



Troubleshoot Communication Difficulties



Contents

| | |
|--|----|
| Communication Difficulties | 3 |
| Procedure A – Keyscan Software Operation | 4 |
| Procedure B – Database IP Address..... | 7 |
| Procedure C – Network Connections | 8 |
| Procedure D – Keyscan Software/ACU Communication | 9 |
| Procedure E – Serial Port Connections | 10 |
| Procedure F – TCP/IP Connections | 11 |
| Procedure G – Modem Connections | 15 |
| Procedure H – Reader/Cards | 19 |

Communication Difficulties

This section is a guide to investigate and correct any of the following common problems that cause system communication failures:

- a Keyscan software module won't open
- the Keyscan Client module reports a Communications Status Failed message
- the Keyscan Client module reports a DB Connection Lost message
- the Keyscan Client module reports Unit Marked Inactive
- the system does not acknowledge a card at a reader

Generally, the communication problems identified above may be the result of one or a combination of the following causes. The table below lists potential causes of communication problems and the procedures to identify and correct them. If the access control system is connected to a network, you may require the assistance of an IT administrator.

| Potential Causes | See Procedure |
|---|---------------|
| Communication Manager is not running. | A, B |
| Keyscan Client software cannot communicate with the Database module on a network (multiple PC installation). | C |
| Communication Manager cannot communicate with the Database module on a network (multiple PC installation). | C |
| Communication Manager cannot connect with the access control units via the TCP to Serial Converter (NETCOM2 or NETCOM6) connection. | C, D, F |
| The Communications Manager cannot connect with the access control units via the serial connection. | E |
| The Communications Manager cannot connect with the access control units via the modem connection. | G |
| The system does not register a card presented at a door reader. | H |

Note

Procedures E & F involve opening the access control panels. Only qualified individuals should perform these procedures, otherwise the equipment could be damaged.

Procedure A – Verify/Start Keyscan Communications

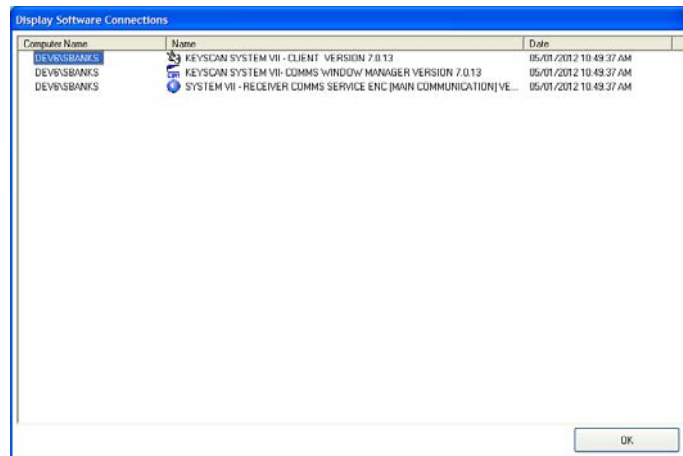
Verify the Communication Manager(s) are running.

The Communications Manager(s) must be running on the PC(s) where they have been installed; otherwise, the system will not operate.

Verify Communication Manager Operation – Keyscan Client

If a Keyscan Client is installed at the PC with the Communication Manager, use the Display Software Connections function located in the Utilities menu. The Display Software Connections screen lists PC(s) currently logged into the Keyscan database with any open Keyscan application including Communication Managers whether they are running as an application or a service.

Display Software Connections Screen



If you are not at a PC with a Keyscan Client, the Communication Managers may be setup to run as a Windows application or as a Windows service. Refer to one of the following subheadings depending on how the Keyscan Communication Manager has been configured:

Single Communication Manager – Windows Application

When the Communication Manager is configured as a Windows application, it normally runs in a minimized state with an icon displayed in the Windows status bar.

Communication Manager Icon – Windows Application



Communication Manager Icon in the Windows Status Bar



If you have an icon in the Windows status bar, the Communication Manager is currently running. Review Procedure B to ensure the correct IP address or computer name has been specified.

If you do not see a Communication Manager icon in the Windows status bar, navigate to Windows start > (All) Programs, and open the Keyscan menu. Select the Keyscan Communications application. A Keyscan user account and password are required to activate the Communication Manager.

