

Telnet Sessions



Connect, Inc.
1701 Quincy Avenue, Suites 5 & 6, Naperville, IL 60540
Ph: (630) 717-7200 Fax: (630) 717-7243
www.connectrf.com

Table of Contents

General Telnet Troubleshooting	1
Environment Troubleshooting	1
3270/5250 Emulations	4
Ethernet Analyzers	5
AS400 Host	6
System Values	6
Workstation ID, LuNames, and New Environment	9
IBM 3270 Host	12
Windows Host	13
Using CIM Server with IX	13
Configuring Under Windows 2000.....	16
Response Time Issues ("Waiting for HOST" Loopback Test)	18
Using Ataman © Telnet Server	19
Wireless Network Worksheet	21

General Telnet Troubleshooting

Environment Troubleshooting

Telnet session problems can be attributed to one or more of the following: Host Environment, Database Environment, Network Environment, TCP Stack being used, and Terminal Power Management.

Setup

Reference the manufacturer's equipment manuals to configure the Access Points and RF terminals for the customer's network.

Assign the Access Point and the RF terminal their individual IP address, Netmask address, and Broadcast address for the customer's network. Attach the Access Point to the same segment of the network as the Host computer. This will eliminate the issue of router and switch configurations.

Note: If you cannot do this, keep in mind that the customer may have to change the router and switch configuration to accommodate the new devices, namely Access Points and RF terminals, to their network. After this is done, the customer will have to provide you with the additional information on the router/switch address for your Access Point/s and RF terminal setups.

Remember to configure the radio parameters within the Access Points and RF terminals to match.

Verification

Verify that you can connect to the individual node, the Access Point, and the RF terminals.

Run the ping command from another system on the segment of the Network where the HOST computer is located to verify the connection to the Access Point and the RF terminal. If you cannot ping the terminal, try pinging the Access Point. If you can not ping the access point, it is likely that your Access point setup is not configured correctly for the customer's network (and you need a router setup) or that there is a hardware problem with the Access Point.

If you can ping the Access Point but not the RF terminal, verify that the radio configuration within the Access Point matches the RF terminal. Also, verify that the Network information is correct within the RF terminal.

Note: The common mistake is the RF terminal has an IP address of, for example, 206.183.69.69 and the RF terminal is pointed at itself for the gateway 206.183.69.69. The gateway address should be 206.183.69.1 for the host where the application that they are going to run resides.

Other issues

The customer sees a "Waiting for Data, Host Process Delay" message or the customer is getting disconnected from the Host system.

This is attributed to one or more of the following issues:

1. If the database has a file or record lock for one user, and the second user tries to access the same data, they will receive "Waiting for Data, Host Process Delay" until the record and or field has been committed by the first user. This is an application/database issue.
2. There may be an issue with the host settings for session life. As part of Host system security, many host systems will disconnect the sessions after a period of inactivity. These Host system variables may be extended at the customer discretion.

Note: The change needs to take place on the Host system, not the Access Point or RF terminal. The linger timer affects the time it may take for the RF terminal to wait before it can reconnect to the given Host System. The Linger will maintain an open connection even though the session no longer exists.

3. There may be an issue with Router/Switch/Network settings for ARP timeouts. We have seen networks in which, after a period of inactivity or too frequent activity, the router/switch throws away the RF terminal Network address from its table. This disconnects the RF terminal session and connection to the Host system.

Note: The customer needs to add static Network address entries for each RF terminal and Access Point to his or her router tables. In a switched environment, the customer needs to ensure that all the switches working with the RF site are updated as fast or faster than an RF terminal cell switch with less than 100ms.

4. There may be an RF Terminal TCP/IP stack, power management, and BIOS issue. The solution is to get the RF terminal manufacturer to fix its Power management in the BIOS so that it does not effect the radio communications.

Note: The RF terminal relies on batteries to operate. Power management is an important part of this equipment's environment. The problem can arise where the power management actually shuts down the RF terminal radio thereby prohibiting the TCP/IP stack from sending or receiving messages. If the Host, such as an AS400, sends out a Timemark packet, the RF terminal will not be able to answer and the Host will disconnect it.

There are two methods of dealing with this issue. Disable it on the Host system or disable power management in the RF terminal.

Most Host network operations will not allow this to be done, as it is an automatic load balance mechanism for the Host. The down side of disabling the RF terminal Power management is the need to replace the batteries frequently in the RF terminal.

5. The RF terminal may be faulty.

Note: Contact the RF terminal manufacturer for instructions on how to run the terminal diagnostic program.

6. The Access Point may be faulty.

Note: Contact the Access Point manufacture for instructions on how to run the Access Point diagnostic program.

7. There may be an application issue. Check the customer application logs for indication of a problem.

Note: To identify application issues in the NT environment, set up the host list to run the "appdemo" program as "VTCOMM". In the IX environment, set up the host list to run "rscan".

Connection Verification

Establish a connection with the RF terminal to the Host.

On the Host, run the NETSTAT program to verify an established connection.

Wait for the disconnect to happen.

Power on the RF terminal.

