

---

# Nomadic Tenets - A User's Perspective


Steve Gadol  
Mike Clary

SMLI TR-94-24

June 1994

## Abstract:

This document will attempt to establish some basic tenets on how nomadic computers should operate. These tenets are derived from practical experience gained from using nomadic computers to access the enterprise-wide information resource at Sun<sup>®</sup>. These tenets are not hard and fast; they are recommendations of how nomadics should work. They will surely be refined as more experience is gained. They do, however, represent a starting point for living and working in a nomadic computing world.

 *Sun Microsystems*  
*Laboratories, Inc.*  
A Sun Microsystems, Inc. Business  
M/S 29-01  
2550 Garcia Avenue  
Mountain View, CA 94043

**email addresses:**  
steve.gadol@eng.sun.com  
mike.clary@eng.sun.com

## *Nomadic Tenets - A User's Perspective*

---

### ***Introduction***

For many people, having a nomadic machine capable of supporting both computing and communications is a captivating vision. Now it's about to become a reality. Rapid growth in popularity of portable PCs and sub-compacts like the HP 100LX foretells the emergence of mobile computing as an important new market, one for which requirements are still very much in the formative stage. This is especially true of the sub-compact and personal data assistant (PDA) segments of the market. These devices have just recently been introduced. Although rapid progress has been made in both hardware and in packaging, important ingredients are missing in the "solutions" that have appeared thus far. One that stands out is a distinct lack of perspective on how the end user will adapt to mobile computing. The young industry building mobile machines hasn't yet figured out what combination of functionality will make them truly useful. A nomadic computer can be much more than a pager but it generally isn't a quite a mobile workstation. It's a new design space—one in which many of the old rules won't readily apply. In many cases, the machines are not being used in similar ways to the usage patterns for desktop workstations. Lack of focus and perspective on the vendor's part can be frustrating to users as they attempt to integrate these nomadic computers into their everyday work.

This document will attempt to establish some basic tenets on how nomadic computers should operate. These tenets are derived from practical experience gained from using nomadic computers to access the enterprise-wide information resource at Sun<sup>®</sup>. These tenets are not hard and fast; they are recommendations of how nomadics should work. They will surely be refined as more experience is gained. They do, however, represent a starting point for living and working in a nomadic computing world.

---

## *The Mobile Office Project*

The Mobile Office project in Sun Microsystems Laboratories, Inc. (SMLI) is targeted to provide users with mobile access to e-mail, on-line calendar and other selected on-line transaction systems. Access to these services is being made available to Sun employees as they move around the Sun campus, commute between home and office, and as they travel domestically or internationally. A central goal for the project is to provide the level of office productivity to nomadic users that, to date, has been only achievable on the desktop office workstations.

For the initial Mobile Office experiments, the system of choice is the HP 100LX palmtop computer combined with a Mobidem<sup>TM</sup> radio modem (see Figure 1). This configuration uses RadioMail<sup>®</sup> as the basis for communications. Alternate means of communications are also available such as CompuServe or X.25 access via Sprintnet<sup>®</sup>.



Figure 1 HP 100LX and Mobidem

---

The Sun organizations involved in this experiment are the Sun Microsystems Computer Corporation (SMCC) Technology Development, SMLI, and Information Resources (IR). The test group is the SMCC Technology Development. Having a small group make daily use of Mobile Office services is seen as key to helping the project separate the valuable and important from the simply technologically appealing. Currently, the Mobile Office project has basic services in place for e-mail and on-line calendar, and provides rudimentary access to other on-line transaction systems. Next steps include developing a secure e-mail facility and extending access to selected on-line transaction systems.

## ***Nomadic Tenets***

The term *nomadic tenets* is defined as the set of basic desired principles of operations for nomadic machines from an end user's perspective. As such, these rules should influence hardware and software engineers' designing solutions for the nomadic user community. Identifying what users want and how they want to use it is of primary importance; technology is secondary.

