Conettix Alarm Communications Troubleshooting Flowchart

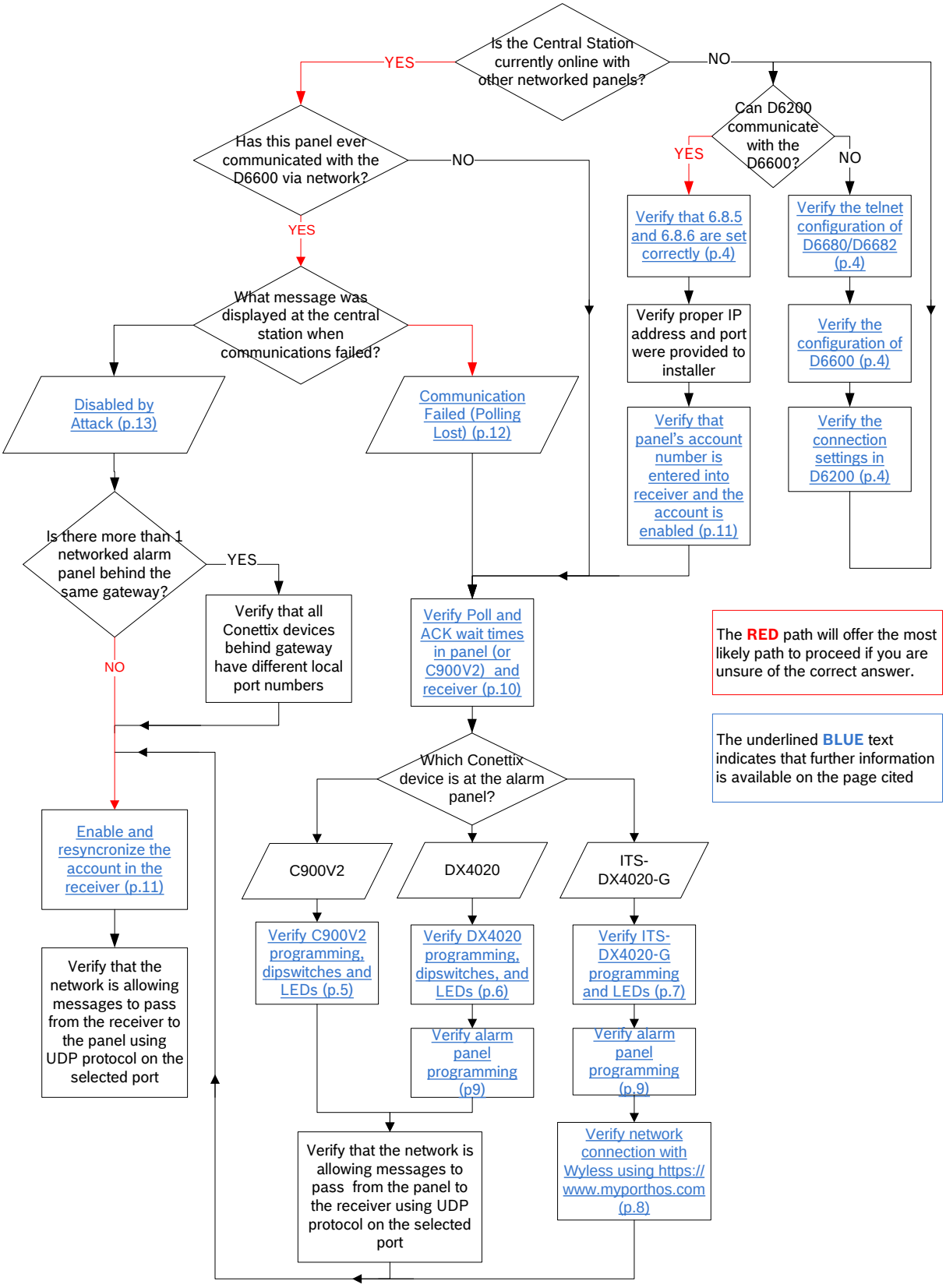


Table of Contents

Conettix Alarm Communications Troubleshooting Flowchart 1
Special Note 3
D6680/D6682 Configuration 4
D6600 Configuration 4
D6200 Configuration in Administration | Connection settings. 4
C900V2 Configuration 5
DX4020 Configuration 6
ITS-DX4020-G Configuration 7
ITS-DX4020-G Wireless Network Connection Details 8
Alarm Panel Programming Configuration (Examples) 9
Recommended Poll, ACK Wait, and Retry Count Settings 10
D6600 Conettix Account Database 11
Communications Fail (Polling Lost) - Explained 12
Disabled by Attack - Explained 13

Special Note

Steps contained in this document are for troubleshooting purposes only. Once troubleshooting is complete, you may need to reconfigure your system to match your specific operating requirements. This document is not intended to replace other documents and should not be used for installation support. Please consult the referenced product's Installation and Operation Guides during use of this document.

