Enterprise Mobility

Samita Chakrabarti
Erik Nordmark
Danny Cohen

Enterprise Mobility

Samita Chakrabarti, Erik Nordmark, and Danny Cohen

SMLI TR-2006-158 June 2006

Abstract:

With the proliferation of Wireless technologies and business globalization, mobility of people and devices have become inevitable.The experience of mobile computing in different campuses or drop-in offices also faces challenges of starting up applications and tools, synchronizing filesystems, maintaining one's desktop environment or even finding a printer location or network services. In this document, we will discuss different types of mobility, issues with mobility, and why it is important to consider the mobility issues. Finally this document discusses a network layer solution for IP mobility for continuous connectivity. It also sheds light on future directions of research on mobility that might be interesting for Sun Microsystems.

Sun Labs
16 Network Circle
Menlo Park, CA 94025

email addresses:
samitac2@gmail.com
erik.nordmark@sun.com
danny.cohen@sun.com

© 2006 Sun Microsystems, Inc. All rights reserved. The SML Technical Report Series is published by Sun Microsystems Laboratories, of Sun Microsystems, Inc. Printed in U.S.A.

Unlimited copying without fee is permitted provided that the copies are not made nor distributed for direct commercial advantage, and credit to the source is given. Otherwise, no part of this work covered by copyright hereon may be reproduced in any form or by any means graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an information retrieval system, without the prior written permission of the copyright owner.

TRADEMARKS
Sun, Sun Microsystems, the Sun logo, Java, Java Card, Sun Linux, Sun Ray, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc. UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

For information regarding the SML Technical Report Series, contact Jeanie Treichel, Editor-in-Chief <jeanie.treichel@sun.com>.All technical reports are available online on our website, http://research.sun.com/techrep/.

Enterprise Mobility

Samita Chakrabarti
Erik Nordmark
Danny Cohen

1.0 Introduction

With the proliferation of wireless technologies and business globalization, mobility of people and devices are inevitable. Although in most cases, corporate employees are able to access the corporate network through Virtual Private Networks (VPN), the experience of accessing data and running applications from outside the office campus is much different than that in the office environment. The experience of mobile computing in a different campus or drop-in offices also faces challenges of starting up applications and tools, synchronizing filesystems, maintaining one's desktop environment or even finding a printer location or network services. On the other hand, Voice-over-IP and streaming media over the Internet Protocol are gaining momentum; many corporations are moving towards Voice-over-IP solutions where the calling or receiving a device could be an IP-phone or a PDA or a soft-phone running on a laptop. However, in today's Internet topology the IP-address changes when the subnet changes; a connection-oriented application which relies on the end-point IP-addresses will stop working when the IP-address changes, and in some cases of mobility, a subnet change is inevitable. In this document, we will discuss different types of mobility, issues with mobility and the importance of such issues. The scope of this document does not allow to specify a particular solution. However, it discusses several options and possible solutions. It also analyzes different mobility scenarios. The document also indicates areas of gaps which can be subject to further investigation and research; it concludes with analysis of possible applications of mobility and their requirements.

The discussion in this document is focused on Enterprise Mobility which includes movement inside the campus, between local and remote campuses of an Enterprise. Thus sometimes we also discuss connectivity to the Corporate network while one is in transit across different campuses geographically; thus mobility in the Internet is also discussed in this context. Our exploration project on Campus or Enterprise mobility mainly focused on the device mobility, although we had also explored user mobility to some extent.

The document is structured as follows. Section 2 discusses different types of mobility and their characteristics, section 3 describes requirements for mobility computing. Section 4 briefly discusses the operator role in mobility. The possible solutions and our exploration discussions take place in section 5. The conclusion provides a table for basic requirements of mobility implementations for different types of usages.

2.0 Types and Characteristics of Mobility

There are different kinds of mobility based on its characteristics and application usage. In this section we will state the different mobility types and their characteristics.

Types	***Sub-types***	***Characteristics***
User Mobility		A user is moving between fixed devices such as non-portable computers. It is possible that the user is moving from one office to another office or one campus to another
	Personal Mobility	It is a sub-type of user mobility. It may indicate user's preference on frequency of movement – based on the fact that the user may be able to receive different services from servers in the network which cater to mobile users.
	Session Mobility	It mostly applies to user mobility when user moves from one fixed device to another but wants to maintain the existing session (Example: Sun Ray™)
	Personalized Mobility	It is also a sub-type of user mobility. It defines personalization of operating environment when a user moves from one device to another
Device Mobility		User carries the computing device from one place to another
	Nomadic Mobility	It is a variation of device mobility. Users are able to access the network when it is available (i.e., office, hotels, airport etc.). The device is disconnected from the network when a network is not accessible or when users choose to stay off-line.
	Continuous Mobility	It is a variation of device mobility. In this case, a device or a user remains continuously connected or reachable from the other end-point.
Application Mobility		Mobility of applications from one device to another when the user decides to switch to a device of different capabilities while maintaining the state of an application

