



CMG-EAM and DCMs with Platinum firmware

Operator's Guide

Part No. MAN-EAM-0001

Designed and manufactured by
Güralp Systems Limited
3 Midas House, Calleva Park
Aldermaston RG7 8EA
England

Proprietary Notice: The information in this manual is proprietary to Güralp Systems Limited and may not be copied or distributed outside the approved recipient's organisation without the approval of Güralp Systems Limited. Güralp Systems Limited shall not be liable for technical or editorial errors or omissions made herein, nor for incidental or consequential damages resulting from the furnishing, performance, or usage of this material.

Issue B 2009-07-17

Table of Contents

1 Introduction	4
1.1 Hardware Overview.....	4
1.2 Software Overview.....	5
1.3 A Note on Terminology.....	6
1.4 Document Conventions.....	7
2 Connecting to the CMG-EAM	8
2.1 Connecting by Serial Port.....	8
2.2 Connecting by the Web Interface (HTTP).....	10
2.3 Connecting by SSH.....	13
3 Operation	15
3.1 Diagnostics and the Summary menu.....	15
3.2 The Control Menu.....	19
3.3 Tools Menu.....	25
3.4 Tools - Removable Disk.....	33
4 Digitiser Configuration	39
5 Data Handling Overview	45
6 Configuration	47
6.1 Password.....	47
6.2 Configuration System.....	48
6.3 Configuration Management.....	50
6.4 Setting the System Identity (Hostname).....	52
6.5 Serial Port Configuration.....	52
6.6 Setting up a PPP Connection.....	54
6.7 Monitoring a PPP connection.....	56
6.8 To Customise GCF Output Settings.....	58
6.9 Configuring NMEA Output.....	60
6.10 Configuring TCP to serial converters.....	61
6.11 Networking.....	64
6.12 Configuring the Network Time Protocol (NTP) Daemon	65
6.13 Configuring the Mail Transfer Agent (MTA)	66
6.14 Configuring the SSH Server.....	67

6.15 Configuring Port Power Limits.....	68
6.16 Configuring Additional Data Input Services.....	69
6.17 Data Storage.....	75
6.18 Configuring Additional Data Output Formats.....	80
6.19 Gralp Secure TCP Multiplexer.....	88
6.20 Routemaster robust networking.....	95
7 Appendices.....	100
7.1 Connector pin-outs.....	100
7.2 Using Minicom.....	105
8 Revision history.....	107

1 Introduction

The CMG-EAM (Embedded Acquisition Module) is a versatile module intended to integrate one or more seismic sensors with various communications systems. It can also act as a stand-alone data recorder or as a communications hub in larger networks.

This document describes the configuration and operation of Platinum Firmware, which is the native firmware of CMG-EAMs and CMG-NAMs (described below). CMG-DCMs can be upgraded to run Platinum firmware: for such units, this manual should be used instead of MAN-DCM-0001.

The CMG-EAM is a Linux-based device but this document assumes no Linux knowledge. The use of Linux provides a high degree of flexibility: Additional functionality can be added on request – contact Güralp Systems for further information.

The CMG-NAM (Network Appliance Module) is a rack-mountable device intended to complement data communications networks using CMG-EAMs, and contains more processing power and storage. Unlike the CMG-EAM, the CMG-NAM is intended for a data centre and consumes considerably more power than the CMG-EAM, which was designed specifically to be a low power device.

1.1 Hardware Overview

Platinum firmware runs on CMG-EAMs, CMG-NAMs and CMG-DCMs. CMG-DCM units (Mk2 and above) shipped with earlier firmware can be field-upgraded to run Platinum firmware either over the internet or from a local data storage device.

The CMG-EAM is based upon an Intel PXA270 32-bit processor running at 312MHz with 64Mb of RAM and 512Mb of on-board flash. The amount of flash memory can be increased with the use of Güralp plug-in flash modules. The CMG-EAM has 100-Base-TX Ethernet, up to 8 serial ports for connecting to external devices and several USB ports.

The CMG-DCM uses an Intel SA1100 (StrongArm) 32-bit processor running at 220MHz with 64Mb of RAM and 192Mb of on-board flash. The CMG-DCM has up to 7 serial ports for external devices and 10-Base-T Ethernet.

The CMG-NAM is a flexible platform but is generally based upon a VIA C7 processor with 512Mb of RAM and various options for local storage, including RAID arrays. It has 100-Base-TX Ethernet.

1.2 Software Overview

The CMG-EAM software is very flexible and can be configured to perform many tasks. An overview of its capabilities is presented here:

- Data acquisition:
 - Data can be acquired in various formats via Ethernet or serial ports.
- Recording:
 - Data can be recorded to removable disk in various formats. Recording initially occurs to internal flash, which is flushed to removable disk when full or on demand. This minimises power usage;
 - The removable disk can be removed at any time without data loss.
- Data forwarding:
 - GCF output via serial port or TCP stream;
 - GCF output via Scream Server (TCP/UDP);
 - Güralp Data Interconnect (GDI);
 - CD1.1 output;
 - WIN output;
 - QSCD (Quick Seismic Characteristic Data; designed by KIGAM) output;
 - GSMS (Güralp Seismic Monitoring System) output.
- Network communication:
 - The CMG-EAM has a built-in wired Ethernet connection;
 - Modem support (Iridium, GPRS, etc.);

- Other connectivity options, such as wireless Ethernet (IEEE802.11) and Bluetooth can be added on request, please contact Güralp sales for more information.
- Processing:
 - Various types of data processing can be carried out by the CMG-EAM. Please contact Güralp sales for more information.

Section 5 gives a description of how data is handled within the CMG-EAM.

1.3 A Note on Terminology

Güralp Systems Ltd are aware that various common technical terms have acquired subtly different meanings for different audiences. The following terms are used consistently within this document and are intended to have the meanings given below:

Sensor

By “sensor”, we mean a seismometer (accelerometer or velocimeter) or other transducing instrument (e.g. geophone or hydrophone) with analogue outputs - i.e. where a continuously varying voltage is used to represent the magnitude of the quantity being measured.

An example of a sensor is the CMG-3T true broadband seismometer, depicted on the right in standard configuration.



Digitiser



By “digitiser”, we mean an electronic device designed to accept analogue inputs from one or more sensors and, using sampling techniques, convert these analogue signals into streams of numerical data, which are then stored or transmitted digitally.

An example of a digitiser is the CMG-DM24 shown on the right in standard form and, on the left, configured for borehole operation.



Digital Sensor or Digital Instrument

By “Digital Sensor” or “Digital Instrument”, we mean a single unit combining the functions of both sensor and digitiser - with the meanings defined above.



Within this document, the term digital sensor is used in the context of either digital inputs - which may usefully be connected to either digitisers or digital sensors - or configuration dialogues which can be used to configure both stand-alone digitisers or the digitiser modules embedded within digital sensors.

An example of a digital sensor is the CMG-3TD true broadband digital seismometer, shown on the left in standard configuration and, on the right, in bore-hole format.



1.4 Document Conventions

When displaying examples of interaction with the command-line interface, a fixed-width typeface will be used:

`Example of the fixed-width typeface used.`

Commands that you are required to type will be shown in bold:

`Example of the fixed-width, bold-face typeface.`

Where data that you type may vary depending on your individual configuration, such as parameters to commands, these data are additionally shown in italics:

`Example of the fixed-width, bold-faced, italic typeface.`

2 Connecting to the CMG-EAM

As the CMG-EAM is a very versatile device, it offers several methods of connection.

The CMG-EAM can be configured via its serial port, via the network interface using SSH or via the network interface using its internal web server. The normal method of control is via the web interface although it may be necessary to use the serial port initially to configure or determine the network address.

2.1 Connecting by Serial Port

The CMG-EAM's *Data Out* port can be connected via a serial (RS232) cable to a serial terminal or PC running either *Scream!* or terminal emulation software. The default settings for the CMG-EAM's Data Out port are as follows:

- 115,200 baud;
- 8 data bits, no parity, 1 stop bit (8N1); and
- No flow control.

In addition, the CMG-EAM (but not the CMG-NAM) has an internal "Console" connector located under the lid. This is a standard 9-way D-sub to which a terminal emulator can be connected. The settings are fixed at 38400 baud, 8N1 and no flow control.

Once you have connected a serial cable, you can run a terminal emulator to interact with the CMG-EAM. Under Windows you are advised to use the terminal emulator shipped with *Scream! v4.5*, although HyperTerminal can be used. Under Unix or Linux, Miquel van Smoorenburg's *minicom* terminal emulator (more details from <http://alioth.debian.org/projects/minicom>) is recommended, although most terminal emulators can be used. An extract from Minicom's user manual is reproduced in Section 7.2, on page 104.

Once connected, press the <Enter> key until you see the login prompt. **Note:** *If a terminal session has just been closed, it can take up to 10 seconds for a new session to start.*

You should log in as *root*, which is the standard Unix "superuser". The password is set to *rootme* when shipped from the factory. To log in, type *root* and press enter. When prompted for the password, type *rootme* (nothing will be echoed while you are typing) and press

<enter>. You will then be presented with a shell prompt, which will accept commands:

```
eam999 login: root
Password: rootme
eam999 ~ #
```

The output may vary slightly due to the configuration of the unit. In particular, the hostname (`eam999` in this example) will be different.

Some applications on the CMG-EAM use a system called “ncurses”, which allows graphical interfaces to be implemented on text-only terminals. This requires the applications to know the type of terminal from which they are being accessed. The terminal type is stored in an environment variable called `TERM`, which is queried with the command

```
eam999 ~ # echo $TERM
vt100
eam999 ~ #
```

(note the use of the \$ sign when accessing the value of this variable) and set with the command

```
eam999 ~ #: export TERM=vt100
```

No spaces should be used around the '=' sign.

The CMG-EAM is aware of over 2,500 different terminal types and uses the “terminfo” system to support them. Files describing each terminal type are stored under the directory (folder) `/usr/share/terminfo` in sub-directories named after the initial letter of the terminal name.

Some settings for specific applications are:

- SSH under Unix, or `puTTY` under Windows (running in SSH mode): no action required - the SSH protocol sets the `TERM` environment variable automatically.
- Minicom under Unix: no change. Minicom emulates a vt100-style terminal and automatically maps the keystrokes and display sequences for the actual terminal you are using, so the default `TERM` setting of `vt100` is correct.
- HyperTerminal under Windows: choose the File menu option “Settings”, and ensure that the terminal type is set to `VT100`.

HyperTerminal will then emulate a vt100-style terminal, which will match the default TERM of vt100 on the CMG-EAM.

These settings will provide the best results for the listed applications. Note that when connecting with SSH from, for example, an xterm window, use of the mouse for menu navigation is supported.

2.2 Connecting by the Web Interface (HTTP)

The CMG-EAM provides a web (HTTP) interface which is intended for most configuration and control tasks. This is the recommended way of controlling the CMG-EAM.

To use the web interface, you must first set up a network address. Some networks use the Dynamic Host Configuration Protocol (DHCP) to automatically assign network addresses; others need manual configuration (normally referred to as “static” addressing). Before you can access the web interface of the CMG-EAM, you must set (for static addresses) or discover (if you use DHCP) its IP address.

If you are setting up an instrument in the laboratory for subsequent deployment in the field, you can set up the final network address using the web interface and over-ride it with a temporary network address using the command line. The web-configured address will take effect when the unit is next rebooted.

DHCP-assigned addresses

If your network uses DHCP to assign addresses, connect the CMG-EAM to the network and reboot it by turning the power off and on again. Your network administrator may then be able to tell you the address that has been assigned to the CMG-EAM but, if not, you can connect via a serial port and issue the `ip` command:

```
eam999 ~ # ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast qlen 1000
    link/ether 00:50:c2:40:54:75 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.101/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::250:c2ff:fe40:5475/64 scope link
        valid_lft forever preferred_lft forever
eam999 ~ #
```

The key things to look for here are the adapter status and the IP address. The first line of the output should contain the word `UP`, confirming that the adaptor has been enabled. The IP address that has been assigned is shown on the line beginning `inet` - in this case, it is `192.168.0.101` (with a netmask of 24-bits indicated by `/24`). **Note:** *With an IP version 6 network, the IP address will be on a line beginning*

inet6. In practice, most networks today are still IPv4, as in the above example.

When using DHCP, it is recommended that the DHCP administrator allocates a fixed IP address to the CMG-EAM's MAC address in order to avoid unexpected address changes.

Assigning a static IP address

If the network you are connecting to does not use DHCP, you must first connect via a serial port in order to configure a static IP address. Connect the CMG-EAM to the network and power-cycle it before proceeding: its network interface will not be enabled unless it sees a network at boot.

Once logged in, issue the following command:

```
eam999 ~ # ip addr add 192.168.0.1/24 dev eth0
```

You can change the IP address to anything you wish. It must be specified in CIDR format where the actual address is followed by the number of bits of the network mask. The above example uses 192.168.0.1 with a netmask of 255.255.255.0 (24 bits of network address). A PC connected to this network could communicate with the CMG-EAM if it was configured to use an IP address of (for example) 192.168.0.2 with a matching netmask of 255.255.255.0.

If you wish to connect to the CMG-EAM from a PC, they must either both have the same network address (usually the first three numbers of the IP address) or be able to connect to each other via routers. In the latter case, you will need to tell the CMG-EAM the address of its default router. Issue the command:

```
eam999 ~ # ip route add default via 192.168.0.254
```

substituting the address of your network's default router in place of the address shown.

Note: *Both the static IP address and any route set in this way are temporary and will only persist until the CMG-EAM is rebooted or powered off. Refer to section 6.11, page 64 for information about permanent static IP addresses and routes.*

Connecting to the web interface

Now that the IP address of the CMG-EAM has been set or determined, you can connect to its web-server. Simply type `http://` followed by the IP address of the unit into your web browser's address bar (e.g.

http://192.168.0.1). You should be prompted for a user-name and password. The user-name is root and the initial password, as shipped, is rootme (the same as on the command line).

If you are connecting to the CMG-EAM over a network that may not be secure, it is recommended to use the HTTPS (secure HTTP) protocol, which uses TLS to encrypt the link. Simply change the http:// prefix to https:// in the browser's address bar. Most browsers will complain that the certificate cannot be verified: This is not a problem: simply press the “accept” button to proceed. The link will then be encrypted and nobody will be able to “sniff the wire” in an attempt to discover passwords and other data.

Once connected and logged in, you will be presented with the main summary screen. This contains general information about the status and health of the CMG-EAM:

Main menu
dcm105

Summary
[System events](#)
[System status](#)
[Version and serial numbers](#)

Control
[Port A sensor](#)
[GSLA-1566](#)
[Power](#)
[Services](#)

Tools
[CDI.1 log analyser](#)
[Firmware](#)
[GCF audit log viewer](#)
[GDI channels](#)

System uptime Status: good — 2009-06-23T09:36:17Z System has been up for approximately 3 days.	GCF in: Port A Status: good — 2009-06-23T09:37:30Z Last 5 minutes: <ul style="list-style-type: none"> • 112 blocks (0.4 per second). • 0 naks (0.0 per second). 	GCF in: Port B Status: unknown — 2009-06-23T09:37:30Z No blocks seen.
GCF in: Port F Status: unknown — 2009-06-23T09:37:31Z No blocks seen.	NTP Status: good — 2009-06-23T09:37:08Z <ul style="list-style-type: none"> • NTP has locked the system clock. • Estimated error is 3444µs. • Clock source is Guralp digitiser. 	

Generated at 2009-06-23T09:37:35Z by libstatus.cgi 1.2.6. Portions of output copyright (c)2009, Guralp Systems Ltd.

If the browser fails to connect, the most likely explanation is that the machine running the browser does not have working network communications to and from the CMG-EAM. This can be verified by “pinging” the IP address of the browser from the command line of the CMG_CMG-EAM:

```
eam999 ~ # ping -c3 192.168.0.2
PING 192.168.0.2 (192.168.0.2): 56 data bytes
```

```
64 bytes from 192.168.0.2: seq=0 ttl=63 time=2.284 ms
64 bytes from 192.168.0.2: seq=1 ttl=63 time=1.129 ms
64 bytes from 192.168.0.2: seq=2 ttl=63 time=1.944 ms

--- 192.168.42.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.129/1.785/2.284 ms
eam999 ~ #
```

To resolve this class of problem, ensure that the cables are functioning (which can be verified by checking the diagnostic lights on most switches/hubs) and double-check that the PC and CMG-EAM are on the same subnet (which means the netmasks must match and the first sections – as defined by the netmask - of the IP addresses must match). The website http://en.wikipedia.org/wiki/IP_address has some useful information for those for whom sub-networking is unfamiliar.

2.3 Connecting by SSH

SSH (secure **shell**) is the most flexible way to control a CMG-EAM, but it is less friendly than using the web interface. It is possible to configure more advanced operations using SSH but the majority of control and configuration tasks can be achieved most easily through the web interface.

SSH is shipped as standard with most Linux distributions and is available for Windows as part of *puTTY*, available for free from <http://www.chiark.greenend.org.uk/~sgtatham/putty/>

To use SSH, you must know or discover the IP address of the unit, as described in the previous section. Once you have the IP address, issue the **SSH** command on the PC you are using:

```
mypc$ ssh root@192.168.0.1
```

Replace **192.168.0.1** with the IP address of the CMG-EAM.

The first time you use SSH to connect to a host, you will be asked to verify the “host key”. This can be ignored the first time but, if you are ever asked this again, it means that either the host key of the CMG-EAM has changed – perhaps because of a firmware upgrade – or there is a network address conflict or, worse, a security problem on your network.

```
fish@fish-desktop: ~/.ssh$ ssh root@192.168.0.1
The authenticity of host '192.168.0.1 (192.168.0.1)' can't be established.
RSA key fingerprint is 62:a6:70:29:d4:1a:db:5a:75:6e:96:13:54:f5:a9:d9.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.1' (RSA) to the list of known hosts.
```

```
root@192.168.0.1's password:  
eam999 ~ #
```

You will be prompted for a password; the default password is `rootme`. Note that no characters will be echoed to the screen as you type the password.

Once connected, you will be presented with a shell prompt which is ready to accept commands.

When you are finished with your SSH session and want to disconnect, type “exit” at the command line, or a <Ctrl>D character. There are a number of escape sequences for controlling SSH, all of which being with a tilde so, if you need to send a tilde character to the CMG-EAM, type two tildes consecutively. For more information, see the section on “Escape Characters” in the SSH manual page at <http://linux.die.net/man/1/ssh>

***Note:** If you plan to use `ssh` regularly to communicate with a CMG-EAM, you can configure the system to bypass the password prompt from a list of pre-authorized computer/user combinations. This procedure involves generating a unique key-pair for the user and PC which will access the CMG-EAM and copying the public half of the key-pair to the CMG-EAM. See <http://suso.org/docs/shell/ssh.sdf> for tutorial information on how to configure this feature.*

3 Operation

This section details how to monitor and control the CMG-EAM. Some functionality is only available from the command line (when connected via a serial cable or via ssh over the network - see the previous section for details on how to do this). To change the way the CMG-EAM operates, see the next section for details on configuration settings.

3.1 Diagnostics and the Summary menu

System Status

To view the overall system status, simply go to the front page of the web interface (or choose the “System status” link in the left-hand frame within the “Summary” box).

From the command line interface, you can view the same information by running `libstatus-query`:

```
eam999 ~ # libstatus-query
=====
2008-05-01T13:57:52Z: Good : System uptime
-----
System has been up for approximately 4 days.

=====
2008-05-01T13:59:16Z: Unknown : GCF in: Port A
-----
No blocks seen.

=====
2008-05-01T13:59:17Z: Good : GCF in: Port F
-----
Last 5 minutes:
* 1532 blocks (5.1 per second).
* 0 naks (0.0 naks per second).

=====
2008-05-01T13:59:14Z: Good : NTP
-----
NTP has locked the system clock.
Clock source is UDP/NTP.

=====
2008-05-01T13:44:11Z: Good : Removable disk 0000-0401
-----
Filesystem type: vfat.
Size: 37.2GiB.
Free: 24.9GiB (66.9%).
Earliest entry: 2008091-gcfraw.
```

In the web view, one box is displayed per port or major subsystem. Boxes may be displayed in red (bad), green (good) or white (no information).

