U S WEST Communications, Inc. Technical Publication

U S WEST Scan-Alert℠ Alarm Signaling Transport Service

77333
Issue A
July 1992

U S WEST Communications, Inc. Technical Publication

U S WEST Scan-Alert℠ Alarm Signaling Transport Service

77333
Issue A
July 1992

NOTICE

This publication describes the technical interface specifications for the U S WEST Scan-Alert[SM] Alarm Signaling Transport Service provided by U S WEST Communications, Inc. to their customers.

U S WEST Communications, Inc. assumes no responsibility for any cost incurred by a given manufacturer in conforming to the requirements of this specification. Conformance to this specification does not constitute a guarantee of a given suppliers equipment and/or its associated documentation for use within U S WEST Communications, Inc.

U S WEST Communications, Inc. makes no representation or warranty, expressed or implied, with respect to the Remote Module that is Customer Provided Equipment (CPE).

U S WEST Communications, Inc. reserves the right to revise this publication for any reason and without any prior notification.

If further information is required, please contact:

U S WEST Business Resources, Inc.
Manager - Information Release
1801 California St., Rm. 1340
Denver, CO 80202
(303) 298-8740

Throughout this publication, the term U S WEST signifies U S WEST Communications, Inc.

PLEASE TEAR OUT AND SEND YOUR COMMENTS/SUGGESTIONS TO:

U S WEST BUSINESS RESOURCES, INC.
Manager - Writing Services
1801 California, Room 1340
Denver, Colorado 80202
(303) 298-8740

Information from you helps us to improve our Publications. Please take a few moments to answer the following questions and return to the above address.

Was this Publication valuable to you in determining our requirements? YES _____ NO _____

Was the information accurate and up-to-date? YES _____ NO _____

Was the information easily understood? YES _____ NO _____

Were the contents logically sequenced? YES _____ NO _____

Were the printed pages legible? YES _____ NO _____

Do you feel the description in the Catalog of Technical Information and/or Digest of Technical Information adequately described this Publication? YES _____ NO _____

If you answered NO to any of the questions and/or if you have any other comments or suggestions, please explain:

_____

_____

_____

_____

_____

(Attach additional sheet, if necessary)

Name _____ Date _____

Company _____

Address _____

_____

Telephone Number _____

1. Introduction

1.1 Scanner-CPE

This publication describes the protocol necessary for Scan-Alert[SM] Technology to interface with Customer Premises Equipment (CPE). ScanAlert[SM] Equipment is referred to in the body of this publication as "Scanner." Scan-Alert[SM] is a method of alarm signal transport between CPE at an alarm agency's customer site and CPE based at the alarm agency. This publication provides sufficient details to enable an alarm agency to successfully interact with the Scan-Alert[SM] System. It also provides details to allow a manufacturer to produce equipment that uses the Scan-Alert[SM] protocol.

Scan-Alert[SM] is an alarm transport product that incorporates a data transmission system designed to transmit data signals over existing telephone lines using a metallic interface at the alarm agency's customer site. It is available in selected locations within U S WEST. Because this product is functional primarily on metallic facilities, it may not be available on all dial tone lines in a given area.

Scan-Alert[SM] Central Office Equipment (COE) polls alarm detection devices (located on a customer's premises) and, upon receipt of an alarm message, transmits a signal to a U S WEST. host processor and generally to an alarm company central station. See Figure 1.

This protocol allows digital communications over the serving facility, with the normal telephone station equipment either on-hook or off-hook, without interrupting the normal telephone service.

Service options include only those transport configurations available for the host - agency data lines, as described in the subsection entitled Host-Agency in Chapter 3.

1.2 Host-agency

This publication also describes the protocol necessary to interface the alarm agency based CPE with the U S WEST host computer.

This protocol allows agencies to transmit and receive digital communications from their offices through the host computer to an alarm detection device.

2. System Operation

2.1 Scanner-CPE

The CPE in the Scan-Alert[SM] network is a device which is polled by the COE Scanner. To eliminate the need to poll the unit excessively when the telephone subscriber is off-hook, the CPE transmits a supervisory tone (low-tone) 36.075 HZ +/- 1%, sine wave with an output impedance of 4.2K ohms +/- 5% and shall provide an output level of -6 dBm +10% -0% as measured with a 900 ohm load. When the CPE has information to send to the COE Scanner, it stops transmitting the low-tone. The COE Scanner responds to the loss of received low-tone and polls the CPE for the message. Communication between the Scanner and the CPE is half duplex.

When polled, the Scanner reports an "alarm" or "no alarm" message. Failure of CPE to respond to polling within 90 seconds is reported to the Alarm Service Provider (alarm company). See Table A.

A feature of this system is its ability to sense whether or not a CPE requires a poll. In the event that a phone is in use and the supervisory tone is sensed, the system may elect not to interrogate the associated CPE. A minimum signal is specified at the Network Interface. See Section 3 for detailed description. The function of the CPE is to provide a communication interface for transmitting data from the customer premises to the Scanner located in a U S WEST Communications, Inc. Scan-Alert[SM] equipped Central Office.

Scan-Alert[SM] will support the reporting of up to eleven different alarm signals and four system maintenance alarms. The system maintenance alarms are translated into data that is reported to the agency. For that reason, the meaning of these alarms is fixed. The four system maintenance alarms are:

- Open-box switch (reports activity and/or tampering with the Customer Premises Equipment).
- Loss of AC power.
- Low CPE battery voltage.
- Diagnostic error in the CPE functions.

