All interfaces in the router network that must be able to join in a multicast group must have IGMP and PIM-SM enabled.

2.16.10.2.2.1 Multicast and VPN

As such – VPN/IPSec does not support the transport of multicast packets. GRE tunneling does support multicast routing – but is not encrypted. Therefore the configuration shown at end of this document – the recommended configuration – uses IPSec encrypted GRE tunnels. Combining the IPSec and GRE will ensure the routing of both unicast and multicast – and still maintaining integrity and intrusion security of the network.

2.16.10.2.2.2 GRE tunneling

Generic Routing Encapsulation (GRE) is a tunneling protocol designed to encapsulate a wide variety of network layer packets inside IP tunneling packets. The original packet is the payload for the final packet. GRE was developed by Cisco and was designed to be stateless; the tunnel end-points do not monitor the state or availability of other tunnel end-points. GRE creates a virtual point-to-point link with routers at remote points on an IP internetwork.

2.16.11 Applicable tools for router programming

The Cisco offers a CLI – Command Line Interface. This is accessible through the console port of the router. Use the blue cable delivered with the router. In this case use the serial port of your PC. You can use any of a variety of terminal emulation programs.

If you know the IP address of one of the Ethernet ports on the router – you can also telnet into the router and use the same CLI.
The configuration of any Cisco router – can be exported from the router and onto a so called TFTP server. The router configuration file is then an ASCII formatted text string. This can be opened – edited and saved by the use of any of a variety of text editor programs.
After editing – the file can be re-imported to the Cisco router. After a reload of the router – it will reflect the newly introduced configuration changes that you made offline.

2.16.11.1 Ultraedit:

- A text editor program for offline editing of configuration files.

2.16.11.2 WordPad:

- A text editor program for offline editing of configuration files. Available typically in Windows.

2.16.11.3 HyperTerminal:

- A Windows standard program that can do both serial communication and also use TCP/IP to connect to router via Ethernet.

2.16.11.4 Putty:

- A very versatile program that does serial and IP connections.

2.16.11.5 3CDeamon:

- A TFTP program from 3COM.

2.16.11.6 Tftp32:

- A TFTP program from http://tftpd32.jounin.net: Freeware.

2.16.11.7 Example of router configuration

```
Rendezvous point router:
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 24-S000-VPN1
!
boot-start-marker
boot-end-marker
!
no logging buffered
no logging console
enable password xxxxx
!
no aaa new-model
!
resource policy
!
ip cef
!
!
!
!
no ip domain lookup
ip multicast-routing
!
!
!
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key s001-s000 address 10.239.24.1
crypto isakmp key s002-s000 address 10.239.24.2
crypto isakmp key s003-s000 address 10.239.24.3
crypto isakmp key s004-s000 address 10.239.24.4
```

```
crypto isakmp key s005-s000 address 10.239.24.5
!
!
crypto ipsec transform-set tetra esp-3des esp-md5-hmac
 mode transport
!
crypto map GRE local-address FastEthernet0/0
crypto map GRE 11 ipsec-isakmp
 set peer 10.239.24.1
 set transform-set tetra
 match address 101
crypto map GRE 12 ipsec-isakmp
 set peer 10.239.24.2
 set transform-set tetra
 match address 102
crypto map GRE 13 ipsec-isakmp
 set peer 10.239.24.3
 set transform-set tetra
 match address 103
crypto map GRE 14 ipsec-isakmp
 set peer 10.239.24.4
 set transform-set tetra
 match address 104
crypto map GRE 15 ipsec-isakmp
 set peer 10.239.24.5
 set transform-set tetra
 match address 105
!
!
!
!
interface Tunnel1
 description "s000-s001"
 ip unnumbered FastEthernet0/1
 ip mtu 1440
 ip pim sparse-mode
 ip igmp version 3
 keepalive 10 3
 tunnel source FastEthernet0/0
 tunnel destination 10.239.24.1
 crypto map GRE
!
interface Tunnel2
 description "s000-s002"
 ip unnumbered FastEthernet0/1
 ip mtu 1440
 ip pim sparse-mode
 ip igmp version 3
 keepalive 10 3
 tunnel source FastEthernet0/0
```

```
 tunnel destination 10.239.24.2
 crypto map GRE
!
interface Tunnel3
 description "s000-s003"
 ip unnumbered FastEthernet0/1
 ip mtu 1440
 ip pim sparse-mode
 ip igmp version 3
 keepalive 10 3
 tunnel source FastEthernet0/0
 tunnel destination 10.239.24.3
 crypto map GRE
!
interface Tunnel4
 description "s000-s004"
 ip unnumbered FastEthernet0/1
 ip mtu 1440
 ip pim sparse-mode
 ip igmp version 3
 keepalive 10 3
 tunnel source FastEthernet0/0
 tunnel destination 10.239.24.4
 crypto map GRE
!
interface Tunnel5
 description "s000-s005"
 ip unnumbered FastEthernet0/1
 ip mtu 1440
 ip pim sparse-mode
 ip igmp version 3
 keepalive 10 3
 tunnel source FastEthernet0/0
 tunnel destination 10.239.24.5
 crypto map GRE
!
interface FastEthernet0/0
 ip address 10.239.24.100 255.0.0.0
 ip access-group 199 in
 ip nbar protocol-discovery
 duplex auto
 speed auto
 no cdp enable
 crypto map GRE
!
interface FastEthernet0/1
 ip address 172.16.0.1 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 duplex auto
```

```
 speed auto
!
ip route 172.16.1.0 255.255.255.0 Tunnel1
ip route 172.16.2.0 255.255.255.0 Tunnel2
ip route 172.16.3.0 255.255.255.0 Tunnel3
ip route 172.16.4.0 255.255.255.0 Tunnel4
ip route 172.16.5.0 255.255.255.0 Tunnel5
!
!
ip http server
ip http authentication local
ip http secure-server
ip pim bidir-enable
ip pim rp-address 172.16.0.1
!
access-list 101 permit gre host 10.239.24.100 host 10.239.24.1
access-list 102 permit gre host 10.239.24.100 host 10.239.24.2
access-list 103 permit gre host 10.239.24.100 host 10.239.24.3
access-list 104 permit gre host 10.239.24.100 host 10.239.24.4
access-list 105 permit gre host 10.239.24.100 host 10.239.24.5
access-list 199 remark ----------------------  199  --------------------------------
access-list 199 permit gre host 10.239.24.1 host 10.239.24.100
access-list 199 permit esp host 10.239.24.1 host 10.239.24.100
access-list 199 permit udp host 10.239.24.1 eq isakmp host 10.239.24.100 eq isakmp
access-list 199 permit gre host 10.239.24.2 host 10.239.24.100
access-list 199 permit esp host 10.239.24.2 host 10.239.24.100
access-list 199 permit udp host 10.239.24.2 eq isakmp host 10.239.24.100 eq isakmp
access-list 199 permit gre host 10.239.24.3 host 10.239.24.100
access-list 199 permit esp host 10.239.24.3 host 10.239.24.100
access-list 199 permit udp host 10.239.24.3 eq isakmp host 10.239.24.100 eq isakmp
access-list 199 permit gre host 10.239.24.4 host 10.239.24.100
access-list 199 permit esp host 10.239.24.4 host 10.239.24.100
access-list 199 permit udp host 10.239.24.4 eq isakmp host 10.239.24.100 eq isakmp
access-list 199 permit gre host 10.239.24.5 host 10.239.24.100
access-list 199 permit esp host 10.239.24.5 host 10.239.24.100
access-list 199 permit udp host 10.239.24.5 eq isakmp host 10.239.24.100 eq isakmp
no cdp run
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
 password xxxxx
 login
!
scheduler allocate 20000 1000
```

```
end
```

Access router:

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 24-S001-VPN1
!
boot-start-marker
boot-end-marker
!
no logging console
enable password xxxxx
!
no aaa new-model
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
ip cef
no ip domain lookup
ip multicast-routing
!
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key s001-s000 address 10.239.24.100
!
!
crypto ipsec transform-set tetra esp-3des esp-md5-hmac
 mode transport
!
crypto map GRE local-address FastEthernet0/0
crypto map GRE 10 ipsec-isakmp
 set peer 10.239.24.100
 set transform-set tetra
 match address 101
!
!
!
```

```
interface Tunnel1
 ip unnumbered FastEthernet0/1
 ip mtu 1440
 ip pim sparse-mode
 ip igmp version 3
 keepalive 10 3
 tunnel source FastEthernet0/0
 tunnel destination 10.239.24.100
 crypto map GRE
!
!
interface FastEthernet0/0
 ip address 10.239.24.1 255.0.0.0
 ip access-group 121 in
 duplex auto
 speed auto
 no cdp enable
 crypto map GRE
!
!
interface FastEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 duplex auto
 speed auto
!
ip route 0.0.0.0 0.0.0.0 Tunnel1
no ip http server
no ip http secure-server
!
ip pim bidir-enable
ip pim rp-address 172.16.0.1
!
!
access-list 101 permit gre host 10.239.24.1 host 10.239.24.100
access-list 121 remark ----------------  121  ----------------------------------
access-list 121 permit esp host 10.239.24.100 host 10.239.24.1
access-list 121 permit udp host 10.239.24.100 eq isakmp host 10.239.24.1 eq isakmp
access-list 121 permit gre host 10.239.24.100 host 10.239.24.1
no cdp run
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 password xxxxx
```

