

Data Management, Inc.
3322 West Loop 306
San Angelo, TX 76904
800 749-8463
325 223-9500



Installation Instructions

Congratulations on your purchase of the new *Integrity Series RT/RT Plus*™ terminal which provides for all of your time attendance needs in Real Time directly from this terminal. Additionally, the RT+ model provides real time clock punches (time transactions) regardless of network availability. When network communication fails, the RT+ terminal automatically enters the Fallback mode and records up to 2,000 punches in real time using a highly accurate on board clock to insure the integrity of your data. Once network operation resumes, the terminal returns to Real Time mode and the TimeClock Plus server automatically retrieves the punches.

These installation instructions present the information that the installer needs at the time the information is needed. These instructions are worded for the non-technical installer with technical information for the IT Department in appendix A and managerial information in appendix B. Appendices C through D deal with Troubleshooting, Frequently Asked Questions, Terminal Key Pad explanation, and a Glossary for Technical Terms,.

Visual cues help you to locate information fast and easy by scanning pages looking for the special fonts that indicate **Subtitles**, **SUBTOPICS**, and **KEYWORDS** (keypad entries, terminal messages, and clickable screen items).

Shipping Inventory

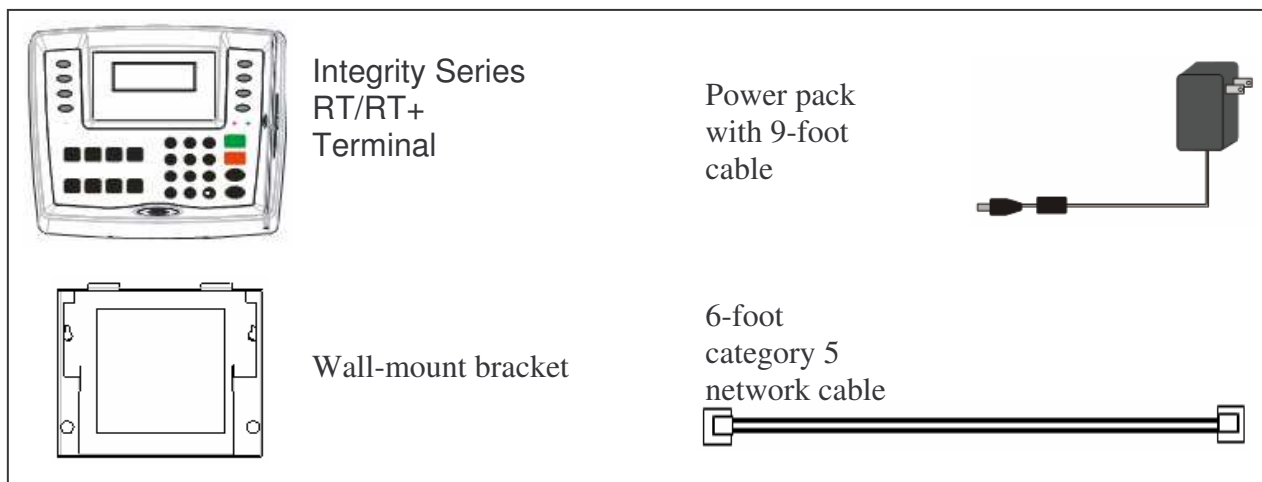




Table of Contents

Shipping Inventory	1
Getting Ready – Things an Installer Needs To Start.....	3
Configuring the Integrity Series RT/RT+ Ethernet Terminal	3
Configuring WinRemote	3
Testing the Terminal	3
Hardware Mounting and Cabling.....	3
Appendix A – Information Provided by Your IT Department.....	3
TERMINAL CONFIGURATION OPTIONS	3
CONFIGURING WINREMOTE OPTIONS	3
Appendix B –a Manager’s Supplemental Guide for Unresolved Punches in TimeClock Manager.....	3
TYPES OF UNRESOLVED PUNCHES	3
Appendix C – Troubleshooting.....	3
MY ETHERNET TERMINAL DOESN’T WORK USING A LONG CABLE.....	3
HOW CAN I GET AN ETHERNET CABLE LONGER THAT 100 METERS TO WORK?	3
WINREMOTE ERROR “THE SYSTEM WAS UNABLE TO START THE PORT”	3
THE TERMINAL IS NOT COMMUNICATING WITH THE SERVER. HOW CAN I TELL IF IT IS A SERVER PROBLEM OR A NETWORK PROBLEM?	3
HOW DO I TEST THE TERMINAL?.....	3
HOW DO I TEST CABLE CONTINUITY?	3
WHAT’S ELECTRICAL NOISE?.....	3
Appendix D – Frequently Asked Questions.....	3
WHAT IS THE ACCURACY OF THE REAL-TIME-CLOCK-CALENDAR?	3
DURING A POWER LOSS, WHAT HAPPENS TO THE REAL-TIME-CLOCK-CALENDAR?	3
HOW LONG CAN TIME TRANSACTIONS SURVIVE WITHOUT POWER?	3
WHAT TRIGGERS FALLBACK MODE?	3
HOW LONG CAN FALLBACK MODE CONTINUE TO OPERATE?.....	3
WHAT HAPPENS WHEN THE NETWORK CONNECTION IS RE-ESTABLISHED?	3
WHERE CAN THE ETHERNET CABLE FROM THE TERMINAL BE PLUGGED IN?	3
WHAT IS THE MAXIMUM LENGTH CATEGORY 5 CABLE THAT I CAN USE?	3
CAN I PLUG THE ETHERNET CABLE DIRECTLY BETWEEN THE TERMINAL AND MY NIC CARD?	3
HOW CAN I FIND OUT WHAT IP ADDRESS THE TERMINAL IS RUNNING ON?	3
Appendix E – Key Functions of the Integrity Series RT/RT+ Terminal	3
Appendix F – Glossary	3



Getting Ready – Things an Installer Needs To Start.

1. There are several pieces of information that your IT Department needs to provide to you regarding your network. Please give them “Appendix A – Information Provided by Your IT Department” located on pages 14 to 20 of this document. While you complete the next 2 steps, your IT Department can gather the network information that you need to configure the terminal and the supporting software.
2. Purchase enough category 5 cable to reach from the terminal to the nearest available network connection from your local network supplier. To meet category 5 specifications, your cable length must be 100 meters (300 feet) or less, and your cable needs RJ-45 connectors which the *Integrity Series RT/RT Plus™* terminal (and virtually any other Ethernet device) uses.
3. You need to examine the wall material where you intend to mount the terminal to determine the appropriate mounting hardware to purchase. (The preferred location is a smooth surfaced interior wall protected from weather and climate extremes. The preferred height is 48 to 52 inches above the floor.)



Configuring the Integrity Series RT/RT+ Ethernet Terminal

1. Terminal configuration does not require a network connection.
2. Within 5 seconds of connecting the power to the unit, press and hold both the **F1** and the **YES\ENTER** keys together. The terminal will beep and the first line of the terminal display will show "**TERMINAL MANAGEMENT**". (If you miss pressing these keys in the first 5 seconds of power, then you must un-plug the power for 2 seconds, and try again).

3.

<u>Terminal Display</u>	<u>Your Entries</u>
XPERT CHECKOUT?	No\Esc
XPERT SETUP?	YES\ENTER
NETWORK SETTINGS?	YES\ENTER

LOCAL IP:

Use the static IP Address provided here by your IT Department. Depending on the number of digits used in your IP Address, it may be necessary to press **YES\ENTER** in order to proceed.

SUBNET MASK:

Use the subnet mask provided here by your IT Department. Depending on the number of digits used in your subnet mask, it may be necessary to press **YES\ENTER** in order to proceed.