On the Host, run the NETSTAT program to verify that you still have a connection to the RF terminal.

Note: If you no longer see a connection established, the Host has either disconnected it from either being idle too long or the RF terminals ARP table has been removed from the Host. This happens on NT servers as a default. In either case, refer to the Host system manuals to determine the changes needed for the idle time out and/or creating static ARP table entries for the RF terminals.

3270/5250 Emulations

AS400 (TN5250) and Mainframe (TN3270) disconnects are known to affect Telnet sessions with wireless devices and IBM hosts (excluding IX).

Both Mainframes and AS400s send out a keep-alive packet to all nodes on the network. This works in a fully powered and wired environment where the node can always respond. However, in a wireless environment the device goes to sleep, which inactivates the radio and more importantly the TCP-IP stack provided by the radio manufacturer.

The following options are available as a resolution:

- Disable the host from sending out the keep-alive or extend it to a reasonable length of time, for example, beyond twice the maximum session inactivity timer. When the terminal is sleeping, the TCP-IP stack provided by the radio/terminal manufacturer cannot respond to the host as it is disabled.
- Disable the power down setting in the terminal so that it can always respond to the host. Battery life for the terminal will be severely impacted. The user may be lucky to get two hours of use. This is manufacturer dependent. Disabling the power down timer of the terminal allows the radio/terminal manufacturer TCP-IP stack to respond to the Host.
- Install one of Connects OpenAir Gateways and run the terminal in thin mode. This will solve both issues. The OpenAir gateway on the wired, fully powered side of the world will respond to the Host, AS400 or the Mainframe, for the RF terminals are sleeping, maintaining the maximum battery life for the sleeping terminals. Using this option will eliminate the need to modify the Host settings and will conserve the battery life.

Ethernet Analyzers

Ethereal is a GUI network protocol analyzer that lets you interactively browse packet data from a live network or from a previously saved capture file. It can read capture files from Sniffer (compressed or uncompressed). Ethereal will determine what type of file you are reading by itself. It is capable of reading any file format compressed using gzip. Ethereal recognizes this directly from the file without needing a `.gz` extension.

Ethereal's main window shows 3 views of a packet. It shows:

- a summary line, which briefly describes the packet
- a protocol tree, which allows you to drill down to exact protocol or field of interested
- a hex dump, which shows you what the packet looks like when it goes over the wire

Ethereal can assemble all the packets in a TCP conversation and show you its ASCII, EBCDIC, or hex data. It has powerful display filters. Ethereal filters more fields than other protocol analyzers. Also, it enables you to use richer syntax to create your filters than other protocol analyzers would allow you to do.

The pcap library performs packet capturing. The capture filter syntax follows pcap library rules. This syntax is not the same as the display filter syntax.

The zlib library is required for compressed file support. If not present, Ethereal will compile but will not be able to read compressed files.

AS400 Host

System Values

This Tech Alert describes the AS400 system values that directly effect TN sessions.

Background

An example of AS400 V5R1 settings is located at:

http://www.connectrf.com/Documents/AS400_V5r1.doc

For specific information on IBM's parameters, please see IBM's WEB pages or contact their technical support.

IBM Link

This IBM Tech Doc is located at:

http://www-912.ibm.com/s_dir/slkbase.NSF/7250f367f6396d2f86256a4f007973d5/b487c419decd13cc8625663b004f897a?

R440 and Higher

At R440, the inactivity timer parameter is not present in the Telnet attributes. The system value QINACTITV fully controls inactivity timers with QINACTMSGQ determining what action to perform.

In order to maintain sessions in a TCP/IP environment, the end node (RF terminal) must respond to the Time Mark values issued by the AS400. In addition, the RF device is under the same session constraints as other nodes on the network, namely, Inactivity time and INZWAIT(linger).

AS400 Important System Values

The following are the values set on the AS400.

Use the WRKSYSVAL AS400 command to obtain information on the QINACTITV timer and QINACTMSGQ.

QINACTITV:

Inactive job time-out.

This specifies when the system takes action on inactive interactive jobs. A change to this system value takes effect immediately. The shipped value is *NONE.

QINACTITV must be one of the following values:

- *NONE The system does not check for inactive interactive jobs.
- 5 - 300 The number of minutes a job can be inactive before action is taken.

QINACTMSGQ

Inactive message queue.

This specifies the action the system takes when an interactive job has been inactive for an interval of time (the time interval is specified by the system value QINACTITV). The interactive job can be ended, disconnected, or message CPI1126 can be sent to the message queue you specify.

If the specified message queue does not exist or is damaged when the inactive time out interval is reached, the messages are sent to the QSYSOPR message queue. All of the messages in the specified message queue are cleared during an IPL. If you assign a user's message queue to be QINACTMSGQ, the user loses all messages that are in the user's message queue during each IPL.

A change to this system value takes effect immediately.

The shipped value is *ENDJOB.

Message queue

*ENDJOB

This ends any job, secondary job, and group jobs. If *ENDJOB is specified, the interactive job is ended along with any secondary job and any group jobs associated with it. If there are many inactive jobs in a subsystem that are to be ended at once, the interactive response time of that subsystem may be slowed down.