```
 login
!
end
```

Observe that the passwords inside the configuration files are anonymised with ”xxxxx”. You can enter any password of your liking to secure your router from unauthorized access.

PART-3: TetraFlex® Applications

3.1 GENERAL SYSTEM DESCRIPTION

3.1.1 TetraFlex V7.5 General System description

For complete system description, refer to ref.1: "TetraFlex v7.5 System description.pdf

3.1.2 Site versus Node:

Until the DAMM TetraFlex® system software was introduced we have used the word "Site" to indicate how many radio sites there were in a system. There was coherency between number of "Sites" and number of "Radio sites".

The DAMM TetraFlex® concept opens for "Sites" meaning the actual geographical position of the equipment and a NODE meaning any unit running a BSC.exe application (except for the redundant BSC).

A node could be a radio node, GW node or a combination of these.

3.1.3 Software packages:

All DAMM TetraFlex® system software packages with all Functions and Applications are available on http://www.damm.dk/ restricted area in encrypted form for a period of minimum 18 months after Release Date

- All Software Releases consist of:
  - Software package with Software Release number.
  - Release Note.
  - Commercial Note.
- A software package can be de-encrypted by means of any valid DAMM dongle.
- If a new Software Release contains bug fixes, which have a serious effect on the operation of a system, the Application Date can be set to an earlier date, and thereby allow execution on systems, where the dongle Application Date Limit has expired. DAMM Support Department is responsible for keeping the www.damm.dk restricted area updated
- Software packages with a Release Date older than 18 months shall be removed from www.damm.dk

3.1.3.1 Software packages execution or update:

The dongle controls which software release and which part of the release that can be executed on the BSC4XX or PC in which the dongle is inserted.
The customer may decide to execute the total package or only some of the files in the package.

If the End-User decides only to execute some of the files in the package he must check the release note for the new release against the release note for the present release and make sure that all files not identical are updated.

3.2 BASE STATION CONTROLLER

3.2.1 BSC.exe description

The core software for the TetraFlex® system is the Node Software (BSC.exe) running as a service under Windows XP or Windows 7. It can run on both the BSC421 and BSC412 Base Station Controllers (and on an ordinary PC or Server as well), and adapts automatically to the detected hardware platform. The BSC.exe service contains all the functions needed to run a complete Tetra system, including Subscriber Register with Security Key Register, Radio Cell, Voice Gateway, Packet Data Gateway (extern connection) / Server (Tetra-Tetra connection) and Application gateway.

The software supports the use of Redundant Base Station Controllers, as one BSC will be active and the other BSC standby. Communication and supervisory between the two BSC's will ensure, that the standby BSC automatically takes over, if the active BSC fails.

3.2.2 BSC-GUI

The user interface for the BSC.exe from version 7.5:

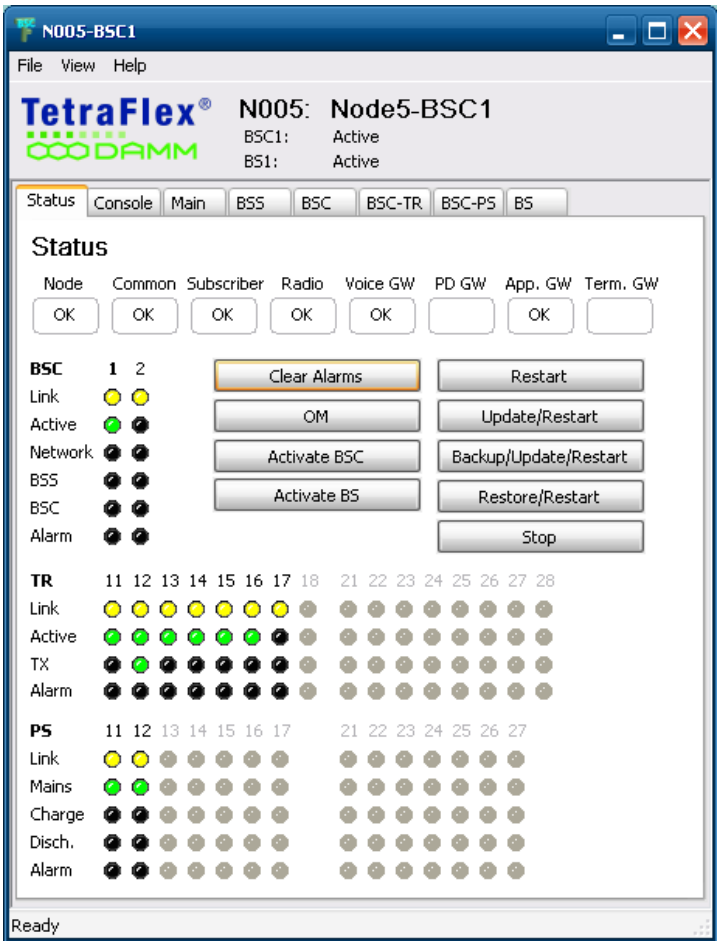


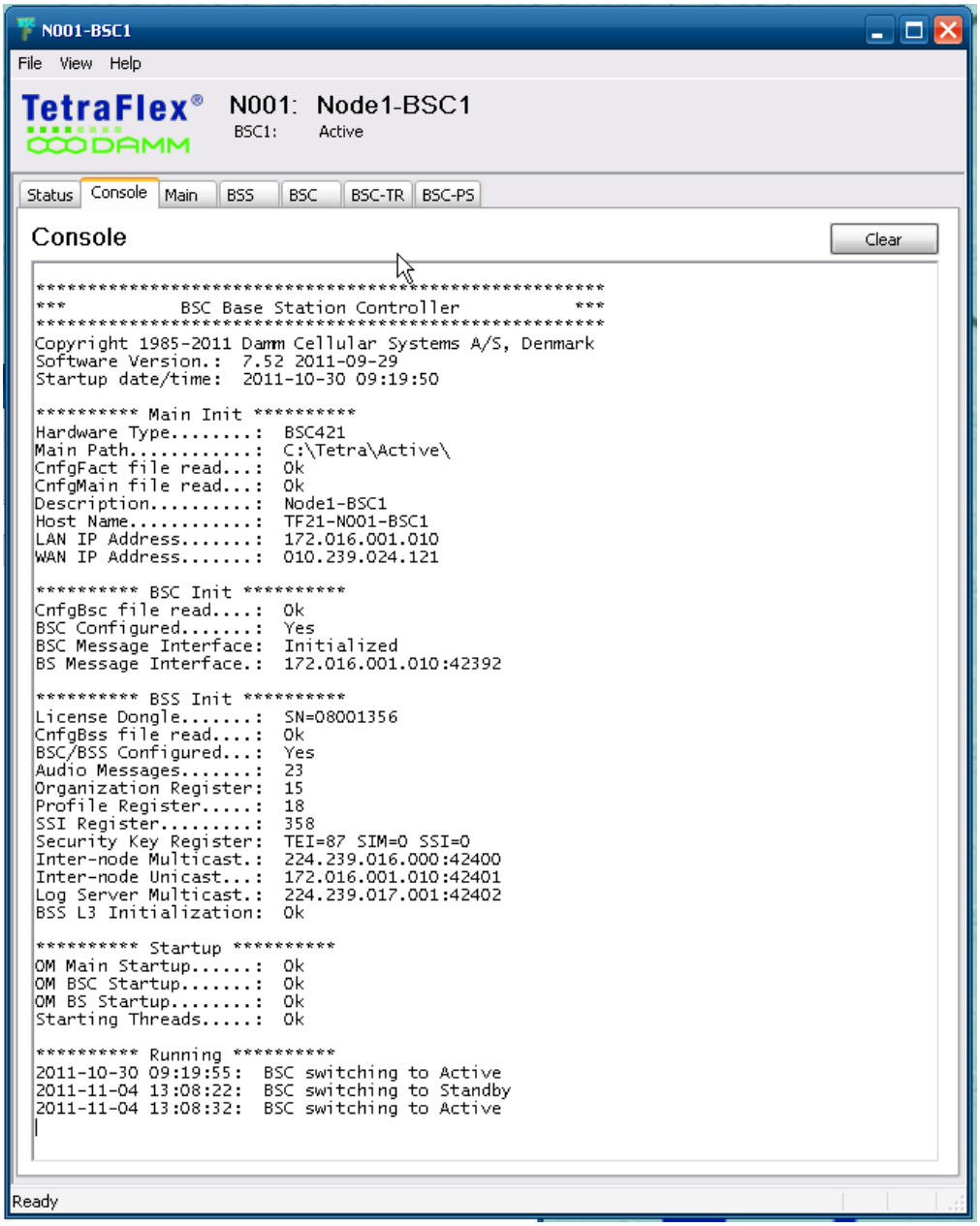
Figure 3-1: BSC-GUI

The BSC-GUI can be started from the TetraFlex Start menu or the Taskbar. The GUI can only operate on the BSC.exe that is running on the same node.

The GUI has 7 tabs (8 for the BS41x version):

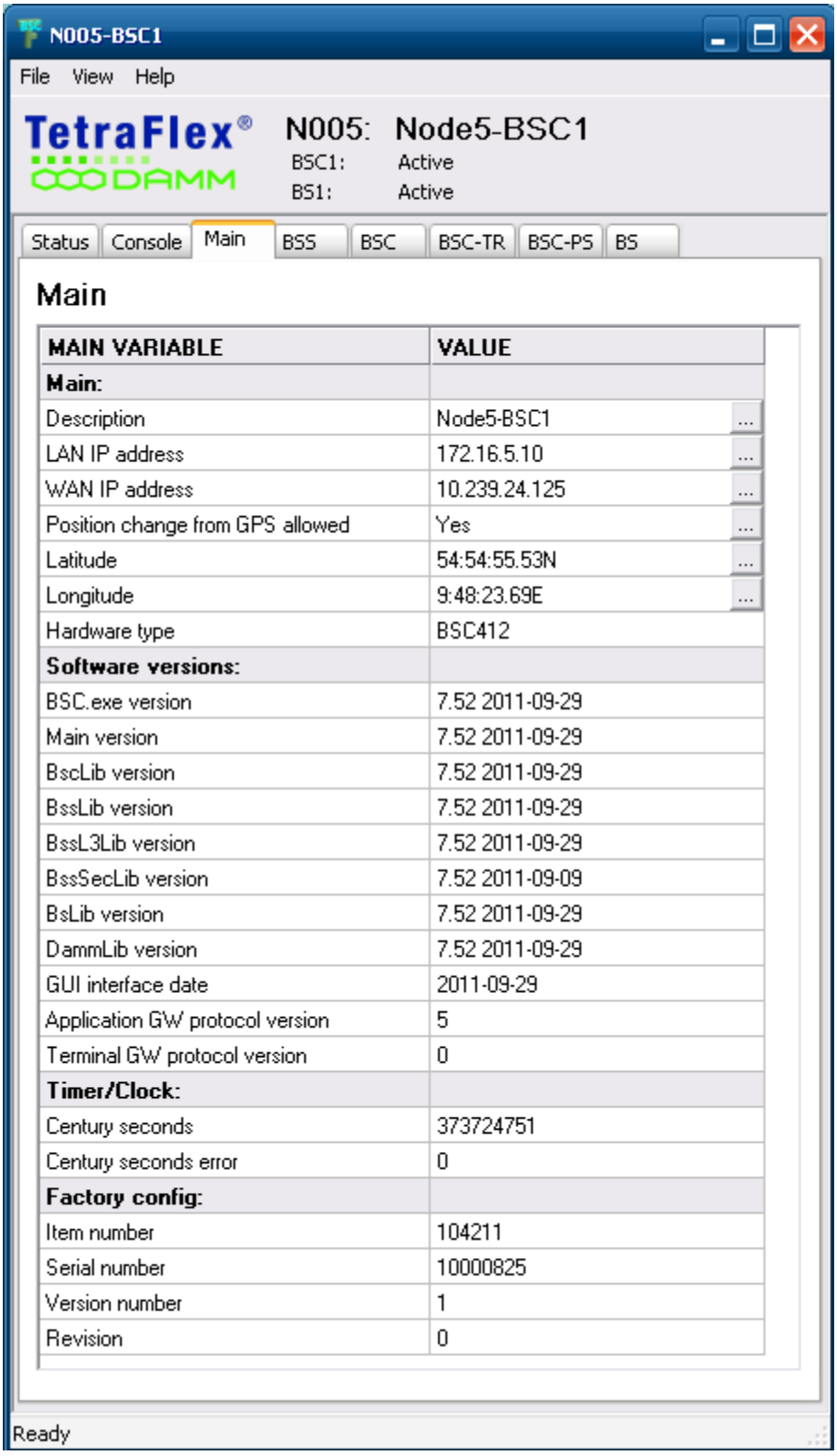
Status: (se figure 3-1) gives an overview of the status of the BSC, TR (Transceivers) and PS (Power Supply's). It is possible to clear alarm, access the OM command system, Activate BSC and BS (Only BS41x), Restart and Stop the BSC, and Update of software and Restore and Backup of software and settings. These are functions also available in Network Management.

Console: The Console window is updated at each BSC start-up, and shows the start-up status of the system. The window is dynamic and will be updated when the status of the BSC changes e.g. from active to inactive



The *Clear* Button deletes the actual content of the console window.

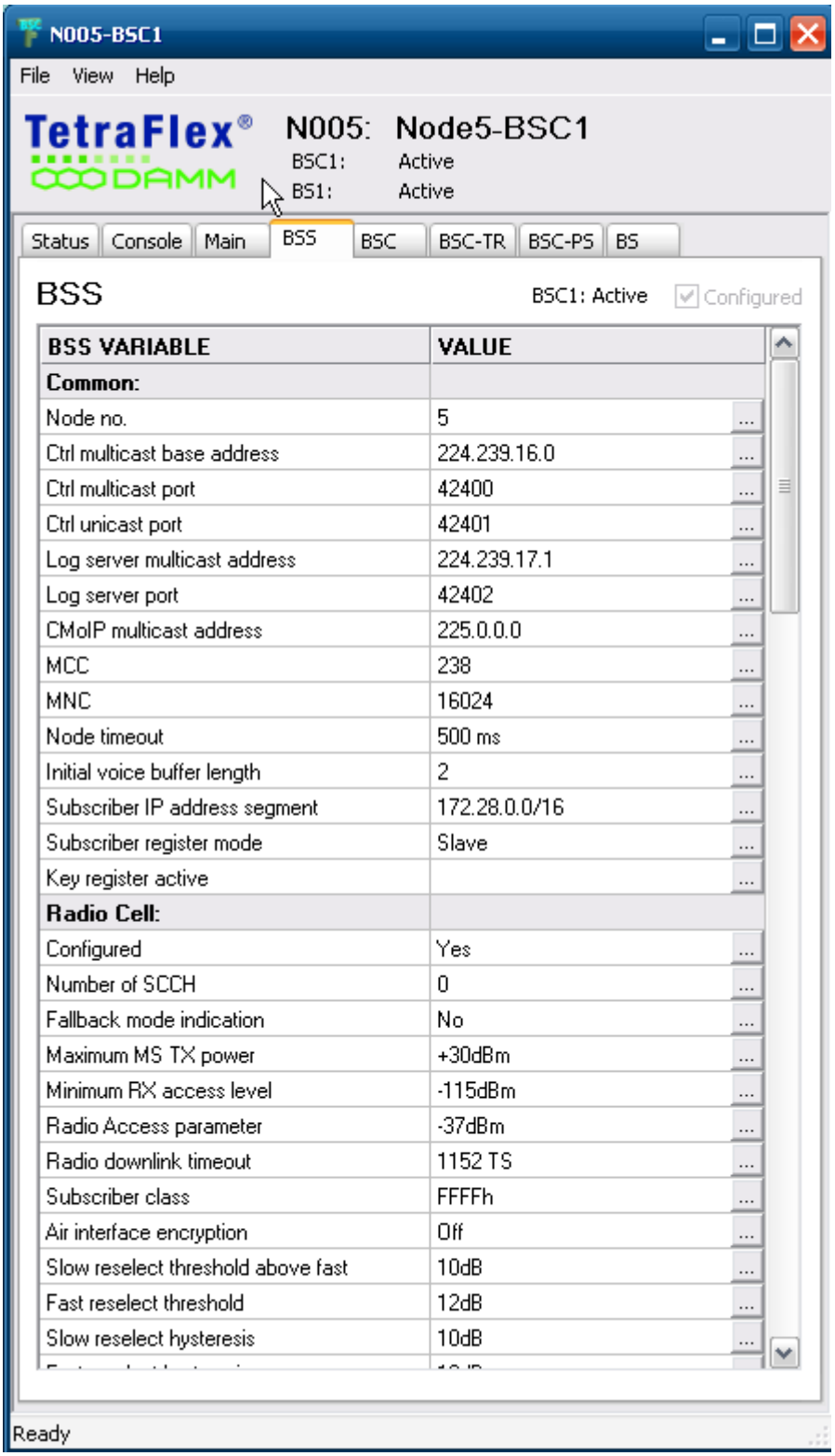
MAIN: From the Main window the fundamental parameters for the BSC can be set and displayed. The corresponding OM command to Main starts with M (e.g. M00). The settings are stored in c:\tetra\active\data\CnfgMain.txt



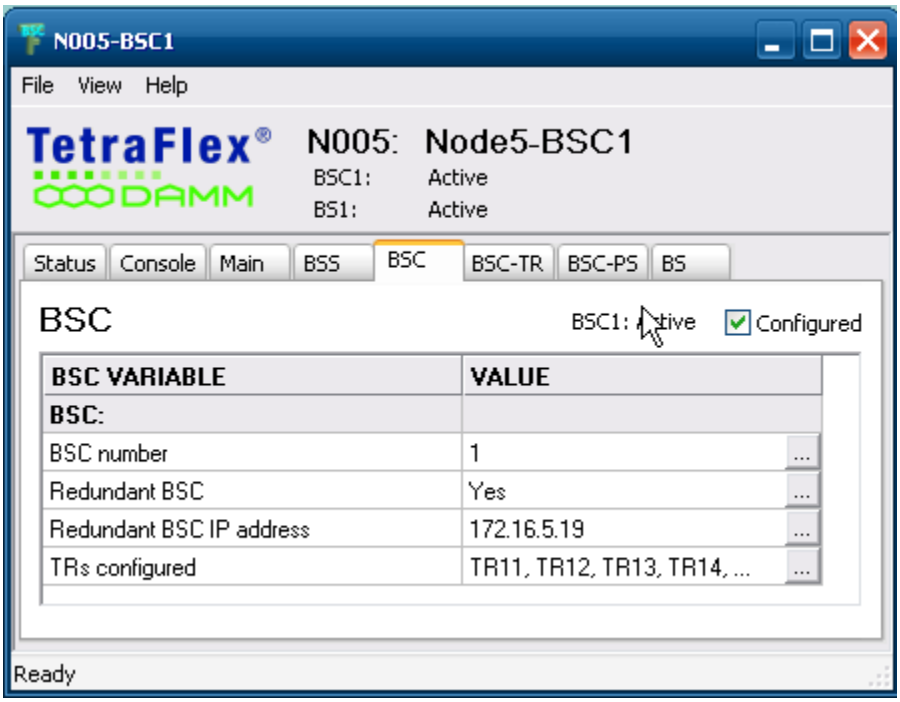
The LAN and WAN address can be selected from the actual IP setting in Windows and the input of GPS data can be enabled and disabled (yes /no). If GPS is enabled the GPS

coordinates are shown in the Latitude and Longitude fields. If it is disabled the coordinates can be set manually.

BSS: From the BSS window most of the SwMI parameters can be set and displayed. The corresponding OM commands to BSS starts with S (e.g. S00). The settings are stored in c:\tetra\active\data\CnfgBss.txt.
The corresponding parameters can be set in NM so please find the explanation for the various parameters in the chapter covering NM –BSC list.



BSC: From the BSC window a Redundant BSC can be defined. Also the Transceivers (TR) connected to BSC can be setup. The corresponding OM command to BSC starts with F (e.g. F00). The settings are stored in c:\tetra\active\data\CnfgBsc.txt



3.3 NETWORK MANAGEMENT

3.3.1 Network Management

The TetraFlex® Network Management (NM) application is a graphical interface to the TetraOM application (OM). This indicates that most of the functions in the NM may as well be executed in the OM using the appropriate OM command

The Network Management (NM) software may be executed on any PC which has an IP connection to the infrastructure. The NM must be able to listen to the multicast which means that the PC must be connected to the LAN

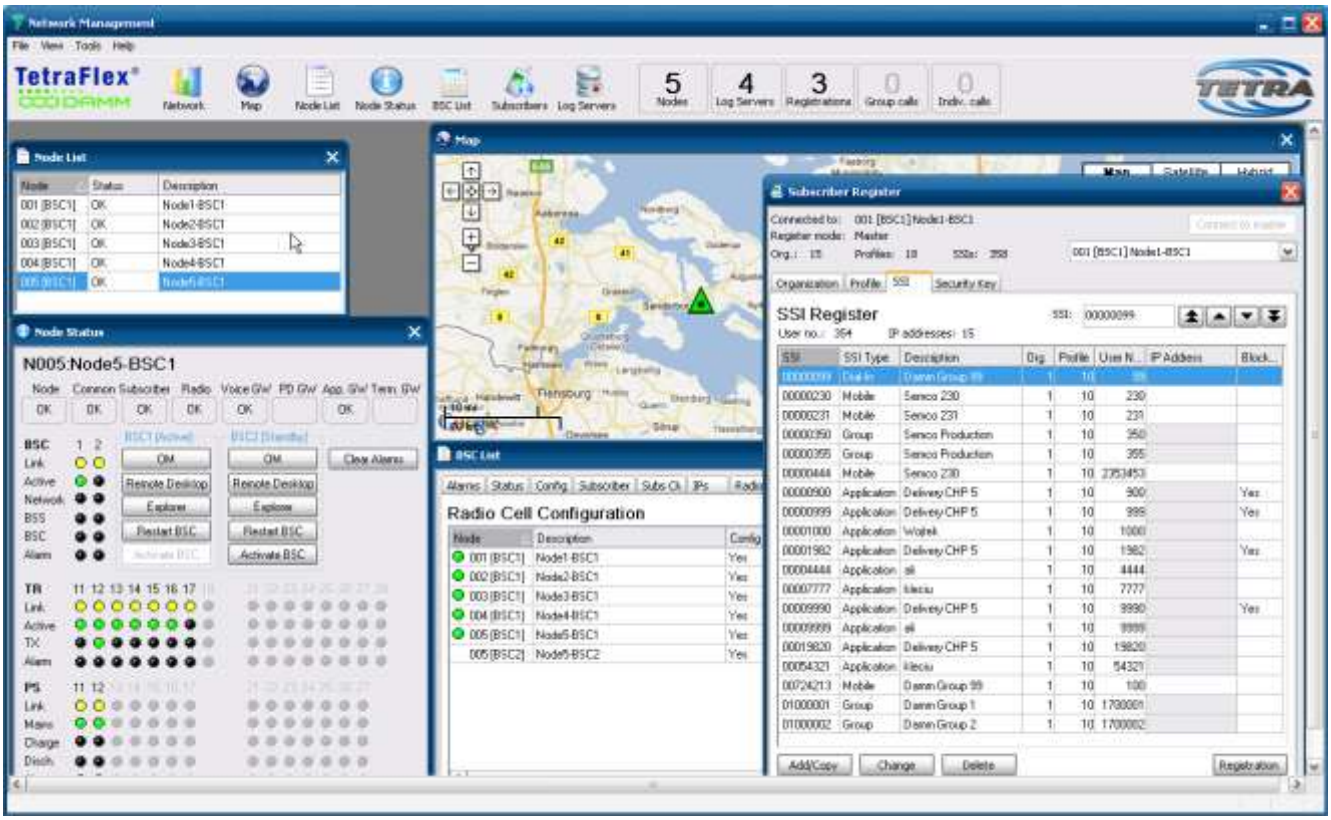


Figure 3-2: Network Management Main Screen

The NM consists of the following components / windows.

3.3.2 Toolbar

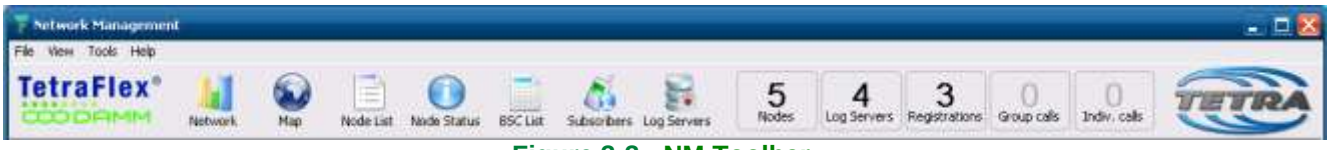


Figure 3-3: NM Toolbar

The toolbar is divided in to two areas

- Command Line. Refer to section the next section
- Graphical tools. Refer to section 3.3.4

3.3.3 NM menu

Figure 3-4: NM command line

The command line has 4 selections:

- File
- View
- Tools
- Help

3.3.3.1 File

Selecting File, two menus appear

- Options

  Selections available under the Options menu

  - Network

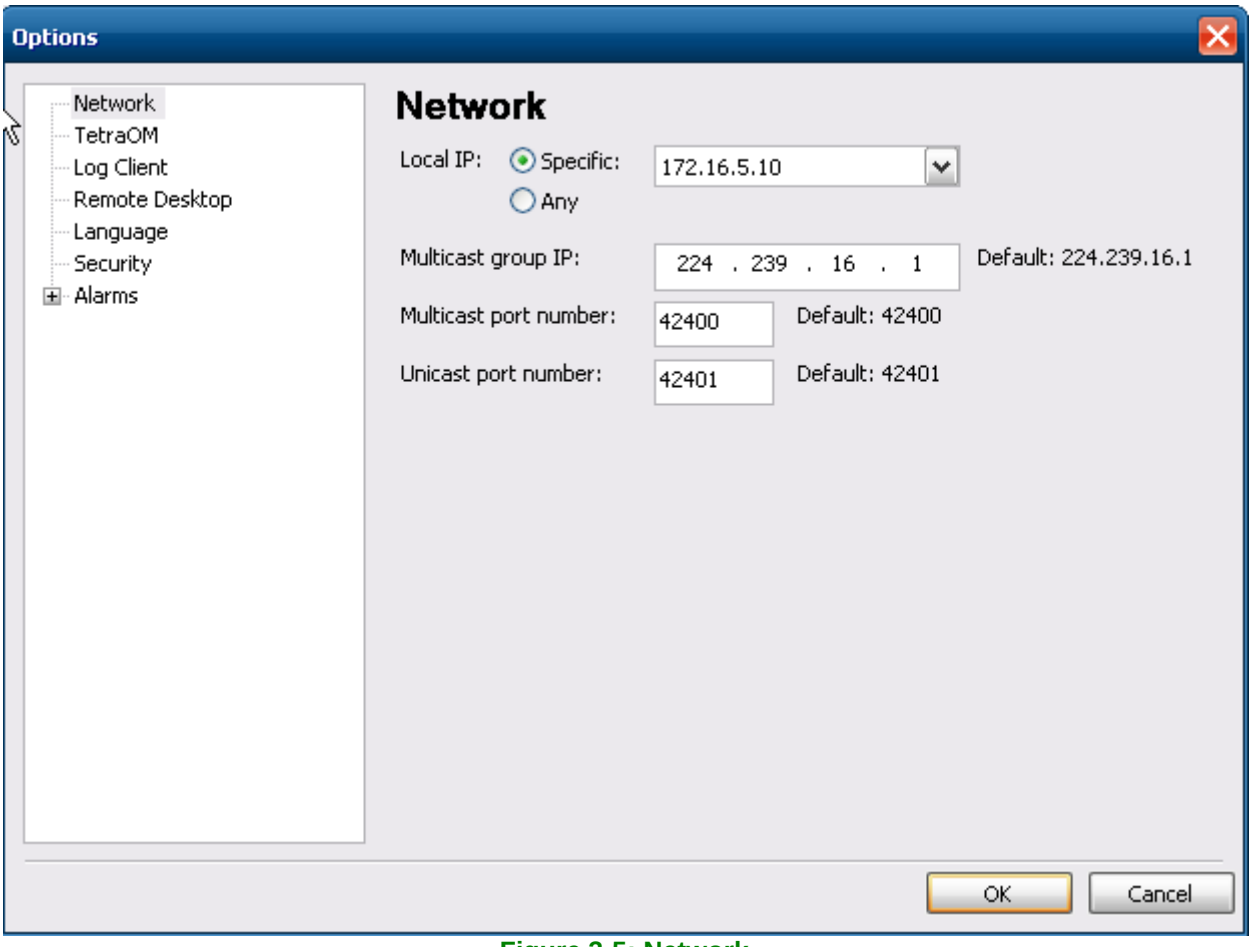


Figure 3-5: Network

The options menu allows the choice of Local IP, Multicast group IP and multicast port number. For multicast settings, please refer to the Multi Site IP networking manual.

As default the Local IP should be set to *Specific* and the LAN IP should be chosen.

- TetraOM

Specifies the path to the Tetra OM application

Figure 3-6: TetraOM path

- LogClient

Specifies the path to log client application

Figure 3-7: Log Client path setup

- Remote Desktop

Allows configuration of the Remote Desktop: Normally preconfigured

Figure 3-8: Remote desktop setup

- Language

When enabled in the dongle various languages can be selected for NM. Default is English.

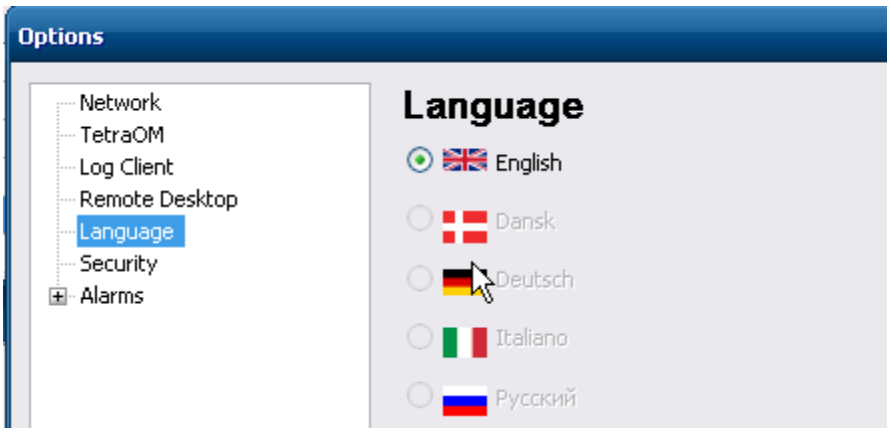


Figure 3-9: Language selection

- Security

There are two security setting that allows or disallows users to make change in System Parameters and Subscribers from NM

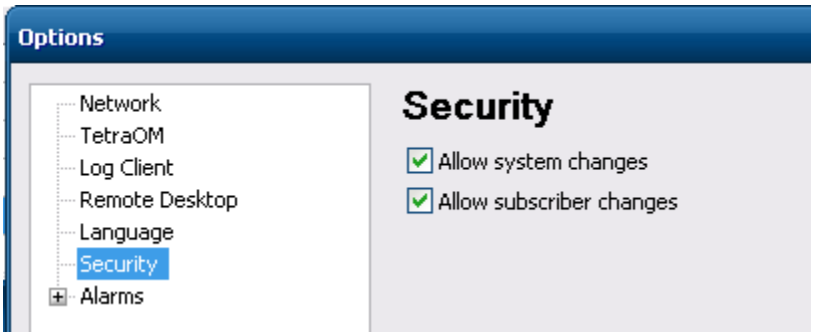


Figure 3-10: Security setting

- Alarms

Configuration of the wav files to be played when an alarm is present in NM

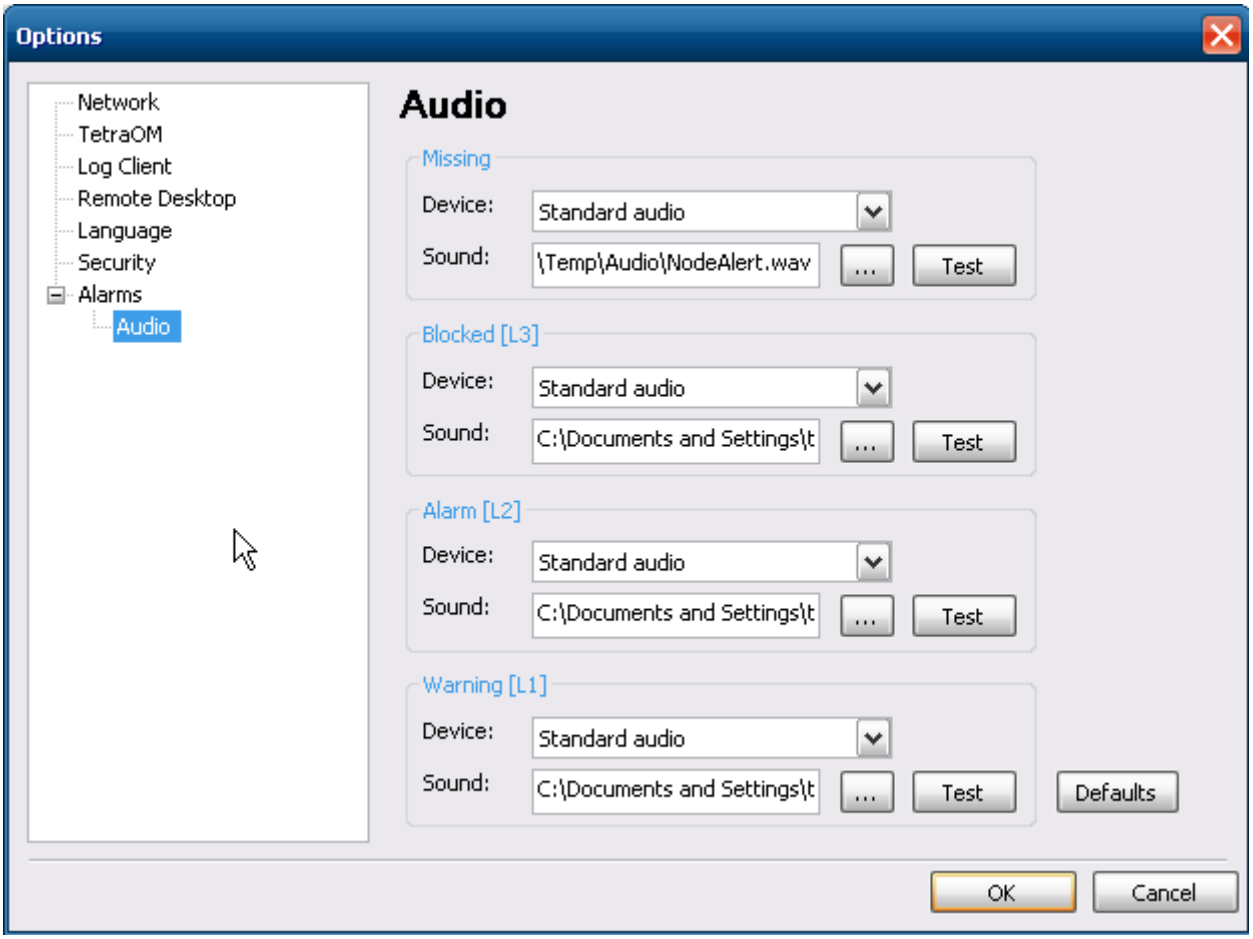


Figure 3-11: Alarm sound configuration

- Exit – Shuts down the application

3.3.3.2 View

The View option allows cascading of windows and selection/deselecting of the status bar in the bottom of the main window

3.3.3.3 Tools

The Tools option allows clearing alarms on all nodes

3.3.3.4 Help

General information regarding the NM version number and link refers to www.damm.dk.

3.3.4 Graphical tools for fast Access and information overview

Figure 3-12: Application select and alarms

The Graphical tool for fast selection has 7 access icons and 5 notifications

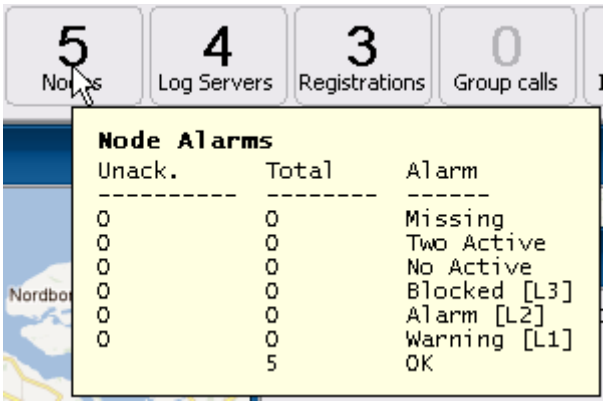
NOTE: the Node, Map, and Status windows are linked. This means that pointing to a node in one of the windows automatically changes the window to show the information's for chosen node.

3.3.4.1 Notification Icons

Four information icons are present on the graphical tool bar.

- Nodes* Number of nodes presently active
- Log Servers Number of Log Servers attached to the system
- Registrations Number of registered units on system
- Group calls Numbers of on-going Group calls
- Indv. Calls Numbers of on-going Individual calls

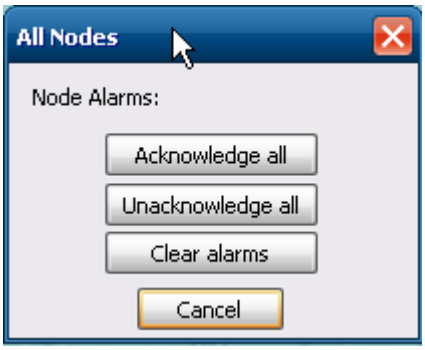
When moving the mouse to the Nodes field the actual status is shown:



- Missing Numbers of nodes with a missing alarm
- Two Active Numbers of nodes where 2 BSC are active at the same time
- No Active Numbers of nodes where no BSC are active
- L3 Blocked Number of level 3 blocking alarms present
- L2 Alarm Number of level 2 non-blocking alarms present
- L1 warning Number of level 1 warnings present
- Ok Number of nodes that are ok, without alarms

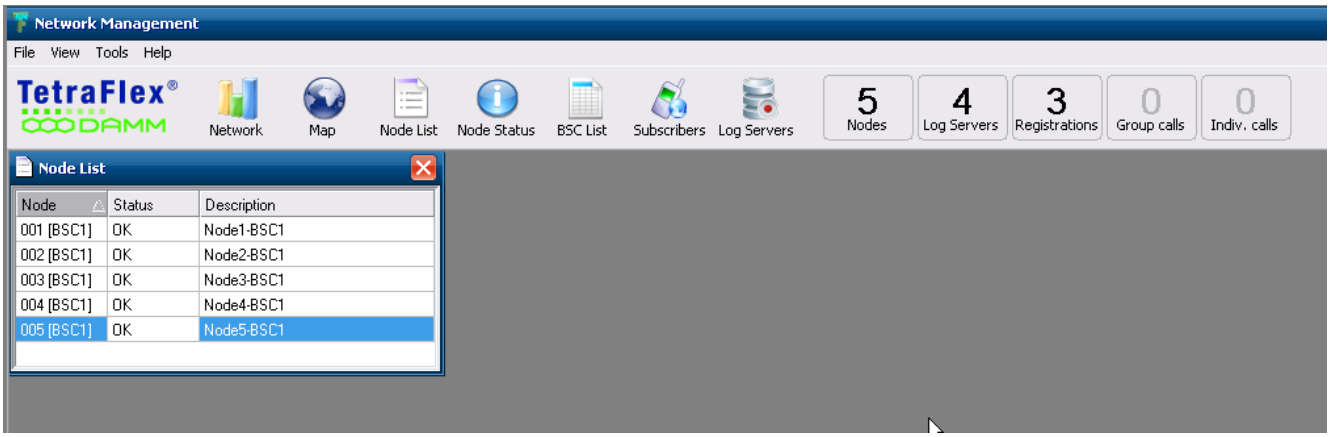
If one of or more Alarms are present the Nodes field turn into red and the alarm sound alerts. A yellow field indicates that one or more warning is/are present.

When right click on the Nodes status you get a dialog to handle alarms:



Ackowledge all: This acknowledges all alarms in the system
Unackowledge all: This unacknowledges all alarms in the system
Clear alarm: Clear all latched alarms in the system

3.3.4.2 Selection Icons



3.3.4.3 Nodes

The node window shows the general status and description of all nodes in the system When Left Mouse Click is executed on a node line, the Node Status window displays the chosen node. Redundant BSC's are not shown in the Node list but in the Node Status window and the BSC list window and the following commands are applicable for the redundant BSC as well if present:

If Right Mouse Click is executed on a node line in the Node List window, a new menu appears with several options:

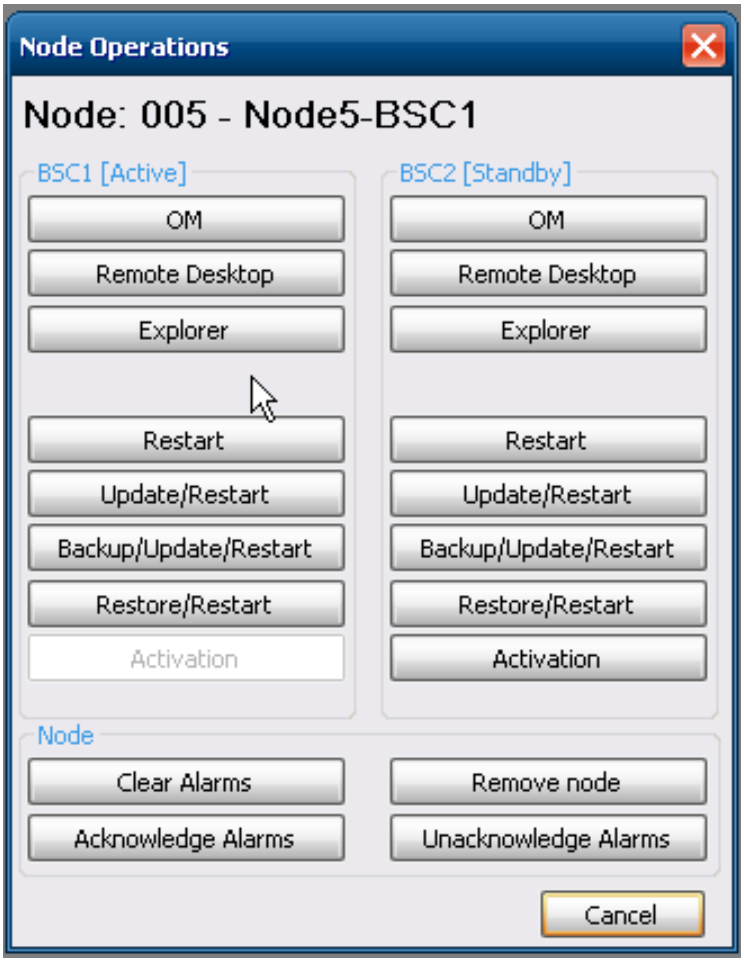


Figure 3-13: Node options showing Active and Standby BSC

- **OM** Start the TetraOM application
- **Remote Desktop** Start a remote Desktop session of the node
- **Windows Explorer** Starts Windows explorer with the address of the node

- **Restart** Restarts the node

- **Update/restart** updates the node with new SW previously deployed (*) to the…\Tetra\Update library and restarts the node

- **Backup/Update/restart** Backs up the node and the updates the node with new SW previously deployed (*) to the …\Tetra\Update library and restarts the node

- **Restore/restart** If Backup/Update/restart has been performed, this option will return to the configuration before the update was performed