The last three system maintenance alarms are unlatched (are one time reporting only) and do not require the alarm agency to respond. The eleven alarm signals and the open-box switch are latched and the alarm must be changed by the alarm agency and do require the alarm agency to respond.

Table A Communications Sequence

Normal Communications Sequence

CPE		Scanner
Transmits supervisory tone: Supervisory tone on	→	May elect to not poll CPE
Supervisory tone off	←	Polls CPE maximum of 52 seconds after tone loss
Transmits alarm or no-alarm message	→	If alarm, transmits alarm to host
	←	Scanner sends acknowledgement to CPE
Supervisory tone on	→	

Open Line Communications Sequence

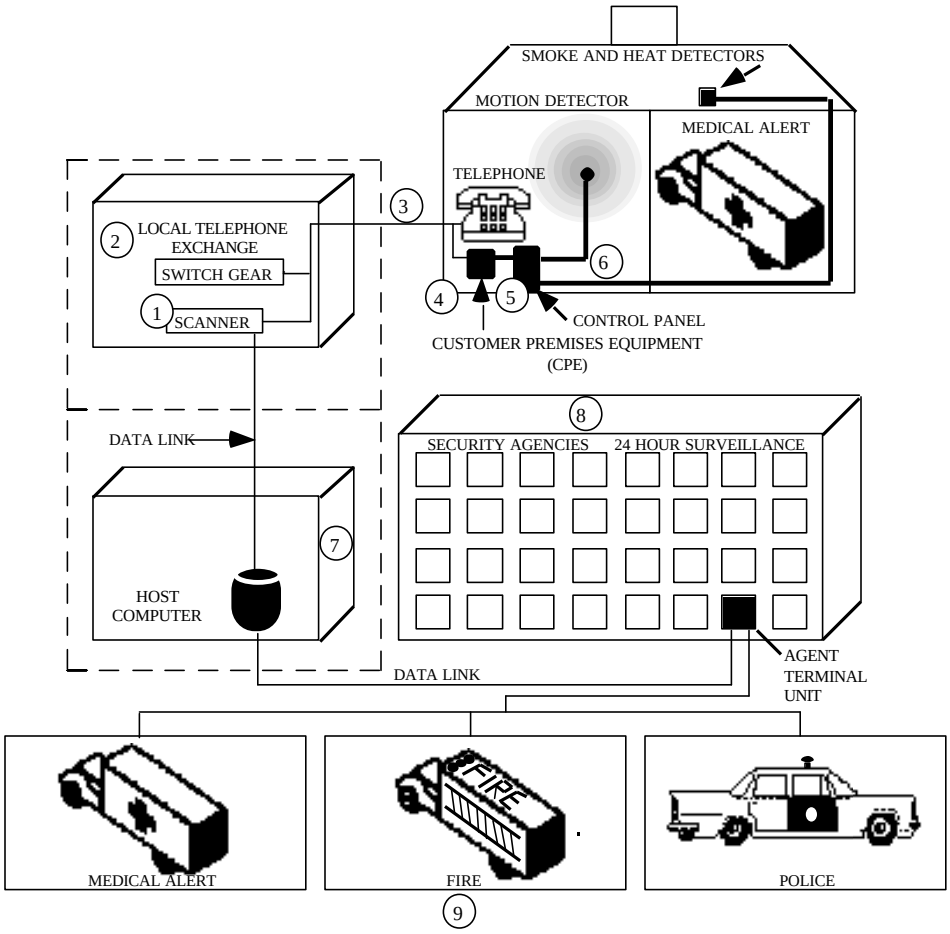
CPE		Scanner
Supervisory tone on	→	May elect not to poll CPE
	Open Line:	Loss of the supervisory tone
	←	Polls CPE maximum of 52 seconds after tone loss
	Open Line:	Without CPE response, sends New Fault report to host

When there is no alarm and no action is required by the alarm agency, or when the alarm agency has acknowledged the alarm and the alarm is still present, the CPE transmits the supervisory tone. To report a change of any alarm signal, the CPE removes the supervisory tone. In the absense of noise on the loop, the Scanner will wait a maximum of 26 seconds before recognizing the loss of the supervisory tone, at which time it will issue a poll a maximum of 26 seconds later.

The CPE starts counting from the moment that the supervisory signal is removed. If the Scanner has not polled the CPE within a fixed period of time, the CPE will output a "Wait" message. This period of time is programmed into the CPE and must not exceed 60 seconds.

This service also reports to an alarm agency that a cut in the telephone line has been detected.

Scanner-CPE and host-agency communications follow a four layer approach; Physical Layer, Link Layer, Packet Layer and Session Layer. The following sections describe each of these layers.



Scan-Alert[SM] Emergency Reporting Service provides a means of identifying and notifying the customer's alarm company of a change in the status of alarm or other type monitoring sensor located on a customer's premises. Scan-Alert[SM] Service utilizes a scanner (1) connected in the Central Office (2) to that customer's single party exchange line (3). The scanner is used to repetitively poll an alarm agency's provided CPE (4) which is connected to an alarm control panel (5), which monitors alarm sensors (6). A change in status (Alarm Condition) in an alarm sensor is recorded in the CPE, then polled by the scanner, and transmitted through the scanner to a centrally located processor (7). The processor will then transmit the change in status to the alarm agency (8) via a data connection. Once the alarm agency receives notice of an alarm condition (fire, burglary, medical, or other), the agency notifies the proper authority (9) or responds according to prearranged instructions with their customer. It is important to note that cut or interrupted lines are also reported to the alarm agency.

