

System Users Guide and Reference Manual

Compact Model



Rackmount Model



System Users Guide and Reference Manual

December 18, 2012

Copyright © 2012 RavenNet Systems, LLC

Contents

1	Introduction	1
2	Terms and concepts	1
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
3	Getting started	8
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
4	Usage options	16
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>L.P.S.C.</i> networks	17
4.6	Network connection to <i>Control Center</i>	17
5	Web page interface	17
5.1	Login	18
5.2	Main page	19
5.3	Config	20
5.3.1	System	21
5.3.1.1	Introduction	21
5.3.1.2	Options within System	21
5.3.1.3	General System	22
5.3.1.4	User Names and Passwords	23
5.3.1.5	Configure ethernet card	23
5.3.1.6	Update <i>Control Center</i>	25
5.3.1.7	Serial Device	26
5.3.1.8	Create Backup File	26
5.3.1.9	Clock adjust	27
5.3.2	E Mail	27
5.3.2.1	Link to EMail server	28
5.3.2.2	Who receives E-mails	30
5.3.3	Restart system	30
5.3.4	Audio Connections	32
5.3.4.1	Introduction	32
5.3.4.2	Selection of <i>Bridge Group</i> operation	32
5.3.4.2.1	Editing and altering <i>Bridge Groups</i>	32
5.3.4.2.2	Individual connection types	33
5.3.4.2.3	<i>Analog</i>	34

	5.3.4.2.4	<i>I.P.S.C.</i>	35
	5.3.4.2.5	<i>RnPc</i>	35
	5.3.4.2.6	<i>RnIPc</i>	36
	5.3.4.2.7	<i>Control Center Inbound</i>	36
	5.3.4.2.8	<i>Control Center Outbound</i>	36
	5.3.4.3	Altering the contents of <i>Super Groups</i>	37
	5.3.4.4	<i>I.P.S.C. other</i>	39
	5.3.4.5	<i>I.P.S.C. Validation</i>	39
5.3.5		<i>Conference Server</i>	40
5.3.6		Radio ID mapping	41
5.3.7		Configuration on attached <i>Gateways</i>	42
	5.3.7.1	Channel common settings on a <i>Gateway</i>	43
	5.3.7.2	Configuration of one TL-Net channel on a <i>Gateway</i>	44
	5.3.7.3	Configuration of one <i>I.P.S.C.</i> channel on a <i>Gateway</i>	45
	5.3.7.4	Configuration of one <i>I.P.S.C.</i> connection on a <i>Gateway</i>	45
	5.3.7.5	Configure serial device	47
	5.3.7.6	USB URI devices	47
	5.3.7.6.1	System report on one USB URI device	48
	5.3.7.7	Control repeater	48
	5.3.7.7.1	Introduction	48
	5.3.7.7.2	Initial Window	49
	5.3.7.7.3	Configuration of attached LTR repeater	49
	5.3.7.7.4	Manage users	50
	5.3.7.7.5	Mass validation of all users	50
	5.3.7.7.6	Validate repeater	51
	5.3.7.7.7	Enable one user	51
	5.3.7.8	System (on remote <i>Gateway</i>)	52
	5.3.7.8.1	General System on a <i>Gateway</i>	52
	5.3.7.8.2	Users and passwords on a <i>Gateway</i>	53
	5.3.7.8.3	Network configuration on a <i>Gateway</i>	54
	5.3.7.9	Restart system (on remote <i>Gateway</i>)	55
5.4		Connections	55
	5.4.1	<i>Control Center Status</i>	56
	5.4.2	Live network	58
	5.4.3	Named members	58
5.5		Calls	59
	5.5.1	Summary	60
	5.5.1.1	Today's calls	60
	5.5.1.2	Before today's calls	60
	5.5.2	Detail	61
5.6		ODBC	61
	5.6.1	Firewalls	61
	5.6.2	ODBC Configuration details	61
5.7		Diagnostics	61
	5.7.1	Web page login status	62
	5.7.2	System status	63
	5.7.2.1	Shell command	64
	5.7.2.2	System log	64
	5.7.3	License information	65
	5.7.4	USB devices	66
	5.7.4.1	USB URI devices	67
	5.7.4.2	USB -- Serial devices	67
	5.7.5	Load levels on	68
	5.7.5.1	CPU load	69
	5.7.5.2	Bandwidth usage	69
	5.7.6	Network Information	70
	5.7.6.1	NAT report	70
	5.7.6.2	Measure bandwidth	71
	5.7.6.3	Connectivity to remote host	73

5.7.6.4	Response time of web pages	74
5.7.6.5	IP address of connected machines	75
5.7.7	Logs of link status	76
5.7.8	Upgrades serviced by Primary Main	77
5.7.9	All Failed Calls	79
5.7.10	Diagnostic on <i>Gateway</i>	79
5.7.10.1	Scan for Hoot-n-Holler devices	80
5.7.10.2	Monitor levels, generate 1khz tone	80
5.7.10.3	Command to LTR	80
5.7.10.4	Reset LTR device	80
5.7.10.5	Network Information	80
5.7.10.5.1	NAT report	80
5.7.10.5.2	Measure bandwidth	81
5.7.10.5.3	Network performance to <i>Control Center</i>	81
5.7.11	Reports on the operation of an audio circuit	83
5.7.11.1	Status	84
5.7.11.2	Status of one audio channel	84
5.7.11.2.1	Message log for one audio channel>	86
5.7.11.2.2	Error log for one audio channel>	86
5.7.11.3	<i>Conference Server</i>	87
5.7.11.4	Announcement tracks on the <i>Conference Server</i>	88
5.8	Net watch	89
5.9	Help	89
6	Troubleshooting	90
6.1	<i>Gateways</i> not connecting with the <i>Control Center</i>	90

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	8
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	9
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	Home window	19
17	Main Configuration window	21
18	System configuration options	21
19	System configuration	22
20	User Names and Passwords	23
21	Alter/View ethernet card settings	24
22	Update <i>Control Center</i>	25
23	Configure serial device on <i>Control Center</i>	26
24	Clock adjust	27
25	EMail	28
26	Link to EMail server	29
27	Configure which people receive which emails	30
28	Restart system	31
29	Selection of the different ways of joining calls together	32

30	Editing of <i>Bridge Groups</i> window	33
31	<i>Analog</i> connection with the <i>Control Center</i>	34
32	Configure <i>I.P.S.C.</i> connection to a <i>Control Center</i>	35
33	Configure a <i>RnPc</i> connection with the <i>Control Center</i>	35
34	Different fields available for a <i>RnIPc</i> connection with a <i>Control Center</i>	36
35	The different fields for a <i>Control Center Inbound</i> to the <i>Control Center</i>	36
36	Different fields for a <i>Control Center Outbound</i> connection - which is created to another <i>Control Center</i>	37
37	<i>Super Group</i> configuration	38
38	An extensive <i>Super Group</i>	38
39	A novel <i>Super Group</i>	39
40	Extend version of the <i>Super Group</i> reported in Figure 39	39
41	40
42	Configuration of the <i>Conference Server</i>	41
43	Radio ID Mapping	42
44	Configuration on a <i>Gateway</i> - option selection	43
45	Configuration Channel common on a <i>Gateway</i>	43
46	Configure one channel window	44
47	Configuration of one <i>I.P.S.C.</i> channel	45
48	Configuration of one Motorola <i>I.P.S.C.</i> connection	46
49	Configure serial device	47
50	Uniquely identifying each USB URI device	48
51	System report of one USB URI device	48
52	Attached repeaters and configuration selection	49
53	Controller, Configuration for repeater 1	50
54	Manage users for repeater 1	50
55	Mass validation of all users on repeater 1 of <i>Gateway a</i>	51
56	Validate repeater 5	51
57	Enable 1 user	52
58	System configurations options on a <i>Gateway</i>	52
59	General system configuration on a <i>Gateway</i>	53
60	Users and passwords on a <i>Gateway</i>	54
61	IP address settings on a remote <i>Gateway</i>	55
62	Connections selection	56
63	<i>Control Center</i> Status	57
64	livenetwork window	58
65	Named Members window	59
66	Previous calls window	59
67	Today's calls in the database	60
68	Calls for a date before today	61
69	Diagnostics window	62
70	Recent Web Page Login/Out activity and current users	63
71	System Status reports	63
72	Shell command output	64
73	System log on <i>Primary Control Center (Primary Main)</i>	65
74	Report on the license settings	66
75	All USB devices attached to <i>Gateway a</i>	67
76	Report on available USB URI devices	67
77	Report on USB -- Serial devices	68
78	Load levels on	68
79	CPU busyness report for <i>Primary Main</i>	69
80	Measured network usage on a <i>Control Center</i>	70
81	Network Information Window	70
82	Measure Bandwidth Window	71
83	Measurement of the bandwidth between the <i>Control Center</i> and <i>rndownload</i>	72
84	Bandwidth measurement completed	72
85	Example connectivity report with remote host	73
86	Percentage of packets dropped between the <i>Control Center</i> and remote site.	74
87	Round trip time for packets between the <i>Control Center</i> and remote site	74

88	Response time of web pages	75
89	IP Addresses of connected machines	76
90	Logs of link status	77
91	Upgrades serviced by <i>Primary Control Center</i>	78
92	Message log on <i>Upgrade Server</i>	79
93	Diagnostic on a remote <i>Gateway</i>	79
94	Network Information Window for a <i>Gateway</i>	80
95	NAT report for <i>Control Center</i>	81
96	<i>Gateway</i> initiated measurement of bandwidth	81
97	Network performance between <i>Gateway a</i> and <i>Primary Control Center</i>	82
98	Abysmal link <i>Control Center</i> to <i>Gateway</i>	83
99	Status report selection for <i>Control Center</i> and <i>Gateway</i>	84
100	Status of one audio channel	85
101	Message log for one audio channel	86
102	Error log for one audio channel	87
103	Status of the <i>Conference Server</i>	87
104	Announcement tracks on the <i>Control Center</i>	88
105	Net watch window	89
106	Help window	90

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	Sample Email Config values	29
6	Different classes of email that can be sent out	31
7	Sample <i>Bridge Group</i>	34
8	<i>ODBC</i> configuration details	62

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 onsenes 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



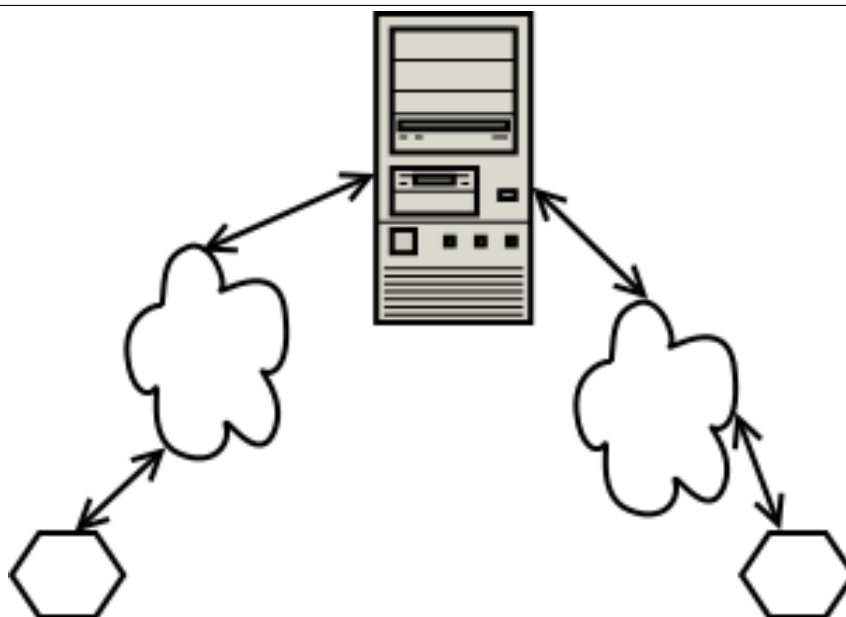
It is expected that the reader has read and understood Section 2 before examining other sections. Given the above condition, the reader can read any other section and should be able to understand the description. Reading other sections first is pointless.

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

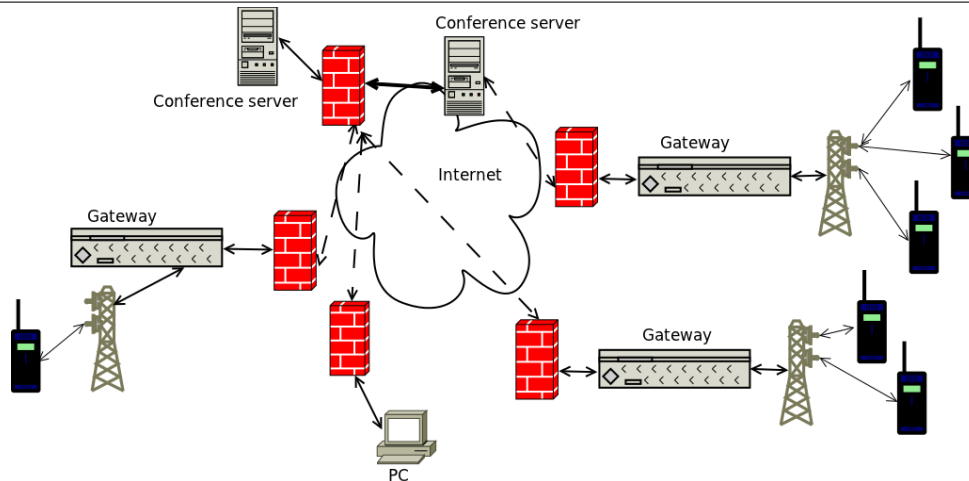
would be possible for a radio (on the left) to speak and a radio on the left hears the spoken words. For this situation, the audio has traversed the link to the *Conference Server* twice.

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 onsent to the *Conference Server*. The *Conference Server* will take the incoming ethernet packets and onsend 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 onsent 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

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	

PC connection. 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..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 232* cannot speak into (or hear from) members of this *Bridge Group*.

Section 5.3.4 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*.

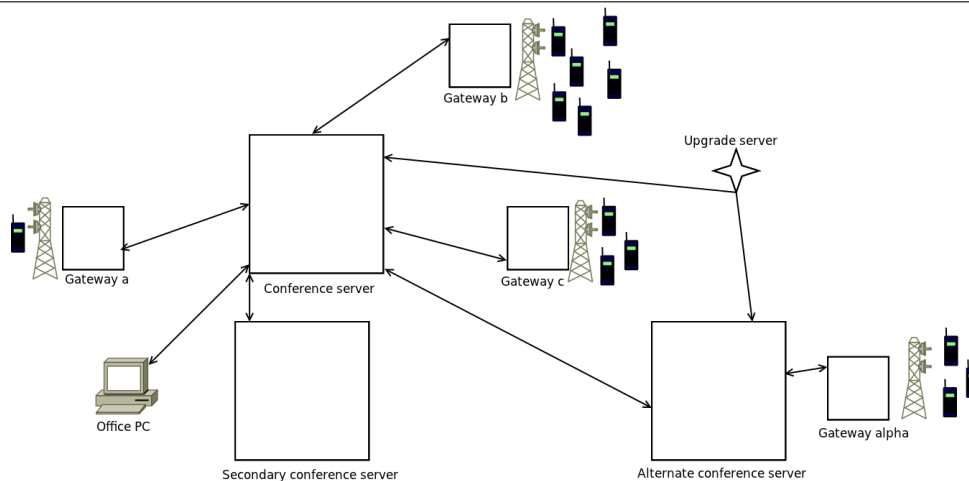
When the *Control Center* is positioned behind a firewall, it is asked that the ports 42420..42427 (UDP and TCP) are forwarded through the firewall to the *Control Center*. The same port forwarding is optional for *Gateways*. With this port forwarding for *Gateways*, it makes it easier to do (remotely) 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 (depicted as blue rectangle with LCD panel) 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 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*.
- 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...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*.

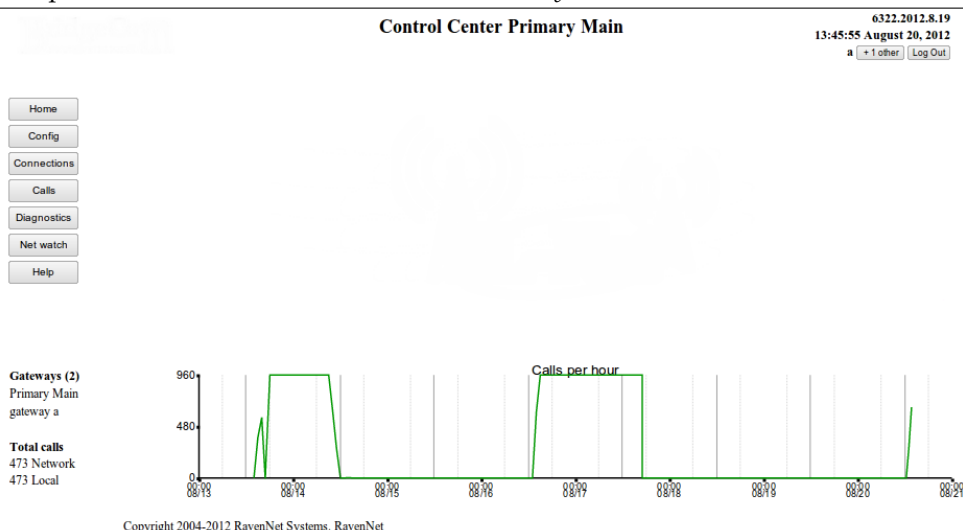
The *Inbound* and *Outbound* entities allow the site maintainer (at each *Control Center*) to keep track of who talks where. Consequently, users at the remote *Control Center* are limited to speak into just one *Bridge Group*. Further, it means that multiple links (between two *Control Centers*) can 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 consistant interface to the *Gateways* - the access method to a *Gateway* is independent of a *Gateways* physical location. 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 minimises 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?rncp.ini`. Put the mouse in the page, click right button to save as. This will save the `rncp.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 `rncp.ini` file specified above.

2.8 Interpretation of graphs

Consider Figure 97 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 7/21 refers to the very beginning of July 21st (which is in the early hours of the morning).

