GRouter4
Single Port 709.1 /852 LON/IP Router
User's Guide

SMART CONTROLS

Printed in USA.

Version 4.14.3.1

Contact Information:

Smart Controls, LLC
10000 St. Clair Avenue
Fairview Heights, IL 62208 USA
Voice: +1 618.394.0300
Fax: 618.394-1575
Web: www.smartcontrols.com
Email: engineering@smartcontrols.com

Table of Contents

List Of Figures

1. Overview

1.1. Introduction

The GRouter (GR4) router supports two open standard protocols, namely ANSI/EIA 709.1 and ANSI/EIA 852. Both the ANSI/EIA 709.1 and ANSI/EIA 852 are defined by the Consumer Electronics Association Technology & Standards R7.1 HCS1 Subcommittee. For more details see `http://ce.org/`. For the sake of brevity the remainder of the document will refer to the standards as 709.1 and 852. 709.1 is also known by its trademarked name, LonTalk®. A 709.1 network is also commonly referred to as a Local Operating Network or LON. This document will use 709.1 network and LON interchangeably.

The 852 protocol acts as the transport service to convey 709.1 messages over *Internet Protocol* (IP) networks. This technique of using another protocol (i.e. 852) to transport a message over an alternate media is often referred to as *tunneling*. In 852 parlance the tunneled protocol is a *Component Network* (CN) protocol. The 852 protocol is a generic tunneling protocol and is not limited to 709.1. However, a particular implementation of the 852 protocol may only support the tunneling of a single CN protocol. The tunneled CN messages have no information or awareness of the tunneling process. Although some of the figures in this document use CN or CN/IP to represent a component network or component network to internet protocol connection, the only CN currently supported by the GRouter device is 709.1

A component network protocol is often called a fieldbus due to its use for machine to machine networking and control in the *field*. This document, however, will only use the term component network or CN.

852 not only provides the vehicle to transport ANSI 709.1 messages across IP, but it also provides management of these connections or routes. A logical grouping of 852 devices that exchange packets is called an 852 channel. One may think of an 852 channel as a kind of *virtual LAN* on an IP network.

A GRouter device forwards 709.1 packets to or from an IP channel (using an Ethernet or WiFi transceiver) and a CN channel (using twisted pair FT-10 or RS-485 transceivers). The GRouter device has a presence on, or physical connection to, both channels. The router takes 709.1 messages from the component network, wraps them in an 852 packet and sends them over the IP network. The GRouter device also receives 852 packets on its IP interface, unwraps them and puts the 709.1 messages on the CN channel. The virtual 852 channel looks like a CN channel to CN nodes. The IP element is transparent. This enables a flat network and is more easily managed and scaled than using CN to IP interfaces that do not hide the IP element from the CN nodes. The important thing is not what the CN to IP device is called but how transparent it makes the IP network appear to the CN nodes.

Network connection devices can operate at different layers of particular networks protocol stack. 709.1 is an OSI 7 Layer type protocol. Whereas the Internet Protocol has only 4 layers. (See Figure Figure 2.1 for a diagram of the different layers of the two protocols.)

Fig.1.1: Network Layers

A network connector is a device that joins different parts of a network. Connectors have a specific name that is dependent on the layer at which the connector operates. For example a

router operates at the network layer and a gateway at the application layer. Because higher layers of the protocol do not have access to some of the information stripped away by lower layers, network connectors operating at different layers have different capabilities. There is also some abuse of terminology so that the descriptions of network connectors from different manufacturers may be confusing. For example, a repeating router may be called a repeater for short. Although a repeating router acts similarly to a physical layer repeater, it operates at the network layer and is not equivalent. It is usually best to find out at which layer a network connector operates.

Fig.1.2: Network Connector Types and Associated Layers

The GRouter device is a more complex connector because is connects two different protocols and also connects the protocols at different layers. On the IP side the GRouter device operates at the application layer and so is appropriately called an IP Gateway. On the 709.1 side the GRouter device operates at the network layer and is appropriately called a 709.1 router. So depending on the user's perspective the GRouter could be called a gateway or router or a router/gateway. (See Figure 2.3)

Fig.1.3: CN to IP Router/Gateway Architecture

The GRouter device also employs a web server for configuration purposes. (See Figure 2.4)

Fig.1.4: GRouter 3 Architecture

1.2. Configuration Parameters

The information required for successful ANSI/EIA 709.1 transport can be broken up into the following two categories: device parameters and channel parameters.

Device parameters include information such as: IP address, IP port, Name, and Address of configuration server.

A channel is a logical grouping of LON to IP routers. The minimum requirement for tunneling ANSI/EIA 709.1 data is the use of two routers. Router A sends data to Router B and vise versa. However, routers can also send data to more than one router. In such a case, Router A sends data to Routers B, C, and D, which in turn send data back.

A channel, then, is defined as a group of routers that all send information to each other. The lines of communication are open in both directions and to all members—a complete mesh of connections.

Typically, channels are managed through the use of a configuration server (called Normal mode see below). The configuration server informs all members in the channel about the channel information, which includes the adding and removing of channel members. Configuration servers are capable of managing multiple channels, while routers belong to only one channel at a time.
Lon to IP routers can also be managed manually by configuring each device uniquely (called

Manual mode, see below). In such a manual configuration, for proper operation, devices must have mutual membership in each other's channel lists. That is if Device A is in Device B's channel list then Device B must be in Device A's channel list. However if Device C is in Device B's channel list, Device C does not have to be in Device A's channel list.

1.3. Modes of Operation

The GRouter device can operate in one of two modes: (1) Manual, (2) Normal.

1.3.1. Manual Mode

In Manual mode the user has control over the GRouter device's configuration only. The user can change the GRouter device's operating information and determine to whom the router will send information. In Manual mode the GRouter device will honor read requests from other devices or configuration servers, but it will block requests to write or change internal parameters. This is a more secure mode and may be preferred on open networks. This mode is also preferable with non-standard configurations such as Flood Mode or DDNS.

1.3.2. Normal Mode

Normal mode allows the user to view configuration data and channel data set by a remote configuration server such as an i.LON® configuration server. The configuration server sets some of the operating parameters of the GRouter device. Configuration servers mostly manage the device's channel. The channel is made up of other devices to which the GRouter device will tunnel or send ANSI/EIA 709.1 data. In Normal mode the adding and deleting of devices is managed exclusively by the assigned configuration server. The configuration server provides a single interface to add and delete devices. Finally, Normal mode permits read access to information by other devices and write access to information for the assigned configuration server.

Note: Echelon's LNS based VNI interface (LonMaker) only works in Normal mode. In order for a GRouter device to communicate directly over an IP channel to a VNI interface requires that the GRouter device be in Normal mode.

1.4. Applications of the GRouter Device

1.4.1. Multi-site building automation networks

The interfaces described here provide the management necessary for the ANSI/EIA 852 to tunnel ANSI/EIA 709.1 packets successfully over IP. This ability provides wide area network (WAN) support to ANSI/EIA 709.1 networks. This allows multi-building or multi-site connection of automation networks.

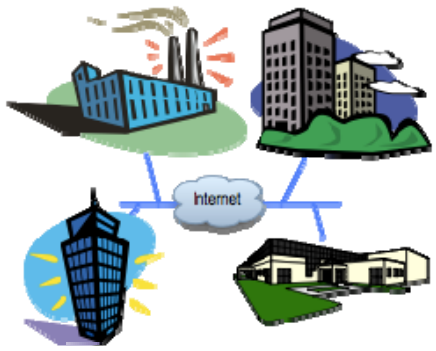


Fig.1.5: Multi-site building automation network with internet connectivity

1.4.2. IP backbones for LON traffic aggregation

Furthermore, since the IP networks can support much higher traffic capacity, GRouter devices can also be used to aggregate 709.1 traffic from several LON channels over one IP channel. The ability to aggregate larger traffic volumes allows several GRouter devices and other 709.1 to IP routers to be used as network backbones for 709.1 networks.

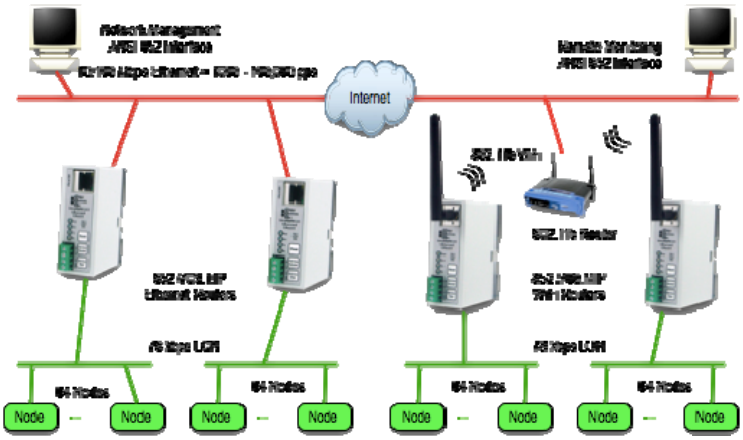


Fig.1.6: Example Hybrid Network

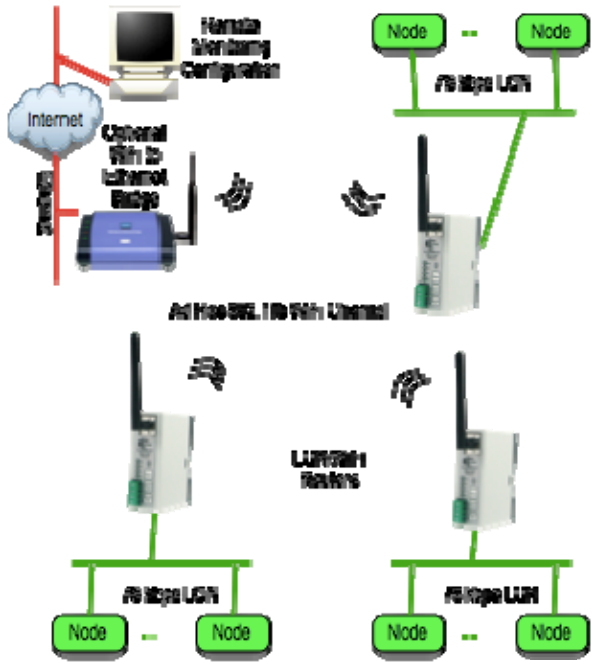


Fig.1.7: Example WiFi Ad Hoc Network

1.4.3. Roaming Connections

Finally, LON to IP gateways may be connected to specialized IP applications instead of to other gateways. Connecting an IP application to a GRouter device provides these specialized

applications with roaming capabilities which would be difficult if these applications were required to be directly connected to the 709.1 network (e.g., GadgetAnalyzer, LonMaker-3, etc.). An example of how several GRouter devices can be interconnected to support an IP backbone for several LON networks is show in Figure 2.5.

1.5. IP Addressing Modes

The GRouter device uses one of two forms of IP addressing: unicast and multicast. Multicast currently only works when in manual mode.

The advantage of multicast is that for networks with multiple Gateways (especially in flood mode), multicast may be more efficient. The disadvantage of multicast is that some internet routers do not support it. Multicast mode can reduce the IP traffic relative to unicast when there are a large number of 852 devices in the channel. Up to 255 devices per IP domain are supported with multicast. Some older IP routers do not support multicast and therefore you will not be able to route 852 packets across a unicast only router with multicast addressing. IP router support for Multicast is not a concern when all the 852 devices share the same subnet. The following figures illustrate the differences between multicast and unicast.

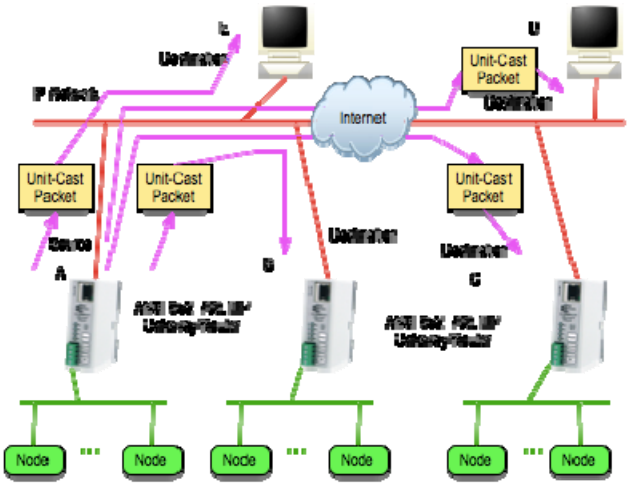


Fig.1.8: Unicast

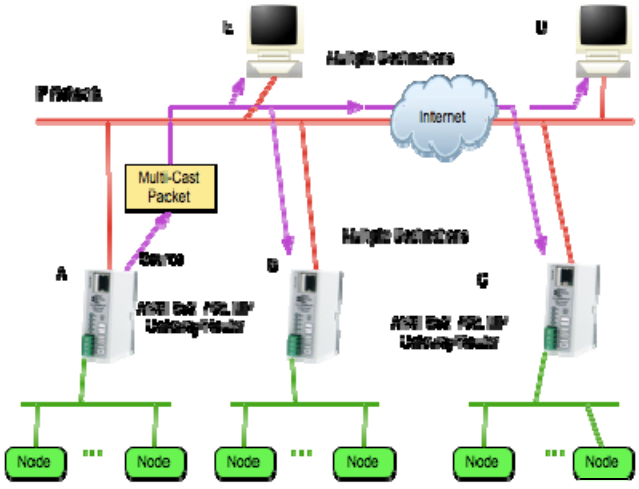


Fig.1.9: Multicast

1.6. System Requirements and Connections

1.6.1. System Requirements

To configure the GRouter device, you will need a web browser such as Internet Explorer, Mozilla, Safari, or Firefox.

The GRouter device will communicate with any of the following:

- Smart Controls Systems Inc. GRouter4, GRouter3, or GadgetGatewayIa (GG1a) 852 router
- Echelon i.LON™ router or LNS VNI based tool such as LonMaker™. The supported versions of LonMaker are versions 3.1 or later including turbo version 3.2x. The supported versions of LNS Server are versions 3.0x or later including 3.2x.
- Coactive Router-LL router
- Any 852-A 852-B or later compliant node

To operate in normal mode an 852 configuration server is required such as the Echelon i.LON configuration server (ILCS). Manual mode does not require a configuration server. The supported version of the ILCS is version 2.x or later.

Note: The GRouter and Router-LL routers can interoperate in either Manual mode or with the Router-LL configuration server.

The Smart Controls Systems GRouter device also needs the following hardware:

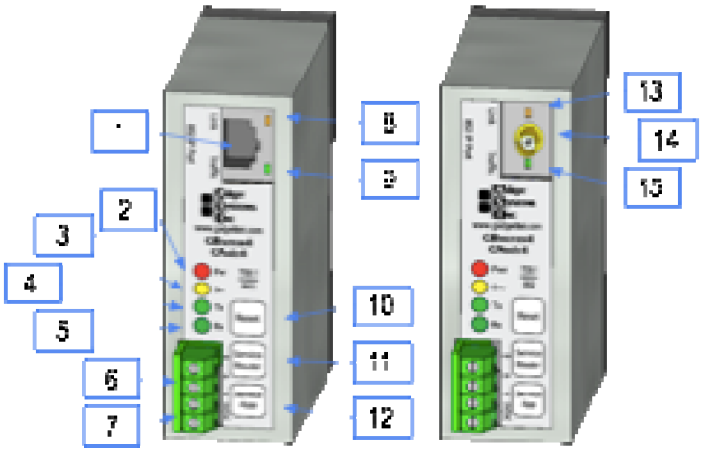
- Cat 5 Ethernet Cable (for Ethernet versions).
- Regulated 5V DC power supply.
- Twisted pair cable for 709.1 (LON) port.

Up to date documentation and firmware is available on Smart Controls's web site at

http://www.Smart Controlssystemsinc.com.

To find out what version of ILCS you are using, select the help>about menu. To find out what version of LonMaker you are using, click on the icon in the upper left hand corner of the window and select the about ... menu. This will also show the version of LNS Server. To see what version of LNS server you are using when you don't have LonMaker, use the Windows Control Panel, Add or Remove Programs, the Echelon LNS Server item, Click here for support info window.

1.6.2. Button, Indicators, and Connectors for GRouter



Index	Description
1	Ethernet 10/100 Base-T Port. RJ-45 Cat-5.
2	Power LED lights when unit powered.
3	Service LED flashes when a service message sent.
4	TX LED flashes to indicate send traffic on the LON Port.
5	RX LED flashes to indicate receive traffic on the LON Port.
6	LON (709.1) Port. May be either FTT-10 or RS-485 transceiver. Check particular configuration of router. 2 Pin, 5mm spacing screw terminal block.
7	5 V power input and ground. Ground pin is also ground for RS-485 transceiver when applicable. Requires regulated 5V. Reverse polarity protected. Reversing polarity for extended time may damage router. 2 Pin, 5 mm spacing screw terminal block.
8	Ethernet Link LED lights when link obtained.
9	Ethernet Traffic LED flashes when traffic on Ethernet port.
10	Reset Button. Resets and restarts router.
11	Service Pin Router. Sends out a service message on both LON and IP sides for the router. If 852 bridging router mode is enabled sends out a service message for both 852 channels. Also used for startup mode selection.
12	Service Pin Application. Sends out a service message on both LON and IP sides only if optional twin mode application is activated. Also used for startup mode selection.
13	WiFi Link LED lights when link obtained. Infrastructure mode solid. Ad Hoc mode, flashing 5 second on, 1 second off. No connection, flashing one second on, one second off.
14	WiFi Port for optional 802.11b WiFi version. Male RP-SMA screw connector. Mates with Female RP-SMA antenna or cable.
15	WiFi Traffic LED flashes when traffic on WiFi port.

1.6.3. Wiring

The standard configuration for the GRouter4 has a 4 pin 5.0 mm spaced screw terminal block. The pins from top to bottom are labeled A, B, ⏚(logic ground), and 5VDC. To use the terminal block unscrew the terminal screws on the block and insert the ends of the appropriate wires into each opening. Tighten the terminal screws. Pins A and B are the 709.1 LON channel port pins. For FTT-10 transceivers, use the A and B pins. The pins are polarity insensitive. For RS-485 transceivers use the A and B pins appropriately and insert the RS-485 ground lead into the terminal block pin with the ⏚ (ground) symbol next to the pin labeled *A*. There are two power input pins labeled ⏚(logic ground) and 5VDC. The GRouter4A requires regulated 5 Volt DC positive on the 5VDC pin. Attach the ground pin from the power supply to the pin labeled ⏚.

The power input is polarity sensitive but does have reverse polarity protection. If after powering up the 5V input, the power LED does not light up, disconnect power and check the polarity of the input power wires before recycling power. Applying a reverse voltage for an extended time period may damage the GRouter4.

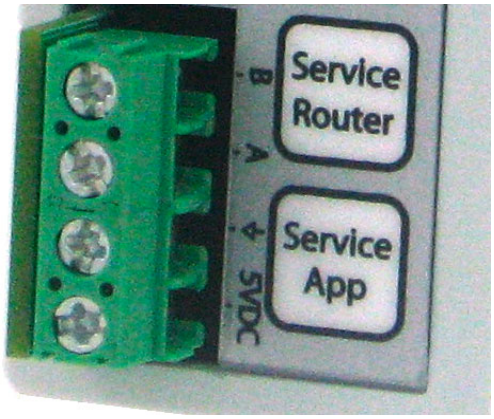


Fig.1.10: Front terminal block detail with standard connector

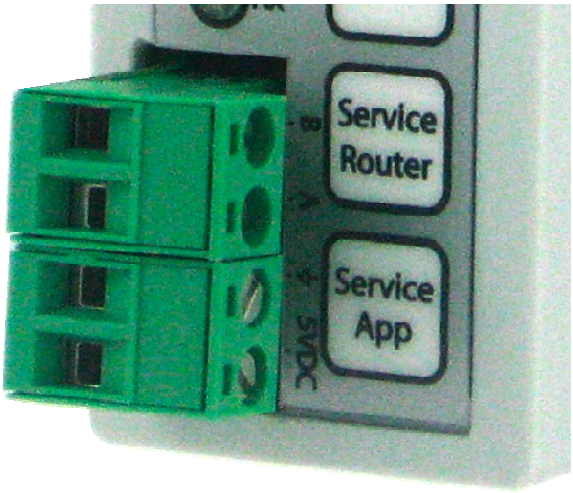


Fig.1.11: Front terminal block detail with optional pluggable connectors

2. Web Configuration

The Web-based GRouter device interface allows the user to access and change configuration data on the GRouter device by using any http Web browser attached to the network. This allows users to make changes to the GRouter device remotely. This chapter familiarizes the user with the various pages of the Web-based Interface and describes the steps necessary to changing configuration data.