DEFAULT GATEWAY:

Use **0.0.0.0** unless your IT Department recommends otherwise. Press **YES\ENTER** to proceed.

LOCAL PORT:

Enter the port number supplied by your IT Department, then press **YES\ENTER**



Configuring the Integrity Series RT/RT+ Ethernet Terminal (continued)

TCP TIMEOUT:

Enter the number of seconds supplied by your IT Department, then press **YES\ENTER**. Data Management, Inc. strongly recommends 60 seconds.

TELNET PORT:

Repeatedly press Clock In until you see either Enable or Disable as specified by your IT Department, then press Yes\Enter

ECHO PORT:

Repeatedly press Clock In until you see either Enable or Disable as specified by your IT Department, then press Yes\Enter

TFTP PORT:

Repeatedly press Clock In until you see either Enable or Disable as specified by your IT Department, then press Yes\Enter

ETHERNET SPEED:

Repeatedly press Clock In until you see either 10Mb Only or 100Mb Only or 10/100Mb Auto as specified by your IT Department, then press Yes\Enter

AUX SETTINGS:

No\ESC

READER SETTINGS:

No\ESC

EXIT?

YES\ENTER

SAVE CHANGES?

YES\ENTER

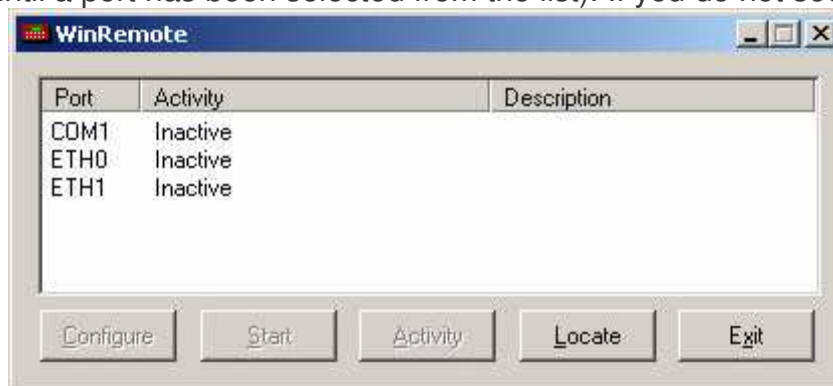
(The Integrity RT/RT+ Series Terminal will reset, and save the network settings you adjusted.)



Configuring WinRemote

Note: This configuration only addresses the few WinRemote options related directly to the setup of the Integrity Series RT/RT+ Terminal. For an explanation of all the options in WinRemote, see the WinRemote section of the TimeClock Plus manual found on the TimeClock Plus installation CD.

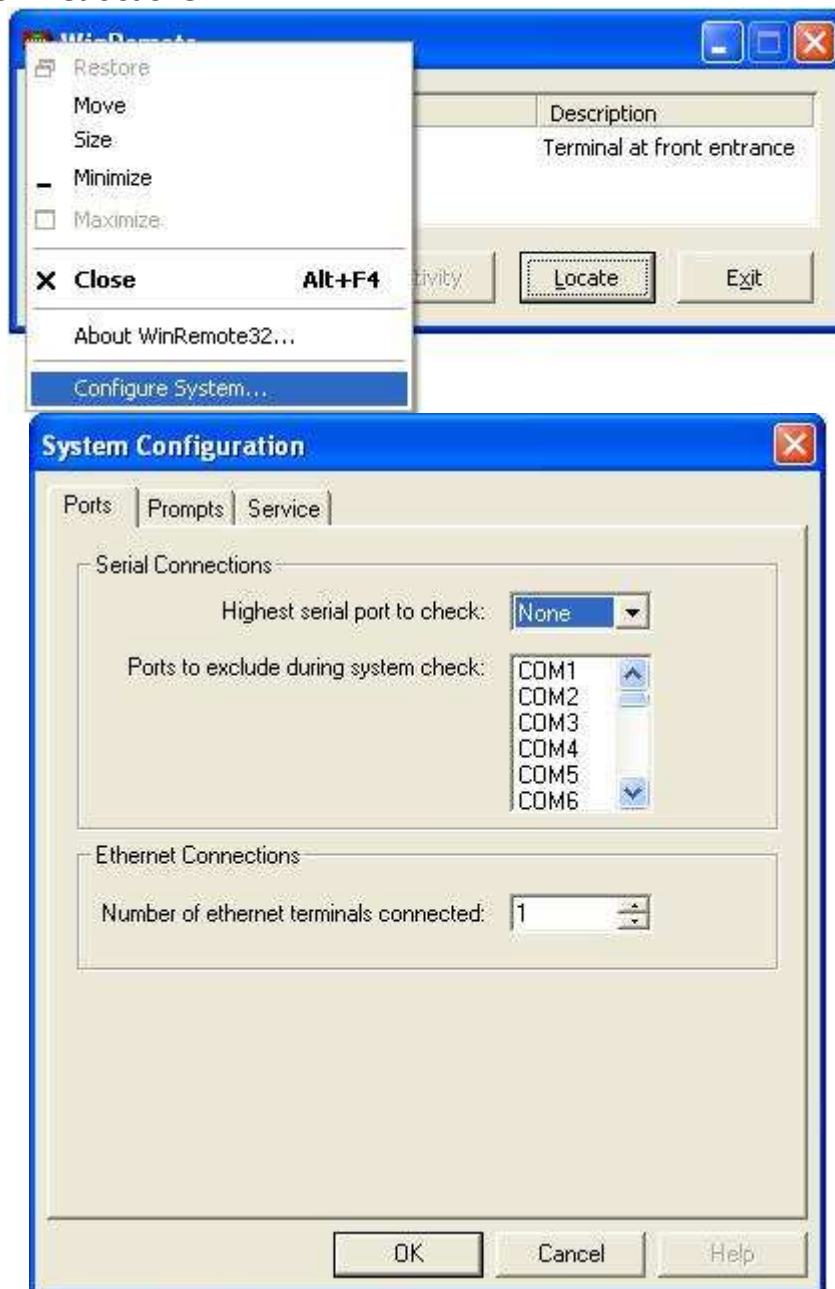
1. Install the TimeClock Plus software, and then return to these installation instructions. For TimeClock Plus software installation instructions, see the "License Agreement & Quick Start Guide" included with the TimeClock Plus CD or view the manual on the TimeClock Plus CD.
2. Verify that you are using the latest software by launching AutoUpdate from the TimeClock Plus menu and click **AVAILABLE**. A new window opens displaying available updates. Click **UPDATE**, then once updates are completed successfully, close the message windows and close AutoUpdate. You are now ready to begin Configuring WinRemote.
3. Verify that your IT Department provided the network related information in steps 10 and 11 below. Without the network information, you can not proceed.
4. During the WinRemote configuration, locating the terminal within easy reach of your server keyboard is the most convenient arrangement.
5. Connect the terminal to your network using the enclosed 6-foot category 5 network cable and apply power to the terminal.
6. Launch the WinRemote software by clicking in sequence **START**, **PROGRAMS**, **TIMECLOCK PLUS 5.x**, **WINREMOTE** and a new window opens on your screen.
7. To access a port for configuration purposes, select it from the table by clicking it to highlight it, and then click on the Configure button (this button will not become enabled until a port has been selected from the list). If you do not see an Ethernet





Configuring WinRemote (continued)

port then right click the title bar (a drop down box opens) and click **CONFIGURE SYSTEM** and enter 1 for the **NUMBER OF ETHERNET TERMINALS CONNECTED** click **OK** and follow screen instructions.





