



# c-Bridge™

## IPSC-x Series

The **c-Bridge™** is an IP-based networking controller designed to enhance wide-area system capabilities and to provide interoperability functionality to MOTOTRBO™ digital communications systems.

**c-Bridge™** controllers connect into MOTOTRBO™ IP Site Connect (IPSC) systems through IP network connections (private or the internet). Whereas IPSC systems are limited to a maximum of 15 repeaters in one network. **c-Bridge™** controllers can be used to expand IPSC systems into very large systems, with hundreds of repeaters connected if needed. They also allow for dynamic bridging between repeaters or groups of repeaters and between time slots, based on Talkgroup ID codes or pre-programmed "patches". **c-Bridge™** systems handle voice (group, private, and All Calls), GPS and ARS data, text messaging, Call Alerts, Radio Query, Radio Enable/Disable, and Emergency Calls. This allows for a fantastic amount of flexibility in the operation of an IPSC system. For example, Emergency Calls and All Calls can be transmitted on one time slot, but be received on both time slots.

Analog interfaces are available to tie into the accessory ports on repeaters, base stations, control stations, or analog dispatch consoles, providing interoperability between MOTOTRBO™ IPSC systems and conventional analog, P25 conventional or trunking, or other non- MOTOTRBO™ systems.

PC-based Client software allows for computer workstation voice dispatching and manual remote bridging control. The PC Client software connects directly into an IPSC system, through a network connection (private or internet) to a **c-Bridge™** controller. No control station radios are needed.



Exceed the 15-repeater limit on MOTOTRBO™ IP Site Connect systems. Systems can consist of hundreds of repeaters

Can be used to reduce bandwidth needed at remote sites in larger IPSC networks

Uses IP network connections (private or internet) into MOTOTRBO™ systems. No control stations needed. Provides excellent audio quality

Allows MOTOTRBO™ to operate over commercial satellite and other high-latency networks

Can provide interoperability between MOTOTRBO™ IP Site Connect systems, non- MOTOTRBO™ systems (analog, P25, etc), and analog dispatch console systems, using optional Analog Interface

Extremely flexible call bridging and 'routing', based on talkgroups and/or pre-programmed 'patches'. Permanently or dynamically bridge between repeaters, groups of repeaters, analog ports, and even between time slots

Built-In network diagnostics - Monitor and troubleshoot IP network problems in IP Site Connect systems

Uses Linux operating system for high reliability

IP-based voice dispatch and manual remote bridging control capability, using PC-based client software (available for Windows or Linux workstations)

### RAYFIELD COMMUNICATIONS

2018 W. Woodland  
Springfield, MO 65807  
417-887-4663

[www.rayfield.net/c-bridge](http://www.rayfield.net/c-bridge)

# **System User's Guide and Reference Manual**

---

Copyright © 2015 RavenNet Systems, LLC

---

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Terms and concepts</b>	<b>1</b>
2.1	<i>Bridge Group</i> . . . . .	3
2.2	Configuration . . . . .	3
2.3	Firewalls . . . . .	4
2.4	Components . . . . .	4
2.5	<i>Control Center Inbound and Outbound</i> . . . . .	5
2.6	Variations . . . . .	6
2.7	It is a computer . . . . .	7
2.7.1	Backup . . . . .	7
2.8	Interpretation of graphs . . . . .	7
<b>3</b>	<b>Getting started</b>	<b>8</b>
3.1	Introduction . . . . .	8
3.2	The two form factors used . . . . .	8
3.3	Sockets provided at the rear of the form factors . . . . .	9
3.4	Three example networks that could be used . . . . .	10
3.5	Initial setup of a <i>Gateway</i> with a Front Panel display . . . . .	12
3.6	Manual setup of network settings on a <i>Gateway</i> . . . . .	13
3.6.1	Static IP setup . . . . .	14
3.6.2	Dynamic IP setup . . . . .	14
3.7	Configuring the <i>Control Center</i> . . . . .	15
3.8	URI - USB device . . . . .	15
<b>4</b>	<b>Usage options</b>	<b>16</b>
4.1	Introduction . . . . .	16
4.2	I run a taxi company . . . . .	16
4.3	My taxi fleets are in two cities . . . . .	16
4.4	Don't need extra <i>Gateway</i> . . . . .	17
4.5	<i>Analog</i> and <i>I.P.S.C.</i> networks . . . . .	17
4.6	Network connection to <i>Control Center</i> . . . . .	17

<b>5</b>	<b>Web page interface</b>	<b>17</b>
5.1	Login	18
5.2	Main page	19
5.3	Pop-up help	21
5.4	Config	22
5.4.1	Call Routing	23
5.4.1.1	Bridge Group configuration	23
5.4.1.1.1	Editing and altering <i>Bridge Groups</i>	24
5.4.1.1.2	Individual connection types	25
5.4.1.1.3	<i>Analog</i>	25
5.4.1.1.4	<i>I.P.S.C.</i>	27
5.4.1.1.5	<i>RnPc</i>	27
5.4.1.1.6	<i>RnIPc</i>	28
5.4.1.1.7	<i>Control Center Inbound</i>	28
5.4.1.1.8	<i>Control Center Outbound</i>	29
5.4.1.1.9	<i>Network Sound</i>	30
5.4.1.1.10	<i>SIP</i>	30
5.4.1.1.11	Altering the contents of <i>Super Groups</i>	31
5.4.1.1.12	Group calling - all groups	33
5.4.1.1.13	Private Voice, Private and group data	33
5.4.1.1.14	Block <i>Radio IDs</i>	33
5.4.1.2	Peer number mapping	34
5.4.1.3	Radio ID mapping	35
5.4.1.4	<i>Conference Server</i>	37
5.4.2	Email	38
5.4.2.1	Link to email server	38
5.4.2.2	Who receives emails	40
5.4.3	Hardware utilities	42
5.4.3.1	Configure ethernet card	42
5.4.3.2	Clock adjust	43
5.4.3.3	Serial Device	44
5.4.3.4	Restart system	44
5.4.4	System Utilities	45
5.4.4.1	General System	45
5.4.4.2	User Names and Passwords	48
5.4.4.3	Update <i>Control Center</i>	49
5.4.5	Backup/Restore	50
5.4.6	Configuration on attached <i>Gateways</i>	50
5.4.6.1	Channel common settings on a <i>Gateway</i>	51

---

5.4.6.2	Configuration of one TL-Net channel on a <i>Gateway</i> . . . . .	52
5.4.6.3	Configuration of one <i>I.P.S.C.</i> channel on a <i>Gateway</i> . . . . .	53
5.4.6.4	Configuration of one <i>I.P.S.C.</i> connection on a <i>Gateway</i> . . . . .	54
5.4.6.5	Configure serial device . . . . .	56
5.4.6.6	USB URI devices . . . . .	56
5.4.6.6.1	System report on one USB URI device . . . . .	57
5.4.6.7	Control repeater . . . . .	57
5.4.6.7.1	Configuration of attached LTR repeater . . . . .	58
5.4.6.7.2	Manage users . . . . .	59
5.4.6.7.3	Mass validation of all users . . . . .	60
5.4.6.7.4	Validate repeater . . . . .	60
5.4.6.7.5	Enable one user . . . . .	61
5.4.6.8	General System on a <i>Gateway</i> . . . . .	61
5.4.6.9	Users and passwords on a <i>Gateway</i> . . . . .	63
5.4.6.10	Network configuration on a <i>Gateway</i> . . . . .	63
5.4.6.11	Email configuration (on remote <i>Gateway</i> ) . . . . .	64
5.4.6.12	Restart system (on remote <i>Gateway</i> ) . . . . .	64
5.5	Calls . . . . .	65
5.5.1	Summary . . . . .	65
5.5.1.1	Today's calls . . . . .	65
5.5.1.2	Before today's calls . . . . .	66
5.5.1.3	X days ago . . . . .	66
5.5.2	Detail . . . . .	66
5.5.3	<i>ODBC</i> . . . . .	67
5.5.3.1	Firewalls . . . . .	67
5.5.3.2	<i>ODBC</i> Configuration details . . . . .	68
5.6	Diagnostics . . . . .	68
5.6.1	Web page login status . . . . .	69
5.6.2	Logs . . . . .	70
5.6.2.1	All failed calls . . . . .	70
5.6.2.2	Logs of link status . . . . .	71
5.6.2.3	System log . . . . .	72
5.6.2.4	System status . . . . .	73
5.6.2.5	License information . . . . .	73
5.6.2.6	Email manager . . . . .	74
5.6.2.7	<i>Conference Server</i> . . . . .	74
5.6.2.7.1	Announcement tracks on the <i>Conference Server</i> . . . . .	75
5.6.3	Load levels . . . . .	76
5.6.3.1	CPU Load levels . . . . .	76

---

5.6.3.2	Transit times . . . . .	78
5.6.4	Network Information . . . . .	78
5.6.4.1	DNS report . . . . .	78
5.6.4.2	NAT report . . . . .	79
5.6.4.3	Measure bandwidth . . . . .	80
5.6.4.4	TCP Retransmit rate . . . . .	83
5.6.4.5	Network traffic volume . . . . .	83
5.6.4.6	Connectivity to remote host . . . . .	84
5.6.4.7	Response time of web pages . . . . .	87
5.6.4.8	IP address of connected machines . . . . .	88
5.6.5	CC↔CC links and gateway status . . . . .	88
5.6.5.1	<i>Control Center</i> Status . . . . .	89
5.6.5.2	Live network . . . . .	90
5.6.5.3	Named members . . . . .	91
5.6.6	Upgrade diagnostics . . . . .	91
5.6.6.1	Upgrade status . . . . .	91
5.6.6.2	Upgrades serviced by <i>Control Center</i> . . . . .	92
5.6.7	LTR and Analog . . . . .	93
5.6.7.1	Monitor levels, generate tone . . . . .	93
5.6.7.2	Command to LTR . . . . .	94
5.6.7.3	Reset LTR . . . . .	94
5.6.7.4	USB devices . . . . .	95
5.6.7.4.1	USB URI devices . . . . .	96
5.6.7.4.2	USB -- Serial devices . . . . .	96
5.6.8	Diagnostic on <i>Gateway</i> . . . . .	97
5.6.8.1	Scan for Hoot-n-Holler devices . . . . .	98
5.6.8.2	Logs . . . . .	98
5.6.8.2.1	System log . . . . .	98
5.6.8.2.2	System status . . . . .	98
5.6.8.2.3	License information . . . . .	98
5.6.8.2.4	Email manager . . . . .	98
5.6.8.3	Load levels on <i>Gateway</i> . . . . .	98
5.6.8.3.1	CPU load levels on <i>Gateway</i> . . . . .	98
5.6.8.3.2	Transit time on <i>Gateway</i> . . . . .	98
5.6.8.4	Network Information . . . . .	98
5.6.8.4.1	DNS report . . . . .	99
5.6.8.4.2	NAT report . . . . .	99
5.6.8.4.3	Measure bandwidth . . . . .	99
5.6.8.4.4	TCP Retransmit rate . . . . .	100

---

---

5.6.8.4.5	Network traffic volume . . . . .	100
5.6.8.4.6	Network performance to <i>Control Center</i> . . . . .	100
5.6.8.5	LTR and Analog . . . . .	103
5.6.8.5.1	Monitor levels, generate 1 kHz tone . . . . .	103
5.6.8.5.2	Command to LTR . . . . .	103
5.6.8.5.3	Reset LTR device . . . . .	103
5.6.8.5.4	USB devices . . . . .	103
5.6.8.6	<i>Gateway</i> channel information . . . . .	103
5.6.8.6.1	Status . . . . .	104
5.6.8.6.2	Status of one audio channel . . . . .	104
5.6.8.6.3	Message log for one audio channel . . . . .	106
5.6.8.6.4	Error log for one audio channel . . . . .	107
5.7	Net watch . . . . .	108
5.8	CC↔CC . . . . .	109
5.9	Help . . . . .	110
<b>6</b>	<b>Troubleshooting</b>	<b>111</b>
6.1	<i>Gateways</i> not connecting with the <i>Control Center</i> . . . . .	111
<b>7</b>	<b>Technical comments</b>	<b>112</b>
7.1	Transcoding of audio . . . . .	112
7.2	Jitter buffer . . . . .	112
7.3	One call is . . . . .	113
7.4	One Complex Call . . . . .	115
7.5	Get Call Log . . . . .	115
<b>8</b>	<b>Acknowledgement</b>	<b>116</b>

---



## List of Figures

1	Simplest possible network . . . . .	1
2	Normal network . . . . .	2
3	Graphical relationship between the components . . . . .	4
4	Example screenshot from a <i>Control Center Gateway</i> combo . . . . .	6
5	Call count over an 8 day period . . . . .	8
6	Compact format - capable of 2 audio channels . . . . .	9
7	Larger rack mount version which can support 20 audio channels. . . . .	9
8	Rear of the compact form factor. . . . .	9
9	Rear of the rackmount box . . . . .	10
10	Five radio two system with <i>Primary Control Center</i> and <i>Secondary Control Center</i> . . . . .	10
11	A simple dispatch system . . . . .	11
12	Illustration of interoperability provided by the system . . . . .	12
13	URI - USB . . . . .	15
14	Initial login window . . . . .	18
15	Username password request window . . . . .	19
16	Returning to a previous session . . . . .	19
17	Home window . . . . .	20
18	Navigation menu as seen by <i>Low User</i> . . . . .	21
19	Pop up help . . . . .	22
20	Main Configuration window . . . . .	23
21	Selection of the different ways of joining calls together . . . . .	24
22	Editing of <i>Bridge Groups</i> window . . . . .	24
23	<i>Analog</i> connection with the <i>Control Center</i> . . . . .	25
24	Configure <i>I.P.S.C.</i> connection to a <i>Control Center</i> . . . . .	27
25	Configure a <i>RnPc</i> connection with the <i>Control Center</i> . . . . .	27
26	Different fields available for a <i>RnIPc</i> connection with a <i>Control Center</i> . . . . .	28
27	The different fields for a <i>Control Center Inbound</i> to the <i>Control Center</i> . . . . .	29
28	Different fields for a <i>Control Center Outbound</i> connection - which is created to another <i>Control Center</i> . . . . .	29
29	Different fields for a <i>Network Sound</i> connection . . . . .	30
30	Different fields for a <i>SIP</i> connection . . . . .	31
31	<i>Super Group</i> configuration . . . . .	32
32	An extensive <i>Super Group</i> . . . . .	33
33	Configuring private voice, private and group data . . . . .	33
34	Block radio IDs . . . . .	34
35	Peer number mapping . . . . .	35
36	Radio ID Mapping . . . . .	36
37	Configuration of the <i>Conference Server</i> . . . . .	37

---

38	Email manager . . . . .	38
39	Link to email server . . . . .	39
40	Configure which people receive which emails . . . . .	41
41	Alter/View ethernet card settings . . . . .	42
42	Clock adjust . . . . .	43
43	Configure serial device on <i>Control Center</i> . . . . .	44
44	Restart system . . . . .	45
45	System configuration . . . . .	46
46	User Names and Passwords . . . . .	48
47	Update <i>Control Center</i> . . . . .	49
48	Configuration on a <i>Gateway</i> - option selection . . . . .	51
49	Configuration Channel common on a <i>Gateway</i> . . . . .	52
50	Configure one channel window . . . . .	53
51	Configuration of one <i>I.P.S.C.</i> channel . . . . .	54
52	Configuration of one Motorola <i>I.P.S.C.</i> connection . . . . .	55
53	Uniquely identifying each USB URI device . . . . .	57
54	System report of one USB URI device . . . . .	57
55	Attached repeaters and configuration selection . . . . .	58
56	Controller, Configuration for repeater 1 . . . . .	59
57	Manage users for repeater 1 . . . . .	59
58	Mass validation of all users on repeater 1 of <i>Gateway a</i> . . . . .	60
59	Validate repeater 5 . . . . .	60
60	Enable 1 user . . . . .	61
61	General system configuration on a <i>Gateway</i> . . . . .	62
62	Users and passwords on a <i>Gateway</i> . . . . .	63
63	IP address settings on a remote <i>Gateway</i> . . . . .	64
64	Previous calls window . . . . .	65
65	Today's calls in the database . . . . .	66
66	Calls for a date before today . . . . .	66
67	Detailed list of recent calls . . . . .	67
68	Diagnostics window . . . . .	69
69	Recent Web Page Login/Out activity and current users . . . . .	70
70	All failed calls . . . . .	71
71	Logs of link status . . . . .	72
72	System log on <i>Primary Control Center (Primary Main)</i> . . . . .	72
73	System status . . . . .	73
74	Report on the license settings . . . . .	74
75	Status of the <i>Conference Server</i> . . . . .	75
76	Announcement tracks on the <i>Control Center</i> . . . . .	76

---

77	CPU busy report for <i>Primary Main</i> . . . . .	77
78	Network Information Window . . . . .	78
79	DNS report for <i>Control Center</i> . . . . .	79
80	NAT report for <i>Control Center</i> . . . . .	80
81	Measure Bandwidth Window . . . . .	81
82	Measurement of the bandwidth between the <i>Control Center</i> and <i>rndownload</i> . . . . .	82
83	Bandwidth measurement completed . . . . .	82
84	TCP retransmit rate . . . . .	83
85	Measured network usage on a <i>Control Center</i> . . . . .	84
86	Example connectivity report with remote host . . . . .	85
87	Percentage of packets dropped between the <i>Control Center</i> and remote site. . . . .	86
88	Round trip time for packets between the <i>Control Center</i> and remote site . . . . .	86
89	Response time of web pages . . . . .	87
90	IP Addresses of connected machines . . . . .	88
91	<i>Control Center</i> Status . . . . .	89
92	Live network window . . . . .	90
93	Named Members window . . . . .	91
94	Upgrade status during an upgrade . . . . .	92
95	Upgrade status during an upgrade . . . . .	92
96	Upgrades serviced by <i>RnSrv</i> . . . . .	93
97	Message log on <i>Upgrade Server</i> . . . . .	93
98	Monitor levels, generate tone . . . . .	94
99	Command to LTR . . . . .	94
100	Reset LTR . . . . .	95
101	All USB devices attached to <i>Gateway a</i> . . . . .	95
102	Report on available USB URI devices . . . . .	96
103	Report on USB -- Serial devices . . . . .	96
104	Diagnostic on a remote <i>Gateway</i> . . . . .	97
105	Network Information Window for a <i>Gateway</i> . . . . .	99
106	<i>Gateway</i> initiated measurement of bandwidth . . . . .	100
107	Network performance between <i>Gateway a</i> and <i>Primary Control Center</i> . . . . .	101
108	Abysmal link <i>Control Center</i> to <i>Gateway</i> . . . . .	102
109	Abysmal link <i>Control Center</i> to <i>Control Center</i> . . . . .	103
110	Status report selection for <i>Control Center</i> and <i>Gateway</i> . . . . .	104
111	Status of one audio channel . . . . .	105
112	Message log for one audio channel . . . . .	107
113	Error log for one audio channel . . . . .	108
114	Net watch window . . . . .	109
115	CC↔CC . . . . .	110
116	Help window . . . . .	111
117	Spacing of packets at destination channel . . . . .	113
118	Components to carry one voice call . . . . .	114
119	Components to carry voice between multiple <i>Control Centers</i> and to radios . . . . .	115

## List of Tables

1	Sample <i>Bridge Group</i> . . . . .	3
2	Pins to be used in DB25 connector . . . . .	16
3	Optional call setup pins . . . . .	16
4	Devices used for screenshots . . . . .	18
5	Devices used for screenshots . . . . .	18
6	Sample <i>Bridge Group</i> . . . . .	26
7	Sample Email Config values . . . . .	39
8	Sample Email Config values (SSMTP method of sending) . . . . .	40
9	Different classes of email that can be sent out . . . . .	41
10	<i>ODBC</i> configuration details . . . . .	68
11	Documents contained in this section . . . . .	116

### Abstract

The use of a networking program which allows radios to extend their range is described. With this program, the audio data is carried over ethernet cables from one site to another. The audio packets travel from the source radio, through an interfacing computer, to a conferencing like system (which duplicates the packets as required) and on sends to 1 (or more) interfacing computers and out to remote radios.

The networking program runs on an appliance like box and presents a web page to the user for configuration and status reporting.

Motorola digital radios, analog radios, and PCs can be connected together to form *Bridge Groups* of unlimited size. Further, multiple disparate networks of these systems can be joined together.

## 1 Introduction

The goal of radio networking is to enable calls from one radio to reach a remote radio, even though they are separated by distances in excess of the transmission range. It should also be possible to link one radio with many other radios. The audio traffic between the radios is carried on some form of ethernet, (eg. public internet, WAN, VPN, or LAN).



### Please read

It is expected that the reader has read and understood Section 2 before examining other sections. Given the above condition, the reader can read any other section and should be able to understand the description. Reading other sections first is pointless.

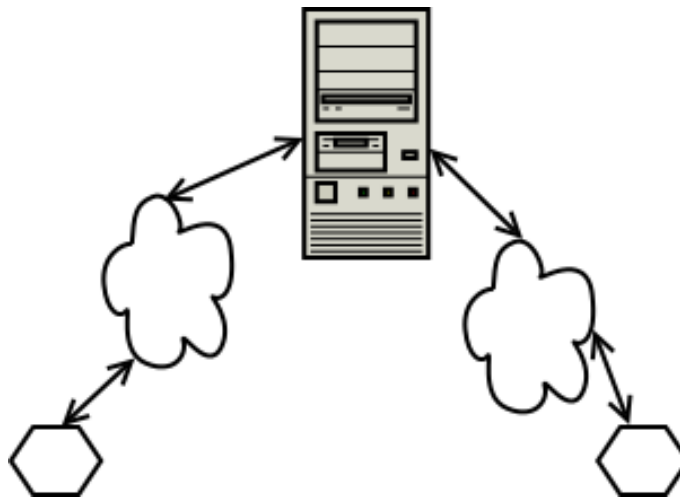
---

## 2 Terms and concepts

This section describes the basic principles that are key to understanding the operation of this program. Every page in this online help is written with the view that the reader has understood the contents of this section.

At its most simplest, the network can be considered as shown in Figure 1 which contains two endpoints and one *Conference Server* in the middle.

Figure 1: Simplest possible network



*The two endpoints (hexagons) which could be radios, PCs, or other hardware are connected to each other via the central box, which operates as a Conference Server. Connection between the Conference Server and endpoints is through the cloud shape, which represents an ethernet based link.*

Figure 1 could be extended to have many more endpoints, but for simplicity two are shown. With such a simple network, an operator at the first endpoint can converse with the operator at the other endpoint, even though they are separated by thousands of miles. Endpoints are typically radios (digital or analog) but they can be PCs. The *Conference Server* in this simple network has minimal work to do. All calls that come in from one side are duplicated and sent to the other side.

Figure 1 does not indicate how many radios are connected to each endpoint. The description above implies just one radio at each endpoint. Suppose there were 20 radios on each endpoint. In this case, the *Conference Server* needs information as to which radio can be connected to which radio. Consequently, it would be possible for a radio (on the left) to speak and a radio on the left hears the spoken words. For this situation, the audio has traversed the link to the *Conference Server* twice.

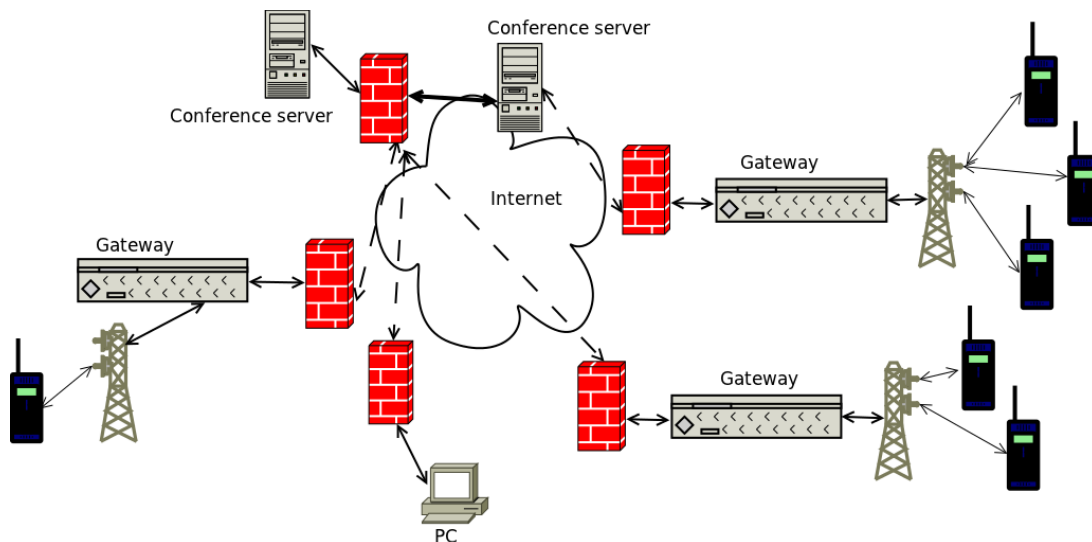
Equally possible would be that the audio from one radio is sent to 39 other radios. The actual grouping of who receives audio is set entirely by the operator of the *Conference Server*. Some radios gets more (or less) permissions as to who they can talk to.

---

In extensive networks, multiple *Conference Servers* are used so that multiple networks of radios/PCs can be connected. Firewalls will be used in some places to reduce the exposure of computers to traffic on the internet. There will be PCs that are connected to the *Conference Server*.

A more complex network is shown in Figure 2 which contains six radios, three radio endpoints, one PC endpoint, and two *Conference Servers*.

Figure 2: Normal network



There are two Conference Servers in this network. One Conference Server has links to a PC and two radio endpoints. The Conference Server on the right has a link to one radio endpoint. The Conference Servers are connected to each other, which means that calls can be sent between any two radios in the diagram (or between a radio and PC). Note that calls which travel from one radio endpoint to another always travel through a Conference Server.

Depicted are three base stations (or Gateways, or endpoints) which connect a radio mast with a firewall, which connects to a Conference Server. It is the base station computer that is responsible for turning the audio data from the radio into ethernet packets, which are on-sent to the Conference Server. The Conference Server will take the incoming ethernet packets and on-send them to the designated recipient(s). The base station computer that receives incoming ethernet packets will turn them into audio data, and send this out the radio mast to the remote operator.

Given the complexity of the possible linking pattern in Figure 2, some definitions are required so that the desired connection pattern can be achieved. At the very least, an endpoint has two variables, *sitename* and *home repeater*. Typically, the *sitename* is a term that has meaning to the operators. The *sitename* describes the physical location of the radio mast. For PC endpoints, Gateways and Conference Servers, the *sitename* is the name that best describes the device's physical location. The *home repeater* can be considered as a channel number, and is between 1 and 20. Use of a *home repeater* number makes it much easier to differentiate between the radio operators at a site. A radio endpoint has a third label, the *userID*, which uniquely identifies one particular radio. From the combination of *sitename*, *home repeater*, and (perhaps) *userID*, it is possible to configure where a call should go.

The terms *Gateway*, base station, and endpoint have been used to describe the entity that has the shortest connection to the radio. Any of these terms are appropriate. For the remainder of this document, the word *Gateway* will be used to describe the entity that connects a radio with the ethernet.

The diagram of Figure 2 has described the *Gateway* as an entity which turns analog audio (from a radio) into ethernet packets, which are on-sent to the *Conference Server*. However, when connecting with Motorola repeaters, there is an ethernet connection between the *Gateway* and repeater. In this case, the *Gateway* takes the ethernet packets from the Motorola repeater and reformats them so that are suitable for the *Conference Server* (or vice versa). When interacting with a Motorola repeater, the word *Gateway* is still accurate as the audio packets are transferred from one network to another network.

## 2.1 Bridge Group

Table 1 gives a simple example of a *Bridge Group* (which is a collection of *sitenames*, *userIDs* and *home repeater* values). This table forms the basis for how this program links calls from one site to another. Each line in the table describes one possible audio circuit, or channel. When one member of a *Bridge Group* sends audio to the *Conference Server*, all other connected members (who match the specified *sitename*, *home repeater* and *userID* values) will receive an exact copy of the incoming audio. Please ensure that you understand this example. Table 1 displays four entries. The first three are radios, and the last is a PC connection.

Table 1: Sample *Bridge Group*

Connection Type	Site Name	home repeater	userID
Analog	Eastern Hills	11	123
Analog	Eastern Hills	1	13
Analog	Blue Mountain	9	233
PC	Main Office	9	

Consequently, when the operator at Blue Mountain (*home repeater* 9, *userID* 233) presses the PTT button, the other three entries in the table will hear what is said. Two of the recipients are connected to the Eastern Hills site, and the third is in the Main Office.

In Table 1, the connection type is reported. The *Blue Mountain* entry (for example) has a connection type of *Analog*. All radios connect through a *Gateway* to the *Conference Server*.

The Blue Mountain site actually has 10 connections to the *Control Center* - where each connection has a *home repeater* value of 1 through 10. Only those users (on the Blue Mountain site) that have connected via the *home repeater* value of 9 can send audio into (or receive audio from) this *Bridge Group*. Further limiting the users at Blue Mountain is the requirement that they are on *userID* 233. Consequently, the Blue Mountain user on *home repeater* 9 and *userID* 139 cannot speak into (or hear from) members of this *Bridge Group*.

Section 5.4.1 describes the editing of *Bridge Groups*. Other information is also entered, but the values listed above are the crucial pieces. It is the information in each line that determines which bridge group is connected to a remote radio. Consequently, the radio at *site name* *Blue Mountain*, *home repeater* 9, *userID* 200 cannot send audio through the *Conference Server* using this *Bridge Group*.

Table 1 is a very simple example of what can be achieved. The table can be much longer - there is no limit to the number of lines. The PC entry (in the Main Office) does not have a *userID* entry as such information is irrelevant (for PC connection types). Other connection types managed by this system have not been listed for simplicity. Additional fields in each row of the table are used for other connection types. The table could have been just one entry. This will route the call nowhere, but it is a valid configuration.

## 2.2 Configuration

Configuration of the system is done via a web page provided by the *Control Center*. Even the configuration of the computers at the base stations (hereafter referred to as *Gateways*) is done via the web page provided by the *Control Center*.

This program has been designed so that all configuration is via a web page. Consequently, there is no need to install software programs on external computers. Thus, this computer can be controlled from a Windows, Mac, Linux, or BSD computer. Even the people who wrote this program interact with it completely via the various web pages.

All of the major browsers have been tested and approved for use with the web server provided by the program. IE6 and later, Opera, Firefox, Safari, and Chrome are all approved for use. The URL used is the concatenation of the strings "*http://*", IP address of the *Control Center*, and *":42420"*. The *":42420"* indicates that a non standard port number is used to supply web pages. Consequently, the web server in the *Control Center* is not detrimentally loaded by search engines that trawl the web. Javascript needs to be enabled on the web browser as it is used for 1)drawing graphs, 2)rendering animated displays and 3)handling button events.

Suppose the *Control Center* is situated at the public IP address of *10.12.13.14*, then the web browser should be connected to *http://10.12.13.14:42420*. Alternatively, if one uses the *dyndns* option and configures the *Control Center* to be at *examplecc.dyndns.org*, then the web browser should be directed to *http://examplecc.dyndns.org:42420*.

## 2.3 Firewalls

The diagram in Figure 2 contains five firewalls. Since firewalls are a normal part of network equipment, the voice/data protocol used will tunnel through and connect the *Gateway* (or PC) to the *Control Center*.

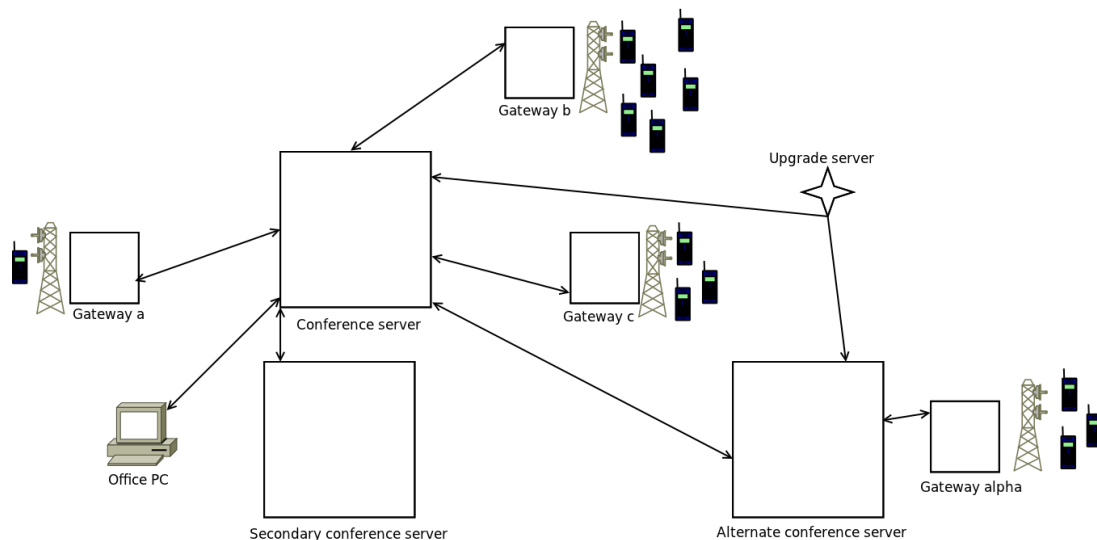
When the *Control Center* is positioned behind a firewall, it is asked that the ports 42420..42432 (UDP and TCP) are forwarded through the firewall to the *Control Center*. The same port forwarding is optional for *Gateways*. With this port forwarding for *Gateways*, it makes it easier to do (remotely) site access and repair.

In some setups, everything could be on the same VPN, which is not accessible from the public internet. In this case, suppose the *Control Center* was at IP address 192.168.30.4. Consequently, configuration of the system would only be possible to people who are connected to the VPN. The browser would be configured to go to `http://192.168.30.4:42420`

## 2.4 Components

The major logical entities within this program are defined in this section. By describing them here, a framework is provided for understanding how the system works.

Figure 3: Graphical relationship between the components



*A block diagram of the relationship between the main components of the system. The radios connect through a radio tower, to the Gateway, which connects with the Conference Server. The Conference Server dispatches (in real time) the incoming call to the designated recipients. The link between the Conference Server and the Alternate Conference Server can be used for transferring calls. Lastly, the Secondary Conference Server is used in the event of the network link to the Conference Server failing.*

The block diagram shown in Figure 3 shows the major components of the system. It is perhaps easiest to explain it with the following statements:

- A call from one radio will be received, passed through the *Gateway*, and then sent to the *Conference Server*.
- Incoming calls to the *Conference Server* are duplicated and sent to each of the specified recipients. A recipient may be a remote radio, which means the audio has to pass through the *Gateway* connected to that remote radio.
- A valid path for a call would be for it to travel from the one radio attached to *Gateway a* through the *Conference Server* to the first radio at *Gateways b & c* and to the Office PC. One possible reverse route would have been for the Office PC to send audio to the first radio at *Gateways a, b & c*.



- A *Conference Server* may experience network failure. In which case, any *Gateways* attached to that *Conference Server* will immediately (within 30 seconds) connect to the *Secondary Conference Server*. This reconnection to a *Secondary Conference Server* is essentially immediate - and will happen even if there is no voice traffic.
- In the same way that a call is sent from a *Gateway* to a *Conference Server*, calls can be sent between two *Conference Servers*.
- If an *Alternate Conference Server* is available (as depicted in Figure 3), and the *Conference Server* fails, the *Alternate Conference Server* will build a link to the *Secondary Conference Server*.
- Calls are not restricted to radios. They may be sent to, or received from a PC. Additionally, calls may be sent from one Conference center to another. Sending calls between Conference centers allows for linking of disparate networks.
- The *Upgrade Server* provides a copy of the latest changes. Should the administrator choose to upgrade the *Conference Server*, then the new image is downloaded from the *Upgrade Server*. The *Conference Server* reboots and runs the new image. The *Gateways* detect that the version of the *Conference Server* has changed, so they update to the new version from the *Conference Server*. In the same way that the *Gateways* upgrade, the *Secondary Conference Server* will upgrade also.
- The term *Conference Server* has been used to describe the central point because that provided a reasonable description of the function :: Duplicating audio from one source to many recipients. However, the *Conference Server* is more than just for handling audio. It manages upgrade images, configuration commands from the administrator, a database for logging past calls, a web server for configuration and reporting of status, performance monitoring of links, and can do the work of a *Gateway*. Consequently, the term *Control Center* is used to describe all the functionality provided by the central point. The term *Conference Server* only implies voice multiplexing and is not broad enough. In this document, when the phrase *Conference Server* is used, a voice multiplexer is being described.
- The *Gateway* is a device whose main purpose is for turning audio information from the radio into something that can be sent to the *Control Center* (or vice versa). In networking terminology, a *Gateway* is something that takes data from one network and transfers the data to a second network. In radio networking, the *Gateway* is similar to a base station. This documentation and program uses the term *Gateway*, even though the *Gateways* described here do much more than transfer voice from one network to another. The additional work of handling upgrades, link monitoring, manage serial port and USB devices, and log all activity would suggest a different term is required. However, the primary work of a *Gateway* is the transfer of voice from the radio network to ethernet, so the term *Gateway* is used.
- The *Gateway* does provide its own web page which can be used in extreme circumstances, such as when the *Control Center (Primary and Secondary)* are unavailable.
- Suppose the link between *Gateway a* (the source of the call) and the *Control Center* passes only some of the network packets of an audio call, then all of the recipients (*Gateway b* to *Gateway g*) will hear poor quality audio. Instead, suppose that just the link between the *Control Center* and *Gateway g* is bad. In this case, the recipients at *Gateway b..Gateway f* will hear great audio. The recipient at *Gateway g* will hear poor quality audio.

## 2.5 Control Center Inbound and Outbound

The inbound and outbound connections on a *Control Center* describe the mechanism of joining two *Control Centers* together. The diagrams of Figure 2 and Figure 3 gives the impression that two *Control Centers* are joined together. The actuality is that two *Bridge Groups* (one from each *Control Center*) are joined together. When a member of one *Bridge Group* sends audio, everyone else in the local *Bridge Group* will hear audio. The members in the *Bridge Group* on the remote *Control Center* will hear the same audio.

Placing the *inbound* and *outbound* connection types together will form one link. At one end (on one *Control Center*) there is an *outbound* connection. At the other end of the link (on a different *Control Center*) there is an *inbound* connection.

The *Control Center Outbound* describes an entity that goes outside and attempts to connect with something out there. Hence, it is described as an *Outbound* link. In the specification of the *Control Center Outbound*, the IP address of the remote *Control Center* (and the emergency/backup *Control Center*) is specified. Note the similarity with the operation of the *Gateway*. On the *Gateway*, one has to specify the *Primary* and *Secondary Control Center*.

The *Control Center Inbound* describes a listening and waiting entity. It waits for the time when the *Outbound* attempts to build the connection. At this point in time, the *Inbound* establishes the reception of the link. When defining a *Control Center Inbound*, one has to specify the *sitename* and link id of the far end. Note the similarity to defining an incoming *Gateway* entry for a *Bridge Group*.

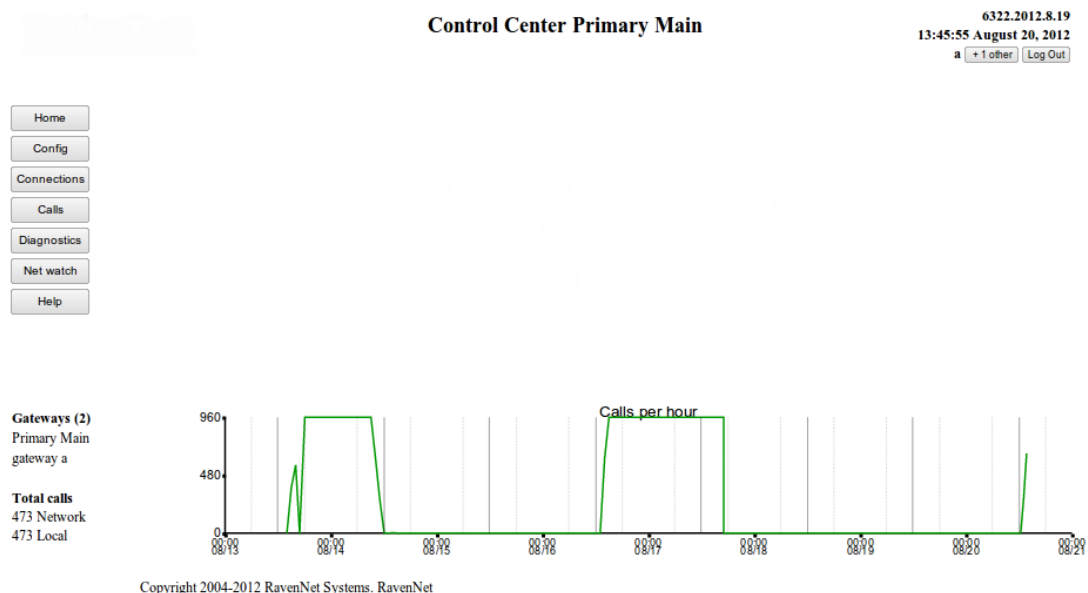
The *Inbound* and *Outbound* entities allow the site maintainer (at each *Control Center*) to keep track of who talks where. Consequently, users at the remote *Control Center* are limited to speak into just one *Bridge Group*. Further, it means that multiple links (between two *Control Centers*) can be maintained at the same time while maintaining tight control over who talks where.