Discussions

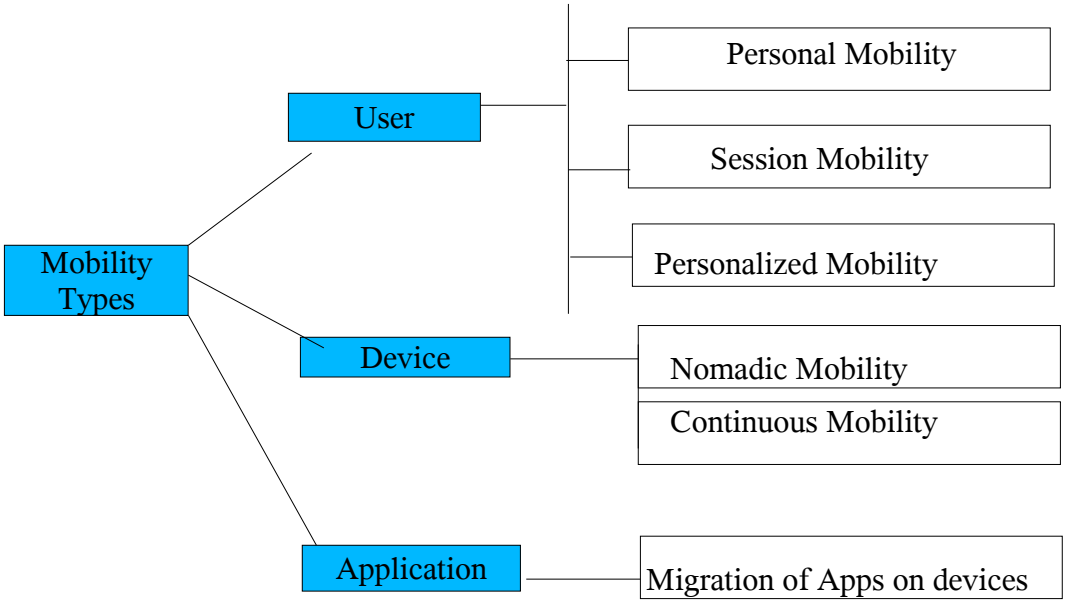


Fig 1. Types of Mobility

Above, we have described different types of mobility and their characteristics. In general, **user mobility** means that the user is moving from a fixed terminal to another fixed terminal. For example, a Corporate employee logs on to a Sun Ray terminal and then moves to a different location followed by logging on to a different Sun Ray terminal. Since Sun Ray user's session is actually run on the Sun Ray server, the user movement does not break the user session as long as the user is in the same server domain. Thus, in the above example of *session mobility*, the user will get back his/her running session at the new terminal. A *personalized mobility* may be achieved by directly taking user's input; for example, taking input or collecting data about the user's intent of stay in a particular location and making some decision based on the pattern of user mobility and usage of resources. This may include the use of different types of access media and frequency of movement of the user across those different access mediums. An access medium has a particular capability of speed, maximum packet size (MTU) etc. These characteristics can determine choices of applications to be run or continued when the user moves from one location to another and consequently changes the access medium. A *personalized mobility* is also an awareness of applications for user-mobility. A user may move from a low-capability device (e.g., PDA with a very small screen) to a regular terminal; the applications and user environment should be smart enough to figure out user's terminal capability and adjust automatically. The examples for personalized mobility may also include knowledge of a user's present location and thus automatic configuration of local printer, local-file server for file updates along with automatic

synchronization of data from time to time with user's home file server, and local network servers (such as web proxy server, network access server, agent services). Applications that support *personalized mobility* service may provide local information, such as emergency phone numbers, restaurant information etc., based on the user's profile and depending on the geographic location of the user. This type of personalized service information could be updated automatically as the user moves from one location to another. The personalized services can also be triggered by the device mobility upon detection of movement from one geographic location to another. However, it requires a special software to map the IP address to a geographic location, though the mapping is not always straight forward due to privacy restrictions on the topological information.

Device mobility is described in two parts – *nomadic mobility* and *continuous mobility*. *Nomadic mobility* is often an example of connecting the device when network is available and starting the applications or simply reconnecting to the new network. Checking email, VPN access, web-browsing at the airport before taking off, then turning off the computing device, and then working off-line on the plane; turning off and again re-connecting the device to the network at the destination is an ideal example of *nomadic mobility*. In the case of *nomadic mobility* , a new connection needs to be made every time the device is connected to the new network. *Continuous mobility*, on the other hand preserves the end-to-end network connection while the user's device changes across different access networks and subnets. C*ontinuous mobility* enables users to continue network applications even when the users move from one building to another or one network to another. If we think about Internet services and applications, Voice-over-IP, streaming video over the Internet, *continuous mobility* is required to keep data flow intact in the middle of network (wireless LAN to GPRS or 3G) and subnet (IP address changes when subnetwork or network changes) changes.

Application mobility can be viewed as migration of application from one network connected device to another. For example, a user starts some network applications at the airport in a handheld device and uses *continuous mobility* to keep the connection alive while in the car, but after arriving home the user wants to move the application to the regular workstation with a monitor while keeping the application states intact. This is deemed to be an interesting research area; a possible solution to this problem can be achieved by applying principles of session mobility and personal mobility where the application state is always maintained at a server which keeps track of the application state and user's terminal capabilities. Another possible solution is process migration over the network and running Java™ isolates [JSR 121]. This is, however, a possible research area to investigate.

Our laboratory exploration on enterprise mobility is mainly based on device mobility using network layer Mobile IPv6 [RFC3775] solution. Thus the discussions on the following sections will touch more on the Mobile IPv6 [RFC3775] device mobility aspect than the user mobility or application mobility areas.

3.0 Requirements for Mobility Computing

Mobility computing has its own challenges due to its nature of computing in new

networks and environments and outside the user Corporate or home ISP network. Although this document's main focus is enterprise mobility, this section may touch upon mobility requirements in general in the industry.

Security

This section discusses security concerns for mobile users, devices in the Corporate environment and on the Internet. Part of the discussion also includes wireless LAN security as an unsecured wireless LAN is an easy way to grant access to the attacker.

There are inherent threats with mobility computing both inside the campus and outside the campus for accessing Corporate information. The threat can arise from both servers and mobile device users. Threat can occur from gaining access to the Corporate network, and then from a fake user trying to act as a Corporate mobile user. On the other hand, a bad guy who has gained access to the Corporate network through wired or wireless network can advertise false mobility services in the network; without proper authentication and security, mobile users' sensitive data can be compromised. The following types of threats are believed to be the common cases that a mobility solution should address – MITM (Man In The Middle), Replay and Reflection attacks. All the above attacks can take place inside the Corporate network if it is not properly secure. Needless to say, these attacks are highly probable in the open Internet. In MITM attack, a rogue device can sit in the visiting mobile node's network and watch the network activity; it can then inject some packet with false IP-address impersonating the peer device of the mobile device and can cause disruption of service or redirection of data to a different unwanted route. It can also simply snoop the sensitive data and stay invisible to the mobile user. A typical scenario with **man-in-the-middle (MITM) attack** is:

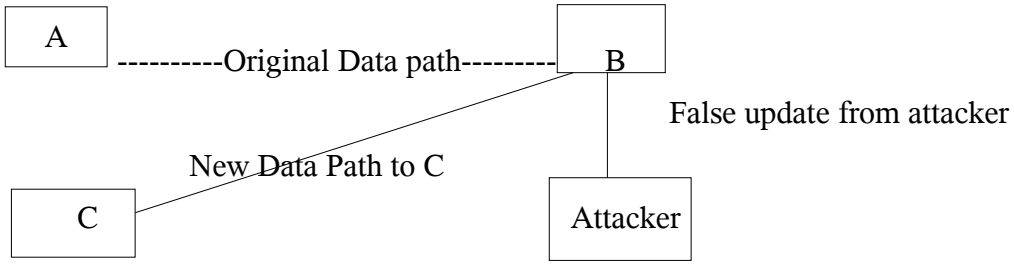


Figure 2: A man-in-the-middle attack scenario

C gets data from B that is meant for A. Attacker acts as man-in-the-middle attack and sends false update to B, as if A has moved to a new location C.

