

IP Mobility: Raising the Bar for Convergence Networks

WHITE PAPER



CONTENTS

Introduction.....	1
3Com's Vision for IP Mobility.....	2
Requirements and Challenges of Enterprise Mobility	3
3Com Convergence Architecture to Enable Enterprise Mobility.....	3
3Com SIP-Capable Firewalls to Enable Tethered IP Mobility.....	5
3Com Wireless Infrastructure to Enable Secure and Non-disruptive Roaming	6
3Com Client Software to Enable Mobile Access Convergence Applications	9
3Com Convergence Services to Enable IP Mobility Across Public Domains	9
Summary	10

Introduction

Analysts predict that the explosive growth in enterprise wireless communications seen during the past few years will continue.

- By 2006 the number of mobile workers in the U.S. will reach 105 million—66 percent of all workers, according to IDC¹.
- 50 percent of enterprises will have wireless e-mail in place within three years, which according to Meta Group² will help trigger a surge of wireless application projects during that time.
- Gartner³ estimates that by 2010, 80 percent of key business processes will involve exchange of real-time information among mobile workers.
- Meta Group⁴ predicts that by 2005, 95 percent of corporate laptops will ship with mobility capabilities. As a result, wireless connectivity within the enterprise will become the norm, "whether or not the business is ready."

Growth in mobility within enterprises has been a grass-roots phenomenon largely driven by end users and the requirements of fast-evolving IP networks. In fact, some enterprises have wireless infrastructures that were deployed entirely by end users independent of the IT group. Gartner analysts estimate that one in five companies has a wireless LAN (WLAN) that the CIO doesn't even know about.

The good news is that many enterprises now recognize that they need to support mobile devices and enhanced mobility

within and beyond their premises.

Enterprises in healthcare, government, education, and high-technology industries with sizable campuses and large populations of mobile workers are proactively deploying managed wireless enterprise infrastructures comprising wireless access points and wireless switching that permit roaming.

While IP-based mobility has been enjoying significant growth, enterprises are also deploying IP-based convergence applications at an accelerated pace. IP telephony and related technologies have gained ground mainly due to the maturity and robustness of enterprise IP networks and the Internet. Sophisticated convergence applications such as unified messaging, conferencing, and instant messaging have enjoyed significant growth, as have convergence services such as presence and standards-based end-user clients such as IP phones.

The confluence of IP-based mobility, convergence applications, and feature-rich mobile devices offers exciting new opportunities for enterprises. They can enhance their end-users' productivity and their customer service levels at a much lower cost than is possible with conventional enterprise mobile telephony solutions based on time-division multiplexing (TDM) technologies.

3Com, as a leader in IP communications and enterprise network infrastructure, including IP-based LANs and WANs, wireless networks, and IP convergence applications, is therefore in a unique position to take convergence to the next level: mobility.

¹ "Managing the Mobility Imperative: Enterprises Embrace Mobility Strategies to Achieve Competitive Advantage", 2004

² "Wireless E-Mail: TCO Versus ROI: Part 1", October 6, 2004, Report # Delta 308

³ "Enterprises Must Assess Impact of Mobile Applications", December 22, 2003 Report #DF-21-4374

⁴ "How to Succeed in Mobile Initiatives", January 6, 2004 Report # Practice 2146

3Com's Vision for IP Mobility

Mobility is the ability to roam and still be accessible to other network users. However, mobility is sometimes regarded as pertaining only to cellular networks. According to this narrow definition, an enterprise user who moves between several different corporate and external locations has to resort to the use of a cell phone regardless of whether a tethered office phone or an enterprise wireless network is available.

Cellular mobility can be quite expensive and sound quality can be poor due to patchy coverage in enterprise locations. Typical cellular devices also lack access to sophisticated convergence applications such as data sharing. In addition, cellular mobility requires users to have multiple phone numbers: one for the office phone, one for the cell phone, and one for the home phone. Customers have to remember multiple numbers to reach an enterprise user, or resort to calling the number that represents the most expensive option—the cell phone.