D6680/D6682 Configuration

- Firmware
  - Scroll to beginning of telnet session.
  - Locate "software version."
  - Upgrade the module to latest firmware.
    - D6680 = 5.8.8.4 (as of 4/12/2011)
    - D6682 = 6.5.8.0 (as of 4/12/2011)
- Server Configuration
  - Verify IP address, gateway, and subnet mask with the network administrator.
- Channel 1 or Channel 2 Configuration. (Whichever one is connected to COM 4 or COM 1 on the D6600)
  - Baudrate: 38400
  - I/F Mode: 4C
  - Flow: 00
  - Port: 7700 (can vary by customer's choice)
  - Connect Mode: CC
  - Datagram Type: 00 or 02. Must match D6600 option 6.8.6
- Security Settings
  - Enable encryption.
    - If set to Yes, encryption key must match the encryption key in D6680/D6682, D6200, DX4020, and C900V2
    - If set to *No*, encryption must be disabled in D6680/D6682, D6200, DX4020, and C900V2

D6600 Configuration

- Option 6.1.5
  - Set to 1 for D6680
  - Set to 2 for D6682
- Options 6.4.1, 6.4.2, or 6.4.3: IP address of computer running the D6200 software
- Option 6.4.4 (may be reserved): Port number of D6680/D6682
- Option 6.4.5: 1
- Option 6.8.5
  - Set to 1 for NNC Mode (recommended). Note: If you change this, verify option 6.4.4 again.
  - Set to 0 for Static Mode
- Option 6.8.6
  - Set to 1 for NNC Mode
  - Unavailable if in Static Mode

D6200 Configuration in Administration | Connection settings

Make sure that Receiver IP and Port match the IP address and Port number programmed into the D6680/D6682 configuration. Also verify that the encryption setting matches the enable encryption option in the D6680/D6682 telnet configuration under Security Settings.

C900V2 Configuration

Note: If the C900V2 is not responding properly, try using filtered power and program at least a 7-digit phone number in the alarm panel for central station communications.

Dipswitches

Consult the *C900V2 Installation Guide* for a full description of all dipswitches.

- 1 – 4 and 10 configure the handshake tone provided by the C900V2 to the panel
- Dipswitch 7 controls the rate of polling messages to the central station (75 or 240 seconds). See *Table 2*.
- Dipswitch 8 should be set to ON for a 6 second delay after dialing before providing the handshake.
- Dipswitch 9 must be ON to enable Anti-Replay

Telnet

- Firmware
  - Scroll to beginning of telnet session.
  - Locate "software version."
  - Upgrade the module to latest firmware.
    - Xport - 01 = Firmware version 5.8.8.3 (as of 4/12/2011)
    - Xport - 03/04 = Firmware version 6.1.8.3 (as of 4/12/2011)
- Server Configuration
  - Verify the IP address, gateway, and subnet mask with the network administrator.
- Channel 1 configuration
  - Baudrate: 9600
  - I/F Mode: 4C
  - Flow: 00
  - Port: 7700 (can vary by customer's choice)
  - Connect Mode: CC
  - Datagram Type: 01
  - Remote IP Address: IP address of central station
  - Remote Port : Network port of central station
- Security Settings
  - Enable encryption:
    - If set to Yes, encryption key must match the encryption key in D6680/D6682, and C900V2.
    - If set to No, encryption must be disabled in D6680/D6682, D6200, and C900V2.

LEDs

- System LED turns green and blinks rapidly.
  - If not, this implies a communications issue between the C900V2 and the central station receiver.
- Dialer LED turns green. Dialer LED blinks green when C900V2 is off hook with panel.
  - If not, this implies a communications issue between the C900V2 and alarm panel.