Figure 1 Scan-Alert[SM]

2.2 Host-agency

The agency based CPE is a device which is polled by the U S WEST host computer. Under normal conditions, the host computer polls the agency based CPE every 2 to 4 seconds. Originally optimized for alarm transport, this protocol allows the agency to send user defined data packets to and from the alarm detection device for a wide variety of applications.

Agencies may only communicate with alarm detection CPEs which are assigned to them in the U S WEST host computer. No agency can obtain another agency's alarm information.

3. Physical Layer

3.1 Scanner-CPE

The physical communications layer for the CPE is a bridged tip/ring, polarity insensitive, connection and all implementations shall abide by Federal Communications Commission (FCC) Regulations, Part 68. The interface shall be designed to provide reliable low speed telemetry over a continuous copper pair, without a gain device, with a maximum total loop resistance of 1600 ohms. See Table B for some typical characteristics.

The polling signal is Frequency Shift Key (FSK) modulated with a center frequency of 2877 +81/-5 Hz. The mark frequency for both transmission and reception shall be 2977 +81/-5 Hz. The space frequency shall be 2777 +5/-27 Hz. The bit width, (the time between two bits) shall be 2.52 milliseconds +/-5%.

The FSK carrier level delivered from the Network Interface to the CPE must be between -5 dBm and -40 dBm. The CPE responds to the polling with a FSK signal at the same carrier frequency. The output level must not fall below -11 dBm and must not exceed -9 dBm. The maximum noise addition to a 10 dBrnC line shall be 0.5 dBrnC.

3.2 Host-agency

The physical communications layer for the agency can be defined in various methods. The Scan-Alert[SM] host provides a RS-232C 1200 baud port, of which the agency is defined as Data Terminal Equipment (DTE). Most installations currently use 4-Wire dedicated data lines, with the 202T type modem standard to transport the communications to the agency premises. The user should check with the local U S WEST Representative for the exact configurations available. See U S WEST Communications, Inc. Technical Publication 77365, "Network Channel and Network Channel Interface Combinations" for a listing of NC and NCI codes used within U S WEST.

Table B Typical Characteristics of Metallic Telephone Lines

- DC loop resistance = 1600Ω
- May or may not have 88 MH load coils (Loaded Cable)
- 1KHz loss of 3.65dB average, with a range of 0.5dB to 16.0dB.
- Dielectric strength (conducter - conducter) of 2.4 kv DC minimum for Polyethylene insulated conductors and 0.5 kv (peak) for pulp insulated conductors.
- Nominal capacitance of 83 μF per mile.
- Loop noise of =20 dBrnC.

4. Link Layer

4.1 Scanner-CPE

Polling is accomplished from the Scan-Alert[SM] Central Office Equipment using serially transmitted data. The alarm detection CPE will respond to the poll with the serial data. The Scanner injects carrier onto the line and then transmits the synchronization pattern (SYNC), followed by the message. The CPE shall interpret the message, using higher levels of the protocol, and be able to begin its response within 15 milliseconds of the end Scanner message.

Scanner SYNC shall be the 6 bit pattern 111010. CPE shall be the 24 bit synchronization pattern 0000 0000 0000 1111 1110 1001. The CPE shall assume that there may be erroneous data due to noise caused by the frequency injection which will follow carrier detect but precede SYNC. This should be ignored. Following SYNC, the Scanner sends 2 bits of information called the EA bits. The E bit, if set, indicates that the message uses data encryption. The A bit, if set, acknowledges that the previous data message was received properly.

In normal circumstances, the CPE shall output low-tone at all times. In the event that the CPE has data it wishes to send the Scanner, low-tone should be removed. The CPE shall define a WAIL time-out which shall be less than 60 seconds. If the CPE has removed low-tone and the Scanner fails to poll data within the WAIL time-out, the CPE may send WAIL, which is defined as SYNC followed by the least significant bytes of the HARD and SOFT IDs exclusive OR'ed. All CPE's which provide alarm transport shall implement WAIL. The data shall not be encrypted in this message. This WAIL shall output twice each second until the Scanner polls the CPE. If the Scanner has not polled the CPE after WAIL has been sent for 120 seconds, the CPE should assume the Scanner is down.

When CPE is connected to the network, it must carry a 16 bit binary identification number. This number will be referred to as the hard identification. The CPE must transmit this number to the Scanner when requested. This number is used in other data messages and in the encryption process described later.

When the CPE is connected, the Scanner will transmit another 16 bit binary identification number. The CPE must receive and store this number for future use. This number will be referred to as the soft identification.

When the first information bit of data coming from the Scanner indicates that data is encrypted, the data to be encrypted will follow the second information bit and extend through the "end of the message," including the "checksum.".

The "checksum" is a four bit wide quantity found by summing the data in question starting with 00EA and the carry bit is added back to the least significant bit. This number is used in other data messages and in the encryption process. The checksum is then inverted. Additionally, CPE must encrypt most messages, using the same data boundaries.

All messages except the "WAIL" message, must carry one or more "checkouts." These "checkouts" will also be included in Scanner to CPE transmissions.

