

Exploring Multi-homing Issues in Heterogeneous Environments

Glenford Mapp and Mahdi Aiash
School of Engineering
and Information Sciences
Middlesex University,
Hendon, London NW4 4BT
Email: g.mapp, m.aiash@mdx.ac.uk

Hélio Crestana Guardia
Department of Computer Science,
Federal University of San Carlos,
Brazil
Email: helio@dc.ufscar.br

Jon Crowcroft
Computer Laboratory
William Gates Building,
JJ-Thomson Avenue,
Cambridge, UK
Email: jon.crowcroft@cl.cam.ac.uk

Abstract—Mobile devices with two network interfaces (WiFi and 3G) are already commercially available. Point-to-point communications such as Infrared and Bluetooth are also readily used. In the near future, mobile phones will have several interfaces including satellite and new technologies such as Ultrawideband. Hence we must assume that such devices will be multi-homed by default. For various reasons, including network congestion, network resilience and increased endpoint bandwidth, there have been several attempts to address multi-homing. Heterogeneous environments with the need to support vertical handover introduce another set of issues which make the need to solve multi-homing problems more urgent. This paper outlines the issues, looks at past efforts and proposes a solution based on the Location_Id/Node_Id concept but also argues that additional support is needed to make such an approach efficient for heterogeneous environments.

Index Terms—Multi-homing, Heterogeneous Networks, Y-Comm Framework

I. INTRODUCTION

The continuing development and wide-spread deployment of wireless networks such as WiFi, 3G, WiMax and Ultrawideband indicate that devices such as mobile phones will soon have several wireless interfaces and will therefore be multi-homed by default. Such devices, called **hetnet** devices, point to a scenario where continuous communication is maintained by seamlessly switching between available networks using vertical handover techniques. Because vertical handover involves changing the point of attachment (PoA) to a network of a different technology, this that means link, network and transport layers may be affected [1]. At the link layer, new MAC addresses must be used while at the network layer, new network (IP) addresses must be found for the device on the new network. In addition, network infrastructure must route incoming packets and reroute old ones to

the new network address. This may result in changes in the route caches of several routers unless the system can work out that the interfaces are co-located. At the transport level, it is necessary that the transport protocol being used can quickly adapt to the network resources being offered by the new PoA in terms of bandwidth and latency which could be completely different from that of the previous PoA [2]. These observations point to the need to urgently investigate naming, addressing and location issues in order to minimize packet loss and service degradation with regard to vertical handover. This paper attempts to address these issues. It first looks at the problem of multi-homing and the various solutions that were developed. It shows that new and future mobile systems will present even more serious multi-homing problems. It then proposes a solution based on the Location_Id/Node_Id concept and also shows how this approach can be enhanced to give added features such as increased security while ensuring that networking functions such as routing are effectively supported. This effort is done in the context of the Y-Comm architecture [3] which attempts to define a complete framework to build future telecommunication systems. Y-Comm not only deals with vertical handover but also includes issues such as Quality-of-Service (QoS), security, etc. The rest of the paper is structured as follows: Section 2 looks at related work. Section 3 looks at the problems related to issues dealing with vertical handover while Section 4 examines the need to support other mechanisms to make the whole process more efficient. In Section 5, a new address format is outlined and in Section 6, testing and implementation are discussed in the context of the Y-Comm architecture. The paper concludes in Section 7.

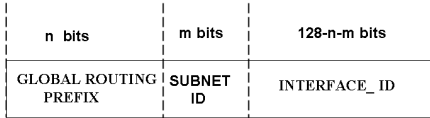


Fig. 1: The General IPv6 Unicast Address

II. RELATED WORK - AN HISTORICAL PERSPECTIVE

When the Internet was young, issues of multi-homing had mainly to do with route optimization due to network congestion and problems associated with link failure in routers. Most end systems only had one network interface and the network address was actually the address of the network interface and not the device itself. The Internet was developed using the TCP/IP Internet Suite and the IPv4 format was used to define network classes by subdividing bits of the IPv4 address. The early Nineties saw the development of IPv6 [4] which was developed to deal with the shortcomings of IPv4, in particular, its growing shortage of addresses. The IPv6 format employs 128-bit addresses but also simplified other aspects of IP packet processing.