When a device moves from one location to another, it needs to send an update about its new location to the proxy-server which acts as a home-server to redirect data to the new location. Sometimes, the mobile device sends such a movement update to another node directly. In all cases, the receiver node of the movement update needs to make sure that it is not a false indication or not from a false mobile-device.

Any protocol for authenticating a movement update has to consider **replay attacks**. That

is, an attacker may be able to replay recent authenticated movement updates to the correspondent and, that way, direct packets to the mobile node's previous location. Like spoofed movement updates, this could be used both for capturing packets and for Denial-Of-Service attack. The attacker could capture the packets and impersonate the mobile node if it reserved the mobile's previous address after the mobile node has moved away and then replayed the previous movement update to redirect packets back to the previous location.

In a related attack, the attacker blocks movement updates from the mobile at its new location, e.g., by jamming the radio link or by mounting a flooding attack, and takes over its connections at the old location. The attacker will be able to capture the packets sent to the mobile and to impersonate the mobile until the correspondent's cache entry for the mobile node expires.

In **flooding attack** the attacker knows that a heavy stream of data is flowing between a mobile node and another node. It then sends a movement update to the sender about B's new address which happens to be another fixed or mobile node on the network, thus redirecting the heavy data stream to another node in the network.

In order to avoid these problems, an authentication and authorization between two communicating mobile nodes or a mobile node and fixed node is necessary before providing the mobility service to the mobile user.

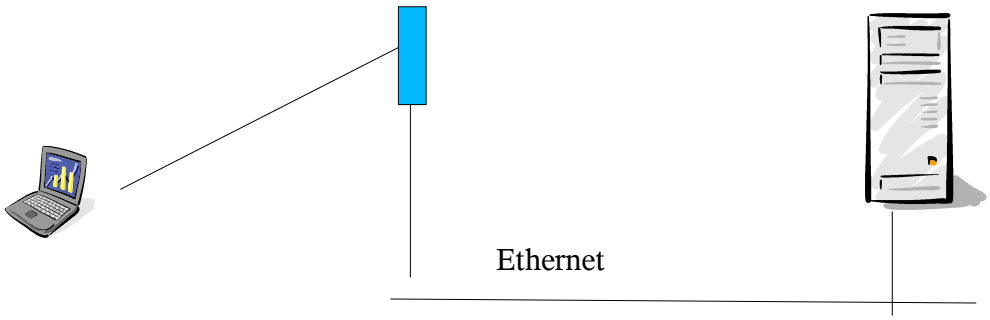
Authentication and **authorization** are necessary for all types of mobility. For example, a user moves from one thin client to another (Sun Ray) from home to office to the airport. In order for users to access the sessions, they need to authenticate the validity of the user and then be authorized to perform the operation. Authorization can occur following the authentication process; authorization can detect if the user privileges are sufficient. In enterprise or Corporate environment, accessing certain applications, systems, files etc. might be privilege-based depending upon the role of the user. In the case of Internet service provider or VoIP service provider, it is necessary to check if the customers have privileges for the type of service they are requesting – it could be the bandwidth of the internet service, or other type of services as per user's service agreement. Thus for authorization, policies are enforced at the content servers and the mobility servers. A policy can dictate user privileges ranging from type of mobility service (plain or route-optimized or 3G), security policies, data services, voice services or ability to access certain files or sites etc. Similarly, the mobile client also needs to set its policies according to the service provider it uses – it may include bootstrapping protocol choices, authentication methods, choice of servers and ISPs (Internet Service Providers) at different situations. In the future, digital rights management (DRM) also needs to be incorporated into the secure mobility mechanism. For example, a user moves from one ISP network to another while continuing to view a video-clip or listening to voice-content. In this case, the mobile client needs to be intelligent enough to figure out its new link characteristics to adjust the content application; in addition, if the digital rights were given to the user@homeisp.com, then the mobile client needs to be smart enough not to start route-optimized service which does not tunnel its data packet through the home server. If the user moves far away from its home server's geographical region and chooses a different home-server at the new location (perhaps in the realm of a different ISP which has agreement with its home ISP), then there must be some way to identify the

user@homeisp.com at the new location as user@newisp.com for the purpose of authentication of digital rights.

Today, in the industry RADIUS [RFC2865, RFC2866] is the most common authentication mechanism as an authentication, authorization and accounting (AAA) method. RADIUS has problems with accurate billing during packet loss and the original proposal had weak security mechanism; the latter was fixed in RADIUS extension [RFC2869] by using EAP [RFC2884] encapsulation in RADIUS protocol. RADIUS is used to provide access to the local network, network services such as Mobile IP or 3G data services. In spite of its problem of detecting packet loss, RADIUS is useful for switching access provider while roaming. IETF (http://www.ietf.org) ROAMOPS workgroup has worked on proposals for roaming across access providers.

Several other authentication mechanism such as Sun's Java Card™, username/password, or challenge authentication using token card can be used for initial user level authentication before opening a mobility service. In the 'Possible Solutions' section we will discuss user access scenarios in detail. In today's nomadic and user mobility environment, token card, username/password are used to gain access to the Corporate network or access user's account through the web.