Configuring WinRemote (continued)

- Click the **CONFIGURE** button, and click the **OPTIONS** tab. From the Company drop down list, choose the company you want to associate with this terminal. If no companies appear in the drop down list, then you must launch TimeClock Manager and create the company before proceeding.

Note: A full explanation of the checkbox options on the **OPTIONS** tab is located in the sub-section “The Options Tab” of the section “Configuring the WinRemote Application” in the User Reference Guide located on the TimeClock Plus installation CD in the file named “MANUAL.PDF”.)

- Click the **TERMINAL** tab. The options in the “Operation Status” frame are new to WinRemote and are a matter of personal choice. These options allow you to set the beeps, tones, and the illumination time of LED status indicators on the terminal. The best approach to setting these options is a “try and see” experimentation. (The other options on this tab are explained in the sub-section “The Terminal Tab” of the section “Configuring the WinRemote Application” in the User Reference Guide located on the TimeClock Plus installation CD in the file named “MANUAL.PDF”.)

The screenshot shows the 'Configure Ethernet ETH0' dialog box with the 'Terminal' tab selected. The dialog has several tabs: Options, Terminal, Display, Badges, Communication, Access, RT+, and Modules. The 'Terminal' tab contains the following sections:

- Description:** A text input field.
- Options:** A group of checkboxes:
 - ☒ Display system time
 - ☒ Display only minutes in time
 - ☐ Auto-start this port
 - ☐ Allow badge test using 00
 - ☐ Allow id terminal using 11
 - ☐ Beep when a key is pressed
 - ☐ Bar code reader attached
 - ☐ Use new command set
- Operation Status:** A section with two columns of settings:
 - Success:** 0 beeps, Tone: 4 (dropdown), LED: 3.0 seconds (0.0-5.0)
 - Failure:** 0 beeps, Tone: 1-Low (dropdown), LED: 3.0 seconds (0.0-5.0)
- QuickPunch:** A section with two checkboxes:
 - ☐ Enable QuickPunch
 - ☐ Ignore QP within how many seconds of another punch: 60 (text input)

At the bottom right are 'OK' and 'Cancel' buttons.



10. Click the **COMMUNICATION** tab. This tab has two new frames, the “Monitoring” frame and the “Time Offset” frame. In the “Ethernet Settings” frame, enter the following items as recommended by your IT Department.

IP ADDRESS

PORT NUMBER

STARTUP DELAY

In the “Monitoring” frame, enter the following items as recommended by your IT Department.

ENABLE CONNECTION MONITORING FOR THIS PORT

ENABLE AUTOMATIC REFRESH FOR THIS PORT

If the server and terminal are in the same time zone, the Time Offset is set to **No OFFSET**. If your terminal is in a different time zone than your server, then choose the appropriate offset (from -12 to +12 hours).

Configure Ethernet ETH0

Options | Terminal | Display | Badges | **Communication** | Access | RT+ | Modules

Ethernet Settings

IP Address: 192 . 168 . 2 . 199

Port Number: 3001

Startup delay (in milliseconds): 1000

Monitoring

☒ Enable connection monitoring for this port
Monitor interval (in seconds): 30

☒ Enable automatic refresh for this port
Refresh interval (in seconds): 15

Time Offset

Offset from company time for this port: No Offset ▼

NOTE: It is recommended that the company option for obtaining the time be set to use the server time adjusted to a specified time zone.

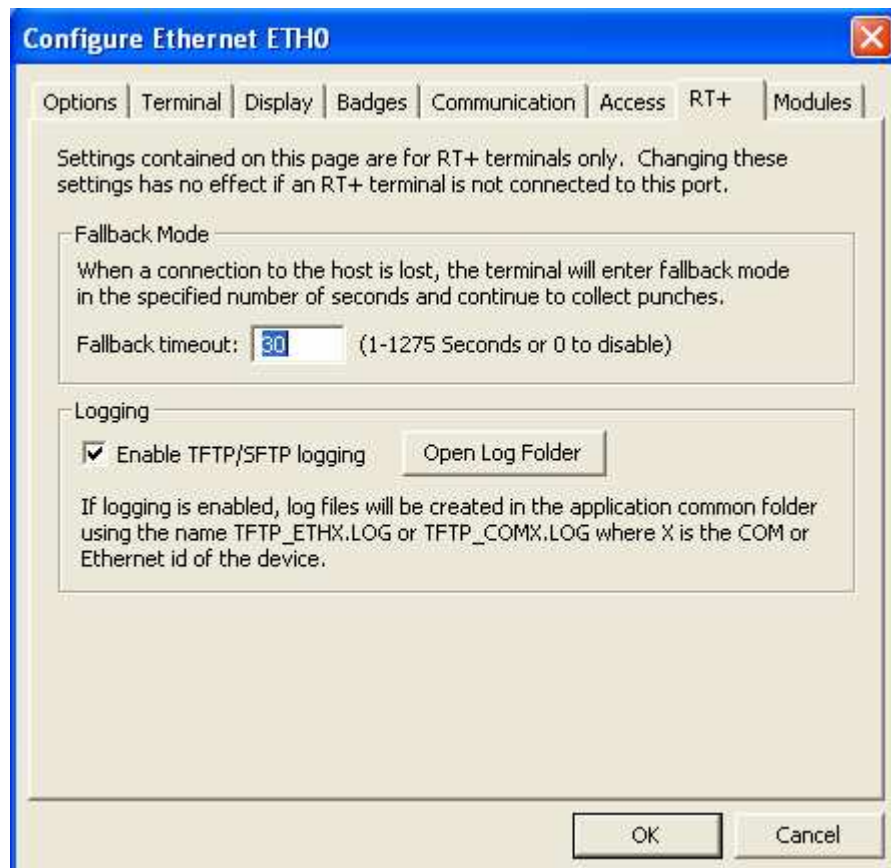
OK Cancel



11. Click the **RT+** tab, and enter the **FALLBACK TIMEOUT** as recommended by your IT Department.

FALLBACK TIMEOUT

Check the **ENABLE TFTP/SFTP LOGGING** option which creates logs with useful information for security checks and helps IT Department and/or Data Management, Inc. Technical Support to resolve problems.

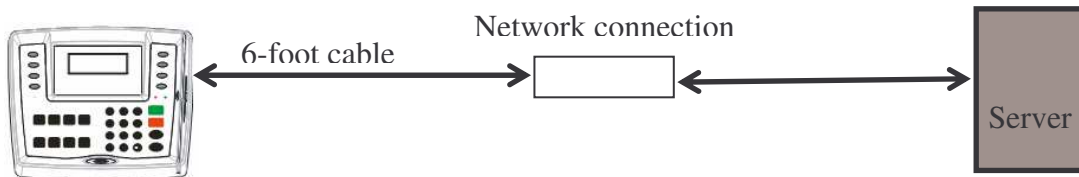


12. Click **OK** and the configuration window closes, and the previous WinRemote window is now visible. Leave this window open, and go to step 4 of the next section "Testing the Terminal".