It maybe helpful to think of the *Control Center Inbound* and *Control Center Outbound* as an audio circuit. The audio circuit is established in a particular order. The *Outbound* goes out and builds it - the *Inbound* waits for the creation event to happen. Once built, audio can be handled in either direction across the link.

## 2.6 Variations

The diagram in Figure 2 shows the *Control Center* as a separate entity to the *Gateway*. In some cases, the *Control Center* and one *Gateway* are combined into one box. Combining a *Control Center* and *Gateway* is done at installation time and reduces the hardware requirements. The web page provided by the *Control Center* maintains a consistent interface to the *Gateways* - the access method is independent of the physical location of a *Gateway*. Thus, if the network contains four *Gateways*, where three are in separate boxes and one is inside the *Control Center* the access method is still the same. All four *Gateways* are accessed via the web page of the *Control Center*. The example screenshot in Figure 4 describes the case where the *Primary Control Center* is running with an internal *Gateway* and there is the external *Gateway a*.

Figure 4: Example screenshot from a *Control Center Gateway* combo



The *Control Center Primary Main* is running as a *Gateway*. Consequently, the list of *Gateways* at the bottom left of the screen does show *Primary Main* as a connected *Gateway*. Note that *Gateway a* has connected to *Primary Main*, so is in the list at the bottom left also.

Note the uniformity of the call count. *Primary Main* has been running an automated test process that works out at 960 calls an hour. From the graph, it finished at 5pm on Friday 17 August 2012. Tests restarted at midday on Monday 20 August.

Configuration of the *Gateway* features on *Primary Main* is done in exactly the same manner as the *Gateway* features on *Gateway a*.

Normally, the *Gateways* are configured via the web page provided by the *Control Center*. However, there are times when this cannot be done (eg. partial network failure) and the user needs to configure the *Gateway*. In this case, you can use the web page provided by the *Gateway*, which has the same addressing format as the *Control Center*.

Additional *Control Centers* can be used in case of network failure. The backup *Control Center* is referred to as a *Secondary Control Center*. The *Primary Control Center* will automatically duplicate all *Bridge Groups*, usernames and all other relevant information to the *Secondary Control Center*. When the internet link to the *Primary Control Center* fails, the *Gateways* transfer

to the *Secondary Control Center*. The transfer normally happens within 30 seconds of complete link failure to the *Primary Control Center*. If the *Gateways* detect partial failure of the link to the *Primary Control Center* (only some packets are lost) it is unknown when or if the transfer happens. The timing of the transfer is determined by the severity of the packet loss rate.

## 2.7 It is a computer

The *Primary Control Center*, *Secondary Control Center*, *Alternate Control Center*, and *Gateway* are all computers running the Linux operating system. The web pages and this documentation have the minimum of computer like terms. The approach taken to using this product is that it is an appliance - something that is just plugged into the wall, connected to the web and used. The networking approach taken minimizes the amount of external device configuration. The update process has been designed to be extremely simple and reliable.

Some points should be made on what you can and cannot do with the system.

1. Do not touch/edit/change the file `/ravennet/copyright.txt`. This will break the license on the box.
2. Do not have a usb flash drive in the computer when the program starts up.
3. Do not upgrade the kernel. This will break the license on the box.
4. It is not expected for you to manually alter any of the files on the computer. Indeed, touching or altering the files may rend the box inoperable.

The developers who wrote and tested this software only interact with the running system via the web page. Consequently, the web page interface is designed for simplicity and ease of use.

5. Like any computer, abrupt power off events are not good. The OS will cope with some power off events. How many of these events is unknown - it depends on the timing of the event. New versions of the software can be transferred to the computer at various times. It is relatively safe to abruptly turn the power off while the new version is being transferred. Abrupt power off while the new version is installing is absolutely dangerous and must be avoided.

### 2.7.1 Backup

It does make sense to copy the configuration file on the *Control Center* and attached *Gateways* as a precaution. There are two ways to do this.

1. Use the *Get Backup File* button from the config page. This will create one `.zip` file that contains the configuration files from the attached *Gateways* and *Control Center*. The `.zip` file contains information on the time and date that the backup file was created. Save this file to a safe place. Should your box need replacing, the backup file contains all the configuration settings required to restore your system to its previous state.
2. Set the browser to `http://ip.address.cc:42420/report?mcp.ini`. Put the mouse in the page, click right button to save as. This will save the `mcp.ini` file for the box at `ip.address.cc`. This approach can be scripted so that a remote computer will extract the configuration file. In this case, use the **wget utility** and bring back the `mcp.ini` file specified above.

## 2.8 Interpretation of graphs

Consider Figure 107 which shows the measured network performance between *Gateway a* and a *Control Center*. The two graphs in this figure are an example of two of the three styles used in this documentation.

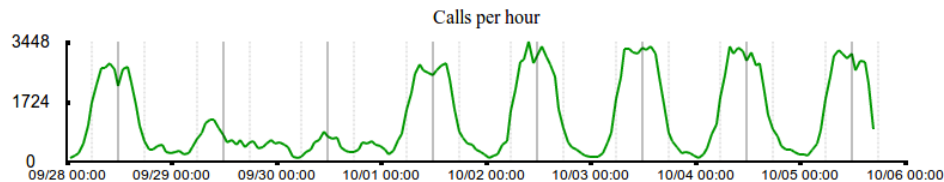
Along the bottom of the graph is the time and date. The time is in 24 hour format (two digits for hours, two digits for minutes, and two digits for seconds). Below the time is the date (two digits for month, then two digits for day). Consequently, 00:00:00 07/21 refers to the very beginning of July 21<sup>st</sup> (midnight).

The y axis may have a linear or logarithmic scale. Typically, linear scales are used when the range of values being plotted is tightly defined. Thus, a performance figure expressed as a percentage will always be a linear scale as the values can only be 0 to 100. A logarithmic scale is used when the range of values being plotted can expand over many orders of magnitude, which is the case with round trip times. For round trip times, the measured value can be between 0.1 milliseconds and 6500 milliseconds (4 orders of magnitude). A logarithmic scale makes it possible to see the relative magnitude of all measured values.

The horizontal lines on the logarithmic scale are always placed at some multiple of 1, 2.5, 5, 7.5, and 10. This placement is illustrated in the bottom graph of Figure 107. On those graphs where three orders of magnitude separate the top and bottom values, only some of the horizontal gray lines have labels.

The third graph style used in Figure 17 is designed to give a quick view of if the system is handling calls, or not. Consequently, the graph is drawn as simply as possible, with only three ticks on the y axis. Call count for previous days (one week) is shown, so the user gets some perspective on how the values for today compare with other days. The y axis is linear. A second example of this graph is given in Figure 5.

Figure 5: Call count over an 8 day period



*The count of calls graph, as reported on the main web page. Note that in the year this data was collected, October 5<sup>th</sup> is a Friday. There is minimal activity in the weekend or evenings. It is only during business hours that the system gets busy. Also visible is the lunch hour - there is a drop in usage around midday.*

## 3 Getting started

### 3.1 Introduction

This document is written for use with a radio networking product that could be described as a set of one (or more) computers that are connected via the ethernet. Interfacing the computers to the radios is achieved with some external hardware. The external hardware may be a Motorola Repeater, or a TL-Net controller.

Section 3 is designed to give you enough information to turn the computer on, connect it to the internet, and then begin the configuration process with a web browser. The information described here is sufficient for a moderately competent person to get underway.

### 3.2 The two form factors used

There are two form factors for the supplied computer. Either, it is in a compact format, as shown in Figure 6

Figure 6: Compact format - capable of 2 audio channels



*The compact form of the supplied computer. Capable of supporting 2 audio channels. Configuration of the IP address of this box can be done using the buttons beside the front screen.*

Alternatively, a larger rackmount version is available, which is shown in Figure 7.

Figure 7: Larger rack mount version which can support 20 audio channels.

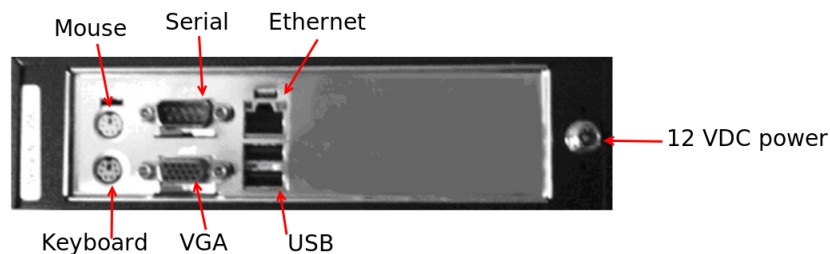


*Rackmount version of the supplied computer. Power and reset switches are shown on the left. Status lights are shown.*

### 3.3 Sockets provided at the rear of the form factors

The rear of the compact form factor is reported in Figure 8.

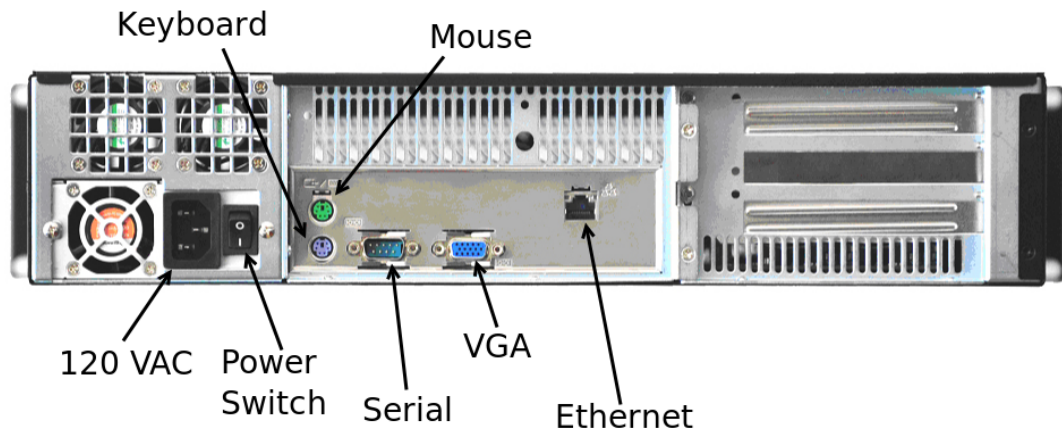
Figure 8: Rear of the compact form factor.



*The back of the compact form factor. The name of the different sockets is given in an endeavor to aid installation.*

The rear of the rackmount form factor is reported in Figure 9.

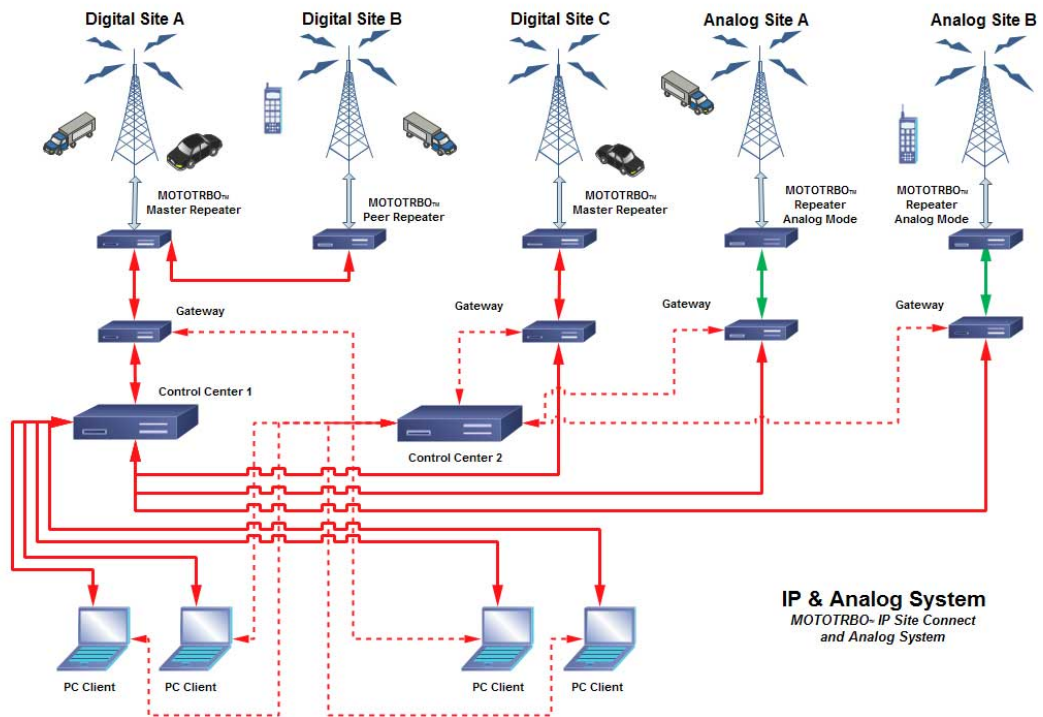
Figure 9: Rear of the rackmount box



The rear of the rackmount form factor. The name of the different sockets is given in an endeavor to aid installation.

### 3.4 Three example networks that could be used

Figure 10: Five radio two system with *Primary Control Center* and *Secondary Control Center*



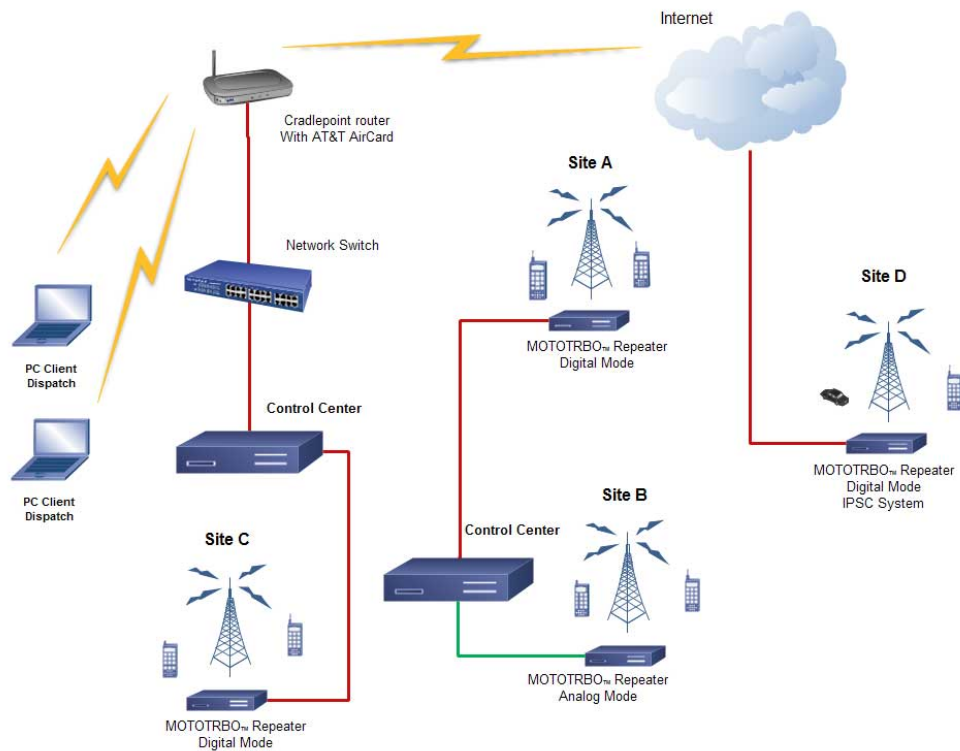
A moderately complex network with five transmitting sites, two Control Centers and four instances of Gateways. Also shown are four PC Clients which are connected to both Control Centers. The Control Centers are arranged so that Control Center 1 is the Primary Control Center. Control Center 2 is the Secondary Control Center.



The *Gateways* connected to *Digital Site A* and to *Digital Site C* speak the Motorola digital protocol. Consequently, any voice that passes through *Control Center 1* can be sent to (or received from) the Motorola endpoints. The analog sites have a *Gateway* at each so that these sites can send audio to/from the digital Motorola endpoints. In the event of network failure for *Control Center 1*, all sites will transfer and start using *Control Center 2*.

A second example network is shown in Figure 11.

Figure 11: A simple dispatch system

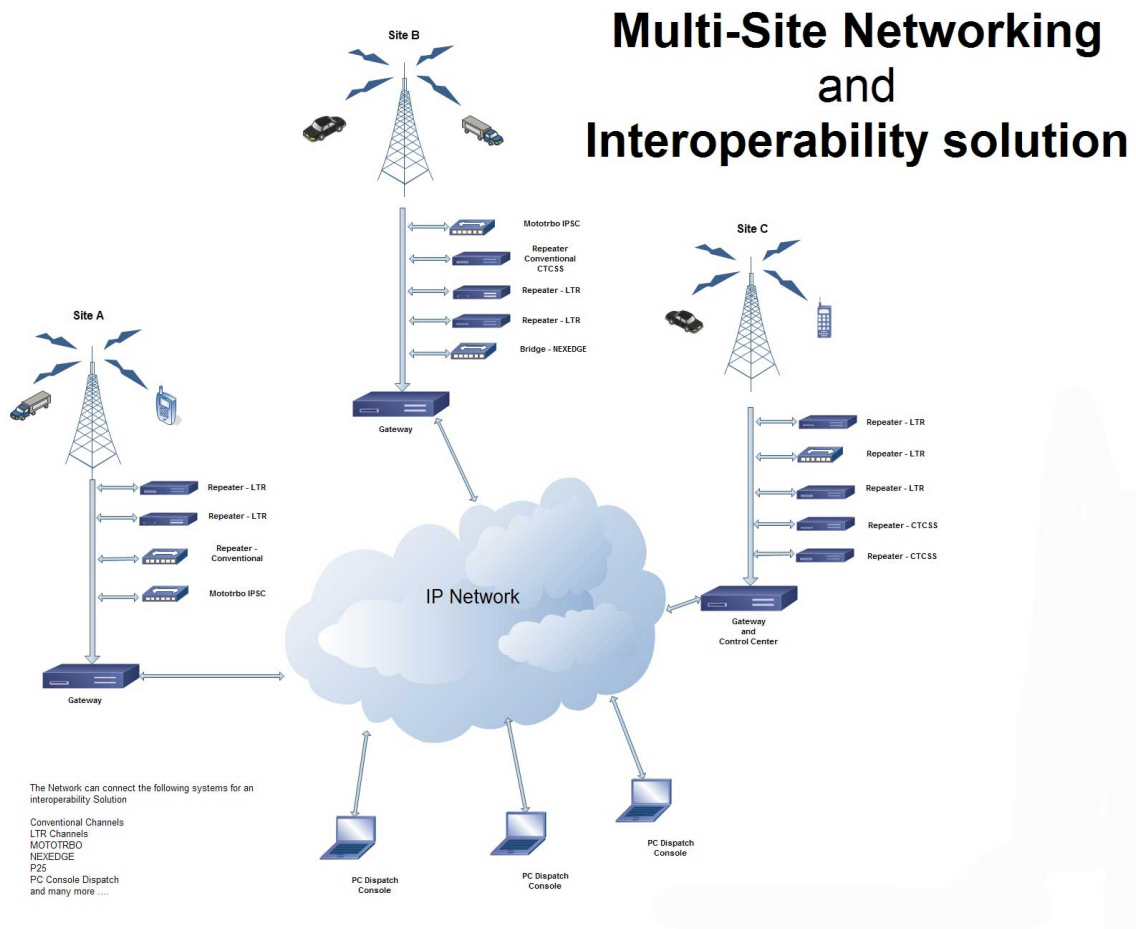


*A four site system with ethernet based communications between them. Both Control Centers are operating as Primary Control Centers. The PC client is operating as a dispatch center, so is initiating (and receiving) calls from any of the Control Centers. The Control Centers are receiving/sending calls to the Mototrbo repeaters.*

For Figure 11, there is no failover *Control Center* to be used in the event of network failure (as was the case in Figure 10). The PC clients are configured to send audio to/receive audio from any of the networks shown in this figure. It is not possible for a radio at *Site A* or *B* to send a call to a radio at *Site C* or *D*. The reason is simple - there is no link between the two *Control Centers*.

A third example network is shown in Figure 12.

Figure 12: Illustration of interoperability provided by the system



A network consisting of many different elements is drawn. There is one Control Center, which is shown as having Gateway functionality. Combining the Control Center and Gateway was described in Section 2.6.

Multiple disparate radio technologies are combined through the deployment of this product. All components are connected via the internet. The internet connection may be public internet, private LAN, or a secure VPN.

### 3.5 Initial setup of a Gateway with a Front Panel display

This section is written with the view that your Gateway is connected to a network that has DHCP in use. Most networks do run DHCP - you can be confident your network is running DHCP if you can put a PC onto your network and then (without configuration changes) browse the public internet.

If your Gateway does not have a front panel LCD display, (or the network does not support DHCP), you should proceed to Section 3.6.

1. Connect your Gateway to your IP network.
2. Connect the power supply to the Gateway and power it on.
3. The display on the Gateway should start scrolling from right to left after 2 minutes.
4. The IP address will be displayed in the scrolling text. If the IP address is not displayed in the scrolling text, a manual setup is required, as described in Section 3.6.



5. From a PC or other device on your network with a web browser enter the following URL in the browser address field.
6. `http://xxx.xxx.xxx.xxx:42420` (where `xxx.xxx.xxx.xxx` is the address displayed on the scrolling display).
7. Login using User = *admin* and Password = *tnet* (see Figure 14)
8. After logging in, the display will be similar to Figure 17.
9. Click *config* on the left side of the screen
10. Click the *system* button
11. Click the IP Address Settings tab. (see Figure 63)
12. The displayed image will be close to that shown in Figure 63. If this particular box is configured to be a *Gateway*, there will be two fields at the top to enter the IP address of the *Primary Control Center* and *Secondary Control Center*. If this box is a *Control Center Gateway* combo, or a *Control Center*, there is no place to enter the IP address of the *Control Center* (since the IP address of the *Control Center* is this box).
13. If the option is there, enter the IP address of the *Primary Control Center*. The address of the *Secondary Control Center* is optional.
14. Enter your desired network information. The meaning of the different fields is explained in Section 5.4.3.1. When done click the RED button at the bottom, which will reboot this box. It should be available again within two minutes.
15. When the computer has finished rebooting, configuration and analysis of events on this *Gateway* should be available from the webpage of the *Primary Control Center*.

### 3.6 Manual setup of network settings on a Gateway

1. Connect a keyboard, power cord and monitor to the ports on the rear of the system. Refer to the diagrams in Section 3.3 if you are unsure of the use of the different sockets. A mouse is not required. The ethernet cable should be plugged in. A serial cable is optional and is used for analog radio systems.
2. Power-up the system by using the power switch on the rear of the unit, and/or the on - off power switch on the front if necessary.
3. Wait 2 to 3 minutes for the system to completely boot.
4. The screen should clear to display the Linux login prompt. The prompt reports the version of CentOS used and the kernel version.
5. The user name is "*admin*" and the password is "*tnet*". The username and password do not require the quote symbol or period symbol - these were added to highlight the particular values. Check that the caps lock key is not on - the login is case sensitive.
6. You should now be at the system level prompt `[root@RavenNet root]#`
7. Type the command `rnnetwork` and press enter.
8. Type the command `rnnetwork` and press enter. You should see a report that **RnNetwork is running** and a prompt requesting your command.
9. Enter the command `h` (help) and the following will be displayed

10.

```
[root@ravennet root]# rnnetwork
RnNetwork is running

Command ? h
Press :
      D on/off      Set DHCP status to on/off
      G ipaddress   Set the IP address to use as a gateway
      I ipaddress   Set the IP address of this box
```

```
N ipaddress  Set the NetMask of this computer
S server     Set the Server to use for DNS requests
E TL-Net Srv Set the TL-Net ServEr for the radio calls
T ethX       Specify the the eThernet device to configure

R           Review current settings
L           ReLoad data from config. file - loose unsaved changes

W           Permanently Write data and apply changes

H or ?     help on this interface
X or Q     exit
```

```
Command ?
```

The following two sections describe the setting of static IP address or dynamic IP address.

### 3.6.1 Static IP setup

It is assumed that the program **rnetwork** is running. Inside this program, you will make the following changes to alter the computer to use static IP address. The particular values altered in this section are described in Section 5.4.3.1.

1. Enter the command **d off** to disable DHCP
2. Enter the IP address for this device using the command **i xxx.xxx.xxx.xxx** where **xxx.xxx.xxx.xxx** is the desired IP address.
3. The netmask is set with the command **n xxx.xxx.xxx.xxx**.
4. The gateway address, or next hop, or default route, is set with the command **g xxx.xxx.xxx.xxx**.
5. The DNS server is set with the command **s xxx.xxx.xxx.xxx**. If unsure of the value to use, try 4.2.2.2.
6. If this device is a *Gateway*, enter the command **e xxx.xxx.xxx.xxx** (or **e myserver.com**).
7. Enter **r** to review the settings.
8. Enter **w** to save the settings and cause an immediate restart of the computer.
9. When the computer has rebooted, it should be possible to access it via the web page of the *Control Center*. The reboot process takes 2 minutes.

### 3.6.2 Dynamic IP setup

It is assumed that the program **rnetwork** is running. Inside this program, you will make the following changes to alter the computer to use a dynamically determined IP address. The particular values altered in this section are described in Section 5.4.3.1.

1. Enter the command **d on** to enable DHCP
2. If this device is a *Gateway*, enter the command **e xxx.xxx.xxx.xxx** (or **e myserver.com**).
3. Enter **r** to review the settings.
4. Enter **w** to save the settings and cause an immediate restart of the computer.
5. When the computer has rebooted, it should be possible to access it via the web page of the *Control Center*. The reboot process takes 2 minutes.

### 3.7 Configuring the *Control Center*

Ideally, the *Control Center* has a static IP address. Consequently, the *Gateways* are guaranteed of being able to connect with the *Control Center*. Alternatively, the *Control Center* is located on the public internet or is in a DMZ. With either location, the *Control Center* can be easily accessed by remote *Gateways*, web browsers for configuration+status reports, or by PC clients. One may follow the steps of Section 3.6 and Section 3.6.1 to alter the static IP configuration on the *Control Center*

1. Prior to powering the *Control Center* up, ensure the ethernet cable is plugged in.
2. Power up the *Control Center* and wait 2 minutes. If the *Control Center* has a front panel display, the IP address will be reported.
3. Use a browser on another computer (mac, windows, linux browsers are all supported) to access the configuration and status web pages provided by the *Control Center*.
4. In the address field of the browser, enter **http://xxx.xxx.xxx.xxx:42420** where **xxx.xxx.xxx.xxx** is the IP address of the *Control Center*.
5. The login process is described in Section 5.1. Once logged in, there are no limitations as you have access at the *admin* level. Press the *Help* button to obtain additional information.

### 3.8 URI - USB device

Some systems use the URI-USB analog radio interface, which is pictured in Figure 13. These devices are detected at program startup. For correct operation, the URI - USB devices must be plugged in before the program starts.

Figure 13: URI - USB



*The URI-USB repeater (or Radio Interface), which connects the voice and control streams of the radio hardware with the Gateway.*

For interfacing with a repeater or control radio station, Table 2 reports the pins (on the DB25 connector) that are relevant.

Optional call setup: Group Ids can be generated by using the following COS pins (instead of using the default pin of 8), as reported in Table 3. Thus, if you put pin 2 high (+5v) a Group ID of 3 will be generated.

Table 2: Pins to be used in DB25 connector

Color	Function	URI-USB pin no	State
Black	GND	13	
Orange	COS in - Goes to COR out of Repeater (Group ID 1)	8	Active Low
White	Line-level Audio in (AC Coupled). Goes to Line Level Audio Out on Repeater	21	
Blue	Audio Out - Goes to Audio In or Mic In on Repeater	22	
Brown	PTT Out - Goes to PTT In on Repeater	1	Active Low
Shield	Shield - Gnd	13	

Table 3: Optional call setup pins

Group id	Pin no	Action
1	8	Active Low (Default)
2	7	Active Low
3	2	Active High (+5v)
4	3	Active High (+5v)

## 4 Usage options

### 4.1 Introduction

In this section (Section 4) we list several possible options for usage. Your situation may be quite different to those listed below. Alternatively, your situation may resemble a combination of those below.

### 4.2 I run a taxi company

The taxis drive over a region of 1000 square miles, and the range of the radios on the cars is too short. Install *Gateways* in the designated region so the radio attached to the gateways cover the entire region. Each *Gateway* is connected via cable modem to the public internet. The *Control Center* is in the main office.

With the PC dispatch software, you can make/receive calls with the designated recipients. A web browser on the PC is used to monitor call traffic on all channels in the *Control Center*.

You will create one *Super Group* that contains entries for all *Bridge Groups*. Timers are used in the *Super Group* so that in the early hours of the morning the *Super Group* goes active and everyone hears all activity.

After installing this network, the accountant noted that there is a cheaper way of connecting the *Gateways* to the public internet. The ethernet cable into the *Gateway* was changed, the *Gateway* was rebooted, and service continued as before.

### 4.3 My taxi fleets are in two cities

Every now and then, I want to send audio to everyone in both cities. I have two *Control Centers* (one in each city) and *Gateways*. Is there a way I can join them? Yes - you will use a *Control Center Inbound+Control Center Outbound* link to join the two *Control Centers*. When dictated by the *Bridge Groups* (and possibly a *Super Group*) audio will pass over the *Control Center Inbound+Control Center Outbound* link and flow to everyone at the same time.

#### 4.4 Don't need extra *Gateway*

The layout of my network is that there is a *Gateway* box right beside the *Control Center* box. It seems a waste to have two very minimally used boxes - can I combine them?

Yes. It is possible to use a *Control Center Gateway* combo type system, where the two components run inside one box. The result is a little weird at first, but does make sense. Both components have the same *sitename*. Consequently, on a combo box, the *sitename* of the *Control Center* is reported at the bottom left of the web page in the list of connected *Gateways*. Configuration of *Gateway* like functions on the combo box are on the web page in exactly the same place as they would be for remote *Gateways*.

The *Control Center* provides an *I.P.S.C.* call validation service. One could combine an *I.P.S.C.* enabled *Gateway* into a *Control Center*, which connects with a Motorola network. In response to an unacceptable call, the transmitter on the Motorola repeater is temporarily shutdown. This prevents rogue calls from taking too much spectrum space.

#### 4.5 *Analog* and *I.P.S.C.* networks

I have both sorts of radios in the networks that I manage. Can I join them?

Yes. Create *Analog* connections and *I.P.S.C.* connections in your *Bridge Groups*. Your default codec will need to be AMBE (or Speex 24.6k). You will need some USB dongles that do the work of converting AMBE encoded voice to raw audio placed somewhere on the network.

Suppose that in the Connections table there are 6 connections with *I.P.S.C.* devices and 3 connections with *Analog Gateways*. Consequently, the Connections table will have 9 lines in it. Three USB dongles are required, which will be mounted on the *Gateways* which connect to *Analog* devices. The default codec will be AMBE.

#### 4.6 Network connection to *Control Center*

The network connection to my *Control Center* is faulty and sometimes gets disconnected. Is there an alternative *Control Center* that can be used?

It is not ideal practice to use a *Control Center* that has a faulty network connection. However, there are times that this happens, such as when the main office is being renovated. In this case, it is suggested that you use a *Secondary Control Center* which is situated off site. Each *Gateway* maintains two connections - one with the *Primary Control Center* and one with the *Secondary Control Center*. In the event of the *Primary Control Center* being disconnected the *Gateway* will automatically switch its calls to the *Secondary Control Center*. Tests during development showed that when removing the ethernet cable from the *Primary Control Center* the *Gateways* started using the *Secondary Control Center* within 30 seconds.

Another situation that might be useful is when the power to *Control Center* is sometimes interrupted. In this case, the *Gateways* will accurately and reliably switch to the *Secondary Control Center*.

Should the network connection to the *Control Center* be flakey, and occasionally lose packets, the situation is simpler. Improve the network connection to the *Control Center*, and do not bother using a *Secondary Control Center*. With a sometimes faulty connection to the *Control Center* the time before transition of the *Gateways* to the *Secondary Control Center* is indeterminate. Further, the partly lossy link will lower the audio quality. In some cases, it will slow down the time for the call to start, which will cause the beginning of the call to be dropped.

The developers and testers in this project have spent many fruitless hours examining bug reports, answering questions, verifying software operation, devising scenarios and tests to replicate reports from the field. And then to discover that the network link is lossy or there is a faulty cable modem. The ideal is to have the *Control Center* in the DMZ with a good internet connection to the *Gateways*. There are diagnostic tools in the program which measure and report the loss of packets on the network over time.

## 5 Web page interface

The web page interface mentioned in Section 2.2 is the method used to access the control and status features of this program. As stated in Section 2.2, all web pages have been designed, tested, and shown to work on all major browsers. In this section an overview of the login process, the screen layout, and the design layout philosophy is explained. From this, it is envisaged that you will gain sufficient insight to be able to do required tasks.

The screenshots in this and later sections have been obtained from three different networks. The first has three *Gateways* and three *Control Centers*, all running on a private network. The names of the *Gateways* has been chosen to match those in the Figure 2. Specifically, the boxes used are:

Table 4: Devices used for screenshots

<i>sitename</i>	<b>IP address</b>	<b>Description</b>
Primary Main	10.0.0.62	<i>Primary Control Center</i>
Main (backup)	10.0.0.61	<i>Secondary Control Center (for 10.0.0.62)</i>
<i>Alternate</i>	10.0.0.3	<i>Primary Control Center</i>
<i>Gateway b</i>	10.0.0.7	<i>Gateway</i>
<i>Gateway a</i>	10.0.0.63	<i>Gateway</i>
<i>Gateway alpha</i>	10.0.0.60	<i>Gateway</i>

Note that the *Primary Control Center* at IP address *10.0.0.3* has no backup. The use of a *Secondary Control Center* is to cover network or power outages at the site of the *Primary Control Center*.

The second network has one *Control Center* which is also running as a *Gateway*, and an additional *Gateway*. The devices used are as follows:

Table 5: Devices used for screenshots

<i>sitename</i>	<b>IP address</b>	<b>Description</b>
<i>RnSrv</i>	127.0.0.1	<i>Primary Control Center and Gateway</i>
<i>RnCentos</i>	74.76.113.143	<i>Gateway</i>

Finally, in some instances screenshots are taken from customer's networks, which are larger than the above test networks. These are used to better represent what a user might actually experience.

This program is regularly updated as new features are requested and old are improved. There may therefore be some discrepancies between this documentation and the version you are using.

## 5.1 Login

On setting the browser to *http://10.0.0.62:42420* (IP address of the *Primary Control Center*) we get the following screen:

Figure 14: Initial login window

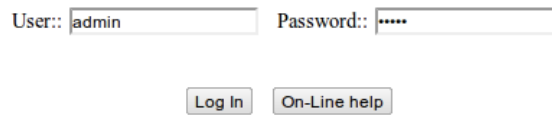
### Access to this service is blocked

You may login, using

*The first window presented on accessing the web page generated by the Primary Control Center.*

After clicking the *Login* button, the user is presented with window shown in Figure 15, which asks for the username and password.

Figure 15: Username password request window



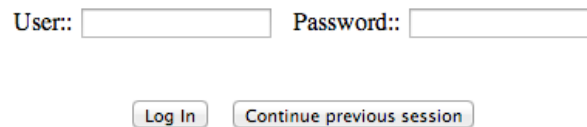
User::  Password::

*The Username/Password window which is used for entering the login details. Not shown is the product logo, which is placed in the middle of this web page.*

The username and password are entered into this window. The entered values are securely transferred over the internet to the web page server on the *Primary Control Center*.

Should there have been an earlier login session that was not logged out, a button is displayed which says *Continue previous session*, as shown in Figure 16. In this case, click the *Continue previous session* button to proceed. This button significantly reduces the number of times you have to enter your details.

Figure 16: Returning to a previous session



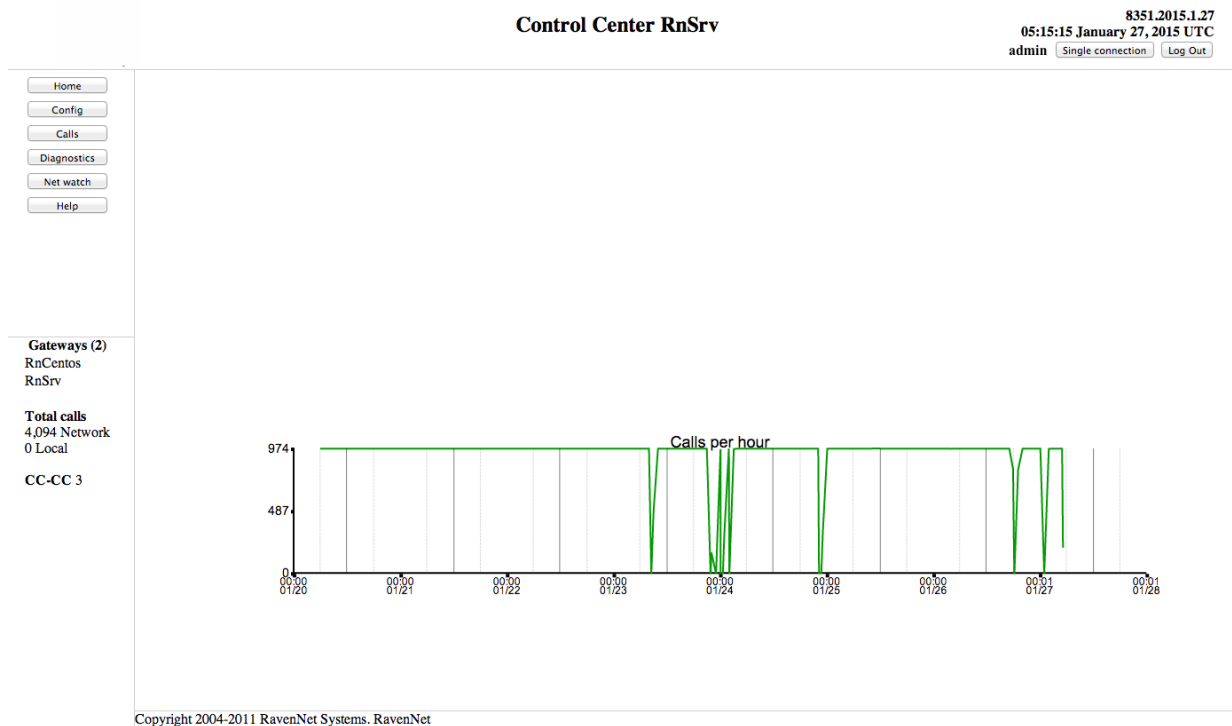
User::  Password::

*Window displayed when returning to the website when the previous session was not logged out. Clicking Continue previous session will allow the user to proceed without re-entering details.*

## 5.2 Main page

After logging in (or pressing *Continue previous session*) the displayed web page is similar to that shown in Figure 17.

Figure 17: Home window



The home page, or home window. This is the main window (or web page) of the program. The display always goes to here after successfully logging in, or when the Home button (top left corner) is pressed.

This screenshot does not contain the company logo, which is at the top left on every web page. Also not shown is the product logo, which is placed in the middle of this web page.

The graph of Calls per hour in the bottom right is very atypical. This screenshot is taken from a machine running uniform test calls at a constant rate. The only time the hourly rate is reduced is when the program is stopped entirely. Most users will see a graph that is more like Figure 5.

Depending on the access level of the logged in user, there will be fewer buttons in the panel at the top left. A person who has just user level rights will not see the config button at the top left.

Once logged in, this window can always be accessed by clicking on the *Home* button at the top left corner. From this page, you can access any feature or service in the program.

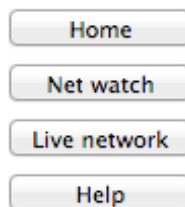
There are several features and components on this Home page that are explained here, which should improve the ease of use.

- In the top left corner the company logo (of the product supplier) is normally displayed. This is blanked out in Figure 17.
- In the middle of the bar at the very top of the page the *Control Center* sitename is displayed. In Figure 17 the sitename of the *Control Center* is *RnSrv*.
- The very top right corner contains three pieces of information. First is the program version number and build date. This will be used in bug reports. Below this is the time/date values used by the *Control Center* and all attached *Gateways*. The time is always displayed in 24-hour time. The date/time value is used in the various graphs and logs of calls and be configured as described in Section 5.4.3.2. Below the date and time is the web page login status. This shows the username of the user currently logged in. Next to this is a button which displays the number of additional users who are also currently logged in. If no other users are logged in (as is the case in Figure 17) it will read *Single connection*. This button is a diagnostic level button which takes the user to the report on logged in web page users. This is described in Section 5.6.1. Next to this is the *Log Out* button, which will terminate the current web browser session immediately. If you do *Log out* by clicking the button, the *Continue previous session* button shown in Figure 16 will not be displayed. Thus, to access this web page after logging out, you will have to enter your details again.



- On the far left below the company logo are seven buttons in a column. This navigation menu is designed to take you quickly to the different areas of the program. This may look slightly different to different users. The *CC↔CC* button is only displayed when this configuration option is selected, as explained in Section 5.4.4.1. Access to some areas is denied to those who have logged in with insufficient access rights, so they will not see some buttons, as shown in Figure 18. Figure 17 shows a user with *Admin* privileges.