In the following discussion, the term *nomad* refers to the person using a nomadic computer. A *nomadic computer* or *nomadic device* includes both the hardware and software. *Nomadness* is a term describing the state of being mobile, but still electronically connected to the enterprise.

### ***1. Nomads are part of an organization.***

The typical nomad is a member of an organization whose need for nomadic devices stems from a requirement to remain in contact with that organization, even while physically remote from the normal workplace, i.e., an office. The organization has an infrastructure which includes a networked computer environment, providing e-mail services and support for on-line transaction systems. In the nomad's primary office, access to this computing environment is provided via a desktop workstation.

This tenet encourages those providing the nomadic computing environment to carefully consider which services to place directly on the nomadic computer and which to include as part of the overall network infrastructure. If too much

---

functionality is placed on the nomadic computer, it becomes a stand-alone system. It may require too many memory and disk resources to be truly mobile. It also may not interoperate well with the enterprise network after being temporarily disconnected. The result can be one of disconnecting the nomad from the organization. If, on the other hand, too much functionality is placed within the enterprise network infrastructure, the nomadic device is effectively crippled because it can't operate on an independent basis when not connected to the network.

Application developers should realize there are choices to be made on the location of application components, i.e., make them part of the network infrastructure or put them on the nomadic computer. In general, it is easier to implement components in the infrastructure than to take on the more difficult task of implementing them on resource-constrained nomadic devices. Individual application requirements must dictate the component location, not the ease of implementation.

In this initial Mobile Office experiment, the nomadic computer has very limited capability and relies heavily on the infrastructure to provide services. Most nomads use the HP 100LX/Mobidem as a smart terminal device into their desktop workstation environment which includes on-line transaction systems, e-mail, and group calendaring applications. Nomads don't use the HP 100LX/Mobidem as their sole machine, but as a window into their environment. Their desktop workstation serves as the mail router, mail archiver, keeper of the calendar, and the basic means to access transaction systems. The nomadic computer retains very little data—only pending messages to be read or sent and some personal data.

***2. Nomadness is primarily concerned with communications, not computing.***

This tenet can be viewed as a corollary to #1. Nomads can have all the computing power in their nomadic device that they could possibly ever use, but it's useless if they can't communicate results, facts, messages, etc. with their home organization.

This observation should guide designers to defocus from the implementation details of the nomadic computer and worry more about communications. Minimal device size, small operating system (OS), smooth user interface, new storage mechanisms, and extended battery life are all important pursuits, but

---

they are all uninteresting without communications. Further, communications is not simply putting a phone on the device, or adding an Ethernet connection or an integral modem; it's software.

Software needs to be developed to handle the intermittent connections nomads make with their office environment. This requires finding a replacement for the current static nature of network address assignments. It also requires developing intermittent transaction queuing managers, and adding support for multiple methods of accessing the network. Unfortunately, systems meeting these requirements are not widely available today.

In the Mobile Office experiment, the primary communications mechanism is RadioMail. In the event the nomad is outside of radio coverage, public carrier services like CompuServe mail can also be utilized. The user's ability to switch between e-mail services requires the desktop workstation to redirect incoming mail away from the default RadioMail account to another available mail service. By remotely activating the switch mechanism, the nomad can use the more pervasive coverage offered by a service like CompuServe.

Implementing the mail switching capability used for the experiment was straight forward because the kind of message-based communication it depends on is inherently simple. No work on transaction queuing or mobile address assignment has yet been initiated. These issues must be addressed in follow-up experiments.

### ***3. Nomads shouldn't have to deal with a whole new infrastructure.***

This also is a corollary to #1. For developers, there can be a real temptation to greatly expand or even overhaul the enterprise infrastructure to prove mobile access. This is most likely the wrong approach. The Mobile Office experiment has shown that, at most, only nominal additions to the infrastructure are really needed. What users expect is a natural integration of the environment provided on their mobile machine with the information and services resident on the enterprise network. The more seamless the integration can be made to appear, the more comfortable users seem to become. Coming up with whole new sets of user interfaces, access methods, and support procedures would confuse users and create a serious problem for system administrators who operate the enterprise network.