*DSCJOB

This disconnects any interactive job, secondary job, or group jobs.

If *DSCJOB is specified, and the job cannot be disconnected, *ENDJOB will be used.

In addition to the System Values, you must also be aware of some TCP/IP settings.

Use the CHGTCPA AS400 command to obtain information on the TCP keep alive.

TCP keep alive 5_____ 1-40320, *SAME, *DFT

TCP keep alive (TCPKEEPALV) – Help

This specifies the amount of time in minutes that TCP waits before sending out a probe to the other side of a connection. The probe is sent when the connection is otherwise idle, even when there is no data to be sent.

The possible values are:

*SAME

The keep-alive time interval value does not change from its current setting.

*DEF

The keep-alive time interval value of 120 minutes is used.

tcp-keep-alive

These specify a keep-alive time interval in minutes. Valid values range from 1 through 40320 minutes (28 days).

Use the CHGTELNA AS400 command to obtain information on the TELNET Attributes.

Inactivity timeout 900_____ 0-2147483647, *SAME, *DFT

Timemark timeout 600_____ 0-2147483647, *SAME, *DFT

Inactivity timeout (INACTTIMO) - Help

This specifies the number of seconds the system allows a TELNET connection to remain inactive before it is ended. When a TELNET connection is inactive longer than the specified length of time, it is ended.

Note: The system may wait an additional 1 to 120 seconds to end the inactive connection.

The possible values are:

*SAME

The time-out value does not change if it was previously set. Otherwise, 0 seconds is used.

*DFT

The time-out value is set to the default of 0 seconds.

inactive-timeout

These specify an inactive time-out period in seconds. Valid values range from 0 through 2147483647 ((2**31)-1) seconds. A value of 0 means that there is no time-out.

The INACTTIMO parameter does not override the connection timer. For example, assume the connection timer (specified on the INZWAIT parameter of the STRTCPTLN command) is set to 120 seconds, and the INACTTIMO parameter is set to 15 seconds. If the connection timer goes off when the inactivity timer is at 14 seconds, the connection timer is reset for another 120 seconds. Even though the inactivity timer would go off a second later, the connection is not ended until the connection timer ends (119 seconds later).

Timemark timeout (TIMMRKTIMO) - Help

This specifies the number of seconds between timemarks. TELNET sends a timemark to each connection at the specified time interval. If TELNET is unable to send the timemark, it ends the connection.

The possible values are:

*SAME

The timemark value does not change if it was previously set. Otherwise, 600 seconds is used.

*DFT

The timemark value is set to the default of 600 seconds.

timemark-timeout

These specify the timemark time-out in seconds. Valid values range from 0 through 2147483647 ((2**31)-1) seconds. A value of 0 means that there is no time-out.

Note: On an AS400 V4R4 release, this value is referred to as "CHGKEEPALV".

Workstation ID, LuNames, and New Environment

AS400 Work Station ID, LuNames for TN3270E, and New Environment can be used to securely manage Telnet sessions and resources on an AS400 or IBM 3270.

The default for the 3270 handler tn3270e is On. You also may disable this option if the host does not support and run it in 3278-2 mode. This is done by specifying "-3270e" on the custom options on the controller.

Below is an example for an AS400 setup.

AS400 Setup Devices Values

If your AS400 does not automatically configure your 5291 mod 1 devices, you can use the CRTDEVDSPP command to do so.

Create Device Desc (Display) (CRTDEVDSPP).

Type choices, press Enter.

```

Device description . . . . . 5291MOD1__ Name
Device class . . . . . *VRT_ *LCL, *RMT, *VRT, *SNPT
Device type . . . . . 5291_ 3101, 3151, 3161, 3162...
Device model . . . . . 1_____ 0, 1, 2, 3, 4, 5, 12, 23...
    
```

Bottom

F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
 F13=How to use this display F24=More keys

Using the AS400 command WRKDEVD, select a 5291 device and use the Rename option.

Work with Device Descriptions

System: POWERNET

Position to _____ Starting characters

Type options, press Enter.

2=Change 3=Copy 4=Delete 5=Display 6=Print 7=Rename
 8=Work with status 9=Retrieve source

Opt	Device	Type	Text
7	5291MOD1	5291	Device created for POWERNET.
_	QPADEV00BK	5291	Device created for POWERNET.
_	QPADEV00BL	5291	Device created for POWERNET.
_	QPADEV00BM	5291	Device created for POWERNET.
_	QPADEV00BN	5291	Device created for POWERNET.
_	QPADEV00BP	5291	Device created for POWERNET.
_	QPADEV00BQ	5291	Device created for POWERNET.
_	QPADEV00BR	5291	Device created for POWERNET.
_	QPADEV00BS	5291	Device created for POWERNET.
			More...

Parameters or command

====> _____
F3=Exit F4=Prompt F5=Refresh F6=Create F9=Retrieve F12=Cancel
F14=Work with status

The Following Screen appears. Enter the new LUNAME: 5291MOD1.

Rename Object (RNMOBJ)

Type choices, press Enter.

