

TNVIP Protocol

Status of this Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

The goal of this document specifies a Telnet profile to support VIP terminal emulation allowing the access to the BULL hosts applications through a TCP/IP network.

Table of Contents

1.	Motivation	2
2.	Background	3
3.	Telnet Options and Commands Used	3
3.1.	Terminal type option	4
3.1.1.	Subnegotiation of the Terminal Type	4
3.1.2.	Terminal-types supported by the TNVIP protocol	4
3.1.3.	TNVIP terminal models	5
3.1.4.	Mailbox name	5
3.2.	End of Record Option	6
3.3.	Binary Transmission option	6
3.4.	Suppress Go Ahead option	7
4.	TNVIP functions	8
4.1.	TNVIP terminal station	9
4.1.1.	Local and online states	9
4.1.2.	Data receiving	10
4.1.3.	Data sending	10
4.2.	TNVIP Server functions	10
4.2.1.	VIP Terminal Manager	10
5.	TNVIP Messages Format	12
5.1.	Address Field	12
5.2.	Command field	13
5.3.	Parameter field	14
6.	The screen flow	14
6.1.	Screen data messages	14
6.2.	Local state monitoring messages	15
6.3.	Screen response messages	16
6.3.1	Page overflow processing	17

6.4.	Screen data purge indication message	17
7.	The printer flow	17
7.1.	Printer data messages	17
7.2.	Printer response messages	18
7.3.	7800 printer status management	19
7.4.	Printer state request message	20
7.5.	Printer state response messages	20
7.6.	Printer purge indication message	20
8.	The Screen Copy Printing flow	21
8.1.	Screen copy request messages	21
8.2.	Screen copy data message	21
8.3.	Screen copy response messages	22
8.4.	Screen copy purge indication message	23
9.	The TM attention	23
10.	The Break Key	24
11.	The Logout Key	24
12.	TNVIP messages list	24
12.1.	Screen Flow	24
12.2.	Printer flow	26
12.3.	Screen Copy Printing messages flow	28
13.	Security Considerations	29
14.	References	30
15.	Author's Address	30

1. Motivation

P200 [7] and 7800 [8] VIP (Visual Information Projection) terminals differ mainly from NVT terminals [1] in that they work in block mode and have the capability to manage an associated printer. Generally in a DSA (Distributed Systems Architecture) network they are managed through the VIP transmission line procedure (character oriented). That is the reason why they are generically referred as VIP terminals.

This document specifies the options to be modified successfully, to pass from the NVT terminal emulation supported on a Telnet connection, to a VIP terminal emulation. It defines also the format of the messages exchanged between the server and the client when the TNVIP protocol is successfully negotiated.

2. Background

VIP terminal family includes a broad range of different terminal types. They work in block mode with an ASCII or 8 binary bits set of characters.

The Bull terminals in the DSA network environment use the services of a Terminal Manager (TM) [2]. It is generally installed in a communication processor (as a Datanet or Mainway system) where it assures the connection with the BULL host application generally through a DSA session.

The Terminal Manager is in charge to present the terminal station and to manage the session connection to the host computer. It offers generally a possibility of dialog with the terminal to allow the user to modify the connection parameters, to manage the session (connection request, abort, etc ..). The set of commands and responses used is called "TM Local Dialog".

3. Telnet Options and Commands Used

The mandatory telnet parameters to be negotiated successfully between the "TNVIP server" and the "TNVIP client" are :

- the Terminal-Type option [3] to define a VIP terminal model and if necessary a Mailbox name to request a specific access point in the "TNVIP server",
- the End Of Record option [4] to delimit the TNVIP message at the Telnet level. As the End Of Record (EOR) code indicates the end of an effective data unit, Telnet should attempt to send the data up to and including the EOR code together to promote communication efficiency.

Others Telnet parameters, can be optionally negotiated as :

- the Binary Transmission option [5], when the terminal emulation uses a 8 binary bits set of characters,
- the Suppress Go Ahead option [6], when no synchronisation of the data transmission from the "TNVIP client" with the DSA session turn or the ISO session token is needed.

When the two parties (the "TNVIP server" and the "TNVIP client") have negotiated successfully a TNVIP terminal type and the EOR telnet option, that means they agree to respect the TNVIP protocol (the TNVIP message format and the exchange rules).

3.1 Terminal type option

IAC DO TERMINAL-TYPE

Sender (the "TNVIP server" party) is willing to receive terminal type information in a subsequent sub-negotiation.

IAC WILL TERMINAL-TYPE

Sender (the terminal "TNVIP client" party) is willing to send terminal-type information in a subsequent sub-negotiation.

3.1.1 Subnegotiation of the Terminal Type

IAC SB TERMINAL-TYPE SEND IAC SE

Sender (the "TNVIP server" party) requests the receiver to transmit his next terminal-type, and switch emulation modes (if more than one terminal type is supported).

IAC SB TERMINAL-TYPE IS tnvip-terminal-model@MB-name IAC SE

Sender (the terminal "TNVIP client" party) is stating the name of his current (or only) terminal-type. Optionally, a mailbox name can be added to request a particular access point in the "TNVIP server". By default, the "TNVIP server" uses a generic access point.

3.1.2 Terminal-types supported by the TNVIP protocol

The TNVIP terminal type string given at the Telnet negotiation is formatted as follows :

<TNVIP-terminal-model> [<@ character> <Mailbox-name>]

The @ character is used as separator between the VIP-terminal-model and the Mailbox-name.

