Remote Control System

Models RCS-8 and RCS-16

•

with Remote Facilities Controller model RFC-1/B

– INSTALLATION AND OPERATION –

Documentation for 8 and 16 channel systems
Standard and extended capability "xl" systems

Sine Systems, inc

www.sinesystems.com

Table of Contents

Section 4 – Operation

Section 5 – Remote Access

Section 6 – Circuit Description and Factory Service

Section 7 – Specifications

Section 1 — Safety Information

⚠️ WARNING! *Only qualified technical personnel should install an RCS-8 or RCS-16 system. An attempt to install this device by a person who is not technically qualified could result in a hazardous condition to the installer or other personnel, and/or damage to the RCS and other equipment. Ensure that appropriate safety precautions are made before installing or servicing this device.*

⚠️ Attention! *Do not remove or defeat the ground prong of the AC plug. The RCS-8 and RCS-16 are designed for indoor use in a dry location. Installation and operation in other locations could be hazardous.*

The RCS-8 and RCS-16 operate on 120 or 240 volts AC. Dangerous and potentially lethal voltages will be present if the cover is removed while it is connected to AC power. For this and other reasons service should be performed only by a qualified technician.

If the fuse is replaced, the new fuse should be of the same type and rating as the original fuse. This value is indicated on the rear panel of the device.

The RCS-8 and RCS-16, as any electronic device, can fail in unexpected ways and without warning. Do not use the RCS-8 and RCS-16 in applications where a life-threatening condition could result if the device were to fail.

Depending on the installation, the control circuits of the RP-8 Relay Panel may be connected to sources of up to 120 volts AC and/or several amperes of current. Under certain conditions, these voltage sources can be lethal. Always use caution when working around these circuits. Disconnect all high voltage and high current sources before servicing the system.

Exercise caution when working near the connectors on the RP-8. The removable connectors used on the RP-8 leave slightly exposed tips even when the connector is in place. The tips are not dangerous but they are pointed. Furthermore, the exposed metal provides a very small point where a short could occur. Be careful when using metal tools near any exposed wiring. Power should be removed form all devices when performing service.

The RCS-8 and RCS-16 contain self-resetting "fuses" that protect it from excessive current. If they become damaged, replacement devices should be of the same type and rating.

1.2   FCC Compliance

The RCS-8 / RCS-16 complies with Part 68 of the FCC rules. On the rear panel of the device is a label that contains, among other information, the FCC registration number and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

The REN is used to determine the number of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most areas, the sum of the RENs should not exceed 5.0. Contact the local telephone company to determine the maximum REN for the calling area.

The RCS-8 / RCS-16 is designed for use with standard modular (RJ-11C) telephone jacks.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the RCS-8 / RCS-16. If this happens, the telephone company usually provides advance notice in order for you to make the necessary modifications to maintain uninterrupted service.

If the RCS-8 / RCS-16 causes harm to the telephone network, the telephone company will notify you in advance of service disconnection. If advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

Please contact Sine Systems, Inc., for repair and/or warranty information if you suspect that the RCS-8 / RCS-16 has malfunctioned. If a defective device is causing harm to the telephone network, the telephone company may request you remove that device from the network until the problem is resolved.

The RCS-8 / RCS-16 cannot be used on public coin service telephone lines. Connection to Party Line Service is subject to state tariffs. Contact your state public utility commission, public service commission, or corporation commission for information.

The RCS-8 / RCS-16 is registered with the Federal Communications Commission and is certified to meet specific safety requirements. It is important that the RCS-8 / RCS-16 not be modified in any way. Modification of this equipment will void the FCC certification, void the warranty, and perhaps pose a hazard to the user of this equipment or to maintenance personnel of your local telephone company.

Service should only be performed by qualified technicians that are familiar with the implications of FCC Part 68 registration. Caution should be used if the RCS-8 / RCS-16 case is opened while still connected to the telephone line. High voltages may be present on telephone lines.

Section 2 — System Description

2.1   General Description

The RCS series remote control systems are an updated, single-chassis version of the RFC-1/B Remote Facilities Controller and RP-8 Relay Panel. These systems consist of a main controller board and one or more interface boards. The controller provides the core remote control features with an embedded RFC-1, wired network interface with web server and telephone line surge suppression. The interface boards provide control relay outputs and telemetry inputs with built-in surge suppression.

The RCS series systems are housed in a standard EIA two space (1U) 19-inch rack mounted case. Front panel controls and indicators depend on the system configuration. There are indicators for power, system status, system connectivity, communications status and other system events. The system has a universal power supply that operates from 90 to 240 volts AC at 50 or 60 Hz.

All connections to the RCS-8/16 are on the rear panel. There are connections for the power supply, network data I/O, relay panel(s), a local telephone and the telephone line. The power supply fuse is accessible from the rear panel.

2.2   System Requirements

The RCS series devices are complete remote control systems with up to 16 internal channels of telemetry and control. RCS series remote controls are backward compatible with existing RP-8 Relay Panels.

RCS series devices require a single grounded power supply outlet. If external RP-8 relay panels are used, they will be powered from the internal power supply and do not require an external power source.

A telephone line terminated in a standard modular connector is required for voice communications. A single-line telephone is required for local control and programming. Compatibility with speakerphones connected to the local jack cannot be guaranteed due to varying power demands.

The data interface requires broadband data service at the site. The service connection to the RCS-8/16 must be provided over wired Ethernet. This will typically be a LAN connection through a router to the Internet. The router will need to open a port so that the RAK-2 web server can be accessed from the Internet.

2.2.1   Broadband Data Service

It is up to the customer to provide a suitable broadband data connection at the site to use the RCS-8/16 web server. The provider and class of service should not matter. If you can browse the Web over the connection then it should be suitable for the task.

It is solely the responsibility of the customer to monitor bandwidth to avoid excessive use fees imposed by some service providers. This system does not generate data at a high speed but it is a full-time network connected device.

The RCS-8/16 can, and probably should, be installed behind a NAT router in most installations. It is not absolutely necessary to use a router but it does afford a measure of protection and a level of convenience during operation. The router must be set up to open a port between the RCS-8/16 and the Internet, otherwise the web server will be available on the local LAN but not from a remote location over the internet.

The RCS-8/16 requires a wired connection to the network. This does not mean that it will not work with wireless broadband service. If a wireless Internet service provider is used then the router must have a wired network port to service the RCS-8/16. Use of wireless devices is not encouraged because there is enough RF energy at many sites to disrupt wireless communications.

2.3   Front Panel Indicators and Controls

All RCS series remote control systems have twelve system status indicators and a single push-button control. Additionally, each model has status indicators that are specific to the model. Model-specific LEDs indicate channel selection state and the state of control relays. Control relay state is present on "xl" models only.
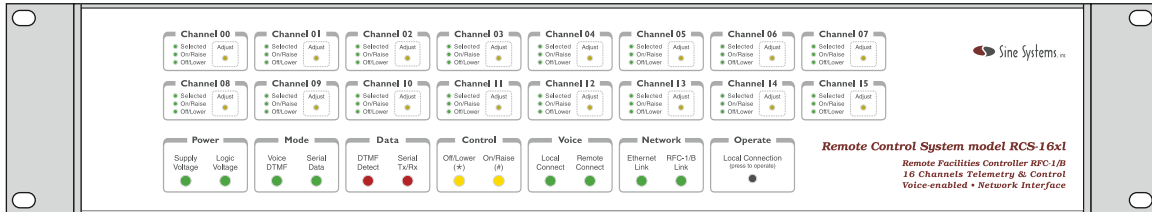

Figure 2.1; RCS-16xl front panel indicators

Status indicators are grouped by function.

- Power Supply LEDs indicate when main supply is present.
- Voice/DTMF and Serial Data indicate what communications mode is currently active. Only one of these indicators will be illuminated at a time.
- DTMF Detect and Serial Tx/Rx indicate data transmission by the appropriate method of communication. In voice mode, DTMF detect indicates the system has detected a telephone key press. In data mode, Serial Tx/Rx indicates that serial data has been transmitted or received.
- Off/Lower and On/Raise LEDs indicate when a control relay is activated.
- Local and Remote Connect indicate that a voice mode user is connected.
- Ethernet Link indicates that a network cable is connected.
- RFC-1/B Link indicates data transactions between the web server and the RFC-1/B.
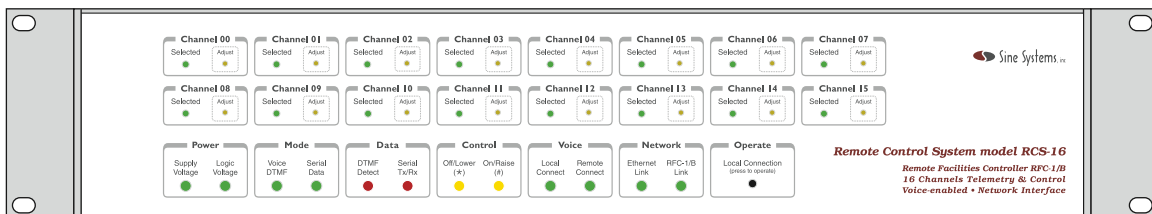

Figure 2.2; RCS-16 front panel indicators

Front panel controls include a push-button for local operation and adjustment pots for telemetry inputs. The local connection button activates the system for local operation through the telephone that is connected to the system.

2.4   Rear Panel Switches and Connections

The rear panel of the RCS series remote control system contains power and I/O connections to the device, the power supply protection fuse and the network reset switch.
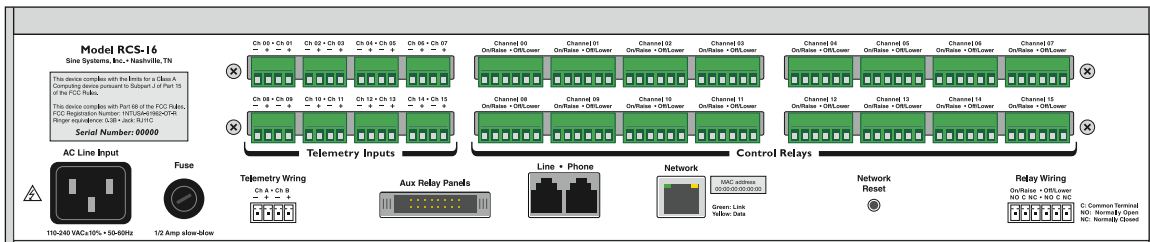

Figure 2.2; RCS-16 rear panel connectors

- Telemetry inputs are made through 4-pin pluggable screw terminal connectors. Each connector supports two inputs.
- Control relays are made through 6-pin pluggable screw terminal connectors. Each connector supports both the on/raise and off/lower connections for a single channel.
- Relay Panels uses a 16-conductor pin/plug type connector. A flat (ribbon) cable connects the RAK-2 to the RP-8 Relay Panels.
- Telephone Line/Phone connections are RJ-11C modular connectors. These are standard telephone line connectors for POTS type telephones and telephone lines.
- Network is a standard RJ-45 connector user for Ethernet connections. LEDs on the connector indicate the status of the network link and data transfer over the wired network port.
- Network Reset is a momentary switch. Unplug all cables and hold this button down for 5 seconds while powering on the reset the network settings to the factory default settings.
- Fuse is a twist-release type fuse-holder. A 5 x 20 mm fuse is installed inside this connector. The fuse value is indicated on the rear panel.
- Power Supply connection uses a standard 3-conductor IEC C13 style AC supply inlet found on PC's and most other modern commercial electronic devices. The ground protection pin should not be defeated or the ability to dissipate power surges will be compromised.

2.5   Internal Switches

The extended features of the "xl" models are enabled using DIP style switches located on the interface boards (i.e., relay panels) inside the RCS device.
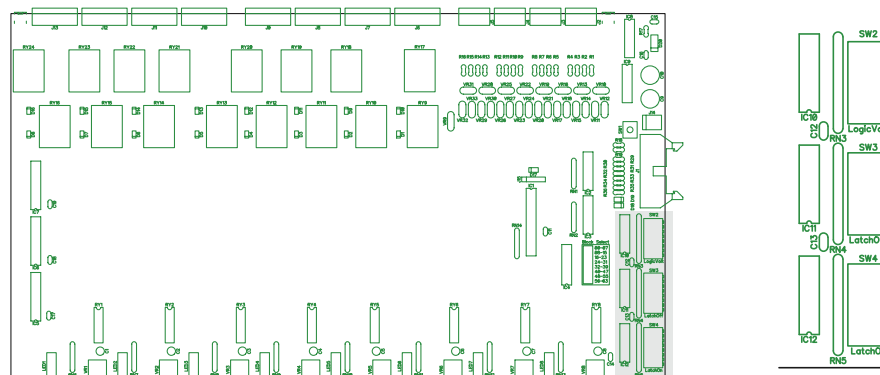

Figure 2.3; Interface board internal feature switches

2.6   Description of Features

The RCS devices have the remote control core of an RFC-1/B with extra circuitry to provide network-based features while retaining the traditional voice communications interface. These systems also have one or more interface boards that provide built-in telemetry and control I/O. Use of networking features requires local LAN support and broadband Internet access.