All data in messages after the EA bits and including the checkouts undergo data encryption. Three types of encryption algorithms masks are used. The particular algorithm employed is a function of the message type. The algorithms are:

- HARD/SOFT
- HARD/HARD
- SOFT/SOFT

These names refer to the Hard and Soft Identification (ID) numbers.

Assuming the following conventions:

H1= most significant HARD ID byte

H0= least significant HARD ID byte

S1= most significant SOFT ID byte

S0= least significant SOFT ID byte

M1= most significant mask byte

M0= least significant mask byte all encryption algorithms use the formula:

M1= [i + 33 hex]

M0= [j + 33 hex]

Where:

i=H0 and j=S0 for the HARD/SOFT encryption type.

i=H1 and j=H0 for the HARD/HARD encryption type.

i=S1 and j=S0 for the SOFT/SOFT encryption type.

The mask is then exclusive OR'ed into the first 4 complete nibbles of the message. For example, if the HARD ID is 1234 hex and the SOFT ID equals 5678 hex, the message 9ABC would be encrypted to read following in the HARD/SOFT encyryption:

i = H0= 34 hex

j = S0= 78 hex

M1 = i + 33 hex = 67 hex

M0 = j + 33 hex = AB hex

msg = 9ABC XOR 67AB = FD17 hex

Thus, the complete encrypted message is FD17 hex. The host will identify what the SOFT ID is, but can not identify what the message is. After the data is encrypted, the message goes through a 4-to-5 bit translation designed to prevent any message from having 4 adjacent ones. The following table describes the encode/decode scheme:

DATA	TRANSLATION
0000	00100
0001	00101
0010	00110
0011	00111
0100	01100
0101	01001
0110	01010
0111	01011
1000	10100
1001	10001
1010	10010
1011	10011
1100	10101
1101	10110
1110	10111
1111	01101

SYNC and the EA bits shall not go through the translation.

4.2 Host-agency

Messages begin with a line feed and are terminated with a carriage return from host to agency. Two types of messages are sent in poll and return:

- Poll without data
- Poll with data

In return, the agency will send two types of messages to the host computer:

- Return without data
- Return with data

In the case that a message has to be acknowledged; ASCII 'A' shall immediately precede the line feed. Additional line feeds may be in the message before the carriage return and should be interpreted according to the protocol. The character immediately preceding carriage return is the checksum, calculated as follows:

- Add CHR A and all CHR's from <LF> until end of received, without <CR>.
- And the result with 3F.
- OR the number by 20.
- This will be the checksum <CKS> in the received messages.
- The checksum is inserted before <CR>.

The host is the master of communications and polls the agency. The agency shall not transmit data onto the line unless it receives a message with proper checksum. Upon receipt of a poll, the agency will transmit the next message it wishes to send.

If the host has failed to poll the agency for 20 seconds, the agency should inform the user of a host-agency communications failure.

5. Packet Layer

5.1 Scanner-CPE

The packet layer definitions shall be implemented in full to assume compliant operations and hence, reliable communications.

Scanner-to-CPE messages fall into the following types (each field described at the end of this section):

RQ1: Poll for Change - This is the normal poll message of the Scanner asking the CPE for new information it may have. It is of the following format:

SYNC EA PPPP HHHH 0000 KKKK

RQ2: Poll for Status - This is a "forced poll," that is the Scanner is requesting the current state of the CPE. It is of the following format:

SYNC EA PPPP HHHH 0001 KKKK

RQ3: Pin State Ackknowledgement - This is the mechanism by which an agency may acknowledge receipt of a pin state change. It is of the following format:

SYNC EA PPPP HHHH 1000 KKKK XYAA ZZZZ LLLL

RQ4: Data Packed - This is a mechanism for the Scanner to send user defined data packets to the CPE. The reader shall note that this has been defined in the cases of RQ3 and RQ6. It is of the following format:

SYNC EA PPPP HHHH 1nnn KKKK ...data... LLLL

RQ5: Poll for HARD ID - This is a request for the CPE to tell the Scanner its HARD ID. It is of the following format:

SYNC EA AAAA BBBB 0110 KKKK

RQ6: Write SOFT ID - This message allows the Scanner to tell the Scanner its SOFT ID. It is of the following format:

SYNC EA PPPP HHHH 1010 KKKK 1100 0000 [2 byte SID] LLLL

RQ8: This message allows the Scanner to verify the SOFT ID and CPE. It is of the following format:

SYNC EA PPPP HHHH 0100 KKKK

RQ9: Output On - This command is used to tell the CPE to turn on its relay (if this applied to the CPE). It is of the following format:

SYNC EA PPPP HHHH 0010 KKKK

RQ10: Output Off - This command turns off the relay (if applicable). It is of the following format:

SYNC EA PPPP HHHH 0011 KKKK

CPE-to-Scanner message falls into the following types (each field described at the end of this section):

RE1: No Change in CPE Status - This is the normal "I'm okay but nothing is new" CPE response. It is of the following format:

SYNC HHHH PPPP 0000 KKKK

RE2: Medium Alarm Report - This allows the CPE to send either one or two pin state changes in a message. It is of the following format:

SYNC CCCC CCCC 0011 KKKK ZZZZ TTTO ZZZZ TTTO LLLL

RE3: Long Alarm Report - This allows the CPE to send its complete state. It is of the following format:

SYNC CCCC CCCC 0100 KKKK [44 bit string] LLLL

RE5: Data Packet - This allows the CPE to send user defined to Scanner. The user should see RE6 to be sure functionality shall not conflict. It is of the following format:

SYNC CCCC CCCC 1nnn KKKK ...data... LLLL

RE6: Transmit HARD/SOFT ID

SYNC CCCC CCCC 1010 KKKK 0100 0000 [2 byte HID] LLLL

-OR-

SYNC CCCC CCCC 1010 KKKK 0100 0001 [2 byte SID] LLLL

The fields are as follows (each character represents a bit):

SYNC - As previously described

EA - As previously described

PPPP HHHH - HARD ID "window" used to determine if two CPEs have been electrically connected via a phone call.

