

Programmable Bell Ringer

Model: CRL1000



USER MANUAL



DISCLAIMER

The information contained in this document is subject to change without notice. Masterclock, Inc. (hereinafter MC) makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. MC shall not be liable for errors contained here in or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

See important *limited warranty* information at the end of this document.

ADVISORY NOTICE

It is the responsibility of the user to determine the adequacy and suitability of this device for the intended use.

Table Of Contents

Introduction	2
Introducing the CRL1000	2
Programmable Events	2
Standard Features Overview	3
<i>WinDiscovery Software</i>	3
<i>Event Time Basic Software</i>	3
Telnet Interface	3
USB Interface	3
Password protection	3
Default Password	3
UTC/Greenwich Mean Time Reference	4
Local Time and Custom Time Offset	4
Time Zone Offsets	4
Daylight Savings Time	4
DHCP/BOOTP Auto-Configuration	4
Device Name/DHCP Name Registration	5
STATIC IP Configuration	5
NTP (Network Time Protocol)	5
NTP Client	6
NTP Addressing Modes	6
LED Time Display	8
Synchronization Status	8
IP Address Announcement	9
Battery Backed RTC and TCXO	9
Non-Volatile Configuration	9
Set to Factory-Default Configuration	10
Serial Port Interfaces	10
Installation	11
Operating Environment	11
Pre-Installation Checklist	11
Quick Start Guide (Network Installation)	12
Configuration Methods	18
WinDiscovery	18
Using WinDiscovery	19
Properties	21
Network Configuration	21
Device Settings	23
Set Password	29
Global Password	30
Set Time/Date (Manual Override Feature)	31
Status	32
LED Display Options	33
Troubleshooting Tips	34
Program and Download a Schedule using Event Time Basic Application	38
Connecting Bells	40
Specifications	42
Communications – Protocols	42
Communications – I/O	42
Timing Characteristics (Standard)	42
Input Power Requirements	43
Output Power Ratings	43
RTC Battery	43
Physical	43
Operating/Storage Temperature & Humidity	43

Compliance 44

Appendix I: WinDiscovery Global Password Feature 45

 Enabling Global Password 45

 Changing the Global Password 46

 Disabling the Global Password 47

Appendix II: Telnet Terminal Configuration 48

 Troubleshooting Tips - Telnet 49

LIMITED WARRANTY 50

 Exclusions 50

 Warranty Limitations 50

 Exclusive Remedies 50

Introduction

Introducing the CRL1000

The model CRL1000 Programmable Bell Ringer operates on an Ethernet network utilizing a built-in Network Time Protocol (NTP) client to accurately set and display system time from up to two NTP servers. Each CRL1000 can operate on a 10/100 MBit local area network (LAN). The device may be configured using the network interface, or via USB. Once configured, the CRL1000 may also be operated off- network.

Included with the CRL1000 is the *WinDiscovery* application that operates under the Windows 2000/XP/2003 Server/Vista and Windows 7 operating systems. *WinDiscovery* is a detection, configuration, & network management software GUI application that works with all Masterclock brand network devices. The CRL1000 may be configured on the network via WinDiscovery or via a Telnet command line menu interface. The CRL1000 may be configured using the USB interface via a command line menu interface.

A scheduling application *MCR Event Time Basic*, is also included with your CRL1000. This application operates under the Windows 2000/XP/2003 Server/Vista and Windows 7 operating systems and allows the user/administrator of the system to program up to 128 Events per day, over a 1 year calendar, for each of the four (4) individual bell ringing circuits.

Other standard features include:

- Additional Telnet interface for alternate configuration and maintenance on non –Windows OS networks
- Internal maintenance free rechargeable battery and battery backed real time clock (RTC) retains time during loss of power or loss of active reference (s)
- Temperature compensated oscillator (TCXO) with holdover stability <165mS/day
- Supports NTP broadcast, multicast, and/or unicast (query) modes of operation
- Fully configurable network settings, including automatic configuration via DHCP/BOOTP , or Static IP addressing support
- Security features include password protection of configuration, encrypted communication, and the ability to disable telnet management access
- UTC time internal reference
- Fully configurable local time offset support with Time Zone and DST time offset, and custom time offsets
- Status display to remotely monitor status and behavior via *WinDiscovery*
- Firmware & function upgradeability

Programmable Events

The CRL1000 includes 4 independent 24VAC programmable circuits, which can be configured via the provided Event Time Basic Windows software.

- Each normally open [NO] circuit can be programmed to actuate bells or other 24VAC signal devices, at a specified time (defined as HH:MM:SS start time) for a specified duration (in seconds) with up to 128 events per day. This event schedule feature is included with the CRL1000.
- For information on using the Event Time Basic Software, install the application [run setup.exe] from the included CD, and view the included help files.

Standard Features Overview

Your CRL1000 has many standard and optional features, which make it a flexible network device. This section describes the standard features of the CRL1000.

The configurable features discussed in this section can be adjusted using - the WinDiscovery software application provided with your CRL1000, or a terminal-style interface accessible via Telnet. Consult the section of this user manual entitled [Configuration Methods](#) for details on how to adjust settings through the aforementioned mediums. Please refer to the [Optional Features](#) section for information regarding the connection and configuration of installed options.

WinDiscovery Software

The CRL1000 is designed to be user friendly yet highly versatile. Included with the CRL1000 is the *WinDiscovery* graphical user interface (GUI) application that operates under the Windows 2000/XP/2003 Server/Vista operating systems. *WinDiscovery* is a user friendly and feature rich network device detection, configuration, & management software application for all Masterclock brand network devices allowing the user to configure and view status of the network devices remotely.

Event Time Basic Software

A scheduling application, *MCR Event Time Basic*, is also included with your CRL1000. This application operates under the Windows 2000/XP/2003 Server/Vista and Windows 7 operating systems and allows the user/administrator of the system to program up to 128 Events per day, over a 1 year calendar, for each of the four (4) individual bell ringing circuits. Schedules are created, and then downloaded from the application to the CRL1000. Multiple schedules may be built, edited, saved (stored) on the computer running the MCR Event Time Basic application. The user may also open and download a previously defined schedule.

Telnet Interface

The CRL1000 includes an additional Telnet terminal style command line interface for configuration on networks that are not Microsoft Windows based. This feature allows the CRL1000 to be configured by and used networks based on Linux/Unix and other operating systems.. To access and configure the CRL1000 Telnet interface please see the Configuration Methods section and/or Appendix II for additional details. The Telnet interface may be disabled.

USB Interface

The CRL1000 includes an additional command line interface for configuration when the unit is not utilized on a network. This feature allows the CRL1000 to be configured by the USB interface on Windows OS's.. To access and configure the CRL1000 via the USB interface, please see the Configuration Methods section and/or Appendix II for additional details.

Password protection

The CRL1000 is provided with a password as a security access feature. Each Masterclock network device has a password access that must be entered before the device will accept configuration changes. Each device or set of devices can have a unique password or they can all share the same password. The password can be changed and retained by the user or by the network system administrator to permit access only to authorized users.

A password can be a maximum of 11 characters and may contain any sequence of letters, numbers, and common punctuation. Passwords are case-sensitive.

Default Password

The CRL1000 contains a factory default password.

The factory default password is “public”.

UTC/Greenwich Mean Time Reference

The CRL1000 reference time is UTC based.

UTC is a time standard which is the basis for the worldwide system of civil time. This time scale is kept by time laboratories around the world, including the U.S. Naval Observatory, and is determined using highly precise atomic clocks. The UTC scale is coordinated in Paris by the International Bureau of Weights and Measures (BIPM).

UTC runs at the rate of the atomic clocks, but when the difference between this atomic time and one based on the Earth approaches one second, a one second adjustment (a "leap second") is made in UTC.

UTC is the local time at the prime reference meridian at Greenwich, England. At a given location on the planet, local time can be displaced (referenced to UTC) by -11 to +12 hours. North and South America are from -3 to -11 hours delayed; most of Europe and Africa and all of Asia and Australia are advanced by +1 to +12 hours. Because the NTP time distribution standard operates with UTC-reference time only, time zone and/or daylight savings (summer) time are not used.

UTC is sometimes colloquially referred to as "Greenwich Mean Time" (abbreviated GMT).

Local Time and Custom Time Offset

The CRL1000 can provide local time offsets and stores this information internally, in addition to the UTC time. The CRL1000 provides flexible configuration options for supporting worldwide time zones and daylight time standards or custom time offsets. A local time reference can be provided by applying either a time zone offset (or bias), daylight saving offset, or a custom time offset.

Time Zone Offsets

A time zone offset (or bias) can be provided to adjust the time for display or time output purposes. A bias can be set as a positive (+) or negative (-) value with a resolution of one second.

Factory default: no offset.

Daylight Savings Time

The CRL1000 provides automatic daylight savings adjustments when configured.

A daylight savings time (summer time) adjustment can be configured separately and in addition to a time zone offset.

Daylight time standards vary widely throughout the world. Traditional daylight/summer time is configured as one (1) hour positive bias. The new US/Canada DST standard, adopted in the spring of 2007 is: one (1) hour positive bias, starting at 2:00am on the second Sunday in March, and ending at 2:00am on the first Sunday in November. In the European Union, daylight change times are defined relative to the UTC time of day instead of local time of day (as in U.S.). European customers, please carefully consult the section entitled Device Settings for details on setting daylight time.

To ensure proper hands-free year-around operation, the automatic daylight time adjustments must be configured using the daylight time option and not with the time zone offset option.

[Note: Factory default: daylight savings time is disabled. You must enable and configure the settings.]

DHCP/BOOTP Auto-Configuration

The CRL1000 can obtain its network configuration automatically from DHCP or BOOTP, when a DHCP server or BOOTP server is available on the network. Utilizing DHCP/BOOTP, the CRL1000 will automatically be assigned its network configuration including an IP address, and additional functions such as DNS server and Router/Gateway settings. This feature is enabled by default.

In addition, the CRL1000 can automatically obtain Time Offset (Time Zone) configuration and the NTP server addresses (primary and secondary). To utilize these features, the DHCP server of the network must be pre-configured with the appropriate configuration items.

DHCP (Dynamic Host Configuration Protocol) is a mechanism for automating the configuration of networked devices that use TCP/IP. When DHCP is enabled, DHCP configuration acquisition will overwrite any manual configuration items. A precursor to DHCP is BOOTP. The CRL1000 can obtain configuration from a BOOTP server when no DHCP server is present. **Factory default: DHCP enabled.**

The following RFC2132-defined optional configuration items are, when available, used by the CRL1000 for configuration purposes:

Option	No.	Comments
Time Offset	2	The value provided will be used for the time zone offset configuration, unless it is defined as zero in which case it will be ignored and the NTD will rely on internal configuration. Note: this option does <u>not</u> provide information appropriate for dynamic daylight savings time use.
Router	3	The first IP address provided will be used for router/gateway configuration.
Domain Name Server	6	Up to two server IP addresses may be specified. NTD clock will treat addresses as primary and secondary DNS servers.
Network Time Protocol Server	42	Up to two server IP addresses may be specified. NTD clock will treat addresses as primary and secondary NTP servers.

[Important Note: A CRL1000 network device will not function properly if configured to use DHCP services when no DHCP server is present on the network.]

[Important Note: A CRL1000 network device will default to a fallback IP address of 169.254.X.Y when no DHCP server is available on the network, where X and Y are random.]

Device Name/DHCP Name Registration

All Masterclock, Inc. network appliances can be provided with a device name. By default, device names are the product name abbreviation followed by the last octet of the device’s Ethernet address (MAC address). If a DHCP server is available on the network when the CRL1000 is installed, the unit will be auto-registered with the DHCP server. The network system administrator can then view this DHCP name registration and the currently assigned IP address, at the DHCP server.

The user or network system administrator may wish to designate device names relating to their own organizational requirements. It is recommended that a robust naming scheme be developed before devices are installed to different locations within an organization.

The device name may be changed from the factory default name by entering a unique name of up to 32 characters. *[Hint: You can change the device name to one convenient for your site – preferably one that helps you to later identify the exact physical location of the device. Up to 32 character device names are supported]*

[Important note: Long DHCP names are not supported - only the first 14 characters of the device name will be registered by the DHCP server.]

[Note: The IP address of the unit is required to configure the CRL1000 with Telnet. The DHCP server can be utilized to provide the IP address of the associated device name that is registered.]

STATIC IP Configuration

The CRL1000 allows for Static IP address, gateway, and DNS, network configuration entries to be made manually if no DHCP/BOOTP server is available. In addition, the NTP server addresses can be adjusted manually. Manual configuration requires disabling the DHCP defaults via WinDiscovery (or other configuration method).

NTP (Network Time Protocol)

NTP is an open-standard time synchronization protocol designed for precision synchronization and maintenance of time/date on computers and other devices attached to TCP/IP networks. NTP itself is transported with the UDP/IP (User Datagram Protocol), and is usually served on port 123. NTP time/date is UTC-referenced, as the protocol has no provisions for representing time zones or daylight savings (summer) time.

A wealth of useful NTP information and resources can be found at <http://www.ntp.org>

NTP Client

The CRL1000 acquires its internal UTC time reference from an NTP timeserver by using a built in NTP client. The NTP client is fully configurable and can operate in several NTP modes to reference both a primary and a secondary NTP server. The client can be disabled in order to allow operation of the unit as a stand-alone unit without network connection.

NTP Addressing Modes

Unicast

The CRL1000 supports the unicast method of NTP packets transfer. Unicast method involves direct transfer of requested information from the NTP server to the NTP client based on a query or NTP time request. The unicast method is supported simultaneously when either the broadcast or multicast modes are selected.

Broadcast

The CRL1000 supports the broadcasting of NTP packets. This feature is useful in situation where network administration may wish to avoid the network traffic created by a large number of clients making periodic NTP requests, or in situations where such periodic requests end up synchronized in such a manner as to exceed the CRL1000's ability to reply. The broadcast mode is a widespread or open-ended broadcast, not intended for any specific IP address.

The CRL1000 provides NTP [UDP] broadcasts using the broadcast address [255.255.255.255].

Note that some firewalls and routers will not forward UDP broadcasts by default. Security configurations may need to be adjusted to allow the UDP broadcast packets to pass on the configured port.

Multicast

The CRL1000 also supports multicast addressing of NTP packets as a recently added feature. As opposed to broadcast mode, which is a widespread or open-ended broadcast of NTP packets whereby, data is sent to every possible receiver (client),. Multicasting is useful because it conserves bandwidth. It does this by replicating packets only as needed within the network to send them only to receivers (clients) that want them, thereby not transmitting unnecessary packets.

The concept of a group is crucial to multicasting. Every multicast requires a multicast group; the sender (or source) transmits to the group address, and only members of the group can receive the multicast data. A group is defined by a [Class D](#) address.

The CRL1000 does not restrict the use of the multicast address assignment and supports the full range of class D multicast addresses or groups from 224.0.0.0 to 239.255.255.255 . These groups or class D address ranges for multicasting are defined and governed by [RFC3171](#), *IANA IPv4 Multicast Guidelines*.

Typically, the multicast address range 224.0.1.0 - 224.0.1.255 (224.0.1/24) [Internetwork Control Block] is utilized for NTP traffic, however, please refer to the [RFC3171](#) for your specific application and implementation.

The Internet Group Management Protocol (IGMP) is a protocol that controls group membership for individual hosts. This protocol only operates in a LAN setting, but is required if you wish to be able to join a multicast group on a host. IGMP is defined in [RFC 2236](#).