2.6.1   Voice Features

Since the RCS-8/16 contains all of the circuitry of an RFC-1, all voice mode features are retained from the original device. This includes the ability to take readings, operate control relays and receive alarm notifications in voice mode over a telephone line. The complete feature set of the RFC-1 can be found in the Installation and Operation manual.

2.6.2   Network Features

The main function of the network interface is to collect readings from the (embedded) RFC-1 and display that data on a website that is accessible over a local LAN and/or the Internet. The Internet connection also enables the system to connect to SMTP compatible email servers to send messages regarding system status.

Additionally, many wireless telephone carriers operate gateways between the Internet and their data networks. This allows the RCS-8/16 to send SMS text messages regarding system status.

Using a built-in SNTP client, the RCS-8/16 can connect to time-servers on the Internet and automatically adjust the clock in the RFC-1 for better long-term accuracy and daylight saving time changes.

The RCS-8/16 generates simple, clean web pages that are easily viewed from a web browser on a computer or mobile device. Web-based security is used to help keep out unauthorized users. Passwords can be assigned for both user level and administrator level.

Network settings are adjustable for compatibility with a variety of network environments. IP settings may be fixed or assigned from a DHCP server. Dynamic DNS can be used to facilitate remote access with a dynamic IP address.

2.6.3   Surge Suppression

The RCS series devices include surge suppression on both the telemetry inputs and the telephone line. A combination of fuses, metal-oxide varistors, gas arrestors and polyswitches are used to protect the system from inbound power surges. External relay panels, if used, can be protected using model SP-8/TO Surge Protector.

2.6.4   Extended Features

Models designated with "xl", specifically RCS-8xl and RCS-16xl, have additional features not present on the standard models. The interface panels used in these devices have the ability to latch any of the control relays independently and the ability to sense dry relay contacts on the telemetry inputs without an external voltage source.

2.7   Description of Controls

2.7.1   Network Reset Button

This button is located on the rear of the RCS-8/16 system. It is used to reset the network interface to the factory default settings. This button has no effect on the settings stored in the memory of the embedded RFC-1.

To reset the RCS-8/16 to factory default settings, disconnect all cables from the RAK-8/16. It is important to disconnect *all* cables including the network connection. Do not ignore this step.

Press the network reset button and hold it for 5 seconds while applying power to the RCS-8/16 system. Release the button and wait 20 seconds while the system resets the memory and restarts. Reconnect the remaining cables.

It may be necessary to cycle power and restart the system again so that the RCS-8/16 can reset the time and date in the embedded RFC-1.

2.8   Interaction with the RFC-1

As mentioned previously, the RCS-8/16 has an RFC-1 remote control embedded in it. The embedded RFC-1 is responsible for transmitter monitoring and control functions and voice communications just as in a standalone RFC-1 installation. Extra circuitry on the controller board provides the web interface and all network related functionality.

Communication between the two system processors takes place over a serial data stream. The RFC-1 takes readings and monitors for alarm conditions as usual. It periodically transmits telemetry readings to the network processor. That processor translates those readings into web pages that are viewable over the network.

Similarly, when an alarm triggers in the RFC-1 it sends data to the network processor. The data is collected by the network processor and it responds by updating the web pages and sending email as necessary.

This system is designed to place as little overhead on the RFC-1 as possible so that it can still operate normally over the voice interface while still providing information over the web interface in a timely manner.

Section 3 — Installation

⚠ **WARNING!** *Only qualified technical personnel should install an RCS-8 or RCS-16 system. An attempt to install this device by a person who is not technically qualified could result in a hazardous condition to the installer or other personnel, and/or damage to the RCS and other equipment. Ensure that appropriate safety precautions are made before installing or servicing this device.*

3.1   System Includes

The RCS remote control system package contains these items:

- Remote Control System model RCS-8/16 or RCS-8xl/16xl
- Modular telephone cable, 7 ft. long
- Ethernet network cable, 5 ft. long
- Power cable, 3 conductor IEC C13
- Rack mounting hardware
- Operation manual

All systems are fully tested before leaving the factory but damage may occur in transport. The RCS-8/16 should be inspected for obvious signs of damage or loose parts when unpacked. If damage is found, save the packing material and report it to the shipping company and the dealer from which it was purchased. Do not install the system.

The RCS remote control system is configured with an embedded RFC-1 and one or two internal relay panels. RCS-8 systems have one internal interface board and RCS-16 systems have two. For more channels, additional RP-8 relay panels may be connected externally and must be ordered separately.

3.1.1   Network Requirements

The RCS-8/16 network interface requires a broadband network gateway, commonly referred to as a broadband modem, and/or a wired router or Ethernet switch. These devices are not included as part of the RCS-8/16 package.

IP Address

Every device connected to an IP network must have a unique IP address. This address is used to reference a specific device on the network. Most networks have a DHCP server that assigns IP addresses to devices on the network. The RCS-8/16 will accept the IP address assigned to it by the DHCP server.

Many routers can be configured to assign a specific IP address to a device based on its MAC address. Alternately, the DHCP client can be disabled and the RCS-8/16 can be manually configured with a static IP address.

Port Numbers

TCP connections have a destination IP address and a port number. Different web services use different port numbers. The RCS-8/16 web server uses port 80, the standard port for HTTP connections.

Email servers use different ports depending on the server configuration. For example, secure SSL servers use a different port than servers that do not use SSL. The port number for email server connections is dependant on the email provider. In the RCS-8/16, the email port is assigned in the email configuration page.

Hardware MAC Address

The hardware MAC address is a unique hardware identifier that is assigned to the RCS-8/16 at the factory. The number is located on a label on the rear of the RCS-8/16 chassis. This number can be used to identify the RCS-8/16 by other network devices such as a LAN router. This address is assigned at the factory and cannot be changed.

3.2   Pre-Installation

This section applies to models RCS-8xl and RCS-16xl only. You may skip this section if you are not installing a system with the extended capabilities of the "xl" models.

3.2.1   Internal Feature Selection Switches

The latching control relay and internal telemetry voltage source features of the "xl" models are enabled with internal DIP style switches. Determine which of these features should be enabled on what channels before mounting the RCS-8xl or RCS-16xl in the rack.

Adjusting the extended feature switches requires removing the top cover of the RCS device. To do this, remove the two Philips-style screws that hold the top cover in place. They are located on the upper edge of the rear panel.
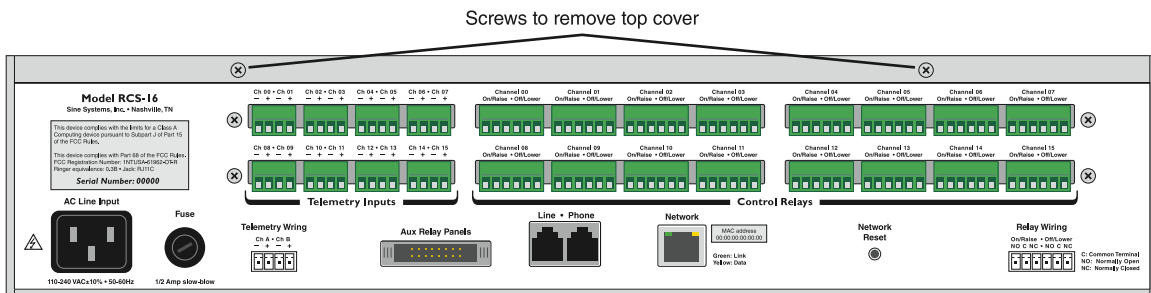

Figure 3.1; Screws to remove top cover

With the RCS-8/16xl front facing you, the option switches are located to near the front, right corner of the device.
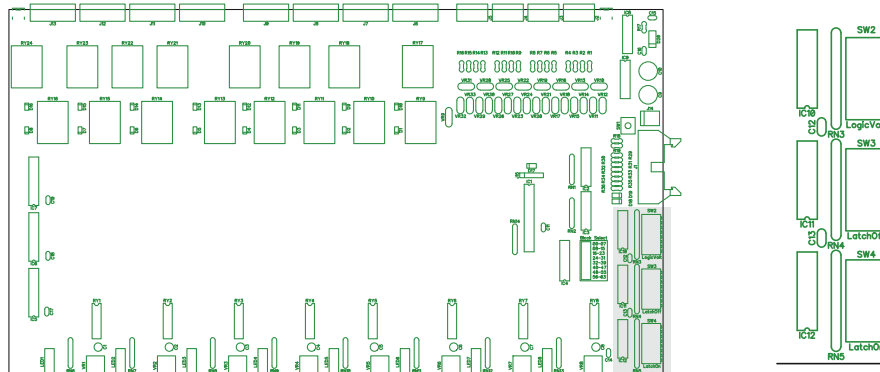

Figure 3.2; Location of feature enable switches

There are three banks of switches. Each bank corresponds to a feature.

- The bank labeled "LogicVolt" controls the internal telemetry logic voltage.
- The bank labeled "LatchOff" controls the latching of the off/lower relays.
- The bank labeled "LatchOn" controls the latching of the on/raise relays.

The switches are numbered from 1 to 8. Switches 1 through 8 correspond to channels 00 through 07 on the first interface board. RCS-16xl systems have two interface boards so switches 1 through 8 correspond to channels 08 through 15 on the second interface board. The location of switch 1 is indicated on the board.

3.2.2 DIP Switches

The DIP-switches in the RCS-8/16xl are positioned at the edge of the interface panels and have side facing switch levers. They can be activated using a small screwdriver or paperclip. There is no need to remove anything from the chassis to access the switches.
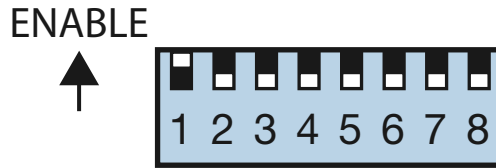

Figure 3.3; Side-accessible DIP switches

Pull a switch lever up to enable the associated feature on the corresponding channel. Push the switch down to disable the feature.

If the label on the side of the switch bank says that down is the "on" position, ignore it. The switch is intuitive like a light switch, flip the switch up to turn it "on" and enable the associated feature.

3.2.3 Latching Control Relays

The control relays in the RCS-8/16xl use momentary activation by default. Latched contacts can be enabled on any control relay on an individual basis if needed.

To enable latched relay contacts on an on/raise relay, flip the switch for the corresponding channel in the switch bank labeled *LatchOn* to the up position.

To enable latched relay contacts on an off/lower relay, flip the switch for the corresponding channel in the switch bank labeled *LatchOff* to the up position.

Disable latching relays by pressing the corresponding switch to the down position.

3.2.4 Telemetry Input Logic Voltage

It is sometimes necessary to monitor a device that provides a relay closure to indicate a status change. The telemetry inputs on the RCS-8/16xl require a voltage to sense a status change. Traditionally, this requires switching an external voltage source through the relay contacts of the external device.

The RCS-8/16xl has an internal logic-level voltage source that can be applied to any telemetry channel so that it can easily sense an otherwise dry relay contact closure.

To enable the input logic voltage on a channel, flip the switch for the corresponding channel in the switch bank labeled *LogicVolt* to the up position.

Disable input logic voltage by pressing the corresponding switch to the down position.

3.3   Installing the System

The RCS-8/16 is housed in a standard EIA two-space (2U) 19-inch rack mounted chassis. The system generates little heat and can be installed in most any convenient rack space.

3.3.1   Connect the Relay Panels (optional)

If used, external RP-8 Relay Panels attach to the RCS-8/16 on the 16 conductor pin/plug type connector labeled "Relay Panels". Simply press the flat cable connector into the relay panel connector on the RCS-8/16 taking notice to orient the keyed portions of the connectors appropriately. The latches will close in on the sides of the cable connector as it is inserted. Gently snap the latches into their locked position to secure the cable into the connector.

External relay panels are powered from the RCS-8/16 power supply. If the RCS-8/16 is installed as an upgrade an existing RFC-1 installation, *disconnect the 12-volt power supply from the RP-8 and remove it from service.*

3.3.2   Connect the Telephone Line and Local Phone

The RCS-8/16 uses standard RJ-11C modular type jacks for the telephone and line connections. The two jacks are located at the center of the rear panel of the RCS-8/16. Connect the telephone line to the jack labeled "Line" and the local telephone into the jack labeled "Phone".

When wiring the telephone line in the building, make the cable as short as possible to reduce the potential for noise pickup and surge damage. Use foil-shielded cable to reduce noise pickup in high RF environments.

3.3.3   Connect the Network

The network interface is an Ethernet connection using an RJ-45 modular type jack operating at 10 Mbits/sec. The jack is located on the rear panel and it is labeled "Network". This is the connection point to the LAN router or swtich.

Some high-speed network devices do not step down to slower speeds gracefully. On a 1 Gbits/sec or faster network, connect the RCS-8/16 to a network port that supports a slower 10 Mbit/sec.

When the RCS-8/16 network controller senses an electrical connection to a router or switch, the "Link" LEDs on both the front and rear of the RCS-8/16 will light. These LEDs indicate a functional electrical connection only. They do not indicate IP address configuration or ability to communicate over the network.

3.3.4   Connect the Power Supply

The RCS-8/16 uses a "universal" power supply that can operate from 90 to 240 volts AC at 50 or 60 Hz. There are no switches or jumpers to adjust the input voltage.