3Com takes a broader approach to mobility by considering the types of networks to which a user may be connected at various times of day, and the availability of cellular infrastructure or cost-effective alternative infrastructure such as enterprise networks at any given location. As shown below, an enterprise user may be at any one of several possible locations:

- At a desk with a tethered desktop phone
- In a corporate office conference room with access to a tethered phone
- Roaming within the corporate location
- Driving between corporate locations, or elsewhere
- Visiting a corporate location with access to a workspace having a tethered desktop phone or a mobile phone on the converged enterprise network
- At a hotel with PSTN or Internet connectivity
- At home with access to a home phone

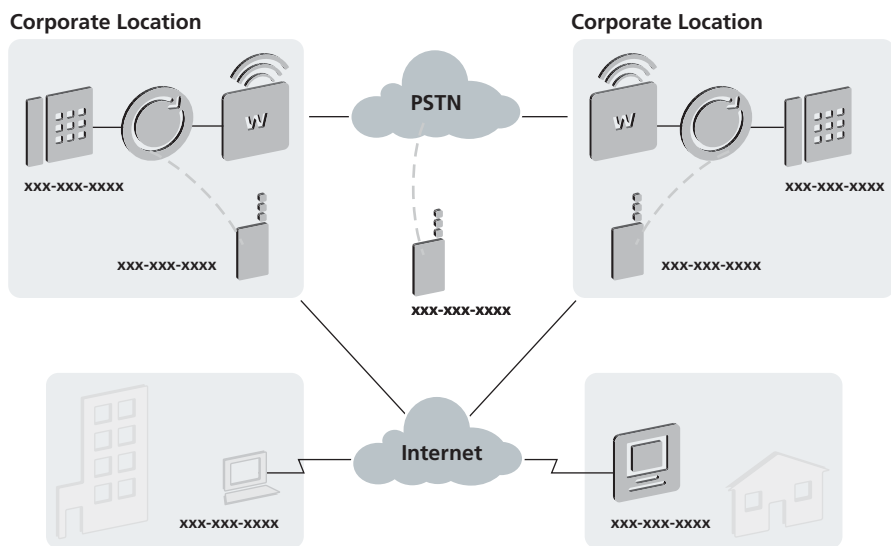
3Com's vision is to provide seamless mobility by allowing users to leverage all the cost-effective alternatives available to them at any particular place or time. 3Com's strategy is to deliver this mobility in three dimensions:

Physical Mobility. The user is able to move between networks, connecting and reconnecting using the most cost-effective network option available. Such options include enterprise LAN, enterprise WAN, wireless LAN, the Internet, and public switched telephone network (PSTN). 3Com's approach delivers mobility at a small fraction of the cost of conventional mobility delivered through cellular networks.

Identity Portability. The user is able to roam within multiple network infrastructures and across network infrastructure boundaries while retaining a single identity. The power of 3Com's approach is that the user is reachable via one access method—such as a single phone number—by customers, colleagues, partners, and friends regardless of which network the user is connected to and where the user is located. Even if an employee should leave the organization, continuity with customers and partners can be maintained through this identity which can be transferred to a replacement employee.

User Interface Universality. The user is able to take advantage of all the services and applications that he or she is authorized to access by means of various devices (desktop phone, desktop computer, wireless device). The user enjoys the same services and appears the same way (presence) to other users no matter how the user is connected to the network.

Mobility in Multiple Dimensions



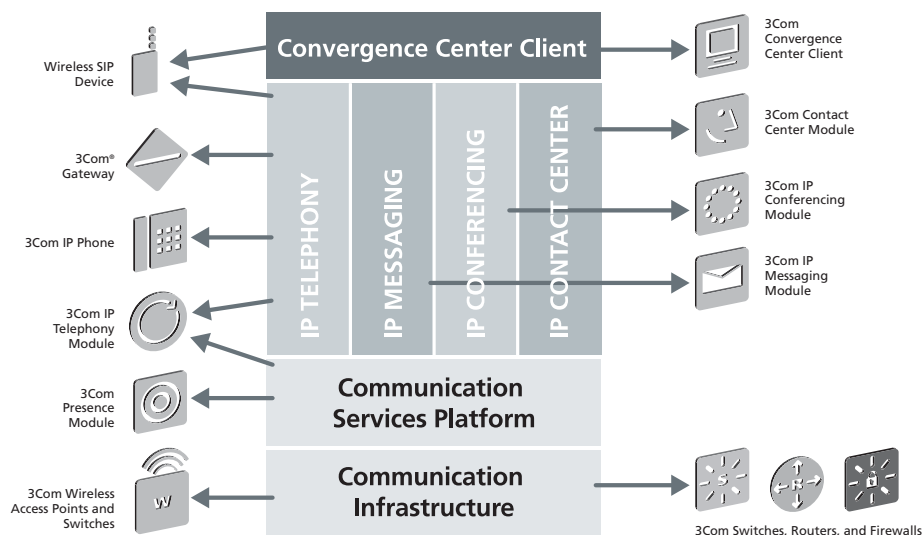
Requirements and Challenges of Enterprise Mobility

