...the broadest narrowband money can buy

RACOM
RADIO DATA NETWORKS

Operating manual

MServer

MServer version 3.0.5

document version 1.0.6
1/29/2010

RACOM s.r.o. • Mirova 1283 • 592 31 Nove Mesto na Morave • Czech Republic
Tel.: +420 565 6595 11 • Fax: +420 565 6595 12 • E-mail: racom@racom.cz

www.racom.eu

Table of Contents

1. Short Introduction 5
    1.1. Installation 5
    1.2. Maintenance Requirements 9
    1.3. Security Requirements 9
    1.4. Passwords 9
2. How it Works 10
    2.1. Radio Network 10
    2.2. Client–Server Model 10
3. Basic Maintenance 12
    3.1. IP Address Setup 12
    3.2. To become a Superuser 13
    3.3. Secure Access 14
    3.4. NTP Server Setup 14
4. MServer diagnostic pages 15
    4.1. UPS 15
    4.2. Server Management 15
    4.3. Daemons 15
    4.4. System 16
    4.5. Configuration 19
    4.6. Diagnostics 21
5. Hardware Options 23
    5.1. Dual Screen 23
    5.2. Computer Case 23
    5.3. Cluster 23
    5.4. Software RAID 24
6. MServer Mapping Data 25
7. Remote Access And Alarm System 26
    7.1. Remote Access Graphical Tools 26
    7.2. Remote Access Command Line Tools 26
    7.3. Remote Troubleshooting 27
    7.4. How to Set-up SSH Keys 28
8. Ranec introduction 29
9. Conditions for MServer Operation 34
    9.1. Important Warning 34
    9.2. Conditions of Liability for Defects and Instructions for Safe Operation of Equipment 34

List of Figures

2.1. Client-server model. 11
3.1. MServer principle. 12
4.1. UPS Status 15
5.1. Cluster principle. 23
7.1. Remote access to MServer – example. 26
8.1. Topology with radio modem on-line status information 29
8.2. Average response 30
8.3. Temperature inside the radio modem 30
8.4. Ethernet port traffic load 30
8.5. Signal coverage – base stations coverage analysis 31
8.6. Signal coverage – signal strength analysis 31
8.7. Signal coverage – signal strength analysis (detail view) 31

8.8. Calculated coverage 32
8.9. Line of sight 33

1. Short Introduction

MServer is a solution for supervising Racom's radio network. It is able to visualize traffic load statistics, radio frequency channel noise analysis, network alarms (and more) from the network – for each radio modem, or for each (virtual) link.

The server is based on an open source solution. It is shipped as a Linux computer with pre–installed and tested software.

MServer is supposed to be a secure and robust solution. The data consistency can be guaranteed only if the server is used according with this manual.

1.1. Installation

1.1.1. Installation steps of the CentOS

Notes:

'+' stands for 'checked' item
'-' stands for 'unchecked' item
<text> stands for button labeled with 'text' that should be pressed

Installation steps:

- Insert bootable DVD
- Run Graphical installation <ENTER>
- Media check – Skip

Graphical installation:

- Welcome screen – <Next>
- Language – English
- Keyboard – U.S. English
- Partitions:
  - Create custom layout – <Next>
    1x: ext3, mount as '/', size 10000 MB
    1x: swap (size 2xRAM size e.g. 4000 MB)
    1x: ext3, mount as 'spareux', size 10000 MB
    1x: ext3, mount as 'data_mysql', size 40000 MB
    1x: ext3, mount as 'data', size – rest of disk space (95409 MB)
    Confirm formatting of the selected partitions. – <Format>
    - In the case of using Software RAID create partitions this way:
      1. On the Disk Partitioning Setup screen, select Manually partition with Disk Druid.
      2. In Disk Druid, choose New to create a new partition.
      3. You will not be able to enter a mount point (you will be able to do that once you have created your RAID device).
      4. Choose software RAID from the File System Type pulldown menu.
      5. For Allowable Drives, select the drive(s) on which RAID will be created. If you have multiple drives, all drives will be selected here and you must deselect those drives which will not have the RAID array on them.
      6. Enter the size that you want the partition to be.

7. Select Fixed size to make the partition the specified size, select Fill all space up to (MB) and enter a size in MBs to give range for the partition size, or select Fill to maximum allowable size to make it grow to fill all available space on the hard disk. If you make more than one partition growable, they will share the available free space on the disk.
8. Select Force to be a primary partition if you want the partition to be a primary partition.
9. Click OK to return to the main screen.

- Repeat these steps to create as many partitions as needed for your RAID setup. Notice that all the partitions do not have to be RAID partitions. For example, you can configure only the /home partition as a software RAID device.
- Once you have all of your partitions created as software RAID partitions, follow these steps:
  1. Select the RAID button on the Disk Druid main partitioning screen.
  2. The 'Make RAID Device' screen appear – here you can make a RAID device.
  3. Enter a mount point.
  4. Choose the file system type for the partition.
  5. Select a device name such as md0 for the RAID device.
  6. Choose your RAID 1 level.
  7. The RAID partitions you have just created appears in the RAID Members list. Select which ones of them should be used to create the RAID device.

     Mount every system mount point (eg. '/', '/data', 'swap', ...) to RAID device.

- OS Loader (keep default settings – Install GRUB boot loader on partition labelled CentOS). – <Next>
- Network devices – eth0 marked as Active on Boot, DHCP
- Time zone
- Root password (e.g. centos)
- Choose software components
  - Desktop-Gnome
  - Desktop-KDE
  - Server
  - Server-GUI

  - Check 'Customize now'
    <Next>
- Customize now:
  - Desktop Environments
    KDE (K Desktop Environment)
    + kdeadmin
  - Applications
    - Games and Entertainment
    Sound and video
    + k3b
  - Servers
    + MySQL Database
  - Base system
    + System tools
    + mc
    <Next>
- Begin of installation – <Next>
- remove installation medium, <Reboot>

- Settings after the first boot
- Firewall
  default settings plus:
  - SSH

    - WWW (HTTP)
    - Secure WWW (HTTPS)
    - enable MySQL i.e: port 3306, TCP
    - enable Dell server management i.e: port 1311, TCP
      <Forward>
- SELinux
  Disabled
  <Forward>
- Kdump
  default settings
  Disabled
  <Forward>
- Date
  Disable Network Time Protocol
  It is possible (and it is preferred option) to enable Network Time Protocol if there is some time server reachable from the server.
  <Forward>
- Create User
    - Username: demo, demo, demo12
      <Forward>
- Sound Card
    - default settings
      <Forward>
- Additional CDs
  <Finish>

1.1.2. MServer installation steps

Installation notes:

If the target server HW is not DELL, please skip item no 1.b/ and 9/. In this case do not forget to set BIOS to automatically start the computer after the power failure.
Configure the `/root/rr_inst/rr_inst.conf` file to:
USE_DELL=0

Installation process:

1. a. Copy installation CD to /
   The files `CENTOS_INSTALL.txt, RHEL_INSTALL.txt` and `INSTALLATION.txt` are not necessary to be copied to the harddisk.
   b. Copy Dell server management installation DVD to `/data/install/`
   It is enough to copy the SYSMGMT directory.
2. - Configure the `/root/rr_inst/rr_inst.conf` – installation configuration file. Choose your install options.
   - Configure the network connection (set static IP address – STATIC IP ADDRESS IS REQUIRED!). Test the connection to the internet – the internet connection is an option. If you do not have an internet connection the '`USE_DVD=1`' option in the `rr_inst.conf` configuration file is mandatory.
   - Open the terminal, log on as root (ATTENTION: use '`su -`' to load all root settings) and run the first installation script:
     `sh /root/rr_inst/rr_inst_first.sh`
   - After finishing this step, server reboots itself.

3. Run 'system to Morse' configuration script to prefill IP settings in the configuration files. When the active Ethernet interface is not 'eth0', fill in the proper value in '/etc/rr_MServer_id' file first.
   rr_ip_s2m.sh
   - Configure parameters in the following files:
     - /etc/morse/morse.conf
     - /etc/morse/morse_p.conf
     - /etc/rr_MServer_id
     - /etc/rr_evlog_mail.cnf
   - Finally run:
     rr_ip_m2s.sh
4. Insert installation DVD. Do not connect any other removable media at this time.

   Note: This step can be omitted if you want to install packages from internet. In this case edit the /root/rr_inst/rr_inst.conf file to:
   USE_DVD=0
5. - Open the terminal, log on as root (ATTENTION: use 'su –' to load all root settings) and run the second installation script:
     sh /root/rr_inst/rr_inst_second.sh
   - In the case of using Software RAID, the configuration of the RAID devices is necessary: fill in the 'ARRAY' configuration line for every raid partition in the file:
     /etc/mdadm.conf
6. - Format Ranec database:
     a. Run Ranec client and log in as user 'admin', password 'admin!!!'
     b. Menu 'Setup – Database – Debug – Tablespace setup'
        Enter unique ID of the server (Please request this ID from your MServer supplier).
7. - Configure remote desktop access – this is an option, it is not mandatory. Those configuration changes makes it possible to manage the server remotely via full graphical user interface.
   - System – Preferences – Remote Desktop
     - + Allow other users to view your desktop
     - + Allow other users to control your desktop
     - - Ask you for confirmation (This option can be set to TRUE for remote assistance. It is necessary to set it to FALSE for remote access (remote control of the server)).
     - + Require the user to enter this password /By default – enter the same password as the demo user has got. You can enter any other password, anyway.
   - System–Administration–Login screen
     - Users
       Include all users from /etc/passwd (not for NIS)
     - Security
       + Enable Automatic Login
       select 'demo' user
   - Configure the VNC server password:
     - On the terminal (logged on as demo user) perform command:
       vncpasswd
       and enter the VNC password.
8. Reboot the server
9. - Configure the DELL Server Management.
   - Run the web browser and enter following address:
     https://localhost:1311 ... and log in as root
     - – System / Alert Management / Physical Disk Warning / Execute application –> fill in '/usr/bin/rr_sysalert_pdiskwarn'
     - – System / Alert Management / Physical Disk Failure / Execute application –> fill in '/usr/bin/rr_sysalert_pdiskfail'

- – System / Main System Chasis / BIOS / Setup / AC Power Recovery Mode –> On

1.2. Maintenance Requirements

Remote access

When you need to access the server remotely, you are allowed to access the server remotely (for maintenance) only through SSH protocol via RSA or DSA keys. This is important from the point of view of server security, mainly when the MServer is accessible from the public Internet.