---

There are two general principles which apply. First, the users mobile computer comes with some kind of user interface. It may be character based or it may be a graphical user interface (GUI) like MS-Windows<sup>TM</sup> or PenPoint<sup>®</sup>. Using the machine to remotely access the enterprise environment shouldn't require the user to learn a new user interface. One of the most common complaints computer users have in general is having to deal with too many interfaces. The principle applies here. Make use of the resident user interface (UI) whenever possible.

The second principle has to do with application integration. Notebook computers supporting systems like MS-Windows or Mac OS come with powerful application integration mechanisms. The resulting operating environment allows users to quickly and easily use information created in or managed by one application in several places. A portion of a spreadsheet can be quickly imported into a document built with a word processor, or a database table can provide information to an analysis routine running in a spreadsheet package. The most natural way for users to incorporate information stored on the enterprise network is for the mobile access interface to support the integration mechanisms with which they are familiar. This decouples the use of the information from its locality.

Fortunately, there aren't many such mechanisms in wide spread use. Implementing a general purpose "exchange" is feasible. The Mobile Office project has already put together the prototype for a general calendar manager filter that makes it possible for the calendar management software resident in the nomad's systems to exchange information with like services running on the enterprise network. Indirectly, nomads, even with different kinds of machines, can exchange calendars with each other. Borland International, Inc. has recently begun shipping its Object Exchange software allowing MS-Windows users to share data via both networks and e-mail. The underlying mechanisms could easily be supported on Sun UNIX<sup>®</sup> systems as well.

The approach advocated here has implications for how future network services and applications should be built. What is becoming very clear is that the network resident portion of the software should strive to minimize UI dependencies. Providing a well structured application program interface (API) rather than an extensive UI, makes it straightforward to construct an appropriate UI. Sometimes the interface the nomadic user employs will be a

---

custom application. In many cases, a very good UI can be more easily constructed using the extension mechanisms that come with many of today's productivity applications like WORD<sup>TM</sup> or Paradox<sup>®</sup>.

#### ***4. Nomadness is not free.***

There are real costs associated with nomadness, primarily with the communication mechanisms. Depending on the infrastructure services, there can also be additional charges associated with using a particular application and costs for data storage. These costs must be borne either by the enterprise or directly by the nomad.

Software structures need to be put in place to capture *billable nomadic events* and charge for them based on published rates. Doing this would allow users to make decisions based on the cost of their use of nomadic computing and communicating services. One model might be to get the same billing resolution that the telephone companies achieve, i.e., to the penny for each service event. The ideal scenario would be to provide advance cost estimation so the user could choose between alternative applications or communications methods on an economic basis.

The initial Mobile Office experiment has not included costing. RadioMail services are currently being supplied on a fixed cost basis, independent of usage. Future experiments should address this issue.

#### ***5. Nomads need flexible communications protocols.***

Conventional enterprise networks provide application developers with a convenient target environment. Network connectivity is assumed to be constant, i.e., computers on the network are assumed to always be connected and able to communicate with each other. Further, the network protocol is consistent, e.g., it's always fixed. At Sun it's TCP/IP. Hence, an application can assume a network connection, say to a database, is always there and is always the same type of connection—it is consistent and constant.

A network that is consistent and constant is predictable, allowing an application to perform transactions using a synchronous procedure call model. This model doesn't hold in the nomadic environment.

---

Nomads, by definition, do not have fixed locations, and not all networking methods will always be available in all locations. The nomadic world more closely fits an asynchronous computing model. This changes the assumptions an application can make. When one cannot be assured of a synchronous connection, one needs to support an asynchronous store-and-forward model. E-mail is a prime example of a store-and-forward application.