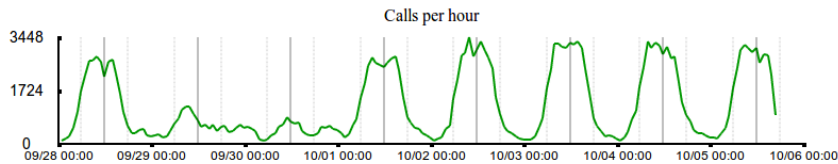
The y axis may have a linear or logarithmic scale. Typically, linear scales are used when the range of values being plotted is tightly defined. Thus, a performance figure expressed as a percentage will always be a linear scale as the values can only be 0..100. A logarithmic scale is used when the range 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 0.1ms 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 97. 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 16 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 5th is a Friday. There is minimal activity in the weekend or evenings. It is only during business hours that the system gets busy.

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.

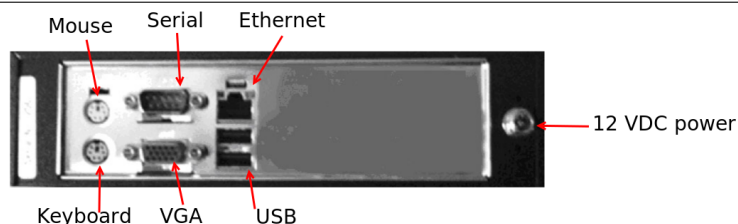


Rackmount version of the supplied computer. Power and reset switches are shown on the left. Status lights are shown.

3.3 Sockets provided at the rear of the form factors

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

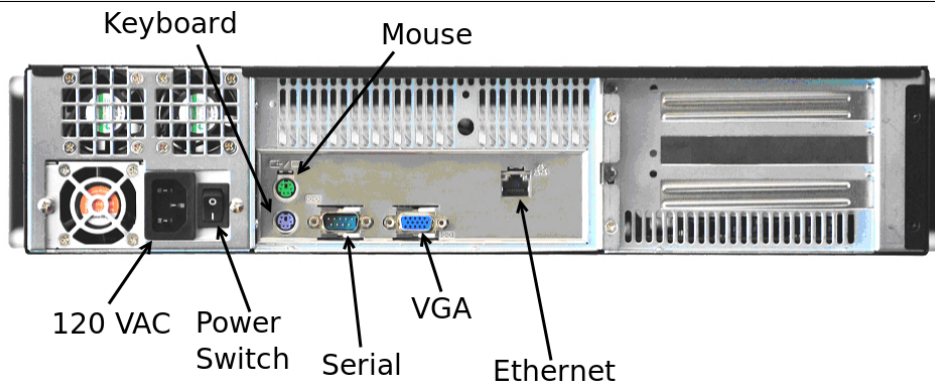
Figure 8 Rear of the compact form factor.



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.

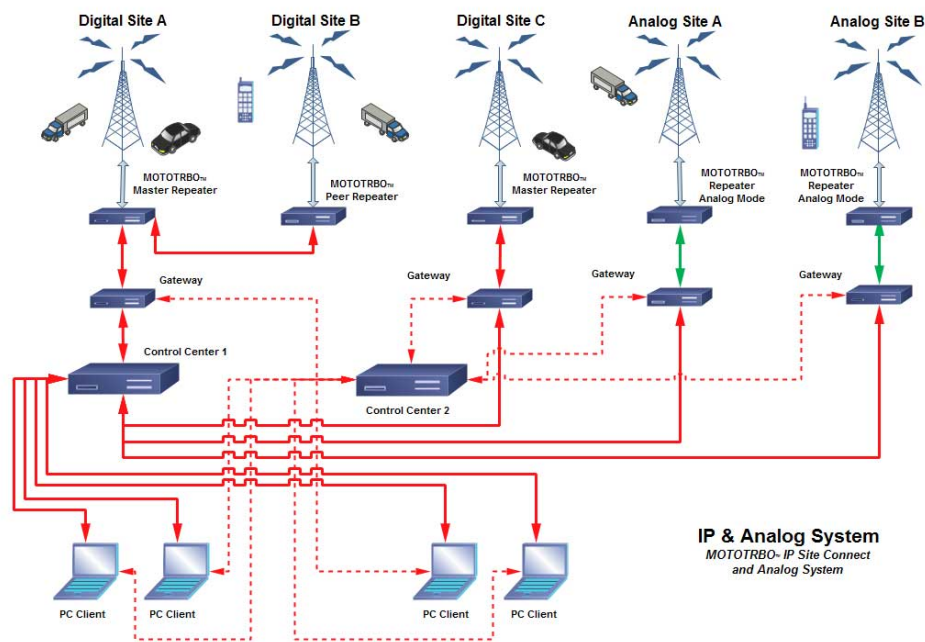
Figure 9 Rear of the rackmount box



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*

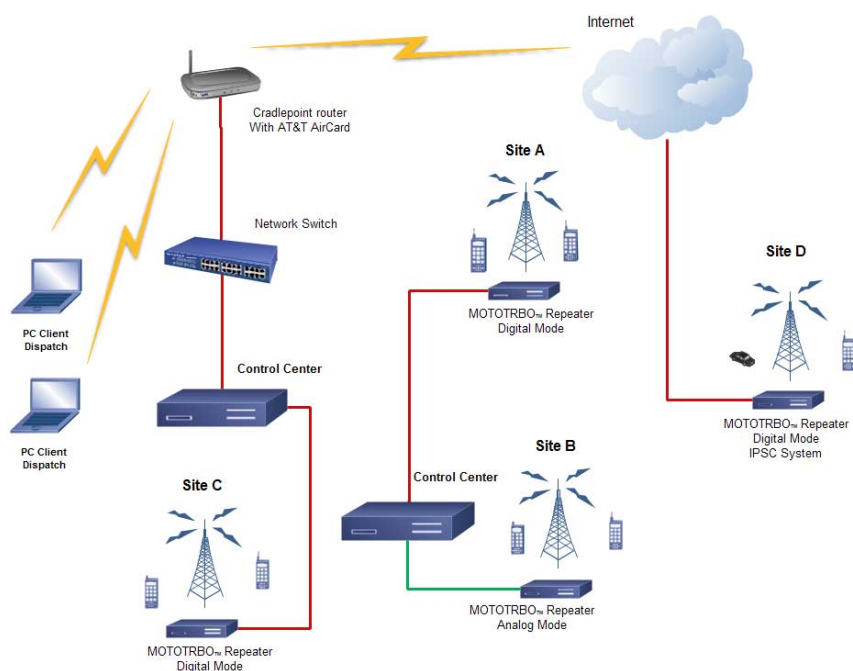


A moderately complex network with five transmitting sites, two Control Centers and four instances of Gateways. Also shown are four PC Clients which are connected to both Control Centers. The Control Centers are arranged so that Control Center 1 is the Primary Control Center. Control Center 2 is the Secondary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

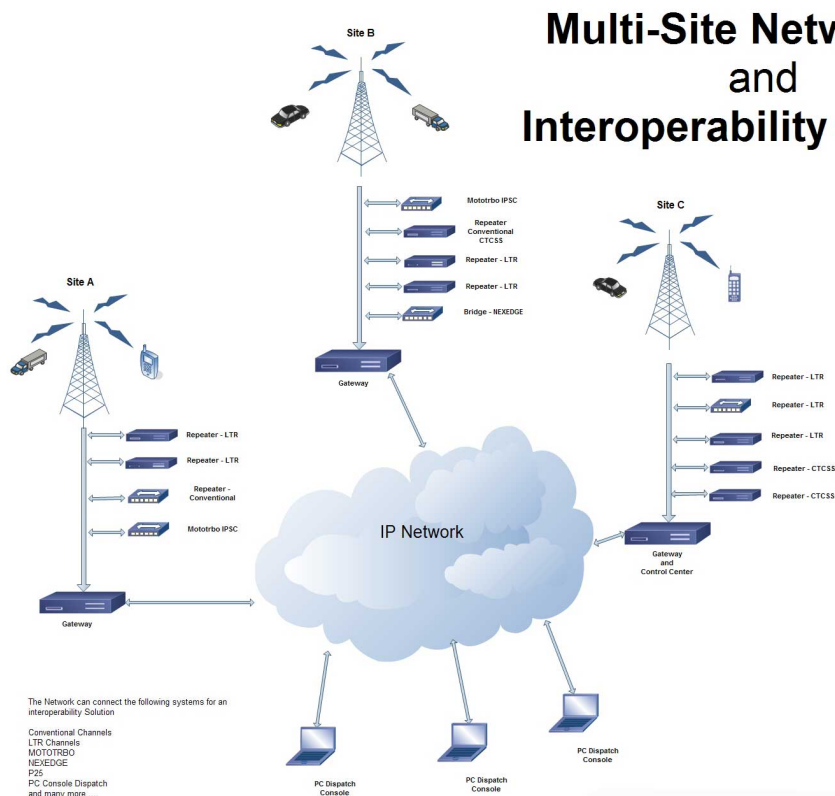


A four site system with ethernet based communications between them. Both Control Centers are operating as Primary Control Centers. The PC client is operating as a dispatch center, so is initiating (and receiving) calls from any of the Control Centers. The Control Centers are receiving/sending calls to 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 16.
9. Click *config* on the left side of the screen
10. Click the *system* button
11. Click the IP Address Settings tab. (see Figure 58)
12. The displayed image will be close to that shown in Figure 61. 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 5.3.1.5. 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 "*tlnet*". The username and password do not require the quote symbol or fullstop - these were added to highlight the particular values. Check that the capslocks 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 **rnnetwork** 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 5.3.1.5.

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 **rnnetwork** 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 5.3.1.5.

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* in 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, where it loses packets sometimes, 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 describes the method used to access the control and status features of this program. As stated there, everything is designed and tested 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 the required task.

The screenshots in this and later sections have been obtained from 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 Note that the *Primary Control Center* at IP address 10.0.0.3

Table 4 Devices used for screenshots

<i>sitename</i>	IP address	Description
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>

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 screenshots in this documentation has been taken over a period of a month. During this month, the program used has changed and evolved. Users have requested features. The documentation process has highlighted some things that are ambiguous. There are some differences between the different screenshots, which are

1. The word *server* had been used to used to describe the *Control Center*. In almost every place that it was found in the screenshots, it was replaced and fixed. However, it may still be found.
2. The word *assistant* was used to describe a *Gateway*. Again, every (well, hopefully) instance has been changed to *Gateway*, but there still may be some cases.
3. The version number displayed at the top right changes from screenshot to screenshot. This gives you some idea as to the order in which the screenshots were collected. Associated with the version number changing, the date and time changes. This is an accurate report of when the image was obtained.
4. Perhaps the most obvious change is the presence (or absence) of two buttons at the top right. One button (*Log Out*) is always there. The second button, which takes the user immediately to a diagnostic screen showing logged in web users is only on some screenshots.

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:

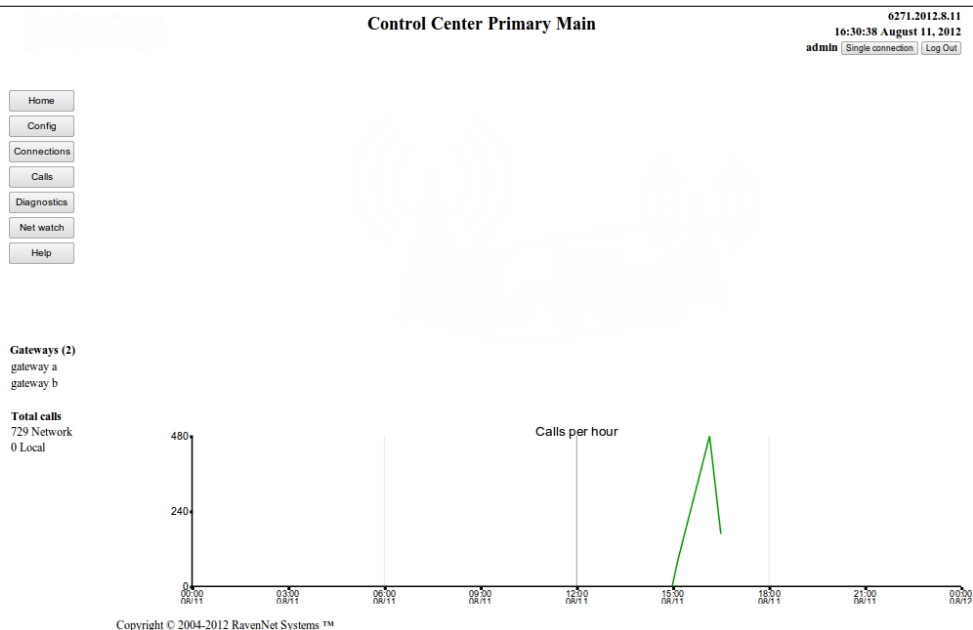
The UserName/Password window which is used for entering the login details. Not shown is the product logo, which is placed in the middle of this web page.

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*. 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.

5.2 Main page

After logging in (or pressing *Continue previous session*) the displayed web page is similar to that shown in Figure 16.

Figure 16 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. The horizontal axis on this graph is 24 hours long (midnight to midnight) and represents data collected on August 11th. There is just one and a half hours of call data - which indicates the machine which provided this image has been up for one hour. Normally, there would be 7 days of call data displayed.

This screenshot was taken from a development machine, so the uptime is quite short.

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

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.

- On the very left, at the top, are seven buttons in a column. These navigation buttons are designed to take you quickly to the different areas of the program. Access to some areas is denied to those who have logged in with insufficient access rights. Anyone who is logged in has access to the *Help* and *Net watch* pages. Only administrators can use the *Config* features.
- At the very top left there is a company logo (who supplied this product), along with the site name of the *Control Center* and the time/date values used by the *Control Center*. The *Gateways* use the same date and time value. The date/time value is used in the various graphs and logs of calls. The web page login status is listed at the top right, where it displays how many people are currently logged into the the *Control Center*. The *Log Out* button will terminate the current web browser session immediately. To access the web page of the *Control Center*, you will be required to login again. At the very right and top, there is the program version number and build date. This will be used in bug reports.
- The pane in the bottom left is a live report of the operational status of the *Control Center*. It lists the connected *Gateways* and the number of calls that have been processed. This screen reports that one *Gateway* is connected. Referring back to Table 4, it is noted that *Gateway b* and *Gateway alpha* are not displayed. This is correct as *Gateway alpha* is connected to a different *Control Center*. Further, *Gateway b* is currently powered off. At different stages of this documentation, different remote *Gateways* could be available, or not. Always, the pane at the bottom left gives you an up to date report of which *Gateways* are connected to this *Control Center*
- At the bottom the copyright message is displayed. This message cannot be altered.
- The button in the title section at the top right is a diagnostic level button. This button, to the left of the *Log Out* button, takes the user to the report on logged in web page users. This is described in Section 5.7.1.
- The large area 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 7 days of performance. Since the *Control Center* has not been operating for long at the time of the screenshot, the graph duration is 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, 08/11 refers to the very beginning of August 11th which is in the early hours of the morning.

When other pages are selected/accessed, the large area in the middle 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).

5.3 Config

The Figure 17 is only accessed by users with *admin* privileges.

Figure 17 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. From this screenshot, it is apparent that Gateway b is not active. Consequently, Gateway b cannot be configured right now.

5.3.1 System

5.3.1.1 Introduction System level of configuration are the variables that uniquely describe this computer. This includes options to adjust the usernames, ethernet card settings, 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.

5.3.1.2 Options within System First, the administrator selects the configuration option required from the screen that is shown in Figure 18.

Figure 18 System configuration options

The seven configuration types that describe things which uniquely identify this computer. Also available are options are general values (that did not fit elsewhere), user names and passwords, and ethernet card settings. Adjustment of the clock (date+time) is within this section, as it did not fit elsewhere.

5.3.1.3 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 19.

Figure 19 System configuration

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.
- *Shell command A* and *B* contain a valid Linux command line expression. The output of the command line expression provides the user with diagnostic information not obtainable elsewhere. These commands provide the user with a means of measuring some quantity not available elsewhere in this program. The output of these commands is reported in Section 5.7.2.1
- *Show IP address on LCD display* is used on those *Control Center* and *Gateways* that have a LCD display on the front which scrolls horizontally. With this flag on, the boxes IP address is reported. Consequently, those with physical access can find the web page from the box. Has no effect if there is no LCD display.
- *Network connectivity host* is the address used in the test reported in Section 5.7.6.3
- *Dns Update* is used if you have registered with the free Dynamic Dns Update service provided at 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*.
- *Log graph data to disk* Various 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 5.7.5) it may help not logging some graphs to disk. Most graphs log data to disk once every ten minutes. The log of entries to the disk is capped so that a week (or less) of data is logged. The data files are text and are in the /ravennet directory.

5.3.1.4 User Names and Passwords 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 Figure 18, when the *User Names and Passwords* button is pressed, the screen changes to that shown in Figure 20.

Figure 20 User Names and Passwords

Edit the list of usernames+passwords that may login to this program. Note that usernames+passwords may be added to the authorization types guest, user, and admin which have low, medium and high privileges in using this program.

This editing window works in the same way as Figure 30, Figure 43, and Figure 37. 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.

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

From Figure 18, when the sitename *IP address settings* button is pressed, the screen changes to that shown in Figure 21.

Figure 21 Alter/View ethernet card settings

6252.2012.8.7
19:36:25 August 07, 2012
+ 1 other [Log Out](#)

Control Center Primary Main

IP/Network settings on Primary Main

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 type="checkbox"/>	DHCP is disabled. Using static IP address.
IP address of this box (eg 192.168.1.102)	<input type="text" value="10.0.0.62"/>	10.0.0.62
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
		127.0.0.1
		67.138.54.100
DNS server (eg 8.8.8.8)	<input type="text" value="10.0.0.2"/>	4.2.2.2
		4.2.2.1
MAC address		00:24:1d:b6:33:ad

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

Click to reboot, use new values

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

Copyright 2004-2012 RavenNet Systems

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. Clicking the

- *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*.

