



hp procurve
networking

january 2003



business
white paper

mobility: preparing the enterprise network

protecting investments with the hp procurve adaptive EDGE architecture

table of contents

introduction	2
the need for enterprise network mobility	2
the evolution of enterprise networks to mobility	4
the HP ProCurve mobility solution	5
the architecture supporting HP ProCurve mobility	5
how the HP ProCurve mobility solution works	6
an effective, affordable solution now and into the future	8
for more information	9

introduction

Connecting mobile users to the enterprise network, once a fairly simple piece of the network security and design puzzle, is now potentially one of the most complicated aspects of network management. Users move about in real time and, increasingly, they want their network connection to move with them. Users want mobility – the ability to send and receive data and voice seamlessly and without interruption as they move from their desk to a conference room, from building to car, office to home, or hotel to airport. With this expectation of seamless and continuous service and its need for inherent session persistence, network access and control evolves to an entirely new level. Setting up and controlling connections through static, fixed ports no longer meets users' expectations.

Network managers today address mobility either proactively by design or reactively by default. In some cases, network managers are bringing wireless access into the network in a controlled and managed way. In other cases, employees are driving adoption, deploying their own wireless or remote access devices and causing network administrators to scramble in order to manage the situation.

Whether planned or not, mobility is occurring in the enterprise network, driven by user demand. A new reality faces network management – it is no longer feasible to delay deployment of remote or wireless networking.

With the emergence of mobility, network managers and IT executives must address two concerns – the technological challenges of effectively and securely operating a mobility-competent network and the business issue of whether the return on investments made in mobility technology and operations is justified.

Mobility-related ROI varies with every industry and particularly for each business based on its unique needs. We leave it to each reader's organization to determine for itself if and when the productivity gains made possible by worker mobility generates a ROI that justifies pursuit of a mobile enterprise network.

This paper explores the need for mobility in the enterprise network and the technological issues network managers must address as mobility evolves from the realm of leading edge to the reality of mainstream use. It explains how control to the enterprise network edge can provide full support for applications today and tomorrow while providing access and mobile connectivity to services and information in an effective, secure and affordable manner.

The market research firm Yankee Group reports that more than 40 percent of workers spend less than half of their time at their primary workspace.¹ To increase productivity among these workers, as well as to obtain the related benefit of increased customer satisfaction, remote access is needed.

Today, remote network connectivity includes both wired and wireless approaches. Wired connections include point-to-point connections within a building, dial-up connectivity and secure Virtual Private Network (VPN) technology. Wireless access is simultaneously becoming more prevalent. According to market research firm Gartner Group, hardware vendors shipped nine million access points and network cards in 2001, up 150 percent over the year 2000. Gartner reports a boom in Wi-Fi™ enabled laptops, growing from 20 percent in 2001 to a projected 90+ percent by the end of 2007.²

the need for enterprise network mobility

¹ Yankee Group, as cited in FORTUNE .com, "WiFi USA," November 10, 2002, Article.

² Gartner Group, as cited in FORTUNE.com, "WiFi USA," November 10, 2002, Article.

In a similar vein, Cahners In-Stat/MDR expects the number of wireless data business users to grow from 6.6 million at the end of 2001 to more than 39 million in 2006, an increase of 600% in five short years. ³

Despite this rapidly growing demand for mobile network services, there is reluctance among network managers and administrators to install wireless or remote access to the enterprise network. Though aware of growing user demand, they either cannot justify the costs of deploying and managing a mobile network or are concerned about the potential security threat mobility could bring to their network.

In recent Giga Information Group surveys of CIOs in European Enterprises, when asked what the greatest challenge was to implementing wireless solutions, 49 percent of the responses cited the ability to justify business benefit. ⁴

This reluctance to implement wireless access can also be attributed to concerns about supporting applications requiring Quality of Service (QoS) or that can affect network bandwidth utilization. These applications require new levels of control and security as well as more sophisticated network allocation capabilities.