DX4020 Configuration

Dipswitches

- Set to Address 88 (Address 92 is also available for GV3 panels. Configured in Routing)

Telnet

- Firmware
  - Scroll to beginning of telnet session.
  - Locate "software version."
  - Upgrade the module to latest firmware.
    - Xport - 01 = Firmware version 5.8.8.3 (as of 4/12/2011)
    - Xport - 03/04 = Firmware version 6.1.8.3 (as of 4/12/2011)
- Server Configuration
  - Verify the IP address, gateway, and subnet mask with the network administrator.
- Channel 1 configuration
  - Baudrate: 9600
  - I/F Mode: 4C
  - Flow: 00
  - Port: 7700 (can vary by customer's choice)
  - Connect Mode: CC
  - Datagram Type:

Panel Version	Datagram Type
G Series: Firmware 6.9 and lower	00
G Series: Firmware 7.0	02
GV2 Series: Firmware 7.05 and lower	00
GV2 Series: Firmware 7.06 and higher	02
GV3 Series: All versions	02
FPD-7024	02

- Security Settings
  - Enable encryption:
    - If set to Yes, encryption key must match the encryption key in D6680/D6682, D6200, andDX4020.
    - If set to No, encryption must be disabled in D6680/D6682, D6200, and DX4020.

LEDs

- BUS – XMIT and BUS – RCV blink once every second.
  - If not, this implies a communications issue between the DX4020 and alarm panel.
- SER – TX blinks when the DX4020 sends a message to the central station over the network.
  - If not, this implies a programming issue in the panel
- SER – RX blinks when the DX4020 receives a message from the central station over the network.
  - If not, this implies a programming issue at the central station or a network issue.

ITS-DX4020-G Configuration

Jumper

- The Config Mode jumper must be open for alarm communications

Programming

- Firmware
  - Displays when connecting with a USB cable before entering the password.
  - Upgrade the module to latest firmware.
    - Version 1.4.3 (as of 4/12/2011)
- Basic Parameters
  - GPRS APN: telargo.t-mobile.com (as provided by https://www.myporthos.com)
  - Bus Address (by panel type):
    - GV2/GV3 Series: 88 (Address 92 is also available for GV3 panels. Configured in Routing)
    - FPD-7024 using GPRS Mode: 250
    - Control panels using Contact ID: 0
  - AES Encryption: 0 (disabled), or 1 (enabled)
  - AES Encryption Key:
    - If AES Encryption was set to 0, disregard this field.
    - If AES Encryption was set to 1(enabled), encryption key must match the encryption key in D6680/D6682, and D6200.
  - Communication paths available (by communication mode):
    - GPRS Mode (ex: GV2/GV3 Series, FPD-7024, Easy Series): 2
    - GSM Mode (ex: non-Bosch panels, FPD-7024, Easy Series): 3
- Advanced Parameters
  - GPRS ACK timeout: See *Table 2*.
  - Trouble Reporting Delay: 120 (Can get false errors if set too low.)
  - Enable low signal strength reporting: Y (If N, will continue trying at lower levels, but may not work under all conditions.)

LEDs

- If the LEDs on the module do not match the table below, consult the ITS-DX4020-G Installation and Operation Guide's Troubleshooting chapter.

Table 1: ITS-DX4020-G LED Status

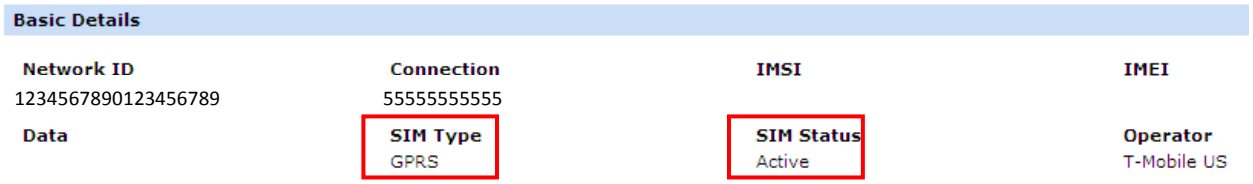
Normal Operating Modes	STATUS	CELL IP	AUDIO ACTIVE	SS1	SS2	SS3	BUS
GPRS (IP) Normal Operation On	ON	ON	X	Signal Strength			ON
GSM (PSTN) Normal Operation	ON	OFF	X	Signal Strength			OFF
Audio Off-Hook	ON	X	ON	Signal Strength			X