Power supply and UPS

The server has to be powered by a UPS which guarantees the server will shut down automatically. This UPS should be shipped from Racom, because it is important, that all shutdown states are tested.

You may also run the server on some independent non-interruptible power source, which is allowed to be interrupted only after manual shut-down of the server.

The server has to be always shut down correctly:

a. Click System -> Shut Down...

b. Open the Linux console, log in as root user, run the command: **shutdown -h now**

If you turn off the server incorrectly, generally any file can be damaged, although the system is carefully tested to be resistant to such power failures. Racom can not guarantee data consistency if you run MServer without a UPS.

1.3. Security Requirements

When you need to access MServer from the Internet we recommend following these rules:

- Use an external firewall. MServer is not designed to be secure against attacks from the Internet, although MServer does run quite a strong firewall itself.
- For maintenance use encrypted access through public key authentication (use SSH protocol and RSA or DSA keys).
- In an external firewall please enable only secure services (SSH and OpenVPN). Racom can help you to operate secure access through an SSH protocol or OpenVPN protocol.

1.4. Passwords

For maintenance Racom uses "srlo" (i.e. "ssh root@localhost") functionality. The superuser's (root's) password should not be used for common access. Don't forget to change the root's password with respect to security issues. It should be used only for local access to the machine, if some failure has to be corrected. Any other remote maintenance access should be done through demo (using public keys) and then through "srlo" feature.

Srlo access have to be allowed by script `rr_srlo_alow`. Script for disabling is `rr_srlo_deny`.

MySQL access is controlled in a similar way. The administrator's password should not be used for common access. In this case use a user's account.

2. How it Works

2.1. Radio Network

The heart of the MServer is an alarm daemon. It collects alarm information from each radio modem with the respect to the low bandwidth of the radio network. Client software Ranec then shows the status of each radio modem:

- green colour — "operating"
- red colour — "not accessable"
- blue colour — "on battery"
- white colour — "unknown"
- magenta colour — "wrong configuration of the alarm daemon"

The alarm daemon dynamically reflects the status of the network. It dynamically computes time-out for changing the state from "operating" or "on battery" to "not accessable". This time-out varies from 10 seconds to 20 minutes, according to the character of the network.

MServer is optimized for "soft start". MServer will not overload the network even when it is connected to the network with (yet) unknown characteristic.

To save the bandwidth of the radio network alarm daemon can use monitoring of some (e.g. central) interface within the Morse network. If the alarm daemon can see any packet coming from a given radio modem (i.e. via monitoring), it implies that the radio modem is not in the "not accessable" state.

If the network is going to be out of order MServer uses a fast mechanism to reduce the network traffic to give the customer's data the highest priority.

Status change to "on battery" and back to "operating" is transferred from each radio modem to MServer's alarm daemon spontaneously – this results in low delays and low bandwidth consumption.

MServer will inform you about any internal problem so that you can trust the green symbols on the screen to show the real state of the network. MServer's client will show you a "white" colour if there is any internal problem.

2.2. Client–Server Model

MServer is based on a client-server model. MServer holds data in an MySQL database – basically network topology data and statistical logs. MServer can run a graphical client – Ranec. Ranec client connects itself into MServer's MySQL database, reads the data repeatedly, and shows it on screen.

A number of clients can be connected to MServer via a local area network. If necessary you can connect yourself remotely.

Ranec client is available for MS Windows XP or Linux.

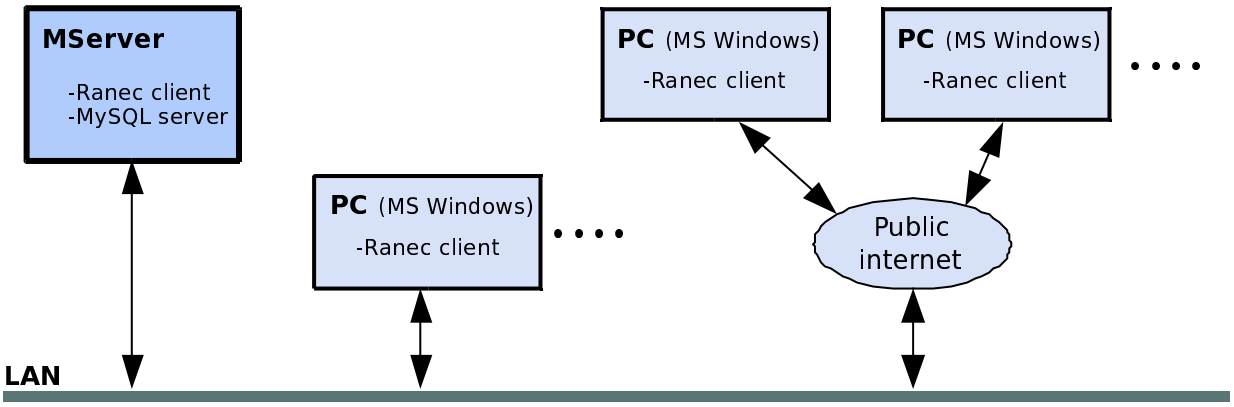


Fig. 2.1: Client-server model.

3. Basic Maintenance

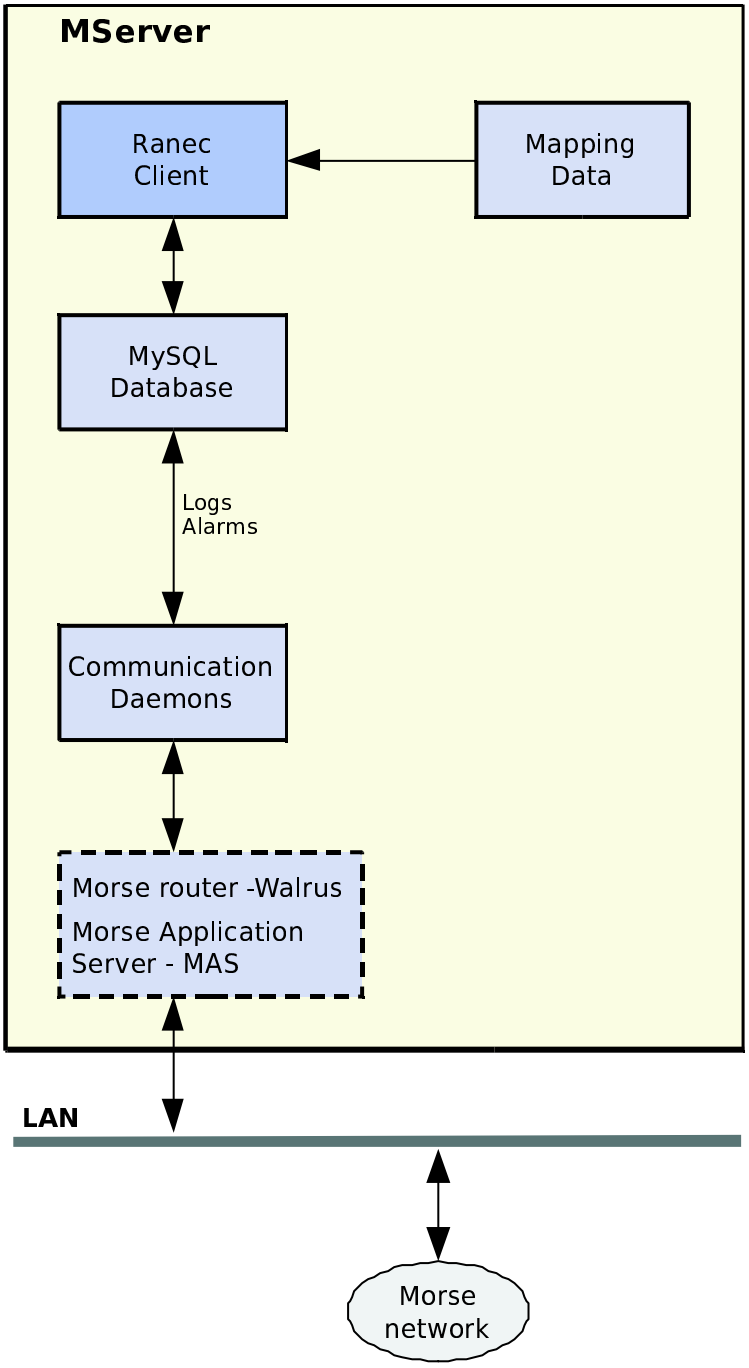


Fig. 3.1: MServer principle.

3.1. IP Address Setup

This is how to change an IP address (and more) of the MServer. For easy setup you can use factory defaults:

- Configuration file:
  Become a superuser (see below) and edit file "`/etc/rr_MServer_id`". Name of the server, IP address, mask, gateway, net device and domain of the server can be setup.

- LAN:
  Become a superuser (see below) and run script "`rr_ip_m2s.sh`". This script will reconfigure net device in accordance with file "`/etc/rr_MServer_id`" and restart it.
- Morse network access:
  Most of the Morse network access parameters are configured in "`/etc/morse/morse.conf`" file (IP address of the Morse Application Server – MAS, database access for the communication daemons, IP address of the walrus).