Object > 5291MOD1 Name
Library *LIBL Name, *LIBL, *CURLIB
Object type > *DEV *ALRTBL, *AUTL, *BNDDIR...
New object RF5291.001 Name

Bottom

F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

After entering the Information, you will need to make it available.

Work with Device Descriptions

System: POWERNET

Position to _____ Starting characters

Type options, press Enter.

2=Change 3=Copy 4=Delete 5=Display 6=Print 7=Rename
8=Work with status 9=Retrieve source

Opt	Device	Type	Text
_	QPADEV0098	5291	Device created for POWERNET.
_	QPADEV0099	5291	Device created for POWERNET.
_	QQAHOST	*APPC	
_	QTIDA	*APPC	
_	QTIDA2	*APPC	
_	Q1PDEV	*APPC	PM400 device
_	Q1SHARE400	*APPC	AS/400 FORUM ACCESS DEVICE
8	RF5291.001	5291	Device created for POWERNET.
_	SPANISH	3179	Device created for POWERNET.

More...

Parameters or command

====> _____
F3=Exit F4=Prompt F5=Refresh F6=Create F9=Retrieve F12=Cancel
F14=Work with status

Select Make Available.

Work with Devices

System: POWERNET

Type options below, then press Enter.

1=Make available 2=Make unavailable 5=Display details
7=Display message 8=Work with controller and line 9=Rename
13=Change description

Opt Device Type Status

1_ RF5291.001 5291 Unavailable (use Opt 1)

Bottom

F1=Help F3=Exit F5=Refresh F9=Command line F11=Display descriptions
F12=Cancel F17=Top F18=Bottom F21=Select assistance level

Work with Devices

System: POWERNET

Type options below, then press Enter.

1=Make available 2=Make unavailable 5=Display details
7=Display message 8=Work with controller and line 9=Rename
13=Change description

Opt Device Type Status

_ RF5291.001 5291 Available to use

Bottom

F1=Help F3=Exit F5=Refresh F9=Command line F11=Display descriptions
F12=Cancel F17=Top F18=Bottom F21=Select assistance level
RF5291.001 made available.

Follow the process for either Twin Client or PowerNet controller for setting LU names to match the AS400.

IBM 3270 Host

The following settings are required on a 3270 host for the logmode table in Twin Client TN3270 terminal emulation.

Below is the entry that was commented out in our logmode table.

```
*****  
* ENTRY FOR NON-SNA MODEL 2 TERMINALS  
* NO ALTERNATE SCREEN DEFINED  
*****  
  
* D4B32782 MODEENT LOGMODE=D4B32782  
*     FMPROF=X'02'  
*     TSPROF=X'02'  
*     PRIPROT=X'71'  
*     SECPROT=X'40'  
*     COMPROT=X'2000'  
*     RUSIZES=X'0000'  
*     PSERVIC=X'000000000000185000007E00'  
*     APPNCOS=#CONNECT
```

This was replaced with:

```
M32782  MODEENT LOGMODE=M32782,      *  
      FMPROF=X'03',                  *  
      TSPROF=X'03',                  *  
      PRIPROT=X'B1',                  *  
      SECPROT=X'90',                  *  
      COMPROT=X'3080',                *  
      RUSIZES=X'87C7',                *  
      PSERVIC=X'020000000000185000007E00'
```

Windows Host

Using CIM Server with IX

This section describes how PowerNet software can be configured to work with the CIM concepts NT Telnet server when coupled with a PowerNet OpenAir IX server.

This support requires addition of some modules that will work with a standard VTERM release.

The ZIP file (tnshim.zip) contains these modules:

- o tnshim (tnshim executable)
- o run.sh (tnshim shell script)
- o tnshim.cf (Host list entry for tnshim)
- o cim.cfk (Key remap file for CIM server)

The reason for the tnshim program is that there is a compatibility problem between SCO's Telnet and the CIM Concepts's NT Telnet server.

The tnshim application can be used as a replacement for the SCO telnet process. This process opens a raw IP socket connection to the target address.

How to Setup and Use

1. Copy these files to the working server directory (/crf).
2. Create the files run.sh and tnshim executable (chmod 777 tnshin run.sh).
3. Rename the cim.cfk file as CIM.380046.cfk. This re-map file has the Clear key for the 3800 46-key terminal set to send a hex "1C" immediately. If you need to support other terminal types, create a keymap entry with the name CIM and it will create a key map file that will work with this host entry.

Example:

CIM.680046.cfk

4. Enter the host list setup and enter a new menu entry titled "tnshim".
5. Select VTERM as the handler type.
6. Select VTERM setup. The line for application should be pre-filled in with the name run.sh. This shell script puts the UNIX console in raw mode and runs the tnshim process.
7. The application command line should be pre filled in with HOST. The run script accepts a command line argument for IP address. You may enter a pseudo name that is setup in TCP/IP address or you may key in the fixed IP on this line.

You can now select this handler to run the CIM server application. To make this process simpler, we may make this type of connection an option within the VTERM product.

