

Architectures for Seamless Roaming in 3GPP-WLAN Integration

Behcet Sarikaya, *Senior Member, IEEE*

Abstract— Seamless roaming between the third generation wireless networks and wireless local area networks can be provided using Mobile IP. However, 3GPP and 802.11-based networks have no native support for Mobile IP. Mobile IP requires the deployment of the home agents and a protocol between the mobile nodes, home agent and the corresponding nodes. We address the home agent placement and home address assignment issues for supporting Mobile IP in 3GPP and 802.11-based networks. Placement techniques for Mobile IP home agents are presented including dynamic HA assignment in either WLAN or GPRS/UMTS domains using Diameter Mobile IP application. Next, we present several IPv4 home address assignment schemes for mobile nodes visiting in WLAN domain such as the mobile VPNs, NAT/NAPT traversal and reverse tunneling. It is shown that HA placement and address management are orthogonal and any combination is possible. Various architectures for both issues are evaluated against the optimal solutions.

Index Terms—Home Agent, Corresponding Node, Mobile Node, Network Address/Port Translation, Reverse Tunneling, Mobile VPN, Accounting, Authorization, Authentication.

I. INTRODUCTION

THE wireless local area networks (WLAN) based on IEEE 802.11 standards [10] are becoming increasingly popular in providing access to the Internet. WLANs are available in a wide range of devices and are now being viewed as the means of ubiquitous broadband access platform [3]. 802.11b can provide link speeds of 11 Mbps and application speeds of 5 Mbps and newer standards such as 802.11a/g provide even higher speeds which is ideal for the Internet based data access. What is missing is the real-time packet services such as voice and video [4].

Public cellular networks have evolved from the first generation analog cell phones to second generation (2G) digital cell phone systems and 2.5G packet based low-bandwidth cell phone systems and finally to high-bandwidth all-IP wireless third generation (3G) networks [2]. Global System for Mobility (GSM) is the most popular 2G standard and General Packet Radio System (GPRS) is its 2.5G and

Universal Mobile Telecommunications Systems (UMTS) is its 3G standard and 3rd generation partnership project (3GPP) is the standardization organization. UMTS can provide a maximum of 2 Mbps data speeds. 3G networks are designed to have wide area coverage for public access to their services as such they can be accessed from public areas, businesses and hot spots. Multimedia messaging (MMS) and IP multimedia subsystem (IMS) are major services to be provided by UMTS. With IMS, users will be able to join teleconferences and receive various location-based services such as guided tours. However it will take several years until IMS is fully available.

WLANs and 3G systems will coexist and there are two scenarios for seamless roaming:

1. WLAN user can access 3G packet-switched (PS) based services and service continuity is provided. The change of access, i.e. handover may be noticeable to the user but there will be no need to reestablish the service. Due to the differences in transmission speeds and the system capacity, the quality of service the user gets in the two domains may differ and may be noticeable.

2. WLAN user can access 3G packet-switched (PS) based services and seamless service continuity is provided. Seamless service continuity means minimizing data loss and break time usually experienced during a handover between 3G and WLAN domains.

Mobile IP is the standard protocol defined for terminal mobility in the Internet and therefore in this paper, we propose Mobile IP as the basic mechanism to provide service continuity. The paper limits the scope to Mobile IPv4, the mobile IP for IP version 4 [1]. Address assignment discussed in Section 4 arises as a technical problem due to the use of Mobile IPv4 because of the well-known address shortage in IP version 4. It should be noted that Mobile IP provides service continuity and seamless service continuity can be provided using standardized extensions of the base protocol such as fast handover. The paper's contributions are in the applications of Mobile IP, dynamic home agent assignment, reverse tunneling, network address translation, or NAT traversal, and virtual private network mobility into the problem of seamless roaming between 3G UMTS-based and 802.11-based networks. Quantitative comparison of the architectures identified and simulation studies are out of scope with this paper.

The remaining sections of the paper are organized as follows: Section 2 introduces related work. Section 3 details

This work was supported in part by the Natural Sciences and Engineering Research Council (NSERC) of Canada under a Discovery Grant.

Behcet Sarikaya is with Computer Science Department, University of Northern British Columbia, 3333 University Way, Prince George, BC, Canada V2N 4Z9 (phone: 250-960-5551; fax: 250-960-5544; e-mail: sarikaya@ieec.org).

the home agent placement architectures in WLAN and UMTS domains. Section 4 describes different methods of IPv4 address assignment to the mobile nodes. Finally Section 5 concludes the paper.

II. RELATED WORK

Wireless LANs based on IEEE 802.11 standard [10] provide economical means of Internet access in the hot spot areas such as airports, hotels, etc. Large scale deployment of WLANs can be made possible if WLANs can be integrated with cellular data networks such as GPRS/UMTS [9]. The mobiles need to have dual interfaces in order to access both networks. In the hot spots, the mobile node (MN) uses WLAN access and outside of the hot spot it uses GPRS/UMTS. Early work on integration has concentrated on authentication, authorization and accounting (AAA) aspects.

The simplest method of interconnecting WLANs with GPRS/UMTS is by using two separate authentication, authorization and accounting (AAA) on two different accounts. This type of interconnection is called open coupling. With open coupling the user does not have access to the advanced security and accounting features of a cellular network. Future services such as IMS can not be offered to WLAN users. The interconnection of WLANs can make authentication, authorization and accounting possible using the user's cellular network account. This type of interconnection is called loose coupling [15]. Loose coupling requires WLAN network interface cards with Subscriber Identity Module (SIM) card for GPRS and UMTS SIM (USIM) card for UMTS interfaces. AAA server in WLAN domain communicates with the home location register (HLR) or home subscriber server (HSS) in order to access user's SIM/USIM card data. A common accounting can be made by the charging gateway of the cellular network receiving the accounting data from AAA server (Figure 1).