(*) The software must be deployed to the ..\Tetra\Update folder in the right sub folder e.g. .. Tetra\Update\Pgm for updating the …\Tetra\Active\Pgm folder. Delete all previous version from the ..\tetra\update folder before updating.

- **Activation** Sets the node to Active
- **Remove node** If a node is deleted, but still active, the node will reappear in the list after a short time.
- **Clear alarms** Latched alarms may be cleared
- **Acknowledge** The alarm sound is shut off
- **Unacknowledged** Alarms Alarm Sound is turned back on

3.3.4.4 Status

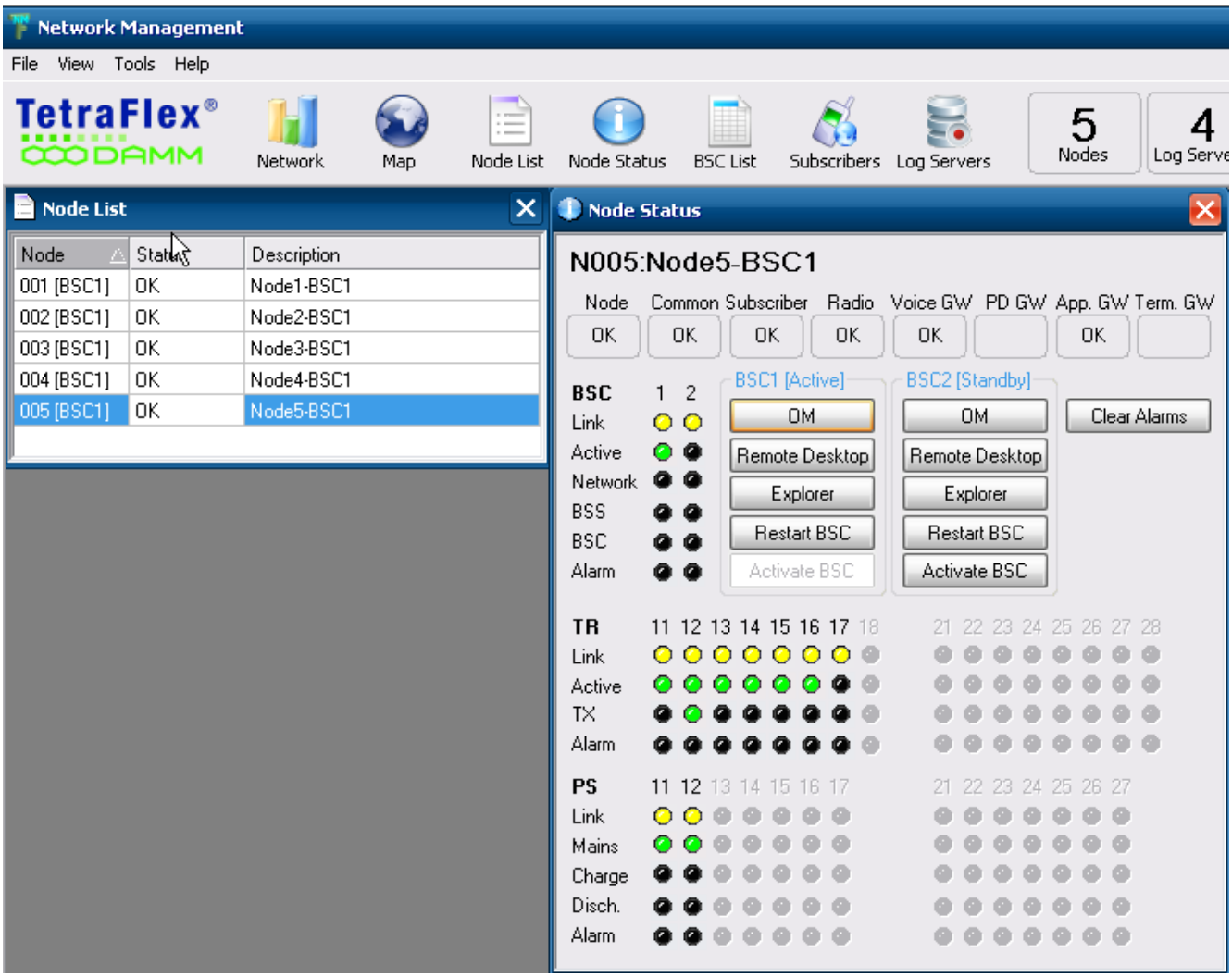


Figure 3-14: Status

The Status window shows the status and alarms for the node chosen in the Node List.

By pressing the specific buttons the window also allows direct connection to (please see the explanation in the previous chapter)

- TetraOM application
- Remote Desktop

- Windows Explorer
- Restart of the BSC.exe
- Clear alarms

And if a standby BSC.exe is present:

- Activation of a specific BSC.exe

3.3.4.5 Map

If connected to the internet, the map window will show Google Map with GPS positions of all registered nodes.

If the internet connection is not present, the map window will be inactive, but the system will continue working as defined.

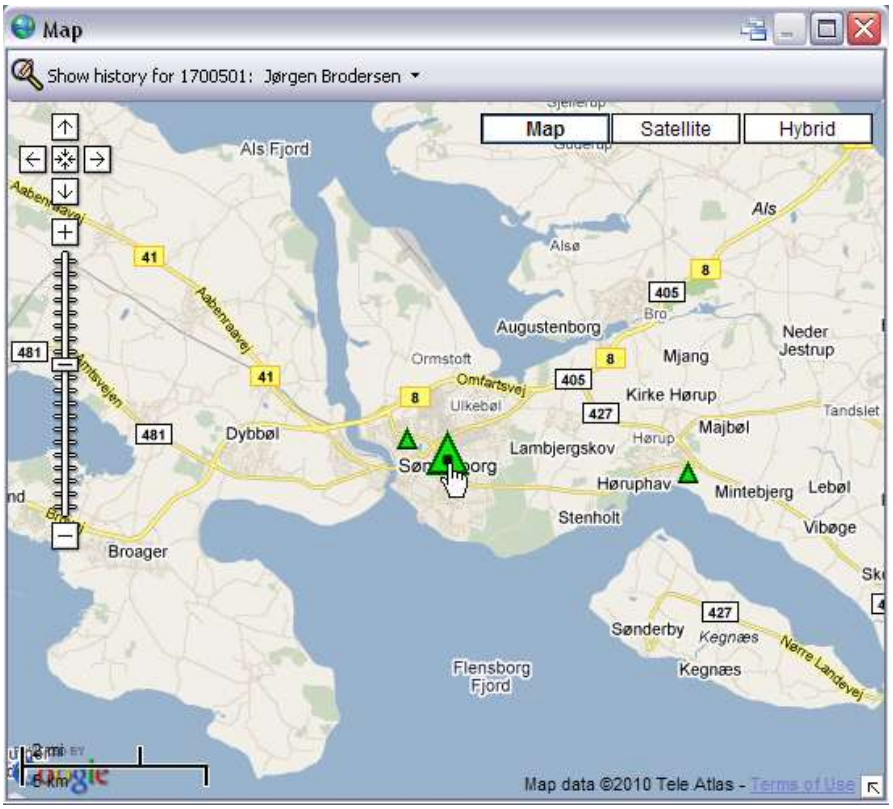


Figure 3-15: MAP

When Left Mouse Click on a node position, the Status and Node window displays information of the selected node.

The selected node will be displayed as 

If an alarm is present the node symbol will turn into red

3.3.4.6 BSC list

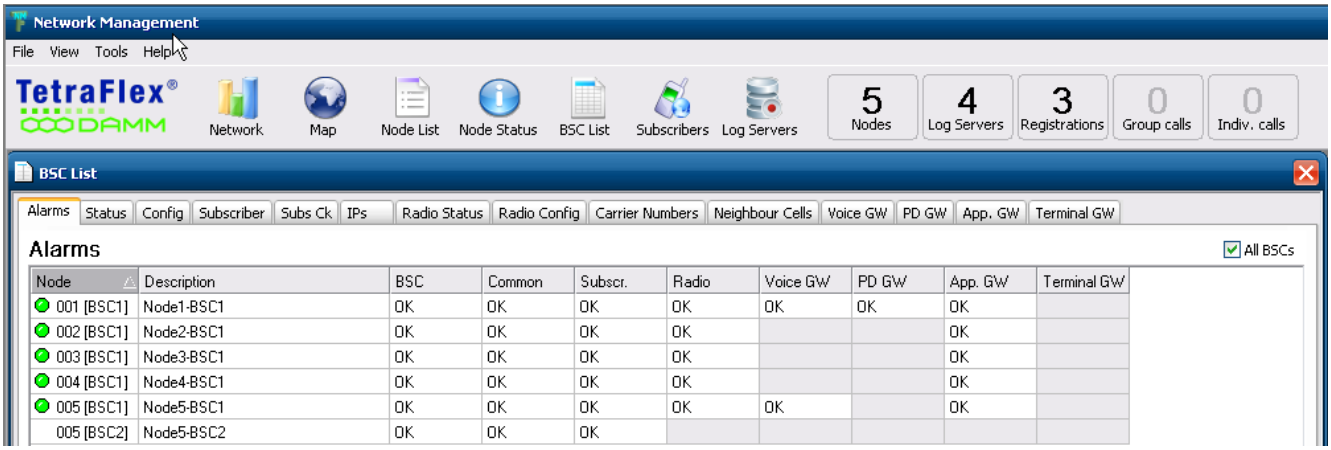
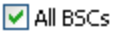
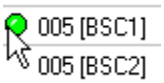


Figure 3-16: BSC List

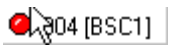
A number of information regarding the node may be chosen by the tabs in the top of the window. Information that are not grayed out may be reconfigured by selecting the appropriate fields using right or left mouse button.



This setting allows seeing and changing the BSC that is not active e.g. Redundant BSC



A green LED indicates a running BSC with no alarm and a BSC without a LED is not active (e.g. Redundant BSC).



A red LED indicates an alarm condition

3.3.4.6.1 Alarms

Indicates whether there is an active alarm present on a node and which component(s) the alarms applies to. The alarm can be Acknowledged and Unacknowledged by right clicking on the field.

3.3.4.6.2 Status

Right mouse click on the node description of a specific node allows a change of the node description.

Status selection also shows information's regarding:

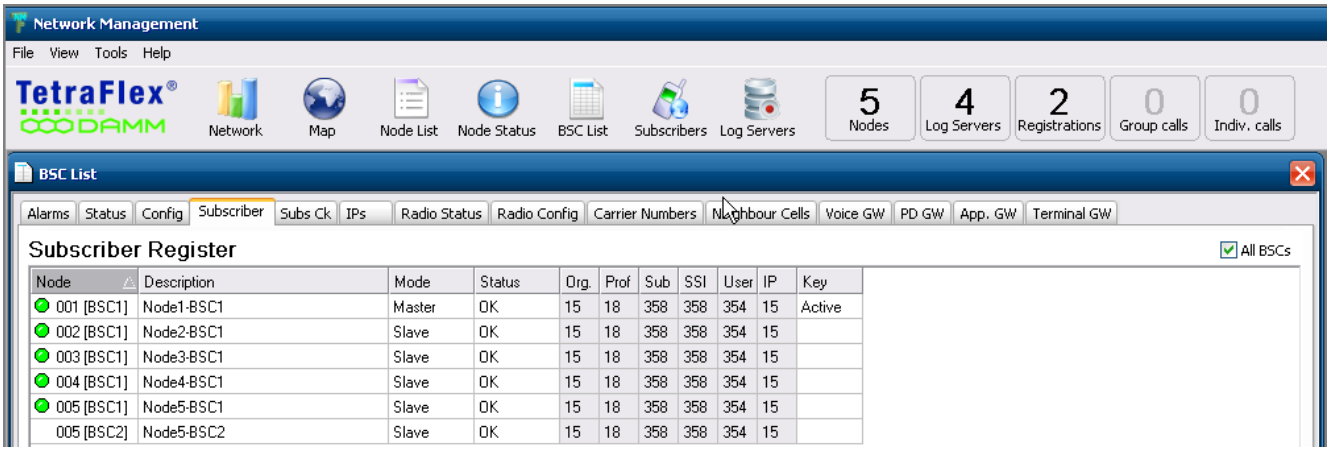
- HW type
- Software Version
- Dongle date limit
- Activation time
- Number of nodes
- Numbers of Log servers
- Last msg. – Last messages received date and time

3.3.4.6.3 Config

Right mouse click on the following items allows the change of the configurations.

- Description
  - Node description, E.g. In the format
  - "System-Node number-Placement" This description is collected and saved in the CnfgMain.txt file. This can also be changed via the BSC-GUI.
- MCC
  - Mobile Country Code. Please use the appropriate code for the country where the system is to be installed (saved in CnfgBss.txt)
- MNC
  - Mobile Network Code
  - NOTE: In certain countries this code must be supplied by the appropriate authorities (saved in CnfgBss.txt)
- GPS
  - If set to "Yes", the position shown on the map is set by the GPS receiver
  - If set to "No" Manual definition of the position is possible (saved in CnfgMain.txt)
- Latitude
  - Manual definition of the position latitude (saved in CnfgMain.txt)
- Longitude
  - Manual definition of the position longitude (saved in CnfgMain.txt)
- IP address Segment
  - The IP address segment used by the Packet Data Gateway to assign an IP to the PC attached to the terminals (saved in CnfgBss.txt)
- Timeout
  - The maximum time a call setup takes using the longest delay in the system.
  - Used to extend the node timeout: E.g. when using satellite connections with long delays (saved in CnfgBss.txt).
- Voice
  - Initial Voice Buffer Length (Voice Frames) – This field is to avoid jitter e.g. when using End to End encryption adds prox. 60 ms delay pr. Voice frame added (default factory setting is 2).

3.3.4.6.4 Subscriber



By right click the Mode-field in the subscriber tab the subscriber register mode type (Master, Slave and Stand-alone) will be chosen (saved in CnfgBss.txt):

Mode:

Master – Used on the node where subscribers will be maintained. The encryption Key Register must reside on this node. A redundant BSC must be set to the same mode as the Active BSC. Only one node can be Master at a time and changing the subscribers are only allowed from this node

Slave – All other nodes in the system

Stand-alone – For test and installation purposes

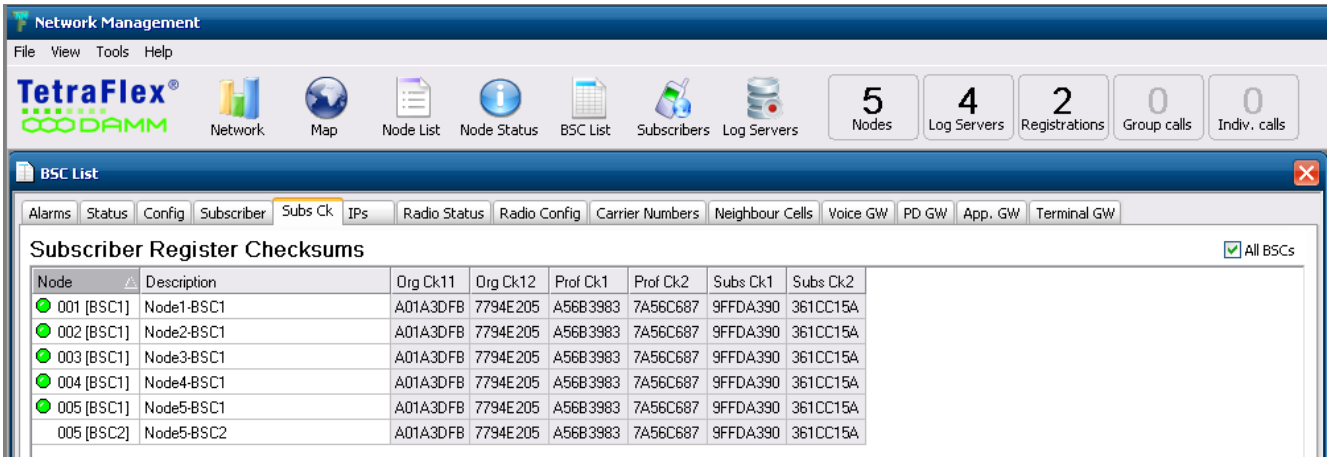
Key:

- Activation of the Security Key Register

Further information in grayed out fields refer to the count of the different subscriber types present in the subscriber register.

To see the non active BSC e.g. Redundant BSC the **All BSC's** flag must be set.

3.3.4.6.5 Sub. Chk



Node	Description	Org Ck11	Org Ck12	Prof Ck1	Prof Ck2	Subs Ck1	Subs Ck2
001 [BSC1]	Node1-BSC1	A01A3DFB	7794E205	A56B3983	7A56C687	9FFDA390	361CC15A
002 [BSC1]	Node2-BSC1	A01A3DFB	7794E205	A56B3983	7A56C687	9FFDA390	361CC15A
003 [BSC1]	Node3-BSC1	A01A3DFB	7794E205	A56B3983	7A56C687	9FFDA390	361CC15A
004 [BSC1]	Node4-BSC1	A01A3DFB	7794E205	A56B3983	7A56C687	9FFDA390	361CC15A
005 [BSC1]	Node5-BSC1	A01A3DFB	7794E205	A56B3983	7A56C687	9FFDA390	361CC15A
005 [BSC2]	Node5-BSC2	A01A3DFB	7794E205	A56B3983	7A56C687	9FFDA390	361CC15A

Shows the two distinct checksums calculated for the Organization (Org Ckx), Profile (Prof Ckx) and Subscriber registers (SubsCkx). If the checksums of all nodes are equal the subscriber registers for all nodes are synchronized.

To see the not active BSC e.g.. Redundant BSC the **All BSC's** flag must be set.

3.3.4.6.6 IP's

Node	Description	LAN	WAN	Red. LAN	Red. WAN	Log Server	Log Server Port
001 [BSC1]	Node1-BSC1	172.16.1.10	10.239.24.121			224.239.17.1	42402
002 [BSC1]	Node2-BSC1	172.16.2.10	[illegible]			224.239.17.1	42402
003 [BSC1]	Node3-BSC1	172.16.3.10	10.239.24.123			224.239.17.1	42402
004 [BSC1]	Node4-BSC1	172.16.4.10	10.239.24.124			224.239.17.1	42402
005 [BSC1]	Node5-BSC1	172.16.5.10	10.239.24.125	172.16.5.19	10.239.28.98	224.239.17.1	42402
005 [BSC2]	Node5-BSC2	172.16.5.19	10.239.28.98	172.16.5.10	10.239.24.125	224.239.17.1	42402

Right mouse click on the following items allows change of the configurations.

- Log Server
  - Log server Multicast control (receiving) IP address (default 224.239.17.1)
  - Log Server Multicast port (default 42400)

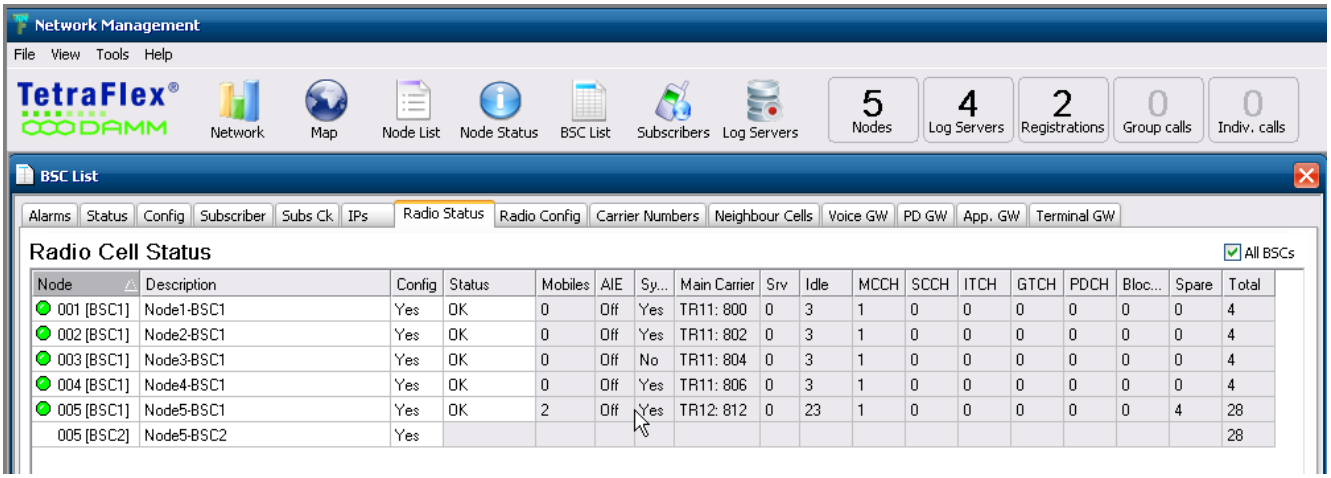
The following is information only (please see the chapter BSC_GUI to make changes)

- LAN
  - LAN IP address
- WAN
  - WAN IP address

- Red. LAN
  - Redundant LAN IP address

- Red. WAN
  - Redundant WAN IP address

3.3.4.6.7 Radio Status



Node	Description	Config	Status	Mobiles	AIE	Sy...	Main Carrier	Srv	Idle	MCCH	SCCH	ITCH	GTCH	PDCH	Bloc...	Spare	Total
001 [BSC1]	Node1-BSC1	Yes	OK	0	Off	Yes	TR11: 800	0	3	1	0	0	0	0	0	0	4
002 [BSC1]	Node2-BSC1	Yes	OK	0	Off	Yes	TR11: 802	0	3	1	0	0	0	0	0	0	4
003 [BSC1]	Node3-BSC1	Yes	OK	0	Off	No	TR11: 804	0	3	1	0	0	0	0	0	0	4
004 [BSC1]	Node4-BSC1	Yes	OK	0	Off	Yes	TR11: 806	0	3	1	0	0	0	0	0	0	4
005 [BSC1]	Node5-BSC1	Yes	OK	2	Off	Yes	TR12: 812	0	23	1	0	0	0	0	0	4	28
005 [BSC2]	Node5-BSC2	Yes															28

Shows the resources used on the nodes

- Config - shows if the Radio cell(s) are configured or not. By right click on the field the radio cell (s) can be set to configured Yes and No

- Status – Shows the actual status – By right click you may acknowledge an unacknowledged alarm

- Mobiles - Number of mobiles presently registered at the node

- MCCH – Main Control Channel (by right click you can see the appropriate frequency)

- AIE – Air interface Encryption off/on

- Sync – Neighbor Cell Synchronization. Shows Yes or No depending on the Sync. setting in Radio Config (see next chapter)

- Srv - Service level – (not enabled at the moment always 0)

- Idle - Number of idle channels (Timeslots)

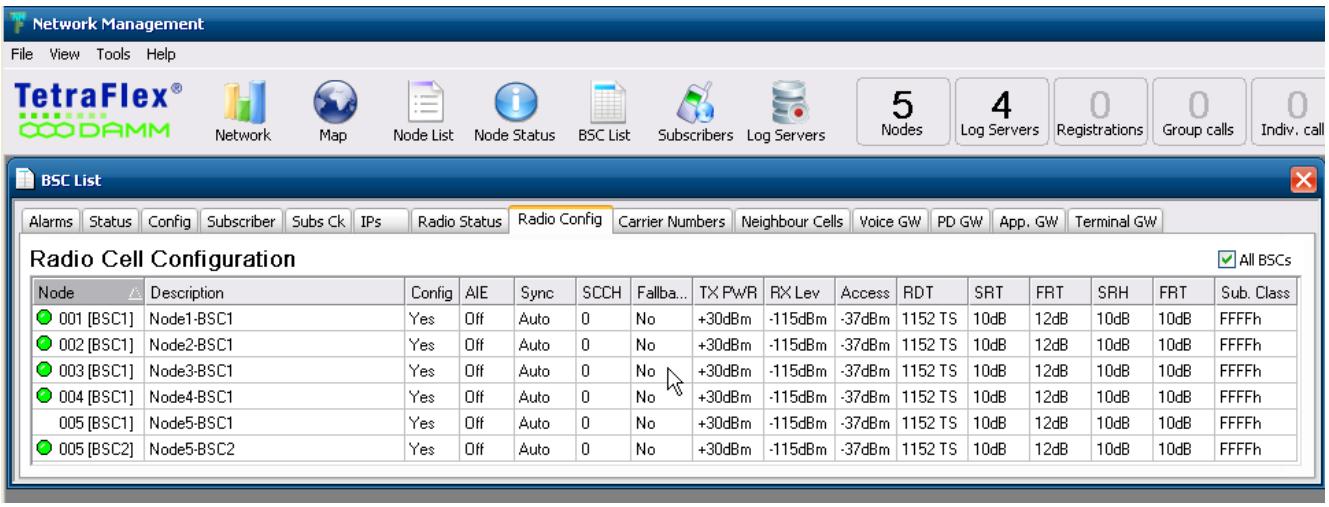
- MCCH – Active Main Control Channel count – number of control timeslots used

- SCCH - Secondary Control Channel Count – numbers of sec. control timeslots used

- ITCH - Individual Traffic Channel Count – numbers of timeslots used for duplex calls
- GTCH - Group Traffic Channel Count- numbers of timeslots used for simplex calls
- PDCH - Packet Data Channel Count-numbers of timeslots used for packet data
- Block - Number of blocked channels (timeslots)
- Spare - Number of Spare channels (timeslots)
- Total - Total Number of channels (timeslots)

A button allows the view to shift between All Nodes and Active Cells

3.3.4.6.8 Radio Config



Node	Description	Config	AIE	Sync	SCCH	Fallba...	TX PWR	RX Lev	Access	RDT	SRT	FRT	SRH	FRT	Sub. Class
001 [BSC1]	Node1-BSC1	Yes	Off	Auto	0	No	+30dBm	-115dBm	-37dBm	1152 TS	10dB	12dB	10dB	10dB	FFFFh
002 [BSC1]	Node2-BSC1	Yes	Off	Auto	0	No	+30dBm	-115dBm	-37dBm	1152 TS	10dB	12dB	10dB	10dB	FFFFh
003 [BSC1]	Node3-BSC1	Yes	Off	Auto	0	No	+30dBm	-115dBm	-37dBm	1152 TS	10dB	12dB	10dB	10dB	FFFFh
004 [BSC1]	Node4-BSC1	Yes	Off	Auto	0	No	+30dBm	-115dBm	-37dBm	1152 TS	10dB	12dB	10dB	10dB	FFFFh
005 [BSC1]	Node5-BSC1	Yes	Off	Auto	0	No	+30dBm	-115dBm	-37dBm	1152 TS	10dB	12dB	10dB	10dB	FFFFh
005 [BSC2]	Node5-BSC2	Yes	Off	Auto	0	No	+30dBm	-115dBm	-37dBm	1152 TS	10dB	12dB	10dB	10dB	FFFFh

Allows configuration of the different radio parameters (per node or system). Right mouse click on the following items allows change of the configurations.

- Config – Transmitter configured Yes or No
- AIE - Air Interface Encryption Off or On
- AIE - Air Interface Encryption activated Yes/No
- Sync - Handover settings. Auto/Yes/No. Auto means: automatically sync. setting e.g. GPS sync. Sync. must be enabled on each node to make seamless handover.
- SCCH - Setup of 1 to 3 secondary control channels (SCCH)
- Fallback - System sends fallback information to the MS. If set to Yes (and Depending on the MS programming) this can be used for the MS to decide to change to a different node that has full service available even if the RSSI level is lower.
- TX PWR - Maximum Mobile Station TX power allowed (not TR output power!)
- RX Lev - Minimum Mobile Station RX access level before leaving a node. During initial scanning, the MS scans for downlink signals and takes this value from the broadcast. Then it checks if the received downlink signal is above this value before it registers to the node. If during the operation the received downlink signal drops

below this level, it leaves the node again without any deregister signaling, and it goes into scanning and checks for a node with better signal.