2.1. Default IP Configuration

The GRouter device is configured through a web browser such as FireFox, Internet Explorer, Safari, or others. In order to connect to the GRouter device from a web browser, the GRouter device and the computer running the web browser must be connected to the same IP network. The factory default IP host address of the GRouter device is 10.0.2.40 with subnet mask of 255.255.255.0. The router's web server is serving http on port 80. The computer running the web browser must be able to access the GRouter device's subnet.

Default Internet Configuration	
IP Host Address	10.0.2.40
IP Subnet Mask	255.255.255.0
Web HTTP Port	80

2.1.1. Ethernet

For Ethernet equipped GRouter devices, first configure the host computer to add an IP interface on subnet 10.0.2.0/255. Connect one end of a Cat5 Ethernet cable to the RJ-45 on the GRouter device and the other end to an Ethernet hub or switch or directly to a computer with a crossover cable or straight through if the computer's Ethernet port supports auto crossover (Auto MDIX). The GRouter Ethernet port is MDI only. In cases where the LAN does not support the default subnet, a direct connection between the GRouter device and the web browser host computer will be needed.

Fig.2.1: Ethernet setup with hub or switch

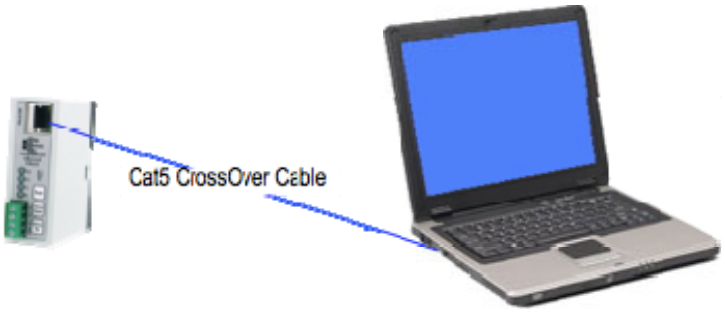


Fig.2.2: Ethernet with direct connect crossover cable

2.1.2. WiFi (802.11b)

For WiFi equipped GRouter devices, an 802.11b WiFi access point or ad hoc connection must be setup between the web browser host computer and the GRouter device. First configure the host computer to add an IP interface on subnet 10.0.2.0/255. Instructions for setting up Windows XP are in the next section. Then setup the WiFi configuration. The default WiFi configuration for the GRouter device is as follows:

Wireless SSID: "Smart Controls"
Wireless Mode: Any Type (Ad hoc or Infrastructure)
Channel: Search
Encryption: None

The access point or ad hoc connection must be set up to allow a connection on a network with SSID of *Smart Controls* or *Any*. There are many different topologies that may be employed for connecting to the GRouter (GRouter) WiFi version. The following figures show some of the more common ones.

Fig.2.3: WiFi setup with access point and Ethernet connection to host computer

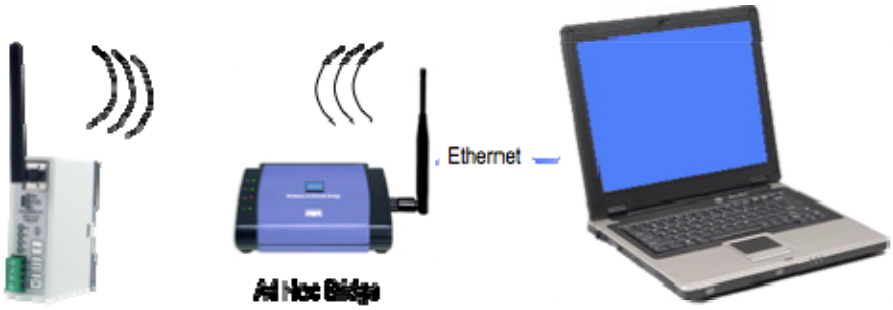


Fig.2.4: WiFi setup with ad hoc bridge and Ethernet connection to host computer

Fig.2.5: WiFi setup with ad hoc WiFi card on PC

Fig.2.6: WiFi setup with access point and WiFi card on PC

2.1.3. WiFi Setup in Windows XP

- Go to the network connections control panel. Right click *wireless connection* and select *properties*.
- Select the general tab. Set the IP address to one that is in the same subnet as the GRouter's default IP of 10.0.2.40 with a subnet mask of 255.255.255.0. For example, you could use 10.0.2.41.
- Go to network properties and select the connection tab. Select manual connect to an available wireless network not automatically connect.
- In the main network connections control panel, create a new wireless network by selecting "add new network". Use the following settings the the network:
  - In the Association Tab set the following fields:
    - SSID: "Smart Controls"
    - Network Auth: open
    - Data Encryption : Disabled
    - Check the "this is a computer to computer network(ad-hoc)" box.
  - In the Authentication Tab leave the settings at the defaults.
  - In the Connection Tab set the following:
    - Check the "connect when this network is in range" box.
- Click Ok, then Ok again to save the settings.
- After a minute or two the computer will automatically connect to the GRouter
- You can now access the GRouter's configuration web pages through a web browser using a url of "http://10.0.2.40".

2.2. Establishing a Connection (Ethernet or WiFi)

Once the IP connection (WiFi or Ethernet) is setup, power up the GRouter device. It takes about 60 seconds for the GRouter device to boot up. On an Ethernet device Boot-up is completed when the yellow link light flashes off once and then back on solid and the green traffic light starts flashing. On a WiFi device, boot-up has completed when the green traffic light starts flashing. Depending on the type of connection, the yellow WiFi link light may or may not flash. In infrastructure mode the yellow light is on solid. In Ad Hoc mode is flashes 5 seconds on, and 1 second off. If no connection, it flashes one second on,and one second off. yellow

2.2.1. Ping to Verify

For either Ethernet of WiFi, to verify that the IP connection has been made send an IP ping to the GRouter device at its default IP host address (10.0.2.40). In Linux, Windows 2k+, or Mac OS X a ping can be sent from the command line as follows:

```
ping 10.0.2.40
```

Then type *enter* or *return*. This will ping 4 times.

```
ping -t 10.0.2.40
```

This will ping continuously until a break control-c is typed.

If there is no response, double check all network connections and cables and device setup. Make sure you can ping out by pinging some other computer on your network. Once you can successfully ping the GRouter device, establish a web connection from a web browser window as follows:

```
http://10.0.2.40
```

Then type *enter* or *return*.

Note: Sometimes when configuring multiple routers in quick succession using the same computer, IP communications will fail temporarily for the next router. The reason for this is that the IP stack on the computer caches the MAC address of each device in an ARP table, indexed to the IP address. The first router that responds on 10.0.2.40 will have its MAC address associated with 10.0.2.40 in the ARP table. Because we ship every router with the same default address, the first time each router is accessed it is on the same IP address. The next router that uses 10.0.2.40 will have a different MAC address and when the computer tries to communicate with it, the computer may use a stale cached MAC address instead. To clear the ARP table entry for 10.0.2.40, in Windows, Linux, or OS X, enter on the command line (or DOS prompt):

arp -d 10.0.2.40

2.2.2. User Name and Password

The GRouter device web interface will prompt for a user name and password. The default user name is *Adept* and the default password is *Gadget*. The user name and password are case sensitive so make sure to use a capital A and capital G respectively. Click OK. You will now be shown the home or status page for the GRouter device web based Configuration Tool. To navigate the various pages in the Tool, simply click the buttons on the left side of the page to link to the appropriate page. The button corresponding to the page that is currently displayed

will be highlighted in pink. Each of the pages in the web based Configuration Tool will be explained in the following sections.

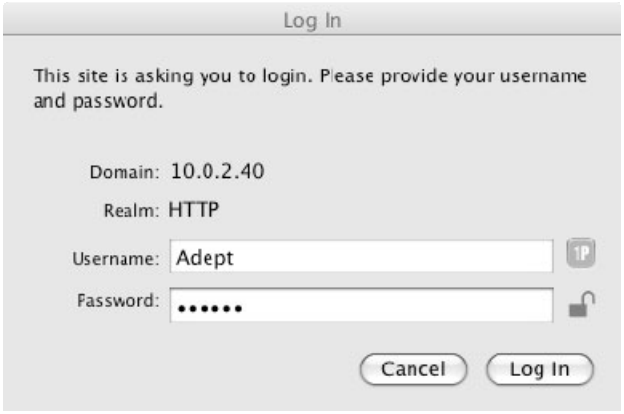


Fig.2.7: User Name and Password Authentication

Once communications have been established, new IP or WiFi parameters may be entered. The procedure is as follows:

- Set up IP and/or WiFi interface between host computer and GRouter device using default network settings
- Reconfigure the GRouter device to use new network settings
- Reconfigure the IP and or WiFi network to use new settings
- Reboot GRouter device and reestablish communications using new settings
- If communications with new settings cannot be established because of lost or incorrect settings then revert GRouter device to factory defaults and start over.

2.3. Restoring Factory Defaults

The web Tool allows customization of the IP address, net mask, WiFi SSID and security settings, HTTP port, web user name, and password. Should any of these settings be forgotten or setup incorrectly, communication with the GRouter device may not be possible. In this event, the IP settings on the GRouter device can be restored to factory defaults so that a known set of IP, WiFi, and web parameters is in effect.

2.3.0.1. Basic Procedure

The basic procedure is to first reboot the device and then while its booting up press and hold one of the service buttons.

To reboot the device, either press and release the Reset button or power cycle the GRouter device. If powering down or resetting the device after making any configuration changes, please use the *Prepare to Power Down* button on the Router Setup page to ensure that a flash write operation induced by the changes is not interrupted by the power down. Interrupting a flash write could corrupt the flash and make the unit inoperable.

Once the router starts rebooting, on the Ethernet version, the yellow link and green traffic LEDs will go on solid while it loads its firmware, on the WiFi version the yellow and green LEDs will go off. This will take about 30 seconds. Firmware load is completed when the yellow light flashes

off and back on and the green light goes starts flashing. About 10 -15 seconds later the router will read the service button state to determine if a reset to defaults is desired. Consequently, one has about 10 seconds after the green light starts flashing to press and hold down one of the two Service buttons and then continue holding until it reads the button state. At which time one may release the Service button.

To restate:

1) Appropriately reboot the router.

2) Wait until the IP Link yellow light goes on and the IP Traffic green light starts flashing.

3) Hold down either the *Service App* or *Service Router* button until the *Tx, Rx* and *Srv* lights all come on solid (about 10 - 15 seconds). These lights will stay on for 3 seconds then go off.

4) Once the *Tx*, *Rx* and *Srv* lights come on, release the service button. (If after holding down the button for 20 seconds the *Tx*, *Rx* and *Srv* lights don't come on then try again from the start.)

What happens next depends on which of the service buttons was pressed.

If the *Service Router* button is pressed, the IP address,port and (when applicable) the WiFi SSID will be reset to factory defaults.

5) After about another minute the router will go into reset. This is indicated by the yellow link light and the green traffic light both going on solid for the Ethernet unit and both going off for the WiFi unit. Another minute later the router will boot up with all the IP parameters set to factory defaults.

If the *Service App* button is pressed, the web user, password, and web server port will be reset to factory defaults.

5)The router will continue its boot-up with all the web parameters set to factory defaults.

If both the *Service Router* and *Service App* buttons are pressed then both the IP and web parameters will be reset to factory defaults.

5) After about another minute the router will go into reset. This is indicated by the yellow link light and the green traffic light both going on solid for the Ethernet unit and both going off for the WiFi unit. Another minute later the router will boot up with all the IP and web parameters set to factory defaults.

Test the restored IP settings by pinging the default IP address and/or entering the default URL into a web browser.

2.4. Web Configuration Parameters

In general there are two types of parameters on the following web configuration pages. The first type take effect immediately upon submission, usually by clicking a submit changes or other similar button. The other type require the router to be rebooted before taking effect. The parameters that require a reboot are marked with a green asterisk.

Submit changes will first store the parameters in RAM and then later, in the background, a copy (actually two copies) will be stored in flash. Power cycling the router before it has time to store the backup copies in flash means that on the next boot-up it may not retain the changed parameters. In some cases power cycling or resetting the router while its writing some of the

critical flash parameters may corrupt flash and make the unit inoperable. The Router Setup page includes a ***Prepare to Power Down*** button that checks the status of any pending flash writes and then either displays a page that indicates it is safe to power down or displays a page with a timer that indicates that one should wait until the timer expires before powering down.

2.5. Status Page

The status page is the home page for the web Tool. The buttons shown on the left will vary depending on what optional services have been enabled in the router. The Router Status Page displays basic information about the status of the Router. Changes to the data cannot be made through this page; it is for information purposes only. Following is a brief description of each item shown on the page

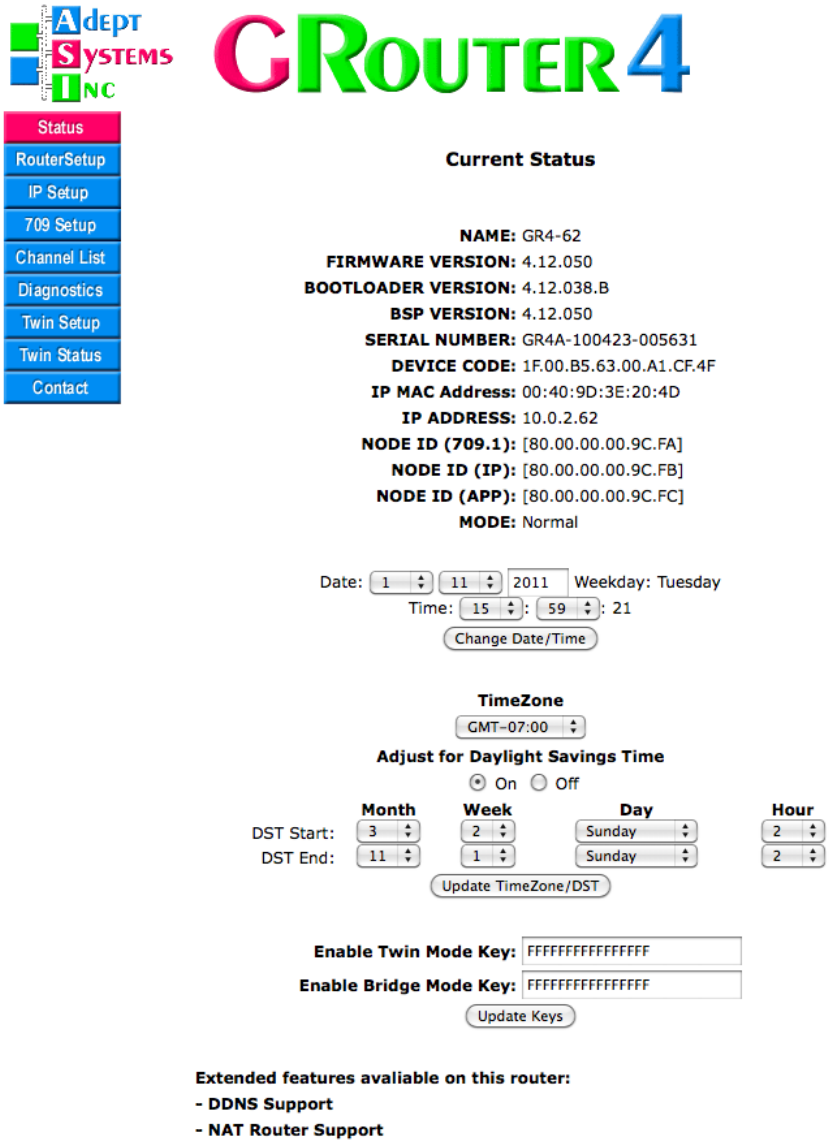


Fig.2.8: Status Page

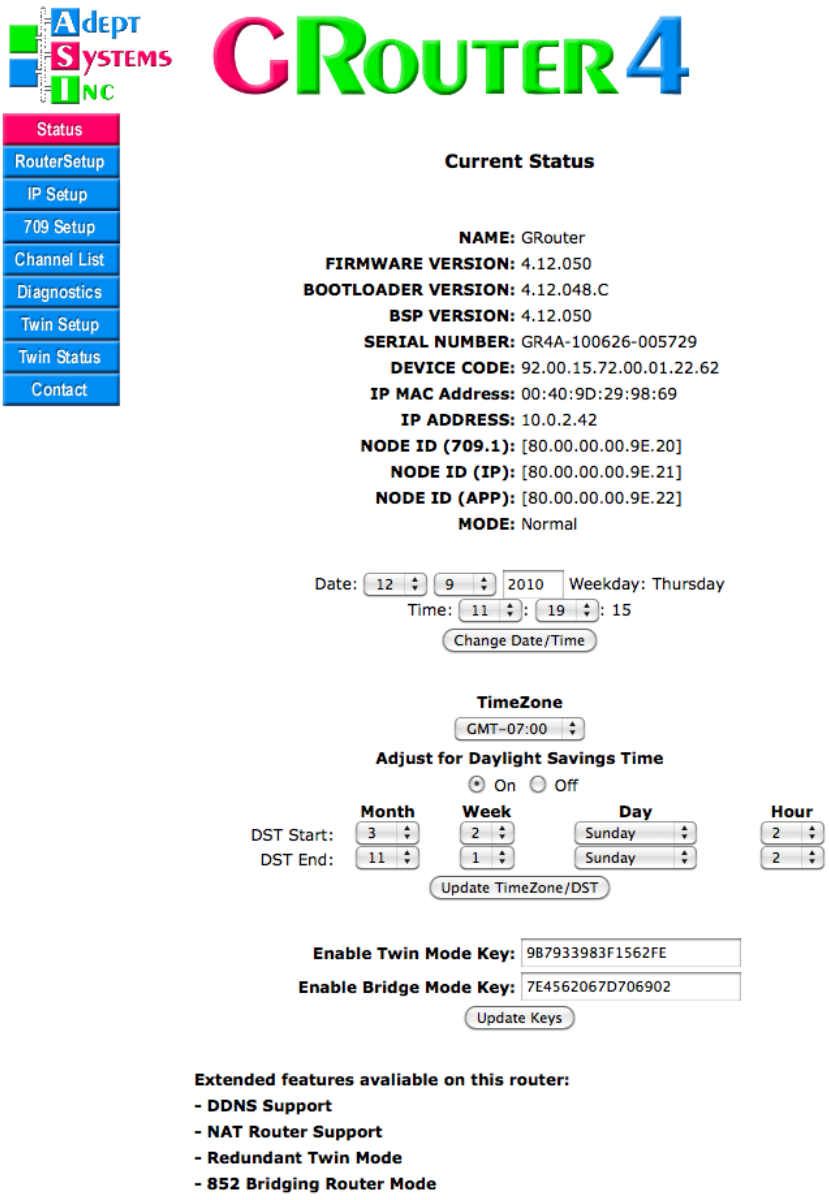


Fig.2.9: Status Page with Bridge and Twin Mode Enabled

NAME: The given name of the router.

FIRMWARE VERSION: The version of the firmware currently loaded on the router. This is the router application code.

BOOTLOADER VERSION: The version of the bootloader currently loaded on the router. The bootloader is responsible for loading the application code into memory and starting it running. Beginning with firmware 4.12 the bootloader is upgradeable and has a version number.

BSP VERSION: The version of the board support package used to build the application firmware. This is mainly for diagnostic and tracking purposes as the BSP is included in the firmware but could be from a different build cycle.

SERIAL NUMBER: The serial number for the router.

DEVICE CODE: The unique device code for the router.

IP MAC ADDRESS: The IP MAC or hardware address assigned to the router's IP port.