With a mobility-competent network, how does roaming work? How can QoS be controlled and well managed? How can network resources be effectively managed? How can real-time bandwidth allocation be handled given greater traffic volatility? Can the network be controlled and yet be flexible enough to meet users needs while staying maintaining business policies? Can a wireless network be made secure? How can the enterprise network be protected as the traditional wired edge (i.e., physical access points) blurs and blends with anytime, anywhere wireless access?

And yet, despite these questions and concerns, network managers must address the issue of mobility. Increasingly, mobile workers are demanding access to the applications that help them do their jobs. In a growing number of cases, resourceful employees set up their own wireless access points or use public gateways to gain access. This crude approach to mobility provides a minimally effective solution for the user while creating numerous problems for the network.

Until now, in terms of implementing mobility network managers have been caught between the proverbial "rock and a hard place." They could postpone adding remote or wireless access to their networks and cope reactively with the security and traffic management problems caused by employee-driven mobile access OR they could proactively implement mobile access and cope with the problems associated with high costs and less than adequate functionality. Some organizations have implemented 802.1X technology to provide wireless access. Until now, though concerns regarding security remain, 802.1X has been the most practical approach due to lower cost and availability within devices. Fortunately, new technologies are available that solve this dilemma, enabling enterprise networks to provide quality of service to users while maintaining control and security.

To meet and manage user demand, enterprise networks must initiate mobile access and services while maintaining control from the center to the edge of their network –

³ Cahner In-Stat/MDR, "Corporate Use of Wireless Data Services Continues to Grow," March 5, 2002, Press release.

⁴ In-Stat/MDR, "Managing a Mobile Workforce: Broadband Access Policies for Remote Workers," November 2002, Report.

the evolution of enterprise networks to mobility

regardless of whether the edge is physical or virtual. Mobility must enable workers to roam from location to location, across subnets with session persistence and without requiring user re-authentication. To do this, the enterprise network infrastructure must evolve toward solutions that are “always-on reliable,” easy to use, affordable and secure. The ability to provide and support technology convergence is a must, with seamless, standards-based interoperability. Organizations will need to work with reliable vendors who understand this new emerging mobile enterprise network and who have the ability to support it.

Until recently, the evolution of the enterprise network – specifically Ethernet – has been driven by the need to move files faster (10 Mbps to 100 Mbps to Gigabit to 10 Gigabit) and to do so without interference (switching). In the process, Ethernet became a truly pervasive technology worldwide in business, education and government for building increasingly cost effective and robust local area networks.

Ethernet is now moving into both new geographic domains – such as metropolitan area networks and mobile wireless connectivity – and new classes of converged applications – such as Voice over IP. This evolution is changing the enterprise network from a file and print sharing resource to a communications platform and, perhaps most important, an anytime, anywhere resource.

Each evolution-enabling innovation – such as the use of Virtual Private Networks (VPNs), common today but virtually unheard of only a few short years ago – is typically accompanied by specific technical and operational challenges that must be met if the innovation is to become viable.

Today, as the range of mobile digital appliances continues to diversify and proliferate, the integration, management and security challenges they bring with them are forcing network managers to look for new command and control solutions. Today’s wired and wireless networks are faced with the challenge of integrating new classes of applications requiring QoS, traffic conditioning and rate limiting so that all coexist on one network. And secure mobility across a range of transports both wired and wireless, inside and out of the office becomes a key element of viable mobile networks.

Maintaining the integrity of the application in a mobile environment is the next logical step as anytime, anywhere mobile access becomes more prevalent in today’s networks, and as the distinction between wired and wireless networks becomes increasingly blurred.

Today, wireless access points, with their limited view of the network edge and the network itself, serve as the point of entry for employees, guests and at times unwelcome users. These wireless access points are tasked with simple permission or denial of access control and have limited abilities in determining user access rights. They may be aware of four or five active devices at their point but are not able to manage overall traffic loads or accommodate the needs of other users on the network. This is particularly important when network resources need to be assigned or realigned to meet application or user requirements.