Figure 18: Navigation menu as seen by *Low User*



The navigation menu as seen by a user with *Low User* privileges. Note that the *Config* and *Calls* pages are not available, and the only *Diagnostics* page available is *Live Network*. *CC↔CC* is not listed as this option is not configured.

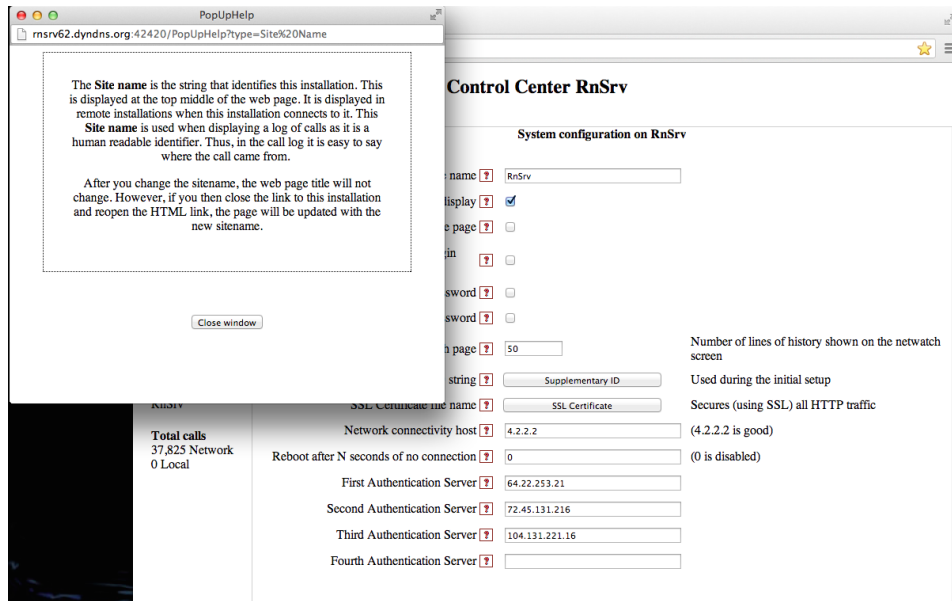
- Below the navigation menu in the bottom left is a live report of the operational status of the *Control Center*. It lists the connected *Gateways*, Figure 17 reports that two *Gateways* are connected: *RnCentos* and *RnSrv* (which is acting as a *Gateway* in addition to being a *Control Center*). The number of calls that have been processed and the number of *Control Center* to *Control Center* links are also reported.
- At the very bottom of the page the copyright message is displayed. This message cannot be altered.
- The large area in the bottom right displays a product logo image and a graph of the call count handled by the *Control Center*. The product logo has been blanked out for this documentation. The graph will report up to the last seven days of performance. If the *Control Center* has not been operating for seven days the graph duration will be shorter. Each element on the horizontal axis always reports a time and date. The date is given in month/day format. Consequently, the entry *00:00, 01/21* refers to the very beginning of January 21<sup>st</sup> which is in the early hours of the morning. More information about the interpretation of this graph is given in Section 2.8.

When other pages are selected/accessed, the large frame in the bottom right with the product logo image and graph will be completely changed. The other areas will change slightly (depending on the call count, connected *Gateways*, product version, and date). For the remainder of this documentation, only this main frame will be pictured, as this is the only part of the page to change.

### 5.3 Pop-up help

On many of the pages in this program a pop-up help system is provided to help users with key terms and phrases. A red question mark in a box (🔍) is displayed next to terms that need definition. When clicked, a new window will open with an explanation of the term. This is shown in Figure 19.

Figure 19: Pop up help

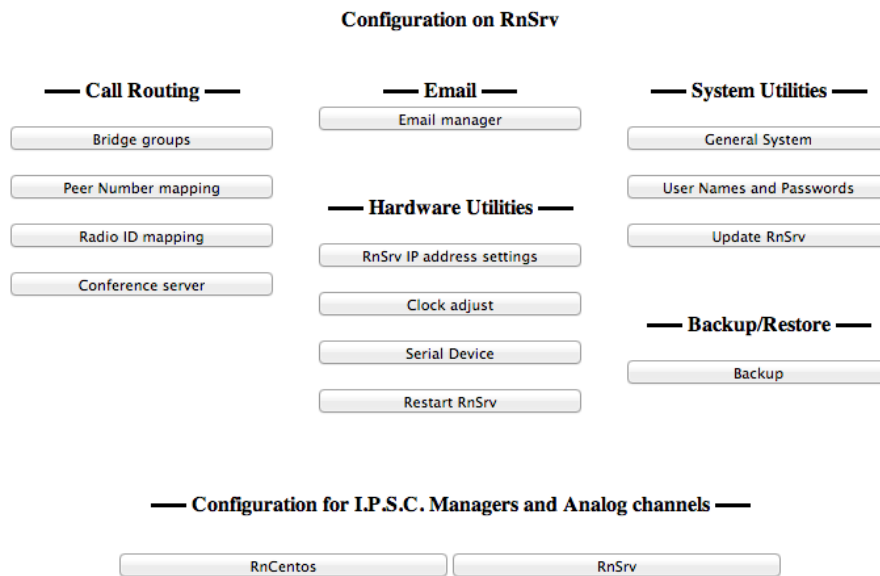


An example of the pop up help, explaining the term sitename from the General system configuration page. When there are several paragraphs of help text, a vertical scroll bar is supplied. At the very bottom of the help text is a close window button.

## 5.4 Config

Selecting *Config* from the left-hand navigation menu in Figure 17 opens the options shown in Figure 20. This option is only accessed by users with *admin* privileges. The *Config* options are divided into five categories. Each are described in the following sections.

Figure 20: Main Configuration window



Configuration on this box (the Primary Control Center) and on attached Gateways is through this web page. The configuration of remote Gateways is via the button(s) at the bottom of the screen. These buttons display the name of the remote Gateway. In this case RnSrv is acting as both Control Center and Gateway. RnCentos is also a Gateway. Consequently, to access the Gateway specific functions of RnSrv you will go through the RnSrv button.

#### 5.4.1 Call Routing

In this section, the adjustment of the content of the mapping of calls from one remote device to another is described. This section of the program is the most important to understand and is expected to be where you spend much of your administrative effort.

##### 5.4.1.1 Bridge Group configuration

Key to understanding how calls are mapped is the term *Bridge Group*, which was briefly described in Section 2.1. The remote entities which connect to a *Control Center* have a particular type and function, which are described in Section 5.4.1.1.2. *Bridge Groups* may be combined together to form a *Super Bridge Group*, or just *Super Group*. One may look on a *Super Group* as creating a virtual *Bridge Group* which consists of many sub *Bridge Groups*. The creation of the *Super Group* can be triggered manually (through the web page), using *RnIPc*, with a timer, or by making a call to a different *Bridge Group*.

There are several different audio connection operations one may undertake, which are described in Figure 21

Figure 21: Selection of the different ways of joining calls together

**Modify bridge groups on RnSrv**

**Joining**

Group Calling

Group Calling - all groups.

Super Groups

Private Voice, Private+Group Data

**Blocking**

Block Radio Ids

Blocked Radio IDs are always blocked

There are three different options for the manner of audio connection types one may do. These have been grouped into this screen for you to select from. It is inside these sections that the pathways are created to determine where the audio is connected to and from.

**5.4.1.1.1 Editing and altering Bridge Groups**

Bridge groups are edited by choosing Group calling in Figure 21. An example screen shot of the editing window is provided in Figure 22

Figure 22: Editing of Bridge Groups window

**Manage Bridge Groups on Primary Main**

Connection type  
all

Bridge Groups  
all

Site name  
all

Link ID  
all

Group ID  
all

Bridge Group	Site Name	Home Repeater Number	Alert on Absent	Group ID	Network access	Regn. mode	Regn. status	Conventional channel	Announcement track
allcomponents	gateway a	1	<input type="checkbox"/>	1	✓	forever	Reg. forever	<input type="checkbox"/>	

Analog Add Entry Delete Entry Modify Entry

edit	Analog	allcomponents	gateway a	1	silence	1	network access	forever	Reg.	trunked
edit	Analog	allcomponents	gateway b	1	silence	249	network access	forever	Reg.	trunked
edit	Control Center Inbound	allcomponents	Alternate	17	silence					

The editing of the Bridge Groups for Analog, I.P.S.C. group, Control Center↔Control Center, and PC calls. The key feature to note is that the select boxes at the top help you to find the desired Bridge Group. From that point, you can select an existing entry from the bottom table and edit it appropriately using the central table. New entries can also be added using the central table.

Editing of the audio connections is all done on this page. This is perhaps best explained with the following list:

- All of the talk maps, or *Bridge Groups* are available on this page. By selecting different options in the select boxes at the very top, fewer of the *Bridge Groups* are available. For instance, if the *Connection type* is set to *RnPc*, and none of the talk maps contain entries of the type *RnPc*, then nothing will be displayed.
- The contents of the select boxes change when the page is refreshed. Thus, changing the connection type (which is the type of device connected to this *Control Center*) will mean that only *Bridge Groups* with the same connection type can be selected from the other drop down boxes.

- An example *Bridge Group* is displayed at the bottom of Figure 22. Screenshots taken from the operation of this program to illustrate connectivity and status use this *Bridge Group*. By consistently using this *Bridge Group* throughout these documents it should be easier to follow what is happening.
- Only one line can be changed at a time - this is in the current entry which is displayed in the center of the page. Immediately below the current entry (or active line) are the option buttons *Add Entry*, *Delete Entry*, and *Modify Entry*. Pressing any of the three option buttons will immediately make the desired change to the current entry. There is no "Are you sure" button. Remember that if you make a mistake, you can then edit the mistake out. The system will cope with a mistake (just that calls will be routed incorrectly or not at all) while a mistake exists.
- The system refuses to create entries with the same matching credentials. Thus, there will never be two (or more) entries from a *Gateway* with the same *sitename*, *home repeater*, and *userID*. If it was possible to create entries with matching credentials, there would be confusion as it implies that two copies of each incoming voice frame are sent to one radio.
- Should you have edits displayed (but not committed) which you wish to erase, then you can edit a different line or go to a new page. Change only happens when you press any of the three option buttons (*Add Entry*, *Delete Entry*, or *Modify Entry*).
- To the left of the *Add Entry*, *Delete Entry*, or *Modify Entry* buttons, there is a word which describes the type of connection being edited. This is meant to be an aid to the user, to make it clear what the connection type is. Note that this word is usually the same as the word in the *Connection Type* drop down select box at the very top of the screen.
- Calls are routed into the *Bridge Group* when there is a line in one *Bridge Group* that matches on *Connection Type*, *sitename*, *home repeater*, and *userID*. Once the *Bridge Group* with a line that matches the incoming call is found, the other lines are marked as where the call will go. The outgoing destinations will match on radio available, *Connection Type*, *sitename*, *home repeater*, and *userID*.

#### 5.4.1.1.2 Individual connection types

The above description gives some insight to describing the overview of managing this feature. In the section, and following subsections, the specifics to setting up each of the available types of audio connections. The available connection types are listed in Table 6.

#### 5.4.1.1.3 Analog

A connection from a remote analog (or LTR) radio system to this *Control Center*. An example screenshot for editing an *Analog* connection type is given in Figure 23.

Figure 23: Analog connection with the Control Center

Connection type Analog		Bridge Groups all		Site name all		Home repeater all		Group ID all	
Bridge Group	Site Name	Home Repeater Number	Alert on Absent	Group ID	Network access	Regn. mode	Regn. status	Conventional channel	Announcement track
allcomponents	gateway b	1	<input type="checkbox"/>	249	<input checked="" type="checkbox"/>	forever	Reg. forever	<input type="checkbox"/>	
Analog    Add Entry    Delete Entry    Modify Entry									
edit	Analog	allcomponents	gateway a	1	silence	1	network access	forever	Reg. trunked
edit	Analog	allcomponents	gateway b	1	silence	249	network access	forever	Reg. trunked
edit	Control Center Inbound	allcomponents	Alternate	17	silence				

Configuring the different fields to describe one Analog connection with the Conference Server.

Note that to the left of the *Add Entry*, *Delete Entry*, or *Modify Entry* buttons the word describing the type of connection being edited is always reported. An *Analog* audio connection requires several fields to be set, which are described with the aid of the above figure. The meaning of the individual fields is as follows:

Table 6: Sample *Bridge Group*

Connection Type	Direction	Calls handled have
<i>Analog</i>	into <i>Conference Server</i>	Originated on a radio and passed through a <i>Gateway</i>
<i>Hoot-n-Holler</i>	into <i>Conference Server</i>	Originated from <i>Hoot-n-Holler</i> device
<i>I.P.S.C.</i>	into <i>Conference Server</i>	Originated on a radio and passed through a Motorola repeater and then a <i>Gateway</i>
<i>RnPc</i>	into <i>Conference Server</i>	Originated on a PC
<i>RnIPc</i>	into <i>Conference Server</i>	Originated on a PC. Remote PC can add/remove elements of a <i>Super Group</i>
<i>Control Center Inbound</i>	into <i>Conference Server</i>	Originated on a remote <i>Control Center</i> . This is half of a <i>Control Center</i> ↔ <i>Control Center</i> link.
<i>Control Center Outbound</i>	built by <i>Conference Server</i>	Originated on this <i>Control Center</i> . This is half of a <i>Control Center</i> ↔ <i>Control Center</i> link.
<i>Network Sound</i>	into <i>Conference Server</i>	Originates on a remote software entity. Allows user code on a PC to receive/send raw audio to the radio network.
<i>SIP</i>	into <i>Conference Server</i>	Enable a <i>Gateway</i> to send/receive voice over IP protocol packets. Thus, the radio network interconnects with SIP clients.

- *Bridge Group* specifies the entity described in Section 2.1. The contents of the current *Bridge Group* is listed at the bottom of the screen. For the diagram in Figure 23, the particular *Bridge Group* being edited is labelled by the word *allcomponents*.
- *Sitename* is a term that specifies the physical location of the *Gateway*. The *sitename* was set on the *Gateway* as described in Section 5.4.6.8.
- *Home Repeater Number* is the unique value that identifies one channel from other channels for a *Gateway*. The *home repeater* is a value in the range of 1..20.
- *Alert on Absent* When checked, sends a warning tone to the originator of a call to this *Bridge Group* if this particular destination is not available when a call is setup.
- *Group ID* is a number in the range 1..250 which identifies the radio being used for the call.
- *Network access* When blank, this particular destination cannot send audio to other members of this *Bridge Group* Note that this particular destination can always receive audio from other members of this *Bridge Group*
- *Regn. mode* provides a means of disabling entries in a *Bridge Group*. When set to *forever*, this entry is never disabled.
- *Conventional channel* enables or disables a feature LTR radio known as *Trunking*, where the *Conference Server* may use a different channel as a valid destination.
- *Announcement track* is an audio sequence previously stored in the *Conference Server*. More details on the track in Section 5.6.2.7.1. This track is played to the recipients of the call before the audio from the originator.
- *Dir. Change* (direction change) will allow calls on this *Bridge Group* to be interrupted by a new speaker.

5.4.1.1.4 I.P.S.C.

A connection from a remote I.P.S.C. (Motorola digital) radio system to this Control Center. An example screenshot for editing an I.P.S.C. connection type is given in Figure 24.

Figure 24: Configure I.P.S.C. connection to a Control Center

Connection type Rnlpc		Bridge Groups all	Site name all	Link ID all	Group ID all
--------------------------	--	----------------------	------------------	----------------	-----------------

Bridge Group	Site Name	Link ID	Alert on Absent	Enable transmit	Mute group
final	wxpc	2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	office

Rnlpc Add Entry Delete Entry Modify Entry

edit	RnPC	final	wxpc	2	silence	yes
edit	Control Center Outbound	final	1	silence	10.0.0.60	out going link
edit	Rnlpc	final	wxpc	2	silence	yes office
edit	I.P.S.C.	final	Monster	10	silence	1

Configuring the different fields to describe one I.P.S.C. connection with the Conference Server.

An I.P.S.C. audio connection requires several fields to be set. These fields were all described previously in Section 5.4.1.1.3.

5.4.1.1.5 RnPc

A RnPc connection is a connection from a remote PC to this Control Center. The PC does not have an ability to remotely enable/disable entries in a super group. An example screenshot for editing a RnPc connection link is given in Figure 25.

Figure 25: Configure a RnPc connection with the Control Center

Connection type RnPc		Bridge Groups all	Site name all	Link ID all	Group ID all
-------------------------	--	----------------------	------------------	----------------	-----------------

Bridge Group	Site Name	Link ID	Alert on Absent	Enable transmit	Mute group
final	wxpc	2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

RnPc Add Entry Delete Entry Modify Entry

edit	RnPC	final	wxpc	2	silence	yes
edit	Control Center Outbound	final	1	silence	10.0.0.60	out going link
edit	Rnlpc	final	wxpc	2	silence	yes office
edit	I.P.S.C.	final	Monster	10	silence	1

Configuring the different fields to describe one RnPc connection with the Control Center.

A RnPc audio connection requires several fields to be set. These fields were all described previously in Section 5.4.1.1.3.

**5.4.1.1.6 RnIPc**

A connection from a remote PC to this *Control Center*. The remote PC client can modify the status of one component in a *Super Group*. An example screenshot for editing a *RnIPc* connection type is given in Figure 26.

Figure 26: Different fields available for a *RnIPc* connection with a *Control Center*

Connection type RnIpc		Bridge Groups all	Site name all	Link ID all	Group ID all
--------------------------	--	----------------------	------------------	----------------	-----------------

Bridge Group	Site Name	Link ID	Alert on Absent	Enable transmit	Mute group
final	wxpc	2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	office

RnIpc   Add Entry   Delete Entry   Modify Entry

edit	RnIpc	final	wxpc	2	silence	yes
------	-------	-------	------	---	---------	-----

edit	Control Center Outbound	final	1	silence	10.0.0.60	out going link
------	-------------------------	-------	---	---------	-----------	----------------

edit	RnIpc	final	wxpc	2	silence	yes	office
------	-------	-------	------	---	---------	-----	--------

edit	I.P.S.C.	final	Monster	10	silence	1
------	----------	-------	---------	----	---------	---

Configuring the different fields to describe one RnIPc connection with the Control Center.

A *RnIPc* audio connection requires several fields to be set. These fields were all described previously in Section 5.4.1.1.3.

**5.4.1.1.7 Control Center Inbound**

This connection type describes a connection from a remote *Control Center* to this *Control Center*. With this connection type, there is a pathway for audio to flow from the *Bridge Group* on one *Control Center* to the *Bridge Group* on a different *Control Center*. An example screenshot for editing a *Control Center Inbound* connection type is given in Figure 27.



Figure 27: The different fields for a *Control Center Inbound* to the *Control Center*

Connection type Control Center Inbound ▼	Bridge Groups all ▼	Site name all ▼	Link ID all ▼	Group ID all ▼
---	------------------------	--------------------	------------------	-------------------

Bridge Group	Site Name	Link ID	Alert on Absent
allcomponents	Alternate	17	<input type="checkbox"/>

Control Center Inbound	Add Entry	Delete Entry	Modify Entry
------------------------	-----------	--------------	--------------

edit	Analog	allcomponents	gateway a	1	silence	1	network access	forever	Reg.	trunked
edit	Analog	allcomponents	gateway b	1	silence	249	network access	forever	Reg.	trunked

edit	Control Center Inbound	allcomponents	Alternate	17	silence
------	------------------------	---------------	-----------	----	---------

Configuring the different fields to describe one *Control Center Inbound* connection with the Conference Server. Note that a *Control Center Inbound* connection is like an Analog or I.P.S.C. connection - it waits for the incoming request.

A *Control Center Inbound* audio connection requires several fields to be set. All of these fields were all described previously in Section 5.4.1.1.3.

#### 5.4.1.1.8 Control Center Outbound

This connection type describes a connection created on this *Control Center* to a remote *Control Center*. With this connection type, there is a pathway for audio to flow from the *Bridge Group* on one *Control Center* to the *Bridge Group* on a different *Control Center*. The *Control Center Outbound* connection type is actively built by the *Control Center*. Other connection types wait for the incoming connection from the remote entity. An example screenshot for editing a *Control Center Inbound* connection type is given in Figure 27.

Figure 28: Different fields for a *Control Center Outbound* connection - which is created to another *Control Center*

Connection type Control Center Outbound ▼	Bridge Groups all ▼	Site name all ▼	Link ID all ▼	Group ID all ▼
--	------------------------	--------------------	------------------	-------------------

Bridge Group	Link ID	Alert on Absent	Primary Control Center	Secondary Control Center	Descriptive label
final	1	<input type="checkbox"/>	10.0.0.60		out going link

Control Center Outbound	Add Entry	Delete Entry	Modify Entry
-------------------------	-----------	--------------	--------------

edit	RnPc	final	wxpc	2	silence	yes
------	------	-------	------	---	---------	-----

edit	Control Center Outbound	final	1	silence	10.0.0.60	out going link
------	-------------------------	-------	---	---------	-----------	----------------

edit	RnPc	final	wxpc	2	silence	yes	office
------	------	-------	------	---	---------	-----	--------

edit	I.P.S.C.	final	Monster	10	silence	1
------	----------	-------	---------	----	---------	---

Configuring the different fields to describe one *Control Center Outbound* connection. The *Control Center Outbound* is outbound, so the user is required to specify the internet location of the destination.

A *Control Center Outbound* audio connection requires several fields to be set. Most of these fields were all described previously in Section 5.4.1.1.3. Two fields not previously described are:

- *Primary Control Center* is the first choice *Control Center* for where this connection should go.
- *Secondary Control Center* is where this connection should be made to, if the first choice is not available

Note the similarities in the setting of these two fields and the values entered in Section 5.4.6.1. The *Gateway* does some buffering of the audio to remove irregularities in the audio packet arrival time. The *Conference Server* does no buffering - audio packets are forwarded immediately by the *Conference Server*. The *Conference Server* does no volume adjustment - it just forwards audio packets. The *Conference Server* does no codec format changes so will not do any analog ↔ digital conversions. This preserves voice quality. The *Gateway* creates a connection to a remote *Control Center* - in exactly the same way as a *Control Center Outbound* creates a connection to a remote *Control Center*.

#### 5.4.1.1.9 Network Sound

This causes the *c-Bridge* to create raw audio packets can be sent to external programs. Python code is available to communicate with *Network Sound* on *c-Bridge*. An AMBE 3000 USB codec is necessary to run this functionality.

Figure 29: Different fields for a *Network Sound* connection

**Manage Bridge Groups on RnSrv**

Connection type Network Sound ▾	Bridge Groups all ▾	Site name all ▾	Link ID all ▾	Group ID all ▾
------------------------------------	------------------------	--------------------	------------------	-------------------

Bridge Group ?	Site Name ?	Link ID ?	Alert on ? Absent
		1	<input type="checkbox"/>

Network Sound
Add Entry
Delete Entry
Modify Entry

*Configuring the different fields for the Network Sound configuration option.*

The meaning of the fields are described in Section 5.4.1.1.3.

*Network Sound* was originally envisaged as tool for monitoring. With the example Python code, it was hoped that users could write a software entity that runs on a standard PC to receive audio packets from the *Gateway* (or *Control Center*). The user's software would write the individual sound packets to disk (or possibly to speaker) and provide a means to listen to the conversations.

For *Network Sound* to work, the user is required to have the requisite codec functionality on the *Gateway*. Thus, if the network uses *I.P.S.C.* connections and connects to Motorola repeaters, the user will be required to have an AMBE 3000 USB dongle plugged into the *Gateway*. However, for LTR (or analog) use, the preferred codec is Speex, which can be handled in the software of the *Gateway*.

#### 5.4.1.1.10 SIP

Radio calls can be connected to the standard telephone network through SIP. Alternatively, SIP programs can be run on a PC. For this feature to be enabled (when connecting with Motorola repeaters), an AMBE 3000 USB codec is required to convert radio codec into G711. However, for LTR (or analog) use, the preferred codec is Speex, which can be handled in the software of the *Gateway*.

Figure 30: Different fields for a SIP connection

**Manage Bridge Groups on RnSrv**

Connection type SIP	Bridge Groups all	Site name all	Link ID all	Group ID all
------------------------	----------------------	------------------	----------------	-----------------

Bridge Group	Site Name	Link ID	Alert on Absent
<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="checkbox"/>

Configuring the different fields for the SIP configuration option. There are less fields than in Figure 23. Only the Bridge Group, sitename, Link ID and Alert on absent fields are present. These operate in the same manner.

The meaning of the fields are described in Section 5.4.1.1.3.

This feature is nearing completion, and has been included in this manual to give the user an indication of future directions. When the right hardware is in place, it is expected to enable a cellphone to make/receive calls from the radio network. Should this feature be of particular interest, please contact technical support to express your view.

#### 5.4.1.1.11 Altering the contents of Super Groups

A *Super Group* allows one to create virtual *Bridge Groups*, where two (or more) *Bridge Groups* are joined to form a much larger entity. One can think of *Bridge Groups* as a means of combining multiple radios together, so that the audio from the source radio reaches all other radios. With *Super Groups* multiple *Bridge Groups* are combined together. Thus, the audio from the source radio can be sent to many more radios - as recipients in all the joined *Bridge Groups* will hear the generated audio. The resulting combination allows one to dynamically join *Bridge Groups* in response to real world events. The possible trigger events from a remote PC, the web page, timer, or activity on a *Bridge Group* have been designed to provide the user with the maximum flexibility.

An alternative way of describing *Super Groups* is to refer back to the description of a *Bridge Group*, which was first described in Section 2.1. Essentially, a *Bridge Group* is a static list of who can talk to who. These easily and clearly describe what connections are made but are totally static. Only the person with administration privileges and has access to a web browser can make changes. To overcome this, *Super Groups* are provided. A *Super Group* provides the user with the means to dynamically merge *Bridge Groups* together to form one larger entity. The *Bridge Groups* that are joined together may only be one element long, or contain hundreds of elements.

The dynamic nature of the *Super Group* is partially illustrated in Figure 31. The presence of elements in a *Super Group* can be controlled by on and off switches. Each of the lines in *Super Group* table represents two switches. An On switch, and a off switch. Referring back to Figure 31 we see that:

- From the bottom of the three lines in the table, the bridge group "here" will be marked as active when the program starts. It does not have a commence time of day, nor does it have a duration. This line is always active. Thus, anyone in the "here" *Bridge Group* will be able to talk to other members of the "here" *Bridge Group* and possibly to members of the "final" *Bridge Group*.
- At 3:45pm on Saturday (day 7), members of the "final" *Bridge Group* will be able talk to (or receive calls from) members of the "here" *Bridge Group*. The joining privileges of "here" and "final" (as specified by this first line) will be provided for 90 minutes.
- At 4:00pm on Saturday, (days 7) The joining of "here" and "final" *Bridge Groups* is suspended for five minutes. This second line of the table is at the same priority (0) as the first line. However, it is more recent, so it is taken as being of higher priority. At 4:06pm on Saturday, "here and "final" *Bridge Groups* will be joined again. This happens as it is the most recent on event for this *Super Group*.

The method for determining when and which *Bridge Groups* are merged together is entered in the configuration page shown in Figure 31. The drop down boxes at the top of the screen (Figure 31) lists the available *Super Groups* and *Bridge Groups*. The operator will assign a *Super Group* name to several *Bridge Groups*. When the entry in the table states it is active, every user in the *Super Group* will hear the same thing.

Figure 31: *Super Group* configuration

**Control Center Primary Main**

---

**Manage Super Groups on Primary Main**

Select Super Group 
Select Bridge + Super Group

Super Group <input type="text"/>	Bridge Group <input type="text"/>	Initial Value <input type="text"/>	Action	Force <input type="text"/>	Trigger <input type="text"/>	Commence <input type="text"/>	Use Timer <input type="text"/>	Duration <input type="text"/>	Priority <input type="text"/>	And Timer <input type="text"/>
<input type="text" value="one collective"/>	<input type="text" value="final"/>	<input type="checkbox"/>	On Off	<input type="checkbox"/> <input type="checkbox"/>	<input type="text"/> <input type="text"/>	<input type="text" value="7 16:00"/>	<input checked="" type="checkbox"/>	<input type="text" value="forever"/> <input type="text" value="00:05"/>	<input type="text" value="0"/> <input type="text" value="0"/>	<input type="checkbox"/> <input type="checkbox"/>

Available operations

**Super Group for "one collective"**

	Super Group	Bridge Group	Initial Value	Action	Trigger Bridge Group	Commence	Timer Status	Duration	Join Status	Priority	And Timer
<input type="button" value="edit"/>	one collective	final	off	On Off		7 15:45	time limited ignored	(01:30) (forever)	idle / void	0 0	or or
<input type="button" value="edit"/>	one collective	final	off	On Off		7 16:00	ignored time limited	(forever) (00:05)	idle / void	0 0	or or
<input type="button" value="edit"/>	one collective	here	On	On Off			ignored ignored	(forever) (forever)	idle / void	0 0	or or

The configuration of the *Super Group* connections. A *Super Group* is the result when multiple (two or more) *Bridge Groups* are merged together. When the merge happens, and which *Bridge Groups* are involved in the merge, is determined by the contents of this window. Users with no privileges can (if allowed by the configuration) cause the merging of *Bridge Groups* to form a *Super Group*.

There are four trigger events by which *Bridge Groups* can be merged together to form a *Super Group*:

1. PC Dispatch applications which have the console features enabled can remotely initiate a merge event.
2. When editing one line in the above table, the user can tick the box for *Force on* (or the box *Force off*) to invoke/stop a merge operation.
3. A timer can be used to turn on the merge process. The timer can be set for the days of the week, and time of the day.
4. Audio activity on one *Bridge Group* can be used to trigger the joining (or removal) of any *Bridge Group* from the *Super Group*. When a *Bridge Group* goes active, it is first used to turn on any relevant lines. And then the super collective of all radios/*Bridge Groups* is determined.

Note that these trigger events can be used to undo the merger and remove a *Bridge Group* from a *Super Group*. Further, these trigger events can be combined together. One possibility would be to have two timers configured for Mon..Friday. One timer runs from 8am-11am and the other timer from 1pm to 5pm. The most recent trigger event (eg, timeout, scheduled event, trigger *Bridge Group*) will always override the previous event. Note too that there is *priority* (precedence/rank) for determining if a line is more less important than others.

A more extensive *Super Group* is reported in Figure 32.

Figure 32: An extensive *Super Group*

**Super Group for "one collective"**

	Super Group	Bridge Group	Initial Value	Action	Trigger Bridge Group	Commence	Timer Status	Duration	Join Status	Priority	And Timer
<input type="button" value="edit"/>	one collective	final	off	On Off		7 15:45	time limited ignored	(01:30) (forever)	idle / void	0 0	or or
<input type="button" value="edit"/>	one collective	final	off	On Off		7 16:00	ignored time limited	(forever) (00:05)	idle / void	0 0	or or
<input type="button" value="edit"/>	one collective	here	off	On Off		1 00:00	ignored ignored	(forever) (forever)	idle / <b>suggest abstain</b>	0 10	or or
<input type="button" value="edit"/>	one collective	here	On	On Off			ignored ignored	(forever) (forever)	idle / <b>suggest join</b>	0 0	or or

An example of a Super Group that contains activity. Note that this is the same as Figure 31 except that a new line has been added. The new line has a larger priority value, so will get more control over the final status.

Figure 32 is an extended form of the *Super Group* shown in Figure 31. The new line in Figure 32 is a request to operate as an OFF line at midnight on the first day of the week. This OFF line has no time limit, so will run for the whole week. This OFF line has a priority of 10, so will supersede lines of lower priority. As a result, radios in the *Bridge Group* "here" will not be able to send audio to radios outside of "here".

**5.4.1.1.12 Group calling - all groups**

This page provides a list of all the groups, allowing the user to map all groupings in one place. The editor functions in a very similar manner to others in the program, such as Figure 23 and Figure 31. By seeing all lines of all *Bridge Groups*, the user can see how everything fits together. Selecting the *edit* button on one line takes the web page to editing one line in that particular *Bridge Group*

**5.4.1.1.13 Private Voice, Private and group data**

Again, this section of the site functions in a very similar way to pages such as Figure 23 and Figure 31.

Figure 33: Configuring private voice, private and group data

**Manage Private Voice Calls.      Manage Data calls (private+group).**

Connection type <input type="button" value="Private Voice, Private+Group Data"/>	Destination name <input type="button" value="all"/>	Site name <input type="button" value="all"/>	Link Id <input type="button" value="all"/>	Private Voice <input type="button" value="either"/>	Data <input type="button" value="either"/>
---	--	---	---	--	---

Destination Name <input <="" td="" type="button" value="?"/> <td style="width: 16.6%;">Site Name <input <="" td="" type="button" value="?"/> <td style="width: 16.6%;">Link ID <input <="" td="" type="button" value="?"/> <td style="width: 16.6%;">Private Voice <input <="" td="" type="button" value="?"/> <td style="width: 16.6%;">Data <input <="" td="" type="button" value="?"/> </td></td></td></td>	Site Name <input <="" td="" type="button" value="?"/> <td style="width: 16.6%;">Link ID <input <="" td="" type="button" value="?"/> <td style="width: 16.6%;">Private Voice <input <="" td="" type="button" value="?"/> <td style="width: 16.6%;">Data <input <="" td="" type="button" value="?"/> </td></td></td>	Link ID <input <="" td="" type="button" value="?"/> <td style="width: 16.6%;">Private Voice <input <="" td="" type="button" value="?"/> <td style="width: 16.6%;">Data <input <="" td="" type="button" value="?"/> </td></td>	Private Voice <input <="" td="" type="button" value="?"/> <td style="width: 16.6%;">Data <input <="" td="" type="button" value="?"/> </td>	Data <input <="" td="" type="button" value="?"/>
<input type="text"/>	<input type="text"/>	111	<input type="checkbox"/>	<input type="checkbox"/>

Editing of private voice, private and group data. When Private voice is turned on, the system will automatically turn on Data.

**5.4.1.1.14 Block Radio IDs**

This section allows the administrator to specify some *Radio IDs* to be blocked. The *c-Bridge* will ignore incoming data and voice calls from these *Radio IDs*. If a radio is aliased (see Section 5.4.1.3) this implies that that we do not want this ID blocked. Checking the *Blocked Radio IDs are always blocked* checkbox means that even if a *Radio ID* is aliased, it will always be blocked if it is on the blocked list.

The editing window is shown in Figure 34.

Figure 34: Block radio IDs

**Add/Modify list of blocked I.P.S.C. Radio IDs for All IPSC managers on RnSrv**

*Editing window for blocking Radio IDs. In this example, all Radio IDs in the range 1-199 will be blocked on all I.P.S.C managers. A specific I.P.S.C manager can also be selected from the drop down menu in the top table. This will refresh the page and show the Radio IDs blocked for the selected manager.*

The editor for the blocked list functions in the same manner as almost all other editors in this program. Note that *Radio IDs* can be entered as a single value (for example: *1*), or as a range of numbers (for example: *1 - 199*), as is the case in Figure 34.

The locking domain refers to how extensive the blocking is. Thus, one can set that a particular radio id is blocked for the specified *I.P.S.C.* manager, or all *I.P.S.C.* managers. The example in Figure 34 has radios *1 - 199* blocked for all *I.P.S.C.* managers on the system.

#### 5.4.1.2 Peer number mapping

This function enables the user to assign a meaningful name (a *User Alias*) to a *Peer Number*. This name will be used on the *Net watch* page (Figure 114). The editing of the *Peer Number* aliases is shown in Figure 35. It is very similar to *Radio ID Mapping* as described in Section 5.4.1.3.

Figure 35: Peer number mapping

**Manage Peer number to User Alias**

Select user alias [dropdown]	Select peer number 204301 [dropdown]	1070 records	Wipe List Confirm <input type="checkbox"/>	Choose File No file chosen Upload file
User Alias		Peer number		
[input]		204301		
Available operations	Add Entry	Delete Entry	Modify Entry	Create CSV File
				Go Back

edit		204301
edit	9M4RMM	502200
edit	AA9VI	311708
edit	AB4L	311219
edit	AE5DN	314000
edit	AE5DN	314003
edit	AE5DN	314007
edit	AG2K	310904
edit	AH6CP	311507
edit	AH6CP	311508
edit	AH6CP	311502

*Editing the Peer Number mapping.*

The top table is used to select values from the existing entries, which are displayed in the table at the bottom of the page. The list can be completely deleted using the *Wipe list* button. The *Confirm* checkbox must be ticked to do this, as a safety net to prevent accidental deleting. New entries can also be added by uploading a CSV file. This works in the same manner as for *Radio ID Mapping* described in Section 5.4.1.3.

The middle table is used to edit existing entries and add new entries. You should choose user aliases that are meaningful to you. Note that in the bottom right corner of this middle table is an empty text field. This can be used for searching through existing entries by entering a search string.

### 5.4.1.3 Radio ID mapping

Motorola radio networks use integer numbers that identify operators. This option provides a means of turning the numbers into a label that has meaning for those viewing the web pages. These names will be displayed on pages such as the *Net watch* page (Figure 114). An example screenshot is shown in Figure 36.

Figure 36: Radio ID Mapping

**Manage radio ID to User Alias**

User Alias	Radio Id
blue hill	1132342

Available operations	Add Entry	Delete Entry	Modify Entry	Create CSV File	Go Back
----------------------	-----------	--------------	--------------	-----------------	---------

edit	blue hill	1132342
edit	md 4223	245623
edit	zx2345	4443343

The mapping of the integer numbers used by Motorola systems to labels that have meaning for those viewing the web pages is managed by this window.

This editing window works in the same way as Figure 46, Figure 22, and Figure 31. Select the group at the very top, make the changes in the large bar at the middle, and then press *Add Entry*, *Delete Entry*, or *Modify Entry* to enact the desired change.

There is no limit to the number of mappings you may use. Depending on the quality of your network link, and the number of entries, the speed of this page can be impacted. The developers have spent much time to ensure this page works as fast as possible.

In the large bar in the middle of the screen the *Create CSV File* button will generate a CSV file of the list, which will be downloaded to the user's computer.

In the bar near the top of the screen (which contains the selection boxes), there is a report of how many entries there are in the current list. Also provided is an option to wipe the list.

In the bar near the top of the screen are two buttons to allow you to read in a text (.txt) file containing many hundreds of possible mappings. Use the *Choose File* and *Upload File* buttons. The text file should contain only lines of text, which could look like:

**Example 5.1** Source data for Figure 36

```
blue hill, 1132342
md 4223 , 245623
zx2345,4443343
```

The text file reported in Example 5.1 was used as the raw data to populate the screenshot in Figure 36. The two fields may be separated by commas (as is the case here) or by tab characters. Space characters are trimmed from the beginning and end of the supplied name. It is acceptable to have space characters in the middle of a name, as shown in Example 5.1.

Note that the act of reading in a text file will append to the current mappings. Should the text file contain a radio id already on the system, the text file will overwrite the value in the system

Should the text file contain two (or more) lines with the same id value, the last duplicate value in the text file will be used. Thus, the earlier duplicate values are ignored. You will note on Figure 36 there is a report of how many records are in the system. This value should be examined before and after reading in a text file. From the change, you get a clue as to how much appending/overwriting there has been.



In the bottom right corner of the middle table is an empty text field. This can be used for searching through existing entries by entering a search string. This is useful when there are many entries on this page.

#### 5.4.1.4 Conference Server

An important part of each *Control Center* is the *Conference Server*. The *Conference Server* transfers (and duplicates) audio packets from the person who is speaking to the selected destinations (as explained in Section 2). An example screenshot for configuring the *Conference Server* is shown in Figure 37.

Figure 37: Configuration of the *Conference Server*

**Conference server settings on Primary Main**

Send warning tone on faulty call setup

Maximum length of calls (seconds)  (180 is good)

Codec for audio on network

- AMBE
- G.711-ALaw-64k
- G.711-uLaw-64k
- GSM-06.10
- SpeexIETFNarrow-11k
- SpeexIETFNarrow-15k
- SpeexIETFNarrow-18.2k
- SpeexIETFNarrow-24.6k (preferred option)
- SpeexIETFNarrow-5.95k
- SpeexIETFNarrow-8k
- iLBC
- iLBC-13k3
- iLBC-15k2

Codec for Multicast audio

- G.711-ALaw-64k
- G.711-uLaw-64k

Available operations

Accept changes

Reset changes

*Adjustment of the Conference Server, which is a part of the Control Center.*

The different components on the *Conference Server* configuration are:

- *Send warning tone on faulty call setup* causes a warning message to be sent back to the radio if a call was created that went to none of the intended recipients. The originator of the call will hear this message when he/she releases the PTT button.
- *Maximum length of calls (seconds)* causes the *Conference Server* to terminate any call that lasts longer than this value. If you do not want termination (even for long calls), set this to a high value (such as 1 million).
- *Codec for audio on network* specifies the compression format of the audio that travels over the ethernet cables. For conveyance of audio from Motorola digital devices, this should be set to *AMBE*. Consequently, there is the minimum of format conversion and so the audio quality is kept to the highest possible level. When it is audio from analog radios, the recommended value is *Speex 24.6* as the audio quality is only slightly reduced.
- *Codec for multicasted audio* specifies the codec to use when interfacing with Hoot-n-Holler devices. If you don't know what these devices are, you can ignore this option.

After making the requisite changes, press the appropriate button at the bottom of the screen.