3.1.3 TNVIP terminal models

The valid TNVIP terminal models are the following ASCII character strings. (The table gives for each terminal model string the hexadecimal number indicating the associated DSA model number defined in the DSA terminal presentation protocols).

P200 family				7800 family			
!	TNVIP model	!	DSA code	!	TNVIP model	!	DSA code
!	VIP7700	!	33	!	VIP7804	!	3E
!	VIP7760	!	3A	!	VIP7804V	!	4A
!	DKU7005	!	3D	!	VIP7814	!	47
!	DKU7007D	!	40	!	HDS7	!	4D
!	DKU7105	!	41	!	VIP8800	!	4F
!	DKU7107D	!	42	!		!	
!	DKU7211	!	45	!		!	
!	DKU7211D	!	4E	!		!	

The D character at the end of the string indicates that the terminal supports the Remote Forms function [9]. It is the capability to store forms in the terminal allowing the host application to display a form stored in the terminal sending a short length command without sending all the data of the form. This function is usually supported by the terminal concentrators.

3.1.4 Mailbox name

The mailbox name allows the "TNVIP client" to request a specialized access point referenced by this name in the "TNVIP server". It is an ASCII character string. Its presence in the Telnet terminal type string is optional. When not present, a generic (default) access can be provided by the "TNVIP server".

When the "TNVIP server" is a gateway to DSA hosts, the mailbox name defines the DSA session access point of the terminal in the server. Its length is limited to 12 characters. Lower case characters are allowed but are processed as upper case. This string is generally used to identify a specific terminal station (having a printer for example) or to use a particular declaration of this terminal in the "TNVIP server".

3.2 End of Record Option

VIP device communications are block oriented. That is, each partner buffers data until an entire "message" has been built, at which point the data are sent to the other side. The end of a message is understood to be the last byte transmitted. The Telnet EOR command is used to delimit these natural blocks of TNVIP data within the Telnet data stream. An <EOR> is sent at the end of each TNVIP message, in both directions.

IAC WILL END-OF-RECORD

The sender of this command requests permission to begin transmission of the Telnet END-OF-RECORD (EOR) code when transmitting data characters, or the sender of this command confirms it will now begin transmission of EORs with transmitted data characters.

IAC DO END-OF-RECORD

The sender of this command requests that the sender of data starts transmitting the EOR code when transmitting data, or the sender of this command confirms that the sender of data is expected to transmit EORs.

3.3 Binary Transmission option

According to the character set used by the emulation, the "TNVIP client" and the "TNVIP server" can be led to negotiate the Telnet binary transmission option.

If either side wishes to transmit the decimal value 255 and have it interpreted as data, it must "double" this byte. In other words, a single occurrence of decimal 255 will be interpreted by the other side as an IAC, while two successive bytes containing decimal 255 will be treated as one data byte with a value of decimal 255.

IAC DO TRANSMIT-BINARY

Sender requests that sender of the data starts transmitting or confirms that the sender of data is expected to transmit characters that are to be interpreted as 8 bits of binary data by the receiver.

IAC WILL TRANSMIT-BINARY

Sender requests permission to begin transmitting, or confirms it will now begin transmitting binary data.

IAC WON'T TRANSMIT-BINARY

If the connection is already being operated in binary transmission mode, the sender of this command demands to begin transmitting data characters which are to be interpreted as standard NVT ASCII characters by the receiver of the data. If the connection is not already being operated in binary transmission mode, the sender of this command refuses to begin transmitting characters which are to be interpreted as binary characters by the receiver of the data (i.e., the sender of the data requests to continue transmitting characters in its present mode).

IAC DON'T TRANSMIT-BINARY

If the connection is already being operated in binary transmission mode, the sender of this command requests that the sender of the data start transmitting characters which are to be interpreted as standard NVT ASCII characters by the receiver of the data (i.e., the party sending this command). If the connection is not already being operated in binary transmission mode, the sender of this command requests that the sender of data continue transmitting characters which are to be interpreted in the present mode.

3.4 Suppress Go Ahead option

The "TNVIP client" can use the receiving of the Telnet GoAhead command as the signal allowing the terminal operator to transmit data. That can allow the synchronisation between the data transmitted from the terminal and the DSA "turn".

When the Suppress Go Ahead option is not negotiated, the "TNVIP server" must send the Telnet Go Ahead command (GA) when its input message queue (from the "TNVIP client") is empty and the DSA turn is at the terminal side, to invite the terminal to transmit some data.

To suppress this mechanism, the "TNVIP client" can request the no sending of the Telnet GoAhead commands by the "TNVIP server", negotiating the Suppress GO Ahead option of the Telnet Protocol.

In this case, the terminal transmission to the "TNVIP server" is synchronised on the transport credit.

Note: The Telnet GA command never need to be sent by the "TNVIP client" even if the telnet Suppress Go Ahead has not been negotiated.

IAC DO SUPPRESS-GO-AHEAD

The sender of this command (the "TNVIP client" party) requests that the sender of data starts suppressing GA when transmitting data.

IAC WILL SUPPRESS-GO-AHEAD

The sender of this command (the "TNVIP server" party) confirms it will now begin suppressing transmission of GAs with transmitted data characters.

IAC DON'T SUPPRESS-GO-AHEAD

The sender of this command (the "TNVIP client" party) requests that the receiver of the command start transmitting GAs when transmitting data.