  The script "`rr_ip_m2s.sh`" sets all items mentioned above to IP address configured in file "`/etc/rr_MServer_id`". Walrus is restarted to changes take effect. This setting fit for the case walrus and database run on the local MServer and MAS is configured inside local walrus. Walrus, MAS and database do not have to run on the one MServer generally. In that case file "`/etc/morse/morse.conf`" has to be configured additionally:
  a. In case you use the internal walrus (eventually you also want to configure MAS in the walrus) – use script "`rr_setr`" and set up Morse routing of walrus. (Please go to menu "EPe", write the configuration and restart walrus from menu "`sgB`" prior to next steps.)
  b. In case you will use MAS in the connected radio modem – become a superuser, edit file "`/etc/morse/morse.conf`" and fill in the IP address of the radio modem into item `RR_MAS_HOST`.
  c. If you don't want to use database on this MServer, edit file "`/etc/morse/morse.conf`" and fill in the IP address of the remote database server into item `RR_DB_HOST`.

  For both cases refer to Morse documentation, how to plan Morse address space, how to set up MAS and Morse routing.

  It is recommended using of the walrus (and MAS) on the MServer.
- DNS (for e-mails):
  Become a superuser and run script "`rr_ip_m2s.sh`". This script will reconfigure DNS server (according to configuration file "`/etc/rr_MServer_id`") and restart it.

Passwords

MServer is shipped with pre-configured user "demo" and password "demo12"; superuser's password is pre-set to "centos". Both passwords should be changed from the command line using command "`passwd`".

3.2. To become a Superuser

After booting up the computer will start the graphical window manager and log in as user "demo" automatically. You can become a superuser (get superuser's shell) in many ways:

- In the menu Applications–>Accessories–>Terminal (i.e. Command line or shell) and start it, or press **Alt-F2** and find Terminal.
  - Then, from this terminal use command `su`, which will ask you for password.
  - Alternatively, if you are a privileged user, use command `srlo`, which will ask you for passphrase. This command enables a couple of users to become a superuser and not to know the root's password.
- Press left **Ctrl** +left **Alt +F1**, login as a superuser and write the password. This can be useful if the graphical environment fails. (**Alt+F7** for going back)
- From a remote machine use an ssh or putty application.

Passwords

MServer is shipped with pre-configured user “demo” and password “demo12”; superuser's password is pre-set to “centos”. Both passwords should be changed from the command line using command “`passwd`”.

3.3. Secure Access

MServer is a very secure machine prepared to be connected to the Internet and accessed remotely from Racom. There are two basic concepts:

- Via SSH keys (you have static IP address):
  To enable secure access please become a superuser and edit file “`/etc/ssh/sshd_conf`” and change item `Password Authentication` to “no”. Then you will have to use rsa or dsa keys to access MServer remotely, which brings the security. You do not need to do this as Racom employees can do everything remotely so just allow them to connect.
- Via OpenVPN client and dynamic IP address (dial-up ISP provider):
  OpenVPN client is preconfigured to be connected with Racom.

3.4. NTP Server Setup

Here we will go through setup of daemon, which synchronizes the time of MServer from the Internet via Network Time Protocol – NTP daemon, or ntpd. Basically you have to set up the time source and add NTP daemon to boot-up scripts.

- First become a superuser and edit file `/etc/ntp/ntpservers`. Find and change line:
  ```
  0.centos.pool.ntp.org
  1.centos.pool.ntp.org
  2.centos.pool.ntp.org
  ```
  Ask your Internet Service Provider for best (nearest) NTP server and add it there.
  Check if your time server is accessible:

  ```
  /etc/init.d/ntpd stop
  ntpdate server_name_or_ip_address
  ```

  Note: while running command ntpdate, ntpd must be stopped.
- Then (as a superuser) run two commands:

  ```
  chkconfig ntpd on
  /etc/init.d/ntpd restart
  ```

  The first will add ntpd to boot scripts, and the second will start ntpd immediately, so you do not have to restart the computer.

  Please note that ntpd will start to operate after 10–20 minutes because first it needs to measure time difference precisely. Refer to ntpd documentation.

  After this works, you can set up the Morse network to get the time from MServer. Refer to Morse documentation – menu "EPe".

4. MServer diagnostic pages

These pages provide you with a set of tools for diagnostics and maintenance of the MServer.

There is possible to start these pages using desktop icon "MServer diagnostic" or used web browser on some PC in the same LAN. As HTTP address use IP address of MServer.

4.1. UPS

On UPS diagnostic pages is possible to see status of UPS. UPS have to be connected using USB port to the MServer. MServer was tested with APC UPS equipment.

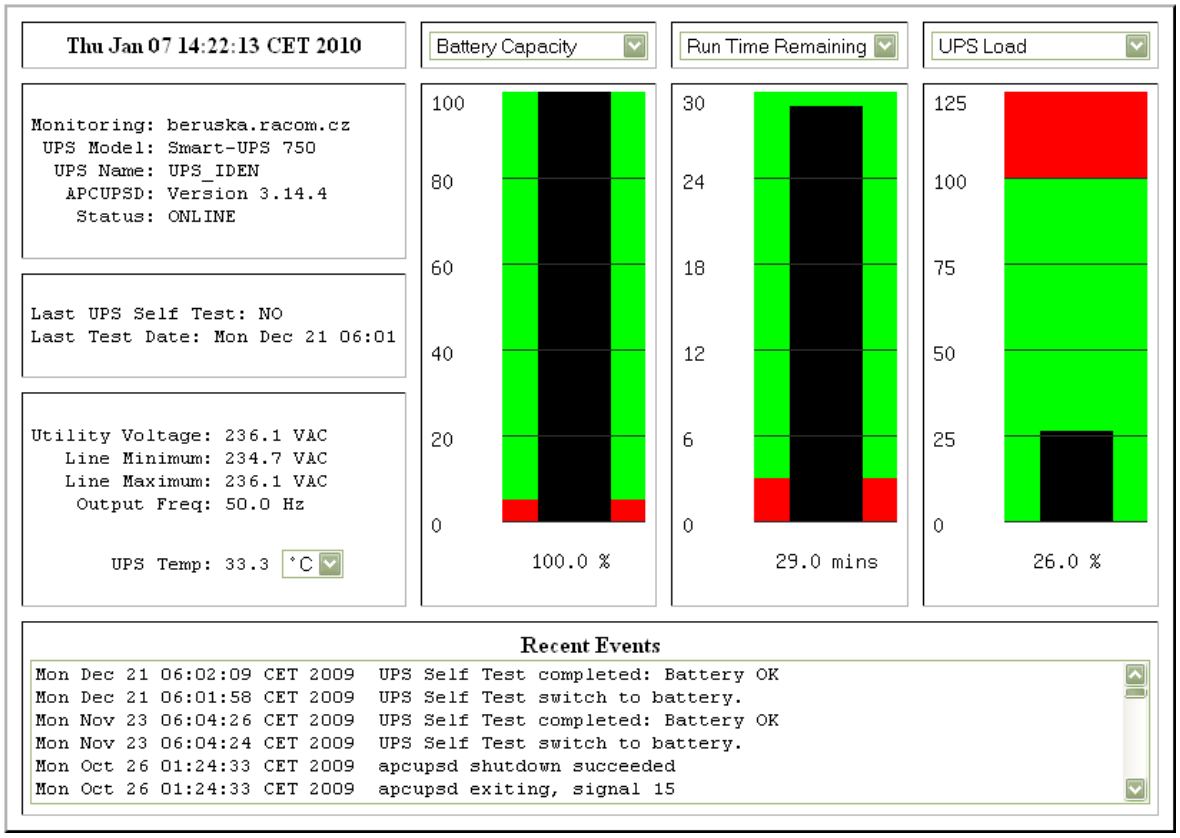


Fig. 4.1: UPS Status

4.2. Server Management

Working only on Dell MServers. These pages are provided by Dell. There is possible to see or change many settings of MServer.

4.3. Daemons

Morse daemons are applications running on background. They are responsible for uploading Morse network status to the MySQL database. The Ranec client is used to display acquired data. The daemons are configured via Ranec client.

First, there are Morse daemons:

- **CtId daemon** is responsible for starting and stopping Alarm, GPS and Stlog daemons according to Ranec configuration.
- **Alarm daemon** is responsible for getting information about health of the communication status with configured nodes.
- **GPS daemon** is receiving GPS data from the network.
- **Stlog daemons** are uploading statistic logs from the configured nodes.
- **Walrus daemon** is Morse router based on unix socket.

Another daemons, according to actual system configuration:

- **NTP-rescue daemon** is responsible for supervision of the NTP protocol. It is enabled only if the NTP protocol is enabled via system configuration (System –> Administration –> Date & Time menu. When changed, systems restart is required.).

4.3.1. Example – Actual status of the configured daemons

Network	Daemon	Status
	ctld	up (pid 24627) 23 seconds
	mysql-rescue	up (pid 28905) 30740 seconds
	ntp-rescue	up (pid 24633) 17 seconds
	rrmtun	up (pid 4673) 6338160 seconds
	rrping-test	up (pid 24601) 65 seconds
	rrswitch-test	up (pid 22549) 648 seconds
	testgps	down 6338160 seconds
	walrus	up (pid 4676) 6338160 seconds

4.3.2. Daemon activity logs

Please select daemon activity log you want to display.

Network	Daemon	Current	last 100	last 10k	last 100k
	ctld	display	display	display	display
	mysql-rescue	display	display	display	display
	ntp-rescue	display	display	display	display
	walrus	display	display	display	display

4.4. System

System logs are logging system activity.

- **Event log** contains system important events. Those events are sent by e-mail as well.
- **Info log** contains only informative messages.

MySQL backup reports contains activity of the MySQL backup system.

MySQL available backups contains list of available backups of the MySQL data.

Disk usage menu gives brief information about whole system disk usage.