E-mail is a very reliable protocol. Given that it is properly addressed to a recipient, and any needed gateways between systems are operative, an e-mail message will get to its destination eventually. Other applications should be able to support that same “gets there eventually” model as well. Many applications don’t need to have an immediate input/response capability. This can be advantageous because a store-and-forward model of communicating is more likely to always be obtainable, albeit slower. In the nomadic environment, speed isn’t always the winner as long as “gets there eventually” doesn’t mean “gets there next week.” With a high speed connection, a store-and-forward mechanism can be very fast and can adequately satisfy even immediate interaction needs.

Store-and-forward communication mechanisms form the basis for connectivity in the current Mobile Office experiments. There is no dependence on synchronous communications over IP connections. A software facility called “Proxy” enables nomads to send messages to their desktop workstations instructing the workstation to execute commands on the nomad’s behalf. Proxy then packages the result in another message and returns it to the nomadic device. Only very limited assumptions have been made about the communications mechanism. With Proxy, the project has already achieved an easy to use, more reliable communications mechanism than would be the case with a synchronous IP protocol. The implications are profound, especially when international travel and the constraints it imposes are factored in.

***6. Nomads want to use multiple devices, but ideally have only one public identity.***

The nomad will most likely have several computers. We expect people to have them in their offices, at home and with them as they travel. These machines are expected to be of different types because they are used at different times and to meet different needs. As the nomad’s location changes, it’s preferable for that person to be able to use whatever is readily available. Currently, with multiple

---

devices, come multiple identities. Each computer has its own identity that needs to be assigned and maintained. The experiments to-date indicate that it is preferable to have only one identity, even though multiple devices can be in use at different times.

If there are multiple identities, the nomad will be known by multiple addresses/names/handles. It is similar to the problem with telephones. A person can have an office number, an administrator number, a home number and a cellular number. This creates a confusing situation. To get in touch with someone, you often have to hunt through a maze of contact points trying to guess where the person might be, or you leave a message at as many places the person might check. The 700 number scenario the telephone companies are starting to implement is a move in the right direction. This same approach needs to be applied to the relationship between nomadic devices and the hosting network infrastructure.

In many cases, it is also preferable for the traveling computer to be personality neutral. Nomadic devices generally retain some private information that makes them personal, but that aside, one would like to be able to easily let a friend use a machine for at least short periods. It would make the nomadic computer more like today's telephone. If someone wants to make a call, they ask without hesitation if they can use your telephone. You may get charged for the call and that's an acceptable social norm. The same scenario generally does not apply to nomadic computers, unless you allow your friend to also impersonate you, at least long enough for them to perform their nomadic activities.

RadioMail imposes on each nomad a second mailbox assigned to their nomadic device (specifically to the Mobidem). To the rest of the world, this looks like another network e-mail address in addition to the one assigned to the nomad's office workstation. Experience has shown that it confuses people when they want to communicate with the nomad. They don't know what address to use to assure the nomad will receive the message in a timely fashion. To eliminate this problem, the Mobile Office project implemented a means to hide the nomadic address and only publicize the desktop workstation's address. This mechanism makes the desktop machine act as the "mail router" for the nomadic device. The workstation's address is the only address the rest of world needs to know.

---

The Mobile Office project has yet to address the personality neutral issues. These should be factored into future experiments.

***7. Nomads consider security mandatory since physical security is negligible.***

Nomadic computers are inherently insecure. They are physically carried around, left in the open, and communicate via publicly accessible channels. Since nomadness is about both communicating and computing, security has to cover both areas.

Communications security requires support for enhanced authentication to protect the host organization's infrastructure. Smart cards, RSA certificates, or similar mechanisms should be incorporated into both the enterprise infrastructure and into the nomadic computer. In addition, a means for encrypting the data transmission is required. As nomadic machines become more prevalent, more and more sensitive data will be transmitted via essentially open channels. A user's confidence in the communication link depends on having significant authentication and privacy mechanisms in place.