Technical Background

The following describes the testing that uncovered the need for the tnshim program. It may be useful information when you suspect you may have a Telnet compatibility problem.

1. In Telnet, the conversation starts with what's called a "Telnet Negotiation". During this process, both ends negotiate the rules of the Telnet conversation that is to take place. What is negotiated are items like the type of terminal, how data will be exchanged, etc. Using the trace function on SCO's Telnet, below is what the negotiations looked like:

SCO's Telnet sent these BIDS asking if the server will support these functions:

```
SENT DO SUPPRESS GO AHEAD
SENT WILL TERMINAL TYPE
SENT WILL NAWS
SENT WILL TSPEED
SENT WILL LFLOW
SENT WILL LINEMODE
SENT WILL ENVIRON
SENT DO STATUS
```

This is the response from the CIM server:

```
RCVD WONT SUPPRESS GO AHEAD
RCVD DONT TERMINAL TYPE
RCVD DONT NAWS
RCVD DONT TSPEED
RCVD DONT LFLOW
RCVD DONT LINEMODE
RCVD DONT ENVIRON
RCVD WONT STATUS
```

The response is that none of these functions are supported. This causes the SCO telnet to enter into some odd state. It basically does not know how to converse with the server.

This leads to odd behavior such as keystrokes not being sent. For example, if you press a function key on the client, it is not sent until the client presses an Enter key. Single key presses are also not passed on.

Below is a Telnet negotiation from an IBM AIX server for comparison.

```
SENT DO SUPPRESS GO AHEAD
SENT WILL TERMINAL TYPE
SENT WILL NAWS
SENT WILL TSPEED
SENT WILL LFLOW
SENT WILL LINEMODE
SENT WILL ENVIRON
SENT DO STATUS

RCVD DO TERMINAL TYPE
```

```
RCVD WILL SUPPRESS GO AHEAD
RCVD DO NAWS
```

```
RCVD DONT TSPEED
RCVD DONT LFLOW
RCVD DONT LINEMODE
RCVD DONT ENVIRON
RCVD WONT STATUS
RCVD IAC SB TERMINAL-TYPE SEND
SENT IAC SB TERMINAL-TYPE IS "VT100"
```

```
RCVD WILL ECHO
SENT DO ECHO
RCVD WONT 200
RCVD DO ECHO
SENT WONT ECHO
```

```
RCVD DONT ECHO
```

2. This type of Telnet server response seems to cause no problems with Windows Telnet and TN based products. The windows telnet is not implemented as tightly to the RFC Spec for Telnet and tolerates this differently.

Most of the UNIX telnet and TCP/IP stacks are implemented truer to the RFC Spec. They are the ones that defined this type of remote access first and helped define the RFC for Telnet.

3. Below are the details of how to run a Telnet trace using SCO' telnet:

Type the following:

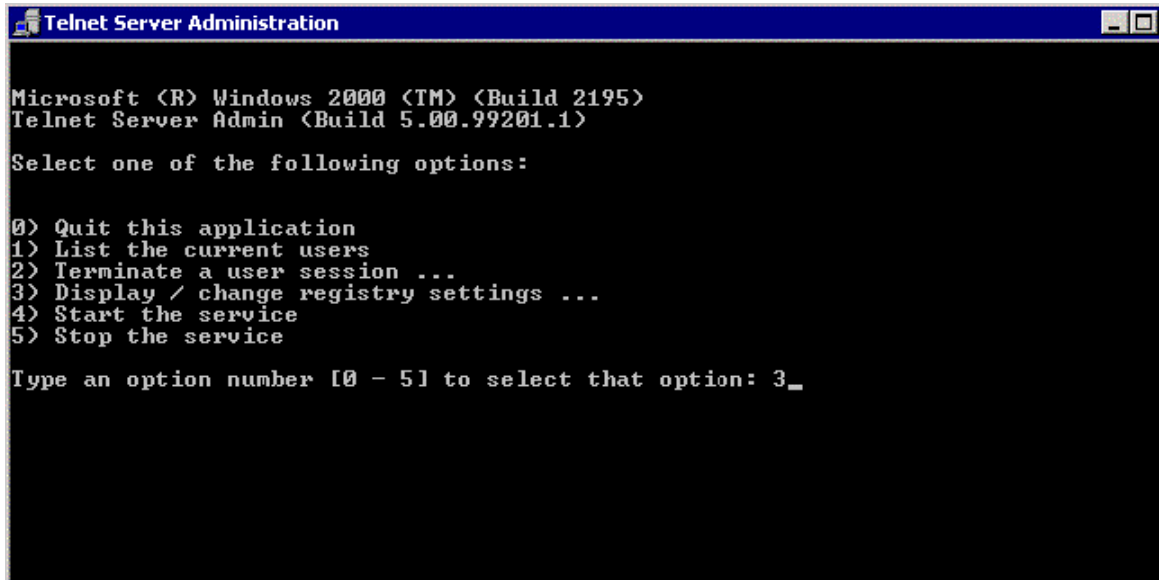
```
cd /
telnet -n tntrace
toggle options
toggle netdata
toggle prettydump
open host
```

When done, exit as normal and the file tntrace.log will have a record of the telnet session.