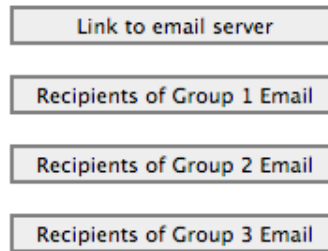
## 5.4.2 Email

This section allows specification of who receives emails to warn of a particular event, and the coordinates of the SMTP mail server. For instance, an email can be sent in the event of a *Gateway* disconnecting from a *Control Center*.

On selecting the *Email manager* button in Figure 20, a screen similar to Figure 38 is shown.

Figure 38: Email manager

### Email settings on RnSrv



*The window for selecting the parameters of connecting to an email server, or specifying who receives email for some event.*

One can either alter the settings that determine the mechanics of actually getting a message sent Section 5.4.2.1. Alternatively, one can adjust which events trigger the sending of emails and the recipients Section 5.4.2.2.

### 5.4.2.1 Link to email server

This program will create email messages and pass them on to the email server. The email server will handle every aspect of the email protocol, such as recipient not reachable and multiple tries. Configuration of the link to the email server is via a window such as shown in Figure 39, which is displayed on pressing the *Link to email Server* button in Figure 38.

Figure 39: Link to email server

**Email:: Link to server for RnSrv**

Email user name

Email password

Domain

SMTP address

From address

port to use for email  Normally 25

available authentication types  l (preferred option)  
 p

Use SSL to transfer message

Use STARTTLS before sending message

For SSMTP sending, and some servers, Login on sending

Verbose reporting of the send process

Use SendMail to send message

Use SSMTP to send message

**Available operations**

The different variables that need to be used when connecting this program to the remote email server. To test that the settings are correct, it is suggested that you use the send test email now checkbox. This will send a message to the email address in the recipient box when the Accept changes button is pressed.

The parameters for describing the connection to the server are listed below. Also listed are the values that would be used if one was using a gmail account as an email server. A fictitious gmail account at the address *radionetworking@gmail.com* and password of *secret* is described in Table 7. Also described in Table 7 is a GMX email configuration that has been anonymized.

Table 7: Sample Email Config values

Label	Gmail value	GMX value
User name	radionetworking@gmail.com	someuser@gmx.com
Password	secret	hidden
Domain	gmail.com	gmx.com
SMTP server	smtp.gmail.com	smtp.gmx.com
From Address		someuser@gmx.com
Port to use for email	587	25
Authentication type	l	p
Use SSL to transfer message	checked	blank
Use STARTTLS before sending message	checked	blank
Recipient of text message	someone@yahoo.com	validemail@address.com
Send test email now	Checked to send email immediately.	Cleared after processing of this page.

Note that some experimentation may be required to find the correct value. In this case, check the tick box at the bottom to initiate the sending of a test email when the *Accept changes* button is pressed. After the test email has been sent, this tick box will be cleared by the program. The email address of the person to receive the test email is never cleared by the program.

The parameters for describing the use of SSMTP to connect to the remote SSMTP server are listed in Table 8 . When SSMTP is used as an email sending agent, the user will have used a shell command to install the *ssmtp* package. The act of editing these values will overwrite the */etc/ssmtp/ssmtp.conf* configuration file. SSMTP is an ideal mail sending agent on Debian linux installations, so has worked well on Ubuntu and Cubieboard installations.

The table below lists are the values that would be used if one was using a gmail account as an email server. A fictitious gmail account at the address *radionetworking@gmail.com* and password of *secret* is described in Table 7.

Table 8: Sample Email Config values (SSMTP method of sending)

Label	Gmail value	Description
<i>User name</i>	radionetworking@gmail.com	This value is often the text to the left of the @ symbol. For this gmail value, the username includes the @ and text to the right.
<i>Password</i>	secret	The invisible text that is kept hidden from other users
<i>SMTP server</i>	smtp.gmail.com	The entity in the their building that on-sends email
<i>From Address</i>		Does little. Future releases of this installation will use this value in the sent email.
<i>Port to use for email</i>	587	Value used is from the email service provider. Typically, it is 22, or 465
<i>Use SSL to transfer message</i>	checked	A security setting.
<i>Use STARTTLS before sending message</i>	checked	A security setting.
<i>For SSMTP sending, login on sending</i>	checked	A security setting.
<i>Use SSMTP to send message</i>	checked	Has to be checked - we are sending a SSMTP message
<i>Use Sendmail to send message</i>	leave blank - unchecked	This must be blank - we are using SSMTP to send this message, so <i>Use SendMail</i> has to be off!

Note that some experimentation may be required to find the correct value. In this case, check the tick box at the bottom to initiate the sending of a test email when the *Accept changes* button is pressed. After the test email has been sent, this tick box will be cleared by the program. The email address of the person to receive the test email is never cleared by the program.

Clues as to what happened when sending the message can be obtained from the diagnostics/email manager/log of messages and error log. Other clues can be obtained by looking in the */var/log* directory of the host linux box and in the files *mail.info*, *mail.err*, *mail.warn*, *mail.log*, and *auth.log*.

#### 5.4.2.2 Who receives emails

The recipients of emails from this program are specified in groups 1, 2, or 3. Each group may have an unlimited number of recipients, and are configured to receive emails in response to some events. Some recipients may wish to have their address in every group. In which case, they will receive duplicates of emails (depending on if two groups share the same event).

On selecting the *Recipients of Group 1 Email* button in Figure 20, a screen similar to Figure 40 is shown.

Figure 40: Configure which people receive which emails

**Who receives what email for Group 1 on RnSrv**

Recipient(s) for messages of this group

On start of this program

On close of this program

Daily report on status

On CC↔CC link bad

Send test email now

Start running new version of code

Gateway connects to server

Gateway breaks from server

Sites identifying information changed.

Users told to die

**Available operations**

Determine who received emails for a particular event. If multiple recipients are required, separate them with a space character. Do not use a comma character. To verify that it works, check the box for sending a test email. On accepting these changes, an email will be sent immediately.

This window determines who will receive email notifications for group 1 events. Also set it for which event group 1 members will receive email.

The meaning of the fields in Figure 40 is explained in Table 9

Table 9: Different classes of email that can be sent out

Label	Description
<i>Destination(s) of this email class</i>	A space separated list of those who will receive messages from this computer for the events checked below
<i>On start of this program</i>	When this program starts up, an email message is sent out. Thus, this computer will send a message after an upgrade. Useful for determining if there are reliability issues.
<i>On close of this program</i>	When this program closes down, an email message is sent. Can be useful for diagnosing some issues.
<i>Daily report on status</i>	Creates a summary of call handled by this system
<i>Send test email now</i>	Initiate the immediate sending of email from this computer
<i>Gateway connects to server</i>	Whenever a <i>Gateway</i> connects to the <i>Control Center</i> , send a message to the designated recipients. Can cause a high volume of emails if there is a poor link between a <i>Gateway</i> and this <i>Control Center</i> .
<i>Gateway disconnects from server</i>	Whenever a <i>Gateway</i> breaks its link to the <i>Control Center</i> , send a message to the designated recipients. There can be a high volume of emails if there is a poor link between one (or more) <i>Gateways</i> and this <i>Control Center</i> .

### 5.4.3 Hardware utilities

#### 5.4.3.1 Configure ethernet card

The settings of the ethernet card may be viewed (or altered) as explained in this section.

From Section 5.4, when the sitename *IP address settings* button is pressed, the screen changes to that shown in Figure 41.

Figure 41: Alter/View ethernet card settings

Field name/description	New value	Current system value
The values below alter the operation of the ethernet card, and are applied to all network operations from all programs on this computer		
Enable DHCP (automatic IP selection)	<input checked="" type="checkbox"/>	DHCP is Active
IP address of this box (eg 192.168.1.102)	<input type="text"/>	74.76.122.176
Netmask of this box (eg 255.255.255.0)	<input type="text"/>	255.255.224.0
Network Gateway address or default route	<input type="text"/>	74.76.96.1
		209.18.47.61
		209.18.47.62
DNS server (eg 8.8.8.8)	<input type="text"/>	8.8.8.8
		4.2.2.2
		4.2.2.1
MAC address		0016ECE17A35
Clicking this button will cause this machine to reboot and use the new values.		
<input type="button" value="Click to reboot, use new values"/> <input type="button" value="Go Back"/>		
Clicking this button will cause this machine to reboot and use the new values.		

*Displays the current settings of the ethernet card in this computer. Optionally, the user may adjust these settings and then click the red button to store the new values. Selecting the checkbox to enable DHCP causes all of the text edit boxes to disappear (as they are not used when DHCP is activated).*

The column at the left gives a name and very brief description of the value. The middle column, which contains editable values, displays the previously entered (or new) value. The column at the very right shows the values read directly from the ethernet card.

- *Click to reboot, use new values* is very drastic. It stores the new values to the computer OS and then reboots the system. The values stored are then used when the computer restarts.
- *Go Back* causes the browser to go back to the previously displayed screen.

The meaning of the different fields is explained below. Note that these fields contain values that relate to the settings of the ethernet card, and describe how this computer will connect to the internet. They do need to be set correctly so that the program can operate. These settings commands have been placed here as a convenience to the operator, so that just about everything on this box is configured via the web page.

- *Enable DHCP (automatic IP selection)* is typically used on *Gateway* boxes that are behind a NAT, ADSL, or cable modem. A *Control Center* will occasionally have DHCP enabled. When DHCP is on, the box will ask (at boot time) some arbitration entity on the local network for the correct IP address, netmask, and DNS server to use.
- *IP address of this box* is the IPv4 location of this computer. It should be entered for a *Control Center* as this means that remote *Gateways* are guaranteed of finding this computer to connect with.

- *NetMask of this box* specifies a bit pattern which indicates what portion of the IP address is common to all devices on this network. From this information, the host computer can determine if a box (with a particular IP address) is accessed on the local network or on the public internet.
- *Network Gateway address or default route* is used on boxes that are behind a NAT/ADSL box/cable modem. The *Control Center* sends packets via this address to entities on the public internet.
- *DNS server* is the network location of the box that can turn a word address (eg *rndownload.dyndns.org*) into an IPv4 address. At the time of writing, the *DNS server* reports that *rndownload.dyndns.org* was at the IPv4 address of *72.45.131.217*.
- *MAC address* is a 12 hex digit string that uniquely identifies the ethernet card used by this computer. This value can never be changed by the user, and so there is no edit box. It is reported as a convenience to the user. Internally, the MAC address is used to uniquely identify the different *Gateways* on the *Control Center*.

When this system runs on a virtual installation, there is no facility to adjust network settings. The reason is that there is no reason for the user to adjust network settings - the box is running correctly at startup. Altering the network settings on an already running virtual system can only create problems.

Further, the virtual software can also be used to run on a Linux PC. In this case, allowing the user to adjust network settings is madness.

### 5.4.3.2 Clock adjust

Clicking *Clock adjust* from *Config* opens the screen shown in Figure 42. This provides a means for the date, hour and minute used by the *Control Center* (and consequently the attached *Gateways*) to be changed to a different value. Changing the clock will initiate a reboot of all machines. The *Gateways* will get the new time from the *Control Center* and update accordingly.

Figure 42: Clock adjust

**Date Time Adjust on RnSrv**

Time Zone selection:: Africa ▾

Enable NTP ⓘ  Enable UTC ⓘ

Month Day Year Hour Minute

<input type="radio"/> January <input type="radio"/> February <input type="radio"/> March <input type="radio"/> April <input type="radio"/> May <input type="radio"/> June <input type="radio"/> July <input type="radio"/> August <input type="radio"/> September <input type="radio"/> October <input type="radio"/> November <input checked="" type="radio"/> December												<input type="radio"/> 0 <input type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4 <input type="radio"/> 5 <input type="radio"/> 6 <input type="radio"/> 7 <input type="radio"/> 8 <input type="radio"/> 9 <input type="radio"/> 10 <input type="radio"/> 11 <input type="radio"/> 12 <input checked="" type="radio"/> 13 <input type="radio"/> 14 <input type="radio"/> 15 <input type="radio"/> 16 <input type="radio"/> 17 <input type="radio"/> 18 <input type="radio"/> 19 <input type="radio"/> 20 <input type="radio"/> 21 <input type="radio"/> 22 <input type="radio"/> 23																																																																																																															
<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr><td><input type="radio"/> 1</td><td><input type="radio"/> 2</td><td><input type="radio"/> 3</td><td><input type="radio"/> 4</td><td><input type="radio"/> 5</td><td><input type="radio"/> 6</td><td><input type="radio"/> 7</td><td><input type="radio"/> 8</td><td><input type="radio"/> 9</td><td><input type="radio"/> 10</td></tr> <tr><td><input type="radio"/> 11</td><td><input type="radio"/> 12</td><td><input type="radio"/> 13</td><td><input type="radio"/> 14</td><td><input type="radio"/> 15</td><td><input type="radio"/> 16</td><td><input checked="" type="radio"/> 17</td><td><input type="radio"/> 18</td><td><input type="radio"/> 19</td><td><input type="radio"/> 20</td></tr> <tr><td><input type="radio"/> 21</td><td><input type="radio"/> 22</td><td><input type="radio"/> 23</td><td><input type="radio"/> 24</td><td><input type="radio"/> 25</td><td><input type="radio"/> 26</td><td><input type="radio"/> 27</td><td><input type="radio"/> 28</td><td><input type="radio"/> 29</td><td><input type="radio"/> 30</td></tr> <tr><td><input type="radio"/> 31</td><td colspan="9"></td></tr> </table>												<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5	<input type="radio"/> 6	<input type="radio"/> 7	<input type="radio"/> 8	<input type="radio"/> 9	<input type="radio"/> 10	<input type="radio"/> 11	<input type="radio"/> 12	<input type="radio"/> 13	<input type="radio"/> 14	<input type="radio"/> 15	<input type="radio"/> 16	<input checked="" type="radio"/> 17	<input type="radio"/> 18	<input type="radio"/> 19	<input type="radio"/> 20	<input type="radio"/> 21	<input type="radio"/> 22	<input type="radio"/> 23	<input type="radio"/> 24	<input type="radio"/> 25	<input type="radio"/> 26	<input type="radio"/> 27	<input type="radio"/> 28	<input type="radio"/> 29	<input type="radio"/> 30	<input type="radio"/> 31										<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr><td><input type="radio"/> 0</td><td><input type="radio"/> 1</td><td><input type="radio"/> 2</td><td><input type="radio"/> 3</td><td><input type="radio"/> 4</td><td><input type="radio"/> 5</td><td><input type="radio"/> 6</td><td><input type="radio"/> 7</td><td><input type="radio"/> 8</td><td><input type="radio"/> 9</td></tr> <tr><td><input type="radio"/> 10</td><td><input type="radio"/> 11</td><td><input type="radio"/> 12</td><td><input type="radio"/> 13</td><td><input type="radio"/> 14</td><td><input type="radio"/> 15</td><td><input type="radio"/> 16</td><td><input type="radio"/> 17</td><td><input type="radio"/> 18</td><td><input type="radio"/> 19</td></tr> <tr><td><input type="radio"/> 20</td><td><input type="radio"/> 21</td><td><input type="radio"/> 22</td><td><input type="radio"/> 23</td><td><input type="radio"/> 24</td><td><input type="radio"/> 25</td><td><input type="radio"/> 26</td><td><input type="radio"/> 27</td><td><input checked="" type="radio"/> 28</td><td><input type="radio"/> 29</td></tr> <tr><td><input type="radio"/> 30</td><td><input type="radio"/> 31</td><td><input type="radio"/> 32</td><td><input type="radio"/> 33</td><td><input type="radio"/> 34</td><td><input type="radio"/> 35</td><td><input type="radio"/> 36</td><td><input type="radio"/> 37</td><td><input type="radio"/> 38</td><td><input type="radio"/> 39</td></tr> <tr><td><input type="radio"/> 40</td><td><input type="radio"/> 41</td><td><input type="radio"/> 42</td><td><input type="radio"/> 43</td><td><input type="radio"/> 44</td><td><input type="radio"/> 45</td><td><input type="radio"/> 46</td><td><input type="radio"/> 47</td><td><input type="radio"/> 48</td><td><input type="radio"/> 49</td></tr> <tr><td><input type="radio"/> 50</td><td><input type="radio"/> 51</td><td><input type="radio"/> 52</td><td><input type="radio"/> 53</td><td><input type="radio"/> 54</td><td><input type="radio"/> 55</td><td><input type="radio"/> 56</td><td><input type="radio"/> 57</td><td><input type="radio"/> 58</td><td><input type="radio"/> 59</td></tr> </table>												<input type="radio"/> 0	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5	<input type="radio"/> 6	<input type="radio"/> 7	<input type="radio"/> 8	<input type="radio"/> 9	<input type="radio"/> 10	<input type="radio"/> 11	<input type="radio"/> 12	<input type="radio"/> 13	<input type="radio"/> 14	<input type="radio"/> 15	<input type="radio"/> 16	<input type="radio"/> 17	<input type="radio"/> 18	<input type="radio"/> 19	<input type="radio"/> 20	<input type="radio"/> 21	<input type="radio"/> 22	<input type="radio"/> 23	<input type="radio"/> 24	<input type="radio"/> 25	<input type="radio"/> 26	<input type="radio"/> 27	<input checked="" type="radio"/> 28	<input type="radio"/> 29	<input type="radio"/> 30	<input type="radio"/> 31	<input type="radio"/> 32	<input type="radio"/> 33	<input type="radio"/> 34	<input type="radio"/> 35	<input type="radio"/> 36	<input type="radio"/> 37	<input type="radio"/> 38	<input type="radio"/> 39	<input type="radio"/> 40	<input type="radio"/> 41	<input type="radio"/> 42	<input type="radio"/> 43	<input type="radio"/> 44	<input type="radio"/> 45	<input type="radio"/> 46	<input type="radio"/> 47	<input type="radio"/> 48	<input type="radio"/> 49	<input type="radio"/> 50	<input type="radio"/> 51	<input type="radio"/> 52	<input type="radio"/> 53	<input type="radio"/> 54	<input type="radio"/> 55	<input type="radio"/> 56	<input type="radio"/> 57	<input type="radio"/> 58	<input type="radio"/> 59
<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5	<input type="radio"/> 6	<input type="radio"/> 7	<input type="radio"/> 8	<input type="radio"/> 9	<input type="radio"/> 10																																																																																																																		
<input type="radio"/> 11	<input type="radio"/> 12	<input type="radio"/> 13	<input type="radio"/> 14	<input type="radio"/> 15	<input type="radio"/> 16	<input checked="" type="radio"/> 17	<input type="radio"/> 18	<input type="radio"/> 19	<input type="radio"/> 20																																																																																																																		
<input type="radio"/> 21	<input type="radio"/> 22	<input type="radio"/> 23	<input type="radio"/> 24	<input type="radio"/> 25	<input type="radio"/> 26	<input type="radio"/> 27	<input type="radio"/> 28	<input type="radio"/> 29	<input type="radio"/> 30																																																																																																																		
<input type="radio"/> 31																																																																																																																											
<input type="radio"/> 0	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5	<input type="radio"/> 6	<input type="radio"/> 7	<input type="radio"/> 8	<input type="radio"/> 9																																																																																																																		
<input type="radio"/> 10	<input type="radio"/> 11	<input type="radio"/> 12	<input type="radio"/> 13	<input type="radio"/> 14	<input type="radio"/> 15	<input type="radio"/> 16	<input type="radio"/> 17	<input type="radio"/> 18	<input type="radio"/> 19																																																																																																																		
<input type="radio"/> 20	<input type="radio"/> 21	<input type="radio"/> 22	<input type="radio"/> 23	<input type="radio"/> 24	<input type="radio"/> 25	<input type="radio"/> 26	<input type="radio"/> 27	<input checked="" type="radio"/> 28	<input type="radio"/> 29																																																																																																																		
<input type="radio"/> 30	<input type="radio"/> 31	<input type="radio"/> 32	<input type="radio"/> 33	<input type="radio"/> 34	<input type="radio"/> 35	<input type="radio"/> 36	<input type="radio"/> 37	<input type="radio"/> 38	<input type="radio"/> 39																																																																																																																		
<input type="radio"/> 40	<input type="radio"/> 41	<input type="radio"/> 42	<input type="radio"/> 43	<input type="radio"/> 44	<input type="radio"/> 45	<input type="radio"/> 46	<input type="radio"/> 47	<input type="radio"/> 48	<input type="radio"/> 49																																																																																																																		
<input type="radio"/> 50	<input type="radio"/> 51	<input type="radio"/> 52	<input type="radio"/> 53	<input type="radio"/> 54	<input type="radio"/> 55	<input type="radio"/> 56	<input type="radio"/> 57	<input type="radio"/> 58	<input type="radio"/> 59																																																																																																																		
<input type="radio"/> 2010 <input type="radio"/> 2011 <input type="radio"/> 2012 <input type="radio"/> 2013 <input checked="" type="radio"/> 2014 <input type="radio"/> 2015 <input type="radio"/> 2016 <input type="radio"/> 2017																																																																																																																											

Click to reboot, and store new values

Clicking this button will cause this machine to reboot.  
The attached Gateways will also reboot. Be very VERY very careful

*The adjust window for the date and time on the Control Center. The Gateways will automatically update to this time on connecting to the Control Center.*

*In this example, the radio buttons are set to the 17<sup>th</sup> of December 2014 at 1:28pm (note the 24-hour time). If a time zone were selected or Enable UTC checked, this time would be over-ridden.*

There are three ways to adjust the date and time:

- Selecting a time zone by choosing a location from the drop down menu at the top of Figure 42.
- Checking the *Enable UTC* box will set the clock to Coordinated Universal Time. This option will over-ride other times selected on this page.

- The operator can manually select a time using the radio buttons in the lower part of Figure 42. Note that the hours are in 24-hour time. The radio buttons are set to display the time and date at the moment the page was rendered. Should an invalid date (such as February 31) be entered, the date setting process is terminated and a warning message is displayed.

### 5.4.3.3 Serial Device

The serial device is used by some *Control Centers* and *Gateways* to interact with external components. It is configured through the window opened by the *Serial Device* button reported in Section 5.4. An example screenshot for configuring the serial device is shown in Figure 43.

Figure 43: Configure serial device on *Control Center*

**Serial device configuration on RnSrv**

Number of data bits  6, 7, 8. (Default is 8)

Number of stop bits  0, 1, 2. (Default is 1)

Parity  none(0) odd(1) even(2) (Default is 0)

Baud  300(0), 1200(1), 2400(2) 4800(3) 9600(4) 19200(5) 38400(6) 57600(7) (Default is 4)

Device starts when program starts

Serial port  COM1 (1) or COM2 (2) or USB (3)

**Available operations**

*Configuration of the serial device on a Control Center. If the serial device on a remote Gateway was being configured (as described in Section 5.4.6.5) the name of the Gateway would be displayed near the top of the screen.*

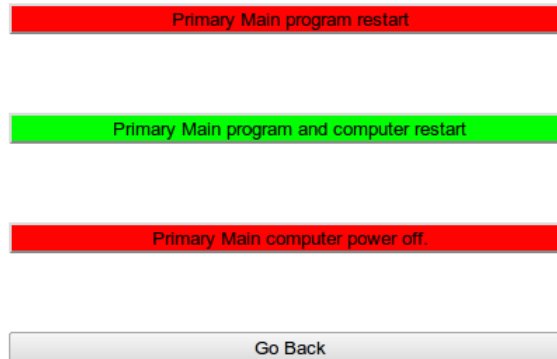
- *Number of data bits* is a standard serial configuration, which is normally set to 8.
- *Number of stop bits* is a standard serial configuration, which is normally set to 1.
- *Parity* is a standard serial configuration, which is normally set to 0, for no parity.
- *Baud* is a standard serial configuration, which is normally set to 4, for 9.6 kbits/sec.
- *Device starts when program starts* should only be on (or checked) for those *Gateways* that have analog radios attached.
- *Serial port* allows the user to specify between either of the two serial devices on the motherboard, or to indicate to use an attached USB-Serial device.

### 5.4.3.4 Restart system

This is the recommended mechanism for stopping the program and (optionally) restarting it. After some configuration changes, the user may wish to restart to verify that the change is permanent. A screenshot of this option is shown in Figure 44.



Figure 44: Restart system

**Primary Main system restart**

The restart system window for a Primary Control Center, which is almost the same as on a Gateway or Secondary Control Center. Normally, the option in green is taken.

Note that each of the displayed buttons has the *sitename* displayed on the button. This is a visual reminder as to what box is going to be restarted. The meaning of the boxes is as follows:

- *Primary Main program restart* shuts the program down and the system will restart in ten seconds. If the program fails to shut down nicely, a manual poweroff on the box is required. Consequently, this option is dangerous and is displayed in red. This option normally completes in 20 seconds and is the quickest.
- *Primary Main program and computer restart* does a guaranteed shutdown and restart of the computer. The restart will always happen but it takes slightly longer. The hardware reboots which will mean the attached audio and serial devices are more likely to restart correctly.
- *Primary Main computer power off* stops the power to the computer running this program. Afterwards, a manual power on is required to get service from this box again. Consequently, this option is colored red to indicate it is dangerous.

When the program is restarted in this fashion, all of the performance logs (network bandwidth usage, etc) are flushed and saved to disk. But, rebooting the system from the console will mean that the program will be stopped at some point, leaving some performance logs not completely written to disk. The network traffic volume report is tested every two minutes, but only updated to hard disk every 40 minutes. Consequently, rebooting the computer from the command line can lose 0-40 minutes of network traffic volume data. A similar timescale exists for any other performance data on the system. The performance logs which can be saved to disk are listed in Section [5.4.4](#).

#### 5.4.4 System Utilities

System level of configuration are the variables that uniquely describe this computer. This includes options to adjust the username and values that are not commonly used. Some of these settings are not required as they are used in some configurations. For completeness, they are made available and are described here.

##### 5.4.4.1 General System

Set the *sitename*, host to use for network connectivity tests, DynDns values, and logging of graphed data to disk. An example screenshot is given in Figure [45](#).

Figure 45: System configuration

**System configuration on RnSrv**

Site name

Show IP address on LCD display

Show CC↔CC links in separate page

Show Minimal Netwatch on Login Window

Report page requires password

Get Files page requires password

Show N lines of history in Netwatch page  Number of lines of history shown on the netwatch screen

Supplementary ID string  Used during the initial setup

SSL Certificate file name  Secures (using SSL) all HTTP traffic

Network connectivity host  (4.2.2.2 is good)

Reboot after N seconds of no connection  (0 is disabled)

First Authentication Server

Second Authentication Server

Third Authentication Server

Fourth Authentication Server

**Dns Update**

DynDns User Name

DynDns Update Password

DynDns Host Name

Require dyndns name update

**Simulate serial messages**

Pseudo Serial On

Pseudo Serial On Two

**Log graph data to disk**

Network bandwidth used

Network Link CC-CC

CPU usage

File handles used

Network link to Master Peer

Memory available

Memory used

Network link to remote box

Network link to Peer

Graph of call count handled by Control Center

TCP retransmit

Graph of browser response time

**Available operations**

The various parameters for configuration of the system. These values could not be categorized anywhere else, so were placed here.

The meaning of the different fields is explained as follows:

- *Site name* This value uniquely identifies the physical location or purpose of this particular hardware. It is used in the various log files, in the titles of various web pages, and to name some buttons so it is absolutely clear which computer will be altered. It is envisaged that the *sitename* will have meaning to the operator. The names used in Table 1 are an ideal example. Names like *Gateway a* should be avoided.
- *Show IP address on LCD display* is an option available for use on a minibox with an LCD display, as shown in Figure 6.
- *Show CC↔CC links on a separate page* will cause the *CC↔CC* diagnostic information, normally displayed on the top of the *Net watch* window (see Figure 78) to be put on a separate page. This will be accessed from an additional button in the navigation menu to the left of every page.
- *Show Minimal Netwatch on Login Window* will give anyone access to the *Net watch* page shown in Figure 114 without logging in. The *Minimal Netwatch* page will not show the *CC↔CC* table at the top of the page. An additional button will be provided on the login screen in Figure 15.
- *Report page requires password* means that a *Low User* or above username and password must be provided to access call data from the text based query interface (at *http://IP address:42420/report*).
- *Get files page requires password* means that a *Low User* or above username and password must be provided to access the *Get files* page at *http://IP address:42420/report*.
- *Show N lines of history in Netwatch page* configures the *Net watch* page described in Section 5.7. This option enables the user to set the number of rows in the table shown on the *Net watch* page.
- *Supplementary ID string* is used in combination with the installation serial number (shown in Figure 74) to provide a unique identification for the installation. DO NOT change these values (unless advised by technical support) as this breaks the licensing on the computer.
- *SSL certificate file name* allows the user to configure all HTTP traffic to be secure. This will impact CPU usage.
- *Network connectivity host* is the IP address of the remote box used for network tests. The strongly suggested value is 8.8.8.8, which is a Google supplied server. Leaving this field blank disables this test. After the screenshot was taken, the code was changed to actively disable 4.2.2.2 as the destination (the current network spec says 4.2.2.2 should be used).
- *Reboot after N seconds of no connection* will set the number of seconds the program will try to connect to the Network connectivity host. After this timeframe the program will reboot. Setting this field to 0 or leaving the *Network connectivity host* field blank will disable this feature.
- *Authentication Servers* are boxes that verify the licensing on this program. At least one of these four must be specified to run the installation on a virtual computer. The value will be provided by technical support.
- *Dns Update* is used if you have registered with the free Dynamic Dns Update service provided at [www.dyndns.org](http://www.dyndns.org). With a dynamic dns value set, the *Gateways* can be configured to connect to the dyndns value managed by the *Primary Control Center*.
- *Simulate serial messages* is for test purposes only. It will test the sound device on the first LTR channel.
- *Log graph data to disk*. Various performance graphs on this system (for example the log of call count on the home page) track measurable quantities. On reboot, these values are lost. However, if this data is logged to disk (by marking the relevant checkbox), then the old data will be loaded back in after a reboot. There is a slight performance hit with every graph logged to disk. If the CPU is showing signs of too much load (Section 5.6.3) it may help not logging some graphs to disk. Most graphs log data to disk once every forty minutes. The log of entries to the disk is capped so that a week (or less) of data is logged. The data files are all in text format. They can be found in the */ravennet* directory. For help in reading and interpreting the contents of these files, please contact technical support.

#### 5.4.4.2 User Names and Passwords

This page enables the administrator to set who logs in to what access level. Further, the passwords for each user is defined in this section. It is suggested that a box running as a *Gateway* has one user and password in the admin level. However, a *Control Center* will have many more values entered.

From Section 5.4, when the *User Names and Passwords* button is pressed, the screen changes to that shown in Figure 46.

Figure 46: User Names and Passwords

**Manage User Names and Passwords on Primary Main**

Select Authorization Level
Admin ▼
admin

<div style="border: 1px solid black; padding: 2px;">User Name</div> <input style="width: 95%; border: none;" type="text" value="a"/>	<div style="border: 1px solid black; padding: 2px;">Password</div> <input style="width: 95%; border: none;" type="password" value="•"/>
--	---

admin
Add Entry
Delete Entry
Modify Entry

Edit	a
Edit	admin
Edit	sample

*Edit the list of usernames+passwords that may login to this program. Note that usernames+passwords may be added to the authorization types Guest, Low User, User and Admin which have low, medium and high privileges in using this program.*

This editing window works in the same way as Figure 22, Figure 36, and Figure 31. Select the authorization type (or access level) to work in with the drop down box at the top and make changes in the middle bar. When the appropriate result is achieved, select *Add Entry*, *Delete Entry*, or *Modify Entry* to enact the desired result. Pressing the *Edit* button in the bottom table will enable you to alter an existing entry.

There are five authorization levels available. Listed from low privilege to high these are:

- *Guest* users can access the *Net watch* and *Help* pages.
- *Low User* can access the *Net watch* and *Help* pages, and will have an extra button in the navigation menu on the left of the screen which takes them to the *Live network* page (see Figure 92) which is accessed through the *Diagnostics* menu.
- *User* can access *Calls*, *Diagnostics*, *Net watch* and *Help* pages.
- *Low Admin* has access to all pages. This is the only authorization level with access to *Config* options. Cannot change any setting in the *Config* options
- *Admin* has access to all pages. This is the only authorization level with access to *Config* options.

Note that where users have access to *Net watch* they will also have access to the *CC↔CC* page if this option is selected in Figure 45.

### 5.4.4.3 Update Control Center

This allows you to see the changes available in the latest release of the software. If you wish to update, you can initiate an upgrade which brings the latest version back to this *Control Center* and installs it. The installation process will reboot this *Control Center*. All of the currently connected *Gateways* will then download the new release from this *Control Center* and install. The *Secondary Control Center* will upgrade at the same time as the *Gateways*, in exactly the same manner. While the updated version is being copied from one machine to another, voice calls can be handled as per normal.

The screen shot below (Figure 47) is an example of the option to upgrade this *Control Center* to the latest available version.

Figure 47: Update Control Center

**6110.2012.7.17**  
19:00:31 July 17, 2012  
Single connection

**Control Center Primary Main**

**Check for updates for Primary Main**

Remote site with recent code

6100 Add a global option to "Channel common" to allow the setting of gain (positive or negative) on the DVSI/Ambe devices.

6090 Add pages and pages of online help documentation. This is a work in progress - some of it will be helpful. Any comments on it - or suggestions for extra text should be sent to technical support. Any text submissions will be gratefully accepted and used. Figures in .png format please.

6054 Enable help button on the main page. Shows the beginning of the online help reports.

6052 Rebuild a component on every connection, rather than reuse it. Makes for more reliable operation when the network performance is abysmal.

6027 When doing an upgrade from a remote box, work harder to get the remote version number from the remote box.

6010 Add a green/red light to indicate the channel is attempting to operate, but not working due to poor sound card or network connection.

Change log

rdownload.dyndns.org is at 6105\_July\_17\_2012\_9.19.37 ( or 6105.2012.7.17)

Information collected at 19:00:06

**Click to confirm**  
  
**Apply now**

The update window for a Primary Control Center. The version number and log of significant changes at the Upgrade Server (Section 2.4) is displayed.

The Upgrade Server is (in this case) rdownload.dyndns.org. As long as the value points to a valid Control Center, any value can be used. The upgrade process will allow you to upgrade, but not downgrade.

The default *Upgrade Server* is rdownload.dyndns.org. The current version number of the *Control Center* supplying the web pages is shown at the very top right of the screen. The version number at the *Upgrade Server* is reported near the bottom of the screen. Should you wish to upgrade to the newest release, simply click the *Get Update* button.

After clicking the update button, a live progress report is displayed at the top of the screen. Ideally, the update system should not be stopped. Should there be a problem, the update process can be stopped by restarting the system (as explained in Figure 44). Restarting the system while the upgrade file is being downloaded is totally safe. Restarting the system after the upgrade file has been downloaded will leave the box in an unknown state.

During the upgrade, the progress can be monitored from *Diagnostics*, as described in Section 5.6.6.1.

The *Primary Control Center* will reboot on completion of install and start running the new version. At this point, the *Gateways* will note the version difference. Each *Gateway* will automatically download the new version from the *Primary Control Center*,

reboot, and run the new version. The *Secondary Control Center* will download the new version from the *Primary Control Center* (in exactly the same way as the *Gateways*). While the upgrade image is being transferred between boxes, calls can be handled as per normal. No calls will be handled when the box is actually rebooting.

In this particular case, the screenshot is from a *Primary Control Center* that is running revision number 6110, dated July 17<sup>th</sup> 2012 (as seen in the top right corner of the screen - see Section 5.2). The *Upgrade Server* is running an older version (number 6105), so upgrades are not reasonable. This screenshot is from a *Control Center* used in the development of the code, so does have the most recent version of code (at the time of this screenshot).

The *Alternate Control Center* can update from any *Control Center* running a more recent version of the code. Suppose the *Primary Control Center* is running a newer version of the code. In this case, the *Remote site with recent code* field would be set to the location of the *Primary Control Center*. Click on the *Refresh Info* button to check the version number and change log of the *Primary Control Center*. Since the *Primary Control Center* does have a newer version, click the *Get Update* button. Immediately, the *Alternate Control Center* will start updating from the *Primary Control Center*.

Also noteworthy is the change log does not contain a mention for every revision. Only significant changes or announcements are placed in the report.

#### 5.4.5 Backup/Restore

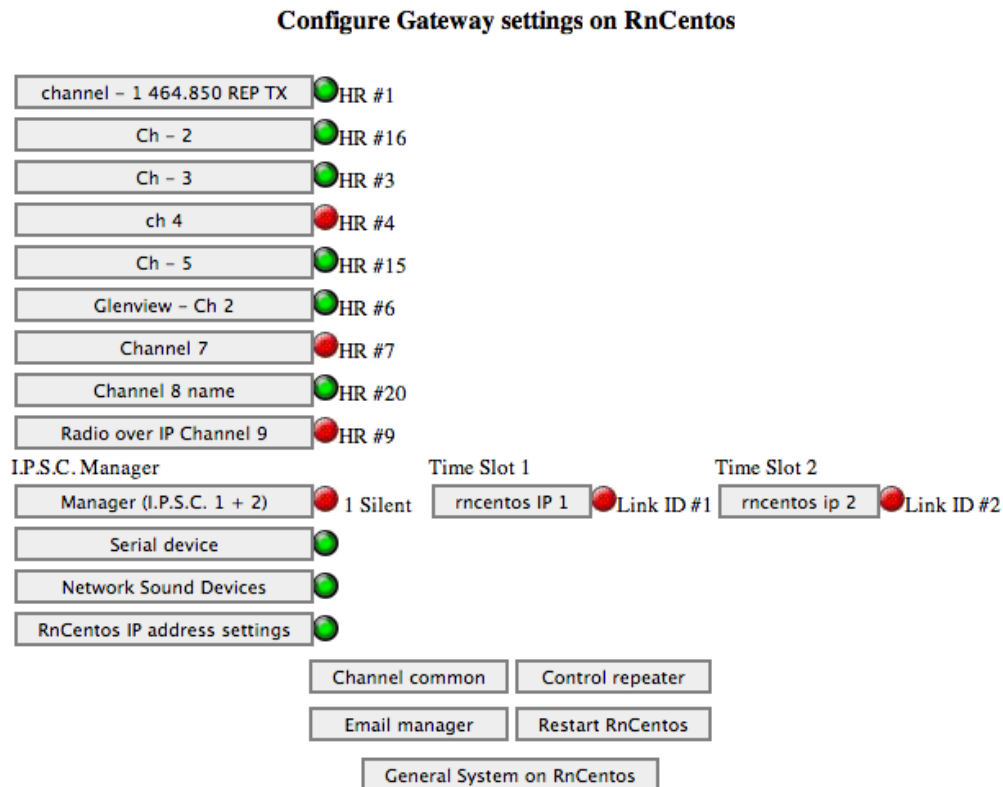
The only files which really should be backed up is the */ravennet/rncp.ini* file. This file is found on the *Gateways* and on the *Control Center*. The contents of this file will vary according to the location. With the *Create Backup File* button one *.zip* file is created which the browser automatically downloads. Inside the *.zip* file is the compressed contents of the *.ini* files from the *Gateways* and *Control Center* on your network. The contents of the *.zip* file clearly state the date and time of the backup. Keep the backup file in a safe place.

There are two times to test the backup system. Before the disaster or after the disaster. Before is much better! To test the backup is good, simply verify that you can use a *zip* archival tool to extract the contents of the backup file.

#### 5.4.6 Configuration on attached Gateways

All *Gateways* that are currently connected to the *Control Center* are listed on *Config* screen shown in Figure 20. By selecting the appropriate button, the user can change some settings on one *Gateway*. The name displayed on each button is the *sitename* of the *Gateway*.

A screen shot of editing the configuration on *RnCentos* (a *Gateway* connected to the *Control Center RnSrv*) is shown in Figure 48. Note that the configuration window on the remote *Gateway* looks similar to the main *Config* window shown in Figure 20, except that the *Control Center* specific settings are not available.

Figure 48: Configuration on a *Gateway* - option selection

The configuration window for RnCentos. The window is similar to that shown in the primary configuration window (Figure 20). There are some additional buttons specific to a *Gateway*, and some buttons removed (which were specific to the *Control Center*). The meaning of the colored lights is explained in Section 5.6.8.6.1.

All configuration windows on the *Gateway* displays the *Gateway's* *sitename* near the top of the web page. In Figure 48 the *sitename* *RnCentos* is displayed close to the top of the window. When changing the configuration on a remote *Gateway*, it is recommended that you check the displayed name regularly to ensure that your changes are happening on the intended *Gateway*. It is a very common mistake to think that the changes are happening on a different *Gateway* to where they are actually happening.

Many of the configuration options for the *Gateways* are similar to the *Control Center*. However, there are some differences. Consequently, the configuration of the *Gateways* are described in the following sections.

#### 5.4.6.1 Channel common settings on a *Gateway*

All of the voice circuits, or audio channels on a *Gateway* are required to connect to the same *Control Center*. Consequently, all channels on a *Gateway* have some parameters which are common. These parameters are described in this section, which are obtained by pressing the *Channel common* button in Figure 48 to give Figure 49.