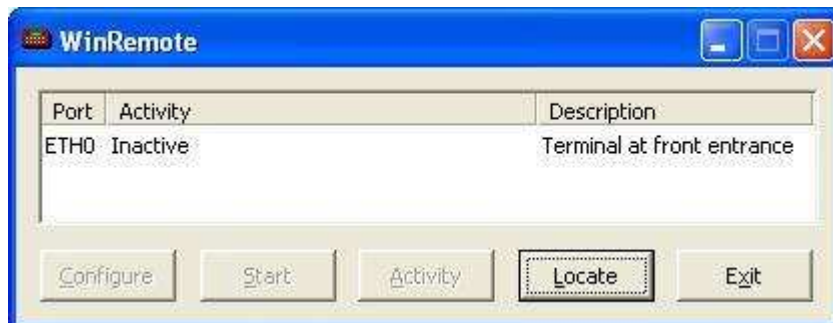


Testing the Terminal

1. During the terminal testing, you will find that locating the terminal within easy reach of your server keyboard is the most convenient arrangement. For this test, use the 6-foot category 5 network cable that shipped with this terminal. Note: The phrase “Network connection” used in this document is a generic term for a connection such as a router, switch, hub, or bridge.



2. Verify that you are using the latest software by launching AutoUpdate from the TimeClock Plus menu and click **AVAILABLE**. A new window opens displaying available updates. Click **UPDATE**, then once updates are completed successfully, close the message windows and close AutoUpdate. You are now ready to begin Configuring WinRemote.
3. If you're not already in WinRemote, then launch the WinRemote software by clicking in sequence **START**, **PROGRAMS**, **TIMECLOCK PLUS 5.x**, **WINREMOTE** and a new window opens on your screen.



4. Select the port associated with the terminal you want to test by clicking on the port name (ETH0 in the above example) and it becomes highlighted. While looking directly at the terminal, click **START** in WinRemote, and the terminal flashes these messages in rapid succession:

INITIALIZING TERMINAL ... ONE MOMENT ...

RETRIEVING PUNCHES FROM DEVICE ... ONE MOMENT ...

After briefly displaying the above two messages, the terminal returns to Real Time mode and waits for an employee to make a punch.



Testing the Terminal (continued)

5. While looking at the terminal, click Stop in WinRemote, and the terminal displays the following message:

TIMECLOCK PLUS OFFLINE

6. If the above test fails, verify your terminal and WinRemote configurations, and repeat the test. If the test still fails call Data Management, Inc. support at (325) 223-9300 Monday through Friday 9:00 a.m. to 5:00 p.m. (central time zone).
7. When the terminal works using the 6-foot cable, then mount your terminal at the location you have chosen per the instructions, "Hardware Mounting and Cabling" on page 12.
8. Presuming that the terminal is mounted and using a different and probably a much longer cable, so we need to test again. At the TimeClock Plus server keyboard, launch the WinRemote software by clicking in sequence **START**, **PROGRAMS**, **TIMECLOCK PLUS 5.x**, **WINREMOTE** and a new window opens on your screen (same as in step 3).
9. Select the port associated with the terminal you want to test by clicking on the port name (ETH0 in the example).

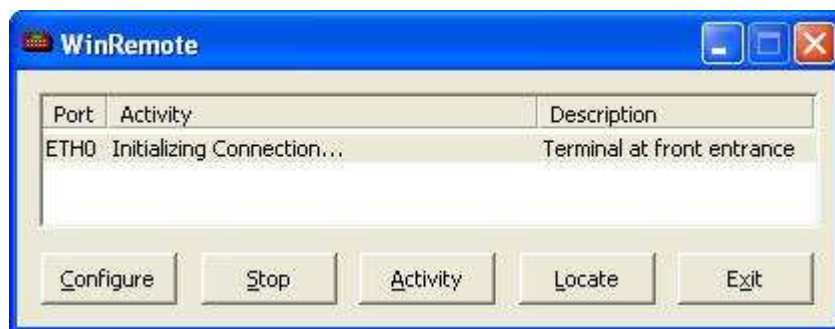


(Instructions continue on next page)



Testing the Terminal (continued)

10. Success is determined by the following screenshots occurring in rapid succession after clicking **START**. If you see something different then go to step 11 on the next page; otherwise, clicking **STOP** will return you to the screenshot shown in step 9. If you installed a *Integrity Series RT Plus™* terminal, then please give a copy of appendix B to each manager having employees that punch on the terminal. Congratulations your installation is finished.





11. The following screenshot indicates a failure, see “Appendix C – Troubleshooting” under the subject of “My terminal doesn’t work using a long cable” on page 23.

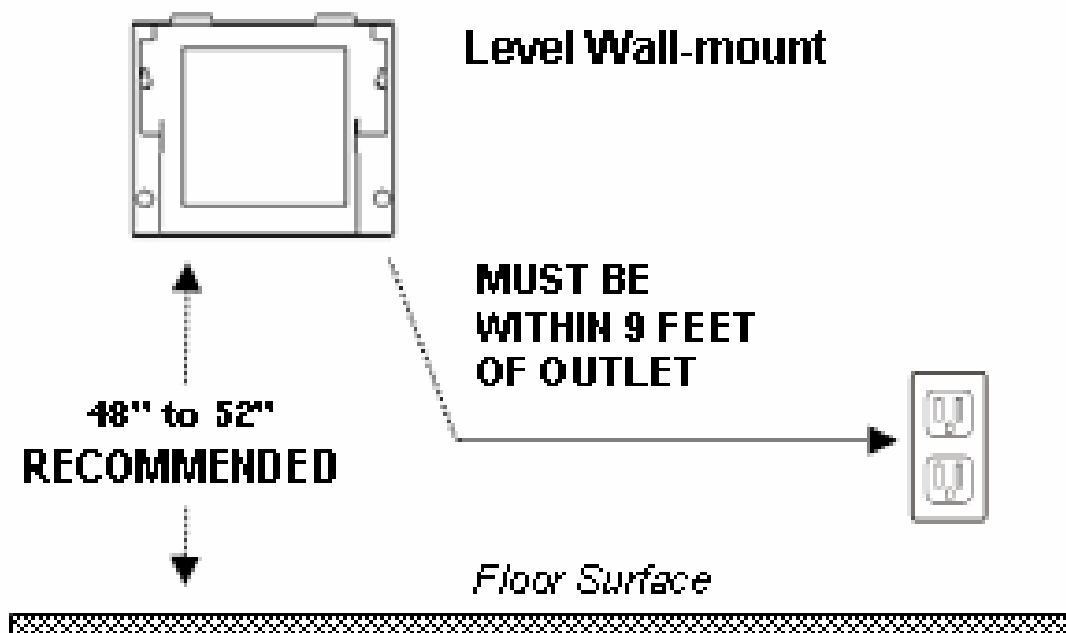




Hardware Mounting and Cabling

Select an interior location protected from weather or extreme temperatures, and a smooth surfaced wall. The mounting hardware is dependent on the type of wall material where the terminal is mounted. Regardless of the wall material the installation proceeds as:

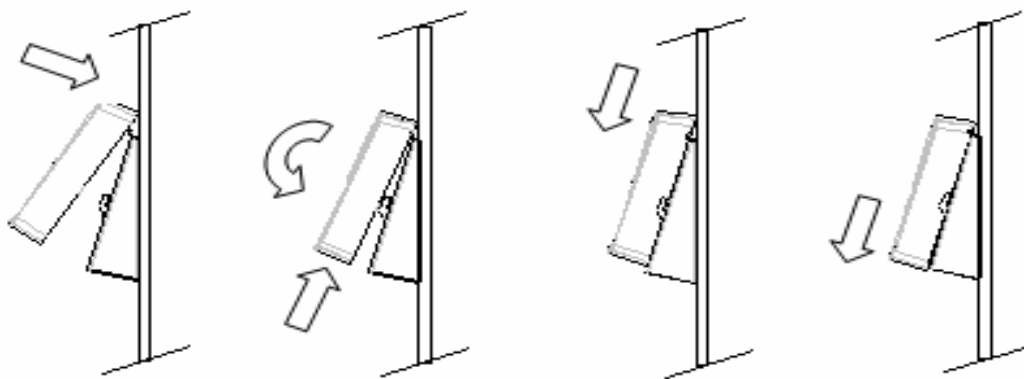
1. Select the most convenient location to mount your new terminal. (The recommended height above the floor is 48 to 52 inches). The maximum cable length specified by the category 5 cable standard is 100 meters, but the shortest cable length is preferred because the shortest length delivers the best signal.
2. Configure the terminal and the server software, and test the terminal as described in "Testing the Terminal" on page 11.
3. For your convenience, the wall-mount bracket is predrilled for either #8 or #10 screws for mounting, but the material that your wall is made of will dictate the method of attachment.