The power cable uses a 3 conductor, IEC C13 style connector on the device end and a region-appropriate connector on the wall end. Most systems are shipped with a power cable suitable for North American installation. Do not remove or disconnect the ground prong of the AC plug. Doing so defeats the internal surge protection.

The main power supply is fuse protected. The fuse is accessed from the rear panel. The fuse rating is shown on the rear panel of the RCS-8/16. If fuse replacement becomes necessary, use one of the specified type and rating. Do not make any attempt to bypass the fuse.

The RCS-8/16 does not have a main power switch. It is the nature of the device to be powered up at all times. Unplug the power cable if it is necessary to power down the system for maintenance or repair.

There are no backup batteries or super-capacitors inside the RCS-8/16. User settings are maintained in memory without backup power even when power is removed for a long period of time.

3.4   System Setup

This section describes RCS-8/16 setup options and RFC-1 options that affect the behavior of the RCS-8/16. RFC-1 options that do not directly involve the RCS-8/16 are not covered in this document. See the RFC-1 Installation and Operation manual for detailed operation and programming information for the RFC-1.

The embedded RFC-1 is setup at the factory specifically to support the RCS-8/16. Care should be taken when making programming changes to the RFC-1 so that operation with the RCS-8/16 is not disrupted. The following documentation assumes that the RCS-8/16 system is operating with the factory settings.

All RCS-8/16 settings, passwords, IP addresses, email addresses, etc., are adjusted from the web user interface. Programming changes to the RFC-1 are made with a voice connection from either a local or remote telephone. The RCS-8/16 cannot be used to adjust the RFC-1 programming. This places a security barrier between the RFC-1 and the Internet and it makes the RCS-8/16 incapable of making unexpected changes to the settings in the RFC-1.

3.4.1   Network Address Discovery

The RCS-8/16 must have a unique IP address to operate correctly on a network. The RCS-8/16 will accept an IP address from a DHCP server if there is one on the network. The default IP address is 192.168.2.2.

Local Network IP Address

It may be difficult to know the IP address that was assigned when the RCS-8/16 accepts an address from a DHCP server. The router that assigns IP addresses on the network usually provides a list of IP addresses in use. The list often includes the name and the MAC address of each device. An RCS-8/16 can be identified by the name "SINESYSTEMSRFC1" or by the MAC address on the label on the RCS-8/16.

Network Device Discovery Tool

The Network Device Discovery Tool can help locate RCS-8/16 devices on the local network. This tool can be downloaded from the Sine Systems website at www.sinesystems.com. The downloaded file installs the discovery tool. The tool polls the local network and returns the IP address of all Sine Systems devices it finds on the network.
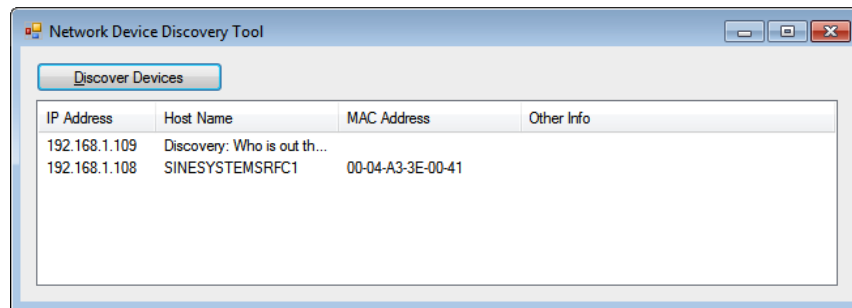

Figure 3.4; Network Device Discovery Tool

If more than one of the same device is found by the discovery tool then individual units can be identified by their MAC address. This is a globally unique hardware identifier. The MAC address is displayed on the *Status* tab of the web interface and on a label on the rear panel of the RCS-8/16.

NetBIOS Identifier

The RCS-8/16 also identifies itself to the network with the NetBIOS name "SINESYSTEMSRFC1". Some network clients, typically Windows based, may access the RCS-8/16 with the URL http://SINESYSTEMSRFC1.

3.4.2 Using the Web Interface

The examples in this section show a typical device with typical settings. Your device may be slightly different.

The default settings in the RCS-8/16 will need to be adjusted to suit individual needs. The RCS-8/16 is configured through the web interface. Configuration data is stored in nonvolatile memory and is retained without power.

The RCS-8/16 web pages require a recent generation web browser. Compatible browsers include: Internet Explorer 7 and higher, Firefox 3.5 and higher, Chrome 5.0 and higher, Opera 10 and higher, Safari 4 and higher, and Safari mobile on iPhone OS 3 and higher. Javascript is required and cookies should be enabled.

Establishing a Connection

To access the RCS-8/16 web interface, enter the network address into the address bar of your web browser. The network address can be typed into the address bar just like the name of a website. For instance, enter http://192.168.1.2 into the address bar to connect to the RCS-8/16 on the local network using the default address.
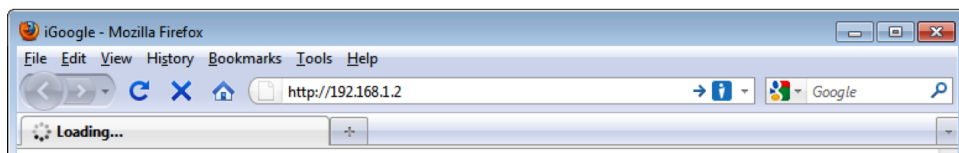
Figure 3.5; Browser address entry

Once installation is complete, you will enter the IP address of the RCS-8/16 at the remote site to connect with the device. The remote address will either be a static IP address that you have assigned to the RCS-8/16 or a symbolic link if you have are using a dynamic DNS service.

The RCS-8/16 web interface is password protected so an authentication dialog requesting a user name and password will appear. The default user name is *user* and the default password is *12345678*. User names and passwords are case-sensitive in the RCS-8/16.
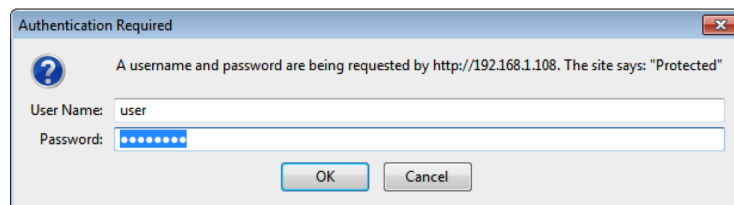

Figure 3.6; User login dialog

The system administrator can change the user name and the system passwords through the web interface. This is described in the system options below.

The RCS-8/16 does not require you to log out when you disconnect. Simply close the web browser to disconnect.

When using a tab-enabled browser, closing the tab that displays the RCS-8/16 connection halts the flow of data between the RCS-8/16 and the web browser but it does not clear any passwords that the browser has stored in its cache. This is not a flaw in the RCS-8/16 but a weakness of the basic web security protocol. The web browser must be completely closed to clear cached passwords. Be sure to close the browser completely and purge all passwords if you use a public computer to access the RCS-8/16!

Readings Page

When the correct user name and password are given, the RCS-8/16 will present the *Readings* page. This page displays the current set of telemetry readings for the connected devices.

Figure 3.7; Telemetry readings page

The upper pane displays the telemetry readings for each channel. The lower pane displays system status items. Readings are updated automatically. The time that the readings were updated is shown in the status area.

Upon installation, the system settings will probably require some adjustments. This section of the documentation continues with system settings portion of the web interface. The rest of the web interface features are described in the *System Operation* section of this document.

Mobile Device Readings Page

The mobile page displays readings with less "chrome" to improve performance and clarity on the smaller display of a typical mobile device. This page is loaded by appending "\moblie" to the network address. For example, http:\\192.168.1.2\mobile. Mobile device optimization is only available for telemetry readings.

3.5 System Settings

> **Items under the Settings menu control the appearance and behavior of the RCS-8/16. Many of the settings alter the way the RCS-8/16 functions on the network. Adjustments should be made only by personnel with knowledge of the network or with guidance from the IT staff. Incorrect settings can adversely affect the network and cause the RCS-8/16 to be unavailable on the network.**
>
> **WARNING!**

The examples in this section show a typical device with typical settings. Your device may be slightly different.

When the browser first connects to the RCS-8/16 web interface the *Readings* page is typically displayed. Select the *Settings* item from the menu bar to access the system settings.
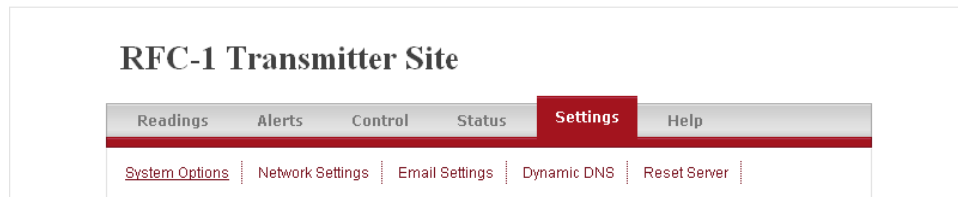

Figure 3.8; Settings menu and submenu

The RCS-8/16 web interface employs administrator level password protection in addition to the user level password protection. This stops casual users from adjusting the system settings and potentially disrupting system operation.

An authentication dialog is displayed when the *Settings* tab is selected. The default user name is **admin** and the default password is **7252**. User names and passwords are case-sensitive in the RCS-8/16.
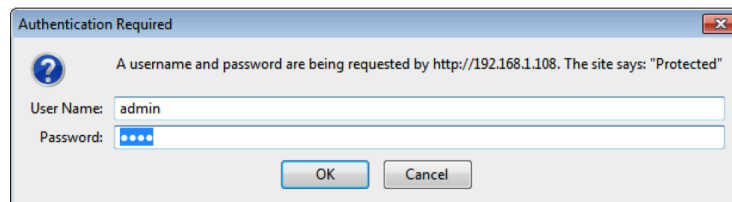

Figure 3.9; Administrator login dialog

Once administrator access has been granted, all settings pages will be available for the duration of the connection. The RCS-8/16 does not require you to log out when changes are complete but you should close the browser to clear all of the passwords from the browser cache. Remember, if you use a tabbed-enabled browser you must close the browser entirely, not just the tab, to clear the cache.

The *Settings* menu opens the *System Options* page by default. You will notice that the *Settings* menu has a submenu. System settings are grouped logically by function and each logical group has a page.

Each page of options has a Save button. Changes are not committed to memory until this button is pressed. Each page operates independent of the others so you must save changes before selecting another page from the menu.

3.5.1   System Options

Figure 3.10; System Options

Website Identifier

This is the heading that appears at the top of each page. Customize the text to help identify a particular site.

User Name / Login

This is the user name that is used to login to the RCS-8/16 web interface. Login information is case sensitive. The default user name is *user*.

User Security Code

This is the security code that is used to login to the RCS-8/16 web interface. This code can contain any characters and can be up to 16 characters long. The default user security code is *12345678*.

Administrator Security Code

This is the security code required to access the RCS-8/16 system options pages. This code can contain any characters and can be up to 16 characters long. The default administrator security code is *7252*.
RFC-1 Access Codes

Main Security Code

This code should match the RFC-1 main security code. It is used when the RCS-8/16 connects to the embedded RFC-1. It can be up to 8 digits long. The only legal values are digits 0 through 9. If the security code in the RFC-1 reads the value "ten", it is an unused digit and should be ignored—do not enter the number "10" to match what the RFC-1 says.

Basic Programming Code

This code should match the RFC-1 basic programming security code. It is used when the RCS-8/16 adjusts the clock and calendar. It can be up to 4 digits long. The only legal values are digits 0 through 9. If the security code in the RFC-1 reads the value "ten", it is an unused digit and should be ignored—do not enter the number "10" to match what the RFC-1 says.

Enable Power-up Time Set

Check this box to enable the RCS-8/16 to set the time in the embedded RFC-1 when the system powers up.

Network Time Sever

Select the network time-server in the region closest to the RCS-8/16 installation.

Time Zone

Select the preferred time zone. Internet based time servers operate on UTC. The time zone setting is used to adjust and display local time.

Daylight Saving Time

Use this to enable or disable daylight saving time adjustment. Select the automatic adjustment option to have the RCS-8/16 automatically recognize daylight saving time in the United States. This setting has no effect on the clock in the embedded RFC-1 unless the daily clock sync feature is enabled.

The RFC-1 also has a setting to automatically adjust the clock for daylight saving time. Do not enable this feature in both devices or the clock will be adjusted twice and will show incorrect time as a result.

Sync Clock Daily

Check the box to enable the daily clock sync feature. The RCS-8/16 will set the clock in the embedded RFC-1 daily. This helps minimize clock drift over time. Enabling this feature also allows the RCS-8/16 to adjust the RFC-1 clock for daylight saving time.

3.5.2   Network Settings

Figure 3.11; Network Settings

Website Server Port

Services on the Internet operate over a specific port. Web servers use a protocol known as HTTP that typically operates on port 80. This is the default setting for the RCS-8/16.

If port 80 is already in use by another server on the local network then one of the devices must be assigned to operate on a different port. The alternate port number should be selected so as not to interfere with other network services. Port 8080 is often used as an alternate port for web servers.