- Access - Radio access parameter -53dBm to -23dBm. This, to reduce the MS output power depending on how close it is to the radio node. The ETSI defines it like this: $P = \text{MIN}(\text{MS\_TXPWR\_MAX\_CELL}, \text{ACCESS\_PARAMETER} - \text{RSSI})$
- This means that a) the MS never chooses an output power above MS_TXPWR_MAX and b) the output power depends on the downlink signal strength RSSI in combination with ACCESS_PARAMETER. The idea is simple: If the MS is close to the BS, it can reduce its output power. ACCESS_PARAMETER defines how much it can reduce it.

  Example: MS_TX PWR = 30dBm, ACCESS = -30dBm
  MS is far away from the radio cell, RSSI=-105dBm.

  P=MIN(30dBm, -30Bm-(-105dBm) = MIN(30dBm, 75dBm) = 30dBm MS transmits full power.

  MS is very close to BS, RSSI=-55dBm.

  P=MIN(30dBm, -30Bm-(-55dBm) = MIN(30dBm, 25dBm) = 25dBm MS transmits with reduced power.

  The value of -53dBm maximizes the effect of power reduction:
  P=MIN(30dBm, -53Bm-(-55dBm) = MIN(30dBm, 2dBm) = 2dBm MS transmits with very reduced power.

  The value of -23dBm minimizes the effect of power reduction:
  P=MIN(30dBm, -23Bm-(-55dBm) = MIN(30dBm, 32dBm) = 30dBm No power reduction yet.

- RDT - Radio Downlink Timeout: This it is a measurement of the downlink quality. The higher the RDT value is, the longer the MS stays on a channel with bad quality. Factory setting middle value (1152TS).

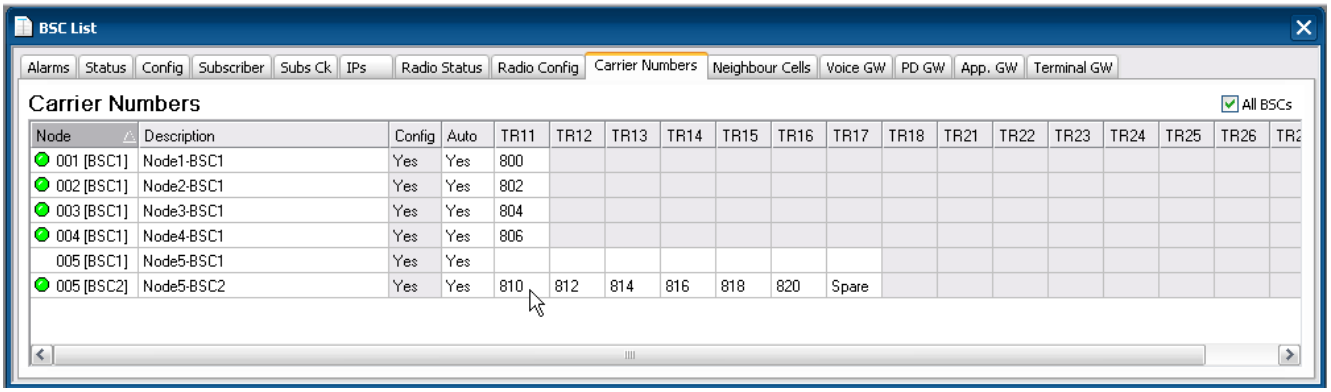
- SRT - Slow Reselect Threshold above fast (Factory setting 10dB)
- FRT - Fast Reselect Threshold (Factory setting 12dB)
- SRH - Slow Reselect Hysteresis (Factory setting 10dB)
- FRH - Fast Reselect Hysteresis (Factory setting 10dB)

The parameters **SRT,FRT,SRH** and **FRH** are for network planning and are defining the behavior of MS cell reselection in a multi node system. The parameters are explained in details in the ETSI EN 300 392-2 is chapt. 18.3.4.4 ”Ranking of neighbour cells” And 18.3.4.5.x “Criteria used during cell reselection”:

Unless there is trouble with MS cell reselection the factory settings should not be changed.

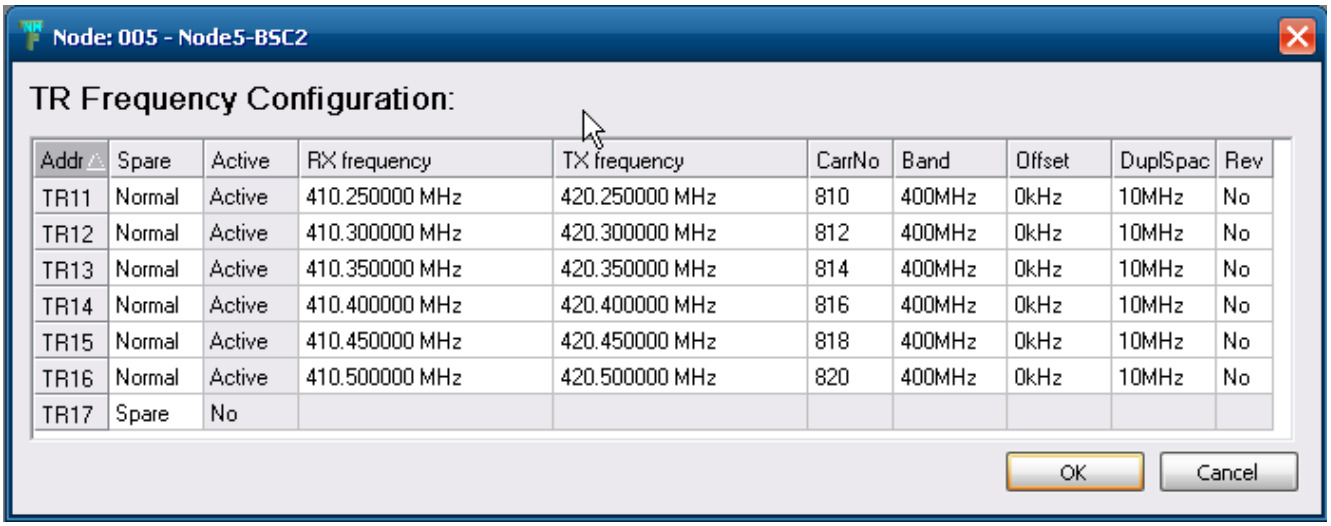
- Sub. Class - Subscriber Class (Class 1-16 , default all class present).These parameters can be programmed in the MS to match the bit pattern of a radio cell to obtain a preferred radio cell to connect to.

3.3.4.6.9 Carrier Numbers



- Auto – Auto convert primitives and frequencies – “Yes” the freq. and carrier number go together – “No” the freq. and carrier number can be set independent of each other.

By right click on TRxx carrier number the TR Frequency Configuration window comes up:



- Spare – Preferred to set to Normal TR operation or TR Hot spare witch in case of a TR fault will switch to the spare TR (with the same Freq. settings)
- RX frequency – Receive Frequency setting *
- TX frequency – Transmit Frequency setting *
- CarrNo – Carrier Number Allows configuration of the carrier number on the node. The carrier number is related to the frequency band selected in the radio configuration menu. E.g. FreqBand: 400Mhz and Carrier number: 800 gives Tx freq. = 420,00 Mhz (800x25khz+400Mhz= 420Mhz)
- Band - Base frequency band
- Offset - Frequency offset (default 0 kHz)
- DuplSpace - Duplex spacing (default 10 Mhz)
- Rev – No: Definition of standard (TX highest) or Yes: Reverse (TX lowest) operation

*) If the auto convert flag is set, then only freq. which are derivable from Tetra primitives are allowed (follows Carrier Number).

3.3.4.6.10 Neighbor cells

Configure the neighbor cells as auto (recommended for small systems covering a uniform area) or manual (recommended for larger systems or small systems covering a line, ex, a highway or a railway etc.

Right mouse click on the following items allows change of the configurations.

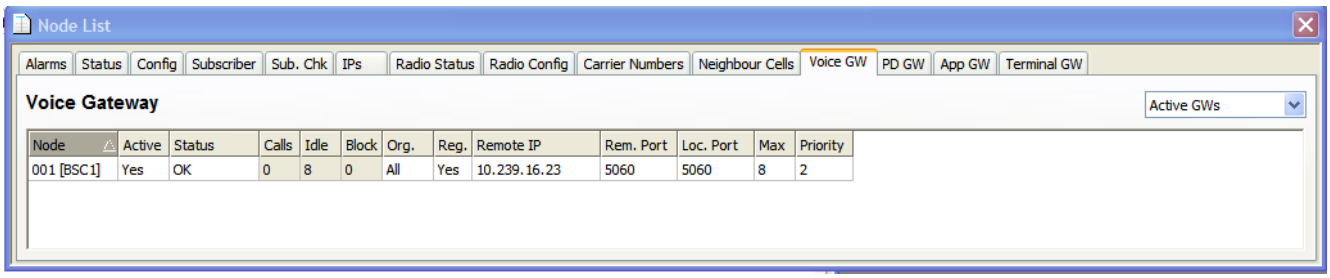
- Mode
  - Change between “Auto (All cells)” and “Selected cells only”
- N1 to N16
  - Neighbor cell setup for the specific node

The following is information only

- Active
  - Activation status of the cell

The drop down Active Radio cells / All nodes changes between display of active nodes only, or both active and not active nodes

3.3.4.6.11 Voice GW



Right mouse click on the following items allows change of the configurations.

- Active — Activation of GW (yes or No)
- Org. — Gateway organization number that are allowed
- Reg. — Selection if GW should register at the SIP device or not
- Remote IP — IP address of SIP device
- Rem. Port — Remote port number. Default 5060
- Loc. Port — Local port number. Default 5060

- Max. — Restriction of simultaneous calls. Must be equal or less than defined in the dongle
- Priority — Priority of Voice GW calls (0-15)

The following is information only:

- Status — Status of GW functions. By right mouse click you can also acknowledge and unacknowledge alarms
- Call — Number of present calls
- Idle — Number of free GW
- Block — Number of blocked GW

The drop down box “Active GWs” / “All nodes” changes between display of active nodes only, or both active and not active nodes. See also section *2.11 Voice Gateway* for Voice Gateway configuration.

3.3.4.6.12 SIP Setup

This setup describes the configuration needed to setup the system for SIP operation

The PABX samples are shown for the Innovaphone IP800, but may be any SIP compatible device. Please consult the user manual and technical staff for the device in question.

The TetraFlex system needs at least one Voice Gateway configured on any node available to operate with a PABX.

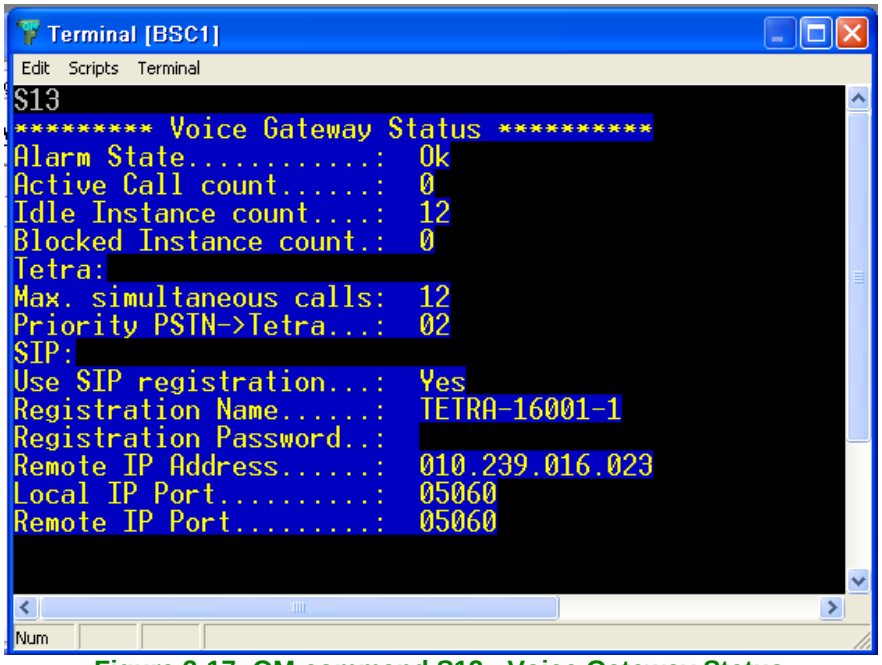


Figure 3-17: OM command S13 - Voice Gateway Status

To configure a Voice Gateway, use the NM application or use the TetraOM as described here (SIP registration name and password can only be set by OM commands):

- The SIP registration name (Alias) must be unique and can be generated by the OM command "**S73/NAME/<SIP registration name>". e.g. "S73/NAME/TETRA-16001-1**". You can also set registration name with the BSCGui-BSS VoiceGW The name must be entered as the SIP Alias name into the PABX as well.

- The SIP registration password is optional and can be generated by the OM command "**S73/PASSWORD/<password>". e.g. "S73/NAME/"** (blank means no password). You can also set the Password with the BSCGui BSS VoiceGW. The password must be entered into the PABX as well.

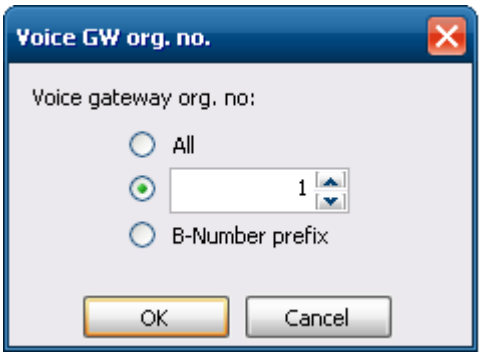
- The Voice GW must be assigned a node number to attach to. This can be setup in NM - Subscriber register in the various profiles where PABX access is wanted or by using the TetraOM command **S21/"Profile No"/VGNODE/"x"/"Node Number**" Where x is 1 for primary GW and x is 2 for alternate GW.

- SIP registration must be set to YES, use NM or TetraOM command **S73/REG/+**

- Remote IP address is the IP of the Voice GW (e.g. IP800). Use NM or TetraOM command **S73/IPADDR/xxx.xxx.xxx.xxx**

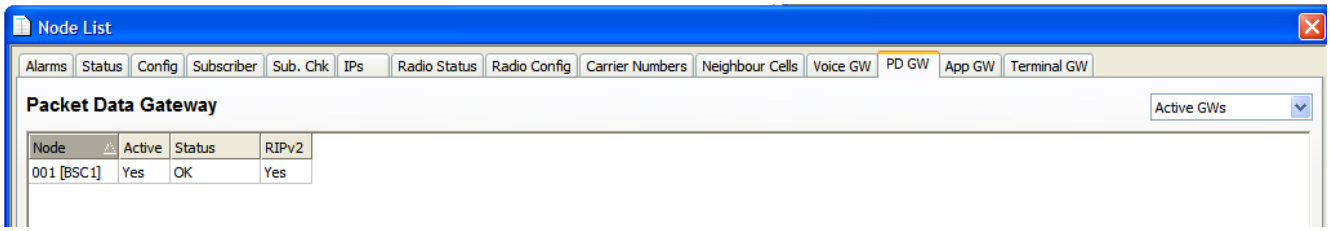
- Voice GW must be activated. Use NM or TetraOM command **73/CNFG/+**

- Organization – can be set to allow all or some organization to make call to trough the Voice GW.



  - All – all organizations are allowed
  - If you specifies an organization ex. 1 only this is allowed
  - B- number prefix, The Org. number for the subscriber is set in front of the dialing number so that the PABX can route this according the org. number.

3.3.4.6.13 PD GW



Note: Use of Packet Data GW's must be set in the Node Dongle.

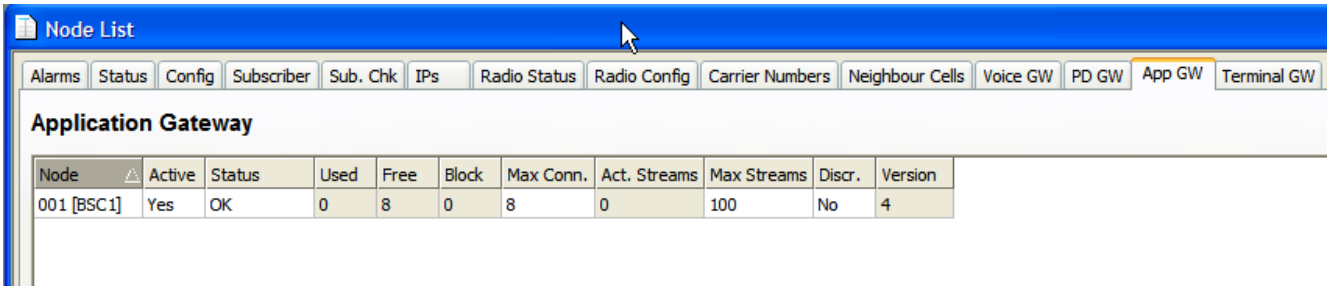
Right mouse click on the following items allows change of the configurations.

- Active - Gateway activated (can be deactivated by right clicking)
- Status – Right click to acknowledge or unacknowledge alarms
- RIPv2 – "Yes" RIPv2 is used – "No" Static routing is used

A drop down box allows the view to shift between All Nodes and Active Cells

For details on the Packet Data configuration please see section *2.12 Packet Data* Gateway.

3.3.4.6.14 App GW



Note: Number of application GW's must be set in the Node Dongle and API dongle must be present in the client PC. DAMM Dispatcher application uses the application GW and uses one connection. To run the Dispatcher a Dispatcher dongle must be present in the PC where the dispatcher is running.

Right mouse click on the following items allows changing the configurations.

- Active - Gateway activated (can be deactivated by right clicking)
- Max - Max connection count, can be changed by right click on it up to the max. in the dongle.

- Discr. – Discreet listening enables or disables discreet listening on the Application gateway e.g. used in the dispatcher.

The following is information only

- Status
  - Used - Used connection counts
  - Free - Free connection counts
  - Block - Blocked connection counts
  - Ver. -Protocol version

A drop down box allows the view to shift between All Nodes and Active Cells

For details of the API configuration please see section *2.13* Application Gateway for setup of the gateway. For details about the API itself, please refer to the .h document and to the API tool box application.

.

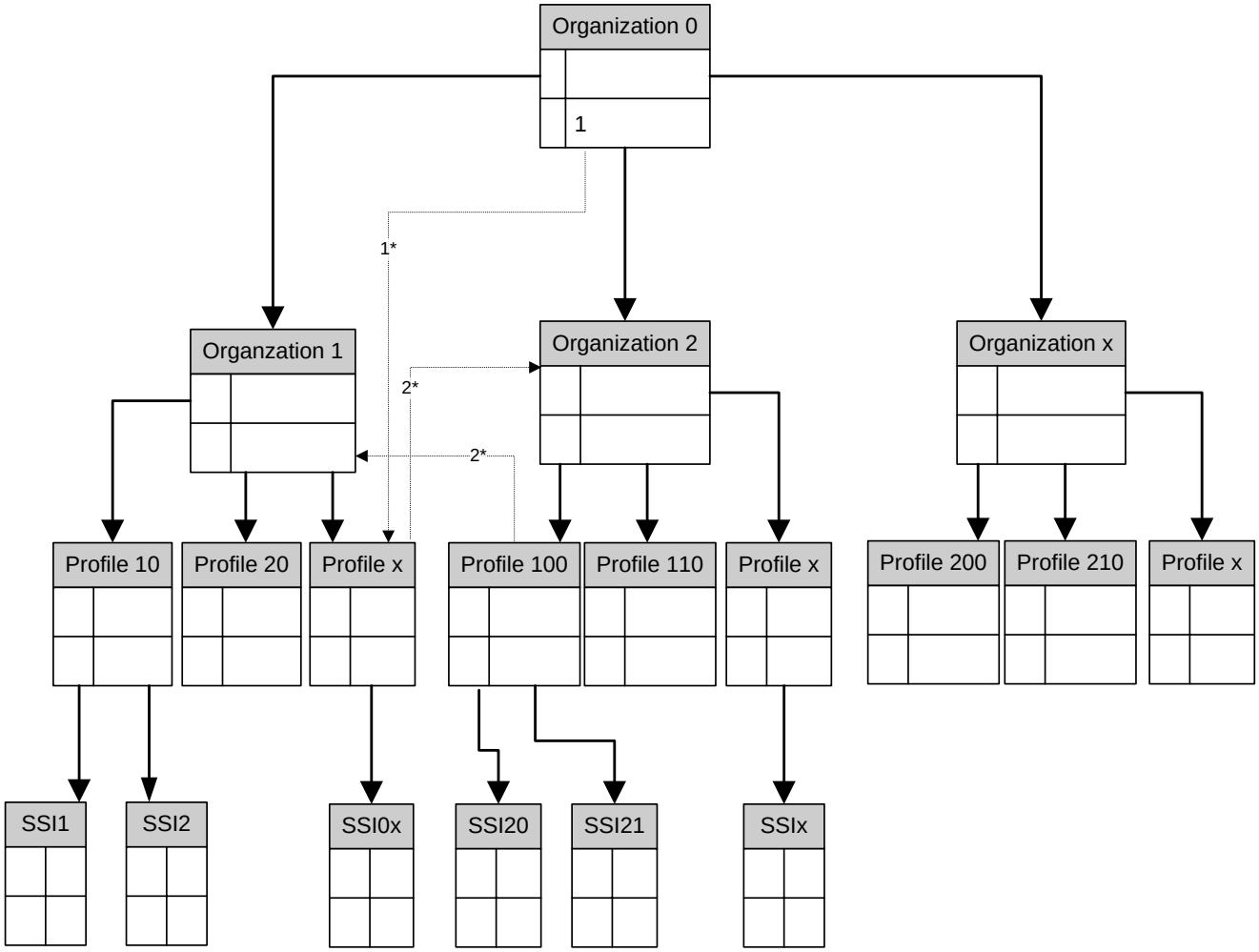
3.3.5 Subscribers

3.3.5.1 Subscriber definition

The subscriber window is divided in to 4 parts

- Organization (Maximum 1000 organizations)
- Profile (Maximum 2.000 profiles standard and 10.000 in optional enhanced ver.)
- Subscriber (Maximum 20.000 subscribers and 150.000 in Optional enhanced ver.)
- Sec. Key (Security Key Update)

The relation between Organization, profile and SSI is shown in this drawing:

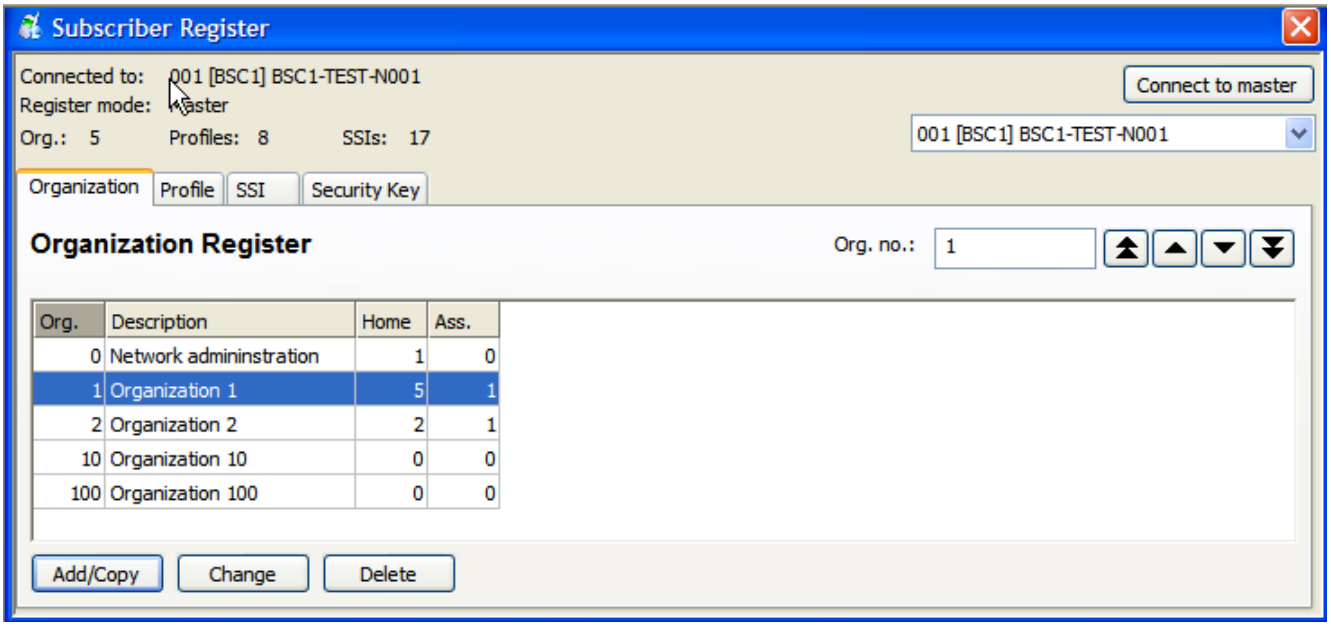


A SSI is related to one Profile and a profile is related to one Organization.

1. A Profile can also be connected to org 0.
2. A profile can also be associated to different organization (see “Profile” - “Associated organizations”).

3.3.5.2 Organization

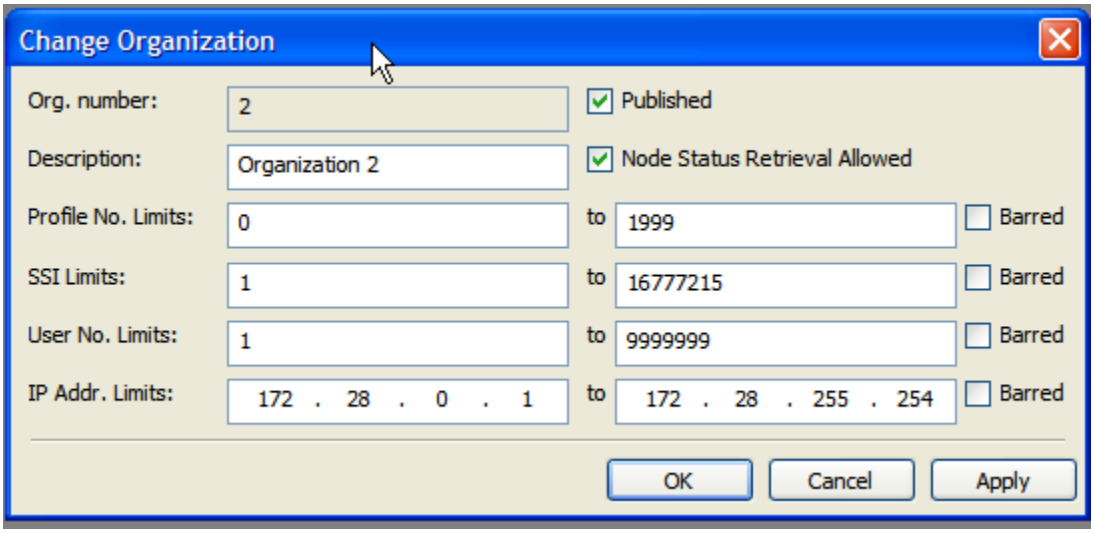
The TetraFlex® System enables several organizations to share one TETRA Network as each of these organizations can use the services as if they were the sole user of the network. The radio users, groups, and call rights within each user organization can be controlled independently.
Organization 0 is intended for the network operator and this Org. can “see” all other organizations. It is also possible to connect Profile/SSI to org. 0, but this should only be used for network administration purpose or as the “master” or “Home” organization.



The main window allows the user to Add/Copy a new organization, change an existing organization or delete an organization.

Add/Copy and Change functions are similar except that in the Change function the organization number cannot be accessed.

By double click on an organization or push the button “Change” the Change Organization dialog comes up:



- Org. Number: The number of the organization. This must be unique and at least org. 0 must always be present. If connecting an API Application or the Dispatcher to org. 0 it is possible to change all org. settings from this application.