The development of IPv6 encouraged new approaches to address some key issues. This is because an IP address attempts to do two things: it is used to identify the network interface to which the packet is sent and it is also used to route packets to the destination. This dual functionality meant that it was difficult to dynamically optimize network routes. A lot of effort related to multi-homing was an attempt to decouple this duality. O'Dell [5] proposed an alternative address format for IPv6 which was based on dynamically changing part of the IPv6 address to allow more effective network management. Though this proposal was not successful, it led to better support for addressing in IPv6 [6]. The IPv6 Global Unicast Address format is given in Figure 1. It consists of a global routing prefix, which usually refers to a domain and a subnet which represents a network within that domain, and an Interface_Id which uniquely identifies the interface so that packets may be routed to it.

Interest in multi-homing on end-devices first came about primarily because of the development of the World Wide Web and hence the need of high-performance servers to have more than one interface to serve global clients. In order to maintain a high throughput it was necessary to be able to switch to another interface when a given network interface was congested or had simply failed. This led to the development of protocols such as the Stream Control Transmission Protocol or SCTP [7] which supported multiple interfaces for each connection.

Client devices with multiple interfaces have recently become commonplace. In the case of wired devices, multiple client interfaces are possible because of the ability of high-performance CPUs to deal with large amounts of data. Such a reality is driving the work on Multipath TCP [8]. In wireless networks, multiple interfaces have been developed to support the need for ubiquitous communication which can be facilitated using efficient vertical handover techniques. Mobile IPv4 [9] and Mobile IPv6 [10] have been invented to deal with handover in Mobile IP networks. These systems use network mechanisms such as Router Advertisements (RAs) and hence can be slow. This led to the development of FMIPv6 [11] which responds to changes in link status to initiate handover.

A. Problems with Multi-homed Mobile Devices

As indicated above, our current work on multi-homing is related to the need to support heterogeneous networking and hence efficient vertical handover. It should be pointed out that the Global Unicast Address is sufficient for horizontal handover where the new point of attachment is of the same technology and hence the same MAC can be used. However, with vertical handover, both the interface and the network address change so that aggravates the multi-homing issue. This means that the networking infrastructure cannot easily collate the new and previous addresses as no part of the address remains fixed after vertical handover. In addition, since there is no relationship between the previous and new addresses, both routes will remain in the route caches of core network routers resulting in sub-optimal network performance since the route cache cannot be effectively maintained.

It should be observed that similar issues will occur when Multipath TCP becomes commonly used as presently there is no way for the networking infrastructure to know that these interfaces are co-located. So that the network infrastructure cannot identify any subflows

of a multipath stream and so cannot optimize the use of core network resources in support of the new mechanism.

III. NODE IDENTIFICATION

A logical approach to this issue is to use a mechanism to identify the node itself. This means that a device can be identified irrespective of the number of interfaces it has. This `Node_Id` operates at the network level and so can be used by the network infrastructure as a unique representation of the end-device. Such an approach has been suggested by several researchers and a number of efforts have been pursued. LINA [12] and LINA6 [13] proposed using a special format to identify a device and there was a mapping mechanism to map LINA addresses to IPv6 addresses. The mapping function took into account the fact that the device was mobile and therefore had location capabilities.

Mapp [14] used an explicit division of the IPv6 address into a Node Identifier and a Location identifier, the `Node_Id` is permanent and is issued by the manufacturer and does not change during the life-time of the object. Transport and higher layers use the `Node_Id` to identify the end-point while the `Location_Id` is managed by the network and lower layers. This presentation also introduced the concept of a **Master locator** which was in the core network and is used to tell corresponding nodes about the networks to which mobile node is currently connected. The corresponding node therefore polls the Master locator to find out the various networks to which the mobile device is currently attached. These ideas are compatible with mobility management mechanisms in commercial mobile networks which use the concept of the Home Location Register (HLR).