IP ADDRESS: The IP address assigned to the router.

NODE ID (709.1): The 709.1-side (LON) unique Node ID number assigned to the router. If 852 bridge mode is enabled this is the near side of the router.

NODE ID (IP): The IP-side unique Node ID number assigned to the router. If 852 bridge mode is enabled this is the far side of the router.

NODE ID (App): If Twin-Mode is enabled, the unique Node ID number assigned to the monitoring application.

MODE: The current operating mode of the router. The two possible modes are *Manual*, and *Normal*.

DATE and TIME: The date (day, month, year), day of week, and time currently stored on the router is displayed in these fields.

Change Date/Time: Enter the desired Date, Day of Week, and Time in the appropriate fields. Click the *Change Date/Time* button. This will update the current values stored in the real time clock.

Time Zone: The time zone is displayed in the pop up field.

Adjust for Daylight Savings Time: Automatic adjust for daylight savings is selected by the On/Off radio buttons.

DST Start, DST End: These popup fields display and allow setting the data when daylight savings time starts and ends.

Update TimeZone DST: Clicking this button will update the TimeZone and Daylight Savings Time settings selected above.

Enable Twin Mode Key: Enter in this field the 16 character key to unlock the *Redundant Twin Mode* feature. Click the *Update Keys* button. The feature should be immediately available and the enhanced feature list at the bottom of the page should then include *Redundant Twin Mode*.

Enable Bridge Mode Key: Enter in this field the 16 character key to unlock the *Bridging Router Mode* feature. Click the *Update Keys* button. The feature should be immediately available and the enhanced feature list at the bottom of the page should then include *Bridging Router Mode*.

Update Keys*:* This button processes the the enhanced feature keys fields and activates the associated features.

The bottom of the page lists the enhanced features supported by this router. These may include one or more of the following: *DDNS Support*, *NAT Router Support*, *Redundant Twin Mode*, *852 Bridging Router Mode*.

2.6. Router Setup Page

The Router Basic Setup Page is used to set up basic configuration properties of the router. Following is a brief description of each item listed on the page, as well as instructions on how to set or change items.

2.6.1. Normal Mode Router Setup

When not in bridging mode the Normal mode router setup page looks like the following.

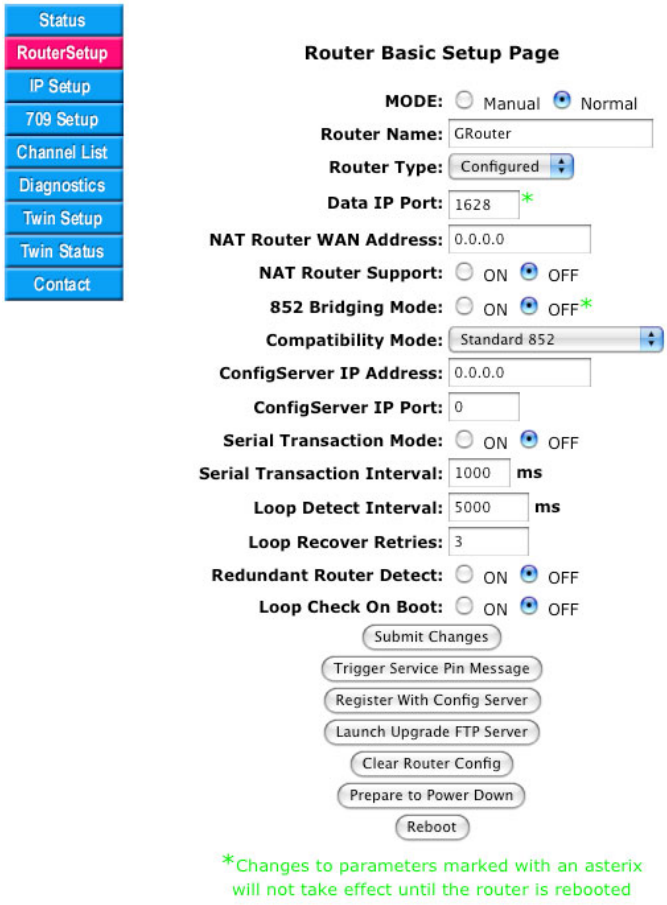


Fig.2.2.10: Router Setup Page

MODE: This displays the current operating mode of the router. To change the router mode, select the radio button that corresponds to the desired mode and then click the "Submit Changes" button. The two possible modes are Manual, and Normal.

- *Manual Mode*: Use manual mode when precise control over the Channel List is desired. In manual mode the user is responsible for the configuration of the Channel List.
- *Normal Mode*: Use normal mode when the router is being configured by a remote configuration server. When in Normal mode, ensure that the Config Server Address is correct (see Config Server Address below).

Router Name: This field allows the user to set or change the name of the router. A descriptive name can be used to give the network administrator information on the location and use of the router (for example, Name: router Room 34). To change the name of the router, type the new

name into the field provided and click the “Submit Changes” button.

Router Type: This popup menu field allows the user to set or change the type of the router. The three choices are *Configured*, *Repeater*, and *Flood*. Select the new value and click the “Submit Changes” button.

- *Configured*: Selecting this router type will cause the GRouter device to filter traffic. The filter rules are based on router tables set on the GadgetGateway by a LON management tool or by the web Tool
- *Repeater*: Repeater mode will drop packets that fail their CRC checks or packets that do not belong to one of the router's domains. Network management packets addressed to the router are not passed but are handled by the router. Otherwise all packets on either side will be forwarded to the other side of the router.
- *Flood*: Selecting this router type will cause the router to forward all packets including network management packets (except those that fail CRC). No other filtering is done. In Flood mode the router is completely transparent to the 709.1 channel. This enables tunneling over IP of some 709.1 networks with odd configurations. Flood type can only be configured in manual mode. Any 709.1 networks connected to GRouter devices in Flood Mode become one large virtual subnet. In contrast with Configured and Repeater modes, Flood mode makes two GRouters appear as essentially a physical layer repeater with two major exceptions:
  - 1) Packets with CRC errors are discarded.
  - 2) Unlike a good physical layer repeater, the gateway can be saturated.

When in Flood Mode, 709.1 network management tools will not be able to communicate with the GRouter device. The router is completely transparent to all 709.1 devices.

DATA IP Port: This field allows the user to set or change the unicast IP port of the router. Enter the new value and click the “Submit Changes” button. The designated default port for 852 client devices is 1628. Changes to the IP port will not take effect until the Router is rebooted.

NAT Router WAN Address: This field allows the user to set or change the WAN IP address of a NAT router. This is only applicable when the router is connected to the internet through a NAT router and needs to communicate with 852 devices on other LANs. To change the value in the field, type in the new value in the dotted format `xx.xx.xx.xx` and click the “Submit Changes” button. When using a NAT router as the internet interface for the LAN upon the GRouter device is connected, the NAT router’s WAN IP address must be static (unless Dynamic DNS is used). The GRouter device’s LAN address must also be static and the 852 port must be mapped by the NAT router.

NAT Router Support: These radio buttons allow the user to set or enable or disable NAT router support. When enabled the node substitutes the NAT Router WAN Address as the source address in appropriate packet headers so that other 852 nodes can respond through the NAT Router. This enables 852 devices that are on other LANs on the WAN side of the NAT router to correctly respond to the local GRouter device. It may or may not be possible to have two GRouter devices on the same LAN side of a NAT Router when NAT support is enabled. Each GRouter would need to have a unique 852 port number mapped by the NAT Router and the NAT router would have to be able to support local loopback of WAN addressed packets. Select

the new value and click the *Submit Changes* button.

852 Bridging Mode: This displays and controls the status of the 852 Bridging Router mode for the router. These buttons only appear if the router has Bridging Router Mode support activated on the *Status Page*. To enable or disable 852 bridging mode, select the radio button that corresponds to the desired state, *On* for enable, *Off* for disable, and then click the *Submit Changes* button. Finally select the *Reboot* button. A description of the configuration of *Bridging Router Mode* is provided in a later section. The device must be rebooted before Bridging mode takes effect.

Compatibility Mode: This popup menu field allows the user to change the configuration server compatibility mode. The three choices are Standard 852, i.Lon Config Server, and CoactiveLL Config Server. Select the new value and click the "Submit Changes" button.

The router-LL config server and some versions of the i.LON config server and were developed before the final version of the ANSI/EIA 852 specification was finalized. Consequently there are variations in how they function.

- *Standard 852 Mode*: Select when using a fully 852 compliant configuration server.
- *Backward Compatibility Mode*: Select when using version 1.x of the i.LON configuration server. This is required for channels with i.LON 1000 devices.
- *Coactive Router-LL (TM) ConfigServer Compatibility Mode*: Select when using the Router-LL configuration server.

ConfigServer IP Address: This field requires information only when the router is operating in Normal mode (See "MODE" above). This is the unicast IP host address of the configuration server for this channel. To change the value in the field, type in the new value in the dotted format `xx.xx.xx.xx` and click the *Submit Change*s button.

ConfigServer IP Port: This field requires information only when the router is operating in Normal mode (See "MODE" above). This is the IP unicast port of the configuration server for this channel. To change the port, type in the new port number (0-65535), and click the *Submit Changes* button. The default designated port for 852 servers is 1629.

Serial Transaction Mode: These radio buttons allow the user to enable or disable Serial Transaction Mode. When enabled the Router will send out 852 configuration updates serially in a round robin fashion to the other 852 devices on the channel instead of in parallel. This means that an update transaction has to complete or time-out with one device before a new transaction is started with the next device. This mode significantly reduces bursts of traffic when devices are added to a channel or their routing data is changed. This may be helpful for low bandwidth 852 channels. Select the new value and click the *Submit Changes* button.

Serial Transaction Interval: This field sets the time interval between successive configuration transactions when Serial Transaction Mode is enabled. The default is 1000 ms. This enables the user throttle the rate at which configuration updates are sent out on the channel and thereby manage traffic. This may be helpful for low bandwidth 852 channels. Enter the new value and click the *Submit Changes* button.

Loop Detect Interval: This value determines the number of milli-seconds between transmission of a loop detection packet. A value of zero disables this feature. The default value is 5000 ms or

5 seconds. Setting this value to much below 1000 is not recommended. If the Loop Detection finds a loop in the network routing, it will cause the GRouter to go unconfigured to prevent runaway traffic. A loop is detected if the router receives its own loop detection message on the opposite side of the router. The router will continue to send loop detection messages and will resume operation once the loop condition is removed. Click *Submit Changes* and the new value is immediately in effect.

Loop Recover Retries: This value determines the number of unsuccessful retires of the loop detection message before a loop condition is considered to have been remedied. The default is three. The minimum allowed value is two. Click *Submit Changes* and the new value is immediately in effect.

Redundant Router Detect: These radio buttons allow the user to enable or disable the detection of redundant 852 routers on the 852 channel. When enabled, no CN data packets are forwarded to any redundant routers. This prevents loops due to redundant routers from occurring. Click *Submit Changes* and the new value is immediately in effect.

Loop Check on Boot: These radio buttons allow the user to change the boot up mode of the router with respect to loop detection. When enabled, the router will not forward CN data packets until after a loop check has completed and no loops were detected. This adds an additional delay at boot-up before the router will begin forwarding packets. The length of the delay is equal to the *Loop Detect Interval* times the number of *Loop Recover Retries*. When disabled, the router will immediately begin forwarding packets on boot-up. Click *Submit Changes* and the new value is immediately in effect.

Submit Changes: This button updates all the configuration information entered on the current web page and refreshes the display.

Trigger Service Pin: This button causes a service pin message to be sent out both the 709.1 and IP interfaces of the router. This can be used when commissioning the router remotely.

Register With Config Server: This button sends an 852 registration request to the config server. This will usually add the device to the config server's list of managed devices. Newer configuration servers may not accept an unsolicited registration message from a device.

Launch Upgrade FTP Server: This button starts up the FTP server needed to perform field upgrades of the GRouter device's firmware. A detailed description of the upgrade process is provided in a later section.

Clear Router Config: This button clears all router configuration information, such as routing tables, back to factory defaults. It does not affect the web or IP address or interface. This is useful when moving the router to a different 852 channel or configuration and a known starting configuration is desirable.

Prepare to Power Down: This button checks the status of any pending flash writes and displays a corresponding web page. If there are no pending flash writes the displayed web page will indicate that it is safe to power down. Otherwise it will display a web page with a timer indicating one should wait until the timer expires before powering down to allow the writes to complete. Once the timer expires a dialog box will display indicating that time is up. This allows one to do something else while flash is writing. The link on the page takes one back to the router setup. If the IP address was changed, the link goes to the new IP address.

Fig.2.11: Safe to Power Down Page

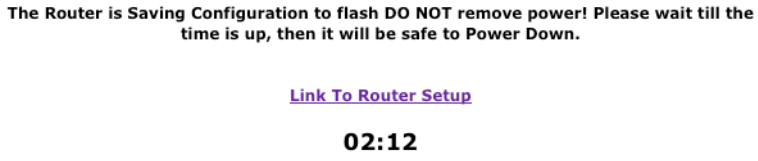


Fig.2.12: Unsafe to Power Down Page

Fig.2.13: Time's Up

Reboot: This button performs a soft reboot of the main processor on the router. This is needed anytime any of the parameters marked with a green asterisk change. The reboot button will also check for any pending flash writes and the reboot will be delayed until the flash writes have completing. When rebooting the following page will be displayed. The page includes a timer with an estimate of when the reboot will be completed, this includes the time to complete flash writes if any. Once the timer expires a dialog will display indicating that the time is up. See above. The link to Gateway will return to the status page of the device at its latest IP address.

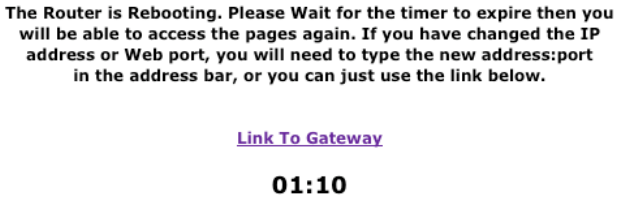
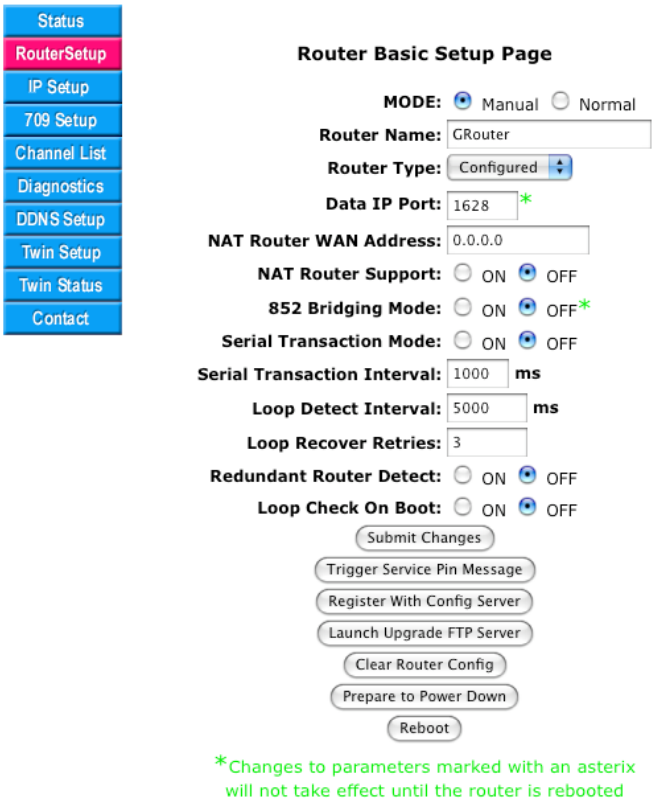


Fig.2.14: Reboot Page

Once rebooting has completed reenter http://10.0.2.40 or whatever the IP address of the router is to go back to the *Status* page.

2.6.2. Manual Mode Router Setup

When in manual mode the router setup page is the same as the Normal mode except that the compatibility mode, configuration server IP address, and, port fields are not displayed.



2.7. IP Setup Page

The IP Setup Page displays status additional information about the Gateway's IP setup not included in the Router Setup page. Following is a brief description of each item listed on the page, as well as instructions on how to set or change items. All the parameters on this page require a reboot before taking effect.

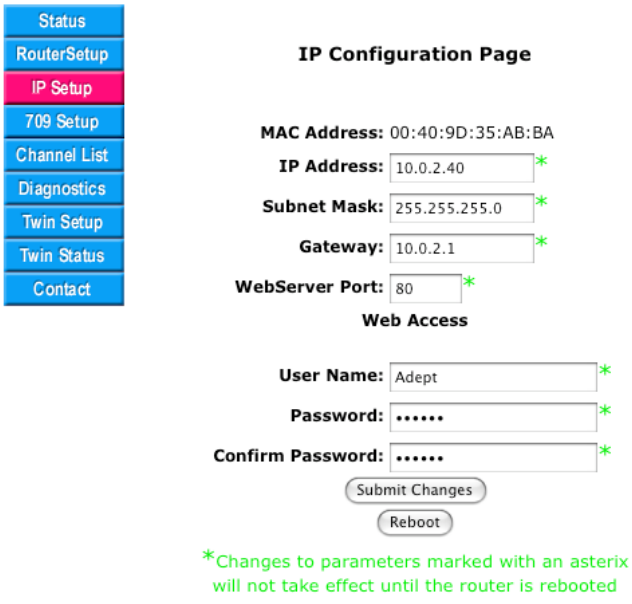


Fig.2.15: IP Setup Page

MAC Address: The physical address of the Ethernet interface in HEX. This is a read only field.

IP Address: The IP address currently assigned to the Gateway. This is the unicast IP host address of the router. To change the value in the field, type in the new value in the dotted format `xx.xx.xx.xx` and click the *Submit Changes* button. The IP host address change will not take effect until after the router is rebooted. Be careful to record the new address as it will not be possible to communicate with the GRouter without a valid IP address.

Subnet Mask: The IP subnet mask assigned to the router. To change the value in the field, type in the new value in the dotted format `xx.xx.xx.xx` and click the *Submit Changes* button. The subnet mask change will not take effect until after the router is rebooted.

Gateway: The address of the IP router or gateway used by the GRouter device to reach other devices that are not in its local network. To change the value in the field, type in the new value in the dotted format `xx.xx.xx.xx` and click the *Submit Changes* button.

Web-Server Port: This field allows the user to change the IP port used by the embedded web server on the device. The default is port 80. When used with a NAT router and port mapping, port 80 may be in use by another device. The device must be restarted before changes to the web-server port will be activated. To change the value, type in the new value and click the *Submit Changes* button and then click the *Reboot* button. A typical alternate web server port is 8080. To access the web server on any port other than 80, use the following format in the web browser:

```
http://IP Address:Port
```

for example

```
http://10.0.2.40:8080
```

Reboot: This button performs a soft reboot of the main processor on the router. This is needed for any of the changes on this page to take effect. When rebooting the Rebooting page will be displayed (see previous section).

2.8. WiFi Setup Page

For GRouter devices equipped with WiFi IP interfaces the WiFi setup button will appear and will display the WiFi setup page.

MODE: This displays the WiFi channel access mode of the router. To change the WiFi mode, select the the desired mode in the popup menu and then click the *Submit Changes* button. The mode will not change until after a reboot. The Four possible modes are Any type, Infrastructure, Ad hoc (join or create), and Ad hoc (join only).

- *Any Type*: Will attempt to connect on each of access modes until it finds one with the chosen SSID.
- *Infrastructure*: Use this mode for connecting to an access point.
- *Ad hoc (join or create)*: Use this mode for creating an ad hoc network if one does not exist or joining one that already exists with the chosen SSID
- *Ad hoc (join only)*: Use this mode for joining an existing ad hoc network

SSID: To change the SSID of the WiFi channel, type the new value into the field provided and click the *Submit Changes* button.

Channel: To change the WiFi channel number select it from the popup menu. To search for an available channel, select *Search*. In search mode, the router will search all channels until it finds one with the chosen SSID. Select the new value and click the *Submit Changes* button.