PPPP is a random pointer to the first bit of a 4 bit "window" into the HARD ID. For example, if PPPP = 8 then HHHH should equal the value of bits 8 thru 11 of the HARD ID. Thus, if PPPP equals 14 then HHHH should equal [b1] [b0] [b15] [b14] of the HARD ID.

AAAA BBBB - A special case of the PPPP HHHH field which should not be checked but used as PPPP HHHH.

HHHH PPPP - On response, the received PPPP HHHH field is nibble reversed to allow the Scanner to verify data.

CCCC CCCC - CPE sequencing number. Session Layer will explain its values.

KKKK - The checksum of all previous nibbles up to and including 00EA.

LLLL - The checksum of all previous nibble up to and but not including KKKK.

nnn - The number of bytes in the ...data... packet. The number of bytes equals nnn+1 except for nnn=111 in which case the number is 9.

...data... - Data as defined in the nnn field.

X - Don't care field

Y - Must be 0

AA - if 00:Acknowledge to a restore or close

- if 01:Acknowledge to a fault

- if 10:Acknowledge to an alarm or opening

- if 11:Not used

ZZZZ - Pin Zone in Question

0000: State change not applicable - used when sending a medium alarm packet and only 1 pin has change state.

0001-1011: Pins 1-11

1100: Box Open (tamper)

1101: AC Power Fail

1110: DC Power Fail

1111: Self Test Failure

TTT Pin States:

000: Used with Pin=0 only

Reporting State

001: Alarm: This alarm has not yet been acknowledged by the Alarm Service Provider.

010: Restore: This alarm has been acknowledged by the Alarm Service Provider and the alarm condition is no longer present.

011: Open: This alarm has not yet been acknowledged by the Alarm Service Provider. For example, this can be used for routine door openings.

100: Close: This alarm has been acknowledged by the Alarm Service Provider and alarm condition is no longer present. For example, this can be used for routing door closings.

101: Outstanding: The Alarm Service Provider has acknowledged the alarm and the alarm is still present.

110: Normal: There is no alarm and no action is required by the Alarm Service Provider.

111: Fault: There is a fault detected in the local loop.

[44 bit string] - Bit string to show current state of all pins:

1112 2233 3444 5556 6677 7888 999A AABB BCCD DEEF FPRX

Where:

The TTT fields of pins 1-11 are in fields 1 thru B.

Fields C thru F are the box open, AC fail, DC fail, and self test fields whose values are:

00: Normal

01: Alarm

10: Restored

11: Outstanding

P: Output State 1=on, 0=off

R. Re-transmit Bit. If set, this message is a re-transmission of a previous state change was not acknowledged within 3 minutes of original transmission.

X: Reserved for future. Set to 0 for present.

The Scanner will recognize four different reporting states for each of the alarms. These are:

- Normal
- Alarm
- Fault
- Open

Scan-Alert^{SM} COE is in continual communication with the alarm detection CPE. The COE will only accept transitions from a specific reporting state to a few other states. For this reason, the CPE may only transition from a specific report state to a set of other report states as follows (except as shown below, each transition requires communication between the CPE and the Scanner):

EXISTING REPORT STATE	EVENT	NEW REPORT STATE
Normal	Change in Input Status	New Alarm
	Change in Input Status	New Opening
	Alarm Loop Fault is Detected	New Fault
New Alarm	Acknowledgement from Alarm agency	Outstanding*
New Opening	Acknowledgement from Alarm agency	Outstanding*
New Fault	New Alarm Input (despite fault)	New Alarm
	New Opening Input*	
	Acknowledgement from Alarm agency	Outstanding*
Outstanding	Alarm Input Stops	New Restore
	Alarm Input Stops	New Closing
	Fault Stops	Normal*
New Restore	New Alarm Input	New Alarm
	New Fault Input	New Fault
	Acknowledgement from Alarm agency	Normal*
New Closing	New Opening Input	New Opening
	New Fault Input	New Fault
	Closing Acknowledged from Alarm agency	Normal*

* Optional Reporting

5.2 Host-agency

Host-to-agency messages fall into the following types (each field described at the end of this section):

Normal "No Data" Poll - This message is sent by the host as a normal poll. It signifies that the host has no new messages for agency but is requesting information from agency. This message does not require the acknowledgement character. Its format is:

<LF> <SP> <*> <CR>

Type 0 - This message tells the agency to output the "text" field to the agency's CRT for viewing by agency personnel. Its format is:

<LF> <SP> <0> ...text... CK4 <CR>

Type 1 - This message provides the agency with information from the alarm detection. Its format is:

<LF> <SP> <1> SID DDDD HHHH XNNN CC M CK1 ...data... CK2 CK4 <CR>

Type 2 - This is the same as a Type 1 message except that it is from a CPE which was previously not responding. Its format is :

<LF> <SP> <2> SID DDDD HHHH XNNN CC K CK1 ...data... CK2 CK4 <CR>

Type 3 - This message denotes a CPE as not responding and returns any data which might have been sent by the CPE. Its format is:

<LF> <SP> <3> SID DDDD HHHH XNNN SS K ...data... CK4 <CR>

Type 4 - Not used.