Main menu
dcm105

Summary
[System events](#)
[System status](#)
[Version and serial numbers](#)

Control
[Port A sensor](#)
[GSLA-1566](#)
[Power](#)
[Services](#)

Tools
[CD1.1 log analyser](#)
[Firmware](#)
[GCF audit log viewer](#)
[GDI channels](#)

System uptime Status: good — 2009-06-23T09:36:17Z System has been up for approximately 3 days.	GCF in: Port A Status: good — 2009-06-23T09:37:30Z Last 5 minutes: <ul style="list-style-type: none"> • 112 blocks (0.4 per second). • 0 naks (0.0 per second). 	GCF in: Port B Status: unknown — 2009-06-23T09:37:30Z No blocks seen.
GCF in: Port F Status: unknown — 2009-06-23T09:37:31Z No blocks seen.	NTP Status: good — 2009-06-23T09:37:08Z <ul style="list-style-type: none"> • NTP has locked the system clock. • Estimated error is 3444µs. • Clock source is Guralp digitiser. 	

Generated at 2009-06-23T09:37:35Z by libstatus.cgi 1.2.6. Portions of output copyright (c)2009, Guralp Systems Ltd.

Red boxes indicate that some part of the system is malfunctioning, and require further investigation. Malfunctions could occur due to hardware failure but the most likely explanation is an incorrect configuration item.

System Events

To view a log of important system events using the terminal, you can run the command `sysevent-query`:

```
eam999 ~ # sysevent-query
Info      | 2008-03-28T15:31:15Z: System booted
+-----+
System has just completed boot process.
```

The most recent event is shown first. The left-hand column shows the severity of the event. This can be, in increasing order of importance, “debug”, “info”, “notice”, “warning”, “error”, “critical”, “alert” or “emergency”.

To view the same list via the web interface, choose the “System events” link in the left-hand frame within the “Summary” box.

Verbose

Title and Date	Level	Entry
System booted 2008-04-29T15:42:47Z	Information	System has just completed boot process.
System booted 2008-04-26T16:30:19Z	Information	System has just completed boot process.
System booted 2008-04-26T10:15:59Z	Information	System has just completed boot process.
System booted 2008-04-26T09:59:46Z	Information	System has just completed boot process.
System booted 2008-04-26T09:48:34Z	Information	System has just completed boot process.
System booted 2008-04-26T09:27:20Z	Information	System has just completed boot process.
System booted 2008-04-26T09:11:02Z	Information	System has just completed boot process.
System booted 2008-04-26T08:54:51Z	Information	System has just completed boot process.
System booted 2008-04-26T08:38:40Z	Information	System has just completed boot process.
System booted 2008-04-26T08:22:29Z	Information	System has just completed boot process.
System booted 2008-04-26T08:06:15Z	Information	System has just completed boot process.

The most recent event is shown first.

Note: At present, very few components use the system events interface; in future versions of the firmware, all system logging will take place using this interface.

System Log

The most important source of information is currently the system log facility (“syslog”). This logs all messages from programs and from the Linux kernel. At present, this can only be viewed from the command line. In future, it will be integrated with the system events page.

To view the system logs, you can use the `tail`, `less`, `grep` or `vi` commands to inspect the file `/var/log/messages` - older files are available as `/var/log/messages.1`, `/var/log/messages.2` etc.

Under Linux you may use the following syntax to view the files:

- `tail /var/log/messages`
Views the last few entries.

- **tail -f /var/log/messages**
As above but also follows the log in real-time. Use <Ctrl>C to stop.
- **less /var/log/messages**
Views the whole log file; use Home/End/Up/Down keys to navigate.
- **vi /var/log/messages**
Those users familiar with the vi text editor may wish to use it as the most powerful way to view log entries.
- **grep -i 'string' /var/log/messages**
Searches for a string or pattern in the log file. This search is case insensitive (-i flag).

`grep` is a very powerful tool for searching for patterns. For more information, see the section on Regular Expressions in the `grep` manual page at <http://linux.die.net/man/1/grep>

Incoming Data

The status web-page has one box for each GCF acquisition process. This box will be updated every minute to reflect the number of packets that have been acquired.

To view details of incoming GCF format data using the command line, use one of the following commands:

- **gdi-dump -l**
Displays a list of channels and segments. For more information, see “GDI Channels Display” in section 3.3 on page 29;
- **gdi-dump -lm**
Displays the the same data, along with meta-data added by the relevant input module; or
- **gdi-dump**
Displays real-time information about each packet arriving, until interrupted by the operator typing a <Ctrl>C character.

Version and Serial Numbers

The “Version and serial numbers” item on the “Summary” menu displays information which may be useful for your own records or when requesting technical support.

3.2 The Control Menu

The “Control” menu of the web interface is a dynamic menu with content that changes depending on the attached devices. Two items on this menu are always present: “Power” and “Services”. CMG-NAM units fitted with RAID arrays will also have a “RAID array services” menu item.

Power Control

The “Power” item on the “Control” menu brings up the following screen, (the contents of which may vary with your hardware configuration):

Power control

Port Power Information				
Port Name	Voltage	Current	Power State	Power Control
Data Out	13404 mV	131 mA	on	Turn off Data Out
Port B	12622 mV	3666 mA	on	Turn off Port B

Reboot
Select this option to reboot the machine. The machine will be restarted without losing power.
<input type="button" value="Reboot"/>

Generated at 1970-01-01T04:19:49.943567998Z by power.cgi 1.0.0. Portions of output copyright (c)1970, General Systems Ltd.

The CMG-EAM mk4 hardware can be fitted with optional sensors to monitor the voltages and currents being supplied to the CMG-EAM and also to devices connected to the CMG-EAM ports, such as digitisers. A program on the CMG-EAM runs constantly in the background and monitors the sensors if they are fitted.

The top table on this page shows the current voltage and current on each sensor-equipped port of the CMG-EAM. There are also buttons to turn the power to the port on and off. Power is turned on by default when the CMG-EAM is powered up, but it can be turned off manually on this page, or automatically if the sensor detects an error condition on the port. See section 6.15 for instructions on setting the error condition limits on the ports. The port can only be turned on if there is no error condition present.

To view the CMG-EAM port power sensor information via the terminal, connect to the CMG-EAM command line as in section 2.1 or 2.3 and run the `powermgr` command.

```
eam999 ~ # powermgr
|=====|
|          Port          | Voltage | Current | Power |
|-----|
|          Data Out     | 13399 mV | 128 mA | on |
|-----|
|          Port B       | 12622 mV | 3666 mA | on |
|=====|
```

To turn the power to a particular port off or on via the terminal, run the `powermgr` command and specify the arguments `-p port_name -s power_state`, as in the example below.

```
eam999 ~ # powermgr -p "Data Out" -s off
'Data Out' power turned off

|=====|
|          Port          | Voltage | Current | Power |
|-----|
|          Data Out     | 13091 mV | 185 mA | off |
|-----|
|          Port B       | 12369 mV | 3666 mA | on |
|=====|
```

CMG-EAMs can be rebooted via the web interface. CMG-NAMs can be both rebooted and powered off. To reboot from the command line prompt, use the `reboot` command.

```
eam999 ~ # reboot
```

Digitiser Control

The CMG-EAM allows *control* of attached digitisers and sensors via the web interface or the command line. To *configure* digitisers, see section 4 on page 39.

The web interface is simpler and requires no detailed knowledge of the attached devices. The command line interface is more powerful but requires detailed knowledge of the digitiser's command line interface and the manual for the digitiser in question should be referred to for further details.

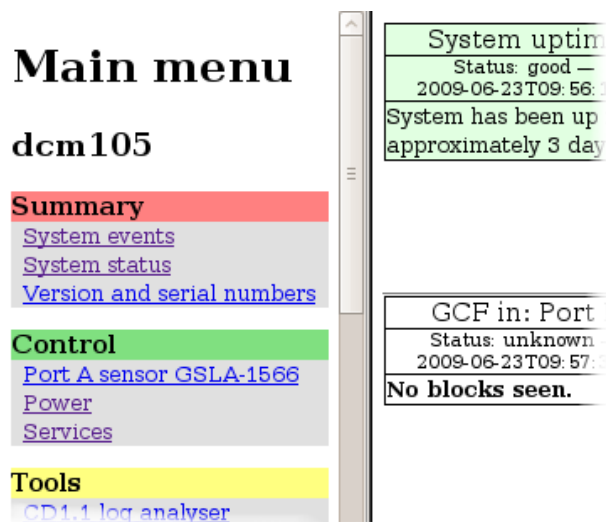
Digitiser/Sensor Control - Web interface

The web interface of the CMG-EAM adapts to include additional options when the CMG-EAM detects attached digitisers and digital sensors.

Extra items in the “Control” menu are associated with digitiser serial numbers. If a digitiser has two sensors attached to it, it is

recommended that an extra serial number be added to the digitiser. See the relevant digitiser manual for information on how to configure this.

The menu items look like this:



In this illustration, the entry

Port A sensor GSLA-1566

indicates the GSL-EAM connection (Port A) of the attached device, the device type (sensor) and its serial number (GSLA-1566). If the instrument is connected via TCP, the EAM connection is shown as host:port.

Selecting one of these menu items takes you to the “Digitiser Control” page. It is shown here in two sections. The first deals with the sensor masses:

Digitiser Control

A830-55TP/Port A/dcm105

Mass positions

<p>Query Masses</p> <p>Display the current mass positions of the instrument.</p> <p><input type="button" value="Run"/></p>	<p>Lock</p> <p>Lock the masses for transport.</p> <p><input type="button" value="Run"/></p>	<p>Unlock</p> <p>Unlock the masses after installation.</p> <p><input type="button" value="Run"/></p>
<p>Centre Masses</p> <p>Centre the instrument's masses.</p> <p><input type="button" value="Run"/></p>		

Buttons are provided to query the mass positions, to lock the masses for transport and unlock and centre them for deployment. The verbatim output from the attached device is displayed in each case. Where a specific device does not support a specific function, the command is safely ignored.

The second section of this web page deals with calibration. Note that all entered values must be integers so, for example, if you wish to calibrate with a 0.5Hz sine-wave, this should be entered as a 2 second period. Please refer to the relevant manuals for your digitiser and sensor for more details of these options.

The screen looks like this:

Calibration

Sine wave Calibration

Perform a calibration using a sine wave.

Component	All <input type="button" value="v"/>
Duration in minutes	<input type="text" value="2"/>
Amplitude (percentage)	<input type="text" value="100"/>
Frequency (Hz) or period (seconds)	<input type="text" value="1"/>
Units	Hz <input type="button" value="v"/>

Square wave Calibration

Perform a calibration using a square wave. The signal consists of a positive step of the given duration, followed by a negative step of the same duration.

Component	All <input type="button" value="v"/>
Duration in minutes	<input type="text" value="2"/>
Amplitude (percentage)	<input type="text" value="100"/>

Random Calibration

Perform a calibration using white noise.

Component	All <input type="button" value="v"/>
Duration in minutes	<input type="text" value="2"/>
Amplitude (percentage)	<input type="text" value="100"/>

Digitiser Control - Command line

The CMG-EAM provides the ability to connect to the terminal of any connected Guralp digitisers in order to configure their operation. To do this, connect to the CMG-EAM terminal as in section 2.1 or 2.3. and run the “data-terminal” command.

```
eam999 ~ # data-terminal
```

Select the desired digitiser (using the up/down arrow keys and Enter to select) from the list that is presented:

This will launch a minicom session (see section 7.2), allowing you to communicate with the digitiser terminal. For example:

```
Welcome to minicom 2.3-rc1

OPTIONS:
Compiled on Feb  9 2008, 16:59:26.
Port /dev/tts/0

          Press CTRL-A Z for help on special keys

LW B68000 CMG-5TD Command Mode
0 blocks in buffer | 256 blocks free
Guralp Systems Ltd - DM+FW v.103 mgs 13/02/08 (Build 65)

CTRL-A Z for help |115200 8N1 | NOR | Minicom 2.3-rc | VT102 | Offline
```

If the session closes due to a time-out (or you close it manually by issuing the GO command) then you will see the message **Killed by signal 15** and minicom will exit shortly thereafter.

If you wish to upload new digitiser firmware, please follow the digitiser manual to prepare it to accept firmware, then use the standard minicom “Send files” (Ctrl-A S) command to initiate an X-Modem upload. Digitiser firmware files may be found under the directory `/usr/share/firmware` on the CMG-EAM. Refer to section 7.2 for instructions on using Minicom. Once complete, please follow the instructions given in the digitiser's manual to complete the process.

Services

The “Services” item from the “Control” menu takes you to the Services Control screen. This screen gives a list of all configured services: services are the background programs that read, convert and write data and carry out the individual functions of the CMG-EAM.

The services are presented in three columns. In the first is given the name of the service and, in italics, its description. The second column shows the word “Stopped” in red for any services which are not running and, for those which are running, the PID (process ID, a unique number which the operating system uses to keep track of running programs) and the date and time that this instance of the service was started. The third column has buttons allowing you to stop, start or re-start each service.

Service Control

DataOut <i>Serial Data Out Port</i>	Running PID: 710 Started: Thu Jan 1 00:00:49 UTC 1970	<input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Restart"/>
PortA <i>Serial Port A</i>	Running PID: 716 Started: Thu Jan 1 00:00:49 UTC 1970	<input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Restart"/>
PortB <i>Serial Port B</i>	Running PID: 722 Started: Thu Jan 1 00:00:50 UTC 1970	<input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Restart"/>
PortC <i>Serial Port C</i>	Running PID: 728	<input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Restart"/>

It is possible to monitor and control services from the command line using the `ps` command and various scripts in `/etc/init.local` and `/etc/init.d`. This should be familiar to Linux users but full details are beyond the scope of this manual.

RAID Array Services

RAID arrays provide increased data security at the cost of extra storage devices. They can prevent the loss of data in the event of a single drive failure. The “RAID Array Services” item on the “Control” menu will only be displayed on CMG-NAMs with RAID fitted. It displays a page which reports the status of and allows simple control of the fitted RAID array. The status of swap partitions are also reported on this page.

3.3 Tools Menu

Firmware

Selecting “Firmware” from the “Tools” menu takes you to a screen from which you can upgrade the firmware of a CMG-EAM, provided it has access to the internet.

Note that this procedure does not upgrade the firmware of connected digitisers. Connected digitisers can be upgraded using the data-terminal command as documented in section 3.2 on page 23.

The CMG-EAM firmware upgrade screen looks like this:

Firmware update

Upgrade from server

Upgrade this system's firmware over the network using the Guralp rsync server.

Option	Description
Upgrade	Standard upgrade from rsync server.
Advanced options	Display advanced upgrade options. Not normally required.

Generated at 2009-03-24T13:47:34Z by firmware.cgi 1.0.0. Portions of output copyright (c)2009, Guralp Systems ltd..

This procedure respects and preserves user configuration settings. In unusual circumstances it may be necessary to overwrite these settings and return the unit to a factory default configuration. The “Advanced options” button takes you to a page which offers this facility:

Firmware update

Upgrade from server

Upgrade this system's firmware over the network using the Guralp rsync server. You may also sync default configuration files, erasing your own settings and restoring the defaults.

Option	Description
Upgrade	Standard upgrade from rsync server.
Upgrade (restore defaults)	Upgrade from rsync server and restore default settings for all programs. Erases user settings.
Upgrade (force factory settings)	Upgrade from rsync server and force factory settings. Erases all changes made to files and settings. Erases data that is not on removable disk.

Generated at 2009-03-24T16:24:55Z by firmware.cgi 1.0.0. Portions of output copyright (c)2009, Guralp Systems ltd..

Firmware can also be updated from the command line. The command `upgrade` without arguments respects and preserves user data and configuration. To restore all default settings, use

```
upgrade --restore-defaults
```

and to additionally clean the entire system (other than the removable disk), use

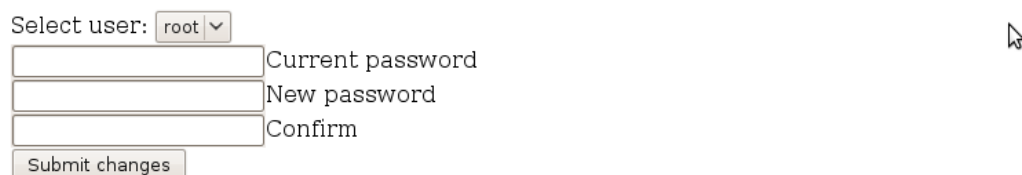
```
upgrade --force-factory-settings
```

When updating a number of instruments simultaneously, it may be desirable to create a local mirror of the Guralp update server rather than repeatedly download the firmware over your internet connection. If you are familiar with `rsync`, you can inspect `/usr/bin/upgrade` and edit `/etc/conf.d/upgrade` - otherwise, please contact Guralp technical support for advice.

Passwords

Selecting “Passwords” from the “Tools” menu takes you to a screen from which you can change the password used for command-line access and for the web interface.

Password change



Select user: ▼

Current password

New password

Confirm

Generated at 1970-01-06T00:11:25Z by passwd.cgi from Pt-users 1.0.1. Portions of output copyright (c)1970, Guralp Systems Ltd..

Currently, the only user configured on a CMG-EAM is root. The same password is used for both login and web authorisation. The password is changed immediately but the built-in web-server can continue to use the old password for some time after a change. If this is a problem, the web service can be restarted from the Services page (see section 3.2 on page 24) by clicking the “Restart” button for the “httpd” service.

Note that there is no way to recover a lost password. Despite much conventional wisdom, you may be safer writing the password down and storing it in a physically secure place rather than risk forgetting it.

GCF Audit Log Viewer

Detailed information about every GCF packet sent or received are stored on the GSL-EAM and can be viewed with the GCF Audit Log Viewer. To access the GCF Audit Log Viewer from the web interface, click on “GCF audit log viewer” on the “Tools” menu. To access the same information from the command line, enter the command

```
gcflogview
```

The initial screen displays all GCF data sources and sinks in a table, together with some summary information:

GCF audit log viewer

GCF audit logs. Select 'View' to view a log in more detail.

Program	Latest entry	Size	View
Port A	2009-07-13T16:36:37Z	256KiB	<input type="button" value="View"/>
Port B	No entries	256KiB	<input type="button" value="View"/>
Port F	No entries	256KiB	<input type="button" value="View"/>
Scream (GCF) network server, instance default	2009-07-13T16:36:33Z	128KiB	<input type="button" value="View"/>
Program	Latest entry	Size	View

Generated at 2009-07-13T16:36:37Z by gcflogview.cgi 1.0.5. Portions of output copyright (c)2009, Guralp Systems Ltd.

In the example display above, it can be seen that Ports B and F are inactive, Port A was receiving GCF data until 16:36 and the default instance of the Scream network server was sending GCF data until the same time.

The “Size” column shows the size of the log buffer allocated to each data source or sink. The log buffer size can be changed from the relevant service or port configuration screens in expert mode.

For example, to allocate a larger log buffer to the GCF receiver running on Port A, click on “Serial ports” from the main menu, then on “Port A - GCF in”, “GCF input settings” and then click the “Expert” button. You will see a drop-down selection list labelled “Audit log size” from which you can select 64Kib, 256Kib, 2MiB or 16MiB.

To change the GCF audit log buffer size for the Scream network server, select “Services” from the “Data transfer/recording” section of the “Configuration” menu then click on “GCF Scream network server”. Click on the entry for the instance you wish to change and then click the “Expert” button at the bottom of the page. You will see a drop-down selection list labelled “Audit log size” from which you can select 64Kib, 256Kib, 2MiB or 16MiB.

Each entry in the table has a “View” button, which shows detail from the relevant log at block (packet) level). The view for Port A is shown here:

GCF audit log viewer

Port A

Recent entries

Time	Type	Details	Hex
2009-07-13			
16:36:37.554	GCF block received	ID: A830-55TPNE Timestamp: 2009-07-13T16:36:36.000000000Z Digitiser: CMG-DM24-mk3 Block type: data Sample rate: 20 samples/second Compression: 32-bit Number of samples: 20	80 07 47 6C 12 9A 80 1A 38 14 E9 94 1F 14 01 14
16:36:37.634	GCF block received	ID: A830-55TPSM Timestamp: 2009-07-13T16:36:36.000000000Z Digitiser: unknown, probably CMG-DM24-mk2 Block type: strong motion Number of words: 50	80 07 47 6C 12 9A 80 06 38 14 E9 94 00 00 04 32
16:36:37.694	GCF block received	ID: A830-55TPEE Timestamp: 2009-07-13T16:36:36.000000000Z Digitiser: CMG-DM24-mk3 Block type: data Sample rate: 20 samples/second Compression: 32-bit Number of samples: 20	80 07 47 6C 12 9A 7E 06 38 14 E9 94 1F 14 01 14

The first column shows the time-that the block was received (not the time-stamp on the block itself) and the second column shows the event type - “GCF block received” in most cases.

