It allows for transparent service continuity during handovers by specifying mechanisms to gather and distribute information from various link types to a handover decision maker. The collected information comprises timely and consistent notifications about changes in link conditions and available access networks. [4]

Note that the scope of IEEE 802.21-2008 is restricted to access technology-independent handovers. Intratechnology handovers, hand- over policies, security mechanisms, media-specific link layer enhancements to support IEEE 802.21-2008, and Layer 3 (L3) and upper-layer enhancements are outside the scope of IEEE 802.21-2008. This article summarizes the salient points of [4], which henceforth is referred to as IEEE 802.21.

IEEE 802.21 facilitates a variety of handover methods, including both hard handovers and soft handovers. A hard handover, also known as "break-before-make" handover, typically implies an abrupt switch between two access points, base stations, or, generally speaking, PoAs. Soft handovers require the establishment of a connection with the target PoA while still routing traffic through the serving PoA. In soft ("make-before-break") handovers, mobile nodes remain briefly connected with two PoAs. Note, however, that depending on service requirements and application traffic patterns, hard handovers may often go unnoticed. For example, web browsing and audio/video streaming with prebuffering can be accommodated when handing over between different PoAs in the range of one network by employing mechanisms that allow transferring the node connection context from one PoA to another quickly.

The main design elements of IEEE 802.21 can be classified into three categories: a framework for enabling transparent service continuity while handing over between heterogeneous access technologies; a set of handover-enabling functions; and a set of Service Access Points (SAPs).

IEEE 802.21 specifies a framework that enables transparent service continuity while a mobile node switches between heterogeneous access technologies. The consequences of a particular handover need to be communicated and considered early in the process and, clearly, before the handover execution. In soft handovers, it is crucial that service continuity, during and after the handover, is ensured without any user intervention. To this end, IEEE 802.21 specifies essential mechanisms to gather all necessary information required for an affiliation with a new access point before breaking up the currently used connection. Interactive applications, such as VoIP, are typically the most demanding in terms of handover delays, and high-quality VoIP calls can be served only by soft handovers. On the other hand, video streaming can accommodate hard handovers, as long as the vertical break-before-make handover delay does not exceed the application buffer interval delay. In the case of hard handovers, handover preparation signaling can initiate the connection context transfer from the serving PoA to the target PoA beforehand.

For instance, lack of the required level of QoS support or low available capacity in a candidate access network may lead the network selecting entity to prevent a planned handover. On the other hand, for example, increasing delay, jitter, or packet-loss rates in the currently serving network may degrade the perceived QoS throughout the network, or only for a particular application, triggering the mobility manager to start assessing the potential of candidate target access networks and subsequently initiate an IEEE 802.21-assisted handover.

IEEE 802.21 also allows the reception of dynamic information about the performance of the serving network and other networks in range. In other words, IEEE 802.21 provides methods for continuous monitoring of available access conditions. However, IEEE 802.21 does not specify any methods for collecting this dynamic information at the link layer.

3.1 Handover-Enabling Functions

IEEE 802.21 defines a set of handover-enabling functions, which are specified with respect to existing network elements in the protocol stack, and introduces a new

logical entity called Media-Independent Handover Function (MIHF). The MIHF logically resides between the link layer and the network layer. It provides, among others, abstracted services to entities residing at the network layer and above, called MIH Users (MIHUs). MIHUs are anticipated to make handover and link-selection decisions based on their internal policies, contextÂ¸ and the information received from the MIHF. To this end, the primary role of the MIHF is to assist in handovers and handover decision making by providing all necessary information to the network selector or mobility management entities. The latter are responsible for handover decisions regardless of the entity position in the network. The MIHF is not meant to make any decisions with respect to network selection.