5.3.1.6 Update Control Center 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 22) is an example of the option to upgrade this *Control Center* to the latest available version.

Figure 22 Update *Control Center*

The screenshot shows the 'Control Center Primary Main' web interface. At the top right, the current version is 6110.2012.7.17, dated 19:00:31 July 17, 2012. There is a 'Single connection' status and a 'Log Out' button. A navigation menu on the left includes Home, Config, Connections, Calls, Diagnostics, Net watch, and Help. Below the menu, it shows 'Gateway (1) gateway a' and 'Total calls: 0 Network, 146 Local'. The main content area is titled 'Check for updates for Primary Main' and features a text input field for the remote site (currently 'rndownload.dyndns.org') and a 'Remote site with recent code' label. A scrollable list of updates is shown, including:

- 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.

 A 'Change log' label is on the right side of the list. Below the list, it shows 'rndownload.dyndns.org is at 6105_July_17_2012_9.19.37 (or 6105.2012.7.17)' and a 'Refresh Info' button. At the bottom, it says 'Information collected at 19:00:06' and 'Click to confirm' with a 'Get Update' button and an 'Apply now' link. The footer contains 'Copyright © 2004-2012 RavenNet Systems™'.

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) *rndownload.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 *rndownload.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 28). 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.

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 17th 2012. 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 writing this documentation).

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.

5.3.1.7 Serial Device The serial device is used by some *Control Centers* to interact with external components. It is configured through the window opened by the *Serial Device* button reported in Figure 18. An example screenshot for configuring the serial device is shown in Figure 23.

Figure 23 Configure serial device on *Control Center*

The screenshot shows a web interface titled "Control Center Primary Main". In the top right corner, it displays the version "6311.2012.8.16" and the date "18:55:12 August 16, 2012". Below this are buttons for "+ 1 other" and "Log Out". On the left side, there is a vertical menu with buttons for "Home", "Config", "Connections", "Calls", "Diagnostics", "Net watch", and "Help". Below the menu, it shows "Gateways (2)" with sub-items "gateway a" and "gateway b", and "Total calls" with "431 Network" and "0 Local". The main content area is titled "Serial device configuration on Primary Main" and contains the following configuration options:

- Number of data bits: 8 (options: 6, 7, 8, Default is 8)
- Number of stop bits: 1 (options: 0, 1, 2, Default is 1)
- Parity: 0 (options: none(0), odd(1), even(2), Default is 0)
- Baud: 4 (options: 300(0), 1200(1), 2400(2), 4800(3), 9600(4), 19200(5), 38400(6), 57600(7), Default is 4)
- hardware manages flow control (Default is off):
- Device starts when program starts:
- Serial port: 1 (options: COM1 (1) or COM2 (2) or USB (3))

At the bottom of the configuration area, there are buttons for "Available operations", "Accept changes", "Reset changes", and "Go Back". The footer of the page reads "Copyright 2004-2012 RavenNet Systems".

Configuration of the serial device on a Control Center. If the serial device on a remote Gateway was being configured (as described in Section 5.3.7.5) 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.
- *hardware manages flow control* determines if it is hardware, or XON/XOFF messages to indicate the beginning/end of data. Normally set to off (blank, XON/XOFF is used).
- *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.

5.3.1.8 Create Backup File 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. If you keep the backup file in a safe place, it is inevitable that you will not need it.

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

5.3.1.9 Clock adjust 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.

A screenshot of the window for adjusting the time and date on the *Control Center* is shown in Figure 24.

Figure 24 Clock adjust

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. At the time this screen shot was taken, no Gateways were connected to this Control Center. The panel at the bottom left clearly reports no connected Gateways. It can be useful to check the bottom left panel for indications of the status of the attached Gateways.

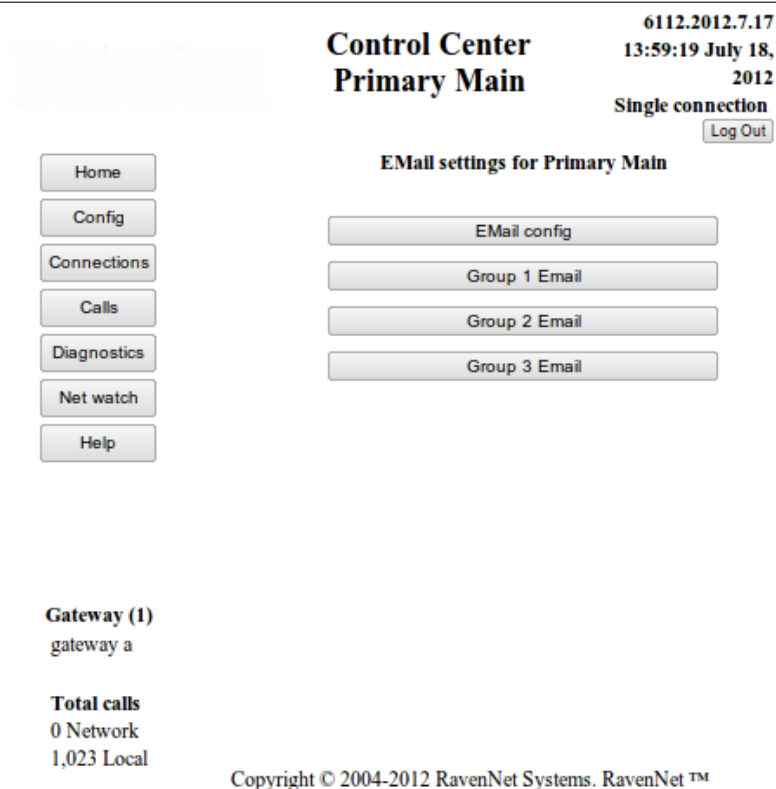
The radio buttons are set to display the time and date at the moment the page was rendered. It is up to the operator of this program to adjust these buttons accordingly. Should an invalid date (such as February 31) be entered, the date setting process is terminated and a warning message is displayed.

5.3.2 E Mail

Specify 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 *E Mail* button in Figure 17, a screen similar to Figure 25 is shown.

Figure 25 EMail



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 to the remote EMail server Section 5.3.2.1 or what events trigger the sending of emails (and the recipients) Section 5.3.2.2.

5.3.2.1 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 26, which is displayed on pressing the *Link to EMail Server* button in Figure 25.

Figure 26 Link to EMail server

Control Center Primary Main

6138.2012.7.20
09:36:14 July 21, 2012
Single connection [Log Out](#)

Home
Config
Connections
Calls
Diagnostics
Net watch
Help

Gateway (0)

Email on Primary Main

User name

Password

Domain

Smtip server

Address

port to use for email Normally 22

available authentication types
 l (preferred option)
 p

Use SSL to transfer message

Use STARTTLS before sending message

Recipient of test message

Send test email now

Available operations

Copyright © 2004-2012 RavenNet Systems™

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 5. Note that some

Table 5 Sample Email Config values

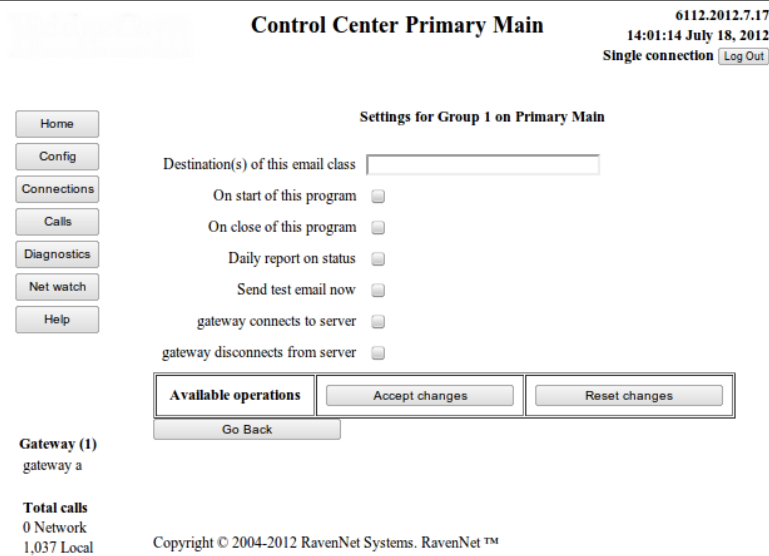
Label	GMail value	Description
User name	radionetworking@gmail.com	this value is often the text to the left of the @ symbol.
Password	secret	the invisible text that is kept hidden from other users
SMTP server	smtp.gmail.com	the IP location of the EMail SMTP server
Address		Some SMTP-servers don't support this. The sent message will use this value as the from address
Port to use for email	587	Value used is from the EMail service provider. Typically, it is 22, or 465
Authentication type	l	l is login. p for plain.
Use SSL to transfer message	checked	a security setting.
Use STARTTLS before sending message	checked	A security setting.
Recipient of text message	someone@yahoo.com	the name of the person to receive the test email message.
Send test email now	only checked when a test message has to be sent	Useful for quickly testing the settings

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.

5.3.2.2 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 17, a screen similar to Figure 27 is shown.

Figure 27 Configure which people receive which emails



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 windows determines who will receive email notifications for group 1 events. Also set is for which event group 1 members will receive email.

The meaning of the fields in Figure 27 is explained in Table 6

5.3.3 Restart system

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 28.

Table 6 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 it's 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> .

Figure 28 Restart system

The screenshot shows the 'Control Center Primary Main' interface. At the top right, it displays the IP address '6110.2012.7.17', the date and time '19:03:05 July 17, 2012', and the status 'Single connection' with a 'Log Out' button. On the left side, there is a vertical menu with buttons for 'Home', 'Config', 'Connections', 'Calls', 'Diagnostics', 'Net watch', and 'Help'. Below the menu, it shows 'Gateway (1) gateway a' and 'Total calls' with '0 Network' and '153 Local'. The main content area is titled 'Primary Main system restart' and contains three colored buttons: a red button for 'Primary Main program restart', a green button for 'Primary Main program and computer restart', and another red button for 'Primary Main computer power off.'. At the bottom of the main area is a 'Go Back' button. The footer contains the copyright notice 'Copyright © 2004-2012 RavenNet Systems™'.

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.

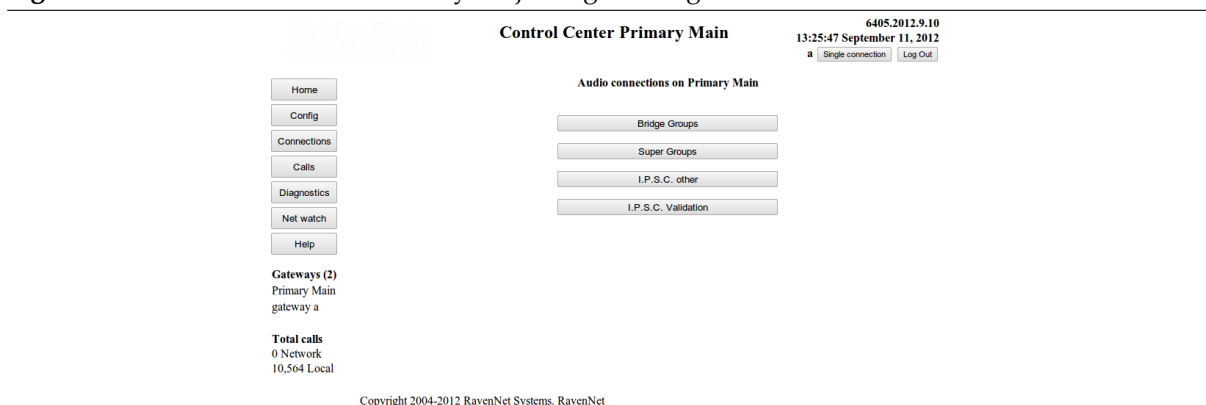
5.3.4 Audio Connections

5.3.4.1 Introduction 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.

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 5.3.4.2.2. *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*.

5.3.4.2 Selection of *Bridge Group* operation There are several different audio connection operations one may undertake, which are described in Figure 29

Figure 29 Selection of the different ways of joining calls together



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.

5.3.4.2.1 Editing and altering *Bridge Groups* An example screen shot is provided in Figure 30

Figure 30 Editing of *Bridge Groups* window

Control Center Primary Main 6399.2012.9.7
20:26:38 September 07, 2012
a | Single connection | Log Out

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	<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					

Home

Config

Connections

Calls

Diagnositics

Net watch

Help

Gateway (1)
gateway a

Total calls
131 Network
0 Local

Copyright 2004-2012 RavenNet Systems

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 take an existing entry, edit it appropriately and then add/delete the entry.

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 30. 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.
- 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*.
- 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.

5.3.4.2.2 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 7.

Table 7 Sample Bridge Group

Connection Type	Direction	Calls handled have
Analog	into Conference Server	Originated on a radio and passed through a Gateway
Hoot-n-Holler	into Conference Server	Originated from Hoot-n-Holler device
I.P.S.C.	into Conference Server	Originated on a radio and passed through a Motorola repeater and then a Gateway
RnPc	into Conference Server	Originated on a PC
RnIPc	into Conference Server	Originated on a PC. Remote PC can add/remove elements of a Super Group
Control Center Inbound	into Conference Server	Originated on a remote Control Center. This is half of a Control Center↔Control Center link.
Control Center Outbound	built by Conference Server	Originated on this Control Center. This is half of a Control Center↔Control Center link.

5.3.4.2.3 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 31.

Figure 31 Analog connection with the Control Center

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:

- *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 31, the *Bridge Group* 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 5.3.7.8.1.
- *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 5.7.11.4. This track is played to the recipients of the call before the audio from the originator.

5.3.4.2.4 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 32.

Figure 32 Configure *I.P.S.C.* connection to 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 *I.P.S.C.* connection with the *Conference Server*.

An *I.P.S.C.* audio connection requires several fields to be set, which are described with the aid of the above figure. An *I.P.S.C.* audio connection requires several fields to be set. These fields were all described previously in Section 5.3.4.2.3.

5.3.4.2.5 RnIpc 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 *RnIpc* connection type is given in Figure 33.

Figure 33 Configure a *RnIpc* connection with the *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"/>	

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 5.3.4.2.3.

5.3.4.2.6 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 34.

Figure 34 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 final	Site Name wxpc	Link ID 2	Alert on Absent <input type="checkbox"/>	Enable transmit <input checked="" type="checkbox"/>	Mute group 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 5.3.4.2.3.

5.3.4.2.7 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 35.

Figure 35 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 allcomponents	Site Name Alternate	Link ID 17	Alert on Absent <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 5.3.4.2.3.

5.3.4.2.8 Control Center Outbound Aa 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* is the

unusual connection type in Table 7 as it is the only connection type that is actively built by the *Control Center*. All 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 35.

Figure 36 Different fields for a *Control Center Outbound* connection - which is created to another *Control Center*

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 RnIpc 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 5.3.4.2.3. 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

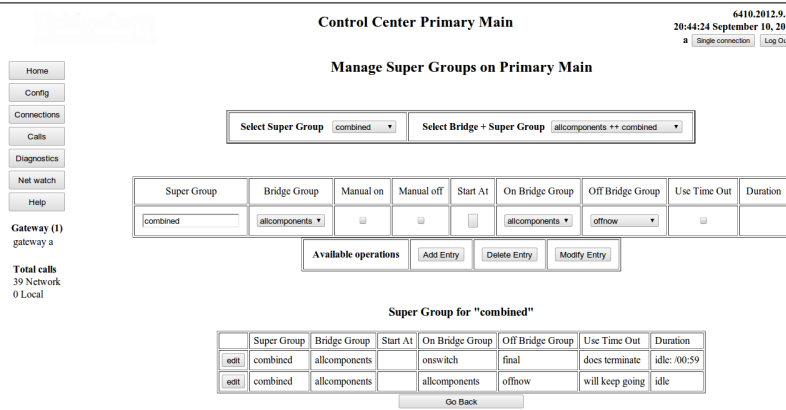
Note the similarities in the setting of these two fields and the values entered in Section 5.3.7.1. The *Gateway* does some buffering of the audio to remove irregularities in the audio packet arrival time. The *Conference Server* does no buffering - audio packets are forwarded immediately by the *Conference 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 A↔D conversions. 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*.

5.3.4.3 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. 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 method for determining when and which *Bridge Groups* are merged together is entered in the configuration page shown in Figure 37. The drop down boxes at the top of the screen (Figure 37) 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 37 Super Group configuration



Copyright 2004-2012 RavenNet Systems

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 Manual on (or the box Manual 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.

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.

Referring back to Figure 37 it lists a very trivial Super Group (combined) which contains just one Bridge Group (allcomponents). Should there be activity in the allcomponents or onswitch Bridge Groups, the Super Group combined will immediately contain the allcomponents entry. Note that both lines have the word idle in Duration field. The second line is never timed, but the first line does have a time limit. Consequently, the first line reports the maximum possible duration in the Duration field.

A more extensive Super Group is reported in Figure 38

Figure 38 An extensive Super Group

	Super Group	Bridge Group	Start At	On Bridge Group	Off Bridge Group	Use Time Out	Duration
<input type="button" value="edit"/>	combined	allcomponents		allcomponents	offnow	will keep going	idle
<input type="button" value="edit"/>	combined	final		onswitch	final	does terminate	idle: /00:59
<input type="button" value="edit"/>	combined	here	2,3,4,5,6 08:00			does terminate	remain: 03:00/03:00
<input type="button" value="edit"/>	combined	here	2,3,4,5,6 13:00			does terminate	idle: /04:00
<input type="button" value="edit"/>	combined	here	7 08:00			does terminate	idle: /09:00

An example of a relatively extensive Super Group.

which is an extended form of the Super Group shown in Figure 37. There are three Bridge Groups that can be part of the reported Super Group. The Bridge Group here is active for:

1. three hours on Monday,Tuesday...Friday mornings

2. four hours on Monday,Tuesday...Friday afternoons

3. nine hours on Saturday

. Note that the weekday morning entry reports that 03:00 remain, which indicates that this capture was taken at 8am on a weekday morning. When there is activity in the *allcomponents Bridge Group*, it is immediately merged into the reported *Super Group*. Similarly, when there is activity in the *onswitch Bridge Group*, the *final Bridge Group* is merged into the reported *Super Group*. If there is audio that originates from the *final Bridge Group*, the *final Bridge Group* is immediately removed from the reported *Super Group*. If there is audio that is sent to the members of the *final Bridge Group*, the *final Bridge Group* is not removed from the reported *Super Group*.