The “Details” column shows the stream ID from the received data block and the block time-stamp. The digitiser ID is shown if it is encoded in the block; otherwise, a best guess is displayed. The rest of the entry shows the block type, sample rate, compression level and the number of samples in the data block.

A hexadecimal display of the block header is shown in the final column.

An example of an audit log display for an out-going data-stream is shown below. This data is for the Scream network server:. The first column now shows the time that the block was transmitted; other details are the same as in the previous example.

GCF audit log viewer

Scream (GCF) network server, instance default

Search within this log

Recent entries

Time	Type	Details	Hex
2009-07-13			
16:27:05.228	GCF block sent	ID: A830-55TP3O Timestamp: 2009-07-13T16:18:44.000000000Z Digitiser: unknown, probably CMG-DM24-mk2 Block type: data Sample rate: 1 samples/second Compression: 16-bit Number of samples: 500	00 07 47 6C 12 9A 7D 54 38 14 E5 64 00 01 02 FA
16:27:05.228	GCF block sent	ID: A830-55TP3Q Timestamp: 2009-07-13T16:18:44.000000000Z Digitiser: unknown, probably CMG-DM24-mk2 Block type: data Sample rate: 1 samples/second Compression: 16-bit Number of samples: 500	00 07 47 6C 12 9A 7D 56 38 14 E5 64 00 01 02 FA
16:27:05.228	GCF block sent	ID: A830-55TPZP Timestamp: 2009-07-13T16:18:44.000000000Z Digitiser: unknown, probably CMG-DM24-mk2 Block type: data Sample rate: 1 samples/second Compression: 16-bit Number of samples: 500	00 07 47 6C 12 9A 81 05 38 14 E5 64 00 01 02 FA

GDI Channels Display

It is often useful, particularly when configuring a CMG-EAM for a complex array, to see a list of the Stream IDs, or channel names, which the CMG_EAM is receiving. The GDI Channels Display feature allows you to view a list of all active channels, together with some additional detail about each.

To access the GDI Channels Display from the web interface, click on “GDI Channels Display” on the “Tools” menu.

Similar information is available from the command line via the command `dumpdata` with the `--list-only` option but the format is optimised for automated processing rather than human consumption. Giving the `--help` option provides usage details. Use of the web interface, however, is recommended.

The following summary screen is displayed:

GDI Status

List of channels.

Name	Format	Active segments	Actions	
A830-55TPC2	Signed 32-bit integer samples 40 samples/second	1 (backfill only)	View details	Dump data
A830-55TPE4	Signed 32-bit integer samples 40 samples/second	1 (backfill only)	View details	Dump data
A830-55TPN4	Signed 32-bit integer samples 40 samples/second	1 (backfill only)	View details	Dump data
A830-55TPZ4	Signed 32-bit integer samples 40 samples/second	1 (backfill only)	View details	Dump data
A830-55TP2O	32-bit floating point samples 1 samples/second	1 (realtime) 2 (backfill)	View details	Dump data
A830-55TP2P	32-bit floating point samples 1 samples/second	1 (realtime) 2 (backfill)	View details	Dump data

The first two columns show the names of the channels, together with information about the data format. The Active segments column shows details of data currently being received. A segment is a contiguous sequence of blocks so any data being back-filled always requires separate segments.

For each channel, you have the option of viewing detailed information about the data or the data itself, by use of the “View details” and “Dump data” buttons.

The “View details” button displays the following screen, shown here in parts:

Channel A830-55TP2O details

Channel information

GDI channel name	A830-55TP2O
Sample format	32-bit floating point samples
Sample rate	1 samples/second

The first section of the screen, above, shows the channel name, sample format and sample rate, as seen on the previous screen.

Segments

Segments are continuous runs of time-series sampled data. Segments never contain gaps. A segment is considered *Realtime* if it has the most recent timestamp of all segments and if the last data for it was received less than 5 minutes ago according to the system clock. Otherwise, the segment is considered to be *Backfill*.

List of active segments.

Segment time	2009-07-14T08:13:00Z	2009-07-10T12:04:21Z	2009-07-10T11:59:20Z
Realtime?	Realtime	Backfill	Backfill
Clock status	Locked. Differential 1µs. Last update at 2009-07-14T08:13:00Z.	Locked. Differential 400µs. Last update at 2009-07-10T12:04:21Z.	Unlocked. Clock never locked; unable to estimate differential. Last update at 2009-07-10T11:59:20Z.
GPS status	Fix: 3D. Location: 51.361208°N -51.361208°W elevation 106.000m. Last update at 2009-07-14T08:13:00Z.	Fix: 3D. Location: 51.361181°N -51.361181°W elevation 114.000m. Last update at 2009-07-10T12:04:21Z.	Fix: 3D. Location: 51.361180°N -51.361180°W elevation 115.000m. Last update at 2009-07-10T11:59:20Z.
Channel flags	No SOH info from digitiser. Are unified status packets enabled?	No SOH info from digitiser. Are unified status packets enabled?	No SOH info from digitiser. Are unified status packets enabled?

The next section of this screen, above, shows, for each active segment, detailed information decoded from the packet header.

The final section, below, shows the metadata associated with the stream, which is derived from the configuration parameters of the relevant input module:

Metadata

Metadata is provided by the acquisition software module. Any metadata field may be overridden in the configuration of the *gdi_base* module.

List of channel metadata.

Name	Value
acquisition-device	Port A
instrument-id	A830-55TP
terminal	A830-55TP
sample-units	cms ⁻²
instrument-type	accelerometer
component	2D
Name	Value

Return to index

Refresh display

The “Dump Data” buttons associated with each channel on the GDI Status display screens like the following:

GDI Status

Channel dump for A830-55TP20.

Please note if this is a status channel there may be little or no data shown here.

Show meta data Show samples

```
New channel: ID 00000010, 32-bit floating point samples, 1 sps: A830-55TP20
  acquisition-device = Port A
  instrument-id = A830-55TP
  terminal = A830-55TP
  sample-units = cms-2
  instrument-type = accelerometer
  component = 2D
New segment: ID 00000010:00000000 2009-07-10T11:59:20Z
New segment: ID 00000010:00000001 2009-07-10T12:04:21Z
New segment: ID 00000010:00000002 2009-07-14T11:32:39Z
Initial subscription list complete
2009-07-14T11:32:39Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.230499
2009-07-14T11:32:40Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.038962
2009-07-14T11:32:41Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.003301
2009-07-14T11:32:42Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.078720
2009-07-14T11:32:43Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.449163
2009-07-14T11:32:44Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.468655
2009-07-14T11:32:45Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.135324
2009-07-14T11:32:46Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.133336
2009-07-14T11:32:47Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.129423
```

Check-boxes are available to toggle the display of both metadata and sample data. These can be changed at any time and the “Restart dump” button used to refresh the display.

For sample data, each line displays the sample's time-stamp, the segment ID, the channel name in parentheses, the sample type and the actual sample value.

A button at the bottom of the screen allows the display to be refreshed with current data. There is also a button which, when clicked, returns the user to the main GDI Channels Display index page, so that another channel can be inspected.

3.4 Tools - Removable Disk

The CMG-EAM allows control of the removable disk through the web interface. Click on the “Removable Disk” link in the “Tools” box in the left-hand menu frame.

Removable disk

Connect removable disk and select action.

Description	Action
View filesystems on attached disks. Use this to check for valid disks, to find how much space is available, to see whether the disk is in use, and to view files on the disk.	<input type="button" value="View filesystems"/>
Write whatever is currently buffered in flash to disk.	<input type="button" value="Flush to disk"/>
Partition and format attached disks. This will erase <i>ALL</i> data on the disk.	<input type="button" value="Format disk"/>

Note: actions may take some time to complete if the disks are not powered up. The web page will not load until after this has occurred. Please be patient.

Generated at 2008-05-01 T10:49:45.904121000Z by rdisk.cgi. Portions of output copyright (c)2008, Guralp Systems Ltd.

The removable disk can be removed at any time without compromising data integrity. However, for efficiency, it is best to remove the disk while it is powered down.

To determine whether the disk is currently in use or not, view the status page. If the removable disk has been accessed within the past week since the last power up, its details will be displayed on this interface. If the disk is currently in use, that will also be displayed.

Alternatively, the removable disk may be administered via the terminal by running the `rdisk` command, an example of which is shown below.



Note that the removable disk is powered down the majority of the time, in order to save power. Commands that access the disk must first power it up and this can take up to thirty seconds. Please be patient and allow the system time to react to such commands.

Installing a New Disk

When a new disk is to be used in the CMG-EAM, it must first be formatted for use. The disk can be formatted by any computer, but the CMG-EAM also has the capability of formatting the disk itself. The CMG-EAM accepts disks formatted in either ext3 format (which is faster and more reliable, but can only be read under Linux systems) or vfat format (slower and possibly less reliable, but can be read under all operating systems). To prepare the disk on a PC, please format it with a single partition containing either of the above filesystems, then insert it into the CMG-EAM.

To prepare the disk on the CMG-EAM via the web interface, navigate to the removable disk page and click on the “Format disk” button. After the disk has powered up, the following screen will appear:

Removable disk

Format and partition disks

Select partition for formatting

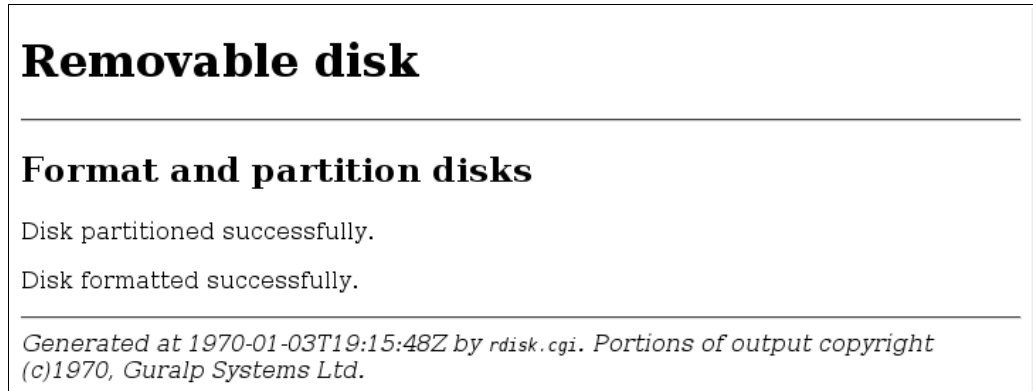
The following disks have valid partition tables. The partitions they contain may be formatted. Select a partition and press the Format button.

Select disk for partitioning

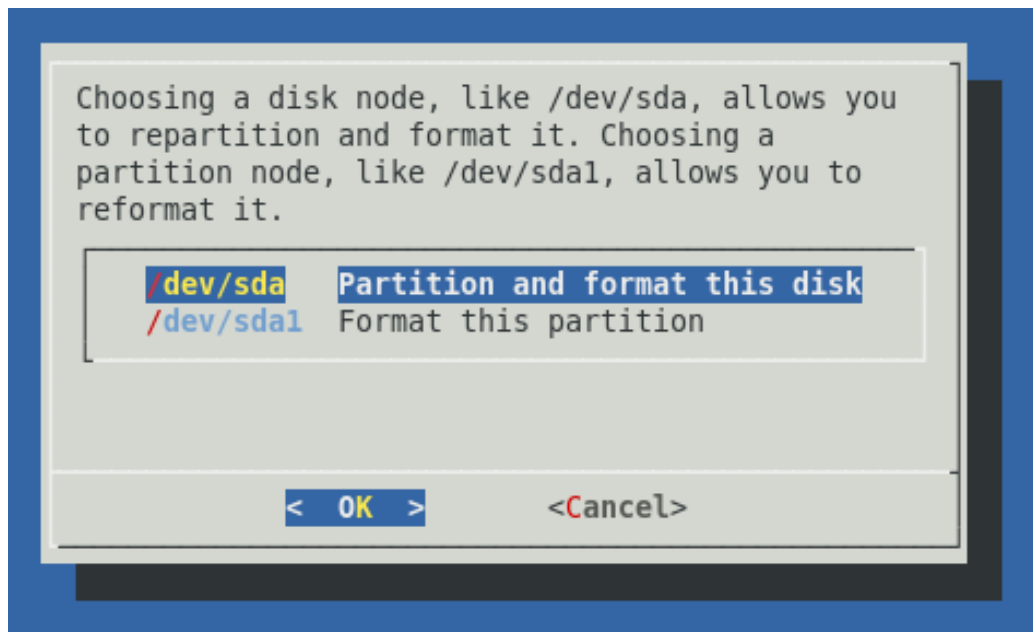
The following disks are attached. Pressing the Partition button will cause the selected disk to be repartitioned and then formatted. This will erase any other partitions and filesystems on the disk.

Generated at 2008-05-01 T10:50:13.352351000Z by `rdisk.cgi`. Portions of output copyright (c)2008, Guralp Systems Ltd.

Click on the “Partition” button. This will format the disk with a single partition containing a FAT32 filesystem, ready for use. It may take some time, depending on the size of the disk. When it has finished, you will see the following screen:



To prepare a new disk from the command-line interface, run the `rdisk` program. Select the “format” option, then select the “Partition and format this disk” option.



This will format the disk with a single partition containing a FAT32 filesystem, ready for use. It may take some time, depending on the size of the disk. When complete, you should see this message:

```
Partitioning successful.  
Format successful.
```

Viewing data on the Removable Disk

The CMG-EAM allows you to view and download data that is stored on the removable disk via the web interface. Navigate to the removable disk page and select the “View filesystems” option. This will power up any connected disks and, after a short delay, present a list of attached disks and their details (filesystem, free space).

Select a disk and you will be able to browse through the list of directories that it contains.

Clicking on the “View Files” buttons takes you to the “Removable disk file index” screen, which displays folders and files. Sub-directories (folders) have a “Follow” button next to them and files have a “Download” button.

The first screen typically looks like this:

Removable disk

Removable disk file index

Filesystem UUID: 0000-0401
Path: /

Choose a subdirectory to follow, or a file to download.

File or directory name	File size	Follow or download
2008091-gc f raw		<input type="button" value="Follow"/>
2008092-gc f raw		<input type="button" value="Follow"/>
2008093-gc f raw		<input type="button" value="Follow"/>
2008094-gc f raw		<input type="button" value="Follow"/>

Each folder contains sub-folders or files of raw GCF data covering a time range typically indicated by the file-name. You can descend into sub-folders by clicking the “Follow” button until you reach the folder level at which the files themselves are stored. From here individual files can be downloaded for analysis.

Removable disk

Removable disk file index

Filesystem UUID: 0000-0401

Path: /2008091-gcfraw

Choose a subdirectory to follow, or a file to download.

File or directory name	File size	Follow or download
.. (up to parent directory)		<input type="button" value="Follow"/>
2008091T1730Z.gcf	8.8MiB	<input type="button" value="Download"/>
2008091T1800Z.gcf	9.5MiB	<input type="button" value="Download"/>
2008091T1830Z.gcf	9.5MiB	<input type="button" value="Download"/>
2008091T1900Z.gcf	9.4MiB	<input type="button" value="Download"/>
2008091T1930Z.gcf	9.4MiB	<input type="button" value="Download"/>
2008091T2000Z.gcf	9.4MiB	<input type="button" value="Download"/>
2008091T2030Z.gcf	9.4MiB	<input type="button" value="Download"/>

Downloading multiple files

If you need to download more than two or three files, you may find it more convenient to use a file transfer protocol such as scp (sftp and rsync are also supported). scp is freely available for Linux/Unix platforms and, as winscp (downloadable from <http://winscp.net>), for Windows computers.

From the EAM's command line, run the `rdisk` utility and select the “power” option (“power up disks for shell session”). You will see the message:

```
Connected to server. Powering up disks...
```

After a number of seconds, you will see the further message:

```
Disks powered up. A new bash session has been created.
```

```
When you exit from this bash session (which you can do with
`exit' or Ctrl-D), the disks will be powered down. The
power will stay on until you exit. Then you will be
returned to your original shell.
```

```
eam999 ~ #
```

The contents of the disk will be visible in a directory under `/media` with a name like `F95D-9A7B`. You will need to keep the disk powered up until you have finished accessing its contents, even remotely.

Data Buffering

The CMG-EAM buffers its data in memory before flushing it to disk. To initiate an immediate flush to disk, use the “Flush to disk” option on the removable disk page of the web interface or run the command

```
gdi-record --flush
```

from the command line.

4 Digitiser Configuration

The “System Setup” sub-menu of the “Configuration” menu alters dynamically to reflect the CMG-EAM's attached devices. For every digitiser detected, an entry appears which allows you to configure the digitiser. To control the digitiser and its attached instrument (sensor locking, mass centring, etc.) see section 3.2 on page 20.

The information shown on this screen is often retrieved from the digitiser using a sequence of background commands over a serial communications line and, so, may take a few seconds to display. It is possible to display this sequence of commands, together with the responses received from the digitiser, and this may be useful both for learning the command-line interface of the digitiser and for debugging any unexpected behaviour. To do this, select “Show full digitiser dialogue in future form submissions” from the miscellaneous section near the bottom of the configuration screen.

The digitiser configuration screen is large and is shown here in sections. The first section displays the digitiser's identification string and serial number and allows these to be set. It also displays the digitiser's software version:

Digitiser Configuration

13AZI-C954/Port A/bench-test

Identity	
System identification	<input type="text" value="13AZI"/>
Serial number	<input type="text" value="C954,00"/>
Software version	v.285

The system identification string and serial number can be changed by altering these fields and then clicking the “Submit changes” button at the bottom of the screen.

The next section configures the digitiser for its attached devices:

Connected devices	
Sensor type	<input type="text" value="CMG-6TD"/> ▼
Timing source	<input type="text" value="NMEA protocol GPS"/> ▼
GPS power cycling	<input type="text" value="Disabled"/> ▼
Device info blocks	
Info block 1 is empty.	
<input type="button" value="Display device info blocks"/>	

The sensor type can be set although this has no effect on the CMG-EAM's operation and acts as a memo field.

The timing source for the digitiser can be set to “NMEA protocol GPS” (which should be used for all GPS devices) or “None”, for situations where there is no timing source.

GPS units can be turned off to save power in battery-powered environments. In order to keep the internal clock synchronised, the GPS unit is regularly turned on for long enough to obtain an accurate time and then turned off. The “GPS power-cycling” drop-down allows you to select the intervals at which this happens (1, 2, 3, 4, 6, 8, 21 or 24 hours) or whether to leave the GPS constantly powered up.

“Info blocks” are areas of storage within the digitiser which can hold arbitrary data. In some applications, such as when generating strong motion packets, they should hold structured information about the attached sensors. Refer to the strong motion set-up guide for more information about this topic. If you do not need them to hold structured data, you can use them to store any information you wish, such as sensor details. There are two info blocks per digitiser. The “Display device info blocks” button shows the contents of the infoblocks and allows you to upload new data to them, should you wish.

The Decimator outputs section of the screen shows and controls which digitiser taps have been configured to output data, both in continuous and triggered states.

Decimator outputs

	Sample Rate		Output			
			Z	N	E	
Tap 1	500sps ▾	continuous	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
		triggered	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Refresh View trigger settings Add new output

Extra taps can be added with the “Add new output” button. The rates available at each tap are dependant on the rate selected at the previous tap: the base sampling rate is 2000 samples per second and each tap can be configured to divide this by either 2, 4 or 5. The available rates are shown in the table below, along with a way to configure each, although there are sometimes very many different ways to configure any given rate.