- Description: Is a free text field for organization description

- Published: If checked the organization is published towards all API applications and the Dispatcher even if they are not a member of this organization. API applications and the dispatcher always get the organization properties for the organization they are connected to.

- Node Status Retrieval Allowed: If checked the Node status can be shown on a API application and the Dispatcher

- Profile No. Limits: If barred is checked, no profile can be generated from an API application or the dispatcher. Existing profiles can always be edited. New profiles must be within this range.

- SSI Limits: If barred is checked no SSI can be generated from an API application or the dispatcher. Existing SSI can always be edited. New SSI must be within this range.

- User No. Limits: If barred is checked no user no. can be generated from an API application or the dispatcher. Existing User no. can always be edited. New User no. must be within this range.

- IP Addr. Limits: If barred is checked no IP address can be generated from an API application or the dispatcher. Existing IP addresses can always be edited. New IP addresses must be within this range.

3.3.5.3 Profile

It is recommended to use breaks in the profile number series e.g. 100, 110 … 200, 210, and so on, as profile number. This will make it possible to create sub-profiles if needed.

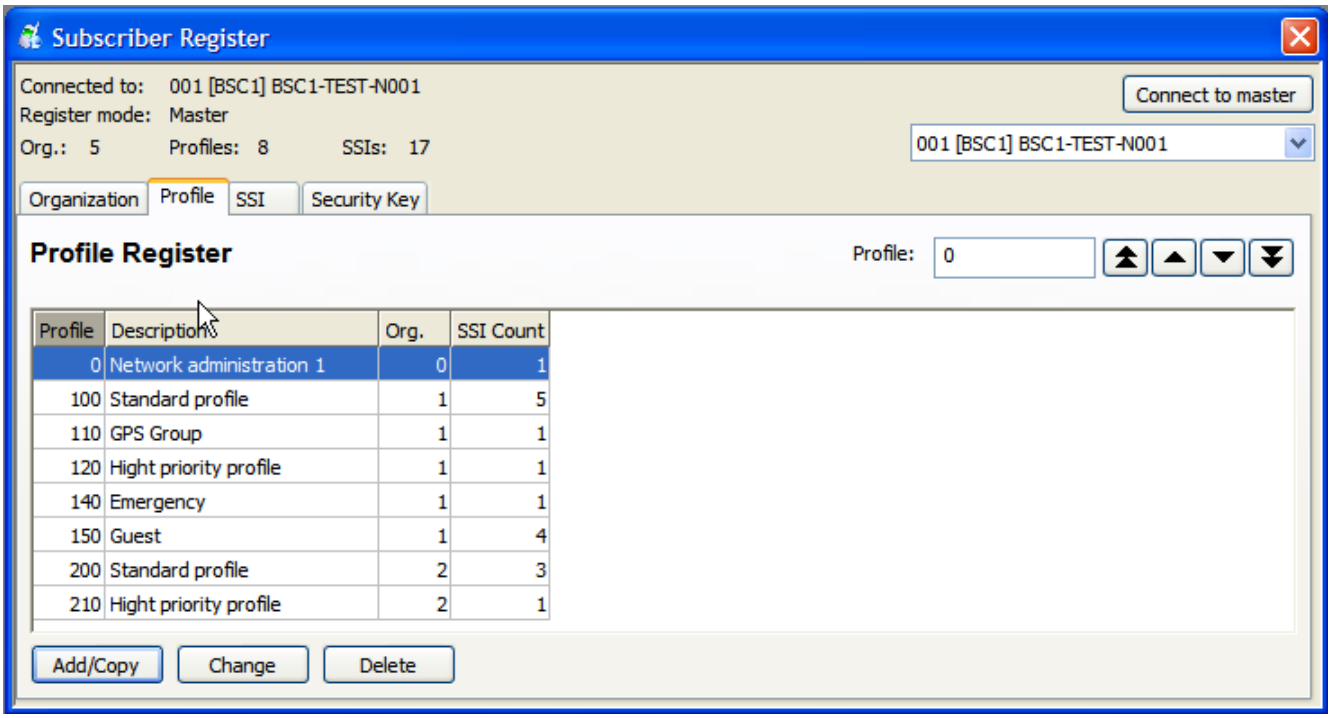


Figure 3-18: Subscriber Profile

The main window allows the user to Add/Copy a new profile, change an existing profile or deleting a profile.

Add/Copy and Change functions are similar except that in the Change function in the profile number cannot be accessed

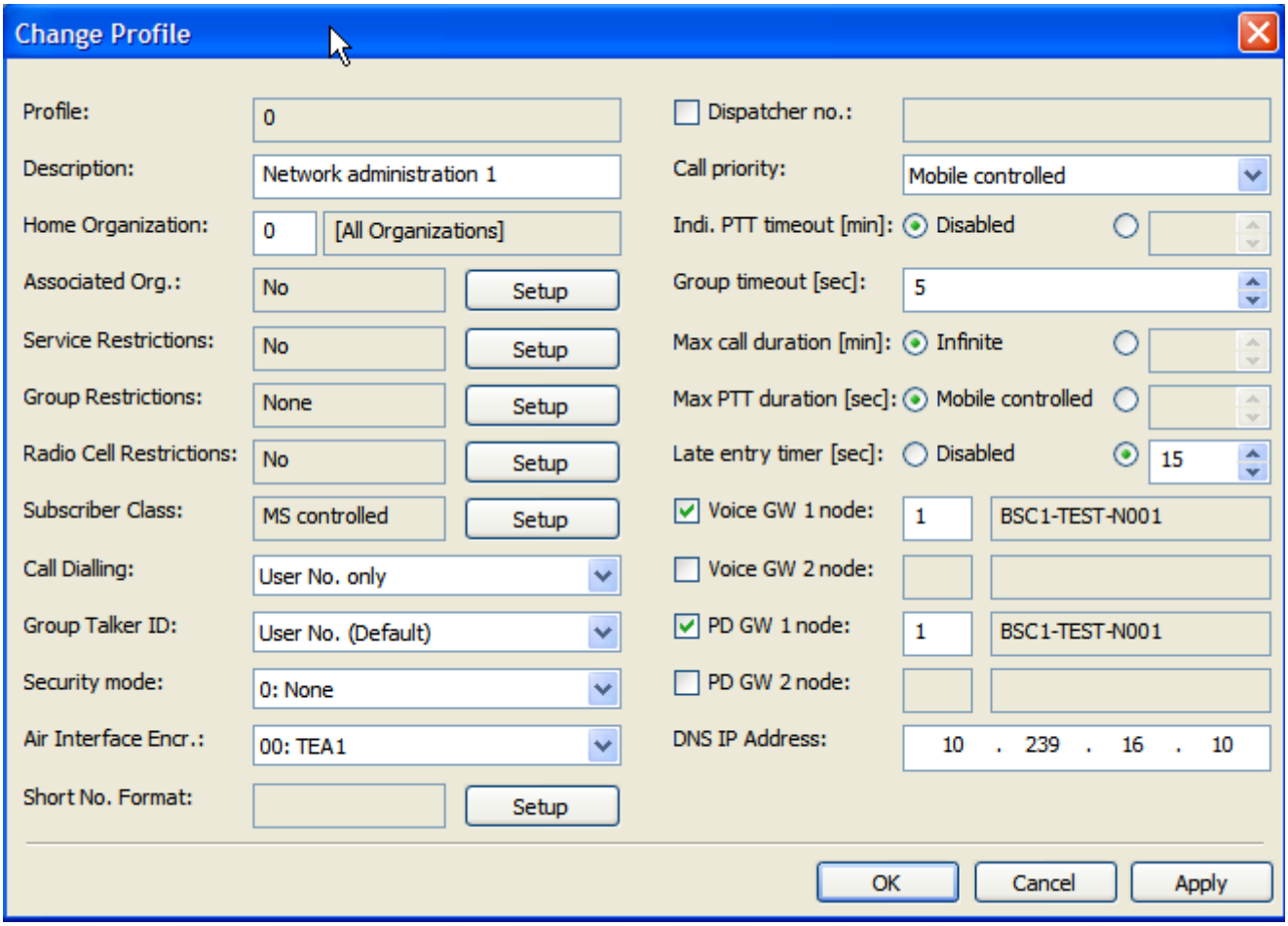


Figure 3-19: Subscriber profile configuration

The following configurations are possible

- Profile number

  The number assigned to the profile and used by the subscriber setting a reference (only valid in the Add/Copy function)

- Description

  The logical profile name related to the profile function.

- Home Organization

  The organization number is a 3-digit number and is recommended as default to be the first 2 digits of the 4-digit Profile number. E.g. org. 01 -> profile 0100…0199, org. 02 ->0200..0299, but there is no binding and is free to organize in the way your organization needs.

  The Organization number 0 has the meaning “All”, and can be used in Profiles for system support people or for all Profiles in systems without Organization division.

- Associated organizations

  Organizations associated with each other will allow calls between the associated organizations.
  Association must be done mutually in both organizations

- Service restrictions

  Option to restrict the services for a given profile regarding Mobile, Dial-in and application behavior. The restrictions are active when the “Active service restrictions” field is checked.

  The Allow field can be Yes, No or CAD (Dispatcher decide if the call shall pass).

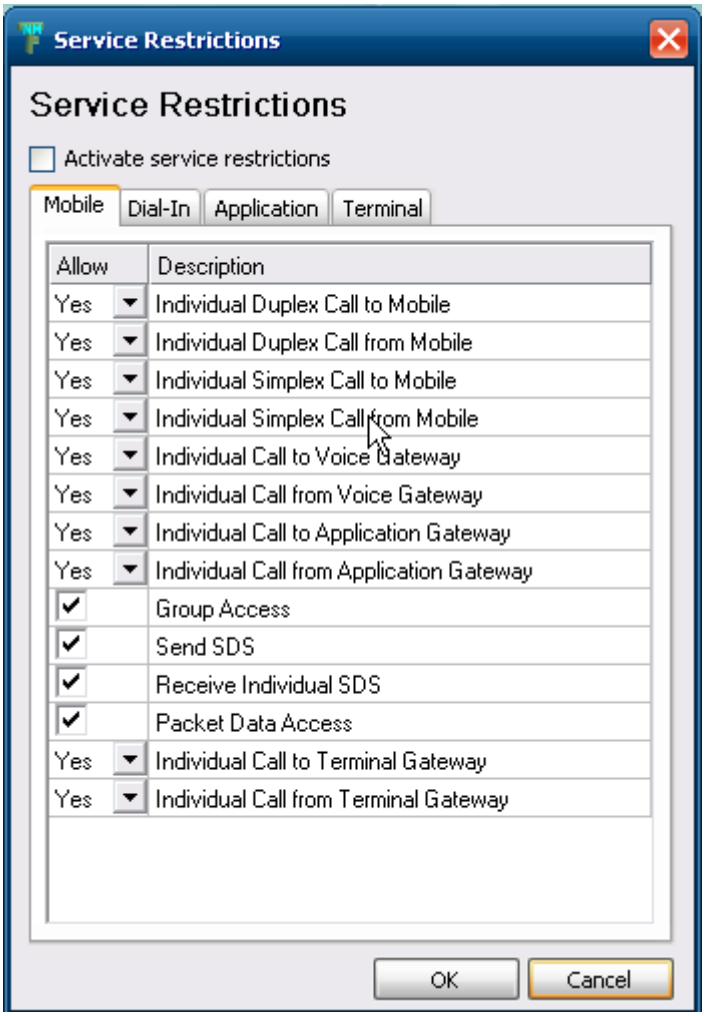
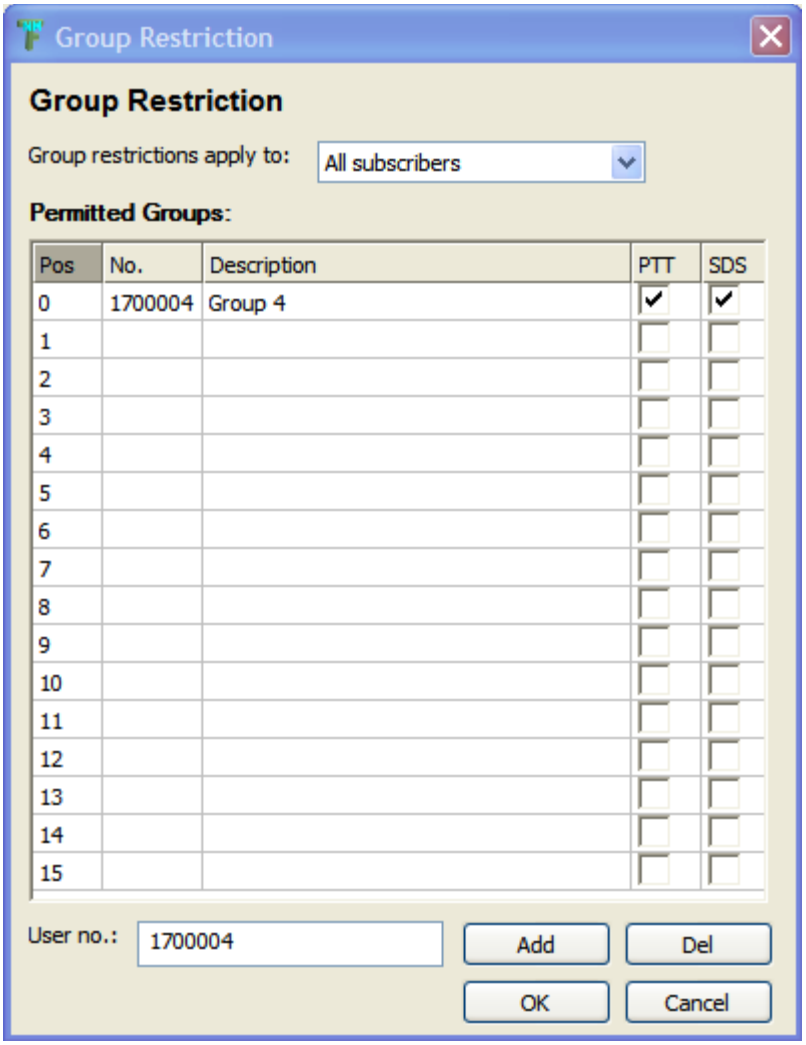


Figure 3-20: Service restrictions

- Group restrictions

  Definition of PTT and SDS restrictions related to the groups in the profile



The *Group restrictions apply to* can be set to *None* (no restriction) *All Subscribers* and only *Dial- in Subscribers*.

- Radio cell restriction

  Radios that belongs to this profile are allowed to attach the checked nodes

  This restriction is only active when the *Activate radio cell restrictions* check mark is set. The *All Nodes* button toggles between active nodes and all nodes.

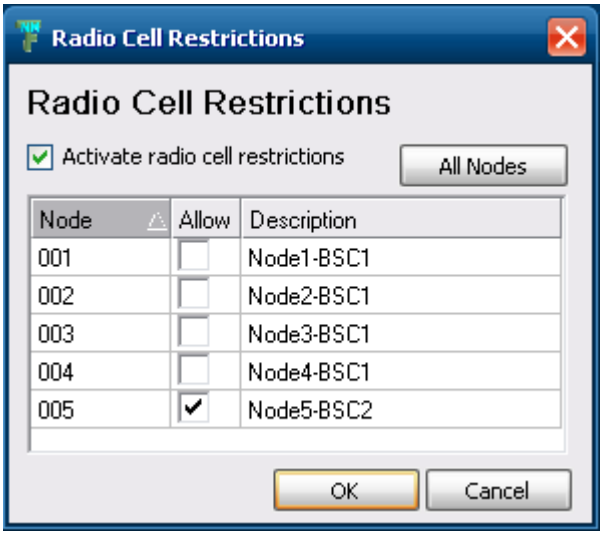


Figure 3-21: Radio cell restrictions

- Subscriber class

  Definition if subscriber class is mobile controlled or defined in the profile

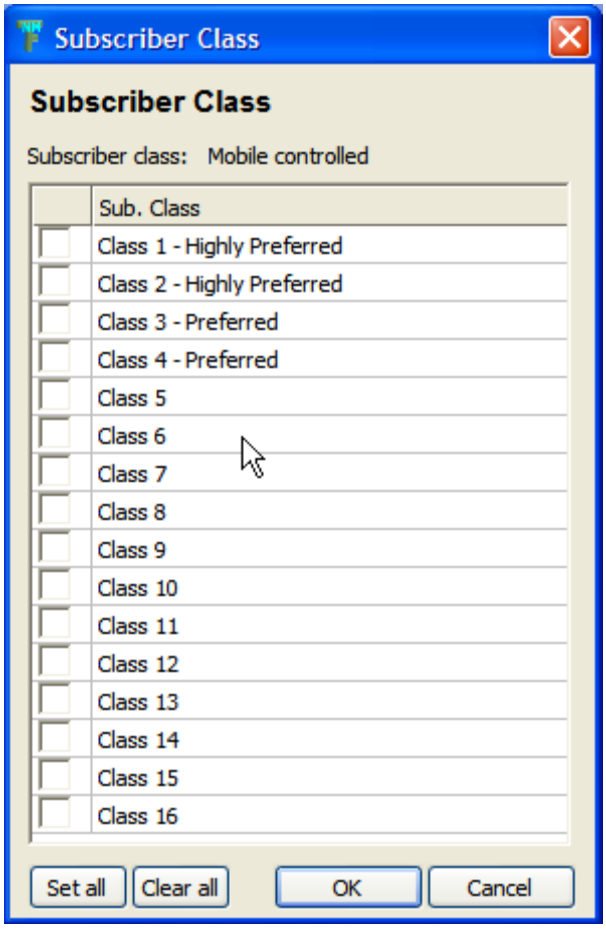


Figure 3-22: Subscriber class

It is possible to set 16 bits in the subscriber class field of the node. 1st bit signaling support of class 1, 16th bit signaling support of class 16.

Bit 1 and 2 are signaling "highly preferred", 3 and 4 are signaling "preferred", rest is "normal". Having all 16 bits set will allow any MS to attempt registration.

The purpose is to have MS registering only with radio cells with matching subscriber classes. I.e. a MS with class 16 - will only try to register with a cell supporting class 16. If a MS has class 2 and class 16 it will prefer a cell with class 2 support before looking at cells with class 16 support.

A MS has a subscriber class programmed. If in the profile setup "MS controlled" is selected, it is the MS's programming that decides about which nodes the terminals will try to attach to.
If defined in the profile, the MS will receive notification from the node about a new set of subscriber classes to work with.

If defined in the profile, the shown options apply

- Call dialing

  Determines whether calls uses the SSI programmed into the terminals or may use either SSI or user numbers defined in the subscriber register.

- Use SSI for group call

  This is a definition which is applicable only to the displayed information.
  The function is implemented to circumnavigate differences in the way certain brands of terminals displays the group information, for an instance Motorola

- Group talker ID

  Can be selected for certain brands op terminals to display group caller ID correctly

- Security mode
  Selection of the applicable security mode

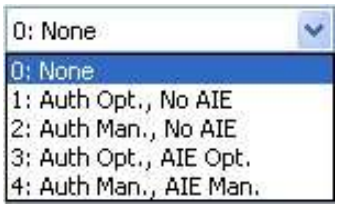


Figure 3-23: Profile security mode

- Air Interface Encryption (AIE)

  Selection of the applicable Tetra Encryption Algorithm.
  TEA1 and TEA3 are by default delivered with the system, but is dongle controlled.
  TEA2 is only delivered upon presentation of a valid permission to use this TEA

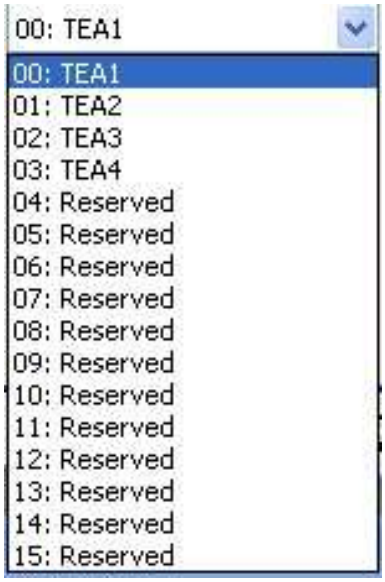


Figure 3-24: TEA details

- Short number

  Enabling user short number for the profile and definition of short number

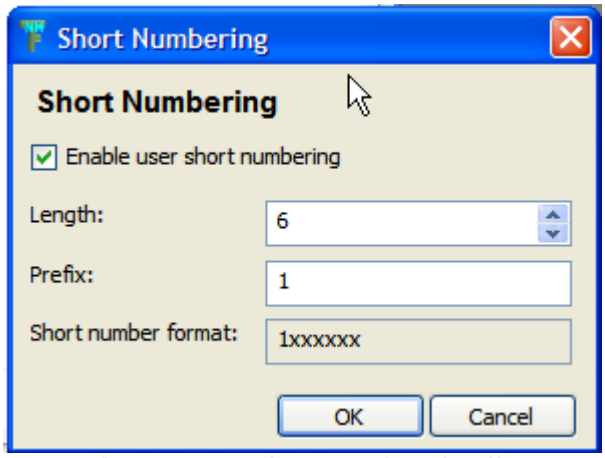


Figure 3-25: Short number details

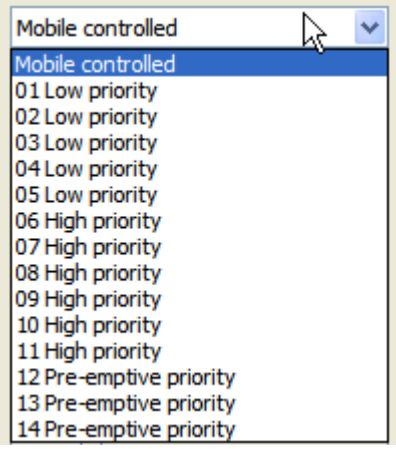
Example shows that the short number is 6 digits with 1 preset
E.g. 234598 place a call to 1234598

- Dispatcher number

  Number of the dispatcher which must be used for an instance error report, Dispatcher controlled PSTN call requests (CAD) etc.

- Call Priority

  The call priority for all mobiles belonging to this profile
  May be selected for 1 to 14 or set to mobile controlled (mobile programmed priority is in use)



01 is the lowest priority and 14 is the highest (priority 15 - pre-emptive can be programmed in the radios and are used for alarms). Pre-emptive priority means that it will take over a timeslot that already is used in case of all timeslots are used.

Timers – Timers are mainly used to restrict unwanted time consuming use of timeslots

- Individual PTT timeout

  Disabled or selectable from 1 to 25 minutes

- Group Timeout

  Time from last PTT is released to group call shut down.
  Selectable from 0 to 20 seconds
  0 sec. is valid, but use with care as this could increase load on the MCCH

- Max Call Duration

  Maximum duration of the call before shut down
  Infinite or Selectable from 1 to 250 minutes

- Max PTT duration

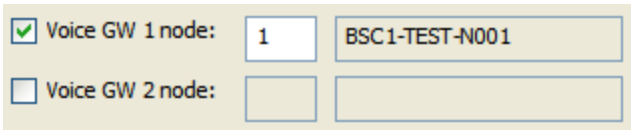
  Maximum time of the PTT
  Mobile controlled or selectable from 2 to 250 seconds

- Late entry timer

Disabled or selectable from 1 to 60 seconds. This means a radio can join a group with a late entry to an ongoing group call selectable from 1-60 seconds.

Voice GW Setup:

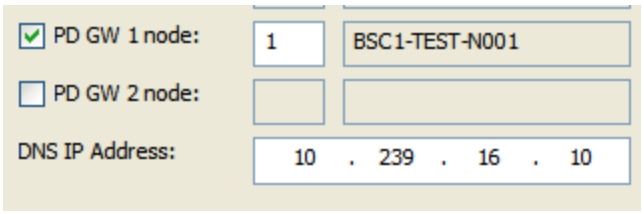
Voice Gateway connection node number



- Voice GW 1 node is the Primary node and Voice GW 2 node is the redundant node

  See section 3.3.4.6.11 for Voice GW setup and test

Packet Data GW Setup:



PD GW connection node

- PD GW1 is the Primary node and PD GW 2 is the redundant node

  See section 3.3.4.6.13 for Voice GW setup and test

DNS IP address

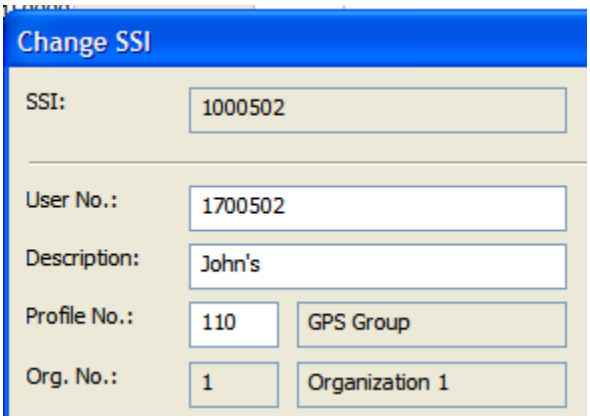
Used by Packet Data setup.
If used, the DNS IP address must point to a DNS server within the network to which the system is connected. It cannot point to a DNS server on, as an example, the internet.

3.3.5.4 Subscriber

The subscriber definition fields are dependent on the type of subscriber selected in the *SSI type* field:

- SSI Type
  - Mobile
  - Group
  - Application
  - Dial-In
  - Emergency
  - Terminal (for future use)
  - Personal (for future use)

The following fields are the same for all types of SSI's:



- SSI
  This is a unique subscriber id - typical the number programmed into the terminal or the number defined for dispatcher or a group. The SSI number must always be assigned to a subscriber and the system doesn't allow using the same SSI number more than one time. The field will be marked yellow when trying to type in the same SSI number twice.

- User Number
  The unique user number assigned to the subscriber. The user number can be used instead of the SSI number to address a subscriber. The system doesn't allow using the same user number more than one time. The field will be marked yellow when trying to type in the same SSI number twice.

- Description
  The description of the SSI. This is a text and it is optional to use.

- Profile number
  The profile number of which the subscriber is a member. The profile description (if there is any) is automatically shown when the profile number is entered. Only existing profile numbers can be used.

- Organization number

Automatically shown when profile number is entered. The organization description (if any) is automatically shown when the profile number is entered.

3.3.5.4.1 Mobile subscriber

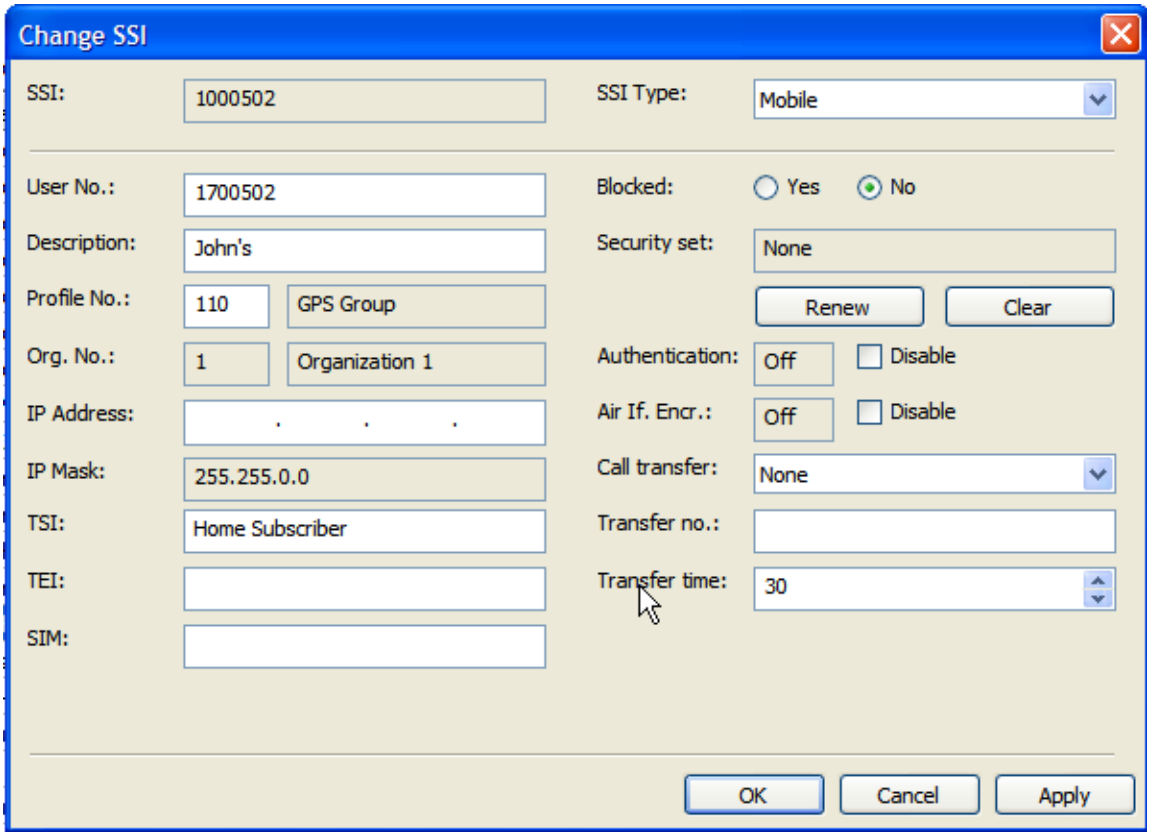


Figure 3-26: Subscriber details

- Blocked
  Select to block the radio access to the infrastructure (Temporary disable)

- IP Address
  If packet data is used, the IP address assigned to the terminal. In the terminal itself the IP address must be set to 0.0.0.0

- IP Mask
  Display field – shows the Subscriber IP Address segment used for packet data, predefined via TetraOM, BSC-GUI or Network Management

  - TSI Tetra Subscriber ID (Prepared for future use, not active in this version only home subscriber can be added)

    Is composed from MCC: MNC: ISSI

This field allows a terminal not belonging to the network to be added without having to reprogram the terminal. The terminal is assigned an ISSI and user number in the normal manner.
If not used, TSI will display “Home Subscriber”

- TEI
  If authentication is used, the correct TEI for the terminal must be entered
  It is highly recommended always to use the correct TEI. This will avoid redefining the whole subscriber register in case authentication is activated at a later time.

- SIM
  SIM number for SIM authentication

- Blocked
  Restrict the mobile from attaching to the system