A novel *Super Group* is reported in Figure 39.

Figure 39 A novel *Super Group*

	Super Group	Bridge Group	Start At	On Bridge Group	Off Bridge Group	Use Time Out	Duration
<input type="button" value="edit"/>	singles	allcomponents		onswitch	offnow	will keep going	active
<input type="button" value="edit"/>	singles	final		onswitch	offnow	will keep going	active
<input type="button" value="edit"/>	singles	here		onswitch	offnow	will keep going	active

A novel *Super Group*

which contains three *Bridge Groups*: *allcomponents*, *final*, and *here*. Should there be activity on the *onswitch Bridge Group* the three *Bridge Groups* listed in this table will immediately merge into the *Super Group singles*. When there is activity in the *offnow Bridge Group*, the merger will be broken immediately. There is no timeout, so the merger can only be broken through manual intervention.

The *Super Group* in the preceding paragraph is extended, to give the *Super Group* shown in Figure 40.

Figure 40 Extend version of the *Super Group* reported in Figure 39

	Super Group	Bridge Group	Start At	On Bridge Group	Off Bridge Group	Use Time Out	Duration
<input type="button" value="edit"/>	singles	allcomponents	1,2,3,4,5,6,7 08:00	onswitch	offnow	does terminate	idle: /09:00
<input type="button" value="edit"/>	singles	final	1,2,3,4,5,6,7 08:00	onswitch	offnow	does terminate	idle: /09:09
<input type="button" value="edit"/>	singles	here	1,2,3,4,5,6,7 08:00	onswitch	offnow	does terminate	idle: /09:00

An extended version of the *Super Group* shown in Figure 39.

which will merge when there is activity in the *onswitch Bridge Group*. The merger will dissolve 9 hours after creation. Should there be more activity on the *onswitch Bridge Group* the timer is reset to 9 hours. In addition to the *Super Group* in the preceding paragraph, it will merge at 8am in the morning. Assuming no activity on the *onswitch Bridge Group*, the merge will be broken at 5pm in the afternoon. Activity in the *offnow Bridge Group* will terminate the merger immediately.

5.3.4.4 I.P.S.C. other configures the direction of data calls, and private voice calls for use with Motorola digital radio networks.

5.3.4.5 I.P.S.C. Validation provides a means to terminate incoming *I.P.S.C.* calls that are unacceptable. The default is to accept all incoming calls. A screenshot of the selection criteria for accepting incoming calls is provided in Figure 41.

Figure 41

6415.2012.9.11
14:39:36 September 11, 2012
a

Control Center Primary Main

Home

Config

Connections

Calls

Diagnostics

Net watch

Help

Gateways (2)
Primary Main gateway a

Total calls
0 Network
7 Local

I.P.S.C. validation on Primary Main

Provides a mechanism to accept/block I.P.S.C. calls that come into this network. The call will start, and should it not meet acceptable criteria, the originating Motorola hardware will be forced to close the call. The default is to accept all incoming calls.

Accept I.P.S.C. calls that do not map to a bridge group

Accept I.P.S.C. calls where Radio ID of originator not in table

Available operations

Copyright 2004-2012 RavenNet Systems. RavenNet

Using the checkboxes, it is possible to only accept calls that come from a radio which is described in the mapping of radio id to english/human readable terms (Section 5.3.6). In addition, it is possible to only accept *I.P.S.C.* calls that map to a *Bridge Group*. The operations can be combined so both requirements have to be met. Consequently, when both options are ticked and a call is in a *Bridge Group* but has an unknown Radio ID, it is blocked.

5.3.5 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. An example screenshot for configuring the *Conference Server* is shown in Figure 42.

Figure 42 Configuration of the *Conference Server*

6110.2012.7.17
19:06:13 July 17, 2012
Single connection

Control Center Primary Main

Conference server settings on Primary Main

Gateway (1)
gateway a

Total calls
0 Network
161 Local

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

Copyright © 2004-2012 RavenNet Systems™

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 multicast 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.

5.3.6 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. An example screenshot is shown in Figure 43.

Figure 43 Radio ID Mapping

Control Center Primary Main

6110.2012.7.17
19:07:19 July 17, 2012
Single connection

Manage radio ID to User Alias

Gateway (1)
gateway a

Total calls
0 Network
163 Local

Select user alias Select radio id 3 records No file chosen

User Alias
blue hill

Radio Id
1132342

Available operations

<input type="button" value="edit"/>	blue hill	1132342
<input type="button" value="edit"/>	md 4223	245623
<input type="button" value="edit"/>	zx2345	4443343

Copyright © 2004-2012 RavenNet Systems™

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 20, Figure 30, and Figure 37. 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. However, the system will be quite slow if you endeavour to put a million entries in. This page will be very slow to load in that case.