Configuring Under Windows 2000

If the terminal does not communicate with the Windows 2000 Telnet server, select Start, Settings, and Control Panel. Click on the Telnet Server Administration icon.

This brings up the following window.



```
Telnet Server Administration

Microsoft (R) Windows 2000 (TM) (Build 2195)
Telnet Server Admin (Build 5.00.99201.1)

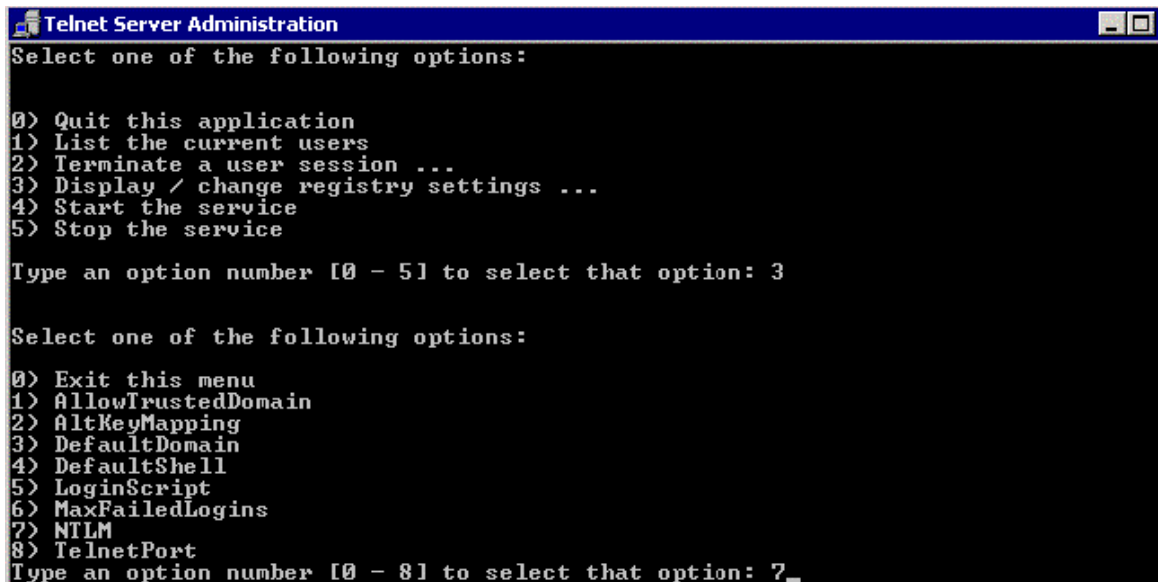
Select one of the following options:

0) Quit this application
1) List the current users
2) Terminate a user session ...
3) Display / change registry settings ...
4) Start the service
5) Stop the service

Type an option number [0 - 5] to select that option: 3_
```

Select 3 to change the settings.

Select the NTLM (NT LAN Manager) option (7).



```
Telnet Server Administration

Select one of the following options:

0) Quit this application
1) List the current users
2) Terminate a user session ...
3) Display / change registry settings ...
4) Start the service
5) Stop the service

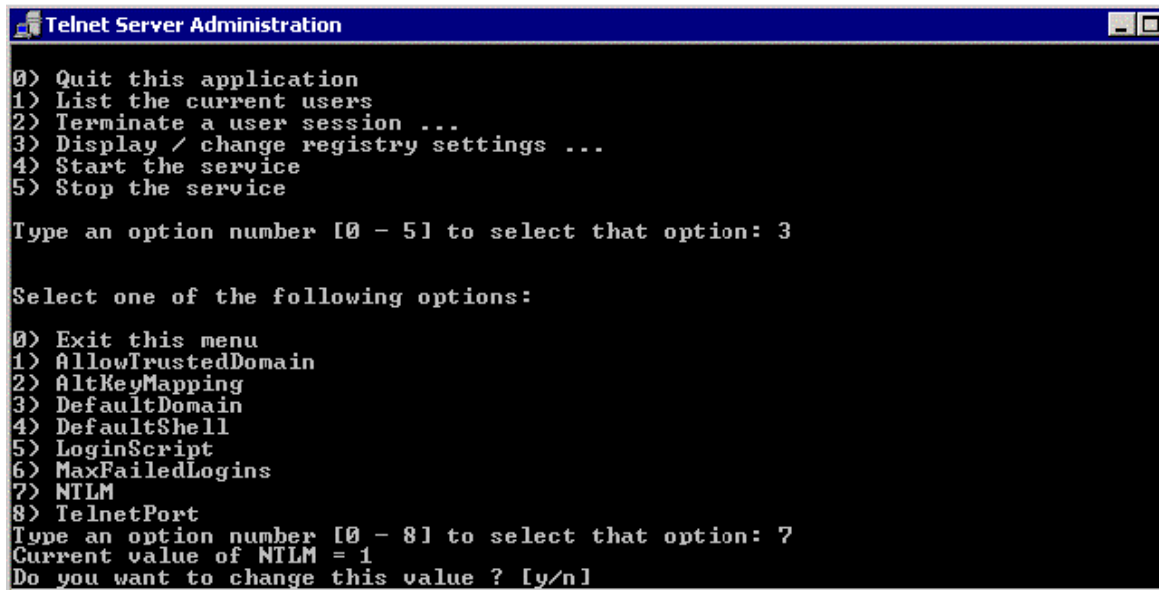
Type an option number [0 - 5] to select that option: 3

Select one of the following options:

0) Exit this menu
1) AllowTrustedDomain
2) AltKeyMapping
3) DefaultDomain
4) DefaultShell
5) LoginScript
6) MaxFailedLogins
7) NTLM
8) TelnetPort

Type an option number [0 - 8] to select that option: 7_
```