Type 5 - This message denotes a CPE was reset. Its format is:

<LF> <SP> <5> SID DDDD HHHH XNNN CC M CK1 ...data... CK2 CK4 <CR>

Type 6 - This message returns to the CPE a message which could not successfully be sent to the Scanner. Its format is:

<LF> <SP> <6> SID JNNN HH L ...data... CK4 <CR>

Type 7 - This message returns information sent from the agency to the host with the reason for its return. Its format is:

<LF> <SP> <7> SID JNNN <SP> R L ...data... CK4 <CR>

Type 8 - This message notifies the agency that the Scanner and host had a message number mis-match. Its format is:

<LF> < SP> <8> SID DDDD HHHH 0NNN CC HH SS CK4 <CR>

Type 9 - This message contains a query which must be displayed to the agency's CRT and responded to by the agency's operator. Its format is:

<LF> <SP> <9> ...text... CK4 <CR>

Type 10 - This message contains a network alarm or restore message in its test field. Its format is:

<LF> <SP> <A> T ...text... CK4 <CR>

Agency-to-host message fall into the following types (each field described at the end of this section):

Normal "No Data" response - This message is sent by the agency as a respond to a poll. It signifies that the agency has no new messages for the host but is operating correctly. This message does not require acknowledgement. Its format is:

<LF> <*> <CR>

Type 0 - This message is used to send a variety of commands to the host. Its format is:

<LF> <0> ...text .. CK4 <CR>

Type 1 - This message is used to send a variety of commands to the alarm detection CPE. Its format is:

<LF> <1> SID NNNN K ...data... CK4 <CR>

Type 9 - This is the response to a host message Type 9. Its format is:

<LF> <9> ...TEXT... CK4 <CR>

The above fields are as follows:

<...> - Single ASCII character represented inside brackets

SID - Scanner ID. 1 byte. Scanner 1 is 20 hex, Scanner 2 is 21 hex, and so forth.

DDDD - Data field. 4 bytes. Not currently implemented. Left as 4 space characters.

XNNN - CPE field. 4 bytes. X is the ASCII character of the X/R which was used to poll the CPE. Set to ASCII 0 in messages from the agency to host. NNN is the ASCII hexadecimal representation of the CPE number. ASCII "000" is CPE 1, "001" is CPE 2, "00F" is CPE 16, and so forth up to "7FF" which is CPE 2048.

HHHH - CPE's HARD ID. 4 bytes. This field is the ASCII hexadecimal respresentation of the HARD ID. For example, ASCII "89AB" means HARD ID 89AB.

CC - Current CPE sequence number. 2 bytes. Logically AND each of the bytes with 0F hex to obtain 2 nibbles which can be combined into a byte with the first nibble being the most significant.

HH - Current Scanner sequence number according to the host. 2 bytes. Decode the same as the CC field previous count.

SS - Current Scanner sequence number. 2 bytes. Decode the same as the CC field. Current count.

CK1, CK2 - Checksums which were used for CPE-Scanner communications. 1 byte each. Delivered to remain in compliance with Computer Inquiry II rules but provides no useful information and can be ignored.

CK4 - Message checksum. 1 byte. See "Link Layer" for explanation.

R - Reject reason field. 1 byte. Tells agency why message was returned.

<SP>=None

<">=Output on not enabled for this CPE

<!>=Agency dies not own this CPE

<#>=CPE not UP

T - Network alarm/restore type

<SP>=Network restore condition

<*>=Network alarm condition

J Control bit for type 6 and 7 message only where J = 1 then:

L= 1 Poll CPE

2 Output off

3 Output on

8 Acknowledge pin

J= 3 then:

L= 0 UP CPE wo/data

L=1 OHP w/data

Data= 1 Enable

0 Disable

3 Delay off

2 Not used

L - Control field for type 6 and 7 message only.

M - Control field for the ...data... field. 1 byte. Content and meaning along with length of ...data... field is a follows:

'0': No change in CPE status. Len = 0 bytes.

'1': Invalid

'2': Invalid

'3': Medium Alarm Report. Len = 4 bytes.

'3"' Long Alarm Report. Len = 11 bytes.

'5': Invalid

'6': Invalid

'7': Invalid

'8': Data packet — Len = 2 bytes. (Also used for acknowledge pin)

'9': Data packet. — Len = 4 bytes.

'A': Data packet. — Len = 6 bytes.

'B': Data packet. — Len = 8 bytes.

'C': Data packet — Len = 10 bytes.

'D': Data packet. — Len = 12 bytes.

'E': Data packet. — Len = 14 bytes.

'F': Data packet. — Len = 18 bytes.

K - Control field for the ...data... field. 1 byte. Content and meaning along with length of ...data... field as follows:

'0': Type 0 command failed — Len = 0 bytes

'1': Poll CPE — Len = 0 bytes

'2': Output CPE off — Len = 0 bytes

'3': Output CPE on — Len = 0 bytes

'4': Invalid

'5': Invalid

'6': UP CPE returned to agency — Len = 0 bytes

'7': Invalid

'8'-'F': See M field for meaning

...data... - Data to/from CPE. Logically AND each with 0F hex to obtain actual data nibbles and combine data nibbles as was explained in CC field. If odd number of nibbles use 0 for final nibble. Several cases are explained below.