When an alternate port is used, the port number must be specified in the browser address as part of the URL. Otherwise the browser assumes that the default port, 80, is used. For example, if port 8080 is used and the address is 127.0.0.1 then the URL would be: http://127.0.0.1:8080. The addition of ":8080" indicates to the browser that an alternate port is in use.

Website Interface Color

This control lets you select the RCS-8/16 interface color scheme. Color scheme selection is stored as a browser cookie so cookies must be enabled for this feature to work. Because this setting is stored on the local device and not in the RCS-8/16, different color schemes can be used on different devices for a single site.

Enable Static IP Settings

Check this box to enable manual configuration of the RCS-8/16 network settings. When the box is not checked, the RCS-8/16 will accept IP settings from a DHCP server on the network. This box is unchecked in the default settings.

All items must be manually configured when static IP settings are enabled. The secondary DNS server is optional.

IP Address

This IP address will be assigned to the RCS-8/16 network interface. It must be provided by your network administrator or by your Internet service provider.

IP Subnet Mask

The subnet mask depends on the IP address and is provided by your network administrator or by your Internet service provider.

Gateway IP Address

This is the address of the device through which the RCS-8/16 communicates with the network and/or the Internet. It is provided by your network administrator or by your Internet service provider.

Primary DNS Server

The IP address of the primary DNS server is provided to you by your network administrator or by your Internet service provider.

Secondary DNS Server

The IP address of the secondary DNS server is provided to you by your network administrator or by your Internet service provider. This item can be considered optional if only one DNS server address is provided.

3.5.3 Email Settings

The RCS-8/16 can translate alarm messages from the embedded RFC-1 and send notification by email when an alarm occurs. The RCS-8/16 sends the message through an Internet email server so this feature requires the address and login credentials for an email server. This data must be supplied by your network administrator or by your email service provider.

Figure 3.12; Email Settings

Enable Email Notification

Check this box to enable email and text message notifications. Uncheck it to disable email and text notifications. Voice alerts are always generated by the embedded RFC-1. This setting has no effect on voice alerts.

Email Delivery Address

This is the address to which email alerts will be sent. Enter the email address of the message recipient here.

Text Message Address

This is a second email address to which email alerts will be sent. It can be any email address but it is often used to store the address of the email to SMS gateway to which text messages can be delivered. Entering an appropriate address causes the RCS-8/16 to send a text message when the system generates an alarm.

Most wireless phone providers operate servers that can translate a properly coded email message and forward to a phone as an SMS text message. The email address is typically *your_number@SMS_gateway*. For instance, if your mobile phone number is (012) 345-6789 and the carrier specific gateway is SMSgateway.internet then the email address would be 0123456789@SMSgateway.internet.

SMS gateway information should be available from your wireless phone service provider. SMS gateways can also be found by searching the web. Use the term "SMS gateway" and your phone service provider name.

Email Sender Address

This is the address from which email alerts will be sent.

Outgoing SMTP Server

This is the name of the mail server through which email alerts are sent. This data is supplied by your email provider.

Send Account User Name

This is the user name of the account from which email alerts will be sent. It is used to login to the email host server.

Send Account Password

This is the password of the account from which email alerts will be sent. It is used to login to the email host server.

SMTP Server Port

The standard SMTP server port is 25 but some providers use port 587. Other ports may be used. SSL secure SMTP typically operates on port 465. Most email servers operate over secure connections to minimize abuse by spammers. This information is supplied by the email provider.

Use SSL Authentication

Check this box to use of SSL encryption for authentication. Most email providers require SSL encryption. This information is supplied by the email provider.

3.5.4 Dynamic DNS

Dynamic DNS service is a way to locate a device on the Internet that does not have a static address. An account with a dynamic DNS service provider is required to use this feature. The account login credentials are stored in the RCS-8/16 and it contacts the dynamic DNS server periodically and updates the IP address.

When using dynamic DNS service, connection to the RCS-8/16 over the Internet is made using a link provided by the dynamic DNS provider. The dynamic DNS server locates the address of the RCS-8/16 and provides the address. This mechanism allows a device with a dynamic IP address to be located as if it had a static address.

If the RCS-8/16 is installed behind a NAT router, and in most cases it should be, then the router must perform the dynamic DNS service. If multiple routers are in service then the router that is connected to the Internet should perform dynamic DNS updates. Many inexpensive routers are capable of performing this function.

Figure 3.13; Dynamic DNS settings

Enable Dynamic DNS

Check this box to enable the internal dynamic DNS client.

Dynamic DNS Provider

Select the dynamic DNS provider from this list. Only the providers in the list are supported.

Dynamic DNS Host Name

This is the name you have registered with the dynamic DNS service provider.

Account Login / User Name

This is your account name on the dynamic DNS server.

Account Password

This is your account password on the dynamic DNS server.

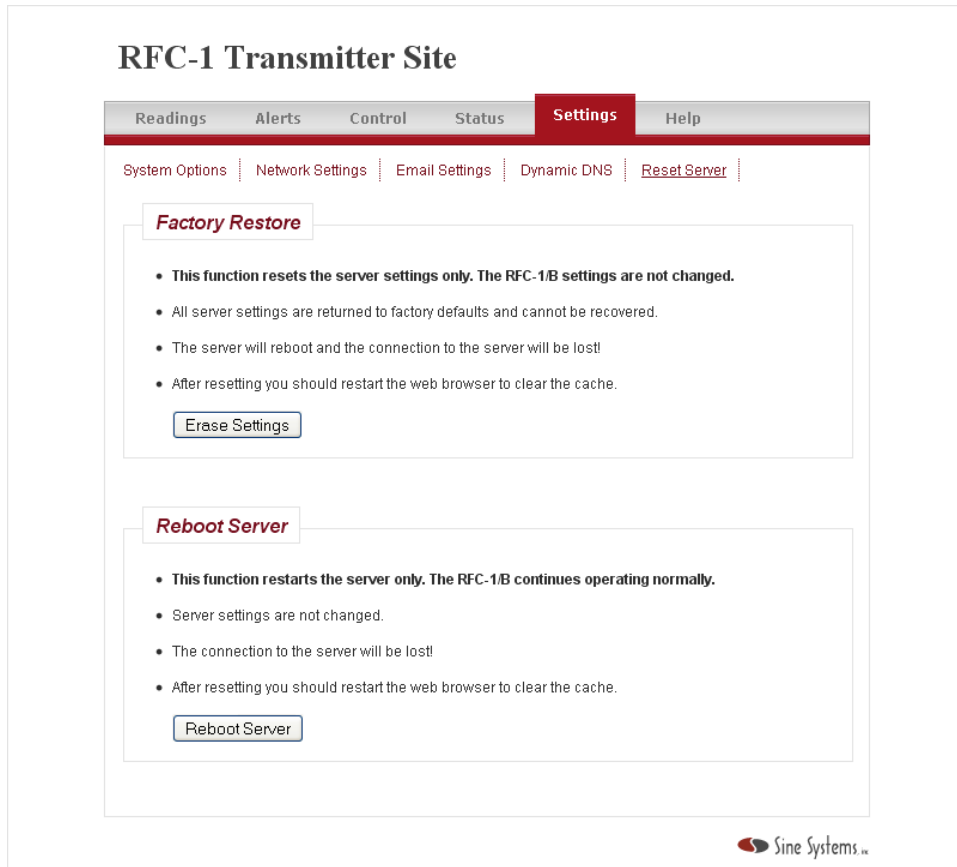### 3.5.5   Reset Server

Figure 3.14; Reset Server page

Factory Restore

Click this button to reset the RCS-8/16 to factory settings. Please read all warnings before clicking the button. The settings of the embedded RFC-1 are not altered.

Reboot Server

Click the button to reboot the RCS-8/16 server. Please read all warnings before clicking the button. The embedded RFC-1 is not reset.

3.5.6   Setup and Restore Embedded RFC-1
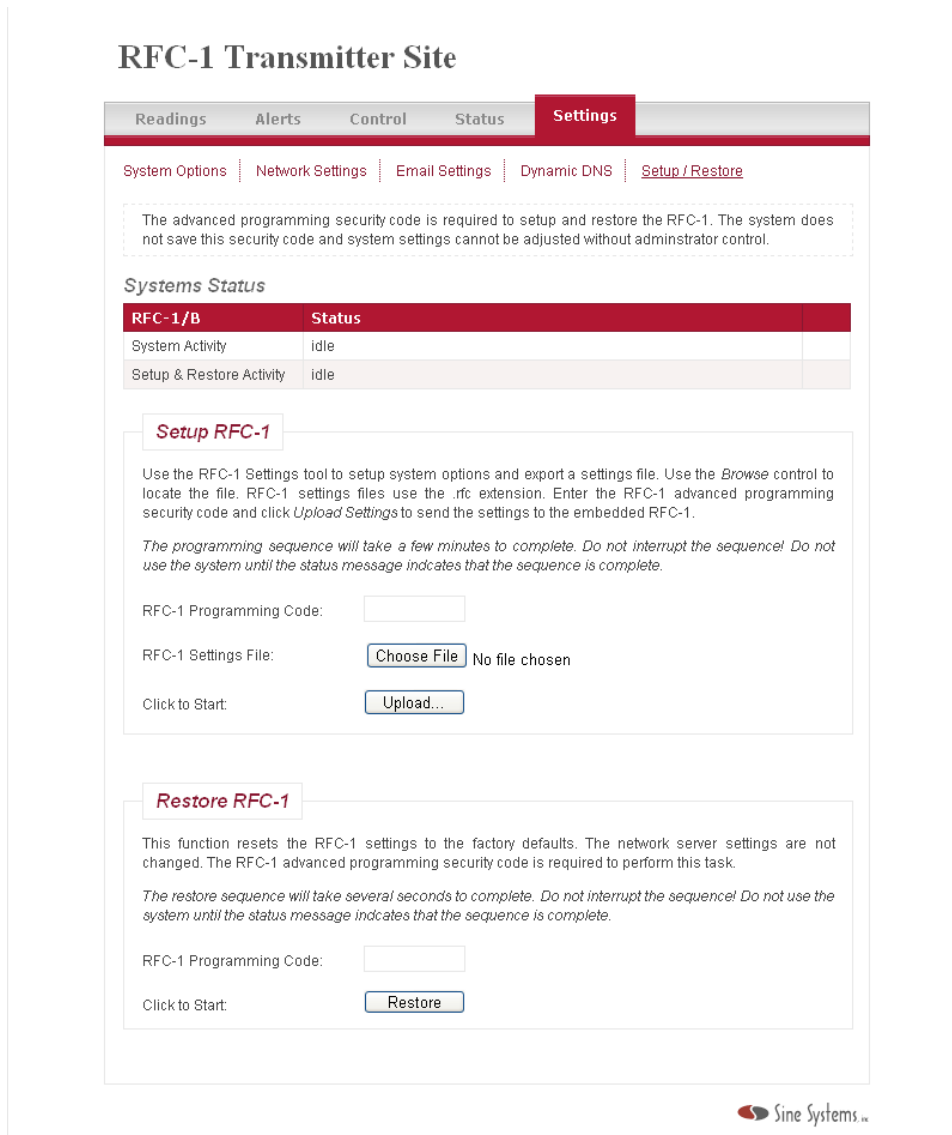
Figure 3.15 Setup and restore embedded RFC-1 page

Both of these functions require the advanced programming security code for the embedded RFC-1. This code is not saved by the RCS-8/16.   The RCS-8/16 can only perform programming tasks under the control of a system administrator.

Setup RFC-1

Use this function to upload new settings to the embedded RFC-1. Use the Windows-based RFC-1 Settings Tool to create a site profile that contains telemetry channel settings, alarms, etc. Export an .RFC data file from the program and upload the file to the RCS-8/16 with these controls. The RCS-8/16 will use the data to program the embedded RFC-1.

Restore RFC-1

Use this function to reset the embedded RFC-1 to the factory settings. Once started, this function cannot be interrupted and the previous settings cannot be recovered.

3.6 RFC-1 Settings

⚠ **WARNING!** *Please carefully consider the information in this section before making programming changes to the embedded RFC-1. Most settings can be programmed as usual. Some items have special considerations and a few settings, such as those that involve the data protocol, should not be altered. Ignoring the recommendations below may cause erratic or undesired system behavior.*

3.6.1 Special Considerations when Programming the Embedded RFC-1

The RCS-8/16 is designed to require as few resources as possible from the embedded RFC-1. Supplying data to the web server is a demanding task that imposes somewhat on the RFC-1 processor. The factory settings are selected to balance the needs of the RCS-8/16 with the overall functionality of the embedded RFC-1.

There are some settings that should not be changed because they are required for the RCS-8/16 to function as designed. There are other features, such as telemetry alarms, that can be used normally but are enhanced by setting in a way that takes full advantage of the RCS-8/16.

3.6.2 How the System Works

A brief description of how the RCS-8/16 interacts with the embedded RFC-1 should help you understand how the system works and why the settings discussed here are critical.

The RCS-8/16 does not maintain a constant connection to the embedded RFC-1. If it did, the RFC-1 would be unable to accept voice mode calls or scan for alarms and this would severely limit the functionality of the device. Instead, the RFC-1 sends a set of readings to the RCS-8/16 at a predetermined interval. The interval is adjustable and is short enough so that readings update in a timely manner but not so short that the RFC-1 cannot perform other functions.

