Independent Submission   Jeffrey Altman
Internet-Draft   Peter Runestig
draft-altman-telnet-fwdx-03.txt   April 2002

Telnet Forwarding of X Window System Session Data

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026. 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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

0. Abstract

This document describes a mechanism via which X Window System client applications may have their communications with the X Windows System server forwarded across a Telnet communications channel. This is desireable 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. Authorization to communicate across the tunnel is provided to the X Windows System client via use of X Display access control 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
FWDX_OPT_DATA	5
FWDX_XOFF	6
FWDX_XON	7

Sub-option Options

FWDX_OPT_NONE	0
FWDX_OPT_NONE_MASK	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 occurances 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 client must respond with the same number of bytes as are provided by the server. If no options are supported by the server, then a single zero byte is to be sent. The eight bit of each byte must be zero.

IAC SB FORWARD_X FWDX_OPT_DATA <option> <option-data> IAC SE

This command is used to communicate data specific to an option negotiated by the client and server. The command may be sent in either direction. <option> is a byte containing the option number (not the option mask). The format of the <option-data> is specific to the option and cannot be specified in this document.

IAC SB FORWARD_X FWDX_XOFF <channel> IAC SE

This command is sent by the telnet server to the telnet client when the specified channel is no longer writeable. When the client receives this command is must immediately stop reading data from the X Server.

```
IAC SB FORWARD_X FWDX_XON  <channel> IAC SE
```

This command is sent by the telnet server to the telnet client when the specified channel becomes writeable. This command must only be sent if a FWDX_XOFF command has previously be been sent without a matching FWDX_ON command.

3. Option Meanings

```
FWDX_OPT_NONE       0
FWDX_OPT_NONE_MASK  0
```

No options are supported by the server or client.

4. Default Specification

The default specification for this option is

```
WONT FORWARD_X
DONT 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 desireable 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. The Telnet Server will also create a temporary .Xauthority file containing entries for each of the X Authority types (MIT-MAGIC-COOKIE-1, XDM-AUTHORIZATION-1, SUN-DES-1, MIT-KERBEROS-5) that it will accept for X Windows System client authorization.

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.

The client will then open the X Windows System display on its local system using the local X Authority data for authorization (if it is available.) If the client is unable to open the display, it sends a FWDX_CLOSE to the server.

The server when receiving the initial message from X Windows System client will parse it for byte order and any specified X Authority data. If no X Authority data is provided or if the X Authority data is invalid, an X Authority error message will be sent to the X Windows System client and the connection will be closed. A FWDX_CLOSE message will be sent to the client.

If authorization is provided, the server will (using the designated byte ordering for this session) replace the initial X Authority data from the X Windows System client with null data and forward the data to the client.

From this point forward 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 negotiation 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 must not be negotiated over an insecure connection. If Telnet AUTH and ENCRYPT or START_TLS are not in use, FORWARD_X must be refused by both the client and server.

Any Telnet server implementing FORWARD_X must implement at least one of the X display access control (XAUTH) methods. A failure to implement access control on the server creates a serious security vulnerability openning the X Windows Server on the client's machine to attack.

FORWARD_X is designed as an extensible protocol with the intention of adding support for the caching and compression of X Windows System messages. 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.

The Telnet server must be able to handle a suspended X client. When an X Client is suspended it will not read data from its data input. In this situation the data path from the Telnet server to the X client will eventually become blocked. The Telnet Server must ensure that no data is lost and that all other Forward X channels as well as normal telnet session processing continue. The FWDX_XOFF and FWDX_XON commands provide the ability for the telnet server to implement flow control for each channel on an individual basis.

7. 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 allocate 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

```
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
```

8. Security Considerations

Although FORWARD_X is independent of Telnet Authentication and Encryption, a Telnet over TLS, the use of FORWARD_X without the use of Telnet Authenticati and Encryption or Telnet over TLS (or other integrity protection) creates a security hole. Therefore, FORWARD_X MUST NOT be negotiated if neither Telnet over TLS nor Telnet Encryption are successfully negotiated and in use.

9. IANA Considerations

IANA is the responsible for assigning all FORWARD_X option numbers. These numbers are to be assigned sequentially.

FORWARD_X options have valid values of 1 to 255 so that they can be represented in a single byte in the FWDX_OPT_DATA message. Each option is assigned both an option value and a bitmask for use in the FWDX_OPTIONS negotiation.

As there are no options defined as the present time an example of the mechanism is provided. Assume we define options ONE, FIVE and EIGHT.

```
FWDX_OPT_ONE         1
FWDX_OPT_ONE_MASK    1        /* Byte 1 of FWDX_OPTIONS */

FWDX_OPT_FIVE        5
FWDX_OPT_FIVE_MASK  16        /* Byte 1 of FWDX_OPTIONS */

FWDX_OPT_EIGHT       8
FWDX_OPT_EIGHT_MASK  1        /* Byte 2 of FWDX_OPTIONS */
```

10. References

X Windows System X Protocol documentation
ftp://ftp.x.org/pub/R6.4/xc/doc/hardcopy/XProtocol/proto.PS.gz

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
Bjorktjaravagen 5 C
821 35 Bollnas
Sweden
Phone: +46-278-35777
EMail: peter@runestig.com
Mailing List: telnet-wg@bsdi.com