Desired output rate	Intermediate steps
4	400, 100, 20
5	400, 100, 20
8	400, 200, 40
10	400, 100, 55
16	400, 80
20	400, 100
25	400, 100
40	400, 200
50	400, 250
80	400
100	400
125	500
200	400
250	500
400	<i>tap 1</i>
500	<i>tap 1</i>
1000	<i>tap 1</i>

The next section displays and controls the transmission of data from the auxiliary and state-of-health channels of the digitiser:

Multiplexor channels	
Auxiliary inputs	System SOH
<input type="checkbox"/> M0 - channel 0	<input checked="" type="checkbox"/> M8 - Z mass position
<input type="checkbox"/> M1 - channel 1	<input checked="" type="checkbox"/> M9 - N/S mass position
<input type="checkbox"/> M2 - channel 2	<input checked="" type="checkbox"/> MA - E/W mass position
<input type="checkbox"/> M3 - channel 3	<input checked="" type="checkbox"/> MB - Calibration signal input
<input type="checkbox"/> M4 - channel 4	<input type="checkbox"/> MC
<input type="checkbox"/> M5 - channel 5	<input type="checkbox"/> MD
<input type="checkbox"/> M6 - channel 6	<input checked="" type="checkbox"/> ME - Temperature
<input type="checkbox"/> M7 - channel 7	<input type="checkbox"/> MF - Pressure (if fitted)

This is followed by the Transmission Mode selection dialogue, which is not reproduced here. One mode can be selected from the following list:

- Direct mode - Data are transmitted in real-time, without being copied to local storage. Only a small transmit buffer is used.
- Filing mode - Data are stored in local flash storage. A periodic status heartbeat is transmitted to inform listeners that data are available from storage.
- Adaptive mode - Data are transmitted in real-time whenever possible. Any unacknowledged transmission is stored, and retransmitted oldest first when the line is not being used for real-time traffic.
- FIFO mode - Data are stored locally and transmitted in strict FIFO order. If the link is lost for a period, real-time data will be delayed while the stored data are transmitted.
- Dual mode - Continuous data are transmitted as if in "direct" mode and Triggered data is stored in flash as if in "filing" mode.
- Duplicate mode - Data are transmitted as if in "direct" mode and also stored in flash as in "filing" mode although without the "heartbeat" operation.

The next section of the web page allows the selection of one of two storage modes, which affect how data are stored in the digitiser's local flash storage:

Storage mode	
<input checked="" type="radio"/>	Enable storage re-use. When local storage is full, new data arriving will over-write the oldest data in the buffer.
<input type="radio"/>	Enable write once storage. When local storage is full, new data arriving will be transmitted as if in "direct" mode and will not over-write the already stored data.
<input type="checkbox"/>	Reset flash buffers on next submit/reboot.

Selecting the check-box will cause any data in the flash storage to be erased and the read pointers to be reset. Use with caution: data will be erased.

The next section controls two settings associated with data transmission:

Transmission parameters	
Heartbeat interval	<input type="text" value="0"/> seconds The periodic status heartbeat is only used with "filing" and "dual" data modes.
Acknowledgement delay	<input type="text" value="150"/> milliseconds How long to wait before a transmission is assumed to have failed.

When the digitiser is in the “filing” or “dual” transmission modes, regular heart-beat messages are sent. This allows software such as Scream! to be aware of the devices even though they are not sending sampled waveform data. The frequency of these messages can be set to an integer number of seconds.

When the digitiser is in the “adaptive” or “FIFO” transmission modes, special action is taken if data cannot be transmitted. The “acknowledgement delay” field controls how long the digitiser waits for an acknowledgement packet before assuming that the link has failed. This should be set to an integer number of milliseconds.

The “Ports” section of the web page allows control of the baud rates of the digitiser's serial ports:

Ports	
Serial port	Baud rate
Data out	<input type="text" value="115200"/> Changing the data out rate will require the same change to be made in your communications software and if fitted the Lantronix Ethernet/WiFi module.
GPS	<input type="text" value="4800"/> This setting is only used for non-GPS operations. If a GPS device is enabled the port will be set to the GPS rate of 4800 baud regardless of this setting.
Data in	<input type="text" value="19200"/>

If a Lantronix Ethernet or WiFi option is fitted, it uses the “Data out” port settings for its internal communications with the digitiser. Changing the associated baud rate requires making a network

connection to the Lantronix unit's web interface and selecting the matching baud rate from its control page.

The final section of the digitiser control web page is entitled "Miscellaneous features". This section will display a warning in red if a discrepancy is detected between the EAM's internal clock and the digitiser's own clock. If the two clocks have reasonable synchronisation, this message is suppressed. A typical warning looks like this:

Digitiser clock is displaced by more than 5 minutes from the system clock. (Plus 7 minutes.)

This section of the page is shown here without the warning:

Miscellaneous features

- Transmit Unified Status Packets. (Recommended)
- Set the digitiser clock from the system clock on next form submission.
- Show full digitiser dialog in future form submissions.

Help Refresh display Submit changes Reboot digitiser

The first check-box enables the transmission of Unified Status Packets. Unified Status Packets are a machine-readable representation of the data carried in the normal, human-readable status streams and allow programs such as Scream! to access complete and consistent state-of-health information regardless of any status stream customisations.

The second check-box allows the re-synchronisation of the digitiser to the EAM's system clock. The third toggles display of the underlying dialogue with the digitiser, as described at the beginning of this section.

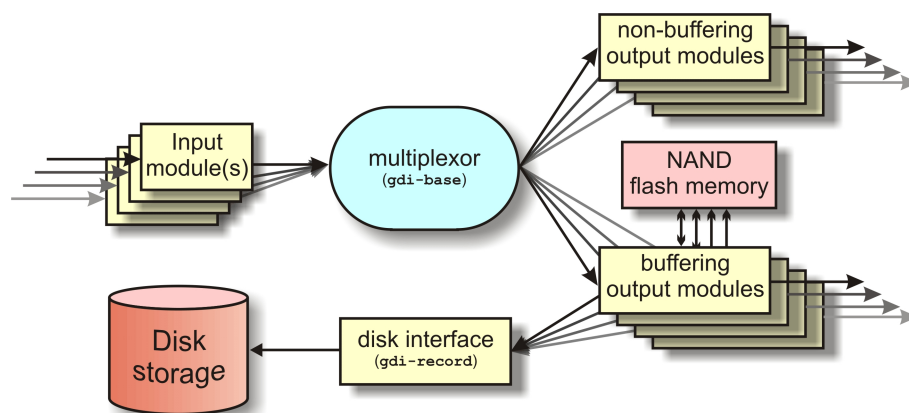
Note that, as with all web interfaces, options selected on this screen will not take effect until the page is submitted.

Extra buttons at the bottom of this page allow the refreshing of the web page display with up-to-date information and offer the opportunity to reboot the digitiser.

5 Data Handling Overview

The data handling system of the CMG-EAM is very flexible, due to the modular software architecture. All data flowing through the CMG-EAM is routed through a single multiplexor module called `gdi-base`. This communicates directly with all input modules, which handle the various incoming data streams, and all output modules, which convert the data into the required formats. All incoming data is stored and accessed internally in an intermediate format, regardless of the format in which it was originally received.

The diagram below shows the basic internal organisation of the CMG-EAM.



The multiplexor makes incoming data available to the output modules. These come in two flavours: simple modules such as those for WIN, GSMS and QSCD simply convert the data streams and output them in the required format; other modules maintain a ring-buffer which is used to, for example, satisfy BRP back-fill requests. The ring-buffers use the NAND flash memory. These output modules also send data to `gdi-record`, which handles all hard disk write requests, regardless of format.

The `gdi-base` and `gdi-record` programs are designed to be stateless, so that the data on the disk are always consistent. This means the system is tolerant of the power or disk being removed at any time.

Any number of input modules can be configured to acquire data in any supported format from any source, simultaneously. These modules convert their data and pass it to the multiplexor. Data can be acquired in any of the following formats, from multiple sources:

- BRP via serial;

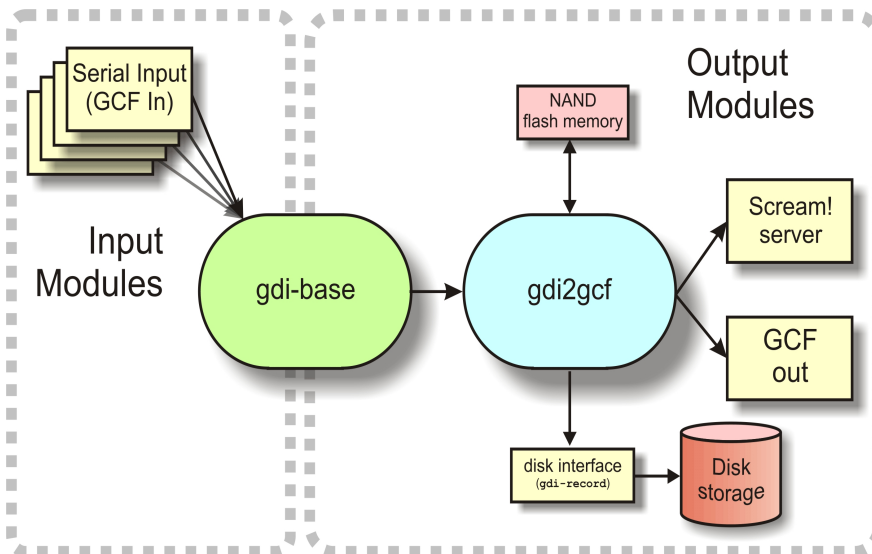
- Scream via 100BaseTX Ethernet or ppp;
- GDI-link via 100BaseTX Ethernet or ppp; and
- CD1.1

The architecture has been designed to support the addition of extra formats simply by adding input modules. Please contact Güralp Systems if you have requirements which are currently unsupported.

Any number of output modules can be configured to send data in any supported format to any destination. The following data formats are supported:

- GCF output via serial port or TCP stream;
- GCF output via Scream (TCP or UDP);
- GDI (Güralp Data Interconnect);
- GDI-link;
- CD1.1;
- WIN format output;
- QSCD - Quick Seismic Characteristic Data (designed by KIGAM) output; and
- GSMS (Güralp Seismic Monitoring System) output.

In the default, factory configuration, the CMG-EAM is configured to receive serial GCF input on all of its serial ports except Data Out. There is a single chain of data through the multiplexor to a Scream server. Data is also recorded to disk in GCF format. This is shown in the following diagram:



6 Configuration

The CMG-EAM is set up to work with Güralp equipment by default. All serial ports except Data Out will be configured to expect GCF (Güralp Compressed Format) input at 38,400 baud (the default baud-rate of the CMG-DM24mk3 digitiser); GCF will be recorded to disk and a Scream server will be running on TCP/UDP port 1567.

There is significant additional functionality which can be enabled but which must first be configured. Configuration can be achieved in three ways: through the web interface (recommended), on the command line (connected via serial line or via ssh), or by editing the configuration files directly.

6.1 Password


When the CMG-EAM is first configured, we recommend that the root password is changed. There is much information available on-line for choosing a strong password, for example:

http://en.wikipedia.org/wiki/Password_strength#Guidelines_for_strong_passwords

To change the password on the command line, run the `passwd` command. This will prompt you to enter the new password twice; if both match, the password will be changed.

To change the password on the web interface, choose the “Passwords” option under the “Tools” menu.

Password change

Select user: 

Current password

New password

Confirm

Generated at 1970-01-06T00:11:25Z by passwd.cgi from Pt-users 1.0.1. Portions of output copyright (c)1970, Guralp Systems Ltd..

Note: the password required to access the web interface will also be changed by this procedure, whether the web interface or command-line utility is used.

Note: There is no way to recover a forgotten password and no way to access a CMG-EAM without one. You have been warned.

6.2 Configuration System

The CMG-EAM uses a consistent configuration system that can be used either through the web interface or through the terminal.

To use the web interface to the configuration system, connect to the CMG-EAM web-server as described in section 2.2. Choose the “All options” link in the left-hand frame within the “Configuration” box to access the various configurable items. Most of the other options in the “Configuration” box are simply short-cuts to various items within the configuration system.

To use the terminal interface to the configuration system, connect to the CMG-EAM terminal as in section 2.1 or 2.3. Run the `gconfig` program to access the various configurable items.

On terminals which support it, the `gconfig` system can be navigated using the mouse to click on labels. The system can always be navigated using the arrow keys to move between fields and the `<return>` key to select the currently highlighted option. The bottom menu bar can be accessed using the function keys F1 – F4. For optimal display, the correct terminal type must be set before `gconfig` is run using the command:

```
eam999 ~ # export TERM=TERM_TYPE
```

The terminal type is dependant upon the terminal emulator you are using and should be chosen as follows:

- `ssh` from Unix, or `puTTY` under Windows in `ssh` mode: no action required - the `ssh` protocol sets the `TERM` environment variable automatically.
- Minicom under Unix: no change. Minicom emulates a `vt100`-style terminal and automatically maps the keystrokes and display sequences for the actual terminal you are using, so the default `TERM` setting of `vt100` is correct.
- HyperTerminal under Windows: using the File menu option “Settings”, ensure that the terminal type is set to `VT100`. HyperTerminal will then emulate a `vt100`-style terminal, which will match the default `TERM` of `vt100` on the CMG-EAM.

Both means of accessing the configuration system show the same information. At the bottom of each page is a menu bar with a set of standard buttons. In `gconfig`, they look like this:



In the web interface, like this:



In gconfig, the <Home> button is replaced by a <Quit> button when the user is at the top-level menu. The <Quit> button exits the gconfig program.

The function of each button is:

- Home – Return to configuration home page
- Help – Reloads the current page, but with additional help text displayed in blue.
- Expert – Reloads the current page, but with additional, more advanced options displayed.
- Submit – Save and act upon any changes that have been made on the current page.

In both interfaces, buttons may be unavailable (displayed in grey on the web and in yellow in gconfig) in certain contexts.

To use the configuration system, navigate to the page relating to the service you wish to configure, make any changes required and then click the Submit button.

Input fields in gconfig can either be free-text-entry, list-selection or boolean (check-box). Use the <TAB> key to move between fields. Simply type the desired text into free-text-entry boxes. Use the <Enter> key in a list-selection field to display the list of available options, then the up and down arrow keys to navigate the list and then the <Enter> key to select the highlighted option. Use the <SPACE> key to set or unset boolean fields. A selected boolean field is shown as {X} and an unselected boolean field is displayed like this: { }

The following sections describe the settings and services which can be configured. Due to the practically identical screens of the web and command-line interfaces, we will only show illustrative screen-shots of the web interface.

6.3 Configuration Management

The CMG-EAM has a comprehensive configuration management system that allows both complete configurations and individual classes of configuration information, such as data processing and networking, to be saved individually and merged during restore.

This feature can be very useful when multiple CMG-EAMs are to be configured for a project. In a typical array with central communications hub arrangement, only two data processing configurations need be created: one for the hub and one for an array element. The latter can then be copied from CMG-EAM to CMG-EAM to avoid having to configure each unit individually. Network configurations need be created for each element of the array and for the hub but these can all be created and stored on a single CMG-EAM. If the complete set of stored configurations is then copied to each machine and to any “hot spares”, then every CMG-EAM becomes rapidly interchangeable: all that is required to deploy a unit is to restore the correct data processing configuration (hub or element) and then restore the appropriate network configuration.

Configuration files can also be backed up and stored on different sites to provide a disaster management resource.

Saving a configuration

From the “Configuration” section of the main menu, select “Save/Restore”. The following screen appears:

Configuration management

Restore

ID.	Date	Time	Description	Actions
1	2009/06/12	14:03	standard config	<input type="button" value="Restore"/> <input type="button" value="Download"/> <input type="button" value="Delete"/>

Save

Checked modules will be saved:

Module	Description
<input checked="" type="checkbox"/> platinum	Main instrument and data processing configuration
<input checked="" type="checkbox"/> network	Networking and communications configuration
<input checked="" type="checkbox"/> userid	User names (ID) and passwords
<input checked="" type="checkbox"/> system	Additional system core configuration

Description

Upload

Archive

Generated at 2009-07-13T15:35:59Z by config-manage.cgi 0.2.3. Portions of output copyright (c)2009, Guralp Systems Ltd.

To save a configuration, use the check-boxes to select which elements you wish to include, enter a descriptive name in the “Description” field and click on “Save configuration”. The configuration is saved onto the CMG-EAM and will appear in the list of saved configurations at the top of the page.

If you are using the web interface, you can download this configuration to the computer running the browser by clicking the “Download” button in the list of saved configurations at the top of the page.

Restoring a configuration

The same screen is used for restoring a configuration. Simply select the required saved configuration from the list at the top of the page and hit the restore button. The following screen appears:

Configuration management

2009/07/13 15:59 test

Restore modules

Checked modules will be restored:

<input type="checkbox"/>	Module	Description
<input checked="" type="checkbox"/>	platinum	Main instrument and data processing configuration
<input checked="" type="checkbox"/>	network	Networking and communications configuration
<input checked="" type="checkbox"/>	userid	User names (ID) and passwords
<input checked="" type="checkbox"/>	system	Additional system core configuration

Restore type

User files restore
 Full (core) restore
 Full restore and purge all other modules

Action

[Return to Configuration management main form](#)

Generated at 2009-07-13T15:59:34Z by config-manage.cgi 0.2.3. Portions of output copyright (c)2009, Guralp Systems Ltd.

The date and time at which the configuration was saved is shown; in the example above, this is the 13th of July, 2009 at 15:59. The name of the configuration is also given; in the example above, this is “test”.

Even if a configuration was saved with all modules selected, it is possible to restore only a subset of configuration information. Select what you wish to restore by ticking or unticking the appropriate check-boxes.

Unless you are recovering from, say, a corrupted device, you should leave the “Restore type” set to “User files restore”.

Click the “Restore configuration” button to load the configuration values from the saved data into the CMG-EAM's files. Depending on the significance of the changes between the saved configuration and the previous, active configuration, you may need to stop and restart a number of services (see “Services” in section 3.2 on page 24) or reboot the unit completely (see “Power control” in section 3.2 on page 19) before all your changes will come into effect.

If you have a reasonable working knowledge of the service configuration files used internally by the CMG-EAM, you may find the dry run facility useful. Clicking the “Dry run restoration” button produces a list of files that would be over-written - but without actually making any changes. This is also a useful tool for exploring the effects of different configuration classes.

6.4 Setting the System Identity (Hostname)

To set the system hostname, connect to the CMG-EAM configuration system via either the web interface or by using gconfig from the command line interface. Follow the link on the front page to the “System identity (hostname)” page.

Use this screen to set the hostname of the CMG-EAM. If the “Allow DHCP Override” tick box is flagged then, when the CMG-EAM requests an IP address from a DHCP server, the DHCP server response will override the hostname set on this screen.

6.5 Serial Port Configuration

The CMG-EAM has several serial ports, and each one can be configured to have a service running on it. The factory default is for the “data out” port to be set up for a terminal (connected at 115,200 baud, 8 data bits, no parity and one stop-bit) and all other ports set up to be ready to accept GCF data from CMG-DM24mk3 digitisers (at 38,400 baud, 8-N-1).

Several other services can be configured to run on the serial ports and their configuration is described in this section. To configure a serial port, connect to the CMG-EAM configuration system via either the web or gconfig from the command line. Follow the link on the front page to the “Serial ports” page.

Serial ports configuration

Select a port to configure:

- [Data Out - Terminal](#)
- [Port A - GCF in](#)
- [Port B - NMEA out](#)
- [Port C - None](#)
- [Port D - None](#)
- [Port E - Terminal](#)
- [Port F - GCF in](#)

[Home](#) [Help](#) [Expert](#) [Submit](#)

Generated at 2008-05-01T10:50:58.833146000Z by GCS. Portions of output copyright (c)2008, Guralp Systems Limited.

The initial screen allows you to select a serial interface to configure. When you select an interface, the following screen will appear:

Port A serial configuration

Name	<input type="text" value="Port A"/> Port name (Fixed)
Port function	<input type="text" value="GCF in. Inbound GCF data gathering"/> <input type="button" value="v"/> Function the port currently supports
Port speed	<input type="text" value="38400"/> <input type="button" value="v"/> Baudrate at which the port operates

- [NMEA output settings](#)
- [GCF input settings](#)
- [GCF output settings](#)
- [PPP network configuration](#)
- [TCP serial converter settings](#)

[Home](#) [Help](#) [Expert](#) [Submit](#)

Generated at 2009-06-23T12:17:10Z by gcs 1.1.5. Portions of output copyright (c)2009, Guralp Systems Limited.