Multiple Communication Managers - Windows Application

When running multiple Communication Managers, each Communication Manager has an icon in the Windows status bar. As an example if you use two (2) Communication Managers, two (2) icons should be visible in the status bar.

Communication Manager Icon – Windows Application



Communication Manager Icons x 2 in the Windows Status Bar



If all the Communication Manager icons are present in the Windows status bar, then all the Communication Managers are currently running. Review Procedure B to ensure the correct IP address or computer name has been specified for the PC with the Keyscan database.

If you do not have all assigned Communication Managers running, right click on Windows start, and select Explore > (Drive) > Program Files > Keyscan application. Double click on the Keyscan Communication application. A Keyscan user account and password are required to activate each Communication Manager. You can also review Configure Communications Managers as an Application in the Keyscan Software Installation Guide for more information.

Communication Manager – Windows Service

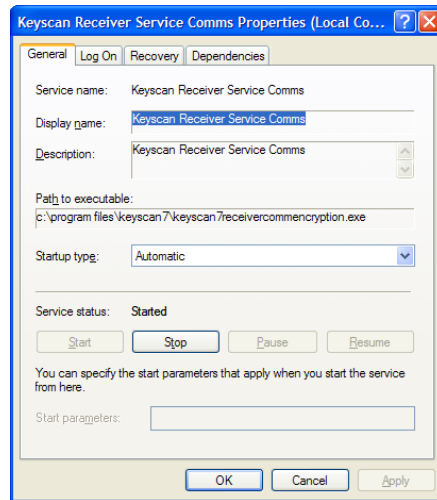
When the Communication Manager is configured as a Windows Service, you must use the Administrative Tools from the Windows Control Panel to verify the Communication Manager(s) are running and, if they are not running, re-start them. When the Communication Managers run as a Windows Service, their icons are not displayed in the Windows status bar.

To verify the Communication Manager is running, select start > Control Panel > Administrative Tools > Services. From the Services screen, scroll down until you locate the appropriate Keyscan service(s). Under the Status column, if the service status is listed as Started, then the Communication Manager is currently operating.

If the Communication Managers are all listed as Started, review Procedure B.

If the Communication Manager(s) is listed as Stopped or it does not indicate a status, double click on the Keyscan service. From the Keyscan Service Properties dialog box, select the Start button. Repeat for each Keyscan service that must be re-started.

Communication Manager – Service Status: Started



Note

If the Windows password that was associated with the Keyscan Communication Service Setup is changed and the PC with the Communication Manager is re-booted, Windows will not resume the service until the password is updated in the Services Properties > Log On screen.

Procedure B – Database IP Address/Computer Name

Verify the IP Address or computer name of the PC with the database (SQL Server 2005 Express) module.

1. Obtain the IP address or the computer name of the PC that has the database module - SQL Server 2005 Express.
2. Go to the PC with the Keyscan Client or Communications Manager that is not opening.
3. Click on **start** > (All) Programs > Keyscan application > Keyscan System Settings.
4. Select a language button from the Language Selection box. English is the default language.
5. Click on the OK button.
6. Check the IP address or computer name specified in the Database Location text box to the actual IP address of the PC with the database module - SQL Server 2005 Express.
7. Enter the correct IP address or computer name.
8. Click on the Save Settings button.
9. Try re-opening the Keyscan application.

Procedure C – Network Connections

Verify the network connections with Keyscan Client or Communications Manager.

1. Get the IP address and the name assigned to the PC that has the database module - SQL Server 2005 Express.
2. Go to the PC that is failing to communicate with the database module.
3. Select **start** > All Programs > Accessories > Command Prompt > Type IPCONFIG at the command prompt.
4. At the DOS prompt, type *ping -a* followed by the IP address of the PC with the database module as shown in the following example:

```
C:\WINDOWS>ping -a 123.123.123.123
```

- If the response is Request timed out, there is no connection to the PC with the database module, or, if the computer name is different, consult with the IT administrator.
- If the response is Reply from... with the correct IP address and the correct computer name of the PC with the database, the two modules are properly connected.