WEP: Select the appropriate radio button. The two choices are Enabled and Disabled. Select the new value and click the *Submit Changes* button. WEP may not be enabled when WPA is enabled and vice versa.

Default Key: WEP stores four different keys that may be used to join a WEP protected network. Only one key is needed for any network . Select which key from the popup menu and click the *Submit Changes* button.

KEY 0 - KEY3: To change the WEP Key of the WiFi channel, type the new value into the field provided and click the *Submit Changes* button. The length of the key may be either 13 Hex digits (for 64 bit encryption) or 26 Hex digits (for 128 bit encryption). The length needed is determined by the access point or ad hoc network settings.

WPA: Select the appropriate radio button. The two choices are Enabled and Disabled. Select the new value and click the *Submit Changes* button. WEP may not be enabled when WPA is enabled and vice versa.

Passphrase: To change the WPA passphrase of the WiFi channel, type the new value into the field provided and click the *Generate WPA PSK from Passphrase* button. The length of the passphrase must be between 8 and 63 characters inclusive.

Generate WPA PSK from Passphrase: This button generates the WPA key from the given passphrase.

User Name: To change the WPA logon user name, type the new value into the field provided and click the *Submit Changes* button.

Password: To change the WPA logon password for the given user, type the new value into the field provided and click the *Submit Changes* button.

Submit Changes: This button updates all the configuration information entered on the current web page and refreshes the display.

Reboot: This button performs a soft reboot of the main processor on the router. None of the WiFi parameter changes will be put into effect until after a reboot. Take care when making changes as an errant configuration may result in loss of communication and no access to the configuration pages. The only way to restore communications may be to reset to factory defaults.

2.9. 709 Setup Page

The 709 Setup Page is used to set up the 709.1 protocol specific properties of the router. This information includes the subnet address, node address, domain address, node ID and node state numbers for both sides of the router and the twin mode monitoring application (when enabled) as well as the subnet and group forwarding tables. Following is a brief description of each item listed on the page, as well as instructions on how to set or change items. The Page has three views, one for Side A (IP), the second for Side B (FTT-10, and the third for the twin mode application (when enabled). In Bridging Router mode both Side A and Side B are IP. The main top section of the page looks like the following.

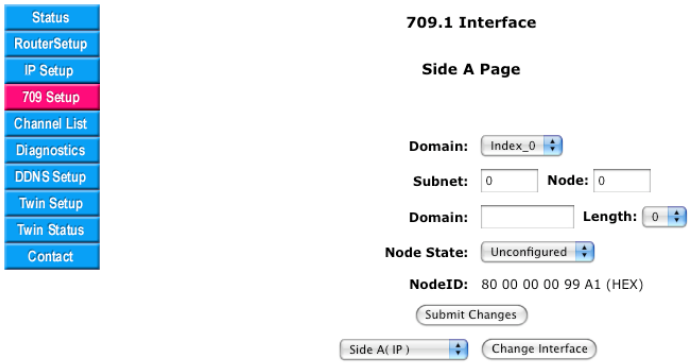


Fig.2.16: 709 Side B Setup Page Main Section

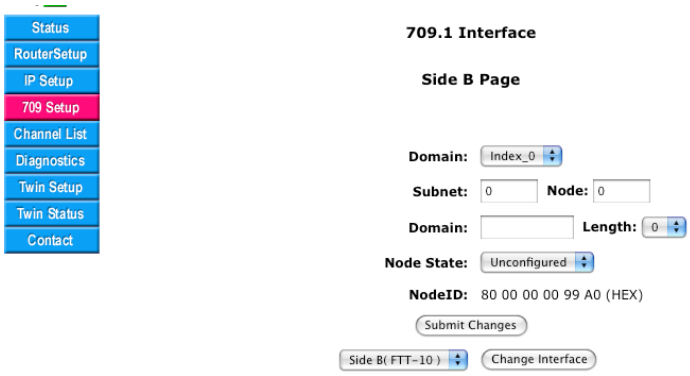


Fig.2.17: 709 Side B Setup Page Main Section

2.9.1. Node Parameters

The management of these parameters is usually performed by a management tool such as Echelon's LonMaker®. If you are using a management tool, it is recommended that these parameters not be changed manually. However, the Interface Menu does allow users to change the interface parameters manually, if desired. Not all node parameters are editable from this interface (for example group membership) and consequently a node may not be fully configured. This capability is provided for debugging or other special circumstances where a network management tool is not available and minimal functionality is needed.
There are three 709 interfaces or stacks on the GR4. These are called Side A, Side B, and Application. The Applications refers to the Twin Mode application when enabled. Each interface

is qualified in parenthesis to the type of channel, IP or component network LON. When in bridging router mode both Side A and Side B are IP and the LON interface is disabled.

Domain Index: A 709.1 node may be a member of two domains. In each domain a node may have a distinct subnet and node number. Choose the domain index to edit then Click *Submit Changes*.

Subnet: When a node is unconfigured the subnet may be zero. Valid configured subnet numbers are from 1 to 255. Enter the subnet number then click *Submit Changes*.

Node: When a node is unconfigured the node number may be zero. Valid configured node numbers are from 1 to 127. Enter the node number then click *Submit Change*s.

Domain Number: The number of valid domains is a function of the *Domain Length*. Zero is a valid domain number but is reserved for network management. Enter the *Domain Number* then click *Submit Change*s.

Domain Length: The *Domain Length* may be 0, 1, 3, or 6 bytes long. Choose the *Domain Length* from the popup menu then Click *Submit Change*s.

Node State: The *Node State* determines whether the node operates in *Configured* or *Unconfigured* mode. In manual mode the default state for a new device is *Unconfigured*. Setting the state to *Unconfigured* allows you to temporarily disable the device while editing the forwarding tables. Choose the *Node State* from the popup menu then click *Submit Change*s.

NodeID: The *NodeID* is a unique 48 bit number assigned to each 709.1 node. This is a read only field in hexadecimal notation.

Submit Changes: This button updates node parameter information for the current interface and refreshes the display.

Interface: To select which interface is to be edited, choose the interface from the popup menu and then click the *Change Interface* button.

- *Side A (LON)*: Selects the *Side A* interface for editing.
- *Side B (IP)*: Selects the *Side B* interface for editing.
- *Application*: Selects the TwinMode Application interface for editing

Change Interface: This button which interface to edit and refreshes the display.

2.9.2. Forwarding Tables

The *709 Setup Page* also allows the direct setting of the 709.1 subnet and group forwarding tables. This is most useful in manual mode or in situations where a special configuration is needed. The forwarding table portions of the page are shown below.

When the Side A interface is shown, the Side A table is used to determine if packets received on the Side A should be forwarded across and transmitted out the Side B . Likewise when the Side B interface is shown, the Side B Table is used to determine if packets received on Side B should be forwarded across and transmitted out Side A.

For each table the bits are displayed from left to right in increasing order of bit position. Bit position one refers to subnet number one and so forth. Clicking on a bit will toggle the bit value and store the new value in memory. A value of one in a bit position means forward, to the

other side of the router, packets addressed to the corresponding subnet or group. A value of zero in a bit position means do not forward, to the other side of the router, packets addressed to the corresponding subnet or group.

For example, a 1 in the subnet table on Side A means forward to side B any packets received on Side A that are addressed to the corresponding subnet. A 0 in the subnet table on Side A means do not forward any packets to side B that are addressed to the corresponding subnet. Likewise for the group table.

Clear Subnet Table: This button clears all the subnet bits by assigning each a value of zero and stores the new values in memory.

Set Subnet Table: This button sets all the subnet bits by assigning each a value of one and stores the new values in memory.

Clear Group Table: This button clears all the group bits by assigning each a value of zero and stores the new values in memory.

Set Group Table: This button sets all the group bits by assigning each a value of one and stores the new values in memory.

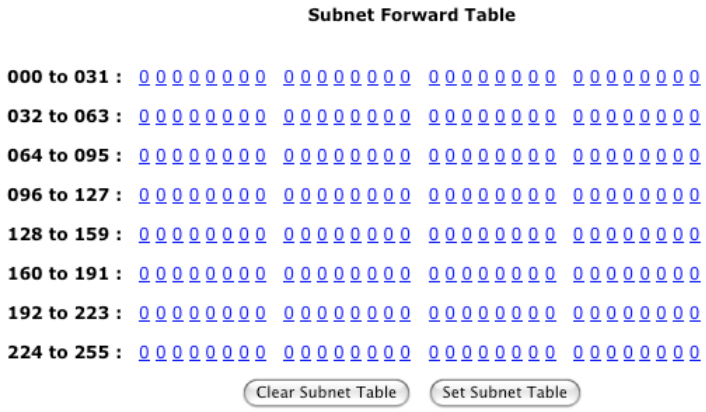


Fig.2.18: Subnet Forwarding Table

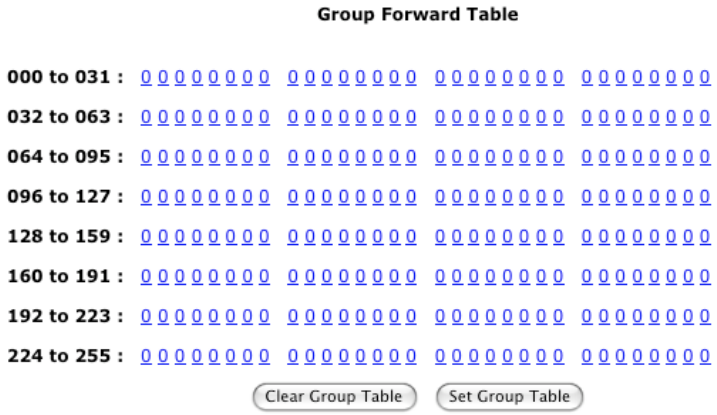


Fig.2.19: Group Forwarding Table

2.10. Channel List Page

In Normal mode the Channel Membership List is controlled by the configuration server. Whereas in Manual mode the Channel Membership List must be configured manually. This page allows the user to add and delete the devices from the 852 channel when in Manual mode. Following is a brief description of each item listed on the page, as well as instructions on how to set or change items. The behavior of the page is different for Normal and Manual mode.

2.10.1. Normal Mode Channel List Page

In Normal mode, the page looks like the following when the device is the only member in the channel.

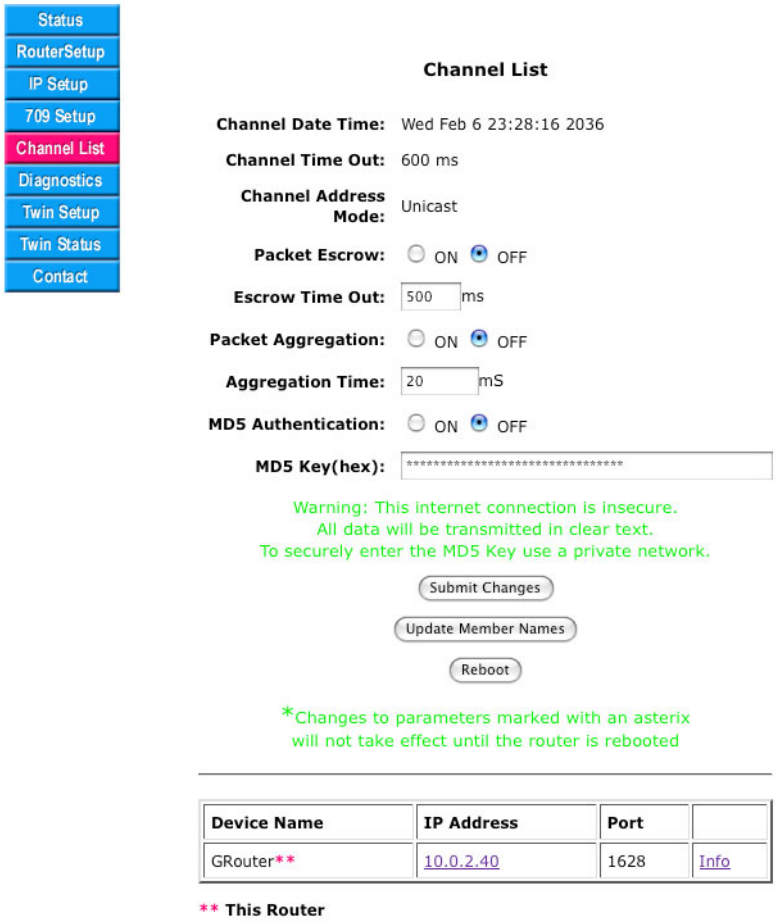


Fig.2.20: Channel List Page

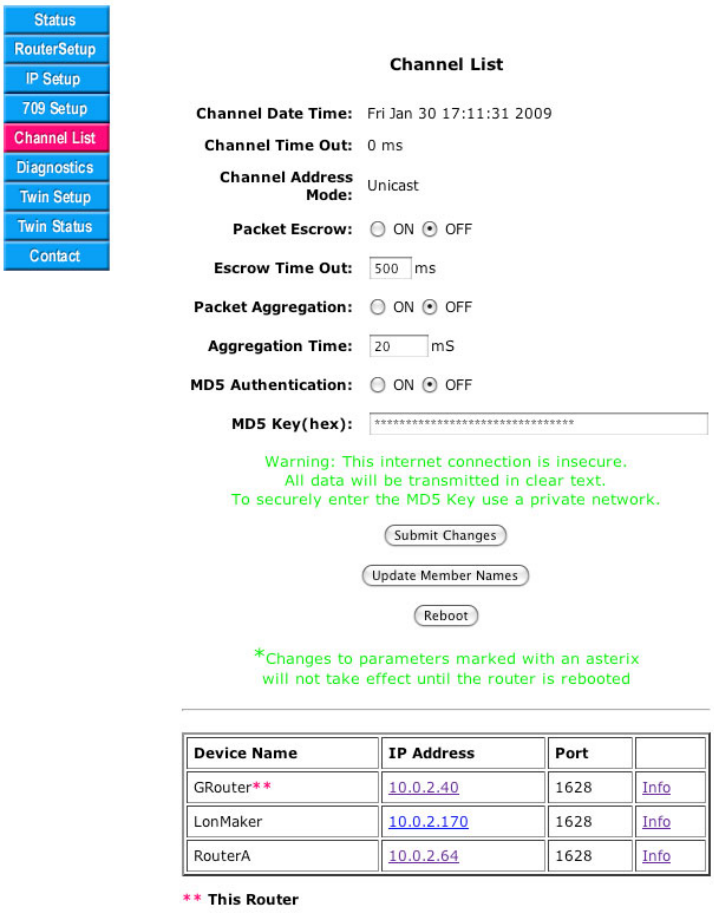


Fig.2.21: Channel List Page with Multiple Members

Channel Date Time: This is the 852 DateTime when the Channel Membership List was last changed. This is a read only field for debugging purposes. In Normal mode, this value is governed by the configuration server.

Channel Time Out: This is the 852 Channel Time Out. This is a read only field for debugging purposes. In Normal mode, this value is governed by the configuration server..

Channel Address Mode: Is either *Unicast* or *Multicast*. *Multicast* is only supported in manual mode. In normal mode, this value is governed by the configuration server.

Packet Escrow: These radio buttons enable or disable Packet escrow mode. Packet escrow is used to escrow and reorder any out of order 852 IP CN Data packets during the escrow time.

Escrow Time: This value determines the time during which 852 IP CN Data packets are escrowed waiting for out of order packets to show up. This only occurs when Packet Escrow is enabled.

Packet Aggregation: These radio buttons enable or disable Packet Aggregation mode. Packet aggregation can be used to reduce the number of 852 IP packets sent to a given device by aggregating multiple 852 IP CN Data packets into one big 852 IP packet.

Aggregation Time: This value determines the time during which outgoing 852 IP CN Data packets are aggregated when Packet Aggregation is enabled.

MD5 Authentication: These radio buttons enable or disable MD5 Authentication of all 852 IP packets sent or received by this device. MD5 authentication provides for enhanced security over the internet. In order to work all devices engaged in communication must have authentication enabled. An MD5 digest is appended to each sent packet. When enabled, unauthenticated packets are dropped. Authentication only works with Echelon Devices or LonMaker when in Standard 852 Mode (see RouterSetup). When in iLONConfigServer Mode, Echelon uses a non standard authentication algorithm.

MD5 Key (hex): This value is the shared secret used by the MD5 Algorithm to compute the authentication digest. The value must be 16 hex pairs (32 hex digits) long. This value should not be sent in the clear over the internet. In order to accomplish this for the Ethernet version, set the MD5 key while the GR4 router (Ethernet) is attached via an isolated Ethernet channel to the PC running a web browser. To set the MD5 Key for WiFi version GR4 routers, first set up the WiFi to use WPA encryption.

Submit Changes: This button updates node parameter information and refreshes the display.

Update Member Names: This button updates the names of the devices in the channel and refreshes the display. The member names are not used by the 852 protocol and are merely displayed as a user friendly way of distinguishing devices. The member names are usually not shown because they are not included in the channel list update messages and must be retrieved explicitly from the devices. Pressing this button will perform the retrieval.

Reboot: This button reboots the device. See the Router Setup page for a detailed description of the reboot button behavior.

Channel List: This lists all the devices in the channel by name. The list also includes the IP address and port of each device. The IP address field is also a link to the status web page of the associated device. The Info field is a link to the device detail page for each device.

2.10.2. Manual Mode Channel List Page

The Manual mode page operation is the same as Normal mode with the exceptions that multi-cast addressing may be specified and devices may be added and removed from the channel. Only those fields that are different from Normal mode are described here. In Manual mode, the page looks like the following.

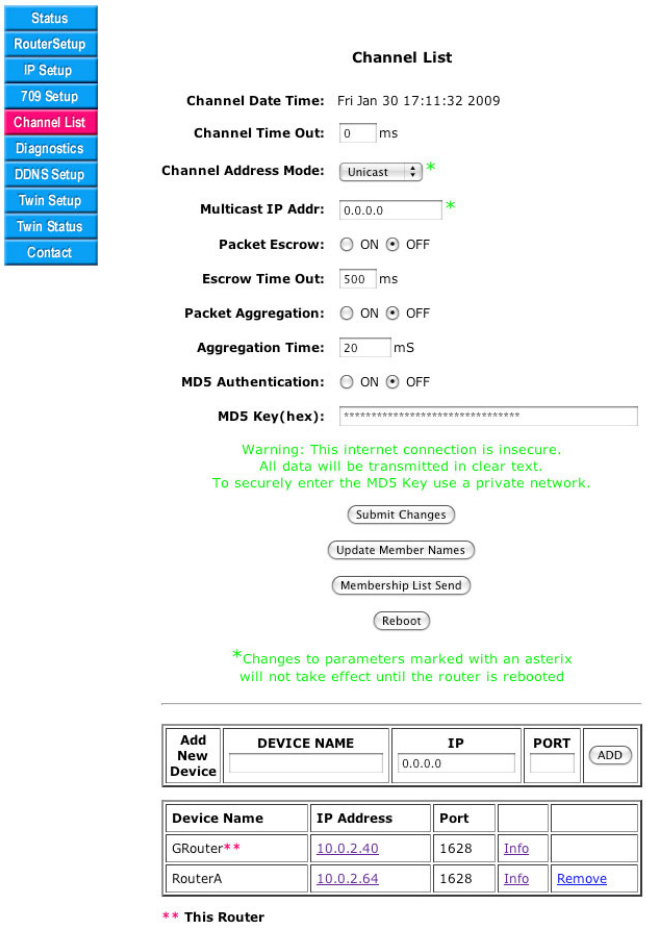


Fig.2.22: Channel List Page in Manual Mode

Channel Address Mode: Is either *Unicast* or *Multicast*. *Multicast* is only supported in manual mode. Select the desired mode from the popup menu and click *Submit Change*s.

Multicast IP Addr: This is the multicast IP address of the router. This is used when the channel in in *Multicast* mode. Multicast addresses are in the range 224.0.0.0 to 239.255.255.255. Addresses ending in ".0 " are reserved. Some addresses ending in ".1" are used for multicast host broadcasts and should also be avoided. Examples of valid multicast addresses include: 225.0.0.2, 225.0.0.3, 225.1.2.3. You may need to check with your network administrator to see what multicast addresses are available for your use. Enter the desired value and click *Submit Change*s. The device will have to be rebooted for any Multi-cast addresses changes to take effect. All devices with same multi-cast address will communicate on port 1628.

