

# Improving connections for mobile workers

White paper

## Executive summary

To increase productivity and customer service, businesses are increasingly moving critical computing applications to mobile users. This shift to mobile computing introduces significant challenges. Compromises in security, productivity, and reliable remote connections can occur if mobile connections are improperly implemented. In addition, technologies deployed for improving connections for mobile workers must provide a long-term infrastructure that is flexible enough to grow and adapt to changing business demands. This paper examines these challenges and offers significant solutions for improving mobile connectivity.

## Introduction

The world's mobile workforce is growing faster than any other segment in the industry. According to analyst reports, spending on mobile devices and mobile applications will grow at a rate of more than 20-percent per year through 2011.<sup>1</sup> A need to stay close to customers and keep workers in touch is driving this growth. Not surprisingly, the major mobile applications used are e-mail and SMS/text messaging. However, project management, customer relationship management (CRM), collaboration, and file sharing applications are becoming increasingly popular outside the walls of the enterprise as companies see real profit in delivering customer service, order entry, and other business functions to the customer's door. This increase in mobile activity creates a significant management challenge for a company's IT department.

Businesses have managed laptops and notebooks in the field for decades, but the new mobile business model adds challenging performance and security issues into the mix. Because of the power and flexibility of laptop computers, full-featured CRM and software-as-a-service (SaaS) applications can be routinely delivered to the field, transforming the typical mobile worker into the equivalent of a virtual branch office. While this mobility can tremendously boost the bottom line, maintaining peak employee performance requires regular, reliable connections to network services – either wirelessly or over a cellular carrier network.

The latest innovation in the mobile workforce is the use of handheld, PDA, and smartphone computers. For example, order entry and customer service applications were once confined to laptop computers. Today's handheld devices are powerful enough to provide client-server computing. Windows Mobile, Symbian, and Mobile Linux operating systems can run full-featured client applications over cellular, WiFi, and new 3G networks, connecting these remote applications to enterprise resources.

From laptops to handhelds, any organization can benefit from mobile applications. But according to many industry analysts, if the underlying infrastructure of mobile computing is not sound, delivering a productive business environment into the field becomes a severe problem. "Vendors and organizations alike must recognize that mobile enterprise solutions are not just about mobilizing a particular application," said Stephen Drake,

<sup>1</sup> Compass Intelligence. "U.S. Mobile Applications Market Expected to Reach \$9 Billion by 2011." Scottsdale, AZ, May 30, 2007.

The main goals of moving workers into the field are to bring them closer to customers and to enhance their productivity. If the performance of mobile applications frustrates this goal in any way, the enterprise stands to lose more than the outlay for devices and software.

program director for IDC mobile enterprise research. “Organizations should seek out suppliers that offer robust underlying infrastructure to support the applications and provide enterprise-grade scalability for future expansion.”<sup>2</sup>

## The challenges of improving the connections of mobile workers

The most critical infrastructure challenges for enterprises implementing a long-term mobile workforce are maintaining optimal bandwidth, ensuring reliable connections, and securing data from client to server and at all intermediate points. Problems in these key areas affect worker productivity, the quality of work, and the security and integrity of the company’s data.

### Bandwidth

Top of mind for remote workers is the performance of their mobile applications. While the computing devices may be up to the tasks assigned to them, the network infrastructure that these applications must use to communicate may be less than optimal. Wireless Ethernet 802.11 – in all its variations – is the most commonly used connection for mobile workers. Theoretical limits may claim transmission speeds of more than 100 Mbps, but this ideal is rarely achieved. Depending on interference with other devices, the distance from the access point, and environmental factors as diverse as weather and light fixtures, wireless Ethernet connections typically achieve only 10- to 70- percent of their rated bandwidth. Most connections average about 50-percent of the rated speed. Intermittent dead zones and slow spots are common.

The most frequent culprit in slower-than-advertised wireless Ethernet speeds, however, is the technology itself. Although wired LAN computers are on segmented and routed lines, wireless computers are unaware of other traffic on the network and must behave accordingly. Using a protocol called Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), wireless traffic must first ask permission to transmit and wait for a response before actually sending data packets. Combining this inherent inefficiency with other environmental factors degrades wireless Ethernet performance. Many transaction-based applications running over these degraded network conditions can timeout in the worst conditions.

CDMA, GSM, and even the new 3G and 4G cellular networks are subject to many of the same environmental and technological limitations as wireless Ethernet, including collision avoidance. An additional factor complicating cellular-based network communications for field workers is moving between cell coverage areas, which necessitates a handover of the signal. In cells with heavy usage, performance can degrade significantly. In addition, carriers may set arbitrary bandwidth restrictions on cell users, often without notification, to reduce congestion and discourage heavy data transmissions – precisely the opposite of what corporate mobile workers need and demand to perform their jobs.