IAC WON'T SUPPRESS-GO-AHEAD

The sender of this command (the "TNVIP server" party) confirms it will now begin transmitting the GA character when transmitting data characters.

4. TNVIP functions

The TNVIP protocol allows the following functions :

- Support of a VIP terminal emulation addressing the screen and its associated printer .
- Selection of the terminal type model at the connection time.
- Specific or generic access to the "TNVIP server" by referencing or not a Mailbox name.
- TNVIP protocol independent of the terminal data presentation protocol (7800 or P200).
- Support of the DSA End To End Acknowledgement.
- Support of the DSA Terminal Manager local attention.
- Support of the DSA turn to the terminal side.
- Support of the DSA secret read.
- Control of the hard copy.

4.1 TNVIP terminal station

The "TNVIP client" acts as the interface adapter between the TNVIP connection and an application program. The "TNVIP client" is mainly defined to support a VIP terminal emulation program but can be used by other else program using the TNVIP protocol.

A VIP terminal emulation manages:

- a screen buffer,
- a printer buffer if it supports the associated printer,
- the interface with the communication line

and runs using the following rules:

When the VIP terminal emulation exchanges a message on the communication line, it is in the BUSY state until the end of the message exchange. That means when the VIP terminal is sending a message it can't receive and when it is receiving a message it can't send.

Note: If a VIP terminal works in the half duplex mode, as the TNVIP protocol uses a Telnet connection it allows a full duplex mode processing.

4.1.1 Local and online states

The VIP terminal has the capability to switch between these two states. The LOCAL state is generally used to process local terminal tests or to modify the configuration. In this state, the data coming from the line are ignored.

The LOCAL state allows the "TNVIP client" to request to the server the screen and printer data flows to be suspended.

The ONLINE state indication allows the "TNVIP server" to resume the screen and printer flows.

For these reasons the TNVIP protocol differentiates the screen and printer flows from the screen copy printing flow and defines to report the two states to the "TNVIP server".

4.1.2 Data receiving

When a VIP terminal emulation receives a data message from the line, according to the address given in the header message, it sends data to the screen buffer or to the printer buffer.

A message received at the screen or printer address is deleted and ignored if the terminal emulation is in the LOCAL state and a BUSY status is returned.

The printer buffer is busy when the terminal is transmitting the data from the printer buffer to the printer device. A data message for the printer is deleted and ignored if the terminal is in the printing state and a BUSY status is returned.

When a BUSY state is encountered, the "TNVIP client" according to the type of message received (request or indication) reports or not the BUSY acknowledgement to the "TNVIP server".

4.1.3 Data sending

A VIP terminal emulation can send message even if the terminal is in the LOCAL state.

4.2 TNVIP Server functions

4.2.1 VIP Terminal Manager

Its function is to act as a gateway between the VIP terminal and the VIP application. Generally the application is a remote DSA application.

It manages the screen and printer devices of the VIP terminal station.

In the following example figure, the "TNVIP server" is a DSA server and manages three VIP terminal units TU1, TU2 and TU3.

Generic access

```

-----
                !----> LD 1S ----> DV 1S (screen) ---->!
MB 1 --> SN 1                                     TU 1
                !----> LD 1P ----> DV 1P (printer) ---->!

```

Specific accesses

```

-----
                !----> LD 2S ----> DV 2S (screen) ---->TU 2
MB 2 --> SN 2
                !----> LD 2P ----> !
                !
                !----> LD 3P ----> DV 3S (printer) ---->!
MB 3 --> SN 3                                     TU 3
                !----> LD 3S ----> DV 3P (screen) ---->!

```

Each Terminal Unit (TU object) is declared as containing one or two devices (DV objects). The Terminal Manager maps this physical representation to a logical representation where the station (SN object) is the logical representation of a terminal unit, and the logical device (LD) object a logical representation of the real device.

- TU1 will be chosen by default on generic request (without mailbox name) or by the MB1 name addressing on specific request. It can manage the associated printer device.
- MB2 will be addressed to access the TU2 terminal unit. TU2 is defined in a specific way because it will be presented to the host application as a station composed of a screen (the TU2 one's) and a printer (the TU3 one's).
- MB3 will be addressed to access TU3 terminal unit. TU3 is also defined in a specific way because the printer device is shared by several logical stations (SN2 and SN3) and must be well identified.

5. TNVIP Messages Format

Each TNVIP message is delimited by the Telnet EOR command.

Therefore, a TNVIP message has the following format:

```
<TNVIP Header> <parameters> <IAC EOR>
```

The TNVIP header is mandatory and have a fixed length of two bytes.

Some TNVIP messages need no parameter. In this case, the TNVIP message has the following construction:

```
<TNVIP Header> <IAC EOR>
```

It is strongly recommended that Telnet commands (other than IAC IAC) should be sent between TNVIP messages, with no TNVIP header and no trailing IAC EOR. If a TNVIP data message containing any other IAC-command sequence (other than IAC IAC) is received, it is implementation dependent when the IAC-command sequence will be processed, but it must be processed. The receiver may process it immediately, which in effect causes it to be processed as if it had been received before the current TNVIP message, or the processing may be deferred until after the current TNVIP message has been processed. It is because of this ambiguity that the presence of Telnet commands within a TNVIP message is not recommended; neither "TNVIP client"s nor "TNVIP server"s should send such data.