Change the setting to 1 and save it.

A screenshot of a Windows console window titled "Telnet Server Administration". The window has a blue title bar with a small icon on the left and standard window controls on the right. The main area is black with white text. The text shows a menu of options, with option 3 selected. The prompt "Type an option number [0 - 5] to select that option:" is followed by the number 3. Then, a second menu is shown with option 7 selected. The prompt "Type an option number [0 - 8] to select that option:" is followed by the number 7. Below this, it says "Current value of NTLM = 1" and "Do you want to change this value ? [y/n]".

```
Telnet Server Administration

0) Quit this application
1) List the current users
2) Terminate a user session ...
3) Display / change registry settings ...
4) Start the service
5) Stop the service

Type an option number [0 - 5] to select that option: 3

Select one of the following options:

0) Exit this menu
1) AllowTrustedDomain
2) AltKeyMapping
3) DefaultDomain
4) DefaultShell
5) LoginScript
6) MaxFailedLogins
7) NTLM
8) TelnetPort
Type an option number [0 - 8] to select that option: 7
Current value of NTLM = 1
Do you want to change this value ? [y/n]
```

Now Stop and Start the Windows Telnet server.

Response Time Issues ("Waiting for HOST" Loopback Test)

Introduction

Host response time is slow.

Problem Description

While using PowerNet, the Host transaction time is slow. Often, this will happen after an application, database, network, or some other host environment has changed.

Resolution

Compile the appropriate loopback test on the application host.

AS400:

Compile the following sections of code and have the terminals run against it from their site. If the response time is good, then the issue is not PowerNet and you will have to look at the application on the host side. If it is slow, move the application to the local site and rerun. If it gets better, then it is a network issue and you will need to resolve that with your network folks.

Or you could have them run against our site at 207.241.78.5 login as "train" password "train". When asked for a test number, take 6.

For the CLP file, view <http://www.connectrf.com/Documents/loopbackcl.txt>.

For the Display file, view <http://www.connectrf.com/Documents/loopbackds.txt>.

UNIX Shell:

```
clear
echo "Connect Loopback Test"
echo "How Many Loops?"
read n
echo "Seconds to Sleep in loop?"
read m
i=`expr 1`
while [ ${i} -le ${n} -o ${n} -eq 0 ]
do
    clear
    echo "Loop: $i"
    date
    sleep $m
    i=`expr ${i} + 1`
done
echo "DONE!"
```

Using Ataman © Telnet Server

The following details the testing that was done with the Ataman © telnet server product for NT using the PowerNet VT Emulation products. This is not an endorsement of this product nor a claim that an extensive test of its capabilities was performed.

Basic setup and session tests were performed to ensure that the two products were able to establish sessions and perform simple tasks.

This section can be used to help troubleshoot connection problems by documenting how each product was installed, setup and tested. It can provide a mechanism to verify the basic functionality of each product.

Problems with NT Telnet servers, in general, are most likely not problems with the server or the emulator products. Most of the problems are NT or network related. There are problems with how TCP/IP was installed and configured, problems with how NT security was setup, and problems with applications that don't obey the rules for character based NT server products.

This section is not meant to give guidance on these subjects but rather document a setup and test procedure to confirm basic functionality.

Where Can I Get this Product?

You can find the Ataman Telnet server on the WEB at this address:

<http://www.ataman.com/>

What Versions Were Used in the Test?

Ataman © Version	Version 2.5 for X86 Processors
PowerNet Version	HHP OEM Version 112503D5
Terminals Tested	HHP Dolphin Alphanumeric BIOS 2.65 RangeLAN2 V3.3
Windows Version	Window NT Release 4.0 Build 1381 with Service Pack 3 installed

How Were the Products Installed and Setup?

1. Create directory: **mkdir c:\atrls2**
2. Unzip files into this directory.
3. Type install command: **atrls install start**
4. This step takes only a few moments and it then displays that Ataman © has been installed and is running.
5. It is necessary to setup an Ataman © user which is done with an icon under the NT control panel.
6. Created a user with these entries only:
User Name: **Greg**
NT user Name: **gwk**
Home Directory: **C:**
Leave all other fields blank

Note: The test was performed with the standard Windows Telnet Client from a networked attached machine running Windows 95. The test was a login and a directory listing.

PowerNet TN Setup

The PowerNet TN VT100 emulation was set up with the default settings and the terminal was loaded with these settings. The IP addresses of the terminal and host were set and a reboot was performed.