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 (or more) 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 43

```
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 43. 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 wipe the current mappings. Should there be a duplicate id value in the supplied text file, the first id value in the text file is ignored.

5.3.7 Configuration on attached Gateways

All *Gateways* that are currently connected to the *Control Center* are listed. 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*. Note that the configuration window on the remote *Gateway* looks similar to this window, except that the *Control Center* specific settings are not available. The configuration window on the *Gateway* displays the *Gateway's sitename* near the top of the web page. A screen shot of editing the configuration on *Gateway a* is shown in Figure 44. Note that the the name *Gateway a* 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*.

Figure 44 Configuration on a *Gateway* - option selection

The configuration window for Gateway a. The window is similar to that shown in the primary configuration window (Figure 17). There are some additional buttons specific to a Gateway, and some buttons removed (which were specific to the Control Center).

5.3.7.1 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 44 to give Figure 45.

Figure 45 Configuration Channel common on a *Gateway*

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.

- The 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 valid IP address, but it could have been a word address (such as *rndownload.dyndns.org*). 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. A value of 20 gives a 20 decibel increase. Figure 45 reports a value of -50dB. Consequently, when audio is turned from compressed digital into raw audio, the volume will be reduced by 50 decibels.

5.3.7.2 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 46. The channel being configured will interact with the TL-Net controller. The screen changed to that in Figure 46 when the operator pressed the button *Ch - 1* in Figure 44. Note the label near the top of the screen that says this channel is on *Gateway a*.

Figure 46 Configure one channel window

6311.2012.8.16
19:01:20 August 16, 2012
a + 1 other Log Out

Control Center Primary Main

Config Ch - 1 on gateway a

Descriptive name of this channel

Home Repeater 1..20

Channel automatically starts on system startup

Amplitude for play volume (to Transmitter) 0 = no audio, 100 = full volume

Amplitude for record volume (from Receiver) 0 = no audio, 100 = full volume

Available operations Accept changes Reset changes

Go Back

Gateways (2)
gateway a
gateway b

Total calls
480 Network
0 Local

Copyright 2004-2012 RavenNet Systems

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 - 1*).
- *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.

5.3.7.3 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 47.

Figure 47 Configuration of one *I.P.S.C.* channel

The screenshot shows the 'Control Center Primary Main' interface. At the top right, it displays the version '6252.2012.8.7', the time '20:51:00 August 07, 2012', and a '+ 1 other' status with a 'Log Out' button. The main title is 'Control Center Primary Main'. Below the title, there is a navigation menu on the left with buttons for 'Home', 'Config', 'Connections', 'Calls', 'Diagnostics', 'Net watch', 'Help', and 'Gateways (2)'. The 'Gateways (2)' section shows 'gateway a' and 'gateway b'. Below the navigation menu, there is a 'Total calls' section showing '771 Network' and '0 Local'. The main content area is titled 'Config Device-1 ipsc mb on gateway a'. It contains several configuration fields: 'Descriptive name of this channel' (Device-1 ipsc mb), 'Link ID' (18), 'Channel automatically starts on system startup' (checked), 'Support voice+data call' (checked), 'Support data call' (unchecked), 'Color Code' (1), and 'Default Radio ID' (111111). There are also three buttons: 'Available operations', 'Accept changes', and 'Reset changes'. At the bottom, there is a 'Go Back' button. The footer text reads 'Copyright 2004-2012 RavenNet Systems'.

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 46.

The meaning of the buttons and some of the fields is the same as in Section 5.3.7.2. 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.

5.3.7.4 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 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 in shown in Figure 48.

Figure 48 Configuration of one Motorola I.P.S.C. connection

6311.2012.8.16
18:08:18 August 16, 2012
a

Control Center Primary Main

Config Manager - dmr E-USA on gateway a

<p>Home</p> <p>Config</p> <p>Connections</p> <p>Calls</p> <p>Diagnostics</p> <p>Net watch</p> <p>Help</p> <p>Gateway (1) gateway a</p> <p>Total calls 55 Network 0 Local</p>	<p>Descriptive name of this channel <input type="text" value="Manager - dmr"/></p> <p>Operate as Master <input type="checkbox"/> I.P.S.C. Master</p> <p>IP address of the Master <input type="text" value="1.2.3.4"/></p> <p>UDP port for the Master <input type="text" value="50073"/></p> <p>Seconds between Keep Alives <input type="text" value="10"/> 3--30</p> <p>Seconds between Regn. attempts <input type="text" value="10"/> 3--30</p> <p>UDP port for this I.P.S.C. connection on this box <input type="text" value="53442"/> 49152-65535</p> <p>Unique ID for this I.P.S.C. connection (PeerID) <input type="text" value="314156"/> 1..4,294,967,294 (0xffff fffe)</p> <p>Silence period to indicate call end (ms) <input type="text" value="750"/> 750ms is default, 300..2000</p> <p>Authentication key for I.P.S.C. comms <input type="text" value="1234"/></p> <p>Log KeepAlive Requests <input type="checkbox"/></p> <p>Log Registration Requests <input type="checkbox"/></p> <p>Force R1.6/1.7/1.8 authentication <input checked="" type="checkbox"/></p> <p>Log XCMP RSSI messages <input type="checkbox"/></p>
--	---

Copyright 2004-2012 RavenNet Systems

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

- *Descriptive name of this channel* has the same meaning and interpretation as in Section 5.3.7.2
- *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.
- *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 authorised 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.
- *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.
- *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.

5.3.7.5 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 49. Note that the *Gateway* on which the serial device configuration is for will be shown near the top of the screen. Configuration of the serial device on a *Gateway* is exactly the same as on a *Control Center*. Consequently, the information in Section 5.3.1.7 can be used to explain the meaning and purpose of the different fields.

Figure 49 Configure serial device

6311.2012.8.16
18:50:02 August 16, 2012
a

Control Center Primary Main

Serial device configuration on gateway a

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)

hardware manages flow control (Default is off)

Device starts when program starts

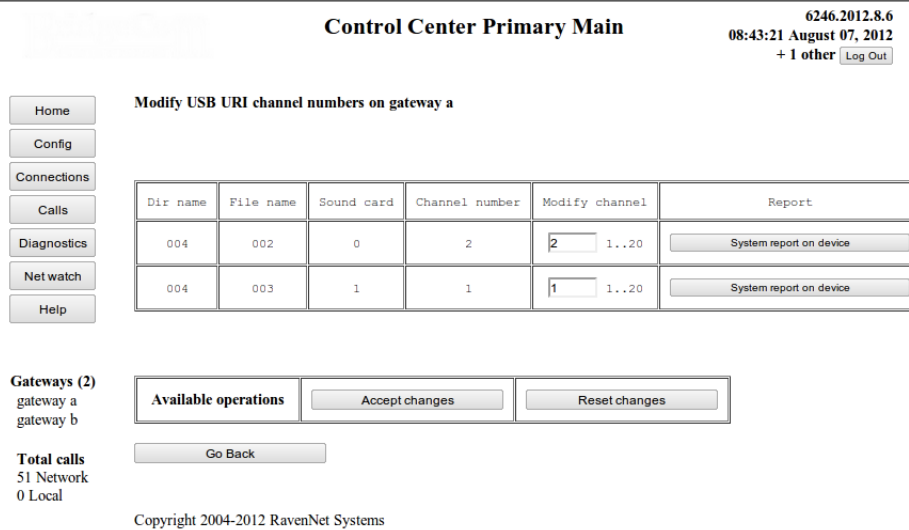
Serial port COM1 (1) or COM2 (2) or USB (3)

Copyright 2004-2012 RavenNet Systems

Configuration of the serial device on Gateway a. Note that the name of Gateway a is reported near the top of the screen. The operation and behavior of the components on this window are identical to those reported in Figure 23.

5.3.7.6 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 50

Figure 50 Uniquely identifying each USB URI device

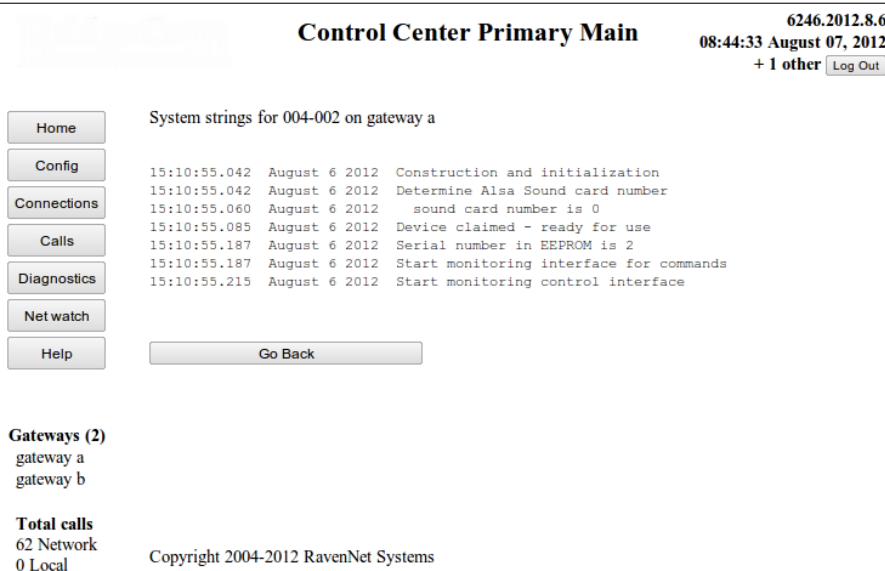


The storing of the identifying values for each attached USB URI device. This example shows two devices connected to Gateway a. They have been edited to have channel numbers of 1 and 2. Pressing the System report on device will put any current edits on hold (or lose them) and take the user to the screen described in Section 5.3.7.6.1.

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.

5.3.7.6.1 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 50. An example report is given in Figure 51.

Figure 51 System report of one USB URI device



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.

5.3.7.7 Control repeater

5.3.7.7.1 Introduction 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.

5.3.7.7.2 Initial Window 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 52.

Figure 52 Attached repeaters and configuration selection

The screenshot shows the 'Control Center Primary Main' interface. At the top right, it displays the date and time '6110.2012.7.17 19:16:02 July 17, 2012' and a 'Single connection' status with a 'Log Out' button. On the left, there is a vertical navigation menu with buttons for Home, Config, Connections, Calls, Diagnostics, Net watch, and Help. Below the menu, it shows 'Gateway (1) gateway a' and 'Total calls' statistics: 17 Network and 168 Local. The main area is titled 'Repeater Controller on gateway a' and lists 20 repeater controllers. Each controller has a 'Configuration' button and a 'Manage users' button. Some controllers are marked as '(Network)'. At the bottom, there is a copyright notice: 'Copyright © 2004-2012 RavenNet Systems™'.

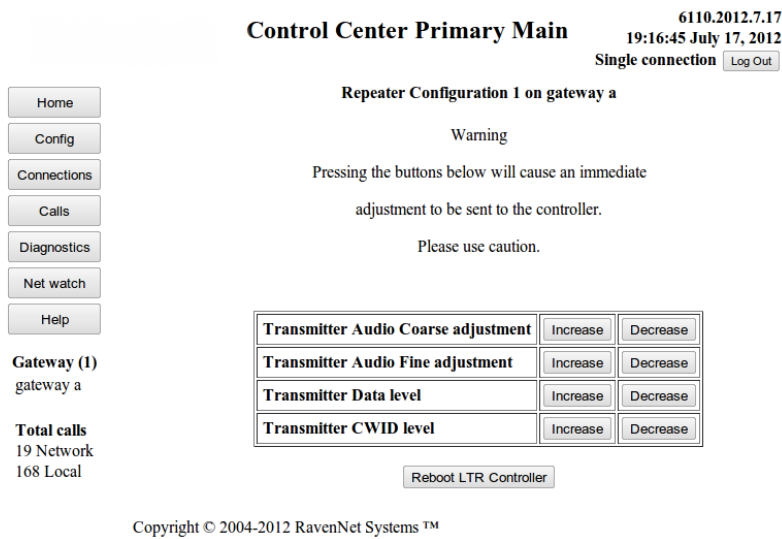
Repeater Controller	Configuration	Manage users	Status
Repeater Controller 1	Configuration	Manage users	(Network)
Repeater Controller 2	Configuration	Manage users	
Repeater Controller 3	Configuration	Manage users	
Repeater Controller 4	Configuration	Manage users	
Repeater Controller 5	Configuration	Manage users	(Network)
Repeater Controller 6	Configuration	Manage users	
Repeater Controller 7	Configuration	Manage users	
Repeater Controller 8	Configuration	Manage users	
Repeater Controller 9	Configuration	Manage users	(Network)
Repeater Controller 10	Configuration	Manage users	
Repeater Controller 11	Configuration	Manage users	
Repeater Controller 12	Configuration	Manage users	
Repeater Controller 13	Configuration	Manage users	(Network)
Repeater Controller 14	Configuration	Manage users	
Repeater Controller 15	Configuration	Manage users	
Repeater Controller 16	Configuration	Manage users	
Repeater Controller 17	Configuration	Manage users	(Network)
Repeater Controller 18	Configuration	Manage users	
Repeater Controller 19	Configuration	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 52 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 5.7.10.3. Those repeaters which are network capable have a buttons on them for configuration and managing users. Further, the word *(Network>* is displayed.

5.3.7.7.3 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 53 shows this. Also provided is an option to restart the LTR controller.

Figure 53 Controller, Configuration for repeater 1

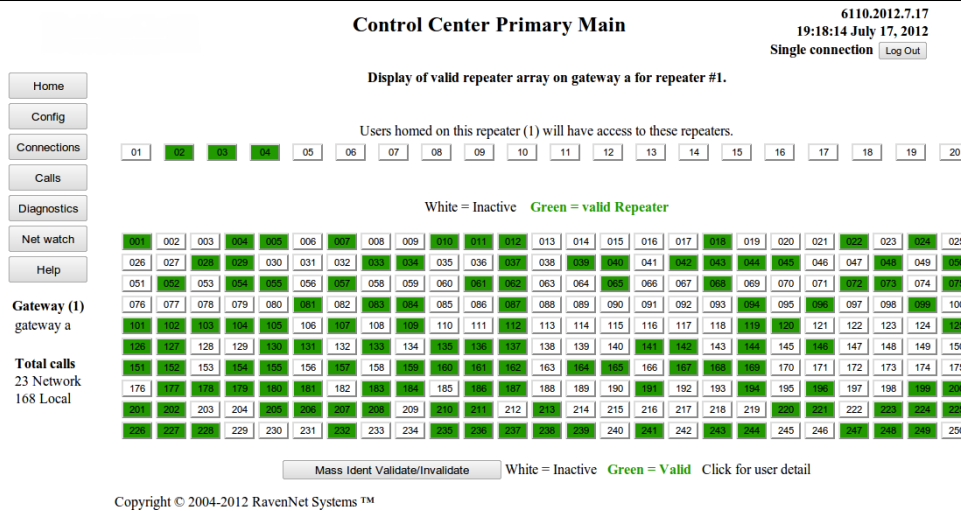


Buttons for immediate change of the Transmitter Audio, Data, and CWID levels. The LTR controller may be rebooted here.

These adjustments affect local repeated audio levels.

5.3.7.7.4 Manage users The features described in this section provide you with 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 54.

Figure 54 Manage users for repeater 1



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 5.3.7.7.6. Users are validated/invalidated through clicking on a user button (which contains three digits) and is explained Section 5.3.7.7.7. 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 5.3.7.7.5).

5.3.7.7.5 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 5.3.7.7.4. An example screenshot is provided in Figure 55.

Figure 55 Mass validation of all users on repeater 1 of *Gateway a*

6269.2012.8.11
12:56:32 August 11, 2012
a + 1 other Log Out

Control Center Primary Main

Mass Validation Repeater 01 on on gateway a

Warning
Pressing the buttons below will cause an immediate
adjustment to be sent to the controller.
Please use caution.

Local usage Validate all Invalidate all

Manage Users Repeater #01

Home
Config
Connections
Calls
Diagnostics
Net watch
Help

Gateway (1)
gateway a

Total calls
25 Network
0 Local

Copyright 2004-2012 RavenNet Systems

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 54.

5.3.7.7.6 Validate repeater Validating of a repeater is through this window, shown in Figure 56. This particular window was obtained after clicking on the repeater button 05 in Figure 54.

Figure 56 Validate repeater 5

6110.2012.7.17
19:20:28 July 17, 2012
Single connection Log Out

Control Center Primary Main

Validate/Invalidate repeater number 5 for home repeater 1

Warning
Pressing the buttons below will cause an immediate
adjustment to be sent to the controller.
Please use caution.

Validate - Invalidate Validate Invalidate

Manage Users Repeater #1

Home
Config
Connections
Calls
Diagnostics
Net watch
Help

Gateway (1)
gateway a

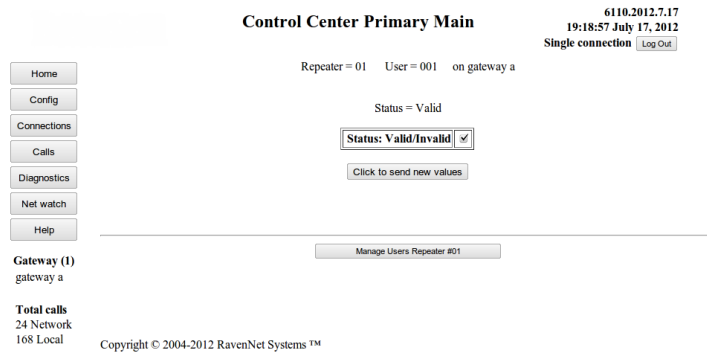
Total calls
28 Network
168 Local

Copyright © 2004-2012 RavenNet Systems™

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.

5.3.7.7.7 Enable one user From Figure 54 *userID* 001 is currently enabled (green box) and could be disabled by left clicking box 001. The screen changes to that shown in Figure 57, where we see that *userID* 001 is currently enabled.

Figure 57 Enable 1 user



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

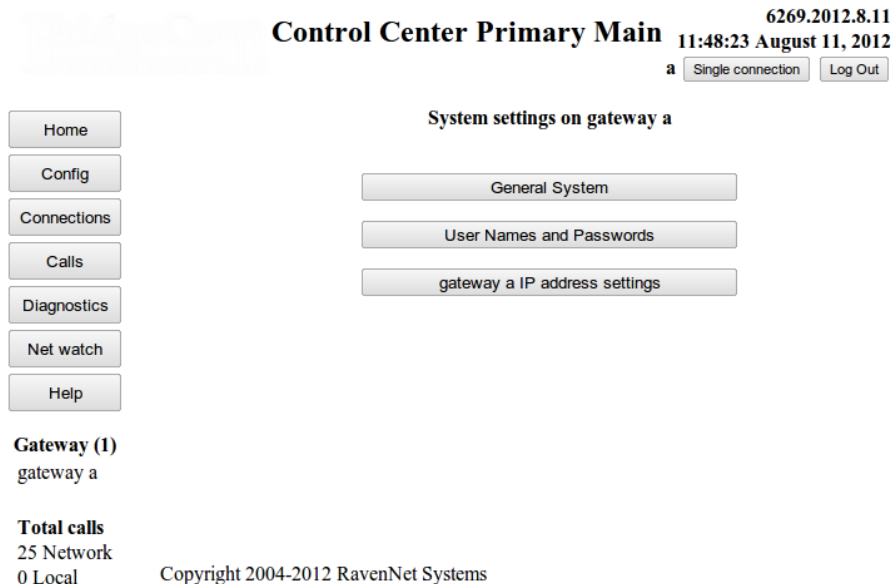
In this case, one would clear the checkbox, and press the *Click to send new values* button.

5.3.7.8 System (on remote 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 5.3.1. The screens presented, and the operation of the buttons is very similar to that described in Section 5.3.1. Except that every screen in this option has the *sitename* of the remote *Gateway* reported in multiple places. The *sitename* is always reported near the top of the screen. It is a very common mistake to think that the changes are happening on a different *Gateway* to where they are actually happening.

There are however some difference that are worth explaining. Consequently, the four different screenshots for configuration of system related things on a *Gateway* are reported here.

On entering this option, the screen looks as shown in Figure 58.

Figure 58 System configurations options on a *Gateway*



Configuration of system related things on a Gateway is similar to that shown in Figure 18. Note however that the site name of the Gateway (in this case Gateway a) is reported on one button and near the top of the screen.

5.3.7.8.1 General System on a Gateway An example screenshot is given in Figure 59, which is very similar to that shown in Figure 19.

Figure 59 General system configuration on a Gateway

6269.2012.8.11
11:49:17 August 11, 2012
a

Control Center Primary Main

System configuration on gateway a

Home
Config
Connections
Calls
Diagnostics
Net watch
Help

Gateway (1)
gateway a

Total calls
25 Network
0 Local

Site name

Shell command A

Shell command B

Show IP address on LCD display

Log graph data to disk

Network bandwidth used

CPU usage

File Handle usage

Network link, Gateway to Control Center

Available operations

Copyright 2004-2012 RavenNet Systems

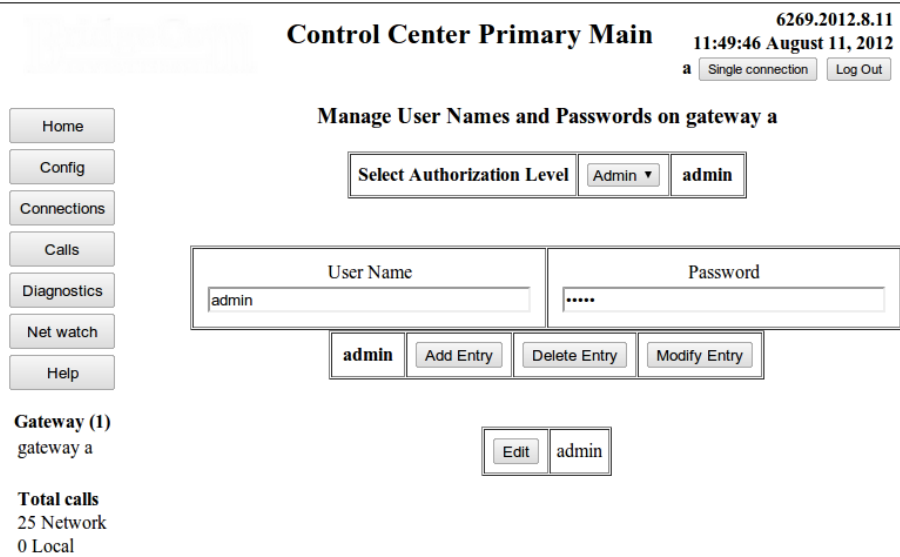
The configuration of general type things on a Gateway. These things fitted best here. The most important parameter is the sitename. After changing the sitename, the pages generated by the Gateway will have the new sitename. The pages generated on the Control Center will have the new sitename when the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

The differences between Figure 19 and Figure 59 are as follows:

1. 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.
2. A Gateway has no Dns Update feature, so there is no need to configure this.
- 3.
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 host 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.
7. A Gateway does 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.

5.3.7.8.2 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. 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. 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 60 shows this for Gateway a.

Figure 60 Users and passwords on a Gateway



Copyright 2004-2012 RavenNet Systems

Configuration of users and passwords on Gateway a. The only difference to when configuring user names and passwords on a Control Center ([xref linked="usernamespasswords"/>](#)) 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.

5.3.7.8.3 Network configuration on a Gateway An example screenshot for changing the network settings on a remote Gateway is shown in Figure 61.

Figure 61 IP address settings on a remote *Gateway*

6269.2012.8.11
11:51:06 August 11, 2012
a

Control Center Primary Main

Home

Config

Connections

Calls

Diagnostics

Net watch

Help

Gateway (1)
