StayLinked

Dropped Wireless Terminal Sessions

Understanding the pain associated with dropped wireless terminal sessions and strategies to prevent it

Situational Overview

A "dropped user session" is the result of a remote RF/Wireless terminal emulation device losing its connection to the host computer and application that it is feeding real-time bar-coded scanning information to and not being able to continue the current process when the connection is re-established.

Because of the frequency with which a connection disruption can occur, dropped user sessions are the number one problem associated with RF/Wireless 5250, 3270 and VT emulation environments. Therefore, it is very important to analyze and understand the true impact of this situation on the various entities within an enterprise when it happens.

This document focuses on detailing the types of real costs and related pain that comes from a dropped user scanning session. Also discussed in this document are strategies and methods that can be implemented to alleviate the situation and create a more reliable RF/Wireless terminal emulation environment.

Users of RF/Wireless 5250, 3270 and VT emulation solutions are typically scanning bar- coded information on materials and goods as part of the process of tracking real-time inventory movement for distribution and retail warehousing enterprises. The information from these scanning sessions is transmitted to host applications that then process the information to provide accurate and timely accounting-related reporting and records retention.

Any disruption in the process of completing an accurate bar-code scanning session will result in a delay or disruption in the process of moving inventory from one location to another and can also result in generating inaccurate accounting information.

A dropped scanning session is not only frustrating and time-consuming for the user who is performing the scanning function, but also for the various IT-related personnel that must get involved to assist with remedial action to resolve the problem. Until recently, this problematic situation has had to be tolerated by both the users and IT-related personnel due to the lack of availability of an effective solution.

What happens when a scanning session is dropped?

Scanning sessions can be dropped by the server-side host computer (IBM AS/400- iSeries, IBM Mainframe-zSeries, RS6000-pSeries, HP9000/HP-UX, Windows Server, etc.) when the connection to the client-side RF/Wireless 5250, 3270 or VT terminal device being used has been disrupted for any period of time. This can be caused by a variety of everyday client-side events including battery replacement, the user going out of access- point range with a device, as well as, a device reset or reboot.

The host server-side processes (jobs) linked to the client device scanning session become abandoned without possibility of re-linking to the client. New server-side processes will need to be established in order to accommodate the user wishing to complete the current scanning job/data collection work at hand.

IT personnel assigned to controlling active processes on the host computer must get involved to identify and delete the abandoned sessions from the system. It is often quite time consuming to identify precisely which process (or processes) are the exact ones tied to the dropped user scanning session. Without host-centric features like "Device Naming", all scanning sessions on the host look the same and there are no indicators that identify processes abandoned this way.

The abandoned process continues to live/run, except it is no longer receiving data from the client device and will not again. Because starting a new client device scanning session will be required, the process that has been abandoned on the host will not be the one the new client-side session will establish contact with. Rather, the new client device session, once started, will spawn a request for a new corresponding server-side process to send its scanning data to.

Further complication for the IT staff is generated from the need to "clean up" behind an abandoned session on the host and preserve the integrity of the data acquisition application and related database records. For example, if a scanning job was partially complete at the time of the disruption, the user may elect to start a new session to re- do the job from the beginning to make sure all items are scanned completely. The partially completed job entries must be located and backed out of the database to avoid duplication and resulting errors.

Another alternative is an equally tedious process that requires the user to confirm with someone on the IT side as to exactly which scanned items in the job were received correctly prior to the disruption. This needs to happen if they wish to determine where to resume the job from in a new session versus starting the job over from the beginning.

In either case, IT staff members must also clear certain "in use" application flags associated with the abandoned process. An application may be licensed according to the maximum number of simultaneous users and an abandoned process left "in use" will register as an active user to the system for licensed access control purposes until it is stopped.

In addition to users having to coordinate in real-time with IT staff members to deal with the dropped session and know where to pick up the process from, they are also impacted negatively by having to start a new client session on their end. To start a new session on the client-side, a user must go through the time-consuming process of signing on to the host computer gain. They must also call up and re-start the appropriate scanning application, and navigate to

the appropriate point in the application where they left off. This is possible only if they were able to determine the exact point with certainty at all.

The bottom line is that all of the time and resources expended to get a user back on their way with the scanning job at hand when a dropped session occurs is 100% un- productive and takes all entities involved away from other important tasks in a reactionary and unplanned manner.

What are the costs associated with dropped scanning sessions?

In tangible terms, the following formula can provide a measurement of lost productivity costs associated with each incident, assuming the associated labor rates for the user and IT staff members involved is made available:

Time to resolve X (IT staff combined labor rate + Scanning user labor rate)

To appreciate the full impact of this situation, it is important to also consider the frequency with which a dropped scanning session is experienced on a daily basis. It is not uncommon for dropped sessions to occur several times in a day for various users if there is no mechanism in place to prevent them from happening.

Therefore, let us consider the following example using some conservative arbitrary numbers to illustrate the potential hard costs that can be realized from these productivity losses:

Assumptions for the example:

a) Average IT staff combined labor rate is $75.00 per hour

b) Average Scanning user labor rate is $25.00 per hour

c) Dropped scanning session problem-resolution time average is 15 minutes

d) Dropped scanning sessions occur 5 times per day per 25-30 wireless user facility as an average

15 mins. (0.25 hrs) X ($75.00 + $25.00) = $25.00 per X 5 =

Daily = $125.00 per facility

Weekly = $625.00

Monthly = $2,500.00

Annually = $30,000.00 per facility

It is important to note that the example we are using here to illustrate hard costs is very conservative. Large enterprises experience a greater frequency of dropped session incidents based on larger numbers of simultaneously active scanning client users.