Telemetry alarms, if used, work the same as in a standalone RFC-1 installation. The difference between the traditional RFC-1 settings and the RCS-8/16 settings is in the action sequence that is triggered when an alarm occurs. The action sequence starts by sending set of telemetry readings to the RCS-8/16 then it performs other tasks as needed.

Even without the specific action sequence, the RCS-8/16 will indicate the alarm condition as part of the telemetry readings. The extra reporting activity informs the RCS-8/16 of the alarm state and this provides the mechanism for features like email alerts.

3.6.3 Affected RFC-1 Features and Options

The RFC-1 local control button is disabled during channel scans. This is a limitation of the hardware communication scheme used by the RP-8 relay panel. It is rarely noticeable in standalone RFC-1 systems because channels scans are short and infrequent. The RFC-1 must scan channels much more frequently to service the RCS-8/16.

A side effect of the increased channel scanning is that the system may be unable to immediately respond to a press of the local control button. The work around is to wait a few seconds and press the button again. This is a minor issue because the RCS-8/16 is typically operated remotely and this does not require use of the local control button.

Other RFC-1 features and adjustments that directly influence the RCS-8/16 are discussed below. All other RFC-1 settings are documented in the RFC-1 *Installation and Operation Manual*.

Features are listed alphabetically in the following discussion. The presentation order has no significance on the importance of each feature.

Action Sequence at Power-on

This feature is also referred to as the power failure alarm in the RFC-1. This feature activates an action sequence when the RFC-1 powers on. Any valid action sequence can be triggered.

Traditionally this feature is used to have the RFC-1 place a phone call that warns of a power failure. This function also sends a data message to the RCS-8/16 so that it can display an alert in the web interface. The data alert should be a part of any user-programmed power-on action sequence. It is typically the first instruction in the action sequence.

This feature is programmed at address 1008 in the RFC-1. Action sequence 10 is used in the RCS-8/16 factory settings. The action sequence sends a data alert and then makes a warning phone call. It is somewhat safe for advanced users to adjust this feature in RCS-8/16 systems.

Clock/Calendar

The time and date must be set for the telemetry auto-scan to work. The RCS-8/16 attempts to set the RFC-1 clock on power up in the factory settings. If the RFC-1 clock stops, so do automatic data updates.

Communications Mode

The communications mode determines the preferred method for incoming connections. The RFC-1 operates over voice and data connections and it will switch between the modes as needed but it cannot do both at the same time.

When the RCS-8/16 is used, the RFC-1 must idle in data mode so that the RCS-8/16 can establish a connection as needed. This does not exclude the use of voice calls because the RFC-1 can switch to voice mode as a secondary option.

The communications mode is programmed at address 1002. The correct setting is voice mode primary with data mode secondary and dedicated control mode is disabled. This setting should not be changed under any circumstances in RCS-8/16 systems.

Date/time trigger

The RFC-1 uses date/time triggers to initiate events automatically by the clock and calendar. When the conditions of a date/time trigger are met, an action sequence is triggered to perform a series of events.

The RCS-8/16 requires the embedded RFC-1 to deliver updated telemetry readings every minute. This places a significant demand on the RFC-1 processor. Be careful not to overload the processor by programming additional date/time triggers that operate frequently.

Avoid programming other events that occur at minute intervals. Timed events perform functions such as adjusting transmitter power levels that occur daily should work normally as long as they are programmed correctly.

It is safe to use this feature as needed as long as the conditions described above are met.

Daylight Saving Time Auto-adjust

As of firmware version 6 the RFC-1 can perform automatic clock adjustment for daylight saving time. The RCS-8/16 also performs this function. Do not enable automatic clock adjustment for daylight savings time in both devices or the time will change two hours instead of one hour.

This feature is typically controlled by the RCS-8/16 and not the embedded RFC-1. The RCS-8/16 can sync time with an Internet time-server for enhanced accuracy.

This feature is programmed at address 1017 in the RFC-1. It is disabled in the factory settings in RCS-8/16 systems. It is safe to enable or disable this feature according to user preferences as long as the conditions described are met.

Inactive System Timeout

The inactive system timeout feature stops the RFC-1 from leaving a user connection active indefinitely. It operates the same on both data and voice connections. The RFC-1 disconnects when a specified period of inactivity passes as a safety precaution.

The RCS-8/16 does not receive telemetry updates when there is an active connection with the RFC-1 in either voice or data mode. This setting should be as short as possible so that the system does not appear to be frozen or otherwise unresponsive to web interface users.

This feature is programmed at address 1000 in the RFC-1. It is set to 30 seconds in the factory settings in RCS-8/16 systems. Adjusting this feature is not recommended in RCS-8/16 systems.

Serial Data Protocol and Baud Rate

Data passes between the embedded RFC-1 and the RCS-8/16 through a serial data connection. The data protocol and baud rate has several settings. The appropriate setting is 9600-8-N-1 for RCS-8/16 systems.

This feature is programmed at address 1005 in the RFC-1. This setting should not be changed under any circumstances in RCS-8/16 systems.

Telemetry Alarm System Enable

The telemetry alarm system enable is a master on/off switch for all of the telemetry alarms. When telemetry alarms are disabled then the RCS-8/16 does not receive telemetry alarm messages from the embedded RFC-1. Telemetry readings are updated normally and alarm conditions will be reflected in the telemetry readings.

This feature is programmed at address 1009 in the RFC-1. It is also adjusted using the command "82" in voice mode. It is disabled in the factory settings in RCS-8/16 systems. It is safe to enable or disable this feature as needed.

Telemetry Alarm Settings and Action Sequences

Telemetry alarms are scanned the same in systems with the RCS-8/16 interface as they are in stand-alone RFC-1 systems. The difference between the traditional RFC-1 settings and the RCS-8/16 settings is in the action sequence that is triggered when an alarm occurs.

In stand-alone systems the default alarm behavior is to place phone calls and this is still an option in RCS-8/16 systems. Voice mode functionality is not lost with the RCS-8/16. When an alarm occurs the embedded RFC-1 should send an alert message to the RCS-8/16 and then place voice mode phone calls if necessary.

The order of the events is critical because the RFC-1 cannot send data to the RCS-8/16 while telephone calls are in progress. Telephone calls take a significant amount of time to complete. Placing calls first imposes an unacceptable delay between the time an alarm occurs and the time the RCS-8/16 can display an alert message or send an email.

The fixed-programming action sequence 10 sends the appropriate data message and then places alarm calls. It is the default action sequence for alarms in the RCS-8/16.

If a user-programmed action sequence is used, site-specific tasks (relay closures, etc.) are normally placed between the data message and the phone calls. To do this, begin the action sequence with the command 8-8, then insert the site-specific commands, and finish the sequence with the command 9-0.

It is safe to program telemetry alarms as needed as long as the conditions above are met. Violating these conditions will not harm the system but the RCS-8/16 may not display alarm messages or send email alerts appropriately.

Telemetry Auto-scan Data Interval

The telemetry auto-scan data feature triggers data updates telemetry data from the embedded RFC-1 to the RCS-8/16. This setting enables telemetry updates and lets the RFC-1 calculate the appropriate delay between updates. The setting is based on the number of relay panels that are installed.

This feature should not be disabled or the telemetry readings will not update.

The telemetry auto-scan data interval is programmed at address 1012 in the RFC-1. The factory setting is appropriate for systems with up to 16 telemetry channels. It is safe to adjust this feature but only if more than two relay panels are installed on the system.

Telemetry Auto-scan Stop Channel

The RFC-1 auto-scan sequence sends telemetry data to the RCS-8/16. The scan sequence always begins with channel 00 and it ends with the auto-scan stop channel.

The stop channel is adjustable. It is normally set the last channel that is in use. There is no reason to scan for telemetry data on unused channels.

The auto-scan stop channel is programmed at addresses 1010 and 1011 in the RFC-1. The factory setting is channel 07 in most RCS-8/16 systems. The factory setting may be different in pre-configured systems. It is safe to adjust this feature as needed.

Telemetry Leading Zero Suppression

When enabled, the leading zero suppression feature removes zeros from telemetry readings that are not significant to the number. This produces numbers that are more natural looking when displayed on web pages and more natural sounding when spoken. Zeros that are significant to the value of the number are not suppressed.

This feature is programmed at address 0998 in the RFC-1. It is enabled in the factory settings in RCS-8/16 systems. It is safe to enable or disable this feature according to user preferences.

Telemetry Settling Time

The telemetry settling time is a brief delay imposed by the RFC-1 when a channel is selected. The delay gives the sample voltage time to stabilize before the processor samples it. This is a global setting that affects all channels.

This setting is relevant to the RCS-8/16 because if the delay is lengthened it accumulates across all of the channels in the scan sequence. If the duration of the scan sequence increases significantly then the time between scans must be lengthened to accommodate. This requires altering the timed event that initiates the telemetry scan. See the discussion of date/time triggers for more information.

Telemetry settling time is programmed at address 0997 in the RFC-1. It is set to 0.4 seconds in RCS-8/16 settings. The factory setting is appropriate in most cases. It is safe to adjust this setting according to user preferences as long as the conditions described are met. Very long delay settings should be avoided.

3.6.4   Programmable Features

Minor programming adjustments are required in the embedded RFC-1 to enable some features of the RCS-8/16. The factory default settings are selected to take advantage of the RCS-8/16 without being overly demanding on system operators or system resources.

Automatic Telemetry Logging by Email

The RCS-8/16 can send email notifications of alarms by enabling that feature in the RCS-8/16 web interface. This can also be used to generate a message at programmed intervals with a little additional programming in the embedded RFC-1. This effectively makes the system generate a log of telemetry readings automatically by email.

The following programming example sets up a timed event in the embedded RFC-1 to send a set of telemetry readings once every hour, on the hour, on every day of every month. The preset action sequence 11 is used to perform the task. In this example we use date/time trigger 1 but any available date/time trigger will work. Starting at address 0632 the programming is shown below.

Addr	Description	Section	- Programming - Default	Current	Alternate Use / Notes
0632	Date/time trigger 1: action sequence	6.6.4	0	11	Alarm block 1: block indicator
0633	Date/time trigger 1: month	6.6.4	0	15	Alarm block 1: alarm
0634	Date/time trigger 1: day - value 1	6.6.4	0	15	Alarm block 1: month
0635	Date/time trigger 1: day - value 2	6.6.4	0	15	Alarm block 1: day of week
0636	Date/time trigger 1: hour - value 1	6.6.4	0	15	Alarm block 1: start hour - V1
0637	Date/time trigger 1: hour - value 2	6.6.4	0	15	Alarm block 1: start hour - V2
0638	Date/time trigger 1: minute - value 1	6.6.4	0	0	Alarm block 1: end hour - V1
0639	Date/time trigger 1: minute - value 2	6.6.4	0	0	Alarm block 1: end hour - V2

This tells the system to trigger action sequence 11, every month, every day, every hour on the hour. The RCS-8/16 will receive the data and interpret it as an alarm and respond accordingly.

This is not technically a telemetry alarm but we are taking advantage of the ability of the RCS-8/16 so send an email when an alarm exists. To avoid ambiguity, the email subject line is different when the RCS-8/16 sends an email based on a timed event versus that of a true telemetry condition.

Perhaps an email every hour is too much data. A simple change to the time trigger sets the event to occur every 2 hour, on the hour, on every day of every month. Again, in this example we use date/time trigger 1 but any available date/time trigger will work. Starting at address 0632 the programming is shown below.

Addr	Description	Section	- Programming - Default	Current	Alternate Use / Notes
0632	Date/time trigger 1: action sequence	6.6.4	0	11	Alarm block 1: block indicator
0633	Date/time trigger 1: month	6.6.4	0	15	Alarm block 1: alarm
0634	Date/time trigger 1: day - value 1	6.6.4	0	15	Alarm block 1: month
0635	Date/time trigger 1: day - value 2	6.6.4	0	15	Alarm block 1: day of week
0636	Date/time trigger 1: hour - value 1	6.6.4	0	15	Alarm block 1: start hour - V1
0637	Date/time trigger 1: hour - value 2	6.6.4	0	2	Alarm block 1: start hour - V2
0638	Date/time trigger 1: minute - value 1	6.6.4	0	0	Alarm block 1: end hour - V1
0639	Date/time trigger 1: minute - value 2	6.6.4	0	0	Alarm block 1: end hour - V2

This tells the system to trigger action sequence 11, every month, every day, every 2 hours on the hour. The event interval can be even longer by changing the 2 at address 0637 to a 3 or a 4. This will trigger a set of readings every 3 hours or every 4 hours.

All of these examples require only a single date/time trigger to be programmed in the embedded RFC-1/B.

Section 4 — Operation

The behavior described and the examples shown in this section are from a typical device with factory settings. Your device may appear or behave slightly different depending on firmware version and system settings.

4.1   Readings Tab

The *Readings* tab is presented when the correct user name and password are given. This tab displays the current set of telemetry readings for the connected devices.