gateway a

Total calls
25 Network
0 Local

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
		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.

Copyright 2004-2012 RavenNet Systems

The parameters for setting the IP address fields on a *Gateway*. Unlike Figure 21 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 5.3.7.1. 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.

5.3.7.9 Restart system (on remote *Gateway*) This option works in the same fashion as in Section 5.3.3. With the exception that it is the remote *Gateway* that is restarted. The screen used in this section is identical to that in Figure 28 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.

5.4 Connections

Figure 62 is accessible by those who have *user* and *admin* privileges. 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. Further, it is apparent which connection is active from this section.

Each connection described in this section is one audio circuit which is linked to the *Conference Server*. Alternatively, 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.

Figure 62 Connections selection

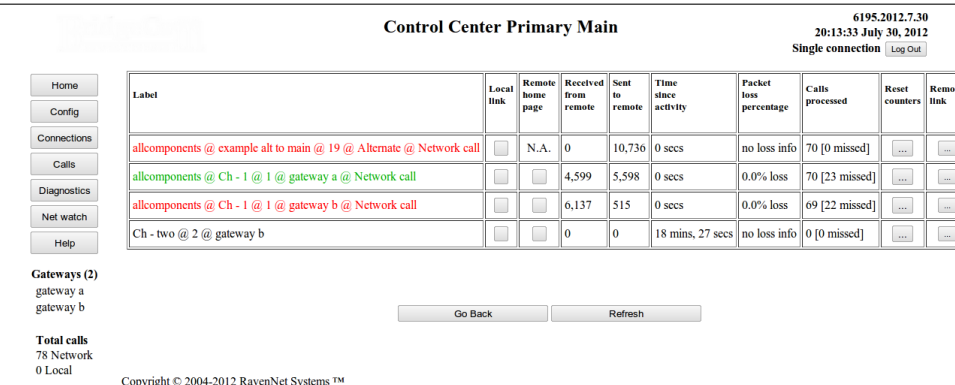
The screenshot shows the 'Control Center Primary Main' interface. At the top right, it displays the version '6325.2012.8.20', the time '19:08:38 August 20, 2012', and the user 'admin' with '+ 1 other' and a 'Log Out' button. On the left is a vertical navigation bar with buttons for Home, Config, Connections, Calls, Diagnostics, Net watch, and Help. Below the navigation bar, it lists 'Gateways (2)' as 'gateway a' and 'gateway b', and 'Total calls' as '16 Network' and '0 Local'. The main content area is titled 'Live connections' and contains three buttons: 'Control Center status', 'Live network', and 'Named members'. Below these buttons, summary statistics are displayed: '2 connections', '0 current start calls', '0 current call dest', '0 local calls', '3 call initiated', and '0 call not completed'. A 'Secondary Control Center' button is located to the right of these statistics. At the bottom, the copyright notice 'Copyright 2004-2012 RavenNet Systems' is visible.

The window displayed on clicking on the *Connections* button from the navigation bar. There are three sub options, along with summary statistics for how many calls have been made made. Further, there is an button to link the display through to the *Secondary Control Center*. The button to the *Secondary Control Center* is only displayed if the *Secondary Control Center* is available.

5.4.1 Control Center Status

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 63.

Figure 63 Control Center Status



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 second 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 Gateway a and sent to the Alternate Control Center, and to Ch-1 of Gateway b. The voice circuit Ch-2 of Gateway b has 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.

Note that Figure 63 does not auto update, nor does it show a log of previous events. Consequently, Figure 63 must be regarded as a "snapshot" of activity on the Conference Server. Figure 63 display shows the activity of the voice circuits in the Control Center, so it is therefore a snapshot of the state of the Conference Server.

The name of one voice circuit could be: *Ch - 2@12@gateway a*. 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 63 there is an entry which is

allcomponents@Ch - 1 @ 1 @ gateway a @ Network call

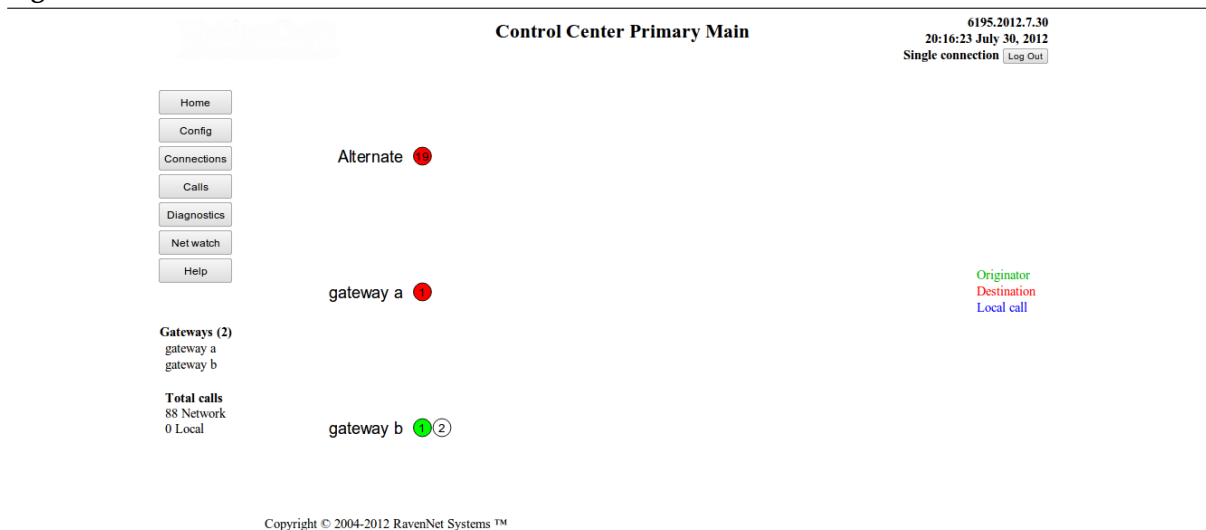
This name contains six noteworthy elements:

1. *allcomponents* 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 *1*
4. The *sitename* is *gateway a*
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*.

5.4.2 Live network

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 64

Figure 64 livenetwork window



Copyright © 2004-2012 RavenNet Systems™

A live display of the state of the current voice circuits, the home repeater numbers (or Link IDs) and the relevant sitenames.

In this figure, there are three devices connected to the Control Center - gateway a, gateway b, and the Alternate Control Center.

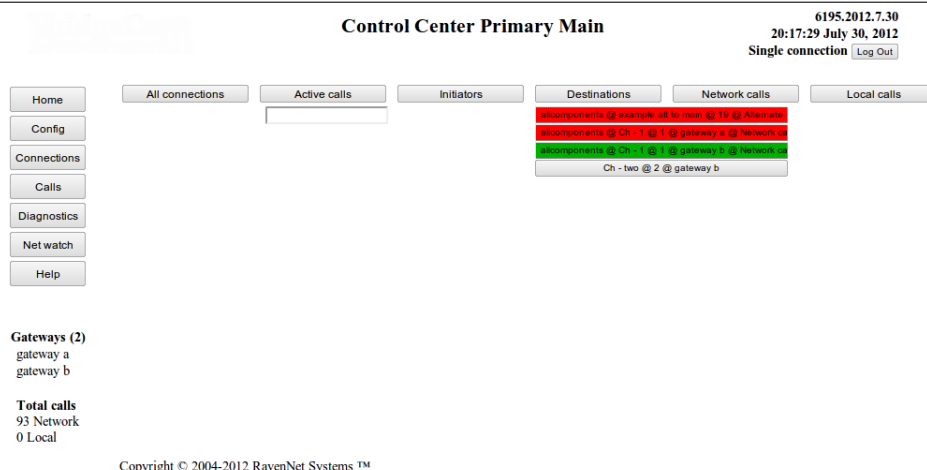
The link between Gateway a and home repeater 1 is sending a call to the Control Center, and so is coloured green. This call is passed on to two endpoints, which are coloured red. The system can cope with many concurrent calls, so this page may have several green circles and many red circles.

The display shows the activity of the voice circuits in the *Control Center*, so it is therefore the behavior of the *Conference Server*.

5.4.3 Named members

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 displayed list can be shortened by the use of the buttons. A string can be entered in the text box to select matching entries which further shortens the displayed list. The display refreshes automatically as an aid to the user. An example screenshot is shown in Figure 65

Figure 65 Named Members window



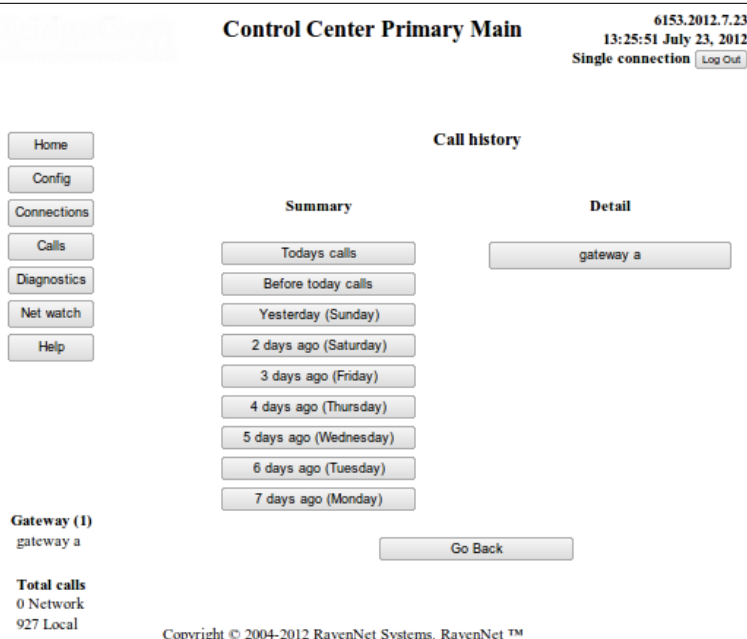
A live listing of the voice circuits currently connected to the Control Center. The list can be shortened by entering text in the clear rectangle on the top left. Only entries that match the text will be reported. In the same manner, by selecting one/some of the buttons at the top of the screen, the 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 63. 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.

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 below.

Figure 66 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 summarised 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

reports the collated call history.

- *Todays calls* creates a new window that provides a means of selecting calls (for today) from the database. Calls are selected on the basis of site name, user name, and access type.
- *Before todays calls* creates a new window that provides a means of selecting calls (from yesterday or earlier) from the database. Calls are selected on the basis of site name, user name, date, and access type.
- *xx Days ago (day of week)* has the same effect as the *Before todays calls* button, except that the date range is preconfigured for the specified date.

5.5.1.1 Todays calls The database can be queried for calls that have happened today. Note that 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 67.

Figure 67 Todays calls in the database

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 68.

5.5.1.2 Before todays calls Shows the accumulated record of calls on one particular day (or date range) that is prior to today. Selecting which day(s) are viewed is via the drop down boxes in the middle, which are shown in Figure 68. This option, to look at calls before today, cannot report calls that happen today.

Figure 68 Calls for a date before today

The window used for selecting which calls from the database are viewed - out of those prior to today.. This window does not have the date range selection options (unlike Figure 68). 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.

5.5.2 Detail

reports the short term record of individual calls. The call record for each connected *Gateway* is available at a click of the relevant button. Within the generated table the calls can be subdivided based on call type.

5.6 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.

5.6.1 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.

5.6.2 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: 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 summarises the record of calls and minimises the cumulative load on the CPU of the *Control Center*

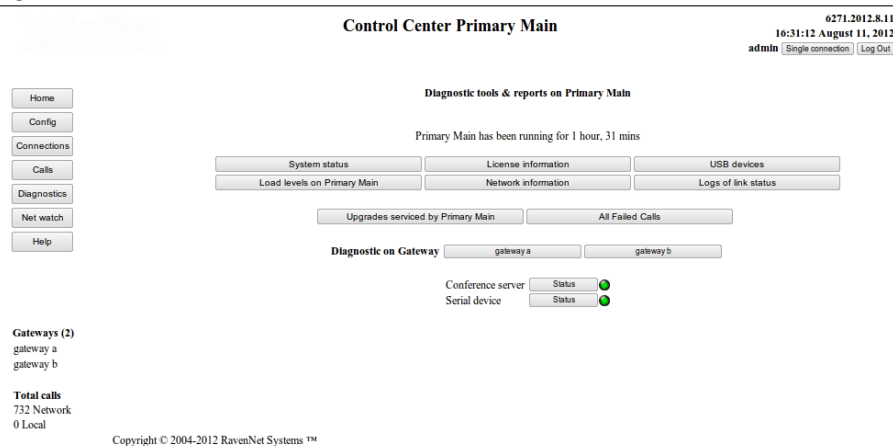
5.7 Diagnostics

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

Table 8 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 fatar.

Figure 69 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.

5.7.1 Web page login status

This section reports the last 50 login/logout events and reports those currently logged in. An example screenshot is shown in Figure 70.

Figure 70 Recent Web Page Login/Out activity and current users

6269.2012.8.11
11:54:55 August 11, 2012
a

Control Center Primary Main

Web page login status and record on Primary Main

Home

Config

Connections

Calls

Diagnostics

Net watch

Help

Gateway (1)
gateway a

Total calls
25 Network
0 Local

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

Login/Logout events

Name	Time	Event
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

Copyright 2004-2012 RavenNet Systems

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.

The report on who is currently active, and who logged in/out. This report is restricted to those who have *user* (or higher) access privileges. Note that in this report, the *admin* user is described as having logged out. In fact, shortly after the *admin* user logged in, his browser was closed. Within 20 seconds, he is marked in the list of events as logged out.

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.

5.7.2 System status

contains the options which fitted nowhere else. *Shell commands A* and *B* display the output of a Linux command line tool, which can be useful for manual monitoring of a measurable quantity. The *System log* contains information on startup, which is a short term one of event. The screenshot of this window is in Figure 71.

Figure 71 System Status reports

6271.2012.8.11
16:40:33 August 11, 2012
admin

Control Center Primary Main

System status on Primary Main

Home

Config

Connections

Calls

Diagnostics

Net watch

Help

Gateways (2)
gateway a
gateway b

Total calls
808 Network
0 Local

Shell command A

Shell command B

System log

Go Back

Copyright © 2004-2012 RavenNet Systems™

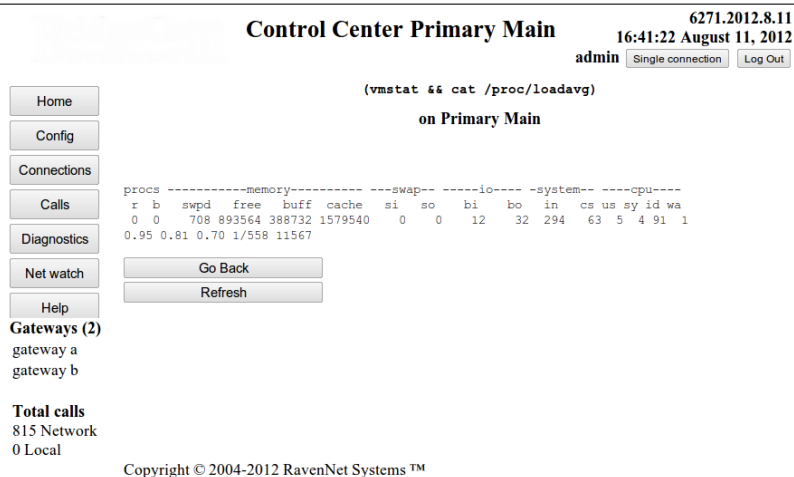
Selection of three different reporting options which provide some insight into the operation of this computer.

The particular shell command(s) executed are configured in Section 5.3.1. There is a five second limit on these commands. Any command will be stopped mid execution if it runs too long. They *System log*

is primarily used to report messages created during program. Sometimes, reports from other processes are added to this log. In the event of weird/erroneous behavior, it can help to check this log for any clues.

5.7.2.1 Shell command This option displays the output of *Shell Command A* (or *B*). It was in Section 5.3.1.3 that the actual value used for these commands was defined. Selecting the button for *Shell Command A* (or *B*) brings up a window similar to Figure 72 where the output of the currently defined command is displayed.

Figure 72 Shell command output



The derived value from the currently configured Linux shell command. Near the top of the screen the command used is reported.

Note that the Linux command that is selected is only allowed to run for five seconds. If the command takes longer than five seconds, the command is abruptly terminated - regardless of the consequences. It is up to the administrator to ensure that the entered command will not be detrimental.

5.7.2.2 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 (from a machine different to the network used in the other images) is shown in Figure 73.

Figure 73 System log on Primary Control Center (Primary Main)

6271.2012.8.11
16:41:40 August 11, 2012
admin

Control Center Primary Main

System log on Primary Main

Home
Config
Connections
Calls
Diagnostics
Net watch
Help
Gateways (2)
gateway a
gateway b
Total calls
816 Network
0 Local

14:59:22.168	August 11 2012	Ubuntu == Description: Ubuntu 12.04 LTS
14:59:22.233	August 11 2012	Possible new dyndns configuration
14:59:22.741	August 11 2012	Configure IPSC Instances
14:59:22.791	August 11 2012	Possible new dyndns configuration
14:59:23.426	August 11 2012	Dns Update running
14:59:23.431	August 11 2012	Dns updates configuration done. Start testing dns every 10 minutes.

Copyright © 2004-2012 RavenNet Systems™

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

The three buttons in Figure 73 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.
- *Refresh* 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.

5.7.3 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

6271.2012.8.11
 16:43:27 August 11, 2012
 admin

Control Center Primary Main

Current license information on Primary Main

RnPc	10	max. number of active incoming RnPc instances this control center will manage
Rnlpc	10	max. number of active incoming Rnlpc 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

-
-
-
-
-
-
-

Gateways (2)
 gateway a
 gateway b

Total calls
 830 Network
 0 Local

Copyright © 2004-2012 RavenNet Systems™

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 server, and can support 20 different connections from the PC program. Twenty different (incoming) ControlCenter-ControlCenter 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.

In this figure, the site name is reported at the very top of the screen and near the top. When this license information is accessed for a Gateway, the sitename of the Gateway will be reported near the top of the screen.

5.7.4 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 again in 30 seconds. This section describes the different diagnostic reports available. The main window for information on the usb devices available is shown in Figure 75, which reports the USB devices available on Gateway a.

Figure 75 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 75 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 75, 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 75 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.

5.7.4.1 USB URI devices The report on the USB URI devices is obtained by pressing the *USB URI devices* button from Figure 75. An example screenshot is shown below, in Figure 76.

Figure 76 Report on available USB URI devices

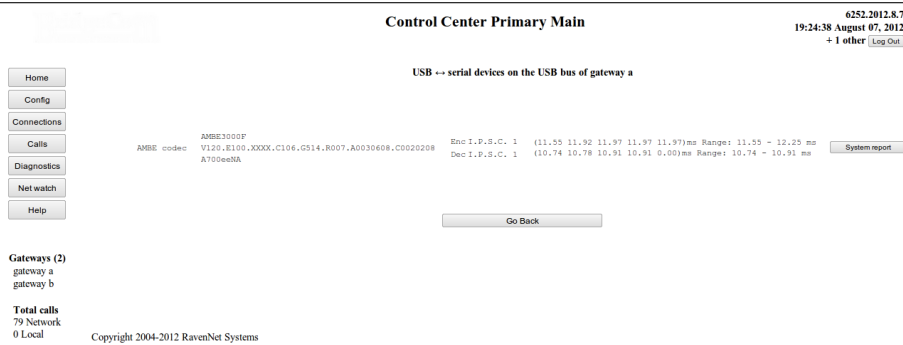
The report on available USB URI devices. Note, this report provides the same information as from Figure 50.

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

5.7.4.2 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 77. Alternatively, the

external entity may be the TL-Net controller. An example screenshot for this section is given in Figure 77 which shows one connected DVSI AMBE codec.

Figure 77 Report on USB -- Serial devices



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.

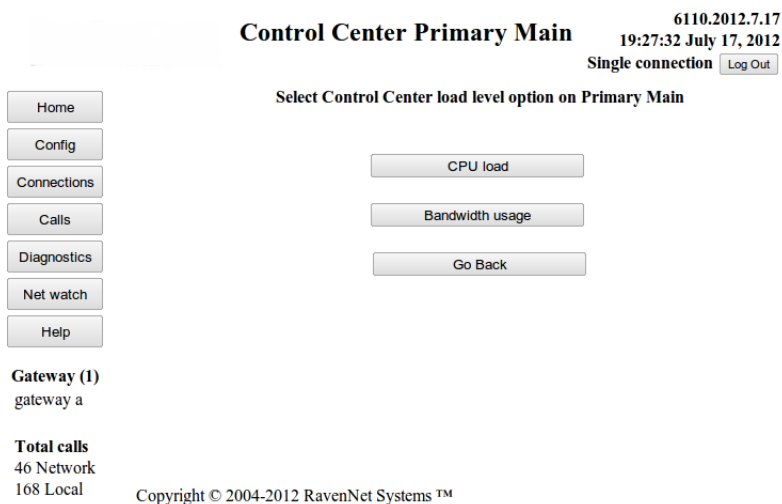
For correct operation of the DVSI AMBE device, it must be able to encode and decode audio in under 15ms. If it takes longer than 20ms, which happens if the device is plugged into a USB1 socket, the audio quality will be bad. Consequently, for DVSI AMBE devices the encode and decode time is measured at configuration time. The measured values are reported in the report shown in Figure 77.

5.7.5 Load levels on

creates a page that describes the CPU activity level over the last 24 hours. Every minute, the cpu busy percentage and load level (a measure of the responsiveness) is recorded. The network usage (measured every minute is available also. 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.

After clicking the Load levels on ... button, a window similar to that shown in Figure 78 is displayed.

Figure 78 Load levels on ...

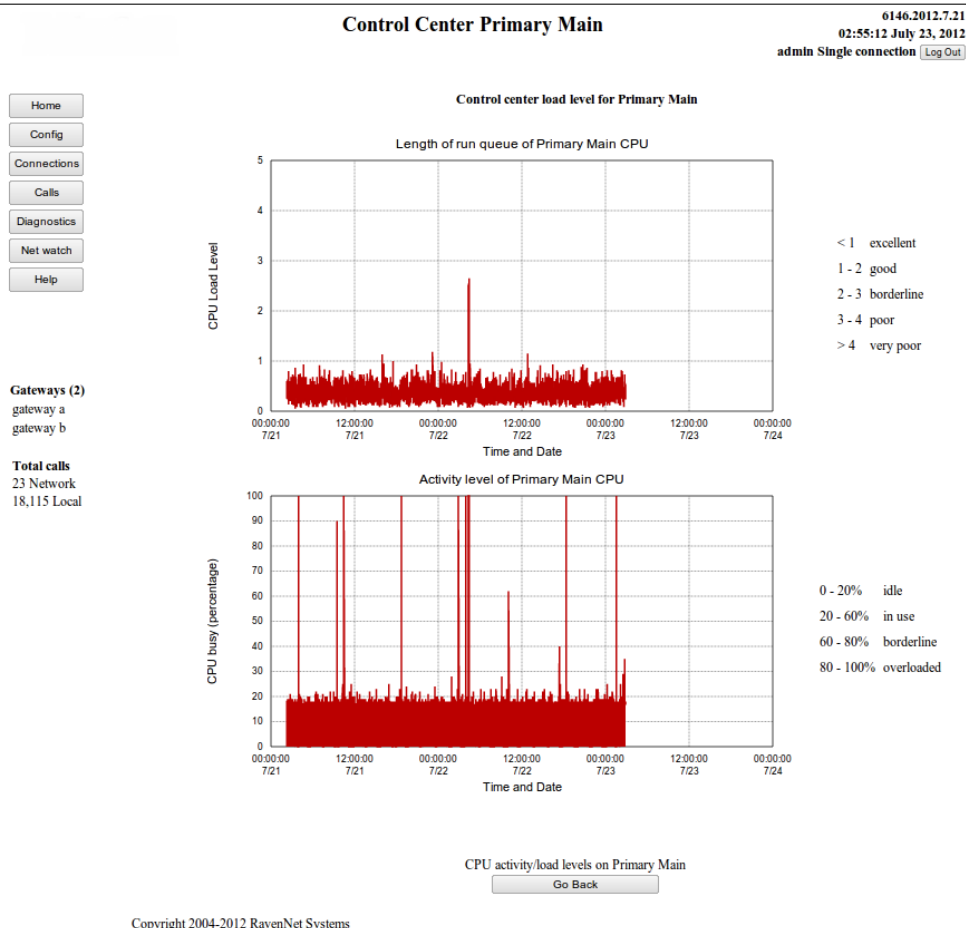


The available options to see different aspects of the load levels on a particular box. It can either be an examination of the CPU activity level, or the measured throughput of the ethernet socket (sum of TX and RX bytes). Both options create graphs, which allow the user to see the time history of these variables. Consequently, the graphs will show if the box has been overloaded for long periods of time.

The operator may select either of these options 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.

5.7.5.1 CPU load Provides a report on how busy the CPU of the computer is. The system has a long running process to record the busyness level of the CPU - which runs very two minutes. Two days of data is stored, and the results are graphed. An example graph is shown in Figure 79.

Figure 79 CPU busyness report for *Primary Main*



Copyright 2004-2012 RavenNet Systems

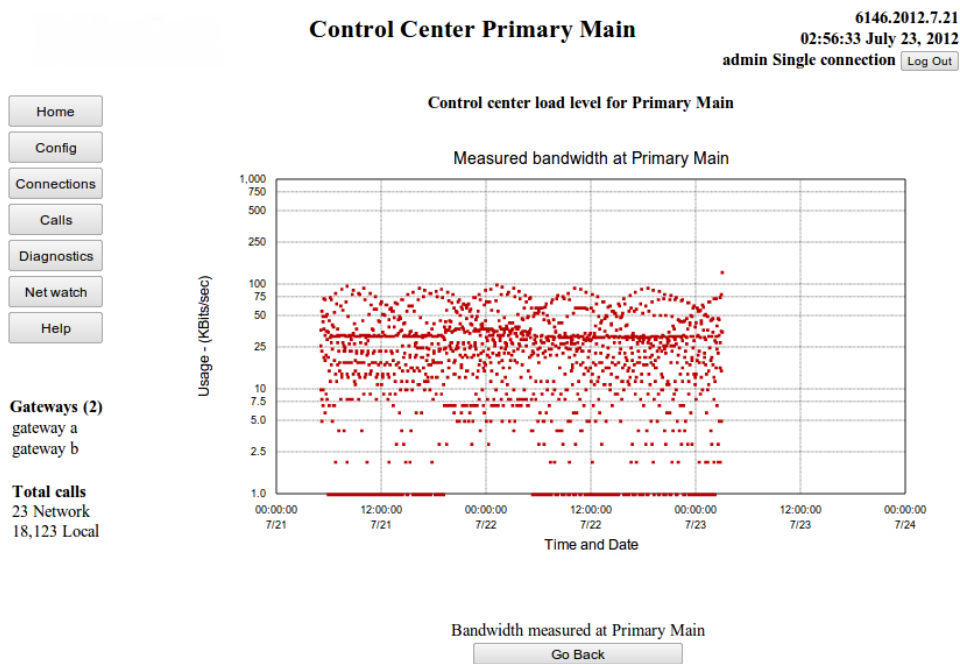
The cpu busyness report for Primary Main. If both graphs reported a high load/usage level, there is probably a problem. In this case, neither graph is excessive, so we conclude the CPU load levels is just fine.

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.
- *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.

5.7.5.2 Bandwidth usage 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 leak to audio quality issues. A sample graph is provided in Figure 80.

Figure 80 Measured network usage on a Control Center



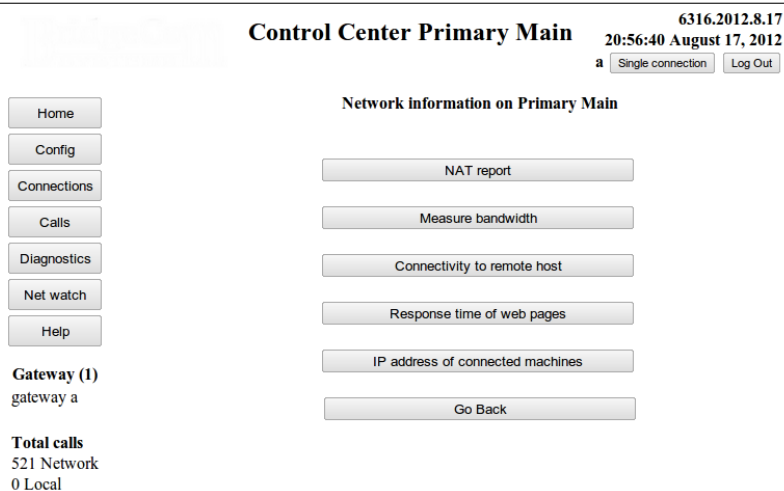