ITS-DX4020-G Wireless Network Connection Details

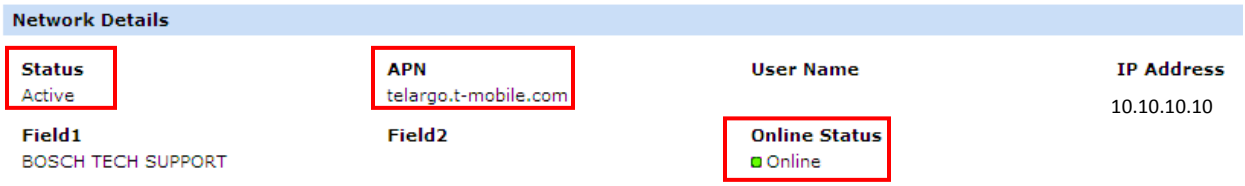
The APN and wireless network connection details of the ITS-DX4020-G can be viewed by browsing to the Wyless Porthos Gateway at https://www.myporthos.com. Log in with the username and password provided to you by Wyless.

Click on the Network tab and browse to the Preview SIM page of the appropriate SIM card.

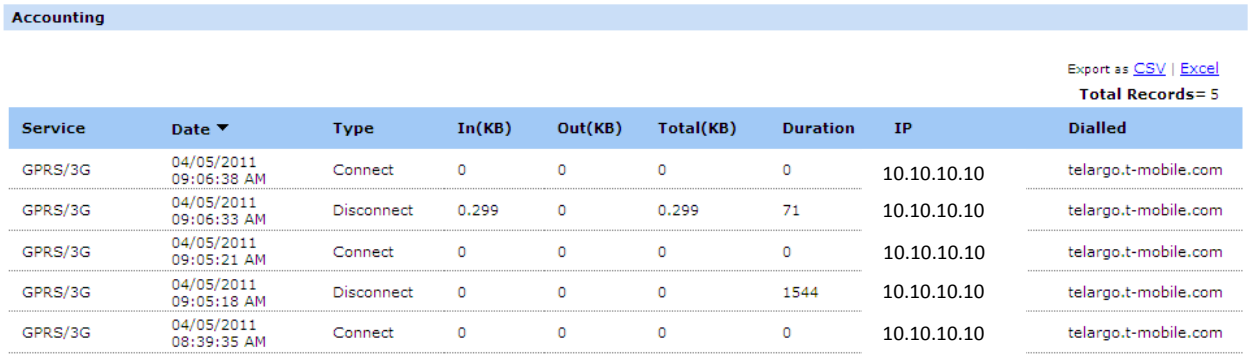
In the Basic Details section, verify the SIM Type and SIM Status.



In the Network Details section, view the Status, Online Status, and verify the APN.



In the Accounting section, review the wireless network connection history.



Service	Date	Type	In(KB)	Out(KB)	Total(KB)	Duration	IP	Dialled
GPRS/3G	04/05/2011 09:06:38 AM	Connect	0	0	0	0	10.10.10.10	telargo.t-mobile.com
GPRS/3G	04/05/2011 09:06:33 AM	Disconnect	0.299	0	0.299	71	10.10.10.10	telargo.t-mobile.com
GPRS/3G	04/05/2011 09:05:21 AM	Connect	0	0	0	0	10.10.10.10	telargo.t-mobile.com
GPRS/3G	04/05/2011 09:05:18 AM	Disconnect	0	0	0	1544	10.10.10.10	telargo.t-mobile.com
GPRS/3G	04/05/2011 08:39:35 AM	Connect	0	0	0	0	10.10.10.10	telargo.t-mobile.com

Alarm Panel Programming Configuration

These following examples show configuration panels connecting to the D6600 using Conettix as the primary method of communications and PSTN as the backup. Please adjust the settings as necessary to match your site's requirements.

GV3 Panel Version 8.11

- Panel Wide Parameters
  - Phone and Phone Parameters
    - Phone 1: Phone number of central station
  - Routing
    - Primary Path Device: SDI 88 Path 1 (SDI 92 Path 1 is also available)
    - Backup Path Device: Phone 1
- Area Wide Parameters | Area/Bell Parameters, Open/Close Options | Area 1 – 8
  - Area 1 Account Number: Verify that you entered the correct account number
- AUXPARM | Enhanced Communications
  - Enable Enhanced Communications: Yes
  - Path 1 IP Address: IP address of central station
  - Path 1 Port Number: Port number of central station
  - Path 1 Poll Rate: See *Table 2*
  - Path 1 ACK Wait Time: See *Table 2*
  - Path 1 Retry Count: See *Table 2*