As the evolution to anywhere, anytime mobile computing continues, the network is extending its reach to provide mobile connectivity with local wireless technology, public high-bandwidth wireless hotspots and digital cellular. Whether a user crosses the network edge via a wireless connection or moves between wired locations becomes less

discernable and more transparent. Understanding how to maintain command from the center while pushing control to the edge is key to enabling mobility while maintaining application integrity, bandwidth allocation and network security.

the HP ProCurve mobility solution

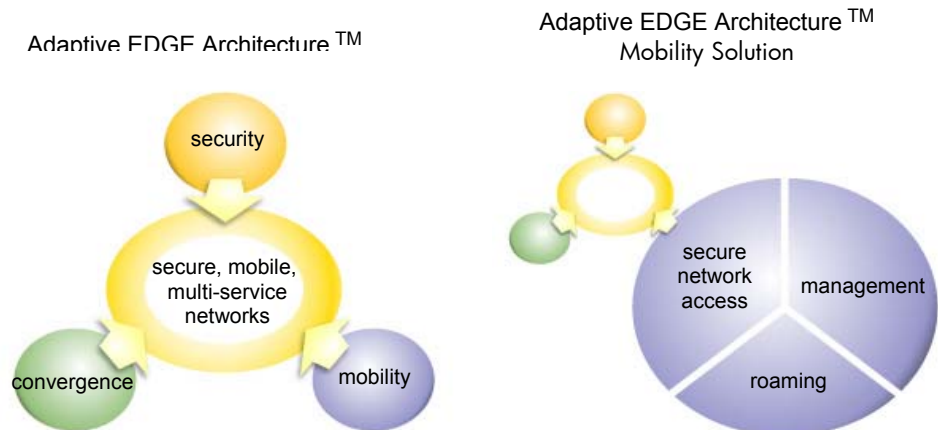
The HP ProCurve mobile networking vision is simple and yet bold – enable the enterprise network to securely provide users full mobility while maintaining QoS levels and to do so at an overall cost that is lower than industry norms.

When one closely examines the issues associated with QoS in a secure mobile environment, one realizes they can only be met with more control and functionality at the edge of the network. Security must be enforced when the user connects at the edge of the network via a wired office connection, a wireless LAN connection or from a remote location via an ISP. New applications will require quality of service, traffic conditioning and rate limiting to allow them to all coexist on one network. Such control must be established at the edge and maintained across the network. Finally, as a user moves from one location to another, the edge must preserve the connection as appropriate from wired to wireless, in the office to out of the office and back again. *Control to the edge* is the only way to offer full support for both today's and tomorrow's new applications while ensuring security and quickly providing appropriate access and mobile connectivity to services and information.

In addition to providing this control to the edge, defining who gets access to which applications, services, and information is a policy decision driven by organization, mission, business needs, job descriptions, customer profiles and more. *Control to the edge* must be paired with *command from the center* driven by business needs and priorities.

the architecture supporting HP ProCurve mobility

Addressing the concerns of network managers and administrators while meeting the needs of today's mobile workers is a fundamental principle of the HP ProCurve Networking Adaptive EDGE Architecture™. It recognizes that in the emerging enterprise network, mobility, convergence and security are related, interactive and interdependent, combining across technologies. It incorporates technologies that handle three key functions: access, control and rights. Working inside an enterprise network, these components manage, protect, and enhance how users access and use the network. And the HP ProCurve EDGE Architecture supports new security methods, new applications, and new connection management solutions for a mobile workforce.