What Test Was Done?

A test was performed to determine that a Telnet Session could be established.

This test was done multiple times with different exit conditions, as follows:

- a. Normal Exit (by typing exit at the NT command prompt)
- b. PowerNet "Session End" Exit (by pressing the PowerNet session end key)
- c. Abnormal end (by cold booting the terminal)

All tests passed and the Ataman © and PowerNet TN products performed well.

Wireless Network Worksheet

Below is a Wireless Network worksheet to establish Ethernet IP's for the customer's network.

What is a netmask?

In administering Internet sites, a netmask is a string of 0's and 1's that mask or screen out the network part of an IP address (IP) so that only the host computer part of the address remains. The binary 1's at the beginning of the mask turn the network ID part of the IP address into 0's. The binary 0's that follow allow the host ID to remain. A frequently-used netmask is 255.255.255.0. (255 is the decimal equivalent of a binary string of eight ones.) Used for a Class C subnet (one with up to 255 host computers), the ".0" in the "255.255.255.0" netmask allows the specific host computer address to be visible.

What is a router?

On the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks to which it is connected. A router is located at any gateway (where one network meets another), including each Internet point-of-presence. A router is often included as part of a network switch.

A router may create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet. Typically, a packet may travel through a number of network points with routers before arriving at its destination. Routing is a function associated with the Network layer (layer 3) in the standard model of network programming, the Open Systems Interconnection (OSI) model. A layer-3 switch is a switch that can perform routing functions.

An edge router is a router that interfaces with an asynchronous transfer mode (ATM) network. A brouter is a network bridge combined with a router.

What is a Host Application server?

The term "host" is used in several contexts, in each of which it has a slightly different meaning:

- 1) In Internet protocol specifications, the term "host" means any computer that has full two-way access to other computers on the Internet. A host has a specific "local or host number" that, together with the network number, forms its unique IP address. If you use Point-to-Point Protocol to get access to your access provider, you have a unique IP address for the duration of any connection you make to the Internet and your computer is a host for that period. In this context, a "host" is a node in a network.
- 2) For companies or individuals with a Web site, a host is a computer with a Web server that serves the pages for one or more Web sites. A host can also be the company that provides that service, which is known as hosting.
- 3) In IBM and perhaps other mainframe computer environments, a host is a mainframe computer (which is now usually referred to as a "large server"). In this context, the mainframe has intelligent or "dumb" workstations attached to it that use it as a host provider of services. (This does not mean that the host only has "servers" and the workstations only have "clients." The server/client relationship is a programming model independent of this contextual usage of "host.")

4) In other contexts, the term generally means a device or program that provides services to some smaller or less capable device or program.

What is an RF terminal?

A RF node is a TCP/IP-connected device whose location and point of attachment to the Internet may frequently be changed. This kind of node is often a cellular telephone or handheld or laptop computer, although a mobile node can also be a router. Special support is required to maintain Internet connections for a mobile node as it moves from one network or subnet to another, because traditional Internet routing assumes a device will always have the same IP address. Therefore, using standard routing procedures, a mobile user would have to change the device's IP address each time he or she connected through another network or subnet.

Since mobility and ease of connection are crucial considerations for mobile device users, organizations that want to promote mobile communications are putting a great deal of effort into making mobile connection uncomplicated for the user. The Internet Engineering Task Force (IETF) Mobile IP working group has developed several standards or proposed standards to address these needs, including Mobile IP and later enhancements, Mobile IP version 6 (MIPv6), and Hierarchical Mobile IP version 6 (MHIPv6).

What is a bridge?

In telecommunication networks, a bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or token ring). You can envision a bridge as being a device that decides whether a message from you to someone else is going to the local area network in your building or to someone on the local area network in the building across the street. A bridge examines each message on a LAN, "passing" those known to be within the same LAN, and forwarding those known to be on the other interconnected LAN (or LANs).

In bridging networks, computer or node addresses have no specific relationship to location. For this reason, messages are sent out to every address on the network and accepted only by the intended destination node. Bridges learn which addresses are on which network and develop a learning table so that subsequent messages can be forwarded to the right network.

Bridging networks are generally always interconnected local area networks, since broadcasting every message to all possible destinations would flood a larger network with unnecessary traffic. For this reason, router networks such as the Internet use a scheme that assigns addresses to nodes so that a message or packet can be forwarded only in one general direction rather than forwarded in all directions.

A bridge works at the data-link (physical network) level of a network, copying a data frame from one network to the next network along the communications path.

A bridge is sometimes combined with a router in a brouter.

Object Addresses	Network Address
Network Netmask	
Network Gateway/Router	
Host Application Server	
RF Terminal Node	
Access Point Node	

About This Document

This document is based on the following Technical Documents in our Notes Database that have been made obsolete: T1089, T1103, T1113, T1114, T1121, T1173, T1194, T1214, and T1216.

Please let us know about any errors in this document at:

<http://207.241.78.223/isoxpert/calltrak.nsf/WebTracking?OpenForm>.