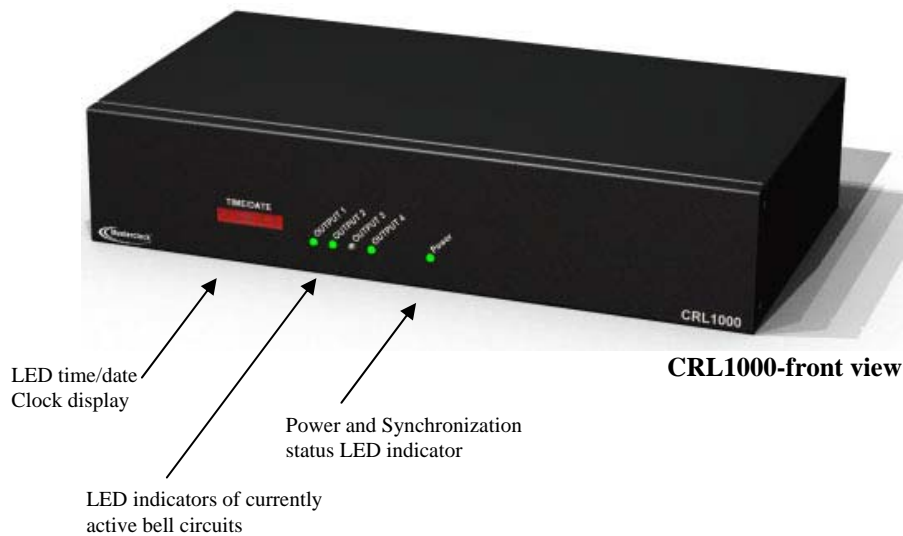
Note: Use of the multicast addressing method requires the use of routers & switches and other network devices that support the Internet Group Management Protocol (IGMP). In addition, the IGMP mode must be enabled and configured for multicasting addressing to be implemented properly. The implementation of multicasting addressing is beyond the scope of support available from Masterclock. Please ensure that your network system components are capable of , and configured properly for IGMP before utilizing the multicast addressing feature.

Note: You will need to check with your firewall vendor to determine how to enable multicast traffic through a firewall. In addition, you may want to read [RFC 2588: IP Multicast and Firewalls](#).

Anycast

The CRL1000 does not currently provide anycast capability.

LED Time Display



The time of the unit is displayed on the 6 digit front panel LED time display. By default, the unit will display the local time (UTC time adjusted by any configured Time Zone and DST offsets) of the device, as currently stored in the internal RTC (real time clock chip). The CRL1000 contains (stores) both an internal UTC time and Local time reference. When no Time Zone and Daylight Saving Time settings have been applied, the internal time reference are the same (i.e. the Local time reference is the same as the UTC reference). The user may configure to always display UTC time, even when device has local time offsets applied. The display can also be configured to display date in various formats, or to alternate between time/date.

Under normal operation the device is on a network and the NTP client is [periodically] locked to an NTP server. When locked to an NTP server, the built in NTP client adjusts the internal RTC to be synchronized to UTC time. Thus, the CRL1000 can track UTC time provided by an NTP server, and operate as an accurate and synchronized bell ringer. When the NTP client cannot access an NTP server, or when operated off-network, the CRL1000 will utilize an internal temperature compensated crystal oscillator and the real time clock. This internal TCXO reference has a maximum drift of +/- 1 minute per year (or 165 milliseconds per day). Thus, even when operated off network, the CRL1000 will have very good accuracy (low drift) relative to UTC time.

The 6 digit LED display provides additional information regarding current IP address, and synchronization status.

Synchronization Status

By default, after 24 hours of operation without an NTP client (no lock to external reference) the LED time/date display will show dashes. This feature is intended to be an indication that the time may not be reliable and locked to NTP. This feature is configurable or may be disabled with WinDiscovery or Telnet.

The CRL1000 will also indicate a locked condition by flashing the green LED labeled “Power” once per second. When the CRL1000 is operating without access to an NTP server, the unit will be in a free-wheeling condition and will be operating only using the internal RTC and TCXO circuit. Under this free-wheeling condition, the CRL1000 will flash the green LED labeled “power” twice per second.

IP Address Announcement

The CRL1000 clock can display its currently assigned network IP address using its LED display. This feature allows the user to identify the IP address of the clock before attempting communication with the unit.

To initiate the IP address announcement, press the RESET button once [do not hold the RESET button in]. The unit will scroll the display to show the following information:

IP:
Followed by the first octet of the IP address and a dot.
Followed by the second octet of the IP address and a dot
Followed by the third octet of the IP address and a dot
Followed by the fourth octet of the IP address

After displaying the IP address, the clock display will revert back to time/date display mode.

Battery Backed RTC and TCXO

The CRL1000 maintains its internal time settings in battery- backed memory located on the RTC chip. A Temperature Compensated Crystal Oscillator provides a freewheeling accuracy (maximum drift) of +/- 1 minute per year (165 mS/day). The battery supplies power to the TCXO 32kHz oscillator and RTC when the unit is powered off. This allows the internal time to be maintained and the time and date to increment, when power is off. Under normal operating condition, the memory devices maintaining the RTC data is powered by the external DC power supply and does not rely on the battery for data retention.

The battery is a maintenance free rechargeable Manganese Lithium type. A built in battery charging circuit is used when the unit is powered on, eliminating the need for maintenance.

Non-Volatile Configuration

The CRL1000 maintains its configuration parameters internally in non-volatile memory. These configuration settings include the assigned [DHCP or Static] IP address and network settings, assigned device name, NTP operational modes, , brightness level, assigned stratum levels, telnet access, RTC usage validity during primary reference outages, and password. The internal configuration is maintained even when power is off. This information, except for the time/date stored in the RTC, may be reset to the factory default state.

Set to Factory-Default Configuration

The CRL1000 is fully tested and then shipped from the factory with factory default settings.

This factory default configuration is defined as:

- UTC reference time (no local time zone offset, daylight saving auto adjustment disabled)
- DHCP configuration mode enabled for Network Address and NTP Server addresses
- Query (Unicast) NTP client mode enabled (broadcast/multicast modes disabled)
- Time Dissemination via Real-Time Clock during reference outages enabled for 24 hours
- Password – set to “public”
- Device name – set to CRL1000-XX:XX (where XX:XX are the last two octets of the MAC address of the unit)
- Telnet - Enabled

The factory defaults may be restored by using the software interfaces methods (WinDiscovery or Telnet) or via using a button located on the rear of the unit.

In some situations (such as a lost password or removal of confidential information prior to sending the unit in for repair service) it may be necessary to return the CRL1000 to its factory default configuration.



CRL1000- rear view

RESET to Factory Default Configuration Button

[Note: To reset configuration to factory default

Depress and hold the “Set to factory default” button for approximately 5 seconds [or until the front panel display goes to all dashes “- - - - -”]

Serial Port Interfaces

The CRL1000 provides a USB serial interface for configuration. These serial interfaces features and protocols are not currently implemented and are reserved for future expansion. The remainder of this section is intentionally left blank. The serial port interface utilizes a menu driven command line interface, which is identical to the Telnet interface.

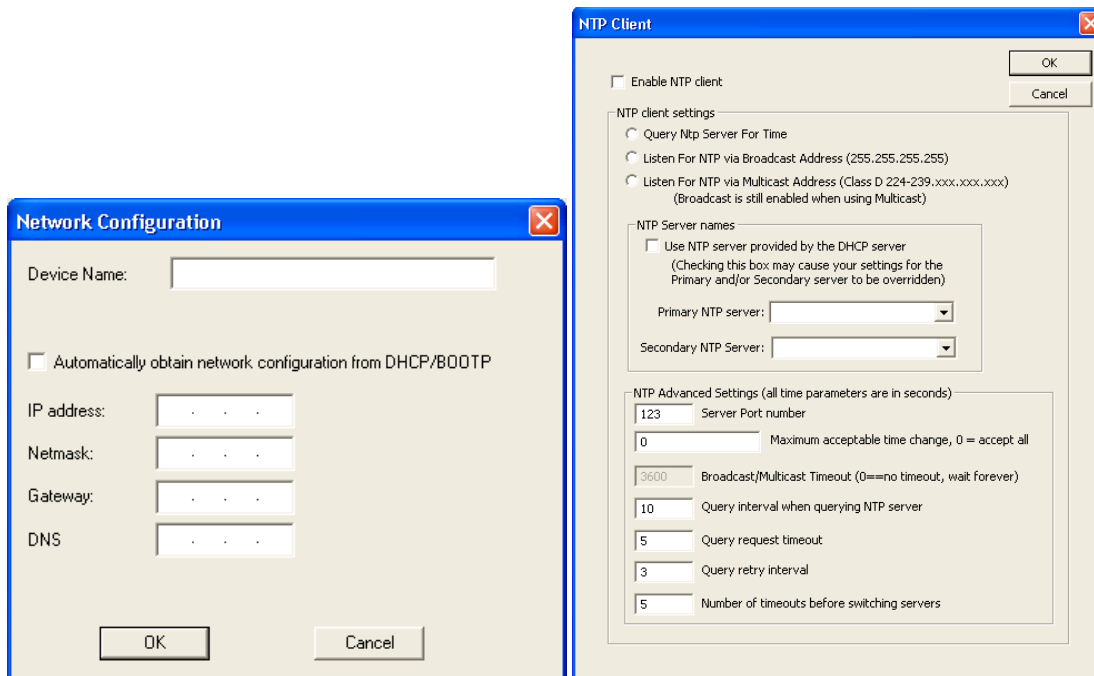
Installation

Operating Environment

The CRL1000 is not water or moisture proof and is designed for indoor use only. Treat it as you would any other delicate electronic device and do not expose it to water, excessive heat or physical abuse. Please see the “Specifications” section for details.

Pre-Installation Checklist

The CRL1000 is a network device with an NTP client enabled and configured for DHCP provided network settings and NTP server addresses by default. Before installing a CRL1000 on a network one should be prepared with the following basic configuration information that the device will require. It may be necessary to obtain some or all of this information from a network administrator in your organization.



Dynamic Networking Configuration (default for all CRL1000 devices)

- __ Confirm that a DHCP/BOOTP service is accessible on the local network
- __ Determine if DHCP server will provide NTP server configuration
- __ Determine if DHCP server will provide time zone configuration

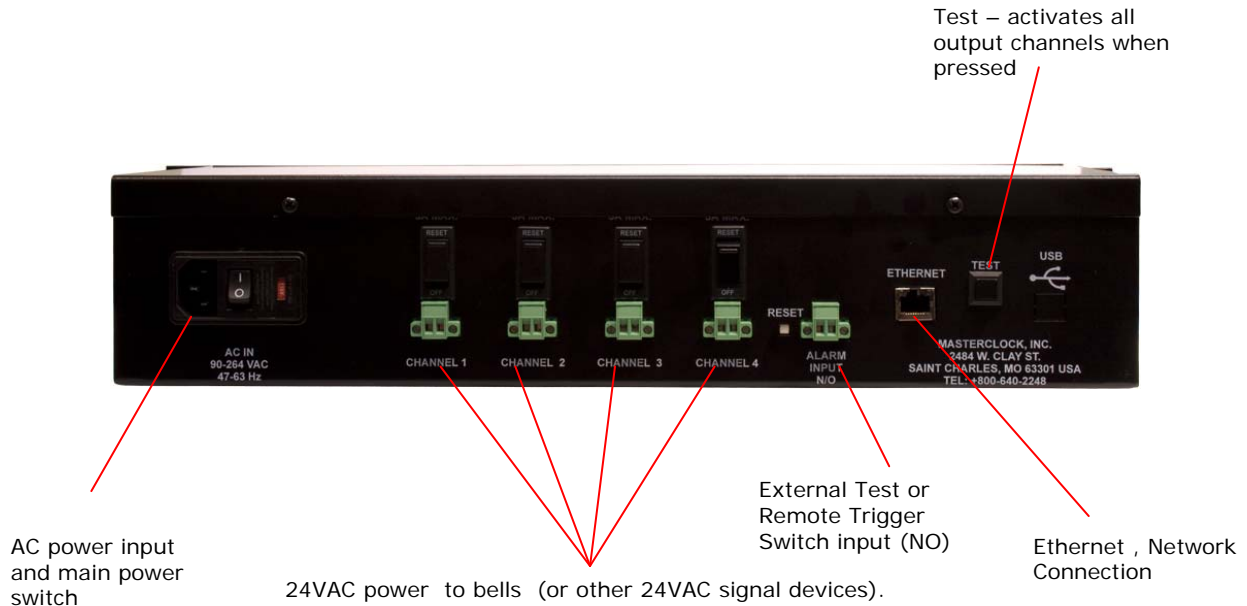
OR

Static Networking Configuration

- __ IP address and netmask designation for device
- __ Primary and secondary DNS (domain name) servers
- __ Gateway/router
- __ Primary and secondary NTP time sources

Quick Start Guide (Network Installation)

1. Make connections to rear of unit



Set of 4, Normally Open (NO) 24VAC powered output channels at 4 amps maximum. Caution: Make all connections to terminal blocks with AC main power and/or each circuit breaker set to OFF.

- Connect the CRL1000 device to your network hub/router/switch using Cat5/5e or Cat6/6e cable making the connection to the RJ45 connector labeled "Ethernet".
- Connect the provided AC power cord to the IEC input connector and to an appropriate AC power source.
- Optional: At this time, you may make wiring connections to the Bells (or other 24VAC signaling device loads) Terminal blocks are provided. See the appropriate section of the user manual for connecting bells.




Caution: Make all wiring connections to the terminal blocks with the AC main power and/or each circuit breakers set to the "OFF" position.

- Apply power by moving the main AC power switch to the “ON” position.
- 1. Monitor the front panel for power up status.
 - When power is first applied the initial sequence of the front panel LEDs is:
 - Unit will show all eights
 - After about 30 to 40 seconds
 - LED display will show all dashes -----
 - Followed by time display showing all 88:88:88
 - all LEDs extinguish briefly
 - Internal RTC (real time clock) time will be displayed
 - Time display incrementing the seconds’ digit once per second (indicating locked to internal TCXO oscillator , and acquiring lock to an external source, if applicable).
 - Once locked to an NTP time server, the “POWER” LED will flash once per second.

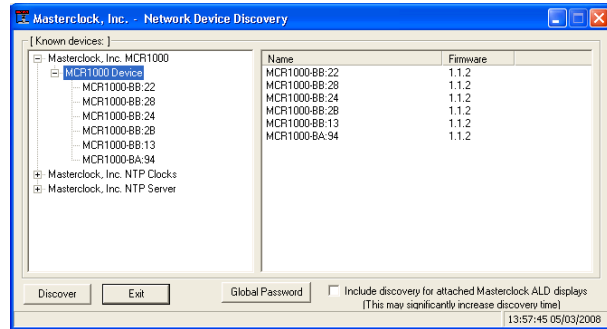
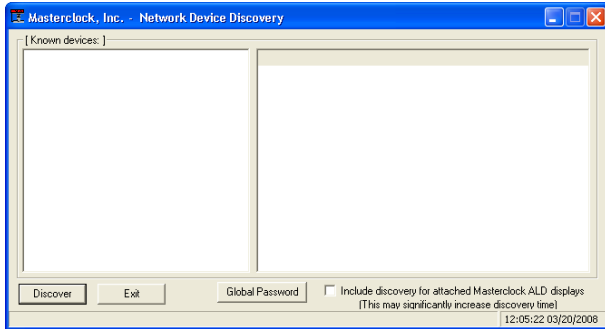
[Note: when configured to obtain network configuration through DHCP, the display may hesitate on startup while DHCP is resolved.]

- 2. Configure the device using your preferred method.