To realize the promise of universal network mobility, several challenges must be overcome.

Security	When users are mobile, connections and data need to cross multiple network boundaries, each of which poses a security threat. Wireless networks present unique threats because rogue users can enter the enterprise network through wireless access points that may not be sufficiently protected as part of IT security protocols. Providing authenticated access to the wireless network and convergence application resources through the wireless domain are important requirements to consider when enabling enterprise mobility.
Roaming	Roaming implies crossing one network boundary and entering another while maintaining communication. Roaming occurs within the enterprise wireless LAN when a user crosses from the user's IP subnet to another. Such roaming can cause disruption, especially in connection-oriented real-time communications such as voice conversations. Maintaining continuous connections and consistent access privileges during switchovers and hand-offs among the wireless networks is essential for enabling convergence applications in enterprise wireless LANs.
Devices	Mobility is enabled by remote tethered devices such as IP phones and handheld devices used by roaming users. These devices communicate with other devices and offer access to convergence applications. Conventional mobile devices cannot access all convergence applications, which may include presence-based conferencing and data sharing. In order to achieve universal IP mobility, mobility devices must have the capability to access all the convergence applications deployed by the enterprise.
Portability	In conventional networks, callers often have to try multiple numbers in order to reach the called party directly. It is much more convenient for callers to access the called user with one enterprise number, which is automatically inherited by any of the devices that the user might employ. Such inheritance enables the consistent appearance—including presence availability—of mobile users to the other users.

3Com® Convergence Architecture to Enable Enterprise Mobility

As shown below, 3Com employs a standards-based, layered architecture for delivering a suite of convergence applications.



Key Aspects of 3Com Convergence Architecture

1. The communications infrastructure is based on the Internet Protocol (IP). This layer uses all the standard components of IP networks, such as IP routers and switches that provide connectivity, virtual LANs and subnet routing, Domain Name System (DNS), and Dynamic Host Control Protocol (DHCP). The higher layers are abstracted from additions and changes to the communications infrastructure.

2. Communication services—including name/address resolution, location services, authentication, session establishment, presence, privacy, redirection, and forwarding—are provided by IETF-specified Session Initiation Protocol (SIP). SIP offers several advantages for enabling 3Com® convergence applications using an IP infrastructure.

SIP uses existing Internet technologies such as DNS for name resolution, URLs for naming, and HTTP and Multipurpose Internet Mail Extensions (MIME) for content packaging and transport. With these capabilities, SIP not only integrates with Internet technologies, it also allows development of applications using popular web technologies and interfaces.

True mobility requires identity portability, including consistent appearance and presence. SIP standards specify several capabilities—including registration, authentication, and presence—which inherently support mobility. 3Com SIP implementation is based on a service-oriented architecture (SOA) that delivers these capabilities network-wide. The architecture allows services to be deployed anywhere in the enterprise network. Convergence clients such as IP phones, soft phones, and SIP-compliant mobile devices, as well as convergence applications such as IP telephony, can access these capabilities by invoking the appropriate SIP-based service across the network.

