MOBILE ACCESS TO THE INTERNET

Jozef NOVIKMEC, Ľubomír DOBOŠ
Dept. of Electronics and Multimedia Telecommunications
Technical University of Košice
Park Komenského 13, 04001 Košice
Slovak Republic

novikmec@pobox.sk, lubomir.dobos@tuke.sk

Abstract

In this paper various aspects of mobile access to Internet are discussed. We mention general Internet protocols and mobile enhancements and also future models that will be used in near future.

Keywords

Mobile, IPv4, IPv6, Cellular IP, Mobile IPv6.

1. IPv4 vs. IPv6

Internet protocol is protocol which powers today Internet. In IPv4, the unique address of each device interface is 32-bit number. This address is represented as four decimal numbers also known as octets separated by dots. (e.g. 62.168.100.12).

After a short Internet story Internet was about to run out of IP addresses. Large number of new users would have no way how to join communication highway. Some Internet observers warned that explosive growth of Internet would prove the IPv4's 32-bit address length, although capable providing unique 4,2 billion hosts, to be inadequate. The solution to this problem (and also some others) seems to be new Internet protocol implementation. New IP version is IPv6.

1.1 Differences between IPv4 and IPv6

IP version 6, also known as IPng (Internet Protocol next generation), was designed, first and foremost, to provide a solution to the address space limitations of its predecessor. Officially finalized in September 1995 by IETF (Internet Engineering Task Force) the protocol's new 128-bit address space descriptor ensures that the "sky" of address space depletion will not fall down for many years. By conservative estimates, IPv6 will support thousand of addresses for each square meter of the Earth's surface.

The IPv6 also carries some new features that make the new IP more inviting. IPv6's automatic address-configuration capability allows a v6-enabled host to discover automatically the information it needs to connect to the Internet or to private TCP/IP network. The new packet header for IPv6 provides the means to reserve bandwidth along a path for quick transport and smooth playback of audio and video traffic. Header options add a means for authenticating and encapsulating IP packet payload for enhance security during transport over a network. The new IP even designed a "dual-stack" and "tunneling" schemes to ensure that IPv6 could be implemented in an IPv4 world smoothly and gradually.

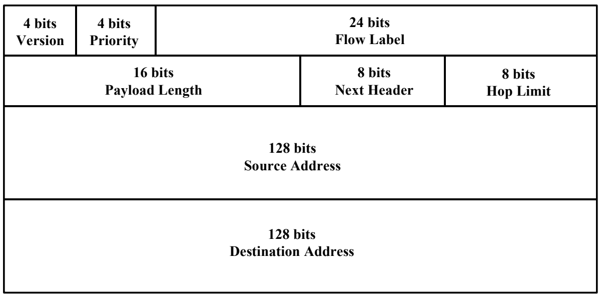

Fig.1 IPv6 Packet Layout.

IPv6 address is more complicated and also has different representation. IPv6 uses eight 16-bit hexadecimal values used to represent a total of 128 bits. (e.g. FEDC:BA98:7654:3210:FEDC:BA98:7654:3210)

The second, or zero suppressed, form allows "::" to indicate multiple groups of suppressed zeroes. Address 1080:0:0:0:8:800:200C:417A may be represented as 1080:8:800:200C:417A.

1.2 IPv4 Extensions

While IETE was working out the details of IPv6, IS managers and networking vendors were addressing the concerns of customers about the limitations of IPv4, especially in the area of address limitations. New technologies, such as DHCP (Dynamic Host Configuration Protocol) and NAT (Network Address Translation) in particular, were introduced in the early 1990s to response the deficiencies in IPv4 addressing and security.

1.3 Quality of Service and Security

Regarding Quality of Services, IPv4 Extensions developed some new protocols such as Real-Time Protocol (RTP), Real-Time Control Protocol (RTCP) for real-time audio and video signaling, and the Resource ReSerVation Protocol (RSVP) which creates a path through the v4 network, talking to equipment and reserving buffering and bandwidth over the path. Those are just like what v6 QoS and bandwidth reservation do although there is no official standard available yet. But the test proves that by using those protocols, IPv4 network can transmit audio and video signals over a long distance without being much degraded.