Hardware Mounting and Cabling (continued)

4. Connect the category 5 cable and power pack cable to the terminal and then attach the terminal to the wall-mount. (For your convenience there are 3 “punch out” holes and 1 predrilled hole for the routing of cables.)



5. Plug in the terminal power pack.
6. To finish the installation go to “Testing the Terminal” step 8.
7. If you installed the *Integrity Series RT Plus*™ terminal, then give a copy of appendix B to each manager having employees that punch on the terminal.



Appendix A – Information Provided by Your IT Department

The person performing the installation of the Integrity Series RT/RT+ Terminal needs information that can vary widely from network to network; therefore, your IT Department needs to provide the information.

This appendix presents background information with criteria and advantages of the possible choices, and then asks for your decision on the matter.

Note: In order that IT Department personnel might better communicate with Human Relation and Payroll personnel, this note about occupational jargon is offered. The common interchangeable terms in IT for “time stamp” or “date stamp” is equivalent to the common interchangeable terms used between Human Relation personnel and Payroll personnel which is referred to as a “punch” or “time transaction”. In appendix A, which is written for IT personnel, the term time stamp is used.

The primary purpose of this terminal is to provide the TimeClock Plus server with a time stamp when an employee presses either of the terminal keys: **CLOCK IN** or **CLOCK OUT**. If the network goes down, the terminal enters the “Fallback” mode and uses an on board clock for its time stamp source. Up to 2,000 time stamps can be stored in flash memory. When network communication is restored time stamps in flash memory are transfer to the server, and the terminal returns to the Real Time mode of operation. Each time the server communicates with the terminal, the on board clock is set to the server time. Setting the terminal time to the server time serves the purpose of time synchronization between any number of terminals and any number of On-Screen TimeClocks, which is a software version of a terminal used on desktops.

Caution: In order to avoid unnecessarily calling attention to your network availability time, Data Management, Inc. recommends conservative settings in this appendix. You have the power to make these settings as liberal as you like, but if carried to an extreme, such settings will interpret heavy Ethernet traffic as a network failure.

TERMINAL CONFIGURATION OPTIONS

This terminal operates as an Ethernet terminal and requires its own unique static IP address. If the communication path between the server and the terminal passes through a gateway, then the gateway information is applicable, otherwise specify



Appendix A – Information Provided by Your IT Department (continued)

0.0.0.0 as the gateway address. If your company is installing a number of terminals then you need to specify the IP Address, subnet mask, and gateway for each terminal.

STATIC IP ADDRESS:

MASK NUMBER:

GATEWAY:

The application that communicates with the terminal is an application called WinRemote and the filename is named WINRMT32.EXE. Because Data Management, Inc. can not predict which ports your current applications use, we provided a programmable port. Please provide the port number you prefer WinRemote and the terminal to use:

LOCAL PORT (if no preference, use 3001):

If the network goes down then the server has no means to communicate with the terminal to force the terminal to reset (close) the terminal communication socket. The purpose of the **TCP TIMEOUT** is to force the terminal to close its socket, and wait for the server to initialize another connection. The programmable range for **TCP TIMEOUT** is 1 – 99 seconds, and 0 seconds will disable the **TCP TIMEOUT**.

When an employee presses **CLOCK IN** or **CLOCK OUT** he/she must wait for either the server to respond or the terminal to enter Fallback mode. Of course the server responds first 99.999% of the time, and when the network does go down the terminal goes into Fallback mode automatically (meaning the chance of an employee pressing a key just as the network goes down and the employee having to wait for a timeout, is about the same odds as winning the lottery!)

But in the case of a busy network with many Ethernet conflicts, the worse case scenario is a timeout that is just enough time to work when the network traffic is low. In this scenario, when the network traffic increases, Ethernet conflicts cause the terminal to repeatedly flip-flop between modes. Each time the mode changes from Real Time to Fallback forces another disconnect and reconnect between server and terminal. Should an employee try to use the terminal, then he or she must wait for the completion of the mode change.



Appendix A – Information Provided by Your IT Department (continued)

After your terminal is in operation, you can see how often your terminal is switching modes by opening WinRemote, and select the port for this terminal and click **CONFIGURE**. Click the **RT+** tab and click the **OPEN LOG FOLDER** button. From the log files shown, open **ACTV1000.LOG** and search for the string “The connection to the device has been lost”.

TCP TIMEOUT (strongly recommend using 60): _____

The purpose of having a **TELNET PORT** is to allow an independent method of testing the network communications separate from the WinRemote application. You can test the network connection with the terminal using the HyperTerminal. Anything you type on HyperTerminal shows in the terminal display and any key you press on the terminal shows in HyperTerminal.

TELNET PORT (recommend Enable) _____

Another method to test network connection to the terminal uses the **ECHO PORT** which will answer a ping request, if the **ECHO PORT** is set to **ENABLE**.

ECHO PORT (recommend enable) _____

The TFTP (Trivial File Transfer Protocol) port is used to flash the terminal firmware.

TFTP PORT (recommend enable) _____

There are 3 communication speed options for this terminal (**10 MB ONLY**, **100 MB ONLY**, or **10/100MB AUTO** which switches between 10Mb and 100Mb communications as needed). Typically, your best choice is **10/100MB AUTO**.

ETHERNET SPEED _____

This concludes the gathering of network related information and option decisions for the terminal configuration. If you will copy your decisions to the installation instructions on pages 5 and 6, then non-technical personnel can configure the terminal(s).

The next page addresses the options used in the WinRemote application that manages the communications between server and terminal.



Appendix A – Information Provided by Your IT Department (continued)

CONFIGURING WINREMOTE OPTIONS

The WinRemote **COMMUNICATION** tab needs the same static IP Address and Port number you chose in the terminal configuration.

IP ADDRESS _____

PORT NUMBER _____

When WinRemote starts there is an option to delay the initial communication with the terminal. The programmable delay range is 0 to 34,463 milliseconds. This option is provided as a tool for dealing with unusual situations and is unique to your server situation.

STARTUP DELAY (if no preference, use 1000): _____

When checked, the **ENABLE CONNECTION MONITORING FOR THIS PORT** causes the server to periodically send a 1-byte data packet to the terminal and then it waits for 45-bytes of data concerning terminal status which is logged to ACTV1000.LOG (located in the TimeClock Plus folder). A programmable range of 30 to 9999 seconds offers great flexibility for unique network specific situations, but unless your particular situation dictates otherwise, Data Management, Inc. strongly recommends 30 seconds. A 30 second setting (used with the other Data Management, Inc. recommendations) requires the loss of 3 or more consecutive server to terminal communications at 30 second intervals before the terminal enters Fallback mode.

