TELNET SUPPRESS LOCAL ECHO OPTION
<draft-rfced-exp-atmar-00.txt>

Status of This Memo

This document is an Internet-Draft. Internet-Drafts are working
documents of the Internet Engineering Task Force (IETF), its
areas, and its working groups. Note that other groups may also
distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six
months and may be updated, replaced, or obsoleted by other
documents at any time. It is inappropriate to use Internet-
Drafts as reference material or to cite them other than as
"work in progress."

To view the entire list of current Internet-Drafts, please check
the "1id-abstracts.txt" listing contained in the Internet-Drafts
Shadow Directories on ftp.is.co.za (Africa), ftp.nordu.net
(Northern Europe), ftp.nis.garr.it (Southern Europe), munnari.oz.au
(Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu
(US West Coast).

Distribution of this document is unlimited.

1. Command Name and Code

     SUPPRESS-LOCAL-ECHO (SLE) 45

2. Command Meanings

IAC WILL SUPPRESS-LOCAL-ECHO

The sender of this command, generally a device operating as an NVT
(network virtual terminal) terminal, CONFIRMS that it will suppress the
local echoing of characters onto its screen. This confirmation makes
valid sense only when the NVT is operating in an asymmetric, half-duplex
communications mode with a co-operating host.
IAC WONT SUPPRESS-LOCAL-ECHO

The sender of this command, generally a device operating as an NVT terminal, CONFIRMS that it will no longer suppress the echoing of locally typed text onto its screen. This confirmation makes sense only when the NVT is operating in a half-duplex mode with a co-operating host.

IAC DO SUPPRESS-LOCAL-ECHO

The sender of this command, generally a host computer, REQUESTS that a client NVT terminal suspend the local echoing of text typed on its keyboard. This request makes good sense only when the NVT and host are operating in an asymmetric, half-duplex terminal mode with a co-operating host. The command should have no effect on an NVT terminal operating in full-duplex mode.

IAC DONT SUPPRESS-LOCAL-ECHO

The sender of this command, generally a host computer, DEMANDS that a client NVT terminal not suppress typed characters that would normally be locally echoed onto the NVT’s terminal screen when operating in an asymmetric, half-duplex mode with a co-operating host. The command would have no effect on an NVT terminal operating in full-duplex mode.

3. DEFAULT

WONT SUPPRESS-LOCAL-ECHO

DONT SUPPRESS-LOCAL-ECHO

As the SLE default, all typed characters at the NVT are either (i) transmitted to the host when in full-duplex operation and are echoed back to the NVT terminal by the host computer, or (ii), when in half-duplex operation, are transmitted to the host and locally echoed within the NVT itself onto the NVT’s terminal screen.

4. MOTIVATION FOR THE OPTION

Telnet is a protocol that may be operated in either a peer-to-peer, fully symmetric mode, or asymmetrically, in a host-terminal mode. Although the original intention for the NVT mode of operation was both asymmetric and half-duplex, where neither the host nor the terminal echoed characters back to one another, the most common mode of usage has come to be one of asymmetric full-duplex communications, where all terminal characters are first transmitted to the host computer and then echoed back to the terminal before being displayed.

Not only has full-duplex communication has proven itself to be quite slow over long distances on the internet, and thus psychologically difficult to tolerate, full-duplex communication is less efficient, requiring twice as many packets be sent and returned.

Half-duplex NVT terminal operation decreases the overall packet count by half. It also renders long-distance NVT terminal operation pleasant to use. Characters are echoed to the terminal screen the instant they are typed. However, a problem arising within half-duplex terminal operation
is that of passwords. Passwords, whose presence would ordinarily be suppressed by a host computer when operating in a full-duplex mode, are made visible in half-duplex. The SUPPRESS-LOCAL-ECHO option allows the host to command the remote terminal to suspend local echoing of typed text for the duration of the period of that password or other similar confidential material is to be inputted.

A more complex method of terminal-local echo suppression is available to telnet users and is described in RFC 726, "Remote Controlled Transmission and Echoing Telnet Option." SUPPRESS-LOCAL-ECHO is a significantly simpler option, requiring much less negotiation between the host and the client terminal, and is thus substantially easier to implement.

5. DESCRIPTION OF THE OPTION

SUPPRESS-LOCAL-ECHO is among the mildest of all telnet options. The SLE commands only act as an advisory flag to synchronize the behavior of a a remote NVT terminal client with a host computer.