IPv6 security is provided by IPsec (IP Security) which is layer 3 ISO/OSI model protocol that can authenticate TCP/IP connections, add confidentiality and integrity to TCP/IP packets, and is transparent to the application and the underlying networking infrastructure. The same protocol can be used to upgrade IPv4 security.

Several features of IPv6 now have equivalent facilities in IPv4:

IPv6 Feature or Function	**IPv4 equivalent or workaround**
Address space expansion: 128-bit address instead of 32-bit v4 address	**Address pooling and reuse:** Through DHCP and address translation
Host autoconfiguration: Built in to IPv6	**DHCP:** comparable means for automated addressing of host in v4 environment.
Quality and class of service: Header options provide bandwidth reservation for audio and video, which are sensitive to interference.	**Quality of service:** Use bandwidth reservation protocol RSVP and real-time protocol RTCP.
Security header: Option available in v6.	**Ipsec:** Security protocol used in v6 is available for implementation in v4.

2. Mobile IPv6

This section specifies the operation of mobile computers using Internet Protocol Version 6 (IPv6). Without specific support for mobility in IPv6, packets destined to a mobile node (host or router) would not be able to reach it while the mobile node is away from its home link (the link on which its home IPv6 subnet prefix is in use), since routing is based on the subnet prefix in a packet's destination IP address. In order to continue communication in spite of its movement, a mobile node could change its IP address each time it moves to a new link, but the mobile node would then not be able to maintain transport and higher-layer connections when it changes location. Mobility support in IPv6 is particularly important, as mobile computers are likely to account for a majority or at least a substantial fraction of the population of the Internet during the lifetime of IPv6.

The protocol operation defined here, known as Mobile IPv6, allows a mobile node to move from one link to another without changing the mobile node's IP address. A mobile node is always addressable by its "home address", an IP address assigned to the mobile node within its home subnet prefix on its home link. Packets may be routed to the mobile node using this address regardless of the mobile node's current point of attachment to the Internet, and the mobile node may continue to communicate with other nodes (stationary or mobile) after moving to a new link. The movement of a mobile node away from its home link is thus transparent to transport and higher-layer protocols and applications.

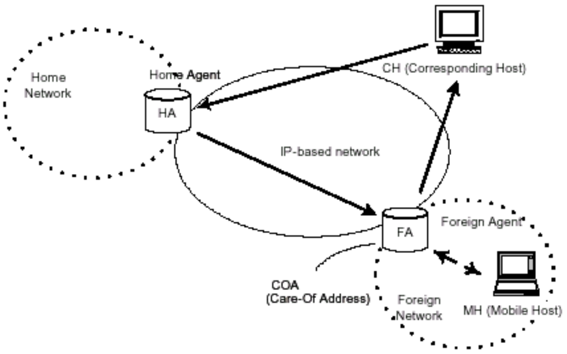

Fig. 2 Mobile IP with Foreign Agent

The Mobile IPv6 protocol is just as suitable for mobility across homogeneous media as for mobility across heterogeneous media. For example, Mobile IPv6 facilitates node movement from one Ethernet segment to another as well as it facilitates node movement from an Ethernet segment to a wireless LAN cell, with the mobile node's IP address remaining unchanged in spite of such movement.

One can think of the Mobile IPv6 protocol as solving the network-layer mobility management problem. Some mobility management applications (for example, handover among wireless transceivers, each of which covers only a very small geographic area) have been solved using link-layer techniques. For example, in many current wireless LAN products, link-layer mobility mechanisms allow a "handover" of a mobile node from one cell to another, reestablishing link-layer connectivity to the node in each new location. Within the natural limitations imposed by link-management solutions, and as long as such handover occurs only within cells of the mobile node's home link, such link-layer mobility mechanisms may offer faster convergence and lower overhead than Mobile IPv6. Extensions to the Mobile IPv6 protocol have been proposed to support a more local, hierarchical form of mobility management, but such extensions are beyond the scope of this document.

The protocol specified in this document solves the problem of transparently routing packets to and from mobile nodes while away from home. However, it does not attempt to solve all general problems related to the use of mobile computers or wireless networks.