**how the HP ProCurve
mobility solution
works**

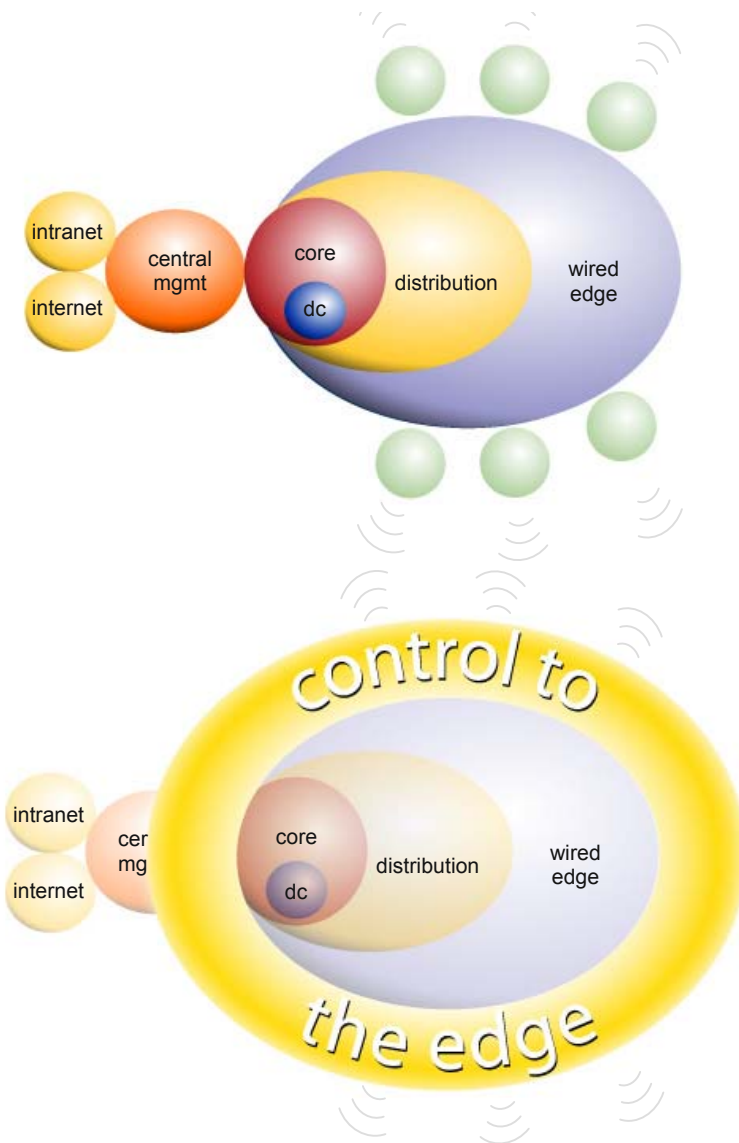
Essential to the design of the HP ProCurve Edge Architecture is the ability to take intelligence out to the edge and incorporate it at the switch. In the case of a wireless network, where an access point may have a limited view of the network edge and the devices attached to it, a “mobility-aware-switch” provides a comprehensive view of the overall network and is able to make decisions based on its broader view. Intelligent mobility-aware-switches can enforce security and bandwidth allocation policies, enable QoS when and where needed, all while maintaining session persistence as a mobile user moves across subnets.

Based on the HP ProCurve EDGE architecture, the HP ProCurve mobility solution is designed to enable a mobile user to move from one location to another, preserving the connection (potential security and productivity issues) and application (potential QoS issues) as appropriate from cable to cable or from wired to wireless, in the office to out and back again. The standards-based nature of the ProCurve solution makes it possible for network managers to implement today’s mobility solutions while also having the ability to accommodate emerging technologies. This is particularly important as network managers integrate mobility into their networks today with an eye toward the next generation networks of tomorrow.

In short, the HP ProCurve mobility solution enables businesses to roll out wireless networks with protection and management at the forefront whether for a small and focused site like a classroom or throughout an entire global organization. The architecture is designed to give network managers control at the edge of the network down to the level of who gets in and what network resources an individual is able to access, what they are allowed to do, as well as when, where and for how long they are allowed to do it. Putting the intelligence for managing mobile users at a level where the entire network’s resources can be seen helps optimize the network for mobile and stationary users/devices alike. It also lowers the overall cost of mobility as access points (by far the most prevalent device in a wireless network) require less intelligence (i.e., less complexity, less cost) as they focus entirely on their primary function: maintaining a network connection.