### Data integrity and reliable connections

Both cellular and wireless Ethernet networks are susceptible to unexpected dropouts and transmission errors for many of the reasons already stated. While advanced error correction and buffering solutions have improved reliability for both technologies over the last few years, dropouts and lost connections remain common. Most client-server applications must be written to prioritize either bandwidth performance or error correction,

“Vendors and organizations alike must recognize that mobile enterprise solutions are not just about mobilizing a particular application. Organizations should seek out suppliers that offer robust underlying infrastructure to support the applications and provide enterprise-grade scalability for future expansion.”

— Stephen Drake, program director for IDC mobile enterprise research

<sup>2</sup> Jaques, Robert. “Mobile Application Market Set for Stellar Growth”. London, December 14, 2006.

typically resulting in tradeoffs. For example, ensuring data integrity during transmission may impact the performance of the application, while optimizing data transfer speeds may introduce a greater likelihood of data corruption.

When wireless devices hand over signals, the original connection is cut, and a new signal is established. Most of the time, this handover – through buffering of data – is accomplished seamlessly, but many times the signal is lost entirely. Similar drops can occur when wireless Ethernet workers move from one access point to another. In such cases, long data transmissions may need to restart entirely to assure data integrity. The client-server applications themselves may time out and need to be restarted. In some cases, data is corrupted on the mobile device, or even on the enterprise server.

## Productivity

For the reasons stated above, mobile workers are susceptible to application restarts, potential data corruption, and slow connection speeds. All of these conditions result in lower productivity. But more importantly, these particular performance issues shake the confidence of the mobile worker. Many workers use such applications less frequently or rely on redundant procedures to ensure their work is safely accomplished. In extreme cases, workers may abandon the use of the application entirely. Therefore, ensuring bandwidth and data integrity is essential, not only from an information infrastructure standpoint, but also from an employee and customer productivity perspective.

Customers, in particular, may suffer as mobile outages or poor performance complicate or miscalculate an order from mobile representatives. These poor field transactions can damage the bottom line and the company's reputation. The main goals of moving workers into the field are to bring them closer to customers and to enhance their productivity. If the performance of mobile applications frustrates this goal in any way, the enterprise stands to lose more than the outlay for devices and software.

## Security

The business benefits of increasing the presence of mobile workers is well documented, but some companies are leery of exchanging sensitive data over mobile applications. Many companies must adhere to strict legal and regulatory mandates for protecting information. Mobile computing adds an additional layer of insecurity to business computing as data moves beyond the confines of enterprise firewalls to public networks.

Wireless Ethernet poses various security vulnerabilities that corporations must address. For example, many installations may not provide even the basic 802.11 Wired Equivalent Privacy (WEP), especially when employees access data in airline terminals, at coffee houses, or through home-based networks. As numerous security research studies have shown, onsite wireless networks deploying WEP are also vulnerable.<sup>3</sup> Because wireless carriers are susceptible to the same forms of data hijacking, data is at risk over cellular networks as well.

Many companies ensure data security for mobile applications by creating custom encryption techniques for these applications. This may provide complete control over the security process, but may also add additional overhead to the application. These custom solutions may also be expensive and time-consuming to implement.

<sup>3</sup> Borisov, Goldberg and Wagner. "Intercepting Mobile Communications: The Insecurities of 802.11." Seventh Annual International Conference on Mobile Computing and Networking. Berkeley: University of California at Berkeley, 2001. 9.

Web-based mobile client applications can use the built-in Secure Socket Layer (SSL) feature when communicating with server applications, but few developers acknowledge that SSL data – while secure when encapsulated – is vulnerable once the SSL packet is unencrypted and at rest on the servers at the edge of the enterprise. Security experts and hackers have documented numerous other flaws in SSL implementation across many operating systems and browsers over the years. While patches and fixes are quickly issued, future vulnerabilities are difficult to predict. For these reasons, many companies combine SSL with other security measures.

### The Circadence® solution for mobile workers

Founded in 1993, Circadence focuses on developing products for WAN security and performance. The Circadence MVO™ 1200 WAN Optimization suite, the core of the company's technology, can be deployed in software, hardware, and integrated application configurations. The Circadence MVO 1200 WAN Optimization suite provides optimal bandwidth, resilient WAN connections, and U.S. Department of Defense (DoD)-grade security as a foundation for building mobile applications.