3.2 Service Access Points

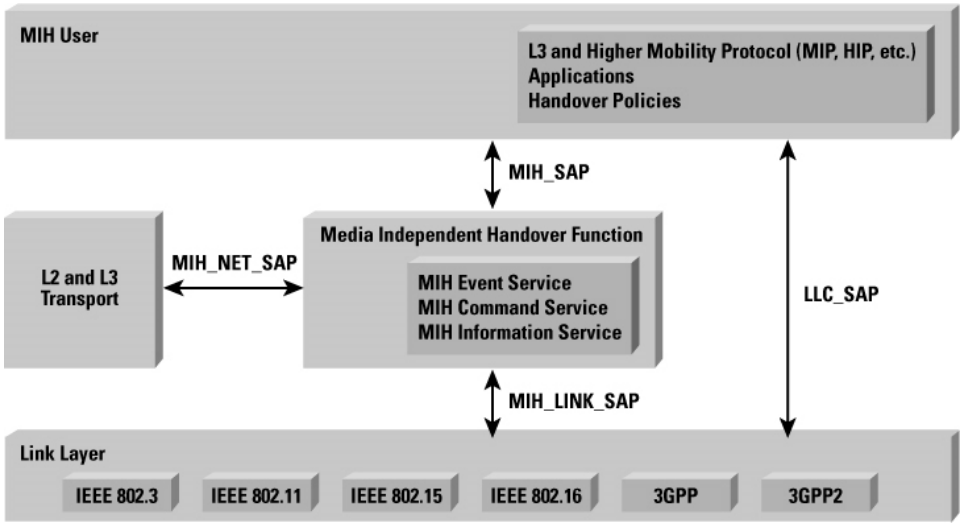

Figure 1. The IEEE 802.21-2008 Reference Model

SAPs with associated primitives between the MIHF and MIHUs (MIH_SAP) give MIHUs access to the following services that the MIHF provides:

- The Media-Independent Event Service (MIES) provides event reporting about, for example, dynamic changes in link conditions, link status, and link quality. Events can be both local and remote. Remote events are obtained from a peer MIHF entity.
- The Media-Independent Command Service (MICS) enables MIHUs to manage and control the parameters related to link behavior and handovers. MICS provides a set of commands for accomplishing that, as we will see later in this article. Commands can be both local and remote. The information obtained with MICS is dynamic.
- The Media-Independent Information Service (MIIS) allows MIHUs to receive static information about the characteristics and services of the serving network and other available networks in range. This information

can be used to assist in making a decision about which handover target to choose and to make preliminary preparations for a handover.

Figure 1 illustrates the general reference model of IEEE 802.21. The scope of IEEE 802.21 includes only the operation of MIHF and the primitives associated with the interfaces between MIHF and other entities. A single media-independent interface between MIHF and MIHU (MIH_SAP) is sufficient.On the other hand, there is a need for defining a separate technology-dependent interface, which is specific to the corresponding media type supported, between the MIHF and the lower layers (MIH_LINK_SAP).

The primitives associated with the MIH_LINK_SAP enable MIHF to receive timely and consistent link information and control link operation during handovers. For example, the currently supported link layers include wired and wireless media types from the IEEE family of standards (for example, 802.3, 802.11, 802.15, and 802.16), as well as those defined by the Third-Generation Partnership Project (3GPP) and Third-Generation Partnership Project 2 (3GPP2). Besides these, IEEE 802.21 specifies a media-independent SAP (MIH_NET_SAP), which provides transport services for Layer 2 (L2) and Layer 3 (L3) MIH message exchange with remote MIHFs. Functions over the LLC_SAP are not specified in IEEE 802.21. [4]

4. Mobile IPv4

The key feature of the Mobile IP (see [RFC2002], [Per98], [Per97]) design is that all required functionalities for processing and managing mobility information are embedded in well-defined entities, the Home Agent (HA), Foreign Agent (FA), and Mobile Node (MN). The current Mobile IPv4 protocol is completely transparent to the transport and higher layers and does not require any changes to existing Internet hosts and routers.