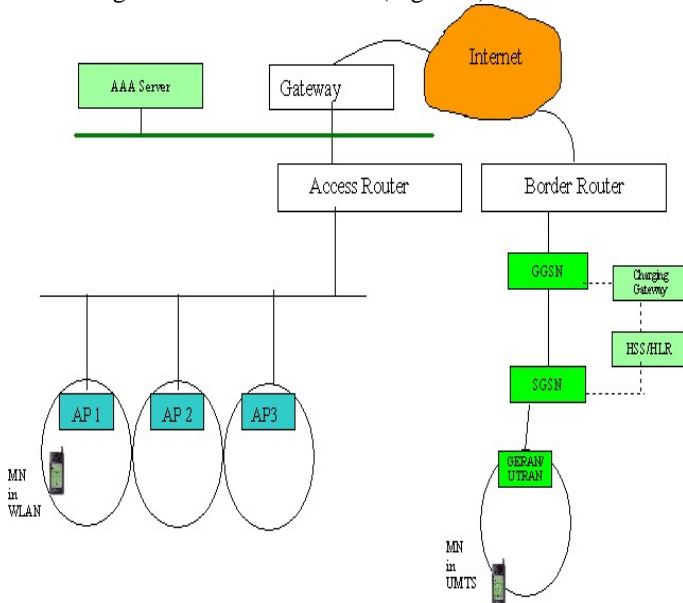


Fig. 1. AAA in WLAN-UMTS Interconnection

Integrating CDMA2000-based 3G networks with 802.11-based networks is facilitated due to the fact that CDMA2000 architecture incorporates support for Mobile IP. Seamless roaming only requires Mobile IP support in 802.11 network. In [16], a new node called IOTA Gateway is introduced at the access router level. IOTA can play the role of the home agent or foreign agent of Mobile IPv4.

A. Mobile IP

In UMTS, Radio Network Controller (RNC) in UTRAN terminates the physical layer and initiates a link layer for IP datagrams. The Packet Data Protocol (PDP) context is established between MN and GGSN and a virtual link providing Layer 2 of the Internet protocol stack is formed consisting of a number of relay devices between MN and GGSN. GPRS Tunneling Protocol (User plane, GTP-U) [11] is the protocol used to encapsulate MN's IP packets and to forward them from RNC to SGSN and from SGSN to GGSN. GTP tries to keep the GGSN the same even if the mobile node moves out to other domains and tunnels the datagrams from the new SGSN to the anchor GGSN (Control Plane GTP, GTP-C). Mobile IP is not used.

On the other hand in WLANs, IP mobility can only be handled with Mobile IP. For seamless communication of the mobile nodes roaming between the two networks, Mobile IP needs to be supported in both GPRS/UMTS and WLAN networks.

Mobile IP is IETF's protocol for supporting node mobility. Mobile nodes (MN) are assigned a home agent (HA) on their home network and in a visited network they may get services from the foreign agents (FA). MN in the visited network gets a new IP address and then registers this address with HA. The new address called care-of address (CoA) is assigned by FA if an FA is available otherwise MN works on the co-located CoA mode and gets an address by other means such as from a DHCP server. Registration is part of Mobile IP and involves sending a Registration Request (RRQ) to HA and receiving a Registration Reply (RRP) from HA. After a successful registration, HA establishes a binding of the home address (HoA) of MN to the care-of address (CoA) of MN and then starts to encapsulate all datagrams sent by correspondent nodes (CN) destined for MN and sends them to the new address. This is called tunneling. A tunnel is not a connection in the sense that there is no error recovery done on the encapsulated datagrams. If no route optimization is involved, Mobile IP is transparent to CNs. The operation of Mobile IP is shown in Fig. 2.

Mobile IP requires the existence of an FA in each foreign subnet MN visits, if there is none then MN uses collocated CoA mode of operation. HA should be a router at the home network. HoA and CoA assigned to MN could be public or private addresses.

B. Private Addresses

Address acquisition in the visited domain is an important operation that we address in this paper. The address can be

public, i.e. unique or it could be private. In today's enterprise networks private addressing has started to be used because of the address shortage in IPv4. In enterprise networks, private addressing is preferred because it provides secure access rather than open and public access to the enterprise network.

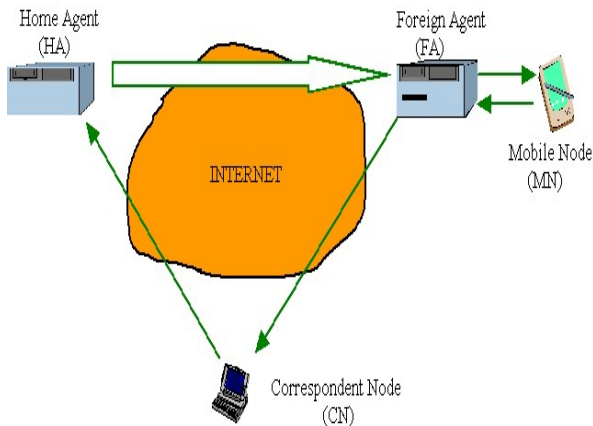


Fig. 2. Mobile IPv4 Architecture

Private addressing is implemented using Network Address/Port Translation (NAT/NAPT) boxes at the entry points to the enterprise networks [20]. A typical architecture is shown in Fig. 3. NAT translates public addresses into private addresses and vice versa.

Mobile IP can be deployed in enterprise networks using private addresses. Home address (HoA) of MNs can be private and the care-of address MNs get in each visited network is also private. Using Mobile IP services MNs can roam in their own enterprise network and get seamless connectivity. The restriction is that MN should stay in the same enterprise network since if MN moves out, its home address can not be routed properly, because HoA is a private address. Fig. 3 shows an enterprise network with three NATs and a HA deployed in one of the subnetworks.

C. Performance of Mobile IP

The use of Mobile IP comes with additional delays incurred due to Mobile IP protocol operations such as registration signaling and HA to MN tunneling. When MN moves in WLAN domain from home to foreign network with an FA an average handover delay is around 5 sec. The delay increases 14% when collocated CoA is used. The applications running on top of Mobile IP suffer some performance degradations as well. Throughput drop for the traffic flow from MN to CN is 9% while a higher throughput drop of 12% is observed from CN to MN due to the additional overhead of HA tunneling.

Real-time applications such as audio and video streams suffer data losses and higher jitter due to the handover delay which is instantaneous. The data loss is recovered over time however occurrences of jitter continue and sometimes could be higher than the tolerance levels for real-time video.

When MN moves from WLAN to GPRS, MN has to connect to GPRS network and then perform a MIP registration with its HA. The handover delay incurred is around 7-10 seconds. This delay could reach 40 seconds when MN is in

collocated CoA mode because GPRS has very low bandwidth capacity. Handover delay of moving from WLAN to UMTS should be the same as moving in WLAN domain due to high bandwidth offered by UMTS [14].