3. Overview of Mobile IPv6

A mobile node is always addressable by its home address, whether it is currently attached to its home link or is away from home. While a mobile node is at home, packets addressed to its home address are routed to it using conventional Internet routing mechanisms in the same way as if the node were never mobile. Since the subnet prefix of a mobile node's home address is the subnet prefix (or one of the subnet prefixes) on the mobile node's home link (it is the mobile node's home subnet prefix), packets addressed to it will be routed to its home link.

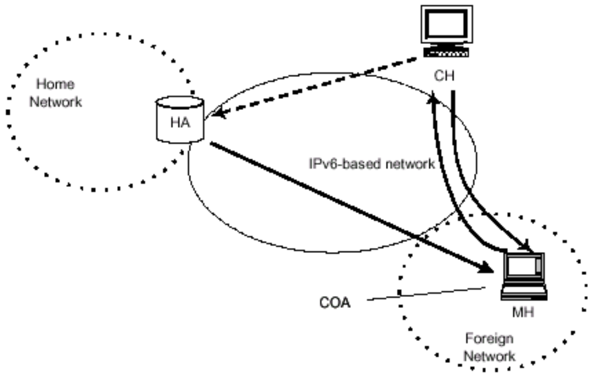

Fig. 3 Mobile IPv6

While a mobile node is attached to some foreign link away from home, it is also addressable by one or more care-of addresses, in addition to its home address. A care-of address is an IP address associated with a mobile node while visiting a particular foreign link. The subnet prefix of a mobile node's care-of address is the subnet prefix (or one of the subnet prefixes) on the foreign link being visited by the mobile node; if the mobile node is connected to this foreign link while using that care-of address, packets addressed to this care-of address will be routed to the mobile node in its location away from home [2].

The association between a mobile node's home address and care-of address is known as a "binding" for the mobile node. A mobile node typically acquires its care-of address through stateless or stateful (e.g., DHCPv6) Address Autoconfiguration, according to the methods of IPv6 Neighbor Discovery. Other methods of acquiring a care-of address are also possible, such as static pre-assignment by the owner or manager of a particular foreign link, but details of such other methods are beyond the scope of this document.

While away from home, a mobile node registers one of its care-of addresses with a router on its home link, requesting this router to function as the "home agent" for the mobile node. This binding registration is done by the mobile node sending to the home agent a packet containing a "Binding Update" destination option; the home agent then replies to the mobile node by returning a packet containing a "Binding Acknowledgement" destination option. The care-of address in this binding registered with its home agent is known as the mobile node's "primary care-of address". The mobile node's home agent thereafter uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the mobile node's home address (or home addresses) on the home link, and tunnels each intercepted packet to the mobile node's primary care-of address. To tunnel each intercepted packet, the home agent encapsulates the packet using IPv6 encapsulation [4], with the outer IPv6 header addressed to the mobile node's primary care-of address.

When a mobile node moves from one care-of address to a new care-of address on a new link, it is desirable for packets arriving at the previous care-of address to be tunneled to the mobile node's care-of address. Since the purpose of a Binding Update is to establish exactly this kind of tunneling, it is specified to be used (at least temporarily) for tunnels originating at the mobile node's previous care-of address, in exactly the same way that it is used for establishing tunnels from the mobile node's home address to the mobile node's current care-of address.

There are reasons why it may be desirable for a mobile node to use more than one care-of address at the same time. However, a mobile node's primary care-of address is distinct among these in that the home agent maintains only a single care-of address registered for each mobile node, and always tunnels a mobile node's packets intercepted from its home link to this mobile node's registered primary care-of address. The home agent thus need not implement any policy to determine the particular care-of address to which it will tunnel each intercepted packet. The mobile node alone controls the policy by which it selects the care-of addresses to register with its home agent.