Device level security is also required. In spite of the ideal being a personality neutral device like a phone, users are going to store personal or confidential data on the nomadic machines. It's not just a window into the nomad's infrastructure and environment. If the machine is lost or stolen, that data needs to be protected. Further, if a lost computer is tampered with or there are attempts to gain access to its data, the machine should provide sufficient protection. Many users would prefer it simply destroy the data. A potentially interesting capability would be to enable nomads to send their nomadic machine a "kill command," and have it destroy the data. This would be analogous to a lost credit card, which is essentially rendered meaningless after it is reported lost or stolen, i.e., you don't have to worry about someone using it. One assumes the user can always obtain the data again, because the enterprise network will provide backup to recover from failures. Hence, lost nomadic computers can be considered a special case of device failure (or maybe more appropriately, user failure).

To-date, the Mobile Office experiment has not included security beyond that provided by the UNIX system hosting the enterprise network at Sun. One of the project's next steps will be to implement a message encryption mechanism for RadioMail.

---

**8. Nomads want to use paging and polling to satisfy two different application needs.**

There are two basic approaches for nomads to stay in touch with their infrastructure: they can receive *pages* from the infrastructure, or they can *poll* the infrastructure for new information. Each has advantages for different types of applications.

Paging works well for applications such as e-mail. It's preferable to receive an e-mail message when it's sent, rather than have to go to the infrastructure (a post office) to pick it up. This is analogous to receiving a phone call. You simply get it when it happens and you can respond if you're available. Like an answering machine the message is left for later retrieval if you are not *connected* at the time the message is sent.

Polling works well in cases where the data is not time sensitive. For example, a price book application for salespeople does not need to have changes immediately updated. Salespersons can access the infrastructure at their discretion to obtain any changes, i.e., they can poll the infrastructure for updates. It would probably be too burdensome to require applications to accept changes every time they are connected to the network. The problem increases with the number of applications.

Paging and polling are distinct communications models. Application design requirements need to dictate which is utilized. One or the other shouldn't be used just because it's available or appealing on purely technical grounds.

The HP 100LX/Mobidem combination allows the nomad to leave just the Mobidem powered up. When it receives an incoming message packet, it will power on the HP 100LX, and the message will be received. In this way, messages coming from the infrastructure will *page* the user. Other services, like access to on-line transaction systems, require users to actively format a message, post it to their desktop workstation, and wait for a response, i.e., the nomad polls the infrastructure.

**9. The nomad will want to access the enterprise network using a variety of access methods.**

In a global enterprise like Sun, there isn't going to be a single universal network access method any time soon. Depending upon where nomads may find themselves, any number of methods may be available. Dialback modem

---

services work well for fixed locations, radio works well for metropolitan areas, and public data networks work well for wider coverage areas. All of these methods have differing rates of failure and availability. This leads to the premise that the nomad needs to be able to take advantage of what ever method works, wherever they are physically located.

Such a “use what works” strategy places an increased burden on both the applications and the infrastructure. If the access method can’t be predictable, then the type of connectivity between the infrastructure and the nomadic device can’t be assumed. For example, it can’t be assumed that a high speed line is available or that some form of TCP/IP can be used. Nomads may very well find themselves one day at home with high speed modems and IP connectivity, and the next day be in a remote location with only a 300 baud message-based access to a public data network. The same applications should be available in both cases.

This is another reason to support store-and-forward asynchronous access methods. A store-and-forward method is not sensitive to the speed of the line or network protocols; it works with a lowest common denominator.

Since the experimental Mobile Office is store-and-forward message-based, it is easy to convert between different access methods. RadioMail is the primary means, but alternate message services can be used. They include MCImail, SprintnetMail, Compuserve, etc. A user can contact the enterprise from a wide variety of locations and choose which service is more readily available, or least expensive. There is no requirement for special protocols, just a simple serial connection.