- Security set
  Date and time for last security set update for this subscriber
  May be Renew or Clear using the appropriate buttons

- Auth.: and Air If. Encr.:
  These fields show the actual status. In case either one is assigned as optional, the function may be selected or deselected by removing or setting the disable options

- Call transfer
  Selection of call transfer type

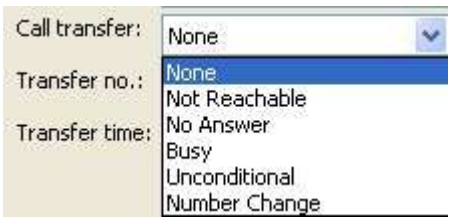


Figure 3-27: Call Transfer details

- Transfer number

  The number to which the call is transferred

- Transfer time

  The time to transfer if not using the unconditional setting

3.3.5.4.2 Group subscriber

Additional fields in group subscribers

- Group Text

If subscriber is a group subscriber, the field will be available for entering the Group Text
This text will be transferred to the group list in the terminals if the group is assigned as a DGNA group

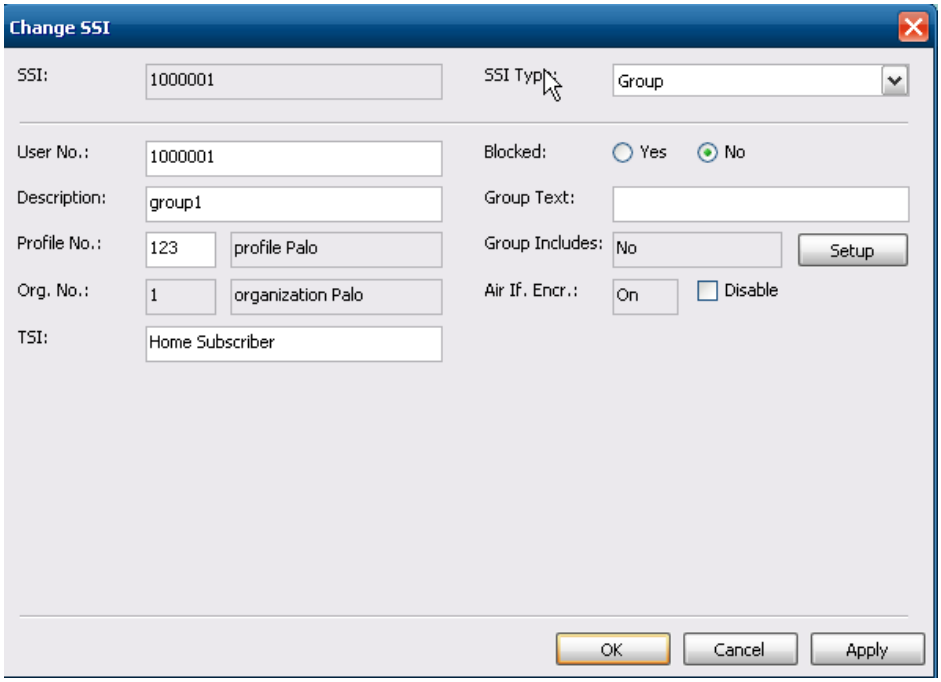


Figure 3-28: Group subscriber

- Group includes

  Option to include other user numbers in the group

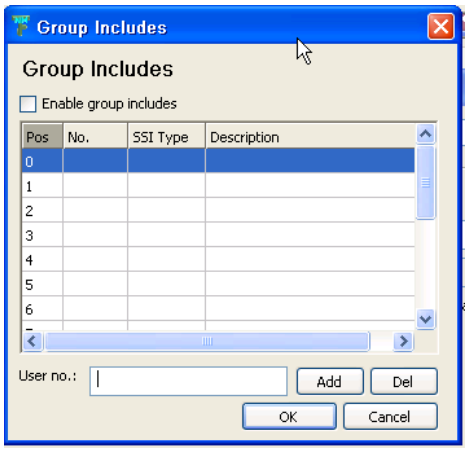


Figure 3-29: Group include

Group include means having possibility to establish a layer of groups so to speak.
Example:

Group 1 Ambulance
Group 2 Police
Group 3 Disaster management

Group 3 is set up with group include on Group 1 and Group 2

Function will be:

Group 1 PTT is heard in Group 1
Group 2 PTT is heard in Group 2
Group 3 PTT is heard in Group 1, Group 2, and Group 3. Members in Group 1, Group 2, and Group 3 can answer. When call times out, Group 1 and 2 can no longer hear each other.

So group include is a sort of temporary connection of the included groups, where the connection is triggered from the including group.

3.3.5.4.3 Application subscriber

- Change sub. Reg.:

  Selection if the subscriber register can be changed/edited from the API client (Probably a dispatcher)

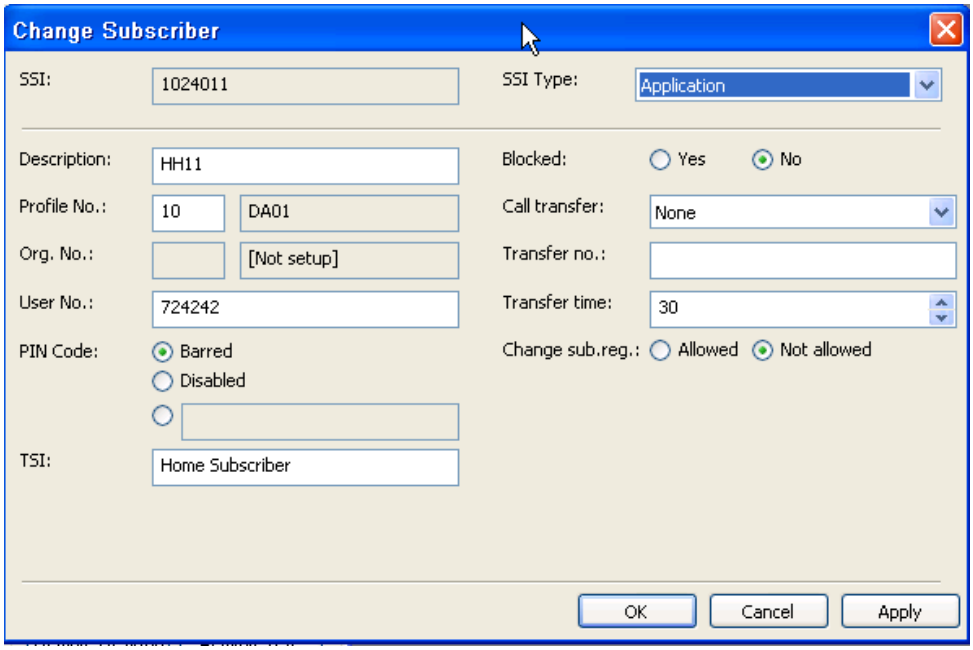
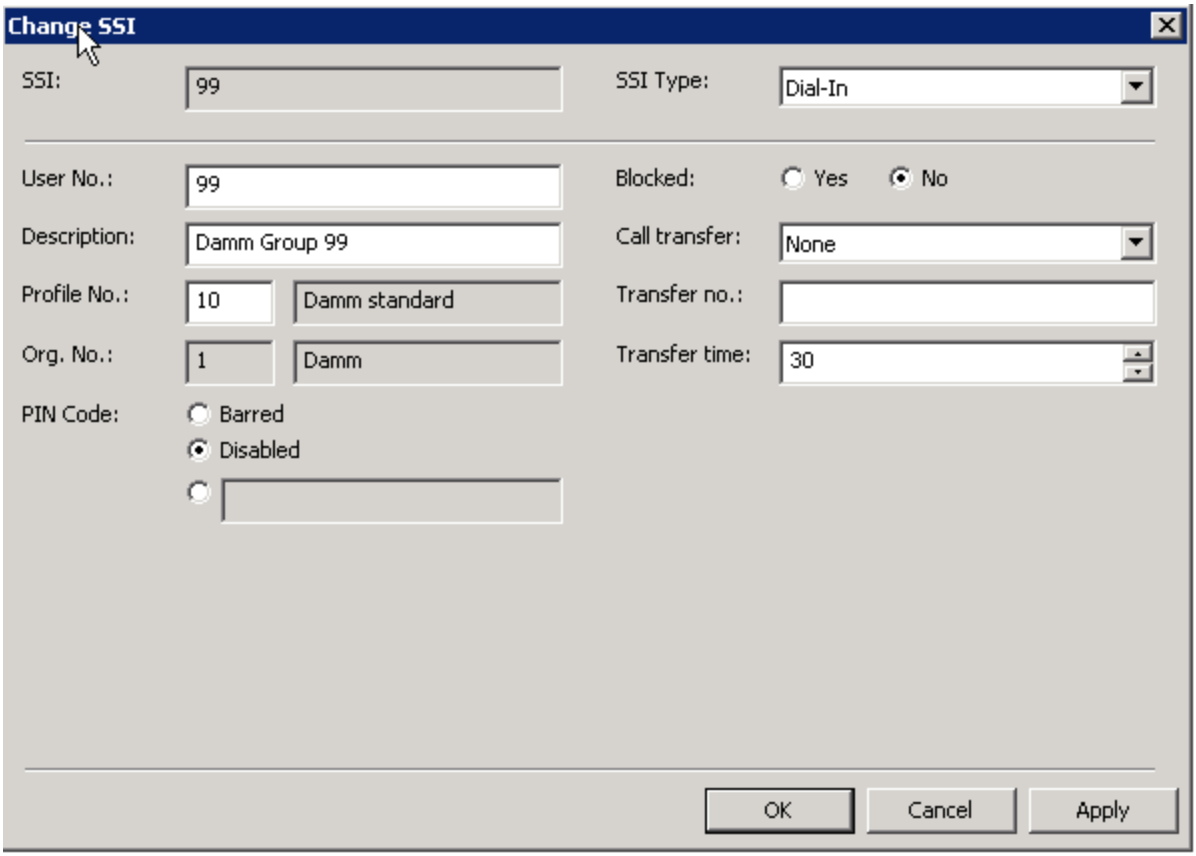


Figure 3-30: Application subscriber

- Pin Code

  Used as access control when connecting to a group call from PSTN telephones (Note: This is not applicable for individual calls from PSTN)
  - Barred: No calls will be possible
  - PIN disabled: No Pin requested
  - PIN entered: Pin must be correct to connect

3.3.5.4.4 Dial-in subscriber



The dial in SSI is an internal number used to access groups through the Voice gateway and to show an identity for the group users.

E.g.: A user with Dial-IN SSI 99 makes a PABX dial in to Group 1700003:

Dial 700000 Damm PABX (Answering machine)
Dial 1700003 Damm group 3 (Answering machine)
Dial 99 Dial-In number

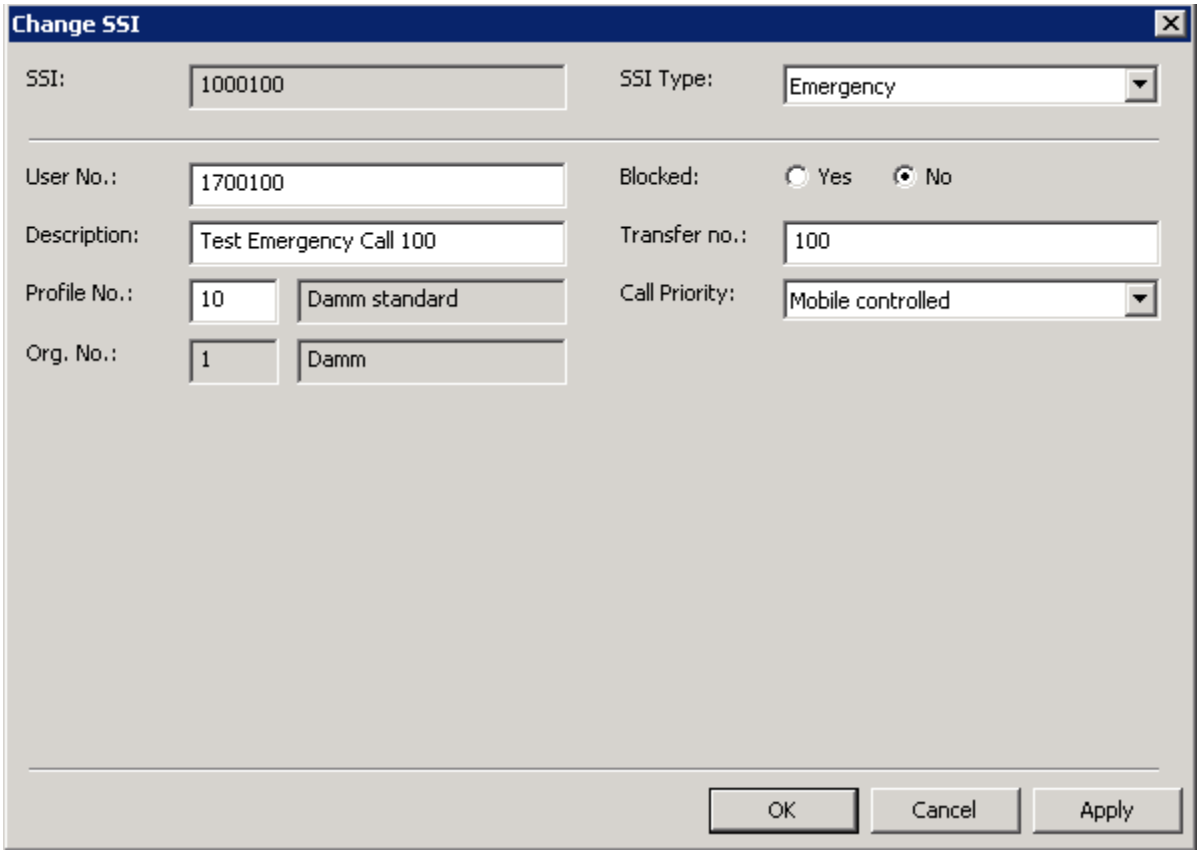
Now the PABX user can make PPT or Voice detect group call and is identified as “99” on the Tetra terminals.

PIN Code – If using a PIN code the Dial-In user is prompted from the Answering machine to enter the PIN-code before he can make the group call.

The PIN-Code options are:

- Barred – Now Dial-In is allowed
- Disabled – The use of PIN Code is disabled no PIN code is needed.
- The PIN code can be from 1 to 999999999

3.3.5.4.5 Emergency subscriber



The Emergency Subscriber is used for Transferring a Tetra Call to the Voice Gateway or another Tetra Subscriber responsible for Emergency e.g. sending it to the public 112 (911) or a another number used for Emergency.

- Transfer no: The number that wants the Tetra call transferred to e.g. 112.

3.3.5.5 Security Key

Figure 3-31: Security Key

Displays information regarding the Security Key Register

- Status
- SIM count
- TEI count

And Import historic

- Last attempt
- Last result
- SIM count
- TEI count

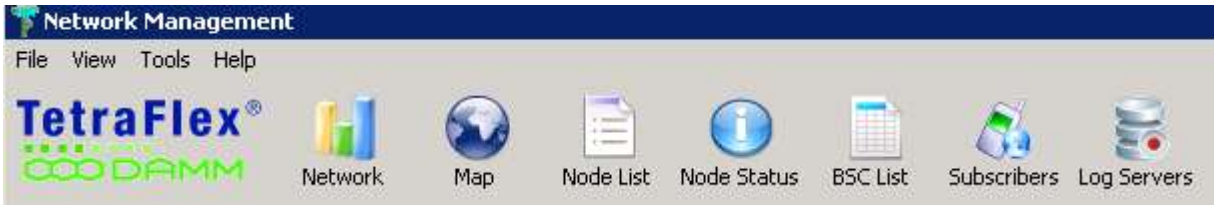
Allow import of security key file generated from the terminal programmer.

These keys will then be encrypted, using the hidden encryption key programmed in the dongle and the key sets generated

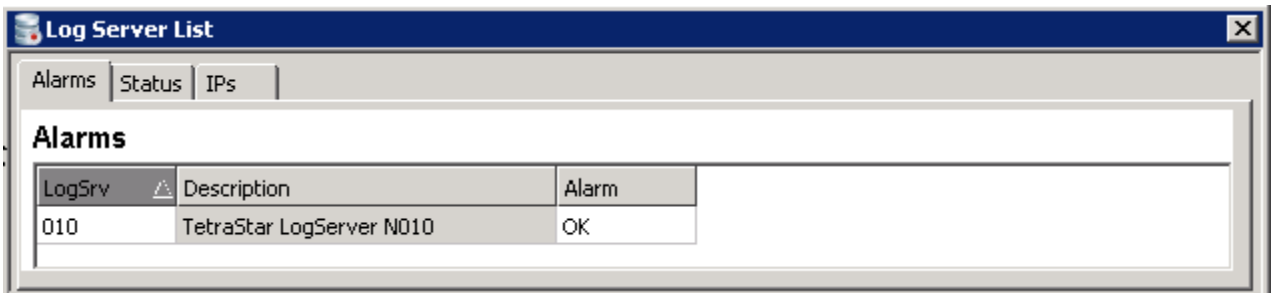
Allows the update of all security keys simultaneously, as opposed to the subscriber update which is valid for the subscriber only.

3.3.5.6 Log Servers

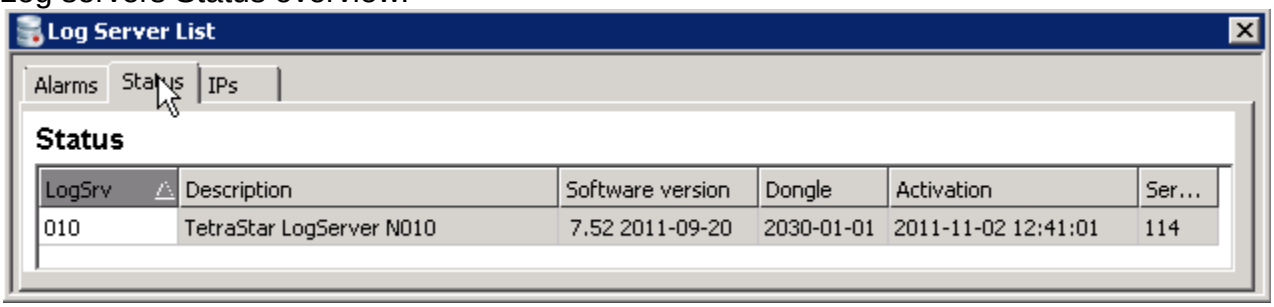
The Alarm state, Status and IP addresses of the Log Server(s) that are attached to the system can be shown by clicking the Log Servers icon:



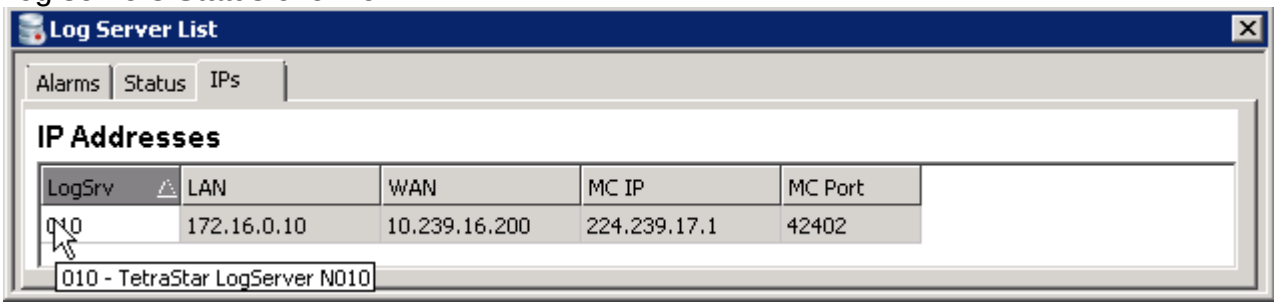
Log servers Alarm overview:



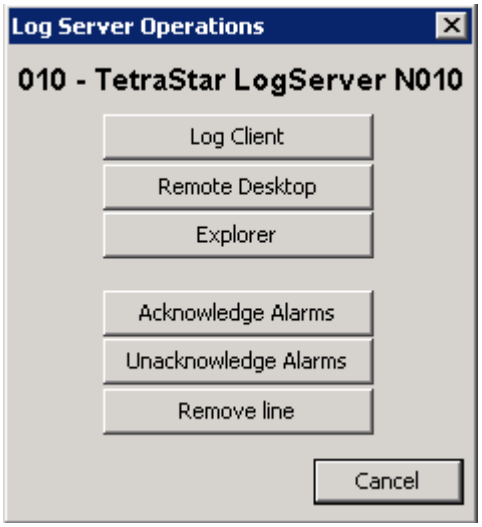
Log servers Status overview:



Log servers Status overview:



When Right click the LogSrv fields you get the Log Server Operations dialog:



- Log Client — Start the Log Client
- Remote Desktop — Starts the Remote Desktop Client
- Explorer — Starts Windows Explorer
- Acknowledge Alarms — Acknowledge log server alarms
- Unacknowledge Alarms — Unacknowledge log server alarms
- Remove line — Remove LogSrv line e.g. if a Log server is not running

3.4 AUTHENTICATION AND ENCRYPTION

3.4.1 Description

This section describes in detail the function of the Security Key Set used for authentication and encryption.
Only the method is described, for further information regarding the Subscriber Register, BSC, distribution of subscriber data etc. please consult the relevant manual sections.

3.4.2 Definitions

K	The key value file generated by the terminal programmer. File is in plain text and contains key value associated to TEI
Dongle Key	The secret key programmed in the Node Dongle. The Dongle Key is enabling the key register in the subscriber register
K^1	The Security Keys derived from the K file and placed in the key register
Security set	The distributed key sets. Should be updated at regular intervals

3.4.3 Description

The key file produced by the terminal programmer (K) is read in to the system and is encrypted using the Dongle Key and placed in a key register (K^1).
This key register is now “protected” by the dongle key.
This means that if the key register is moved to another node, the Dongle key must be moved as well.

The content of the key register (K^1), decrypted with the dongle Key, and the TEI or SIM reference value is used to produce a security set (Derived keys) which is placed in the Master Subscriber Register and distributed to the Subscriber Register on the other nodes as SSI + Security Set. After this the TEI / SIM reference is essentially no longer used.

When updating the Security Set, the K^1 key and the SSI is used to generate a new distributed Security Set.

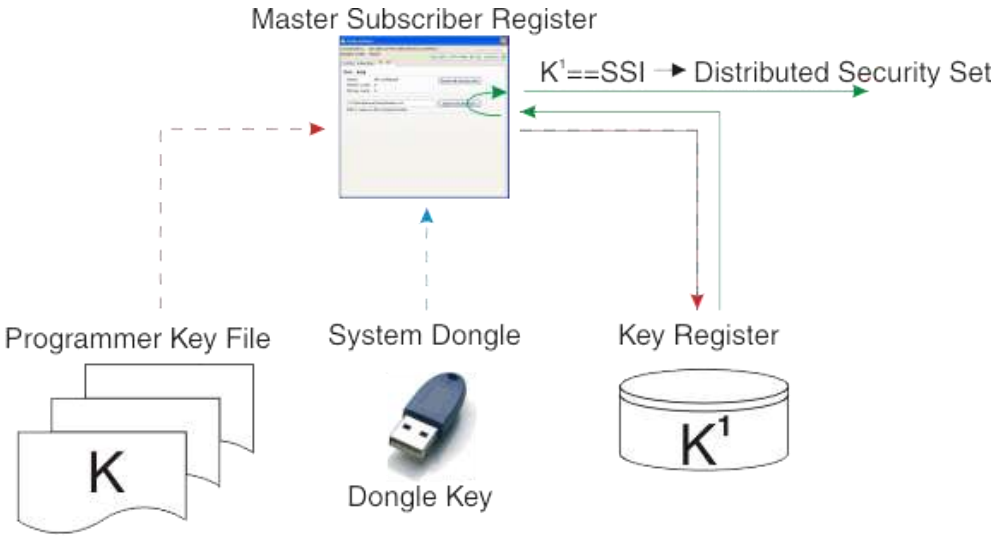


Figure 3-32: Key principles

3.4.4 Backup

It is essential that the K values are kept at a safe place that means to place the programmer key file in a safe place.

Backup should always consist of at least:

- Master Subscriber Register
- Key Register

3.4.5 Restore

If the node containing the Master Subscriber register is isolated or removed, the system will continue to work as usual except that new terminals cannot be added to the Subscriber register.

When using encryption/Authentication it is recommended to wait adding subscribers until the node containing the Master Subscriber Register is available again.
Alternatively it is possible to assign another node as Master Subscriber register and add the subscribers to this register.

After adding subscribers, the Key File (K) is read into the Subscriber Register as described previously.

This will create a new Key Register on this node containing the K^1 values for the new terminals.

The disadvantage of this is that when the Security Sets must be updated, both nodes must be updated, so this method is NOT recommended

In case the node containing the Master Subscriber Register is totally lost or an exchange or change of node for some other reason is preferred, then all Key Files (K) can be read in

again on the new node using the dongle Key belonging to this node, and the key sets updated.
This node is now containing the Master Subscriber Register and Security Key register.

3.5 DISPATCHER

3.5.1 General Description

The Core of the Dispatcher is the TetraFlexApi.dll. It contains all the core elements to be able to connect an Application to the TetraFlex® system. As standard, the TetraFlexApi.dll is delivered with a GUI (Graphical User Interface). This provides the complete Dispatcher Application.

The TetraFlexApi.dll contains a fully documented API (Application Programming Interface) TetraFlexApi.h file which allows the DAMM supplied GUI to be replaced with other GUI applications provided from third party vendors. Thereby applications with other features and in other languages are very easily implemented without any need to touch the core interface to the system.

The TetraFlexApi.dll is delivered with a DAMM License Dongle to permit the use.
DAMM dispatcher from V7.30 and ahead requires a dispatcher entry in the dongle to be able to start. Dispatcher from V7.40 and ahead requires a Microsoft .NET Framework and MS SQL Compact database to be installed. This is valid for the DAMM dispatcher only, not for any third party application.
The TetraFlexApi.dll is intended to be used on a Windows XP or Windows 7 platforms.

Any Node (Base Station, Gateway node etc.) of the TetraFlex® system can have an Application Gateway activated, and each gateway can handle several simultaneous application connections. The connection from the application to the system is done with standard IP protocols (TCP/UDP) to the external (WAN) side of the node, and the application can be located anywhere provided a standard IP connection to the node's external WAN side is possible.

The TetraFlexApi.dll configuration includes a list with one or several IP addresses of Application Gateways. The TetraFlexApi.dll will scan through the list and try to register with the first IP on the list, if found the scan is stopped, otherwise an attempt to register with the next IP entry in the list is made (like a mobile scanning through its frequency list). The registration occupies an SSI position. A PIN-code Authentication is added to prevent other applications to register with same SSI. This allows redundant gateway connections and allows the application to be moved to new locations without any reconfiguration.

The TetraFlexApi.dll supports a.o. to display the DAMM Dispatcher Phonebook with all subscribers belonging to its own Home Organization and all Associated Organizations.
The phone book is an extract from the TetraFlex® subscriber register which is automatically uploaded to the dispatcher using its own dedicated multicast address. This means that the home organization subscriber register can be maintained from the dispatcher provided access has been granted in the subscriber register.
Dispatcher functions include Individual-, Group- and Broadcast calls, monitoring of all active calls including individual simplex and duplex calls, sending and receiving SDS, adding DGNA groups, performing discreet and ambience listening etc. Additional features are planned to be added in coming releases. For further information regarding future features, see the Feature