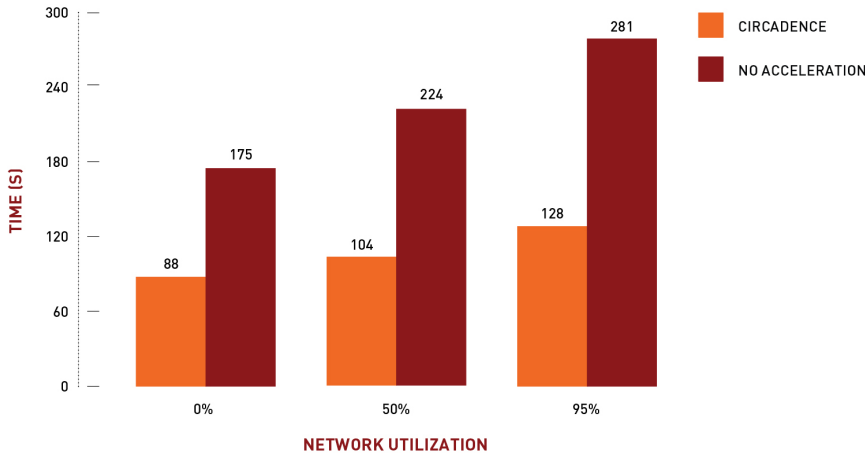
The core technology used in the Circadence MVO 1200 WAN Optimization suite is Circadence's patented optimization protocol. The algorithms in Circadence's protocol offer the dual functions of providing accelerated and uninterrupted WAN connections. In addition, Circadence has worked closely with government and defense clients over its more than 15-year history to incorporate the most sophisticated security features into its optimization protocol.

### Circadence performance

In independent tests, a leading enterprise database developer recently quantified throughput gains when using Circadence MVO products with mobile and wireless laptop devices. Using a mobile field service test scenario, the vendor ran a suite of field service applications over standard and Circadence MVO-enabled wireless connections. The application test bed performed a new customer service request, a service request update, and four other field application operations. To simulate real-world network traffic conditions, the test bed also introduced network congestion to simulate zero to moderate (50-percent) to high (95-percent) network utilization. The results were consistent. Throughput using Circadence MVO was exactly double that of a standard connection in a zero network utilization environment. When operating in a moderately congested environment, Circadence MVO performance was 108-percent better than a standard wireless connection. Even in highly congested simulations, Circadence MVO-enabled connections provided 110-percent higher throughput than a standard wireless network. Figure 1 compares Circadence MVO performance to the non-accelerated network.

Figure 1

FIELD SERVICE APPLICATION TIMES COMPARED

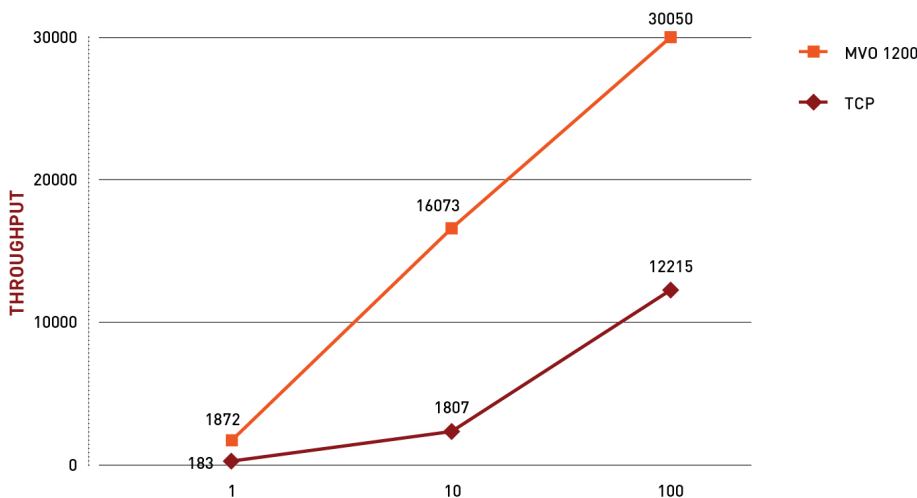


A nationwide cellular carrier also performed similar tests over its CDMA network and showed even more dramatic results. In this scenario, a standard laptop using a peripheral card connected to the CDMA network was used to access a series of web pages. The test bed ran both standard TCP and Circadence MVO-accelerated connections. During the test, CDMA-connected laptops accessed websites one at a time. As the test progressed the Circadence MVO-enabled laptops showed increased efficiency in rendering the sites with access times double that of un-accelerated TCP connections. Figure 2 shows the results of these tests over the CDMA cell network.

Whether over standard wireless 802.11 or public cellular networks, the Circadence MVO 1200 WAN Optimization suite improves performance of any data application by tunneling through TCP network congestion.