Figure 49: Configuration Channel common on a *Gateway*

**Channel common settings on RnCentos**

Location of Primary Control Center	<input type="text" value="rnsrv62.dyndns.org"/>	
Location of Secondary Control Center	<input type="text"/>	
Minimum size (ms) of audio buffer	<input type="text" value="50"/>	50..3000 (100 is good)
Maximum size (ms) of audio buffer	<input type="text" value="3000"/>	100..3000 (500 is good)
Seconds between connection attempts	<input type="text" value="2"/>	0..30 (1 is good)
AMBE A→D Boost (Db)	<input type="text" value="0"/>	-50 .. 50 (-50 is quiet, 0 is unchanged, 50 is very loud, reboot to install)
AMBE D→A Boost (Db)	<input type="text" value="0"/>	-50 .. 50 (-50 is quiet, 0 is unchanged, 50 is very loud, reboot to install)
Percentage gain applied to all tx audio	<input type="text" value="600"/>	0..1000 (100 is unity gain)

0 Mute  
 100 Normal  
 500 5X Boost  
 1000 10X Boost

Available operations

Accept changes

Reset changes

*The parameters that are common to all channels on a Gateway are edited in this window.*

The different values are described here. When completed, the user may select any of the three buttons at the bottom (*Accept changes*, *Reset changes*, or *Go Back*) to get the desired result.

- *Location of the primary/secondary control centers* is a text string that is resolved by the computer to an IP address. Here, it is a word address (*rndownload.dyndns.org*) but it could have been a valid IP address. Note that the location does not contain :42420, and does not contain *http://*.
- The minimum and maximum size of the audio buffer determines the amount of buffering applied to audio received from the *Control Center*. The buffer will dynamically adjust the size depending on the variation in arrival times of the audio packets. In some cases, the user may wish to use the same value for minimum and maximum. In this case, there is no dynamic resizing of the buffer. The buffer size contributes to the delay in receiving audio from the person who is speaking. Should the delay range for the buffer be too small, there will be a decrease in the audio quality.
- *Seconds between connection attempts* slightly reduces the load on the *Control Center* when all channels on all *Gateways* start at the same time. This spaces out the start time of each channel.
- *Percentage gain to all tx audio* applies to analog radio signals, and is a way of raising the average volume of all audio received from this *Gateway*.
- When using *I.P.S.C.* (Motorola radios) it may be necessary to convert the Motorola format (compressed Digital) to raw Audio (or vice versa). The supplied USB devices (or AMBE devices) that were installed on a *Gateway* to do this task can have a gain (increase or decrease) applied at the time of conversion. Typically, a value of 0 is used for no change. This is the case in Figure 49. For a value of, for example, -50dB, audio turned from compressed digital into raw audio will be reduced in volume by 50 decibels. A value of 20 gives a 20 decibel increase.

#### 5.4.6.2 Configuration of one TL-Net channel on a *Gateway*

Primarily, these parameters affect how this channel interacts with the *Control Center*. An example screenshot is provided in Figure 50. The channel being configured will interact with the TL-Net controller. The screen changed to that in Figure 50 when the operator pressed the button *Ch - 2* in Figure 48. Note the label near the top of the screen that says this channel is on *RnCentos*.



Figure 50: Configure one channel window

**Config Ch - 2 on RnCentos**

Descriptive name of this channel

Home Repeater  1..20

Channel automatically starts on system startup

Amplitude for play volume (to Transmitter)  0 = mute, 100 = full volume

Amplitude for record volume (from Receiver)  0 = mute, 100 = full volume

Enable direction change mid call

<b>Available operations</b>	<input type="button" value="Accept changes"/>	<input type="button" value="Reset changes"/>
-----------------------------	---	--

*Configuration of the channel specific values on a remote Gateway.*

- *Descriptive name* is used to describe this particular channel. The value is displayed on the appropriate button, used in log records, and is displayed on the *Control Center*. This name is displayed near the top of the screen in bold. It is recommended that you use a name which is more meaningful (to you) than the name in the above figure (*Ch - 2*).
- *Home repeater*; is used to identify this channel from others on the *Control Center*. This value is used when routing calls to/from a *Bridge Group*. For analog radios, it has a second meaning (that is specific to the external TL-Net hardware).
- *Channel automatically starts* is a way of stopping this particular channel from operating. With the checkbox blank, no audio will pass through this channel to/from the *Control Center*. When this checkbox is ticked, the channel will run and repeatedly attempt to connect to the *Primary Control Center* (or *Secondary Control Center* if the *primary* is not available). Should this channel not connect, additional information can be found in the operational log of this channel, or on the operational log of the remote *Conference Server*.
- *Amplitude play/record* provides channel specific control of the audio volume for analog radios.
- *Accept changes* puts the changes to the channel immediately.
- *Reset changes* and *Go Back* provide a means of ignoring any active edits.

#### 5.4.6.3 Configuration of one *I.P.S.C.* channel on a *Gateway*

When connecting with Motorola repeaters via the Motorola proprietary *I.P.S.C.* protocol, some values need to be assigned to each channel. When connected with a Motorola repeater, each *I.P.S.C.* channel can be considered as though it simulates a radio. Consequently, each *I.P.S.C.* channel has a Radio ID and color code. Note that all odd numbered *I.P.S.C.* channels represent a radio on slot one. All even numbered *I.P.S.C.* channels represent a radio on slot two. An example screenshot for configuring one *I.P.S.C.* channel is shown in Figure 51.

Figure 51: Configuration of one *I.P.S.C.* channel

**Config Device-1 ipsc mb on gateway a**

Descriptive name of this channel

Link ID  1..20

Channel automatically starts on system startup

Support voice+data call

Support data call

Color Code  0--15

Default Radio ID  For calls from non radio source, (1--16776414)

**Available operations**

Configuration of one *I.P.S.C.* channel on Gateway a. Note that this window has a similar mode of operation to the window shown in Figure 50.

The meaning of the buttons and some of the fields is the same as in Section 5.4.6.2. The meaning of the remaining fields is explained in the following list.

- *Support voice+data call* means that *Gateway a* identifies itself to the Motorola *I.P.S.C.* network as being capable of handling voice and data calls. If the *Control Center* is running a codec other than AMBE, there will need to be enough DVSI/AMBE usb devices to handle the audio codec work. One DVSI/AMBE device will be required for each *I.P.S.C.* channel that is voice capable.
- *Support data call* means that *Gateway a* identifies itself to the Motorola *I.P.S.C.* network as being capable of handling data calls.
- *Color Code* is a value chosen by the network planner, so that calls to/from this box are correctly placed in the appropriate group.
- *Default Radio ID* is the value assigned to calls that leave *Gateway a* and go to the connected Motorola repeater, which then go onto the air. This value identifies this *Gateway a* as one particular radio.

#### 5.4.6.4 Configuration of one *I.P.S.C.* connection on a *Gateway*

The Motorola *I.P.S.C.* protocol mandates that two slots (one and two) connect to a Motorola repeater via one network connection. Consequently, *I.P.S.C.* channels 1 and 2 use the same Motorola *I.P.S.C.* network connection. Each Motorola *I.P.S.C.* network connection on a *Gateway* represents one Peer on a Motorola network. The configuration of one connection to the Motorola network is shown in Figure 52.

Figure 52: Configuration of one Motorola *I.P.S.C.* connection

**Config Manager (I.P.S.C. 1 + 2) on RnCentos**

Descriptive name of this I.P.S.C. Manager	<input type="text" value="Manager (I.P.S.C. 1 + 2)"/>	
Operate as Master	<input type="checkbox"/>	Connects to remote I.P.S.C. Master
IP address of the Master	<input type="text"/>	1.2.3.4 or somebox.dyndns.org - no default value
UDP port for the Master	<input type="text" value="50622"/>	a value in range of 40000--42419 OR 42444--65535
Seconds between Keep Alives	<input type="text" value="10"/>	3--30
Seconds between Regn. attempts	<input type="text" value="10"/>	3--30
UDP port for this I.P.S.C. connection on this box	<input type="text" value="51096"/>	40000--42419 OR 42444--65535
Unique ID for this I.P.S.C. connection (PeerID)	<input type="text" value="12866"/>	16,776,415
Silence period to indicate call end (ms)	<input type="text" value="753"/>	750ms is default, 300..2000
Authentication key for I.P.S.C. comms	<input type="text" value="94530"/>	
Recipient(s) of email if there are too many Come/Go events	<input type="text"/>	
Log KeepAlive Requests	<input checked="" type="checkbox"/>	
Log Registration Requests	<input checked="" type="checkbox"/>	
Manager automatically starts	<input type="checkbox"/>	
Log events at the XCMP/XNL level	<input type="checkbox"/>	
Log I.P.S.C. status packets	<input type="checkbox"/>	

<b>Available operations</b>	<input type="button" value="Accept changes"/>	<input type="button" value="Reset changes"/>
-----------------------------	---	--

*Setting the parameters specific to defining one connection with the Motorola I.P.S.C. network.*

- *Descriptive name of this I.P.S.C. Manager* has the same meaning and interpretation as in Section 5.4.6.2
- *UDP port for this I.P.S.C. connection on this box.* This value is unique, and cannot be used by any other *I.P.S.C.* connection on this *Gateway*. If this *Gateway* is behind a firewall, and there are Motorola boxes that are part of this network who are on the other side of the firewall, please ensure that this port on the firewall is forwarded to this *Gateway*. Further, check that the firewall is *I.P.S.C.* compliant and will correctly pass *I.P.S.C.* traffic to this *Gateway*. The NAT test described in Section 5.6.4.2 will assist.
- *Operate as Master* is a checkbox to determine if this *I.P.S.C.* connection is the Master - and manages entry to the *I.P.S.C.* network. Clicking this button will cause the entry boxes for some fields to immediately appear/disappear (these fields are not required for the *I.P.S.C.* Master).
- *UDP port for the Master* specifies the UDP port number of the *I.P.S.C.* Master instance (that this *I.P.S.C.* connection instance will connect to on startup). This field disappears if this *I.P.S.C.* connection instance is operating an *I.P.S.C.* Master.
- *IP address of the Master* specifies the IPv4 address of the *I.P.S.C.* Master instance (that this *I.P.S.C.* connection instance will connect to on startup). This field disappears if this *I.P.S.C.* connection instance is operating an *I.P.S.C.* Master.
- *Seconds between Keep Alives* sets the frequency that keep alive packets are sent from this *I.P.S.C.* connection instance to other members of the *I.P.S.C.* network. A low value will cause this *I.P.S.C.* connection instance to quickly detect and act if a remote Peer has gone unresponsive. This field disappears if this *I.P.S.C.* connection instance is operating an *I.P.S.C.* Master.
- *Seconds between Regn. attempts* sets the frequency of requests to any remote *I.P.S.C.* member. A shorter value will mean the Registration process is quicker if packets are lost in the network. This field disappears if this *I.P.S.C.* connection instance is operating an *I.P.S.C.* Master.
- *Unique ID for this I.P.S.C. connection (PeerID)* is a Motorola *I.P.S.C.* specific number that identifies this connection from other Motorola *I.P.S.C.* entities. All boxes in one Motorola *I.P.S.C.* network will have a different Unique ID. Note that one *Gateway* can be in several Motorola *I.P.S.C.* networks at the same time. It is therefore possible for all *I.P.S.C.* connections on one *Gateway* to have the same Unique ID since every connection is in a different network. This will lead to confusion and is not recommended.

- *Silence period to indicate call end (ms)* is used when no end of call frame is received. In this case, the program waits the specified period before marking the call as finished.
- *Authentication key for I.P.S.C. comms* is the string (40 characters max long) that is used when verifying incoming packets have come from an authorized source.
- *Log KeepAlive Requests* is an aid to tracking Keep Alive requests from this program or from other repeaters. When on, it causes all Keep Alive related events to be recorded in the *I.P.S.C.* log of messages. One can turn this on, check the keep alive messages are coming in by examining the relevant log, and then turning off. If an *I.P.S.C.* Manager receives *KeepAlive* messages from a remote *I.P.S.C.* peer, it will therefore be able to receive voice packets from that peer.
- *Log Registration Requests* is an aid to tracking registration requests from this program or from other repeaters. When on, it causes all registration related events to be recorded in the *I.P.S.C.* log of messages.
- *Manager automatically starts* will start the operation of the *I.P.S.C.* manager with the commencement of the program.
- *Force R1.6/1.7/1.8 authentication* Should be left on - which forces the program to only use the new style of authentication.
- *Log XCMP RSSI messages* is a debugging option, and causes all XCMP events to generate reports which are put in the XCMP log of messages.

#### 5.4.6.5 Configure serial device

The serial device is used for interacting with the external TL-Net hardware, which is used with analog radios. An example configuration screenshot is shown in Figure 43. Configuration of the serial device on a *Gateway* is exactly the same as on a *Control Center*. Consequently, the information in Section 5.4.3.3 can be used to explain the meaning and purpose of the different fields. Note that the *Gateway sitename* on which the serial device configuration is for will be shown near the top of the screen, instead of the *Control Center*.

#### 5.4.6.6 USB URI devices

The USB based sound card, which has a DB25 connector and connects to a USB plug is a sound card that can optionally be used on analog radio systems. It is known by some as "the black thing". A picture of the device is shown in Figure 13. This device has an Erasable EPROM built into it. This program provides the operator the means to store an identifying value into the device, so that on boot the devices are always associated with the correct channel. If the computer is booted when the URI device is connected to the USB bus, the computer will always provide an option to edit the configuration of this device. An example screenshot for editing the configuration is shown in Figure 53

Figure 53: Uniquely identifying each USB URI device

**Modify USB URI channel numbers on gateway a**

Dir name	File name	Sound card	Channel number	Modify channel	Report
004	002	0	2	<input type="text" value="2"/> 1..20	<input type="button" value="System report on device"/>
004	003	1	1	<input type="text" value="1"/> 1..20	<input type="button" value="System report on device"/>

<b>Available operations</b>	<input type="button" value="Accept changes"/>	<input type="button" value="Reset changes"/>
-----------------------------	---	--

*The storing of the identifying values for each attached USB URI device. This example shows two devices connected to Gateway a. They have been edited to have channel numbers of 1 and 2. Pressing the System report on device will put any current edits on hold (or lose them) and take the user to the screen described in Section 5.4.6.6.1.*

If four USB URI devices are attached, they are configured to have channel numbers of 1,2,3, and 4. By swapping the configured numbers, one can swap the mic/speaker from one card to another.

**5.4.6.6.1 System report on one USB URI device**

It is possible to examine the Linux kernel generated messages for one USB URI device. This report is obtained from the window described in Figure 53. An example report is given in Figure 54.

Figure 54: System report of one USB URI device

**System strings for 004-002 on gateway a**

```

15:10:55.042 August 6 2012 Construction and initialization
15:10:55.042 August 6 2012 Determine Alsa Sound card number
15:10:55.060 August 6 2012 sound card number is 0
15:10:55.085 August 6 2012 Device claimed - ready for use
15:10:55.187 August 6 2012 Serial number in EEPROM is 2
15:10:55.187 August 6 2012 Start monitoring interface for commands
15:10:55.215 August 6 2012 Start monitoring control interface

```

*The Linux specific report on one USB URI device. There is little of interest here, except for showing that the card has been configured and initialized correctly.*

**5.4.6.7 Control repeater**

This section provides the operator with the means to restrict users to those who have access rights. Further, it provides a means to manage the use of channels. Consequently, the 20 slots on the repeater bus can be distributed in a manner that gives maximum

benefit to users.

If a TL-Net controller is connected to the *Gateway*, buttons are displayed which can be clicked on. A typical display is shown in Figure 55.

Figure 55: Attached repeaters and configuration selection

<b>Repeater Controller on gateway a</b>			
Repeater Controller 1	<input type="button" value="Configuration"/>	<input type="button" value="Manage users"/>	(Network)
Repeater Controller 2	Configuration	Manage users	
Repeater Controller 3	<input type="button" value="Configuration"/>	<input type="button" value="Manage users"/>	
Repeater Controller 4	Configuration	Manage users	
Repeater Controller 5	<input type="button" value="Configuration"/>	<input type="button" value="Manage users"/>	(Network)
Repeater Controller 6	Configuration	Manage users	
Repeater Controller 7	<input type="button" value="Configuration"/>	<input type="button" value="Manage users"/>	
Repeater Controller 8	Configuration	Manage users	
Repeater Controller 9	<input type="button" value="Configuration"/>	<input type="button" value="Manage users"/>	(Network)
Repeater Controller 10	Configuration	Manage users	
Repeater Controller 11	<input type="button" value="Configuration"/>	<input type="button" value="Manage users"/>	
Repeater Controller 12	Configuration	Manage users	
Repeater Controller 13	<input type="button" value="Configuration"/>	<input type="button" value="Manage users"/>	(Network)
Repeater Controller 14	Configuration	Manage users	
Repeater Controller 15	<input type="button" value="Configuration"/>	<input type="button" value="Manage users"/>	
Repeater Controller 16	Configuration	Manage users	
Repeater Controller 17	<input type="button" value="Configuration"/>	<input type="button" value="Manage users"/>	(Network)
Repeater Controller 18	Configuration	Manage users	
Repeater Controller 19	<input type="button" value="Configuration"/>	<input type="button" value="Manage users"/>	
Repeater Controller 20	Configuration	Manage users	

*The available repeaters from the TL-Net device. Since there are buttons on this screen, we have confidence that serial communications with the TL-Net device is working.*

If it takes five (or more) seconds for the display to be generated, and unlike Figure 55 contains no buttons, check the serial device for messages to and from the TL-Net device. It may be that the serial connection is faulty. Alternatively, the TL-Net controller needs to be in TL-Net mode. Placing the controller in the correct mode is achieved by resetting it, with the *Command to LTR* button described in Section 5.6.8.5.2. Those repeaters which are network capable have a buttons on them for configuration and managing users. Further, the word *(Network>* is displayed.

#### 5.4.6.7.1 Configuration of attached LTR repeater

The Transmitter Audio, Data, and CWID level of the attached repeater can be adjusted. In this section, we illustrate the configuration of repeater 1. Figure 56 shows this. Also provided is an option to restart the LTR controller.

Figure 56: Controller, Configuration for repeater 1

**Repeater Configuration 1 on gateway a**

Warning

Pressing the buttons below will cause an immediate adjustment to be sent to the controller.

Please use caution.

<b>Transmitter Audio Coarse adjustment</b>	Increase	Decrease
<b>Transmitter Audio Fine adjustment</b>	Increase	Decrease
<b>Transmitter Data level</b>	Increase	Decrease
<b>Transmitter CWID level</b>	Increase	Decrease

Buttons for immediate change of the Transmitter Audio, Data, and CWID levels. The LTR controller may be rebooted here.

These adjustments affect local repeated audio levels.

**5.4.6.7.2 Manage users**

The features described in this section provide you with the means to manage the active repeater array and user validation on the TL-Net system. You have the option to validate all users, or invalidate all users. A typical screen is shown in Figure 57.

Figure 57: Manage users for repeater 1

Display of valid repeater array on gateway a for repeater #1.

Users homed on this repeater (1) will have access to these repeaters.

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

White = Inactive    Green = valid Repeater

001	002	003	004	005	006	007	008	009	010	011	012	013	014	015	016	017	018	019	020	021	022	023	024	025
026	027	028	029	030	031	032	033	034	035	036	037	038	039	040	041	042	043	044	045	046	047	048	049	050
051	052	053	054	055	056	057	058	059	060	061	062	063	064	065	066	067	068	069	070	071	072	073	074	075
076	077	078	079	080	081	082	083	084	085	086	087	088	089	090	091	092	093	094	095	096	097	098	099	100
101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125
126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200
201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225
226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250

   White = Inactive    Green = Valid    Click for user detail

The report of which users are active on repeater 1. Uses may be marked inactive through the use of the relevant button. Many users are active. As a sample, users 101-105 are active, but 106 is idle.

Repeaters are enabled/disabled through clicking on a repeater button (at the top, contains 2 digits) which is explained Section 5.4.6.7.4. Users are validated/invalidated through clicking on a user button (which contains three digits) and is explained Section 5.4.6.7.5. Should one wish to enable/disable all users at the same time, it is suggested that *Mass Ident Validate/Invalidate* button is used (as described Section 5.4.6.7.3).

#### 5.4.6.7.3 Mass validation of all users

All of the users on repeater can be validated (or invalidated) at the same time. This is achieved by using the *Mass Ident Validate/Invalidate* button described in Section 5.4.6.7.2. An example screenshot is provided in Figure 58.

Figure 58: Mass validation of all users on repeater 1 of Gateway a



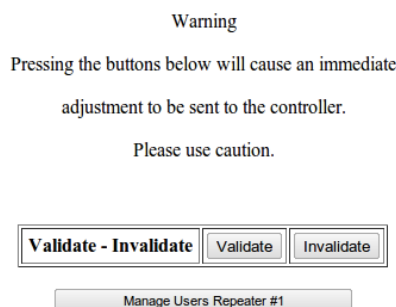
All of the users on repeater 1 of Gateway a may be validated/invalidated with this options. Pressing the Manage Users Repeater #01 will return to Figure 57.

#### 5.4.6.7.4 Validate repeater

Validating of a repeater is through this window, shown in Figure 59. This particular window was obtained after clicking on the repeater button 05 in Figure 57.

Figure 59: Validate repeater 5

#### Validate/Invalidate repeater number 5 for home repeater 1



Alter the validation of repeater 5, when homed on repeater 1. values. By marking repeater 5 as valid, users homed on repeater 1 will have access to repeater 5.



#### 5.4.6.7.5 Enable one user

From Figure 57 *userID* 001 is currently enabled (green box) and could be disabled by left clicking box 001. The screen changes to that shown in Figure 60, where we see that *userID* 001 is currently enabled.

Figure 60: Enable 1 user

Repeater = 01    User = 001    on gateway a

Status = Valid

Status: Valid/Invalid

Click to send new values

---

Manage Users Repeater #01

*Option to disable/enable one particular user on the TL-Net controller.*

In this case, one would clear the checkbox, and press the *Click to send new values* button.

#### 5.4.6.8 General System on a Gateway

This section describes the configuration of System things on a remote *Gateway*. The operation of this feature is almost identical to that described in Section 5.4.4. An example screenshot is given in Figure 61, which is very similar to that shown in Figure 45.

Figure 61: General system configuration on a *Gateway*

**System configuration on RnCentos**

Site name

Show IP address on LCD display

Show CC↔CC links in separate page

Show Minimal Netwatch on Login Window

Show N lines of history in Netwatch page  Number of lines of history shown on the netwatch screen

Supplementary ID string  Used during the initial setup

SSL Certificate file name  Secures (using SSL) all HTTP traffic

No connection *Control Center* Reboot N Seconds  (0 is disabled)

First Authentication Server

Second Authentication Server

Third Authentication Server

Fourth Authentication Server

**Dns Update**

DynDns User Name

DynDns Update Password

DynDns Host Name

Require dyndns name update

**Simulate serial messages**

Pseudo Serial On

Pseudo Serial On Two

**Log graph data to disk**

Network bandwidth used

CPU usage

File handles used

Network link, Gateway to Control Center

Network link to Master Peer

Memory available

Memory used

Network link to Peer

TCP retransmit

**Available operations**

*The configuration of general type things on a Gateway. These things fitted best here. The most important parameter is the sitename. After changing the sitename, the pages generated by the Gateway will have the new sitename. The pages generated on the Control Center will have the new sitename when the Gateway reconnects.*

The differences between Figure 45 and Figure 61 are as follows:

1. *Report* and *Get files* pages do not exist so there is no option to require a password.
2. Since the only entity a *Gateway* should ever connect to is the *Control Center*, there is no point in testing the connection to

another box. Consequently, there is no option for setting the host to use for testing *Network connectivity*.

3. There is no *Control Center* to *Control Center* link for a *Gateway*. A *Gateway* does, however, keep track of the status of the link to the *Control Center*. The loss rate of UDP packets, and the round trip time, is recorded and is available. Consequently, the *Gateway* does log the quality of the network link.
4. A *Gateway* does not run a test for *Network connectivity*, so there is no data to log here. Consequently, the option to log graph data for *Network link to remote box* is not available on a *Gateway*
5. The *Gateway* does not display a graph of calls handled on the main web page. Consequently, the *Gateway* has no option for *Graph of call count handled by Control Center*.
6. Normally, there is no browser connected to a *Gateway*. Thus, there is no point in recording the browser response time.

#### 5.4.6.9 Users and passwords on a *Gateway*

It is possible to access the web page provided by a *Gateway* and this is done in the same way as one accesses the web page of a *Control Center* (see Section 5.1). Under normal operation, the *Control Center* will take the appropriate page from a *Gateway* and display the page as part of the *Control Center*'s page, to be accessed through the *Control Center*'s *Config* page. However, when the *Control Center* is not available, but the *Gateway* is available, it can be necessary to directly configure the *Gateway*. To prevent anyone from configuring the *Gateway*, it is suggested that the administrator installs some password protection on the *Gateway*. The screen in Figure 62 shows this for *Gateway a*.

Figure 62: Users and passwords on a *Gateway*

**Manage User Names and Passwords on gateway a**

Select Authorization Level Admin ▾ admin

<div style="border: 1px solid black; padding: 2px;"> <p style="text-align: center;">User Name</p> <input style="width: 95%; border: none;" type="text" value="admin"/> </div>	<div style="border: 1px solid black; padding: 2px;"> <p style="text-align: center;">Password</p> <input style="width: 95%; border: none;" type="password" value="....."/> </div>
---	--

admin
Add Entry
Delete Entry
Modify Entry

Edit
admin

*Configuration of users and passwords on Gateway a. The only difference to when configuring user names and passwords on a Control Center (Section 5.4.4.2) is the sitename of the box (which is reported near the top of the screen).*

Note that it is perfectly valid to have no users or passwords configured on a *Gateway*. This will prevent everyone from accessing the *Gateway* directly. Even with no names or passwords on a *Gateway*, the *Gateway* can still be configured from the web page of the *Control Center*.

#### 5.4.6.10 Network configuration on a *Gateway*

An example screenshot for changing the network settings on a remote *Gateway* is shown in Figure 63.

Figure 63: IP address settings on a remote *Gateway*

**IP/Network settings on gateway a**

Field name/description	New value	Current system value
Location of Primary Control Center	<input type="text" value="10.0.0.62"/>	10.0.0.62
Location of Secondary Control Center	<input type="text" value="10.0.0.61"/>	10.0.0.61
The values below alter the operation of the ethernet card, and are applied to all network operations from all programs on this computer		
Enable DHCP (automatic IP selection)	<input type="checkbox"/>	DHCP is disabled. Using static IP address.
IP address of this box (eg 192.168.1.102)	<input type="text" value="10.0.0.63"/>	10.0.0.63
Netmask of this box (eg 255.255.255.0)	<input type="text" value="255.255.255.0"/>	255.255.255.0
Network Gateway address or default route	<input type="text" value="10.0.0.2"/>	10.0.0.2
DNS server (eg 8.8.8.8)	<input type="text" value="10.0.0.2"/>	67.138.54.100 4.2.2.2 4.2.2.1
MAC address		00-40-63-F6-36-69

Clicking this button will cause this machine to reboot and use the new values.

Clicking this button will cause this machine to reboot and use the new values.

The parameters for setting the IP address fields on a Gateway. Unlike Figure 41 there are two additional text entry fields for setting the location of the Primary and Secondary Control Center. These two additional fields do not disappear when the DHCP checkbox is ticked/unticked.

Providing the additional text entry fields for setting the location of the *Primary* and *Secondary Control Center* is a duplication as this information is set in Section 5.4.6.1. The ability to set the location of the *Control Center* in two different places is designed to aid the user during setup of the boxes.

#### 5.4.6.11 Email configuration (on remote Gateway)

Email is configured on a *Gateway* in a similar manner as for a *Control Center*, described in Section 5.4.2. There are some differences, there are no options to send emails on *CC↔CC link bad*, *Gateway connects to Control Center* and *Gateway breaks from Control Center*, as these are only applicable to *Control Centers*. There is also an additional option for *New connection with an IPSC Manager/Peer* as this is only applicable to *Gateways*. If a box is acting as both *Control Center* and *Gateway* the options for both *Control Center* and *Gateway* will appear on this page.

When managing multiple boxes it is strongly recommended that only one box is assigned to one email account. If more than one box is connected to only one email account, multiple emails from the same IP address can arrive at the same time. An email provider may mistake this for a security breach, causing issues.

#### 5.4.6.12 Restart system (on remote Gateway)

This option works in the same fashion as in Section 5.4.3.4, with the exception that it is the remote *Gateway* that is restarted. The screen used in this section is identical to that in Figure 44 except that the buttons display the name of the remote *Gateway*. Further, the screen displays the name of the remote *Gateway* below the title bar.

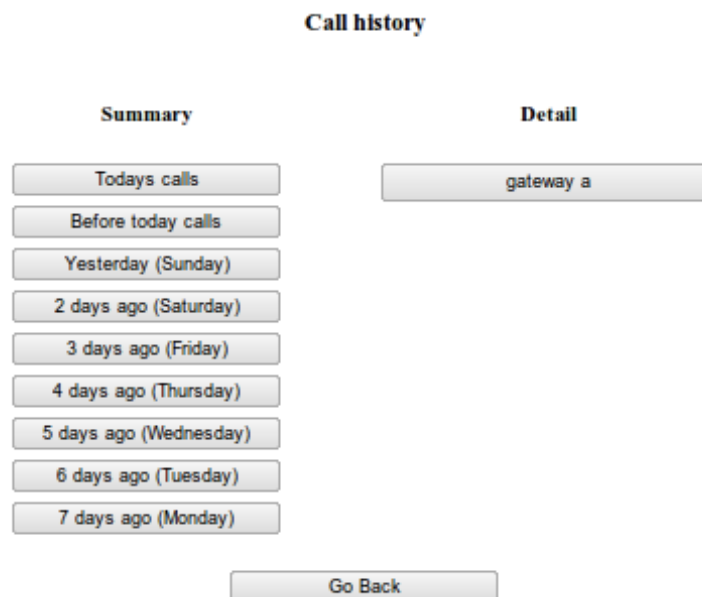
When the remote *Gateway* is restarted, there is a report that the remote *Gateway* is restarting. At the left bottom of the screen, the name of the remote *Gateway* disappears from the list. If the remote *Gateway* was setup to restart, the list at the bottom left will

then show the name of the remote *Gateway* when it restarts. This process can take between 20 seconds and 1 minute. If it takes longer than 2 minutes, it is probable that there is a network configuration issue on the remote *Gateway* - DNS is not working.

## 5.5 Calls

The *Calls* window is accessible by those who have *user* and *admin* privileges. It is designed to report the completed calls that have been handled by the *Control Center*. A sample screenshot is provided in Figure 64.

Figure 64: Previous calls window



The window displayed on clicking on the Call button from the navigation bar. The selection of which log is examined is based on the source of the call, or on date.

All calls that pass through the *Control Center* are recorded in three places. There is a short term record, which holds (at most) the last 100 calls that have passed through the *Control Center*. The count of calls is then summarized and stored in a database for a long term record. Remote computers may view the database contents if they support *ODBC*. To directly view the database contents, or short term record, one may use the options provided in this window.

### 5.5.1 Summary

This section reports the collated call history stored on the database. The database can be queried by date by using the buttons in the left hand column of Figure 64.

#### 5.5.1.1 Todays calls

This button creates a new window which allows the database to be queried for calls that happened today. Note that it is the accumulated calls from today, where today is defined as starting at midnight. The last ten (or so) minutes of calls are buffered in computer memory before writing to the database. This saves computer resources in writing information to the database. The screen for selecting the calls of today is shown in Figure 65. Calls can be selected on the basis of site name, user name, and access type.

Figure 65: Todays calls in the database

**View Database**

Site name	User name	Access type
all sites ▼	all users ▼	both ▼
<input type="button" value="Query Database"/>		
<input type="button" value="Go Back"/>		

The window used for selecting which calls from the database are viewed - out of those available for today. Note that this window does not have the date range selection options provided in Figure 66.

### 5.5.1.2 Before todays calls

This creates a window which allows the user to search for calls from a customized date range (from yesterday or earlier). Selecting which day(s) are viewed is via the drop down boxes in the middle, which are shown in Figure 66. This option, to look at calls before today, cannot report calls that happen today. As in *Todays calls*, calls can also be selected on the basis of site name, user name, and access type.

Figure 66: Calls for a date before today

**View Database**

Site name	User name	Earliest date	Latest date	Access type
all sites ▼	all users ▼	2012 ▼ July ▼ 19 ▼	2012 ▼ July ▼ 19 ▼	both ▼
<input type="button" value="Query Database"/>				
<input type="button" value="Go Back"/>				

The window used for selecting which calls from the database are viewed - out of those prior to today. This window does have the date range selection options (unlike Figure 66). The date range selected to be viewed is only one day wide - it can be altered by the user to view call summary for any date range.

### 5.5.1.3 X days ago

These buttons work in the same manner as *Before todays calls* (Section 5.5.1.2), except that the date range is preconfigured for the specified date.

## 5.5.2 Detail

The right hand column of Figure 64 has buttons which report the short term record of individual calls (up to 100 calls). The call record for each connected *Gateway* is available at a click of the relevant button. This will generate a table similar to that shown in Figure 67.

Figure 67: Detailed list of recent calls

Detailed list of recent calls on RnSrv : : Analog and Ipvc Voice.

<input type="button" value="Go Back"/> <input type="button" value="Refresh"/> <input checked="" type="button" value="Analog"/> <input checked="" type="button" value="Ipvc Voice"/> <input type="button" value="Ipvc Data"/>													
start time	duration	ch	name	radio id	radio id	site name	Loss rate last call						
01 01:37:27.3 Jan/27	3.2	2	Ch - 1	g							RnSrv	0.0%	1715986449
01 01:37:23.6 Jan/27	3.2	2	Ch - 1	g							RnSrv	0.0%	1715986449
01 01:37:19.9 Jan/27	3.2	2	Ch - 1	g							RnSrv	0.0%	1715986449
01 01:37:16.2 Jan/27	3.2	2	Ch - 1	g							RnSrv	0.0%	1715986449
01 01:37:12.5 Jan/27	3.2	2	Ch - 1	g							RnSrv	0.0%	1715986449
01 01:37:08.8 Jan/27	3.2	2	Ch - 1	g							RnSrv	0.0%	1715986449
01 01:37:05.1 Jan/27	3.2	2	Ch - 1	g							RnSrv	0.0%	1715986449
01 01:37:01.4 Jan/27	3.2	2	Ch - 1	g							RnSrv	0.0%	1715986449
01 01:36:57.7 Jan/27	3.2	2	Ch - 1	g							RnSrv	0.0%	1715986449
01 01:36:54.0 Jan/27	3.2	2	Ch - 1	g							RnSrv	0.0%	1715986449
01 01:36:50.3 Jan/27	3.2	2	Ch - 1	g							RnSrv	0.0%	1715986449
01 01:36:46.6 Jan/27	3.2	2	Ch - 1	g							RnSrv	0.0%	1715986449
01 01:36:42.9 Jan/27	3.2	2	Ch - 1	g							RnSrv	0.0%	1715986449

Detailed list of recent calls on RnSrv (a reminder that RnSrv is both Control Center and Gateway). RnSrv is a test box running uniform calls of 3.2 second duration every four seconds. Most users will see more variability in this table.

Within the generated table the calls can be filtered based on call type. At the top of the table are buttons with call types on them. When these buttons are green (*Analog* and *Ipvc Voice* in Figure 67) those call types will be displayed in the table. In Figure 67 *Ipvc Data* calls will not be displayed. Clicking these buttons will toggle the call types displayed.

This page is not updated live by the browser. To see calls made since the page was loaded, use the *Refresh* button at the top of the table to refresh the page.

### 5.5.3 ODBC

As noted in earlier in this section on Section 5.5, the database can be accessed via *ODBC*. The *Control Center* supports *ODBC*, or Open DataBase Connection, which enables any computer to access the database of call logs. The documentation of *ODBC* uses the word "server" to describe where the database is. This documentation uses the words *Control Center* to indicate where the server is. To ease confusion, the word *server* is used in this section to describe the *Control Center* (which has the inbuilt database). The gui programs for reading the database use the word *server* to indicate where the database is.

The term *client*, or *client computer* is used to describe the entity which is trying to remotely access the database (which is on the *server*). The client may be any computer that can manage the *ODBC* protocol.

#### 5.5.3.1 Firewalls

If there is a firewall between the *server* and *client computer*, make sure that TCP port 5432 of the firewall is pointed at the *server*. Consequently, all TCP requests that go to the public IP address of the firewall (on port 5432) will be directed to the *server*. In

this way, the *server* will be able to answer ODBC requests that originate from outside of the firewall.

### 5.5.3.2 ODBC Configuration details

These documents will not attempt to explain how to use every *ODBC* program (on every platform) to connect to the database. The parameters which should be used are:

Table 10: *ODBC* configuration details

Parameter	Value	Description
Database name	call_data	Specifies the one possible database
User Name	root	
Description	test	
SSL Mode	disable	no security here
Port	5432	This value was chosen
Password	tlnet	password to the root account on the <i>Control Center</i>
Variable types	PostgreSQL ANSI (which is 0..255)	
Conversion	LF to CR/LF	Required for Linux->windows line feeds
Access level	read only	Any changes could be fatal.

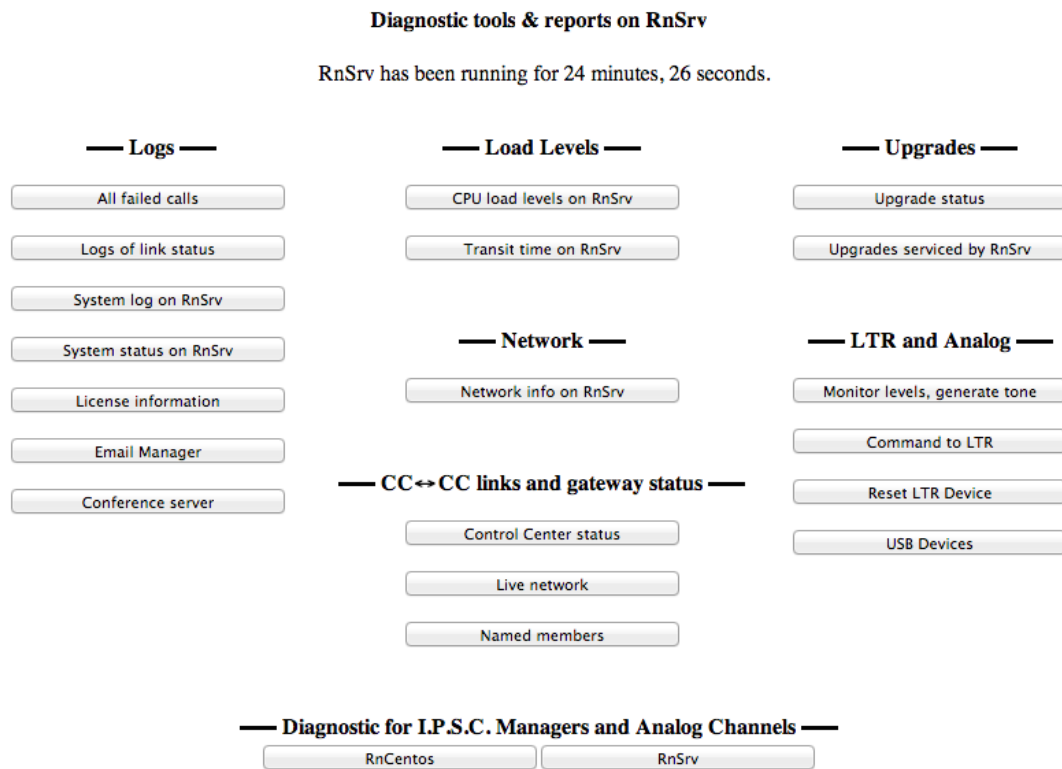
There are two tables in the database. The first table records the calls for today. The second table is much longer, and contains all previous calls. The first call (that is recorded to the database) after midnight causes the transfer of all records to the second table. This summarizes the record of calls and minimizes the cumulative load on the CPU of the *Control Center*

## 5.6 Diagnostics

The *Diagnostics Window* is accessible by those who have *user* and *admin* privileges. It is designed to report information that will help troubleshoot problems.



Figure 68: Diagnostics window



The diagnostics window, which lists the available diagnostic type operations. Also shown are links to the attached Gateways. Consequently, diagnostic type features can be carried out on the remote Gateway through this web interface.

### 5.6.1 Web page login status

Although this is a diagnostics level option, this section is not accessed through the diagnostics window in Figure 68. Instead it is accessed through the button at the very top right of the page, next to the *Log out* button (as described in Section 5.2). This page is restricted to those who have *User* (or higher) access privileges. This section reports the last 50 login/logout events and reports those currently logged in. An example screenshot is shown in Figure 69.

Figure 69: Recent Web Page Login/Out activity and current users

**Web page login status and record on Primary Main**

<b>Current Web sessions</b>			
<b>Name</b>	<b>Access level</b>	<b>Time</b>	<b>Address</b>
rob	user	11:54:20 August 11 2012	10.0.0.61
a	admin	11:41:06 August 11 2012	127.0.0.1

<b>Login/Logout events</b>		
<b>Name</b>	<b>Time</b>	<b>Event</b>
rob	11:54:20 August 11 2012	login
admin	11:53:14 August 11 2012	logout
admin	11:52:38 August 11 2012	login
a	11:41:06 August 11 2012	login

A report on the users who have logged in and out from this system, and the currently logged in users. Note that both tables are in reverse chronological order.