Wireless Networks have become very common in Enterprise and public places such as airport, shops, hotels etc. This paragraph discusses the common practices for security and mobility in the wireless networks. IEEE802.11 security offers WEP(Wired Equivalent Privacy) which is vulnerable to easy attacks by the hackers who can compute the encryption key. IEEE 802.1X is a port authentication security protocol which is used for wired and wireless networks for initial authentication for network access and derivation of encryption key. In a wireless network,



<---EAP Over Wireless---> [AP]<---------RADIUS Messages --------->[Radius Server]

Figure 3 : 802.1X WLAN Security

IEEE 802.1X is generally used in conjunction with EAP methods and a RADIUS server. The access point (AP) and the client device need to be able to process the EAP [RFC 2884] messages; usually access point is associated with a RADIUS server which processes the encapsulated EAP messages and verifies the authentication of the user or device and sends a response back to the access point. Upon successful authentication, the

access point allows the requester to access the network by accepting and forwarding packets from/to the requester. When a user and the corresponding mobile wireless device moves in IEEE 802.1X protected wireless LAN, the device needs to re-authenticate itself as it joins the new network. By using a backend server like RADIUS server (or LDAP), the device security information can be obtained and processed from any WLAN network access point. With change in WLAN networks, it is likely that the device gets a new IP-address. Although HTTP protocols work transparently over IP-address change, many other applications that depend on TCP connection-based protocol stop working. In order to solve the problem for continuous mobility, either the application, or the Network layer or the link-layer needs to take care of keeping the connection alive in spite of the address change. The mobility solution at the network layer is called Mobile IP [RFC3220, RFC3775] which uses tunneling mechanism between the mobile device and its home mobility server. The datalink layer (L2) solution can be done by L2 tunneling at the access points or by using dynamic VLANs. However, the L2 solution does not work across different access media, but a Network Layer (L3) solution can be transparent across movement from cellular (3G or GPRS) to Wireless LAN. In case of a L3 solution, such Mobile IPv6 [RFC3775], there is additional security for the service. IPsec is used for securing the tunnel between the mobile device and the Home server. IETF is working on a secure bootstrapping protocol for Mobile IPv6 service [BootStrap] and another optional security protocol for Mobile IPv6 mainly for 3GPP2 usage of the technology in their existing architecture for mobile wireless data services. Thus it is important to obtain authentication security at the link-layer and network layer, while service authentication and authorization can be implemented at the higher level of protocol layers.

Performance

Performance in the mobility environment means applications, access or routing performances, although all types of performance are measured by user experience. In the case of user mobility or session mobility, it is important to get back to the user's environment prior to the movement as seamlessly as possible. It also means how efficiently the user can access the home file-systems remotely or access the running applications that were started before the movement. In the case of device mobility, there is a delay in getting the device configured into the new network, plus the delay due to any mobility hand-off, if applicable. In a wireless LAN environment, there are three reasons for performance delay 1) receiving a beacon; 2) security association at the link-layer, if applicable; and 3) association and re-association delay with the access point. When IP-address of the device changes and/or the link-layer access media changes, mobility hand-off delay needs to be considered for performance measurement (in case of continuous mobility such as Voice-over-IP clients). Both mobility hand-off and link-layer hand-off delays can be reduced by pre-authentication and pre-configuration of the network by using pro-active algorithms. IETF is working on solutions for hand-off performance in the MIPSHOP working group.

Besides the network association, there may be some delay associated in routing path between the corresponding node and the mobile node when the mobile node is away from home network. In this case the packets from the corresponding node have to travel via the home network. This can cause delay in a situation where home network is located far apart geographically from the mobile-node's current roaming location; it may mean that

there are more hops between the new location of mobile-node and the corresponding node or there is a slow link somewhere in the new path. In such a situation, one can make use of Mobile IPv6 Route Optimization algorithm [RFC3775] which allows direct communication of the correspondent node with the mobile node without always going through the home network. In order to achieve continuous data transmission amidst changing networks, the goal is to keep the delay within 100ms or less.

Quality Of Service

Quality of service (QoS) mostly implies the quality of network bandwidth that the user has signed up for. Quality of service may provide different bandwidth to a user for different applications instead of providing flat bandwidth for data, voice and video. For example, an ISP offering triple play (voice, video and data) may provide higher data rate for video and lower data rate for voice and data. However, the question is if the user has signed up for M bit/sec data rate with ISP X, then should the user expect to receive the same data rate while roaming on the same type of link? The answer encompasses the policy aspect of the business model as well. When a user or device moves from home network to another public network (hotel, airport, coffee shops, etc.) and its access network provider changes, the user should expect the same level of data rate only when its home ISP has service level agreement with the roaming ISP, such that the new access network checks the authentication of the user and then verifies the authorization of the user's service. The authorization part can dictate the user's approved data rate and its conditions. RSVP (Resource Reservation Protocol) and Diffserv are used in the Internet for handling QoS. But these protocols are developed for static network and one or the other does not work quite well in case of mobility. There is ongoing work at IETF and the Industry to handle mobility and QoS efficiently. Many suggest a combination of both RSVP and Diffserv for mobility. In this model, RSVP is performed end-to-end and enforced only at the edge networks at the both points. Thus RSVP is not enforced in the Internet or middle network where the access networks do not have any control over the routers. Hence the routers in the middle use Diffserv for best effort provisioning as requested by the access network. During handover, it is possible that the user does not receive the same QoS bits immediately; there is a ramp-up time between what the default QoS is in the access network and the negotiated QoS at the end of the hand-off procedure. The above description on QoS handling assumes that the mobility management takes place at the network layer or above.

Movement Detection

For nomadic mobility, when the device is not powered off as it is moved, the device needs to be able to detect when its movement creates a need to reconfigure network parameters such as its IP address and default router(s).

This capability is even more critical for continuous mobility, where the device needs to quickly determine whether it can keep its current network parameters, or needs to acquire a new IP address, etc. If it acquires a new IP address, it then needs to quickly send an update about its new location (IP address) to its Home Agent. Thus the performance requirement for movement detection is quite high in the case of continuous mobility.

We refer to the general notion of verifying whether the device is still attached to the same subnet and acquiring new IP configuration parameters in a new subnet, as Detecting Network Attachment (DNA). The mechanisms for this is being standardized in the IETF as this is written. [RFC4135, DNAv4, DNAv6].

Tolerance of Heterogeneity

Movement of user from one Corporate location to another, or one large system to a small system causes changes in the user experiences. For example, working on a small device like a PDA restricts the screen size and fonts; when a user moves from a small Sun Ray system to a workstation, the user should be able to read with larger fonts in a larger screen. Mobility-aware applications should be smart enough to figure out the user's preference in different devices and should be able to set the environment accordingly. This can include turning on speech-to-text recognition or auto turn-on feature of sound, and video capabilities. This type of services can be characterized as device-aware services.

Similarly, there is a need for location-aware services. Location-aware service is useful for providing the user the same type of service while roaming: it includes carry-forward of the user's environment to the new location when the user moves but the device does not.