Membership List Send: This button sends a copy of the this device's membership list to all the other devices in the list. When in manual mode a device will accept a membership list from any device already in its own list. Together with the Membership List Send button, this enables easy configuration of large manual mode channels without the overhead of a configuration server. Designate one device as the source of the channel list, (say device A). Enter all the other devices in Device A's channel list (say B, C, D) for example. No go to each of the other devices and only add Device A to their channel lists. Now go back to Device A and press the Update Member Names button on Device A. Now all the other devices will have their channel lists set the same as Device A's.

Reboot: This button reboots the router. See the Router Setup page section for a more detailed description.

Add New Device: This form adds a new device to the channel list. Enter the device name, IP address, and port in the associated fields and the click the *ADD* button.

Channel List: This lists all the devices in the channel by name. The list also includes the IP address and port of each device. The IP address field is also a link to the status web page of the associated device. The Info field is a link to the device detail page for each device. The remove link will remove the associated device from the channel list.

2.11. Device Detail Page

The device detail page provides useful information about the addressing and configuration of each device. This page is accessed from the a device's *Info* link in the channel list.

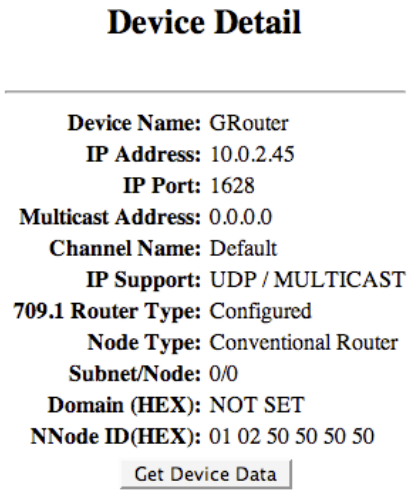


Fig.2.23: Device Detail Page

Device Name: The name of the device.

IP Address: The current IP address of the device.

IP Port: The current IP Port number on which the device is communicating.

Multicast Address: The address that the device uses if it is set to multicast addressing.

Channel Name: The name of the channel to which the device belongs.

IP Support: The protocols supported by this device. These include *UDP*, *TCP*, and *Multicast*.

709.1 Router Type: The type of router of the device. The possible types are *Configured*, *Repeater*, or *Flood*.

Node Type: The mode in which the router is operating. The only type currently supported is *Conventional Router*.

Subnet/Node: The ANSI/EIA 709.1 subnet number and node number of the device. This information is not always available.

Domain (HEX): The domain number of the ANSI/EIA 709.1 device. This information is not always available.

Node ID (HEX): The IP-side Node ID of the device.

Get Device Data: Clicking this button will retrieve all of the information from the device and update the Device Detail Page. This button is not displayed on the device detail page of the local device.

2.12. Diagnostics Page

The Diagnostics Page provides statistics about the performance of the router. This page is helpful in debugging configuration as it can show that packets are being forwarded across the router.. Following is a brief description of each item listed on the page, as well as instructions on how to set or change items.

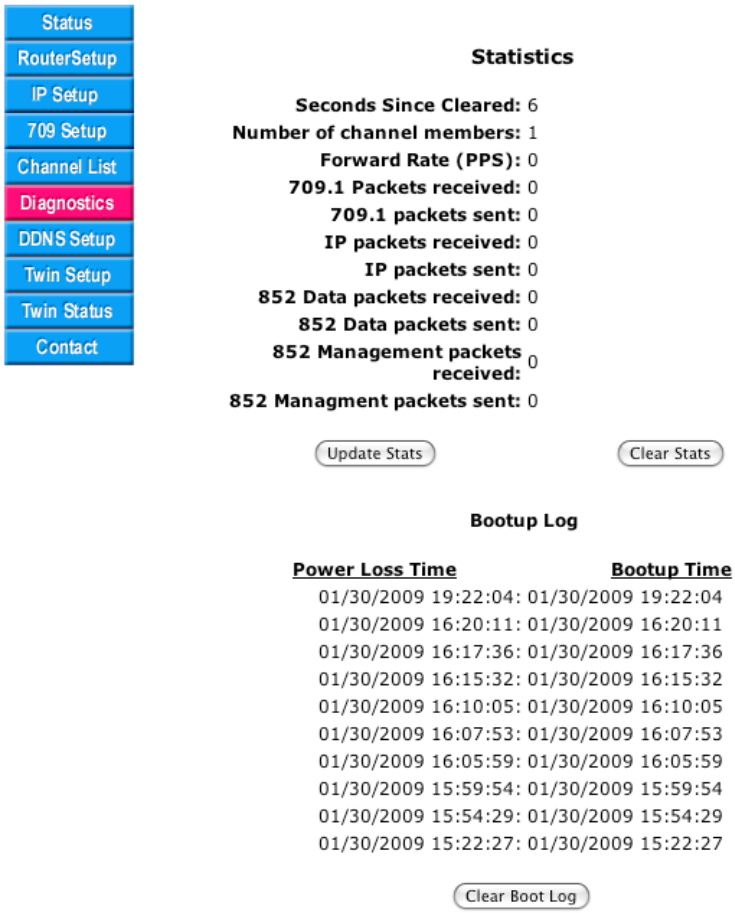


Fig.2.24: Diagnostics Page

Seconds Since Cleared: This is the number of seconds since the statistics were cleared. This is a read only field for debugging purposes.

Number of Channel Members: This is a read only field for debugging purposes. When not in Bridging mode, this is the number of devices in the 852 channel on Side B (IP). In Bridging Mode however, both Side A and Side B are IP channels. In Bridging mode this provides the number of devices in the Side A channel only.

Forward Rate (PPS): This is the average number of packets per second forwarded by the router since the statistics were cleared.

709.1 packets received: This is the total number of packets received in from Side A (709.1) by the router since the statistics were cleared. In Bridging mode this provides the total number of IP 852 packets received in from Side A.

709.1 packets sent: This is the total number of packets sent out to Side A (709.1) by the router

since the statistics were cleared. In Bridging mode this provides the total number of IP 852 packets sent out to Side A.

IP packets received: This is the total number of 852 packets received in from Side B (IP) by the router since the statistics were cleared. This total includes both all the 852 data packets and the 852 configuration (management) packets.

IP packets sent: This is the total number of 852 packets sent out to Side B (IP) by the router since the statistics were cleared. This total includes both all the 852 data packets and all the 852 configuration (management) packets.

852 Data packets received: This is the total number of 852 Data packets only received in from Side B (IP) by the router since the statistics were cleared.

852 Data packets sent: This is the total number of 852 Data packets only sent out to Side B (IP) by the router since the statistics were cleared.

852 Management packets received: This is the total number of 852 Management packets only received in from Side B (IP) by the router since the statistics were cleared.

852 Management packets sent: This is the total number of 852 Management packets only sent out to Side B (IP) by the router since the statistics were cleared.

Update Stats: This button updates the statistics and refreshes the display.

Clear Stats: This button zeros out the statistics, restarts the statistics time counter and refreshes the display.

Bootup Log: This list shows the last ten date and times that the GRouter device has been reset or power cycled. The first column labeled Power Loss Time shows the time the device was powered off or reset. The second column labeled BootUp time shows the time the device rebooted. If the times are identical then the device was reset not power cycled. If the times are different the difference is the length of time the device lost power.

Clear Boot Log: This button clears the boot up log and sets all the times and dates to zeros.

2.13. DDNS Setup Page

The *DDNS Setup Page* allows the configuration of DDNS capability. This page only appears when in manual mode. Following is a brief description of each item listed on the page.

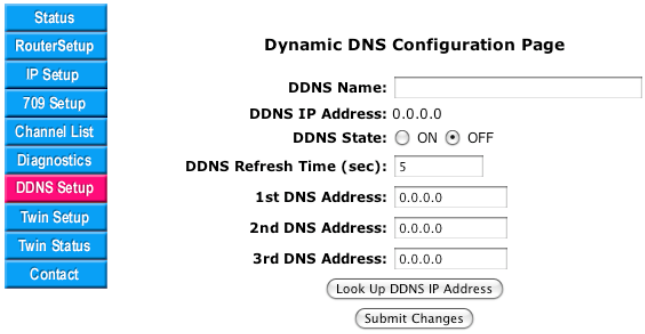


Fig.2.25: Dynamic DNS Configuration Page

DDNS Name: The is the domain name for the associated NAT router that includes DDNS support. The DDNS name is hosted by `dyndns.com`.

DDNS IP Address: This is the current WAN address of the NAT router.

DDNS State: These two radio buttons are used to enable or disable DDNS support. For DDNS to work, *DDNS State* must be *On* and the device must be in manual mode and NAT support must also be enabled.

DDNS Refresh time: This field is used to set how many seconds expire before a node does a DNS lookup of the DDNS name in order to see if its DDNS IP address has changed. If so it updates the other nodes with its new IP address.

1st DNS Address: This is the IP address of a DNS server. The GRouter device performs DNS address lookups on of the *DDNS Name* with this server.

2nd DNS Address: This is the IP address of a DNS server. The GRouter device performs DNS address lookups on of the *DDNS Name* with this server if the first server is not available.

3rd DNS Address: This is the IP address of a DNS server. The GRouter device performs DNS address lookups on of the *DDNS Name* with this server if the first and second servers are not available.

Look Up DDNS IP Address: This button forces an immediate DNS address lookup of the devices *DDNS Name*.

Submit Changes: This button updates the configuration memory of the device and refreshes the web page to reflect any changes.

2.14. Contacts Page

The Contacts Page contains contact information and links for Smart Controls Systems, Inc.

Fig.2.26: Contacts Page

3. Optional Features

3.1. 852 to 852 Bridging Router Mode

In order to better support large installations with dozens of IP to LON routers a GRouter device can be configured in 852 to 852 bridging router mode. Its an IP 852 bridge and a 709.1 LON Routers. In this mode one GRouter device is an IP bridge between two logical 852 channels looks like a LON router to any LON devices. When acting in bridging router mode, the router is a member of two logical 852 channels sharing one ethernet interface. The router bridges traffic between the two 852 IP channels. This overcomes limitations of some network managers on the number of 852 devices per channel and provides for enhanced scalability by partitioning the 852 traffic seen by any given router. Some network management tools with an 852 interface have an artificially low limitation on the number of 852 devices that the tool can communicate with on its 852 channel. For low bandwidth 852 channels, Bridging Router mode allows partitioning of the 852 devices so that the low bandwidth devices can be on a different 852 channel from the high bandwidth devices.

The architecture of the GRouter in bridging router mode is shown below.

Fig.3.1: 852 Bridging Router Architecture

3.2. Bridging Router Setup

When 852 to 852 bridging router mode is enabled the GG router has two IP side 852 interfaces. One is labeled the Side A and the other the Side B. Both interfaces share the same IP host address but each interface has a unique IP port and a unique configuration server (when in Normal mode). Each side can be in either Normal or Manual mode independently. In addition, Serial Transaction Mode can be independently enabled or disabled on each side. The description below only includes those fields that are unique to Bridging Router mode. When 852 bridging router mode is enabled there could be up to two configuration servers, one for each of the bridged channels, that is, Side A and Side B.

3.2.1. Router Setup Page

When *852 to 852 Bridging Router Mode is enabled*, the router setup page looks like the following.

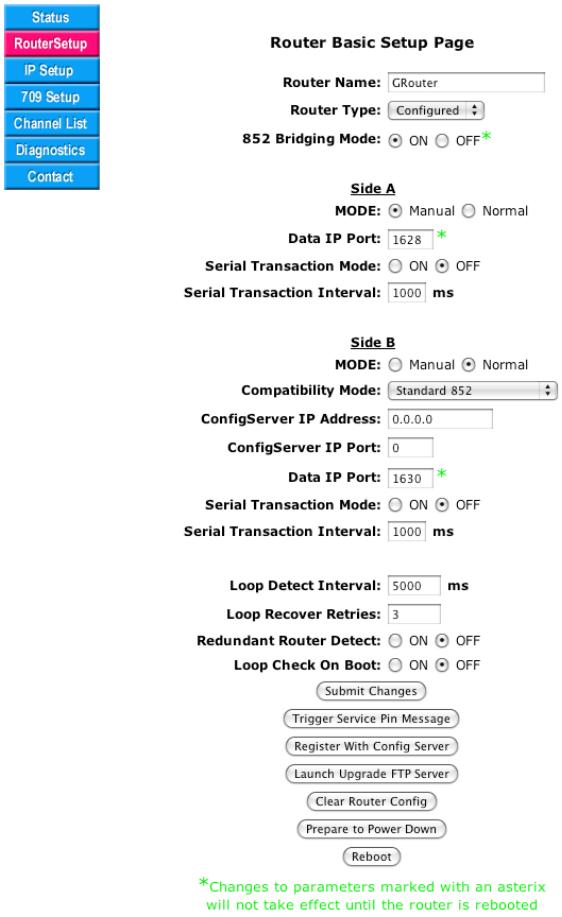


Fig.3.2: Bridging Router Mode Setup Page

Side A Mode: These radio buttons determine the operational mode for Side A, either Manual or Normal. To change select the appropriate radio button and click the Submit Changes button.

Side A Data IP Port: This field appears when the router is in 852 bridge mode. It allows the user to set or change the Side A unicast IP port of the router. To change the port, type in the new port number (0-65535), and click the *Submit Changes* button.

Side A ConfigServer IP Address: This field appears only when the router is operating in 852 Bridge mode and Side A is in Normal Mode. This is the unicast IP host address of the configuration server for the Side A 852 channel. To change the value in the field, type in the new value in the dotted format `xx.xx.xx.xx` and click the *Submit Changes* button.

Side A Serial Transaction Mode: These radio buttons allow the user to enable or disable Serial Transaction Mode for Side A. When enabled the Router will send out 852 configuration updates serially in a round robin fashion to the other 852 devices on the channel instead of in parallel. This means that an update transaction has to complete or time-out with one device before a new transaction is started with the next device. This mode significantly reduces bursts of traffic when devices are added to a channel or their routing data is changed. This may be helpful for low bandwidth 852 channels. Select the new value and click the *Submit Changes* button.

Side A Serial Transaction Interval: This field sets the time interval between successive configuration transactions when Serial Transaction Mode is enabled for Side A. The default is

1000 ms. This enables the user throttle the rate at which configuration updates are sent out on the channel and thereby manage traffic. This may be helpful for low bandwidth 852 channels. Enter the new value and click the *Submit Changes* button.

Side A ConfigServer IP Port: This field appears when the router is in 852 bridge mode and Side A is in Normal mode. It allows the user to set or change the Side A unicast IP port of the config server for the Side A 852 channel. To change the port, type in the new port number (0-65535), and click the *Submit Changes* button.

Side B Mode: These radio buttons determine the operational mode for Side B, either Manual or Normal. To change select the appropriate radio button and click the Submit Changes button.

Side B Data IP Port: This field appears when the router is in 852 bridge mode. It allows the user to set or change the Side B unicast IP port of the router. To change the port, type in the new port number (0-65535), and click the *Submit Changes* button.

Side B ConfigServer IP Address: This field appears only when the router is operating in 852 Bridge mode and Side B is in Normal Mode. This is the unicast IP host address of the configuration server for the Side B 852 channel. To change the value in the field, type in the new value in the dotted format `xx.xx.xx.xx` and click the *Submit Changes* button.

Side B ConfigServer IP Port: This field appears when the router is in 852 bridge mode and Side B is in Normal mode. It allows the user to set or change the Side B unicast IP port of the config server for the Side B 852 channel. To change the port, type in the new port number (0-65535), and click the *Submit Changes* button.

Side B Serial Transaction Mode: These radio buttons allow the user to enable or disable Serial Transaction Mode for Side B. When enabled the Router will send out 852 configuration updates serially in a round robin fashion to the other 852 devices on the channel instead of in parallel. This means that an update transaction has to complete or time-out with one device before a new transaction is started with the next device. This mode significantly reduces bursts of traffic when devices are added to a channel or their routing data is changed. This may be helpful for low bandwidth 852 channels. Select the new value and click the *Submit Changes* button.

Side B Serial Transaction Interval: This field sets the time interval between successive configuration transactions when Serial Transaction Mode is enabled for Side B. The default is 1000 ms. This enables the user throttle the rate at which configuration updates are sent out on the channel and thereby manage traffic. This may be helpful for low bandwidth 852 channels. Enter the new value and click the *Submit Changes* button.

Register With Config Server: This button sends an 852 registration request to the appropriate config server for Side A and separately to the config server for Side B when either/both Side A and Side B are in normal mode. This will usually add the device to the config server's list of managed devices.

3.2.2. 709 Setup Page

When *852 to 852 Bridging Router Mode is enabled*, the 709 setup page shows both Side A and Side B has IP channels.

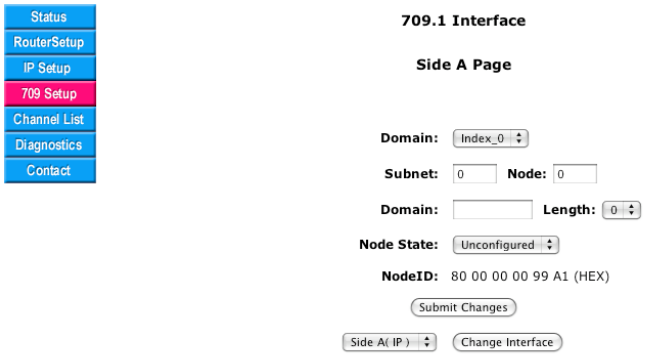


Fig.3.3: Bridging Router Mode Setup Page

3.2.3. Bridging Router Mode Channel List Page

In Bridging Router mode there are two channel lists, one for each side of the router. The channel list page will display either Side A or Side B, whichever one is selected. The items on the page will be dependent on whether the particular side in in Normal or Manual mode. See the documentation for the Channel list page given previously for details. Only those fields that are different for Bridging mode are documented below

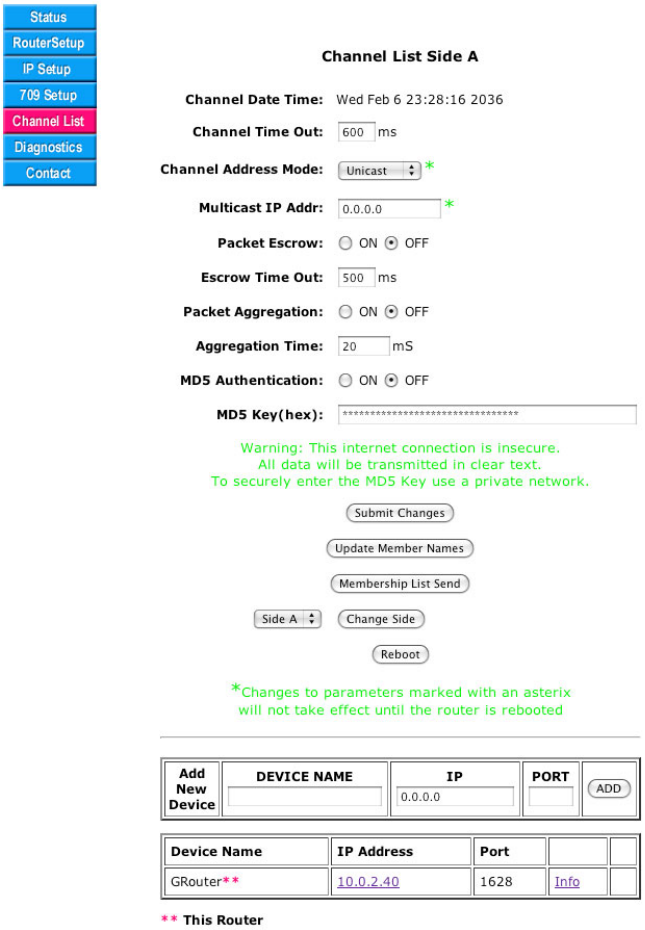


Fig.3.4: Side A Channel List Page in Manual Mode

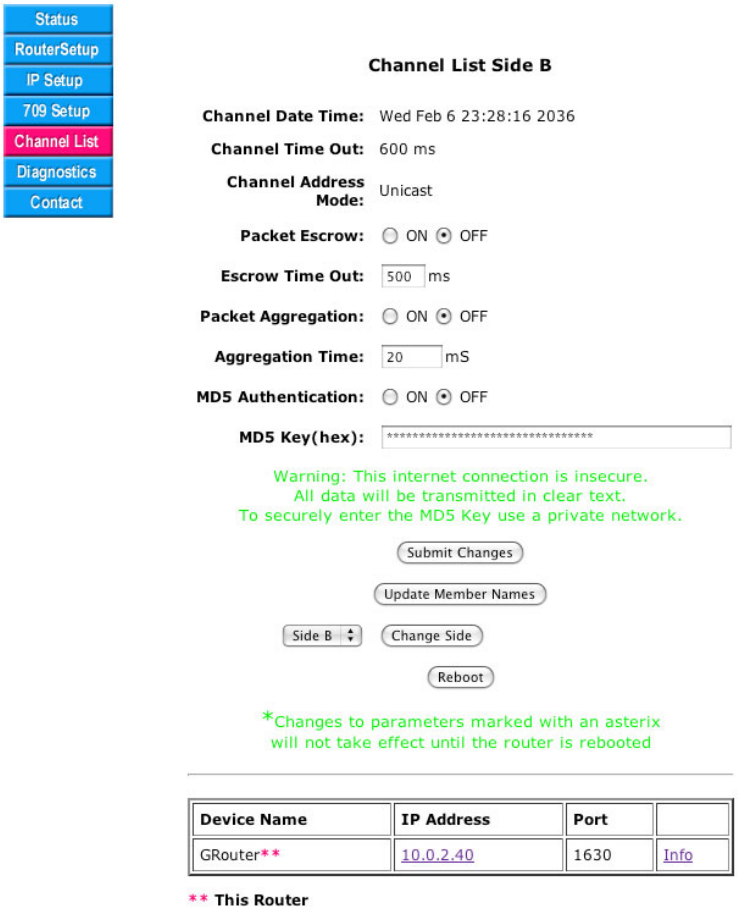


Fig.3.5: Channel List Page in Manual Mode

Side: This pop up field selects which Side to display. To change sides select the desired side and then click the Change Side button.