The TNVIP header contains 2 bytes. The first one indicates the address <ADR> and the second the command <CDE>.

5.1 Address Field

The <ADR> address field is mandatory and is defined on one byte.

The TNVIP protocol defines 3 addresses:

- ADR = SCREEN = 96 (0x60) for the screen commands flow,
- ADR = PRINTER = 104 (0x68) for the printer commands flow,
- ADR = SCPM = 105 (0x69) for the screen copy printing commands flow.

A request message with an unknown or unsupported address will be discarded by the receiver which replies with a NOT-AVAILABLE response message.

5.2 Command field

The <CDE> command field is mandatory and defined on one byte.

The command byte <CDE> is structured as follows:

<Command-Type><Message-Type>

- The Command-Type fills the six most significant bits of the <CDE> byte. The most significant bit is always 0.

Its value is ranged from 0 to 31 included. It defines the command associated to the message for the flow identified by the address field.

- The Message-Type fills the two less significant bits of the <CDE> byte.

0 = Indication message. No response message is expected. An indication message with an undefined command type or with an unknown address is deleted and ignored.

1 = Request message. The sender of a request message is waiting for a response message having the same address value. When a request message is sent for a given address, it is not allowed to send another request to the same address before the receiving response. If an end point receives a request before having sent the response of the previous request, it deletes the second request but have to send back a PROTOCOL-VIOLATION response after the response of the first request. A request message with a not defined address is replied to by a NOT-AVAILABLE response message. A request message with an unknown or unsupported command <CDE> for this address will be deleted by the receiver and replied to by an UNKNOWN-COMMAND response message.

2 = Response message. This message is the response to the current request message. The receiver of this message is allowed to send another request message on the flow defined by the ADR field.

3 = Response and request message. This message is a positive response to the current request message sent by the receiver, but is also a request message.

The following table gives the <CDE> commands list with their hexadecimal values

Command	Indication	Request	Response	Resp/Req
DATA	00	01		
PASSW	04	05		
ACK			0A	
ERROR			0E	
BUSY			12	
ABORTED			16	
PURGED			1A	
NOT-AVAILABLE			1E	
PROTOCOL-VIOLATION			22	
UNKNOWN-COMMAND			26	
PURGE	28			
LOCAL-STATE		2D		
ONLINE-STATE	30			
STATE-REQ		35		
READY			3A	
STANDBY			3E	
COPY-REQ		41		
LOCAL-COPY				47

5.3 Parameter field

This field has a variable length and its content is depending on the two previous fields (address and command).

6. The screen flow

All the following messages contain the value SCREEN = 96 (0x60) in the ADR field.

6.1 Screen data messages

These messages are defined to transport in the parameter field of the TNVIP message, the data in the terminal presentation negotiated by the "Terminal Type" telnet command.

The parameter has the following format:

```
<FC1> <FC2> <STX> < screen data>
```

- The FC1, FC2 bytes are the functions codes of the VIP procedure transmission [9]. Their values are comprised between 32 (0x20) included and 127 (0x7F) included.

- The STX byte is defined by the value 2 and acts as the introducer of the screen data.

A screen data message can be sent in a request or in an indication message. The command values are defined as follows:

<CDE> = DATA indication = 0

<CDE> = DATA request = 1

<CDE> = PASSWORD indication = 4

<CDE> = PASSWORD request = 5

Generally, the "TNVIP server" only sends indication messages to the screen. The request message is used mainly for the printer device. But a DSA/TNVIP gateway server should use the screen data request message when it processes a DSA end to end acknowledgement request from the DSA application and synchronizes the response message receipt with the DSA end to end acknowledgement.

The password request and the password indication message are defined, to be used by the programs in the "TNVIP client" machine which don't emulate terminal. In this way, they have the indication that a secret read (password acquisition) is requested by the "TNVIP server". When the program is a terminal emulation this information is not necessary because the data contains the terminal presentation command to request this secret read.

6.2 Local state monitoring messages

Before to switch in the local state, the "TNVIP client" sends a LOCAL-STATE request message to the "TNVIP server". This last one sends back an acknowledgement message and suspends the screen and printer data flow until it receives a LINE-STATE indication message.

Note: In the local state, only the messages from the "TNVIP server" to the screen or printer devices are deleted. The messages from the "TNVIP client" screen device or the messages associated to others addresses are allowed.

The following command values are defined as:

<CDE> = LOCAL-STATE request = 45 (0x2D). It is sent by the "TNVIP client". There is no parameter field.

<CDE> = ONLINE-STATE indication = 48 (0x30). It is sent by the "TNVIP client" to indicate the "TNVIP server" is allowed to resume the screen data flow. There is no parameter field.

6.3 Screen response messages

These messages are indications used to respond to the screen data request previously received.

The command values are defined as follows:

<CDE> = ACK response indication = 10 (0x0A). The screen data previously received has been well processed or the LOCAL STATE is acknowledged by the "TNVIP server". There is no parameter field.

<CDE> = ERR response indication = 14 (0x0E). The screen data previously received has not been correctly processed. There is no parameter field.

<CDE> = BUSY response indication = 18 (0x12). The screen data previously received has been deleted because the terminal is in the local state. There is no parameter field.

<CDE> = ABORTED response indication = 22 (0x16). The receipt of the screen data request has been aborted by a reset terminal command. There is no parameter field.