List description released with the TetraFlex® package and placed in the C:\Tetra\Active\Doc directory

The TetraFlexApi.dll will at registration check for correct protocol version. When the TetraFlex® system software is updated with new features on the Application Gateway, the TetraFlexApi.dll will also be updated and shall be installed at the GUI applications.

The TetraFlexApi.dll will be fully backward compatible, which means that older GUI applications can use a newer version of TetraFlexApi.dll.

3.5.2 TetraFlex® Dispatcher Functionality

The Dispatcher application is developed to run on a Windows XP or Win7 platform. To launch the Dispatcher application the following things are required:

- IP connectivity to an Application GW on the IP backbone network.
- Hardware dongle with API client and DAMM dispatcher enabled.
- A valid Dispatcher SSI and user number defined in the subscriber register
- A valid PIN code (optional) defined in the subscriber register
- Organization 0 (Zero) defined in the subscriber register, also if this is organization is not in use

Furthermore the dispatcher requires that Microsoft .NET framework and Microsoft SQL Compact to be installed on the Dispatcher PC

When the Dispatcher application is launched the main window appears

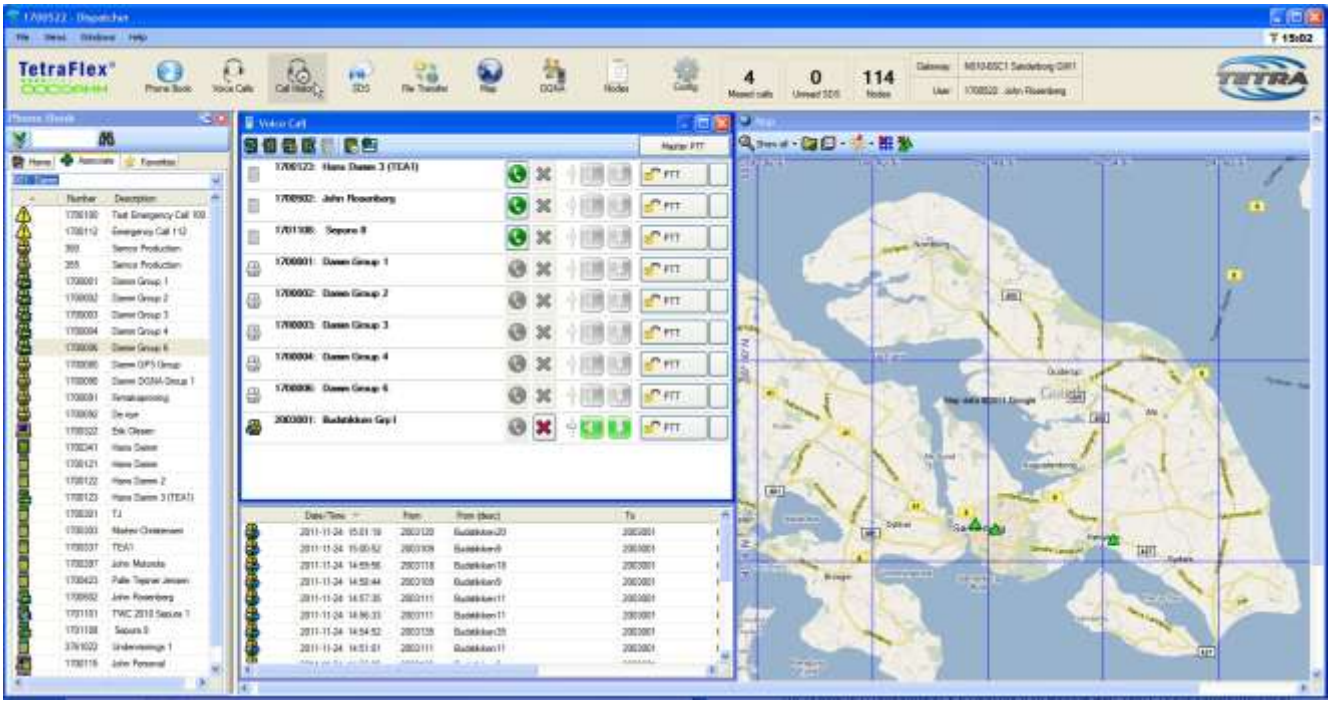


Figure 3-33: Dispatcher Main window

From the toolbar it is possible to open the Phonebook-, Voice Calls-, SDS-, Position-, File Transfer, -DGNA, -Nodes and the Config views. Notice that the dispatcher connection information is provided as well.
Double click on the “Missed Call”, “Unread SDS” and “Node” icons will open the respective windows in case they were closed down or bring the windows to front in case they are open.

Figure 3-34: Dispatcher Tool Bar

3.5.3 Views

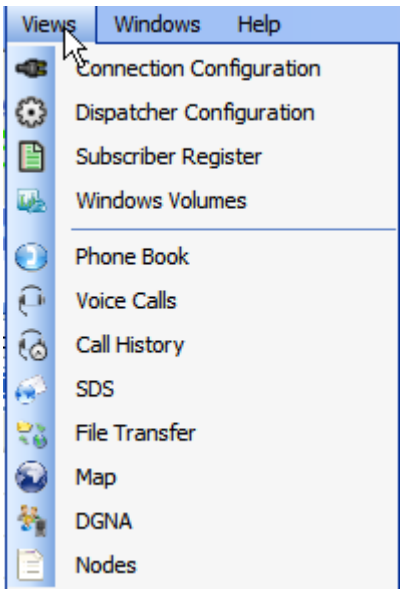


Figure 3-35: Views

3.5.3.1 Connection Configuration

Refer to part 2 section 2-13 for configuration explanation

Figure 3-36: Connection Configuration

3.5.3.2 Dispatcher Configuration

The dispatcher configuration selection opens a window with 5 tabs. Configuration may also be entered using the configuration icon 

3.5.3.2.1 Audio

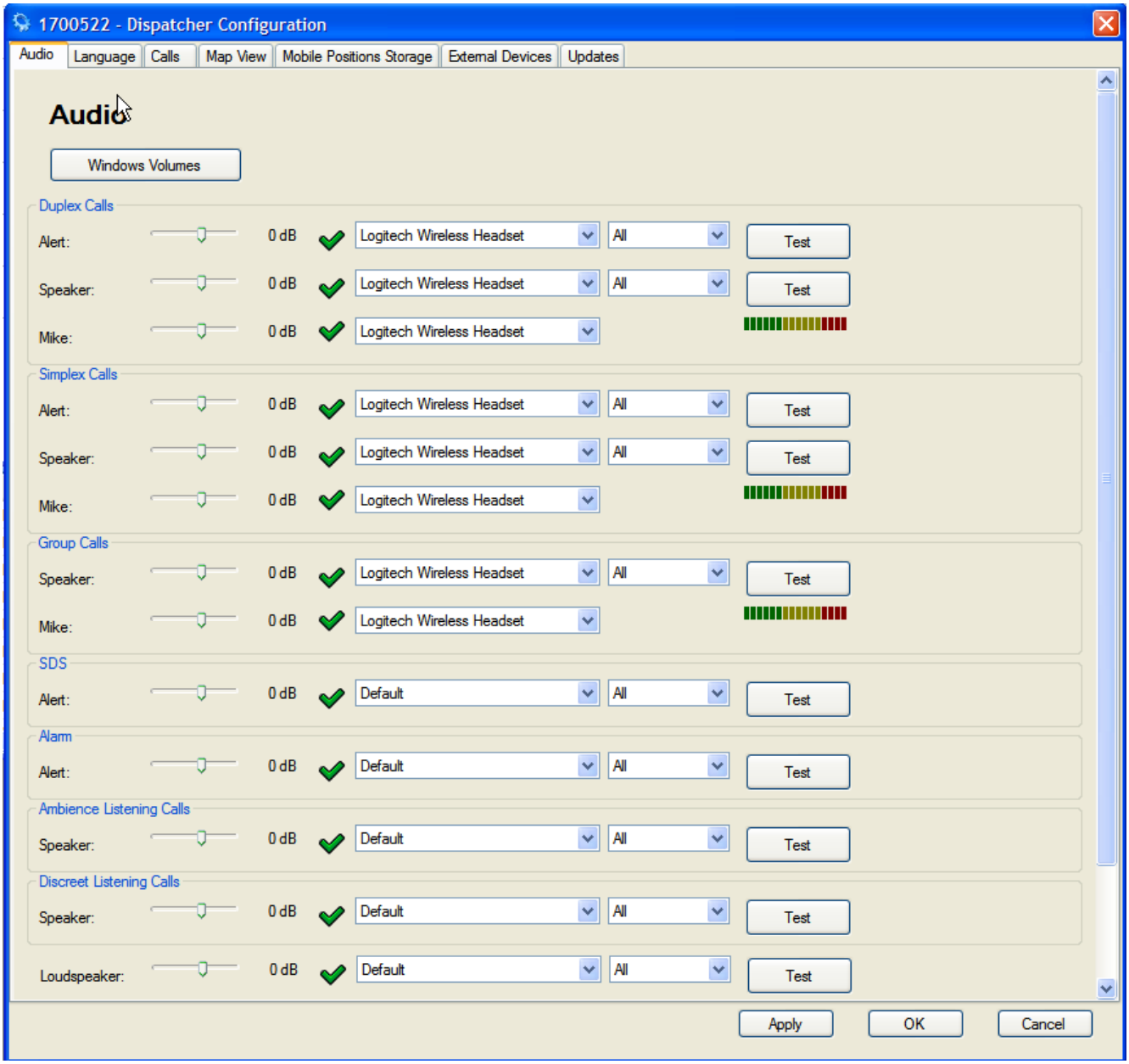


Figure 3-37: Dispatcher Configuration

The audio tab allows configuration of the Speaker and Microphone settings for the different call types and alerts. If the PC running the dispatcher has more sound devices, it is possible to redirect the sound for the different call -and alert types to individual sound devices.

- Test button- Each call -and alert type has its own test button that can be used for testing the in and output.

- Windows Volumes button - Gives an overview of which Windows sound devices is active in Windows. If a device is adjusted to 0 dB a red alert comes up to indicate that this device cannot be used for audio input or output.

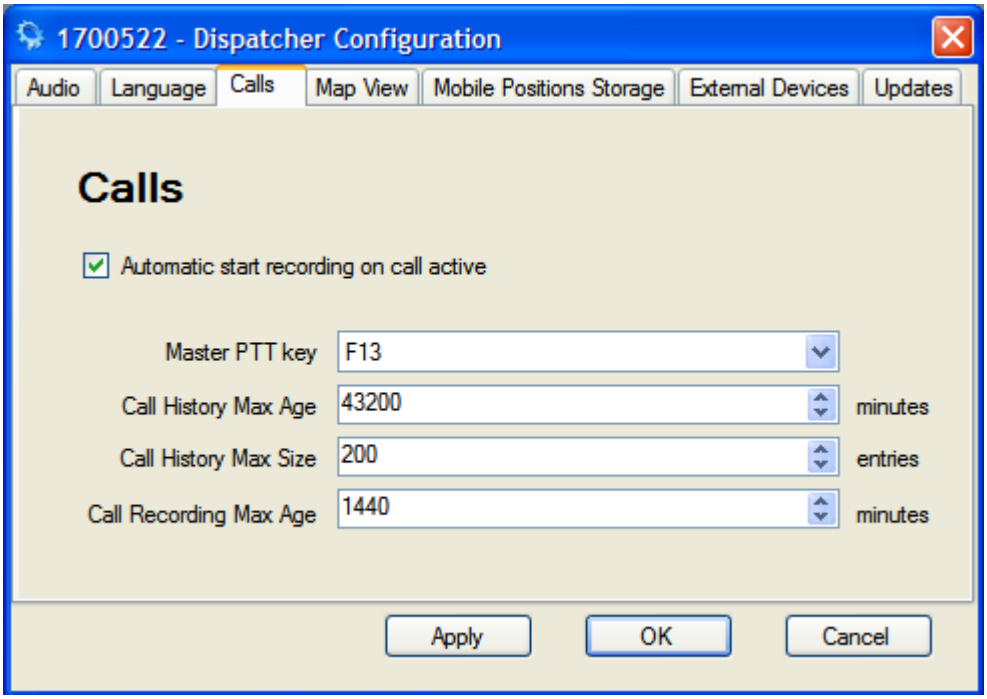
3.5.3.2.2 Language

Figure 3-38: Language Setting

The Language tab allows setting of the dispatcher language

NOTE: The selection is dongle controlled, and English is always present with the option to select additional languages.

3.5.3.2.3 Calls



The Calls dialog is used for setting the Master PTT key used, and number of records stored for the Call history.

- Master PTT key – The PC functions key F1-F12 that you want to use for the Master PPT call in the dispatcher. If using the Damm foot switch, F13 has to be selected.
- Call History Max Age – 60 to 518400 min. (360days). The max. numbers of minutes that a call will be showed in the call history database before it will be deleted.
- Call History Max. Size – 20 to 5000 entries. This is the max. numbers of calls that can be stored in the database.
- Call Recording Max. age - 60 to 518400 min. (360days). The max. numbers of minutes a voice call recording will be showed in the call history database before it will be deleted.

Call History max age, call history max. and call recording max age are depending on each other i.e. the lowest setting, will be the numbers of records that are kept in the database.

3.5.3.2.4 Map View

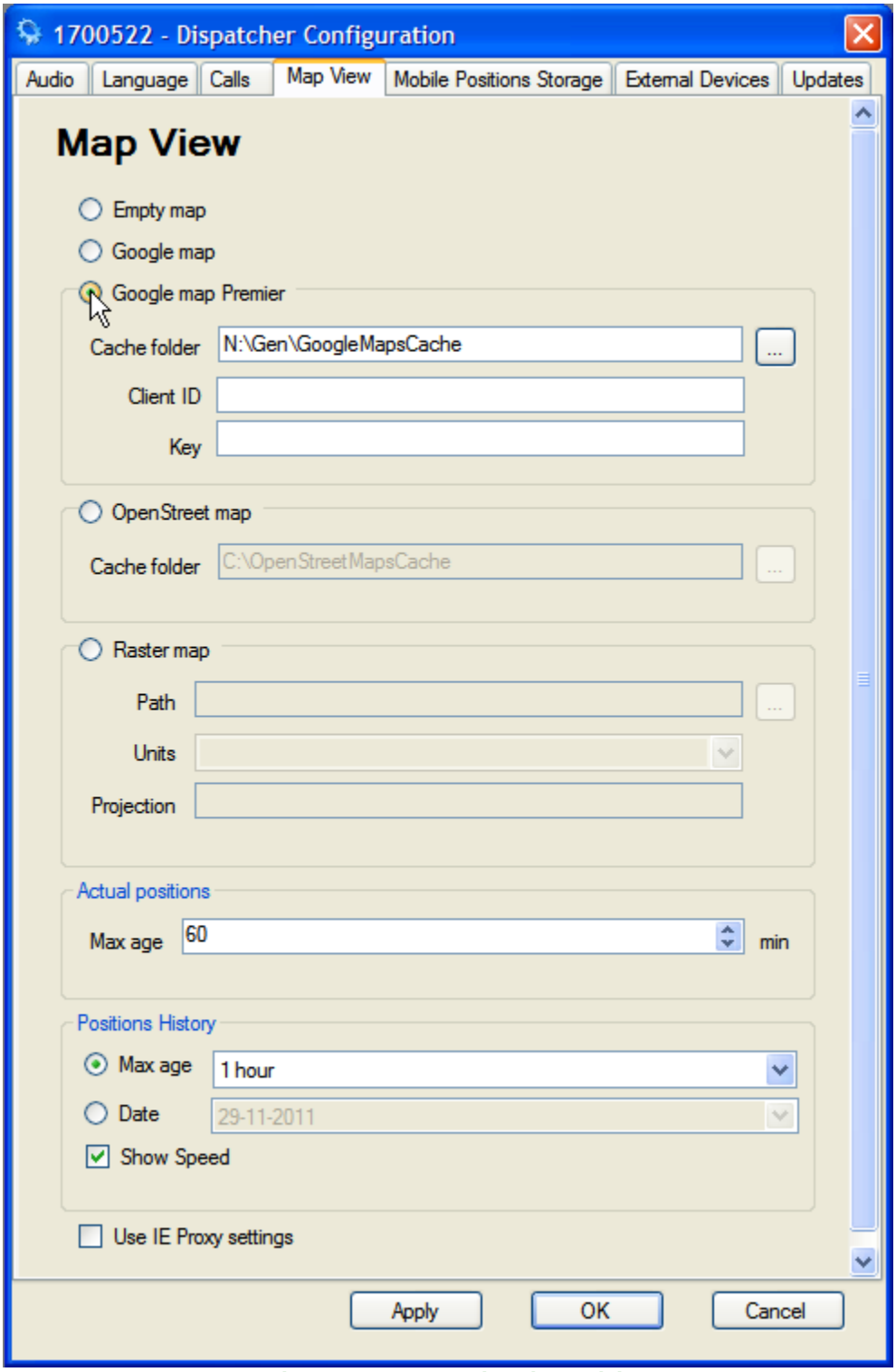


Figure 3-39: Map View (Google)

The Map view has the following options for showing geographic maps with Radio GPS positions and node positions in the dispatcher:

- Empty map – No back ground maps are shown, this can be used for showing overlay shapes in ESRI format* in the map view. Empty maps also gives the option to show RSSI measurement and lines between the position history points.

- **Google map** – Standard Google maps. These are like the maps you get when accessing http://maps.google.com/ and off course this requires an internet connection to access.

- **Google map premier** – Uses Google maps, but with a more advanced interface to be able to show e.g. RSSI measurement and lines between the position history points on the map. It is possible to cache Google maps to speed up the changing of the maps or zoom in and out on a map. If the Internet connection is broken it is possible to use the cached maps, but with the limitation that areas and zoom levels that are not cached, will not be shown. The **cache folder** is used to define where the cached maps are stored to and retrieved from. It is possible to get a premium Google account that makes it possible to get faster updates of the maps and without limitations of how many maps it is possible to collect. If you have a Google maps Premier license, Login information can be added in the **client Id** and **Key** fields. It is possible to add layers on top of these maps in ESRI shape format.

- **Open Street maps** – Free geographic data. It is possible to show e.g. RSSI measurement and lines between the position history points on the map. It is possible to add layers on top of these maps in ESRI shape format*. The **cache folder** is used to define where the cached maps are stored and retrieved from.

- **Raster maps*** – This map format makes it possible to make your own map in GEO TIFF or ERDAS ECW format. In the **Path** field you can select the directory where the GEO Tiff or ERDAS ECW files are placed. If selecting a map in one of these formats the **Units** and **Projection**** fields will automatically be filled in if the map file is provided with this information. If the projection information is not provided in the map file it can be typed in manually. If the projection -or units parameters are not correct you will either get a warning or the map will not be shown correct.

*) ESRI-Shape format and Raster maps are Dongle controlled and has to be purchased separately.

**) Projection - *A map projection is any method of representing the surface of a sphere or other shapes on a plane. For further explanation refer to* *http://en.wikipedia.org/wiki/Map_projection*

The projection of your maps should be inserted here in the PROJ.4 Cartographic Projections Library format defined by OSGeo. Refer to http://trac.osgeo.org/proj

To find the actual projection the webpage http://www.spatialreference.org could be used by selecting ESRI references, the actual ESRI number corresponding to your map and then Proj4.

Example: +proj=utm +zone=32 +ellps=GRS80 +units=m +no_defs

A description of the different parameters is to be found at:
http://trac.osgeo.org/proj/wiki/GenParms

- Actual positions Max age: This is the max. time the actual position of a Radio will be shown on a map after the Radio has deregistered or the GPS signal is lost. The value can be from 1 to 600 minutes.

- Position History Max age: The time frame the position history will be shown on map. The setting can be from 1 hour to 1 day or you can set the date from where you want to show the history.

- Show Speed: Shows information regarding speed and direction (heading) in the positions history list and detail information on each GPS point on the map

- Use IE Proxy settings: If this is checked online maps like Google and Open Street view will use the proxy setting of IE to locate a proxy server to get access to the internet.

3.5.3.2.5 Mobile Positions Storage

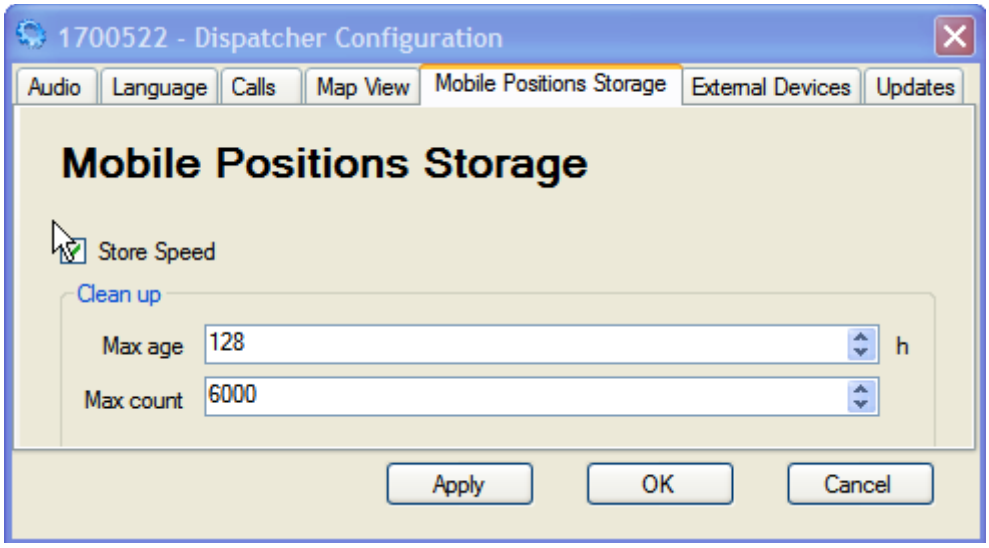


Figure 3-40: Mobile Positions Storage

Shows selections for:

- Speed Stored: The Speed information is saved in the database
- Clean up. Maximum number of hours (1-700 hours) before the position history is deleted. Max. count is the number of records that can be stored before clean up (20 to 6000). These two settings are depending on each other and it is either the age or the numbers of records that decide when the oldest record will be deleted, whatever comes first.

3.5.3.2.6 External Devices

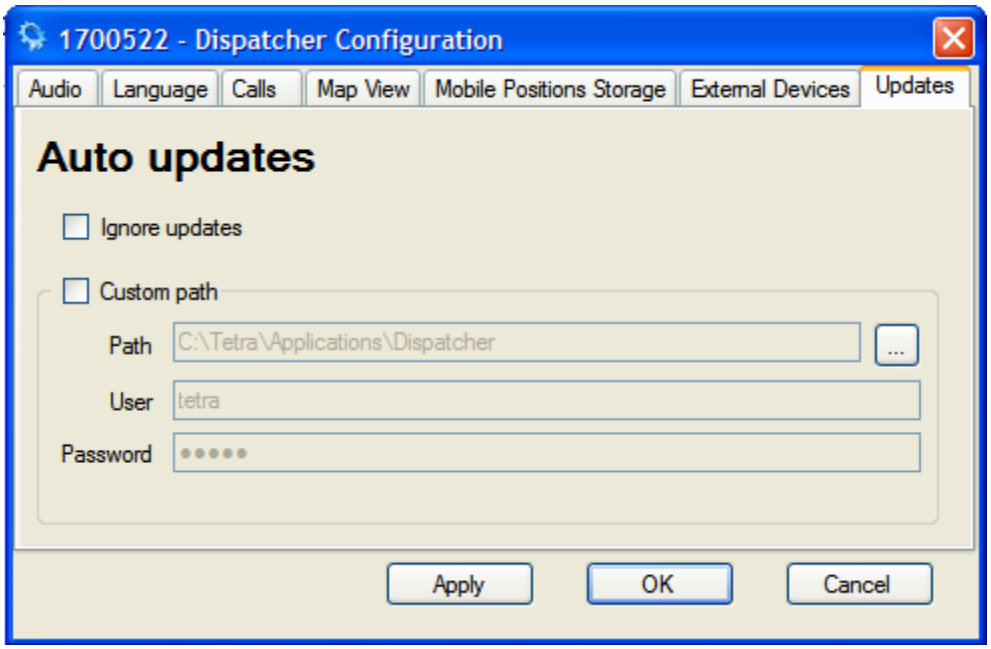
External devices presently supported is the ADU200 USB input/output box manufactured by Ontrak Control Systems inc. www.ontrak.net

Functions available are a contact close (box relay output K0 normally energized) upon an alarm SDS or alarm call to the dispatcher or group monitored by the dispatcher.

Figure 3-41: Ontrak alarm box

Please refer to the ADU200 manual for further information

3.5.3.2.7 Updates



The Auto updates function will search for newer Dispatcher version when the Dispatcher is running. I will search either on the share on the node where it is connected to, or on the custom path that that can be set up with this dialog.

- Ignore update: The Dispatcher will not search for new updates.
- Custom path: **Path** is the local or network path that you want to use for update and the **User** name and **Password** must be a valid user for this path

3.5.3.3 Subscriber Register

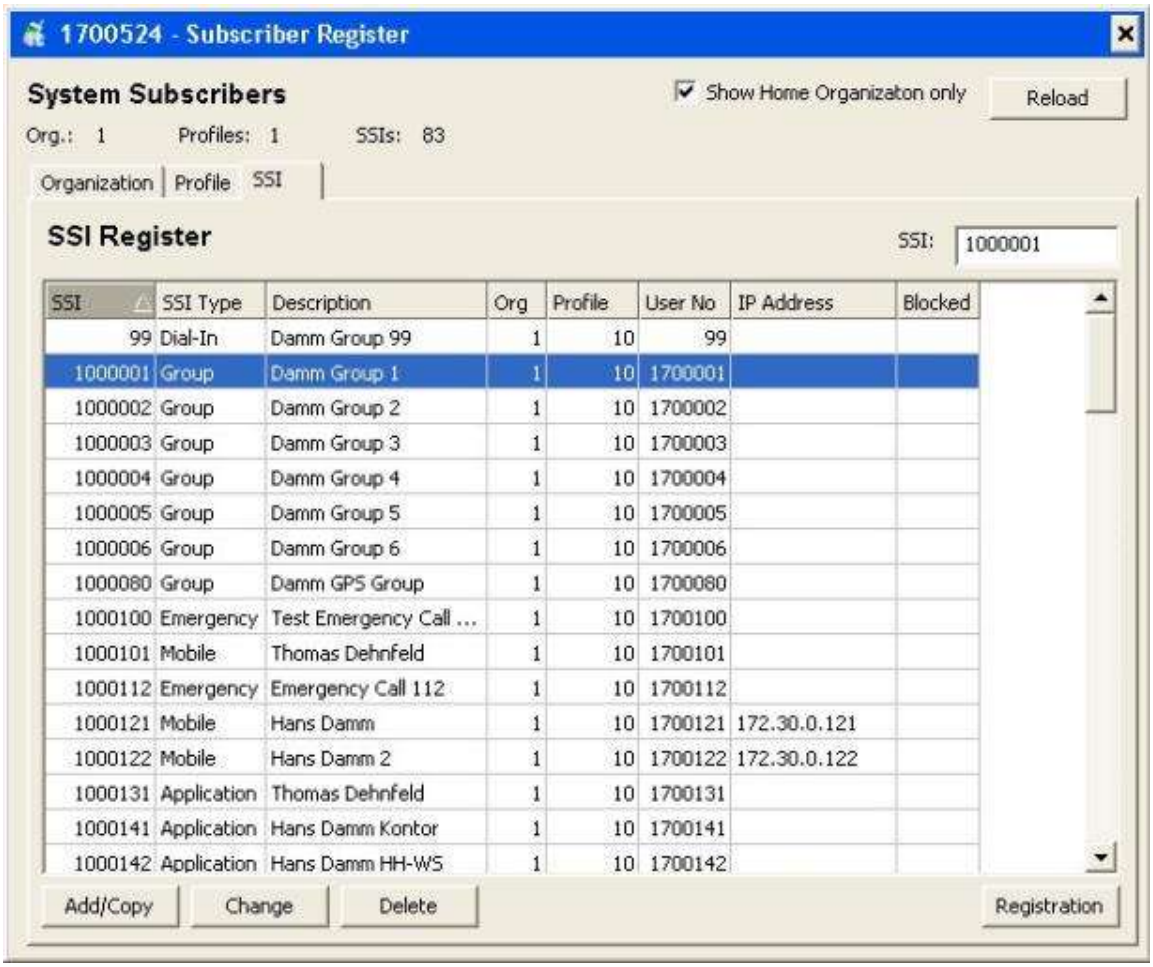


Figure 3-42: Subscriber register

The Subscriber Register is read into the Dispatcher for editing and maintaining All organization, profiles and SSI belonging to the dispatcher's home organization or associated organizations. These can be seen and changed if the "Subscriber Register changes "allowed" flag is set for Application SSI the Dispatcher is connected to (see figure 3-45).

There is no way to set this flag from the Dispatcher if it is not already is set, you have to use the Network Manager to do that.

The **Show Home Organization only** check mark toggles between showing all organization or only home organization.

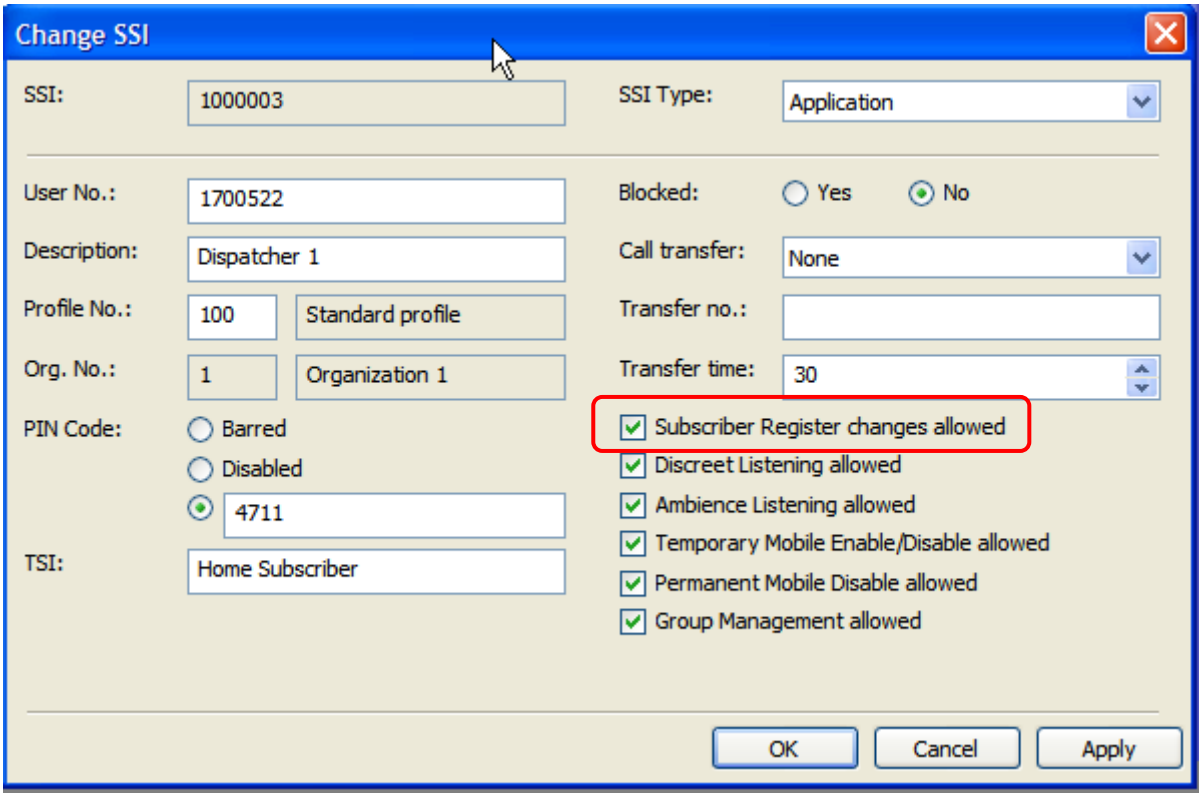


Figure 3-43: Subscriber register change

For more information regarding the Application SSI please the chapter Network Manager – Subscriber.

3.5.4 Phonebook functionality

The Phonebook window  is activated from the Dispatcher Tool Bar or from the top bar Views selection. From this panel the Dispatcher is able to initiate various types of calls and send Status and Text SDS's.
The Phone Book contains a list of subscribers belonging to the same Home and Associated Organization as the Dispatcher. This list is provided by the TetraFlex® infrastructure and is obtained via the Application Gateway by means of the dedicated subscriber multicast address.