Figure 2

CDMA DATA THROUGHPUT ON STANDARD TCP VERSES



## Resilient connection

In addition to performance increases, Circadence's protocol maintains a patented resilient connection from point-to-point in the WAN session, even if cell or wireless carriers drop signals. Link Resilience™ combines efficient tunneling with superior buffering to maintain connections over spotty networks or during dropped signals. As a result, fewer data streams are interrupted or halted, and applications sensitive to timeouts remain running. Link Resilience maintained application data continuity during WAN tests of dropped connections. When the signal resumed, the data application did not know the connection had been lost. The amount of time to keep the connection alive for applications is decided by the Circadence MVO user and is configurable. In a standard TCP environment, the timeout is determined by router defaults. This persistent connection ensures data integrity, prevents costly restarts and retries over the network, and improves both application and mobile worker productivity. Links over cellular networks are similarly protected from intermittent outages.

## Security

Circadence has a long history of working with the most demanding security-conscious customers. The algorithms deployed in its patented protocol meet or exceed the standards of the DoD for providing secure connections. In addition, Circadence MVO connections are secured from point-to-point, unlike SSL security that is shed at the gateway server decryption point. Mobile applications can use SSL, however, in conjunction with Circadence MVO products to provide an even greater layer of protection. Tests confirm that no degradation in acceleration occurs when SSL is used in tandem with the Circadence MVO 1200 WAN Optimization suite.

## Flexibility of deployment

Circadence MVO technology is available in numerous configurations to provide the greatest flexibility to meet the needs of mobile workers and the company. The Circadence MVO 1200 WAN Optimization suite accelerates and secures WAN connections for mobile workers and includes:

- **Circadence MVO Software suite** – As a software-only product, the Circadence MVO Software suite can be installed on client devices and application servers. This package supports Windows and Linux, and is portable to almost any POSIX-compliant operating system.
- **Circadence MVO Appliance** – The Circadence MVO Appliance is a hardware-based router that sits at the enterprise edge to connect and manage a collection of mobile or public network connections. This solution not only centralizes Circadence MVO connections, but also ensures survivability during denial-of-service attacks. The Circadence MVO Appliance is DoD-certified for classified installations.
- **Virtual Circadence MVO** – The Virtual Circadence MVO enables enterprise administrators to embed Circadence MVO technology into virtualized server applications and operating systems. This solution provides support for Oracle VM, VMware, Microsoft Virtual Server, Xen, and other virtualization solutions, and can serve as a virtual gateway.
- **Circadence MVO Windows Client** – Operating as agent software on a Windows PC or server, this Circadence MVO client enables companies to install client and server-side peer-to-peer or client-server Circadence MVO configurations. The software requires slim resources and is transparent to the user.
- **Circadence MVO Mobile** – Circadence MVO optimization is available for Windows Mobile, Symbian, and Mobile Linux devices on secure digital (SD), USB, and compact flash (CF) cards. SaaS applications for mobile workforces can be securely delivered and reliably connected.

Circadence MVO components can be mixed and matched to provide a complete mobile computing infrastructure. Because all components are modular, the system can adapt as the needs of mobile applications grow. The Circadence MVO 1200 WAN Optimization suite does not require modifications to a company's existing network infrastructure, thereby reducing the cost of mobile computing integration.

## Conclusion

Performance, the resilience of network connections, and the security of mobile data are all factors in creating a successful and productive mobile work environment. When mobile employees see gains in productivity and customer satisfaction from using well-designed mobile applications, customers and the enterprise both benefit. Companies need to ensure that actual mobile applications are not only a boost to their organizations, but also that the underlying network infrastructure is fast, resilient, and secure. Circadence provides a flexible, cost-effective, and nearly non-invasive solution for improving connections for mobile workers.

## About Circadence

Since 1993, Circadence has leveraged the power of advanced technologies to pioneer smarter, faster, and more cost-effective solutions for improving IT performance. What started with an innovative platform for making massively multiplayer online games run faster has quickly grown into the most capable suite of optimization solutions available. Based in Boulder, Colorado, Circadence continues to expand today's possibilities with tomorrow's technologies – addressing new, growing concerns with dynamic, high-performance solutions. Only Circadence offers the most capable IT innovation solutions available – proven to outperform some of the world's most demanding challenges. For more information on Circadence, visit [www.circadence.com](http://www.circadence.com).

© 2010 Circadence. All rights reserved. Circadence, the Circadence logo, "Technology powered by tomorrow," Circadence MVO and Link Resilience are trademarks or registered trademarks of Circadence in the U.S. and in other countries. All other trademarks referenced in this document are the property of their respective owners.