NetMotion® WIRELESS

MOBILE SESSION PERSISTENCE

What It Is, Why It Matters, and How It Works

Executive Summary

Mobile computing delivers higher productivity, but achieving the full benefit requires a user experience that matches an "in-the-office" experience. Unlike wired networks, however, wireless networks are not continuously available. The ability to deliver applications reliably over those unreliable networks is termed "persistence."

Makers of Virtual Private Network (VPN) software use different approaches to achieving persistence, but only a *mobile* VPN that offers full application session persistence can duplicate what computer users experience in the office.

A Wired-Network Experience for Mobile Workers

Mobile computing promises increased productivity by giving workers in the field access to the same applications they use in the office. Key to this "in the office" experience is reliable application performance over the wireless WAN. However, compared to high-speed Ethernet networks, wireless WANs transmit data at slower speeds, with higher error rates, higher latency, and more jitter.

Roaming mobile devices have constantly changing IP addresses, which can affect worker productivity.

As a mobile device roams from network to network, its IP address changes. And as it moves through coverage gaps it is only intermittently available.

Line-of-business applications that are not specifically designed for a mobile environment become unstable, resulting in lost or corrupt data and ultimately decreasing the productivity of the mobile workforce. The ability of an application or technology to overcome these differences and enable the reliable transmission of application data over unreliable networks is referred to as "persistence."
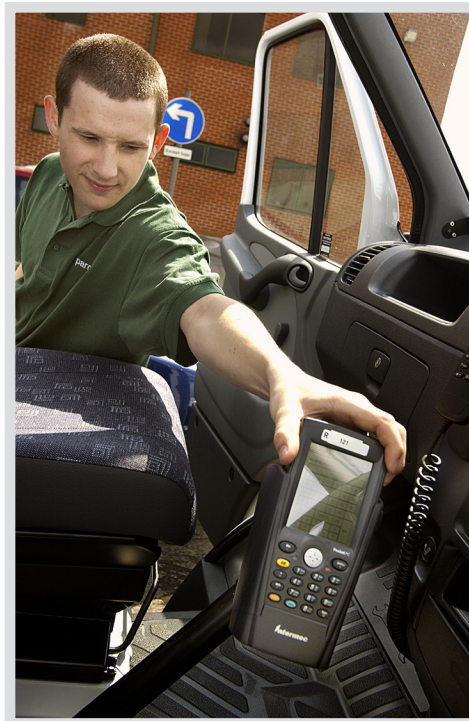
Definitions of Persistence

Many VPN vendors talk about "persistence," and there are three basic ways in which the term is used when describing a mobile VPN. Each approach has its value, but only application session persistence maintains the in-office experience mobile workers require to be productive. The three basic approaches are:

1. Persistence of Browser Sessions

Browser-session persistence is applicable to browser-based SSL VPNs. This approach is similar to e-commerce applications that remember the contents of a shopping cart between visits. It works by setting session cookies in the browser so that if users close their browsers or they go to another Web site, they can resume VPN sessions by simply returning to the SSL gateway.

Persistence of this type is limited to applications available through a Web portal; it does nothing to address the needs of organizations that deploy more sophisticated line-of-business applications.

2. Persistence of an IP Address

IP-address persistence is typically enabled by protocols such as MobileIP. It solves a fundamental VPN routing problem: how can traffic be sent to a remote client when that client roams from network to network and the client's real IP address changes? While the persistence of an IP address solves a routing issue, it does nothing to preserve the integrity of data being sent as those addresses change, nor does it solve the problems associated with gaps in network coverage and performance issues that are common in even the most robust wireless networks.

3. Persistence of Application Sessions

Application-session persistence shields applications from changes in the network environment by intercepting network calls and proxying those calls through a dedicated server on the core network. With this approach, application-session state and data integrity are maintained through address changes, network coverage gaps, and suspend-resume cycles without any modification to existing applications or reduction in functionality.

Real Results:

Grange Insurance Speeds Claims Processing

Grange adjusters use Mobility XE as the foundation for accessing claims, estimating applications, and uploading photographs while in the field.

" Our mobile claims associates need a stable and reliable environment with constant access to their applications. With NetMotion, we are able to ensure our consistent performance—in and out of coverage areas. "

—Butch Knowlton,
Manager of Claims Projects &
Business Analysis

JEA Achieves 30% Productivity Increase

JEA field workers spent a lot of time trying to re-connect as they moved from location to location. Once they deployed Mobility XE, the disconnect problems disappeared. Workers log in one time at the start of their session and remain connected throughout the workday. The utility noted a 30% productivity increase and more home service orders completed.