ENABLE CONNECTION MONITORING FOR THIS PORT (recommend 30) _____

When checked, the **ENABLE AUTOMATIC REFRESH FOR THIS PORT** forces the terminal display to refresh by sending 95-bytes of data from the server to the terminal on a repeating interval of 15 to 9999 seconds. This option is provided as a tool for unusual situations. If your particular network situation requires that you change **ENABLE CONNECTION MONITORING FOR THIS PORT** to a longer period of time than 30 seconds, then check **ENABLE AUTOMATIC REFRESH FOR THIS PORT** and set it to 30 second.

ENABLE AUTOMATIC REFRESH FOR THIS PORT (recommend unchecked) _____



Appendix A – Information Provided by Your IT Department (continued)

When the network connection fails (for whatever reason) it becomes impossible for the server to tell the terminal to reset its communication hardware. That task must be accomplished by the terminal alone. The terminal closes its communication socket when the **TCP TIMEOUT** expires. Then the terminal waits for the server to initialize another connection, but it's not reasonable to wait forever! The waiting period is controlled by a second timer called the **FALLBACK TIMEOUT**. If the server has not reestablished the connection with the terminal by the time **FALLBACK TIMEOUT** expires, then the terminal begins operating in Fallback mode while it continues to wait for the server to reestablish network communication. When the server reconnects with the terminal then WinRemote sends the **FALLBACK TIMEOUT** value to the terminal as part of the terminal reconnect and initialization information.

A programmable range of 1 – 1,275 seconds, (and 0 seconds disables the **FALLBACK TIMEOUT**) provides for a wide range of unique and unusual situations, but unless your network situation dictates otherwise, Data Management, Inc. strongly recommends 30 seconds.

FALLBACK TIMEOUT (recommend 30) _____

For a terminal to enter Fallback mode, both **TCP TIMEOUT** (recommend 60 seconds) and the **FALLBACK TIMEOUT** (recommend 30 seconds) must both expire. If **ENABLE CONNECTION MONITORING FOR THIS PORT** is set to the recommended 30 seconds, then the combination of these three time settings guarantee there must be 3 consecutive communication failures over 90 consecutive seconds. These are very conservative settings that were chosen, because no network should ever suffer so many Ethernet conflicts as to cause a false indication that the network is down. The network traffic generated by these conservative settings is only 90 bytes of data per minute.

Using a sniffer you may find how to make option settings that reduce your network traffic to a mere 16 bytes of data per minute, but it is not recommended. These time settings are strongly recommended, because if (and depending on, and how) certain options are setup in TimeClock Manager, a time stamp in Fallback mode may require each employee's manager to manually add job related information to each time stamp that occurred in Fallback. In the event of a true network failure, these time stamps are invaluable, but less conservative time settings may draw unwanted attention to your network availability.



Appendix A – Information Provided by Your IT Department (continued)

To determine if the terminal(s) are entering Fallback mode, you can search the ACTV1000.LOG file (located in the TimeClock Plus folder) for the string, "The connection to the device has been lost". If you find the string, you may desire to have more consecutive communication failures before the terminal goes into the Fallback mode. You can require 6 consecutive communication failures by opening the WinRemote application and checking the option **ENABLE AUTOMATIC REFRESH FOR THIS PORT** located on the **COMMUNICATIONS** tab and set the time for this option to 15 seconds. The maximum number of consecutive failures can be achieved by choosing options to display the time at the terminal in the format of HH:MM:SS. These options are in the terminal tab of WinRemote. Check **DISPLAY SYSTEM TIME** and un-checking **DISPLAY ONLY MINUTES** in time. By displaying the time in seconds the server must communicate with the terminal every second and if you followed Data Management, Inc. recommendations, that's 90 consecutive network communication failures!

This concludes the gathering of network related information and option decisions for the WinRemote configuration. If you will copy your decisions to the installation instructions steps 10 and 11 on pages 9 and 10, then non-technical personnel can configure WinRemote.

Consider keeping a copy of this appendix in the IT Department for future reference.



Appendix B – a Manager’s Supplemental Guide for Unresolved Punches in TimeClock Manager

This appendix is applicable only to the *Integrity Series RT Plus™* terminal.

Congratulations on your purchase of the new *Integrity Series RT Plus™* terminal that provides freedom from network problems. When network communication fails, the terminal automatically enters the Fallback mode and records up to 2,000 time transactions to insure the integrity of your data. Once network operation resumes, the terminal returns to the Real Time mode and the TimeClock Plus server automatically retrieves the transactions.

But, what if one of your employees mistakenly enters the wrong employee number during Fallback mode? That and other situations that invalidate the clock transaction are referred to as an unresolved punch. You can view these unresolved punches in TimeClock Manager by clicking **EMPLOYEE**, and clicking **UNRESOLVED PUNCHES**. Specify the date range that you are interested in, and click **UPDATE**.

If you find there are unresolved punches, then click the unresolved punch that you are interested in, which will highlight the unresolved punch, then click the **EDIT** button and the Edit Hours window opens with that particular employee’s hours showing.

TYPES OF UNRESOLVED PUNCHES

1. The employee canceled out of the operation.
2. The operation timed out waiting on employee input.
3. The employee is not clocked out and tried clocking in.
4. The employee is not clocked in and tried clocking out.
5. The employee tries clocking in or out before their clock in or out time.
(*This can occur if rounding is enabled.*)
6. The employee does not have a clockable job code.
(*See “Initial Setup of TimeClock Manager” in the User Reference Guide located on the TimeClock Plus installation CD in the file named “MANUAL.PDF”.*)
7. The employee is suspended.
(*The employee number entered at the terminal matches an employee number in the database, but that person is noted in the database as a suspended employee.*)



Appendix B – a Manager's Supplemental Guide for Unresolved Punches in TimeClock Manager (continued)

8. The employee is terminated.
(The employee number entered at the terminal matches an employee number in the database, but that person is noted in the database as a terminated employee.)
9. The employee is not setup for job costing.
(See "Initial Setup of TimeClock Manager" in the section of the User Reference Guide located on the installation CD in the file named "MANUAL.PDF".)
10. The employee has a conflicting shift.
(In Fallback mode, the employee did actually clock in, but when the network started working TimeClock Manager rejected the punch due to a conflicting shift. The reality is that the employee did in fact clock in and either is still working or worked until he/she clocked out.)
11. The employee id entered was not found.
12. The employee is trying to clock in but is restricted because they are in overtime already.
(In Fallback mode, the employee did actually clock in, but when the network started working TimeClock Manager rejected the clock in due to overtime. The reality is that the employee did in fact clock in and either is still working or worked until he/she clocked out.)
13. The employee is trying to clock in or out too early based upon their schedule and is not accepted because of schedule restrictions.
(In Fallback mode, the employee did clock in or clock out, but when the network started working TimeClock Manager rejected the clock action due to schedule restrictions.)
14. The employee is trying to perform an operation that is not within the scheduled window so it is not being accepted.
(In Fallback mode, the terminal does not have access to the employee's schedule which is stored on the server. Therefore, the employee did clock in or clock out, but when the network started working TimeClock Manager rejected the clock action due to the time being outside of his/her schedule.)



Appendix B – a Manager’s Supplemental Guide for Unresolved Punches in TimeClock Manager (continued)

15. The employee is trying to clock in but is restricted because they are over the maximum number of hours that can be worked without a supervisor override.
(In Fallback mode, the terminal does not have access to the employee’s hours which are stored on the server. Therefore, the employee did clock in or clock out, but when the network started working again, TimeClock Manager rejected the clock action due to the time being outside of his/her maximum number of hours worked.)