<CDE> = PURGED response indication = 26 (0x1A). The processing of the screen data request has been aborted by a purge indication message. There is no parameter field.

<CDE> = NOT-AVAILABLE response indication = 30 (0x1E). The screen device is not supported. Normally this command has never to be generated because the screen device should always be present. There is no parameter field.

<CDE> = PROTOCOL-VIOLATION response indication = 34 (0x22). The screen request received has been deleted because an other screen request is already in process. That means several screen request messages have been sent without waiting for the response. It is a consequence of the non-compliance of the protocol. There is no parameter field.

<CDE> = UNKNOWN-COMMAND response indication = 38 (0x26). The screen request received has been deleted because the <CDE> field value is unknown. It is a consequence of the non-compliance of the protocol. There is no parameter field.

6.3.1 Page overflow processing

The page overflow processing is not supported through the TNVIP protocol to avoid the retransmission of the message. That leads the "TNVIP client" side to process it locally. When a data message induces a page overflow, the terminal emulation alerts the user possibly requesting (in manual mode) an "enter" action before clearing the screen and reprocessing the data received.

Note: When the "TNVIP client" is processing a page overflow, the terminal emulation should be in the BUSY state and should stop getting message from the line ("TNVIP server") until the page overflow processing is complete.

6.4 Screen data purge indication message

This message is used to purge the current screen request message. When the side which receive the message has not already acknowledged the screen request, it tries to abort the processing of the request and returns a screen purged response message. If it has already replied, it ignores and deletes the message.

The following command value is defined as:

<CDE> = PURGE indication = 40 (0x28). There is no parameter field.

7. The printer flow

All the following messages contain the PRINTER value 104 (0x68) in the ADR field. The support of this address is optional. If the "TNVIP server" doesn't address this device, no message with this address will be exchanged. If the "TNVIP client" receives a request message with this address and does not support the printer, it replies with a printer NOT-AVAILABLE response message.

7.1 Printer data messages

These messages are defined to transport the printer data in the parameter field of the TNVIP message. These messages are only sent from the "TNVIP server" to the "TNVIP client".

The parameter has the following format:

<FC1> <FC2> <STX> <printer data>

- The FC1, FC2 bytes are the function codes of the VIP procedure transmission. Their values are ranged from 32 (0x20) to 127 (0x7F) included.

- The STX byte is defined by the value 2 and acts as the introducer of the printer data.

To manage correctly the printer device, the protocol only defines request message. Whereas the "TNVIP server" is ensured that the "TNVIP client" processes a screen data message only when the previous one have been processed. When it receives a printer data message, the "TNVIP client" transfers it in the printer buffer. The terminal is busy only during this transfer. So, if the "TNVIP client" receives another printer data it deletes them because the previous printing (transfer between the printer buffer and the printer) is not ended.

The printer data structure depends on the terminal presentation family (P200 or 7800). The two presentations define two modes of printing. The first one needs the printer data are in the presentation of the screen (7800 or P200 commands) and data are converted by the terminal in the printer presentation (TTY, SDP, copy). The second mode allows to give the printer data in the real presentation of the printer. For this reason it is called "transparent print".

In the P200 terminal presentation, transparent print data are introduced by the sequence of the two ASCII characters ESC Z (0x1B 0x5A). P200 formatted print are introduced by the sequence of two ASCII characters ESC X (0x1B 0x58) or ESC Y (0x1B 0x59).

In the 7800 terminal presentation, transparent print data are introduced by the command PTD (Print Transparent Data). 7800 formatted print are introduced by the command PHD (Print Host Data).

<CDE> = DATA request = 1 (0x01).

7.2 Printer response messages

These messages are used to report the printing end status of the printer data request previously received.

The following command values are defined as:

<CDE> = ACK response indication = 10 (0x0A). The printer data previously received have been well processed.

<CDE> = ERR response indication = 14 (0x0E). The printer data previously received have not been correctly processed (invalid command, buffer overflow , printer off...)

<CDE> = BUSY response indication = 18 (0x12). The printer data received have been deleted because the previous printing request is

not ended. Several printer data request messages have been sent without waiting for the response.

<CDE> = ABORTED response indication = 22 (0x14). The printing has been aborted by the terminal operator.

<CDE> = PURGED response indication = 26 (0x18). The printing request has been aborted by a printer data purge indication message.

<CDE> = NOT-AVAILABLE response indication = 30 (0x1E). The printer device is not supported.

<CDE> = PROTOCOL-VIOLATION response indication = 34 (0x22). The printer request received has been deleted because an other printer request is already in process. That means several printer request messages have been sent without waiting for the response. It is a consequence of the non-compliance of the protocol. There is no parameter field.

<CDE> = UNKNOWN-COMMAND response indication = 38 (0x26). The printer request received has been deleted because of an unknown <CDE> field value. It is a consequence of the non-compliance of the protocol. There is no parameter field.

For all the above commands, the parameter field may contain specific terminal status if one was requested in the printer data received (response to PDENQ 7800 terminal presentation command).

7.3 7800 printer status management

When emulating a 7800 terminal [8], the "TNVIP client" takes charge of adding to the printer data the printer differed status request (PDENQ 7800 command) to synchronize the printing end with the sending of the printer acknowledgement response.

Some DSA applications are written to manage the 7800 printer status, so they send themselves the printer status request at the beginning of the printer data. That is the reason why when the "TNVIP client" receives this command at the beginning of the printer data, it must send back the 7800 status response in the parameter field of the printer data response message.