(1) Medium Alarm Report. Reports 1 or 2 pin state changes.

Nibbles 1 &3: Pin Number

0: Ignore this nibble and the next

1 & 11: Pins 1-11

12: Box tamper

13: AC fail

14: Battery fail

15: CPE self test

Nibbles 2 &4: Pin State. Shift Right 1 bit

0: Used only for pin=0

1: Alarm

2: Restore

3: Opening

4: Closing

5: Outstanding condition

6: Normal

7: Fault

(2) Long Alarm report. The CPE sends its entire pin state in one message. Compacts data into a 44 bit string and interpret bits as below:

111 222 333 444 555 666 777 888 999 AAA BBB CC DD EE FF PRX

111 thru BBB: Pin state of pins 1 thru 11. See above for contents.

CC thru FF: State of in order, box, tamper, AC fail, DC fail, and CPE self test.

Contents are:

0: Normal

1: Alarm

2: Restore

3: Outstanding

P: State of Output Relay. 0=off, 1=on

X: Reserved for future use. Set to 0 for present.

(3) Special cases of the data packet, not to be used as an ordinary data

packet.

(3a) Pin State Acknowledgement. Len=2 bytes (K or M = '8'). The following content is the ...data... field.

Nibble 1: 3S hex where S is the pin state to acknowledge

S=0: Acknowledge of reset or close

S=1: Acknowledge of fault

S=2: Acknowledge of alarm or open

Nibble 2: 3p hex where p is the pin number to acknowledge

(3b) CPE responds to UP CPE command by sending agency its HARD ID. Len=6 bytes (K or M = "A"). Once the ...data... is combined into 3 bytes, the first byte is the 40 hex, the second is the most significant byte of the HARD ID and the third is the least significant.

Note: 40 hex, tells us the message contains the HARD ID.

(3c) Data packet. Up to 18 nibbles of user defined data. To transmit, logically OR data each nibble with 30 hex.

6. Session Layer

This is the highest defined layer of the protocol.

6.1 CPE Sequence Number

The alarm detection CPE shall generate a sequence number to allow the redundant sides of the network to discard duplicate messages which have taken different paths to the same host. Upon power up the sequence number shall be zero and increment each time the CPE transmits any REX message except RE1. The sequence number is 8 bits wide and shall wrap around to zero as needed.

6.2 Communication Initialization

The alarm detection CPE shall not output any information (i.e., low-tone or WAIL) until it is initialized, following power up or power cycling sequence (i.e.,"RESET"). Upon "RESET" the CPE shall be uninitialized, and shall not respond until the UP-CPE command is received and responded to, i.e., "was reset". The Scanner sends an encoded RQ5. The CPE shall then respond with an unencoded RQ6 with the HARD ID. The Scanner then sends an RQ6 encoded HARD/HARD to write the SOFT ID with the CPE. The CPE shall then keep low tone off to solicit a poll RQ1 from the Scanner. The CPE shall respond to the RQ1 with an RE3 encoded HARD/SOFT. At this time communications are initialized and the CPE shall output low-tone or WAIL based on the protocol and state of the system. Thereafter, the CPE shall not respond to unencoded messages of any type.

6.3 Responses to Scanner Commands

Each of the RQ messages requires a certain type of encoding and response from the CPE. None of these responses are applicable until after the CPE has received the UP command.

VI.3.1 RQ1

This is the normal Scanner poll message. It is always encoded HARD/SOFT. The CPE may respond with RE1, RE2, or RE5 as conditions dictate. Any response shall be encoded HARD/SOFT.

VI.3.2 RQ2

This is the "forced poll" state typically issued from the agency. The user is requesting the current information on the state of the CPE. This shall be encoded HARD/SOFT. The CPE shall respond with either an RE3 or RE5. Any response shall be encoded HARD/SOFT. The CPE shall turn off low-tone after responding to a poll for status, this will cause the Scanner to poll for change, which is the acknowledgement that the status message was received. (The forced poll is also known as a Solicited poll.)

VI.3.3 RQ3

This is a pin state acknowledgement for alarm transport. If the application is non-alarm, and the interfaced agency does not send pin state acknowledgements, this message will not be sent. If it is sent, it shall be used to resolve the current state of pin. Below shows the allowable states a pin can have:

NORMAL ---> ALARM >>> OUTSTANDING ---> RESTORE >>> NORMAL

NORMAL ---> OPEN >>> OUTSTANDING ---> CLOSE >>> NORMAL

NORMAL ---> FAULT >>> OUTSTANDING ---> RESTORE >>> NORMAL

Where:

---> State change is made by the CPE as needed.

>>> State change made upon receipt of state acknowledgement.

The state changes alarm, fault, restore, open and close shall be sent by the CPE to the Scanner upon detection. Transmission of the Outstanding and Normal states are optional.

VI.3.4 RQ4

This message allows the Scanner to send user defined data to the CPE. It shall be encoded HARD/SOFT. The CPE shall respond to the Scanner as if an RQ1 were received.

VI.3.5 RQ5

This message allows the Scanner to request the HARD ID at any time. After the CPE is UP this message shall be encoded SOFT/SOFT for the CPE to respond. The CPE shall send back a SOFT/SOFT encoded RE6 with the HARD ID.