SUPPRESS-LOCAL-ECHO only has valid meaning when telnet communication has been established in an asymmetric, half-duplex mode of operation between a co-operating host and a client NVT terminal. In a half-duplex mode of host-terminal operation, the host commands the terminal to perform no echoes. Similarly, the terminal also commands the host to perform no echoes and places itself in such a mode that all typed characters are locally echoed to its screen. All subsequent communications between the host and the terminal are one-way.

A host computer program inherently "knows" when confidential information such as passwords are to be suppressed. At the beginning of such password entry, when in half-duplex operation with a co-operating NVT terminal, the host computer should issue a DO SLE to the remote client terminal.

The remote terminal then suspends all local echoing of text until the password entry has been completed, a process monitored by the host computer. Once password entry has been completed, the host computer issues a DONT SLE, at which point local echoing of text on the remote NVT must resume.

If the remote client NVT terminal is operating in full-duplex mode, the receipt of DO and DONT SLE commands would have no meaning and therefore must have no effect.

6. IMPLEMENTATION SUGGESTIONS

To fully utilize the internet and communicate with all available host computers, an NVT client terminal almost certainly should have two modes of operation: full- and half-duplex.

Full-duplex communication requires a round-trip circuit for each packet sent from the client NVT terminal to the host computer and back again before those characters are displayed on the terminal’s screen, thus perceived transit times that are many times that of half-duplex communications. Further, twice the number of packets must be sent and received in full-duplex as in half-duplex. Nonetheless, full-duplex communication has become the defacto standard of the telnet-based NVTs.
and therefore must be supported.

In order to properly support both full- and half-duplex communications, a mode status flag must be present in the NVT terminal. When in a full-duplex mode, an NVT should respond do both a DO SLE and a DONT SLE with a WONT SLE and do nothing otherwise.

In contrast, when an NVT is switched to half-duplex mode, the NVT must first send a DONT ECHO command to the host computer. Only when the host computer responds with a WONT ECHO should the NVT set its internal flag to half-duplex mode and begin locally echoing all characters typed at its keyboard to its screen.

When in the half-duplex mode of operation, upon receipt of a DO SLE command, the NVT terminal should suspend local echoing. It otherwise must continue to transmit all typed text to the host computer. Similarly, the NVT terminal must resume local echoing of characters when a DONT SLE command is received from the host.

Because the DO/DONT SLE commands are advisory only, the NVT terminal need not return WILL/WONT SLE acknowledgements to the host, although such acknowledgements are recommended. However, the acknowledgements cannot have any effect on the behavior of the host computer. The host must continue to receive text from the remote NVT under any circumstance, thus such acknowledgements must effectively be ignored by the host.

Further, the host computer can use its current echoing status as an indication of whether or not it should be issuing DO/DONT SLE commands. If the host is in an echoing state, where all incoming characters are echoed back to the remote NVT terminal, there is no valid reason for the host computer to be issuing DO/DONT SLE commands to the remote NVT terminal. The only time that the SLE commands will carry meaning is when the remote NVT terminal is in a half-duplex mode of operation and the remote NVT has requested and received acknowledgement of echo suppression in the host.

7. SECURITY CONSIDERATIONS

The negative impact of the SLE option on overall telnet use security is quite minimal, but not completely non-existent. Almost all current telnet transmissions are performed in clear text and are thus highly susceptible to "sniffer" interceptions.

The DO/DONT SLE command transmissions from the host will inherently tend to be transmitted just before and after passwords are typed in at the remote NVT client. Because of this, a surreptitious automatic procedure could be programmed to seek out the DO/DONT SLE commands and automatically extract passwords from the reverse data flow.

If the text transmission were performed in cleartext, nothing would be learned that could not be deduced otherwise. Only the possibility of automatically bracketing and extracting passwords would be new. Similarly, and perhaps much worse, if the entire text transmission were encrypted, the location and length of passwords could be identified within the reverse flow from the timing of the DO/DONT SLE command transmissions.

However, conversely, because the DO/DONT SLE commands will inherently bracket password entry on the NVT terminal, the DO/DONT SLE commands
could be faithfully used to cause a remote NVT client to fall into a special (or alternate) encryption mode that lasts only for the duration of password entry, actually augmenting overall security.