Procedure D – Keyscan Software/ACU Communication

Verify ACU communication from the Keyscan Client module.

1. From a PC with the Keyscan Client, log on to the appropriate site.
2. From the Client main screen, select the Quick Buttons menu > Selective Update.
3. From the Panel Updates screen, click on the down arrow to the right of Unit Selection and select the unit from the drop down list.
4. Click on the Test Unit Communications button.
 - If the result is Successfully Tested, the ACU is communicating with the Keyscan Client.
 - If the result is Invalid Password, the ACU password does not match the site information password. Check the password that was entered on the Site Unit Setup form in the Keyscan Client. If the password is set to the factory default KEYSCAN, clear the memory of the ACU and re-upload.
 - If the result is No Response, then:
 - (a) Check to see if all devices are powered up using a voltmeter;
 - (b) Check to see if port transmission is working – com port, modem or Ethernet (TCP/IP);
 - (c) Check for typical sounds associated with a modem – the dial up sound or the answering exchange sound. Test the phone line using an analog phone to be sure the phone line is operating;
 - (d) Check whether the serial port is active. Use Device Manager in Windows. See Loop Back Test for Serial Ports to verify the serial port is working.

Note

Procedure D may also be performed at a Communications Manager.

Procedure E – Serial Port Connections

Performing a loop back test will determine if your serial port is operating correctly.

To perform the loop back test

1. Go to the location of the access control unit and remove the TD & RD wires from the main circuit board, CB-485, CPB-10, or CPB-10-2 that is connected to the computer. These conductors transmit and receive ASCII data.
2. Short the wires together.
3. Go to the PC with the Communications Manager.
4. Log on to the Communications Manager. Be sure to select the appropriate site.
5. Click on the Unit Diagnostics button.
6. Select the Select Communications menu > Switch Unit > appropriate ACU (must have com port assignment).
7. Press any letter on the keyboard. The letter pressed on the keyboard should echo back to the monitor. If this didn't happen, the com port isn't available or the wiring is suspect. If the letter echoed back to the monitor, proceed to the next step.
8. Return to the ACU.
9. Un-short the TD and RD wires and leave them disconnected.
10. Return to the PC with the Communications Manager and press a letter on the keyboard. If an echo occurs, either you have a conflict with another device or a faulty com port. Type AT and press Enter on the keyboard. If OK is displayed on the screen, you have a conflict with the modem on the same port. If there was no echo on the screen, the result indicates there is no conflict with a modem. Contact the provider of the PC for further hardware support.
11. Return to the ACU and re-connect the TD and RD wires to their proper terminals.

Procedure F – TCP/IP Connections

These procedures are divided into two (2) sections as follows:

- testing TCP/IP connections with a NETCOM2 or a NETCOM2P
- testing TCP/IP connections with a NETCOM6 configured for Reverse Network Communication.

Important – Before You Start

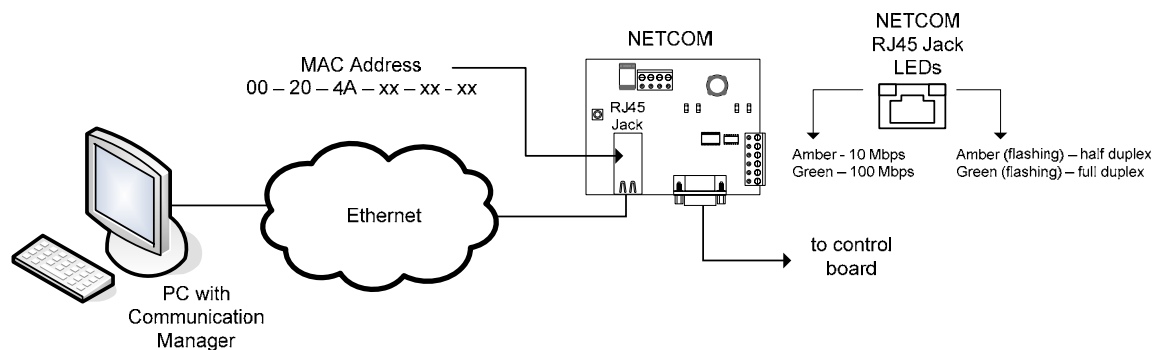
If Telnet is not installed on the PC used to conduct the TCP/IP Connections troubleshooting procedures, consult with the IT administrator.