The 7800 terminal presentation defines also immediate printer status request and response (PENQ which allows to get an immediate response indicating the current printer status). These commands have to be exchanged in the TNVIP screen data flow.

7.4 Printer state request message

This message is sent by the "TNVIP server" to know the printer state of the "TNVIP client" without sending printer data.

The following command value is defined as:

<CDE> = STATE-REQ request = 53 (0x35). There is no parameter field.

7.5 Printer state response messages

These messages are sent by the "TNVIP client" in order to report the printer state to the "TNVIP server".

The following command values are defined as:

<CDE> = READY response indication = 58 (0x3A). The printer state is ready to print. There is no parameter field.

<CDE> = STANDBY response indication = 62 (0x3E). The printer device is in standby and is temporarily unavailable. There is no parameter field.

<CDE> = PURGED response indication = 26 (0x1A). The printer state request has been aborted by a printer state purge indication message. There is no parameter field.

<CDE> = NOT-AVAILABLE response indication = 30 (0x1E). The printer device is not supported. There is no parameter field.

<CDE> = PROTOCOL-VIOLATION response indication = 34 (0x22). The printer state request received has been deleted because another printer request is already in process. That means several printer request messages have been sent without waiting for the response. It is a consequence of the non-compliance of the protocol. There is no parameter field.

<CDE> = UNKNOWN-COMMAND response indication = 38 (0x26). The printer state request received has been deleted because the <CDE> field value is unknown. It is a consequence of the non-compliance of the protocol. There is no parameter field.

7.6 Printer purge indication message

This message is used by the "TNVIP server" to purge the current printer request message. When the "TNVIP client" receives this message, if it has not already acknowledged the printer data, it aborts the printing and returns a printer data purge acknowledgement

response message. If it has already replied, it ignores and deletes the message.

The printer purge command value is defined as:

<CDE> = PURGE indication = 40 (0x28). There is no parameter field.

8. The Screen Copy Printing flow

All the following messages contain the SCPM address value 105 (0x69) in the ADR field. The support of this address is mandatory.

8.1 Screen copy request messages

As the printer device can be used by the "TNVIP server", if the terminal user wishes a screen copy printing, the "TNVIP" client has to synchronize the user request with the "TNVIP server" printing .

The TNVIP protocol defines that the "TNVIP client" has to inform the "TNVIP server" when it wants to print a screen copy and waits for its authorization before beginning

The following command values are defined as:

<CDE> = COPY-REQ request = 65 (0x41). It is used from the "TNVIP client" to the "TNVIP server" to request a screen copy printing.

<CDE> = LOCAL-COPY response and request = 71 (0x47). It is sent by the "TNVIP server" to acknowledge the COPY-REQ message indicating the screen copy can be done locally. It is also a request message because it is equivalent to a screen copy data request message and the "TNVIP server" is waiting for a screen copy response message from the "TNVIP client" but on the SCPM flow. There is no parameter field.

8.2 Screen copy data message

They are defined in order to transport in the parameter of the message the screen copy data in the terminal presentation. It is used by the "TNVIP client" when it wants to send the screen copy data directly to the DSA application (a VIP terminal using a VIP transmission procedure indicates this special request by the STA byte =PRT=0x1A).

The parameter field has the following format:

<FC1> <FC2> <STX> <screen-copy-data>

- The FC1, FC2 bytes are the functions codes of the VIP procedure transmission. Their values are ranged from 32 (0x20) to 127 (0x7F) included.
- The STX byte is defined by the value 2 and acts as the introducer of the screen data.

Screen copy data message can be sent in a request or indication message.

The command values are defined as follows:

<CDE> = DATA indication = 0

<CDE> = DATA request = 1

8.3 Screen copy response messages

These messages are sent by the "TNVIP client" (local copy) to report the end of printing status of the screen copy.

The ACK response is also used by the "TNVIP server" to acknowledge a screen copy data request sent to the host application.

The ERR message is also used by the server to refuse a COPY-REQ message.

The following command values are defined as:

<CDE> = ACK response indication = 10 (0x0A). The "TNVIP client" reports the screen copy has been well printed or the "TNVIP server" acknowledges the screen copy data request. There is no parameter field.

<CDE> = ERR response indication = 14 (0x0E). The screen copy has not been correctly printed (invalid command, buffer overflow ...) or has been refused by the "TNVIP server". It can optionally contain a reason code value defined on one byte.

- 1 : The printer is busy, retry later.

<CDE> = BUSY response indication = 18 (0x12). The screen copy has not been correctly printed because the printer device is already printing. There is no parameter field.

<CDE> = ABORTED response indication = 22 (0x16). The screen copy has been aborted by the terminal operator. There is no parameter field.

<CDE> = PURGED response indication = 26 (0x1A). The screen copy request message has been aborted by a purge indication message. There is no parameter field.

<CDE> = NOT-AVAILABLE response indication = 30 (0x1E). The screen copy has not been correctly printed because the printer device is not supported. There is no parameter field.

<CDE> = PROTOCOL-VIOLATION response indication = 34 (0x22). The screen copy request received has been deleted because an other screen copy request is already in process. That means several screen copy request messages have been sent without waiting for the response. It is a consequence of the non-compliance of the protocol. There is no parameter field.