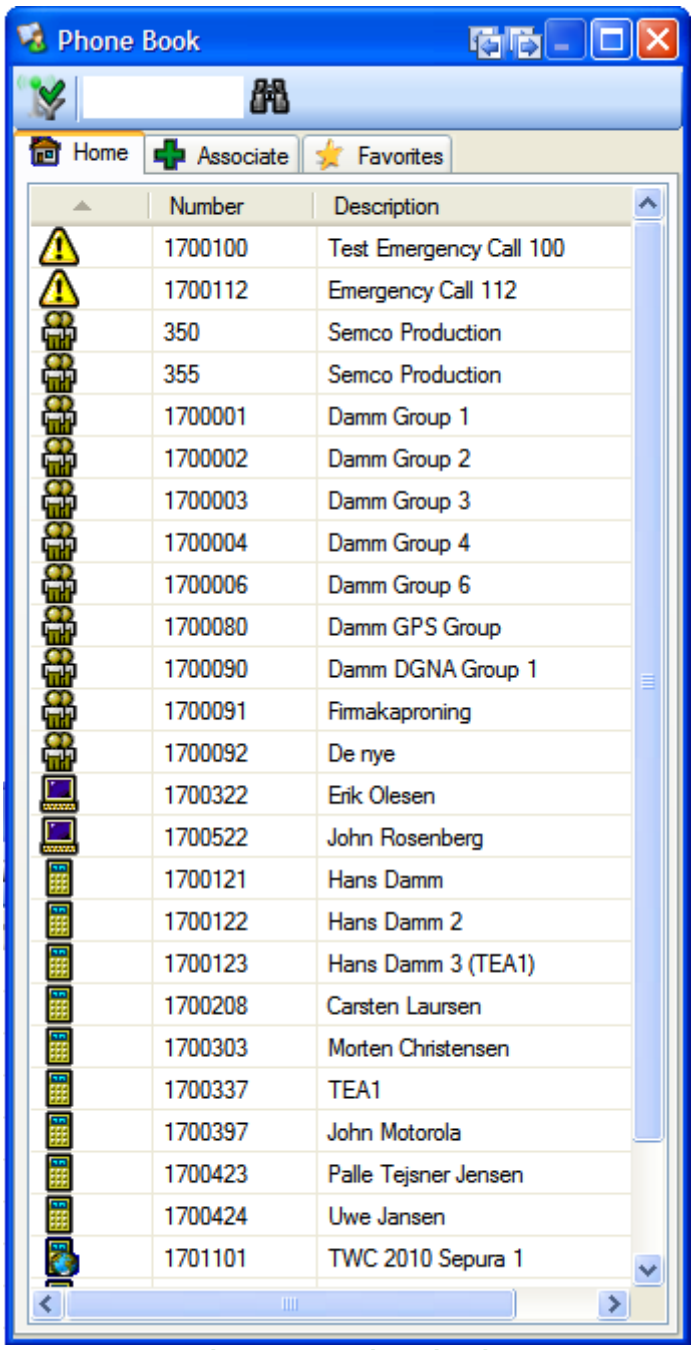


Figure 3-44: Phonebook

3.5.4.1 Mobile indicators in the phonebook

Indicates a mobile with a group selected
Indicates a mobile with a group active, but not selected in the mobile (scanned group)
Indicates a mobile which is not registered to the system

3.5.4.2 Phone book docking

The Phone Book window may be floating or docked either to the left or right edge of the dispatcher window. To dock, use the left or right arrow in the top bar of the phone book and to float use the floating symbol

3.5.4.3 Phone Book Search

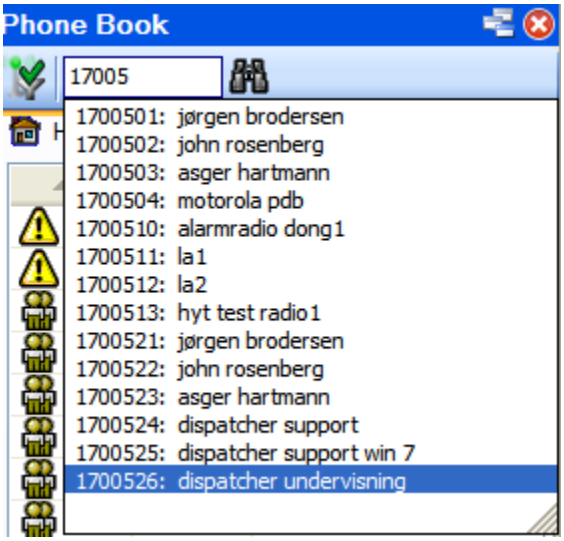
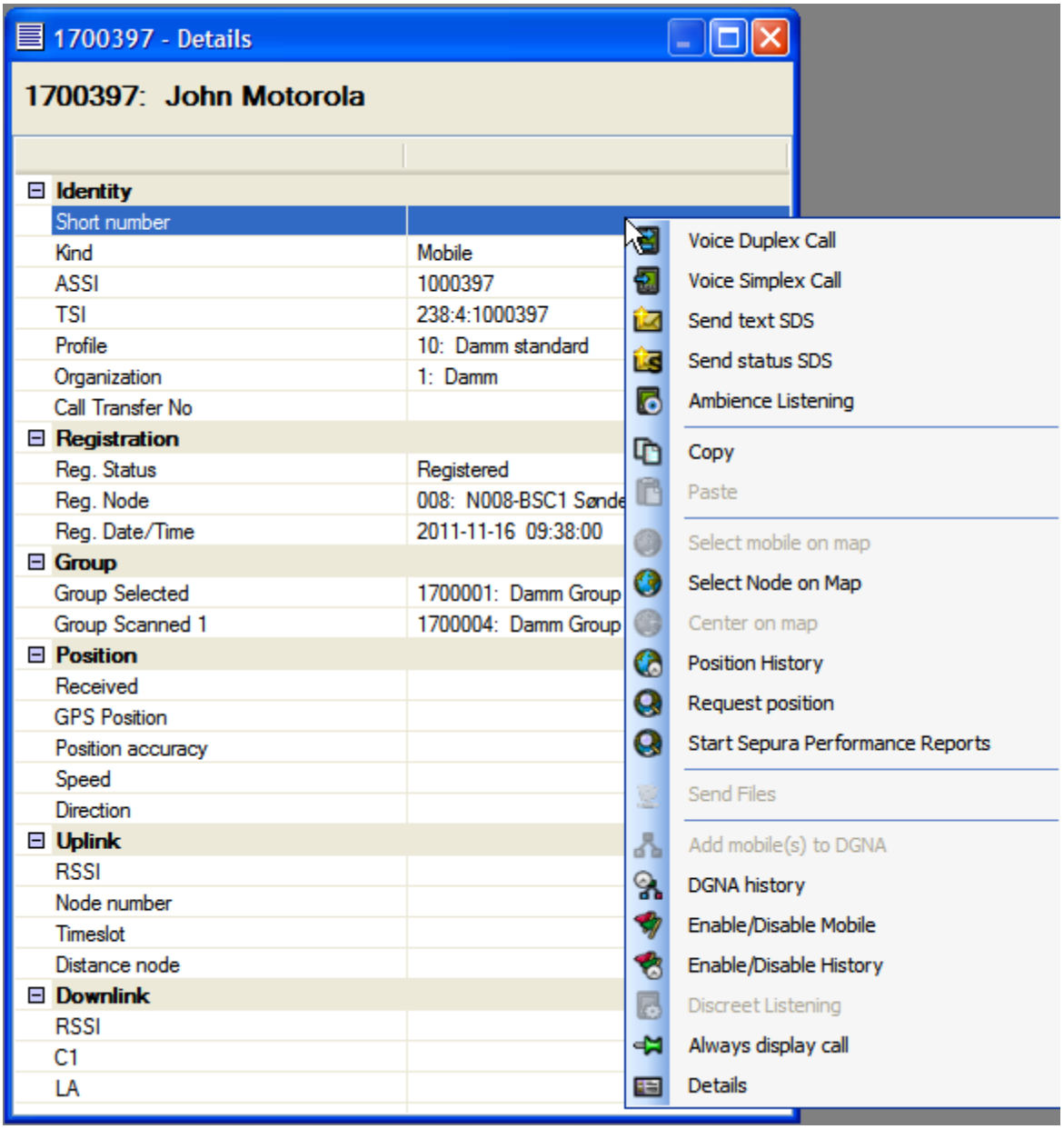


Figure 3-45: Search dialogue

It is possible to search for a user number, SSI or name, in the Search field. When double clicking on a subscriber the details dialog is shown. By right click in detail view you can select the call you want to establish.



3.5.4.4 Direct call

When double click on a subscriber in the Phone list you can establish a direct standard (group call if a group SSI, Individual duplex call if an individual SSI etc.) to these subscribers.

3.5.4.5 Call dialog

To manually initiate a call, right click on the desired subscriber (in this case a group)

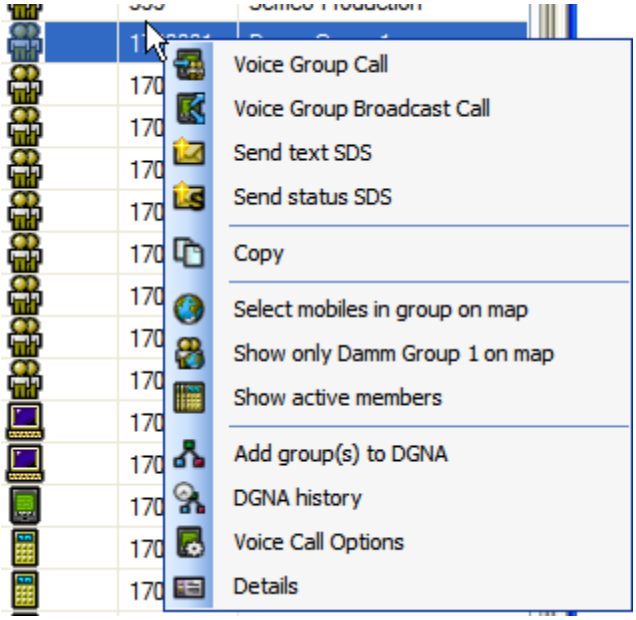
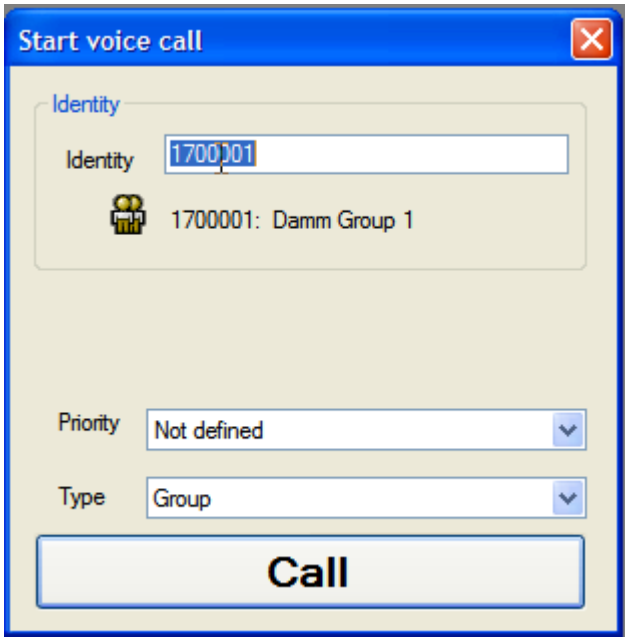


Figure 3-46: Group Call dialogue

Then select the function required



It is possible to change the **Priority** of this call and **Type**.

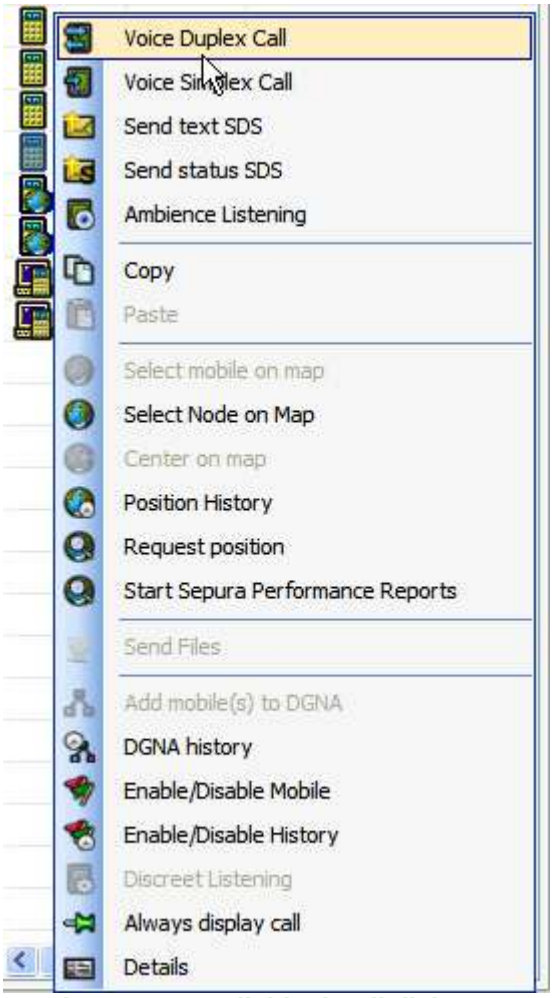


Figure 3-47: Individual Call dialogue

When the desired subscriber is found, right click on the result and select the desired function to be performed from the call dialog

NOTE: Selections may be active or grayed out according to the subscriber selected configuration

3.5.4.6 Show Associated Organizations

When selecting **Associated** from the Phone book menu, the subscribers in Associated Organizations are shown and the functions that you can perform are similar to the Home Organization list

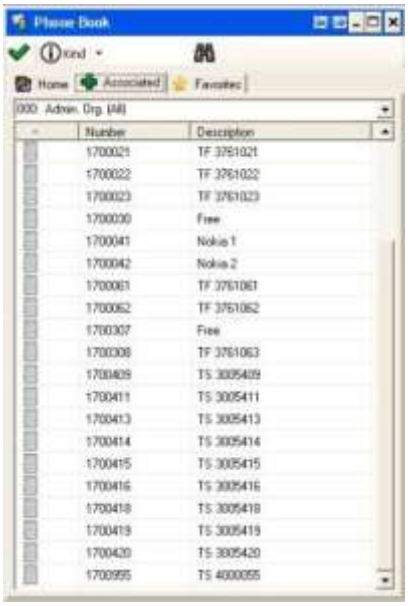


Figure 3-48: Associated organizations

3.5.4.7 Show favorites

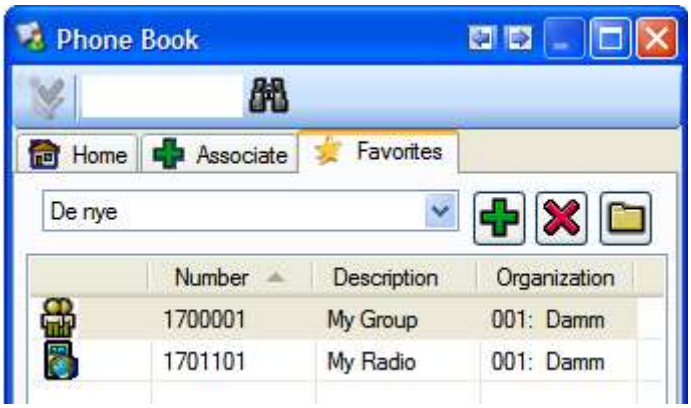


Figure 3-49: Favorites

In favorites, any number reachable form the infrastructure can be entered, this includes Tetra SSI's, PABX/PSTN numbers etc. and the Description can be changed without changing it in the subscriber register.

3.5.4.7.1 Show only registered subscribers

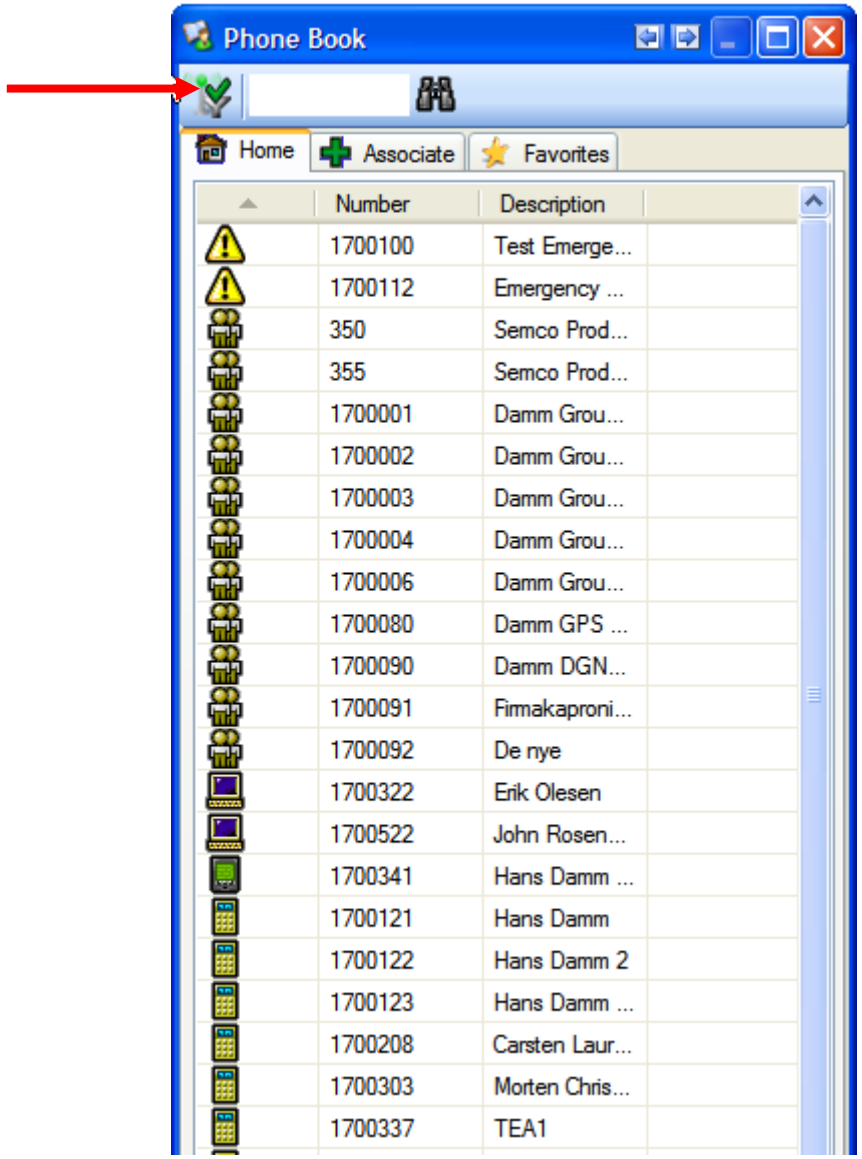


Figure 3-50: Subscriber view

This function allows the view of either all subscribers or only subscribers currently registered at the system. When all subscribers are selected, non registered subscribers will be shown as grayed out.

NOTE: Subscribers which has registered in the system and who leaves without proper deregistration (pulling off the battery, out of coverage etc.) will still show as registered until a proper de-registration has taken place

3.5.4.8 Voice Calls

The Voice Call window can display all ongoing call activity; this includes group calls and all types of individual calls (only if discreet listening option is set in the dongle and BSC settings). All calls are shown as a separate line in the voice call window. The call line includes call information. Any call from and to the dispatcher and any call between terminals is shown with one active call line per call.
The active call line indicates in its title bar whether it is an individual- or a group call, please see Figure 3-51 and Figure 3-53.
In a simplex call, where speech only flows in one direction at a time, the active call line has an active PTT button.

3.5.4.9 Subscriber always displayed

For subscribers frequently used, it is possible to transfer the subscriber to the Voice Call window on a permanent basis, making the call more simple (Just press the PTT button)

To do this either drag the subscriber (Group or individual) from the phone book and drop it in the Voice Call window or, for group calls, right click on the subscriber, select “Voice Call Options” and “ Always shown”

To remove from the Voice Call window, right click on the subscriber and select “Display only when active”

Figure 3-51: Active Call window with group calls

3.5.4.10 Volume control

During active calls, it is possible to adjust the call volume individually for each call.This is done by moving the slider positioned between the LS and MIC icons up or down. While moving, the level change in dB will be shown.
When the specific call is ended, the volume will be reset to 0 dB

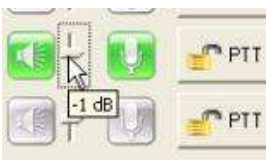


Figure 3-52: Call volume control

3.5.4.11 Master PTT button

The master PTT button allows more calls to be executed simultaneously, like a kind of broadcast.

Selecting a call or number of calls using the field to the right of the standard PTT button, the field(s) will show an  icon indicating that the call has been selected for master PTT.

When the master PTT button is pressed, calls will be made to all selected subscribers.

To revert to a single subscriber PTT when more is selected for master PTT, double click on the desired subscribers' master PTT icon and all other selections will be reset

3.5.4.12 USB foot switch

Master PTT activation can be configured to be executed by means of a USB foot switch (DAMM delivered. For configuration of the foot switch, please refer to the instructions delivered with the switch)
In the main menu bar select "Config → Audio" then go to the bottom of the configuration page and change the Master PPT key settings to the desired value 

, normally F13 (Default)

Figure 3-53: Active Call window with master PTT

3.5.4.13 Standard PTT Button

The standard PTT button  is shown as a standard windows button with an "open-lock" icon.
The PTT is requested only when the PTT button is pressed. However if the mouse is released over the lock icon then the icon is changed to a "closed-lock"  icon and the PTT will stay in the requested state until the button is pressed again outside the lock icon.

The PTT can be used also for a duplex call if the microphone is muted 
When the microphone is muted, then the microphone is temporary open when pressing the PTT (Dark green icons ).

The temporary muted microphone is shown with a light green icon with a red cross 

3.5.4.13.1 Alternative audio devices

To add audio to a second audio device present and selected in the configuration menu (headset, micro telephone, second sound card etc.) use mouse right click on the audio icon.
Added devices are shown in dark green with a speaker icon inserted 
The audio device is configured from the Audio tab in the Dispatcher Configuration dialog.

3.5.4.14 Audio device error

Errors in assignment of an audio device are indicated by a red configuration icon on the main tool bar  .A common reason for this is when the Windows Audio device level is set to 0 or no sound card installed.

During an active call, error icons  will be shown in case the maximum number of voice streams allowed (dongle configured) is exceeded for the call

3.5.4.15 Standard voice call

The voice call window has provisions for fixed display of a group in the window making it faster to select and call the group. A displayed fixed group is indicated by a green pin in the phonebook group icon

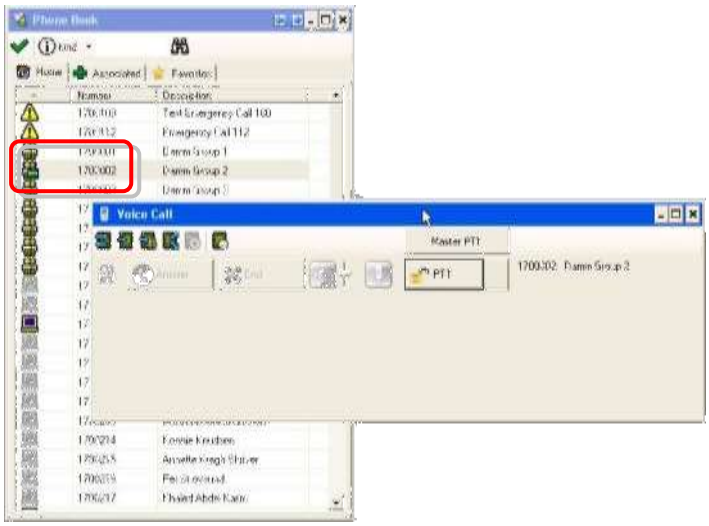


Figure 3-54: Fixed Group Indication

To select fixed groups, right click on the phonebook group and select Voice Call Option

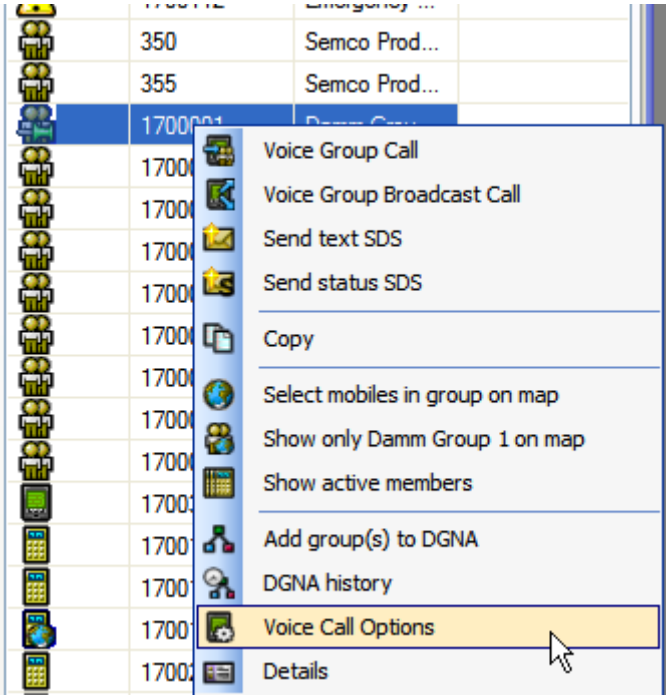


Figure 3-55: Voice call Option

Then select **Always Displayed** in the option menu

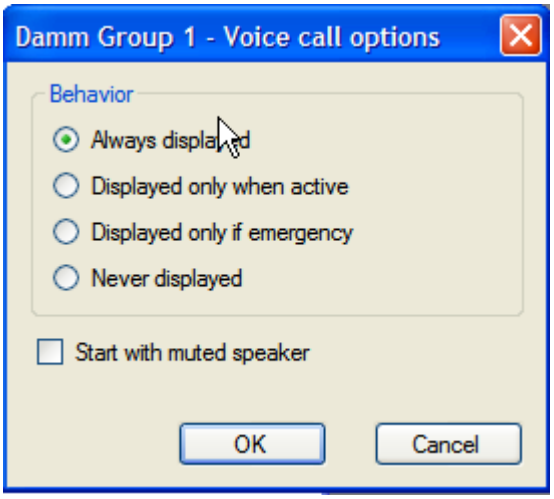


Figure 3-56: Always Displayed

To deselect, use the **Never displayed** option or one of the other options.

3.5.5 Call Authorized by Dispatcher (CAD)

This service is configured in the subscriber register profile and allows the dispatcher to verify call requests before calls are allowed to proceed. This is a useful service to utilize when radio user discipline needs to be maintained. This service also reduces the amount of radio traffic on a network as only essential work related calls are permitted. However, the frequent need for all communication between terminal users and the time delay experienced in authorizing calls may make this service unacceptable for some user organizations.

Service restrictions may be set up as Yes, CAD or No, where “Yes” will allow the service, CAD requires the dispatcher defined in the relevant profile to authorize the service, and No will disallow the service. NOTE that the restrictions are not active until “Activate Service Restrictions” is selected

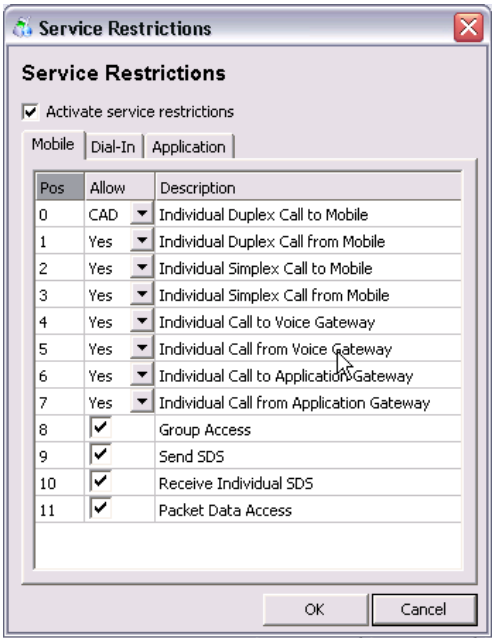


Figure 3-57: CAD Service Restrictions

3.5.6 Call Merge (dispatching)

This service allows the dispatcher to through connect a calling party to any other subscriber. Just call the desired subscriber and, when connection is established, drag the calling party (using the left user icon) to the new subscriber, drop it and confirm the connection.

This function also allows merging of two ongoing calls

Figure 3-58: Call Merge

3.5.7 Receiving Emergency calls

Emergency calls will be indicated in the Voice call window as a red bar containing the standard voice call options.
Also an alarm tone will be played and the ADU200 relay contacts will close. Alarms can be reset by answering / selecting the call

Figure 3-59: Emergency Call

In case the call is not answered, the missed call icon in the main tool bar will turn red and a red notification line will be added to the Voice call history window

Figure 3-60: Missed emergency call

Double clicking on the missed call icon with missed call window closed, will open up the Voice Call History with the missed call filter activated to enter the corrective action handling.

Figure 3-61: Missed Emergency Call

The icon will be shown as either answered  or missed 

3.5.8 Voice Call History

The Voice Call History logs the call activity of the Dispatcher. In this window it is possible to see the call information. All call activities are time stamped and logged and all responses from the infrastructure are logged as well.

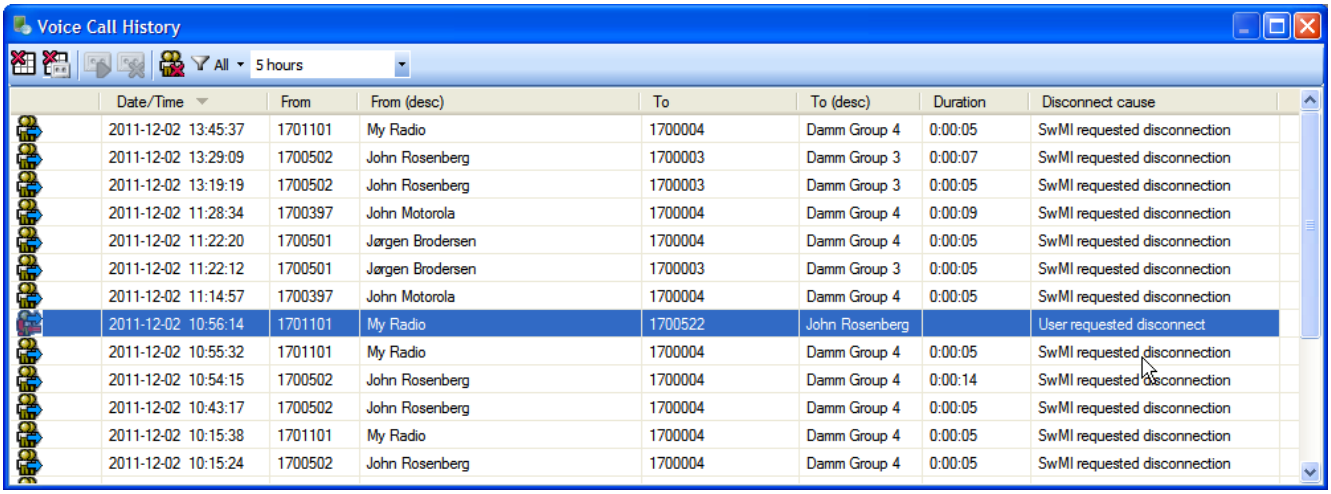


Figure 3-62: Voice Call History

 Clears the Voice call History list

 Clear all voice recording from the dispatcher

 Playback voice recording. The Icon is grayed if no there is no voice recording on the call history line you have selected.

 Clear the voice recording on the selected call history line

 Show / hide group calls

Filter for showing All, Incoming, Outgoing and Missed calls in the voice call history list.

Selecting the time period shown in the voice call history list (1 hour to 3 month)

In the voice call history list is possible to sort the different columns by clicking in the column header.

By clicking a voice call line it is possible to playback the voice recording, but only on lines with green indication