Before you start, verify that all the panel settings including the serial number have been entered correctly in the Client's Site Unit Setup screen. Also verify that the control board and/or communication board has the correct jumper settings. Incorrect settings will cause communication issues.

Ensure the NETCOM device has power and it was previously programmed with the Keyscan NETCOM Program Tool utility. If the NETCOM device was not programmed with the Keyscan NETCOM Program Toll utility, it will not communicate.

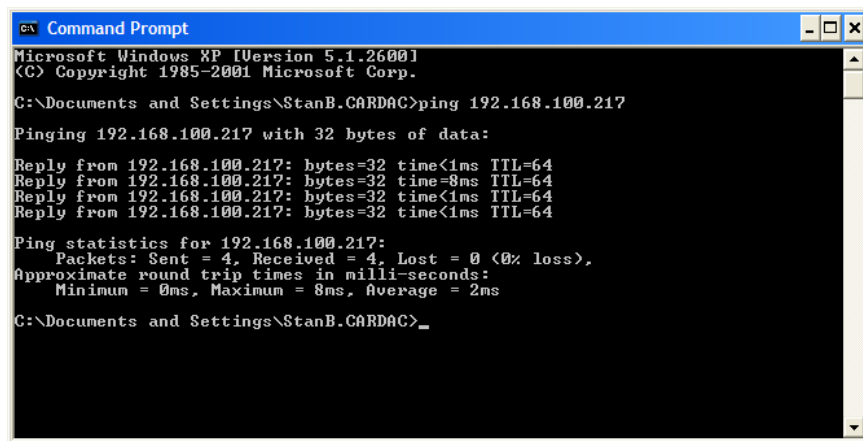
Test NETCOM2 Connection

Keyscan recommends that you perform these procedures from the PC with the Communication Manager assigned to the NETCOM2 device that you are troubleshooting.



PING the NETCOM

1. At a PC on the network from the Command Prompt, PING the NETCOM2's IP address.



```
CA Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\StanB.CARDAC>ping 192.168.100.217

Pinging 192.168.100.217 with 32 bytes of data:

Reply from 192.168.100.217: bytes=32 time<1ms TTL=64
Reply from 192.168.100.217: bytes=32 time=8ms TTL=64
Reply from 192.168.100.217: bytes=32 time<1ms TTL=64
Reply from 192.168.100.217: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.100.217:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms

C:\Documents and Settings\StanB.CARDAC>_
```

- If the PING was successful go to step 2.
- If the PING was unsuccessful indicated by a 'Request timed out' message, consult with a network administrator for security/firewall settings that may affect network connectivity
- If security/firewall settings are not an issue, use a cross-over cable to establish a connection between the NETCOM and a laptop. The laptop must be in the same IP address range as the NETCOM. PING the NETCOM again. If successful the NETCOM is operating correctly. Consult the network administrator to resolve network connectivity.

Telnet NETCOM IP Address - Port 9999

2. Select Run... from the Windows *start* menu.
3. In the Run text box, type TELNET, the IP address of the NETCOM2 unit, followed by 9999, select OK and within 3 seconds of the TELNET screen opening, press the Enter key.
4. Select option 1 Channel 1 and press the Enter key.
5. Press the Enter key line by line and verify the NETCOM settings are correct. An example screen is shown on the following page.
 - Change any settings that are incorrect
 - Ensure the NETCOM baud rate matches the control board
 - If the NETCOM is on a WAN, after reviewing the NETCOM settings, select option 0 Server, press the Enter key and confirm the Gateway address is correct before going to step 6.