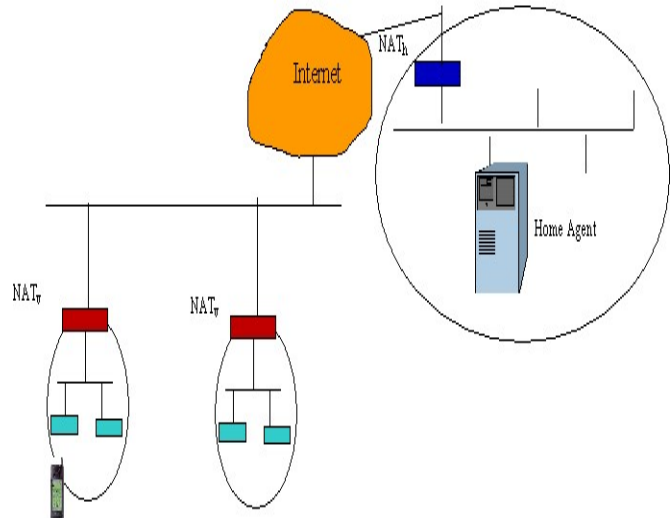


Fig. 3. Private Networks with NAT/NAPT Boxes

III. HA PLACEMENT

There are several requirements in HA placement. For the users of UMTS, the HA should be placed in UMTS network. However, UMTS did not incorporate Mobile IP into its architecture so any new entities to be added must create minimal impact on the overall UMTS operations. When HA is placed in UMTS network for mobiles that roam in WLAN networks, the traffic from the correspondent nodes is routed to the UMTS network. Assuming on the average the corresponding node will send at the application rate of 5 Mbps, the traffic increase in and out of UMTS may reach 1 Gbps if the number of mobiles in WLANs exceed 200. This fact also places another requirement of trying to minimize the effects of the traffic increase.

We present four different architectures in which to place an HA in UMTS network. An alternative to these architectures is to place HA dynamically in UMTS and in WLAN.

A. Architecture 1

HA can be placed in between the border router and a specific GGSN. The GGSN needs to be selected by all mobiles that need to use Mobile IP during PDP context establishment phase in UMTS access. The mobile is always connected to the home network when it is in UMTS and so it does not need any registration with HA. Fig. 4 depicts Architecture 1. In this figure, 3 access points (APs) are configured to be under one IP subnetwork for which the access router (AR) is the subnet router. There are other configurations possible such as one-to-one mapping of APs with the subnetworks with collocated AP and AR.

When the mobile moves to WLAN domain, it needs to register with HA. After successful registration, HA starts to

tunnel the traffic to the mobile.

FA in WLAN domain can be placed at AR as shown in the figure, if no FA is deployed MN has to use collocated CoA mode. In UMTS, due to the placement of HA, if MN establishes PDP context with the specific GGSN then MN, from Mobile IP point of view, is considered at home, so no Mobile IP support is needed. Even if MN roams and changes SGSNs, it only needs to use link layer mobility provided by GTP tunnels.

An advantage of Architecture 1 shown in Fig. 4 is its simplicity, intrinsic Mobile IP support and minimal change to UMTS architecture. A disadvantage of Architecture 1 is that HA must be able to perform very high speed routing, as fast as a GGSN does.

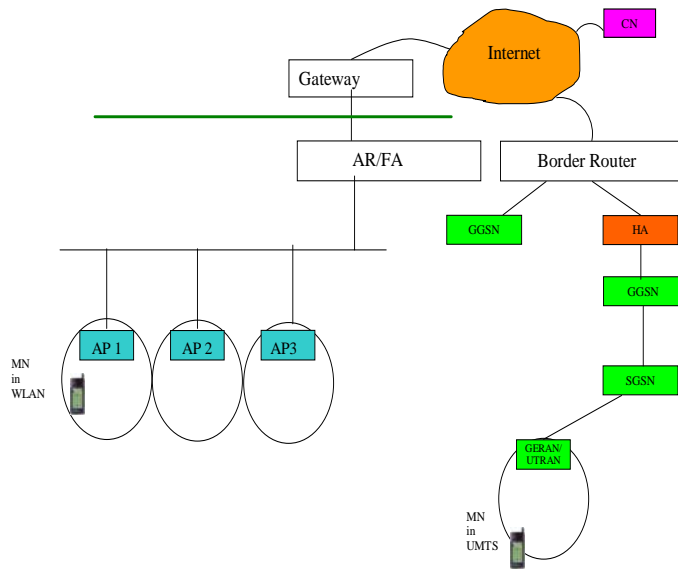


Fig. 4. Architecture 1

B. Architecture 2

HA and GGSN can be connected to the border router instead of tightly coupling HA to GGSN. HA in this architecture now can serve all GGSN's in the domain.

FA in WLAN domain can be placed at AR as shown in Figure 5, if no FA is deployed MN has to use collocated CoA mode. In UMTS, due to the minimum impact requirement, no FA is supported. Mobile IP can be used if MN can be configured in collocated CoA mode. Outgoing datagrams are reverse tunneled to HA because the source address (HoA) is not equal to CoA obtained from GGSN using PDP context activation. The reverse tunneling on top of L2 tunneling (GTP tunneling) can be avoided if ingress filtering is not imposed at GGSN. The mobile registers with HA in the new subnet and starts to use Mobile IP's roaming services (see Figure 5).

Advantages of Architecture 2 are its simplicity and scalability. Only one new entity is added to the UMTS network and the solution is scalable because HA can be scaled as the number of Mobile IP users increase. Compared with Architecture 1, HA does not need to route all GGSN traffic which is another advantage for this architecture.

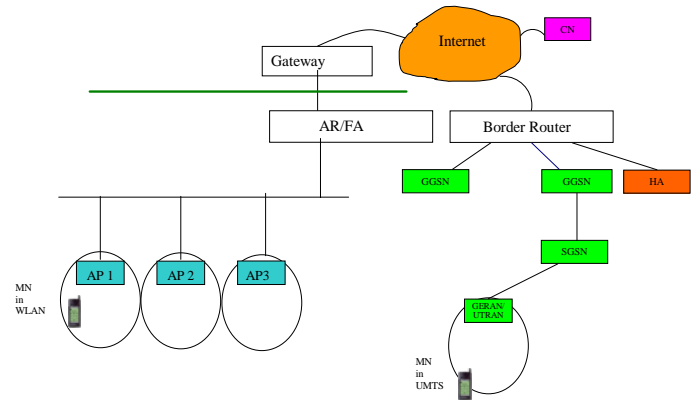


Fig. 5. Architecture 2

C. Architecture 3

HA can be collocated with one of the GGSNs in UMTS network. The mobiles that need Mobile IP services select this GGSN during PDP context establishment. The address assigned to the PDP context is also used as the mobile's Home Address (See Figure 6).

An advantage of HA being collocated with GGSN is that in this case HA does not need to perform proxy ARP [13] interactions for the mobiles. In UMTS network, as in Architecture 1, MNs are in their home network and therefore do not need any Mobile IP services. The disadvantages of Architecture 3 are the load of HA operations that are added to GGSN and the need to reserve the home addresses assigned to the mobiles when they roam into WLANs. These disadvantages do not exist in Architecture 1.