Only when a user clicks the *Log out* button will their session be ended and labelled as a *logout* event. They would then need to re-enter their login details to access the page, which is recorded as a *login*. If they leave their browser open but inactive for ten minutes, or if they close their browser, it will be recorded as a *suspend* event. In this case they could return to their session using the *Continue previous session button* (see Figure 16), which is marked as a *login* event.

Note also the remote address of user *a* is given as *127.0.0.1*. In this case, the *Primary Control Center* was running a graphical session with one displayed browser. Since the browser was running on the *Primary Control Center*, the *Primary Control Center* marked the external address as *127.0.0.1*. Which is another way of saying that the *Primary Control Center* and user *a* are on the same computer.

## 5.6.2 Logs

### 5.6.2.1 All failed calls

This will open the window shown in Figure 70. This option is only available on *Control Centers*, and contains a log of calls that have failed and why they failed. This can be useful in diagnosing why calls go nowhere, or do nothing.

Figure 70: All failed calls



*Menu with different categories of failed calls.*

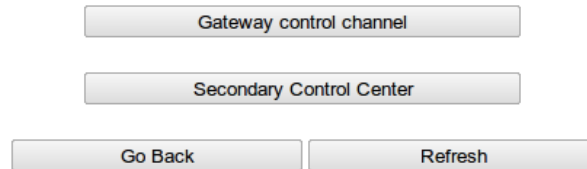
The possible types of errors are separated into five pages, as follows:

- *Ignored B messages* reports on calls that were unable to be placed into a *Bridge Group*. This could occur because of the *Bridge Group* setup, if there is no line matching this call it will not be placed. If there are no other entities in the *Bridge Group* and the radio is making a local call, there will also be an error. If the *Bridge Group* is already in use there will be an error.
- *Unclosed B messages* occur when there was no request to close the call.
- *Conflicting* calls can occur when two calls come in at the same time. They can also happen when a call is setup and goes through to the *Bridge Group* destinations, then another destination tries to join the *Bridge Group* partway through the call.
- *Did not complete* occurs when an end of call message was not received, probably due to a failure at the far end.
- *Recent error calls* provides a list of recent errors. This list can be searched by *sitename*, *Home Repeater*, *Group ID* and date and time. The error messages can provide a hint as to why a call failed to go through.

### 5.6.2.2 Logs of link status

Provides a text record of events that happened to break/establish connections between the *Control Center*, *Secondary Control Center* and *Gateways*. Examination of these logs will show (for example) when the *Primary Control Center* went down and the *Gateways* started using the *Secondary Control Center*. Depending on the endpoint type, different listings will become available. For example, the *Secondary Control Center* will never display a button listing the status of the link to the *Secondary Control Center*. A *Gateway* will display a button listing the status of the link to the *Secondary Control Center*. In Figure 71 there is a sample screenshot taken from the *Primary Control Center*.

Figure 71: Logs of link status

**Logs of control links on Primary Main**

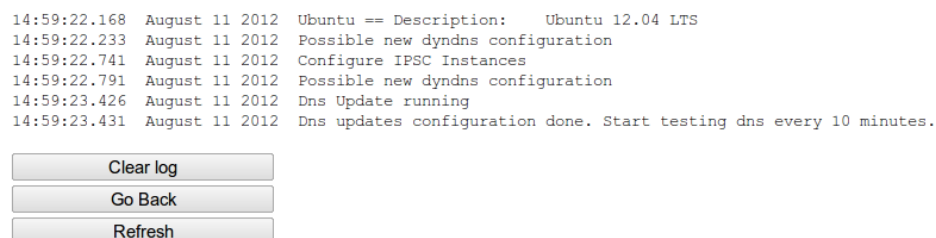
The log of link status, as reported by the Primary Control Center. By clicking the relevant button, the user can access the report on the connection to the Secondary Control Center, or the Gateway Control Channel. The Gateway Control Channel log is the combined report for managing all remote Gateways. In this case, two are reported on.

Refreshing the page will rebuild the display, and any new messages since the last loading of the page will be added to the log.

**5.6.2.3 System log**

Provides a report on miscellaneous items that did not fit elsewhere. Typically, the items in the system log are to do with startup of the system. An example output is shown in Figure 72.

Figure 72: System log on Primary Control Center (Primary Main)

**System log on Primary Main**

Screenshot from a development system (which is running Ubuntu Linux - a normal Control Center runs Centos). The startup messages are recorded - primarily it shows the system has initiated the dynamic DNS update process so that the Control Center can be found by a word address (like examplecc.dyndns.org). At the bottom left, the names of the two attached Gateways is reported.

Two buttons are displayed, Clear log and Go Back. These buttons are described in the text below.

The two buttons in Figure 72 below the log messages are defined as:

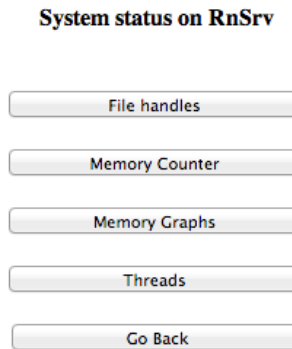
- *Clear log* Remove all the contents of the log - can be useful if the log is long and the page is slow to display.
- *Go Back* Takes the display back to the previous screen.

Refreshing the page causes the display to be rebuilt with the current log. If new messages have been added to this list, this option will show the new messages.

### 5.6.2.4 System status

This is a *Debug* option. For most clients, this will not be present on the *Diagnostics* menu, as it is not relevant for most users. For help with using these options, please contact technical support.

Figure 73: System status



*System status options. This may not be available for use on your system.*

### 5.6.2.5 License information

This page provides a summary of the factory configured settings. The settings reported describe the manner in which this box is configured to run (*Control Center*, *Secondary*, *Gateway*, how many voice channels, etc) and reports the current version of this box. The screenshot in Figure 74 gives a sample of what can be seen.

Figure 74: Report on the license settings

**Current license information on Primary Main**

RnPc	10	max. number of active incoming RnPc instances this control center will manage
RnIpc	10	max. number of active incoming RnIpc instances this control center will manage
Limit Gw Chan	1000	max. number of active gateway channel instances this control center will manage
Srv-Srv	10	max. number of active inbound server-server instances this control center will manage
Control Center	true	if true, this box will act as a primary or secondary control center
Serial No	asdfasdfadf	A string to uniquely identify this installation
Name one	a name	Top line on LCD display
Name two	ame two.	Second line on LCD display

Only nonzero fields are shown

Build Info :: 2012 August 11 13:37:18 SVN Revision:6271

Go Back

*The currently configured license information for this computer. The site name is displayed near the top. It is clear that Primary Main is configured to run as a Control Center, and can support 20 different connections from the PC program. Twenty different (incoming) Control Center ↔ Control Center links can be established. For those instances that run on an embedded box with a LCD display panel, the text on the panel is described here.*

*The particular build number this program is running is reported at the very bottom. This is the same information as is reported in the very top right of the display (see Figure 17).*

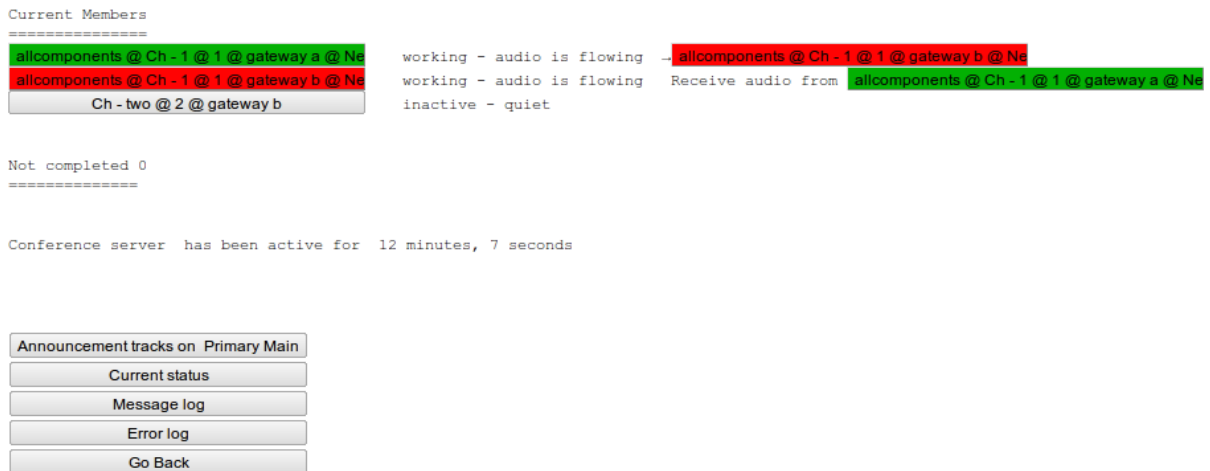
In this figure, the *sitename* of the *Control Center* is at the top of the frame. When this license information is accessed for a *Gateway*, the *sitename* of the *Gateway* will be reported near the top of the screen.

### 5.6.2.6 Email manager

This section provides a report on emails sent by the system because of certain events. This is configured as described in Section 5.4.2.

### 5.6.2.7 Conference Server

This button is only available on a box running as a *Control Center (Primary or Secondary)* and provides access to the "engine" that glues calls together, creates *Control Center Outbound* connections, and handles incoming connection requests. An example screenshot for the *Conference Server* is shown in Figure 75.

Figure 75: Status of the *Conference Server***Status Conference Server on Primary Main**

*Current status of the Conference Server. Only Gateway a, home repeater 1 is currently available. Consequently, calls from Gateway a will go nowhere. The log of messages generated by the Conference Server are available through the message log and error log buttons.*

*Note that there is no mention of the Alternate Control Center here. Clearly, the Alternate Control Center is not attached to this Conference Server*

The *Conference Server*, which is the entity for handling and duplicating voice streams to multiple recipients, provides here a list of available audio circuits. As can be seen from the display, only *Gateway a, home repeater 1* is currently active. The buttons drawn for each active direction may be clicked on to give more information on the relevant connection.

At the bottom of the screenshot in Figure 75 there are five buttons, which are briefly explained here.

1. *Announcement tracks on ...*: The remote PC can put audio files onto this *Control Center*, which can then be configured to play at the beginning of each call. A brief description of the announcement tracks can be found in Section 5.6.2.7.1.
2. *Current status*: Regenerates this window with any new data.
3. *Message log*: The history of text reports generated by the *Conference Server*. This can provide clues as to why remote *Gateways* cannot connect to this server. This report describes when remote entities connect and disconnect.
4. *Error log*: Causes the more serious messages to be displayed. It is useful to check this log if a remote *Gateway* cannot seem to connect to this *Control Center*.
5. *Go Back*: Causes the browser to return to the previously displayed screen.

#### 5.6.2.7.1 Announcement tracks on the *Conference Server*

This is a mechanism that allows a predefined tone (or message) to be played at the beginning of each outgoing call from the *Conference Server*. Alternatively, one may consider the following description. When a call is received from some remote entity (say *Gateway a*), the *Conference Server* duplicates each packet of audio and sends the duplicated packet to each of the designated recipients (who are currently connected to the *Conference Server*). Prior to duplicating the packets of the incoming call, the *Conference Server* sends out the packets of pre recorded message or tone. This announcement track has been preloaded onto the *Conference Server*.

The announcement tracks were loaded from .wav files on a PC, which the PC program (*RnPc*) transferred to the *Conference Server*. The PC program has compressed the raw audio using the current codec on the *Conference Server*. Consequently, the *Conference Server* just sends the file out at the beginning of the call, without having to do any audio compression work (which

saves much CPU time). The currently loaded announcement tracks can be viewed from the *Announcement tracks* button in the *Conference Server* status window (Figure 75). An example screenshot is below in Figure 76.

Figure 76: Announcement tracks on the *Control Center*

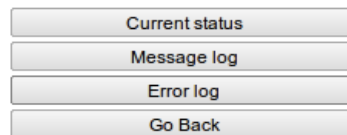
#### Status of Announcement tracks on Primary Main

Current announcements are

SpeexIETFNarrow-24.6k	sample_message.wav
-----------------------	--------------------

Server has loaded in 1 announcement from remote PC client(s)

```
Statistics
=====
active      0
terminated 1
```



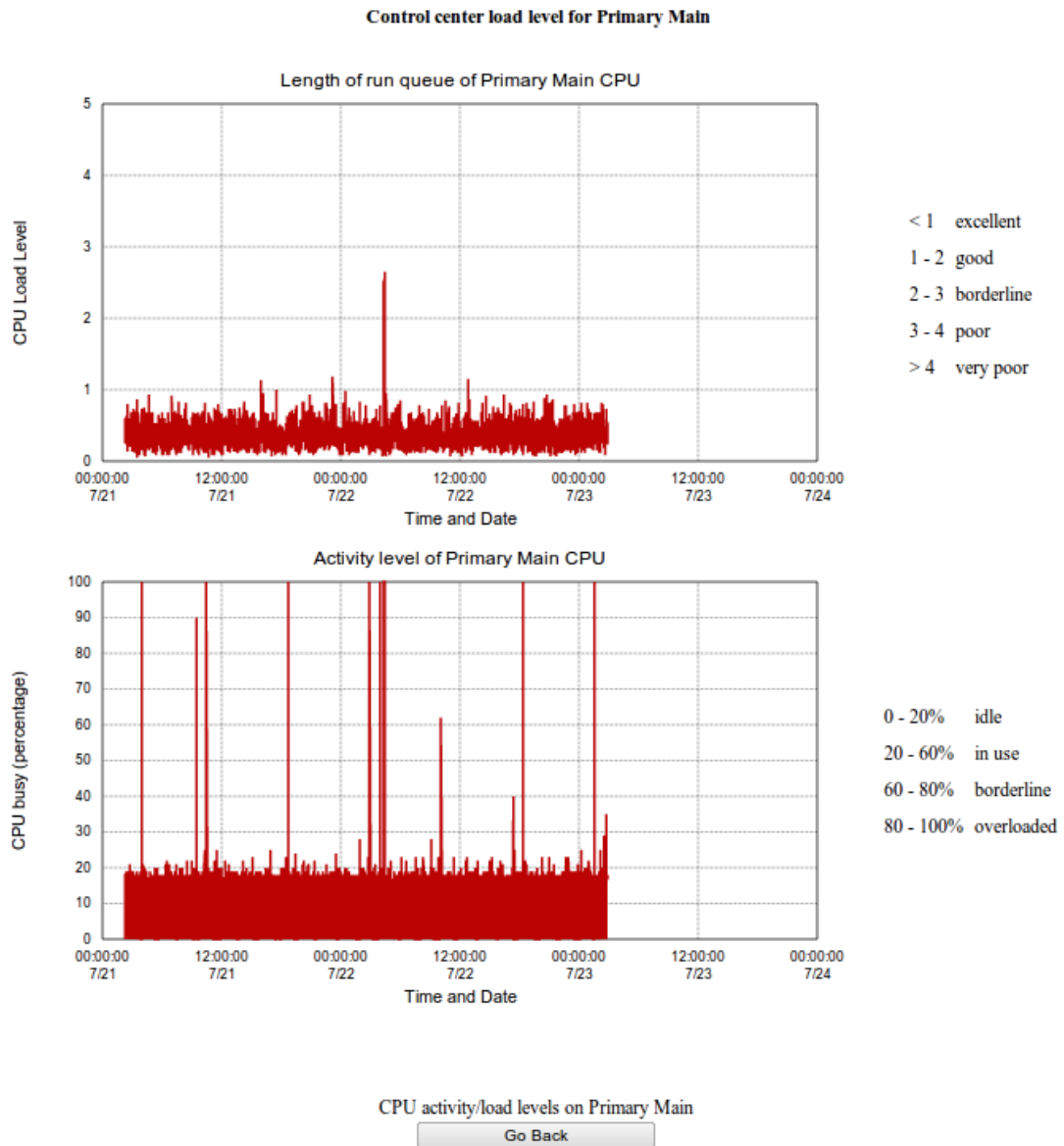
*The report of the current announcement tracks on the Conference Server. There is one track loaded, sample\_message for the Speex 24 codec. The log of operation of the announcement server can be viewed by the relevant buttons, which work the same as everywhere else in this program.*

### 5.6.3 Load levels

#### 5.6.3.1 CPU Load levels

This option creates a page that describes the CPU activity level. The system has a long running process to record the activity levels which runs every two minutes. The CPU busy percentage and load level (a measure of the responsiveness) is recorded. Two days of data is stored. Older data than this is deleted. This data is graphed, which allows the user to see the time history of these variables. A sample graph is provided in Figure 77. The operator may use these graphs to gain an impression of the long term running load on this box. Momentary overloading is acceptable - permanent overloading is bad as it indicates audio quality loss.



Figure 77: CPU busyness report for *Primary Main*

The CPU busyness report for Primary Main. If both graphs reported a high load/usage level, there is probably a problem. In this case, neither graph is excessive, so we conclude the CPU load levels is just fine. Note that this button will always display the site name of the box being considered. In this, the Primary Control Center is being looked at, so the sitename of the Primary Control Center is displayed.

The variables graphed in these two plots are defined as:

- *Run queue length* or CPU load (top graph) is a report that describes how much work is delayed - or how much is waiting to run. Alternatively, this graph reports how much latency the system has. In this graph there is minimal latency.
- *Activity level* or CPU busy percentage is a measure of how often the CPU is idle, doing nothing. This graph reports that *Primary Main* is idle most of the time.

For a large system it may be acceptable to have run queue lengths in the order of 11. These graphs can therefore be somewhat ambiguous. To overcome this, the transit times of the *Conference Server* is provided, as described in Section 5.6.3.2.

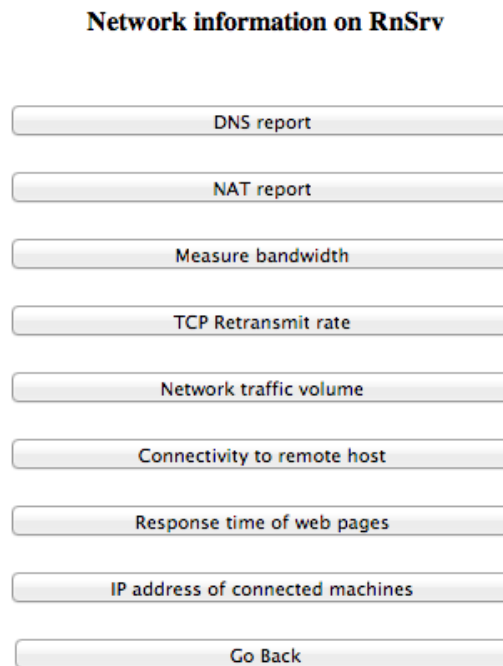
### 5.6.3.2 Transit times

These graphs are provided as a means to unambiguously measure the performance of the *c-Bridge*. The transit time recorded is the time taken for a packet to come in, be received, sent, and go out. In other words, it measures the time delay in the *c-Bridge*. The transit time should always be less than 500 milliseconds. If there is no transcoding it should be less than 100 milliseconds.

### 5.6.4 Network Information

This option generates a window with sub options, that provide a different view of the performance of the internet connection. The generated window is displayed in Figure 78

Figure 78: Network Information Window



*The different options available for examining the status of the network link.*

#### 5.6.4.1 DNS report

This section provides a means to check three common boxes on the network. This includes *www.motorola.com*, *www.rndownload.dyndns.org* (the *Upgrade server*) and *www.dyndns.org*. The page reports on their location, and reports gives a rating of the connection.

Figure 79: DNS report for *Control Center*

```

DNS test for three external sites on RnSrv
02:48:27 January 27 2015
Time required:: 0.572 seconds for DNS test.

Server: 209.18.47.61
Address: 209.18.47.61#53

Non-authoritative answer:
www.motorola.com canonical name = www-ch.motorola.com.edgekey.net.
www-ch.motorola.com.edgekey.net canonical name = www-ch.motorola.com.edgekey.net.globalredir.akadns.net.
www-ch.motorola.com.edgekey.net.globalredir.akadns.net canonical name = e1900.b.akamaiedge.net.
Name: e1900.b.akamaiedge.net
Address: 23.64.119.224

Server: 209.18.47.61
Address: 209.18.47.61#53

Non-authoritative answer:
www.rndownload.dyndns.org canonical name = rndownload.dyndns.org.
Name: rndownload.dyndns.org
Address: 72.45.131.217

Server: 209.18.47.61
Address: 209.18.47.61#53

Non-authoritative answer:
www.dyndns.org canonical name = dyndns.org.
Name: dyndns.org
Address: 204.13.248.116

DNS lookup of three sites took less than 3 seconds. Rating good - unless the above tests aborted early.

```

*The DNS report for the Control Center RnSrv.*

#### 5.6.4.2 NAT report

This provides a report of the public IP address and the type of any NAT/firewall in front of this box. There is a simple check to determine if the NAT has the requisite ports open. Each IPSC has a port associated with it which must be open. Each is tested for correct NAT operation. An example screenshot of the test result is shown in Figure 80. The public IP address of *RnSrv* is shown below the result table.

Figure 80: NAT report for *Control Center***Open ports on RnSrv**

01:50:19 January 8 2015

Time required::2 seconds

Status	Port	Description	#servers tried	Elapsed	Server
RavenNet media supported	42420	<input type="button" value="Open"/>	5	0	stun.ideasip.com
RavenNet media supported	42421	<input type="button" value="Open"/>	1	0	stun.voip.aebc.com
RavenNet media supported	42422	<input type="button" value="Open"/>	2	0	stun1.voiceeclipse.net
RavenNet media supported	42423	<input type="button" value="Open"/>	1	0	stun.voipbuster.com
RavenNet media supported	42424	<input type="button" value="Open"/>	1	0	stun.voxgratia.org
RavenNet media supported	42425	<input type="button" value="Open"/>	2	0	stun.ideasip.com
RavenNet media supported	42426	<input type="button" value="Open"/>	3	0	stun.voipbuster.com
RavenNet media supported	42427	<input type="button" value="Open"/>	1	0	stun.noc.ams-ix.net
RavenNet media supported	42428	<input type="button" value="Open"/>	1	0	stun.voip.aebc.com
RavenNet media supported	42429	<input type="button" value="Open"/>	1	0	stun.voxgratia.org
RavenNet media supported	42430	<input type="button" value="Open"/>	1	0	stun1.voiceeclipse.net

Public address:74.76.122.176

The report on the particular NAT in from of the Control Center with sitename RnSrv. The ports tested (42420..42430) are required to be open for correct operation of the Control Center. Additional details on what the report means can be obtained by clicking the relevant button.

**5.6.4.3 Measure bandwidth**

The measure bandwidth page brings up a selection of hosts where bandwidth can be measured to. Measurement of bandwidth is a 10-15 second test that sends many packets down the link and is therefore a snapshot of the available capacity In Figure 81 there is a sample screen shot of the measure bandwidth window, as generated by the *Control Center*.

Figure 81: Measure Bandwidth Window

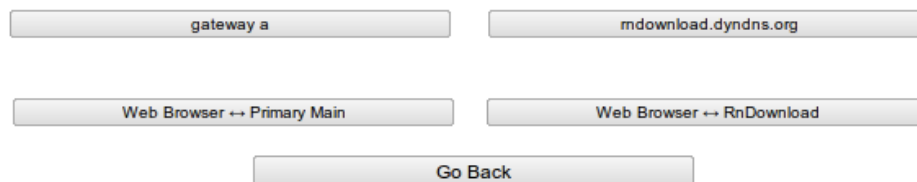
**Bandwidth measurement on Primary Main**

The bandwidth and round trip time test takes 10 seconds to complete. The page will refresh after the test has completed.

This test uses UDP packets which are identical in size to the audio packets. The measured bandwidth is the maximum you can reasonably expect to squeeze down the link. The measured round trip time will be similar to what your audio packets will experience.

There may be a momentary loss of audio packets while the this test runs.

Finally, the measured loss rate will be similar to what you experience with your audio traffic.



*The measure bandwidth window, as generated by the Control Center. Note that it is possible to measure the available bandwidth between the Control Center and a) each Gateway, b) this web browser, and c) the Upgrade Server. Finally, the bandwidth between this web browser and the Upgrade Server can be measured as an aid to diagnosing network issues. When the diagnostic feature of measuring bandwidth is used on a remote Gateway, fewer options are available. In this case, only bandwidth between the Control Center and the remote Gateway can be measured.*

The bandwidth measurement test has two parts. Each test lasts five seconds. Both tests use packets that are identical in size and type to what is used for audio. From this it can be determined what is likely to happen to real audio. The first test is a bandwidth test that floods the link with packets. During this test there may be a loss of audio packets for other users of the *Control Center*. This flood test measures the available capacity of the link. Then, there is a connectivity test which sends a stream of packets at normal audio packet intervals. The percentage of packets that is dropped and the average round trip time is reported. From looking at the final figures, one gets an impression of what the link is like (at the time the test was run).

The bandwidth between this *Control Center* and *rndownload.dyndns.org* is being measured, - a process that takes just over 10 seconds. While the bandwidth is measured, a window similar to Figure 82 is displayed:

Figure 82: Measurement of the bandwidth between the *Control Center* and *rndownload***Bandwidth measured on Primary Main to gateway b**

19:15:39 August 7 2012

Please wait for a few seconds. Testing ... testing ... 10 sec

The bandwidth between *rndownload.dyndns.org* and this *Control Center* is being measured. During the measurement process, a live display (similar to above) is generated. The page normally refreshes every two seconds. If there is a good link between *Control Center* and web browser, the page will update every second.

After the bandwidth has been measured, a display similar to that shown in Figure 83 is generated.

Figure 83: Bandwidth measurement completed

**Bandwidth measured on Primary Main to gateway b**

19:15:40 August 7 2012

Bandwidth: 35.612 Mbps

This link is capable of carrying (at best) 1166 simultaneous calls.

Latency: 0 milliseconds (excellent)

Audio packets take approx. 0 ms to travel from "gateway b" to this control center to "gateway b".  
The latency is excellent.

Drop rate : 0.0% (excellent)

When conveying the packet stream for one audio conversation, 0.0% of the packets were dropped in the network.  
The drop rate is excellent.

## Additional technical info

throughput	test size	Rx 46370 of 46370
	capacity	27.599 Mbps
connectivity	test size	Rx 85 of 85
	round trip time	0.39 / 0.42 / 0.52 ms (min/avg/max)

The bandwidth between *rndownload.dyndns.org* and this *Control Center* has been measured. The process took 11 seconds. The measured bandwidth is 0.4Mbps/sec, which is enough to carry many simultaneous voice calls. Ideally, it is 14 simultaneous voice calls. In practice, it is probably closer to 7 calls. The latency of 300 ms is long (for voice calls) but it will suffice. In this case, the path between the *Control Center* and 4.2.2.2 is through an ADSL modem and across the Pacific Ocean, so a latency of 300ms is very acceptable. The drop rate of nearly 4% is too high for audio calls. However, the audio is not going to be sent over the long path to *rndownload.dyndns.org*.

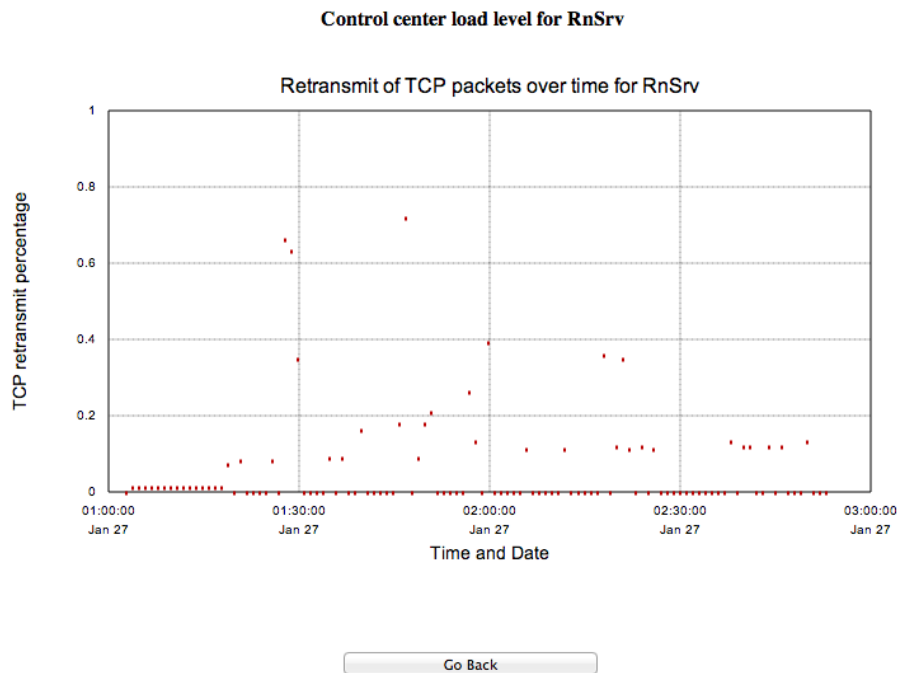
After this graph was taken, the development team were advised not to use 4.2.2.2 as the remote host. It is strongly suggested to use a value like 8.8.8.8.

The measured performance above is not ideal - remote users trying to control this *Control Center* will probably experience slow response times to clicking on web page elements.

#### 5.6.4.4 TCP Retransmit rate

This test gives an indication of the network reliability to users. It is measured by a Linux kernel by sending TCP packets to remote hosts. Ideally, the TCP retransmit rate should be zero, meaning there is no retransmit. However, some slightly higher values below 1% are tolerated.

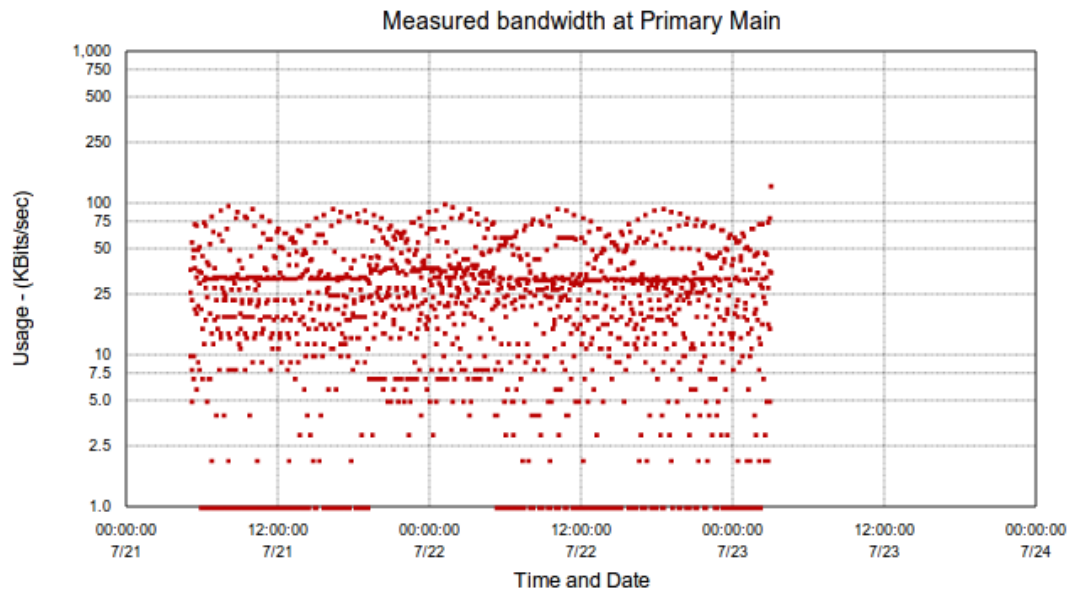
Figure 84: TCP retransmit rate



*TCP retransmit rates for the Control Center RnSrv. The majority of readings are at zero, which is ideal. There are some isolated higher readings, but all are below 1%. This is therefore an acceptable graph.*

#### 5.6.4.5 Network traffic volume

In an effort to track and diagnose audio quality issues, there is an automated process which measures (every two minutes) the bandwidth in the ethernet ports of the computer. Two days of records are available. Older data than this is deleted. This graph is designed to provide evidence for if the computer/network connection is overloaded - which would lead to audio quality issues. A sample graph is provided in Figure 85.

Figure 85: Measured network usage on a *Control Center*

Bandwidth measured at Primary Main

[Go Back](#)

*The measured network usage - which is almost always below 100 kilo bits/sec. Since this box is attached to a 100Mbits/sec LAN, there is no reason for thinking packets might be lost in the network.*

This particular graph was recorded from a two day period, and the usage is several orders of magnitude lower than the capacity of the LAN. For the site *Primary Main*, the network is not overloaded.

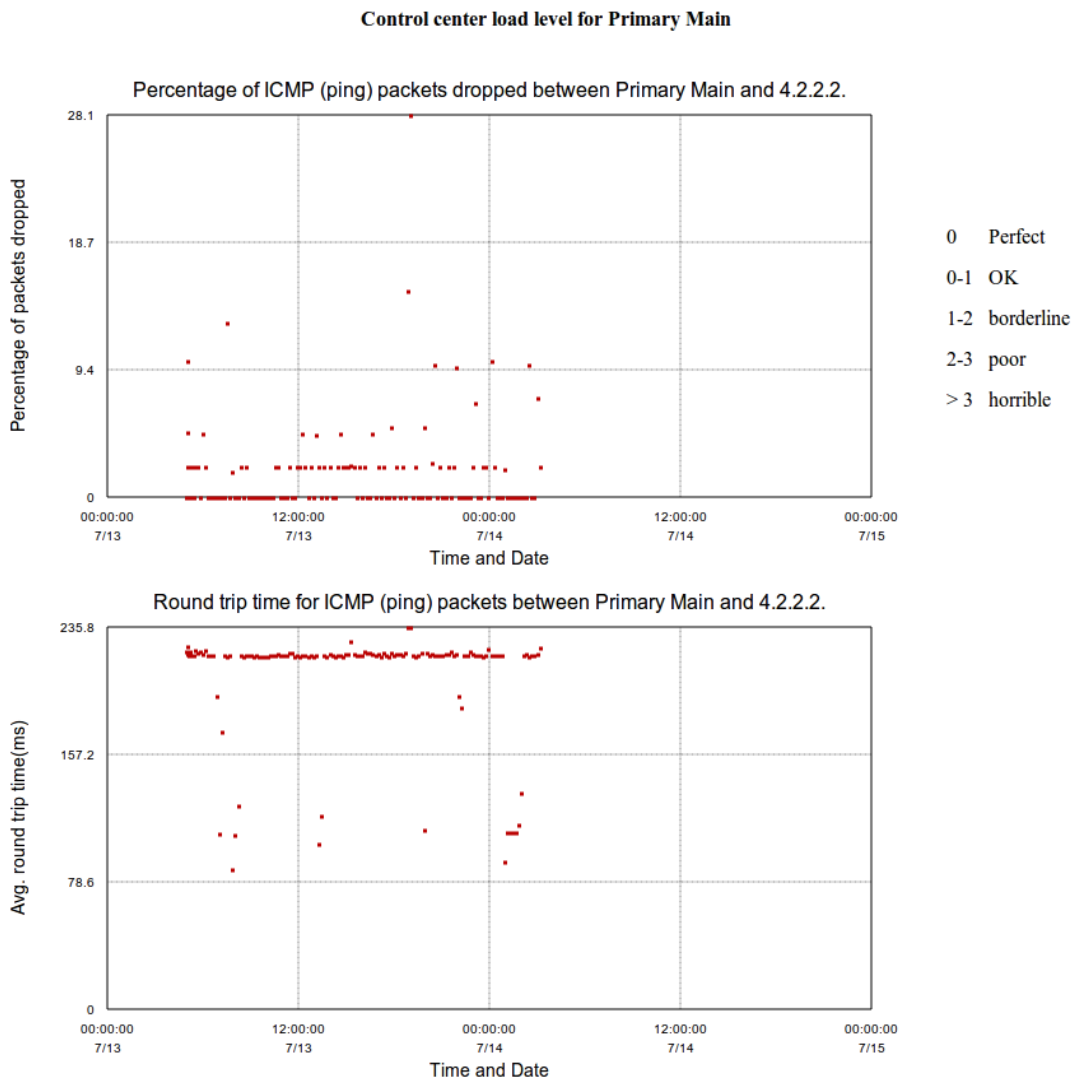
#### 5.6.4.6 Connectivity to remote host

This reports the loss rate and round trip time for ping packets that travel between this computer and remote host. The remote host is configured as described in Section 5.4.4.1. This provides an estimate of the connection of the *Control Center* to an external host. Consequently, some information is available as to whether the web pages will be slow or fast to respond. Furthermore, if there is a high drop rate for packets, one can infer that audio packets will also be dropped, which can suggest an audio quality issue.

An example screenshot, taken over two days of operation is shown in Figure 86.



Figure 86: Example connectivity report with remote host



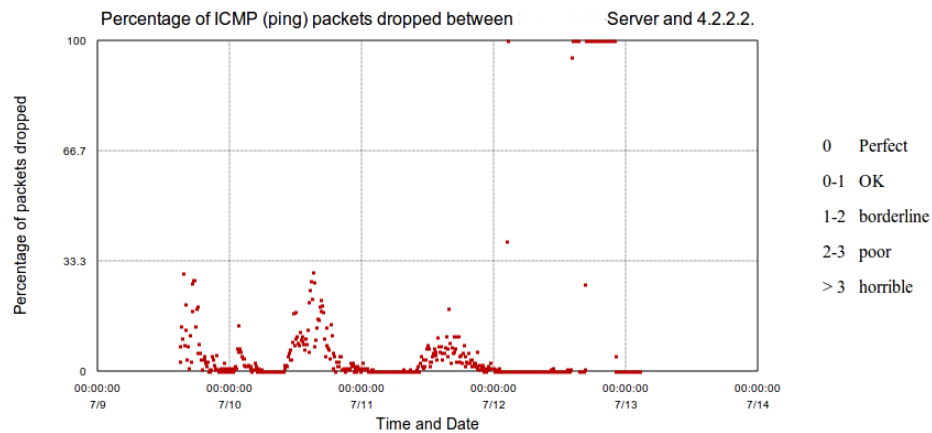
*The report of connectivity between the Primary Control Center and the remote host (4.2.2.2). Almost all of the packets have the same round trip time, which suggest no variation in the route and the link is never saturated. This implies the user will have reasonable audio quality. Several packets have been lost in the network. The cumulative fraction that is lost to the remote host is not reported.*

*This graph was collected on a different day to other graphs in this document. In the last twelve hours before this screenshot was taken, no Gateways were connected. Consequently, there will be no option (at the time this graph was collected) to do diagnostics or configuration on any remote Gateways. The remote Gateways are not available to be examined/changed.*

To be certain how this link is performing, one should also check the connectivity graphs between the *Gateways* and *Control Center* (Section 5.6.5.1).

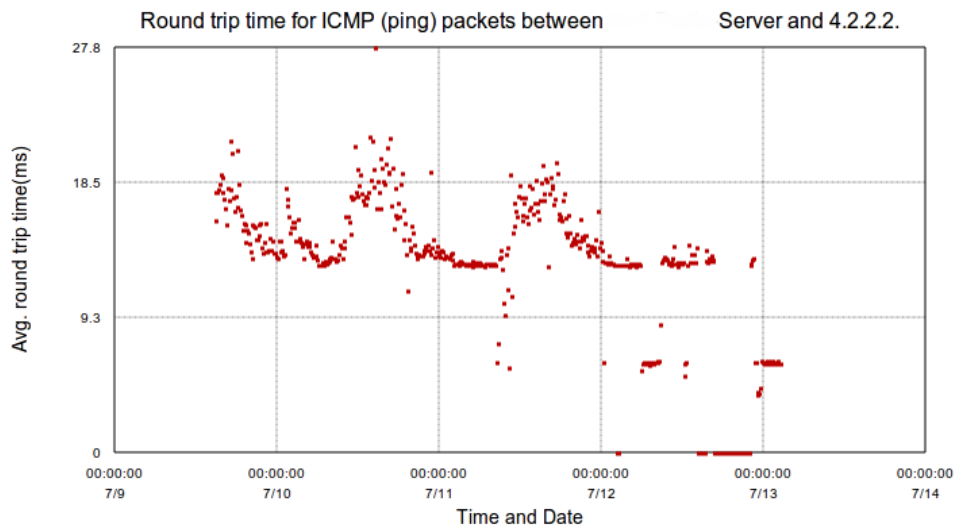
To illustrate the purpose of this feature, consider the graphs in Figure 87 and Figure 88. The data in these graphs was copied from a customer who had a particularly poor network connection. As can be seen from the title of the graphs, the *sitename* of the *Primary Control Center* has been blanked out.

Figure 87: Percentage of packets dropped between the *Control Center* and remote site.



The percentage of packets dropped when communicating with the remote site at 4.2.2.2. Note the daily periodicity in the graph - the drop rate is high during the day, good at night.

Figure 88: Round trip time for packets between the *Control Center* and remote site



The average round trip time for ICMP packets between this *Control Center* and the remote host at 4.2.2.2. The same daily pattern is observed as in Figure 87. Note also that in the last day graphed, there is a period of time when all packets are dropped. During this interval, the Secondary *Control Center* was used to handle calls. When all the packets were dropped, the round trip time is reported as 0ms. Any other value would have been misleading. To not graph the dropped packets gets confusing - one does not know if the test is running if nothing is graphed.

These two graphs illustrate a *Primary Control Center* that is operating with a very poor network connection. The network connection is not correctly handling packets - they are being dropped. Consequently, audio packets will be dropped during periods of peak load.