It is possible that while a mobile node is away from home, some nodes on its home link may be reconfigured, such that the router that was operating as the mobile node's home agent is replaced by a different router serving this role. In this case, the mobile node may not know the IP address of its own home agent. Mobile IPv6 provides a mechanism, known as "dynamic home agent address discovery", that allows a mobile node to dynamically discover the IP address of a home agent on its home link with which it may register its (primary) care-of address while away from home. The mobile node sends an ICMP "Home Agent Address Discovery Request" message to the "Mobile IPv6 Home-Agents" anycast address for its own home subnet prefix and thus reaches one of the (possibly many) routers on its home link currently operating as a home agent. This home agent then returns an ICMP "Home Agent Address Discovery Reply" message to the mobile node, including a list of home agents on the home link. This list of home agents is maintained by each home agent on the home link through use of the Home Agent (H) bit in each home agent's periodic unsolicited multicast Router Advertisements [2].

The Binding Update and Binding Acknowledgement destination options, together with a "Binding Request" destination option, are also used to allow IPv6 nodes communicating with a mobile node, to dynamically learn and cache the mobile node's binding. When sending a packet to any IPv6 destination, a node checks its cached bindings for an entry for the packet's destination address. If a cached binding for this destination address is found, the node uses an IPv6 Routing header (instead of IPv6 encapsulation) to route the packet to the mobile node by way of the care-of address indicated in this binding. If, instead, the sending node has no cached binding for this destination address, the node sends the packet normally (with no Routing header), and the packet is subsequently intercepted and tunneled by the mobile node's home agent as described above. Any node communicating with a mobile node is referred to in this document as a "correspondent node" of the mobile node, and may itself be either a stationary node or a mobile node.

Since a Binding Update, Binding Acknowledgement, and Binding Request are each represented in a packet as an IPv6 destination option, they may be included in any IPv6 packet. Any of these options can be sent in either of two ways:

- the messages can be included within any IPv6 packet carrying any payload such as TCP or UDP.
- the messages can be sent as a separate IPv6 packet containing no payload. In this case, the Next Header field in the last extension header in the packet is set to the value 59, to indicate "No Next Header".

Mobile IPv6 also defines one additional IPv6 destination option. When a mobile node sends a packet while away from home, it will generally set the Source Address in the packet's IPv6 header to one of its current care-of addresses, and will also include a "Home Address" destination option in the packet, giving the mobile node's home address. Many routers implement security policies such as "ingress filtering" that do not allow forwarding of packets that have a Source Address that appears topologically incorrect. By using the care-of address as the IPv6 header Source Address, the packet will be able to pass normally through such routers, yet ingress filtering rules will still be able to locate the true topological source of the packet in the same way as packets from non-mobile nodes. By also including the Home Address option in each packet, the sending mobile node can communicate its home address to the correspondent node receiving this packet, allowing the use of the care-of address to be transparent above the Mobile IPv6 support level (e.g., at the transport layer). The inclusion of a Home Address option in a packet affects only the correspondent node's receipt of this single packet; no state is created or modified in the correspondent node as a result of receiving a Home Address option in a packet.

4. Cellular IP

The Cellular IP protocol is intended to provide efficient access and local Mobility Management (MM) for Mobile Stations (MSs). Cellular IP may be used for subnets covering local to metropolitan areas and is suitable for frequently moving Mobile Stations. The protocol has the potential for complementing Mobile IP in providing global terminal mobility. Cellular IP is similar in functionality to GPRS. The Cellular IP Gateway (GW), as shown in Fig.1, can be compared to the Serving GPRS Support Node (SGSN). A Cellular IP gateway interfaces to the Internet to provide global connectivity using Internet as a backbone, while GPRS defines its own core or backbone network, separate from the Internet, and defines a Gateway GPRS Support Node (GGSN) for interfacing to the Internet [3].

GPRS Mobility Management suffers from the added complexity of handling the integration with the GSM circuit switched scheme. Cellular IP does not have this problem since it will support all services, including speech, based on packet switching.

IP datagrams between Mobile Stations on the same Cellular IP subnet, or Base Station Subsystem (BSS) in GPRS terms, do not leave the BSS, but are switched in the gateway. Fig. 1 gives an overview of the architecture. All Uplink traffic (i.e. traffic from the Mobile Station in the direction of the gateway) is supposed to originate at a Mobile Station. Uplink traffic is routed based on standard IP routing (static routing or simple dynamic routing) and will arrive at the gateway. The gateway decides whether the traffic should leave the BSS or go to a local Mobile Station. All upstream Protocol Data Units (PDUs) are used to update the cache structure maintained by Cellular IP nodes. There are two types of caches, the Routing cache and the Paging cache. Both types consist of triplets or mappings of the form <IP-address, interface, expiration time> [1].