Note

For a NETCOM2 or NETCOM2P, Keyscan supports a Connect Mode of C0 – accept incoming connection as shown in the screen on the following page.

```

Telnet 192.168.100.160
0 Server
1 Channel 1
3 E-mail
5 Expert
6 Security
7 Defaults
8 Exit without save
9 Save and exit          Your choice ? 1
Baudrate (57600) ?
I/F Mode (4C) ?
Flow (00) ?
Port No (3001) ?
ConnectMode (C0) ?
Send '+++ in Modem Mode (Y) ?
Show IP addr after 'RING' (N) ?
Auto increment source port (N) ?
Remote IP Address : (000) .(000) .(000) .(000) ?
Remote Port (0) ?
DisConnMode (00) ?
FlushMode (80) ?
Pack Cntrl (01) ?
DisConnTime (15:00) ?:
SendChar 1 (00) ?
SendChar 2 (00) ?

```

6. After you have reviewed the NETCOM settings do one of the following:
 - If you changed any settings, select option 9 Save and exit and press the Enter key
 - If you did not change any settings, select option 8 Exit without save and press the Enter key
7. Select Run from the Windows *start* menu.
8. In the Run text box, type TELNET, the IP address of the NETCOM2 unit, followed by 9999, select OK and within 3 seconds of the TELNET screen opening, type M (upper case).
9. From the TELNET window, type TT (upper case)
10. Press the Enter key.
11. The line with port 3001 (line 5 in the example screen capture on the next page) lists the IP address of the PC with the Communication Manager assigned to the NETCOM.

About Port 9999 and Port 3001

When using Telnet with the TT command, note the following about the two ports listed in the above heading:

Port 9999 – is a diagnostic/administrative access port used by Telnet - in the screen image below, line 04 lists 09999 followed by the IP address of the PC with the open Telnet session

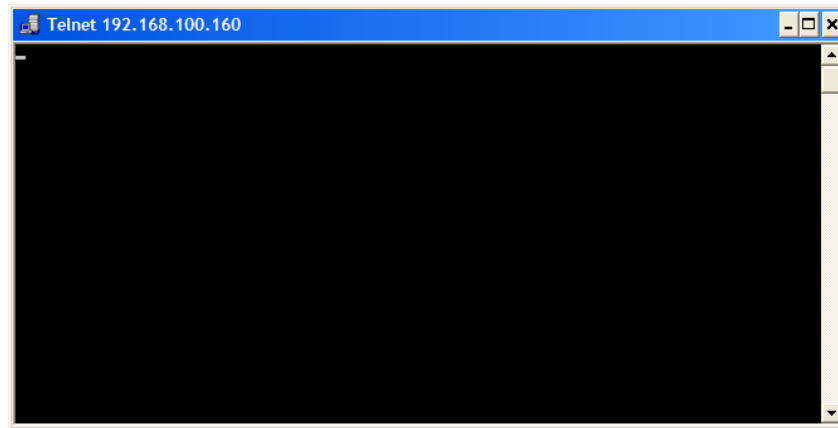
Port 3001 – is an outbound remote port – in the screen image below, line 05 lists 03001 as the outbound port followed by an IP address which should be the IP address of the PC with the Communication Manager.

```

Telnet 192.168.100.160
MAC address 00204AAFA888
Software version U6.6.0.2 (080926) XPIEXE
Press Enter for Setup Mode
*** NodeSet 2.0 ***
0>TT
00:00000 0 0.0.0.0/00025 r00000 t00000 rtry 0
01:00000 1
02:00000 1
03:00000 1
04:09999 2 192.168.100.99/02068 r00000 t00095 rtry 0
05:03001 2 192.168.100.24/49639 r00000 t00000 rtry 0
06:00000 0 0.0.0.0/00000 r03939 t03939 rtry 0
07:00000 0 0.0.0.0/00000 r03939 t03939 rtry 0
08:00000 0 0.0.0.0/00000 r03939 t03939 rtry 0
09:00000 0 0.0.0.0/00000 r03939 t03939 rtry 0
10:00000 0 0.0.0.0/00000 r03939 t03939 rtry 0
11:00000 0 0.0.0.0/00000 r03939 t03939 rtry 0
0>

```

- If the IP address listed for port 3001 is not the PC with the assigned Communication Manager, investigate the PC showing the IP address for port 3001 and verify Communication Manager assignments.
- If port 3001 is not listed, verify the assigned Communication Manager is currently running.
- If the assigned Communication Manager is running, turn off the assigned Communication Manager and Telnet the NETCOM IP address 3001. (Type TELNET, the IP address of the NETCOM2 unit, followed by 3001, and select OK.) If the screen is blank, port 3001 is open.