<CDE> = UNKNOWN-COMMAND response indication = 38 (0x26). The screen copy request received has been deleted because the <CDE> field value is unknown. It is a consequence of the non-compliance of the protocol. There is no parameter field.

8.4 Screen copy purge indication message

This message is used to purge the current screen copy request message. When the "TNVIP server" or the "TNVIP client" receives this message, if it has not already acknowledged the request message, it returns a screen copy purge acknowledgement message. If it has already replied, it ignores and deletes the message.

The following command value is defined as:

<CDE> = PURGE indication = 40 (0x28). There is no parameter field.

9. The TM attention

The TM attention is the signal used to activate the local dialog of the DSA Terminal Manager.

The Telnet Abort Output (AO) command [1] is the mechanism used to implement the TM attention key support in TNVIP.

IAC AO (0xFF 0xF5)

In order to implement the TM attention key support, "TNVIP clients" should provide a key (or combination of keys) that is identified as mapping to the TM attention key. When the user presses this key(s),

the "TNVIP client" should transmit a Telnet AO command to the "TNVIP server".

Upon receipt of the AO command, a "TNVIP server" that implements the DSA Terminal Manager should enter in what will be loosely termed "TM Local Dialog", suspending the eventual DSA host connection, else it should simply ignore it.

10. The Break Key

Generally, there is no break key on the real VIP terminal. The break signal is transmitted to the host application through a TM local dialog command (\$*\$BRK for example)

On "TNVIP client" emulating VIP terminal, it is often possible to map the break signal on a special key combination or by other way (using mouse ...).

The Telnet Break (BRK) command [1] is used to map the Break signal of the TNVIP.

```
IAC BRK (0xFF 0xF3)
```

11. The Logout Key

The Telnet Interrupt Process (IP) command [1] can be used to map the logout command of the TM Local Dialog (\$*\$LO for example) if it is implemented on the "TNVIP server".

```
IAC IP (0xFF 0xF4)
```

12. TNVIP messages list

All the TNVIP commands are summarized here after (and the values are given in hexadecimal).

12.1 Screen Flow

Data request (allowed in the two ways)

```
SCREEN DATA-REQ <FC1> <FC2> STX [<screen-data>] IAC EOR
60      01      <FC1> <FC2> 02  [<screen-data>] FF  EF
```

- Allowed responses to the screen Data request.

```
SCREEN ACK IAC EOR
60      0A  FF  EF
```

```
SCREEN ERROR  IAC EOR
60      0E      FF  EF
```

```
SCREEN BUSY   IAC EOR
60      12      FF  EF
```

```
SCREEN ABORTED IAC EOR
60      16      FF  EF
```

```
SCREEN PURGED IAC EOR
60      1A      FF  EF
```

Password request (only from the "TNVIP server" to the "TNVIP client")

```
SCREEN PASSW-REQ <FC1> <FC2> STX [<screen-data>] IAC EOR
60      05      <FC1> <FC2> 02 [<screen-data>] FF  EF
```

- Allowed responses to the password request.

```
SCREEN ACK     IAC EOR
60      0A     FF  EF
```

```
SCREEN ERROR  IAC EOR
60      0E     FF  EF
```

```
SCREEN BUSY   IAC EOR
60      12     FF  EF
```

```
SCREEN ABORTED IAC EOR
60      16     FF  EF
```

```
SCREEN PURGED IAC EOR
60      1A     FF  EF
```

Local state request (only from the "TNVIP client" to the "TNVIP server").

```
SCREEN LOCAL-ST IAC EOR
60      2D      FF  EF
```

- Allowed responses to the Local state request.

```
SCREEN ACK     IAC EOR
60      0A     FF  EF
```

```
SCREEN PURGED IAC EOR
60 1A FF EF
```

Responses to request violating the TNVIP protocol (allowed in the two ways)

```
SCREEN NOT-AVAIL IAC EOR
60 0E FF EF
```

```
SCREEN PROT-VIOL IAC EOR
60 22 FF EF
```

```
SCREEN UNKN-CDE IAC EOR
60 26 FF EF
```

Indications (allowed in the two ways)

```
SCREEN DATA-IND <FC1> <FC2> STX [<screen-data>] IAC EOR
60 00 <FC1> <FC2> 02 [<screen-data>] FF EF
```

```
SCREEN PURGE IAC EOR
60 28 FF EF
```

Password indication (only from the "TNVIP server" to the "TNVIP client").

```
SCREEN PASSW-IND <FC1> <FC2> STX [<screen-data>] IAC EOR
60 04 <FC1> <FC2> 02 [<screen-data>] FF EF
```

On line state indication (only from the "TNVIP client" to the "TNVIP server").

```
SCREEN ONLINE-ST IAC EOR
60 30 FF EF
```

12.2 Printer flow

Data request (only from the "TNVIP server" to the "TNVIP client")

```
PRINTER DATA-REQ <FC1> <FC2> STX [<printer-data>] IAC EOR
68 01 <FC1> <FC2> 02 [<printer-data>] FF EF
```

- Allowed responses to the printer data request.

```
PRINTER ACK [<status>] IAC EOR
68 0A [<status>] FF EF
```

```
PRINTER ERROR [<status>] IAC EOR
68 0E [<status>] FF EF
```

```

PRINTER BUSY [<status>] IAC EOR
68      12  [<status>] FF  EF