VI.3.6 RQ6

This message allows the Scanner to write a new SOFT ID to the CPE. It is encoded HARD/HARD. After the CPE is UP this message shall be handled as an RQ1.

VI.3.7 RQ8

This message allows the Scanner to verify the SOFT ID has been sent and received by the CPE. It shall be encoded HARD/HARD. The CPE shall respond with a HARD/HARD encoded RE6 with the SOFT ID.

VI.3.8 RQ9 and RQ10

These messages turn the output relay on and off. They shall be encoded HARD/SOFT. See RQ1 for handling.

6.4 Host-agency Overview

The agency equipment allows an agency to monitor alarm detection CPEs in various locations. It is necessary to understand the basic terminology to understand CPE communications. CPEs are UP when they are in normal communications mode with the network. CPEs which have not been initialized (UP) into the system are DOWN.

6.5 Communication Initialization

CPEs must be UP before they will communicate with the network. To do this, the agency must request U S WEST to add the alarm detection CPE to the system and data base with the proper options and connections and then have the agency based CPE send the UP CPE command for the proper Scanner-CPE number. If the CPE is operating correctly, communications will begin at this time and the agency based CPE will be able to receive messages from the alarm detection CPE.

6.6 Host Message Handling

Each of the Host messages require a certain action on the part of the agency. They are explained below.

- Immediate Response To Any Poll

  The agency should send whatever next message it wishes to send.

- Message Types: 0, 2, 3, 5, 6, 7, 8, 10: agency CPE should display this message on its CRT in a manner readable to the user as it pertains to the particular application.

- Message Type 1: The agency CPE should display this message on its CRT in a manner readable to the user and queue messages to acknowledge pins for the states alarm, restore, open, close, and fault if applicable to the intended use of the system.

- Message Type 9: The agency CPE should display this query on its CRT. The user's response should be packaged as a Type 9 response and queued for transmission.

6.7 Agency Message Handling

Each of the agency messages require a certain action on the part of the Host. They are explained below.

Message Type 0: Allows the agency to pass commands to the host. Currently they include (but are not limited to):

HELP

UP STU

DOWN STU

ENABLE OFF-HOOK POLLING

DISABLE OFF-HOOK POLLING

SEND SUPERVISOR

POLL STU

For a complete list of commands, the user should type HELP. These commands are sent as text via ASCII characters and interpreted by the host to make future additions and local variations possible without changing agency software.

Message Type 1: Allows the agency to send information to the alarm detection CPE. See the packet layer for a detailed description of choices.

k = '1': Poll CPE

k = '2': Output Off

k = '3': Output On

k = '8': Pin Acknowledgement

Message Type 9: Allows the agency to respond to a Type 9 host command. Sent as text to prompt the agency for input.

6.8 System Requirements of the Agency

The agency should be able to process messages at a rate of at least 1 per second. If the agency does not acknowledge a host message, the host will attempt to re-transmit it. However, if greater than a pre-determined threshold number of messages are waiting for the agency, the host will begin to purge non-acknowledged messages. When the host is busy it will not acknowledge agency messages. If this happens a pre-determined number of times, the agency should alert alarm subscribers that messages are not being taken and to try later. In the event the host link is down, the agency should de-queue messages for the host and alert the alarm subscribers.

7. Definitions

7.1 Acronyms

COE	Central Office Equipment
CPE	Customer Provided Equipment
DTE	Data Terminal Equipment
FCC	Federal Communications Commission

7.2 Glossary

ASCII

American Standard Code for Information Interchange. A standard 8-bit information code used with most computers and data terminals.

bit

A binary digit. A unit of data in binary notation.

bps

Bits per second, e.g., 1200 bps. In data transmission, it is the number of binary zero and one bits transmitted in 1 second. Modern terminology uses "bit/s," e.g., 1200 bit/s.

byte

A consecutive number of bits usually constituting a complete character or symbol. If the length of the byte is not specified it is conventionally assumed to have a length of 8-bits. In the Digital Data System, a byte refers to an arbitrary group of 8 consecutive bits; it does not correspond to a byte of customer data.

dBrnc

Weighted noise power in dBm measured by a noise measuring set with C-Message weighting.

Loaded Cable

Inductance, in the form of "Load Coils", is placed on longer metallic cables to improve the cable's voice transmission performance.

Parity Check

Making the number of ones in a grouping of bits either always even or always odd. This permits detection of bit groups that contain single errors. It may be applied to characters or blocks.

Ringer Equivalence

A numeric indicator which is an inverse function of on-hook impedance and resistance, called the Ringer Equivalence Number (REN). All registered terminal equipment which can affect on-hook impedance and resistance are assigned a REN. The sum of all such REN's on a given telephone line shall not exceed 5 but may be fewer depending on the ringing voltage source and the facility serving the line (FCC Part 68.312).

STU

Subscriber Terminal Unit.

8. References

8.1 Bellcore Technical Advisory

TA-NPL-000912 Compatibility Information for Telephone Exchange Service, February 1989.

8.2 Other Technical References

Part 68, Connection of Terminal Equipment to the Telephone Network of the Federal Communications Commission's "Rules and Regulations" may be purchased from the Superintendent of Documents, Government Printing Office, Washington, D.C. 20402.

8.3 U S WEST Communications, Inc. Technical Publications

77365 Network Channel and Network Channel Interface Combinations, Issue A, March, 1989.

8.4 Trademarks

Scan-Alert[SM] Service Mark of U S WEST Communications, Inc.