Similar efforts eventually led to the development of the 64-bit Global Identifier (EUI-64) [15] which is independent of the `Interface_Id`. These ideas have also been recently pursued in the development of the Identifier Locator Network Protocol or ILNP [16]. ILNP attempts to use DNS facilities to support mobile devices. A related approach is to use cryptographic techniques to identify not just the node but the actual IP stack or Computing Platform. This is called the Host Identify Protocol(HIP) Architecture [17]. A HIP identifier is 128 bits and uses cryptographic techniques which provide authentication and hence increased security. HIP identifiers can be considered more reliable than IP addresses and so can be used by the transport and higher layers to represent the connection.

IV. ADDITIONAL CONCERNS

Though the Location/Node identifier concept is interesting and can be used to support vertical handover, it raises several issues in order to make it operationally viable. These are highlighted below:

- **The effect on the Location_Id part:** Since IPv6 addressing involves the use of an `Interface_Id`, which pertains to a specific network, it is possible to use the other parts of the address to signal different address types such site-only or multicast addresses on the same network. However, since the `Node_Id` and not the `Interface_Id` is being used in this research, the `Location_Id` must represent a real network and there must be a mapping between the `Location_Id` and the `Interface_Id`. This means that other ways must be found to represent multicast addresses as well as scope. This is necessary so that networking performance at the link level can be maintained.
- **The efficiency of routing mechanism:** as indicated above, the Location/Node split may not increase the efficiency of routing especially at ingress and egress routers which must be able to map all the different interfaces to several peripheral networks for each device. Since the route cache in routers is finite, in order to use the cache effectively, it would worthwhile to be given hints about which location identifiers should definitely be cached; i.e., when the device is stationary in the relevant network and conversely when this situation changes, due to mobility and/or handover, so that the relevant route can be quickly removed from the route cache.
- **Security and access:** there is now a growing concern about Denial-of-Service (DoS) attacks on the Internet. Though mechanisms such as Network Address Translation (NAT) can be used to reduce the visibility of end-devices especially client machines, more work is needed to protect servers which can be too exposed. Recently, a new concept called Ring-Based security has been introduced by the Y-Comm group [18]. This is an enhancement of Off by Default! [19]. In Ring-based security, a server operates within a defined scope and only machines within that scope can talk to it. Packets sent from devices outside the scope are detected and destroyed by the network infrastructure. There are 4 scopes being proposed: LOCAL - only processes on the same machine can forward packets through such an interface (so a loopback interface is an example of

an interface that supports LOCAL scope). The next scope level is LAN scope. Only entities with the same network LAN address as the server are able to access the server. The next scope is defined as the DOMAIN scope. Here only devices in the same domain are allowed access to the server. Finally there is a GLOBAL scope in which the server can be globally accessed. We believe it would be beneficial to incorporate scope into the network address so that it can be enforced by network routers and switches.

- **Interfaces matter:** Though the Location/Node identifiers remove the need for an Interface_Id at the network level, being able to use or identify a specific interface is valuable for a number of reasons. Firstly as already pointed out, a server or a server farm may use a number of network interfaces on the same network. In such circumstances, it may be good for diagnostic and performance reasons to know exactly which interface is being used to process a given connection. Secondly, *pseudo interfaces* have proven to be a very popular mechanism to implement a number of additional features. For example, IPSec [20] has been effectively implemented as a pseudo interface. So the ability to specify interfaces would allow such mechanisms to be directly supported. In addition, the concept of anycast addresses can also be supported using this idea. This could also be used to provide more effective support for Multipath TCP as it will be possible for the system to quickly identify which interfaces are being used for a given multipath flow.

- **Support for point-to-point and point-to-multipoint networking:** Though networks such as Ethernet naturally embody the idea of a network address, in point-to-point networks like Bluetooth, such a concept and hence a Location_Id may in fact be superfluous. All that is required is to map an interface identifier to a given MAC address to enable communication.