Downstream traffic is simply routed along the traces of the upstream traffic.

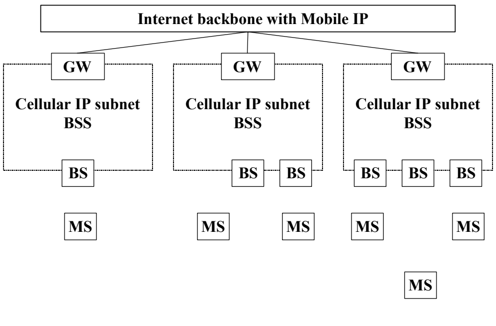

Fig.4 Cellular IP architectural overview

There may be zero or more intermediate routers in a BSS, and the Base Station (BS) may be physically integrated with the gateway. RLC/MAC and GSM RF represent possible reuse of GPRS/GSM layer one and two radiohop protocols. The BSS nodes, except for the BS, may be implemented based on off the shelf router software and hardware, only with minor enhancements to incorporate cache management based on the PDUs and procedures described below [3].

4.1 Protocol Data Units (PDUs)

Cellular IP has defined a Base Station Beacon and two new Mobility Management PDUs:

BS Beacon (Net-ID, IP address of gateway) is transmitted at regular intervals on the air interface by the BS. The identification of the BS or Cell ID is received via the MAC layer.

Paging-update (IP packet with protocol type set to IPPROTO_CELLIPRU) is sent upstream from the Mobile Station to the gateway and may carry Registration payload (payload is the information carried for the layer above).

Route-update (IP packet with protocol type set to IPPROTO_CELLIPRU) is sent upstream from the Mobile Station to the gateway and may carry Registration payload.

Normal user to user IP datagrams sent in the upstream direction have semantic significance to the Mobility Management, and reduces the need for submission of control PDUs.

4.2 Base Station Subsystem (BSS)

All the Cellular IP nodes (BS, Routers and gateway) maintain a Soft-state Route cache, and selected nodes maintain a Paging cache. For simplicity and reliability Paging caches also contain entries for Mobile Hosts that are registered in Route caches. This implies that the Route and Paging cache update procedure are almost identical both for the Idle and the Active state. The only difference is that Route caches are not updated by Idle state Paging-updates, while all up-link packets update the Paging cache (user data, Paging-update and Route-update).

4.3 Cellular and Mobile IP Interworking

Fig. 5 describes the protocol stacks for basic interworking between Cellular and Mobile IP. The gateway (GW) should implement the functionality of the Mobile IP Foreign Agent (MIP FA) in its right half, and the Cellular IP GW in the left half. The relaying of Protocol Data once the Cellular IP Registration is initiated or carried out the GW can register at the Mobile IP Home Agent (HA) [5].

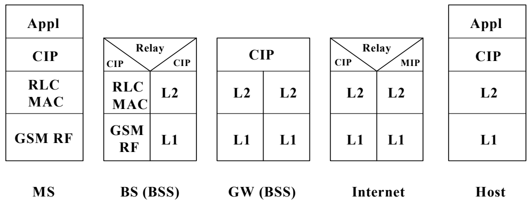

Fig. 5: Cellular and Mobile IP Transmission and Control Plane

5. HAWAII and Cellular IP

The Handoff-Aware Wireless Access Internet Infrastructure (Hawaii) is a domain-based approach for supporting local mobility. Hawaii uses path set-up schemes based on caching. Forwarding cache entries for each attached Mobile Station is implemented in specific routers. This support intra-domain micro-mobility and interworks with Mobile IP to provide inter-domain macro-mobility. These path set-up schemes, based on two way handshakes, reduce mobility related disruption to user applications and by operating locally reduce the number of mobility related updates. Mobile Stations retain their network address while moving within the domain, reducing signaling and simplifying Quality of Service support. Hawaii, like Cellular IP, aims at extending Mobile IP to allow efficient global multimedia mobility.