Appendix C – Troubleshooting

MY ETHERNET TERMINAL DOESN'T WORK USING A LONG CABLE

Verify that your terminal works as described in “Testing the Terminal” on page 11 of this document. This verification means your network setup is good, your terminal setup is good, the terminal hardware is good, and the network switch is good. Here are the remaining possible problems:

1. Verify you're using a category 5 cable.
2. Verify the cable is 100 meters or less in length which is the maximum length allowed in the category 5 specifications.
3. Visually inspect the connectors for damage, and test the cable continuity. (See “How do I test cable continuity?” on page 24 of this document for details.)
4. After verifying the previous three items, then the only possibility left is electrical noise. See “What's electrical noise?” on page 25 of this document for details.

HOW CAN I GET AN ETHERNET CABLE LONGER THAN 100 METERS TO WORK?

This is a request your IT Department should help you with.

WINREMOTE ERROR “THE SYSTEM WAS UNABLE TO START THE PORT”

This error occurs if WinRemote isn't able to take control of the IP Address specified in the WinRemote Communication tab. The problem may be the result of another network device using the same IP Address. To test for duplicate IP Address assignments, remove the Ethernet cable from the terminal and open a DOS prompt. Type PING *ip_address*, where *ip_address* represents the IP Address used in the WinRemote Communication tab.

If the ping command receives a reply, then the IP Address is currently in use by another device in the network and you must choose another IP Address for the terminal. See “Configuring the Integrity Series RT/RT+ Ethernet Terminal” and “Configuring WinRemote” for instructions for changing the IP Address.

If the ping command does not receive a reply, then verify that the terminal and WinRemote are both using the same IP Address and the same port number. See “Configuring the Integrity Series RT/RT+ Ethernet Terminal” and “Configuring WinRemote” for instructions for changing the IP Address and port number.



Appendix C – Troubleshooting (continued)

THE TERMINAL IS NOT COMMUNICATING WITH THE SERVER. HOW CAN I TELL IF IT IS A SERVER PROBLEM OR A NETWORK PROBLEM?

On the terminal under the F4 key is a Light Emitting Diode (LED) labeled “Status”. If the LED color is:

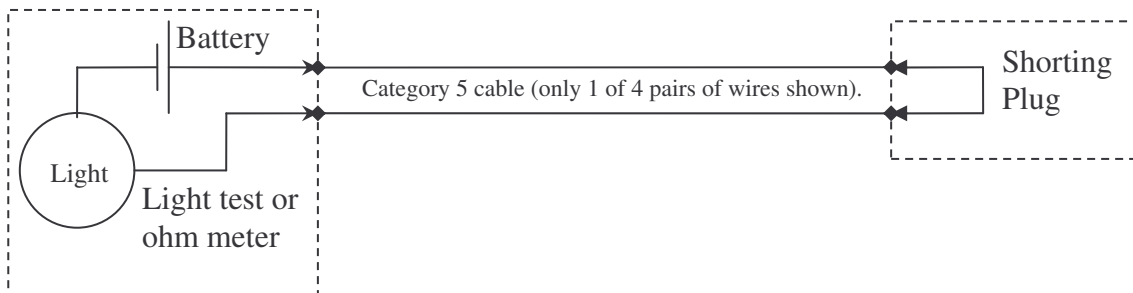
- Green the terminal is communicating with the server.
- Yellow the terminal is communicating with the network, but not the server. In this case, the server may be down or WinRemote is not running or a cable between the server and the network may have been removed.
- Red the terminal is not communicating with the network. The network may be down or the cable connection between the terminal and the network has been removed.

HOW DO I TEST THE TERMINAL?

See “Testing the Terminal” on page 11 of this installation document.

HOW DO I TEST CABLE CONTINUITY?

Visually inspect the connectors of your network cable for damage, and replace them if necessary. If the cable is visible, also visually inspect it for cuts, and replace if necessary. Lastly, build or purchase a female shorting plug that allows you to short the pins of the cable at one end, and then use an ohm meter or light test at the other end of the cable to test for continuity.





Appendix C – Troubleshooting (continued)

WHAT'S ELECTRICAL NOISE?

Electrical noise is an unusual problem, but a very real problem when it occurs. If your network cable runs in close proximity to a device that uses a great deal of electricity (or if your network cable runs in close proximity to the power lines to a device that uses a great deal of electricity) then there is a significant chance of introducing noise into your network cable. Another possibility is a device that creates a very strong magnetic field, high powered medical equipment, welding equipment, degaussing equipment, or fluorescent lighting. Whatever the source of electrical or magnetic noise, the solution is the same: move the cable away from the source (the further, the better).

In the extreme case of X-ray equipment, welding equipment, or radio-frequency transmitters, it may be necessary to use shielded network cable.



Appendix D – Frequently Asked Questions

WHAT IS THE ACCURACY OF THE REAL-TIME-CLOCK-CALENDAR?

+/- one minute per month

DURING A POWER LOSS, WHAT HAPPENS TO THE REAL-TIME-CLOCK-CALENDAR?

Data and time are maintained during power loss via an internal battery. The date and time are always current. The backup battery maintains date and time up to a year, and is synchronized with the server each time the server connects to the terminal.

HOW LONG CAN TIME TRANSACTIONS SURVIVE WITHOUT POWER?

One year

WHAT TRIGGERS FALLBACK MODE?

- The destruction or removal of the network cable.
- Loss of power to network devices such as Ethernet Switches, Hubs, etc.
- Network devices taken down for service
- The server locking up
- Accidentally turning off the server or WinRemote

HOW LONG CAN FALLBACK MODE CONTINUE TO OPERATE?

Until the non-volatile memory in the terminal is full. It takes 2,000 clock operations (Clock In or Clock Out), using a 10 digit ID to fill the memory.

WHAT HAPPENS WHEN THE NETWORK CONNECTION IS RE-ESTABLISHED?

The WinRemote server takes control of the terminal, and downloads any clock operations that took place in Fallback mode.

WHERE CAN THE ETHERNET CABLE FROM THE TERMINAL BE PLUGGED IN?

Any place you can add a computer to your network (to a hub or switch) using a standard category 5 cable, or you may plug it directly into the Network Interface Card (NIC) using a crossover cable.



Appendix D – Frequently Asked Questions (continued)

WHAT IS THE MAXIMUM LENGTH CATEGORY 5 CABLE THAT I CAN USE?

The maximum length specified by the category 5 standard is 100 meters

CAN I PLUG THE ETHERNET CABLE DIRECTLY BETWEEN THE TERMINAL AND MY NIC CARD?

You need a special category 5 cable referred to as a crossover cable and it is very likely that you can purchase it at a local computer store.

HOW CAN I FIND OUT WHAT IP ADDRESS THE TERMINAL IS RUNNING ON?

When the terminal is online you can press 11 to have the terminal show you're the IP Address and how long the device has been online. Note: If the terminal does not respond to 11, then the option needs to be enabled in WinRemote. Refer the manual on the TimeClock Plus installation CD in the WinRemote section.