Ease of Configuration

Mobility in Enterprise environments is quite common, yet we often face the problem of finding a printer, finding DNS servers and network parameters (IP address, default routers). Running DHCP is often a solution for mobility in order to transparently configure network parameters and DNS server addresses. This document states the following goals for ease of configuration in a mobile environment:

- Auto-configuration of network parameters (IP address, default routers, etc.) and network services such as DNS servers, NFS servers, printers, etc.
- Auto-configuration of other network services specific to the mobility aware applications
- Auto-access to the secure Corporate local area network or other secure ISP network by using a common standard access mechanism with pre-shared information or certificate mechanism for authentication
- Auto-detection of change of quality of access medium, such that the system can determine when to ask the user to start or stop certain applications depending on the throughput of the link. For example, a video application may warn user that it does not have enough bandwidth to perform at the start time. Similarly, other applications may intelligently inform the user that it would be using a changed throughput for the application. A mail client may intelligently make the decision to not attempt to open a large attachment remotely.

4.0 Operator Services

In order to envision mobility, this document depicts a few possible scenarios for operator services. The Operator services could be cellular or Wireless LAN or Cable Operators.

The document assumes that the mobility management is handled at the network layer and above, thus inter-technology hand-off is not part of the discussion.

ISP is the mobility service provider: This is the simplest scenario where the access and mobility service is offered by the same service provider and operator.

Separate Network Access Provider and Service Provider: User uses credit card information, 802.1X WLAN authentication, PANA, Universal Access Method, challenge-response mechanism with a userid using Java Cardor other access mechanism to obtain access to the local access network. It then dynamically or statically figures out its mobility server and requests service from the mobility server in the user's service provider network. In most cases there might be a service agreement between the service provider and the network access provider. On the other hand, they might be unrelated services.

Separate Network Access, ISP and Mobility Service Provider: This situation is a bit more complex than the above where the user's mobility service provider is not the same as the Internet Service Provider. In this case, a policy agreement between the ISP and mobility service provider helps for billing and QoS. The Access Network operator is responsible for reliable data delivery of packets during the hand-offs, by using the hints from the mobile node about the next to-be-visited network and buffering data for the recently departed user or the arriving user. IETF has been working on a network layer fast hand-off solution for network layer mobility; the solution handles both network-assisted hand-off and mobile-node-assisted hand-off situations.

5.0 Possible Solutions

As we have discussed earlier regarding different types of mobility, the solution for solving mobility problems is different for each type of mobility scenario. The focus of this document is device mobility - assuming it changes its IP-address when the mobile device changes subnets or network.

5.1 Our Exploration

We conducted an exploration on Campus mobility with a focus on device movement as opposed to user movement to stationary devices at different locations.

The Problem

When a user uses a laptop or other portable IP-device from the office to a TCP session and then moves to a different location, the device gets a new IP-address. Thus the TCP connection breaks and the user has to restart applications such as ssh, rlogin, telnet, ftp or video-stream services, Voice-over-IP, etc.

The objective of the exploration was to find an effective solution which does not affect the user applications upon movement from one IP-subnet to another IP-subnet.

Link-layer (L2) Approach

Device mobility solutions can be handled at the link layer or network layer or at the application layer. Link layer solutions provide transparency to the network layer when the device moves from one link to another. Link layer solutions exist today for wireless access points and wireless LAN switches which either can tunnel the packet to the new access network AP or wireless LAN switch or it uses VLAN solutions and static routes at the link layer. This solution works in one type of access technology in small scale. For global networking in a multi-technology access environment, the link layer solution of device mobility falls short, especially when the mobile device needs to maintain continuous connectivity.

Application Layer Approach

Solving device mobility at the application layer is also possible by having the application realize that the device IP-address has changed. The application then closes the present connection and re-establishes a new connection with the new IP-address. This works transparently with many protocols such as HTTP, but other applications that depend on end-point address stability need to suffer a delay in detection of movement, closing and re-connecting. This also mandates modification of existing software to handle mobility or running a new set of applications. Normally, the initiating end-point would not know if the remote point application supports the mobility feature unless there is a standardized handshake mechanism for this purpose. Thus application-level mobility has limited scope and has issues with wider scope of usages.

Network Layer(L3) Approach

Mobility solution at the network layer solves the above problems that link layer and application-level solutions have, i.e., it works across different access media and it works transparently with existing applications.

We have looked into Mobile IPv6 solution [RFC3775, RFC3776] for network layer mobility. We have actively participated and provided leadership in the standardization process of this protocol at IETF and its Interoperability events across the Industry and educational institutions. Mobile IPv4 (predecessor of Mobile IPv6) has been deployed in 3GPP2 wireless IP networks. 3GPP2 is considering using Mobile IPv6 for its next generation wireless IPv6 networks. Major industry leaders in Systems and Networking, and academic institutions had implementations on Mobile IPv6. Sun's prototype implementation on Mobile IPv6 is on route-optimization. Our prototype has successfully interoperated with other implementations at the Connectathon (http://www.connectathon.org) event. The following describes how the Mobile IPv6 protocol works:

Mobile IPv6 Basic Operation:

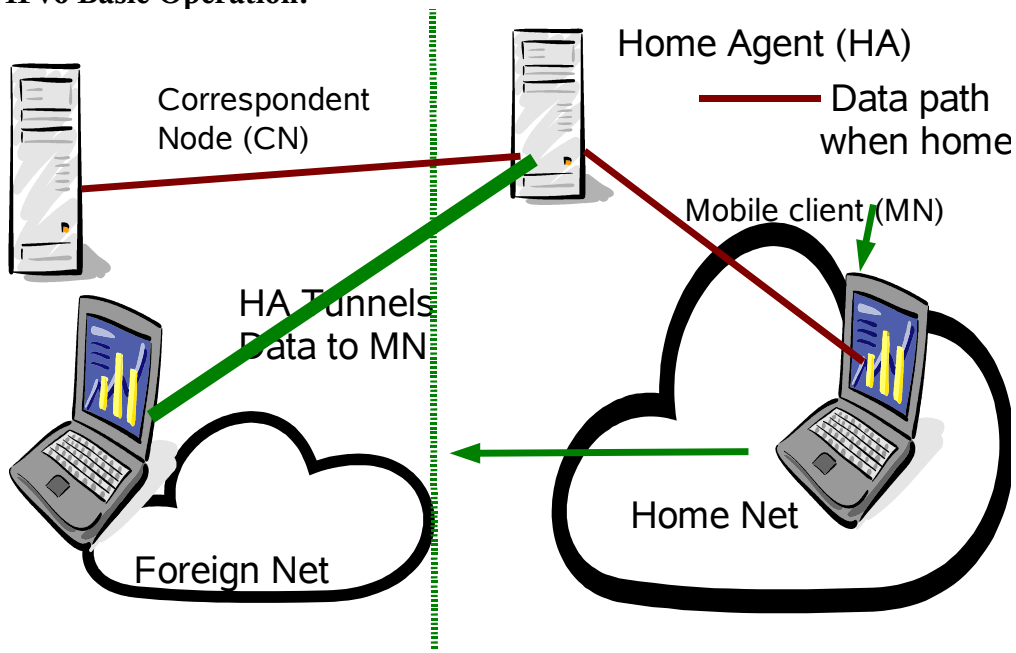


Figure 4: Basic Mobile IPv6 Components

Mobile IPv6 solves the problem of breaking TCP or other end-point-dependent connections when the IP-address changes due to movement of the device from one network to another. It actually introduces a proxy called a Home Agent (HA) server which acts as the forwarder of existing connection to the new location. The mobile client (MN) needs to register with the Home Agent securely and upon movement, the mobile-client sends binding update to the Home Agent using IPsec transport mode by giving information about its new IP-address. The Home Agent then verifies the authentication of the user and creates an IPsec tunnel between the Home Agent and the mobile node. The Home Agent acts as a proxy for the network discovery process in the local network and it forwards packets, destined to the mobile-client's home IP-address, to the newly created tunnel. The mobile-client picks up the packets on the other end of the tunnel, decapsulates and passes the data part to the upper layer. The applications and transport layers do not see any change in IP-address although the mobile-client has moved away from its home. The correspondent node (CN) in the above diagram is the node with which the mobile-client has already started a connection while at home. We will use the same definition of correspondent node(CN) for the rest of the document. A correspondent node (CN) could also be a mobile-client such as a cell-phone.

Mobile IPv6 with Route Optimization (RO):

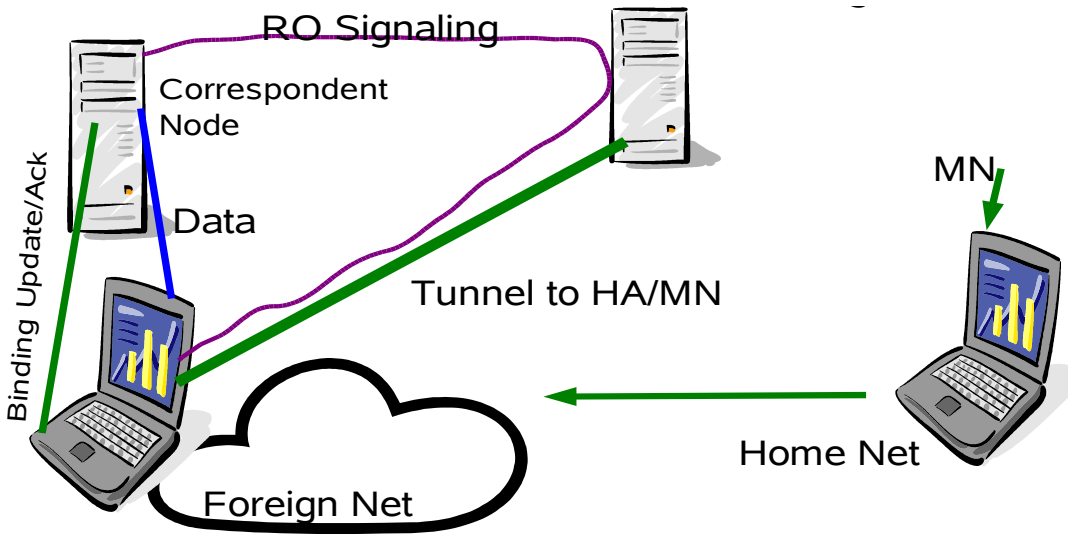


Figure 5: Mobile IPv6 Route Optimization

In some situations, the flight of a packet through the Home Agent adds delay to the packet round-trip time. It depends on the number of hops between the new location of the mobile node and the Home Agent, and between the correspondent node and the mobile node. Also the link quality of the paths between these entities is a major factor. If it turns out that one round-trip time of a packet exchanged directly between mobile node and the correspondent node takes less time than the one via Home Agent, the mobile node can fire-up the route-optimization technique for efficient data delivery. Round-trip time is usually measured by the time between an ICMP packet is sent and when the reply returns from the destination. The route-optimization part of Mobile IPv6 affects both the correspondent node and the mobile node. The correspondent node is typically a web or other application server. For the route-optimization support, the correspondent node keeps a binding cache and uses that information to route the packet to the mobile node's new location instead of its home IP address. Similarly, the route-optimized mobile node implementation knows this packet is bound to its current address and it then replaces that address by home-address before passing the packet to the upper layer. There are security concerns in route-optimization as any attacker on the path of the mobile node can potentially impersonate and launch an attack on the correspondent node or other nodes in the visited network. The protocol introduces a medium level security by IP-address testing and using symmetric cryptography for dynamic key exchange between correspondent and the mobile node. However, the community is not convinced yet on the level of security for critical deployment, and more work on improving security and latency of initiation of the route-optimization is in progress at the IETF in mobility working groups. Our exploration also included a demo of streaming video over IPv6 network using Sun implementation of correspondent node and a third party Home Agent and mobile nodes. We demonstrated that the video streaming service from route-optimized Sun correspondent node (Streaming server) continues on the new network

almost seamlessly when the mobile node was moved from one subnet to another; without the route-optimized Mobile IPv6 server implementation, the streaming flow stops immediately when the mobile node changes the subnet or network. The streaming media server program uses the end point IP(v6) addresses once the connection is established between the video-server and the video-client. If the video-server implementation of Solaris™ kernel did not run the prototype Mobile IPv6 correspondent node route-optimization implementation and the Mobile IPv6 Home Agent, the video-client request would have contained a different IP-address at the new location – the streaming server implementation would not process that request as it does not match with the original IP-address of the client for that video session.

