Telnet Forwarding of X Window System Session Data

0. Abstract

This Internet-Draft describes a mechanism via which X Window System client applications to which a telnet session has been established may have their communications with the X Windows Server forwarded via the Telnet communications channel. This is desirable when the Telnet session is established through a Firewall or Network Address Translator which does not allow arbitrary connections to be created from the host machine to the client machine; or when the Telnet session is using an authenticated and encrypted channel and that same security is desired for the X Window System session data.

1. Command Names and Codes

FORWARD_X 49 (assigned by IANA)

Sub-option Commands

FWDX_SCREEN 0
FWDX_OPEN 1
FWDX_CLOSE 2
FWDX_DATA 3
FWDX_OPTIONS 4

Sub-option Options

FWDX_OPT_NONE 0

2. Command Meanings

IAC WILL FORWARD_X

The server side of the connection sends this command to indicate that it is willing to send and receive X Window System session data via the telnet connection. The client must not send this command.

IAC DO FORWARD_X

The client side of the connection sends this command to indicate
that it is willing to send and receive X Window System session data via the telnet connection. The server must not send this command.

IAC WONT FORWARD_X

The server side of the connection sends this command to indicate that it is not willing or able to send and receive X Window System session data via the telnet connection. If the client receives IAC DO FORWARD_X it must respond with IAC WONT FORWARD_X.

IAC DONT FORWARD_X

The client side of the connection sends this command to indicate that it is not willing or able to send and receive X Window System session data via the telnet connection. If the server receives IAC WILL FORWARD_X it must respond with IAC DONT FORWARD_X.

IAC SB FORWARD_X FWDX_SCREEN <screen> IAC SE

The client side of the connection sends this command to the server to indicate to the server the screen (or monitor) number being used by the local X Window System server. <screen> is a single octet with legal values of 0 to 255. The screen number is to be used by the server when constructing the DISPLAY environment variable to be used on the host.

The server side of the connection must not send this command.

IAC SB FORWARD_X FWDX_OPEN <channel> IAC SE

The server side of the connection sends this command to the client to indicate that a new X Window System session is being started and that a new channel should be allocated. <channel> is two octets in network byte order.

The client side of the connection must not send this command.

IAC SB FORWARD_X FWDX_CLOSE <channel> IAC SE

Either side of the connection sends this command to indicate to the other that the channel has been terminated and that the associated resources should be freed. <channel> is two octets in network byte order.

IAC SB FORWARD_X FWDX_DATA <channel> <data> IAC SE

Either side of the connections sends this command to the other to forward X Window System session data across the Telnet connection. <channel> is two octets in network byte order. <data> is an arbitrary length stream of bytes. All occurrences of 0xFF in the data stream must be doubled to avoid confusion with telnet commands.

IAC SB FORWARD_X FWDX_OPTIONS <bitmask bytes> IAC SE

The server sends this command to the client to specify the list of options which are supported by the server. The client responds with this command to indicate the subset of the specified options that are to be used. The must respond with the same number of bytes as are provided by the server. If no options are supported a single zero byte is to be sent.

3. Option Meanings

FWDX_OPT_NONE
No options are supported by the server or client.

4. Default Specification

The default specification for this option is
WONT FORWARD_X
DON'T FORWARD_X

meaning there will not be any forwarding of X Window System session data.

5. Motivation

Firewalls and Network Address Translators sometimes make it impossible for X Window System clients to connect to the local X Window System server. In these situations it is necessary to have a method to forward (or tunnel) the data along a connection which is already established.

When Telnet Authentication and Encryption or Telnet over TLS are in use it is desirable to afford the same level of protection to the X Window System session data that is afforded to the Telnet session data.

This option provides a mechanism for using the Telnet connection as a tunnel which then applies its own level of security to the X Window System sessions.

6. Implementation Rules

WILL and DO are negotiated only at the beginning of the Telnet session to obtain and grant permission for future FORWARD_X sub-negotiations. After WILL and DO are exchanged the client must send a FWDX_SCREEN negotiation so the server may establish the appropriate DISPLAY environment variable.