4.4.1. System logs

Log	last 100	last 10k	last 100k
Event log	display	display	display
Info log	display	display	display

4.4.2. System backup

The system is backed up to several directories

- `/data/backup/system` – actual copy of the Linux system.
- `/data/backup/data` – actual copy of the /data partition, i.e.: home directories, system logs, user data. The /data/not_backuped directory is not backuped.
- `/data/backup/mysql-zrm` – short history of the MySQL data backups (see MySQL backup reports and MySQL available backups menu).
- `/data/backup/_tgz` – .tgz files created by running the **sh /usr/bin/rr_back_tgz.sh** command (root privileges are necessary to run this command). This command creates a .tgz archive from the actual backup snapshots (`'/data/backup/system' and '/data/backup/data'` directories)

```
Example - Backup directory sizes:

56K     /data/backup/mysql-zrm
14G     /data/backup/data
8.3G    /data/backup/system
22G     /data/backup/
```

4.4.3. Example – MySQL backup reports

Report type	Report
dailyrun	2010-01-07 01:00:06
dailyrun	2010-01-06 01:00:05
dailyrun	2010-01-05 01:00:06
weeklyrun	2010-01-04 01:00:05
dailyrun	2010-01-03 01:00:09
dailyrun	2010-01-02 01:00:09
monthlyrun	2010-01-01 01:00:05

4.4.4. Example – MySQL available backups

Here is the list of the available backups

```
REPORT TYPE : restore-info

backup_set  backup_date          backup_level  backup_directory                    ▶
 backup_status comment
-------------------------------------------------------------------------------------------------------
dailyrun Thu Jan  7 01:00:02 2010         0 /var/lib/mysql-zrm/dailyrun/20100107010002  ▶
Backup success ----
dailyrun Wed Jan  6 01:00:02 2010         0 /var/lib/mysql-zrm/dailyrun/20100106010002  ▶
Backup success ----
dailyrun Tue Jan  5 01:00:02 2010         0 /var/lib/mysql-zrm/dailyrun/20100105010002  ▶
Backup success ----
dailyrun Sun Jan  3 01:00:03 2010         0 /var/lib/mysql-zrm/dailyrun/20100103010003  ▶
Backup success ----
dailyrun Sat Jan  2 01:00:04 2010         0 /var/lib/mysql-zrm/dailyrun/20100102010004  ▶
Backup success ----
dailyrun Thu Dec 31 01:00:04 2009         0 /var/lib/mysql-zrm/dailyrun/20091231010004  ▶
Backup success
```

How to make MySQL backup right now:

1. Open the Linux console and login as root user
2. Run the backup command:
   sh rr_back_db.sh

How to recover MySQL data from an existing backup:

1. Open the Linux console and login as root user
2. Stop all daemons accessing the database:
   svc -d /service/ctld/ /service/rr_morse_*
   All applications using the database that is being restored must be stopped.
3. Run the recover command with the selected backup from the list above (backup_directory column).
   mysql-zrm --action restore --backup-set dailyrun --source-directory selected_directory
   It is possible to restore only some tablespaces selectively:
   mysql-zrm --action restore --backup-set dailyrun --source-directory selected_directory --databases "db1 db2"
4. Run the database integrity check script, phase 1:
   myisamchk -ser /var/lib/mysql/*/*.MYI
5. Start the MySQL server:
   /etc/init.d/mysqld start
6. Run the database integrity check script, phase 2:
   mysqlcheck --all-databases -ser
7. Start the daemons again:
   svc -u /service/ctld/

4.4.5. Disk status

Example – Disk usage

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/md0              9.5G  8.2G  799M  92% /
/dev/md3              112G   92G   15G  87% /data
```

```
/dev/md4               15G  962M   13G   7% /data_mysql
/dev/sdb7             303G  128G  160G  45% /data_nonraid
/dev/md1              9.5G  151M  8.9G   2% /spareux
tmpfs                1014M     0 1014M   0% /dev/shm
```

Check the individual mount points ("Mounted on") for sufficient disk space, from time to time.

- The "**/**" partition contain the linux system.
- The "**/data**" partition contain the home directories, system logs and backups.
- The "**/data_mysql**" partition contain the MySQL data.

Software RAID status

```
Personalities : [raid1]
md1 : active raid1 sdb2[1] sda2[0]
      10241344 blocks [2/2] [UU]

md2 : active raid1 sdb3[1] sda3[0]
      4096448 blocks [2/2] [UU]

md3 : active raid1 sdb5[1] sda5[0]
      120897024 blocks [2/2] [UU]

md4 : active raid1 sdb6[1] sda6[0]
      15358016 blocks [2/2] [UU]

md0 : active raid1 sdb1[1] sda1[0]
      10241280 blocks [2/2] [UU]

unused devices:
```

4.5. Configuration

Custom configuration of the MServer is stored in the configuration files:
The most important files:

- `/etc/morse/morse.conf` file stores the Morse daemons specific data (IP addresses of the MAS host and database host, database login informations ...).
- `/etc/rr_MServer_id` file stores the server specific data (serial number, IP settings of the Ethernet card ...).

Remote access to the MServer

The remote access to the MServer is possible via ordinary SSH connection (`ssh` command from the Linux or `putty.exe` tool from the Windows). The firewall is open by default for the SSH, HTTP and HTTPS connection (HTTP connection is necessary to view diagnostic pages remotely and HTTPS connection is necessary to view Dell server administration remotely).

It is possible to view and control entire desktop remotely. If you want to enable this feature, please run the following command (as user root from the command prompt):

- **rr_vnc_enable.sh** ... to enable remote access to GNOME desktop, or

- **rr_vnc_disable.sh** ... to disable remote access

4.5.1. Morse.conf

The `'/etc/morse/morse.conf'` configuration file contain configuration of the Morse utilities (Morse utils, daemons, walrus...) environment.

Example:

```
Morse base address of the Morse Application Server as configured
in the MAS parameters of the MAS host. 0x000000FF mask is supposed.  69AAE1FE
IP address of the MAS host                                          192.168.1.2
IP address of the Walrus host                                       192.168.1.2
Database login name used by Morse daemons                           morse
Database tablespace used by Morse daemons                           morse
IP address of the MySQL database server                             192.168.1.2
Morse daemons e-mail destination address                            demo@server.racom.cz
Morse daemons e-mail source address                                 alrm@server.racom.cz
MySQL database backup user                                          mysqlbackup
```

The `morse.conf` configuration file can be modified by running following scripts. The scripts must be executed by power user ('maintain').

- **sudo rr_config_u2c.sh** – Modify the file by answering the questions.
- **sudo rr_ip_s2m.sh** – Modify the file according to system IP settings.
- **sudo rr_ip_u2m.sh** – Modify the file by answering the questions (IP settings only).

4.5.2. MServer

The `'/etc/rr_MServer_id'` configuration file contains basic information about this specific MServer.

Example:

```
MServer version                         3.0.5
MServer serial number                   xxxxxx
MServer database unique number          2
MServer name                            server.racom.cz
MServer primary ethernet device         eth0
IP address of this device               192.168.1.2
IP Mask ...                             255.255.255.0
IP gateway ...                          192.168.131.256
MServer domain                          racom.cz
MServer serial port device name
MServer serial port device number       1
```

The `'/etc/rr_MServer_id'` configuration file can be modified by running following scripts. The scripts must be executed by power user ('maintain').

- **sudo rr_ip_u2m.sh** – Modify the file by answering the questions.
- **sudo rr_ip_s2m.sh** – Modify the file according to system IP settings.
- **sudo rr_ip_m2s.sh** – This script does not modify the `rr_MServer_id` file. It is used to apply changes, made to this file directly (e.g. by text editor).

4.5.3. Log mail

The '/etc/rr_evlog_mail.cnf' configuration file contains configuration of the e-mails being sent from the server in case of a new event comming to the Event log (file '/var/log/rrsys/rrevlog').

```
Event log emails recipients             root@server.racom.cz, it@racom.eu
MServer name in ev.log emails subject   MSERVER_xxxxxx
Event log emails sender                 mserver
```

The '/etc/rr_evlog_mail.cnf' configuration file can be modified by power user ('maintain').

4.5.4. MySQL backup configuration

The configuration files are stored in '/etc/mysql-zrm' directory and 'dailyrun', 'weeklyrun' and 'monthlyrun' subdirectories. The 'mysql-zrm.conf' configuration file exist for each type of backup (daily, weekly and monthly).

```
daily backups      retention-policy="8D"
weekly backups     retention-policy="5W"
monthly backups    retention-policy="3M"
```

4.5.5. Setrdial configuration

It is taken from '/etc/morse/dialer.cnf' and from the '/etc/rr_MServer_id' configuration files. The '/etc/rr_MServer_id' values (serial port where telephone modem is connected) are taken with higher priority.

```
MServer serial port device number   1
Serial port idle [ms]               20
```

List of pre-configured destinations (as filled in '/etc/morse/dialer.cnf' configuration file).

Destination name	Telephone number
test	577
test2	548

The '/etc/morse/dialer.cnf' configuration file can be modified by power user ('maintain').

The connection command is executed as:
rr_setrdial destination_name

4.6. Diagnostics

There are a few basic diagnostic tools to test MServer configuration and connection to the network.

4.6.1. Database connection

If the configuration of the database connection parameters is OK and the MySQL server is running, you should see the basic information about MySQL server status. Otherwise you will see some error message or no output:

```
--------------
mysql  Ver 14.12 Distrib 5.0.45, for redhat-linux-gnu (i686) using readline 5.0
```

```
Connection id:          39406
Current database:       morse
Current user:           morse@mserver
SSL:                    Not in use
Current pager:          stdout
Using outfile:          ''
Using delimiter:        ;
Server version:         5.0.45 Source distribution
Protocol version:       10
Connection:             192.168.131.178 via TCP/IP
Server characterset:    latin1
Db     characterset:    latin1
Client characterset:    latin1
Conn.  characterset:    latin1
TCP port:               3306
Uptime:                 28 days 2 hours 50 min 47 sec

Threads: 1  Questions: 3550359  Slow queries: 0  Opens: 371082  Flush tables: 1  Open ▶
tables: 64  Queries per second avg: 1.461
--------------
```

It is possible to get another information about database by executing following scripts. Ordinary user privileges are sufficient to execute the scripts:

- **sudo rr_test_db.sh S** – print longer status information.
- **sudo rr_test_db.sh p** – print actual connections for 'morse' user.
- **sudo rr_test_db.sh n** – print actual network list from 'morse' tablespace.

4.6.2. MAS connection

If the configuration of the Morse Application Server connection parameters is OK and the MAS is properly configured, you should see the successful address seek result and trace info (just a single address – result of address seek). Otherwise you will see some error message or no output:

```
Morse API, ver. 10.0.84.0,(c) 2004, RACOM s.r.o., Czech republic.