Change Side: This button changes the Side displayed to the side specified by the Side field.

3.3. Redundant Twin Mode

The Twin Redundant Mode enables two GRouter devices to operate as a redundant pair for high availability applications without generating duplicate traffic. This enhanced capability increases reliability and eliminates some single mode failure sources. A simple diagram showing a redundant connection between two channels is shown below.

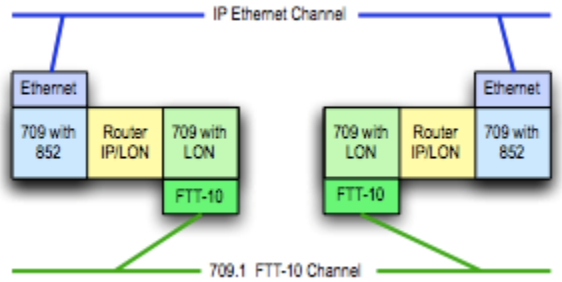


Fig.3.6: Two redundant routers between the same channels

Although it is possible for a pair of conventional 709.1 routers to be identically configured and connected between the same two channels, this configuration induces a doubling of the traffic between those two channels. The built-in duplicate detection mechanism in 709.1 discards the duplicate packets at each receiving node. However, the doubled traffic load could tax network bandwidth and create other problems.

In *Redundant Twin Mode* (or for the sake of brevity, *Twin Mode*), both routers are identically configured and connected between the same two channels as per the case described above but unlike the case above only one of the two routers is forwarding packets. This feature achieves the increased system reliability of having a redundant backup router without the drawbacks of doubled traffic. The Twin Mode routers monitor each others health and operational status and dynamically activate forwarding as needed should one of the other fail. Failures are detected, diagnosed, and reported so that repairs can be made to maintain continuous availability. Should there be a fault in either interface then both routers will go active and forward traffic until the fault has been healed. In addition, the router configuration is periodically automatically synchronized between the two routers to reduce fail-over time and increase the fidelity between the backup and primary router operation. Also supported is manual synchronization which makes it more convenient to replace one of the redundant pair and replicate its configuration. A high availability building network can be constructed using pairs of redundant twin mode routers and a redundant switched ethernet network. An example network showing the application of Twin Mode is shown below.

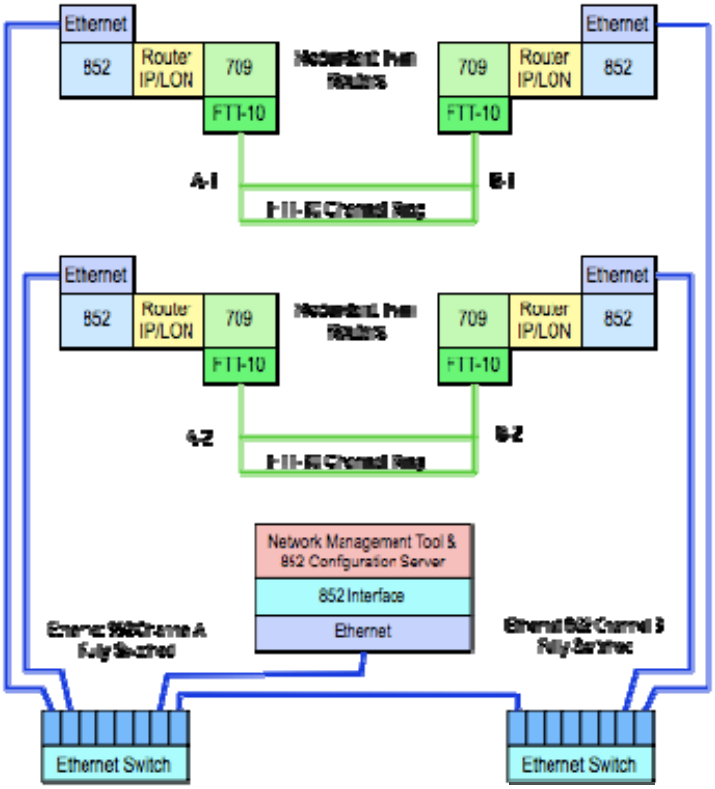


Fig.3.7: Redundant Twin Mode Application

3.3.1. Definitions

For the purpose of clarifying the descriptions the following definitions are used:

Failure: A failure is detected whenever a heart beat times out without receiving a monitoring packet from both interfaces. Only the active node sends monitoring packets. The inactive node passively listens for the monitoring packets. The inactive twin always forwards monitoring packets. In order for an active node to receive a monitoring packet it has to complete a round trip, such as, out IP side to twin, in IP side of twin, out 709.x side of twin, in 709.x side, or going the other way, out 709.x side to twin, in 709.x side of twin, out IP side of twin, in IP side. A failure may be detected on one or both interfaces.

Fault: Once a failure is detected, both twins perform a diagnostic by actively interrogating each other on both interfaces. If the interrogation on a particular interface fails, then a fault has occurred on that interface. An alarm is generated when a fault has been determined. A fault on a particular interface is cleared whenever a monitoring packet is received or if a diagnostic interrogation succeeds. A cleared fault generates an `alarm cleared`.

Both nodes independently report failures and faults. It is possible to have a failure but not a fault. The converse is not true. It is possible for only one twin to report a failure. For example, if either interface has failed the active node will not receive any round trip monitoring packets so it will report a failure on both interfaces. However, it will only report a fault on one. In the same event the inactive twin will report a failure on only one interface not both. The inactive will report a fault on one interface.

Alternatively, if one interface fails and then some time later the other interface fails, the initially active twin will not diagnose the second fault. The initially inactive twin, however, will diagnose the second fault. Therefore, in order to fully characterize the failure and fault state of a redundant pair the state of both devices must be examined. Moreover, the monitoring application is on the LON side. In the event of an IP failure the alarm SNVT sent by the active node may not be received by a monitor HMI on the IP side. Although the alarm is sent out both sides, the IP side has failed so the alarm can't propagate on the IP side and the inactive twin may not have switched to forwarding mode in time to forward the alarm packet. Nevertheless, the inactive device will also detect the fault and its alarm will propagate.

3.3.2. Status SNVT

The twin monitoring application has a status SNVT type 93. If bound, the status SNVT is propagated either on a timer, or when it is updated by the monitoring application, or both, or neither. If `propagate on update` is off and the update time is zero then the status SNVT will never be scheduled for propagation. In this case the only way to read the status SNVT is to poll it. If `propagate on update` is off and update time is non zero then the status SNVT will propagate at an interval specified by the update time. If `propagate on update` is on and update time is non zero then the status SNVT will propagate both on the update time interval and anytime the status is changed. If the update time is zero and `propagate on update` is on then the status SNVT will only propagate when changed or updated by the monitoring application. Typically, the status is updated when the twin mode state changes.

The fields used in the status SNVT are as follows:

`comm_failure` is set to 1 when there is either a monitoring failure or a diagnostic detects a fault. `comm_failure` is not set to 0 until all failures and faults have cleared.

`reserved2` is set based on the system state. See the following table.

Bit values for reserve2 status byte (big endian)	
Bit	**Value**
7	1 Active State, 0 Inactive State
6	1 Forwarding, 0 Dropping
5	1 Repair State, 0 Not Repair State
4	1 Diagnostic State, 0 Not Diagnostic State
3	1 IP side failure, 0 No IP side failure
2	1 LON side failure, 0 No LON side failure
1	1 IP side fault, 0 No IP side fault
0	1 LON side fault, 0 No LON side fault

3.3.3. Alarm SNVT

The monitoring application also has an Alarm2 SNVT type 164. This alarm is propagated whenever a fault is detected or cleared. The fields used in the Alarm2 SNVT are as follows:

`alarm_type` is set to 1 whenever a diagnostic detects a fault. alarm_type is set to 0 when all faults have cleared.

`description` is set to an ASCII text description of the associated fault state whether IP or LON or both are cleared.

3.3.4. Status Report UNVT

The monitoring application has a status report UNVT that includes some extra information that would not fit in the Status SNVT. The status report UNVT is scheduled for propagation whenever one of its fields is updated. It will only be propagated if bound or polled. The c structure for the UNVT is as follows:

```
typedef struct
{
   unsigned char  Status;
   char           reserved[3];
   uint32         totalArbs;
   uint32         totalFailuresIP;
   uint32         totalFailuresLON;
   uint32         totalFaultsIP;
   uint32         totalFaultsLON;
   uint32         secsSinceClear; // seconds
   uint16         forwardRate; // packets per second
   char           reserved[2];
}  UNVTStatusType;
```

The fields are as follows:

`Status` is an 8 bit number. The bit definitions are given in Table 1. It is the same information reported in the Status SNVT reserved field.

`totalArbs` is the total number of active state arbitrations since the last time the statistics were

cleared.

`totalFailuresIP` is the total number monitoring packet failures detected by this device of the IP interface since the statistics were cleared.

`totalFailuresLON` is the total number of monitoring packet failures detected by this device of the LON interface since the statistics were cleared.

`totalFaultsIP` is the total number of diagnostic faults detected by this device of the IP interface since the statistics were cleared.

`totalFaultsLON` is the total number of diagnostic faults detected by this device of the LON interface since the statistics were cleared.

`secsSinceClear` is the count of seconds since the statistics were last cleared.

`forwardRate` is computed as the total number of packets forwarded divided by the number of seconds since the forward rate was last calculated. The forward rate is updated whenever the UNVT is updated and at least one second has expired since the last update.

3.4. Twin Setup Page

This page configures the twin mode redundant router feature. Twin mode is an optional enhancement and is not activated in a standard router. If your device does not support redundant twin mode contact Smart Controls to find out how redundant twin mode might be activated. This page does not appear if NAT support is enabled. Following is a brief description of each item listed on the page

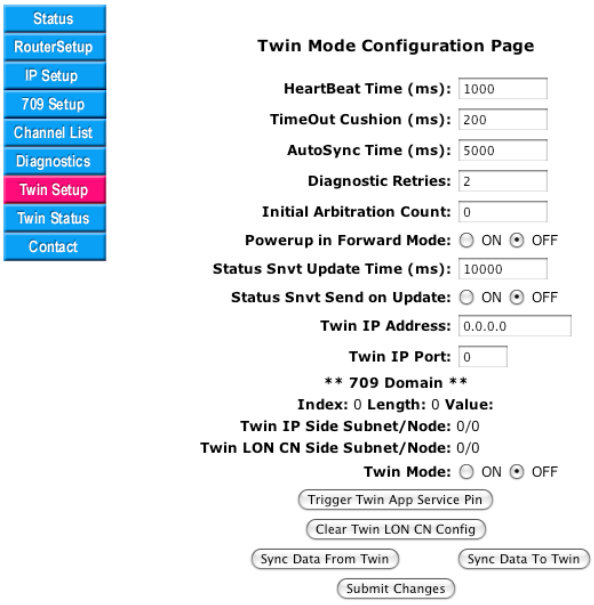


Fig.3.8: Twin Mode Setup Page

HeartBeat Time: This sets the time period in milliseconds between cycles of the twin mode monitoring packets. The active member of the redundant pair or *active twin*, sends out two round trip monitoring packets during each *HeartBeat* period that test both the 709.1 and IP interfaces of both routers. The default is 1000 ms. Increasing the *HeartBeat Time* increases the fail over latency time. Decreasing it increases network traffic and load on the router. A practical

lower limit is 100 ms.

Timeout Cushion: This sets the time period in milliseconds of latency cushion for the time out for failure detection of the monitoring packets. In other words, if after a time equal to HeartBeat Time + Cushion, both monitoring packets are not detected by a router then a monitoring failure has been deemed to have occurred. The routers then go to an active diagnostic mode. The cushion should always be less than the HeartBeat Time but greater than the expected latency due to propagation delays. The default is 200 ms.

AutoSync Time: This sets the time period in milliseconds between automatic synchronization attempts from the twin to the inactive twin. The default is 5000 ms.

Diagnostic Retries: This sets the number of retries that the active diagnostic interrogation request/response message will use. A diagnostic is sent out from each interface (709 and IP) whenever a monitoring failure occurs. If the interrogation packet fails after *Diagnostic Retries* number of retries then a fault of the associated network interface will have been deemed to have occurred. This will generate an alarm. The default is two retries. If spurious faults occur, it may be because *Diagnostic Retries* is too low and the diagnostic responses are getting lost due to collisions. The odds of lost packets due to collisions decrease significantly for retry counts above Four.

Initial Arbitration Count: The arbitration count is a 64 bit number. The redundant twins use an arbitration count encapsulated in the monitoring packets to determine which member of the pair should be active. The twin with the highest count wins the arbitration and goes active while the one with the lower count will go inactive. If both have the same count, then they both pick random counts until one wins the arbitration.

On boot up both routers will default to active. The ensuing arbitration will result in one of the routers going inactive. This menu option can be used to guarantee that a particular router will win the boot up arbitration on the next reboot. The desired active one should have the higher *Initial Arbitration Count*. Use this menu option to set the *Initial Arbitration Count* appropriately. The arbitration count is incremented twice per *HeartBeat Time*. The relative difference between initial arbitration counts should be set big enough to account for any variable latency in boot up time. The default is zero. If both nodes are set to zero, which ever node boots up first will go active and start incrementing its arbitration count. The other node will also go active but because it booted up later its arbitration count will be lower and will lose the arbitration and go inactive. The arbitration count will eventually roll over to zero. Thus, on the next arbitration after roll over the active and inactive nodes will switch. Given that the arbitration count is a 64 bit number, for a *HeartBeat Time* of 1 second and an *Initial Arbitration Count* of zero, the rollover time is more than 292 billion years.

To reiterate, the initial arbitration count is only going to have an effect if there is an arbitration on boot-up. An arbitration only occurs when both nodes are in active forward state. In order to force the inactive node to be active one must set the arbitration counts on both nodes and then reboot both nodes.

Powerup in Forward Mode: On boot up both routers will default to active. As a result, they could both forward packets thereby resulting in a spike of duplicate traffic until arbitration completes. Setting this option to *Off* will disable forwarding of packets by both routers until arbitration completes and only one router goes active. The default is *Off*.

Status SNVT Update Time: The twin monitoring application has a status SNVT type 93. If bound the status SNVT is propagated either on a timer or when it is updated by the monitoring application or both or neither. The Status SNVT update time determines the maximum time between propagations. If the update time is non zero, every update time ms a status SNVT is scheduled for propagation. It is propagated even if the status has not been updated. If the update time is zero then no propagation is scheduled on a timed interval. For a more detailed description of the Status SNVT see Section 2.5.5.

Status SNVT Send on Update: This option schedules the status SNVT for propagation whenever the SNVT is updated or the status changes. This is event driven and not time driven. For a more detailed description of the status SNVT see Section 2.5.5.

Twin IP Address: This field displays/sets the redundant twin's IP address

Twin IP Port: This field displays/sets the redundant twin's IP port

709 Domain: These fields display the common domain address used for both the IP and LON 709.1 stacks.

Twin IP side Subnet/Node: This field displays the subnet/node address of the twin's IP side 709.1 stack.

Twin LON CN side Subnet/Node: This field displays the subnet/node address of the twin's LON component network side 709.1 stack.

Twin Mode ON/OFF: These radio buttons turn twin mode on or off.

Trigger Twin App Service Pin: This button propagates a service pin message from the twin mode monitoring application. This enables remote commissioning of the twin mode application.

Clear Twin LON CN Config: This button clears the component network configuration about its twin from this device's memory.

Sync Data From Twin: This button manually requests a sync packet from its twin.

Sync Data To Twin: This button manually sends a sync packet to its twin.

Submit Changes: This button updates the configuration memory of the device and refreshes the web page to reflect any changes.

3.5. Twin Mode Status Page

The *Twin Mode Status Page* displays operational state and statistics information about the *Redundant Twin Mode* operation. Twin mode is an optional enhancement and is not activated in a standard router. If your device does not support *Redundant Twin Mode* contact Smart Controls to find out how it might be activated. Following is a brief description of each item listed on the page.

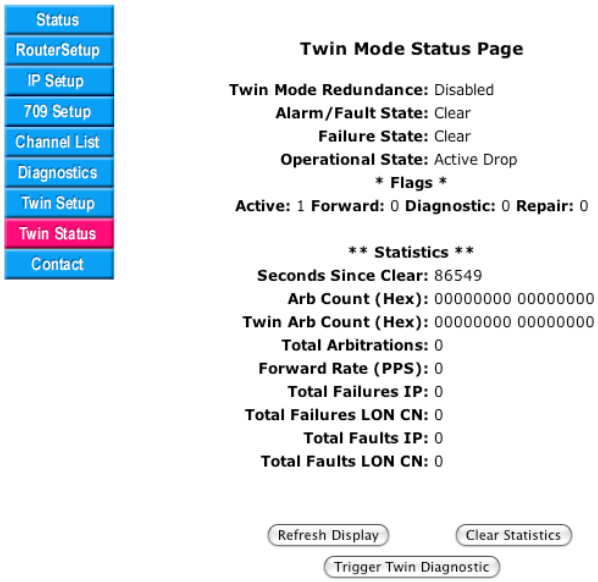


Fig.3.9: Twin Mode Status Page

Twin Mode Redundancy: This field indicates whether twin mode is enabled or disabled (on/off).

Alarm/Fault State: This field indicates the status of any alarms or faults.

Failure State: This field indicates the status of any monitoring failures.

Operational State: This field indicates the twin mode operational state.

Flags: This field indicates the twin mode operational state flags for debugging.

Seconds Since Clear: This field indicates the number of seconds since the statistics were last cleared.

Arb Count: This field indicates this device's arbitration count.

Twin Arb Count: This field indicates the twin's arbitration count.

Total Arbitrations: This field indicates the total number of active state arbitrations.

Forward Rate: This field indicates the rate in packets per second of packets forwarded by the router in either direction.

Total Failures IP: This field indicates the total number of monitoring failures of the IP interface since the statistics were last cleared.