The 3Com architecture also allows the services to be located and administered centrally⁵, while the services are available to every client and application across the network in a global manner. Using this services-oriented architecture, the 3Com SIP-based communication services layer delivers key services that are critical to IP

mobility. These include:

- A standards-based authentication and registration service through which a name with its IP address (or URL) can be registered dynamically.
- 3Com leverages this capability to enable users to log in their identity (e.g. phone numbers) at communication devices other than their desk phones, enabling users to receive calls made to their desk phone numbers at locations other than their desks, such as remote offices, hotels, and home offices.
- The ability of multiple devices such as telephones to receive connections (calls) simultaneously and complete the call with the device that responds first.
- 3Com leverages this capability to enable identity portability to multiple devices and multiple locations, enhancing mobility for traveling and work-at-home users.
- Notification to the presence server of the presence and availability (presence state) of compliant (SIP) clients.
- The server “publishes” the presence state to all the other subscribing clients, letting each user know when another user is available on the network—even if the user is mobile—so that the user can be included in a call or ad hoc conference.
3. 3Com offers a suite of applications that leverage the SIP-based communications service platform. Convergence application modules include IP Telephony, IP Messaging, IP Conferencing, and IP Contact Center. As a result of abstracting these applications from the communications layer through IP and SIP-based communications services, these applications are not dependent on a particular type of network infrastructure. They run equally well on an enterprise IP, wireless LAN, or public Internet service infrastructure. All the convergence services and applications are delivered to SIP-capable clients. In addition, the 3Com Convergence Applications Suite offers a complete array of voice-over- IP (VoIP) gateways to bring non-SIP devices such as analog phones into the SIP world.
 4. While conventional telephony devices can access most of the convergence applications, including IP Telephony, IP Messaging, and IP Conferencing, certain

⁵ Note that the services may also be optionally administered locally in each enterprise location, or in regional enterprise locations.

services provided by 3Com convergence applications require a rich user interface. For example, 3Com IP conferencing provides a data sharing capability that allows two users in conference to have shared access to each other's screens, desktop applications, or files. This type of service requires a user interface that is

beyond the capabilities of conventional telephony devices. To enable access to such application services, 3Com offers Convergence Center Client software that can be ported to a variety of client devices, including software-downloadable IP phones, mobile SIP devices, and desktop and laptop computers.

3Com SIP-Capable Firewalls to Enable Tethered IP Mobility

As just indicated, 3Com SIP-based convergence architecture allows portability of users' identity to different devices and mobility from one device to another. These capabilities are useful in a variety of scenarios such as the following:

- An enterprise user traveling to a different corporate location, even an international location, can log his or her identity (e.g. telephone number) to a temporary device that can receive or place calls.
- An enterprise user staying at a hotel can connect to the enterprise network and log an identity using a convergence center client to receive or place calls.
- An enterprise user working at home can connect to the enterprise network, log in through an IP phone or convergence center client, and receive or place calls.

The first scenario is enabled by authentication and registration (note that this is commonly known as registrar in SIP parlance) services provided by the 3Com communications services layer. In addition to the authentication and registration services, the latter two scenarios require a secure infrastructure to enable remote communications with a mobile user.

The conventional way to provide remote access for mobility is to use virtual private networks (VPNs). VPNs offer authenticated and encrypted access to the enterprise network, so the user is virtually inside the enterprise network and has access to all of the enterprise resources that the user would normally access while on site. Because VPNs consume significant processing and network resources, encrypt data, and expose all the resources within the enterprise network to the VPN user, they are typically reserved for on-demand access to business applications and for infrequent and short-duration connectivity.

Enterprises that want to offer Internet connectivity to convergence applications rather than the entire enterprise application

suite, long-duration connections, and frequent connectivity (such as access to IP telephony from home) require a more scalable and cost-effective solution than a conventional VPN can provide.

A more appropriate solution is to access the convergence applications without VPNs and restrict such connections to the enterprise convergence suite whenever the Internet connection is available. However, direct access for Internet-based clients and SIP devices to the enterprise network is prohibited in most enterprises, since firewalls are typically configured to block traffic that attempts to open ports and enter the network. Traffic from outside the corporation is generally restricted to a few selected addresses and a few selected ports that are not widely publicized. The rest of the traffic is restricted to resources in the DMZ.

As a result, remote users who inherit dynamic addresses through DHCP cannot connect to convergence applications located inside the corporate network, including IP telephony services. Yet opening up the firewall for convergence application traffic is tantamount to an open invitation for denial-of-service attacks and infiltration of the corporate network by hackers.