- If the connection failed, a device or firewall is impeding communication. Consult with the IT administrator.

Test NETCOM6 Reverse Network Communication Connection

Troubleshooting a NETCOM6 with a reverse network communication is divided into two (2) sets of procedures depending on the type of IP address assigned to the NETCOM6:

- NETCOM6 with a static IP address
- NETCOM6 with a dynamic IP address

Please note networks can be highly structured and extremely complex. Firewalls and security protocols may inhibit communication. You may be required to consult with the network administrator for assistance.

Refer to the one of the following sub-headings depending on the type of IP address assigned to the NETCOM6 – static or dynamic.

NETSTAT

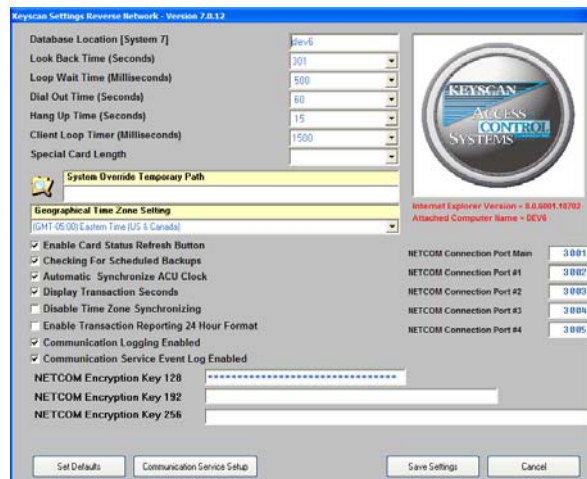
As an alternative for TELNET, you can use NETSTAT from the Command Prompt at the PC where the Encrypted Reverse Network Communication Manager is installed.

- NETSTAT -B -P TCP -N 30

Verify NETCOM6 Remote Port Assignment

You can confirm the remote port connection(s) for the NETCOM6 from the Keyscan System VII Reverse Network Settings Encryption under the Programs menu. This is especially important if you are running multiple Communication Managers or have changed the default port assignment(s). Note the Communication Manager/NETCOM Connection Port (Remote Port) assignments:

- Keyscan7ReceiverCommEncryption – NETCOM Connection Port Main
- Keyscan7ReceiverCommEncryption1 – NETCOM Connection Port #1
- Keyscan7ReceiverCommEncryption2 – NETCOM Connection Port #2
- Keyscan7ReceiverCommEncryption3 – NETCOM Connection Port #3
- Keyscan7ReceiverCommEncryption4 – NETCOM Connection Port #4

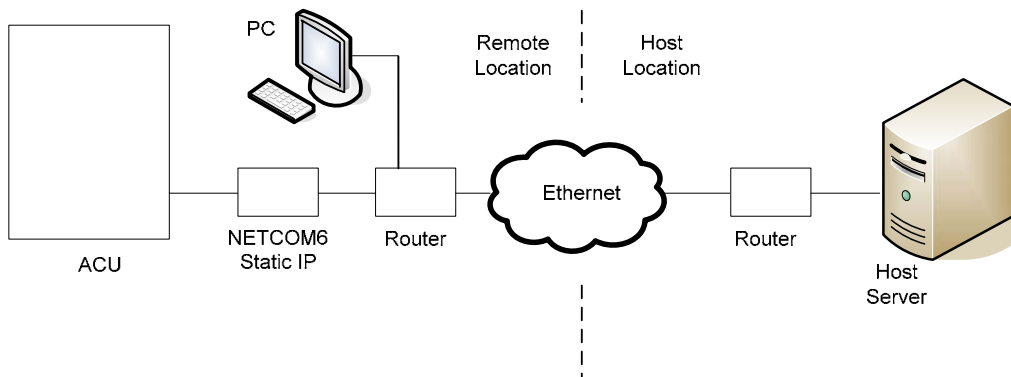


Test a NETCOM6 with a Static IP Address Connection

Troubleshoot a NETCOM6 with a static IP address using reverse network communication from the remote location as depicted in the illustration below:

- From the Remote Location:
 - PING the NETCOM6 IP Address
 - TELNET to verify the settings – see the TELNET Screen with NETCOM6 Configuration Settings below
 - TELNET – M – TT to verify the Remote Port

NETCOM6 with Static IP Address – Reverse Network Communication



TELNET Screen with NETCOM6 Configuration Settings

```
Telnet 192.168.100.178
0 Server
1 Channel 1
3 E-mail
5 Expert
6 Security
7 Defaults
8 Exit without save
9 Save and exit      Your choice ? 1
Baudrate <9600> ?
I/F Mode <4C> ?
Flow <00> ?
Port No <0> ?
ConnectMode <C6> ?
Send '+++' in Modem Mode <Y> ?
Show IP addr after 'RING' <N> ?
Auto increment source port <N> ?
Remote IP Address : <000> .<000> .<000> .<000>
Remote Port <3001> ?
DisConnMode <00> ?
FlushMode <00> ?
Pack Ctrl1 <01> ?
DisConnTime <15:00> ?
SendChar 1 <00> ?
SendChar 2 <00> ?
```

Refer to the Test NETCOM2 section for PING and TELNET command lines and instructions.

Note

If troubleshooting the NETCOM6 with a static IP address from the host side where routers are in place at the host and remote locations, both the routers must be open for ports 9999 and the remote port.

Connect Mode

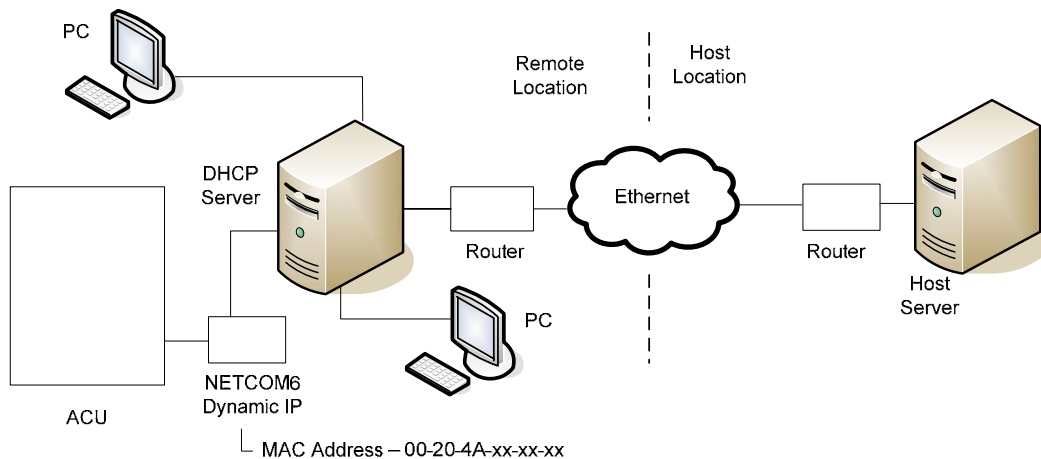
The NETCOM6 also supports Connect Mode 06 - outgoing connections only with no echo.

Test a NETCOM6 with a Dynamic IP Address Connection

Troubleshoot a NETCOM6 with a dynamic IP address using reverse network communication from the remote location as depicted in the illustration below:

- From the remote location:
 - Determine the IP address of the NETCOM6 by looking up the following:
 - a. DHCP server connections table
 - b. Router connections table – look for the NETCOM6 MAC address assigned to the dynamic IP address
 - PING the NETCOM6 IP Address
 - TELNET to verify the settings - see the TELNET Screen with NETCOM6 Configuration Settings below
 - TELNET – M – TT to verify the Remote Port

NETCOM6 with Dynamic IP Address - Reverse Network Communication



TELNET Screen with NETCOM6 Configuration Settings

```
Telnet 192.168.100.178
0 Server
1 Channel 1
3 E-mail
5 Expert
6 Security
7 Defaults
8 Exit without save
9 Save and exit      Your choice ? 1

Baudrate <9600> ?
I/F Mode <4C> ?
Flow <00> ?
Port No <0> ?
ConnectMode <G6> ?
Send '+++' in Modem Mode <Y> ?
Show IP addr after 'RING' <N> ?
Auto increment source port <N> ?
Remote IP Address : <000> .<000> .<000> .<000>
Remote Port <3001> ?
DisConnMode <00> ?
FlushMode <80> ?
Pack Cntrl <01> ?
DisConnTime <15:00> ?
SendChar 1 <00> ?
SendChar 2 <00> ?
```

Procedure G – Modem Connections

Test a modem connection.