The serial port name is preconfigured to match the label on the CMG-EAM enclosure. The port function and baud rate can be selected from the menu. Some functions have additional configuration items associated with them, and these can be accessed via the links. The following services can be selected:

- **None** – The port has no function associated with it and any data will be ignored;

- **Terminal** – The user can log into the CMG-EAM using a serial terminal or terminal emulator on this port;
- **PPP** – The CMG-EAM can use a GPRS / Iridium modem connected to this port;
- **GCF in** – The CMG-EAM will receive GCF data packets from Güralp Digitisers connected to the port;
- **GCF out** – The CMG-EAM will retransmit all incoming GCF data packets out via the port;
- **NMEA out** – The CMG-EAM will send NMEA streams (GPS data) from this port - for example, to connected digitisers.
- **NMEA in** – The CMG-EAM will receive NMEA streams (GPS data) from connected GPS devices and, if NTP is configured (see the section on NTP configuration), it will use this data to synchronise its internal clock.
- **TCP Serial** – The CMG-EAM acts as a TCP-to-serial converter, relaying data received via this serial port over a TCP connection. This mode requires further configuration.

6.6 Setting up a PPP Connection

The CMG-EAM includes software that allows it to connect to a remote system using a point-to-point protocol (PPP) connection from one of its serial ports. This would typically be used when connecting via a GPRS or Iridium modem. To configure this connection, you will need a user ID and authentication code (the PAP secret) as required by the remote server. In addition, a dial up script specific to the service you are using must be created. If one does not already exist for your service, please contact Güralp support.

To set up this connection, connect to the CMG-EAM configuration system via either the web interface or by using gconfig from the command line interface. From the main screen select “Serial ports” and select the port to which the modem is connected. Change the function of the port to “PPP”, with the correct baud rate for the modem (see section 6.5 on page 52). Click “Submit” to save these changes. Go back to the configuration of the serial port and click on “PPP network configuration”.

You will see this screen (shown in parts):

Port A PPP Settings

Connection type	Local serial link (active/client mode) <input type="button" value="v"/> The connection style to use
Number of seconds to power down modem between calls	<input type="text" value="0"/>

IP addresses and routing

This section can be left empty if the remote end of the link performs all the configuration. Otherwise, some or all options may be supplied. If the remote

Choose the required connection type from the following list:

- Local serial link (active/client mode)
- Local serial link (passive/server mode)
- GPRS connection via Vodafone
- GPRS connection via T-Mobile

and set the desired time-out for the modem, if required.

The second section of this page handles the network configuration:

IP addresses and routing

This section can be left empty if the remote end of the link performs all the configuration. Otherwise, some or all options may be supplied. If the remote link is also the router, you should use the "Default route" option.

Local IP address	<input type="text"/> Sets the local IP address. Omit if remote end assigns one
Remote IP address	<input type="text"/> Sets the remote IP address. Generally omitted
Local IP address (IPv6)	<input type="text"/> Sets the local IP address. Omit if remote end assigns one
Remote IP address (IPv6)	<input type="text"/> Sets the remote IP address. Generally omitted
Default route	<input type="checkbox"/> Causes PPP daemon to provide the default route

In the majority of cases, the remote PPP daemon will set these parameters, in which case this section can be left blank.

The final section of this page handles PPP security. Enter the User ID and PAP secret received from your service provider in the appropriate fields. Click “Submit” to save the changes. The CMG-EAM should now be able to connect via PPP.

Authentication

If you are using authentication, you may fill out this section. Otherwise, it can be left untouched.

User ID	<input type="text"/> User identity to supply if requested
PAP secret	<input type="text"/> Optional secret that matches the user ID
Require peer authentication	<input type="checkbox"/> Requires that the remote peer authenticate itself to the local PPP daemon

Generated at 2009-06-23T12:19:50Z by gcs 1.1.5. Portions of output copyright (c)2009, Guralp Systems Limited.

The standard Linux commands `ppp-on`, `ppp-off`, `ip`, `ping`, and `traceroute` are available from the command line for use in controlling and testing PPP connections but it is also possible to configure a “watchdog” service to monitor a PPP connection and automatically restart it should it fail. This is described in the next section.

6.7 Monitoring a PPP connection

PPP connections can be monitored and, should they fail for any reason, automatically restarted. To configure this facility, connect to the CMG-EAM configuration system via either the web interface or by using `gconfig` from the command line interface. From the main screen, select “System services” and then, under Network Utilities, select “PPP link watchdog”.

You can create a number of watchdogs if you are running PPP on several ports. This screen allows you to select any of the existing watchdog services for re-configuration or to create a new watchdog service.

PPP link watchdog instance selection

- [Create new service instance](#)

Home Help Expert Submit

Generated at 1970-01-06T17:39:40Z by gcs. Portions of output copyright (c)1970, Guralp Systems Limited.

In this instance, no services are configured, so the only option is to create a new service.

When “Create a new service instance” is selected, the following screen is displayed:

PPP daemon watchdog

User description	<input type="text" value="PPP link watchdog. Instance 1"/> User label for the service instance
Enable	<input type="checkbox"/> Enable the service at system startup
Delete	<input type="checkbox"/> Delete this service instance
Daemon startup delay	<input type="text" value="30"/> s Length of time, in seconds, for the PPP daemon to start
Test command	<input type="text" value="/bin/ping -c 5 gstm.guralp.com"/> Command to run to test the link is active
Time between tests	<input type="text" value="30"/> s Length of time, in seconds, between test runs
Reboot fail count	<input type="text" value="30"/> Number of failures before system is rebooted

Home Help Expert Submit

Generated at 1970-01-06T17:39:42Z by gcs. Portions of output copyright (c)1970, Guralp Systems Limited.

If you are configuring a number of watchdogs, you can use the “User description” field to give each of them memorable names.

The Enable box should normally be checked but can be left unchecked if you only want to use the associated PPP connection occasionally.

An existing watchdog service can be stopped and its configuration deleted by selected the “Delete” check-box and then clicking the “Submit” button.

If the PPP connection relies on a modem link for its transport, there may be a significant delay between instructing the PPP link to start and the connection being established. So that the watchdog does not falsely detect a failed link during this period, it can be instructed to sit idle for a number of seconds before it begins to test the link. The length of the required delay should be entered into the “Daemon startup delay” field.

Once the start-up delay time has elapsed, the watchdog periodically tests the connection. To ensure that there is a valid end-to-end connection where, for example, a multi-hop link is in use, the exact method of testing is user-configurable. The most common method used is to use the `ping` command to verify ICMP connectivity to the ultimate remote host, but you are free to use the command or script of your choice here, so long as it returns a non-zero exit status on link failure.

When using `ping`, you should always use the `-c count` option or the command will never return.

The contents of the “Time between tests” field determines how often the configured test is applied. It can be set high to conserve bandwidth or set low to improve failure response times. It can also be used to keep a sparsely-used link alive where a “disconnect-on-inactivity” feature would otherwise interrupt it.

If the link test fails repeatedly, the CMG-EAM is rebooted. The number of failed tests before this happens is controlled by the “Reboot fail count” field.

The `ppp` watchdog service can be started, stopped and restarted using the “Services” page under the “Control” menu. See section 3.2 on page 24.

6.8 To Customise GCF Output Settings

If the CMG-EAM is configured to send GCF data out of one of its serial ports to a remote station via a device with high latency, e.g. a radio modem, it may be necessary to increase the time-out value used for communications. To change this time-out, connect to the CMG-EAM

configuration system via either the web interface or by using gconfig from the command line interface. From the main screen, select “Serial Ports”, then the name of the port that the modem is connected to. Select the the “GCF Output settings”.

Port A block recovery protocol settings

ACK/NAK timeout	<input type="text" value="150"/> ms Time to wait for ACK/NAK before transmitting next block (in milliseconds).
Mode	<input type="text" value="Direct - simple transmission with link error correction but no backfill"/> ▼ Block transmission mode

Output filtering

This section allows you to choose whether to transmit all GCF blocks as they are received from the GCF convertor, or only a subset.

Output type	<input type="text" value="All blocks"/> ▼ Select which types of block to transmit
Max sample rate	<input type="text"/> samples per second If filtering by sample rate, the maximum sample rate to send

If filtering by channel name, the channels to be transmitted should be entered into the table below. The exact name of the channel must be given, in the format SYSID-STRID.

Channel name	Delete
<input type="text"/>	
<input type="text"/>	

On this screen the time-out value can be set as required for your application. There is currently only one transmission mode available, so the Mode drop-down is not active.

If you wish to retransmit only certain blocks - e.g. from a particular component or at a particular sample rate, the rest of this screen can be used to set up filtering. You can choose to transmit all blocks, only status blocks, to filter by sample rate or to filter by channel name.

Select the desired filtering type in the drop-down and fill in the maximum sample rate or a list of channel names if required.

Press the Submit button when all required input fields have been populated.

6.9 Configuring NMEA Output

The CMG-EAM can generate simulated GPS data (NMEA-0183) to synchronise a connected digitiser's clock. In this case, the internal clock of the CMG-EAM is used as a reference for the digitiser, which must be controlled using NTP (See section 6.12 on page 65).

To use this function, connect to the CMG-EAM configuration system via either the web interface or by using gconfig from the command line interface. From the main screen, select "Serial Ports", then the name of the port that is connected to the digitiser's "GPS" port. Change the function of the port to "NMEA Out", with the baud rate of 4800. Click "Submit" to save these changes. Go back the configuration of the serial port and click on "NMEA output settings".

You will see this screen:

Serial Port PortA NEMA Settings

Latitude	<input type="text" value="0000.000,N"/>
	Device latitude. Format 0000.000,N
Longitude	<input type="text" value="00000.000,E"/>
	Device longitude. Format 00000.000,E
Height	<input type="text" value="000.0"/>
	The device height in meters
Geoid	<input type="text" value="00.0"/>
	The difference between sea level and geoid height
Invert PPS	<input type="checkbox"/>
	Whether the pulse per second signal should be inverted
<input type="button" value="Home"/> <input type="button" value="Help"/> <input type="button" value="Expert"/> <input type="button" value="Submit"/>	

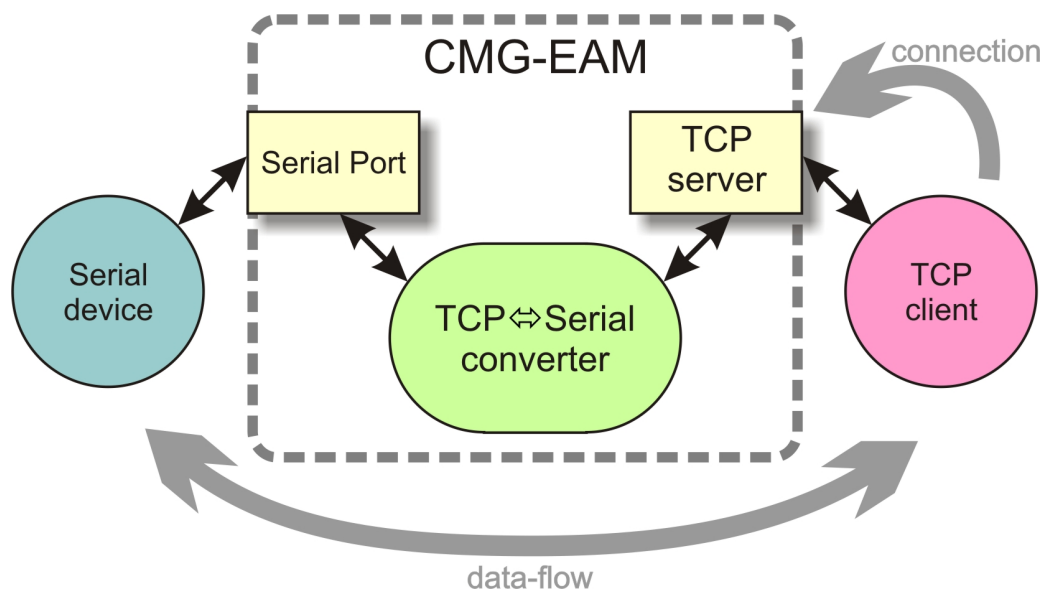
Generated at 2008-05-01 T10:51:09.724604000Z by GCS. Portions of output copyright (c)2008, Guralp Systems Limited.

On this screen you can configure the NMEA sentences that will be sent to the digitiser. You can specify the location (latitude, longitude, elevation), the geoid (the offset of the location from the theoretical earth surface) and whether to invert the Pulse-Per-Second signal (if unchecked, the PPS line will be briefly asserted each second, on the second and held to ground at other times). It is not essential that the position string sent matches the physical location of the digitiser, as only the GPS time signal is used. Click "Submit" to save the changes.

6.10 Configuring TCP to serial converters

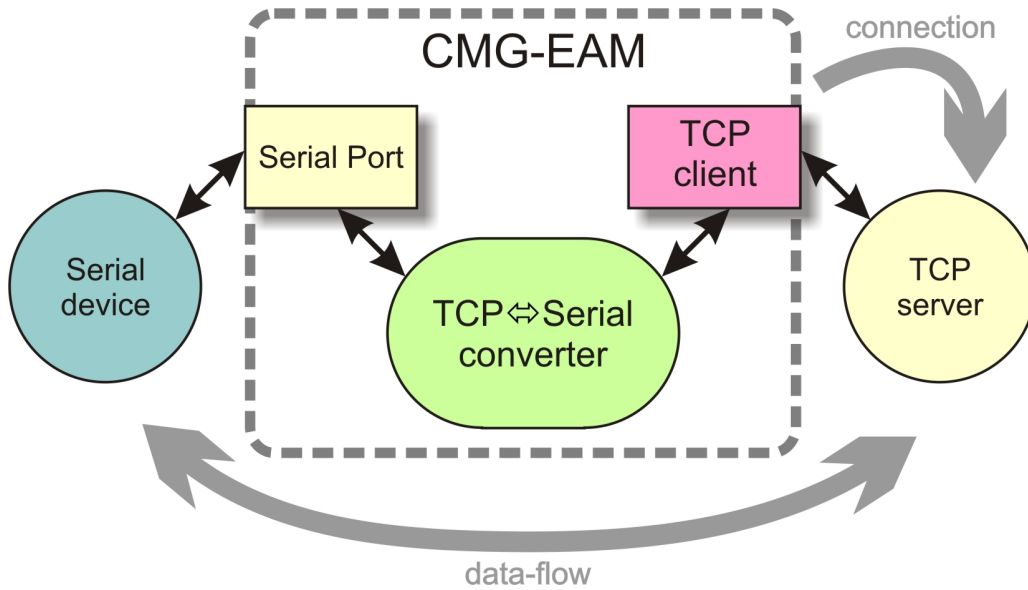
The CMG-EAM can act as a TCP to serial converter, effectively transporting data between one (or more) of its serial ports and a TCP connection. There are two different modes of operation, as detailed below. Any number of serial ports can be configured as TCP converters, as long as the TCP port numbers do not clash.

In “Simple server” mode, the CMG-EAM listens for incoming TCP connections and, should it receive one that matches its configured rules, accepts the connection and begins copying data between the serial port and the TCP connection.



The CMG-EAM can be configured to only listen on particular addresses and ports, to only accept connections from certain addresses or blocks of addresses and to reject connections from certain addresses or blocks of addresses.

In “Simple client mode”, the CMG-EAM will connect to an external TCP server on a particular address and port and then copy data bidirectionally between the serial port and the network port.



To configure the converter, select “Serial Ports” in the configuration menu, then choose the required port. Set the function to “tcp serial converter”, select the baud rate, and save the settings. You can then use the “TCP serial converter settings” button at the bottom of the page to configure the converter.

The converter's configuration page allows you to choose the mode at the top (“Operation mode”). The other options on the page are only required in certain modes; see below for which modes require which options.

Simple server mode

In Simple server mode, the converter opens the serial port and creates a TCP server socket. Whenever a client connects to the socket, the converter reads raw data from the serial port and writes it to the client, and reads raw data from the client and writes it to the serial port. The serial port hardware control lines cannot be read or altered in this mode.

Simple server mode has two relevant options: the list of addresses to listen to, and an optional list of addresses to filter. The server can listen on multiple simultaneous local ports and addresses (although only one client can be active at a time).

The “Bind host” option is usually left blank. If specified, it is the name or IP address on which this server socket will listen. For example, if you specify “localhost” here, then this socket will only listen for incoming connections on the loopback address, and not on the external Ethernet port. Leave it blank to listen to all addresses.

The “Bind service” option must be specified. It is the TCP port number (1-65535) or service name (such as “tcpserial”) for the socket. This can be anything you choose, although we recommend that you use the names `tcpserial`, `tcpserial1`, `tcpserial2` and so on through to `tcpserial15`, which are pre-defined to correspond to port numbers 10002, 10003, through to 10017.

The mapping from port names to port numbers is configured by the conventional Linux file `/etc/services` which can be edited from the command line if required.

If desired, you can configure a list of addresses from which to accept connections. If no addresses are configured, then all incoming addresses will be accepted. Otherwise, connections will only be accepted if they match an entry in the table with its Reject box unticked. Entries are matched in order; as soon as a match is made, the connection is accepted or rejected, and no further processing is done.

The “IP addresses” fields can each specify a host name, an IP address or an IP address range (given in CIDR format). For example, to accept connections from LAN addresses, you can add the addresses:

- **10.0.0.0/8**
(anything from 10.0.0.0 to 10.255.255.255);
- **172.16.0.0/12**
(anything from 172.16.0.0 to 172.31.255.255);
- **192.168.0.0/16**
(anything from 192.168.0.0 to 192.168.255.255); and
- **127.0.0.1**
(loopback address).

Simple client mode

This mode of operation is similar to simple server, except that the CMG-EAM establishes an outgoing TCP client connection rather than listening on a socket. It writes raw data from the serial port to the remote server, and writes raw data from the remote server to the serial port. It does not support the querying or setting of the serial port hardware control lines.

In this mode, only a single option needs to be provided: the contact details for the remote server (IP address and port). The format of this option is “host,service”. The host may be a hostname or an IP address.

The service may be a TCP port number or a service name from `/etc/services`.

6.11 Networking

From this screen you can select to configure the physical interface, any virtual network (VLAN) settings or the network services NTP (network time protocol) and SMTP (simple message transfer protocol, or email transport).

Networking configuration

Select a network interface to configure:

- [eth0 - Primary wired network interface](#)
- [Create a new interface](#)

or a network service:

- [Network Time Protocol \(NTP\) daemon](#)
- [Mail Transfer Agent \(e-mail service\)](#)

Generated at 2008-05-01 T10:50:38.590985000Z by GCS. Portions of output copyright (c)2008, Guralp Systems Limited.

Network Interface Configuration

The CMG-EAM has a single Ethernet adaptor fitted. To configure this, select the line “eth0 – Primary wired network interface”. The parameters for this interface, including DHCP or static addressing, can be configured on the following screen, shown here in parts.

Network Interface eth0

Device	<input type="text" value="eth0"/> Device name (Fixed)
MAC address	<input type="text" value="00:50:c2:40:50:22"/> MAC address (Fixed)
Description	<input type="text" value="Primary wired network interface"/> User description of the interface
Enable interface	<input checked="" type="checkbox"/> Allow the interface to be used
Startup enable	<input checked="" type="checkbox"/> Start the interface at system startup
Enact on submit	<input type="checkbox"/> Check to enact changes when page is submitted. Uncheck to enact on reboot.
Configuration method	<input type="text" value="DHCP (Dynamic Host Configuration Protocol)"/> Determines how the interface parameters are discovered and set

Tick the “Enact on submit” check-box if you wish your changes to take effect immediately. If this check-box is left unticked, changes will take place the next time the CMG-EAM is booted.

To configure the CMG-EAM for DHCP, select “DHCP (Dynamic Host Configuration Protocol)” under the “Configuration method” option, make sure the “Enact on submit” check-box is ticked and press the “Submit” button. DHCP is the recommended way to configure networks, as it centralises management and solves many problems (setting of default routes, etc.). You should ask your DHCP administrator to allocate a fixed IP address to the CMG-EAM's MAC address.