Total Failures LON: This field indicates the total number of monitoring failures of the LON interface since the statistics were last cleared.

Total Faults IP: This field indicates the total number of diagnostic faults of the IP interface since the statistics were last cleared.

Total Faults LON: This field indicates the total number of diagnostic faults of the LON interface since the statistics were last cleared.

Refresh Display: This button manually updates the statistics including recalculating the forward rate.

Trigger Twin Diagnostic: This button manually forces the device to perform a diagnostic on both its interfaces.

4. Network Integration and Management

4.1. Manual Mode Example

Configuring in Manual Mode

This section contains step-by-step instructions on configuring two GRouter devices to tunnel 709.1 packets over IP between each other. This will create an IP backbone for a 709.1 network.

- Using the web configuration pages, set up IP addresses, subnet masks, and IP gateway addresses for the two routers. Connect the routers to the same IP network. Using a PC attached to the network, verify that the routers can be pinged. Consult with the network administrator to procure the IP address, subnet mask, and gateway address, if not already known.
- Set both routers to manual mode. This is done on the Router Setup Page.
- Add each router's IP address and communications port number (the default port is 1628) into the other router's channel list. Set the addressing type to unicast or multicast in the channel details menu. This is done on the Channel List Page.
- Once steps 1–3 have been completed, the routers will be able to communicate with each other over the IP network. This can be verified by pressing the service pin on one of the routers and checking the Diagnostics Page on the other router for packets received. The fields "Data Packets Received" and "IP Packets Received" should increase with each service pin.
- For the routers to tunnel traffic, the 709.1 interfaces must be set up. This can be done on the 709 Setup Page or with a network management tool such as LonMaker. Refer to the management tool's documentation on commissioning routers. For example, the GRouter can be commissioned using the Router icon within LonMaker.

4.2. Normal Mode With i.LON Configuration Server Example

This section contains step-by-step instructions on configuring the GRouter device with an i.LON Configuration Server.

- Using the web configuration pages, set up IP address(es), subnet mask(s), and IP gateway address(es) for the router(s). Connect the router(s) to the same IP network as the PC running the configuration server. Using a PC attached to the network, verify that the routers can be pinged. Consult with the network administrator to procure the IP address, subnet mask, and gateway address, if not already known.
- Set the router(s) to normal mode. Set the configuration server address to the address of the computer that is running the i.LON Configuration Tool. Set the configuration server port to that used by the i.LON configuration server. The default is 1629. Set the compatibility type to i.LON Configuration Server. Register the device with the configuration server by clicking on the ***Register With Config Server*** button. This is done on the Router Setup Page.
- Go to the i.LON configuration server window and drag the GRouter device from the orphans list to the desired channel. The router(s) should be added to the same channel. After a few seconds, the router devices should turn green.

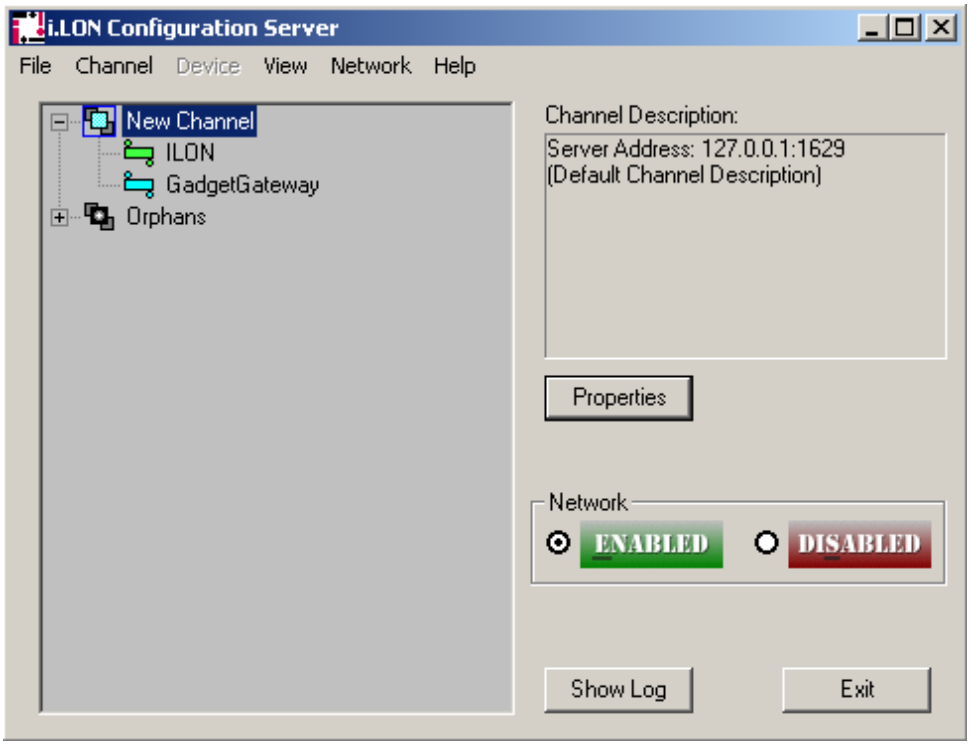


Fig.4.1: Configuration Server Screen

- Verify that the GRouter device is configured correctly by checking the *Channel List Page* on the router. If configured correctly, the router will have an entry in its Channel List for each router shown in the configuration server's channel list.
- The routers will now communicate with each other over IP and will tunnel packets between networks once they have been commissioned using LonMaker or another compatible network management tool.

4.3. Communicating With Lonmaker With IP Interface

This section describes how to connect LonMaker as an 852 device on the same channel as the GRouter device.

- Setup the GRouter device and the configuration server as per the preceding section
- Attach the computer running LonMaker to the same IP network with the GRouter device. This may be the same computer as that running the configuration server but with a different IP port for LonMaker. LonMaker must be running with an open network whose network interface is set to this IP channel. Consult the LonMaker manual for instructions. LonMaker should show up in orphans list in the configuration server window.
- Drag LonMaker onto the channel where the GRouter device resides. If all the devices do not go green, then right-click the Channel icon and select the *Commission Members* option.
- Add both the GadgetGateway and the PC that is running the LonMaker software to the i.LON Configuration Tool. Both devices should be added to the same channel. When the devices have been added to the Configuration Tool, right-click the Channel icon and select the "Commission Members" option. After a few seconds, both the LonMaker PC and the GRouter devices will turn green.

- You will now be able to install and commission the GRouter devices as 709.1 routers in the LonMaker network diagram.

4.4. Commissioning GRouter Device With LonMaker

There are two ways that a network management tool such as LonMaker can communicate with and commission a GRouter device. The first way is for the network management tool to be connected to a LON channel that is connected to the LON channel for the GRouter. The connection may go through several other routers. The second way is for the network management tool to be directly connected to the same 852 IP channel as the GRouter device. In either case once a viable connection has been established the network management tool may now install and commission the GRouter device into its network diagram

- If the LonMaker diagram already has the IP channel wherein the GRouter is member then go to the next step. Otherwise, create a new IP channel.
- Create a new TP-10 channel in the LonMaker Visio screen.
- Drag a router device onto the network and uncheck the “Commission Device” box. Set up the router to communicate between the IP channel and the TP-10 channel.
- Once the device has been set up, right-click the device and select *Commission*. Choose the *Service Pin Install* option. When LonMaker indicates that it is waiting for the service pin, press *SRV P1* on the GRouter device. If the router and LonMaker are communicating properly, LonMaker will commission the GRouter device, and the router device will turn green in the LonMaker application. The following screen shots show how this is done.

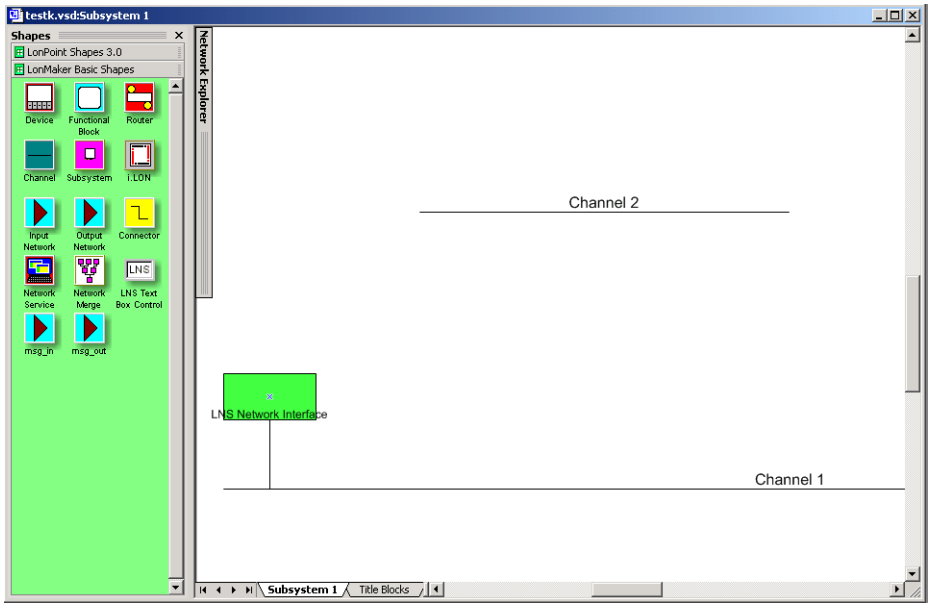


Fig.4.2: Initial LonMaker Drawing

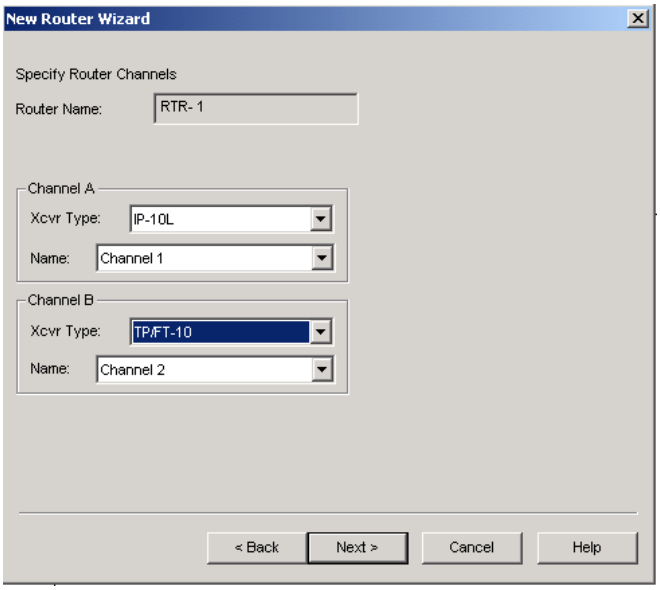


Fig.4.3: Router Channel Setup

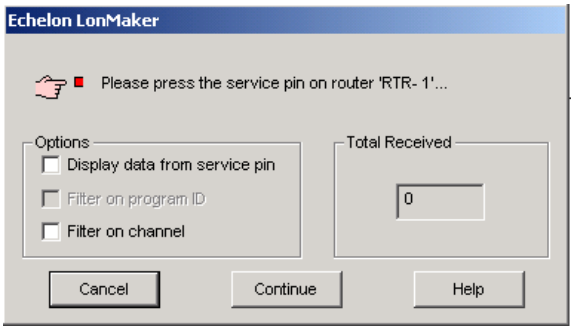


Fig.4.4: Service Pin Dialog

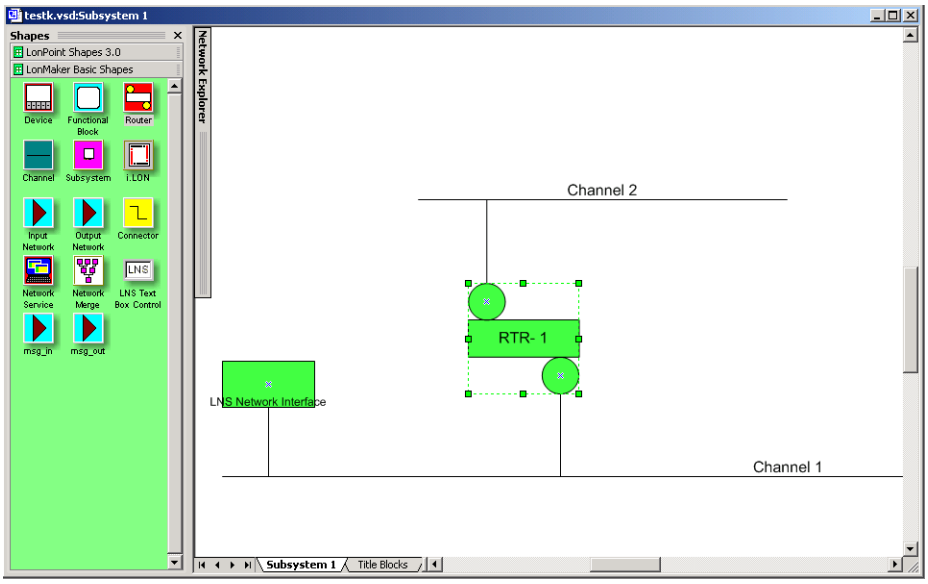


Fig.4.5: Fully Commissioned Router

4.5. NAT Router Example

This section contains step-by-step instructions on how to set up a GadgetGateway router for

operation on the LAN side of a NAT router. The NAT support mode enables a GRouter device to operate on the LAN side of a NAT (Network Address Translation) router. The setup is shown in the following figure.

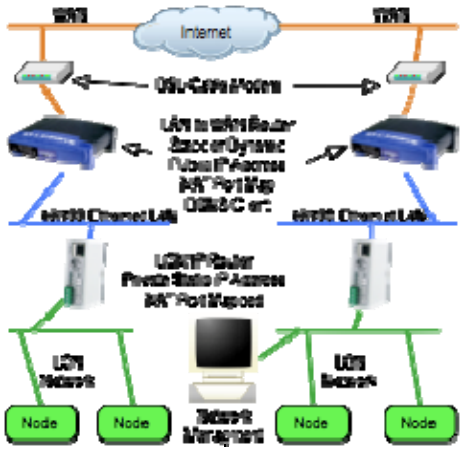


Fig.4.6: NAT LAN to WAN Architecture

- Setup the IP parameters for the GRouter as per the *Manual Mode* or *Normal Mode* instructions above.
- Configure the NAT router to port map the 852 port. If you need to access the GRouter web interface from the WAN side then you must also set up and port map the http web server port for the GRouter device.
- Enter the static WAN IP address of the NAT router into the *NAT Router WAN Address* field on the GRouter device's *Router Setup Page*.
- Select the radio button to enable NAT support. Click *Submit Changes.*
- Continue configuring the GG in either Manual or Normal mode as described in previous sections.

4.6. DDNS Router Example

The DDNS support mode enables a GRouter device to operate on the LAN side of the NAT (Network Address Translation) router that is also a DDNS client. Routers of this type may have dynamic IP addresses. Please refer to the figure above for an example of this architecture. This section contains step-by-step instructions on how to set up a GRouter device for operation on the LAN side of a NAT-DDNS router.

- Follow the instructions in the previous section for setting up NAT support with the exception that the GRouter device must be in manual mode and the NAT WAN address of the NAT-DDNS router does not have to be entered.
- On the *DDNS Setup Page,* set the *DDNS Name* of the NAT router, the *DDNS Refresh Time*, the *DNS Server Names*, and *Enable DDNS.* Click the *Submit Changes* button. If you do not have a DDNS domain name for the NAT-DDNS router, you must go to `dyndns.org` and register for one.

- Verify DDNS is working by doing a manual look up the IP address using either the web or serial interface. The router's DDNS IP address should show up in the *DDNS IP Address* field.
- Continue configuring the GRouter device in manual mode to add other 852 devices to its channel etc.

4.7. Redundant Twin Mode Example

Redundant Twin Mode enables two GRouter or GGIa routers to operate as a redundant pair for high availability applications. This enhanced capability increases reliability and eliminates some single mode failure sources. This section contains step-by-step instructions on how to set up a pair of routers for operation in *Redundant Twin Mode*.

- Check the *Twin Setup Page* to see if the *Twin IP Side Subnet/Node* field is set to 0/0. Check also to see if the *Twin LON CN Side Subnet/Node* field is set to 0/0. If not you must first click the *Clear Twin CN Config* button. Also make sure *Twin Mode* is *OFF*.
- Set up an IP address, subnet mask, and gateway address for each router. Using a PC, ping each router to ensure that it is communicating on the IP network.
- Set up the 852 interface (either manual or normal mode) for both the routers and add them to the same 852 channel.
- Verify that the routers are configured correctly by checking the *Channel Lists* on the routers.
- Commission both routers using an appropriate network management tool.
- The GadgetGateway routers are now ready to be configured for Twin Mode. Because the routers are connected between the same two channels a loop will be created. The automatic loop detection on the routers will detect the loop and one of the routers will stop forwarding. As a result, the serial console will print out messages indicating such. You may disregard these messages as the routers will automatically recover once in twin mode.
- On router A's *Twin Mode Setup Page*, enter the IP address and port of router B in the *Twin IP Address* and *Twin IP Port* fields. This should be the same IP address and port used for 852 communications by router B. This step uniquely identifies B as Router A's Twin.
- On router B's *Twin Mode Setup Page*, enter the IP address and port of router A in the *Twin IP Address* and *Twin IP Port* fields. This should be the same IP address and port used for 852 communications by router A. This step uniquely identifies A as Router B's Twin.
- On router B's *Twin Mode Setup Page*, click the *Sync Data From Twin* button. Router B should now display router A's 709.1 (IP and LON CN) subnet/node addresses.
- On router B's *Twin Mode Setup Page*, click the *Sync Data To Twin* button. Router A should now display router B's 709.1 (IP and non IP) subnet/node addresses. To verify go to router A's router A's *Twin Mode Setup Page*.
- On router B's *Twin Mode Setup Page*, enable *Twin Mode* by selecting the associated *ON* radio button.
- On router A's *Twin Mode Setup Page*, enable *Twin Mode* by selecting the associated *ON* radio button. The routers will now act as a redundant pair.
- Go to the *Twin Status Page* to observe operational state and failure statistics.

- The monitoring application on each router is now ready to be commissioned. Repeat the following steps for each router.
- Drag a new device shape onto the LonMaker drawing. The device should be attached to the channel on the LON side of the GRouter device. Setup and commission this device. Use the SRV App to send a service pin for the monitoring application.
- Drag a new functional block onto the lonmaker drawing and associate it with the newly created device. The status and alarming network variables are now ready to be bound.

The sequence of dialog boxes you will encounter is given below.