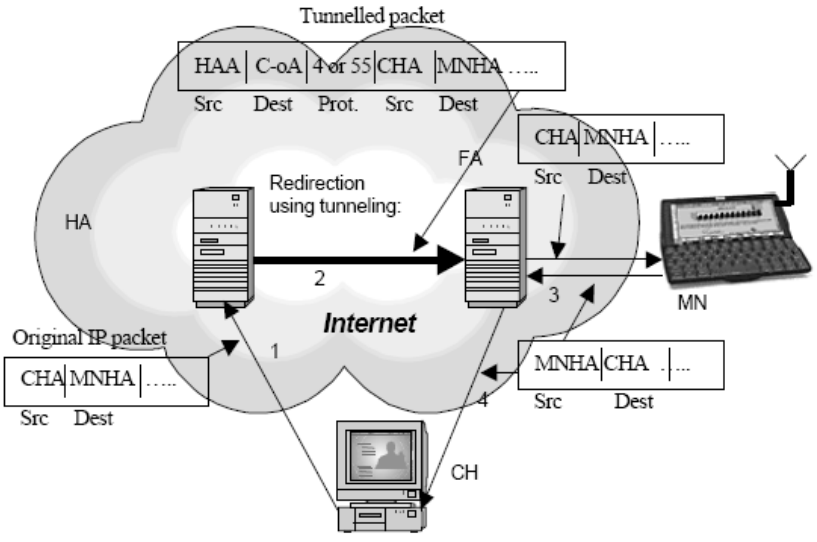

Figure 2. MIP packet flow

The Mobile IP protocol allows the MNs to retain their IP address regardless of their point of attachment to the network. This can be fulfilled by allowing the MN to use two IP addresses. The first one, called home address, is static and is mainly used to identify higher layer connections, e.g., TCP. The second IP address that can be used by a MN is the Care-of Address. While the mobile is roaming among different networks, the Care-of Address changes. The reason of this is that the Care-of Address has to identify the mobile's new point of attachment with respect to the network topology. In Mobile IPv4 the Care-of Address management is achieved by an entity called Foreign Agent.

The Mobile Node, using its home address is appearing to be able to receive data on its home network, through a Home Agent. In the situation that the mobile roams into a foreign region, it will need to obtain, a new Care-of Address via the Foreign Agent. Note that, in this situation the Mobile Node can also obtain a new Care-of Address by contacting the Dynamic Host Configuration Protocol (DHCP) [RFC1541] or Point-to-Point Protocol (PPP) [RFC1661]. This new Care-of Address will be registered with its Home Agent. At the moment that the Home Agent (see Figure 2) receives a packet that has to be send to the mobile, it delivers it from the home network to the mobile's Care-of Address. The delivery can take place only if the packet is redirected or tunneled, such that the Care-of Address appears as the destination IP address. The Home Agent tunnels the packet to the Foreign Agent. After receiving the packet, the Foreign Agent will have to apply the reverse transformation to decapsulate it, such that the packet will appear to have the mobile's home address as the destination IP address. After decapsulation, the packet is sent to the Mobile Node. Due to the fact that the packet arrives at the Mobile Node, being addressed to its home address, it will be processed properly by the upper protocol layers, e.g., TCP. The IP packets sent by the Mobile Node, are delivered by standard IP routing procedures, each to its destination. When the Mobile IP packet flow, then the routing situation is typically called triangle routing, since the packet sent by the correspondent host follows the path 1,2 and 3, while the packet sent by the Mobile Node will follow routes 3 and 4.

4. Mobile IPv6

Mobile IPv6 is an IETF standard that has added the roaming capabilities of mobile nodes in IPv6 network. RFC 3775 has described this standard in detail. The major benefit of this standard is that the mobile nodes (as IPv6 nodes) change their point-of-attachment to the IPv6 Internet without changing their IP address.

This allows mobile devices to move from one network to another and still maintain existing connections. Although Mobile IPv6 is mainly targeted for mobile devices, it is equally applicable for wired environments. .

The need for Mobile IPv6 is necessary because the mobile nodes in ‼fixed¶ IPv6 network can↕t maintain the previously connected link (using the address assigned from the previously connected link) when changing location.

To accomplish the need for mobility, connections to mobile IPv6 nodes are made (without user interaction) with a specific address that is always assigned to the

mobile node, and through which the mobile node is always reachable. Mobile IPv6 is expected to be used in IP over WLAN, WiMAX or BWA.

Several terms and information are necessary to understand Mobile IPv6: A foreign link defines a link that is not the mobile node↕s home link. A Care-of address denotes an address that is used by the mobile node while it is attached to a foreign link. Whenever a mobile node moves from the home link to a foreign link, it is always (still) reachable by its home address, regardless of its location in IPv6 network.

Home address signifies that the mobile node is logically connected to the home link. Also, the association of a home address with a care-of address for a mobile node is known as a binding. Home agent is a router (on the home link) that maintains registrations of mobile nodes that are away from home and their current addresses. A Correspondent node is an IPv6 (not necessarily Mobile IPv6 capable) node that communicates with a mobile node.

IPv6 Mobile IPv6 uses the IPv6 features such as address auto-configuration, Neighbor discovery and extension header for its operation.

It uses both types of auto-configuration such as stateless (Network prefix + interface ID) and stateful auto-configuration (DHCPv6). The neighbor discovery feature allows performing the following:

- How each other's presence is discovered and how to find routers
- How each other's link layer addresses are determined
- How to maintain reachability information

Extension headers provide routing headers for route optimization and destinations option header for mobile node originated diagrams. In addition, Mobile IPv6 also requires mobile nodes to carry out IPv6 decapsulation.