V. A NEW ADDRESS FORMAT

In order to deal with these issues we are proposing an additional field for network administration. This field is used to qualify the use of the Location and Node Identifiers by the network infrastructure. So we are proposing to change from a **Location_Id/Node_Id** address format to a **Location_Id/NetAdmin/Node_Id** address format. This transition is shown in Figure 2.

We believe the Node_Id can be represented using the EUI-64 format. The 64 bits for the Location_Id is split

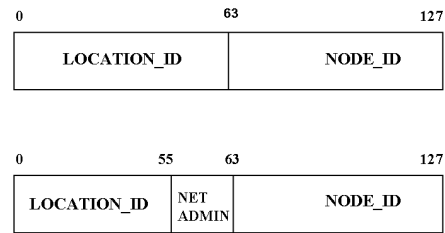


Fig. 2: The New Address Format

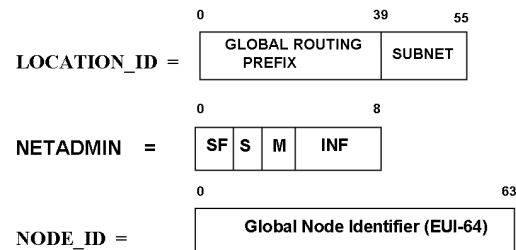


Fig. 3: The NewAdmin Fields

to give 8 bits for the network administration fields and 56 bits for network identification. The NetAdmin field is described as follows:

- The Scope field, or **SF**, is two bits long and is used to indicate the accessible range of incoming requests for this Node_Id. So the value 0,0 denotes that the Node_Id has local scope and can only be contacted via local mechanisms such as the loop-back interface. Any attempt to use a Location_Id which maps to a network interface will generate an error. The value, 0,1, represents LAN scope in which the node is only accessible by other devices on the same LAN. In terms of IPv6 only packets where the src Location_Id represent link addresses will be delivered to this node. The value 1,0 is used to signal that only machines on the same site are allowed to access the server. Thus, again in terms of IPv6 all packets sent to the server must

have a `Location_Id` that indicates that the sender is in the same administrative domain as the server. A value of 1, 1 denotes that the device can be globally accessed.

- The **S** or static bit is used to indicate that the device is stationary in the network given by the `Location_Id`. For wired networks this will be done automatically. However, this bit can also be set for a mobile device if a location system which tracks the mobile node has determined that the mobile device has been at a specific location for some time and is effectively stationary. The setting of this bit can be used by the network infrastructure to put the association between the `Node_Id` and the corresponding `Location_Id` in its route cache. This is extremely useful for network servers which are usually stationary. If the mobile device moves from the stationary location then this bit is unset. This is noted by the routers and so the association is removed from their caches.
- The **M** bit indicates whether the `Node_Id` represents a multicast group. This may be used to deliver data to multiple machines on the same network, or to support global multicast mechanisms. It could also be used for short-range point-to-multipoint communications by directly mapping the interface to a multicast address.
- The Interface number field, or **INF**, is used to indicate which interface is being used for a particular connection and is 4 bits long. A value of 0 means that the packet may be delivered to any one of the available interfaces on a device, while a value of 0xF is used as a broadcast mechanism and so the packet will be delivered to all the available interfaces simultaneously. An INF value of 0x1 tends to signify the primary interface for the device.

A. Implementing this new format on the current IPv6 Networks

The authors believe that little additional work will be needed to implement this new format on the current IPv6 Network Architecture. Many IPv6 networks still use a form of the Aggregatable Global Unicast Address.

In order to implement the new format we suggest a new 3-bit prefix is used to signal that a new IPv6 format is being explored. Support for a 64 EUI Node_Id format is already available and should be used instead of the `Interface_Id`. The `Location_Id` could be similar to the rest of the Aggregatable format with the reserved 8 bits being used for the NetAdmin field. Routers and Gateways will

first read the new prefix and then use the NetAdmin bits and the `Node_Ids` of the source and destination addresses to determine if the packet can be forwarded based on the scope. If the static bit is set, the router looks in the route cache for the route.