Appendix E – Key Functions of the Integrity Series RT/RT+ Terminal

CLOCK IN	During Real Time and Fallback modes, the employee presses this key to initiate a clock in operation. During Offline mode the terminal displays TERMINAL MANAGEMENT and the CLOCK IN functions to scroll through a list of items to choose from.
CLOCK OUT	During Real Time and Fallback modes, the employee presses this key to initiate a clock out operation. During Offline mode the terminal displays TERMINAL MANAGEMENT and the CLOCK OUT functions to scroll through a list of items to choose from.
NO\ESC	This key is used to cancel out of the current screen, and go back to the previous screen.
YES\ENTER	This key is used to enter/submit the information after it has been entered via the numeric keys
0-9	These keys are used to enter a numeric value
.	This key is used to enter a decimal
←	This key is used as a backspace to remove numeric values that have been entered
COST CODE	This key is used to change cost codes. (Not available in the Fallback mode.)
JOB CODE	This key is used to change job codes. (Not available in the Fallback mode.)
START BREAK	This key is used to go on break. (Not available in the Fallback mode.)
OPTIONS	This key is used to test badges or to check the terminal id and what computer it is being hosted on. (Not available in the Fallback mode.)
HOURS	This key is used to view employee hours. *If enabled in TimeClock Manager defaults. (Not available in the Fallback mode.)
SCHED	This key is used to view employee schedules. *If enabled in TimeClock Manager defaults. (Not available in the Fallback mode.)
ACCRUAL	This key is used to view employee accrual totals. *If enabled in TimeClock Manager defaults. (Not available in the Fallback mode.)
OTHER	This key is currently not being used, but will provide additional functionality in the future.
F1-F8	These keys are 'soft keys'. They are currently used by modules to allow enrollment access and configuration. They will provide additional functionality in the future with additional options and the possibility of being mapped. (Not available in the Fallback mode.)



Appendix F – Glossary

Bandwidth	The number of bits per second (bps) or bytes per second of data transmitted.
Barcode reader	is an optical device that reads the bar code on the back of an employee's identification badge. You may purchase the badges and/or reader at Data Management, Inc. at (800) 749-8463.
Baud Rate	The rate at which a device can transmit data specified as bits per second (bps). Named after the French engineer Jean Maurice Emile Baudot.
Category 5 cable	A cable terminated by RJ-45 connectors with 4 pairs of twisted copper wire that supports frequencies up to 100 MHz and bandwidths up to 1,000 Mbps. It is used for 10Base-T, 100Base-T, and 1,000Base-T networking.
Echo Port	is an option that can be enabled on the Integrity Series RT/RT+ Terminal to allow it to respond to pings. It is useful for diagnosing problems with network connections, but should not be left enabled long term due to possible Denial of Service attacks.
Electrical continuity	is the ability to conduct electricity such as copper wire.
Ethernet	one of the most widely implemented LAN standards supports data transfer up to 100Mbps. The Ethernet standard was developed in 1976 by Xerox Corporation in cooperation with DEC and Intel..
External Reader	a mechanism connected to the terminal via cable that reads data from an employee's badge. You may purchase the badges and/or readers at Data Management, Inc. at (800) 749-8463. See barcode, magnetic, and proximity readers in this glossary for more details.
Fallback	is a mode of operation for the Integrity Series RT/RT+ Terminal when the network goes down. In Fallback mode the terminal can record up to 2,000 employee time transactions while it waits (for up to a year) for the network to start working again.



Appendix F – Glossary (continued)

Bridge	is a device that receives an Ethernet signal from one cable and amplifies that signal to full strength before sending the signal to another cable. The primary use of a bridge occurs when you need to send an Ethernet signal more than 100 meters which can be done by inserting a bridge every 100 meters or less.
Fallback Timeout	is the time between the Integrity Series RT/RT+ Terminal closing its network socket and the time the terminal enters the Fallback mode of operation. The Fallback Timeout allows the server time to reconnect with the terminal.
Gateway	A computer or server on a network that separates one network from another network. In your home, the gateway is your ISP that connects you to the internet.
Hub	is a network device that receives data, and then “broadcast” it to several other network devices at the same time and leaves it to the other network devices to determine whether to accept or ignore the data. Switches are better than hubs, because a switch does not broadcast, but sends the data to the one device that needs it.
Internal Reader	a mechanism included in the terminal that reads data from an employee’s badge. You may purchase the badges and/or readers at Data Management, Inc. (800) 749-8463. See barcode, magnetic, and proximity readers in this glossary for more details.
Internet	is the global network that connects more than 100 countries using TCP/IP protocols with millions of computers.
Intranet	a privately owned network at a person’s home or business that is not directly connected to the internet. If the intranet does have connection to the internet, it is kept separate by a gateway that blocks the internet’s visibility to see any intranet device behind the gateway.
IP	(pronounced as separate letters) Short for Internet Protocol.
IP Address	is a number used to identify a computer or device on a TCP/IP network. It must be a unique number on the network.



Appendix F – Glossary (continued)

IT	is short for Information Technology. It is pronounced as separate letters. IT is a general term for all facets of managing and processing information (principally associated with a large organization or company).
Magnetic reader	is a device that reads a magnetic strip on the back of employee badges. You may purchase the badges and/or reader at Data Management, Inc. (800) 749-8463.
Meter	One meter is the same as 39.5 inches
MHz	is the abbreviation for megahertz. One MHz is one million cycles per second written as either 1MHz or 1,000,000Hz.
Millisecond	stands for one thousand of one second. The abbreviation for millisecond is ms.
Network	A group of two or more computers that are connected together.
Network connection	a generic phrase used in this document meaning a connection to a router, switch, hub, or bridge.
Ohm meter	a meter that can determine how resistive a component is to electricity passing through the component.
Parity	is a method of verifying data has been transmitted accurately. The parity bit is added to every data unit. (A data unit is typically seven or eight bits). The parity bit for each unit is set so that all bytes have either an odd number or an even number of set bits. In the case of serial transmission of data, 1 or 2 set bits are appended to the data unit to indicate the end of the parity check.
Port	a vague term that can refer to either hardware or software, but in either case it refers to a method of moving data from one item to another.
Proximity reader	reads a Radio Frequency Identification (RFID) which is a very weak radio transmission produced by a tiny semiconductor device embedded inside of an employee's identification badge. You may purchase the badges and/or reader at Data Management, Inc. (800) 749-8463.



Appendix F – Glossary (continued)

Punches	within this document punches refers to a time transaction and comes from the old days when people used a punch card in a time clock to document their arrival at work. Punches mean the same as “time transactions”.
Real Time	means occurring immediately or responding immediately or without any delay. Real time refers to computer events that occur at the same speed as real life events.
RJ-45 connector	is a shorthand name for Registered Jack-45 connector. The connector is an eight-wire connector and commonly used with Ethernet networks. The RJ-45 connector appears similar to the RJ-11 connectors used on telephone equipment, but the RJ-45 is somewhat wider than the RJ-11 connector.
Router	is a device that provides a network connection to forward data to two or more computers and/or networks. Routers are better than hubs or switches because routers use headers and forwarding tables to determine the best path for forwarding the data. Routers communicate with each other and configure the best route between any two routers.
Server	a computer or device on a network dedicated to managing or providing services to a network, meaning that they perform no other tasks besides their server tasks.
Static IP Address	an IP address that does not change.
Switch	receives data from one network device and sends it to the one of several devices that needs the data. Switches are better than hubs because hubs don’t have the intelligence to determine which network device needs the data. Switches are not as good as routers, because routers can determine the best route to reach the network device that needs the data.
Subnet Mask Number	Used in combination with the IP Address to specify the maximum number of nodes in a network.
TCP Timeout	is the amount of time you configure the Integrity Series RT/RT+ Terminal to wait for a network communication before closing its network socket which is a form of resetting the terminal’s network communication.



Appendix F – Glossary (continued)

Telnet	is a well known communication protocol used with a great many network devices. In the Integrity Series RT/RT+ Terminal, telnet is useful for diagnosing network connection problems and verifying the operation of the terminal.
Terminal Buttons	See Appendix E – Key Functions of the Integrity Series RT/RT+ Terminal
TFTP	is an abbreviation for Trivial File Transfer Protocol which is a simple form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP) and provides no security features.
Time transactions	see punches.