4.1 Mobile IPv6 Operation

When a mobile node is away from home, it sends information about its current location to the home agent. A node that wants to communicate with a mobile node uses the home address of the mobile node to send packets. The home agent intercepts these packets, and using a table, tunnels the packets to the mobile node's care-of address.

Mobile IPv6 uses care-of address as source address in foreign links. Also, to support natural route optimization, the Correspondent node uses IPv6 routing header than the IP encapsulation. The following discussion makes Mobile IPv6↕s understanding more clear by highlighting the benefit of Mobile IPv6 over mobile IPv4.

- Route Optimization is a built-in feature for Mobile IPv6. In mobile IPv4, this feature was available via an optional set of extensions that was not supported by all nodes.
- There is no requirement of foreign Agents in Mobile IPv6. As mentioned previously, Neighbour Discovery and Address Auto-configuration features enable mobile nodes to function in any location without the services of any special router in that location.
- There is no ingress filtering problem in Mobile IPv6 (In Mobile IPv4 this happens because the correspondent node puts its home address as the source address of the packet). In Mobile IPv6, the correspondent node puts the care-of address as the source address and having a Home Address Destination option, allow the use of the care-of address to be transparent over the IP layer.

Whereas IPv6 allows the deployment of millions of always-on, IP enabled devices, each with its own unique IP address, Mobile IPv6 enables mobile terminals to maintain their IP connectivity as they move across several networks. The goal for Mobile IPv6 is to provide provides seamless mobility for next generation mobile services and applications and across several access technologies such as WCDMA, WLAN etc. Additionally, Mobile IPv6 provides route optimization techniques to reduce handoff latencies.

Mobile IPv6 is a powerful enabler for the next generation of services such as peer-to-peer services, push services and Voice over IP (VoIP) which demand always-on global reachability and seamless mobility. Mobile IPv6, along with fast-handoffs and context transfer mechanisms will be essential for the large scale deployment of real-time services such as VoIP and broadcast services.

4. Mobility Management

Mobility Management is one of the major functions of a GSM or a UMTS network that allows mobile phones to work. The aim of mobility management is to track where the subscribers are, so that calls, SMS and other mobile phone services can be delivered to them. [10]

4.1 Location update procedure

A GSM or UMTS network, like all cellular networks, is a radio network of individual cells, known as base stations. Each base station covers a small geographical area which is part of a uniquely identified location area. By integrating the coverage of each of these base stations, a cellular network provides a radio coverage over a very much wider area. A group of base stations is called a location area, or a routing area.

The location update procedure allows a mobile device to inform the cellular network, whenever it moves from one location area to the next. Mobiles are responsible for detecting location area codes. When a mobile finds that the location area code is different from its last update, it performs another update by sending to

the network, a location update request, together with its previous location, and its Temporary Mobile Subscriber Identity (TMSI).

There are several reasons why a mobile may provide updated location information to the network. Whenever a mobile is switched on or off, the network may require it to perform an IMSI attach or IMSI detach location update procedure. Also, each mobile is required to regularly report its location at a set time interval using a periodic location update procedure. Whenever a mobile moves from one location area to the next while not on a call, a random location update is required. This is also required of a stationary mobile that reselects coverage from a cell in a different location area, because of signal fade. Thus a subscriber has reliable access to the network and may be reached with a call, while enjoying the freedom of mobility within the whole coverage area.

When a subscriber is paged in an attempt to deliver a call or SMS and the subscriber does not reply to that page then the subscriber is marked as absent in both the MSC/VLR and the HLR (Mobile not reachable flag MNRF is set). The next time the mobile performs a location update the HLR is updated and the mobile not reachable flag is cleared.

4.2 TMSI

The "Temporary Mobile Subscriber Identity" (TMSI) is the identity that is most commonly sent between the mobile and the network. TMSI is randomly assigned by the VLR to every mobile in the area, the moment it is switched on. The number is local to a location area, and so it has to be updated each time the mobile moves to a new geographical area.

The network can also change the TMSI of the mobile at any time. And it normally does so, in order to avoid the subscriber from being identified, and tracked by eavesdroppers on the radio interface. This makes it difficult to trace which mobile is which, except briefly, when the mobile is just switched on, or when the data in the mobile becomes invalid for one reason or another. At that point, the global "international mobile subscriber identity" (IMSI) must be sent to the network. This is a unique number that is associated with all GSM and UMTS network mobile phone users. The number is stored in the SIM card. The IMSI is sent as rarely as possible, to avoid it being identified and tracked.