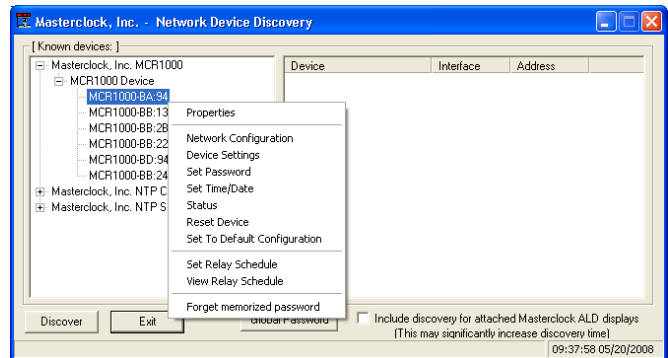
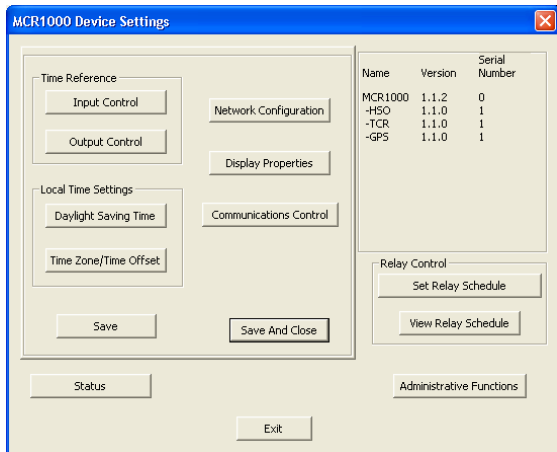
At this time, the CRL1000 can be communicated with over the local network using the *WinDiscovery* application. *WinDiscovery* can detect and identify the CRL1000 through the exchange of broadcast messages even when TCP/IP networking parameters are not configured on the same network.
 - Once the CRL1000 has a valid network configuration and the IP address of the unit is known, it can also be accessed via Telnet by computers in the same logical network.
 - Configure the device for network operation using WinDiscovery or Telnet.
 - 2. Install WinDiscovery from CD
 - Insert the WinDiscovery CD supplied with your Masterclock network device into the computer running Windows 2000,XP,2003 Server, or Vista operating system, to which you plan to install and configure from.
 - The Installshield application will begin automatically if AutoRun is enabled on your system.
- Otherwise, browse to the CD root directy and click the setup.exe file to begin the installer. 

3. **Run WinDiscovery to discover your device on the network**

- Run the WinDiscovery application from the Start button – or from
 "C:\Program Files\Masterclock\WinDiscovery Standard Edition \windiscovery.exe

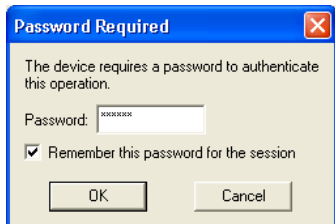


- Click Discover -----> A list of detected network devices will be displayed
- Select the device you wish to configure



- Single click for full device menu OR Right click for shortcut menu

Note: A password is required to make configuration changes.



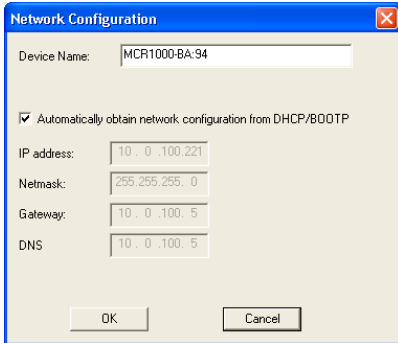
When prompted for a password, enter "public", and select "Remember this password for the session" option, or use Global Password button feature on main screen.

The default password is: public

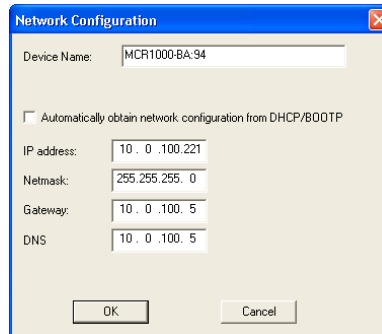
The password may be changed by selecting the Administrative functions button and the Set Password option in the full menu or by simply using the Set Password option of the device shortcut menu

4. Configure network settings

- Select *Network Configuration* button or *Network Settings* option



The 'Network Configuration' dialog box shows the 'Device Name' as 'MCR1000-BA-94'. The checkbox 'Automatically obtain network configuration from DHCP/BOOTP' is checked. The IP address is '10.0.100.221', Netmask is '255.255.255.0', Gateway is '10.0.100.5', and DNS is '10.0.100.5'. There are 'OK' and 'Cancel' buttons at the bottom.

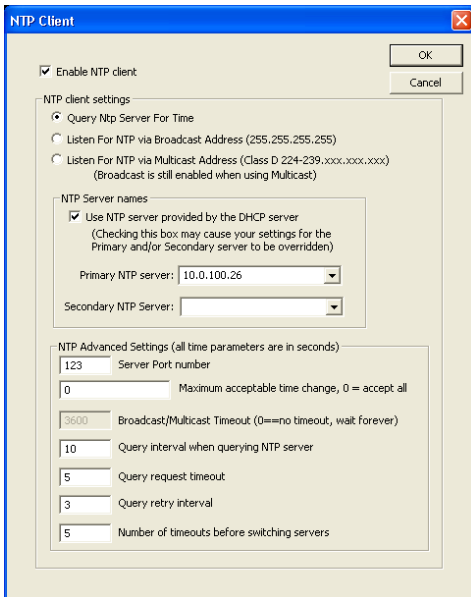


The 'Network Configuration' dialog box shows the 'Device Name' as 'MCR1000-BA-94'. The checkbox 'Automatically obtain network configuration from DHCP/BOOTP' is unchecked. The IP address is '10.0.100.221', Netmask is '255.255.255.0', Gateway is '10.0.100.5', and DNS is '10.0.100.5'. There are 'OK' and 'Cancel' buttons at the bottom.

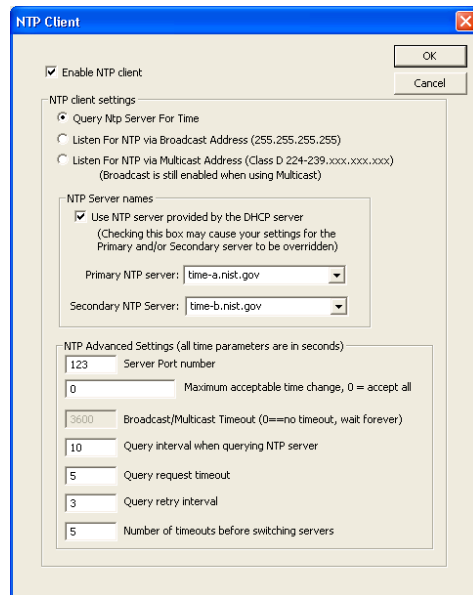
- Use DHCP settings OR Enter Static IP address, Netmask, Gateway, DNS

5. Configure NTP client settings

- Select *Input Control* button and then *NTP Client Settings* button or *Device Settings* option
- Select desired NTP client mode (Unicast/Query [default], Broadcast, or Multicast)
- Set NTP server address(es)



The 'NTP Client' dialog box has 'Enable NTP client' checked. Under 'NTP client settings', 'Query Ntp Server For Time' is selected. Under 'NTP Server names', 'Use NTP server provided by the DHCP server' is checked. The Primary NTP server is '10.0.100.26' and the Secondary NTP Server is empty. Under 'NTP Advanced Settings', the Server Port number is '123', Maximum acceptable time change is '0', Broadcast/Multicast Timeout is '3600', Query interval is '10', Query request timeout is '5', Query retry interval is '3', and Number of timeouts is '5'. There are 'OK' and 'Cancel' buttons at the top right.



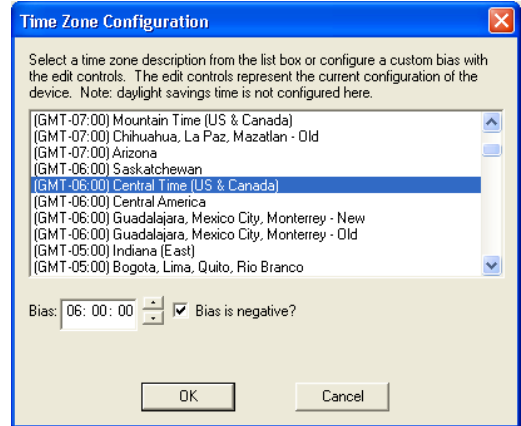
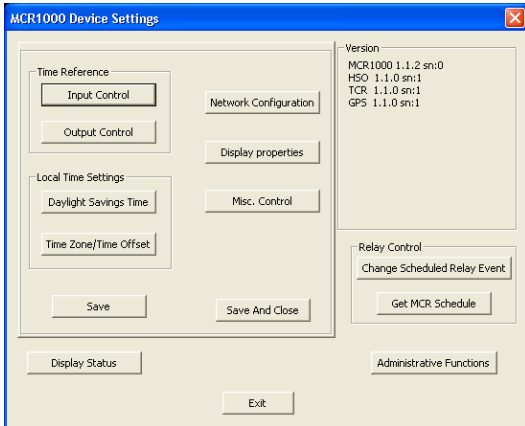
The 'NTP Client' dialog box has 'Enable NTP client' checked. Under 'NTP client settings', 'Query Ntp Server For Time' is selected. Under 'NTP Server names', 'Use NTP server provided by the DHCP server' is unchecked. The Primary NTP server is 'time-a.nist.gov' and the Secondary NTP Server is 'time-b.nist.gov'. Under 'NTP Advanced Settings', the Server Port number is '123', Maximum acceptable time change is '0', Broadcast/Multicast Timeout is '3600', Query interval is '10', Query request timeout is '5', Query retry interval is '3', and Number of timeouts is '5'. There are 'OK' and 'Cancel' buttons at the top right.

- Use NTP server provided by DHCP server OR Disable DHCP & Enter NTP server addresses

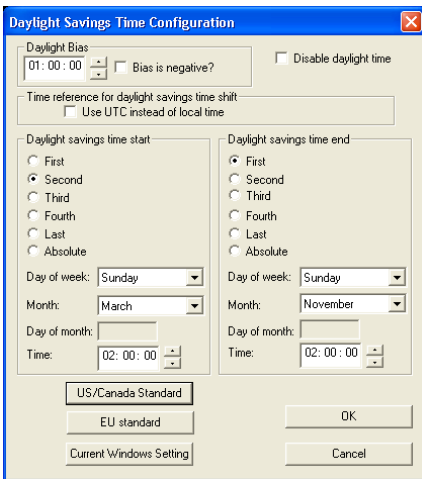
Note: IP addresses or URL addresses (including Internet NTP server addresses) may be used in the NTP server fields; if a DNS server is provided in the network settings, the URL will be resolved automatically to an IP address.

6. Optional: Configure local time

- Set local time using time zone and daylight savings offsets from UTC time, if desired
- Note: UTC time is still primary system time. Either UTC or local time may be displayed



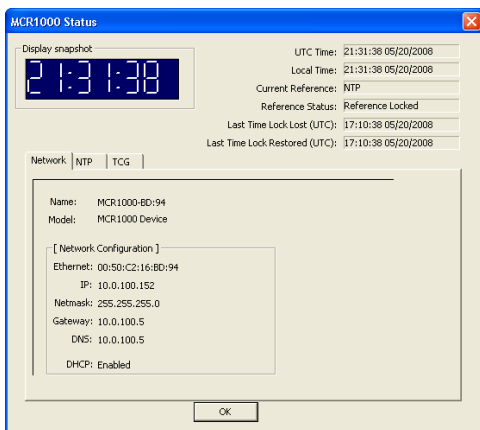
- Select *TimeZone/Time Offset* button -----> Select the time zone of interest
- Select *Daylight Saving* button----->



- Deselect disable daylight saving time,
 - Select desired standard from preset button options
- OR Enter DST rules manually

7. Apply all device configuration changes

- Use the *Save and Close* button to apply all device setting configuration changes

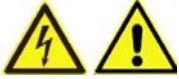


8. View Status

- Select *Display Status* button from device menu or Status option from the right click menu.
- Select the *Network* tab, or select the tab of the desired installed option
- Confirm the units UTC and local time using remote status display and status condition as being synchronized to the source.
- ❖ See the CRL1000 user manual for additional details

9. Wire and Test the Bell Circuits

- If you have not already done so, make wiring connections to the bell signaling circuits using 24VAC bell or other 24VAC signaling device loads. Terminal blocks are provided. Four 24VAC power output channels or circuits are available. The maximum load current is 4 Amps per circuit. Refer to the appropriate section of the user manual for connecting bells.



Caution: Make all wiring connections to the terminal blocks with the AC main power and/or each circuit breakers set to the "OFF" position.

- After you have verified the bell wiring, set the individual output channel circuit breakers to the "RESET" position. This will supply 24VAC power to the output channels when either activated by the schedule or when the "TEST" button is pressed.
- Press the "TEST" button located on the rear of the unit. The bells (or other signaling devices) should sound on all output channels, until the button is released. The front panel status LEDs will light when each corresponding output circuit is active.

10. Install MCR Event Time Basic from CD

- Insert the *MCR Event Time Basic* CD supplied with your Masterclock network device into the computer running Windows 7, Vista, XP, or 2000 operating system, to which you plan to install and configure schedules.
- The Installshield application will begin automatically if AutoRun is enabled on your system.

Otherwise, browse to the CD root directly and click the setup.exe file to begin the installer.



11. Create and Download a Schedule

- Run the *MCR Event Time Basic* scheduling application to create and download a schedule to ring the attached bells on one or more of the output channels available on the CRL1000. Refer to the supplied Help file included with the scheduling application for details.
- Monitor your device to ensure the schedule is functioning. The front panel status LEDs will light when each corresponding output circuit is active. You may wish to create and load a small test schedule to the CRL1000, in order to verify operation.

END Quickstart Guide

Configuration Methods

Basic network configuration of the CRL1000 is configured via the *WinDiscovery* software supplied with the unit, or via Telnet. Only one configuration method should be used at a time.

WinDiscovery

The *WinDiscovery* (WD) program is a Windows OS based program supplied with the CRL1000. WinDiscovery is supported under Windows 2000/XP/2003 Server/Vista operating systems. To install the WinDiscovery program on your server, workstation, or PC, complete the following steps:

1. Insert the WinDiscovery CD that shipped with your CRL1000 or download the latest version from the support area of www.masterclock.com
2. If AutoRun is enabled on your PC the Installshield Wizard installation will begin automatically. Otherwise, browse to the CD root directory and run the 'setup.exe' application.
3. Select the installation options by selecting either the standard or custom installation. By default the standard installation will install all user manuals and application notes along with the WinDiscovery application. The custom installation will allow the optional installation of the user manuals and application notes.
4. By default, the setup utility will suggest installing files to C:\Program Files\Masterclock\WinDiscovery. (Another path may be selected if desired.)

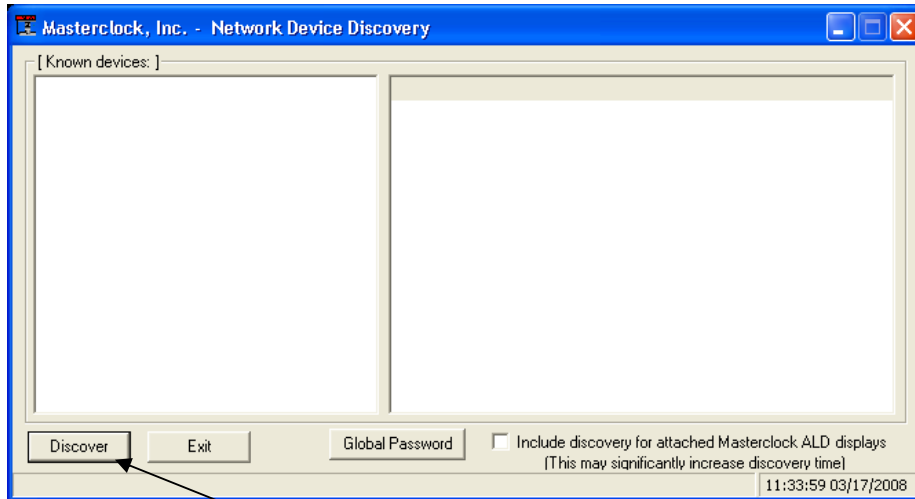
Potential Network Topology Communication Problems

Networks separated by physical routers will often block UDP broadcasts preventing WinDiscovery from locating devices on a remote network. Under such circumstances, WinDiscovery must be operated from a computer within the remote network or *the networks devices (routers) separating the networks must be configured to pass through (both directions) UDP traffic (including broadcasts) on port 6163.* Consult your network administrator for additional information.