1. Go to the PC with the appropriate Communications Manager.
2. Log on to the Communications Manager.
3. Select the Utilities menu and enable Communication Port Status. The text of the Communication Port Status reported in the transaction window should be green.
4. Click anywhere within the Communication Manager's transaction window to stop transaction reporting.
 - If message – Com # Port Open (Modem), indicated in green, the port is available to the Communications Manager. Go to the next step.
 - If message – Unexpected Com Port Error, consult with the PC provider.
5. Click on the Unit Diagnostics button.
6. From the Unit Diagnostics window, select the Select Communications menu > Switch Unit > appropriate ACU (must have com port assignment).
7. Type AT and press Enter on the keyboard. The window displays OK.
8. Type ATDT and the phone number of the remote ACU and press enter on the keyboard. One of the following messages is displayed in the window.
 - No Carrier – Host modem has no line out. Consult with phone provider.
 - Busy – Line is busy. Retry last step. If problem continues, consult with phone provider.
 - Connect 9600 – Modem is communicating. Investigate ACU hardware.
 - Connect ### (lists another baud rate other than 9600) – Modem compatibility problem. Contact Keyscan technical support.

Procedure H – Reader/Cards

Test a reader or a card

Card does not read at the reader. Generally the most common error is an incorrect batch number or card number entry. (The batch number may also be referred to as the site code or facility code.)

To Test a Card/Reader from the Client software

1. Go to the reader and scan the card a minimum of six times. An Invalid Code alarm is not generated until after the 5th pass of the card over the reader.
2. Return to the PC with the Keyscan Client software. Be sure you have logged on to the appropriate site.
3. From the Client main screen, click on the Display Online Transactions quick button. If there is an Invalid Code message, then the potential problem could be an incorrect card batch/number entry, the card is not on file, or the card has been archived.
4. Close the Online Transaction form.
5. From the Client main screen, click on the Cardholder Database quick button > Edit/Delete Card(s).
6. From the Search Access Card Holders form, enter the cardholders first and last name in the appropriate fields.
7. Click on the Find Card(s) button. Check the card information and make any necessary corrections. Be sure to save the changes if you altered the card holder record.
8. Return to the reader and re-scan the card to ensure it works. If the card information was correct and it still does not read at the reader, continue to the next step.
9. Return to the PC with the Keyscan Client and click on the Update Changes quick button.
10. From the Panel Updates form, click on the down arrow to the right of Unit Selection, and, from the drop down list, select the ACU that controls the reader.
11. Click on the View Reader Diagnostics button.
12. Go to the reader and scan the card.
13. Return to the PC with the Keyscan Client. If the reader is working, the batch and card numbers are listed in the black window of the Panel Updates form. If this is the case, re-check the card information. If there is no card information listed in the black window, the reader or the wiring may be faulty. Call your service vendor.
14. Press the escape (Esc) key then click on the Exit button of the Panel Updates form to return to the Client main screen.

To Test a Reader/Card from the Communications Manager

This procedure is an alternative method for dealers to test cards or readers from a Communications Manager.

1. Log on to the Communication Manager. Be sure to select the appropriate site.
2. Click on the Unit Diagnostic button.

3. From the Unit Diagnostic form, click on the Select Communication menu, and select the appropriate access control unit.
4. From the Enter Command prompt, type R. This opens the Reader Diagnostic utility.
5. Press Enter. Leave the Reader Diagnostic window open.
6. Return to the reader and present the card to the reader.
7. Return to the Communications Manager PC. If the reader is working, the Reader Diagnostic utility will have recorded the Batch # and the Card #. If this is the case recheck the card information.
8. If there is no data recorded by the Reader Diagnostic utility, then it is most probable that the reader or wiring is faulty. Call your service vendor.

Example of Unit Diagnostics window