A key use of the TMSI is in paging a mobile. "Paging" is the one-to-one communication between the mobile and the base station. The most important use of broadcast information is to set up channels for "paging". Every cellular system has a broadcast mechanism to distribute such information to a plurality of mobiles.Size of TMSI is 4 octet with full hex digits and can't be all ones.

4.3 Roaming

Roaming is one of the fundamental mobility management procedures of all cellular networks. Roaming is defined[1] as the ability for a cellular customer to automatically make and receive voice calls, send and receive data, or access other services, including home data services, when travelling outside the geographical coverage area of the home network, by means of using a visited network. This can be done by using a communication terminal or else just by using the subscriber identity

in the visited network. Roaming is technically supported by mobility management, authentication, authorization and billing procedures.

A "location area" is a set of base stations that are grouped together to optimise signalling. Typically, 10s or even 100s of base stations share a single Base Station Controller (BSC) in GSM, or a Radio Network Controller (RNC) in UMTS, the intelligence behind the base stations. The BSC handles allocation of radio channels, receives measurements from the mobile phones, controls handovers from base station to base station.

To each location area, a unique number called a "location area code" is assigned. The location area code is broadcast by each base station, known as a "base transceiver station" BTS in GSM, or a Node B in UMTS, at regular intervals.

In GSM, the mobiles cannot communicate directly with each other but, have to be channeled through the BTSs. In UMTS networks, if no Node B is accessible to a mobile, it will not be able to make any connections at all.

If the location areas are very large, there will be many mobiles operating simultaneously, resulting in very high paging traffic, as every paging request has to be broadcast to every base station in the location area. This wastes bandwidth and power on the mobile, by requiring it to listen for broadcast messages too much of the time. If on the other hand, there are too many small location areas, the mobile must contact the network very often for changes of location, which will also drain the mobile's battery. A balance has therefore to be struck.

4.4 Routing Area

The routing area is the PS domain equivalent of the location area. A "routing area" is normally a subdivision of a "location area". Routing areas are used by mobiles which are GPRS-attached. GPRS ("General Packet Radio Services"), GSM’s new data transmission technology, is optimized for "bursty" data communication services, such as wireless internet/intranet, and multimedia services. It is also known as GSM-IP ("Internet Protocol") because it will connect users directly to Internet Service Providers (ISP). The bursty nature of packet traffic means that more paging messages are expected per mobile, and so it is worth knowing the location of the mobile more accurately than it would be with traditional circuit-switched traffic. A change from routing area to routing area (called a "Routing Area Update") is done in an almost identical way to a change from location area to location area. The main differences are that the "Serving GPRS Support Node" (SGSN) is the element involved.

5. Related Technologies

5.1 Improved Location Management Scheme Based on Autoconfigured Logical Topology in HMIPv6

This scheme is proposed to solve the existing problem using the autoconfigured logical topology, while examining in detail the MN’s operation. The scheme does not require a BU in HA and CNs to autonomously configure the logical topology

between neighboring MAPs [7]. Subsequently applying the scheme to find neighboring MAPs for each MAP of an initial MN in HMIPv6.

5.1.1 Motivation. Each MAP configures by using the autoconfigured logical topology having route and cost information between MAPs. Each MAP also forecasts the neighboring MAP's movement location, and performs a BU. Through the autoconfigured logical topology, it is possible to support fast handoff based on anticipated information as well as location update and packet delivery costs. It is also possible to transfer the profile for authentication in advance since neighboring MAP's information on the security architecture, called AAA(Authentication, Authorization, Accounting) is known, and applying the QoS resource reservation.

We assume that the information between MAPs is known in advance. Figure 3 shows the autoconfigured logical topology between MAPs [6]. Each MAP must be accessible to the information for neighboring MAPs to configure the autoconfigured logical topology with neighboring MAPs. If a MAP stores the information on a single static table, when a new MAP is added, the neighboring MAPs may have to update the table themselves in order to reconfigure the autoconfigured logical topology [6].