5.2 A scenario for Continuous Mobility at the Enterprise Network

In order to use voice/video/data over the IP network on the mobile devices in the office campus, mobility service is useful apart from video server and SIP server or enterprise IP-PBX box. The architecture can handle any application that depends on endpoint IP addresses provided the mobile-device runs the Mobile IP(v6) implementation.

The architecture assumes that the user has access to the local wireless network and access to the authentication server and other servers through VPN or direct corporate network access. The user device may be configured with some pre-shared secret to start IPsec communication with the Home Agent server. The user optionally may identify itself to the Identity server to get access to the Corporate network. It then uses DNS server to receive an SRV record for its Home Agent's name for the network. The node then starts the mobility service by registering with the Home Agent. Registration with Home Agent means that the Home Agent will acknowledge this node as part of its home network and it will provide forwarding service to the node when it moves outside its network. The initiation of mobile-node with a new network is called bootstrapping. Bootstrapping can happen when a user starts a fresh mobility service or boots the device in a new network. For better security and dynamic bootstrapping process, please refer to the IETF BMIP proposal [BMIP].

The following diagram depicts a scenario for continuous Mobility at the Campuses:

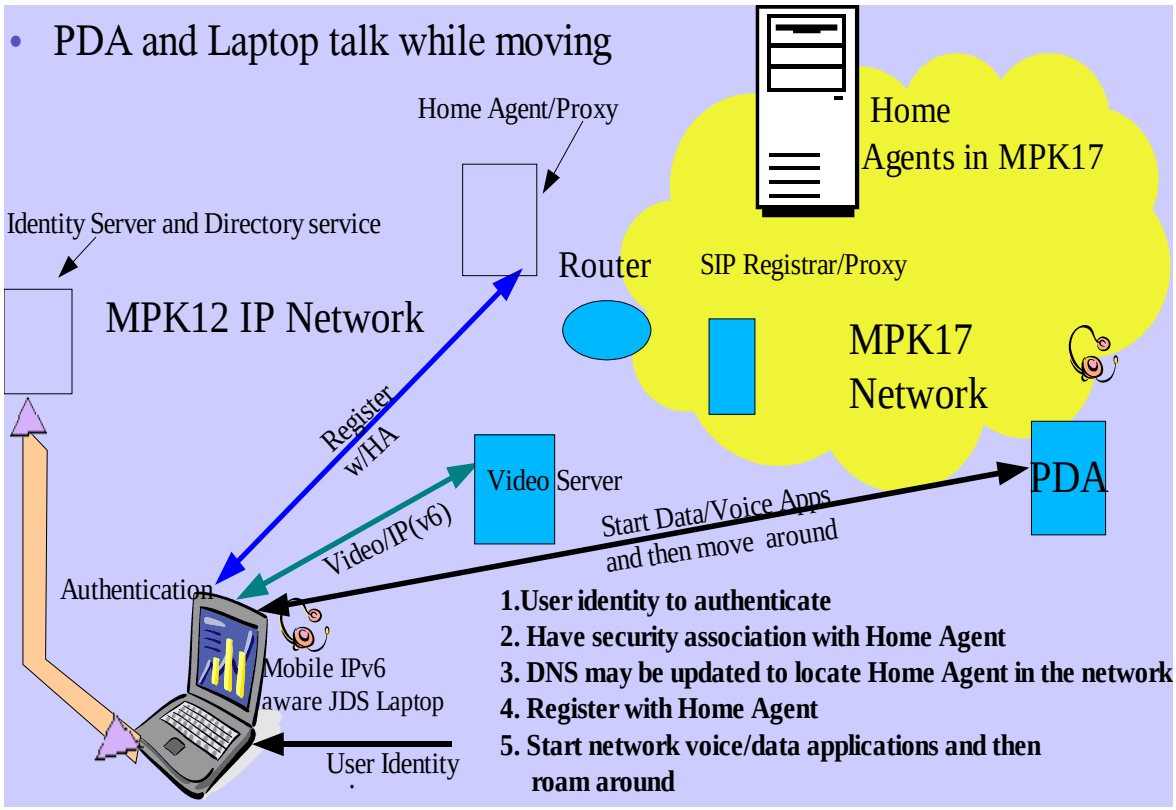


Figure 6: A Deployment Scenario of Secure Mobile IPv6 in the Enterprise Network

6.0 Analysis Of Gaps

The exploration finds that the following areas need attention for further research and development:

- Application mobility across devices: The authors believe that the Java isolate migration technique could be a powerful tool for application mobility across devices. More research should be done on this area for application mobility support.
- Session mobility: File system migration and the ease of user configuration for a mobile user using Sun Ray are useful functionalities that enahnce Sun Ray usability.
- Mobility aware applications: Develop mobility aware applications which will take hints from the lower layer for movement and act accordingly. These applications may also detect changes in device location, configurations, etc. and automatically provide user specific services.
- Movement Detection and MAC layer: Solaris and JDS (Sun Java™ Desktop System) Linux do not autodetect movement and autoconfigure accordingly, or pass the information to the upper layer. Automatic movement detection and self-configuration are necessary Operating System networking features for mobile wireless laptops across multiple subnet changes.
- Network Layer: An inter-Campus deployment of continuous mobility is needed as per feedback from many engineers. Providing support for 'Mobile Network' (NEMO) would be an interesting advanced development project. Sun Solaris/Linux box can act as mobile routers as well as mobile nodes. The Home Agent Service is a checklist item

that Solaris OS should provide.

7.0 Conclusion

The following chart is a guideline for the requirement analysis of mobility characteristics. The purpose of the chart is to identify underlying mobility requirements for a set of potential applications for mobility.

Application	***Security***	***Performance***	***QoS***	***Movement Detection***	***Tolerance Of Heterogeneity***	***Auto-configur-ation***
Voice	Authentication/Authorization (Required)	hand-off < 100ms	Optional	Yes Required	Not required	Yes Required
Video	DRM, Authentication (Required)	Yes (Over WLAN, Broadband)	Yes	Yes Required	Desirable	Yes Required
Data	Yes	Desirable	Optional	Yes Required	Optional	Yes Required
Nomadic Mobility	Yes	Desirable	Optional	Optional	Optional	Desirable
Application Mobility	Yes	Migration time < 1 sec	N/A	N/A	Yes	Yes Required
User Mobility	Yes	Yes	Desirable	Yes Required	Yes	Yes Required
Device Mobility	Yes Required	Yes	Optional	Yes Required	Optional	Yes Required

This document also identifies the gaps in mobility implementations in Sun Solaris or Linux product offerings in section 6. At the time of writing of this document, Solaris or Sun™ Linux do not provide a network mobility solution in its stack. The analysis of gaps section provides guidelines for future implementation and research work in the field of enterprise mobility.