" Maintaining a persistent connection lets JEA workers get more work accomplished and greatly reduces the complexity of mobile computing. "

—Bonnie Anderson,
Systems Administrator

Why Persistence Matters

Through real user scenarios, the value of application session persistence over other approaches is clear. Application session persistence replicates the in-office experience; without it, the workday is spent working around limitations.

What happens to my applications if I roam outside of network coverage?

Application Performance Outside of Coverage	
Application Session Persistence (with Mobility XE Mobile VPN)	• Your IP-based applications automatically resume where they left off as soon as you come in range of network coverage, even if the application was using network resources at the moment you went out of range, or if you were out of range for an extended period of time.
Browser Session Persistence	• You must re-authenticate to the SSL gateway. Only applications hosted on a web server resume where they left off.
IP Address Persistence	• Data transfer between client and server stops when the network coverage goes away. The data in transit at that time is lost, and the application requires a restart.

What happens if I suspend or hibernate my device during data transfers?

Suspend During Data Transfer	
Application Session Persistence (with Mobility XE Mobile VPN)	• When you resume, any IP-based application automatically picks up where it left off before you suspended the device, even if the application was using network resources when you suspended or hibernated.
Browser Session Persistence	• The data transfer fails and must be restarted.
IP Address Persistence	• The data transfer fails and must be restarted.

How long will my applications persist when I'm outside of coverage?

Application Persistence Outside of Coverage	
Application Session Persistence (with Mobility XE Mobile VPN)	• Your IP-based applications can persist indefinitely, although some network operating systems and applications have session timeouts that prevent indefinite persistence. • (By default, Mobility XE maintains application sessions for several days.)
Browser Session Persistence	• Applications persist only as long as the browser session cookie is valid.
IP Address Persistence	• Applications persist only until either the client or the server attempts to make a network connection. At that point the exact behavior depends on the application itself; most become unresponsive while waiting for an answer from a resource that is no longer connected and require restarting.

Mobility XE Mobile VPN

The Mobility XE® Mobile VPN from NetMotion Wireless is a solution for session persistence. It persists connections through the many situations that interrupt connectivity in a mobile environment, while working with any application.

The Mobility XE mobile VPN moves beyond the basic functionality provided by browser session persistence and Mobile IP. It sustains application sessions even through no-coverage zones, suspend-and-resume cycles, changes in network types (for example, from WWAN to WiMAX to WiFi), and the losses of connectivity inherent in mobile computing.

When a Mobility XE user encounters a coverage gap, open application sessions are maintained until the user's network connection is re-established. If a user loses connectivity while an application is transmitting data, Mobility XE suspends the transmission — for days, if necessary. As soon as connectivity is re-established, Mobility XE resumes transmitting the data at the exact point the application was interrupted. Other VPNs in these situations lose application sessions, causing data loss and corruption, and force users to log on again and restart applications.

How Mobility XE Achieves Persistence

Instead of connecting directly with the application servers on the host network, mobile devices running the Mobility client communicate through the Mobility server. The server proxies the connections, maintains the state of each client, and whenever the client is unreachable it holds any pending data for later transmission. The Mobility server also handles the translation between the fixed virtual IP address that identifies the client on the host network, and the point-of-presence IP address that changes as the client roams between various networks.

When a device loses contact with the network, the Mobility XE client works transparently with the operating system on the mobile device to keep client-side application sessions active. The Mobility client and Mobility server keep the secure VPN tunnel alive, by mutual agreement, unless one issues a disconnect. Meanwhile, the Mobility server and application servers on the host network exchange acknowledgements with each other. This keeps the application session alive and preserves the state of any transactions. When the client comes back in range, any interrupted data transfer resumes.

The tunnel remains available and application sessions persist in many different scenarios:

- Suspending operation on the mobile device and later resuming it

- Moving to a different location on the network

- Connecting a mobile device over slow, bandwidth-challenged, or high-latency networks

- Encountering interference from microwaves, stairwells, elevator shafts — anything that interferes with radio signals

- Changing network interfaces (for example, from a WLAN to a WWAN card)

- Moving across gaps in coverage

Because Mobility XE works at the operating system level, it is hidden from the applications, and applications behave as they do on a wired network. This allows off-the-shelf applications to run without modification in the wireless environment.

Conclusion

The success of any mobile VPN deployment is measured by the improved productivity of the mobile work force, and application persistence is key to achieving that success.

The persistence in Mobility XE hides the complexity of the underlying wireless networks from applications. With Mobility XE, critical business applications just work and mobile workers can get more done.

NETMOTION®
WIRELESS

www.NetMotionWireless.com

FOR MORE INFORMATION, CONTACT US:

United States
Seattle, Washington
Telephone: (206) 691-5500
Toll Free: (866) 262-7626
sales@netmotionwireless.com

Europe
Germany and France
centraleasterneurope@netmotionwireless.com

United Kingdom
northerneurope@netmotionwireless.com