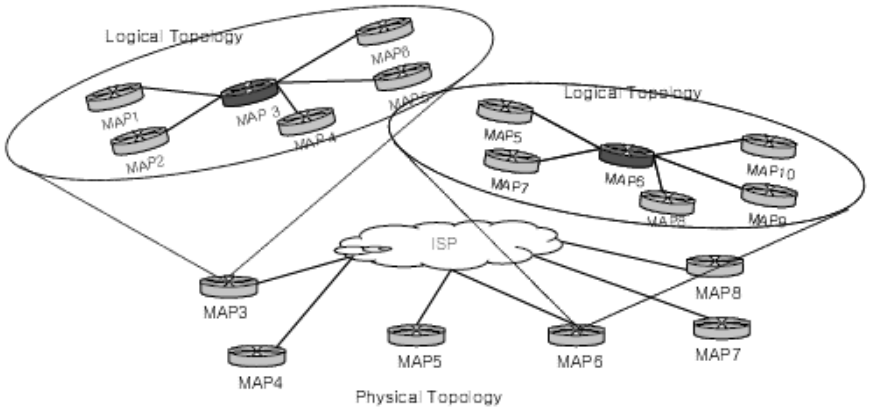

Figure. 3. Logical topology between MAPs

5.1.2 The Scheme Based on Logical Topology. We name the MAPs are named by sequence numbers such as MAP1, MAP2,...,MAPq for convenience. MAP1 already has a table to manage the neighboring MAPs and generates another table to manage the MN. In addition, MAP1 registers all CNs connected to HA and MN using its own RCoA. When HA and CN have the BU message, they store the MN's RCoA to use while connecting with a MN. A

BU message does not transmit to HA and CNs when MN moves within MAP. Instead, MAP receives this message to record the information for the location update based on MN's LCoA. A MN receives adjacent MAP information in the form of a table, which selects MAP2 because MAP2 has the smallest hop number in the table. For this step, we use the algorithm to select a MAP that has the shortest distance. MN sends MAP1's RCoA and initial MAP's RCoA to the MAP2 when MN registers

to the MAP2. The MAP2 sends its RCoA and initial MAP's RCoA to the MAP1, and then the MAP1 compares the initial MAP's RCoA with itself. Therefore, when HA transmits data, the data is delivered by this route. This scheme saves signaling costs in comparison with the existing schemes, like HMIPv6. Similarly, when a MN moves from MAP2 to MAP3, the MN transmits the registration message (MAP2's RCoA, initial registration MAP's RCoA) to MAP3, and then MAP3 transmits two messages to MAP1. In this case, MAP1 deletes MAP2's RCoA in the MN's list since it contains the MAP's RCoA and records MAP3's RCoA. MAP1 and MAP3 are then linked through the registration. Therefore, the proposed scheme is not required to send the binding information to the HA and CNs.

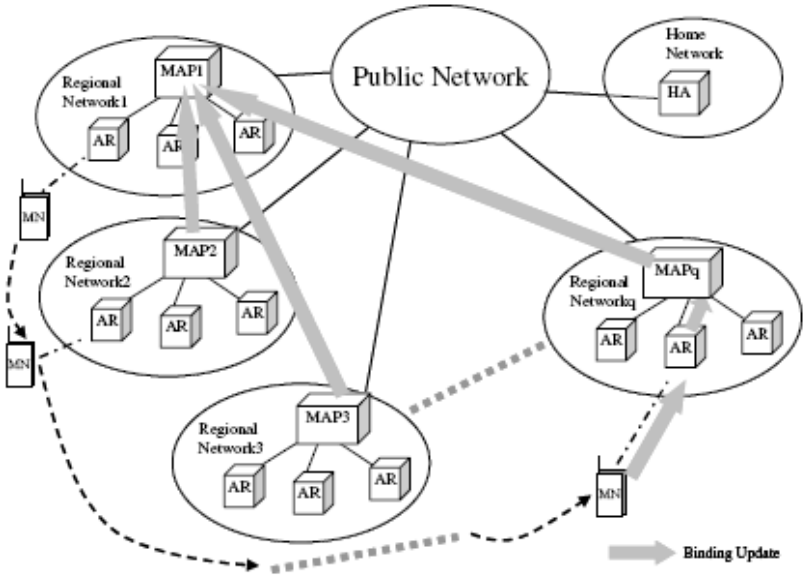

Figure. 4. Binding Update of the Scheme

As shown in Figure 4, we consider a MN moving from MAP1 to MAPq as an example of global handoff. In the proposed scheme, the greatest achievment comes from a step reduction, while not continuously keeping links to several steps. The maximum number of forwarding links allowed between MAPs is not fixed but optimized for each MN to minimize the total signaling cost. The optimal number is obtained, based on the operational difference between the existing scheme and the proposed one. MIPv6 allows MNs to move around the internet topology while maintaining the reachability and ongoing connections between the mobile and CNs. To do this the MN sends the BU to its HA and all CNs communicating every time it moves. Hence, increasing the number of CNs influences the system performance in negative manner. However the proposed scheme is independent of the number of CNs while the MN moves in forwarding steps as we have discussed.