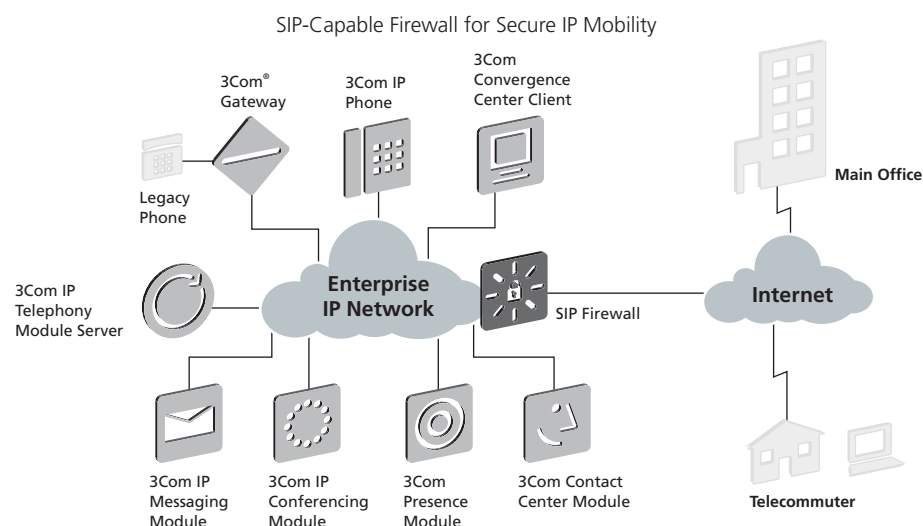
To solve this security issue, 3Com offers a SIP-capable firewall. As shown in the figure on the following page, a SIP firewall resides at the border of the enterprise network and monitors VoIP signaling protocols such as SIP registration and session establishment arriving from the Internet. It intelligently assigns and memorizes end-point addresses so they can be used statefully for real-time traffic within the context of a session. The SIP firewall also acts as a SIP proxy while enabling SIP sessions through the firewall, executing the following steps:

1. SIP signaling comes in on a dedicated port (usually 5060) at the firewall.

2. The SIP registrar (registration service) is consulted to determine the private address at which the recipient is located, and the signaling is passed on to the recipient.
3. Once the two clients have agreement that they want to set up a session, the firewall dynamically opens UDP ports, with the port numbers agreed upon during setup.
4. The firewall allows media traffic through the ports opened during the session.

SIP firewalls offer the following benefits:

- Protection of convergence applications from intruders and denial-of-service attackers at the firewall
- Control of call admission into the IP telephony system
- Concealment of the internal address space from the public Internet
- Support of VoIP-optimized and VoIP-protocol-cognizant network address translation services



3Com Wireless Infrastructure to Enable Secure and Non-disruptive Roaming

Most enterprise networks are optimized for users who work at fixed locations. Such static optimizations are achieved by configuring the user as a part of a virtual LAN or IP subnet. In addition, user privileges are configured into access control lists (ACL) on router and switch ports in fixed locations such as wiring closets and the data center. As users roam through wireless LANs, they will come within the radio coverage of an access point that is attached to a different port on a different switch and router subnet than their home subnet (subnet on which they are configured), VLAN, or router and switch ports. This creates challenges in terms of security and disruption to continuous communication.

As part of the 3Com Wireless LAN Mobility System, 3Com offers wireless LAN switches with 3Com Wireless Switch Manager software to centrally manage and control 3Com wireless LAN Managed Access Points (MAPs). The switch manager enables central MAP configuration and optimization of radio-frequency (RF) coverage and performance. These wireless solutions help secure the enterprise

network from intruders while providing continuous communications.

Secure Access to Network Services. Rogue access points and rogue users are a major security concern in enterprise wireless LANs. It is not uncommon for enterprise users to introduce access points inside the network that are not authorized by IT. Methods of controlling unauthorized access include sweeping the enterprise manually to detect rogue access points, and using packet sniffers to analyze Layer 1 and Layer 2 information to detect packets transmitted by rogue access points. 3Com Wireless Switch Manager software provides scheduled or on-demand RF scans to identify unauthorized access points and ad-hoc networks. It then alerts the central IT staff of anomaly in the network. Dedicated access points can continually sweep the airspace for 24/7 protection in environments that require rigorous security.