Personal or network computer firewall applications, such as ZoneAlarm©, BlackIce, Symantec Client Firewall, or the Windows OS firewall may also prevent WinDiscovery from operating correctly. *Configure the firewall to allow bi-direction UDP traffic on port 6163 or temporarily disable the firewall while using the WinDiscovery application.*

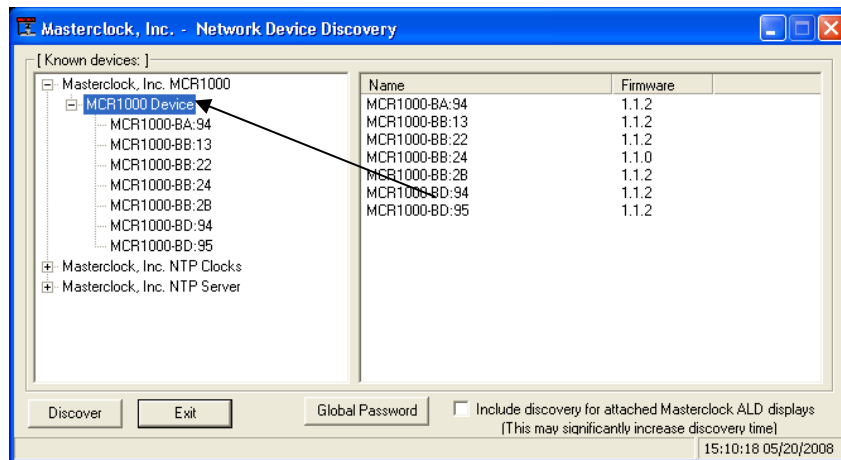
Using WinDiscovery

Open the WD program by clicking the shortcut on your desktop (or other fashion dictated by your installation). Only one user should be using WD at a time, and other methods should not be used to manage the CRL1000 while using WD.



Click the *Discover* button on the lower left of the screen.

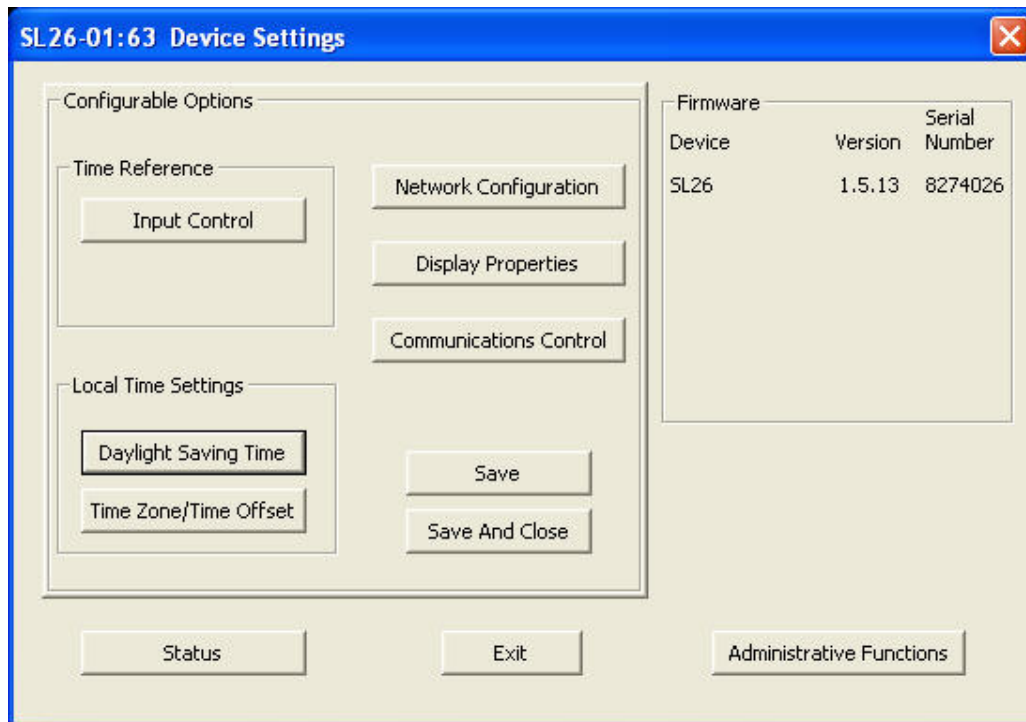
All Masterclock, Inc. network appliances accessible on the network will announce their presence. The real-time status bar will display the count of devices found. When complete, a list of device families and groups will be displayed in the left pane of the WD window. Click on the plus [+] sign to the left of any family or group to open and view device types that were found.



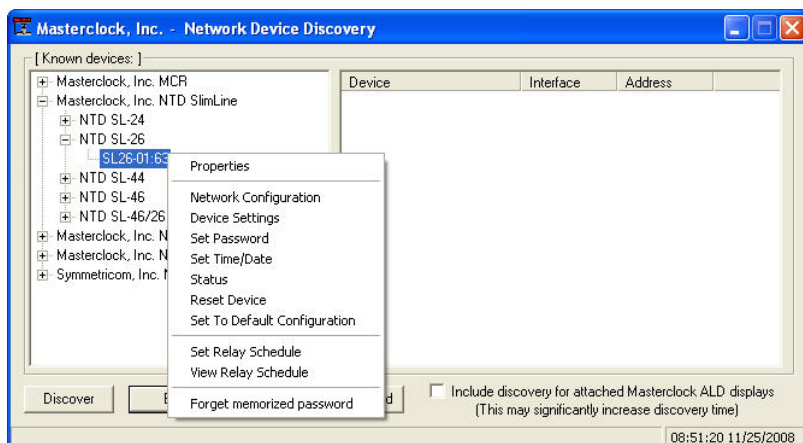
Clicking on the [+] of any device group will list in the right pane of the WD window all devices of that type found along with their current firmware version. To configure another device group, click on the device name in the left window and the device names will then appear in the right window, ready to be managed.

To configure and manage a device, select the device name and either double click to obtain the main device settings window or right mouse click to access a shortcut menu.

The Device Settings window allows for access to all CRL1000 device features (standard and optional).



The shortcut menu allows for easier access to certain features.



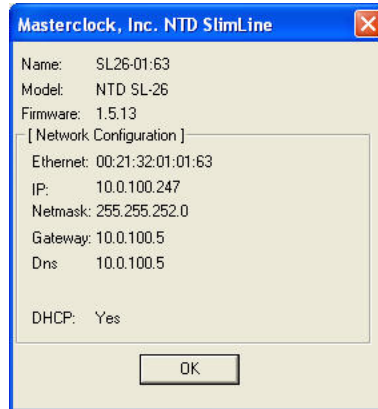
The current shortcut menu choices are:

- Properties
- Network Configuration
- Device Settings
- Set Password
- Set Time
- Status
- Reset Device
- Set to Default Configuration (Factory default settings)
- Set Relay Schedule
- View Relay Schedule
- Forget memorized password

Clicking a menu choice opens a new window for that function. When working in the management windows, use the *Apply* and *OK* button to accept changes that you have made. Use the *Cancel* button to exit the screen without applying changes. NOTE: *Cancel* does not undo changes that have been saved using the *Apply* button.

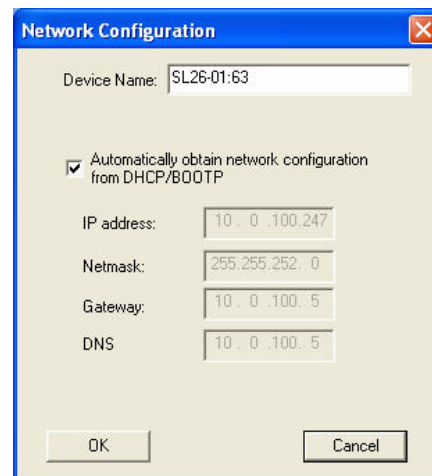
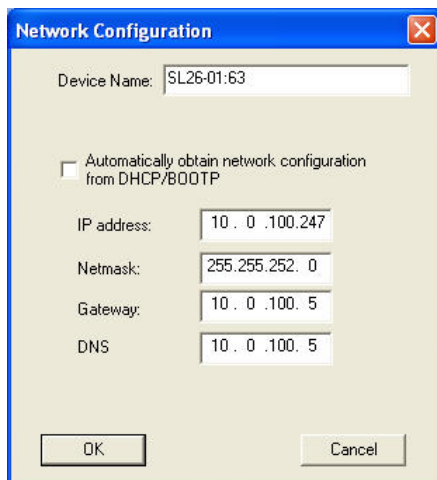
Properties

The properties of the CRL1000 device of interest can be viewed in summary form, using this shortcut menu selection. Under “Properties” the device name, model, and network configuration settings are available.



Network Configuration

The network settings must be established for the CRL1000 to be accessible to the network. You must be a network



administrator or have their support to complete these functions. Your network administrator determines the information for the Network Settings.

[Note: The default factory setting for network configuration is to use DHCP/BOOTP.]

[Note: If a DHCP server cannot be found on the network by the CRL1000, the IP address will be assigned a fallback IP address of 169.254.xxx.xxx]

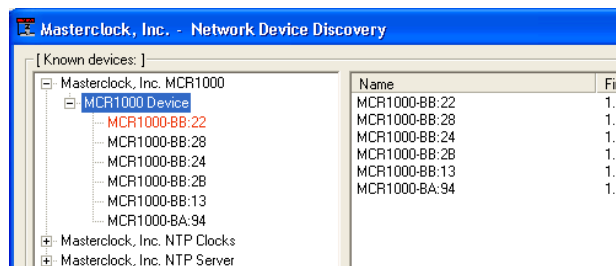
To utilize static IP addressing, de-select the checkbox for “Automatically obtain network configuration from DHCP/BOOTP”. You must then enter the IP address, Netmask, Gateway, and DNS suitable for your network.

[Note: The static IP address you enter must not be in use by another device on the network, this includes IP address ranges reserved for use by the DHCP server. If a static IP address is used which creates a duplicate IP address condition, the CRL1000 will have an address conflict with the device and each device may become unstable or erratic on the network]

169.254.xxx.xxx IP (fallback) address

DHCP is enabled by default. If DHCP is enabled and no DHCP server can be found the CRL1000 network address will default to (or fallback to) a 169.254.xxx.xxx address.

This 169.254.xxx.xxx is a link local address range (i.e. not allowed on the internet) and is used by Microsoft when their DHCP clients cannot find a DHCP server.



*[Note: Devices which have been assigned a fallback IP address of 169.254.xxx.xxx will be displayed in the main WinDiscovery window with **RED** text, indicating a problem with the configuration.]*

Device Name/DHCP Name Registration

Each CRL1000 network device is programmed at the factory with a factory device name. This name includes the model name CRL1000 and a “MAC address” extension containing the last two octets of the unique MAC address. For example: CRL1000-BA:94

The device name may be changed from the factory default name by entering a unique name of up to 32 characters. *[Hint: You can change the device name to one convenient for your site – preferably one that helps you to later identify the exact physical location of the device. Up to 32 character device names are supported]*

[Important note: Long DHCP names are not supported - only the first 14 characters of the device name will be registered by the DHCP server]

[Note: The IP address of the unit is required to configure the CRL1000 with Telnet. The DHCP server can be utilized to provide the IP address of the associated device name that is registered.]

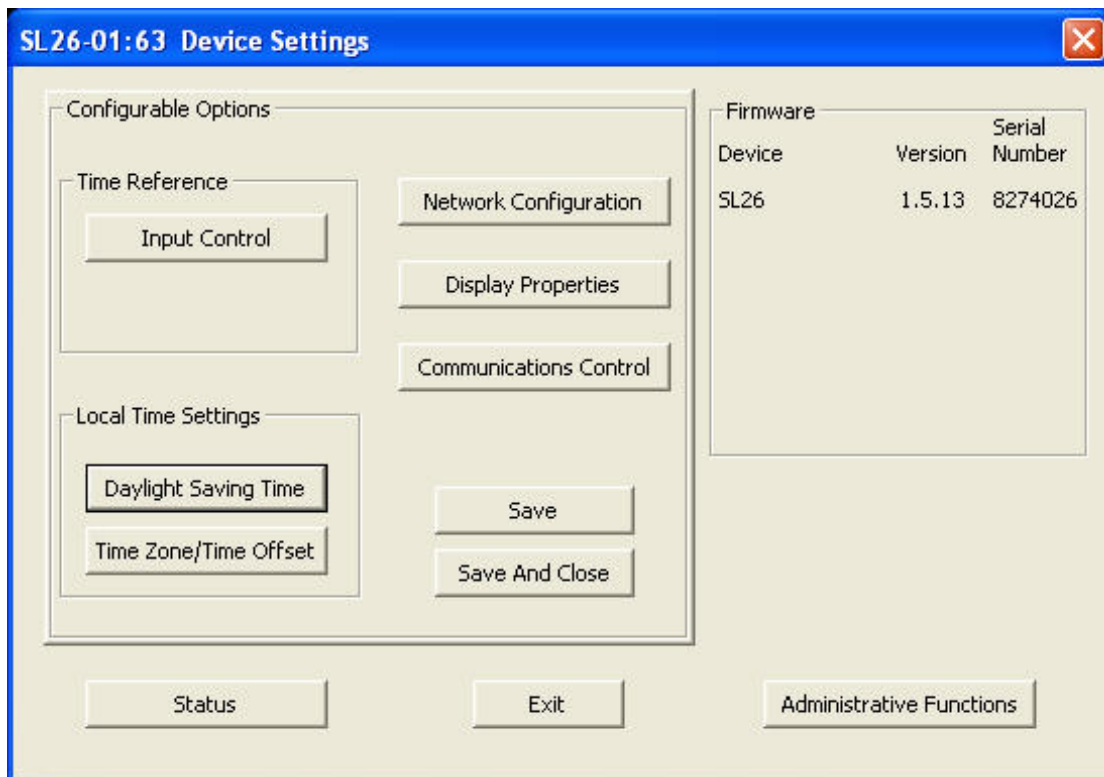
Device Settings

Each CRL1000 network device can be fully configured to display local time (or date) in the format that you prefer, using time zone offsets and DST settings to completely customize it relative to UTC time. In addition, the device settings window includes access to all configuration options for network, time references for input and output, display properties, relay control, administrative functions such as password, as well as a status display.

Any changes made in this window will not be applied until you click the “Save” button, or the “Save And Close” button.

Input Control - Network Time Protocol [NTP] Client Parameters – Allows for setting the NTP mode and parameters of the NTP client in the network device. These settings are located in the upper left hand section of the device settings window

The Primary Source information must be configured in order to acquire time from an NTP source. Enter either the IP address or Internet address (URL) for the NTP source. If available, enter a Secondary Source for backup.



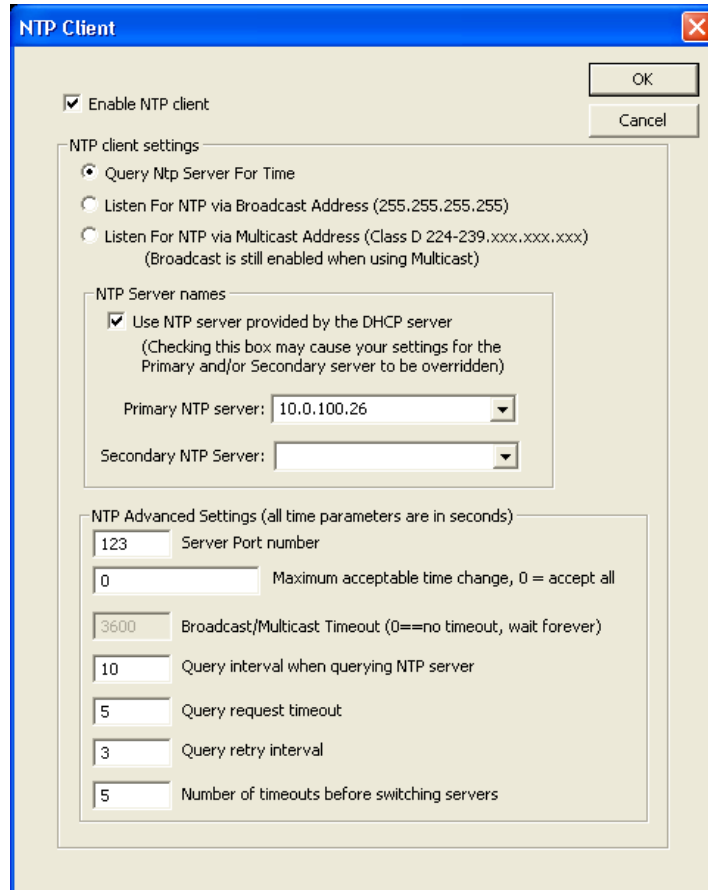
The primary and secondary server information can automatically be configured by the DHCP server when selecting the “Use NTP server(s) address provided by DHCP server” provided your DHCP server is configured to do so. Consult your IT /Network Administrator to utilize this option [DHCP Server Option 042].