VI. NETWORK ADDRESSING FOR FUTURE MOBILE SYSTEMS

A. The Y-Comm Architecture

Y-Comm is an architecture for heterogeneous networking [21]. The architecture consists of two frameworks. The Peripheral Framework deals with issues in peripheral networks while the Core Framework deals with issues in the core network. In this architecture, the Peripheral Framework and the Core Framework are brought together to represent a future telecommunications environment which supports heterogeneous devices, disparate networking technologies, network operators and service providers. The Peripheral Framework runs on the mobile device while the Core Framework is distributed through the network infrastructure. Security in Y-Comm is implemented using an Integrated Multi-layer Security (IMS) module which is closely integrated with the network infrastructure. In addition, Y-Comm uses the concept of targeted security models which is used to protect entities in the network [22].

B. Vertical Handover in Y-Comm

Y-Comm supports a number of different handover types [23], the most complicated of which is called pro-active handover in which a mobile node attempts to determine when and where to handover before the mobile node reaches that point. The parameter called **Time Before Vertical Handover** denoted by TBVH, is calculated [24]. TBVH allows the higher layers of Y-Comm to take evasive action to minimize the effect of performance degradation due to handover.

Since proactive handovers attempt to determine when and where handover should occur, it is necessary to have a knowledge of networks in the local area including their topologies, QoS characteristics and `Location_Ids`. This information along with the direction and speed of the mobile as well as the QoS of on-going connections is used by the Policy Management Layer (PML) to determine where and when handover should occur. The PML calculates TBVH - the period after which handover will occur. This information is communicated to the Vertical Handover Layer which immediately requests resources to do a handover.

Once the PML decides to handover, the new IP address, the new QoS as well as TBVH are communicated to the upper layers. Given TBVH, the upper layers are expected to take the necessary steps to avoid any packet loss, latency or slow adaptation. For example, it may be possible for the End-Transport Layer to signal an impending change in the QoS on current transport connections and to begin to buffer packets ahead of the handover. After handover, the previous channel used by the mobile node is released. The new IP address is obtained using auto-configuration by combining the Location_Id of the new network with the Node_Id of the device. The *NetAdmin* bits of the new address may also change. If vertical handover has occurred as opposed to horizontal handover then the value of the **INF** will change. If the new network is a wired network, then the Static bit will also be set.

C. Current Work

Work has begun at the Computer Laboratory, University of Cambridge on developing a Y-Comm Testbed which will be used to test vertical handover using the new address format as proposed in this paper. The testbed will first develop the lower layers of the Y-Comm architecture in a Linux based environment. Management layers will be implemented in a single user process. This will allow us to test different types of handovers. To build a small Core Network, Linux routers, each supporting two or more wireless interfaces, will be developed.

VII. CONCLUDING REMARKS

In this paper, we have explored a network address format to support heterogeneous environments. This work enhances the location/node identifier concept by using an extra field to provide a number of key mechanisms. This new format will be tested on a Y-Comm testbed which is currently being built.