3Com also recognizes that controlling rogue access points alone is not sufficient for optimum security. Sometimes, it is the rogue

user who represents a security threat and the rogue access point is merely one of the enablers. A rogue user may use several techniques, including spoofing MAC address, to gain access to the corporate resources, even if the rogue access points are detected and eliminated. Therefore, controlling rogue access at the user level is just as important as discovering rogue equipment.

Another security concern is that user ACLs and permissions are typically configured as a part of a subnet according to wired IP network best practices. In order for roaming users to get access to the network resources as they roam on a wireless LAN, network permissions based on ACLs need to follow users as they roam. Without this capability, roaming users will be denied service at various segments of the enterprise wireless LANs.

To ward off rogue users and limit wireless network and network resource access to legitimate users, 3Com wireless LAN switches offer Identity-Based Networking™. This innovative capability delivers network services based on user identity instead of ports or devices. In convergence applications, 3Com SIP implementation performs authentication of users based on their IDs (such as phone number or URL). The same ID may be used by the wireless LAN switch to authenticate the user.

During the authentication process, the system learns each user's network authorization attributes such as VLAN/subnet membership, ACLs, and Mobility Profiles which may limit where the user is allowed to roam. Multiple wireless LAN switches may be grouped into a Mobility Domain™ to share user profiles and databases, supporting mobility and security

across the entire network infrastructure—including remote offices. The wireless LAN switches that form the Mobility Domain authenticate each user and enforce their network authorizations wherever they roam based on a single sign-on.

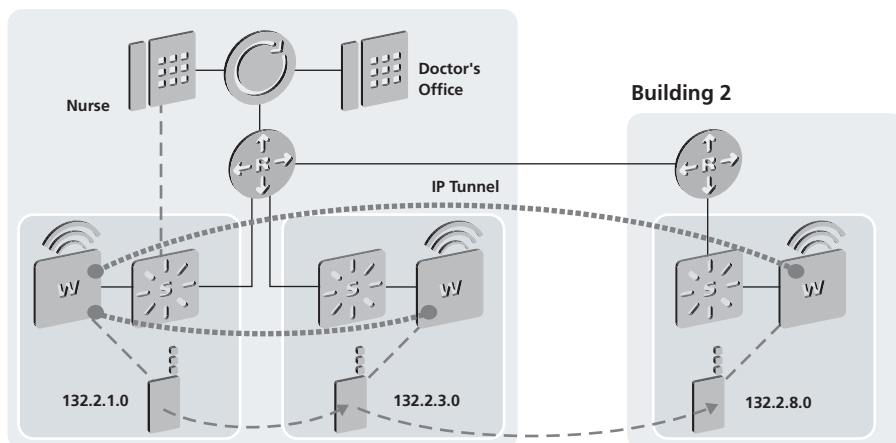
3Com Wireless Switch Manager software also monitors RF signal strengths from each user and ascertains the location of the user relative to the enterprise floor plans based on signal strengths and radio coverage of the access points. Using this capability, the switch manager can locate rogue users and prevent rogue access.

Subnet Roaming. Subnet roaming occurs when the user roams to an access point hosted by a wireless LAN switch whose network port is not directly connected to the roaming user's VLAN/subnet. Mobile devices involved in live communications, such as mobile SIP phones, may inherit IP addresses of different subnets and suffer disruption of communications, conversations, and connections. To prevent such disruptions, the 3Com Wireless LAN Mobility System supports subnet roaming with Identity-Based Networking that allows the Mobility System to enforce network authorizations based on the user's identity, even when the user roams across subnets. In addition, Identity-Based Networking provides seamless, non-disruptive switchover from one IP subnet or VLAN to another while the user is roaming between subnets. As users roam, the mobility systems allow the user to roam from one wireless LAN switch to another by leveraging Layer 2 tunneling technology.

To illustrate the ability of the 3Com Wireless LAN Mobility System to provide seamless

Hospital Campus Using the 3Com Wireless Mobility Solution

Building 1



and continuous connectivity during subnet roaming, consider the real-world healthcare scenario shown in the diagram on page 7.