Fri Jan  8 11:24:32 2010
 address seek...: 69AAE1FF
Got 1 addresses

------------------------------------------------------------------------------
Fri Jan  8 11:24:32 2010, target local:

69AAE1FF
>>!
```

It is possible to get another information about MAS by executing following scripts. Ordinary user privileges are sufficient to execute the scripts:

- **rr_test_mas.sh s** – print service status.
- **rr_test_mas.sh v** – print MAS device firmware version.

5. Hardware Options

5.1. Dual Screen

MServer is available with a dual port video card, so that you can use two monitors, one mouse, single keyboard, big radio network and two cups of coffee simultaneously.

5.2. Computer Case

MServer is available in three basic versions:

1. SATA / software raid / big tower – Cheapest, but stable and robust solution,
2. rack case – Middle price solution,
3. third party server – Choose your own Dell or HP server. We are ready to install MServer on it.

5.3. Cluster

MServer is ready to operate in cluster mode. You can have two servers, one is active and the other is passive. If one server fails, the other will become active.

Cluster software will send e-mails to inform you about status changes.

The actual status of the cluster can be displayed from: "`MAIN MSERVER MENU /Settings /Others /Cluster Status`"

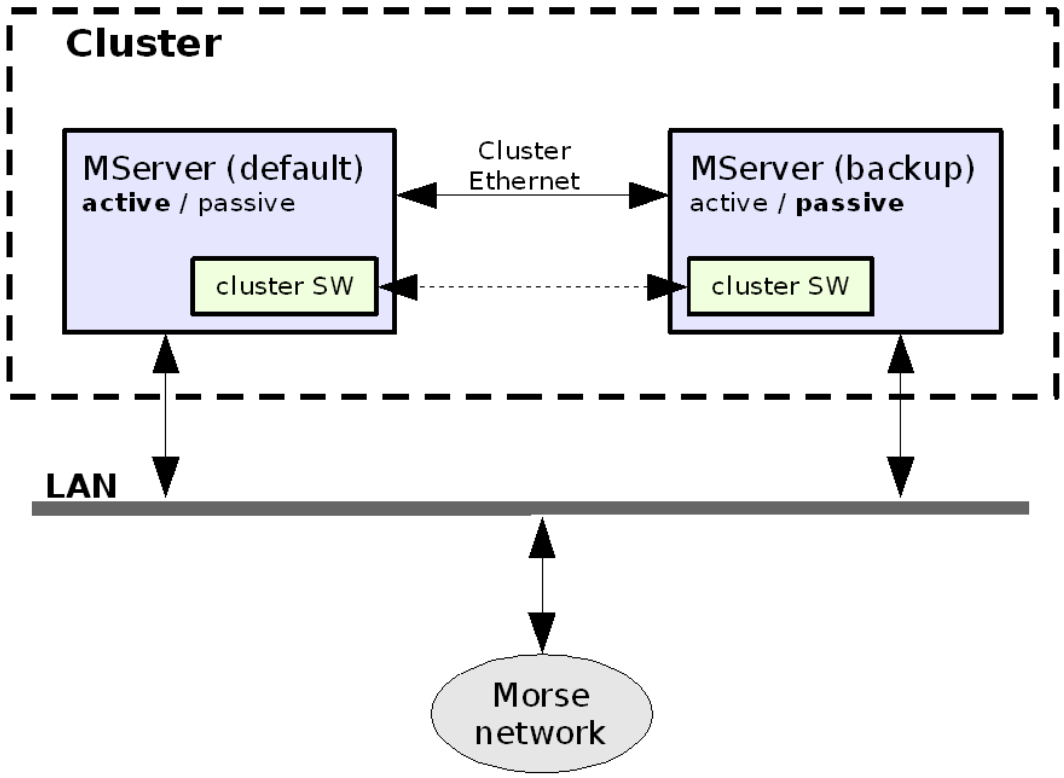


Fig. 5.1: Cluster principle.

5.4. Software RAID

If your MServer runs on a SATA disk it uses a software raid feature. This mirrors data to both disks in such a way that you are able to recover any of it after a fault. If one disk is faulty MServer sends a warning e-mail. After that e-mail you should contact Racom to let you fix the problem and place your data on to a spare disk.

The actual status of a software RAID can be displayed on MServer WWW interface: http://localhost/cgi-bin/mserver-diag/home/df.cgi

6. MServer Mapping Data

Free Vector Maps

MServer is shipped with a set of very simple vector maps covering almost the whole globe. These maps are fetched from http://www.maproom.psu.edu/dcw (these maps are quite old – they can be used for the first steps with MServer).

Look for them in the directory: `/data/maps/rvm/`

Raster Data

Raster format (bmp) is recommended for a serious job with Ranec server. Data must be equipped with positioning files. Ranec client (part of MServer) can switch the raster maps (with various resolution) according to the current zoom.

We prepare a huge number of coordinate systems for Ranec client. This will be suitable for any raster data.

Free SRTM Data

MServer is shipped with SRTM (Shuttle Radar Topography Mission) data. This is fetched from http://srtm.usgs.gov and is equipped with positioning files. This data covers almost the whole planet. Predefined areas of 3 arc second (90 meter) covers the globe between 61 degrees N and 56 degrees S latitude.

This data can be used for visibility diagrams and for “coverage computation” functionality of MServer.

Look for it in the directory: `/data/maps/srtm3/`

7. Remote Access And Alarm System

Remote access to MServer is often very helpful when one needs some non-trivial network configuration. One can simply plug the radio modem into the MServer and Racom experts can then easily set up configuration of this modem via access to remote MServer.

One can also access MServer's graphical tools remotely via the Internet. All you need is a laptop with Internet connectivity.

7.1. Remote Access Graphical Tools

Ranec client – graphical client capable of showing the status of the Morse network.

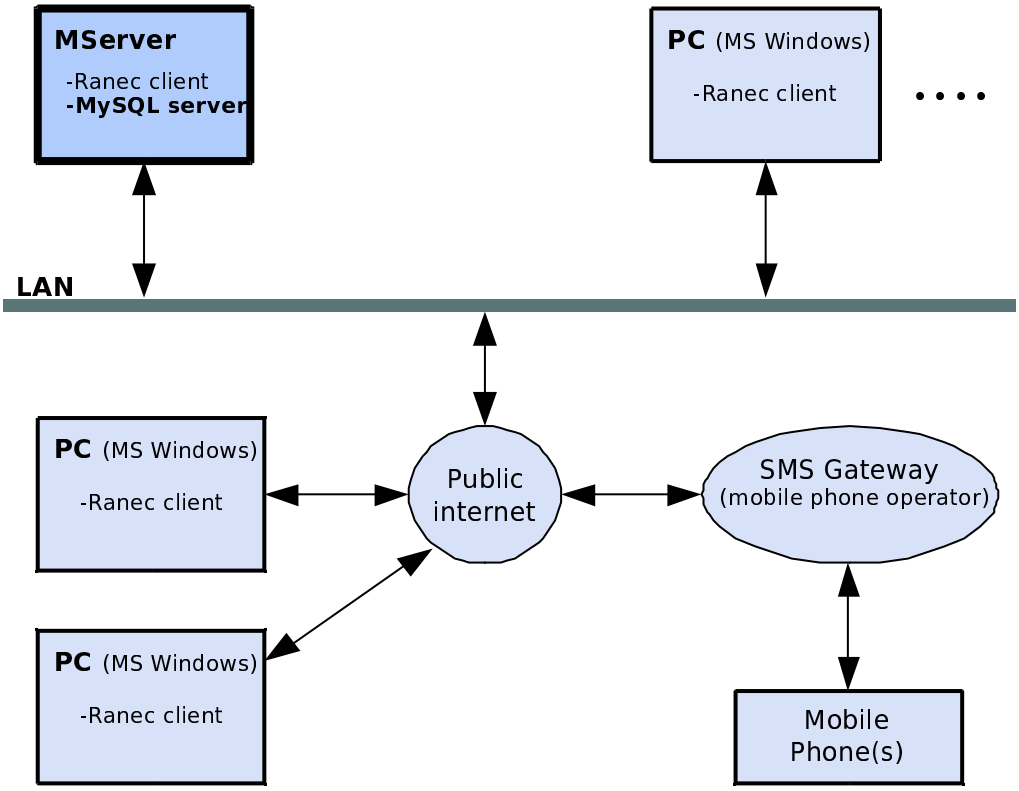


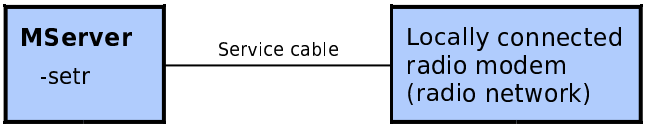
Fig. 7.1: Remote access to MServer – example.

7.2. Remote Access Command Line Tools

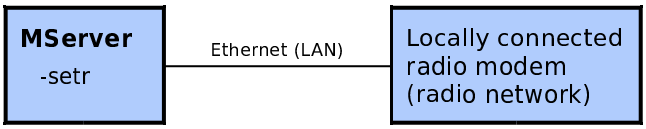
It defines a set of tools which can be used remotely by a serviceman. These tools are placed within the MServer. When one is able to get remote access to the command prompt of MServer one is able to use such tools:

- Service terminal via the service cable to a locally connected radio modem
- Service terminal via Ethernet to a locally connected radio modem
- Service terminal via a dial-up connection to a remote radio modem
- Dial up connection to a remote MServer:
  - Service terminal via a service cable to a locally connected radio modem
  - Service terminal via Ethernet to a locally connected radio modem

Examples:



A serviceman, or Racom expert, can access a remote radio network via a remote MServer and via a service cable.



A serviceman, or Racom expert, can access a remote radio network via a remote MServer and via Ethernet.

7.3. Remote Troubleshooting

Such Remote Access Tools (see above) can typically be used by two people: a Racom expert and a skilled serviceman. What can happen:

An alarm e-mail goes via the SMS gateway as an SMS message to a mobile phone. Then a serviceman can connect his laptop (MS Windows) to the public Internet and then via an OpenVPN protocol to OpenVPN Server (and thus connect to the MServer). Until the keys are lost, or the laptop is lost, this connection is pretty secure.

Two applications can be used:

- Remote access Graphical Tools, namely Ranec client.
- Putty SSH client obtains a connection to an SSH server and the command prompt. Via this connection the Remote Access Command Line Tools can be used.

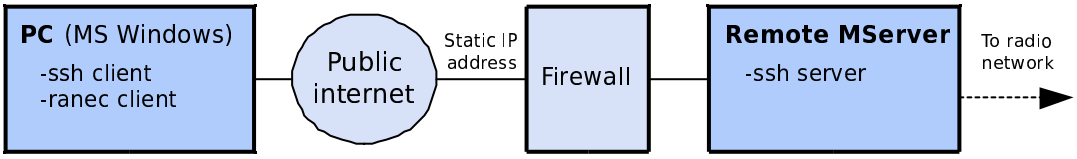
If the serviceman has a serious problem, or some new equipment, he can call for help as follows.

A Racom expert can be connected to a remote MServer via the public Internet in two ways:

- Directly via an SSH protocol. This requires a static IP address (and a leased line for the Internet connection) at the remote MServer.
- Directly via an SSH protocol. This requires a static IP address (and a leased line for the Internet connection) at the remote MServer.

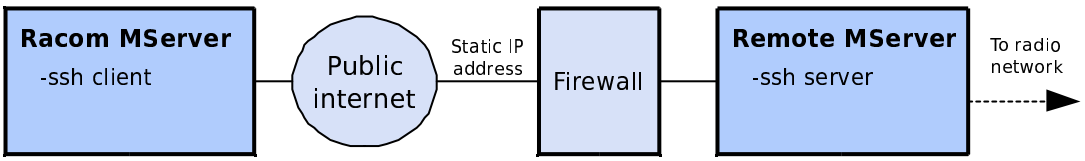
Via both connections the Remote Access Command Line Tools can be used.

Examples:



This network arrangement enables:

- Remote access Graphical Tools – Ranec client
- Putty SSH client – enables Remote Access Command Line Tools.



Access via SSH server only – highest possible security. Does require static IP address. This network arrangement enables Remote Access Command Line Tools.

7.4. How to Set-up SSH Keys

SSH server is always placed in the MServer. SSH client can be run from MS Windows (we recommend Putty software) or from Linux (we recommend OpenSSH package). MServer uses SSH protocol version 2.

Generally you have to generate keys – SSH protocol uses two parts of a key – public part and private part. The private part should be kept in your computer, and the public part is to be copied to a number of servers you want to access. The private part of the key can be secured by passphrase – if the key (or the computer) is lost the key can not be used by anyone. Passphrase is an extra password you will always be prompted for when you will attempt to use the key. Please use more secure DSA keys instead of older RSA keys if there is a choice.

Set up the SSH keys for Linux

1. Generate the key:
   ssh-keygen -t dsa ... enter the pass phrase when prompted.
2. Give the public part of the key (`~/.ssh/id_dsa.pub`) to the system administrator. Don't use plain text in an e-mail for this purpose, use an attachment in an extra file! The administrator will add the content of this file into the file `~/.ssh/authorized_keys` in your home directory. You must be the owner of such a file and rights should be set to "`chmod 600 ...`".
3. Check the SSH configuration `/etc/ssh/ssh_config`. The protocol version order should be "`Protocol 2,1`", or "`none`".

MS Windows

1. Install the newest stable version of the Putty software.
   http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
2. Run `PUTTYGEN.EXE` and generate a DSA key with the passphrase enabled.
3. Save the private part of the key to your disk (e.g. to the directory of the putty program).