Figure 4.1; Readings tab

The upper pane displays the telemetry readings for each channel. The lower pane displays telemetry status information. Readings are updated automatically.

The Readings tab has no controls, aside from the menu, and in a secure environment it should be reasonably safe to leave this tab displayed to monitor the site. Keep in mind that readings are updated continuously as long as there is a browser connection. This may be an issue if a metered broadband service plan is used.

4.1.1   Telemetry Readings

The RFC-1 supports a maximum of 64 telemetry channels but most systems do not use all of the available channels. Channels that are not used, and therefore are not updated, are displayed with a message that indicates that the channel is unused.

The *Telemetry Readings* table scrolls independently of the page. This table shows data for about 16 channels on most displays. This is the data from two fully loaded RP-8 relay panels.

4.1.2   Telemetry Status

The time that the telemetry readings were updated is shown in the status area. This data comes from the embedded RFC-1. It is refreshed automatically every time the readings are updated by the embedded RFC-1.

The status area displays data from the most recent telemetry alarm if it exists in the log. This provides a convenient way to monitor system status from the *Readings* tab. This data comes from the telemetry alarm log that is described in detail in the next section.

4.2   Alerts Tab

The Alerts tab contains a list of recent critical system events. Telemetry alarms generated by the RFC-1 occupy the upper pane and a log of recent system events occupies the lower pane. The Alerts tab has a single control; a clear button erases all telemetry alarms and system events from the log.

Figure 4.2; Alerts tab

4.2.1   Telemetry Alarms

The embedded RFC-1 sends a message to the RCS-8/16 when a telemetry alarm occurs. The RCS-8/16 stores the most recent events and displays them in the *Telemetry Alarms* portion of the *Alerts* tab.

Telemetry alarms are displayed with the time that the event occurred. This information comes from a time stamp that the embedded RFC-1 delivers with the telemetry data. Given that the RCS-8/16 can be viewed from a browser located almost anywhere, it is possible that the time shown here does not agree with local time.

The alarm data is not automatically cleared when the alarm condition returns to normal. The embedded RFC-1 is monitoring for alarms and it only sends a message when the alarm triggers. The RCS-8/16 has no way to know that the alarm is cleared and reset the display automatically. The alarm event data is displayed until a user clears the log.

4.2.2   System Events

The RCS-8/16 logs certain events aside from those that are delivered by the embedded RFC-1. This includes changes to system settings and daylight saving time changes. These system events are display in a separate status area of the *Alerts* tab.

4.3   Control Tab

Figure 4.3; Control tab

The control relays on the RP-8 relay panel can be operated through the RCS-8/16 web interface. The RCS-8/16 will connect to the embedded RFC-1 and issue the appropriate commands.

The RCS-8/16 does not maintain an active connection to the embedded RFC-1 at all times. Doing this would interfere with the ability of the RFC-1 to operate effectively. Voice mode connections would not be possible and the alarm system would be ineffective.

To operate the control relays the RCS-8/16 must first establish a communications with the embedded RFC-1. The RCS-8/16 must connect and authenticate using a security code, as would any user of the RFC-1. Once connected, the RCS-8/16 will send appropriate commands to operate the controls and disconnect.

Operating the RFC-1 control relays requires entry of a control security code. The RCS-8/16 must authenticate using this security code just like any other user. The control security code must be given *every* time a control command is issued. The control security code is never stored in the RCS-8/16 memory.

The RCS-8/16 is not able to perform any of the RFC-1 control functions without user intervention. The RFC-1 can, however, perform any of its programmed functions independently of the RCS-8/16.

4.3.1   Programmed Control

The *Programmed Control* area of the *Control* tab sends command to the embedded RFC-1 to activate one of the action sequences. An action sequence is a programmed sequence of commands stored in the RFC-1 memory to perform a specific task. Common tasks include turning a transmitter on, turning it off or changing the power.

To start an action sequence, enter the control security code in the appropriate area of the web interface. Select the action sequence from the selection box and click the start button.

Watch the status area for progress updates. Do not issue a command until the system indicates that it is idle.

4.3.2   Manual Control

The *Manual Control* area of the *Control* tab is similar to programmed control except that a single channel command is issued instead of a programmed sequence of commands. Control relays are momentary in most RFC-1 systems so a single command is all that is required to operate a control relay.

To manually activate a control relay, enter the control security code in the appropriate area of the web interface. Select the channel number from the selection box and click the appropriate button to activate either the on/raise or off/lower relay. Watch the Control Status area for messages.

Watch the status area for progress updates. Do not issue a command until the system indicates that it is idle.
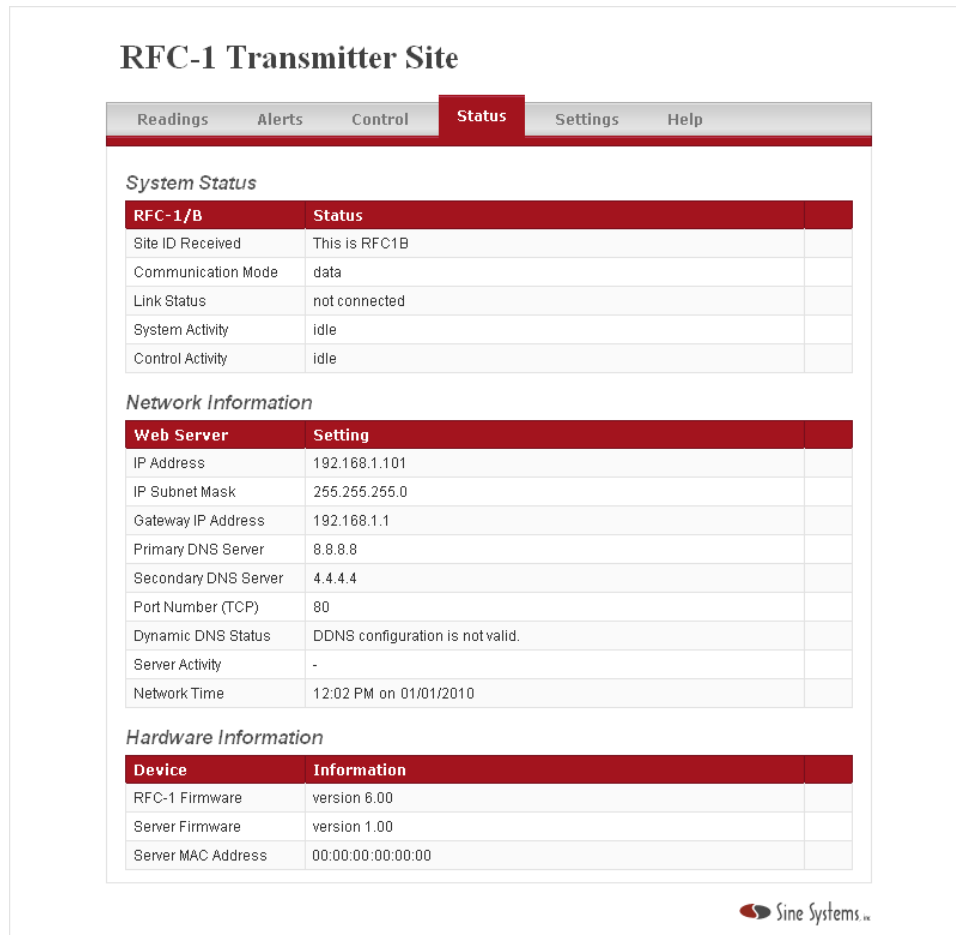
4.3.3   Control Status

This area of the *Control* tab displays messages about the progress of control commands. It also tells you when the system is busy receiving data from the embedded RFC-1. The RFC-1 will not accept control commands when it is updating the telemetry readings. Do not click any of the command buttons if the status indicator displays a "please wait" message. The activity indicator will display "idle" when the RFC-1 is available to accept commands.

4.3.4   Telemetry Readings and Status

The Telemetry Readings and Status areas of the *Control* tab are the same as those on the *Readings* tab. They provide a convenient way to monitor the system for changes while controls are operated.

4.4   Status Tab

The Status tab displays a summary of the operational status of the RCS-8/16 system. Information is categorized into three major categories: system status, network information and hardware information. The tab has no controls.

Figure 4.4; Status tab

4.4.1   System Status

The working state of the embedded RFC-1 is shown in this area. Interactions between the RCS-8/16 and the RFC-1 are indicated with messages displayed in this area.

4.4.2   Network Information

The network settings and the status of optional network services are displayed in this area.

4.4.3   Hardware Information

Information that is specific to the hardware is displayed here. This includes firmware revisions for both the embedded RFC-1 and the RCS-8/16.

4.5   Settings Tab

The *Settings* tab provides access to the various system settings. The settings are broken down logically and are displayed on multiple pages. The pages are accessed through a submenu on the *Settings* tab.
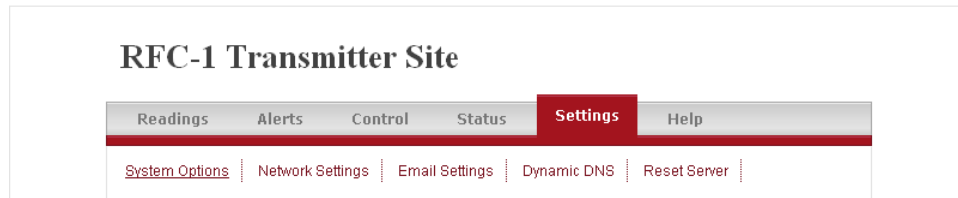

Figure 4.5; Settings tab and submenu

All of the available settings are described in Section 3 of this document.

Secton 5 — Remote Access

⚠ **WARNING!**

The RCS-8/16 must be accessible from the local network before attempting to access it remotely over the Internet. Internet access adds an additional level of routing complexity that should be avoided until basic system operation has been established.

5.1   Introduction

This brief guide is intended to supply enough information to set up a relatively simple connection between the RCS-8/16 and an Internet-connected PC or mobile device. This guide is not a substitute for a knowledgeable IT professional.

This manual is not intended to teach IP networking and routing nor is it intended to replace your IT department. Your IT professional should be consulted before you attach any device to the network.

Sine Systems can answer technical questions involving operation of the RCS-8/16. Questions regarding router configuration and networking should be directed to your IT department.

5.2   IP Networking Primer

The following is an oversimplification of how the Internet works. If you need more details, there are plenty to be found on the web. This primer is a crash course in networking that will provide you with just enough data to be dangerous.

The Internet works using IP Address and ports. Every device on the Internet has an IP address. The address is used to pass data to and from that device. Data travels though ports. Ports are a convention to help route data.

5.2.1   Data Ports

Ports are used to identify the type of data and route it to the appropriate destination. The Internet works by agreeing on standard port numbers for certain types of data traffic. Specifically, web pages are typically served over port 80. This is the port we will use in this guide since it is focused on making the RCS-8/16 website visible on the Internet.

Be aware that port 80 is used to deliver web traffic by convention but this does not mean that other ports cannot be used. In fact, if there is another web server on the local network that uses port 80 then another port must be used. This involves finding an unused port, 8080 is often selected, and setting the RCS-8/16 to use that port.

5.2.2   Public and Private IP Addresses

There are two types of IP addresses: public and private. Public IP addresses are routable, can be used, on the Internet. Private IP addresses can be used only on local networks.

Most local networks uses private IP addresses so data on these networks cannot be routed over the Internet. Data on these networks must be translated to a public IP address before it can pass over the Internet. This is called network address translation, NAT, and it is one of the functions performed by a router.

Why is this important? Because the RCS-8/16 is typically installed on a local network using private IP addresses. Any data that the RCS-8/16 generates can be seen on the local network but cannot pass over the Internet, cannot be viewed from a remote location, until the data is translated to a public IP address by a router.

5.2.3 Port Forwarding

To view the RCS-8/16 website over the Internet, a router must pass requests for web page data from the Internet to the RCS-8/16 and send the requested data to the remote browser over Internet. To do this, the router must be setup to pass data on port 80 to the private IP address of the RCS-8/16. This is called port forwarding.

5.2.4 Static LAN IP Address

Port forwarding requires the router to know the private IP address of the RCS-8/16. Once assigned, the IP address must not change or port forwarding will fail. If the IP address of the RCS-8/16 changes then the router will not be able to forward data between the RCS-8/16 and the Internet. This type of address is a static IP address.

5.2.5 Static WAN IP Address

A static IP address on the LAN allows the router to locate the RCS-8/16 on the LAN when an incoming connection is requested but what about the IP address on the Internet side of the router? In other words, what address does a remote user request in order to connect to the router that services the RCS-8/16?

If the router that services the RCS-8/16 is assigned a static IP address from the broadband service provider then simply enter that IP address in the web browser. The router will forward the http request to the RCS-8/16 according to the port forwarding settings. Most service providers will assign a static IP address for a small additional fee.

5.2.6 Dynamic WAN IP Address

If the router that services the RCS-8/16 is not assigned a static IP address from the broadband service provider then the IP address is dynamic. In this case the WAN IP address of the router will change any time the broadband service provider chooses to do so. The workaround is to use a dynamic DNS service to track the changes.

5.2.7 Dynamic DNS

Dynamic DNS is a service that associates a name with an IP address. Associating names with IP addresses is not unusual since this is how most websites work. The dynamic DNS service provider stores the IP address of a site that changes periodically.