If you need to use a static address, change “Configuration method” to “Static” and submit your IP address and, if required, default route in the following boxes. You can then submit the form. Note that IP addresses must be given in CIDR format, where the dotted quad address is followed by the number of bits defining the netmask, e.g. 192.168.0.1/24).

Static IP address

The following parameters are used only in a static configuration.

IP address	<input type="text"/>
	Address in IPv4 or IPv6 format, with CIDR format netmask (see help)
Default route (gateway)	<input type="text"/>
	The IP address of the gateway router, for access to other networks
<input type="button" value="Home"/> <input type="button" value="Help"/> <input type="button" value="Expert"/> <input type="button" value="Submit"/>	

Generated at 2009-07-14T15:27:46Z by ccs 1.1.5. Portions of output copyright (c)2009, Guralp Systems Limited.

There are many additional, advanced options available on this screen if you change to expert mode, including MTU, extra DHCP arguments, and multi-homing options.

6.12 Configuring the Network Time Protocol (NTP) Daemon

The Network Time Protocol (NTP) is a method of synchronising the clocks of computer systems over networks, including those with variable latency, such as packet-switched networks, allowing the CMG-EAM to keep its internal clock accurate. This must be set up correctly if you intend to use the CMG-EAM to generate a clock for connected digitisers using “fake” GPS data-streams (NMEA out) - see section 6.9 on page 60.

To use this function, connect to the CMG-EAM configuration system via either the web interface or by using gconfig from the command line interface. From the main screen, select “Networking” and then “NTP (Network Time Protocol)”.

Network Time Protocol

Acquire time from connected GPS	<input type="checkbox"/>	Allows NTP to acquire the time from connected GPS receivers.
Acquire time from connected digitisers	<input type="checkbox"/>	Allows NTP to acquire the time from suitable digitisers.
The following servers will be queried for the time. You can specify a server by hostname or by IP address.		
Server address	Delete	
rhodium.calleva.guralp	<input type="checkbox"/>	
<input type="button" value="Home"/> <input type="button" value="Help"/> <input type="button" value="Expert"/> <input type="button" value="Submit"/>		

Generated at 2008-05-01 T10:50:50.398449000Z by GCS. Portions of output copyright (c)2008, Guralp Systems Limited.

The NTP daemon runs constantly in the background and sets the clock of the CMG-EAM using any sources configured in this screen. It can acquire the time from a connected GPS device if the “Acquire time from connected GPS” is checked. It can acquire the time from a connected Guralp digitiser if the “Acquire time from connected digitisers” check-box is ticked. Other local or internet time servers can be configured in the remaining boxes as either IP addresses or hostnames.

6.13 Configuring the Mail Transfer Agent (MTA)

The CMG-EAM software can send alerts about important events by email if this feature is configured. To set up this function, connect to the CMG-EAM configuration system via either the web interface or by using gconfig from the command line interface. From the main screen, under “Networking”, select “Mail”.

Mail Transfer Agent

These parameters control the Mail Transfer Agent (MTA) used to relay e-mail between machines.

Enable MTA	<input checked="" type="checkbox"/>	Start the MTA at system startup
Smart host	<input type="text" value="quartz.lan"/>	Smart delivery host (leave blank to attempt direct delivery)
Mail host identity	<input type="text"/>	Our identifying name (leave blank to use the global hostname)
Postmaster alias	<input type="text"/>	The mail address all "system" mail should be directed to
<input type="button" value="Home"/> <input type="button" value="Help"/> <input type="button" value="Expert"/> <input type="button" value="Submit"/>		

Generated at 2008-05-01 T10:50:33.161794000Z by GCS. Portions of output copyright (c)2008, Guralp Systems Limited.

The MTA can be enabled and disabled as required using the “Enable MTA” check-box. The “Smart host” field allows you to specify the machine (hostname or IP Address) to which the MTA will attempt to deliver outgoing email. The optional “Mail host identity” specifies the hostname from which outgoing emails should appear to originate. If this field is left blank, the real hostname is used. The “Postmaster alias” allows you to specify the address to which all internally generated mail should be sent: This should be set to the email address of the CMG-EAM's administrator.

6.14 Configuring the SSH Server

The CMG-EAM has an ssh server running on its Ethernet port which allows remote terminal access.

The ssh server, `sshd`, can not currently be configured using `gconfig` although it can be configured via the web interface. If web access is unavailable, it is possible to configure `sshd` from the command line by directly editing the configuration files.

Configuring sshd via the web interface

From the main screen of the web interface, under Configuration, Networking, select “SSH server”. The screen is not reproduced in this document as it is particularly large, due to the amount of explanatory text. Each option is, however, discussed.

The version of `sshd` installed (openSSH) supports both version 1 and version 2 of the ssh protocol. Version 1 has some well-known weaknesses and should be avoided if at all possible, but some commercially available systems still do not support v2, so v1 is supported here for compatibility. The “Enable SSH Protocol v1” check-box should be de-selected unless your ssh client cannot support v2 or

cannot be upgraded to support it. Click the “Change server options” button to commit this change.

If you want to download the ssh server's public key to allow the connecting host to check and verify the CMG-EAM's identity, use the relevant “Download server public key” button – there is one each for protocol versions 1 and 2. There is also the capability to command the CMG-EAM to create a new private/public key pair from this screen.

To configure password-less login to the CMG-EAM, you can upload the public key of the connecting machine to the CMG-EAM using the “New client key” section. Browse for the key file (usually named `id_dsa.pub`) and upload it here. This will allow password-less root access to the system from that machine.

Client keys which have been uploaded are displayed in the “Authorised client keys” section. Any existing authorised keys can be removed: Select the check-box next to the key you wish to remove and click “Remove selected keys”.

NOTE: password-less login via ssh v2 is, perhaps counter-intuitively, the most secure way to access your CMG-EAM. There is a useful discussion of the ssh protocol and full details of its usage at the site <http://tinyurl.com/whyssh>

6.15 Configuring Port Power Limits

As described in section 3.2, the CMG-EAM mk4 can be fitted with sensors to monitor the power consumption of devices connected to its ports, such as the CMG-DM24 Digitiser. The sensors monitor the bus voltage and current being drawn by devices. If these exceed certain limits, the sensor will automatically shut off the power to the port. It can only be re-enabled once the error condition has been removed, as described in section 3.2.

To set up the port power limits on the CMG-EAM, connect to the CMG-EAM configuration system via either the web interface or by using `gconfig` from the command line interface. From the main screen select “All options”, then “Power management options”. If the option is not displayed, you have a CMG-EAM that is not fitted with sensors.

On this screen is a list of all of the ports that are fitted with power management sensors. You can fill in any limits you want to set in the table.

DCM Power Management

The DCM mk4 has hardware to automatically turn off the power supply to external devices if it detects error conditions with the supply. These limits can be set for each port separately.

Port Settings

Port Name	Current Limit (mA)	Min Bus Voltage (mV)	Max Bus Voltage (mV)
Data Out	<input type="text"/>	<input type="text"/>	<input type="text"/>
Port B	<input type="text"/>	<input type="text"/>	<input type="text"/>

Generated at 1970-01-01T06:19:17.675113229Z by gcs. Portions of output copyright (c)1970, Guralp Systems Limited.

- The “Current Limit (mA)” field sets the maximum current that can be drawn from the port, specified in milliamps. If this is exceeded, the port will be turned off automatically.
- The “Min Bus Voltage (mV)” field sets the minimum allowable bus voltage for the device connected to the port, specified in millivolts. If the bus voltage falls below this, the port will be turned off automatically.
- The “Max Bus Voltage (mV)” field sets the maximum allowable bus voltage for the device connected to the port, specified in millivolts. If the bus voltage goes above this, the port will be turned off automatically.

6.16 Configuring Additional Data Input Services

By default, the CMG-EAM is configured to receive GCF data from each of its serial input ports. It has the capability to receive simultaneous data from additional sources and in additional formats. The configuration of additional input formats is described in this section. CD1.1 input is covered in a separate manual, MAN-EAM-0011. If you require an input format not already covered, please contact Guralp support.

GDI link receiver

GDI is a highly efficient, low latency protocol for communicating between GSL-DCMs, GSL-EAMs and GSL-NAMs. It allows direct communication between the gdi-base modules (see section 5 on page 45) at each end of the link. State of health information is attached to samples before transmission.

GDI links have transmitters, which send data, and receivers which receive it. These terms do not refer to the direction of initiation of the

network connection: a receiver can initiate a connection to a transmitter and vice versa.

To configure a GDI link receiver, connect to the CMG-EAM configuration system via either the web interface (select “All options”) or by using gconfig from the command line interface. From the main screen select “services”, then “GDI link receiver”. The next screen shows a list of all GDI link receiver instances that have been configured on the CMG-EAM.

GDI link receiver instance selection

Select the GDI link receiver instance you wish to configure:

- [GDI link receiver. Default instance - Disabled](#)
- [Create new service instance](#)

[Home](#) [Help](#) [Expert](#) [Submit](#)

Generated at 2009-06-23T13:08:49Z by ccs 1.1.5. Portions of output copyright (c)2009, Guralp Systems Limited.

In most cases, you will only need a single instance and you can enable and reconfigure the Default Instance for your requirements.

Clicking on the Default Instance link brings up the screen shown overleaf.

You can enter a descriptive name for the instance: this is useful if you are configuring multiple instances but, in most cases, this can be set to the hostname of the CMG-EAM.

The Network Settings section allows you to set an optional “client name” which will be visible from the GDI link server.

If the GSL-EAM has multiple network addresses, you can limit the GDI link receiver to use only one of them by entering it in the “Local IP address” field. If left blank, the receiver will listen on all configured addresses.

The default GDI link port is 1566 but this can be over-ridden if desired - you would want to do this if you had multiple instances running on the same address - by entering a port name or number in the “Local port/service” field.

Backfill is the process whereby missing data is recovered. It can be disabled if desired but, in most cases, you should leave this enabled.

GDI Link Receiver

gdi-link-rx receives samples in the native protocol of the Platinum software suite, called Guralp Data Interconnect. This is a low-latency real-time transmission protocol which sends encoded state of health with samples.

User description	GDI link receiver. Default instance User label for this receiver module
Default service is always enabled	

Network settings

Client name	<input type="text"/>	Used to identify this receiver to other transmitters. Leave empty for default.
Local IP address	<input type="text"/>	IP address or host name to listen on. Leave empty for default.
Local port/service	<input type="text"/>	Service name or TCP port number to listen on. Leave empty for default.

Backfill

Enable backfill	<input checked="" type="checkbox"/>
Directory	<input type="text" value="/var/lib/gdi-link-rx.default"/> Directory under which backfill state files are stored.

The remainder of the screen (not shown) contains a table within which you can configure the GDI link servers to which this receiver should listen. For each server, you should set:

- the peer name: this should match the server name configured on the
- the remote host: this is the DNS name or IP address of the GDI link server
- the remote service/port: the default is 1565 but, if you have configured a different port on the GDI link server, you should enter the same port here.
- enable at start-up
- filtering: you can filter by sample rate or channel names

When you have entered all the required information, press Submit.

BRP - GCF From Network Enabled Digitisers

The CMG-EAM has the ability to receive data from network enabled digitisers such as the CMG-6TD. Data can be received from any number of digitisers, by creating multiple GCF BRP receivers.

To set up a GCF BRP receiver on the CMG-EAM, connect to the CMG-EAM configuration system via either the web interface (select “All options”) or by using gconfig from the command line interface. From the main screen select “System services”, then “GCF BRP network client”. The next screen shows a list of all GCF BRP receiver instances that have been configured on the CMG-EAM.

GCF BRP network client instance selection

- [Create new service instance](#)



Generated at 2009-07-10T11:16:15Z by ecs 1.1.5. Portions of output copyright (c)2009, Guralp Systems Limited.

To configure a GCF BRP receiver, select “Create new service instance”. The following screen allows you to configure the parameters of the service.

The “User description” field sets the name of the service; this should be set to a meaningful name for the data that it will be receiving, such as the IP or hostname of the network digitiser.

The User label is another optional field. If set, this label is used to identify the particular client instance in log-files.

The service can be enabled or disabled at boot-up using the “Enable” check-box or deleted entirely using the “Delete” check-box.

Specify the hostname or IP address of the network digitiser in the “Remote Server” box and the port (name or number) that the digitiser is transmitting on in the “Remote service” box.

Network BRP client settings

User description	<input type="text" value="GCF BRP network client. Instance 1"/> User label for the receiver instance
User label	<input type="text" value="Network BRP in 0"/> Application label used for identification in logs
Enable	<input type="checkbox"/> Enable this BRP receiver at system startup
Delete	<input type="checkbox"/> Delete this BRP receiver instance
Remote server	<input type="text"/> The remote server to connect to for data
Remote service	<input type="text" value="10002"/> The remote service or port number to connect to
Allow disconnects	<input checked="" type="checkbox"/> Attempt to reconnect broken TCP connections
Disable rewind	<input type="checkbox"/> Disable BRP rewinding, for DM24s in adaptive mode etc.

Generated at 2009-07-10T11:29:49Z by ccs 1.1.5. Portions of output copyright (c)2009, Guralp Systems Limited.

If the “Allow disconnects” check-box is ticked, the instance will attempt to automatically recover from lost connections by trying to reconnect to the server.

If the “Disable rewind” check-box is ticked, no attempts will be made to request missing data blocks. This should only be selected if the server is unable to fulfil such requests.

Data from Scream! servers

The CMG-EAM has the ability to receive data over the network from Scream! servers. Data can be received from any number of Scream! servers by creating multiple Scream! receivers.

GCF Scream network client instance selection

- [Create new service instance](#)

Generated at 2009-07-10T14:20:01Z by ccs 1.1.5. Portions of output copyright (c)2009, Guralp Systems Limited.

To set up a Scream! receiver on the CMG-EAM, connect to the CMG-EAM configuration system via either the web interface (select “All options”) or by using gconfig from the command line interface. From the main screen select “System services”, then “GCF Scream network client”. The resulting screen shows a list of all Scream! receiver instances that have been configured on the CMG-EAM.

To configure a Scream receiver, select “Create new service instance”. The following screen, allows you to configure the parameters of the service.

Scream network client

User description	<input type="text" value="Scream network client. Instance 1"/> User label for the convertor instance
Enable	<input type="checkbox"/> Enable the convertor at system startup
Delete	<input type="checkbox"/> Delete this convertor instance
Please note this page has additional descriptions for the sections below; press the Help button to view them.	

Network options

Local address	<input type="text"/> Local interface address or hostname. Leave blank for all.
Local service	<input type="text" value="scream1"/> Local port number or service name. Leave blank for default.

Servers

Each server requires a unique name. This is used for configuration and logging only.

Name	Hostname	Service	Type	Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	UDP ▾	
<input type="text"/>	<input type="text"/>	<input type="text"/>	UDP ▾	
<input type="text"/>	<input type="text"/>	<input type="text"/>	UDP ▾	

Generated at 1970-01-04T21:44:02Z by gcs. Portions of output copyright (c)1970, Guralp Systems Limited.

The “User description” field sets the name of the service; this should be set to a meaningful name for the data that it will be receiving, such as the IP or hostname of the Scream! server.

The service can be enabled or disabled at boot-up using the “Enable” check-box or deleted entirely using the “Delete” check-box.

If the CMG-EAM has multiple IP addresses, you can optionally restrict the client so that all connection attempts are made via only one address by putting it in the “Local address” field. You can also specify

that requests should be made from a specific port number by entering it in the “Local service” field. These two fields can normally be left blank.

In the “Servers” section, you specify the details of the Scream! servers from which you want to pull data. The “Name” field should contain a descriptive name for identification purposes. The “Hostname” field can contain the DNS name or IP address of the desired server. The “Service” field should contain the UDP/TCP port number on which the server is listening for data requests. Port numbers can be mapped to names using the standard Linux `/etc/services` file, which can be edited from the command line.

In the “Type” column, choose whether you wish to use UDP packets or TCP connections. With UDP packets, the GCF protocol keeps track of which packets have been received and automatically requests retransmission of any missing data. TCP, on the other hand, is a connection-orientated protocol which handles packet sequencing and retransmission itself (at the cost of a little extra network overhead).

6.17 Data Storage

Data can be recorded to internal and external storage, in raw GCF format or in miniSEED format. The options that control this process are all on one page but, given its size, it is shown here in sections. To configure data storage, connect to the CMG-EAM configuration system via either the web interface (choose “All options”) or by using `gconfig` from the command line interface. Select the option “Disk recording”.

gdi-record

The program `gdi-record` records data packets to internal and external storage. The default settings for this service will work in most

Disk recording configuration

These parameters control global disk recording operation and the removable disk support daemon (`rdisk`).

Disable all recording	<input checked="" type="checkbox"/>	Disable all data recording to disk
Recycle files	<input type="checkbox"/>	Remove old files from the hard disk when low on space.
Check output flush	Every 5 minutes <input type="button" value="v"/>	How often to check whether output needs flushing
Using the removable disk support daemon. Use expert mode if you wish to disable.		

installations but, if you wish to fine-tune the behaviour of `gdi-record`, you can alter the following configuration options:

- Disable all recording. This option unconditionally disables all recording on the device.
- Recycle files – If this option is checked then the data journaller will remove the oldest files from external storage to make room for new data when the external storage becomes full. If this option is not checked the, when the storage becomes full, the journaller will check periodically for free space and start writing again when it can.
- Check output flush – in order to reduce power consumption, `gdi-record` does not write continuously to the hard drive. Data are buffered in flash memory and, at a configurable interval, these data are checked to see which complete files can be written to disk. Use the option to control how often this happens.

GCFraw Options

GCFraw is the native recording format of the CMG-EAM. It can be read directly by `Scream!` and other GSL software packages are available for conversion into other formats.

GCFraw recording

These parameters control the recording of raw GCF packets.

Disable GCF recording	<input type="checkbox"/> Disable the recording of raw GCF data.
File period	30 minutes ▾ Time span held in each output file

GCFraw recording is enabled by default. To disable it, select the “Disable GCF recording” check-box.

GCF files contain data from all streams and can grow quite large. The data are split into manageable chunks on the basis of sample times. By default, every thirty minutes the current file is closed and recording recommences to a new file. This interval can be changed using the “File period” drop-down. The options are 15 or 30 minutes and 1, 2, 3, 4, 6 or 12 hours.

Extra options are introduced to this screen by pressing the “Expert” button. These include file name format control for GCF and miniSEED. See the following section for details.

Mini-SEED Options

For some applications, it is more convenient to store the data directly in mini-SEED format. The third section of the “Disk data recording” page controls options related to recording in this format.

mini-SEED recording

These parameters control the recording of data as mini-SEED packets.

Disable mini-SEED recording	<input checked="" type="checkbox"/> Disable recording data as mini-SEED packets.
Caution if enabling mini-SEED recording check the state of the Disable all setting at the top of this form.	
File period	3 hours <input type="button" value="v"/> Time span held in each output file
<input type="button" value="Home"/> <input type="button" value="Help"/> <input type="button" value="Expert"/> <input type="button" value="Submit"/>	

Mini-SEED recording is disabled by default. To enable it, clear the “Disable mini-SEED recording” check-box.

By default, every three hours the current mini-SEED file is closed and recording recommences to a new file. This interval can be changed using the “File period” drop-down. The options are 15 or 30 minutes and 1, 2, 3, 4, 6 or 12 hours.

Extra options are introduced to this screen by pressing the “Expert” button. These include file name format control for GCF and miniSEED.

The “File name format” field allows files to be given descriptive names to help identify the data within. Escape sequences, which all begin with a '%' character, are used to insert variables such as the data or stream name into the file-name; each escape sequence is replaced with the relevant value. Any non-escape sequence characters are copied verbatim into the file-name. All numbers are decimal and will have leading zeroes added to fill the number of digits.

The escape sequences available are:

- **%d** 2 digit day of month (01-31)

- **%H** 2 digit hour in 24 hour clock (00-23)
- **%j** 3 digit Julian day
- **%m** 2 digit month (01-12)
- **%M** 2 digit minute (00-59)
- **%y** 2 digit year i.e. without century digits (00-99)
- **%Y** 4 digit year

- **%s** 5 char SEED station identifier (spaces are removed from all SEED Ids)
- **%c** 3 char SEED channel identifier
- **%n** 2 char SEED network identifier
- **%l** 2 char SEED location identifier

If the format string ends in a `.extension` (without any escape sequences in the extension) then this extension will be noted and used in some other locations – e.g. for the top level date directory.