The default, well-known port for NTP service is 123. This can be changed if desired.

[Note: some NTP/SNTP servers will expect NTP clients to operate on port 123 and cannot be configured to utilize alternate ports.]

Query NTP server for time (Unicast Mode for NTP) - By default, the NTD clock will operate only in Unicast /Query mode using server port 123.

This mode is selected exclusively when neither the listen for NTP broadcast nor the listen for NTP multicast modes are selected.

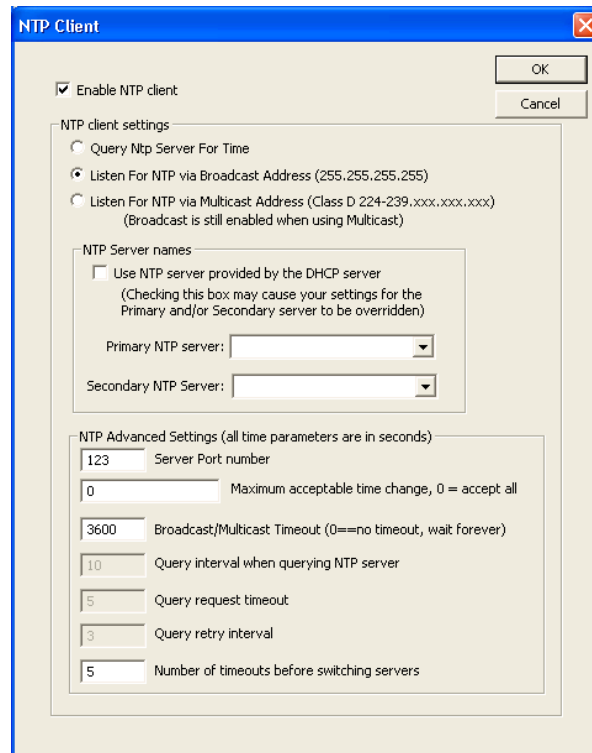


NTP Advanced Settings

Advanced settings allow for the adjustment of additional network communication settings. Under most typical operating circumstances it is not necessary, nor is it suggested to change the advanced settings options.

[Hint: If the advanced settings have been altered for your device and you begin experiencing difficulty in getting your clock to synchronize to the NTP time server, or the clock begins acting erratically, such as performing soft restarts; try returning the advanced settings to the default values shown above.]

Listen for NTP broadcasts — The network clock can be configured to listen to NTP broadcasts by selecting the “Listen for NTP via broadcast address [255,255,255,255]” checkbox.



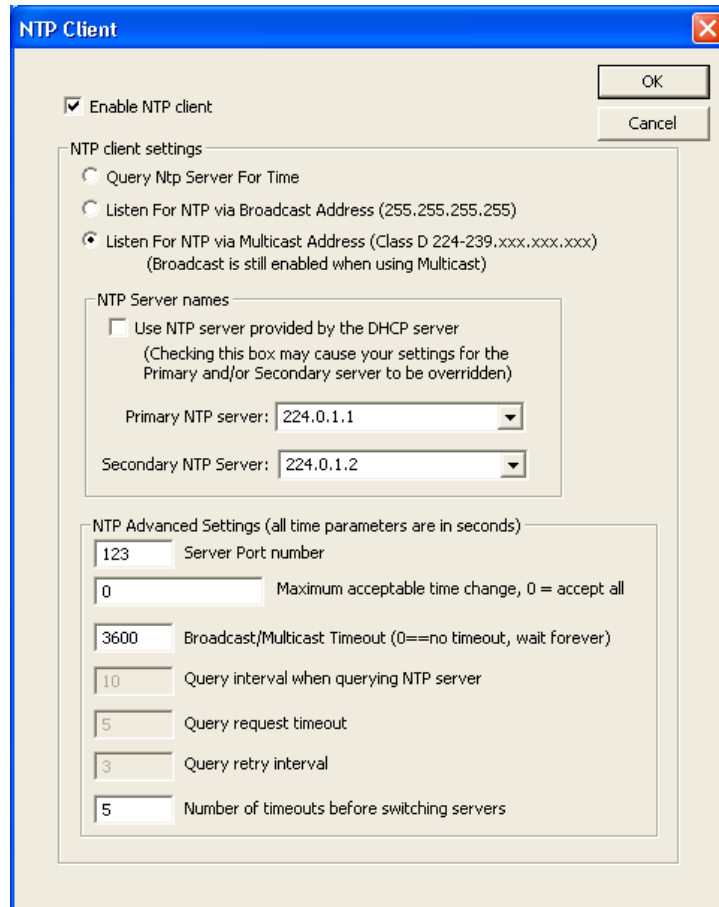
The Broadcast/Multicast timeout period (in seconds) is adjustable when this mode is selected.

[Note: While listening to NTP broadcasts, the device can also query the time server.]

[Note: Some NTP/SNTP clients will expect NTP servers to operate on port 123 and cannot be configured to utilize alternate ports.]

Listen for NTP via Multicast Address

The network clock can be set up to listen to NTP using multicast addressing by selecting the “Listen for NTP via multicast address(es)” checkbox.



When enabled, the multicast class D / group address may be specified as well as the frequency that multicast broadcasts will be issued. This can be changed as desired. The ntp client can listen for NTP multicast broadcasts using the full class D/ group address range. The ntp client does not restrict the use of the multicast address assignment and supports the full range of class D multicast addresses or groups from 224.0.0.0 to 239.255.255.255. These groups or class D address ranges for multicasting are defined and governed by [RFC3171](#), [IANA IPv4 Multicast Guidelines](#).

Typically, the multicast address range 224.0.1.0 - 224.0.1.255 (224.0.1/24) [Internetwork Control Block] is utilized for NTP traffic, however, please refer to the [RFC3171](#) for your specific application and implementation.

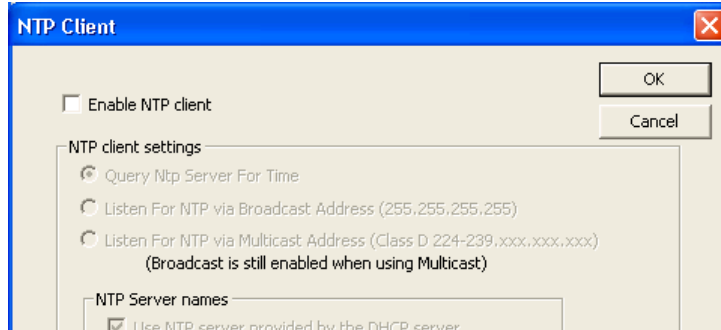
[Note: While listening to NTP broadcasts/multicasts, the ntp client cannot be configured to query the time server.]

[Note: Some NTP/SNTP clients will expect NTP servers to operate on port 123 and cannot be configured to utilize alternate ports.]

The network client can be configured to either query the NTP time server at a selected interval, to listen to NTP broadcasts only, or to listen to multicast broadcasts. When multicast mode is selected, the client will also listen to broadcast messages. The default configuration is to query the NTP server at 10-second intervals. To configure the device to only listen to NTP broadcasts, click the checkbox for “Listen for NTP broadcasts only”, and enter a “Broadcast/Multicast Timeout” in seconds. The default timeout is 3600 seconds.

Disabling the network client.

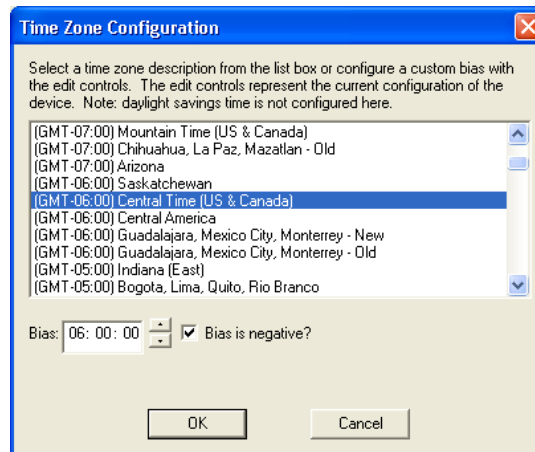
The CRL1000 device has the NTP client enabled by default. It may be desirable to disable the NTP client for certain applications such as those where the CRL1000 will not reside on a network during typical operation. The NTP client may be disabled by deselecting “Enable NTP client” option.



Local Time Settings

Time Zone/Time Offset

The Time Zone/Time Offset button included in the right half of the window, gives the clock complete flexibility to display any time zone. First select the time zone, by clicking the Time Zone button. This opens a new window that gives you a list of time zones, including descriptions to help with the selection. Select the Time Zone and click *OK* to close the window. Changes are not applied until you click *OK* or the *Apply* button on the main Configuration window.

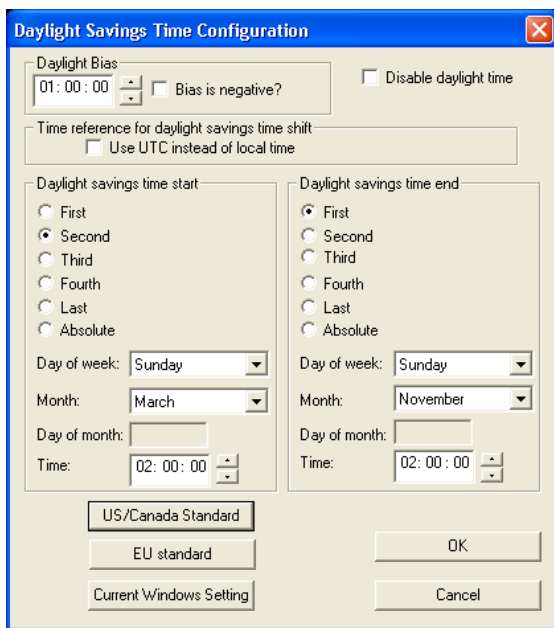


Daylight Saving Time Settings

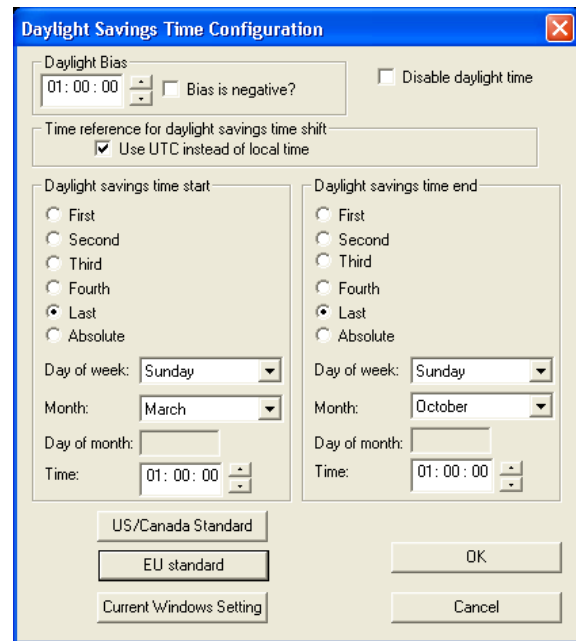
The Daylight Saving Time button, also included in the right half of the window, give the clock complete flexibility to display any time zone and DST combination. First select the time zone, by clicking the Time Zone button as described above. Next click the *Daylight Savings Time* button to configure the Daylight Savings Time, if appropriate.

You may use either of the following options are available for setting the DST rules.

- manually enter the daylight saving time rules.
- select the convenient preset DST rules for “US/Canada Standard” button
- select the convenient preset DST rules for “EU Standard” (European Union) button
- select the convenient “Current Windows Setting” button to apply the DST rules as currently configured for your current Windows OS.



US/Canada DST standard [adopted Spring 2007]



EU DST standard

Click *OK* to close the Window. The DST rules will be applied when you click *OK* or *Apply* on the main Configuration window.

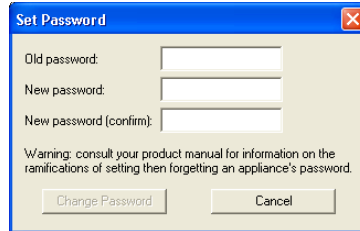
Set Password

Each network device has a password access that must be entered before the device will accept configuration changes. Each device or set of devices can have a unique password or they can all share the same password.

The factory default password is “public”.

The “Set Password” function allows the password to be changed for the device(s) of your network..

A password can be a maximum of 11 characters and may contain any sequence of letters, numbers, and common punctuation. Passwords are case-sensitive.



The 'Set Password' dialog box contains three input fields: 'Old password:', 'New password:', and 'New password (confirm):'. Below the fields is a warning message: 'Warning: consult your product manual for information on the ramifications of setting then forgetting an appliance's password.' At the bottom are two buttons: 'Change Password' and 'Cancel'.

WARNING: If the password is lost, the user must reset the CRL1000 using the “Set to Factory Default” button on the front of the unit. This will cause the unit to return all configuration to factory-default settings.

When a password is set for a device, each time you click OK or Apply for that device you will be asked for the password. You may create a unique password for each device. You may enable the ‘Remember this password for the session’ checkbox to eliminate typing the password for each configuration change.

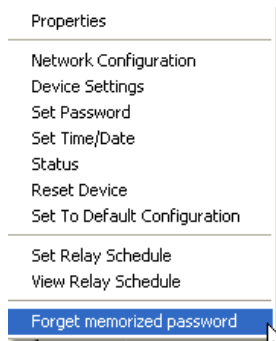


The 'Password Required' dialog box displays the message: 'The device requires a password to authenticate this operation.' It includes a 'Password:' field with masked characters, a checked checkbox labeled 'Remember this password for the session', and 'OK' and 'Cancel' buttons.

[Note: each device listed can have a unique password associated with it, which will default to the factory default password. You must enable the “Remember this password for the session” checkbox for each device that is being configured.]

WinDiscovery will not remember or store the password (s) after the session is closed. It is important for the user/system administrator to maintain passwords in a safe place.

If you enter the wrong password and selected the “remember password” checkbox, you will receive an error upon selecting OK or Apply to any configuration changes. You can close the WinDiscovery session to “forget” the password(s), however this will require entering the password again for each device. Alternately, you can remove the incorrect password entry during a WinDiscovery session by going to the right click menu for the device and selecting Forget memorized password option. This option will be added to the right click list and will only be displayed if a password is memorized.

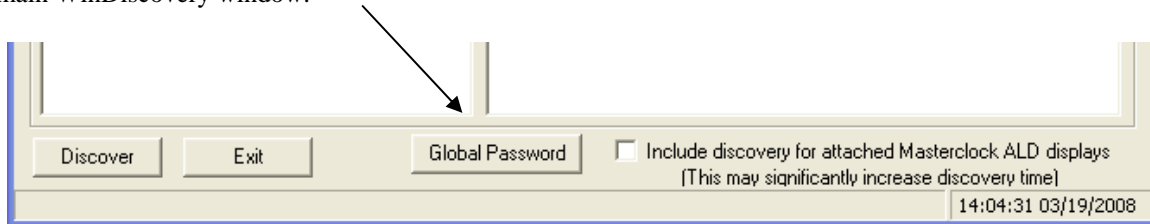


[Note: the factory default password is: “public”]

[Hint: To remove password protection for a device, select the Set Password command. You will be prompted to enter the old password. Enter the old password. Do not enter any values into the New Password or Confirm Password fields. Click OK to save. Upon you next session, you will not be prompted for a password for the clock.]