- A nurse looking for a doctor would typically call the number assigned to the doctor's office phone at the doctor's desk.
- If the doctor is in the vicinity of his or her office but roaming with a wireless device in the same subnet as the office (subnet 132.2.1.0), the doctor would be reachable through the wireless LAN. If the doctor is using a SIP-compliant mobile IP device and is authenticated with the office number on the wireless SIP device, the call would be automatically routed by the 3Com SIP-based IP telephony server to the doctor's mobile device in the 132.2.1.0 subnet.
- Consider that the nurse is informing the doctor that a patient needs the doctor's attention in another part of the hospital, which is covered by a different set of wireless switch and access points and connected to a different subnet (subnet 132.2.3.0), shown in the preceding diagram in the lower right of Building 1.
- While the doctor is walking to the patient's subnet area, the nurse provides the patient's history. While in conversation with the nurse, the doctor roams into this other subnet and comes within the radio coverage of a wireless LAN switch in this subnet.
- The wireless LAN switch that detects the doctor's identity automatically searches its local Mobility Domain database of wireless LAN switches to find the home (where the doctor is permanently configured) wireless LAN switch, whose network port is directly attached to the doctor's office VLAN/subnet. Once the home wireless LAN switch is found, the wireless LAN switch hosting the roaming doctor establishes an IP tunnel to the home switch and forwards the doctor's conversation to that switch. The home switch, in turn, forwards the traffic over the SIP session that is already in progress with the nurse.
- After visiting the patient, the doctor roams to another building, located in a different subnet (132.2.8.0) within the hospital campus to consult with a specialist about the patient. When the doctor comes within the coverage of another visited wireless LAN switch located in the remote building, that switch performs the task of locating the home switch of the doctor and establishing an IP tunnel with the home switch.

- If the nurse calls the doctor about another patient, the call is automatically routed from the home switch through the IP tunnel to the visited switch located in the remote building.

This scenario is applicable in several types of environments, including airports, educational institutions, and businesses with large campuses and multiple offices.

Since the process of locating the home switch and establishing a tunnel may result in unnecessary delay and processing, 3Com wireless LAN switches multiplex multiple users' traffic on an existing tunnel, if one has already been established to support another session between the visited switch and the home switch of the user. If the roaming user is in the same subnet as the user with whom he or she is communicating and they are both within the coverage of the same wireless LAN switch, the switch short-circuits the tunnels to and from the roaming user's home switch, and switches the traffic locally without hopping multiple tunnels.

In summary, 3Com mobility solutions, together with 3Com convergence applications, offer three key benefits for roaming users:

1. Regardless of the subnet in which the user (mobile client) is defined and where the user is roaming, the client always has the same IP address.
2. Regardless of the access point with which the mobile client is associated, the wireless switch that controls the access point forwards the traffic to the appropriate wireless switch at which the client is defined. This switch, in turn delivers the traffic to the appropriate end point or application.
3. Independent of the persistent address assigned to the client, the user can register with the appropriate SIP-based communication services layer component, such as IP telephony server. When the client's enterprise number is dialed, the client can receive the call even if the user is roaming in a different state or country.

3Com Client Software to Enable Mobile Access Convergence Applications

3Com's strategy is to provide access to convergence applications from users' desktops and mobile devices. Because 3Com convergence architecture is based on SIP, desktop and mobile devices compliant with SIP (user agents) are required. 3Com offers a complete array of SIP-compliant desktop devices, including IP phones and software-based convergence clients. In addition, since SIP is becoming a widely accepted standard, several third-party vendors—such as RIM and PulverInnovations—provide SIP-compliant devices. 3Com plans to offer its own SIP devices and will work with industry leaders to offer a wide array of other SIP-compliant solutions.

Certain aspects of convergence applications, such as data sharing, need a richer user interface than the interface provided on conventional phones and mobile SIP devices. As previously mentioned, to provide access to convergence applications from desktops as well mobile devices, 3Com has implemented the user interface required for convergence applications as a hardware-independent, portable software platform, the Convergence Center Client. 3Com will work with leading mobile SIP device vendors to port this software to their platforms, so that the power of convergence applications is at users' fingertips while they roam.