After receipt of FWDX_SCREEN the server will define a DISPLAY variable on the host which shall cause all future X Window System sessions created within that Telnet session to be redirected to the Telnet server. This DISPLAY variable must point to a socket or other mechanism via which the Telnet Server will be able to listen for new X Window System sessions.

Whenever the server accepts a new X Window System session it allocates a new channel and sends a FWDX_OPEN negotiation to the client. The client allocates any necessary resources for the support of the channel and opens a local connection to the X Window System Server specified by the local environment.

All data read by the server from the X Window System clients or from the X Windows Server by the client are forwarded to the peer via the use of a FWDX_DATA negotiation.

When the X Window System client closes the connection the server will send a FWDX_CLOSE negotiation to the client. If the X Window System Server closes the connection the client with send a FWDX_CLOSE to the server.

The Telnet server should not allocate X Window System display number 0 but instead should leave it available for the local X Window System server on the same machine.

The Telnet client should not negotiate FORWARD_X if it does not have a local X Window System server available.

FORWARD_X takes precedence over Telnet X-Display Location and the DISPLAY variable transmitted via Telnet Environment. If FORWARD_X has been negotiated prior to the receipt of other display information, this subsequent information must be ignored.

FORWARD_X is designed as an extensible protocol with the intention of adding support for the caching and compression of X Windows System messages; automatic creation and forwarding of X Windows System Authority data; or even acting as a proxy for Kerberos authenticated X Windows System connections. FORWARD_X options are negotiated using the FWDX_OPTIONS messages. Each option is to be given its own bit value. As many bytes of bit mask data as are needed to represent the options may be allocated with one restriction: the 8th bit of each byte may not be assigned.

After publication of this I-D as an RFC the authority to issue option bit
values will be given to IANA.

7. Security Considerations

FORWARD_X is independent of Telnet Authentication and Encryption, and Telnet over TLS. Use of FORWARD_X without the use of Telnet Authentication and Encryption or Telnet over TLS does not provide any privacy benefits.

Until such time as the automatic forwarding of Xauthority data is supported, when the Telnet Server creates a socket to listen for new X Window System clients it should ensure that the connections it accepts have originated on the same machine on which it is executing (and when possible verify the identity of the user making the connection.) Otherwise, the listen socket may be used to gain access via an otherwise secure channel to the Telnet client’s X Window System server.

8. Example

Initial negotiations

S: IAC WILL FORWARD_X
C: IAC DO FORWARD_X

Server and client have agreed to negotiate FORWARD_X

S: IAC SB FORWARD_X FWDX_OPTIONS 00 IAC SE
C: IAC SB FORWARD_X FWDX_OPTIONS 00 IAC SE

Server and client agree that no Forward X options are to be used.

C: IAC SB FORWARD_X FWDX_SCREEN 00 IAC SE

Server established a listen socket on port 6001 (display 1) and puts an DISPLAY=<ip-address>:<display>.<screen> (i.e. 127.0.0.1:1.0) variable into the local environment.

The server receives a connection from an X Window System client and allocates channel 0:

S: IAC SB FORWARD_X FWDX_OPEN 00 00 IAC SE

Client creates connection to local X Window System server.

Server receives data to send from X Window System client to X Window System server.

S: IAC SB FORWARD_X FWDX_DATA 00 00 <data> IAC SE

X Window System server replies:

C: IAC SB FORWARD_X FWDX_DATA 00 00 <data> IAC SE

X Window System client closes the connection:

S: IAC SB FORWARD_X FWDX_CLOSE 00 00 IAC SE

Authors’ Addresses

Jeffrey Altman
Columbia University
Watson Hall Room 716
612 West 115th Street
New York NY 10025
Phone: +1 (212) 854-1344
EMail: jaltman@columbia.edu

Peter Runestig
Orsangesvagen 83