Global Password

In conjunction with the standard Set Password function, a global password access feature has been added. The Global Password feature allows you to use a global password to configure all devices have the same /common password between them. The global password access feature eliminates the need to enter a password for each device each time a device is being reconfigured or a session of WinDiscovery is started. Access to the global password feature is located the main WinDiscovery window.



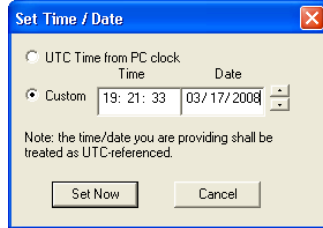
[Note: The Global Password feature works on only those clocks with the same password as the global password. The global password is saved in the registry of the PC running the WinDiscovery application and must be re-entered at each PC that WinDiscovery is being used upon.]

For more information regarding how to use the global password feature of WinDiscovery – see appendix I

Set Time/Date (Manual Override Feature)

The Set Time/Date menu item lets you manually set the time and date for the CRL1000. The function may be most useful for demonstration, in lab situations, environments where an external reference time signal is not available, when the built in NTP client is disabled, a network connection to an NTP server is not available, or when the incoming time code to the TCR option does not have year or date encoding. The time for the CRL1000 can either be set to the time of the PC or a manual custom time can be entered.

The CRL1000 will revert to the battery backed RTC and TCXO and maintain <165mS day drift during power down (outages) and/or storage.

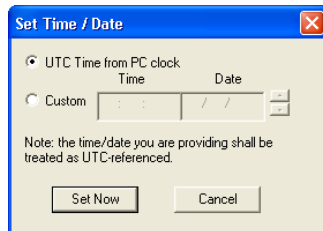


Set Time / Date screen – custom [use UTC time]

To set the time manually it is suggested to use a preset time source for best overall initial accuracy. While either method may be used, the “UTC Time from PC Clock” is recommended over the “Custom” manual entry method.

[Note: for the purpose of maintaining its internal clock, the CRL1000 time server always assumes the time entered is UTC and saves this information as the internal UTC time.]

For best results using the “UTC Time from PC Clock” method , first set the time on the PC that WinDiscovery is installed on, using an NTP/SNTP client pointed to either an Internet NTP time server or another reliable CRL1000. Immediately follow the time setting of the PC, by selecting the “UTC Time from PC Clock” option, and press the “Set Now” button.



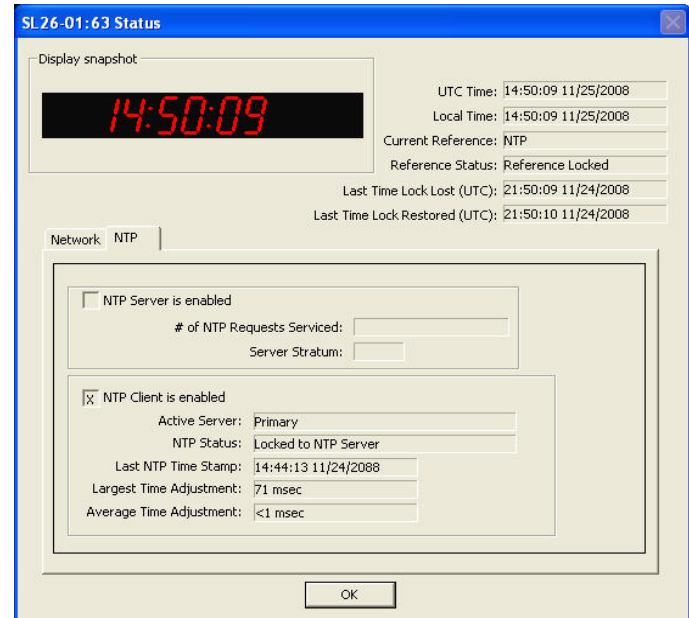
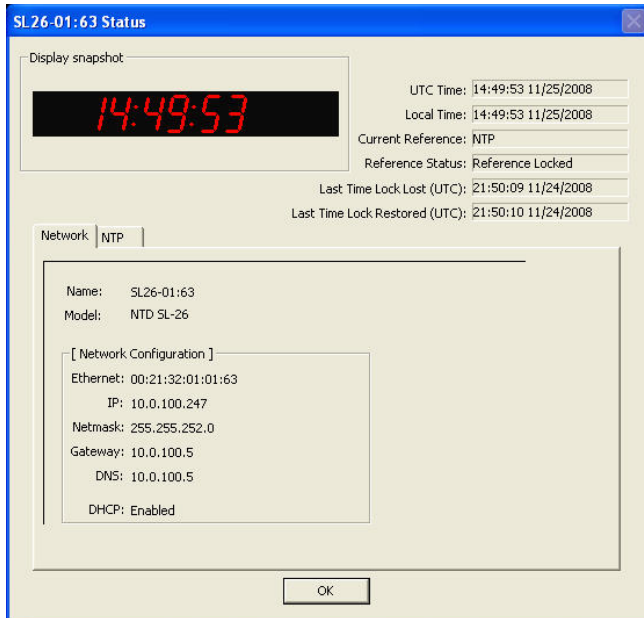
Set Time / Date screen – UTC Time From PC Clock

Status

Provides current status on the CRL1000's operation, including current UTC time/date on the unit, the Local time that is entered via the time zone and DST offsets , as well as other operational information relative to the available device and any installed options.

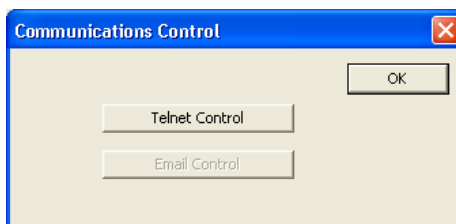
UTC Time: Current UTC time reference stored in the real time clock

Local Time: Current local time reference stored in the real time clock with applied time zone and DST offsets if enabled.



CRL1000 status may be monitored using the NTP tab.. Note that in this instance, the NTP client is locked to the primary NTP server.

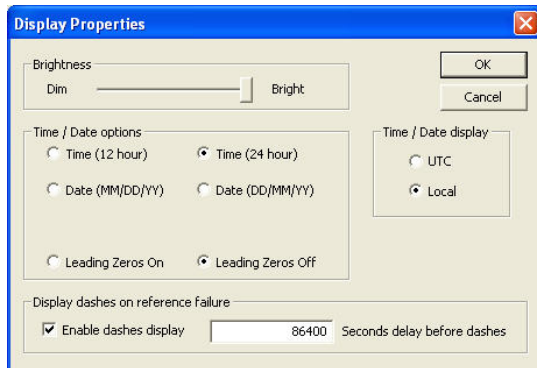
Communications Control – Certain advanced features may be configured using the “Communications Control” button. These features include , access to the telnet configuration interface .



LED Display Options

Your CRL1000 device contains a 6 digit LED display for time/date. The LED digital display may be used to display either time or date in various formats.

The six digit LED display can be configured to display time in 12 or 24-hour format, or date in MM:DD:YY, indicated as US, or DD:MM:YY, indicated as European format, or YYMMDD indicated as Asian format.



Configuring the front panel display is accomplished by using the “[Display Properties]” section of the main device settings window. The brightness control is a sliding bar to vary the brightness of the clock. This feature is useful to accommodate lighting conditions and viewer needs.

The front panel LED display can be configured to display local time instead of UTC reference time by using the Time Zone and Daylight Saving Time buttons to enter a local time offset. See the previous sections for setting Time Zone and DST offsets to obtain local time.

Time information may be displayed in either 12 or 24 hour mode. An LED dot (decimal point) on the front panel display option located in the bottom right hand of the LEDdisplay acts as an AM/PM indicator when the unit configured to display time in the 12 hour mode. *When ON, the LED indicates the displayed time is **PM**.*

Leading zero suppression may be applied.

The CRL1000 device will flash its green status LED at a rate of 1 Hz (once per second) when it is not synchronized to an external NTP server reference. This is the default configuration for the display if it is not synchronized to an NTP time server. However, It will continue to display time using its internal battery backed RTC (real time clock) while unsynchronized

The network device’s 6 digit time/date display may be set to display dashes to indicate that the unit is not synchronized to an NTP timeserver (or another time input source) when the internal time reference is not valid or trusted.

By default, the models CRL1000 will display time for a period of 24 hours from loss of the primary reference source. During this “free-wheeling” or “holdover” period, the CRL1000 will rely on the internal real-time clock (RTC) and temperature compensated crystal oscillator, (TCXO) oscillator, which has a typical holdover of +/- 1 min /year (+/- 165mSec drift over 24 hours or +/- 6.875 mSec drift over 1 hour). The CRL1000 will continuously discipline the internal RTC to provide maximum accuracy, while the NTP client is able to synchronize to the NTP server reference.

The maximum “Validity” duration is adjustable in 1-hour increments.

To always allow time display and always consider the internal clock source “valid”, set the validity duration to a value of zero “0”

Deselect the “ ” if you do not want the CRL1000 to display time using the internal RTC and TXCO oscillator while the unit is free-wheeling.

Troubleshooting Tips

[Important Note: WinDiscovery uses bi-directional UDP messaging on port 6163 for both the discovery process and to communicate configuration and status packets to and from the Masterclock® network clock(s). Delivery of UDP messages/packets is not guaranteed. If you experience intermittent problems with WinDiscovery, try closing the current session and restart the application. If this does not resolve the issue try the following trouble shooting tips, or switch to an alternate method of configuration such as telnet.]

All CRL1000 units are fully checked and system tested at the factory for proper operation before shipment and unless physical damage is found, the unit is probably functional.

Problem: Unable to find [discover] the Masterclock® network device(s) on the network with WinDiscovery.

Possible reasons/solutions:

1. Verify that you have supplied power to the network device.
2. The discovery process was not complete before selecting clock(s). After selecting “Discover” button, wait until the discovery status indicates 100% completion.
3. Verify that the network device is a Masterclock® brand. WinDiscovery is not designed to work with network products from other vendors.
4. Verify that the network device is on the same physical network as the computer from which you are running WinDiscovery.
5. If the computer is separated from the device by a router (on a remote network) or a firewall it is likely that the router/firewall is blocking communication with the device. Run WinDiscovery from a computer within the remote network, or ask a network system administrator to configure the router/firewall in question to pass through (both directions) UDP broadcasts on port 6163 [Note: If this does not resolve the detection problems you may additionally configure to pass through both directions UDP broadcasts on ports 6165, 6166, and 6264]. Some routers will not forward UDP broadcasts across networks – currently, this capability is required to use WinDiscovery for enterprise-level management of Masterclock, Inc. network appliances. If you are running a personal firewall product, such as ZoneAlarm™ or BlackICE™, or the built in Windows firewall you must adjust their configuration to pass through (both directions) UDP traffic on port 6163.
6. Verify that the hub/router/switch is capable of supporting the 10MB speed that the attached network device requires.
7. Verify that a DHCP/BOOTP server is present on the network. If the clock has been configured to use DHCP for network configuration but no DHCP/BOOTP server is present, the clock may not respond to discovery requests for up to twenty seconds after power-on. [Note: DHCP configuration is enabled as a factory-default.] In addition, the clock will reset its address (fallback) to one within the link-local address space (169.254.xxx.xxx) when no DHCP server is present or is not able to be reached. Reset the clock to initiate a new DHCP IP address request, or use static IP address mode. Consult your network system administrator to ensure that a DHCP server is present and accessible on your network and/or to obtain a list/range of available IP addresses.
8. Verify that the network device and the computer running WinDiscovery are attached to the network.
9. Verify that all network cables, hubs, etc. are in proper working order. Be sure that Ethernet crossover cables are not being used where inappropriate.

Problem: Device was found using WinDiscovery, but the status display is intermittent or not updating and/or clock does not appear to be responding to configuration changes under the current WinDiscovery session.

Problem: Device(s) previously found during a recent session of WinDiscovery do not show up during the current session.

Problem: The device’s status or settings displayed under WinDiscovery show garbled characters.

Possible reasons/solutions:

1. The WinDiscovery application has been open for too long and the device’s configuration(s) has(have) changed. For example, this can occur if the DHCP server has issued new/refreshed addresses. Close the WinDiscovery application and restart.
2. The discovery process was not complete before selecting clock(s). After selecting “Discover” button, wait until the discovery status indicates 100% completion.
3. Verify that the physical network cables and equipment and configuration for UDP have not changed.

4. Verify that you are currently the only user accessing the clock via WinDiscovery or telnet.
5. The network may currently be experiencing heavy traffic which is reducing bandwidth and/or causing collisions with the UDP messages/packets between the clock(s) and WinDiscovery. Since delivery of UDP messages are not guaranteed, this can cause WinDiscovery to not receive the latest configuration or status packets, and thus show outdated or garbled information. In some cases, the clock may not be discovered and displayed in the WinDiscovery device tree. In others, previously discovered clocks may no longer be accessible or responding.
 - Press the “Discover” button again and wait until the discovery process completes. This will occasionally resolve issues with units not being discovered.
 - Close the current WinDiscovery session and restart the WinDiscovery application.
 - Take steps to increase the bandwidth and reduce network traffic.
 - If this is an ongoing problem, consider the Telnet configuration method or remove the clock system to an isolated LAN.

Problem: Device appears in RED text under WinDiscovery device tree.

Problem: Device is being assigned an IP address of 169.254.xxx.xxx

Problem: Device not maintaining its assigned IP address.

Problem: Device function is erratic, appears to periodically reset itself.

Possible reasons/solutions:

1. Incorrect network configuration may be causing the device to receive a fallback IP address and or perform soft restarts. Verify that the IP address configured for the clock is correct. If you manually enter (or DHCP assigns) an IP address that already exists on the network, this will create an IP address conflict. The device will reset its address (fallback) to one within the link-local address space. Determine the cause of fallback IP address and resolve issue. View the error status field under the status window to help determine the cause of why the clock received a 169.254.xxx.xxx. Near the bottom of the Status window the error will be displayed. (If there is no error the text box will not be displayed.)

*[Note: Devices which have been assigned a fallback IP address of 169.254.xxx.xxx will be displayed in the main WinDiscovery window with **RED** text, indicating a problem with the configuration.]*

When the Ethernet interface is initialized the network device will verify that the IP address (either static or assigned by DHCP) is not being used by another device on the network. If a conflict is found the NTD clock will default to a 169.254.xxx.xxx address. The IP address that caused the error is saved and returned as an error to WinDiscovery. This error status is available to the user via the Status window on WinDiscovery.

- If static IP addressing is being used the original conflicting static IP address can be restored by doing a soft restart of the device using either WinDiscovery or telnet prior to changing any other configuration parameters.

[IMPORTANT NOTE: if the configuration of the network device is changed while a 169.254.xxx.xxx is being use, then the current 169.254.xxx.xxx address will become the permanent static address and the original conflicting static address is lost. At this point, it is necessary to manually change the static IP address to a one that will not conflict, or you may do a “Reset Configuration” to restore the system to factory default settings.]

- If DHCP was selected and the network device fell back to a 169.254.xxx.xxx address approximately every 10 [depending upon the “Advanced Settings” values] minutes the Ethernet interface will be reinitialized and the NTD clock will attempt to get an IP address from the DHCP server. If the NTD is successful, the error will be cleared and the new address from the DHCP server will be used. If a discovery was done using WinDiscovery or telnet was used this initialization will be delayed by 2 hours.

Problem: Device appears to ‘reset’ periodically.

Possible Reasons/solutions:

1. Check the network connection and setup. If DHCP is enabled [*Note: DHCP is enabled by default*] and a DHCP server is not active on the local network the clock will hesitate periodically while attempting to resolve DHCP configuration. To correct the problem, switch to manual networking configuration or determine why the local DHCP server is not operating.
2. If the device cannot resolve its DHCP address in DHCP mode, the unit will periodically perform a soft restart to re-initialize its communication port and DHCP configuration. See the trouble shooting section on fallback IP address
3. If the device has not been configured with at least one valid DNS server (or that DNS server is down) hesitations similar to those described in #1 will occur. At least one valid DNS server is required for operation.