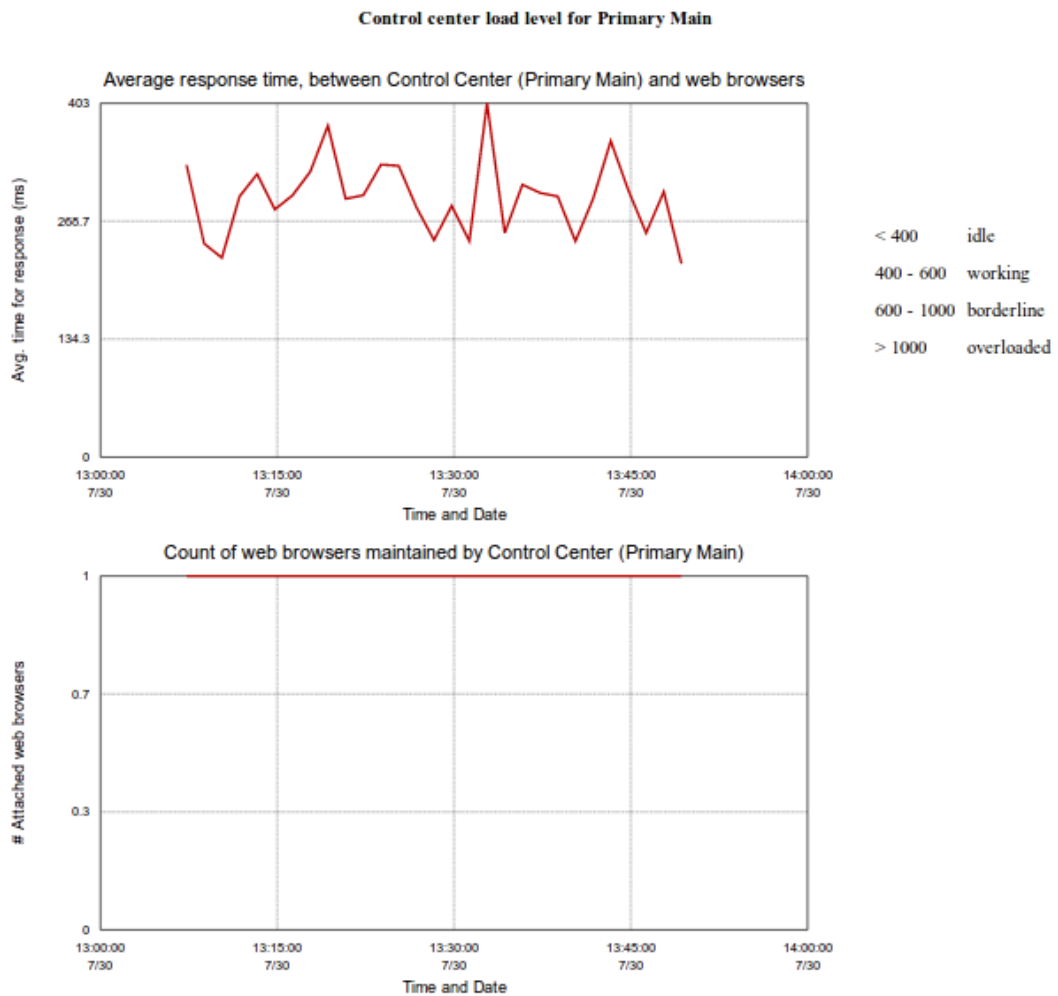
If the drop rate for audio packets is over 5%, then the perceived audio quality is abysmal. The graph here is reporting variable drop rates of between 0 and 40%. For the users of the system, this will lead to frustrating performance. Ideally, the drop rate should be below 1%.

### 5.6.4.7 Response time of web pages

This reports the average roundtrip time for packets between the *Control Center* and all logged in web browsers. Also reported is a count of how many web browsers are attached. This page provides a measure of the responsiveness experienced by users of the web page server.

An example screenshot is displayed in Figure 89.

Figure 89: Response time of web pages



*At the time this graph was captured, the Control Center had been operating for 40 minutes. Simple requests sent from the browser to the Control Center were answered in an average of 300ms, as seen from the top graph. There was 1 browser attached the entire time, which can be seen from the bottom graph.*

Every three seconds, the browser asks the *Control Center* for the count of calls and number of attached *Gateways*. This information is then displayed in the bottom left corner of the screen. The top graph reports the time (measured by the browser) for the request to be sent, processed, and returned back.

In other words, the browser measures the time taken for the *Control Center* to answer a query on how many calls have happened. The time recorded by the browser is passed to the *Control Center* for subsequent display (on this graph). By observation of this graph, we get an idea of the minimum delay the browser will have. It consequently does not measure the time taken to load a web page that has 1 million records.

### 5.6.4.8 IP address of connected machines

This lists the *Gateways* and web browsers attached to this Control Center. The version number of the remote *Gateways* and a reset link button is provided. Displaying the version number quickly shows if the *Gateways* have (or have not) upgraded correctly. The reset link button option will temporarily close the control channel between the *Control Center* and *Gateway*. It will have no effect on voice quality. A sample image of this window is shown in Figure 90.

Figure 90: IP Addresses of connected machines

#### IP addresses of Gateways connected to Primary Main

Site	IP Address	Version Number	Remove site
Alternate	10.0.0.3	6270	Restart
gateway a	10.0.0.63	6270	Restart

#### Current Web sessions

Name	Access level	Time	Address
rob	user	11:54:20 August 11 2012	10.0.0.61
a	admin	11:41:06 August 11 2012	127.0.0.1

Go Back

*The report of the IP addresses of connected machines. One Gateway is listed there (Gateway a). The Alternate Control Center is listed, as it does have a voice connection with the Primary Control Center. Two web browsers have a link, and their IP addresses are shown. The users who have logged in (using the web browser) are shown.*

One username in Figure 90 is quite meaningless - the letter *a*. It is recommended that you use a longer name. A username can be any length.

### 5.6.5 CC↔CC links and gateway status

The pages reported in this section provide different views of the currently linked voice circuits. Two of the pages described in this section show calls happening in real time. This section makes it apparent which connections are active.

Each connection described in this section is one audio circuit which is linked to the *Conference Server*. In other words, this section reports the audio paths that are available right now. In contrast, the *Bridge Group* describes what connections can be joined together (with no regard for if they even exist). The final result of who talks to who is determined by the *Bridge Group* reduced to those who are available (as reported in this section).

When you are setting up your *Bridge Groups*, the pages described in this section should be consulted on a regular basis. Within these pages, you have access to the internal logs of the individual connections and can see the start call/end call commands. When audio is flowing, the name of a *connection* will change. The name reports the *Bridge Group* in use and the descriptive label. The color of the name changes to indicate the direction of audio flow.

The number of links between *Gateways* and *Control Centers* is limited by configuration and hardware capabilities. The reported links in these windows are dynamic, and will change color and name to represent any audio activity.

### 5.6.5.1 Control Center Status

This page reports a table that summarizes the current voice links between the *Gateways* and the *Control Center*, the number of audio packets handled, the loss rate, the calls that have been processed, and buttons to reset/remove links. An example screenshot is shown in Figure 91.

Figure 91: Control Center Status

Label ?	Local link ?	Worst loss rate ?	Received from remote ?	Sent to remote ?	Time since activity ?	Packet loss percentage ?	Calls processed ?	Last call loss rate ?	Reset counters ?	Remove link ?
tomsrv @ 1 @ Giant	<input type="checkbox"/>	100.0%	0	0	27 minutes, 0 seconds	no loss info	0 [0 missed]	0/0 Not avail.	...	...
tomsrvsdfsdfsdf @ 2 @ Giant	<input type="checkbox"/>	100.0%	0	0	27 minutes, 0 seconds	no loss info	0 [0 missed]	0/0 Not avail.	...	...
wxpc @ channel - 1 464.850 REP TX @ 1 @ RnCentos @ Network call	<input type="checkbox"/>		0	22,009	2 seconds	no loss info	413 [0 missed]	0/0 Not avail.	...	...
Ch - 3 @ 3 @ RnCentos	<input type="checkbox"/>		0	0	25 minutes, 10 seconds	no loss info	0 [0 missed]	0/0 Not avail.	...	...
Glenview - Ch 2 @ 6 @ RnCentos	<input type="checkbox"/>		0	0	25 minutes, 16 seconds	no loss info	0 [0 missed]	0/0 Not avail.	...	...
Ch - 5 @ 15 @ RnCentos	<input type="checkbox"/>		0	0	25 minutes, 20 seconds	no loss info	0 [0 missed]	0/0 Not avail.	...	...
Ch - 2 @ 16 @ RnCentos	<input type="checkbox"/>		0	0	25 minutes, 23 seconds	no loss info	0 [0 missed]	0/0 Not avail.	...	...
Channel 8 name @ 20 @ RnCentos	<input type="checkbox"/>		0	0	25 minutes, 13 seconds	no loss info	0 [0 missed]	0/0 Not avail.	...	...
wxpc @ Ch - 1 @ 2 @ RnSrv @ Network call	<input type="checkbox"/>		23,982	0	2 seconds	0.0% loss	450 [37 missed]	0/54 0.0%	...	...

Statistics and information on the voice circuits currently connected to the Control Center. The number of audio packets that have been sent to/received from the remote site is shown. The last line is green, which indicates that (from the view of the Control Center) this is the originator of the call - at this point the call comes into the Control Center. There is a link to this channel (as seen by the conference center), which is the local link.

Note that all the audio activity is in one direction. It is received from Ch-1 of RnSrv and sent to Ch-1 of RnCentos. All the voice circuits in black have been idle.

For links that have been very active, the user may wish to reset the counters so that the numbers are smaller and more meaningful. In this case, use the relevant button.

A more thorough reset of the counters is achieved by resetting the link. Within seconds the retry mechanism on the Gateway will restore the link.

Observe the top two lines, which describe two CC↔CC links to remote installation with a sitename of Giant. There have been no calls on these links. However, the inbuilt loss detection mechanism has endeavored to send voice packets over the link. All of the packets sent were lost. The inbuilt loss detection mechanism stores its data in a form suitable for review - click on the button in the Worst loss rate column. You will see this button is red (angry - all data is lost).

Note that Figure 91 does not auto update, nor does it show a log of previous events. Consequently, Figure 91 must be regarded as a "snapshot" of activity on the Conference Server. Figure 91 display shows the activity of the voice circuits in the Control Center, so it is therefore a report of the current state of the Conference Server.

The name of one voice circuit could be: *Ch - 3 @ 3 @ RnCentos*. This name consists of four noteworthy items:

1. The *Channel Name* is a term that has meaning to the operators and describes the nature of one channel on the *Gateway*.
2. The *home repeater* is a numeric value assigned to one channel on the *Gateway*. This value is used in the TL-Net system. This value is used in the *Conference Server* to distinguish between two channels from one site.
3. The *sitename* is a term that has meaning to the operator and will (ideally) describe the physical location of the *Gateway*.
4. Black text, which means no current activity

When a voice circuit is carrying audio data, the text and color displayed indicate current status. From the example in Figure 91 there is an entry which is

*wxpc @ Ch - 1 @ 2 @ RnSrv @ Network call*

This name contains six noteworthy elements:

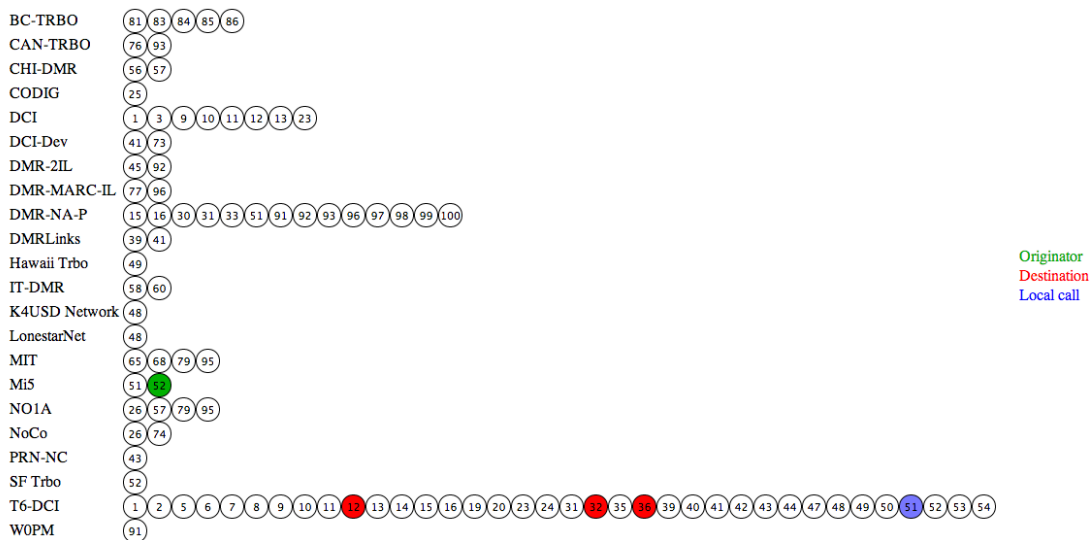
1. *wxpc* is the name of the *Bridge Group* this call belongs to. All entries in this table with this *Bridge Group* name will share the same audio stream.
2. A *Channel Name* of *Ch - 1*.
3. The *home repeater* is 2.
4. The *sitename* is *RnSrv*.
5. The word *Network call* which indicates this is a call that goes through the *Control Center*.
6. Green text, which means this circuit is originating a call into this *Control Center*.

In Figure 91 both *tornsrv @ 1 @ Giant* and *tornsrvsdfsdfsdfsdf @ 2 @ Giant* report a worst loss rate of 100.0%. Clicking these red buttons will take the user to a page with two graphs showing the loss rate and round trip time for this audio connection. These are similar to the graphs reported under *Connectivity to remote host* (Section 5.6.4.6).

### 5.6.5.2 Live network

This option provides a succinct live graphical display of the active/inactive voice links between the *Control Center* and *Gateways*. The display refreshes automatically. Also displayed is the voice links between *Control Centers*. An example screenshot is shown in Figure 92.

Figure 92: Live network window



A live display of the state of the current voice circuits, the home repeater numbers (or Link IDs) shown inside the circles and the relevant sitenames, shown in the column to the left.

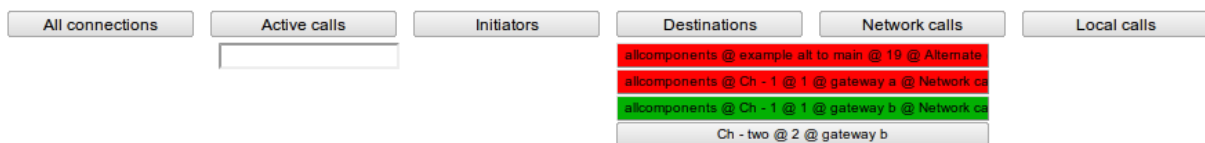
In this figure, the link between Mi5 and home repeater 52 is sending a call to the Control Center, and so is colored green. This call is passed on to three endpoints, which are colored red. There is also a local call occurring at sitename T6-DCI and home repeater 51. The system can cope with many concurrent calls, so this page may have several green circles and many red circles, in addition to blue circles.

The display shows the activity of the voice circuits in the *Control Center*, so it is therefore the behavior of the *Conference Server*. A user with *Low User* privileges will be able to access this display through a *Live Network* button in the navigation bar on the left of the page. They do not have access to other *Diagnostics* level functions.

### 5.6.5.3 Named members

This page provides a live display of both the calls that come into (or leave) the *Control Center* and the voice links to the remote *Gateways*. The display refreshes automatically as an aid to the user. An example screenshot is shown in Figure 93

Figure 93: Named Members window



A live listing of the voice circuits currently connected to the *Control Center*. The list can be shortened by entering text in the clear rectangle on the top left. Only entries that match the text will be reported. In the same manner, by selecting one/some of the buttons at the top of the screen, the list will be shortened to match only the selected buttons.

The display shows the current activity of the voice circuits in the *Control Center*, so it is therefore the behavior of the *Conference Server*. The status of the *Conference Server* can be viewed in Figure 91. Left clicking on one particular entry (say *Ch - 2 @ 12 @ gateway a*) will take the page to examine the status of this particular voice connection.

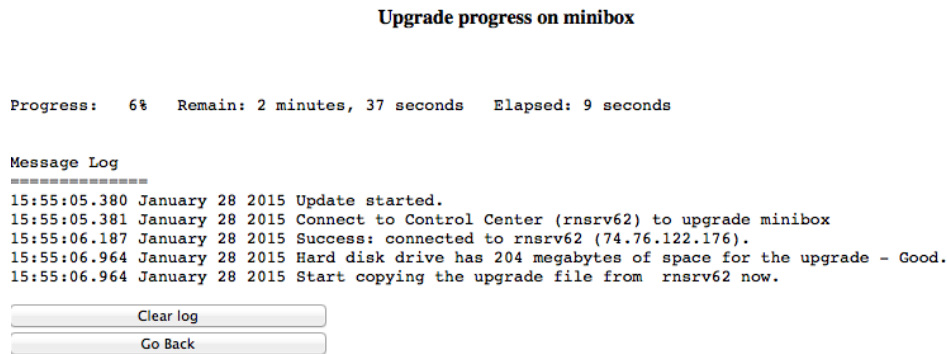
Using the buttons at the top of the page will narrow the list down to only the specified calls. Clicking the *Active calls* button, for example, will cause the page to only list calls that are currently active. In Figure 93 we would not see the entry *Ch - two @ 2 @ gateway b*. To return to viewing all entries, click *All connections*. A string can also be entered in the text box to only select matching entries, further shortening the displayed list. If, in Figure 93, we had selected *Active calls* and then typed in *gateway b* we would then only see the entry *allcomponents @ Ch - 1 @ 1 @ gateway b @ Network calls*. This feature is useful if we are only interested in, for example, a specific *Bridge Group* or *sitename*.

## 5.6.6 Upgrade diagnostics

### 5.6.6.1 Upgrade status

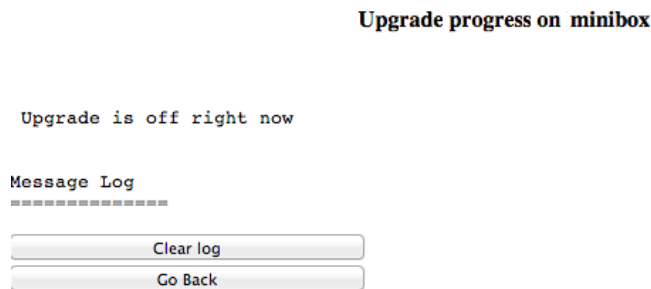
This page is useful while an upgrade is running. It will give an indication of the progress of the upgrade, and report any issues with disk space, network traffic, and the source upgrade file. Figure 94 shows what this page looks like during an upgrade, Figure 95 shows what this page will look like while there is no current upgrade.

Figure 94: Upgrade status during an upgrade



*Report on upgrade progress during an upgrade on the Control Center Minibox. Here, RnSrv is the Upgrade Server. At this point in the upgrade the files are being transferred across from RnSrv to Minibox. Restarting Minibox now would be okay, and would cancel the upgrade. Once Minibox starts updating, powering down may cause significant damage.*

Figure 95: Upgrade status during an upgrade



*Upgrade status page when no upgrades are currently active. There will be no messages to display.*

### 5.6.6.2 Upgrades serviced by *Control Center*

This is a report of which boxes this *Control Center* has sent upgrades to. Perusal of the logs does show if a remote *Gateway* had trouble getting the upgrade image down (which could indicate a network issue). Multiple attempts from the same box normally indicate an error. If the *Control Center* is being upgraded, there will be a live report at the top panel of the web page with the estimated time remaining. Consider the screenshot in Figure 96, which shows the upgrades serviced by *RnSrv*.



Figure 96: Upgrades serviced by *RnSrv*

**Status of upgrades provided on RnSrv**

Current Upgrades  
 =====  
 There are no current upgrades

Completed Upgrades  
 =====

Remote Gateway	Duration	Completed at
RnCentos (74.76.113.143) x86	1 second	22:27:10 January 30 2015

Statistics  
 =====  
 active 0  
 completed 1

The upgrades serviced by the Primary Control Center. The list clearly shows that the remote box at 74.76.113.143 has brought down 1 upgrade image. The upgrade was downloaded in one second, which is typical for when both boxes are the on the same local area network.

Multiple attempts from the same remote box normally indicate an error. The exact error can be determined by examining the logs at the upgrading machine, or at the machine providing the upgrade.

Note too the architecture, which is reported in the leftmost column. It is an x86 machine. Other possibilities are cb (cubieboard) and 64b for a 64 bit machine.

The buttons at the bottom of Figure 96 allow one to see the log of events, clear the log of events, and see the log of error events on the *Upgrade Server*. For brevity, only one screen shot is shown, the log of events in Figure 97.

Figure 97: Message log on *Upgrade Server*

**Messages of upgrades provided on RnSrv**

```

22:26:58.073 January 30 2015 Construct handler for Update and Time Service
22:27:06.839 January 30 2015 Completed reading of the upgrade file "/root/rnds_8368_January_31_2015_10.57.5". Provide it now to all requesters.
22:27:07.483 January 30 2015 Completed reading of the upgrade file "/root/cb_rnds_8368_January_31_2015_10.57.5". Provide it now to all requesters.
22:27:08.813 January 30 2015 Completed reading of the upgrade file "/root/64b_rnds_8368_January_31_2015_10.57.5". Provide it now to all requesters.
22:27:09.104 January 30 2015 Request from cpe-74-76-113-143.nycap.res.rr.com
22:27:09.191 January 30 2015 Update and Time Service of RnCentos (74.76.113.143) x86 commences now.
22:27:10.785 January 30 2015 RnCentos (74.76.113.143) x86 [duration 1 second] is terminated.
22:27:59.598 January 30 2015 Add request from cpe-74-76-113-143.nycap.res.rr.com
22:27:59.604 January 30 2015 Answer time request from rnsrv62.dyndns.org (74.76.113.143).
22:28:02.581 January 30 2015
22:31:14.095 January 30 2015 Add request from cpe-74-76-113-143.nycap.res.rr.com
22:31:14.095 January 30 2015 Answer time request from rnsrv62.dyndns.org (74.76.113.143).
22:31:17.100 January 30 2015
  
```

The log of events on the Upgrade Server. There are no warning type messages here - it appears from the point of this Upgrade Server (which is part of a Control Center) that each upgrade worked correctly. An upgrade over the public internet may takes as long at 10 minutes, but an upgrade is normally around 1-2 minutes.

## 5.6.7 LTR and Analog

### 5.6.7.1 Monitor levels, generate tone

Use the buttons in this window to create sound to go out to the radio, from which you can adjust levels here to get the right volume. Alternatively, record incoming sound from the radio and adjust levels appropriately. Once the desired levels are found,

the system will use these values in subsequent radio calls.

Figure 98: Monitor levels, generate tone

**Audio Levels. Monitoring and 1khz test tone on RnSrv**



*Caption text*

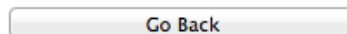
### 5.6.7.2 Command to LTR

Gives the user a chance to do system related work on a LTR (analog) radio system. Consult technical support for advice.

Figure 99: Command to LTR

**Alter LTR components on RnSrv**

Command To LTR has been sent



*Caption text*

### 5.6.7.3 Reset LTR

Gives the user a chance to do system related work on a LTR (analog) radio system. From time to time, the external LTR related hardware can be "scrambled" by external events. This particular command will reset the LTR system and is equivalent to a power off event.

Figure 100: Reset LTR

**Alter LTR components on RnSrv**

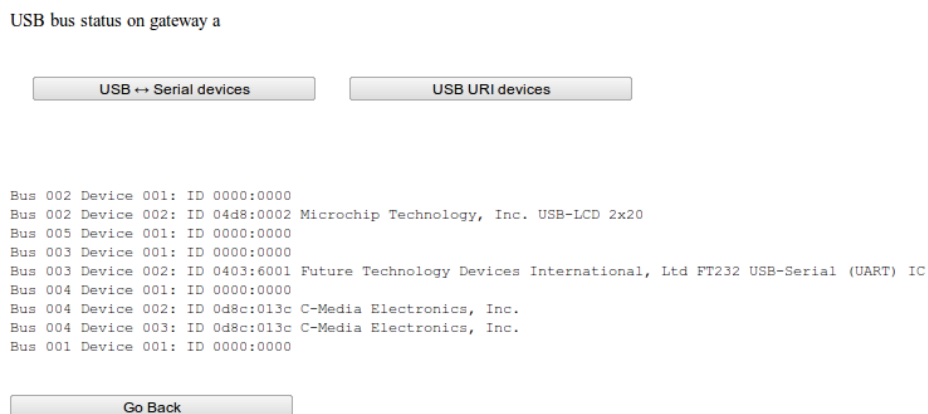
Reset has been sent to the LTR device


 A screenshot of a software interface showing a single button labeled "Go Back". The button is rectangular with rounded corners and a light gray background.

Caption text

**5.6.7.4 USB devices**

USB devices are optionally connected to the *Gateways* to provide audio collection/generation, serial interfaces, and compression/expansion of audio data packets. This page reports on the available devices, status, and log of operation. USB devices can be attached to the *Control Center* and/or *Gateway*. They are detected at program startup and are configured for use at that stage. Inserting a USB device into the computer after bootup is pointless, as the device will not be detected. Conversely, removing a device after the program has started will probably cause the program to stop operation immediately. It will reset itself, and should be operational within 30 seconds. This section describes the different diagnostic reports available. The main window for information on the USB devices available is shown in Figure 101, which reports the USB devices available on *Gateway a*.

Figure 101: All USB devices attached to *Gateway a*

*The contents of the USB bus on Gateway a. This report could have been run on Primary Main, but for the computers used in these docs, the Primary Control Center has an empty USB device list.*

The report in Figure 101 includes a reference to a *Microchip Technology, Inc. USB-LCD 2x20*. This refers to the LCD display on the front of the host computer. Many of the devices that run this program have this LCD display. Its presence (or not) has no influence on the reliability of this program.

From the picture in Figure 101, two USB URI devices are there (they show up as *C-Media* devices on this report). Additional information on these USB URI devices can be found in the following sections.

Figure 101 mentions a Future Technologies device. This is a very generic term for some device on a USB bus. In this particular case, it refers to a DVSI AMBE audio codec. Additional information on this device is found in the following sections.

### 5.6.7.4.1 USB URI devices

The report on the USB URI devices is obtained by pressing the *USB URI devices* button from Figure 101. An example screenshot is shown below, in Figure 102.

Figure 102: Report on available USB URI devices

**USB URI devices on gateway a**

Dir name	File name	Sound card	Channel number	Report
004	002	0	2	<input type="button" value="System report on device"/>
004	003	1	1	<input type="button" value="System report on device"/>

*The report on available USB URI devices. Note, this report provides the same information as from Figure 53.*

This section is useful, as it provides absolute confirmation that the system has detected, recognized, configured, and enabled some USB URI devices. If more devices are plugged in than are reported, there is a problem.

### 5.6.7.4.2 USB -- Serial devices

These entities connect the USB socket on the host computer with an external entity. The external entity may be an audio codec, as shown in Figure 103. Alternatively, the external entity may be the TL-Net controller. An example screenshot for this section is given in Figure 103 which shows one connected DVSI AMBE codec.

Figure 103: Report on USB -- Serial devices

**USB ↔ serial devices on the USB bus of gateway a**

AMBE codec	AMBE3000F V120.E100.XXXX.C106.G514.R007.A0030608.C0020208 A700eeNA	Enc I.P.S.C. 1 Dec I.P.S.C. 1	(11.55 11.92 11.97 11.97 11.97)ms Range: 11.55 - 12.25 ms (10.74 10.78 10.91 10.91 0.00)ms Range: 10.74 - 10.91 ms	<input type="button" value="System report"/>
------------	--	----------------------------------	---	--

*A report on the attached DVSI AMBE device. It is configured for use for channel 1 (for encode and decode). The serial device and manufacturer ID string are reported.*

For correct operation of the DVSI AMBE device, it must be able to encode and decode audio in under 15ms. If it takes longer than 20ms, which happens if the device is plugged into a USB 1 socket, the audio quality will be bad. As an aid to diagnosing conversion issues, the program tests every DVSI AMBE device for conversion speed. The conversion speed is measured when the program starts and is reported in Figure 103. It is expected that if there are DVSI AMBE devices, the user will have checked their conversion speed is under 15ms.

### 5.6.8 Diagnostic on Gateway

Clicking on the buttons at the bottom of Figure 68 with the *sitename* of a Gateway takes the web page to the diagnostic page on the remote Gateway box. The diagnostic page there is similar to this page. Note that the Gateway's *sitename* is listed at the top of the page. There is no report option for Upgrades serviced by the Gateway. There is no reporting on all failed calls, *Conference Server* or *Control Center* links. In Figure 104 there is an example screenshot of how this looks, taken for *RnCentos*.

Figure 104: Diagnostic on a remote Gateway

**Diagnostic tools & reports on RnCentos**

RnCentos has been running for 19 hours, 30 minutes.

**— Logs —**

System log on RnCentos

System status on RnCentos

License information

Email Manager

**— Load Levels —**

CPU load levels on RnCentos

Transit time on RnCentos

**— Network —**

Network info on RnCentos

**— LTR and Analog —**

Monitor levels, generate tone

Command to LTR

Reset LTR Device

USB Devices

**— Gateway channel information —**

channel - 1 464.850 REP TX	HR #1
Ch - 2	HR #16
Ch - 3	HR #3
ch 4	HR #4
Ch - 5	HR #15
Glenview - Ch 2	HR #6
Channel 7	HR #7
Channel 8 name	HR #20
Radio over IP Channel 9	HR #9
<b>I.P.S.C. Manager</b>	
Manager (I.P.S.C. 1 + 2)	1 Silent
Serial device	
Network Sound	

Time Slot 1

rncentos IP 1 ● Link ID #1

Time Slot 2

rncentos ip 2 ● Link ID #2

The diagnostics image, taken for RnCentos. Note that the name of the remote Gateway is displayed at the very top of the working area, which is immediately below the title bar. Immediately below the gateway's name is the time this Gateway has been operating, which can be different to how long the Control Center has been running. The duration that the Gateway has been running provides clues as to the stability and reliability of this program. Further, the button for displaying the load levels reports the name of the remote Gateway.

### 5.6.8.1 Scan for Hoot-n-Holler devices

This is used on *Gateways* when a custom piece of external hardware is available. If the name means nothing to you then ignore this button.

### 5.6.8.2 Logs

#### 5.6.8.2.1 System log

As for a *Control Center* (described in Section 5.6.2.3), this is a report on messages that did not fit elsewhere, mostly concerning the startup of the box.

#### 5.6.8.2.2 System status

This is a debug option which is not used on most customer systems. See technical support for more help and information.

#### 5.6.8.2.3 License information

Functions in approximately the same manner as for a *Control Center*, as described in Section 5.6.2.5. However, there is no license information for the *Control Center* or the limit of *Gateway* channels, as neither is relevant to a *Gateway*.

#### 5.6.8.2.4 Email manager

Functions in the same manner as for a *Control Center*, as described in Section 5.6.2.6.

### 5.6.8.3 Load levels on *Gateway*

#### 5.6.8.3.1 CPU load levels on *Gateway*

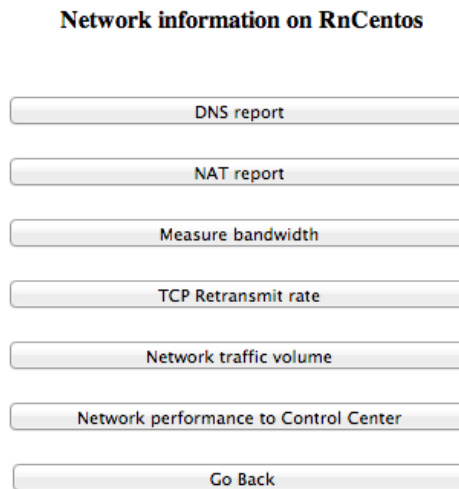
This page produces two graphs indicating the load level on the box. This is essentially identical to a *Control Center*, as described in Section 5.6.3.

#### 5.6.8.3.2 Transit time on *Gateway*

This is essentially identical to a *Control Center*, as described in Section 5.6.3.2.

### 5.6.8.4 Network Information

This option generates the screen shown in Figure 105 when run on a remote *Gateway*. In this case, where the user is looking at *Network information* on a *Gateway*, only options relevant to a *Gateway* are available. An example of this is shown in Figure 105.

Figure 105: Network Information Window for a *Gateway*

The diagnostics, network information page as shown on a *Gateway*. The gateway's name is on the page near the top of the screen.

Comparing Figure 78 and Figure 105 several differences are apparent. Several fields are not visible: *Connectivity to remote host*, *Response time of web pages*, and *IP address of connected machines* as the *Gateway* never has a connection to any of these entities.

#### 5.6.8.4.1 DNS report

Just as for a *Control Center* (see Section 5.6.4.1), this tests the connection and location of three key boxes.

#### 5.6.8.4.2 NAT report

Is essentially unchanged from Section 5.6.4.2. It is only the *Control Center* that must have open ports, which means that the *Gateway* can establish a link to the *Control Center*. This report does describe the status of the NAT which can have an influence on *I.P.S.C.* connections (used for Motorola digital radios).

The system checks the status of this computer. If any ports are required to be open (such as when this box is running as an *I.P.S.C.* Master peer, these ports on the NAT are checked for being open.

When this test runs, all *Gateway* channels on this box are temporarily closed down. This means that the test can examine ports that were in use by the *Gateway* channels.

#### 5.6.8.4.3 Measure bandwidth

Provides fewer options to that listed in Section 5.6.4.3. The user may only measure the available bandwidth (throughput and drop rate) between the *Gateway* running this test and the *Control Center*. An example screenshot is shown in Figure 106.

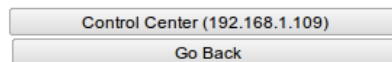
Figure 106: *Gateway* initiated measurement of bandwidth**Bandwidth measurement on gateway a**

The bandwidth and round trip time test takes 10 seconds to complete. The page will refresh after the test has completed.

This test uses UDP packets which are identical in size to the audio packets. The measured bandwidth is the maximum you can reasonably expect to squeeze down the link. The measured round trip time will be similar to what your audio packets will experience.

There may be a momentary loss of audio packets while the this test runs.

Finally, the measured loss rate will be similar to what you experience with your audio traffic.



*A Gateway is about to initiate the process of measuring the bandwidth. Since a Gateway only connects to the Control Center, there is only one place that a Gateway needs to measure the bandwidth to.*

**5.6.8.4.4 TCP Retransmit rate**

This indicates how reliable the network is. It works in the same manner as for a *Control Center*, described in Section 5.6.4.4.

**5.6.8.4.5 Network traffic volume**

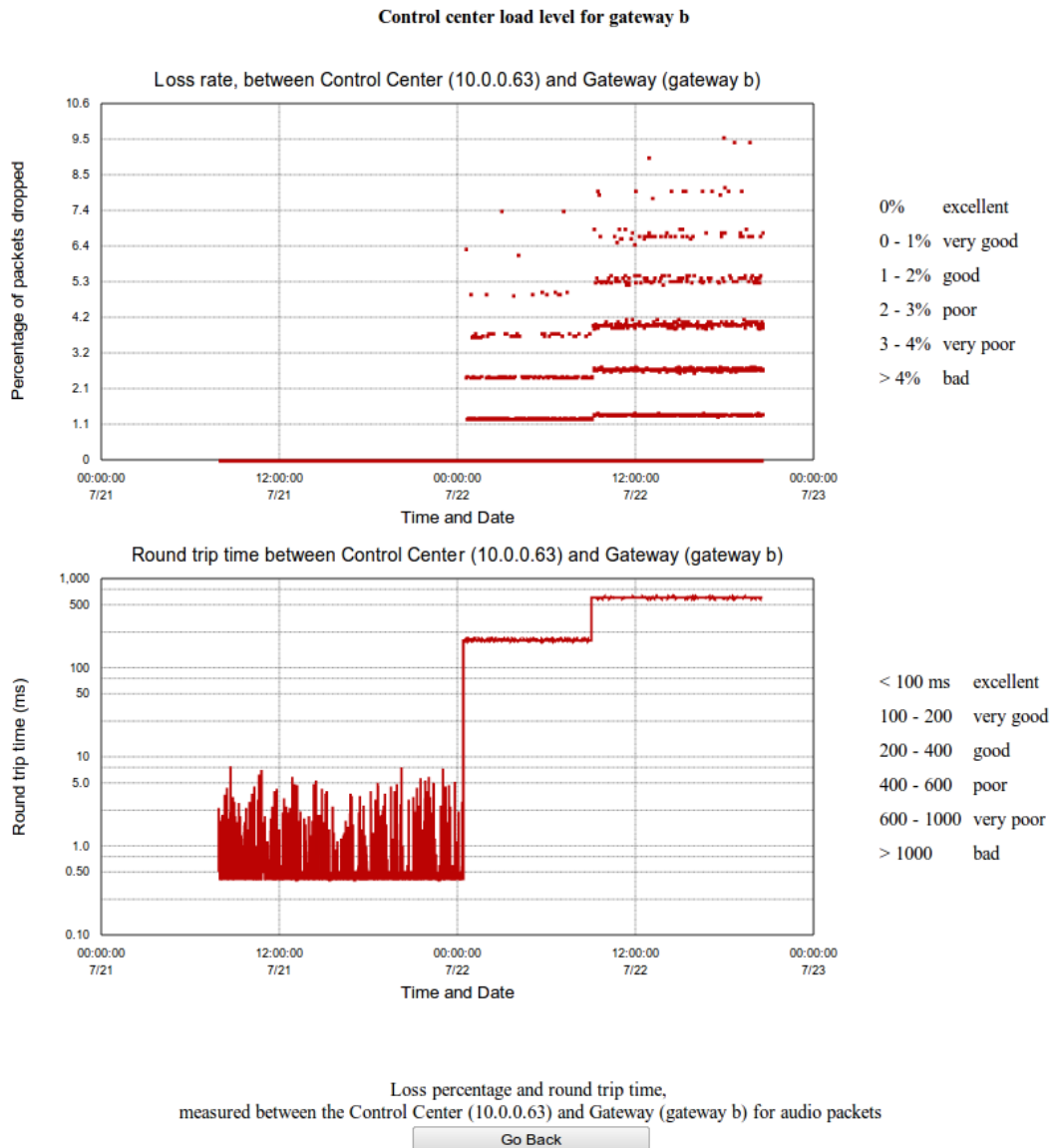
Just as for a *Control Center*, this graph indicates whether overloading of the computer/network is a problem. See Section 5.6.4.5 for more detail.

**5.6.8.4.6 Network performance to *Control Center***

Generates a graph that reports the long term results of connectivity between the remote *Gateway* and the *Control Center*. The name of the *Gateway* is reported at the top of the screen. An interesting graph is reported in Figure 107.



Figure 107: Network performance between Gateway a and Primary Control Center



The measured performance of the network between Gateway b and the Primary Control Center. Note that the bottom graph uses a logarithmic scale to describe the round trip times. There are three distinctly different periods in this graph, where the performance is perfect, borderline, and abysmal.

Note that the bottom graph uses a logarithmic scale to describe the round trip times. A cursory inspection suggests that the variation in the round trip time for the first period in the graph contains wild variations. However, the magnitude of these variations is less than 10ms, so the variation is actually very minor. The drop rate in the second and third period does get quite high, which suggests a voice quality issue. There is no voice quality issue in the first period.

This long running network performance test examines the link for connectivity for all the time that the Gateway is active. This test will never saturate the link between the Control Center and Gateway with data.

To summarize the data shown in Figure 107, it falls into three periods:

1. 18 hours long, round trip times 0.4-7.5ms, loss rate 0.0%. Excellent network conditions. Voice quality will be near perfect
2. 10 hours long, round trip times 400ms, loss rate 0-2%. There are a few data points over 2% loss rate - these are the exception so can be ignored.

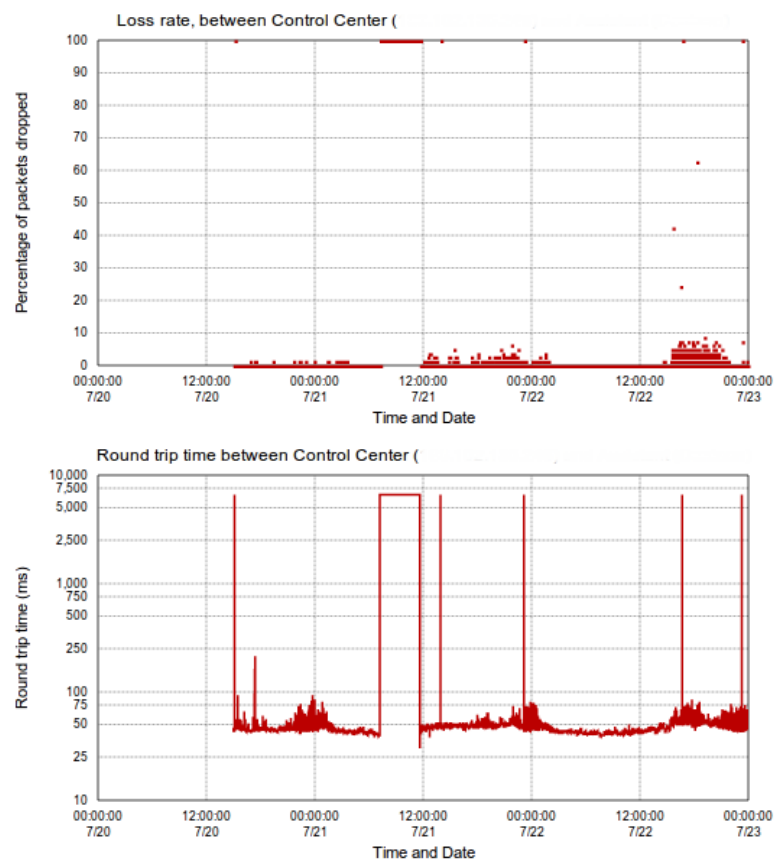
- 12 hours long, round trip times 600ms, loss rate 0-4%. Again, there are some data points over 4%, but these are ignored as they are the exception.