```

```

PRINTER ABORTED [<status>] IAC EOR
68      16  [<status>] FF  EF

```

```

PRINTER PURGED [<status>] IAC EOR
68      1A  [<status>] FF  EF

```

```

PRINTER NOT-AVAIL [<status>] IAC EOR
68      1E  [<status>] FF  EF

```

State request (only from the "TNVIP server" to the "TNVIP client")

```

PRINTER STATE-REQ IAC EOR
68      35      FF  EF

```

- Allowed responses to the state request.

```

PRINTER READY IAC EOR
68      3A      FF  EF

```

```

PRINTER STANDBY IAC EOR
68      3E      FF  EF

```

```

PRINTER PURGED IAC EOR
68      1A      FF  EF

```

```

PRINTER NOT-AVAIL IAC EOR
68      1E      FF  EF

```

Responses to request violating the TNVIP protocol (allowed in the two ways)

```

PRINTER PROT-VIOL IAC EOR
68      22      FF  EF

```

```

PRINTER UNKN-CDE IAC EOR
68      26      FF  EF

```

Indication (only from the "TNVIP server" to the "TNVIP client")

```

PRINTER PURGE IAC EOR
68 28 FF EF

```

12.3 Screen Copy Printing messages flow

Copy request (only from the "TNVIP client" to the "TNVIP server")

```
SCPM COPY-REQ  IAC EOR
69  41          FF  EF
```

- Allowed responses to the copy request (from the "TNVIP server" to the "TNVIP client")

```
SCPM  ERROR  <reason> IAC EOR
69    0E     <reason> FF  EF
```

```
SCPM  PURGED  IAC EOR
69    1A      FF  EF
```

```
SCPM  NOT-AVAIL  IAC EOR
69    1E          FF  EF
```

```
SCPM  LOCAL-COPY-RQ  IAC EOR
69    47             FF  EF
```

Local copy request (only from the "TNVIP server" to the "TNVIP client")

```
SCPM  LOCAL-COPY-RQ  IAC EOR
69    47             FF  EF
```

- Allowed responses to the local copy request (from the "TNVIP client" to the "TNVIP server").

```
SCPM  ACK  IAC EOR
69    0A   FF  EF
```

```
SCPM  ERROR  IAC EOR
69    0E     FF  EF
```

```
SCPM  BUSY  IAC EOR
69    12   FF  EF
```

```
SCPM  ABORTED  IAC EOR
69    16       FF  EF
```

```
SCPM  PURGED  IAC EOR
69    1A      FF  EF
```

```
SCPM  NOT-AVAIL  IAC EOR
69    1E          FF  EF
```

Data request. (only from the "TNVIP client" to the "TNVIP server")

```
SCPM DATA-REQ <FC1> <FC2> STX [<screen-data>] IAC EOR
69  01          <FC1> <FC2> 02 [<screen-data>] FF  EF
```

- Allowed responses to the data request

```
SCPM ACK IAC EOR
69  0A   FF  EF
```

```
SCPM PURGED IAC EOR
69  1A     FF  EF
```

```
SCPM NOT-AVAIL IAC EOR
69  1E         FF  EF
```

Responses to request violating the TNVIP protocol (allowed in the two ways)

```
SCPM PROT-VIOL IAC EOR
69  22         FF  EF
```

```
SCPM UNKN-CDE IAC EOR
69  26         FF  EF
```

Indications (allowed in the two ways)

```
SCPM DATA-IND <FC1> <FC2> STX [<screen-data>] IAC EOR
69  00          <FC1> <FC2> 02 [<screen-data>] FF  EF
```

```
SCPM PURGE IAC EOR
69  28     FF  EF
```

13. Security Considerations

Security issues are not addressed in this document. It is anticipated that once authentication mechanisms have become well established, use of them can be made by TNVIP. One of the important uses of authentication would be to answer the question of whether or not a given user should be allowed to "use" a specific terminal.

14. References

- [1] Postel, J., and J. Reynolds, "Telnet Protocol Specification", STD 8, RFC 854, USC/Information Sciences Institute, May 1983.
- [2] "Communications. MainWay. Terminal Management. DNS-E", Ref : 39A213EB Rev00, BULL S.A.
- [3] VanBokkelen, J., "Telnet Terminal-Type Option", RFC 1091, FTP Software, Inc., February 1989.
- [4] Postel, J., "Telnet End of Record Option", RFC 885, USC/Information Sciences Institute, December 1983.
- [5] Postel, J., and J. Reynolds, "Telnet Binary Transmission", STD 27, RFC 856, USC/Information Sciences Institute, May 1983.
- [6] Postel, J., and J. Reynolds, "Telnet Suppress Go Ahead Option", STD 29, RFC 858, USC/Information Sciences Institute, May 1983.
- [7] "Affinity V2. DKU7107 Reference Manual"
Ref : 40 A2 23 WA, BULL S.A.
- [8] "Affinity V2. VIP7800 Reference Manual"
Ref : 40 A2 24 WA, BULL S.A.
- [9] "Bull Questar 200. TCS 7424 et TCS 7434. Transmission de donnees. Manuel de reference"
Ref : 80 F2 41DC Rev0, BULL S.A.

15. Author's Address

Jean-Yves Dujonc
BULL S.A.
rue Jean Jaures
78340 Les Clayes-sous-Bois
France

Phone: 1 30 80 62 95
Fax: 1 30 80 65 40
EMail: J.Y.Dujonc@frcl.bull.fr