Problem: Unable to communicate with the CRL1000 on the network with Telnet

1. If the CRL1000 has been configured to use DHCP for network configuration but no DHCP/BOOTP server is present, the CRL1000 may not respond to discovery requests for up to twenty seconds after power-on. [*Note: DHCP is enabled as a factory-default.*]
2. Verify that you have the correct IP address for the unit and the IP address did not change. If using DHCP to provide the IP address, this address may change periodically, you must know the IP address of the unit to use the TELNET interface.
3. Verify that the device does not have the Telnet interface disabled.

[Note: for security purposes, the Telnet interface can be disabled. When disabled, you will no longer be able to access the unit with Telnet. To re-enable the Telnet feature, one of the other configuration methods must be used, or the unit must be reset to factory default configuration.]

Problem: The UTC date/time is incorrect and the unit does not retain time settings when powered down/up.

The CRL1000 maintains its internal time in battery backed memory located using a real time clock. The battery supplies power to the TCXO 32kHz Oscillator and real time clock when the unit is powered off. This allows the internal configuration to be maintained and the time and date to increment, when power is off. Under normal operating condition, the memory devices maintaining the real time clock data is powered by the internal DC power supply and does not rely on the battery for data retention.

Note: If the CRL1000 does not retain its Date/Time settings (often indicated by the front panel time display counting up from ‘zero’) the battery will likely need replacement.

Check and replace the battery, if necessary. The battery type is a “maintenance free” 3V rechargeable Magnesium Lithium battery and can be replaced by a qualified technician, or the unit can be sent to technical support at Masterclock for repair/replacement for service using our RMA procedure. See the “Specifications” section for details on the recommended battery replacement, or contact technical support for assistance.

Problem: You have lost your password.

Possible reasons/solutions:

1. The password cannot be recovered if it is lost. Reset the clock to the factory default configuration using the procedure described in the Configuration section. After the clock has been reset to factory defaults, the unit must be reconfigured. The factory - default password is “*public*”

Problem: Multiple error window titled “Bad Password” continues to pop-up each time a configuration setting is applied.

Possible reasons/solutions:

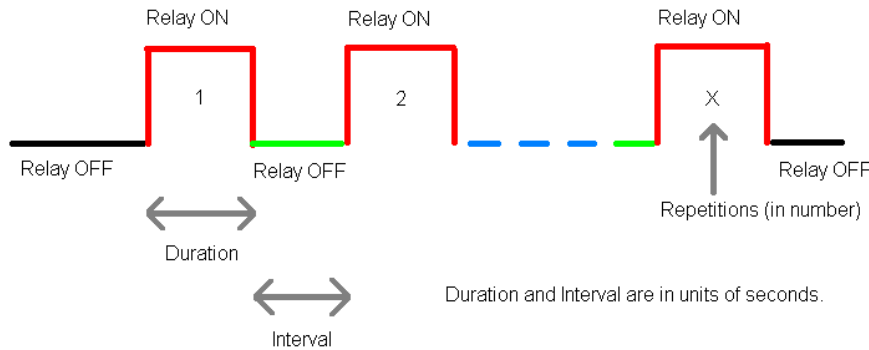
1. You have entered and “remembered” an incorrect password in the password windows. This is now causing multiple error indication windows titled “bad password” to pop-up for each portion of the configuration message that is being sent to the clock. You must clear the memorized password using one of the two options below.
2. WinDiscovery only remembers the password for the current session, close the WinDiscovery session and reopen. All passwords will be forgotten by the WinDiscovery application.
3. As alternative to closing the WinDiscovery session, Right click on the device being administered in the main WinDiscovery window. The right click pop-up menu now contains an entry for “Forget Memorized Password”. Select this option.
4. You are using a global password that is different from the password of the unit you are trying to administer. Change the global password to match that of the unit, or change the unit password to the global password.

If these troubleshooting tips do not solve your problem, contact technical support at **support@masterclock.com** or call (636) 724-3666. If these troubleshooting tips do not solve your problem, consult the support area of the www.masterclock.com website

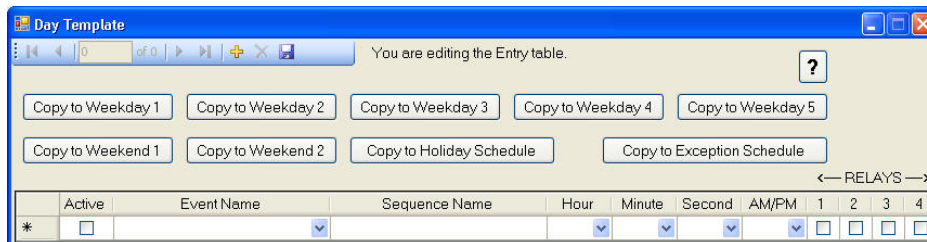
Program and Download a Schedule using Event Time Basic Application

Once you have configured your CRL1000 for network operation using WinDiscovery or Telnet, you can then program an event schedule and download it to the CRL1000. The MCR Event Time Basic application supplied with the CRL1000, allows the user to schedule events to occur at specified times for specified output channels. Up to four (4) independent channels can be scheduled with up to 128 events per day, over an entire calendar year.

Each event is comprised of a defined sequence. A sequence is a set of instructions to activate and deactivate an output channel (internal SSR - Solid State Relay) according to a specified ON time (duration), OFF time (interval), and number of repetitions.

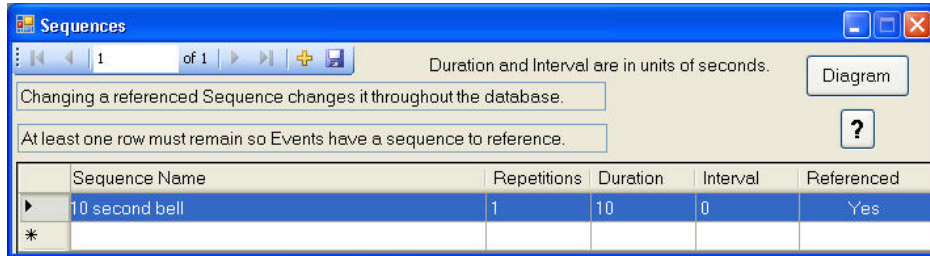


A template is available to create a standard day comprised of up to 128 events. The standard day template can be applied (copied) to define weekdays and weekend days, independently. Holiday and exception schedules can also be defined for handling special instances. A help file is included with the Event Time Basic application, which provides additional details.

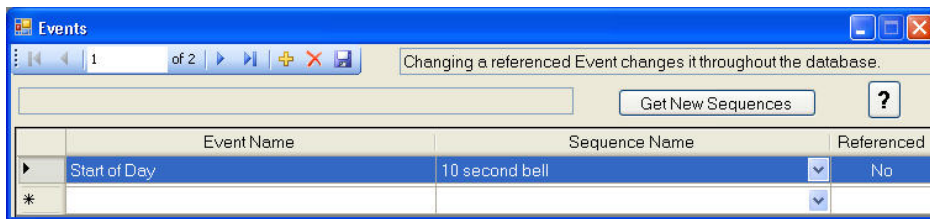


The example below is used to ring a bell or bell system on weekdays (Monday thru Friday) continuously for 10 seconds, with the event ending at the top of hour at 8:00:00 a.m.

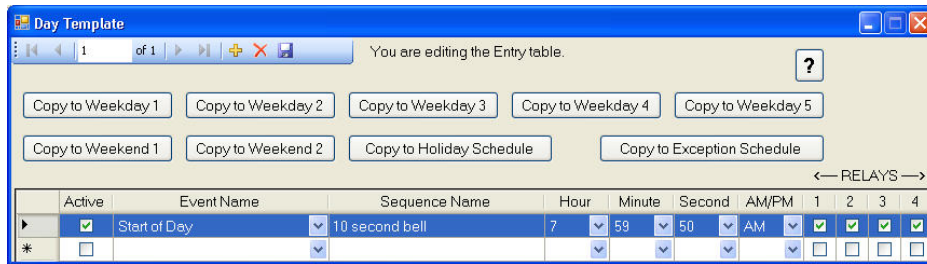
Step 1: Define a sequence with an ON time of 10 seconds, zero interval, and one repetition (ie 1 cycle). Save the sequence with a unique name: 10 second bell. When you define an event using the sequence, the sequence will be referenced (i.e. In use)



Step 2: Define an event using the sequence, and save with a unique name. [Up to 128 unique named events can be defined and saved.]. When you use an event in a day, holiday, or exception schedule, it will be referenced (i.e.in use)



Step 3: Create a day schedule from the standard day template that calls the event at a specified time. Define which channels the event controls. In this instance, the events defined start time would be at 07:59:50 AM, and would control all bells, so select channels 1,2,3, & 4. You can select whether you wish the event to be active or not active.



Hint: you can define and save a full standard day as a template, with all possible events. Then you can recall (open) the standard day and then make active only certain events that get copied to specific days (weekdays, weekend days, holidays, or exception days). In this instance, we want to make the event active.

Step 4: Copy the day schedule to individual days of the week. In this instance, copy to weekday 1, weekday 2, weekday 3, weekday 4, weekday 5.

Step 5: Save the newly schedule (essentially a full calendar year).

Step 6: Select the CRL1000 of interest and download the schedule to the device.

This was only a simplified example of creating and downloading a simple single event schedule. Refer to the help file of the MCR Event Time Basic for additional information.

Connecting Bells

NOTE: For installations that need to conform to the National Electrical Code, you must use their guidelines for wiring bells and other signaling devices. Contact your local electrician or authority to determine what is legal and required for your local region.

The CRL1000 contains four independent 24VAC output channels (powered circuits) that may be wired and programmed for controlling signaling devices.

Each channel (or signaling circuit) is a Normally Open (NO) 24VAC power supply with rated output at 4 amps maximum recommended load current.

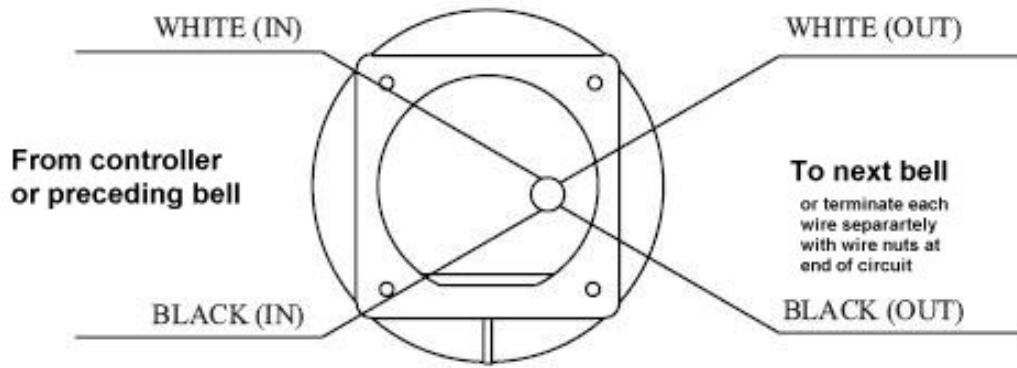
Each output channel is protected with a self-resetting thermal circuit breaker, and contains a power switch with OFF/RESET settings. When placed in the “OFF” position, power is removed from the circuit. When placed in the “RESET” position, internal 24VAC voltage is available to the NO (normally open) Solid State Relay (SSR), and the circuit may be “live” depending upon the state of the SSR as controlled by the applied schedule, or in the event that the “TEST” or “ALARM/TRIGGER” switches are active. In the open or OFF state, no output voltage is available. (Each circuit is OFF).

Upon activation of a scheduled event, closure of the “TEST” switch, or closure of the Normally Open “Trigger/Alarm” Input (terminal block on rear), the SSR actuates (closes) and 24VAC power is present on the output channel(s), until either the scheduled event ends, the scheduled event indicates an open interval, or the “TEST” or “ALARM/TRIGGER” switches are released. A scheduled event can operate/control one, or more (up to 4) output channels. The “TEST” and “ALARM/TRIGGER” switches affect all four output channels, simultaneously.

The typical load rating of 24VAC bell devices ordered from Masterclock will be 0.2 Amps. Thus, each output circuit or channel can support up to 20 [Masterclock] bells. Therefore, the total maximum recommended load for the CRL1000 is 4 channels x 4 amps per channel = 16 amps total, or 80 Masterclock brand bells rated at 0.2 Amps each @ 24VAC.

Each output channel is provided with a screw type two-piece terminal block for connection of bells or other signaling devices. The terminal blocks can support wire sizes in the range of 18 gauge to 12 gauge (AWG, American Wire Gauge). It is recommended to use multi-stranded wire, in the largest available gauge to reduce the impedance of each wire run, while retaining flexibility. Twisted pair may be used and is recommended to reduce the overall inductance of the cable run. In some instances, 18 gauge solid copper wire pairs, such as thermostat wire may be sufficient for your application to reduce cost, however, 12 gauge stranded, twisted pair wire is suggested for most installations requiring multiple bells or long runs on a single circuit.

Bells may be connected in a series connection, in which a bell’s input is connected to the output of a previous bell as shown in the diagram below.



The first bell in the series circuit is connected to the terminal block of an output channel of the CRL1000. The final bell in the sequence is connected to the second last bell. However, its output terminals are individually capped with wire nuts. Do not connect the power and return lines as this will create a short circuit, and do not add any termination resistors. The disadvantage of a series circuit is that as each subsequent bell and wire run is added to the circuit, the total impedance increases, while the total current of the first sections of the circuit wiring must also increase. The effect is that the overall length of the run must be reduced in order to compensate for the I^2 loss (power), the associated temperature rise in the wire and insulation, and the voltage drop along the run.

Bells may also be connected to a distribution terminal block or terminal strip [not provided] with individual wires/cable pairs to create a parallel circuit. The terminal block or terminal strip is connected by a short wire run to the terminal block of a channel of the CRL1000. In this parallel distribution each wire run (pair) must only supply the current necessary to power one bell. This allows for maximum distance, minimum power loss, minimum temperature rise, and minimum voltage drop. This parallel circuit may be preferred for installations requiring a large number of bells or other signaling devices over large distances.

A combination of parallel /series circuit wire distribution may also be used.

Finally, you may add additional CRL1000 devices to your installation to reduce the required number of signaling devices or total length of each cable run.

The choice of distribution method will depend upon many factors. Please consult your local electrician or authority or the NEC in your area for determination of the distribution method for your application.

Specifications

Communications – Protocols

- **DHCP/BOOTP (default)**
- **Static IP addressing**
- **Network Time Protocol**
 - IPV4 (RFC3171)
 - SNTP V4 (RFC 2030)
 - NTP version 3 (RFC 1305)
 - UDP, port 123 (default)
 - Unicast (Query) mode [port 123, default]
 - Broadcast mode [255,255,255,255 default]
 - Multicast mode (RFC3171 IANA IPV4 Multicast Guidelines)
- **Configuration (Network)**
 - WinDiscovery Network Discovery and Configuration utility
 - Windows 2000, XP, 2003 Server, Vista OSs
 - Proprietary packet protocol – UDP, port 6163
 - Device Password or Global Password support
 - Telnet – TCP, port 23 (default)
- **Serial Port (option)**
 - USB 2.0,

Communications – I/O

Ethernet (10/100Mbps) RJ45, 10/100 baseT
Length of communication cable (Cat5/5e) 100 meters maximum

USB USB 2.0 -Type B
Length of communication cable 3 meters maximum
The communication settings for the USB port are: 57600 baud, 8 data bits, 1 stop bit, no parity.