Collocating GGSN with HA works well except when there is a clash in behavior: GGSN terminates any active PDP contexts if the mobile is roaming in WLAN hot spots and it is not in the UMTS footprint and the address is released. HA however has to keep this address in order to perform tunneling for the mobile.

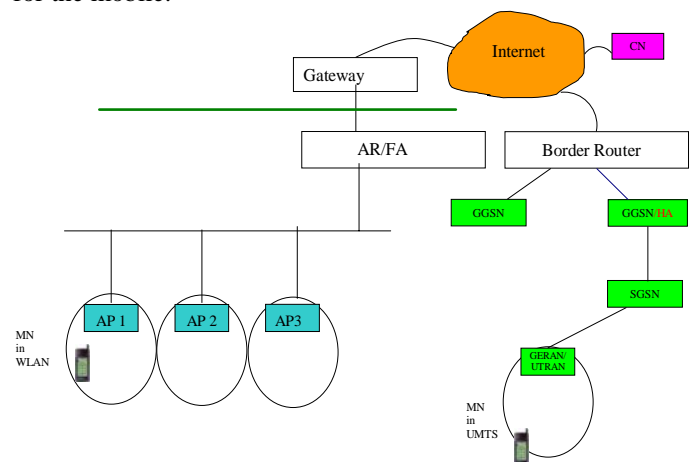


Fig. 6. Architecture 3

D. Architecture 4

Among previous architectures introduced only in Architecture 2 Mobile IP is supported in UMTS. Architecture 4 is a slight modification of Architecture 2 with the addition of a Foreign Agent as shown in Fig. 7. Since GGSN is the default router of the mobiles under its coverage area, FA is best collocated with GGSN.

In Architecture 4 the mobile when roaming in UMTS needs to select a different GGSN and use it as FA in getting a care-of address (the address associated with the PDP context) and register this address with HA.

The disadvantage of Architecture 4 is that the operation of Mobile IP is a partial replacement of UMTS' GTP, i.e. GTP and Mobile IP together introduce redundant mobility handling operations such as encapsulation/decapsulation in the data path.

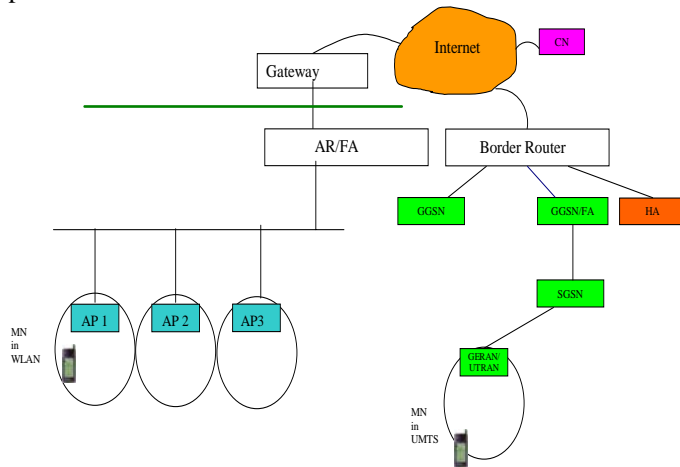


Fig. 7. Architecture 4

E. Dynamic Home Agent Assignment

If the mobiles use an HA that is deployed in UMTS network when roaming in WLAN network, UMTS network may get overloaded with WLAN traffic. The solution to this problem is to dynamically assign an HA in WLAN domain.

Dynamic HA assignment can be done using an FA in the local subnet and Authentication, Authorization and Accounting (AAA) servers in the local and home domains [4]. HA is the home agent when MN is at UMTS domain and the local home agent HA_1 is the home agent when MN is at WLAN. AAA entities of AAAL in WLAN and AAAH in UMTS are also required.

Figure 8 shows dynamic HA assignment protocol operation. Dynamic HA assignment starts with the mobile sending a Mobile IPv4 Registration Request message to FA in which the HoA and HA address fields are set to 0.0.0.0 and 0.0.0.0, respectively. MN has to provide its Network Access Identifier (NAI) so that AAAL can identify MN's AAAH. FA then sends an AA-Mobile-Node-Request (AMR) message (DIAMETER protocol [5]) to AAAL. AAAL assigns a local

HA to MN and adds this to AMR and sends it to AAAH. AAAH determines HA_1 address using domain name system (DNS) and sends Home-Agent-MIP-Request (HAR) message to HA_1 . Local HA generates MIP Registration Reply in a Diameter AVP which is included in Home-Agent-MIP-Answer (HAA) and sends it to AAAH. AAAH then sends an AA-Mobile-Node-Answer (AMA) back to AAAL. AAAL relays it to FA. As a result, Mobile IP tunnel is established with the local HA.

Dynamic HA assignment requires the new address acquired by the mobile to be made known to the corresponding nodes in the Internet. IETF's mechanism for doing this is called domain name system (DNS).

If an FA and AAA servers are not available, dynamic HA assignment can be achieved by MN sending RRQ to the requested HA address. MN can obtain this address either using DHCP Mobile IP Home Agent Option or MN could learn HA hostname using the service location protocol and then use DNS lookup on this name [17].

In case there are several HA servers in the local domain, all with the same address which the DNS returns, finding the nearest HA is a special case of **anycast routing** [19].

MN moves to WLAN domain from UMTS and does a DNS lookup for an HA server using a generic name such as `www.HAServer.com`. DNS lookup returns an IPv4 anycast address, e.g. 10.0.0.1 as the address of such a server. MN sends the RRQ to this address and RRQ is routed by Router 1 to HA Server A because it is the nearest server (Figure 9). HA should however indicate its unicast address in RRP which is used by MN as its HA address.

F. Evaluation

Dynamic HA assignment has several advantages over the other four architectures: two requirements on WLAN-3G integration of minimal traffic increase and minimal or no new entities on UMTS are well satisfied (if Architecture 1 or 2 is used when MN is in UMTS domain).

Disadvantages of dynamic HA assignment are that it is complicated to deploy in a multi-vendor environment and since dynamic HA assignment requires the change of MN's HoA, MN's sessions do not continue. It is possible to keep a single accounting session for a roaming MN if AAA protocol based dynamic HA assignment is used.

Route optimization is a Mobile IP concept in which CNs can be made to direct their packets to MN after the first few going to HA. Route optimization is difficult to achieve in Mobile IPv4 and no standard protocol exists. Clearly, route optimization is the best architecture for HA placement since it eliminates all the disadvantages of all 5 architectures presented above. Since route optimization can not be achieved, the next best architecture is dynamic HA assignment.

IV. IP ADDRESS MANAGEMENT

In this section we will extend the architectures of Section 3 to enable private addressing with Mobile IPv4. Each mobile

may be assigned a private care-of address, collocated care-of address or a private home address. Combinations of public and private address assignments will also be investigated.