5.2 Connection and Session Management for QoS-Guaranteed Multimedia Service Provisioning on IP/MPLS Networks

5.2.1 QoS-Guaranteed per-Class-Type Virtual Networking in an Intra-AS Domain Network. Configuration of scalable per-class-type virtual networks in an intra-AS domain network is one of the key traffic engineering function in QoS-guaranteed DiffServ provisioning. As shown in Figure 5, the NMS (network management system) in each AS domain network configures multiple virtual networks for each DiffServ class-type considering the QoS parameters. In a per-class-type virtual network, multiple QoS-guaranteed TE-LSPs are established among PE routers to configure connectivity of full mesh topology. The DiffServ-aware-MPLS AS domain network provides the network-view information of IP/MPLS routers, data links among routers, and CSPF (constraint-based shortest path first) routing function. The QoS-guaranteed per-class-type virtual network function can be provided as the connectivity management API (application programming interface) of Parlay/OSA (Open Service Architecture) standard [8].

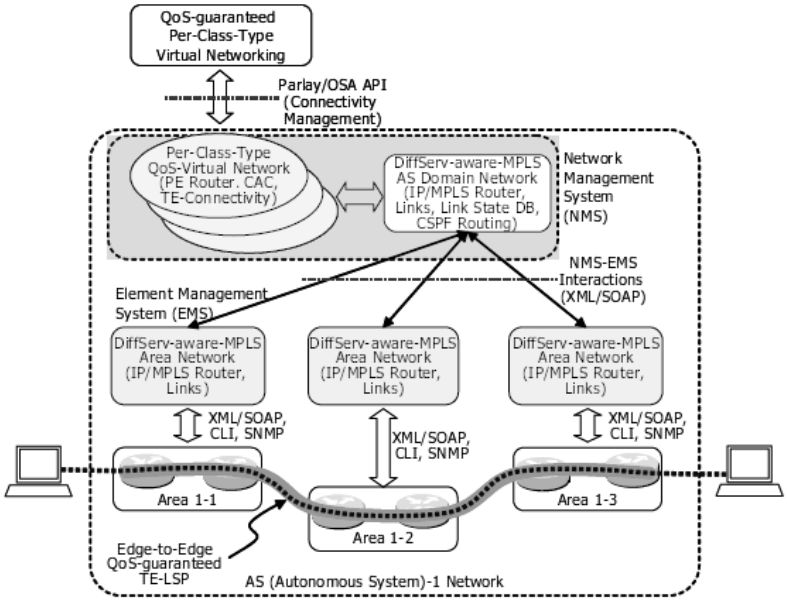

Figure. 5. QoS-guaranteed per-class-type virtual networking in an AS domain network

5.2.2 QoS-Guaranteed per-Class-Type Virtual Networking Among Inter-AS Domain Networks. The configuration of per-class-type virtual networks across multiple AS domain network is very important to support QoS-guaranteed DiffServ efficiently through multiple AS domain networks without scalability problem. In order to configure virtual networks for DiffServ class-types, the NMS establishes edge-toedge TE-LSP in two-level hierarchy: (i) establishment of ASBR (autonomous system boundary router)-to-ASBR trunk TE-LSP as inter-AS transit tunnels, and (ii) establishment of edge-to-edge QoS-guaranteed TE-LSP through the transit tunnels among ASBRs.

In order to establish QoS-guaranteed ASBR-to-ASBR transit TE-LSP, the network resource availability and traffic engineering parameters of each AS domain network must be collected. Current BGP (border gateway protocol), unfortunately, only provides reachability & route information, and does not provide traffic & QoS information of the route. As an alternative solution, Web-service architecture can be used to implement the interactions among NMSes for AS domain networks [8].