Performance and scalability improvements are achieved by reducing route update traffic. The number of control messages received by the Mobile IP Home Agent is three times higher than the number of control messages received by the Hawaii gateway (domain router) for a large cellular BSS covering 980 square km. The calculations also show that this area can be covered without any difficulty in processing mobility related control messages. The configuration in Fig. 5 is valid also for the Hawaii version of cellular access, and the above comparison was based on a tree level subnet with one gateway (domain router), seven intermediate nodes connected to twenty Base Stations each.

It is reasonable to believe that Cellular IP may perform slightly better than the Hawaii protocol since a similar Cache approach is used and no dynamic IP routing is needed also for traffic in the downstream direction. The option not to include Cache management in every router imposes the requirement on the standard routers to route on dynamically assigned Care-of addresses, or perform forwarding possibly in multiple directions based on a default scheme, e.g. similar to the paging procedure defined for Cellular IP.

Both the Hawaii and the Cellular IP scheme eases support of controlled service quality by limiting the number of resource reservations that must be re-established when Mobile Stations move within the subnet.

The viability of the cellular approaches is based on the assumption that most user mobility is local to a domain, and in particular local to the administrative domain of the network. Since an administrative domain is under the control of a single authority, it is feasible to locally install routers enhanced for cellular Mobility Management.

5.1 Differences between HAWAII and Cellular IP

The major difference between the two approaches is related to Handoff procedures and to path refresh (i.e. Cache management). There is also some difference in subnet internal forwarding of data traffic, and Hawaii involves dynamic routing when only selected nodes implement the mechanisms for path Caching. Fig. 8 shows a simplified version of the Hawaii Mobile Station Mobility Management, leaving out details like the distinctions between power up, and intra- and inter-domain Handoff. The figure shows that Handoffs are acknowledged, not just repeated as initially proposed for Cellular IP. This confirms that the Mobile Station has been cleared for receiving downstream user data. It is assumed that a confirmation will also be required as part of an efficient security scheme.

6. Conclusions

Today Internet is moving to the mobility. Everybody who knows advantages and uses Internet everyday in the work and also at home, now wants to be connected every time and everywhere. In this article we mentioned some methods, protocols and issues about mobility in IP networks that solve macro and micro mobility problems. With starting of IPv6 commercial implementation we should be prepared to implement also mobility protocols and provide connection everywhere to users. There are already commercial services provided by Japan communication provider NTT Communications [6], [7].

References

[1] Cellular IP: Overview.
http://www.comet.columbia.edu/cellularip/overview.htm

[2] PERKINS, CH. IP Mobility Support. Internet RFC 2002, October 1996.

[3] VALKO, A., CAMPBELL, A. T., GOMEZ, J. Cellular IP, Internet draft, November 1998.

[4] VALKO, A. Cellular IP: A new approach to Internet host mobility. November 1998.

[5] CAMPBELL, A. T., GOMEZ, J., SANGYHO, K., BILL, P., VALKO, A., TURANYI, Z. A cellular IP testbed demonstrator

[6] NTT Communications' IPv6 Activities
http://www.v6.ntt.net/globe/index_e.html

[7] IIJ (Internet Initiative Japan)
http://www.iij.ad.jp/network/index-e.html

About Authors...

Ľubomír DOBOŠ was born in 1956 in Vranov n/T, Slovak Republic. He received the Ing. (M.Sc.) degree and CSc. (Ph.D) degree in Radioelectronics from the Faculty of Electrical Engineering and Informatics, Technical University of Košice, in 1980 and 1989, respectively. Now he is Associate Professor at the Department of Electronics and Multimedia Telecommunications, Faculty of Electrical Engineering and Informatics, Technical University of Košice. His research interest includes wired and wireless communication systems.

Jozef NOVIKMEC was born in Trebišov 28th of May 1978. He graduated on the Technical University of Košice, Dept. of Electronics and Multimedia Telecommunications, Faculty of Electrical Engineering and Informatics in 2001. His research interest is mobility support in IP networks.