***10. Nomadic users will cause more failures than those caused by hardware or software bugs.***

Failures will occur for a number of reasons from hardware to software bugs, but the primary cause of failure will be operator error. The nomad will disconnect the device at inopportune times, reset the device when it appears to be hung, delete important files inadvertently, or modify settings in the belief that they are fixing something. These failures will happen regardless of the precautions taken in training or software design.

---

Since it's a given that operator errors will occur, two primary facilities need to be in place. One is a basic backup mechanism that allows the nomad to store all volatile data to the infrastructure in some organized fashion. In the event of a failure, the nomad can refresh the nomadic device from the backup maintained in the infrastructure. Applications need to consider this as part of the design, and not as an afterthought by implementing bulk file transfers.

Also needed is the notion of the nomadic environment reboot. If nomads corrupt the environment resident on their nomadic computer so that it no longer operates, they should be able to call for a reboot to reinitialize the environment. So, as long as a primal "boot-block" (that the user should not be able to access) is not destroyed, reboot should bring the nomadic machine back into operation. The boot-block implementation could be nothing more than a slow speed connection to the infrastructure. Once a connection is established, the boot process could reinstitute a level set from recent backups. Information restored would include such things as state for any pending transactions, clearing and resetting passwords, reactivating authentication mechanisms, as well as recovering application files and settings. The goal would be to provide the nomad with a fallback position that doesn't require system administrator intervention.

No work has been done yet in the experimental Mobile Office on this issue except for basic backups of nomadic devices to desktop workstations. No sophisticated automated facilities have been put in place. More than once both its creators and users wish they had been there.

## *Conclusions*

Experiences gained from initial experiments carried out by the SMLI Mobile Office project has lead to the tenets presented here. Although much work, especially in the areas of security and application integration, remains to be done to validate these tenets across a wide spectrum of users, the early results have certainly supported them. The most important lesson learned thus far is the value of limiting changes made to the network infrastructure. Introducing mobility does not have to come at the price of a major overhaul. The simple combination of RadioMail and the Proxy mechanism have enabled several people to work away from their offices much more effectively than was previously possible. Over time, enriching the environment with features like

---

security and the ability for the nomadic computer's native applications to better share information with the enterprise network should make the Mobile Office both an attractive alternative and an attractive addition to office-based workstations.

## *References*

Bagby, David. "Concepts for a Nomadic Strategy at Sun." Internal SMLI Document.

Deutsch, Peter L. "Beyond Mail—Scenarios." Internal SMLI Document.

Deutsch, Peter L. "Nomadics & Software." Internal SMLI Document.

Deutsch, Peter L. "A Nomadic Manifesto, Sun's Nomadic Strategy, 1993-1997." Internal SMLI Document.

Hewlett Packard Company. *HP 100LX User's Guide*. 3d ed. 1993.

RadioMail Corporation. *HPLX RadioMail User's Guide*. 1993.

Turbyfill, Carolyn. "A Technical Nomadic Strategy." Internal SMLI Document.

---

© Copyright 1994 Sun Microsystems, Inc. The SMLI Technical Report Series is published by Sun Microsystems Laboratories, 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, and the Sun logo are trademarks or registered trademarks of Sun Microsystems, Inc. UNIX and OPEN LOOK are registered trademarks of UNIX System Laboratories, Inc. All SPARC trademarks, including the SCD Compliant Logo, are trademarks or registered trademarks of SPARC International, Inc. SPARCstation, SPARCserver, SPARCengine, SPARCworks, and SPARCcompiler are licensed exclusively to Sun Microsystems, Inc. Mobidem is a trademark of Ericsson GE Mobile Communications Holding Inc. RadioMail is a registered trademark of RadioMail Corporation. Sprintnet is a registered trademark of Spring Communications Company L.P. MS-Windows and WORD are trademarks of Microsoft Corporation. Paradox is a registered trademark of Borland International, Inc. PenPoint is a registered trademark of GO Corporation. All other product names mentioned herein are the trademarks of their respective owners.