The default format string is `%Y%j-%H%M-%s-%c-%n-%l.mseed`

Slashes “/” will cause subdirectories to be created. Using them as date separators will have unintended and, usually, undesirable consequences.

Some examples

The default `%Y%jT%H%MZ-%s-%c-%n-%l.mseed` includes every piece of information possible. The date format matches that used by the GCF recorder. This will produce file-names like:

`2008315T1442Z-TEST1-BHE-NN-LL.mseed`

To combine all the channels from a given station simply omit the channel marker from the file name format string:

`%Y%jT%H%MZ-%s--%n-%l.mseed`

It is recommended that the “--” is left in place to highlight the omitted channel id. This will produce file-names like:

```
2008315T1442Z-TEST1--NN-LL.mseed
```

If you specifically want to include a marker to identify that it contains all channels, the use of a lower case string will differentiate it from a regular channel name, which is always presented in upper case.

```
%Y%jT%H%MZ-%s-all-%n-%l.mseed
```

yields file-names like:

```
2008315T1442Z-TEST1-all-NN-LL.mseed
```

If you prefer human readable dates, rather than using the Julian date

```
%Y_%m_%d-%H:%M-%s-%c-%n-%l.mseed
```

yields file-names like:

```
2008_08_14-14:42-TEST1-BHE-NN-LL.mseed
```

Note: don't use / as a date separator as this will split the data into sub-directories which is probably not the desired result.

It is often required to separate the data into sub directories by network and station prefix. In this case, it is recommended that the network and station id are still included in the file-name so that the contents of the file are still recognisable even if it is moved to a different location.

```
%n_%s/%Y%jT%H%MZ-%s-%c-%n-%l.mseed
```

will store the data like this:

```
NN_TEST1
    2008315T1442Z-TEST1-BHE-NN-LL.mseed
    2008315T1452Z-TEST1-BHE-NN-LL.mseed
    2008315T1502Z-TEST1-BHE-NN-LL.mseed
    ...
NN_TEST2
    2008315T1442Z-TEST2-BHE-NN-LL.mseed
    2008315T1452Z-TEST2-BHE-NN-LL.mseed
    2008315T1502Z-TEST2-BHE-NN-LL.mseed
    ...
```

6.18 Configuring Additional Data Output Formats

By default, the CMG-EAM is configured with a single Scream! Server. The Scream! Server is configured to send out all data that it receives. It has the capability to send out this data in any combination of formats simultaneously, if additional output formats are configured as in this section. Sending data in CD1.1 format is covered by a separate manual, MAN-EAM-1100. If an output format that you require is not covered, please contact Guralp support.

GDI Link Transmitter

GDI is a highly efficient, low latency protocol for communicating between GSL-DCMs, GSL-EAMs and GSL-NAMs. It allows direct communication between the gdi-base modules (see section 5 on page 45) at each end of the link. State of health information is attached to samples before transmission.

GDI links have transmitters, which send data, and receivers which receive it. These terms do not refer to the direction of initiation of the network connection: a receiver can initiate a connection to a transmitter and vice versa.

To configure a GDI link transmitter, connect to the CMG-EAM configuration system via either the web interface (select “All options”) or by using gconfig from the command line interface. From the main screen select “services”, then “GDI link transmitter”. The next screen shows a list of all GDI link transmitter instances that have been configured on the CMG-EAM.

GDI link transmitter instance selection

Select the GDI link transmitter instance you wish to configure:

- [GDI link transmitter. Default instance - Enabled](#)
- [Create new service instance](#)

Generated at 2009-06-23T14:14:09Z by ecs 1.1.5. Portions of output copyright (c)2009, Guralp Systems Limited.

In most circumstances you will only need a single GDI link transmitter but this screen allows you to create more if desired.

To configure the transmitter, click on the link corresponding to the required instance. You will see the following screen (only the top part of which is shown here):

GDI Link Transmitter

gdi-link-tx transmits samples in the native protocol of the Platinum software suite, called Guralp Data Interconnect. This is a low-latency real-time transmission protocol which sends encoded state of health with samples.

User description	GDI link transmitter. Default instance User label for this transmitter module
Default service is always enabled	

Network settings

Client name	<input type="text"/> Used to identify this transmitter to other receivers. Leave empty for default.
Local IP address	<input type="text"/> IP address or host name to listen on. Leave empty for default.
Local port/service	<input type="text"/> Service name or TCP port number to listen on. Leave empty for default.

Backfill

By default, backfill is disabled. Be sure to enable it if required, and to set up an associated directory cleaner task to manage buffer space.

Enable backfill	<input type="checkbox"/>
Directory	<input type="text" value="/var/lib/gdi-link-tx.default"/> Directory under which backfill files are stored.

The description of the instance can be changed if desired. This may be useful if you have multiple instances. This description is seen when viewing running services or configuring instances. It is not seen by the clients.

Subsequent instances can be enabled or disabled with a check-box but this is absent from the page for the default instance because the default instance is always enabled.

The instance name, as seen by the client, can be set in the first field under “Network settings”. A suitable default is used if this field is left blank.

If the CMG-EAM has multiple network addresses, it can be restricted to listen for incoming connections on only one of them by entering its

address here. If left blank, the transmitter will listen on all available instances.

The default service (port) for the transmitter is 1565 but an alternative port can be entered here if required.

Backfill is the process whereby missing data is recovered. It can be disabled if desired but, in most cases, you should leave this enabled.

The remainder of the screen (not shown) contains a table within which you can configure the GDI link clients to which this transmitter should send data. For each client, you should set:

- the peer name: this should match the server name configured on the
- the remote host: this is the DNS name or IP address of the GDI link client
- the remote service/port: the default is 1566 but, if you have configured a different port on the GDI link client, you should enter the same port here.
- enable at start-up

When you have entered all the required information, press Submit.

Güralp Seismic Monitoring System

GSMS is a protocol designed by Güralp Systems to send real time, low latency strong motion data. To set up a GSMS server on the CMG-EAM, connect to the CMG-EAM configuration system via either the web interface (select "All options") or by using gconfig from the command line interface. Select "System Services", then "GSMS Sender". The next screen shows a list of all GSMS server instances that have been configured on the CMG-EAM.

GSMS Sender instance selection

- [Create new service instance](#)

Generated at 2008-05-01 T10:51:33.897928000Z by GCS. Portions of output copyright (c)2008, Güralp Systems Limited.

To configure a GSMS server, select “Create service instance”. The following screen allows you to configure the parameters of the server.

GSMS sender configuration

User description	<input type="text" value="GSMS sender. Instance 1"/> User label for the transmitter instance
User label	<input type="text"/> Application label used for identification in logs
Enable	<input type="checkbox"/> Enable the transmitter at system startup
Delete	<input type="checkbox"/> Delete this transmitter instance

Network parameters

Bind host	<input type="text"/> The hostname or IP address the server will bind to. Leave empty for all.
Service port	<input type="text" value="9001"/> The TCP and UDP port number or service name to listen on.

Push hosts

Protocol	Push host	Service	Delete
UDP ▾	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
UDP ▾	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
UDP ▾	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

The name (User description) of the server should be set to a meaningful name for the data that it will serve. The optional User Label field can be filled in with a name which will then be used to identify this instance in log files. The server can be enabled or disabled at boot-up using the “Enable” check-box or deleted entirely by selecting the “Delete” check-box.

To configure the server to listen for incoming data requests on a specific IP address, set this in the “Bind host” box. By default it will listen on all configured interfaces. Set the port that you want the server to listen on in the “Service Port” box.

If you want the server to pro-actively send data to remote GSMS receivers, enter their IP addresses and port numbers in the “Push hosts” table. For each, select TCP or UDP from the drop-down list as the protocol to use - this must match the receiver's setting.

The GSMS server need not send all data from all channels to its clients: it is possible to select which channels are transmitted. Select one of the three different transmission modes:

- Automatic: all channels are transmitted and named automatically
- Semi-automatic: all channels are transmitted and names can be mapped using a configuration table
- Manual: only channels named in the configuration table are transmitted.

The relevant part of the screen looks like this:

Channels

Select which channels to transmit. See help for more details.

Naming mode Automatic - all channels are transmitted and named automatically
Select how channels are selected for transmission and named

System name	Output channel name (SEED)	Delete
A830-55TPE4	A830.BHE..55	<input type="checkbox"/>
A830-55TPZ4	A830.BHZ..55	<input type="checkbox"/>
A830-55TPN4	A830.BHN..55	<input type="checkbox"/>
A830-55TP00	A830.SOH..55	<input type="checkbox"/>

The software will attempt to populate the table based on incoming data streams so it is a good idea to configure all input sources and run the system for a few minutes before completing this table.

Quick Seismic Characteristic Data

QSCD is a protocol developed by KIGAM (<http://www.kigam.re.kr/eng>) to send strong motion results, which are computed every second. To set up a QSCD server on the CMG-EAM, first configure the relevant strong motion data sources, then connect to the CMG-EAM configuration system via either the web interface (select "All options") or by using gconfig from the command line interface. Select "System Services", then "QSCD Sender". The next screen shows a list of all QSCD server instances that have been configured on the CMG-EAM.

KIGAM QSCD (Quick Seismic Characteristic Data) sender instance selection

- [Create new service instance](#)

Home Help Expert Submit

Generated at 2009-07-10T15:49:15Z by ecs 1.1.5. Portions of output copyright (c)2009, Guralp Systems Limited.

To configure a QSCD sender, select “Create service instance”. The following screen allows you to configure the parameters of the server. As it is a large screen, it is shown here in pieces.

QSCD sender configuration

User description	<input type="text" value="KIGAM QSCD (Quick Seismic Characteristic Data) sender. Instance"/> User label for the transmitter instance
Enable	<input checked="" type="checkbox"/> Enable the transmitter at system startup
Delete	<input type="checkbox"/> Delete this transmitter instance

The User description of the server should be set to a meaningful name for the data that it will serve. The server can be enabled or disabled at boot-up using the “Enable” check-box or deleted entirely by selecting the “Delete” check-box.

Network parameters

Station name	<input type="text" value="DCM10"/>	5 letter SEED like station name to identify transmission	
Push host	Service	Delete	
<input type="text" value="rhodium"/>	<input type="text" value="9001"/>	<input type="checkbox"/>	
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	

Like SEED, QSCD links require a unique name to identify the source of the data. This should be entered into the “Station name” field.

To send QSCD data to remote hosts, enter their DNS names or IP addresses in the table, with the associated service name or port number for each. Port names and numbers are associated with each other in the standard Linux `/etc/services` file.

Strong motion data channels

Select the instrument being used for QSCD packets here. The instrument must be a CMG-DM24mk3 set up for strong motion mode (including SI output).

Instruments which seem to be configured for strong motion:
A830-55TP

Instrument	<input type="text" value="A830-55TP"/>		
Enter instrument name (SYSID-SER) here. Omit last two digits from channel name.			
<input type="button" value="Home"/>	<input type="button" value="Help"/>	<input type="button" value="Expert"/>	<input type="button" value="Submit"/>

Generated at 2009-07-14T16:07:30Z by gcs 1.1.5. Portions of output copyright (c)2009, Guralp Systems Limited.

The CMG-EAM scans all incoming data and prepares a list, in the correct format, of the names of instruments which are sending strong motion results. Enter one of these names in the “Instrument” field.

The QSCD protocol only supports a single instrument. If you need to transmit results from multiple instruments, you should configure multiple QSCD sender instances, one for each instrument.

WIN Sender

WIN is a Japanese seismic data format. To set up a WIN sender on the CMG-EAM, connect to the CMG-EAM configuration system via web or terminal. From the main screen select “Services”, then “WIN Sender”. The next screen shows a list of all WIN sender instances that have been configured on the CMG-EAM.

WIN Sender instance selection

[• Create new service instance](#)

<input type="button" value="Home"/>	<input type="button" value="Help"/>	<input type="button" value="Expert"/>	<input type="button" value="Submit"/>
-------------------------------------	-------------------------------------	---------------------------------------	---------------------------------------

Generated at 2008-05-01T10:51:54.208661000Z by GCS. Portions of output copyright (c)2008, Guralp Systems Limited.

To configure a WIN sender, select “Create service instance”. The following screen allows you to configure the parameters of the sender. It is shown here in parts.

WIN format transmitter configuration

User description	<input type="text" value="WIN sender. Instance 1"/> User label for the service instance
User label	<input type="text"/> Application label used for identification in logs
Enable	<input type="checkbox"/> Enable the transmitter at system startup
Delete	<input type="checkbox"/> Delete this transmitter instance

The “User description” of the service should be set to a meaningful name for the data that it will send. The “User label” can be set to

distinguish this instance from others in the log files. The sender can be enabled or disabled at boot-up using the “Enable” check-box or deleted entirely by selecting the “Delete” check-box.

The WIN transmitter can be configured to be either a TCP server to multiple clients, or a UDP sender to a single address. If you want to send the data to multiple clients, set up the CMG-EAM as a TCP server and the remote machines as clients that connect to it.

Network parameters

Protocol	TCP server accepting multiple clients <input type="button" value="v"/> Set the protocol used for transmission
Hostname	<input type="text"/> Hostname or IP address to use
Service	9999 <input type="text"/> Service or port number to use
Max delay	5 <input type="text"/> Maximum delay before data is transmitted (seconds)
Early transmit size	450 <input type="text"/> Packets exceeding this size may be transmitted early
UTC offset	+9 hours (JST) <input type="button" value="v"/> Hour offset from UTC to apply to timestamps

To configure the sender as a TCP server, select “TCP server accepting multiple clients” from the “Protocol” drop-down list. To use a specific IP address to listen for requests from clients, set this in the “Hostname” box. By default it will listen on all interfaces. Set the port that you want the server to listen on in the “Service” box.

If you only want to send the data to a single UDP server, select “UDP datagrams sent to specified address” from the “Protocol” drop-down list. Configure the remote machine's hostname or IP address in the “Hostname” box and set the port number that the remote machine will listen on in the “Service” box.

The WIN sender will buffer up data before it is sent so that outgoing packets have a second's worth of data from all channels. If no data is received from some channels within a certain time limit, the data from other channels will be transmitted anyway. This limit is specified by the value in the “Max delay” field and defaults to five seconds. If a packet in construction exceeds the size specified by “Early transmit size” this packet will also be sent early.

The WIN Format uses the local time in order to time-stamp packets. The offset of the local time-zone from UTC used in the GCF data is specified in the “UTC Offset” box.

The final table, shown overleaf, specifies the mapping from GDI channel names to WIN channel numbers. *Note:* previous versions of the firmware required this mapping to be entered in SEED notation but this is no longer the case.

Channels

GDI channel name	WIN channel number	Delete
A830-55TP00	<input type="text"/>	<input type="checkbox"/>
A830-55TP20	<input type="text"/>	<input type="checkbox"/>
A830-55TP2P	<input type="text"/>	<input type="checkbox"/>
A830-55TP2Q	<input type="text"/>	<input type="checkbox"/>
A830-55TP2R	<input type="text"/>	<input type="checkbox"/>

6.19 Guralp Secure TCP Multiplexer

The Guralp Secure TCP Multiplexer (GSTM) is a method by which TCP and UDP connections can be tunneled in both directions over a single TCP connection. It is an essential tool in situations where local network service providers cannot provide fixed (static) IP addresses.

For example, in an installation involving a single, central data collection point and multiple, remote sensor sites it is sometimes impractical for the sensor sites to be allocated static IP addresses. Using GSTM allows the remote sites to initiate a single GSTM TCP connection to the central site. Once established, further TCP and UDP connections can be initiated in either direction: their packets are tunnelled over the GSTM link.

If no sites in an array can be assigned fixed IPs, including the central data collection point, a GSL-EAM or GSL-NAM can be installed anywhere that has a fixed IP address and used as a communications hub. All sites initiate GSTM connections to the hub, which can then act as a communications router, forwarding individual connections as required.

The initial link is established from a GSTM client to a GSTM server.

The GSTM Client

To set up a GSTM client on the CMG-EAM, connect to the CMG-EAM configuration system via web or terminal. From the main screen select “Services”, then “Guralp secure TCP multiplexor client”. The next screen shows a list of all GSTM client instances that have been configured on the CMG-EAM.

Guralp secure TCP multiplexor client instance selection

- [Create new service instance](#)

Home Help Expert Submit

Generated at 2009-06-23T15:41:59Z by gcs 1.1.5. Portions of output copyright (c)2009, Guralp Systems Limited.

To configure a GSTM client, click “Create new service instance”. The resulting screen allows you to configure the parameters of the new instance.

Guralp secure TCP multiplexor client configuration

User description	Guralp secure TCP multiplexor client. Instance 1 User label for this GSTM client instance
Enable	<input type="checkbox"/> Enable the GSTM client at system startup
Delete	<input type="checkbox"/> Delete this GSTM client instance

The “User description” field allows you to enter a mnemonic description of this instance, which may be useful if you intend to run multiple instances. The client can be set to start automatically when the CMG-EAM boots by clicking the “Enable” check-box, or deleted from the system entirely by clicking the “Delete” check-box.

The client will automatically connect to a GSTM server who's DNS name or IP address is specified in the “Server” field, using a port who's service name or number is specified in the “Port/service” field. The client identifies itself to the server using a username: this can usefully be set to the hostname of the CMG-EAM.

Server settings

Server	<input type="text"/> Hostname or IP address to connect to.
Port/service	<input type="text" value="gstm"/> TCP port number or service name to connect to.
Username	<input type="text" value="dcm105"/> Name used to identify client to server.
Encryption key	<input type="text"/> Pre-shared key used to encrypt communications. Must match server.

Note: The username is the means by which the server refers to this client.

GSTM communication is encrypted using TLS. Each end of any GSTM link needs to be configured with the same pre-shared key. If the server has already been configured, the server administrator will give you a value for the “Encryption Key” field; Otherwise, enter a random string into this field and let the person administering the server know what you have used.

Link settings

Exit delay	<input type="text" value="30"/> Number of seconds to wait on exit before restarting.
Watchdog interval	<input type="text" value="30"/> Number of seconds between sending watchdog probes.
Failover services	<input type="text"/> Services to start when link fails.
Link established command	<input type="text"/> Command to issue when a good link is established.

Generated at 2009-06-23T15:49:43Z by ccs 1.1.5. Portions of output copyright (c)2009, Guralp Systems Limited.

If the GSTM link fails for any reason, it is automatically restarted. There may be situations where the link cannot be restarted so, to prevent almost continuous restart attempts and consequent processor thrashing, a time delay is implemented between a link failure and a restart attempt. This defaults to thirty seconds but a different value can be configured if desired by entering it in the “Exit delay” field.

If a configured link carries no traffic for an extended period, the client will send “watchdog” packets to the server. This serves two functions: it reassures the client that the link is still usable and it defeats any

“automatic disconnect on idle” mechanisms which may be active on some links. The time, in seconds, between such watchdog probes can be configured by entering a value in the “Watchdog interval” field.

If the watchdog packets do not elicit a response from the server, the link is assumed to have failed and, optionally, an additional service can be started in response. This will typically be another GSTM client in order to establish a back-up link. The GSTM client to be started should be identified here by its service descriptor, which takes the form `gstm-client.n` where `n` is an integer: 0 denotes the first configured client instance, 1 the second and so on.

When the GSTM link is established or re-established, it is possible to run an arbitrary command. Any text entered in the “Link established command” field is passed to the Linux shell for execution, so this can be a single command or the path to a shell script to execute multiple commands. Please contact Guralp support if you need assistance with this feature.

The GSTM Server

GSTM clients initiate connections to GSTM servers. To configure a GSTM server on the CMG-EAM, connect to the CMG-EAM configuration system via web or terminal. From the main screen select “Services”, then “Guralp secure TCP multiplexor server”. The next screen shows a list of all GSTM client instances that have been configured on the CMG-EAM.

Guralp secure TCP multiplexor server instance selection

- [Create new service instance](#)

[Home](#) [Help](#) [Expert](#) [Submit](#)

Generated at 2009-06-23T15:55:34Z by ccs 1.1.5. Portions of output copyright (c)2009, Guralp Systems Limited.

This screen lists all currently configured server instances. Click on any server in the list to reconfigure it or, to create a new instance, click on “Create new service instance”.