With the HP ProCurve mobility solution, network access is only as far away as the nearest Ethernet port. Wired and wireless connections are treated the same; each is a point on the network edge. The edge is where mobile users connect to the enterprise network and where security policies are enforced. (see the diagram, “HP ProCurve Mobility and Control to the Edge)

HP ProCurve Mobility and Control to the Edge



Only control to edge provides the robust functionality needed to support mobility in current and future application types securely. Whether the connection is remote or local, wired or wireless, HP ProCurve mobility places emphasis on a unified security scheme between the client and the network edge – before access is granted – through use of industry standards and key protocol capabilities. The HP ProCurve EDGE Architecture is designed so that authentication and control can be managed on an individual basis, redirecting and logging all network traffic generated by each wireless device, solving the problem of mobile network security.

Access managers sit between the clients and the network. All traffic between each user and the rest of the network passes through the device where policies are enforced. A control server handles wireless network control and rights-management functions. All access managers in the same domain communicate with a single control server that coordinates access and rights. Because the access managers handle all per-packet operations while the control server coordinates access to network-centric information, the architecture is extremely scalable.

The rights manager, part of the control server, takes care of authentication, user information and policies. Using its own or an external database, the rights manager directs the process for user authentication and control of client access to network resources. By connecting each access point to an access manager, the manager is able to send the MAC address of a device trying to connect to the network to the control server where user identification and rights can be confirmed and appropriate action can be taken. So rather than simply allowing or denying access, the control server tells the access manager details about the user's rights, enabling security and control to be initiated at the enterprise network edge.

Once a session has been enabled, access managers track and forward the active session from manager to manager as a user moves between locations, keeping the session live and uninterrupted. As the session is forwarded among access managers, each manager checks with the control server. In this case, where the control server has already authenticated the session, information is passed back to the access manager allowing the session to continue. This process takes place at Layer 3, allowing the user to maintain seamless connectivity anywhere in the networking across multiple subnets.

**an effective,
affordable
solution now
and into the
future**

The HP ProCurve mobility solution approach of placing greater intelligence at the switch while driving control to the network edge translates directly into a low cost of deployment and a lower total cost of ownership and operation, making it an effective and affordable solution today.

By enhancing the intelligence at the switch, and therefore reducing complexity and cost, resident in the most numerous devices on the mobile network – access points – the overall cost of mobility is greatly reduced. And rather than receiving less quality as is often the case when costs are reduced, the HP ProCurve mobility solution provides *greater* security, reliability, effectiveness and ease of use while reducing costs.

Fault-tolerant designs combine with the highest levels of integration, from switches to access devices and beyond, to ensure HP's renowned commitment to quality and reliability. Mobile access approaches use plug and play designs, policy-based management schemes and QoS for simplicity of deployment and use.

And HP's ongoing commitment to and support of evolving industry standards ensures that the mobility solution implemented today will remain viable for years in the future. The investment made in mobility today, at its lowered cost of deployment, will result in greater than typical returns as its useful life extends – due to its ability to evolve with emerging technologies and equipment – well beyond traditional timeframes.

**for more
information**

More information about HP ProCurve Adaptive EDGE Architecture is available at <http://www.hp.com/rnd/architecture>.

More information about HP ProCurve networking solutions and products is available at <http://www.hp.com/go/hpProCurve>.

HP is a leading global provider of products, technologies, solutions and services to consumers and businesses. The company's offerings span IT infrastructure, personal computing and access devices, global services and imaging and printing. HP completed its merger transaction involving Compaq Computer Corp. on May 3, 2002. More information about HP is available at <http://www.hp.com>.