In addition to the pure costs associated with productivity losses, other potentially costly aspects associated to this situation and the resulting delays in inventory movement include missed shipping deadlines to customers, lack of available material for steps in a manufacturing process, warehouse location crowding as new material arrives for the same space, as well as a multitude of other factors impacting physical inventory logistics.

How can dropped RF/Wireless terminal sessions be prevented?

Traditionally, RF/Wireless terminal emulation products and solutions have been based on using software that resides on the wireless device (client-side) that provide an interface for display sessions to connect with a generic Telnet service on the host. The problem with this approach of performing the emulation on the client side is that the environment that the emulation software must operate within is inherently more unstable than the application host and prone to unplanned outages.

All of the events previously mentioned in this document that can cause a disruption in a scanning session (battery replacement, the user going out of access-point range with a device, a device reset or reboot, etc.) are all part of the client device environment and out of the client-resident terminal emulation software solution's control.

Therefore, deploying terminal emulation software on the client side of the wireless connection does not offer the opportunity to create a solution to prevent the dropped (or abandoned) session condition. This reality is one of the key drivers that has motivated software solution providers to adopt more server-based solution architectures today that feature very thin client software functionality. This is done to lessen the impact of unexpected client-side events on the integrity of the overall connectivity solution. Unfortunately, some of those solutions feature a PC gateway server between the client devices and the target host, which creates a single-point-of-failure.

The AS/400-iSeries host-computing environment, as an example of a highly-reliable host platform, is one of the most stable application run-time environments being used by enterprises today. Users of the AS/400-iSeries server platform experience industry leading reliability/up-time metrics of 99.9+% (less than 7 hours of planned and unplanned down-time per year). The same is absolutely not true of client-side scanning devices that routinely experience unplanned disruptions in operation. TN5250 client-side emulation solution providers have focused their efforts on improving the process of recovering from a dropped session (faster loading of client software, streamlined log-ins, roll-back and recover database logic, etc.) and lessening its impact versus pursuing a preventative solution.

eBusiness Solution Pros, Inc. (eSP) and its application software developers have chosen to go a different direction from the rest of the RF/Wireless terminal emulation solution providers. In order to create a more reliable offering that includes a solution to prevent dropped sessions, eSP has created a host-based RF/Wireless terminal emulation solution. The product is called StayLinked™, and it utilizes a new-generation client/server model that uses a thin client-resident

StayLinked

software application on the wireless device in conjunction with a centralized, host computer resident wireless terminal session/screen emulator server process.

StayLinked prevents dropped terminal session pain

Among the many benefits derived from implementing a host-based terminal emulation model, the ability to prevent dropped terminal user sessions is by far the most advantageous and valuable. StayLinked is built upon a host computer resident server- sided emulation strategy, and it features functionality that keeps user scanning sessions alive despite the occurrence of routine outages associated with wireless handheld computing/data capture devices.

Even if the client-side terminal user's process is disrupted for any of the reasons previously mentioned (battery replacement, the user going out of access-point range with a device, a device reset or reboot, etc.), the StayLinked host-side terminal emulation application keeps track of exactly where the session was interrupted and automatically returns the user to the precise point where they were in their job prior to the disruption encountered on their end. The server-side application software is responsible for maintaining the pointer as to exactly where a scanning job is versus the client-side application. As long as the server-side process is running, the job is not abandoned.

The StayLinked server-side application features software that acts as a session handler, managing the condition and status of all connected RF/Wireless client devices performing terminal emulation jobs. As all 5250, 3270 or VT terminal screen emulation is being performed on the host computer, the only responsibility of the small client-side software application running on the scanning devices is to receive screens and forward keystrokes/characters over the wireless connection. The session handler on the host side receives the characters (or bar codes) from each device that it is monitoring and passes them through the screen terminal emulation session software to the appropriate application for processing.

This type of character-by-character sending approach makes the client device passive in the wireless terminal session process. Non host-based solutions that perform all session emulation functions on the client make the device environment active in the process requiring it to stay un-disrupted, for any reason, to avoid a dropped session.

An added benefit of host-based emulation is that all wireless terminal devices can be managed from a single, reliable location. Centralized device management is a supplied feature of the StayLinked solution enabling the StayLinked application administrator to:

- View all device connections and all of their important properties
- Set remote device configurations
- Reboot remote devices

- Send software updates to remote devices
- Send and receive files from remote devices
- Send administrator messages to remote devices
- Monitor and troubleshoot problems with remote devices in real-time

Unlike typical Telnet and "fat client" solutions, StayLinked client licenses are not tied to specific wireless devices. This allows any wireless terminal device to be used in conjunction with the server-side screen emulation.

Summary

In order to prevent the potentially huge productivity time losses, as well as the tangible and intangible costs associated with dropped RF/Wireless 5250, 3270 and VT terminal sessions, any viable solution must feature server-based emulation architecture. Otherwise, the best any other approach can hope to offer is a limiting of the impact of the dropped session situation and streamlining of remedial processes. Furthermore, the most reliable server/environment to run the emulation software on is usually the computing platform where the applications are hosted.

At the time of publication for this document, StayLinked from eBusiness Solution Pros, Inc. is the only host-based RF/Wireless terminal emulation solution commercially available in the market.

The events that cause client-scanning devices to lose connectivity with their hosts can be reduced, but cannot ever be eliminated completely. Now, with StayLinked there is a way to completely shield the enterprise from the negative impact of these situations.

StayLinked prevents dropped/abandoned wireless terminal user sessions, adds centralized device management and leverages the reliability of the application host computing platform and the IT infrastructure already in place to manage host-based applications.

For further information or technical assistance, please contact your StayLinked Certified Partner or you may contact us directly:

15991 Red Hill Avenue Suite 210
Tustin, CA 92780

(714) 918-7700 (Main Office)
(714) 918-7817 (Technical Support)

http://www.staylinked.com
support@staylinked.com