A. Architecture 1- NAT/NAPT Traversal

In this architecture MNs have locally assigned dynamic private addresses and they are behind NAT/NAPT hardware. MN may have a private or a public HoA. In order for MN to register its CoA, NAT/NAPT traversal using UDP header is needed. MN's interface or FA encapsulates outgoing datagrams with IP and UDP headers. NAT/NAPT modifies the source address of the external header from CoA to its public IP address. NAT/NAPT also establishes a binding between UDP ports and CoA for this traffic. Decapsulated traffic from HA is normally routed to CN [6]. When CN sends datagrams to MN, HA uses UDP tunneling to add IP and UDP headers. IP header has NAPT's public address as its destination. NAT/NAPT can then use the binding to modify the destination to CoA of MN and MN's interface decapsulates the datagram (Figure 10).

The first case considered by the NAT/NAPT traversal protocol is where MN gets assigned a private CoA (CoApr) in the visited WLAN network and the home address (HoA) is public at the home network. Since HoA is public there is no need to have a NAT/NAPT box at the home network. The second case is where HoA is private which brings two important requirements, e.g. NAT/NAPT processing is required at the home network and MN to CN traffic needs to be tunneled to HA, also known as reverse tunneling as in Architecture 2 below.

If MN has a public HoA, MN or FA to HA UDP tunneling, e.g. reverse tunneling, may not be needed in case NAT/NAPT recognizes and does not filter out public addresses and if there is no ingress filtering, i.e. no packet dropping based on the source addresses not belonging to the local network. In this case MN to CN traffic is routed without any tunneling. CN to MN traffic still needs to be tunneled from HA and NAT/NAPT traversal can be achieved using UDP tunneling.

B. Architecture 2- Reverse Tunneling

In this architecture, HA assigns private HoAs to MNs from the address space defined in RFC 1918 [12]. NAT/NAPT hardware is not used. FA in WLAN domain and HA in GPRS/UMTS domain all have public addresses and therefore datagrams tunneled by HA can be delivered to MN. For outgoing datagrams, a reverse tunnel [7] has to be established from FA or directly from MN to HA as shown in Figure 11.

An advantage of Architecture 2 is that it does not require the use of a NAT/NAPT hardware and yet it allows GPRS/UMTS HA to assign private home addresses to MNs. MNs in this architecture can only communicate with CNs in the same address space.

The possibility of more than one MNs with the same private HoA but assigned to different HAs is a disadvantage of this architecture. An FA is needed in order to direct the traffic to the right MN. FA can use HA address to find the

right binding for the traffic tunneled from HA. MAC addresses are used to distinguish the MNs for outgoing traffic from MNs.

Private addressing architecture 2 does not work with HA placement architecture 2 and 4 because HA in these two architectures can not route the packets reverse tunneled from MN or FA.

The advantages of reverse tunneling are that it allows ingress filtering at the visited network and the source IP address between MN and CN stays the same, allowing the session continuity.

C. Architecture 3- Mobile VPN

If GGSN and HA belong to an enterprise network, i.e. they are behind NAT/NAPT then MN should be configured with mobile virtual private network (VPN) software. VPN provides IP security associations and encryption and Mobile IP provides seamless mobility in foreign networks. Mobile VPN enables private HoAs and CoAs to be assigned to MNs and traversal of NAT/NAPTs in the communication paths between MN and CN (Figure 12). This architecture providing IP security (IPsec) and IP mobility (Mobile IP) at the same time is the most powerful architecture if it can be realized. Both of these technologies use their own IP level tunneling to encapsulate IP datagrams.

When MN configured with an active VPN session moves into a foreign network (indicated as NAT_f in Figure 12) it needs to register its collocated care-of address with an HA located in foreign (external) network called HA_x, establishes a VPN tunnel (using the Internet Key Exchange – IKE), registers VPN tunnel inner address as its collocated CoA with HA in its home network called HA_i by sending RRQ for this registration inside the IPsec tunnel [18]. This protocol requires the simultaneous use of two HAs and the packet processing overhead is high since each packet sent by a corresponding node needs to be encapsulated three times by HA_i, VPN server and HA_x, respectively, to be decapsulated at MN. MN needs to reverse tunnel each packet to HA_x encapsulating three times in order to ensure correct delivery to CN.

Mobile VPN architecture can be integrated into HA placement architecture 2 in Section 3.2 as shown in Fig. 12 where VPN home network and HA_i are in UMTS domain and WLAN is the external network containing HA_x. HA placement architecture 4 does apply as well, as it only incurs having FA functionality at GGSN. HA placement architectures 1 and 3 seem also equally to apply which means that the mobile VPN addressing architecture is orthogonal to HA placement techniques presented in Section 3.

D. Evaluation

For public cellular networks, mobile VPN architecture (Fig. 12) is not the right mode of operation since the users are not enterprise users but rather the general public. If public IP addresses can be assigned then there would be no requirement for any NAT/NAPT traversal and reverse tunneling. Therefore we establish that the optimal addressing architecture can be

provided to MNs with public/ global addresses using IP level security (IPsec) with IP level mobility (Mobile IP) moving the security associations with each handoff. There is no standard protocol to achieve this architecture in IPv4.

Otherwise the next preferred architecture is Architecture 3 due to its support for a more general mobile VPN solution. Architecture 1 or Architecture 2 can be used with their limitations in mind due to their simplicity.

V. CONCLUSION

Wireless LANs are increasing in popularity which means that its users will no longer be content with the Internet only data access and there will be need and commercial interest to introduce 3G packet-switched services such as multimedia messaging, IP multimedia subsystem, instant messaging, presence and location based services and so on. Therefore an integration of WLANs with 3G public cellular networks such as 3GPP will bring advantages to the users as well as the service providers.

We concentrated on service continuity and seamless service continuity of WLAN-GPRS/UMTS interconnection using Mobile IP. Large scale deployment of Mobile IP will not be possible without a thorough understanding of various architectures of home agent placement and IPv4 address assignment to the mobile nodes. We have identified that Mobile IP route optimization which enables MN to communicate with CNs, virtually eliminating HAs, is the optimal technique. In the absence of a standard route optimization protocol, the dynamic home agent assignment satisfies the requirements best. The mobile virtual private network architecture leads to the best address assignment technique in the absence of an optimal technique with secure peer-to-peer addressing which is only possible if IP layer can be changed. We have also introduced various other architectures that can be used in practice, each with an advantage of its own.