4. Copy the public part of the key to some text file (use keyboard and notepad to copy this data and save. Do not use the file created by puttygen as it is in an unusable format). Give this file to the system administrator. Don't use plain text in an e-mail for this purpose, use an attachment in an extra file! The administrator will add the content of this file into the file `~/.ssh/authorized_keys` in your home directory. You must be the owner of such a file and rights should be set to "chmod 600 ...".
5. Set up the putty software. SSH protocol should be set to version 2. Set up the path to the private part of previously generated key.

8. Ranec introduction

Ranec (**RA**dio **NE**twork **C**entre) software package is primarily designed to serve radio network management, diagnostics and service. Ranec is also ready to ease the design of the radio networks. Easy to use front end interface to Ranec wide functionality is ready to fulfil all kinds of the user requirements.

Please see full Ranec documentation[1].

Network supervision

Typical area of usage covers monitoring and management of fixed and mobile Morse radio networks. Ranec contains set of tools capable of analysis of the actual network topology and supervision an on-line status of the individual radio modems.

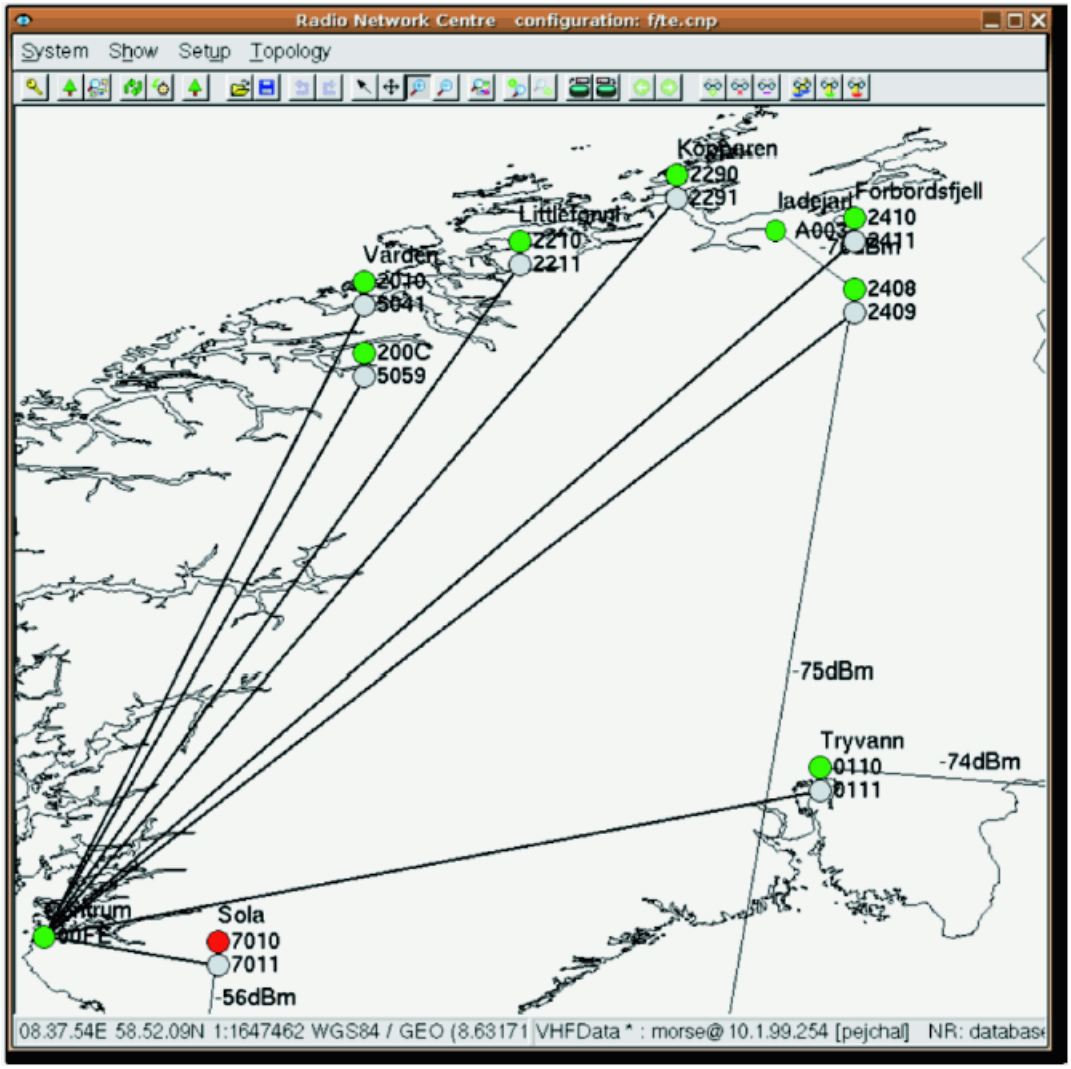


Fig. 8.1: Topology with radio modem on-line status information

Another set of tools is capable of uploading the statistical data from the radio modems. There are many types of available statistical data.

[1] http://www.racom.eu/eng/support/ranec/index.html

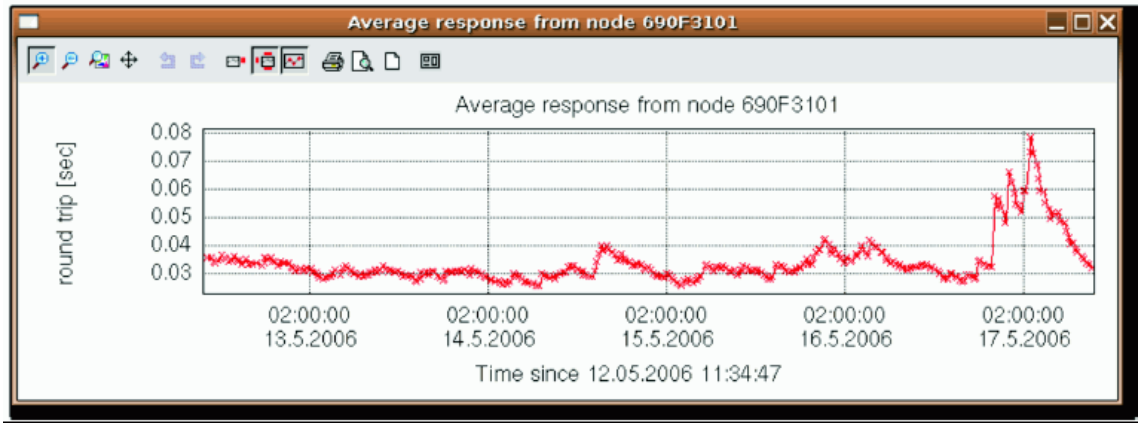


Fig. 8.2: Average response

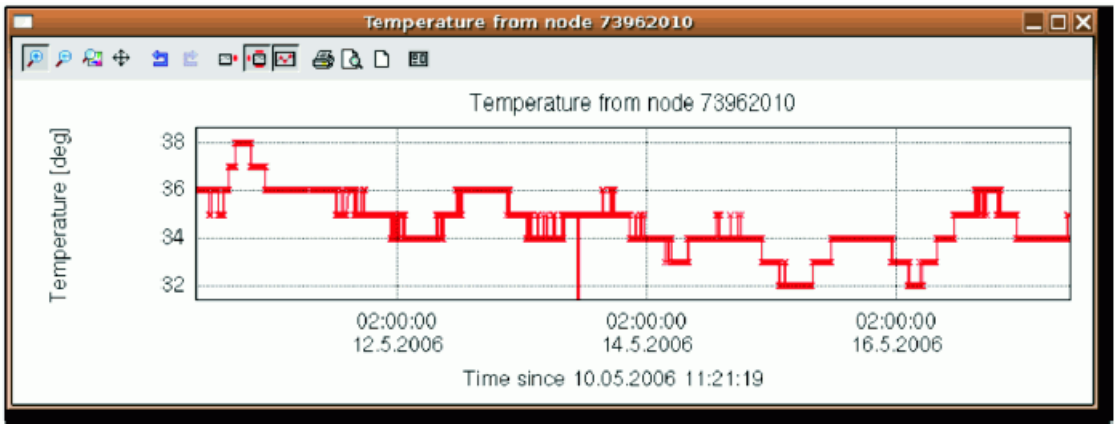


Fig. 8.3: Temperature inside the radio modem

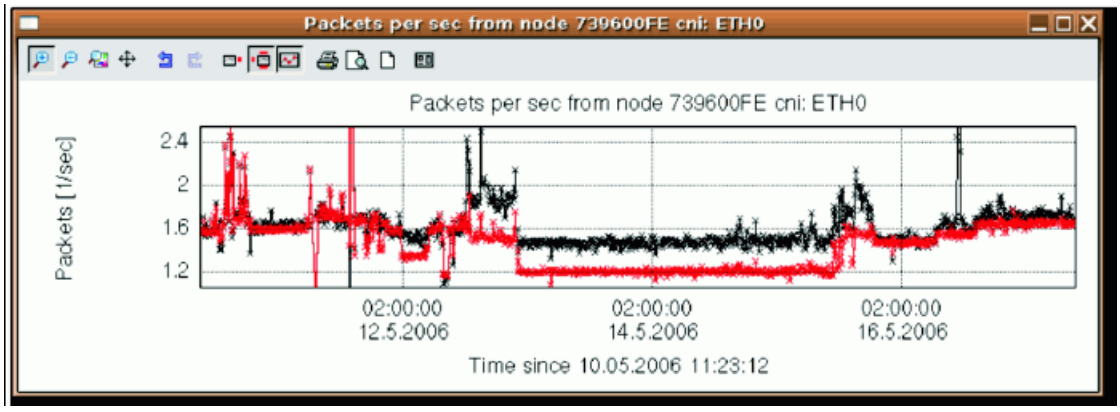


Fig. 8.4: Ethernet port traffic load

Mobile station can be tracked immediately on-line or off-line using historical data later on. Mobile station position and signal strength data stored in the database can be used to analyse the measured signal coverage.

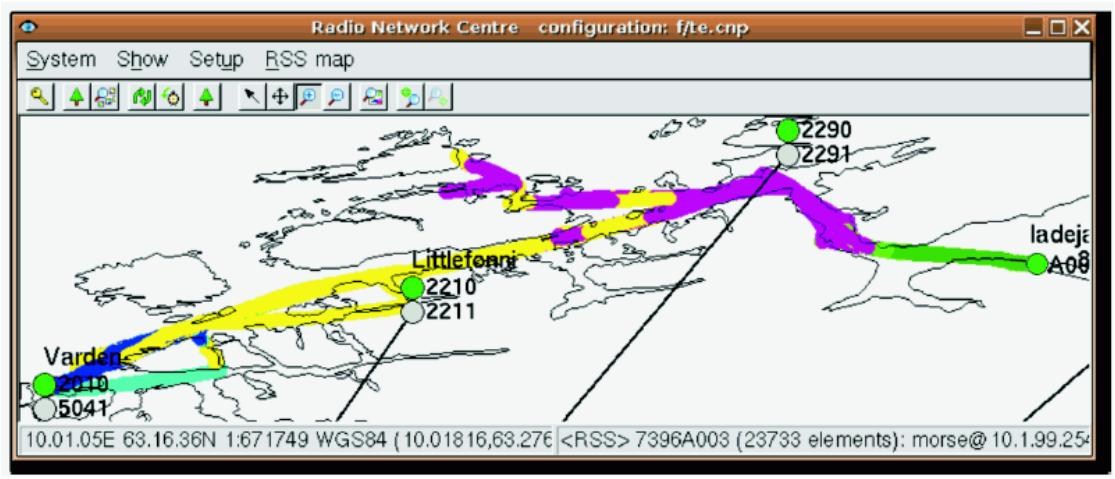


Fig. 8.5: Signal coverage – base stations coverage analysis

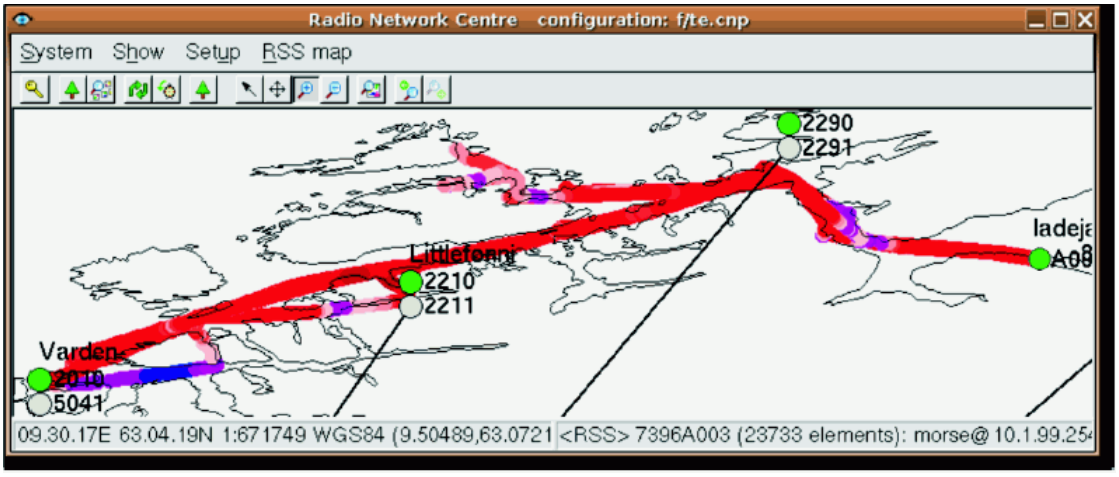


Fig. 8.6: Signal coverage – signal strength analysis

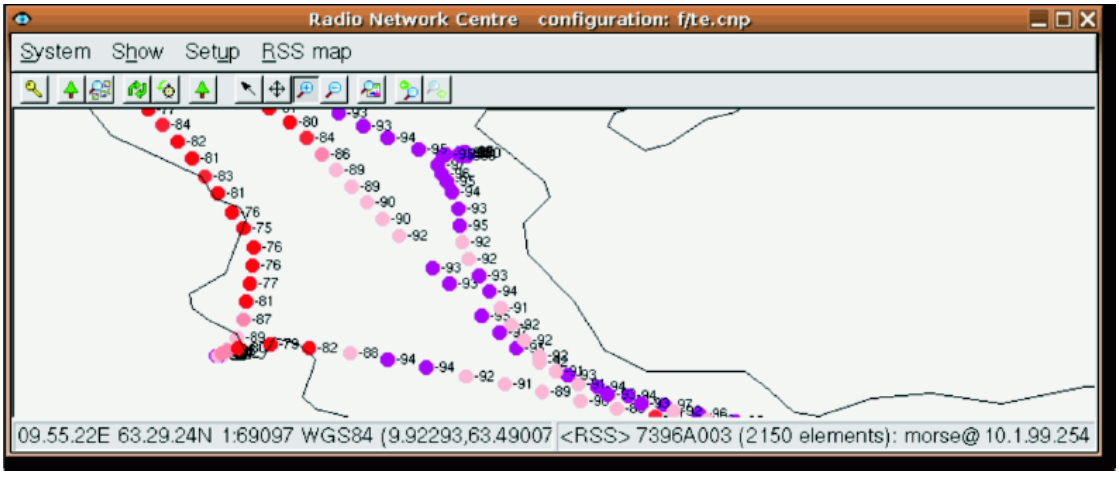


Fig. 8.7: Signal coverage – signal strength analysis (detail view)

Network topology drawn during the network development can be saved for service purposes. Information contained in the network diagram is the entry point to the network for the servicemen. Direct Ranec communication capability to the destination Morse device was implemented.

Network design

Capability to draw and display network topology is the Ranec basic functionality. Set of standard symbols and connection lines is used to draw the networks. Bitmap icons are currently used to display the mobile stations, thereby the user interface is more transparent. All the drawn network topology symbols are used to make a user interface for the network diagnostic. Drawn topology can be used as a kind of documentation. Simple network hierarchy is supported. Search tools to explore large networks are provided.

SRTM3 digital terrain model can be used to optimize network design. Line of sights as well as the theoretical signal coverage can be calculated.

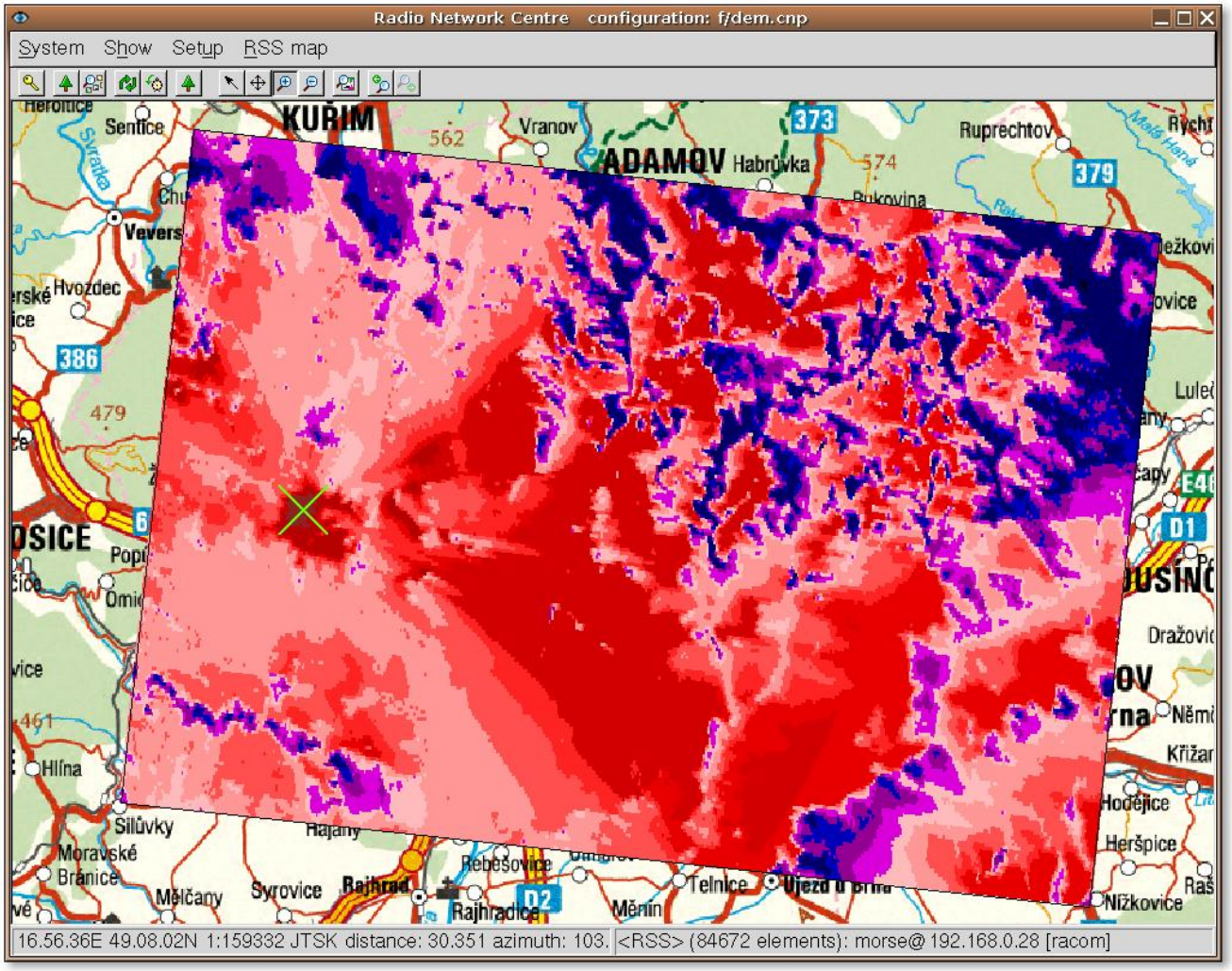


Fig. 8.8: Calculated coverage

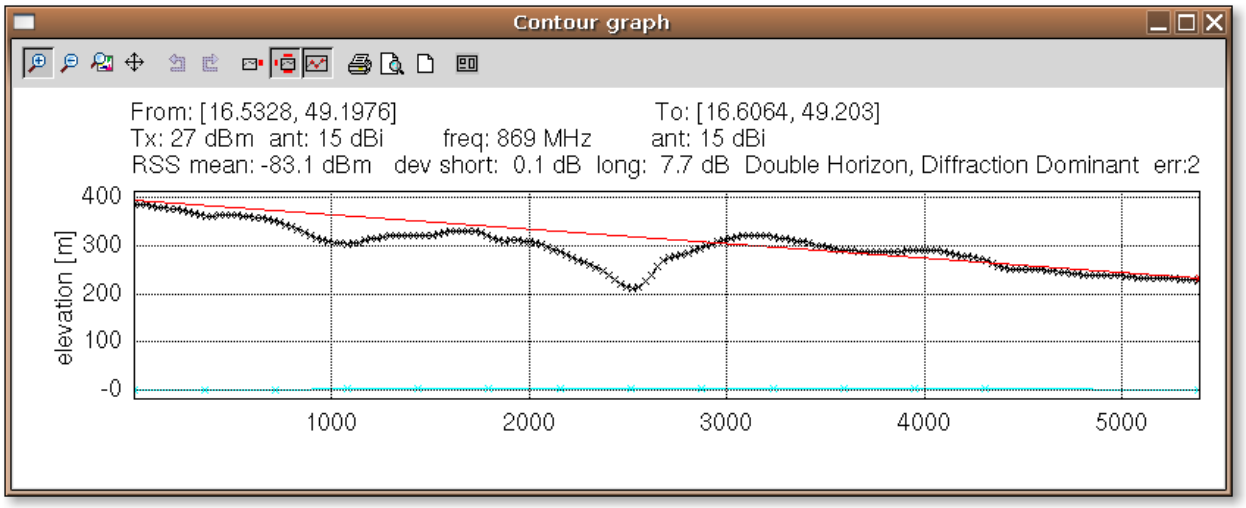


Fig. 8.9: Line of sight

Client–server architecture

All the network topology data are stored on the central server. Network topology can be saved in the file as well. Network diagnostic data are periodically collected from the network and stored on the central server. Powerful MySQL database is used as the data storage engine.