Timing Characteristics (Standard)

Type Temperature Compensated Crystal Oscillator (TCXO)
Stability (Accuracy/Drift with NTP lock) +/- 1 min/year (0-40 C) , +/- 3 min/year (41 to 50 C)
Accuracy NTP Client Network Client 1-10mS typical, 10 sec query (default)

Input Power Requirements

AC Input Voltage 100-240 VAC +/-10% (90-264VAC), 50/60 Hz Hz
 AC Input Connector..... Universal IEC input connector with ON/OFF power switch.
 AC power consumption 720 VA, 6 Amps @ 120 VAC, 3 Amps @ 240 VAC
 Protection..... AC line fuse, output thermal fuse (per channel), 5A




Caution: there are no user serviceable parts inside the CRL1000.
 Please contact the factory if you require servicing or repair.

Output Power Ratings

AC Power (per channel) 120 Watts Maximum
 AC Power (total)..... 480 Watts Maximum
 AC Voltage..... 24VAC
 AC Current (per channel) 5 Amps Maximum
 AC Current (total)..... 20 Amps Maximum
 Circuit Breaker (per channel) Self Resetting Thermal fuse, 5A rating, with ON/OFF switch
 Connectors..... Terminal block, 2 position, screw type, 18 AWG to 12 AWG

RTC Battery

Battery is for maintaining real time clock circuit only:

Battery		Replacement
3V, 17 mAh, Maintenance Free Rechargeable Manganese Lithium		3V,17 mAh, Coin Cell Maintenance Free Rechargeable Manganese Lithium Panasonic ML1220/F1A



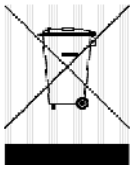

Physical

Size: 19w x 3.5h x 9.25d in **Weight:** 19.5 lbs
 48.3w x 8.9h x 23.5d cm 8.85 kg

Operating/Storage Temperature & Humidity

Operating Temperature..... 0 to +70°C (0 to 40°C, +/- 1 min/year for standard TCXO)
 Relative Humidity Up to 90% (non condensing @ 25°C)
 Storage Temperature..... -40 to +70 °C

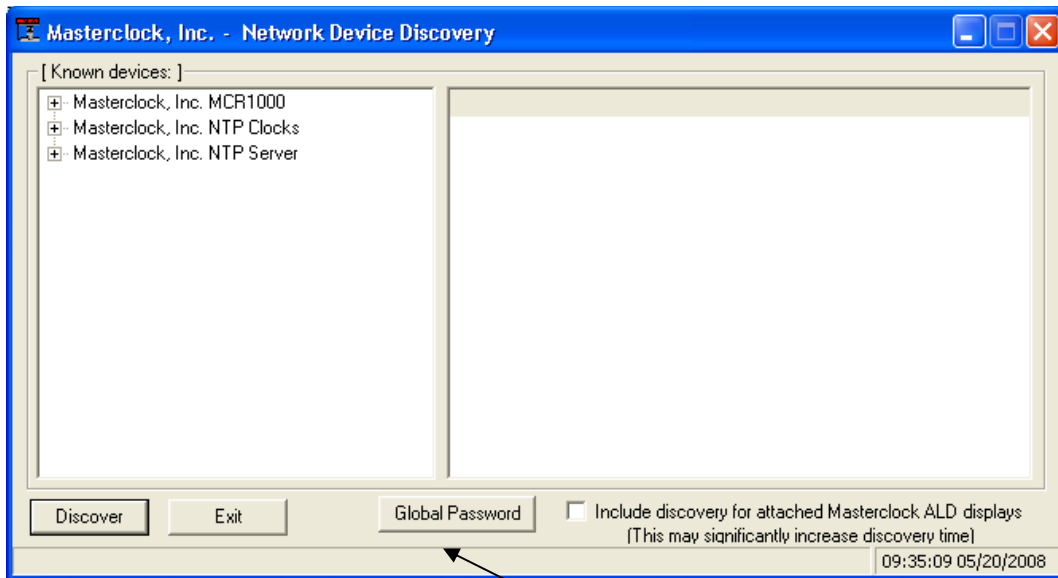
Compliance

	<p>This device complies with part 15, Subpart B of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation</p>
	<p>Models CRL1000S base model or with GPS, HSO, options Electromagnetic Compatibility 89/336/EEC ; 92/31/EC ; 93/68/EEC ; 2004/108/EC <u>Tested and Conforms to the following EMC standards :</u> EN61000-3-2:2000 (Harmonic Current Emission) EN61000-3-3:1995 + A1:2001 (Voltage Fluctuations & Flicker) EN61000-4-2:2000, ,3,4,5,6,8,11 (ElectroStatic Discharge, RF Immunity, Fast Transient CM, Surge, RF Injection CM, Power Frequency Magnetic Field, Voltage Dips) EN61000-6-3:2001 (EMC Emissions –Generic Commercial) EN55022:1998+A1:2000 +A2:2003 CISPR22</p> <p>Low voltage directive 2006/95/EC <u>Tested and Conforms to the following Safety standards:</u> EN60950-1:2001 (Safety of Information Technology Equipment)</p>
	<p>Waste Electrical and Electronic Equipment Directive (WEEE) 2002/95/EC</p> <p>The CRL1000 is considered WEEE Category 3 (IT and Telecommunications Equipment as defined by the WEEE Directive and therefore fall within the scope of the WEEE Directive.</p> <p>For more information about Masterclock’s WEEE compliance and recycle program, please visit the Masterclock WEEE/RoHS website at http:// www.masterclock.com/rohs.htm</p>
	<p>Restriction of the Use of Certain Hazardous Substances Directive 2002/95/EC</p> <p>The CRL1000 is considered WEEE Category 3 (IT and Telecommunications Equipment as defined by the WEEE Directive and therefore fall within the scope of the RoHS Directive.</p> <p><u>These units are RoHS Compliant except that they will be manufactured using the RoHS Directive exemption allowing the use of lead in "solders for servers, storage and storage array systems, network infrastructure equipment for switching, signaling, transmission as well as network management for telecommunications". Reference RoHS Directive Annex Point 7 as amended by 2005/747/EC.</u></p>

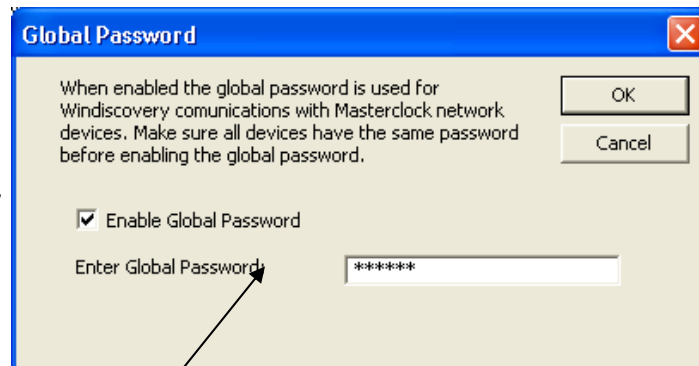
Appendix I: WinDiscovery Global Password Feature

A significant feature has been added to *WinDiscovery* V2.6.0 and greater, which allows for the use of global passwords. Prior to the implementation of a global password feature, a password was required to be entered for each device being administered during a *WinDiscovery* session. With the global password feature enabled, a single password may be entered once during an initial session. All devices with that password may then be administered without entering the password for each device. The global password information is saved in the registry of the computer running *WinDiscovery*.

Enabling Global Password



- To utilize the global password, select the “Global Password” button on the main screen of *WinDiscovery*.



- Enable the global password feature by selecting the “Enable Global Password” checkbox.
- Enter the global password.
- Select “OK”
- At this point the global password settings will be saved in the registry of the computer running *WinDiscovery*.
- During this session, and subsequent sessions of *WinDiscovery* , you will not have to enter the password.

[Note: The global password information is saved in the registry, and if enabled, does not require the password to be entered during subsequent WinDiscovery sessions. To maintain security for your system you may wish to disable the global

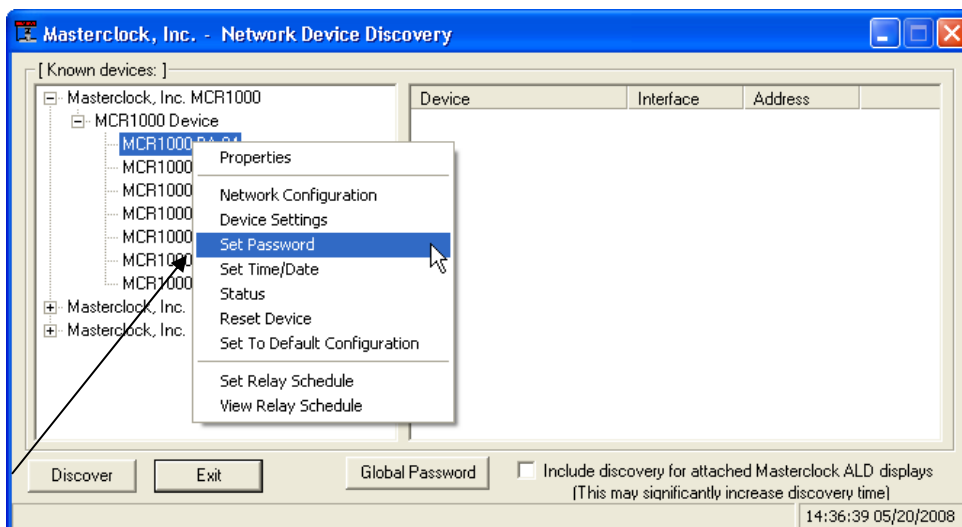
password at the end of each session, or only place WinDiscovery in a password protected user account or Administrator account which restricts access to the WinDiscovery application].

[**Note:** The global password being used must exactly match the existing password on all the devices being administered. For example, on any new system being installed, the factory default password on all devices is “public”. Therefore, the global password must also be set to “public”. To use a global password other than “public”, the password for each device of the group must be changed using the “Set Password” command (available on the right click menu of the item). The global password does not overwrite the existing password for a device, therefore any device with a different password cannot be administered.]

Changing the Global Password



- Turn of the global password feature in *WinDiscovery* by deselecting the “Enable Global Password” checkbox.
- Use *WinDiscovery* to manually change the password for each device to the new “desired” global password by using the “Set Password” command. (Available under the right click menu for each device)



- Enter the new password information and select the “Change Password” button.



- Repeat for each device in the group that is to use the global password.



- Re-enable the global password feature by selecting the “Enable Global Password” checkbox.
- Enter the new global password.

Disabling the Global Password



- Turn of the global password feature in *WinDiscovery* by deselecting the “Enable Global Password” checkbox.
- It is not necessary to delete the information from the global password field.

Appendix II: Telnet Terminal Configuration

A terminal-style command line configuration interface is available via Telnet. The Telnet interface provides the functional equivalent to the configuration parameters and status information of those available by WinDiscovery. To connect with the CRL1000 with Telnet, use any standard Telnet client application, specifying the IP address of the CRL1000 as the server with which to connect. The factory default port is well-known Telnet server port 23.

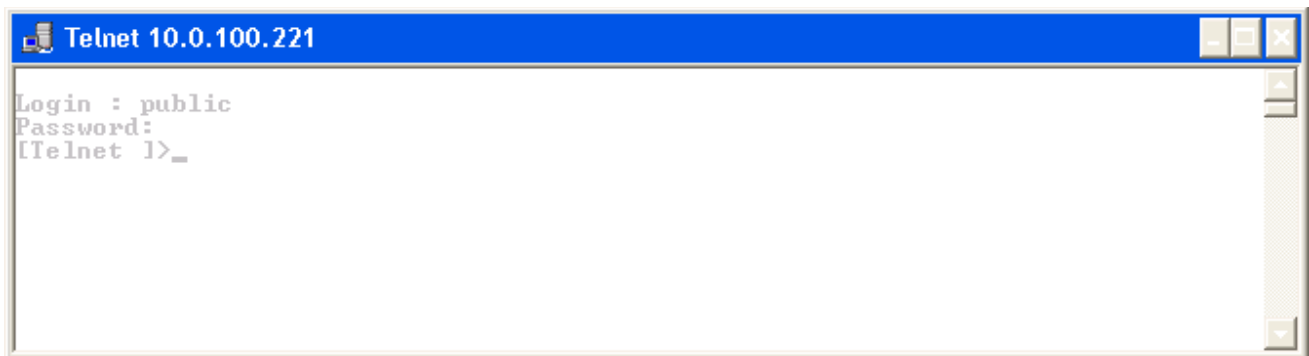
[Note: The IP address of the unit is required to configure the CRL1000 with Telnet. By default, the CRL1000 is configured to obtain an IP address via DHCP. If a DHCP server is available on the network when the CRL1000 is installed, it can be utilized to provide the IP address of the associated device name that is registered with the server.]

Configuration via Telnet may not be convenient for devices operating with a factory default network configuration since the IP address is not known. The CRL1000 will have a factory default of using DHCP for obtaining a network IP address.

Hint: Use the WinDiscovery application to establish first-time networking configuration or use only on systems with a DHCP server available..

If you are not familiar with the Telnet application, or command line interface, ask your network system administrator for assistance.

Upon entering the CRL1000 configuration via Telnet, the initial login screen is shown below.
When prompted for “Login” enter your username : default user name is “**public**”
When prompted for “Password” enter your password: default password is “**public**”



At the “[Telnet]>” command prompt you may enter “?” or help to display the main menu



[Note: The Telnet interface does not use any type of security other than a password for initial access. The Telnet interface can be disabled to provide added security. When disabled, you will no longer be able to access the unit with Telnet. To re-enable the Telnet feature, one of the other configuration methods such as WinDiscovery must be used, or the unit must be reset to factory default configuration.]

[Note: If Telnet is disabled, the current session will be ended and the user must use WinDiscovery, or the Reset to Factory Configuration button to re-enable it.]

Exiting Telnet

To exit the terminal interface, select option ‘X’.

Troubleshooting Tips - Telnet

Problem: Unable to communicate with the CRL1000 on the network with Telnet

1. If the CRL1000 has been configured to use DHCP for network configuration but no DHCP/BOOTP server is present, the CRL1000 may not respond to discovery requests for up to twenty seconds after power-on. [Note: DHCP is enabled as a factory-default.]
2. Verify that you have the correct IP address for the unit and the IP address did not change. If using DHCP to provide the IP address, this address may change periodically, you must know the IP address of the unit to use the TELNET interface.
3. Verify that the device does not have the Telnet interface disabled.

[Note: for security purposes, the Telnet interface can be disabled. When disabled, you will no longer be able to access the unit with Telnet. To re-enable the Telnet feature, one of the other configuration methods must be used, or the unit must be reset to factory default configuration.]

LIMITED WARRANTY

This Masterclock, Inc. (hereinafter MC) product warranty extends to the original purchaser.

MC warrants the CRL1000 against defects in materials and workmanship for a period of one year from date of sale. If MC receives notice of such defects during the warranty period, MC will, at its option, either repair or replace products, which prove to be defective.

Should MC be unable to repair or replace the product within a reasonable amount of time, the customer's alternate remedy shall be a refund of the purchase price upon return of the product to MC. This warranty gives the customer specific legal rights. Other rights, which vary from state to state or province to province, may be available.

Exclusions

The above warranty shall not apply to defects resulting from improper or inadequate installation or maintenance by the customer, customer-supplied software or interfacing, unauthorized modification or misuse, operation outside of the environmental specifications for the product or improper site preparation and maintenance (if applicable).

Warranty Limitations

MC MAKES NO OTHER WARRANTY, EITHER EXPRESSED OR IMPLIED, WITH RESPECT TO THIS PRODUCT. MC SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

In any state or province which does not allow the foregoing disclaimer, any implied warranty of merchantability or fitness for a particular purpose imposed by law in those states or provinces is limited to the one-year duration of the written warranty.

Exclusive Remedies

THE REMEDIES PROVIDED HEREIN ARE THE CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES. IN NO EVENT SHALL MC BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER BASED ON CONTRACT, TORT, OR ANY OTHER LEGAL THEORY.

In any state or province which does not allow the foregoing exclusion or limitation of incidental or consequential damages, the customer may have other remedies.