The measured network usage - which is almost always below 100 kilo bits/sec. Since this box is attached to a 100MBits/sec LAN, there is no reason for thinking packets might be lost in the network.

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.

5.7.6 Network Information

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 81

Figure 81 Network Information Window



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

5.7.6.1 NAT report is a report of the public IP address and the type of any NAT/firewall in front of this box. There is simple check to determine if the NAT has the requisite ports open.

5.7.6.2 Measure bandwidth page brings up a selection 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 82 there is a sample screen shot of the measure bandwidth window, as generated by the *Control Center*.

Figure 82 Measure Bandwidth Window

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 83 is displayed:

Figure 83 Measurement of the bandwidth between the *Control Center* and *rndownload*

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 84 is generated.

Figure 84 Bandwidth measurement completed

The bandwidth between *rndownload.dyndns.org* and this *Control Center* has been measured. The process took 11 seconds. The measured bandwidth is 0.4Mbits/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*.

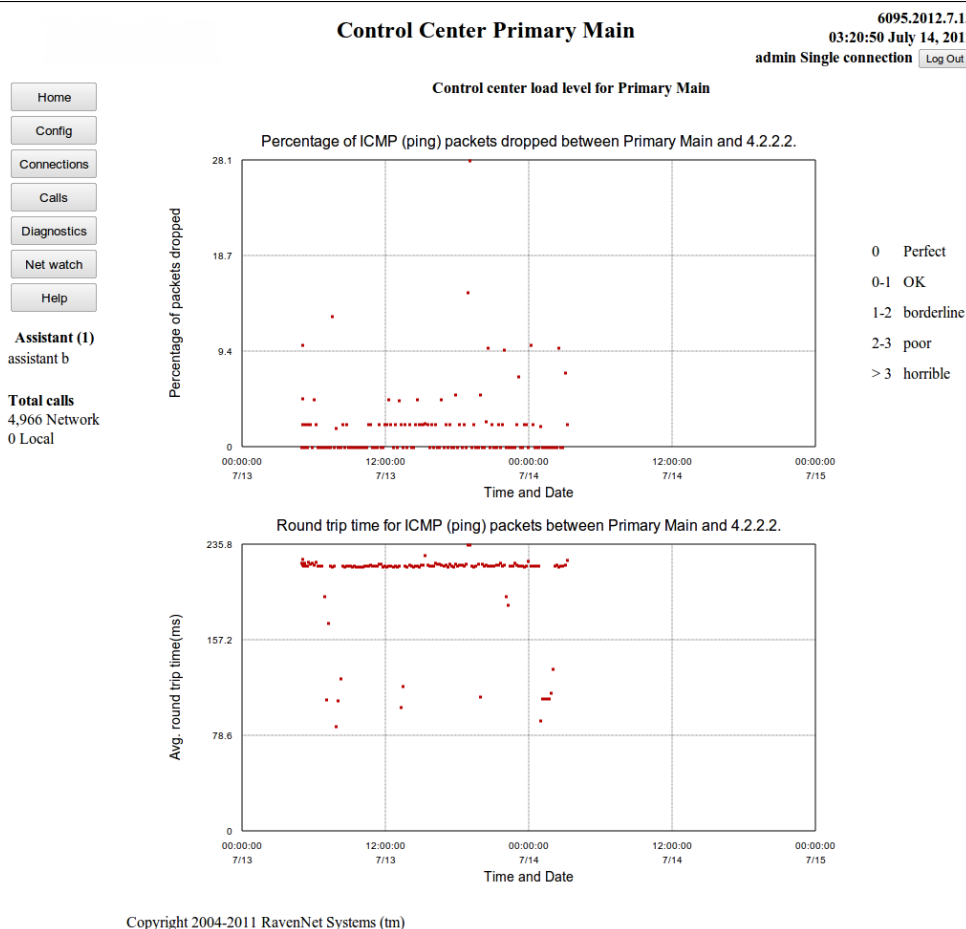
The measured performance above is not ideal - remote users trying to control this *Control Center* will

probably experience slow response times to clicking on web page elements.

5.7.6.3 Connectivity to remote host 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 5.3.1. This provides an estimate of the connection of the *Control Center* to an external host. Consequently, some hint is available to determine if the web pages will be slow/fast to respond. Further, if there is a high drop rate for packets, one can infer that audio packets will also be dropped, which can suggest if there will be an audio quality issue.

An example screenshot, taken over two days of operation is shown in Figure 85.

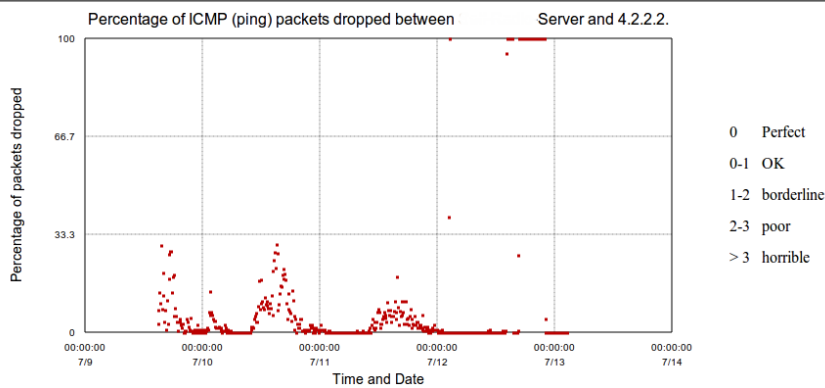
Figure 85 Example connectivity report with remote host



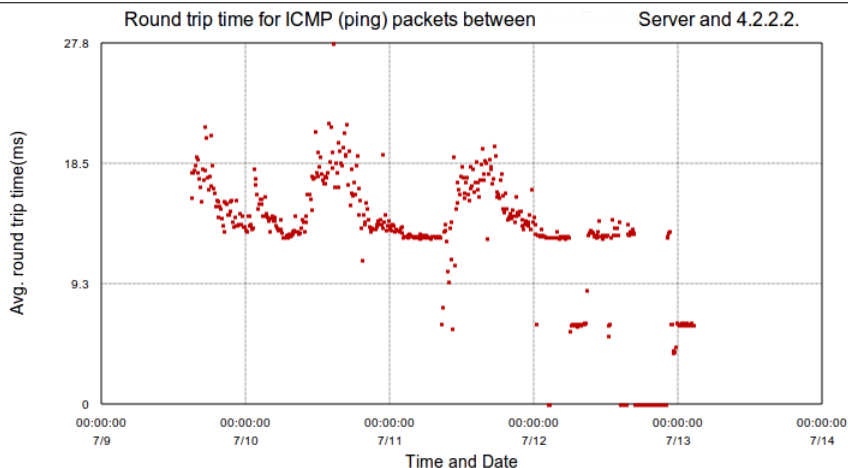
The report of connectivity between the Primary Control Center and the remote host (4.2.2.2). Almost all of the packets have the same round trip time, which suggest no variation in the route and the link is never saturated. This implies the user will have reasonable audio quality. Several packets have 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. From the bottom left of this figure, it is clear that no Gateways are 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 for between the *Gateways* and *Control Center*

To illustrate the purpose of this feature, consider the graphs in Figure 86 and Figure 87. The data in these graphs was copied from a customer who has 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 86 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 87 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 86. 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.

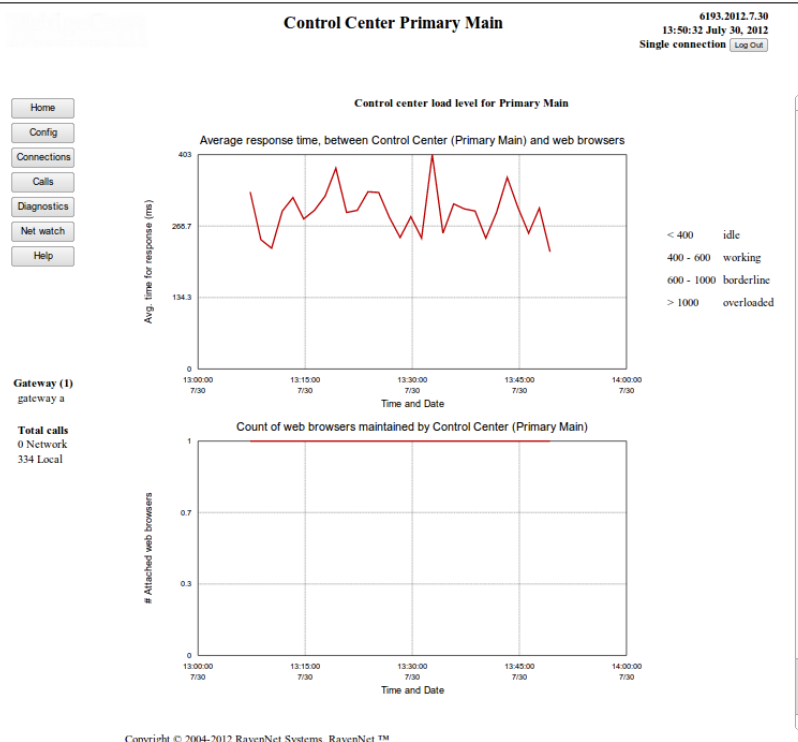
These two graphs illustrate a *Primary Control Center* that is operating with a very poor network connection. The network connection is not correctly handling packets - they are being dropped. Consequently, audio packets will be dropped during periods of peak load.

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%.

5.7.6.4 Response time of web pages 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 88.

Figure 88 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.

5.7.6.5 IP address of connected machines 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 89.

Figure 89 IP Addresses of connected machines

Control Center Primary Main

6269.2012.8.11
12:54:53 August 11, 2012

a [+ 1 other](#) [Log Out](#)

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

Gateway (1)
gateway a

Total calls
25 Network
0 Local

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](#)

Copyright 2004-2012 RavenNet Systems

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 89 is quite meaningless - the letter s. It is recommended that you use a longer name. For the record, the username can be any length.

5.7.7 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 90 there is a sample screenshot taken from the *Primary Control Center*.

Figure 90 Logs of link status

6110.2012.7.17
 19:32:31 July 17, 2012
 Single connection

Control Center Primary Main

Logs of control links on Primary Main

-
-
-
-
-
-
-

Gateway (1)
gateway a

Total calls
58 Network
168 Local

Copyright © 2004-2012 RavenNet Systems™

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, 2 are reported on.

5.7.8 Upgrades serviced by Primary Main

is a report of which boxes this *Primary 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). If the *Primary 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 91, which shows the upgrades serviced by the *Primary Control Center*.

Figure 91 Upgrades serviced by *Primary Control Center*

6146.2012.7.21
02:34:36 July 21, 2012
admin Single connection

**Control Center Primary
Main**

Home

Config

Connections

Calls

Diagnostics

Net watch

Help

Status of upgrades provided on Primary Main

Current Upgrades
=====

Description	Progress	Elapsed time	Est. Remining time

Completed Upgrades
=====

Remote Gateway	Duration	Completed at
monster (10.0.0.61)	0 seconds	02:28:49 July 21 2012

Gateway (1)
gateway a

Total calls
0 Network
36 Local

Statistics
=====

active 0
terminated 1

Copyright 2004-2012 RavenNet Systems

The upgrades serviced by the Primary Control Center The list clearly shows that the remote box at 10.0.0.3 has brought down 4 upgrade images. Each upgrade was downloaded in four seconds, which is typical for when both boxes are the on the same local area network. The remote box was not able to use the supplied image and tried many times to get an image. Multiple attempts from the same remote box normally indicate an error. In this case, the developer code on the remote box was causing it to try again and again.

The buttons at the bottom of Figure 91 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 92.

Figure 92 Message log on Upgrade Server

6146.2012.7.21
02:35:18 July 21, 2012
admin Single connection

Control Center Primary Main

-
-
-
-
-
-
-

Gateway (1)
gateway a

Total calls
0 Network
38 Local

Messages of upgrades provided on Primary Main

02:28:48.660	July 21 2012	Request from monster
02:28:48.760	July 21 2012	Update Service of monster (10.0.0.61) commences now.
02:28:49.559	July 21 2012	Upgrade of monster (10.0.0.61) [duration 0 seconds] is terminated.

Copyright 2004-2012 RavenNet Systems

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 Primary 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.

5.7.9 All Failed Calls

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.

5.7.10 Diagnostic on Gateway

takes the web page to the diagnostic page on the remote Gateway box. The diagnostic page there is similar to this page. Notable differences are the Gateways name 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. In Figure 93 there is an example screenshot of how this looks, taken for gateway a.

Figure 93 Diagnostic on a remote Gateway

6110.2012.7.17
19:21:38 July 17, 2012
Single connection

Control Center Primary Main

-
-
-
-
-
-
-

Gateway (1)
gateway a

Total calls
31 Network
168 Local

Diagnostic tools & reports on gateway a

gateway a has been running for 1 hour, 29 mins

Ch - 1	HR #1	<input style="color: green; font-weight: bold; font-size: small; width: 40px; height: 15px; border: none; border-radius: 3px; text-align: center; vertical-align: middle;" type="button" value="Status"/>
Serial device		<input style="color: green; font-weight: bold; font-size: small; width: 40px; height: 15px; border: none; border-radius: 3px; text-align: center; vertical-align: middle;" type="button" value="Status"/>
USB URI Devices		<input style="color: green; font-weight: bold; font-size: small; width: 40px; height: 15px; border: none; border-radius: 3px; text-align: center; vertical-align: middle;" type="button" value="Status"/>

Copyright © 2004-2012 RavenNet Systems™

The diagnostics image, taken for remote Gateway a. 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.

5.7.10.1 Scan for Hoot-n-Holler devices is used on *Gateways* when a custom piece of external hardware is available. If the name means nothing to you then ignore this button.

5.7.10.2 Monitor levels, generate 1khz tone is used on *Gateways* to quickly test and set the audio volume levels for each channel.

5.7.10.3 Command to LTR 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.

5.7.10.4 Reset LTR device 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.

5.7.10.5 Network Information generates the screen shown in Figure 94 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 94.

Figure 94 Network Information Window for a *Gateway*

6146.2012.7.21
02:58:51 July 23, 2012
admin Single connection [Log Out](#)

Control Center Primary Main

Network information on gateway b

Home
Config
Connections
Calls
Diagnostics
Net watch
Help

Gateways (2)
gateway a
gateway b

Total calls
23 Network
18,138 Local

Copyright 2004-2012 RavenNet Systems

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 81 and Figure 94 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.

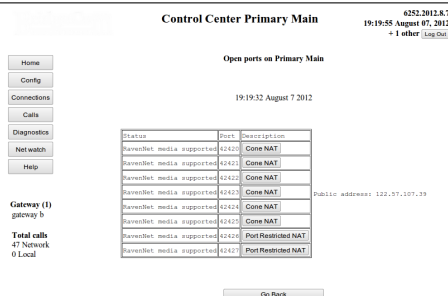
5.7.10.5.1 NAT report Is essentially unchanged from Section 5.7.6.1. It is only the *Control Center* that must have open ports, which means that the *Gateway* can establish a link to the *Control Center*. This report does describe the status of the NAT which can have an influence on *I.P.S.C.* connections (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.

An example screenshot of the test result is shown in Figure 95. The public IP address of *Primary Main* is shown to the right of the result table.

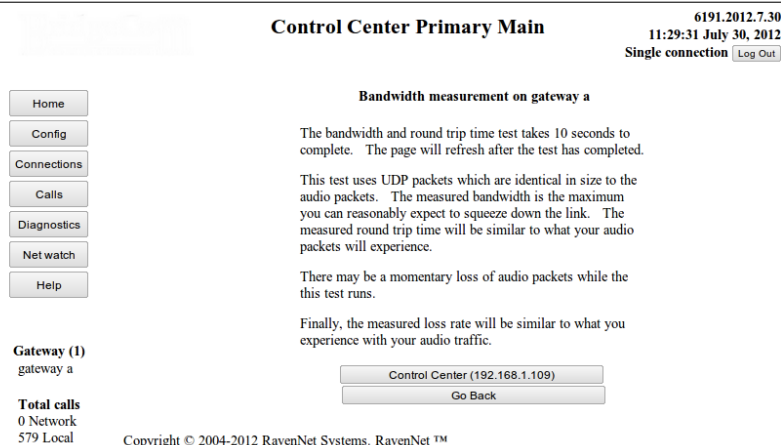
Figure 95 NAT report for Control Center



The report on the particular NAT in from of the Control Center with sitename Primary Main. The ports tested (42420..42427) 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. In this case, the report says that an external box cannot establish a connection to this Control Center. Consequently, external Gateways will not be able to connect to this Control Center. Web browsers (not on the LAN of the Control Center) will not be able to connect to this Control Center.

5.7.10.5.2 Measure bandwidth Provides fewer options to that listed in Section 5.7.6.2. 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 96.

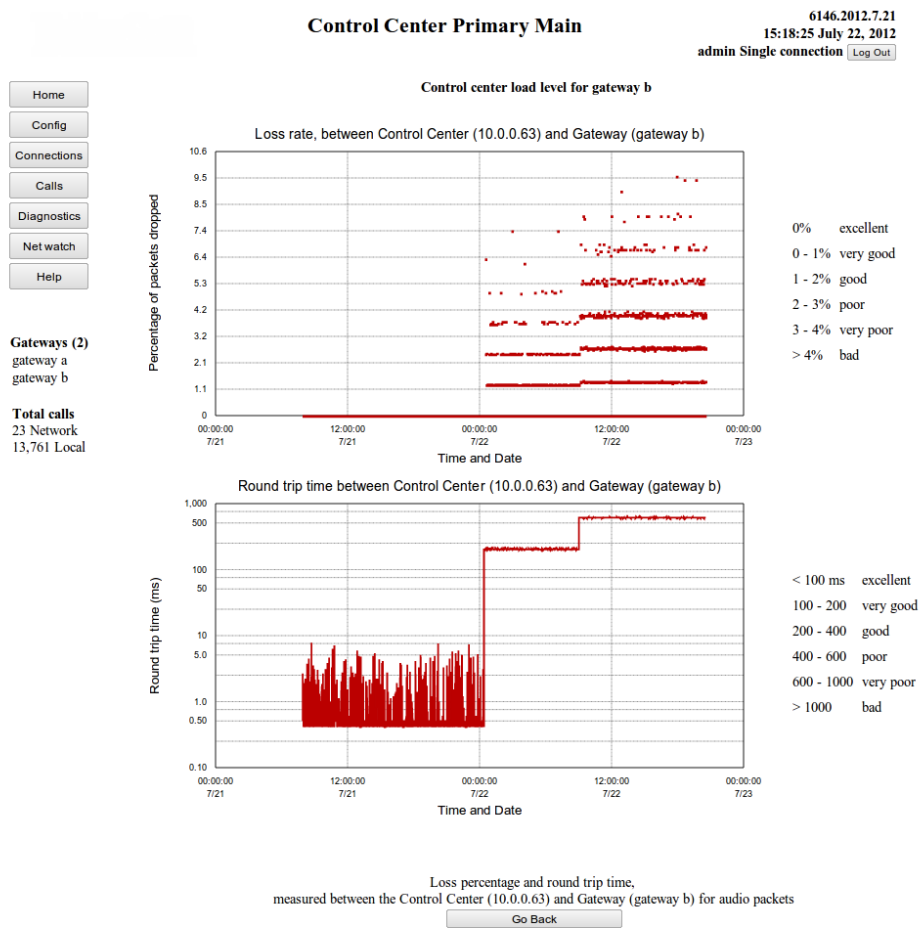
Figure 96 Gateway initiated measurement of bandwidth



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.

5.7.10.5.3 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 97.

Figure 97 Network performance between Gateway a and Primary Control Center



Copyright 2004-2012 RavenNet Systems

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 summarise the data shown in Figure 97, it falls into three periods:

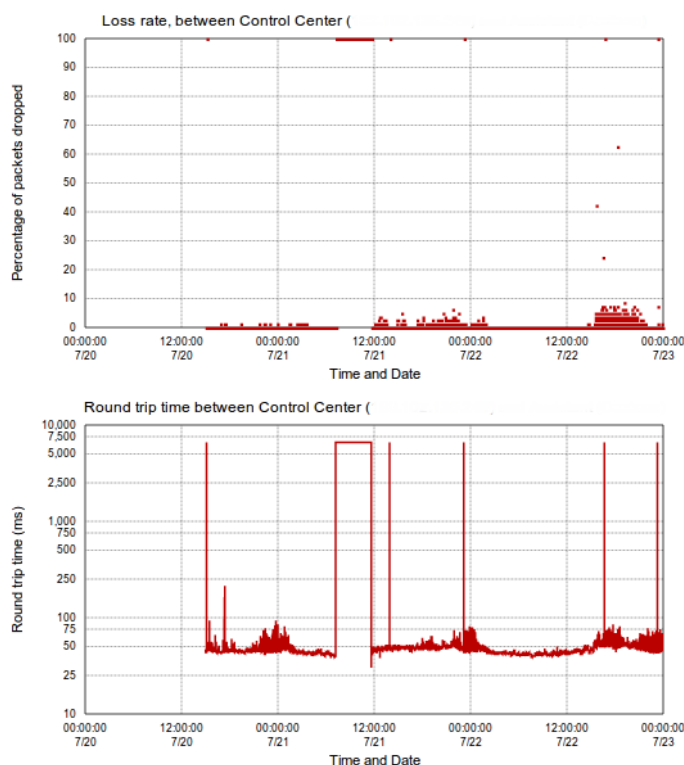
1. 18 hours long, round trip times 0.4-7.5ms, loss rate 0.0%. Excellent network conditions. Voice quality will be near perfect
2. 10 hours long, round trip times 400ms, loss rate 0-2%. There are a few datapoints over 2% loss rate - these are the exception so can be ignored.
3. 12 hours long, round trip times 600ms, loss rate 0-4%. Again, there are some datapoints 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 good calls, and then bad calls, and then more bad calls, and then good 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 might be an issue.

To give the reader an understanding of the importance of this diagnostic feature, consider the graph shown in Figure 98.

Figure 98 Abysmal link *Control Center* to *Gateway*

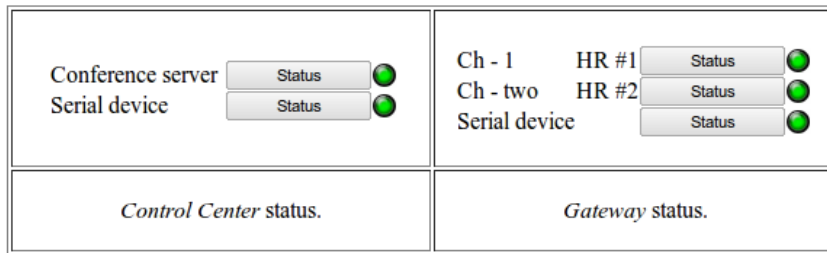


Long term report of the link between a Control Center and a Gateway. There is a four hour window (just before midday on July 21st) where no packets travelled between the Control Center and the Gateway. Clearly, the remote Gateway was not sending/receiving audio to/from the Control Center. On other days, 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.

5.7.11 Reports on the operation of an audio circuit

In Section 5.4 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 99.




Figure 99 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 both 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 5.7.11.1. The *home repeater* number of the audio channel is displayed to the left of the button.

5.7.11.1 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 good connection

between the Gateway and Control Center that can carry voice is indicated by . A connection (or entity) that is not active is reported as . Finally, 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.

5.7.11.2 Status of one audio channel An example screenshot for the status of one audio channel is displayed in Figure 100. A window similar to this can be obtained by pressing the status button in Figure 99. 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 just causes the status report for this channel to be redisplayed.

Figure 100 Status of one audio channel

6246.2012.8.6
 19:17:16 August 06, 2012
 Single connection [Log Out](#)

Home

Config

Connections

Calls

Diagnostics

Net watch

Help

Control Center Primary Main

Status Ch - 1 on gateway a

Summary
 =====
 Time : 03:16.48.771
 Status : Operational
 Active for: 1 min, 56 secs

USB URI device
 =====
 Alsa card number is 1
 Play level=70, Record level=22
 Write Frames to USB URI device 0

Sound card operation
 =====
 Read time (56.42 56.78 57.10 57.39 57.65 57.88 58.09 58.28 58.45 56.02)ms Range: 34.36 - 112.95 ms
 Write time (59.78 59.80 59.82 59.83 59.85 59.86 59.87 59.70 59.73 59.75)ms Range: 29.79 - 90.14 ms
 Device name Device name not currently available
 Minimise USB bus usage.

Connection to 10.0.0.62 active for 1 minute, 56 seconds
 Current codec is SpeexIETFNarrow-24.6k
 Audio flow status : quiet - no flows
 Time difference between Primary Control Center and Ch - 1 is 2.259 seconds.
 the Primary Control Center is ahead of Ch - 1

Audio Packets Transferred
 =====
 lost No packets received, no loss report
 received 0 packets from 10.0.0.62 (10.0.0.62)
 send 1627 packets to 10.0.0.62 (10.0.0.62)

Jitter buffer
 =====
 Buffer overruns 0
 Consecutive buffer overruns 0
 Consecutive marker bits 0
 Current depth 0 packets
 Current jitter time 120 ms
 Last write time stamp 0 ms
 Min Jitter time 120 ms
 Max Jitter time 3000 ms
 Packets too late 0
 Target jitter time 120 ms

Audio bandwidth 24.22 KBits/sec
 Total bandwidth 31.25 KBits/sec

Copyright 2004-2012 RavenNet Systems

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

The text report in the top half of Figure 100 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 *Active for* 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 5.3.3).
- 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 5.3.5. 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.
- 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.

5.7.11.2.1 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 101 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 100.

Figure 101 Message log for one audio channel

0240.ZUI2.8.0
19:16:04 August 06, 2012
Single connection [Log Out](#)

Control Center Primary Main

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
03:14:58.863	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

Gateway (1)
gateway a

Total calls
16 Network
0 Local

Clear messages log
Current status
Message log
Error log
Go Back

Copyright 2004-2012 RavenNet Systems

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.

5.7.11.2.2 Error log for one audio channel In Figure 102 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 rebuild 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 100.

Figure 102 Error log for one audio channel

6246.2012.8.6
19:16:38 August 06, 2012
Single connection [Log Out](#)

Control Center Primary Main

Home

Config

Connections

Calls

Diagnostics

Net watch

Help

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

Gateway (1)
gateway a

Total calls
21 Network
0 Local

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.

5.7.11.3 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 103.

Figure 103 Status of the Conference Server

6246.2012.8.6
19:24:36 August 06, 2012
Single connection [Log Out](#)

Control Center Primary Main

Home

Config

Connections

Calls

Diagnostics

Net watch

Help

Status Conference Server on Primary Main

Current Members