REFERENCES

- [1] P. Vidales, L. Patanapongpibul, G. Mapp, and A. Hopper, "Experiences with Heterogeneous Wireless Networks - Unveiling the Challenges," in *Proceedings of Second International Working Conference on Performance Modeling and Evaluation of Heterogeneous Networks*, July 2004.
- [2] D. Cottingham and P. Vidales, "Is Latency the Real Enemy in Next Generation Networks?" in *Proceedings of First International Workshop on Convergence of Heterogeneous Wireless Networks*, July 2005.
- [3] G. Mapp, F. Shaikh, J. Crowcroft, D. Cottingham, and J. Baliosian, "Y-Comm: A Global Architecture for Heterogeneous Networking (Invited Paper)," in *3rd Annual International Wireless Internet Conference (WICON)*, October 2007.
- [4] S. Deering and R. Hinden, "RFC 2460," in *RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification*. IETF, December 1998.
- [5] O. M., "GSE - An Alternative Addressing Architecture for IPv6," 2007 February, internet Draft.
- [6] R. Hinden and S. Deering, *RFC 4291 IP Version 6 Addressing Architecture*, IETF, February 2006.
- [7] Stream, *RFC 4960 - Stream Control Transmission Protocol*, IETF, September 2007.
- [8] D. Wischik, M. Handley, and M. B. Braun, "The resource pooling principle," *ACM Computer Communications Review*, vol. 38, no. 5, pp. 47–52, 2008.
- [9] C. Perkins, "RFC 3344," in *RFC 3344 - IP Mobility Support for IPv4*. IETF, August 2002.
- [10] D. Johnson, C. Perkins, and J. Arkko, *RFC 3775 - Mobility Support in IPv6*, IETF, June 2004.
- [11] R. Koodli, *RFC 4068 - Fast Handovers for Mobile IPv6*, IETF, July 2005.
- [12] I. Ishiyama, K. Uehara, H. Esaki, and F. Teraoka, "LINA: A New Approach to Mobility in Wide Area Networks," *IEICE Trans. Commun.*, vol. E84-B, no. 8, August 2001.
- [13] M. Kunishi, M. Ishiyama, K. Uehara, H. Esaki, and F. Teraoka, "LIN6: A New Approach to Mobility Support in IPv6," in *Proceedings of the International Symposium on Wireless Personal Multimedia Communication*, 2006.
- [14] G. Mapp, "Is IPv6 the key to a Global Network Infrastructure," in *IPv4 to IPv6 Migration Conference*, September 2001.
- [15] I. S. Association, "Guidelines for 64-bit Global Identifier (EUI-64)," 2007 IEEE.
- [16] A. R., "ILNP Concept of Operation," 2008 June, internet Draft.
- [17] R. Moskowitz and P. Nikander, "Host Identity Protocol Architecture," January 2005, internet Draft.
- [18] G. Mapp, M. Aiash, A. Lasebae, and R. Phan, "Security Models for Heterogeneous Networking," in *International Conference on Security and Cryptography (SECURITY 2010) Athens, Greece*, July 2010.
- [19] H. Ballani, Y. Cathwate, S. Ratnasamy, T. Roscoe, and S. Shenker, "Off by Default," in *Proceedings of the Fourth Workshop on Hot Topics in Networking (HotNets-II)*, November 2005.
- [20] N. Doraswamy and D. Harkins, "IPSec: The New Security Standard for the Internet, Intranets and Virtual Private Networks," in *Prentice Hall Security Series*. Prentice Hall, 2003.
- [21] G. Mapp, D. Cottingham, F. Shaikh, P. Vidales, L. Patanapongpibul, J. Baliosian, and J. Crowcroft, "An Architectural Framework for Heterogeneous Networking," in *Proceedings of the International Conference on Wireless Information Networks and Systems (WINSYS 2006)*, August 2006, pp. 5–10.
- [22] M. Aiash, G. Mapp, A. Lasebae, and R. Phan, "Providing Security in 4G Systems: Unveiling the Challenges," in *Proceedings of the Sixth Advanced International Conference in Telecommunications, (AICT 2010), Barcelona, Spain*, May 2010.
- [23] G. Mapp, F. Shaikh, M. Aiash, R. Vanni, M. Augusto, and E. Moreira, "Exploring Efficient Imperative Handover Mechanisms for Heterogeneous Networks," in *Proceedings of the International Symposium of Emerging Ubiquitous and Persuasive Systems, Indianapolis, USA*, August 2009.
- [24] F. Shaikh, G. Mapp, and A. Lasebae, "Proactive Policy Management using TBVH Mechanism in Heterogeneous Networks," in *Proceedings of the International Conference and Exhibition on NEXT GENERATION MOBILE APPLICATIONS, SERVICES and TECHNOLOGIES (NGMAST'07)*, September 2007.