GV2 Panel Version 7.03

- Panel Wide Parameters
  - Phone and Phone Parameters
    - Phone 1: Phone number of central station
  - Routing
    - Primary: 1
    - Backup: 1
  - Enhanced Routing
    - Route Group 1 Primary SDI: Yes
- Area Wide Parameters | Area/Bell Parameters, Open/Close Options | Area 1 – 8
  - Area 1 Account Number: Verify that you have the correct account number
- GV2AUX| Enhanced Communications
  - Enable Enhanced Communications: Yes
  - Path 1 IP Address: IP address of central station
  - Path 1 Port Number: Port number of central station
  - Path 1 Poll Rate: See *Table 2*
  - Path 1 ACK Wait Time: See *Table 2*
  - Path 1 Retry Count: See *Table 2*
  - Path 1 Anti-Replay: Yes

Recommended Poll, ACK Wait, and Retry Count Settings

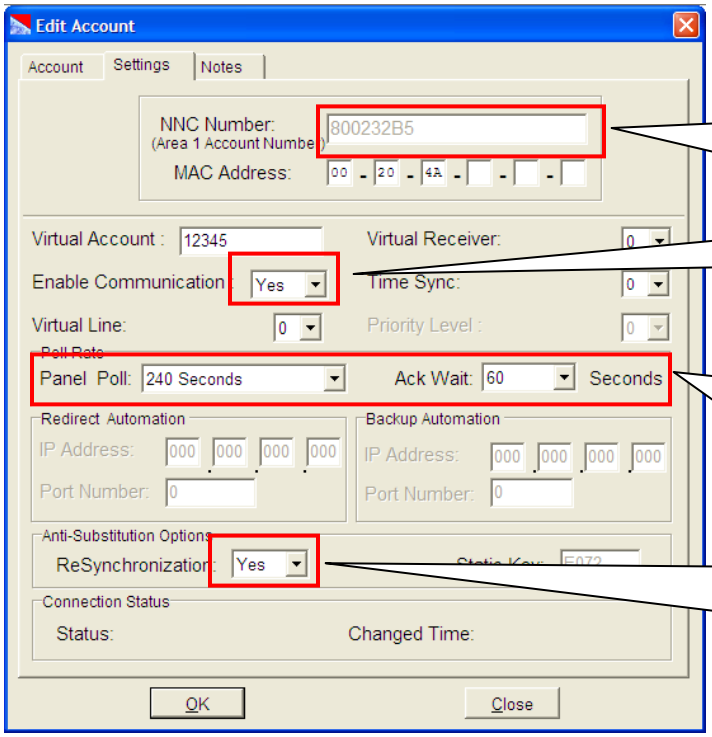
Table 2: Timing Parameters

Recommended Supervision Settings *Required Supervision Interval*	**UL Listed Burg or Fire** 300 sec [1]	**Hourly** 1 hr	**Medium Security** 4 hr	**Daily Supervision** 25 hr
Panel Settings				
Panel Poll Rate (sec)	240 (4min)	3240 (54min)	12600 (3.5hr)	65535 (24hr)
Panel ACK Wait (sec)	10	60 (1min)	300 (5min)	300 (5min)
Panel Retry Count	5	5	5	10
ITS-DX4020-G Settings				
GPRS ACK timeout (sec)	70	370	600	600
GPRS Session timeout (hrs)	4	4	4	25 hrs OR < carrier timeout
D6600/D6100i Receiver Settings				
Account Poll Rate	240	1 hr	4 hr	25 hr (v1.35 only)
Account ACK Wait	60	15	15	15

[1] – For a single communications technology per NFPA 72 – 2010 Edition: 26.6.3.1.4.1. If multiple technologies are used, such as an ITS-DX4020-G or PSTN, then the supervision time can be up to 24 hours to report a failure per NFPA 72 - 2010 Edition: 26.3.1.4.2.

D6600 Conettix Account Database

In the D6200 software, browse to *Network* | *Network Account Database Management* | *Open/Manage Network Account Database Configuration from Receiver*. Double-click on the account and click on the *Settings* tab.



The account number must be entered properly. Preceding 0's are allowed.

Enable Communication must be set to Yes.

Panel Poll and Ack Wait times. See *Table 2*.

Set ReSynchronization to Yes. (This will change to No after the connection is established.