As shown in Figure 6, NMS of each AS domain network would register the available connectivity services among ASBR in the AS domain network through Web service registration. The ingress NMS queries the UDDI registry to get the URL of WSDL for the NMS of destination network to which the destination CPN (customer premises network) is attached. It then retrieves the information of neighbor NMS, recursively, until one of the neighbor of the intermediate NMS is itself. Based on the collected AS domain network connectivity information and the available transit networking attributes (i.e., available bandwidth, edge-to-edge transfer delay, etc.), the originating NMS can find the constraintbased shortest path between the ASBRs of the originating AS domain and the destination AS domain. Multiple ASBR-to-ASBR transit TE-LSPs may be configured with different route for the virtual transit networks according to DiffServ class-types.

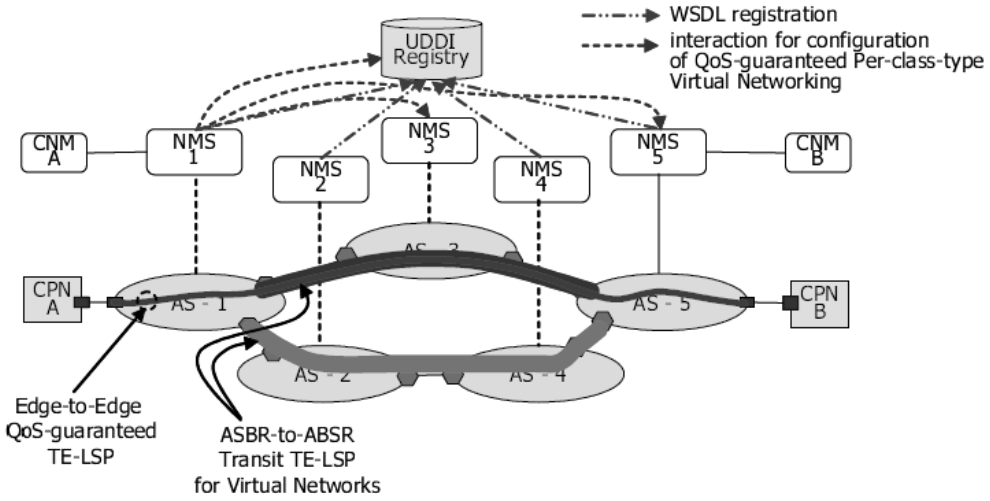

Figure. 6. Configuration of transit virtual networks

The ingress NMS then configures intra-AS DiffServ-aware-LSP in the originating AS domain network with configuration of DiffServ-aware packet processing at ingress provider edge (PE) router, requests the destination NMS to setup the LSP at destination domain network, and finally completes the edge-to-edge DiffServ-aware-LSP through the transit trunk TE-LSP of transit virtual network for the requested DiffServ class-type.

7. Conclusion

Mobile IP is at its best in a large network. Roaming in an area where the transceivers cover only a very small geographic area, the mobility can be achieved by a simpler manner. A wide use of Mobile IP requires that a considerably high number of routers support it, otherwise the routing will be less optimal. Keeping in mind the benefits of compatibility, this can be considered as a minor - and temporary – inconvenience. In this paper, we review IP mobility and its components. And also, we review current technologies related to IP mobility.

References

[1] Ville Ollikainen (1999) MOBILE IP explained http://www.tml.tkk.fi/Opinnot/Tik-111.550/1999/Esitelmat/MobileIP/Mobip.html

[2] Wikipedia – IP Mobility http://en.wikipedia.org/wiki/Mobile_IP

[3] Wikipedia – Proxy Mobile IP http://en.wikipedia.org/wiki/Proxy_Mobile_IP

[4] Esa Piri and Kostas Pentikousis, VTT Technical Research Centre of Finland, "IEEE 802.21" The Internet Protocol Journal, Volume 12, No.2

[5] Kaushik Das "Mobile IPv6" http://ipv6.com/articles/mobile/Mobile-IPv6.htm

[6] Jongpil Jeong, Hyunsang Youn, Hyunseung Choo, Eunseok Lee, "Improved Location Management Scheme Based on Autoconfigured Logical Topology in HMIPv6" , O. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3480

[7] F. Preparata, et al., "Computational Geometry (Monographs in Computer Science)," Springer-Verlag Berlin and Heidelberg GmbH & Co., October 1990.

[8] Young-Tak Kim, Hae-Sun Kim, Hyun-Ho Shin, "Session and Connection Management for QoS-Guaranteed Multimedia Service Provisioning on IP/MPLS Networks", O. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3480

[9] http://doc.utwente.nl/65994/1/tr-ctit-99-21.pdf

[10] Wikipedia – Mobility Management http://en.wikipedia.org/wiki/Mobility_management