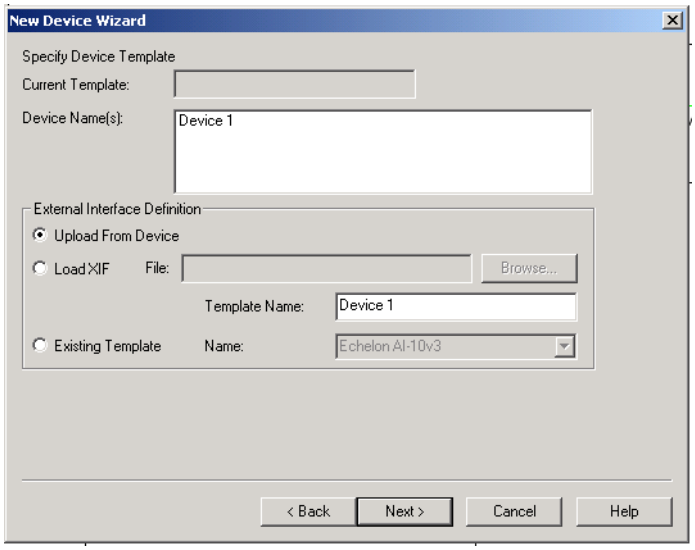


Fig.4.7: LonMaker New Device Dialog

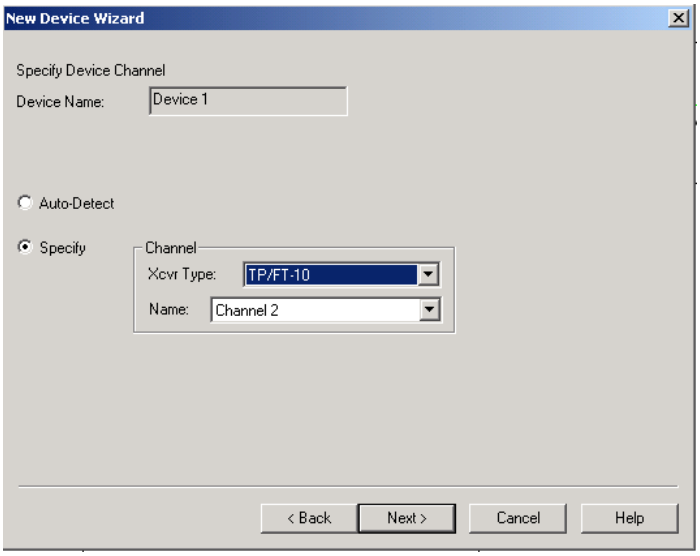


Fig.4.8: LonMaker New Device Channel Dialog

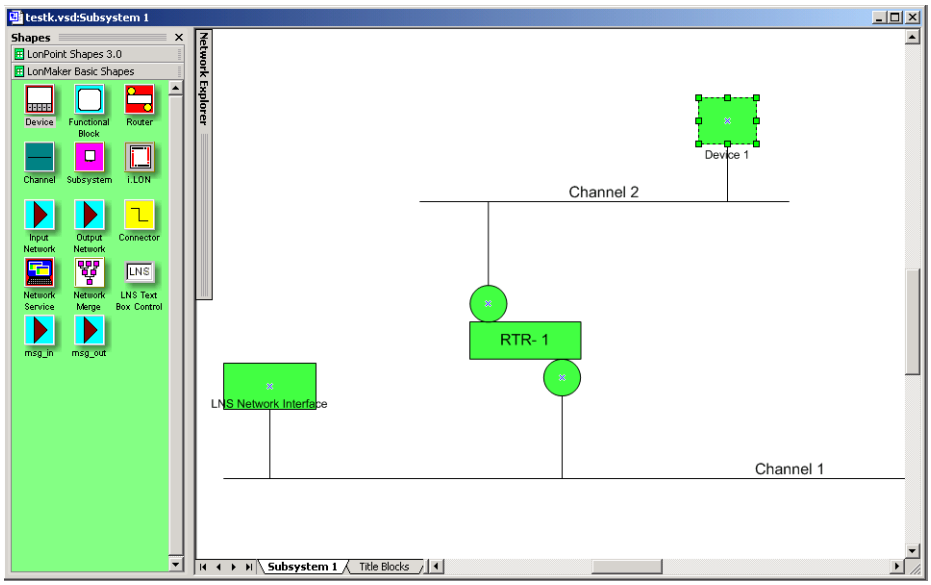


Fig.4.9: LonMaker Drawing With Commissioned Monitoring Device

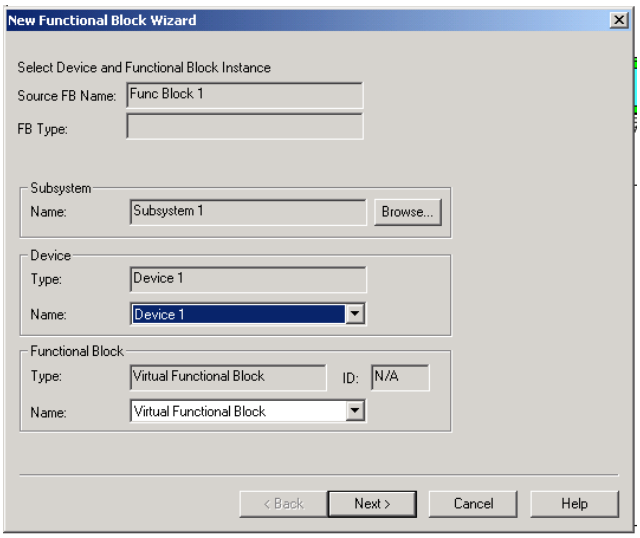


Fig.4.10: New Virtual Functional Device Dialog

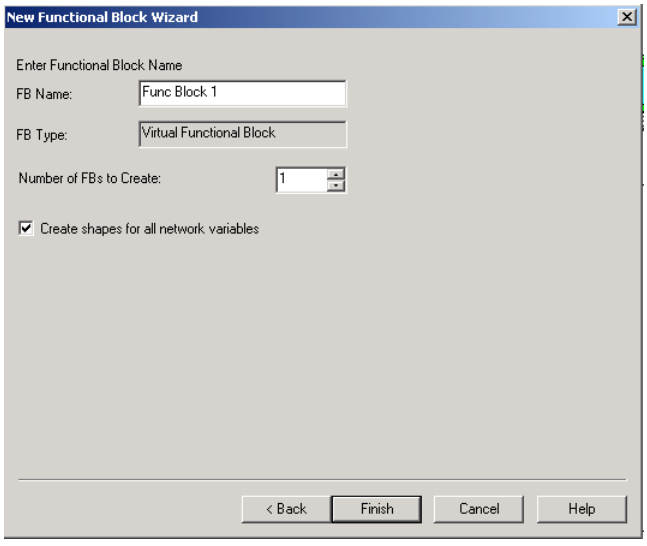


Fig.4.11: Functional Blocks NV Shapes Dialog

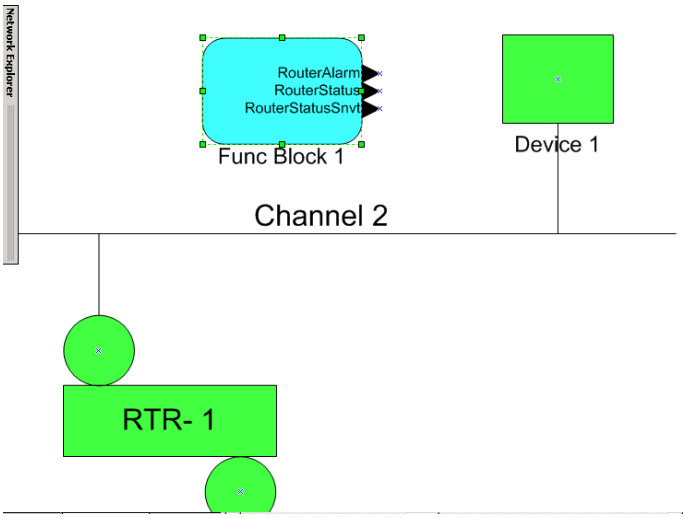


Fig.4.12: Functional Block On Drawing

4.8. Configuring with the Coactive Router-LL

4.8.1. Manual Mode

This section contains step-by-step instructions on configuring a Coactive Router-LL and a GRouter device in manual mode to tunnel 709.1 packets between each other over IP.

- Using the web configuration pages for the GRouter and the serial menu for the Router-LL, set up IP addresses, subnet masks, and IP gateway addresses for the two routers. Connect the routers to the same IP network. Using a PC attached to the network, verify that the routers can be pinged. Consult with the network administrator to procure the IP address, subnet mask, and gateway address, if not already known.
- Set both routers to manual mode. This is done on the Router Setup Page for the GRouter, and through the Basic Setup page on the Router-LL's Web Interface.
- Using the appropriate web pages on each router, add each router's IP address and communications port number (the default port is 1628) into the other router's channel list. Set the addressing type to unicast or multicast in the channel details menu.
- Once steps 1–3 have been completed, the routers will be able to communicate with each other over the IP network. This can be verified by pressing the service pin on one of the routers and checking the Diagnostics or Statistics Page on the other router for packets received.
- For the routers to tunnel traffic, the 709.1 interfaces must be set up. This can be done on the 709 Setup Page or with a network management tool such as LonMaker. Refer to the management tool's documentation on commissioning routers.

4.8.2. Normal Mode With Router-LL Configuration Server

- Using the web configuration pages, set up IP address(es), subnet mask(s), and IP gateway address(es) for the router(s). Connect the router(s) to the same IP network. Using a PC

attached to the network, verify that the routers can be pinged. Consult with the network administrator to procure the IP address, subnet mask, and gateway address, if not already known.

- Set the router(s) to normal mode. Set the configuration server address and port to the address and port of the Router-LL configuration server. The Router-LL configuration server only communicates on the non-standard port 2009 (not 1629). Set the compatibility type to Coactive Router-LL. Register the device with the configuration server by clicking on the ***Register With Config Server*** button. This is done on the Router Setup Page. The device should now show up in the device list on the Coactive Configuration Server web page.
- Verify that the GRouter device is configured correctly by checking the Channel List on the router. If configured correctly, the router will have two entries in its Channel List: itself and the Router-LL.
- The GRouter device and the Router-LLs will now communicate with each other over IP and will tunnel packets over IP once they have been commissioned using LonMaker or another compatible management tool.

5. FTT-10 XCVR LonTalk Network Termination

When using an FTT-10 XCVR, the network wiring should be terminated, or performance may suffer. This is especially true for long wire runs or noisy environments. Typically, an external terminator is used. The GRouter4, however, does have an optional internal terminator for those applications where it is desirable or convenient to terminate at the router. When the optional internal terminator is installed, a jumper on header JP1 is used to configure the type of termination. In order to do this the case must be opened. Disconnect the power and network before opening the case. Use caution and appropriate electrostatic safety precautions whenever working with the case removed. If the center pin of JP1 is jumpered to the pin labeled *Free*, then the terminator is set for free topology mode. If the center pin of JP1 is jumpered to the pin labeled *Bus*, then the terminator is set for bus mode. If the center pin is not jumpered to either the Bus or Free pins then the terminator is disabled. The following figures show photos of JP1 with the jumper in the 3 different settings.

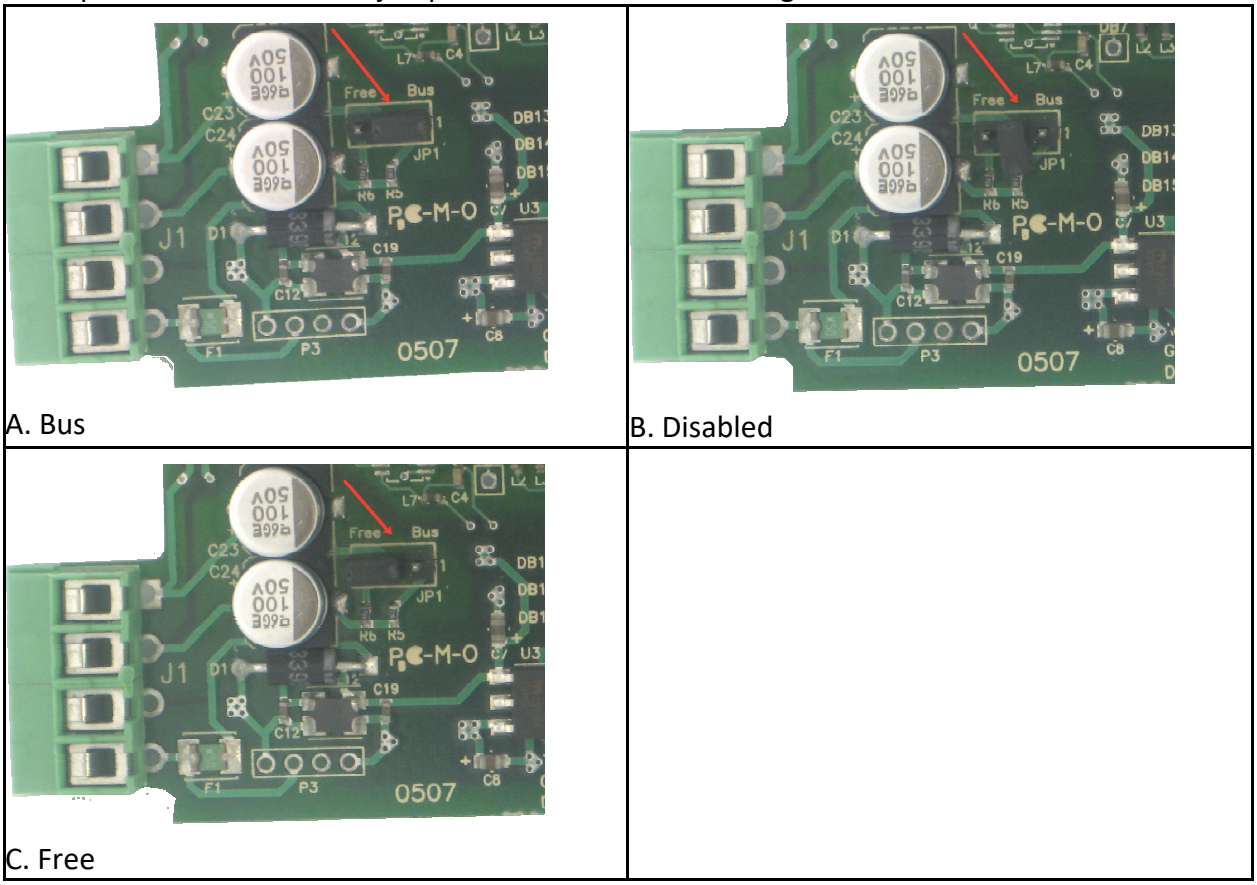


Fig.5.1: Optional internal terminator: A. Bus Topology, B. Disabled, C. Free Topology.

6. Firmware Upgrade Instructions

The GRouter device's firmware can be upgraded using ftp over the IP interface. This feature allows GRouter device users to take advantage of enhancements and features that may become available in the future.

Both the application firmware and the bootloader may be upgraded using ftp. Although 4.12 is the first time that the bootloader has been upgraded. Consequently prior to 4.12 there was no need to distinquish between application firmware and bootloader firmware. To avoid confusion, starting with version 4.12, the application firmware file names end in image.bin and the bootloader file names end in rom.bin. There are different versions of both application firmware and bootloaders for the Ethernet and WiFi versions of the GRouter4. This is also reflected in the file names. The Ethernet versions have "eth" in the filename and the WiFi versions have "wifi" in the filename.

For example at the time of this writing the latest version release of the application firmware is version 4.12.058 and the corresponding firmware filenames are GR4_4_12_058_eth_image.bin for the Ethernet version and GR4_4_12_058_wifi_image.bin for the WiFi version. Likewise the latest release version of the bootloader is 4.12.048.C for Ethernet with corresponding filename GR4_4_048_C_eth_rom.bin. Moreover the latest release version of the bootloader for WiFi is 4.12.053.D with corresponding filename GR4_4_048_C_wifi_rom.bin.

One may upgrade either the bootloader of the application firmware in any order. However prior to 4.12 versions of the application firmware do not display the bootloader version on the web page. Also prior to 4.12 versions of the bootloader will have a blank version number.

To upgrade the application and/or bootloader firmware; first obtain a copy of the new firmware file for the appropriate type of GR4 Ethernet or WiFi.

In order to perform an update, the FTP server application must be running on the GRouter device. This is launched by clicking the button named *Launch Upgrade FTP Server* in the *RouterSetup Page*.

On the host computer launch an ftp client from the command line. This is done the MS Windows cmd prompts by typing ftp following by a space and the IP address of the GR4 in dotted notation. The format is *ftp XX.XX.XX.XX*.

It will prompt for user name. The user name is case sensitive and is as follows:

GRouter

The password is blank.

Set the transfer mode to binary and enable hash marks in order to see progress. Put the new image.bin file onto the GRouter device as image.bin. It will take a couple of minutes to complete the transfer and burn the flash. Be patient. Once the transfer is complete, quit the ftp client. At this point the GRouter device will finish writing its flash and then automatically reboot with the new firmware installed. It will take a couple of minutes for this to happen. Do not remove power from the device until the procedure has completed. Prematurely, removing power can corrupt the flash and make the unit inoperable. The last sector of flash is not written until after one quits the ftp client. The firmware is downloaded in chunks. The hash marks will pause while each chunk is written to flash then update quickly when a new chunk is

downloaded. If a firewall is running on the PC it may prevent FTP from working. It may make the connection but nothing will download. If this happens there will be no hash marks printed. In this event turn off the firewall.

6.1. Upgrading Application Firmware Example

An example ftp session is shown below:

The Application firmware is upgraded using *image.bin*. Transfer must always be in binary mode set by the *bin* command. Not using binary mode will corrupt the firmware and make the unit unusable. Notice the syntax of the ftp *put* command. When *put* is entered without arguments, it first prompts for the *Local file* which is the new firmware, and second prompts for the *Remote file* which must always be *image.bin*, when upgrading the application firmware. To restate, the *Remote file* for upgrading the application firmware must always be *image.bin*. If *rom.bin* is used it will overwrite the bootloader and make the unit inoperable.

```
>ftp 10.0.2.42
Connected to 10.0.2.42.
220 NET+OS 6.3 FTP server ready.
User (10.0.2.42:(none)): GRouter
230 User GRouter logged in.
ftp> bin
200 Type set to I.
ftp> hash
Hash mark printing On  ftp: (2048 bytes/hash mark) .
ftp> put
Local file GR4_4_14_011_eth_image.bin
Remote file image.bin
200 PORT command Ok.
150 About to open data connection.
################################################################################
################################################################################
################################################################################
################################################################################
#################
226 Transfer complete
ftp: 668222 bytes sent in 2.86Seconds 233.64Kbytes/sec.
ftp> bye
221 Goodbye.
```

At this point the GRouter will continue writing flash for a minute or two and then reboot on its own. Once it has finished rebooting the status page will display the new firmware version.

For wifi the example is as follows:

```
>ftp 10.0.2.42
Connected to 10.0.2.42.
220 NET+OS 6.3 FTP server ready.
User (10.0.2.42:(none)): GRouter
230 User GRouter logged in.
ftp> bin
200 Type set to I.
ftp> hash
Hash mark printing On  ftp: (2048 bytes/hash mark) .
ftp> put
Local file GR4_4_14_011_wifi_image.bin
Remote file image.bin
200 PORT command Ok.
150 About to open data connection.
################################################################################
################################################################################
################################################################################
################################################################################
#################
226 Transfer complete
ftp: 668222 bytes sent in 2.86Seconds 233.64Kbytes/sec.
ftp> bye
221 Goodbye.
```

6.2. Upgrading Bootloader Example

An example ftp session is shown below:

The Bootloader is upgraded using *rom.bin*. Transfer must always be in binary mode set by the *bin* command. Not using binary mode will corrupt the firmware and make the unit unusable. Notice the syntax of the ftp *put* command. When *put* is entered without arguments, it first prompts for the *Local file* which is the new bootloader, and second prompts for the *Remote file* which must always be *rom.bin*, when upgrading the bootloader. To restate, the *Remote file* for upgrading the bootloader must always be *rom.bin*. If *image.bin* is used instead it will overwrite the application. The units application firmware will have to be recovered using the tftp recovery method.

```
>ftp 10.0.2.42
Connected to 10.0.2.42.
220 NET+OS 6.3 FTP server ready.
User (10.0.2.42:(none)): GRouter
230 User GRouter logged in.
ftp> bin
200 Type set to I.
ftp> hash
Hash mark printing On  ftp: (2048 bytes/hash mark) .
ftp> put
Local file GR4_4_12_048_C_eth_rom.bin
remote file rom.bin
200 PORT command Ok.
150 About to open data connection.
##########################
226 Transfer complete
ftp: 55444 bytes sent in 0.13Seconds 443.55Kbytes/sec.
ftp> bye
221 Goodbye.
```

At this point the GRouter will continue writing flash for a minute or two and then reboot on its own. Once it has finished rebooting the status page will display the new bootloader version.

For wifi the example is as follows:

```
>ftp 10.0.2.42
Connected to 10.0.2.42.
220 NET+OS 6.3 FTP server ready.
User (10.0.2.42:(none)): GRouter
230 User GRouter logged in.
ftp> bin
200 Type set to I.
ftp> hash
Hash mark printing On  ftp: (2048 bytes/hash mark) .
ftp> put
Local file GR4_4_12_053_D_wifi_rom.bin
Remote file rom.bin
200 PORT command Ok.
150 About to open data connection.
##########################
226 Transfer complete
ftp: 55444 bytes sent in 0.13Seconds 443.55Kbytes/sec.
ftp> bye
221 Goodbye.
```