Set of supervision applications is running on the server. These application are monitoring network status and uploading the radio modem statistical data. All the data are stored in the central database. Unlimited number of the Ranec clients can be connected to the central server at one moment (see Figure 2.1. – Client–server model). No additional network load is caused, because Ranec client downloads the data from the central database typically and not from the radio network directly. Linux and Microsoft Windows clients are available without any software licenses.

Set of tools for remote server administration are ready to allow Racom specialists to help the customers in their specific situations.

Ranec – miscellaneous

- There are some differences of the Ranec client when running on Linux or Windows platform:
  - The Windows client can not be configured to run alarm control automatically at the application startup.
    menu "`Setup/Program Configuration/Alarm Parameters/RunAlarm Control`" in the Linux Ranec client.
  - Some tools are not available in the Windows client:
    menu "`Tools/Netlock/...`", "`Tools/Lines/Fetch...`", "`Tools/Nodes/Fetch...`"
- To remove all statistical logs from database the script "`rr_mysqllogs_delete.sh`" can be used (you have to become a superuser to run the script).

  Beware! All historical data of the Morse networks will be deleted.
- **Note!** Time synchronization of the Morse network modems (including walrus) is necessary to correct data displaying.

9. Conditions for MServer Operation

9.1. Important Warning

RACOM s. r. o. (hereinafter referred to as RACOM) is the exclusive owner of all rights to this operating manual. All rights reserved. Any duplication of this manual in any way, shape or form, or translation to any other language (without the prior written consent of the owner of the rights) is strictly forbidden.

RACOM retains the right to make changes to the technical specification or functions of this product or to terminate production of this product without advance written notice to the customer.

RACOM firmware is available free of charge. Source code is the property of RACOM and is not available to any user. Any commercial use of the software with this licence is strictly forbidden. Changes to software and documentation are forbidden.

RACOM firmware is released with the intention that it will be useful, however without any specific guarantees. Under no circumstances is the author or any other company or person responsible for incidental, accidental or related damage arising as a result of the use of this product. The manufacturer shall not provide the user with any form of guarantee containing assurance of the suitability and applicability for its application.

RACOM products are not developed, designed or tested for use in equipment which directly affects the health and life functions of humans or animals and neither as part of other important equipment, and RACOM does not provide a guarantee if company products are used in such equipment.

9.2. Conditions of Liability for Defects and Instructions for Safe Operation of Equipment

Please read these safety instructions carefully before using the product:

- Liability for defects does not apply to any product that has been used in a manner which conflicts with the instructions contained in this operator manual, or if the equipment has been tampered with.
- Equipment mentioned in this operator manual may only be used in accordance with instructions contained in this manual. Error–free and safe operation of this equipment is only guaranteed if this equipment is transported, stored, operated and controlled in the proper manner. The same applies to equipment maintenance.
- In order to prevent damage to the router and other terminal equipment the supply must always be disconnected upon connecting or disconnecting the cable to the router data interface. It is necessary to ensure that connected equipment has been grounded to the same potential. Before connecting the supply cable the output source voltage should be disconnected.
- Only undermentioned manufacturer is entitled to repair this devices.