Other issues in 3GPP-WLAN integration include the use of RADIUS as the AAA protocol instead of DIAMETER and accounting policies which are inherently different in 3G and in WLAN domain. RADIUS can handle inter-domain operation only by using vendor specific extensions and there is none defined for 3GPP. Technical means of continuity of the accounting session when handover from 3G domain to WLAN domain or vice versa need to be investigated in order

to arrive at solutions for an integrated charging.

Future research is needed towards an indepth analysis and performance modeling of the architectures introduced in this paper. Further investigations are expected to lead to improved algorithms for dynamic home agent assignment and mobile VPN access.

REFERENCES

- [1] C.E. Perkins, "Mobility Support in IP", IETF RFC 3344, Aug. 2002.
- [2] B Sarikaya, "Packet Mode in Wireless Networks: Overview of Transition to Third Generation", IEEE Communications Magazine, Sept. 2000, pp. 164-172.
- [3] P. S. Henry, H. Luo, "Wi-Fi: What's Next?", IEEE Comm. Magazine, Dec. 2002, pp. 66-72.
- [4] S. Garg, M. Kappes, "Admission Control for VoIP Traffic in IEEE 802.11 Networks", Globecom 2003, San Francisco, pp. 3514-3518.
- [5] P. R. Calhoun, T. Johansson, C. Perkins, "Diameter Mobile IPv4 Application", IETF Internet-Draft draft-ietf-aaa-diameter-mobileip-18.txt, March 2004.
- [6] P.R. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, "Diameter Base Protocol", IETF RFC 3588, Sept. 2003.
- [7] H. Levkowitz, S. Varaala, "Mobile IP NAT/NAPT Traversal using UDP Tunneling", IETF RFC 3519, January 2003.
- [8] G. Montenegro, Reverse Tunneling for Mobile IP, IETF RFC 3024, Jan. 2001.
- [9] 3GPP TS 23.060, General Packet Radio Service (GPRS); Service description; Stage 2, Release 5, January 2003.
- [10] ANSI/IEEE Std 802.11, "Wireless LAN Medium Access control (MAC) and Physical Specifications," IEEE, 531 pp., 1999 Edition.
- [11] S. Li, C. Tsao, "Enhanced GTP: An Efficient Packet Tunneling Protocol for General Packet Radio Service", ICC 2001, Helsinki, pp. 2819-2823.
- [12] Y. Rekhter, et al., "Address Allocation for Private Intranets", IETF RFC 1918, Feb. 1996.
- [13] D. Plummer, "An Ethernet Address Resolution Protocol", IETF RFC 826, Nov. 1982.
- [14] Info-Communications Development Authority of Singapore, "Trial-Based Study of Next Generation Wireless LAN", Technical Report, Dec. 2002.
- [15] M. Buddhikot, et al., "Design and Implementation of a WLAN/CDMA2000 Interworking Architecture", IEEE Communications Magazine, Dec. 2003.
- [16] M. Buddhikot, et al., "Integration of 802.11 and Third-Generation Wireless Data Networks", IEEE INFOCOM 2003, April 2003.
- [17] M. Kulkarni, A. Patel, K. Leung, "Mobile IPv4 Dynamic Home Agent Assignment", Internet Draft, Jan. 2004.
- [18] S. Varaala, "Mobile IPv4 Traversal Across IPsec Based VPN Gateways", Internet Draft, Sept. 2003.
- [19] D. Katabi, J. Wroclawski, "A Framework for Scalable Global IP Anycast (GIA)", SIGCOMM 2000, Aug. 2000.
- [20] Kara, "Private-to-Private Communications over the Internet", IEEE Computer Magazine, May 2004, Vol. 37, No. 5, pp. 53-59.