The following screen appears (shown here in parts):

Guralp secure TCP multiplexor server configuration

User description	<input type="text" value="Guralp secure TCP multiplexor server. Instance 1"/> User label for this GSTM server instance
Enable	<input type="checkbox"/> Enable the GSTM server at system startup
Delete	<input type="checkbox"/> Delete this GSTM server instance

The “User description” field is useful if several instances are to be created. Enter meaningful names here to help distinguish between them.

An instance can be set to start automatically when the CMG-EAM boots by ticking the “Enabled” check-box and deleted entirely by ticking the “Delete” check-box.

Server settings

Bind host	<input type="text"/> The hostname or IP address the server will bind to. Leave empty for all.
Service port	<input type="text" value="1599"/> The TCP port number or service name to listen on.
TCP keepalive	<input type="checkbox"/> Enable sending TCP keepalives (enabling the watchdog is preferred)
Watchdog interval	<input type="text" value="30"/> Period in seconds between watchdog messages

If the CMG-EAM has multiple IP addresses, the GSTM server can be constrained to listen on only one of them by entering its address in the “Bind host” field. If this field is left empty, the server will listen on all available IP addresses.

In the “Service port” field, enter the service name or port number on which you want the server instance to listen. If you are configuring multiple server instances, each needs a unique service/port. The service name to port number mapping is stored in the standard Linux file `/etc/services`, which can be edited from the command line.

The server is capable of generating TCP keep-alive packets in order to defeat any automatic “disconnect on idle” mechanisms which may be present on the link. Tick the “TCP keepalive” check-box to enable this feature.

Like the GSTM client, the GSTM server also generates watchdog packets to monitor for link failure. These may also be more effective at maintaining a link than TCP keep-alives because some network devices automatically block and/or spoof keep-alive packets. Watchdog packets are sent after a certain amount of time when the link appears to be idle and at regular intervals thereafter until traffic is detected. This time interval can be configured by entering an integer value, in seconds, in the “Watchdog interval” field.

Client setting

Client name	Encryption key	Startup command	Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	
<input type="text"/>	<input type="text"/>	<input type="text"/>	
<input type="text"/>	<input type="text"/>	<input type="text"/>	
<input type="text"/>	<input type="text"/>	<input type="text"/>	
<input type="text"/>	<input type="text"/>	<input type="text"/>	

A single GSTM server instance can accept simultaneous connections from multiple clients. For each client, a row in the “Client setting” table needs to be filled in.

The “Client name” column should contain the username, as configured in the GSTM client. The encryption key should match that configured in the client (see the notes in the client configuration section on page 90 for more information).

The GSTM server can run an arbitrary command when a client successfully initiates communication. Any text entered into the “Startup command” column is passed to the Linux shell for execution. The path to a shell script can be entered here if it is required to run multiple commands. Contact Gralp support if you need assistance with this feature.

Port forwards

Listen address	Listen service/port	Target client	Target service/port	Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	

Generated at 2009-07-13T09:04:06Z by ccs 1.1.5. Portions of output copyright (c)2009, Gralp Systems Limited.

An active GSTM link can forward arbitrary TCP connections to the clients from any host that can access the server. The system is very flexible but complex configurations can become confusing. We suggest you adopt the following strategy:

1. Pick a private sub-network, not used elsewhere, to map to the clients. Nominate an address in this subnet to represent each client. For example, if you have seven clients, you could use addresses 10.99.0.1 through to 10.99.0.7 inclusive.
2. Configure all of these addresses as additional IP addresses on the sever. To do this, click on “Interfaces” under “Networking” in the “Configuration” section of the left-hand-side menu in the web interface or, if using the command line, choose “Networking” from the main menu in gconfig. Select the appropriate interface (typically eth0) and, on the resultant page, scroll to the bottom and click the “Expert” button. Scroll down to the “IP aliasing” table and enter all of these addresses in CIDR format, one per line, into the table. CIDR format requires that the number of “network bits” be entered after the IP address, separated by a slash (eg 10.99.0.1/24). Unless you have more than 256 clients, you should use 24 network bits. When the table is full, press the submit button to add extra entries if necessary.
3. Return to the GSTM server configuration page. For each combination of client and service/port that you wish to access, fill in a row of the table:
 - “Listen address” should contain the address of the client on the private subnet that you have just allocated.
 - “Listen service/port” should contain the service name or port number of the service to which you wish to connect. For example, to access a web server at a client, you would enter `http` or `80`.
 - “Target client” should contain the username entered when configuring the GSTM client on the target CMG-EAM.
 - “Target service/port” should contain the same number as the second column: “Listen service/port”.

When the table is full, press the submit button to add extra entries if necessary.

Remote machines wishing to access services on clients via the GSTM server then need only configure a route to the appropriate new address. Default port numbers can then be used in applications such as browsers and Scream!, reducing the amount of configuration required.

Another strategy would use a single address and port-number mapping to achieve the same goals. This is equally effective but requires that remote machines wishing to access services on clients via the GSTM server use non-standard ports for those services. Many people find address mapping with direct port correspondence, as described above, easier to work with.

6.20 Routemaster robust networking

Routemaster is a Güralp-developed system for providing high-availability networking over multiple, redundant communication links. It is useful when a remote site has access to, for example, both a low-cost, high-speed but not entirely reliable network link (such as some DSL links) and also a high-cost, low-speed alternative link (such as via a satellite phone).

Routemaster allows up to three links to be configured per instance, designated the primary, secondary and tertiary links. The primary link is the preferred link and all traffic will be routed over this link for as long as it is available. Should traffic be interrupted on the primary link for any significant time, the secondary link is brought up and used. The primary link is repeatedly tested while the secondary link is in use and, should it become available again, traffic is re-routed via the primary link and the secondary link is dropped. Should both the primary and secondary link be unavailable simultaneously, the tertiary link is brought up and used while both the primary and secondary links are tested. The tertiary link is dropped as soon as either the primary or secondary link becomes available again.

All route-switching is achieved without interrupting the overlying connections.

Routemaster is typically configured on a GSL-EAM at a sensor or array site, to which network coverage may be intermittent, but relies on “test responders” being configured at the other end of the link. The main configuration is described in the next section while that of the test responder is described afterwards.

Configuration

To set up Routemaster on the CMG-EAM, connect to the CMG-EAM configuration system via web or terminal. From the main screen select “Services”, then “RouteMaster robust networking support”. The next screen shows a list of all Routemaster instances that have been configured on the CMG-EAM.

RouteMaster robust networking support daemon

Enable	<input type="checkbox"/>	Enable RouteMaster at system startup
Delete	<input type="checkbox"/>	Delete RouteMaster configuration
Change link command	<input type="text"/>	Command to invoke when switching between alternate links.

Routemaster can be configured to start when the CMG-EAM boots by ticking the “Enable” check-box. The configuration for a particular instance can be deleted entirely by ticking the “Delete” check-box and then clicking on “Submit”.

It is possible to run an arbitrary command or sequence of commands when Routemaster selects a different link to use. Any text entered into the “Change link command” field is passed to the Linux shell for execution. If multiple commands should be run, place them in a shell script and enter the path to the script in this field. If you need assistance with this feature, please contact Gralp support.

The web page contains three identical sets of configuration parameters for each link: the primary (preferred), secondary and tertiary (last resort) links. Only the parameters for the primary link are described here.

Primary link

User identifier	<input type="text" value="Primary link"/>	Will be displayed in status reports to identify the link.
Enable command	<input type="text"/>	Command to enable/start the link operating (if necessary).
Disable command	<input type="text"/>	Command to disable/stop the link operating (if necessary).
Enable delay	<input type="text" value="5"/> s	Delay after issuing the enable command.
Test target IP	<input type="text"/>	IP address or hostname of the test target.

Enter a descriptive name for the link in the “User identifier” field. This name will be used in log files and status messages.

The “Enable command” field should contain a command to enable the primary link. This may be a single command with arguments, such as

```
ip route add 10.1.0.0/24 via 192.168.0.1
```

or a more complicated sequence of commands contained in a shell script, the path to which should be specified. The field should be left blank if no command is required as with, for example, an “always on” link such as DSL.

The disable command functions similarly - it is executed when the link is detected to be broken and would typically contain a command like

```
ip route del 10.1.0.0/24 via 192.168.0.1
```

or the path to a shell script. This field should also be left blank if no command is required.

The “Enable delay” field allows you to specify, in seconds, how long to wait after issuing the Enable command before attempting to send traffic over the link. This can be zero for an “always-on” link but may need to be ten seconds or more for a dial-up connection.

	<input type="text"/>	Delay after issuing the enable command.	
Test target IP	<input type="text"/>	IP address or hostname of the test target.	
Test target service	<input type="text" value="routemaster"/>	Service name or port number for the test target.	
Test period	<input type="text" value="30"/> s	Time between tests when the link is running.	
Host add command	<input type="text"/>	Command to add host route to be used for testing.	
Host delete command	<input type="text"/>	Command to delete the testing host route.	
Destination	Gateway	Metric	Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	
<input type="text"/>	<input type="text"/>	<input type="text"/>	
<input type="text"/>	<input type="text"/>	<input type="text"/>	

Routemaster checks for the availability of routes by sending probe packets to a Routemaster test responder on the remote host. It is a good idea to configure an additional IP address on the remote host for this purpose so that a route can be brought up on a “failed” link purely for testing, without risking re-routing traffic from the back-up link. This additional IP address should be entered in the “Test target IP” field.

The “Test target service” field should be filled with the service name or port number on which the Routemaster test responder is configured on the remote host. If the remote host is only running one responder, this field can be left at its default (the routemaster service is defined as port 1615). If the remote host is running multiple responders and you wish to query one particular one, you should enter a unique service name or number here, which matches the port set in the responder's configuration dialogue.

The “Test period” field controls how often Routemaster checks to see if a link is available. If this value is too long, the response to link failures will be sluggish. If it is too short, you may experience “false alarms” and needless use of the back-up (secondary or tertiary) link.

Routemaster will bring up a dedicated host route when checking for link availability so as not to interfere with existing traffic on another link. The commands to bring up and tear down these host routes should be entered in the “Host add command” and “Host delete command” fields. These will typically be commands like

```
ip route add 10.1.0.1 via 192.168.0.1
```

and

```
ip route del 10.1.0.1 via 192.168.0.1
```

Note the lack of a CIDR number (eg /24) to signify a host route.

Immediately after the link is established, any additional routes configured in the remainder of this dialogue are also brought up. Destination should be either a network address in CIDR format or a host address. Gateway and Metric have their usual meanings.

The Test Responder

The Routemaster Test Responder is used by Routemaster to check whether a particular link is available or not. Routemaster sends probe packets across the link to the responder and listens for its replies.

To set up a Routemaster Test Responder on the CMG-EAM, connect to the CMG-EAM configuration system via web or terminal. From the main screen select “Services”, then “RouteMaster routing test responder”. The next screen shows a list of all Routemaster test responder instances that have been configured on the CMG-EAM.

RouteMaster routing test responder

- [Create default service instance](#)

Home	Help	Expert	Submit
------	------	--------	--------

Generated at 2009-07-13T15:16:11Z by ccs 1.1.5. Portions of output copyright (c)2009, Guralp Systems Limited.

Select the instance that you wish to reconfigure or click on “Create default service instance” to create a new one.

The following screen appears:

RouteMaster network test responder

Enable	<input type="checkbox"/>	Enable RouteMaster responder at system startup				
Delete	<input type="checkbox"/>	Delete RouteMaster responder configuration				
Bind list	<input type="text" value="routemaster"/>	List of interfaces and ports to use. Leave blank for "all".				
<table border="1"> <tr> <td>Home</td> <td>Help</td> <td>Expert</td> <td>Submit</td> </tr> </table>			Home	Help	Expert	Submit
Home	Help	Expert	Submit			

Generated at 2009-07-13T15:17:21Z by ccs 1.1.5. Portions of output copyright (c)2009, Guralp Systems Limited.

The service can be set to start automatically when the CMG-EAM boots by ticking the “Enable” check-box. The configuration of this instance can be deleted entirely by ticking the “Delete” check-box”.

If the “Bind list” field is left blank, the Routemaster Test Responder will respond to probe packets sent to the Routemaster port (1615) on any interface. If it is desired to restrict this, enter a space-separated list of address:port pairs (each with a colon, ':', separating the IP address from the port number).

7 Appendices

7.1 Connector pin-outs

PORTs A, B, C....

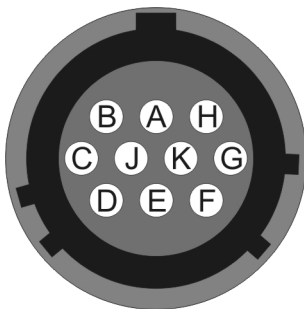
These are standard 10-pin “mil-spec” sockets, conforming to MIL-DTL-26482 (formerly MIL-C-26482). A typical part-number is 02E-12-10S although the initial “02E” varies with manufacturer.

Suitable mating connectors have part-numbers like ***-12-10P and are available from Amphenol, ITT Cannon and other manufacturers.



The pin-out is such that the port can be connected to the serial output of a DM24 digitizer using a straight-through cable.

Pin	Function
A	Power 0 V
B	Power +10 to +35 V
C	RS232 RTS
D	RS232 CTS
E	RS232 DTR
F	RS232 DSR
G	RS232 ground
H	RS232 CD
J	RS232 transmit
K	RS232 receive



Wiring details for the compatible plug, ***-12-10P, as seen from the cable end.

DATA OUT port

This is a standard 10-pin “mil-spec” plug, conforming to MIL-DTL-26482 (formerly MIL-C-26482). A typical part-number is 02E-12-10P although the initial “02E” varies with manufacturer.

Suitable mating connectors have part-numbers like ***-12-10S and are available from Amphenol, ITT Cannon and other manufacturers.



The pin-out is the same as the serial output of a DM24 digitizer, allowing you to insert a CMG-EAM into a pre-existing installation and maintain connectivity.

Pin	Function
A	Power 0 V
B	Power +10 to +35 V
C	RS232 CTS
D	RS232 RTS
E	RS232 DTR
F	RS232 DSR
G	RS232 ground
H	RS232 CD
J	RS232 receive
K	RS232 transmit



Wiring details for the compatible socket, ***-12-10S, as seen from the cable end.

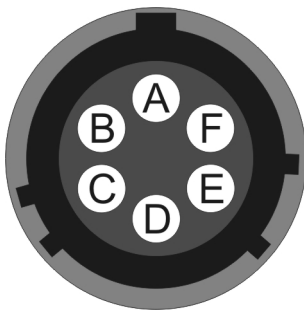
USB connector

This is a standard 6-pin “mil-spec” socket, conforming to MIL-DTL-26482 (formerly MIL-C-26482). A typical part-number is 02E-10-06S although the initial “02E” varies with manufacturer.

Suitable mating connectors have part-numbers like ***-10-06P and are available from Amphenol, ITT Cannon and other manufacturers.



Pin	Function
A	+5 V DC (USB Type A pin 1)
B	Data -ve (USB Type A pin 2)
C	Data +ve (USB Type A pin 3)
D	0 V (USB Type A pin 4)
E	Shielding
F	Switched power +10 to +35 V

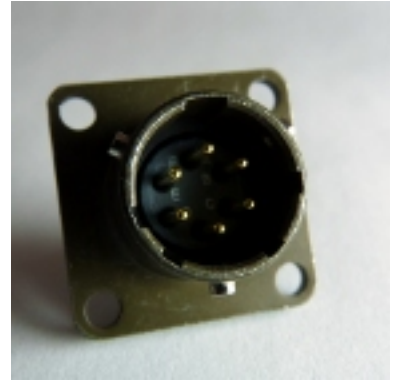


Wiring details for the compatible plug, ***-10-06P, as seen from the cable end.

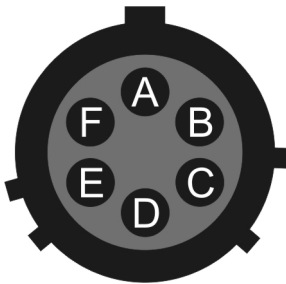
NETWORK connector

This is a standard 6-pin “mil-spec” plug, conforming to MIL-DTL-26482 (formerly MIL-C-26482). A typical part-number is 02E-10-06P although the initial “02E” varies with manufacturer.

Suitable mating connectors have part-numbers like ***-10-06S and are available from Amphenol, ITT Cannon and other manufacturers.



Pin	Function
B	Data transmit +ve (RJ45 pin 1)
C	Data receive +ve (RJ45 pin 3)
E	Data receive -ve (RJ45 pin 6)
F	Data transmit -ve (RJ45 pin 2)



Wiring details for the compatible socket, ***-10-06S, as seen from the cable end.

7.2 Using Minicom

The CMG-EAM includes the Linux program minicom as a terminal emulator for use with serial devices, including Güralp digitisers. The following is part of the minicom man page.

Minicom is window based. To pop up a window with the function you want, press Control-A (from now on, we will use C-A to mean Control-A), and then the function key (a-z or A-Z). By pressing C-A first and then 'z', a help screen comes up with a short summary of all commands.

For every menu the following keys can be used:

- UP arrow-up or 'k'
- DOWN arrow-down or 'j'
- LEFT arrow-left or 'h'
- RIGHT arrow-right or 'l'
- CHOOSE Enter
- CANCEL ESCape.

The screen is divided into two portions: the upper 24 lines are the terminal-emulator screen. In this window, ANSI or VT100 escape sequences are interpreted. If there is a line left at the bottom, a status line is placed there. If this is not possible the status line will be showed every time you press C-A. On terminals that have a special status line, it will be used if the termcap information is complete and the -k flag has been given. Possible commands are listed next, in alphabetical order.

- C-A** Pressing C-A a second time will just send a C-A to the remote system. If you have changed your "escape character" to something other than C-A, this works analogously for that character.
- A** Toggle 'Add Linefeed' on/off. If it is on, a linefeed is added before every carriage return displayed on the screen.
- B** Gives you a scroll back buffer. You can scroll up with u, down with d, a page up with b, a page down with f and, if you have them, the arrow and page up/page down keys can also be used. You can search for text in the buffer with s (case-sensitive) or S (case-insensitive). N will find the next occurrence of the string. C will enter citation mode. A text cursor appears and you specify the start line by hitting Enter key. Then scroll back mode will finish and the contents with prefix '>' will be sent.
- C** Clears the screen.
- E** Toggle local echo on and off.

- F** A break signal is sent.
- I** Toggle the type of escape sequence that the cursor keys send between normal and applications mode. (See also the comment about the status line below).
- J** Jump to a shell. On return, the whole screen will be redrawn.
- K** Clears the screen, runs kermit and redraws the screen upon return.
- L** Turn Capture file on off. If turned on, all output sent to the screen will be captured in the file too.
- O** Configure minicom. Puts you in the configuration menu.
- P** Communication Parameters. Allows you to change the bps rate, parity and number of bits.
- Q** Exit minicom without resetting the modem. If macros changed and were not saved, you will have a chance to do so.
- R** Receive files. Choose from various protocols (external). If you have the filename selection window and the prompt for download directory enabled, you'll get a selection window for choosing the directory for downloading. Otherwise the download directory defined in the Filenames and paths menu will be used.
- S** Send files. Choose the protocol like you do with the receive command. If you don't have the filename selection window enabled (in the File transfer protocols menu), you'll just have to write the filename(s) in a dialog window. If you have the selection window enabled, a window will pop up showing the filenames in your upload directory. You can tag and untag filenames by pressing spacebar, and move the cursor up and down with the cursor keys or j/k. The selected filenames are shown highlighted. Directory names are shown [within brackets] and you can move up or down in the directory tree by pressing the spacebar twice. Finally, send the files by pressing ENTER or quit by pressing ESC.
- T** Choose Terminal emulation: Ansi(color) or vt100. You can also change the backspace key here, turn the status line on or off, and define delay (in milliseconds) after each newline if you need that.
- W** Toggle line-wrap on/off.
- X** Exit minicom, reset modem. If macros changed and were not saved, you will have a chance to do so.
- Y** Paste a file. Reads a file and sends its contents just as if it would be typed in.
- Z** Pop up the help screen.

8 Revision history

2008-03-16	A	New document
2009-06-16	-B	Major re-write for GDI. First official release.