```
allcomponents @ Ch-1 @ 1 @ gateway a @ Ne working - audio is flowing - allcomponents @ Ch-1 @ 1 @ gateway b @ Ne
allcomponents @ Ch-1 @ 1 @ gateway b @ Ne working - audio is flowing Receive audio from allcomponents @ Ch-1 @ 1 @ gateway a @ Ne
Ch-two @ 2 @ gateway b inactive - quiet
```

Not completed 0

Conference server has been active for 12 minutes, 7 seconds

Gateways (2)
gateway a
gateway b

Total calls
85 Network
0 Local

Announcement tracks on Primary Main

Current status

Message log

Error log

Go Back

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 103 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 5.7.11.4.
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* Return to the previous screen, which causes the browser to display the previously displayed screen.

5.7.11.4 Announcement tracks on the Conference Server 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 103). An example screenshot is below in Figure 104.

Figure 104 Announcement tracks on the *Control Center*

6246.2012.8.6
 19:34:49 August 06, 2012
 Single connection

Control Center Primary Main

<input type="button" value="Home"/> <input type="button" value="Config"/> <input type="button" value="Connections"/> <input type="button" value="Calls"/> <input type="button" value="Diagnostics"/> <input type="button" value="Net watch"/> <input type="button" value="Help"/>	<p>Status of Announcement tracks on Primary Main</p> <p>Current announcements are</p> <table border="1" style="width: 100%; border-collapse: collapse; margin: 5px 0;"> <tr> <td style="padding: 2px;">SpeexIETFNarrow-24.6k</td> <td style="padding: 2px;">sample_message.wav</td> </tr> </table> <p>Server has loaded in 1 announcement from remote PC client(s)</p> <p>Statistics ===== active 0 terminated 1</p> <div style="margin-top: 10px;"> <input type="button" value="Current status"/> <input type="button" value="Message log"/> <input type="button" value="Error log"/> <input type="button" value="Go Back"/> </div>	SpeexIETFNarrow-24.6k	sample_message.wav
SpeexIETFNarrow-24.6k	sample_message.wav		
<p>Gateways (2) gateway a gateway b</p> <p>Total calls 8 Network 0 Local</p>			

Copyright 2004-2012 RavenNet Systems

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.

5.8 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 105.

Figure 105 Net watch window

6076.2012.7.3
20:02:50 July 04, 2012

Single connection

Control Center Primary Main

Home

Config

Connections

Calls

Diagnostics

Net watch

Help

Assistants (2)
assistant a
assistant b

Total calls
468 Network
0 Local

Network watch Filter: Peer

CC->CC

Current Talker

start time	duration	ch	name	source peer id	source radio id	source peer alias	source radio alias	Group ID	RSSI (dBm)	site name
20:02:55.6 Jul/4	1.0	1	Ch - 1							assistant a1

Voice Log

start time	duration	ch	name	source peer id	source radio id	source peer alias	source radio alias	Group ID	RSSI (dBm)	site name
20:02:31.6 Jul/4	12.1	1	Ch - 1							assistant a1
20:02:07.6 Jul/4	12.0	1	Ch - 1							assistant a1
20:01:43.6 Jul/4	12.0	1	Ch - 1							assistant a1
20:01:19.6 Jul/4	12.0	1	Ch - 1							assistant a1
20:00:55.6 Jul/4	12.0	1	Ch - 1							assistant a1
20:00:31.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:59:43.6 Jul/4	12.0	1	Ch - 1							assistant a1
20:00:07.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:59:19.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:58:55.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:58:31.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:57:43.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:58:07.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:57:19.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:56:55.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:56:31.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:55:43.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:56:07.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:55:19.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:54:55.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:54:31.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:53:43.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:54:07.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:53:19.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:52:55.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:52:31.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:51:43.6 Jul/4	12.0	1	Ch - 1							assistant a1
19:52:07.6 Jul/4	12.0	1	Ch - 1							assistant a1

Copyright © 2004-2011 RavenNet Systems ®

The window which enables all with login privileges to watch network activity.

At the top of the screen there are some buttons which enable more (or less) call information to be displayed. Clicking the buttons will automatically add/remove information from the display. None of these buttons can alter the performance of the *Control Center* in any way. Since the system can handle digital calls from Motorola devices, fields for peer ID, Radio ID, RSSI are listed. These fields are left empty for LTR calls. When calls are conveyed *Control Center* to *Control Center*, these are recorded in the *CC->CC* table, which is accessed by clicking on the relevant button at the top of the screen.

The *CC to CC* button is on, so the line displaying the links between *Control Centers* is displayed. At the moment, there is a call going from this *Control Center* to a remote *Control Center*. From the perspective of this *Control Center*, the outgoing link is a destination, so is displayed in the red color. The *Current* button is green, which means the *Current talker* table is displayed. The *Voice* button is green, so voice calls are displayed. Since the *Destination* button is off, recipients of calls are not displayed. Since entries in the *Current talker* table represent active calls, the duration reported will be increased with each display update.

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 106.

Figure 106 Help window

6344.2012.8.23
18:50:35 August 23, 2012
admin

Control Center Primary Main

Radio networking over the internet [Next](#)

Radio networking over the internet

Table of Contents

- [1. Introduction](#)
- [2. Terms and concepts](#)
 - [2.1. Bridge Group](#)
 - [2.2. Configuration](#)
 - [2.3. Firewalls](#)
 - [2.4. Components](#)
 - [2.5. Control Center Inbound and Outbound](#)
 - [2.6. Variations](#)
 - [2.7. It is a computer](#)
 - [2.7.1. Backup](#)
 - [2.8. Interpretation of graphs](#)
- [3. Web page interface](#)
 - [3.1. Login](#)
 - [3.2. Main page](#)

Copyright 2004-2012 RavenNet Systems

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*