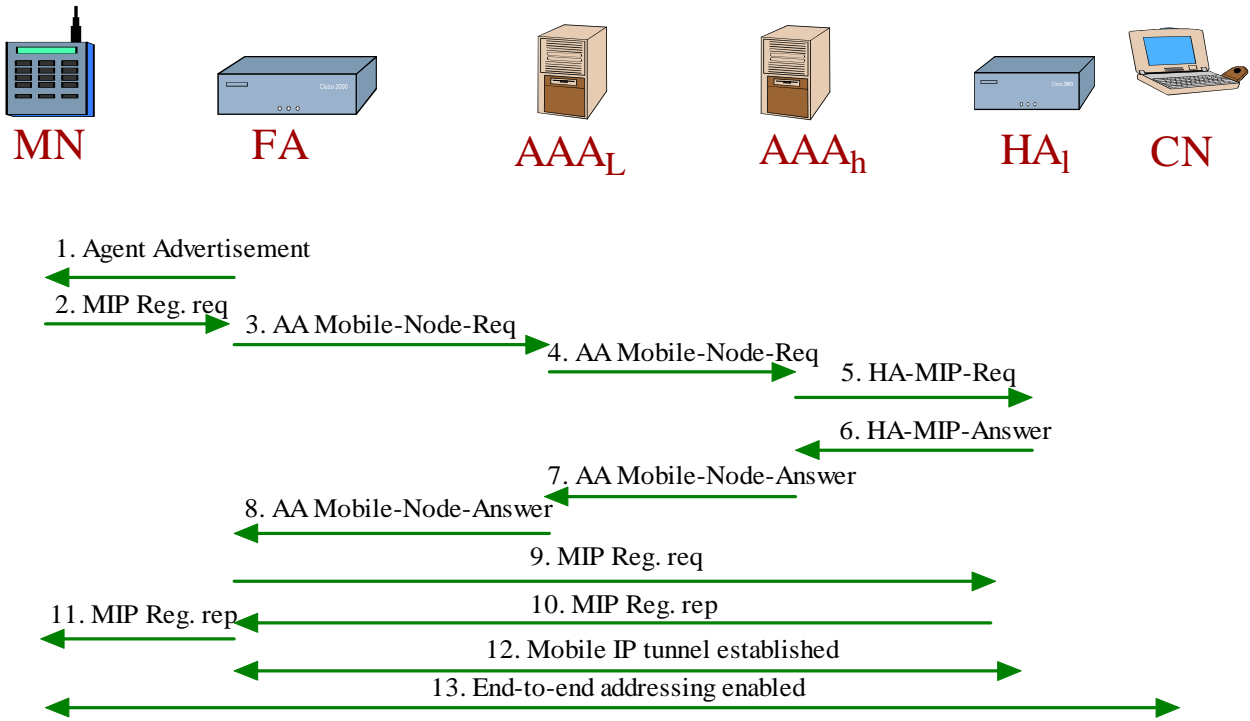


Fig. 8. Dynamic HA Assignment Message Sequence

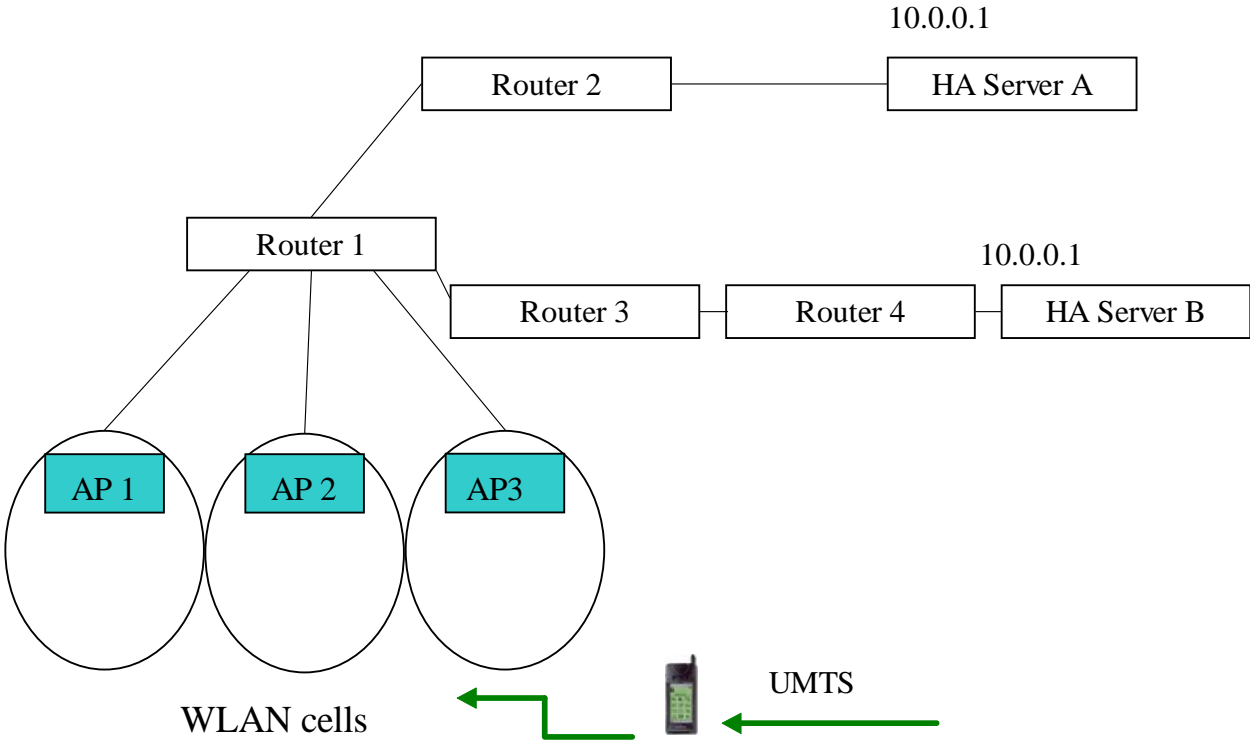


Fig. 9. Dynamic HA Assignment with Anycast Routing

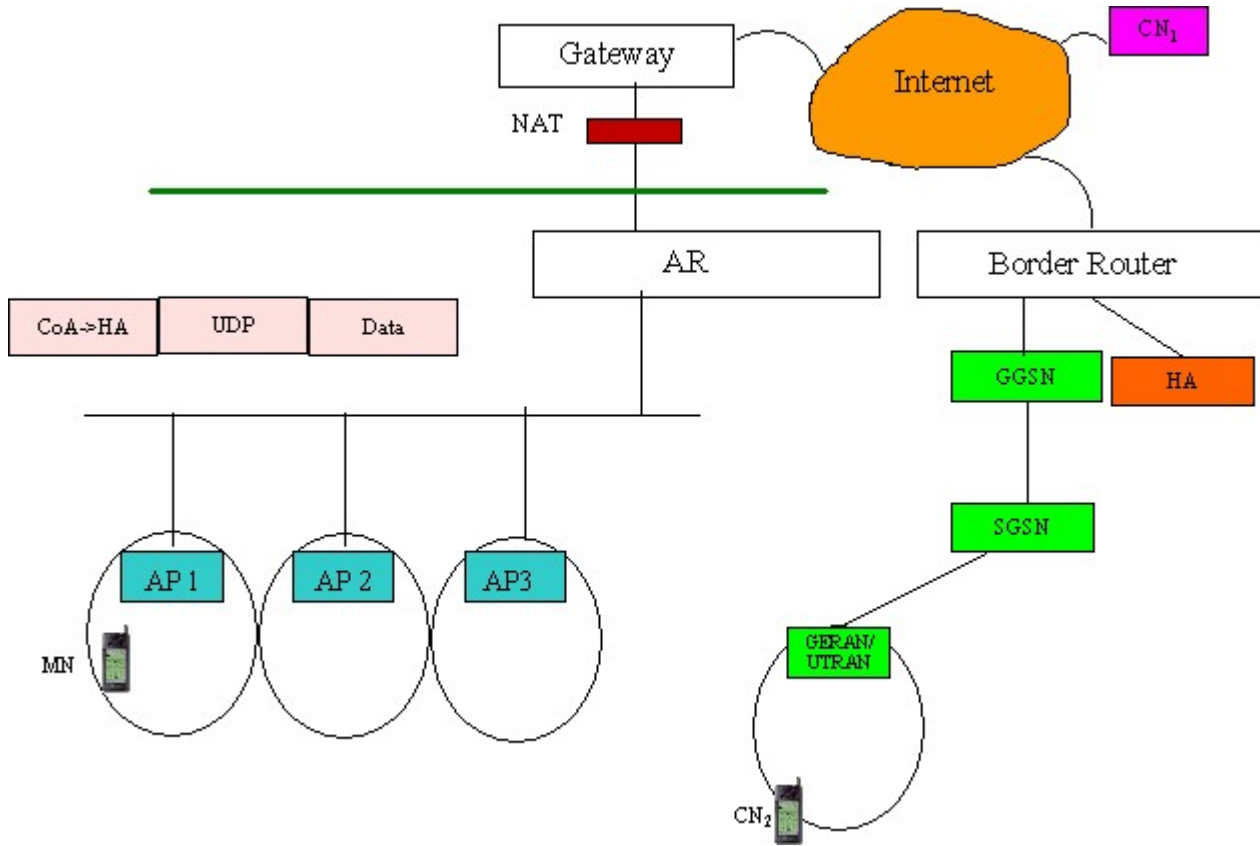


