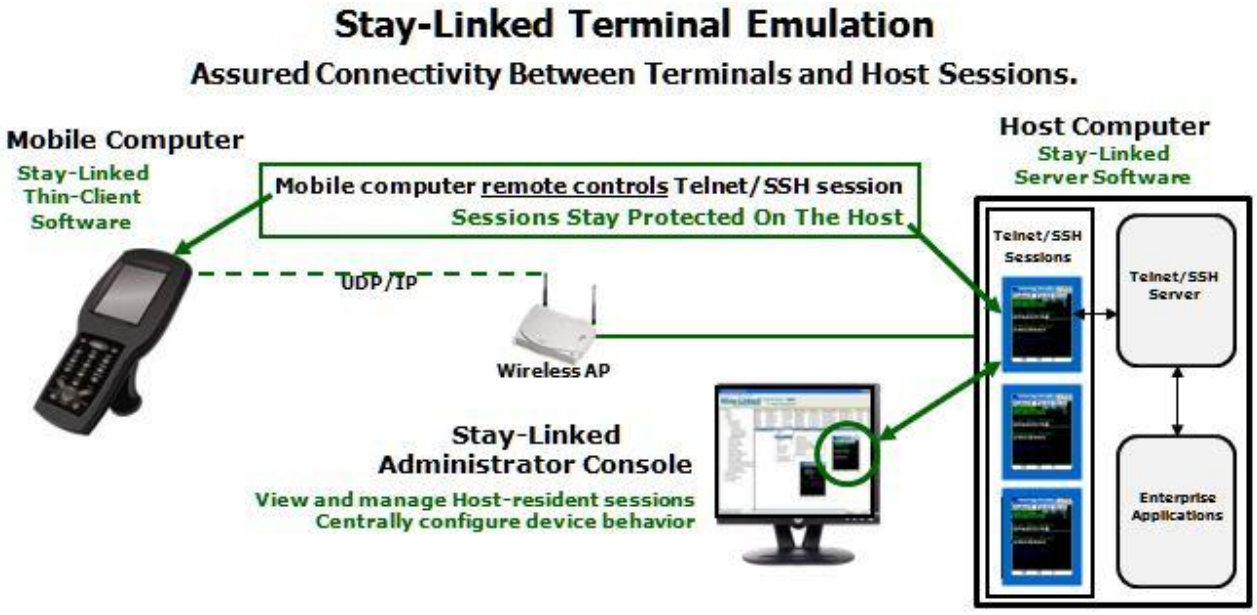
7 Quick Reasons to Select Stay-Linked

1. **No dropped sessions. Ever!**

   With Stay-Linked, Telnet or SSH terminal emulation sessions reside on the Host computer, where they are isolated from the wireless environment. If a device connection is lost, the user's session on the host stays open, allowing the user to pick up where they left off as soon as the unit reconnects.

   Wireless workers and IT staff get relief from device lockups and connection issues. The end result: a better bottom line for your business.

   Here's how it looks:



2. **No controllers or "session persistence" proxy servers needed.**

   Customers continually report to us how happy they are to unplug controllers and eliminate proxy servers. That's only possible with Stay-Linked.

   Stay-Linked goes beyond session persistence—your sessions are as safe and secure as your Host system. And while others have tried to solve their device-side emulation problems by creating proxy servers, or by making you use a controller, they just don't do what Stay-Linked does.

3. **Never Buy Terminal Emulation Again**

   Replacement devices can be ordered without the cost of terminal licenses, because Stay-Linked is licensed on the Host, on a concurrent-user basis. All you need is Stay-Linked client software installed on your new devices (many manufactures pre-load Stay-Linked), and you're ready to connect.

   And you can mix and match devices, knowing that Stay-Linked will work with them all—allowing you to slowly roll out devices if that's what your budget calls for.

4. The Stay-Linked Administrator Console: The most powerful tool in the industry for managing emulation environments and terminal devices

The Stay-Linked Administrator console application—included with the purchase of licenses—allows Help Desk staff to centrally manage all terminal emulation sessions and settings, and to easily manage concurrent-user license keys, via any network-connected Windows computer.

A few of the Administrator's features:

- TE user sessions can be interactively managed from the help desk to monitor sessions, take control of sessions, share sessions, or transfer sessions to the control of a new device—even when the user's device can't communicate with the host or if it becomes completely disabled.
- Data can be managed before it is passed to the Host application—allowable scans can be defined, prefixes/suffixes can be added or deleted, keyboard maps can be defined and edited, etc. These behaviors can be assigned to custom-defined device groups.
- There's no need to push emulation settings out to individual devices; emulation settings are maintained on the Host-based Server, are managed by the Administrator, and are assigned to a device when a session starts.
- Integrated terminal device management features are all performed using the same Administrator console application.

5. Security to Meet the Toughest Requirements

Stay-Linked developed its proprietary and unique Client2Host™ thin-client protocol to keep terminal emulation sessions safe on the Host.

- All Telnet or SSHv2 communication takes places internally within the Host system, where it is most secure.
- No Telnet is ever broadcast over the network.
- Data transmitted between the remote device and the Host (keystroke/scan input data and returning screen changes) is encrypted, and also travels within existing network security schemes.
- Terminal device management communication between the Stay-Linked Administrator console and remote devices uses this same secure connection method.

6. Network- and NAT-Friendly Communication

By using UDP/IP protocol in its Client2Host connection, Stay-Linked remains quiet on the network except to send input from the device to the Host, and to send the resulting emulation screen changes back from the Host to the device. Stay-Linked bypasses the typically-used TCP/IP protocol, so there's no constant connection keep-alive "pinging" on the network between the Host server and the remote device. Demands on the network are minimized.

Additionally, and as an additional benefit of the use of the UDP/IP protocol, network firewalls, NAT, and TCP/IP port restrictions do not present problems for Stay-Linked communication.

7. Stay-Linked Works Within All Types of Networks, Including Cellular

- Mobile devices that are capable of connecting to host systems via wide-area broadband access (Windows Mobile Smart Phones, RF equipped PDAs and laptops, etc.) can access host-based 5250/3270, VT100/220 and SSHv2 screen applications in real-time.
- Wide-area users benefit from the same host-based session persistence/reliability, management capabilities, high-performance response, and robust security as all of the other Stay-Linked users.