3Com Convergence Services to Enable IP Mobility Across Public Domains

This discussion has focused on mobility within enterprise premises, including roaming across wireless LAN domains and access to enterprises from remote locations through the Internet. Roaming can also occur when a wireless user crosses over from an enterprise wireless LAN to the public cellular air space. Providing the ability to roam from private wireless LANs to public cellular networks and vice versa is of great interest to 3Com. 3Com recognizes, however, that this is a complex issue—not only because of the technical challenges but also because of the business and commercial concerns of the various operators involved.

To overcome these challenges, multiple independent networks—including the enterprise network, PSTN (SS7), and public cellular networks—must interoperate. In addition, the business entities responsible for these networks must collaborate though part of a highly competitive environment. Therefore, while 3Com is making significant progress in this area, especially in solving the technical issues, fulfillment of this requirement is expected to take longer than the technical solutions that are within 3Com's control.

In the interim, 3Com understands that users benefit from single-identity portability, not just within enterprise boundaries but also while they are in public wireless space. In other words, the single number at which calls are received anywhere within the enterprise

must work while the user is roaming outside the enterprise. With this in mind, 3Com offers a convergence service for routing user calls to alternate numbers, including those in public wireless domains. A user can set up a routing profile that will route all calls to the devices on which the user's unique identity is authenticated. These devices will receive the call first. Furthermore, the user profile can be set up to try other numbers in case the call attempts are not successfully completed on the authenticated device.

The capability of finding the user at numbers other than those on the authenticated devices by sequentially following the user at alternative numbers is called find me/follow me. With this capability, the user can set up a cell phone and other non-SIP-compliant phone number, (such as a home number) as a contact option.

Brandon Regional Health Authority in Manitoba, Canada, uses the find me/follow me capability to enhance its homecare services. The medical center relies on 3Com powered convergence applications to enhance both internal and public communications. The built-in find me/follow me service allows homecare workers to forward their calls to their tablet PCs equipped with a cellular communication capability and 3Com pcXset™ software. This essentially transforms the portable computers into mobile phones that work on the road and in patients' homes.

Summary

True mobility goes beyond cell phones. Enterprise-level mobility requires cost-effective network options and communication devices for access to convergence applications. 3Com takes a broad view of mobility that encompasses roaming users as well as remote users who are away from their desktops. The 3Com strategy includes identity portability to enable single-number appearances regardless of the device or the network through which the user is accessing the convergence applications and services. In addition, the strategy covers access to rich convergence applications from a variety of devices, tethered and mobile, employed by users while they are mobile.

3Com offers a variety of products architected to work together to provide true mobility. Its SIP-based convergence architecture delivers

mobility through single-identity portability. Furthermore, 3Com IP mobility solutions solve security concerns by safeguarding the border of the enterprise network from intruders on the Internet and by protecting against rogue wireless users. These solutions allow users to roam within enterprises and be continuously connected, as well as to roam outside the enterprise and be easily located through find me/follow me capabilities.

3Com offers solutions and products that deliver the full power of convergence through mobility infrastructures. By bringing about the confluence of enterprise mobility, convergence applications, and convergence clients that include mobile devices, 3Com is raising the bar for convergence networks.



3Com Corporation, Corporate Headquarters, 350 Campus Drive, Marlborough, MA 01752-3064

To learn more about 3Com solutions, visit www.3com.com. 3Com is publicly traded on NASDAQ under the symbol COMS.

The information contained in this document represents the current view of 3Com Corporation on the issues discussed as of the date of publication. Because 3Com must respond to changing market conditions, this paper should not be interpreted to be a commitment on the part of 3Com, and 3Com cannot guarantee the accuracy of any information presented after the date of publication. This document is for informational purposes only; 3Com makes no warranties, express or implied, in this document.

Copyright © 2005 3Com Corporation. All rights reserved. 3Com and the 3Com logo are registered trademarks of 3Com Corporation. Exercise Choice and pcXset are trademarks of 3Com Corporation. Identity-Based Networking and Mobility Domain are trademarks of Trapeze Networks. All other company and product names may be trademarks of their respective companies. While every effort is made to ensure the information given is accurate, 3Com does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice.

503146-001 02/05