Fig. 10. Private Addressing Architecture 1

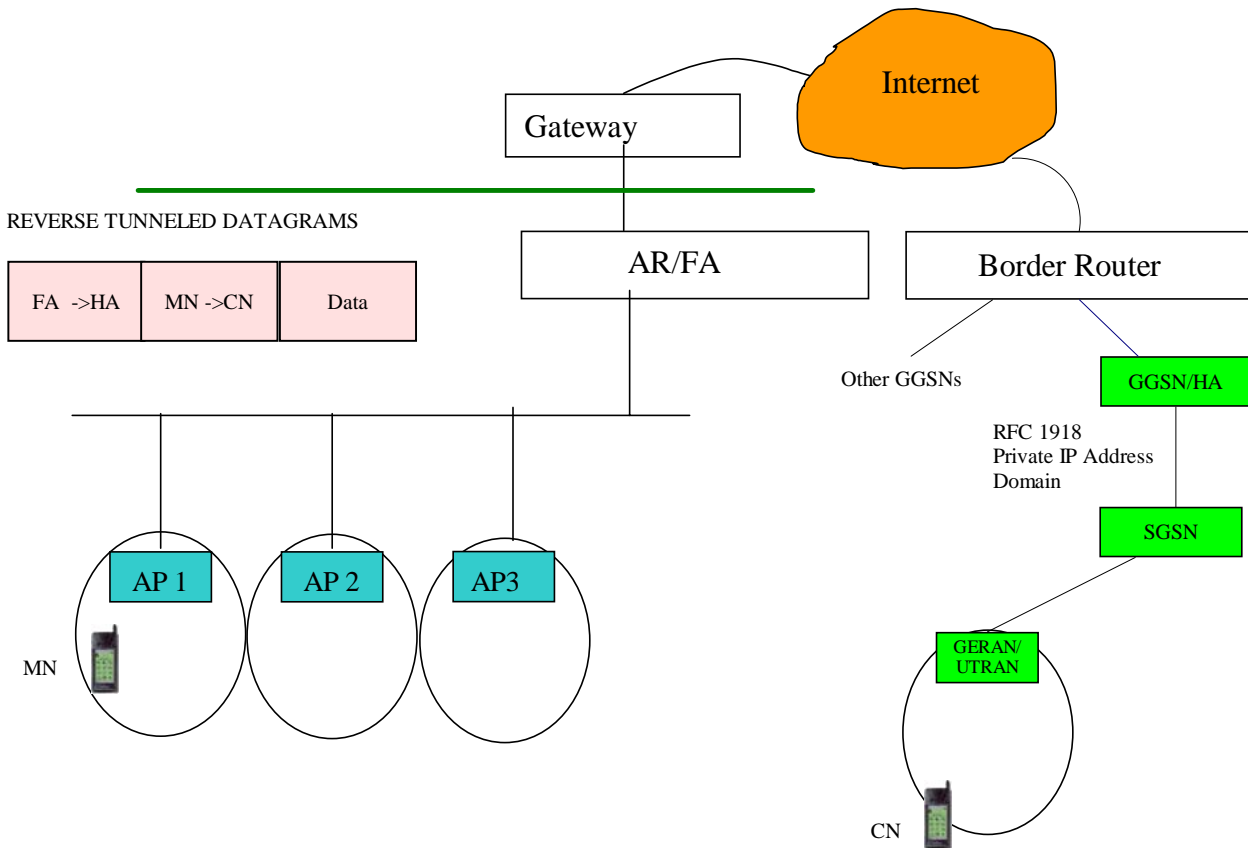


Fig. 11. Private Addressing Architecture 2

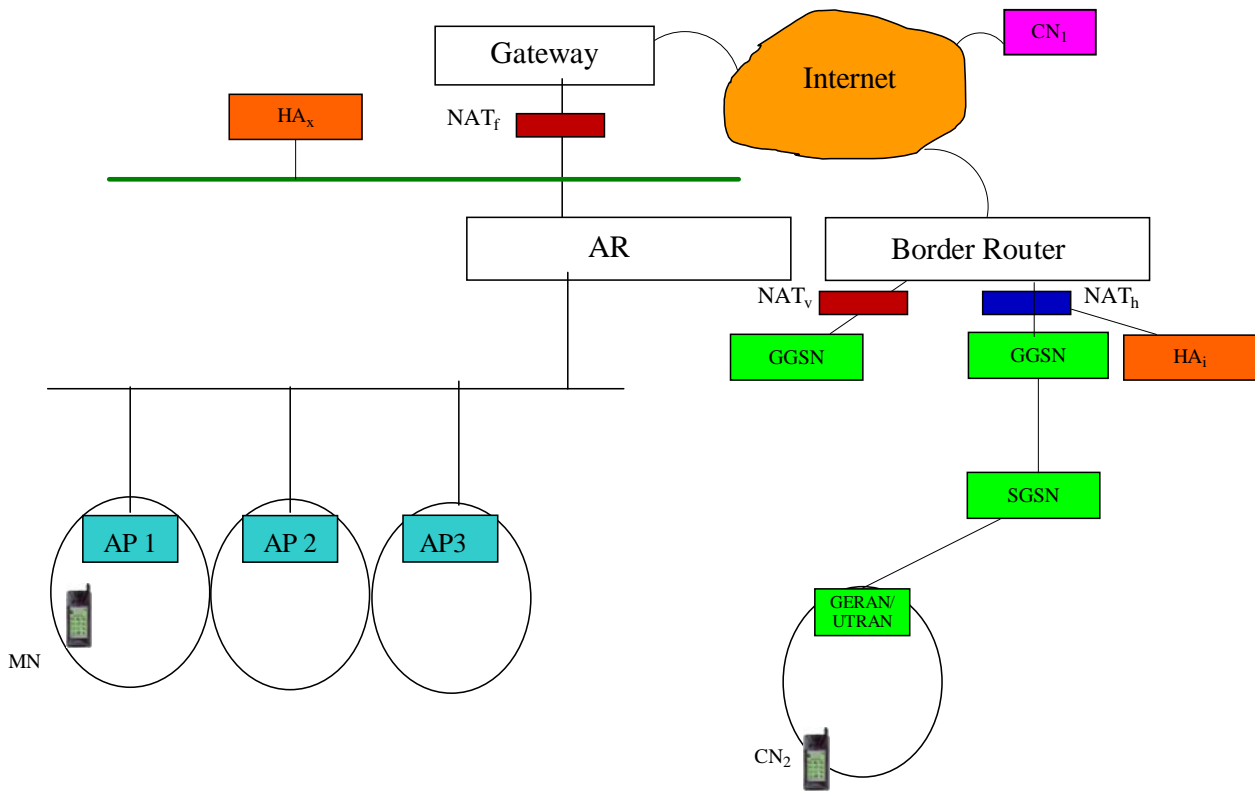


Fig. 12. Private Addressing Architecture 3