This data was collected with the same computers used throughout this documentation. Network commands were used to introduce random delays and packet loss which simulates real world networks. If this was a real world network (second or third period) users would experience both good calls and bad calls. Some on one particular call would report the quality as good while others would report the quality as bad.

These network performance graphs are very important for getting a perspective on audio quality issues. If there are significant periods of lost packets, or large variation in round trip times, the audio quality will be poor. The issue of lost packets is so important that this program has many diagnostic tools to determine how frequently and when packets are being lost. This information is reported so that people with *user* and *admin* access privileges can find where there might be an issue.

To give the reader an understanding of the importance of this diagnostic feature, consider the graph shown in Figure 108.

Figure 108: Abysmal link *Control Center* to *Gateway*

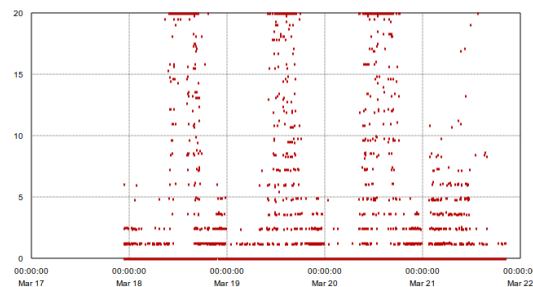


*Long term report of the link between a Control Center and a Gateway. There is a four hour window (just before midday on July 21<sup>st</sup>) where no packets travelled between the Control Center and the Gateway. Clearly, the remote Gateway was not sending/receiving audio to/from the Control Center. On other days, late in the day, there is considerable (over 2%) loss of packets. The only conclusion that can be reached is that this Gateway has a poor quality link to the Control Center.*

The *Primary Control Center* that this *Gateway* connected to has 6 other *Gateways*. The other 6 *Gateways* have "excellent" links to the *Primary Control Center* - no packets loss, no variation in round trip time. This particular *Gateway* has an abysmal connection to the *Primary Control Center*. Suppose the *Bridge Group* is such that each *Gateway* has 1 user, all *Gateways* are in the same *Bridge Group*, and only this *Bridge Group* is used. When a user at this particular *Gateway* (with the bad link) speaks, everyone will hear bad quality audio. When a user at a different *Gateway* speaks, only the user at this *Gateway* (with the bad link) hears bad quality audio. Every other user hears good quality audio.

A second and more important picture to illustrate the diagnostic benefit of this graph is shown in Figure 109.

Figure 109: Abysmal link *Control Center* to *Control Center*



Long term report of loss rate on the link between a *Control Center* and a *Control Center*. This particular graph contains data from a 5 day period, which is the maximum length stored for this graph type. Loss rates over 20% are not displayed as this is meaningless for voip (at a loss rate of 20% it is unintelligible). There is a daily pattern - in the evening the loss rate is high. This indicates that the ISP (or some other network entity) is doing packet shaping to minimize traffic.

This data was collected from a real site which carried real audio. If your loss graphs look similar (or worse), then your audio quality issues are not the fault of this program.

Figure 109 could have been collected on a *Control Center* to *Gateway* link - the graphing engine and data collection process is the same. Note that the loss pattern is quantized to multiples of 1.2%. This is because each test consists of 84 audio packets (connectivity test is 5 seconds long, 60ms between audio packets) and thus the reported loss rate is a multiple of 1/84.0. These results are combined to give an hourly average. The worse hour is reported in the “Control Center Status” table (Figure 91).

## 5.6.8.5 LTR and Analog

### 5.6.8.5.1 Monitor levels, generate 1 kHz tone

This is used on *Gateways* to quickly test and set the audio volume levels for each channel.

### 5.6.8.5.2 Command to LTR

This is used on *Gateways* to cause the attached TL-Net controller to go into TL-Net mode. After clicking this option, a message goes out the serial port, which can be viewed from the status of the serial device, message log. If the name means nothing to you then ignore this button.

### 5.6.8.5.3 Reset LTR device

This is used on *Gateways* to cause an immediate reset of the attached TL-Net controller. This can restore operation of the controller, which can be required after power outages. Again, if the name means nothing to you then ignore this button.

### 5.6.8.5.4 USB devices

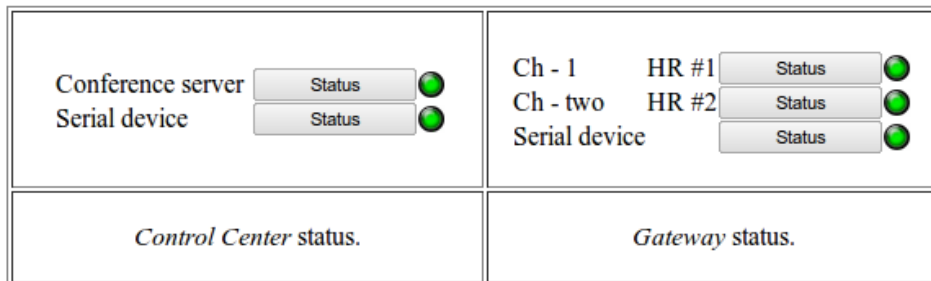
This is very similar to the *USB devices* diagnostic options for the *Control Center*, as described in Section 5.6.7.4.

## 5.6.8.6 Gateway channel information

In Section 5.6.5 the idea of audio circuits (or audio channels) was introduced, and various displays of the connections to this *Conference Server* were reported. In this section, some of the components on this box are described, and the operational logs generated by these entities. Some of the entities below are *Gateway* specific. Some are *Control Center* specific. All of them can

be found on a box that is running as a box which has combined *Control Center-Gateway* functionality. Consider the two partial screenshots in Figure 110.

Figure 110: Status report selection for *Control Center* and *Gateway*






The left image reports the status options available on a Control Center box - which is to access the report on the Conference Server and Serial Device. On the right, the status report for the audio channels running on a Gateway and Serial Device are available. Should there have been more audio channels operational, there would have been more status reports available. Should this particular Control Center have been running in combination with a Gateway then one would see a longer status option list that contains a Conference Server, a Serial Device and audio channels from a Gateway.

Status reports for an audio channel (running on this *Gateway*), a *Conference Server*, and a *Serial Device* are available by clicking the relevant button. The operational status of each component is reported by the colored light drawn to the right of the button. The meaning of the lights is reported in Section 5.6.8.6.1. The *home repeater* number of the audio channel is displayed to the left of the button.

#### 5.6.8.6.1 Status

The operational mode of an audio circuit reported on these diagnostic pages is indicated by the colored light to the right of the button. On *Gateway*, the channel name and *home repeater* (or Link ID) is reported. The meaning of the colored light is explained as follows:

-  A green light indicates a good connection between the *Gateway* and *Control Center* that can carry voice
-  A red light shows a connection (or entity) that is not active.
-  A green light with a red cross indicates the channel is attempting to connect to the *Control Center*. If a channel has been attempting to connect to the *Control Center* for many seconds, there is an error of some sort. Either the *Control Center* is currently unavailable, the network has failed, or there is a configuration problem. Note that the status symbol for the *Conference Server* will never display the green light with red cross.

The serial device will display the red, green, and green with cross lights to indicate it is stopped, running correctly, and attempting to run but cannot operate (respectively). The third state, green light with cross, has a similar meaning to when used on audio channels. Configured to run and is attempting to run but cannot run. This normally indicates faulty configuration. Check the status messages - error and general messages for more clues as to the problem.

#### 5.6.8.6.2 Status of one audio channel

An example screenshot for the status of one audio channel is displayed in Figure 111. A window similar to this can be obtained by pressing the button with the channel name in Figure 104. All status reports follow this layout style. A text report of what is happening and some buttons to report the messages & error logs. Note the button for *Current status*, which causes the status report for this channel to be refreshed and updated.

Figure 111: Status of one audio channel

**Status channel - 1 464.850 REP TX on RnCentos**

```

Summary
=====
Time           : 19:09.48.243
Time since creation: 1 hour, 38 minutes
Status        : Operational
Use Any port - on 16396
48977 rx, 9 in queue

USB URI device
=====
Alsa card number is 2
Play level=70, Record level=80
Write Frames to USB URI device 54,891

Sound card operation
=====
Read time (59.00 59.00 59.00 59.00 60.00 59.00 59.00 59.00 59.00 59.00)ms Range: 56.00 - 16.00 ms
Write time (39.00 79.00 39.00 79.00 39.00 79.00 39.00 79.00 39.00 79.00)ms Range: 0.00 - 14.00 ms
Device name write to radio Alsa device 2 read from radio Alsa device 2
Minimise USB bus usage.

Sound Device
=====
→radio from Control Center
17:31:46.121 January 30 2015 plughw:2 is now opened for sound
→Control Center from radio
17:31:46.121 January 30 2015 plughw:2 is now opened for sound
Counter:: Reads 98,031 Writes 101,560
Threads for reading and writing of audio are running. Good

Connection to rnsrv62.dyndns.org active for 1 hour, 38 minutes, 3 seconds
Current codec is SpeexIETFNarrow-24.6k
Audio flow status : Control Center sends audio to radio
Time difference between Primary Control Center and channel - 1 464.850 REP TX is 0.1 seconds.
the Primary Control Center is ahead of channel - 1 464.850 REP TX

Audio packets to/from Control Center
=====
Receiver has 48,977
lost 0.0% loss (0,48,977)Control Center (rnsrv62.dyndns.org) → Gateway (channel - 1 464.850 REP TX).
received 48,977 packets from the Control Center (rnsrv62.dyndns.org 74.76.122.176)
send 0 packets to the Control Center (rnsrv62.dyndns.org 74.76.122.176)

Jitter buffer
=====
Pre Queue : Rx: 48,977 Tx:48,977. Net size is 0
Current length : 120 ms
Target size : 120 ms
Max size : 3000 ms
Avg Gap : 59.97ms.
Avg Variation : 0.32ms.
Detailed Jitter Buffer Report

Codec performance
=====
Audio bandwidth 24.22 KBits/sec
Total bandwidth 31.25 KBits/sec

Current status
Message log
Error log
Go Back

```

The status of one audio channel (channel - 1 464.850 REP TX) is provided, which gives some diagnostic information that can help diagnose some operational issues.

The text report in the top half of Figure 111 is explained here.

- The date and time of the report is listed first. The Status of *Operational* indicates that the channel has connected satisfactorily with the *Control Center*. The *Time since creation* indicates how this computer has been operational.
- Sound card operation provides some insight about the audio device used. If it is operating well, the values reported will be close to the average value of 60. When the sound card has become "confused" (which can happen with power issues) the read and write times may drop to 0.0 - which prevents the channel from operating. In this case, the channel will restart with a

warning message to the error/message log in the hope that the fault can be cured. The real fix may be a power cycle event, or a simple restart of the box (from the web page, Section 5.4.3.4).

- The times and dates in the error and message logs are from the clock on *Gateway a*. Consequently, it is useful to know if there is a discrepancy between the *Gateway* time and time on the *Control Center*. Remember that the clock at the very top right of the web page is the *Control Center* time.
- The current codec is reported here. The codec specifies the algorithm used to compress the audio so that the bandwidth required to transfer it over the wire is less. The particular codec used was set on the *Control Center* and is described in Section 5.4.1.4. All *Gateways* connected to a *Control Center* use the same codec so that there is no quality loss when audio is transferred from one format to another.
- Audio packets transferred is a simple report based on all calls since this channel connected to the *Control Center*. The loss percentage figure gives some insight as to audio quality issues, and only reports on packets loss from audio calls.
- Jitter buffer is the entity which dynamically resizes itself to cope with variations in the audio packet arrival time. The range of resizing for the jitter buffer is from 0.12 to 3.0 seconds. Clicking on *Detailed Jitter Buffer Report* will take the user to a page which gives a report for each call made.
- The audio bandwidth is the amount of bandwidth required for the particular codec if compressed audio data could be sent to (or received from) the *Control Center* without ethernet headers. However, packet headers (UDP headers, RTP headers, IP headers) are required. Including these headers, the bandwidth required to send the compressed audio data on the wire is higher, which gives the Total bandwidth figure.

#### 5.6.8.6.3 Message log for one audio channel

The message log, or record of general events, gives some insight as to activity on one particular channel. From the screenshot in Figure 112 it is clear that the particular channel is part of an automated testing system - the calls going through have a particular length. This log only records the last 300 messages. The message log can be cleared with the relevant button. Pressing the *Current status* button takes the screen back to that shown in Figure 111.

Figure 112: Message log for one audio channel

## Messages Ch - 1 on gateway a

```

03:14:51.613 August 6 2012 Attached USB URI device for channel 1
03:14:51.703 August 6 2012 Configuration change - stop and start this channel
03:14:51.703 August 6 2012 Now launch this channel
03:14:51.721 August 6 2012 Write audio to USB URI
03:14:51.788 August 6 2012 Start Reading of RTP Audio Frames Ch - 1
03:14:51.807 August 6 2012 Ch - 1 could not send Start talk message B0101001 - Primary Control Center as channel is marked as not connected.
03:14:52.399 August 6 2012 Cause Ch - 1 to start connection with Primary Control Center. (10.0.0.62)
03:14:52.402 August 6 2012 Successful connect for Ch - 1 to 10.0.0.62 (10.0.0.62)
03:14:52.404 August 6 2012 Initiate upgrade to 6246_August_6_2012_17.11.59
03:14:52.404 August 6 2012 Ch - 1 indicate tcp control thread is setup
03:14:52.407 August 6 2012 Ch - 1 TCP connection to Primary Control Center (10.0.0.62) is now active
03:14:52.416 August 6 2012 USB URI Open reader for Alsa device 1
03:14:52.417 August 6 2012 USB URI Open writer for Alsa Device 1
03:14:52.807 August 6 2012 Stop audio message of (B0100000) from LTR is ignored as Ch - 1 is quiet - no flows
03:14:52.807 August 6 2012 Ch - 1 sends "WarnUser" to Primary Control Center on B message collision.
03:14:52.808 August 6 2012 Ch - 1 sends WarnUserNow - Primary Control Center
03:14:52.979 August 6 2012 Update RECD volume for alsa device 1 to 22
03:14:52.993 August 6 2012 Update play volume for alsa device 1 to 70
03:14:53.703 August 6 2012 Update play volume for alsa device 1 to 70
03:14:53.725 August 6 2012 Ch - 1 sends newhomerepeater1 - Primary Control Center
03:14:53.758 August 6 2012 Update RECD volume for alsa device 1 to 22
03:14:53.810 August 6 2012 Ch - 1 sends B0101001 - Primary Control Center
03:14:55.490 August 6 2012 Ch - 1 sends repeaterarray - Primary Control Center
03:14:55.807 August 6 2012 Ch - 1 sends B0100000 - Primary Control Center
03:14:55.807 August 6 2012 Call Ch - 1 - Primary Control Center lasted 2.0 seconds
03:14:56.807 August 6 2012 Ch - 1 sends B0101001 - Primary Control Center
03:14:58.563 August 6 2012 Ch - 1 sends repeaterarray - Primary Control Center
03:14:59.808 August 6 2012 Ch - 1 sends B0100000 - Primary Control Center
03:14:59.808 August 6 2012 Call Ch - 1 - Primary Control Center lasted 3.0 seconds
03:15:00.807 August 6 2012 Ch - 1 sends B0101001 - Primary Control Center
03:15:04.807 August 6 2012 Ch - 1 sends B0100000 - Primary Control Center
03:15:04.807 August 6 2012 Call Ch - 1 - Primary Control Center lasted 4.0 seconds
03:15:05.808 August 6 2012 Ch - 1 sends B0101001 - Primary Control Center
03:15:10.808 August 6 2012 Ch - 1 sends B0100000 - Primary Control Center
03:15:10.808 August 6 2012 Call Ch - 1 - Primary Control Center lasted 5.0 seconds
03:15:11.809 August 6 2012 Ch - 1 sends B0101001 - Primary Control Center
03:15:17.807 August 6 2012 Ch - 1 sends B0100000 - Primary Control Center
03:15:17.807 August 6 2012 Call Ch - 1 - Primary Control Center lasted 6.0 seconds
03:15:18.808 August 6 2012 Ch - 1 sends B0101001 - Primary Control Center
03:15:25.806 August 6 2012 Ch - 1 sends B0100000 - Primary Control Center
03:15:25.806 August 6 2012 Call Ch - 1 - Primary Control Center lasted 7.0 seconds
03:15:26.808 August 6 2012 Ch - 1 sends B0101001 - Primary Control Center
03:15:34.810 August 6 2012 Ch - 1 sends B0100000 - Primary Control Center
03:15:34.810 August 6 2012 Call Ch - 1 - Primary Control Center lasted 8.0 seconds
03:15:35.808 August 6 2012 Ch - 1 sends B0101001 - Primary Control Center

```

Clear messages log
Current status
Message log
Error log
Go Back

The log of status and activity messages generated by audio channel 1 on Gateway a. The date and time values reported are from the clock on Gateway a. Many calls from Gateway a have been made to the Control Center.

#### 5.6.8.6.4 Error log for one audio channel

In Figure 113 there is a report of the error messages associated with one particular audio channel. These messages are specific to this one channel and normally contain a description of when startup, connection, and stopping happened. A channel that has a poor connection to the *Control Center* will have rebuilt the connection to the *Control Center* many times. There will therefore be many connection related messages. Sometimes, this log will contain clues as to why this channel is having trouble connecting to the *Control Center*. This log only records the most recent 300 messages. Older messages are deleted. The log of error messages can be cleared with the relevant button. Pressing the *Current status* button takes the screen back to that shown in Figure 111.

Figure 113: Error log for one audio channel

**Error log Ch - 1 on gateway a**

```
03:14:51.703 August 6 2012 Ch - 1 is starting.
03:14:51.787 August 6 2012 Start Reading of RTP Audio Frames Ch - 1
03:14:52.401 August 6 2012 Successful connect for Ch - 1 to 10.0.0.62 (10.0.0.62)
03:14:52.404 August 6 2012 Ch - 1 indicate tcp control thread is setup
```

Clear error log
Current status
Message log
Error log
Go Back

*The error messages recorded by audio channel 1 which is running on Gateway a. There have been no connection problems - this channel has connected quickly and has remained connected to the Control Center.*

## 5.7 Net watch

The *Net watch* window is accessible by those who have *guest* (or higher) privileges. It reports the active calls and a short term log of recent calls to/from the *Control Center*. When handling digital calls from Motorola devices, parameters such as the Radio ID, RSSI value, peer ID are also reported. An example screen shot is provided in Figure 114.



Figure 114: Net watch window

start time	duration	ch	name	source peer id	source radio id	source peer alias	source radio alias	Bridge Group	Dest. RadioId	RSSI (dBm)	Site name	Loss rate
21:49:01.590 Jan 7	0.0	2	Ch - 1 g					wxpc			RnSrv	Not avail.
<input type="button" value="-1"/> <input type="button" value="+1"/>												
History												
21:48:54.190 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:54.190 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:54.190 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:50.490 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:46.790 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:50.490 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:46.790 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:50.490 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:46.790 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:50.490 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:46.790 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:50.490 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:46.790 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:50.490 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:46.790 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:43.089 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:43.089 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:43.089 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:39.390 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:35.690 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:31.989 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:31.989 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:31.989 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%
21:48:28.289 Jan 7	3.2	2	Ch - 1 g					wxpc			RnSrv	0.0%

The window which enables all with login privileges to watch network activity. This screenshot is taken from a test machine which is running test calls that are 3.2 seconds in duration every five seconds. There is one call currently active shown in the top table, and previous calls are recorded in the bottom table. Note that in this case the CC↔CC table is not displayed as it is on a separate page.

This display is updated live. There are three tables shown:

- The topmost table, comprised of buttons with the *sitenames* of *Control Centers* shows the *Control Center* to *Control Center* links. This table can be put onto a separate page to be accessed from the navigation bar by configuring *General system*. The functionality of this table is therefore described in Section 5.8. If this option is selected, this table will not be displayed on the *Net watch* page, as is the case in Figure 114.
- The middle table shows calls that are currently active. The duration reported will therefore be increased with each display update. More than one call can be active at any one time, so there will be multiple rows. If there are no calls currently active the table will have a row of blank fields.
- The larger bottom table shows a brief call history. The number of calls recorded can be configured from *General system* (as described in Section 5.4.4.1). As active calls finish they will be added to the history, and the lowest call in the *History* table will be bumped off the end. The number of rows will always be as set in *General system*.

Since the system can handle digital calls from Motorola devices, fields for peer ID, Radio ID and RSSI are listed. These fields are left empty for LTR calls.

The font size of the display can be increased and decreased by using the *-1* and *+1* buttons that are under the active call table.

## 5.8 CC↔CC

The CC↔CC options can be brought into a separate page to be accessed by the user from the navigation bar on the far left of the screen. This usage option can be selected by configuring *General system* as described in Section 5.4.4.1. This will generate

the menu shown in Figure 115. It is accessible to all user privileges. When calls are conveyed *Control Center* to *Control Center* these are recorded on this page.

Figure 115: CC↔CC

BC-TRBO 81	CHI-DMR 57	DCI 3	DMR-NA-P 100	DMR-NA-P 92	DMRLinks 41	Mi5 52	NO1A 79
BC-TRBO 83	CODIG 25	DCI 9	DMR-NA-P 15	DMR-NA-P 93	Hawaii Trbo 49	MIT 65	NO1A 95
BC-TRBO 84	DCI 1	DCI-Dev 41	DMR-NA-P 16	DMR-NA-P 96	IT-DMR 58	MIT 68	NoCo 26
BC-TRBO 85	DCI 10	DCI-Dev 73	DMR-NA-P 30	DMR-NA-P 97	IT-DMR 60	MIT 79	NoCo 74
BC-TRBO 86	DCI 11	DMR-2IL 45	DMR-NA-P 31	DMR-NA-P 98	K4USD Network 48	MIT 95	PRN-NC 43
CAN-TRBO 76	DCI 12	DMR-2IL 92	DMR-NA-P 33	DMR-NA-P 99	LonestarNet 48	NO1A 26	SF Trbo 52
CAN-TRBO 93	DCI 13	DMR-MARC-IL 77	DMR-NA-P 51	DMRLinks 39	Mi5 51	NO1A 57	WOPM 91
CHI-DMR 56	DCI 23	DMR-MARC-IL 96	DMR-NA-P 91				

-1 +1 Columns(8):: -1 +1

The window displayed on clicking on the CC↔CC button from the navigation bar. At the moment, there is a call going from the DCI Control Center to a remote Mi5 52. The destination is displayed in red, the originator in green.

The font size of the display can be changed using the left-most *-1* and *+1* buttons under the table. The number of columns displayed in the CC↔CC table can be changed by using the *-1* and *+1* buttons to the right.

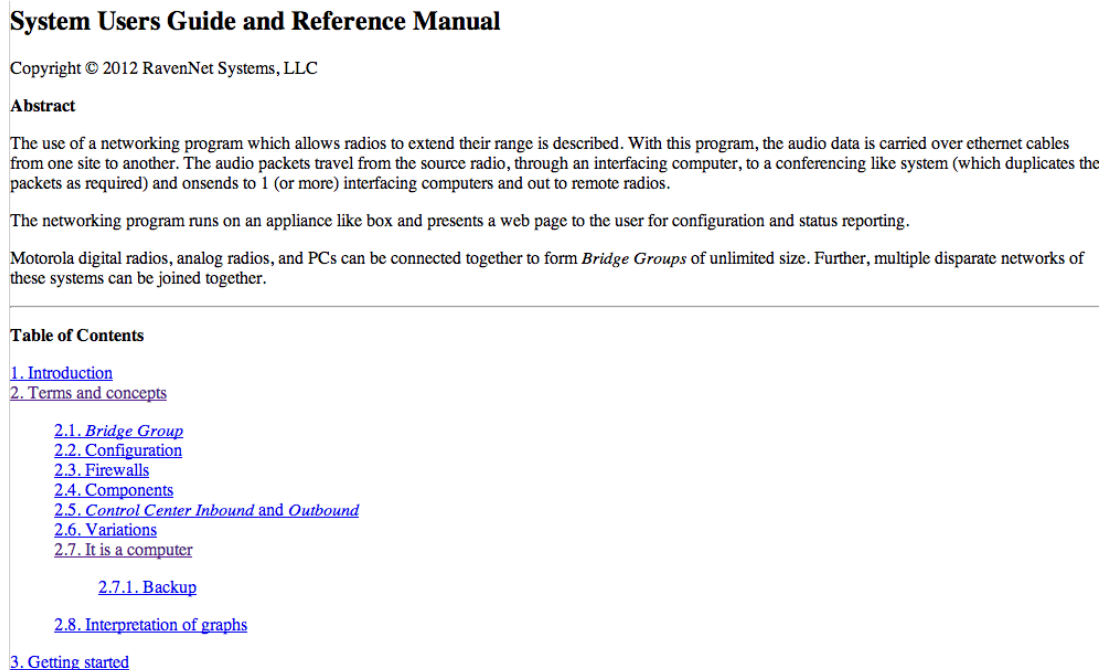
If there are any problems with a connection, this *Control Center* will be shown in orange.

Clicking on any of the *Control Center* sitemames will take the user to a more detailed report of the connection. This is very similar to the functionality of the *Conference Server* page described in Section 5.6.2.7.

## 5.9 Help

The *Help Window* is accessible by those who have *guest* (or higher) privileges and provides an online set of pages to describe features in this program. An example screen shot is provided in Figure 116.

Figure 116: Help window



The help window, which is presented on clicking the Help button in the navigation bar.

## 6 Troubleshooting

In this section, we endeavor to give some useful tips as to getting the system to work, and what to look out for. Common problems are described and the appropriate solution

### 6.1 Gateways not connecting with the *Control Center*

1. The *Control Center* should be contactable via a web browser. If it is not possible to access a web page from the *Control Center*, there is no chance of getting a *Gateway* to contact the *Control Center*.
2. If the *Control Center* is behind a firewall, and the *Gateway* accesses the *Control Center* over the public internet, check that the ports 42420..42427 (UDP and TCP) are forwarded through the firewall to the *Control Center*
3. The *Gateways* should be configured to connect to the public IP address (or dyndns name) of the *Control Center* This can be achieved by putting a web browser on the same local area network as the *Gateway* and putting the url to be `http://IP_address_gateway:42420` and going to the *Config/Channel Common* page.
4. Check the level of connection with the *Control Center*. You may have a link for control and diagnostics on the remote *Gateway*, but there is no audio. In this case, examine the status of the individual voice circuits on the remote *Gateway*. Does the message log (or error log) indicate anything - is there trouble with the sound card? Sometimes, a complete power down of the *Gateway* cures problems with sound cards. Are the individual channels on the *Gateway* marked as *Channel automatically starts on system startup*
5. Are the channels on the *Gateway* connecting, and then immediately disconnecting? There can be clues in the logs of the *Conference Server* on the *Control Center* - look in *Diagnostics/Conference Server* and examine the logs. Alternatively, look in the logs for the channel in question on the remote *Gateway*

## 7 Technical comments

In this section, we explain some of the hows and whys of the internals of program operation. It may provide some with a better understanding of the operation of the program.

Nothing in the sections below is commercially secret. Each of the comments below can be deduced by looking at the packets on the ethernet cable with wireshark (network sniffing tool).

### 7.1 Transcoding of audio

During the design and development process, it was clear that the majority of CPU time would be consumed with turning audio from one compression format to another. Alternatively, transcoding of the audio from one audio codec (e.g. Speex24K) to another (e.g. GSM0610) would consume inordinately large amounts of CPU time. Further, it was apparent that the responsiveness of the system would suffer if the CPU was crippled by transcoding. Worse, the audio quality was going to be adversely impacted by each transcode event. Consequently - there is the absolute minimum transcoding of audio.

When audio comes from a digital radio (e.g. Motorola) it is in AMBE 2+ format. These AMBE 2+ format packets are sent to the designated destination point. In this case, the packets will typically end up at Motorola radio, where they are sent on in AMBE 2+ format.

Sometimes, the packets from the digital radio are sent out in a SIP call. In this case, they will be transcoded to G711 and on-sent. The quality impact of this is minimal.

When audio is sent from one *Control Center* to another *Control Center*, it is demanded that both *Control Center* use the same codec. When attempting to build a *Control Center--Control Center* link and each end uses a different codec, there will be messages at the inbound end about different codec format. These messages are displayed in the logs of the conference server.

### 7.2 Jitter buffer

Voice over IP applications, like this one, are required to have a jitter buffer. This is simply because some audio packets take longer to travel over the same link as other packets. As the different travel time can vary by hundreds of milliseconds, something is required to smooth out the arrival time of audio packets. The entity responsible for smoothing is called a jitter buffer.

There is a jitter buffer at the exit point of this system. Thus, if a call goes: IPSC --> manager --> *Control Center* --> *Control Center* --> manager --> IPSC, there will be two jitter buffers deployed. One at each end. This example has five arrows drawn. Suppose it had been a more convoluted example and had many *Control Center-Control Center* links. There would still only be two jitter buffers deployed. One at each end.

The spacing of the packets at the jitter buffer can be inspected. Thus, the system records the time gap between packets that arrive at the destination endpoint for each call. Only the last 20 calls are recorded. If you go to the diagnostics page for the destination channel of the call (which is the channel just before the destination radio), click the status button, there is a somewhat technical report on the channel operation. In this page, there is a button, "Detailed Jitter Buffer Report" which lists the results for the last 30 calls. The results for one call, which could be something like that reported in Example 7.1.

---

#### Example 7.1 Arrival spacing times for one 35 second long call

---

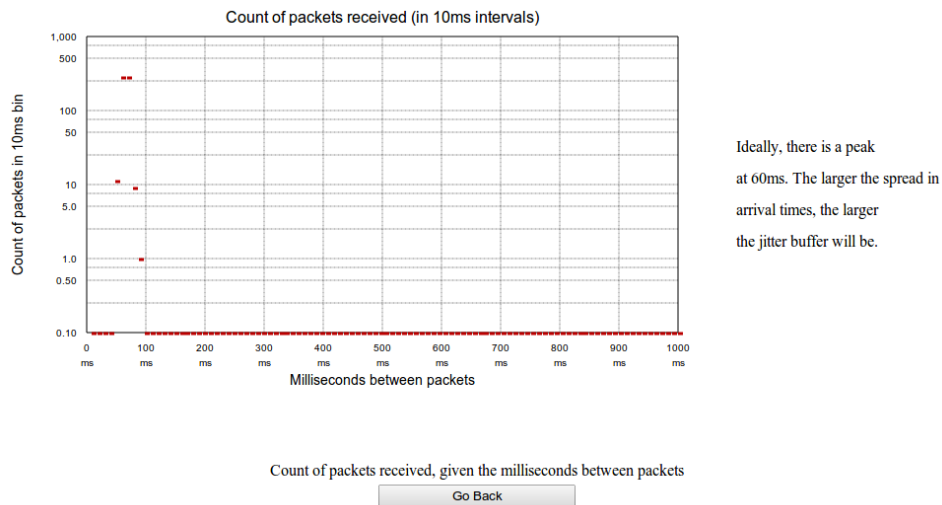
```
Start/Stop at: 15:13:32.481 15:14:07.343
Packets 581   Ran Dry 0   Average gap 60.00ms.   Call duration 34,862ms.
  0-100:581  100-200:0   200-300:0   300-400:0   400-500:0   500-600:0   600-700:0   ←
    700-800:0  800-900:0   900-1000:0  > 1000ms:0   largest 89ms
```

---

We see that the call started at 13 minutes past 3 in the afternoon, and ran for 45 seconds. The call consisted of 581 packets of data that were carried over the network. These packets were (essentially) carried with minimal variation in transmit time - the average gap was close to 60ms. The packets left the source radio with a gap of 60ms. All 581 packets were received with a spacing of between 0 and 100ms. That spacing is reported in the text report above. The report says that 0 packets arrived with a spacing of more than 100ms). The spacing can be shown graphically, by clicking on the "Graph Data" button, to give an image as shown in Figure 117.

---

Figure 117: Spacing of packets at destination channel



*A graphical report of the spacing of the packets at the destination of the call. This graph provides some insight as to what happened if the call quality was poor. However, most packet spacing issues are resolved by the jitter buffer.*

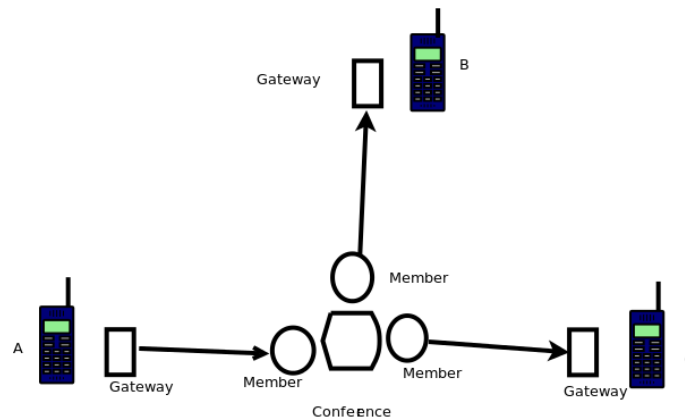
At the bottom of the text report of the last 20 calls, there is one final section, which totals the data for the reported calls. This gives a second perspective on what the jitter buffer is being asked to deal with.

### 7.3 One call is

In this section, we describe what components are used to handle a voice call. By understanding what these components are, you will be able to determine what happened when a call did not go to the designated recipients. It will help you to decide how your network should be laid out. Please make every effort to fully comprehend each paragraph in this section.

Voice from the source radio (Radio A in Figure 118) has been configured to go to radios B and C. First, the voice is converted from radio waves and turned into an internal format, that can be sent between computers. The entity responsible for format conversion is called a *Gateway*. In networking terms, a *Gateway* is something that allows for connection between networks (that may have completely different protocols). From Figure 118, the voice from radio A is sent to a conference room who has three members. The conference room is responsible for duplicating the voice (from radio A) and giving it to the designated recipients.

Figure 118: Components to carry one voice call



A pictorial representation of the components need to convey voice from radio A (at the left) to the recipients (radios B and C). There is a conference server in the middle, which duplicates the voice data and sends this data to the designated recipients. The gateways at the recipients take the voice data and send it out to radios B and C.

The members of the conference room who receive the audio send it to the designated gateways, at which point it is format converted and sent to radios B and C.

Section 7.3 does not make it clear where the computers are, and where the computers are not. It could be that the gateway functionality for radios A, B, and C is in the same computer as the conference room. Alternatively, some of the gateways are in the same computer. Or, four computers could be required to create this network. It all depends on how many radios are going to be connected.

When a call is created (or stopped) there are messages created in a log file. The gateway and member components in Figure 118 will record the start and end of each call. This log of messages can be accessed from the web page. The gateway is found from clicking on the main button for diagnostic, and then selecting the relevant gateway computer, and then the status button. The members of the conference server can be found from the main button for Connections, "Control Center Status," and then the local link for the relevant participant.

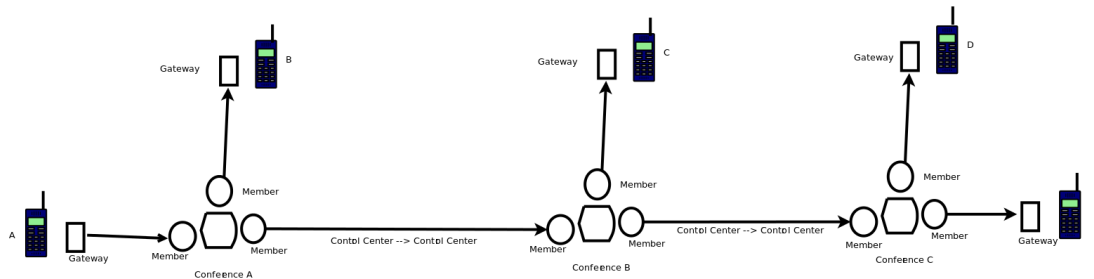
Suppose a call does not reach the designated recipients - even after multiple attempts. Check the path of the call.

- It will have come in a gateway connection somewhere. Find the log of messages of the relevant gateway connection. Check it came in.
- Now the call goes to a member of a conference. Go to the relevant *Control Center* and find the "Control Center Status" and local link. Does this report receiving the talk start and end messages - what does the log of messages report?
- You can see a live report of the *Control Center* that is responsible for duplicating the voice data of the call -- go to connections/Named members. Put the call through again. And again. See if the designated recipients lit up. Are the designated recipients displayed? If the designated recipients are not drawn - they are not going to receive the call. A second possibility is that the talk map is incorrectly configured. Sometimes, the call goes through, but not others. Members of a conference, or gateway connections, can only carry one call at a time. The named members display in connections (on a *Control Center*) helps as it shows the live status of all members of a conference at the same time.
- Inside the "Connections" tab, "Named members" is a live report of the status of the conference server members. If you click on any of the members, you will go to a page that lists details specific to that member on the conference server. The log of messages for that member are available. This message log gives details on when the call started and finished. The name of the member of the conference room (which is drawn on the box) contains information about where the *Gateway* entry. When the call starts, the text displayed is altered and the name of the designated talk map is reported. The color of the entry changes to indicate if it is the originator (green) or destination (red) of the call.

## 7.4 One Complex Call

In Section 7.3 there was a relatively simple call. This call went from a gateway component, to a conference room, to a gateway, and then out to two radios. A far more complex call is shown in Figure 119.

Figure 119: Components to carry voice between multiple *Control Centers* and to radios



A pictorial representation of one voice call (that starts from radio A) and reaches radios B, C, D, and E. Note that this call is sent between different conference rooms. The link type used to get the call between a conference room is described as a *Control Center Inbound* and *Control Center Outbound*. Note that a *Gateway* component is used when the voice call leaves the network and goes to a destination radio.

The call handling shown in Figure 119 has a number of interesting features which are described in the following points.

- There is a jitter buffer in operation at the gateways immediately prior to radios B, C, D, and E. There is no jitter buffer in operation on the *Control Center Inbound* or *Control Center Outbound* links.
- Every member of the three conferences (in this example, 9 members) will have a record of the call start and call end. Thus, if you go to the *Control Center* for one conference, and look in “Connections”, “Control Center status” and then click on the local link entry for the relevant Member entry, the log of messages should include the talk start/end message.
- The audio quality heard by the person at radio B may be much better than that heard by the person at radio E. - The reason could be that the network link between Conference B and Conference C is saturated and dropping packets. This can be verified. Go to the either *Control Center*, “Connections”, “Control Center status” and click on the local link for a member that connects the two *Control Centers*. Inside the local link is a button for “CC-CC link status”. Click on this button to see a report of how well this link has performed. The resultant graph reports on the loss rate of packets (it should be less than 1%) and the variation in round trip time. Some variation is ok - the jitter buffer will deal with this. Loss rate is bad.
- There are at least three different boxes represented in Figure 119. For it to be only three, each of the *Gateways* has been integrated into the same box as the *Control Center*. Consequently, each *Control Center* would be a combo - refer back to Section 2.6 and the diagram displayed in Figure 4.
- There could be eight different boxes represented in Figure 119. Each *Gateway* entity is running on a different computer. Each *Control Center* runs on a different computer. The exact configuration used depends on the requirements of the network required. With a very small number of radios to network together, combining some of the *Gateways* into the same box as the conference room make sense.
- For the voice call depicted in Figure 119 to work, there are three different talk maps that have been defined - one on each *Control Center*. If the talk map on the right most *Control Center* is incorrect, radios B and C will still hear the call from radio A.

## 7.5 Get Call Log

On the netwatch page, there is a report of the call history (last 50 calls) that have been handled by the *Control Center*. This information can also be accessed by way of a python script. This section describes the steps and the python script that is used. Consequently, a person using some remote computer can access the call log on a *Control Center* by running a python script. Repeated invocations of the python script will recover the call history since the previous invocation.

There are two documents in the directory `/usr/local/ravennet` which are

Table 11: Documents contained in this section

Document	Description	HTML Link
<i>get_call_log.py</i>	python script to read the full netwatch page information	<a href="#">Download (use right button, save link as,, or just click)</a>
<i>get_minimal_call_log.py</i>	python script to get contents of minimal netwatch page	<a href="#">Download/view Windows format</a>
<i>instructions_get_call_log.txt</i>	instructions on the use of the python scripts	<a href="#">Download/view Windows format</a>
<i>get_active_calls.py</i>	report in 1 (or more) lines of text the active calls table (from NetWatch page)	<a href="#">Download/view Windows format</a>
<i>v_installer</i>	report the linux script that will install a base system onto a Centos 5.8 virtual system.	<a href="#">Download/view Windows format</a>

## 8 Acknowledgement

Many thanks to the various contributors to this document. Hours of work have been expended to bring this document to the point where it will enable you to do the things that you want to do (talk with others). The technical team are grateful for the support and help from the following people::

- Mike NO7RF