8.0 References

[BMIP] Boot-Strapping Mobile IPv6. J. Kempf, E.7 Nordmark, S. Chakrabarti. December 2004, Work in progress. Internet Draft. Http://www.join.uni-muenster.de/Dokumente/drafts/draft-chakrabarti-mip6-bmip-00.txt

[BootStrap] Problem Statement For bootstrapping Mobile IPv6, A. Patel, January 2005, Work in Progress. Internet Draft. draft-ietf-mip6-bootstrap-ps-03.txt

[DNAv4] Detecting Network Attachment in IPv4 (DNAv4), B. Aboba, J. Carlson, S. Cheshire, December 2005. Work in progress. Internet draft. draft-ietf-dhc-dna-ipv4-18.txt

[DNAv6] Detecting Network Attachment in IPv6 Networks (DNAv6), B. Pentland, Ed. October 2005, Work in progress. Internet draft. draft-pentland-dna-protocol3-00.txt

[JSR 121] Application Isolation API Specification. Krzysztof Palacz. December 2005

[RFC3775] Mobility Support in IPv6. D. Johnson, C. Perkins, J. Arkko. June 2004.

[RFC3776] Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents. J. Arkko, V. Devarapalli, F. Dupont. June 2004.

[RFC3220] IP Mobility Support for IPv4. C. Perkins, Ed. August 2002.

[RFC2884] Extensible Authentication Protocol (EAP). B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, Ed. June 2004.

[RFC2865] Remote Authentication Dial In User Service (RADIUS). C. Rigney S. Willens, A. Rubens, W. Simpson. June 2000.

[RFC2866, 2867] RADIUS Accounting. C. Rigney. June 2000.

[RFC2869] RADIUS Extensions. C. Rigney, et al. June 2000.

[RFC2132] Dynamic Host Configuration Protocol. R. Droms. March 1997.

[RFC4135] Goals of Detecting Network Attachment in IPv6. JH. Choi, G. Daley. August 2005

9.0 Definition Of Terms

3GPP2 – Third Generation Partnership Project 2 http://www.3gpp2.org

DHCP – Dynamic Host Configuration Protocol

DNS - Domain Name Services

DRM - Digital Rights Management

GPRS – General Packet Radio Service: a mobile data service available to users

ICMP – Internet Control Message Protocol

IEEE - http://www.ieee.org

IETF - Internet Engineering Task Force http://www.ietf.org

IP - Internet Protocol version 4

IPv6 - Internet Protocol version 6

ISP - Internet Service Provider

MIPSHOP – Mobility for IP: Performance, Signaling and Hand-off Optimization

MTU - Maximum Transmission Unit

NEMO- IETF Network Mobility Workgroup

NFS - Network File Service

PANA- Protocol for Carrying Authentication for Network Access

QoS - Quality Of Service

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

VLAN - Virtual Local Area Network

VPN - Virtual Private Network

VoIP - Voice Over Internet Protocol (IP)

WLAN- Wireless Local Area Network (IEEE 802.11 a/b/g)

10.0 Acknowledgment

Thanks to Roger Meike, Research Director in Sun Labs for encouragement in writing this report and giving ideas for applicability guidelines. Also thanks to Lisa Pavey, for supporting the mobility exploration project at the CTO office. Thanks to Jeanie Treichel and Pete St. Pierre for final reviews of this document.

About the Authors

Samita Chakrabarti
Staff Engineer

Samita Chakrabarti received her M.S. in Computer Science from the State University Of New York at Albany and a B.Sc/B.Tech in Physics and Electronics from the University Of Calcutta, India. Prior to joining Sun Microsystems in 1996, Ms. Chakrabarti worked at Amdahl Corporation and Tandem Computers as a Network Software Engineer. At Sun, she has worked in Solaris Networking Technology, CTO/Network Technology Office, and Sun Microsystems Laboratories. She was one of the contributors in the Solaris IPv6 industry-leading project at Sun; she is a contributing IETF member in IPv6, Mobile IPv6, 6LowPan and Mobile IPv4 working groups. Ms.Chakrabarti worked on the Enterprise Mobility project at the CTO Office where she developed a Mobile IPv6 Route-Optimization prototype and contributed towards Mobile IPv6 IETF standards. Most recently she has been involved with the Sun SPOT project at Sun Labs where she led the mesh-networking effort for the Sun sensors and designed the adhoc multihop stack on top of IEEE 802.15.4 radio. Her area of work-interests involves Mobility, Low Power Adhoc routing and IPv6 networking.

Erik Nordmark
Distinguished Engineer

Erik has been at Sun since 1989. He has spent most of this time on networking centered around IP such as IP Multicast, IPv6, Web performance, TCP/IP multithreading, STREAMS, as well as significant technical work in the Internet Engineering Task Force. The IETF work has included working on many parts of IPv6 and serving for five years as an IETF Area Director and as such a member of the Internet Engineering Steering Group (IESG). Currently the IETF work includes Scalable IPv6 Multihoming (shim6), Detecting Network Attachment (DNA), and Transparent Interconnection of Lots of Links (TRILL).

Before he joined Sun, Erik worked at the Swedish Institute of Computer Science. He holds degrees from Linkoping University, Stanford University, and Uppsala University.

Danny Cohen
Distinguished Engineer

Danny Cohen was educated in Technion (Israel), MIT, and Harvard, where he received his PhD from Ivan Sutherland, a Sun fellow.
He was on the Computer Science faculties at Harvard, Technion, and Caltech, then he lead a research division at USC/ISI for about 20 years. Looking for a change in his life style he left ISI and co-founded Myricom. He is now working on a research project at Sun Microsystems, developing a high-productivity supercomputer for DARPA.

Danny pioneered realtime applications over computer networks, including first realtime visual flight simulation on a general purpose computer, realtime radar simulation, realtime packet-voice, voice-over-IP, and packet-video. He has started the MOSIS system, and contributed to the development of digital libraries. His main interest in recent years is high speed networking.

Danny is perhaps best known for coining the terms "Big Endians" and "Little Endians".