An account, often free, is established with a dynamic DNS host. A name for the IP address is stored with the account. For example, the link name could be "mydynamicRCS.site". The router at the RCS-8/16 site is setup with the credentials to connect to the account. The router periodically updates its IP address with the dynamic DNS host.

When you want to connect to the RCS-8/16, browse to the named link that is stored in the dynamic DNS account. That would be "mydynamicRCS.site" in this example. The dynamic DNS host looks up the associated IP address and forwards the request for data to the address. The router at that IP address receives the data request and passes it to the RCS-8/16. The RCS-8/16 fulfils the request for data by serving the requested web page.

5.3   Procedure

The steps to setup remote access to the RCS-8/16 are:

1. Assign a static LAN IP address to the RCS-8/16
2. Adjust the port for HTTP connections if necessary
3. Setup port forwarding to the RCS-8/16
4. Setup dynamic DNS for the site if necessary

You should already know how to access your router and adjust the settings. Consult the router manual or the website of the manufacturer for assistance with router access and setup.

5.3.1   Assign Static LAN IP Address

Begin by assigning a static LAN IP address to the RCS-8/16 and verify that the RCS-8/16 is accessible at the assigned address from the local network. If you cannot access the RCS-8/16 from the local network then you will not be able to access it remotely.

The RCS-8/16 has options for setting a static IP address, network address mask, gateway IP address and DNS servers. If you manually assign an IP address, make sure that it lies outside of the DHCP address pool of the router. Otherwise, the router may try to assign the same address to another device resulting in a conflict.

Alternately, the router may be able to assign the same IP address to the RCS-8/16 every time it boots based on the MAC address of the RCS-8/16. This is often called address reservation, DHCP reservation or static DHCP. The MAC address of the RCS-8/16 can be found on a label on the device if it must be entered manually.

Manually assigning an IP address is slightly easier to setup. The disadvantage is that you must keep a record of what device is assigned so that you do not assign that address to another device. It is more difficult to reconfigure the network, if that becomes necessary, since all manually assigned devices must be reconfigured.

Static DHCP setup is slightly more difficult to setup but has an advantage in that the router assigns the IP address, network address mask, gateway IP address and DNS server addresses. It is easy to reconfigure the network by adjusting settings in the router. However, this feature is not included in all routers.

5.3.2   Adjust HTTP Port

The RCS-8/16 uses the standard HTTP port 80 to serve web pages. The default setting works fine in most cases. If there is another device on the network that serves web pages though the router then one of the devices must be adjusted to serve data on another port. Otherwise, port forwarding will fail to one or both devices.

The RCS-8/16 has an option to set the HTTP port. Port 8080 is a commonly used substitute port. If any port other than 80 is used then the port number must be appended to the address when it is entered into the browser. For example, if port 8080 were used then the address would be entered as: http://192.168.2.2:8080.

Be aware that some routers have an option for remote management that, if enabled, can potentially cause a conflict. A router does not normally serve web firmware adjustment pages over the WAN port but it might do so if remote management is enabled. In this case the router may also attempt to send HTTP data over port 80. Disable remote management in the router settings or assign a different port for HTTP to resolve this conflict if necessary.

5.3.3 Setup Port Forwarding

Port forwarding should not be setup until you have assigned a static LAN IP address, adjusted the HTTP port as needed and verified that the RCS-8/16 is accessible on the LAN with the settings that have been applied.

Port forwarding is performed by the router so all adjustments to setup this function are made in the router firmware. The setup procedure is similar in most routers but specific details depend on the make and model of the device. There is a wealth of information available on the web—use the search terms "port forwarding" and you router model.

The goal is to forward HTTP data on port 80, or the substitute port, to the static LAN IP address of the RCS-8/16. Forward both TCP and UDP data if this option is presented.

Some routers have a feature called port triggering in addition to port forwarding. The functions are similar but port forwarding should be used for the RCS-8/16.

Some routers support universal plug and play, UPnP, to automatically open ports as needed. The RCS-8/16 does not support UPnP at this time.

5.3.4 Setup Dynamic DNS

The site must have a known IP address to be accessible from the Internet. If the site has been assigned a fixed IP address by the service provider then dynamic DNS is not necessary.

Dynamic DNS settings are available in the RCS-8/16 but these settings should only be used if the RCS-8/16 is not connected to a router. This is not a recommended configuration.

The router is responsible for performing dynamic DNS resolution since it is the device connected directly to the Internet. All settings for this function are made in the router firmware. The setup procedure is similar in most routers but specific details depend on the make and model of the device.

Before setting up an account with a specific DDNS host, verify that your router supports that provider. Devices vary in the depth of support for DDNS. Most router DDNS settings involve nothing more than setting the host name and supplying the account login credentials.

5.4 Router Setup Examples

The following examples demonstrate setup with two commonly available routers. There are many routers available from these and other manufacturers. Sine Systems has certainly not performed exhaustive testing across all brands and models. Your results with any given make and model will almost certainly vary.

Screen captures and addresses shown are examples. Router menus will vary with model and firmware version. Any valid private IP address subnet can be used.

Use of brand or product names is for illustration purposes. All trademarks are property of their respective companies.

5.4.1 Netgear RP614 Router
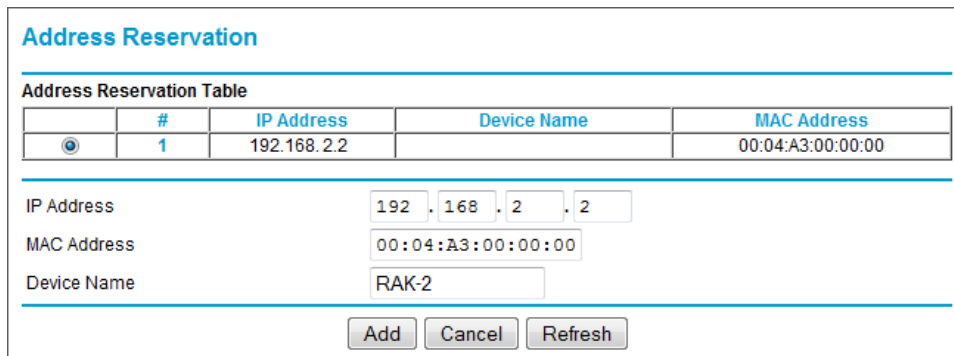
The Netgear RP614 is an inexpensive, readily available wired router that has options that make it appropriate for use with the RCS-8/16. The unit used for demonstration supports port forwarding and has "address reservation" for static LAN IP addressing.

In our example, the IP address of the router is 192.168.2.1 and the RCS-8/16 is assigned the address 192.168.2.2 by the router using address reservation. This setup ensures that the RCS-8/16 always receives the same IP address from the router.

5.4.2 Netgear Router—Address Reservation

The RCS-8/16 is connected to the router and has already received an IP address from the router DHCP server. Navigate to the LAN IP Setup menu. The bottom portion of the display shows a table that is labeled *Address Reservation*. If no reservations have been made then the table will be empty.

Click the Add button to add an entry to the reservation table. A display similar to the one shown below will appear. Each row of the table corresponds on one of the devices connected to the router. Our table shows only the entry for the RCS-8/16 for clarity.

Figure 5.1; Address Reservation entry display

Select the row with the MAC address that corresponds to the MAC address of your RCS-8/16. The IP address and MAC address fields below the table will be populated with the data for the RCS-8/16. The IP address that is displayed is the address that is currently assigned to the RCS-8/16. Edit the IP address if you would like to assign a value other than the one that is shown.

Enter an identifier in the device name field. This is the name that appears in the address reservation table. It has no significant effect on the reservation. Click the Add button to add the new reservation to the table.

The display will return to the LAN IP Setup and the Address Reservation table should have the entry for the RCS-8/16 that was just added. Click the Apply button to make this address reservation active.

Figure 5.2; LAN IP Setup display

The router will most likely reboot to apply the new settings. Allow it a minute or so to restart then login again to continue the setup.

5.4.3   Netgear Router—Port Forwarding

Navigate to the *Port Forwarding* page of the router settings. If port forwarding has not been used for other devices then the forwarding table will be empty similar to the one in the figure below.

Figure 5.3; Empty port forwarding table

Choose Port Forwarding from the service type options. Select HTTP from the *Service Name* drop-down tool. Enter the IP address of the RCS-8/16 in the area labeled Server IP Address then click the Add button.

The display will update and the table will contain the new port forwarding entry for HTTP service. The start and end ports are automatically set to port 80 as a result of selecting HTTP as the service.

Figure 5.4; Completed port forwarding table

To set a custom port for HTTP, select the radio button next to the appropriate entry in the service table and click the *Edit Service* button. A *Custom Services* display appears that allows the entry to be customized.
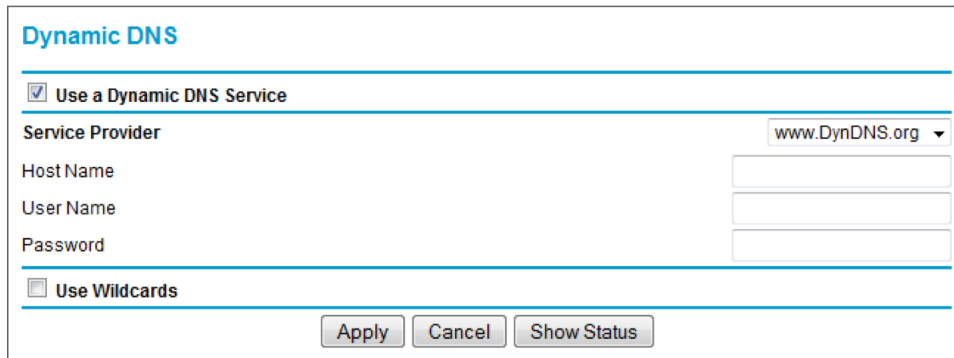

Figure 5.5; Custom port forwarding entry

Enter the substitute port number for both the starting port and ending port. Then click the *Apply* button to store the new port setting and make it active.

5.4.4   Netgear Router—Dynamic DNS

If dynamic DNS is required, use the menu to navigate to the *Dynamic DNS* page. Check the *Use a Dynamic DNS Service* box to enable dynamic DNS in the router.

This version of the router supports only one DDNS provider. Make sure you have an account with a DDNS service provider that is supported by the router.

Figure 5.6; Dynamic DNS settings

The remaining entries depend on the DDNS host and the user specific account settings. This data should be obvious once the DDNS account has been setup with the host. Enter the appropriate account credentials for *Host Name, User Name* and *Password* and click the *Apply* button to save the settings and activate DDNS in the router.

5.4.5   Linksys BEFSR41 Router

The Linksys BEFSR41 is an inexpensive, readily available wired router that has options that make it appropriate for use with the RCS-8/16. The unit used for demonstration supports port forwarding but has no provision for static DHCP.

In our example, the IP address of the router is 192.168.2.1 and the RCS-8/16 is assigned the address 192.168.2.2 manually in the RCS-8/16 settings.

5.4.6   Linksys Router—Static IP Address

Assign a static IP address to the RCS-8/16 using the settings in the RCS-8/16. The RCS-8/16 settings are discussed previously in this document.

This does pose one potential issue. How do you log into the RCS-8/16 to assign a static IP address when you do not know the current IP address that was assigned by the router using DHCP? Most routers can display a table of DHCP clients that will help you locate the IP address for a specific device.
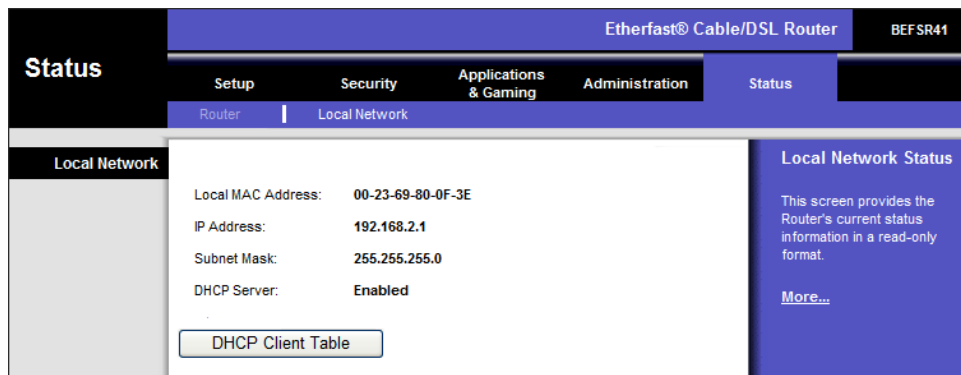

Figure 5.7; Router Status page

In the case of the BEFSR41, navigate to the Status tab then select the Local Network submenu. Click the button labeled *DHCP Client Table* on that page and a new window will appear. The window contains the IP address and MAC address of all devices that have been assigned an IP address from the DHCP server.
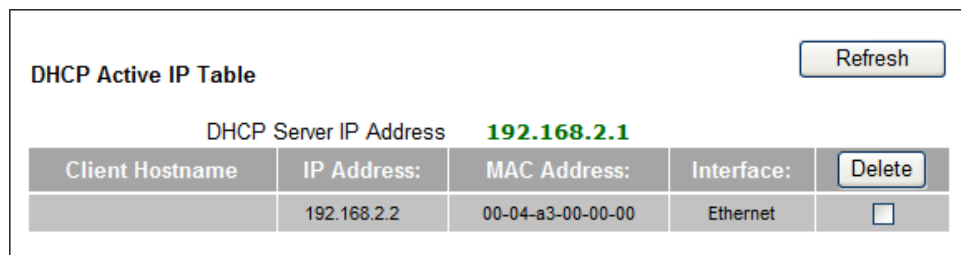
Figure 5.8; DHCP Active IP Table

Our table has been edited to show only the RCS-8/16 for clarity but it is likely that the table will contain other devices. The RCS-8/16 is easily identified as a Sine Systems device if the router is able to accept the hostname that it presents. Otherwise, find the IP address of the RCS-8/16 by locating its MAC address in the DHCP table. The MAC address of the RCS-8/16 is located on a label on the rear panel of the device.