Communications Fail (Polling Lost) - Explained

(Excerpt from **Knowledge Base Article 3931**)

This message is stating that the receiver did not receive a poll from the panel in the programmed amount of time. The receiver's Netcom Account Database has a Poll and Ack wait time for each account. For example, for UL Listed panels the Poll is set to 240 seconds and the ACK to 60 seconds. The receiver is simply going to total these two numbers together (240 + 60) to expect a poll from the panel within 300 seconds. After the configurations have been verified in the panel, Conettix module, D6600, and D6680/D6682, a Communications Fail (Polling Lost) message is most likely to occur when packets are getting blocked or dropped in the network.

FIX: (for non UL listed accounts)
If the account normally restores soon after failing, you can increase either the Poll or ACK wait in the receiver for that account. This will tell the receiver to wait longer for a poll from the panel before generating a Communications Fail message. As the panel is going to continue sending messages until it gets a response from the receiver, more time will allow for more attempts from the panel to try and get to the receiver. For example, if the account normally fails and then restores 5 seconds later, you could increase the Poll in the receiver for at least 5 more seconds (Poll = 245, ACK=60). To be safer, you could increase the poll 15 seconds more (Poll = 255, ACK = 60) to eliminate the Communications Fails and then work your way back down to a lower poll time to find the happy median.

FIX**:** (for UL listed accounts)
If the above fix does not help, you can lower the Poll time programmed in the panel. If you lower it from 240 (recommended) to 230, for example, this will result in the panel sending polls to the receiver more frequently. If the first poll doesn't succeed, then it will begin the retries 10 seconds sooner. This greater number of communication attempts will allow for a greater chance that the polling message will make it through the network to the receiver before a failure message occurs.

Important Note:
While these fixes will help cure the symptoms of the problem, they are a “Bandaid” over the real issue. The main problem is likely that something in the network is causing the Netcom traffic to occasionally get blocked/dropped. Often times, this is seen to occur when networks are using Level 3 switches. These can use Q.O.S. (Quality of Service) which prioritizes the different types of traffic. If UDP traffic (used for Conettix) has a low priority, then it could potentially get dropped if a higher priority message needs to get through the same path at the same time. The best way to diagnose the exact cause and location of the packet loss would be to use a network sniffer at the trouble location to see where in the network the packets are having trouble passing through.

Disabled by Attack - Explained

(Excerpt from **Knowledge Base Article 4062**)

The Conettix system has a built in security feature called "Anti-Replay." Each time the panel (or C900V2) sends a message to the receiver, it will include a key-code in the message. This code will change for every message to help the receiver recognize when it has received a duplicate message from the panel. Both the receiver and panel (or C900V2) know which key-code will be used next. If it gets the same message with the same key-code, then this is a "replay." By default, if the receiver sees 3 replays, it will generate a "Substitution Error." By default again, if the receiver gets 20 Substitution Errors, it will disable the account, output the message "Disabled By Attack" and change the Enable status from “Yes” to “No.” This process provides the extra security of blocking a 3rd party from trying to mimic good communication from the site.

In a properly operating system, it is not unusual to get sporadic substitution errors in the following scenario.

1. The panel sends a message to receiver.
2. The receiver gets the message and sends an acknowledgement back.
3. The receiver now expects to get a new key-code from the next message.
4. Somewhere in the network, the acknowledgement from the receiver is dropped (doesn't make it to panel).
5. The panel does not receive the acknowledgement in the required time since it was dropped, so it thinks that the receiver did not get that message
6. The panel sends the exact same message (with the same key code) to the receiver again.
7. The receiver receives this and sees that it is a duplicate message
8. If this occurs 3 times, the receiver gives a “Substitution Error.”

This scenario may happen occasionally as messages can get dropped while going through the network. This is not a serious issue as long as communication continues without shutting off due to a "Disabled by Attack" message. If you do get a "Disabled by Attack" message and the receiver changes the Enable status to No, you will want to verify a couple of settings. Change your datagram type in your receiver (6.8.6) and the D6680 to datagram type 02. This will send the response from the receiver back to the original source port across the network allowing for the packets to be routed more easily to the originating device. You will also want to make sure that the receiver's network is allowing traffic out, and the remote site is set up to allow traffic in as well as to route the messages back to the correct Conettix module.

If this occurs frequently and the central station is already set for Datagram 02, then the Network Administrator (usually at the panel side) will want to check his network for what is causing this loss. Usually they will find that they have Level 3 switches with Quality of Service turned on. This may give UDP traffic a lower priority on the network and drop the UDP messages when other, higher priority, messages are going through. They can also analyze the network to see where these messages are being dropped.

-End of Document-