5.4.7   Linksys Router—Port Forwarding

Navigate to the *Applications & Gaming* tab and then select the *Port Range Forwarding* submenu of the router settings. If port forwarding has not been used for other devices then the forwarding table will be empty.

Figure 5.9; Port Forwarding table

In the first available entry position, enter an "Application" name. This can be any name that allows you to easily identify the device that this entry services.
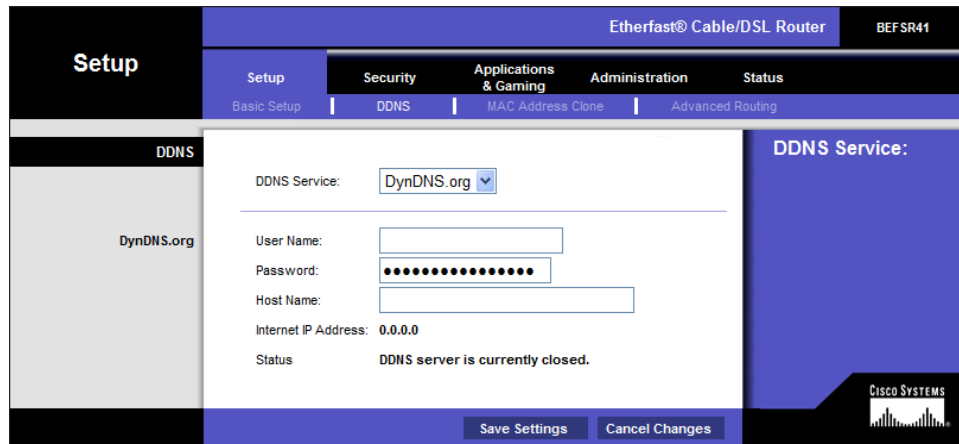
Enter 80 for both the Start and End port numbers. If you have used a substitute port number, such as 8080, then enter that port number in both positions. The protocol can be left at the default setting, "Both".

Enter the remaining portion of the IP address of the RCS-8/16 in the appropriate area. Check the box at the end of the row to enable this entry then click the *Save Settings* button.   The entry will be saved and the router may reboot.

5.4.8   Linksys Router—Dynamic DNS

If dynamic DNS is required, navigate to the *Setup* tab and then select the *DDNS* submenu of the router settings. Select one of DDNS providers from the *DDNS Service* drop-down to enable dynamic DNS in the router.

This version of the router supports two DDNS hosts. One is a free service and one paid subscription DDNS service. Choose a DDNS service provider that is supported by the router and setup an account.

Figure 5.10; Dynamic DNS settings

The remaining entries depend on the DDNS host and the user specific account settings. This data should be obvious once the DDNS account has been setup with the host. Enter the appropriate account credentials for *User Name, Password* and *Host Name* then, click the *Save Settings* button to save the settings and activate DDNS in the router.

Section 6 — Circuit Description and Factory Service

⚠️ **WARNING!** *Only qualified technical personnel should install and service the RCS-8 and RCS-16. An attempt to service this device by a person who is not technically qualified could result in a hazardous condition to the installer or other personnel, and/or damage to the RCS-8, RCS-16, RP-8 or other equipment. Ensure that safety precautions are made before installing this device.*

There is very little user-serviceable circuitry in the RCS-8/16. It is typically easier to return a damaged RCS-8/16 to Sine Systems for service. The factory service policy is given below.

6.1   Circuit Descriptions

RCS-8 and RCS-8xl systems contain two circuit boards: a main processor board and an interface board. RCS-16 and RCS-16xl systems contain an extra interface board that provides the extra bank of I/O channels.

The main processor board is the same in all devices. There are two versions of the interface panel: the standard version and the extended capability "xl" version.

6.1.1   Main Processor Board

The RCS-8/16 main processor board has a set of accessory circuits that operate with the embedded RFC-1/B. Much of the RCS-8/16 is transparent to the RFC-1/B. The RCS-8/16 has sub-processors that handle the network data I/O and some of the front panel indicators.

The embedded RFC-1/B performs all remote control tasks. A description of the RFC-1/B circuitry is in the RFC-1 Installation and Operation manual.

The main processor board contains power supply circuits, network interface, front panel indicators and telephone line surge suppression.

System power is supplied by a switching supply that provides 24 VDC at 1.0 amp or higher and 5 VDC at 3 amps. The main processor board is powered from the 24 VDC supply. This feeds a bridge rectifier and a bulk capacitor for conditioning. An LM317 regulator sets the operating voltage for the embedded RFC-1 at 17.5 - 18.0 VDC.

An LM7805 or equivalent linear regulator generates the 5VDC supply for the front panel LEDs and control logic. An LM317 generates the 3.3 VDC supply for the network microcontroller, memory and network interface hardware.

LED1 lights when the main supply is powered. This LED indicates that the 24 VDC supply is working. LED2 indicates the 5 VDC logic supply has power. Both indicators are visible from the front panel.

A small microcontroller, IC4, samples signals from the expansion port of the RFC-1/B and drives the front panel indicators LED3, LED4, LED5 and LED6. These LEDs indicate the operating mode of the RFC-1/B, voice or data, and indicate detection of DTMF tones and data I/O.

The control relay indicators, LED7 and LED8, are driven by the relay control signals. Diodes D5 and D6 set a voltage threshold for operation.

LED9 and LED10 indicate the type of voice connection, local or remote. These LEDs are controlled by the corresponding relay drivers in the embedded RFC-1.

The network status indicators, LED11 and LED12, are driven by signals from the network processor and interface controller. The microcontroller, IC1, communicates with the embedded RFC-1/B and translates the data into web pages stored in the serial EEPROM, IC6. This data is then sent to the network through the Ethernet controller IC2. Crystal X1 is 25 MHz time-base for the network controller. The network connector has embedded transformers.

The telephone line surge suppression is comprised of several passive components. Gas arrestor SP1, resistors R9-R12 and VR4-VR5 perform the RCS-8/16 side of the protection. There is more surge protection downstream in the RFC-1/B telephone line interface.

6.1.2   Standard Interface Board

The standard interface board is very similar to a combined RP-8 relay panel and SP-8 surge protector. A complete description of the RP-8 is included in the RFC-1/B Installation and Operation manual.

Power, addressing and control signals for the standard interface board are supplied through the 16-pin flat cable. Bulk power is a pseudo-regulated 9-10 VDC. A Zener diode drops the supply voltage to about 5.5 VDC to supply the integrated circuits, LEDs and relays.

A 74HC42 decodes the channel block address lines and an 8-position jumper is used to select the active channel block. A CD4028 decodes the channel and an ULN2803 drives the control and telemetry input relays.

Each telemetry input has a 5.1K resistor in series with each leg of the input. Surge suppression is provided by MOVs on each input. Each telemetry input feeds a relay that switches the telemetry samples to the telemetry bus.

6.1.3   Extended Interface Board

The extended interface board, used in the "xl" models, uses similar circuitry to the standard interface panel for the telemetry inputs and control outputs. Unlike the standard model, the extended model has a microcontroller that is able to operate all control relays and telemetry inputs independently.

A 5 VDC power is supplied through power connector J14. This supply has a much higher current capacity than the standard supply to support the latching control relays. Capacitors C9 and C10 buffer the supply and diode D20 provides surge suppression.

Channel selection and control signals arrive on J1 from the 16-pin flat cable. All digital signals from the main controller board are optically isolated by IC2 and IC3.

The extended features of the "xl" models are controlled by three banks of 8-position DIP switches. Each bank controls a function: telemetry logic voltage, of/lower control relay latching or on/raise control relay latching. Switch 1 corresponds to the lowest number channel on the board, which depends on the channel block selection. The microcontroller reads the state of the switches through three 74HC597 shift register ICs.

A 74HC42 decodes the channel block address lines and an 8-position jumper is used to select the active channel block. The microcontroller monitors the block selection signal to determine if it should react to the control signals.

When a channel is selected, the microcontroller decodes the channel number from the isolated input signals. It sends data to a TPIC6595 to engage the appropriate relay to switch the corresponding telemetry sample on the bus.

When a control relay command occurs, the channel number is decoded and data is sent to a TPIC6595 to engage (or disengage) the appropriate control relay. The TPIC6595 is a combination shift register, data latch and relay driver.

Two CD4052 ICs switch the internal logic voltage to the telemetry inputs as needed. When the logic voltage is enabled on a channel and the channel is selected, the microcontroller engages switches in these ICs to apply the logic voltage to the appropriate telemetry input.

6.2   Factory Service Policy

Terms are subject to change without prior notice.

6.2.1   Warranty

Sine Systems, Inc. guarantees our products to be free from manufacturing defect for a period of one year from the original date of purchase from Sine Systems, Inc. This warranty covers the parts and labor necessary to repair the product to factory specifications.

This warranty does not cover damage by lightning, normal wear, misuse, neglect, improper installation, failure to follow instructions, accidents, alterations, unauthorized repair, damage during transit, fire, flood, tornado, hurricane or acts of God and/or nature.

Warranty Service

There is no charge for repair service on items covered under warranty. The customer is responsible for payment of shipping charges to return equipment to Sine Systems for service. Damage due to negligence, lightning or other acts of nature are not considered warranty issues.

Service Policy

Sine Systems offers same day repair service on all of our products. We typically repair and return products within 24 hours of arrival whenever it is feasible to do so. Because we offer immediate service, we do not provide loaner equipment. If we cannot immediately repair a product, we may offer other options at our discretion.

Sine Systems does not require prior authorization on repairs. See the factory repair service page on our website, www.sinesystems.com, for details on returning products for service. Sine Systems is not responsible for items lost in transport or delivered to an incorrect address.

6.2.2   Return Policy

This policy only applies to equipment purchased directly from Sine Systems, Inc. Equipment purchased through a third party vendor (dealer) is subject to the return policy of the vendor. Arrangements for return or exchange must be handled through the vendor.

Sine Systems policy on returns and exchanges with the factory is broken down according to the following schedule:

30 days

Items may be returned within thirty days from the date that they ship from our factory. Sine Systems will apply a full refund, less shipping charges, provided that the equipment is in new condition. There must be no cosmetic damage, all accessories must be included and unopened and all manuals must be included and undamaged. If any items are missing, damaged or opened, a 5% restocking fee will be applied.

60 days

Items may be returned within sixty days from the date that they ship from our factory. Sine Systems will apply 15% restocking fee. This fee covers the cost of returning the items to new condition, replacing accessories, replacing manuals and re-packaging. These items must eventually be sold as reconditioned instead of new.

Beyond 60 days

After sixty days, Sine Systems will recondition the equipment according to our repair policy but we will not accept it for return or exchange.

Section 7 — Specifications

7.1   RCS-8 / RCS-16 Electrical and Mechanical

7.1.1   Connections

Relay panel: 16-conductor 0.1" pitch pin/plug
Telephone: RJ-11C modular connector
Local phone: RJ-11C modular connector
Network: RJ-45 modular connector, Ethernet over twisted-pair
Telemetry: 4-conductor 3.81 mm pitch pluggable screw-terminal
Control relay: 6-conductor 3.81 mm pitch pluggable screw-terminal

7.1.2   Indicators—front panel

Main power: green LED
Logic power: green LED
Voice mode: green LED
Data mode: green LED
DTMF detect: red LED
Data Tx/Rx: red LED
Control on: yellow LED
Control off: yellow LED
Voice local: green LED
Voice remote: green LED
Network link: green LED
RFC-1/B link: green LED
Channel select: green LED
Control on/raise: green LED
Control off/lower: green LED

7.1.3   Indicators—rear panel

Network link: green LED
Network data: yellow LED

7.1.4   Controls—rear panel

Reset: network reset button

7.1.5   Power

Input: 90-240 Volts AC @ 50/60 Hz
Fuse: 0.5 Amp slow-blow 5 x 20 mm

7.1.6   Dimensions

Size: 19" (w) x 6.5" (d) x 1.75" (h)
Weight: 3 lbs.

7.1.7   Environmental

This device does not generate a significant amount of heat. It should only be installed indoors in a dry environment. This device complies with the limits for a Class B computing device pursuant to Subpart J of Part 15 of FCC Rules.

7.2   RCS-8 / RCS-16 Schematic Diagrams