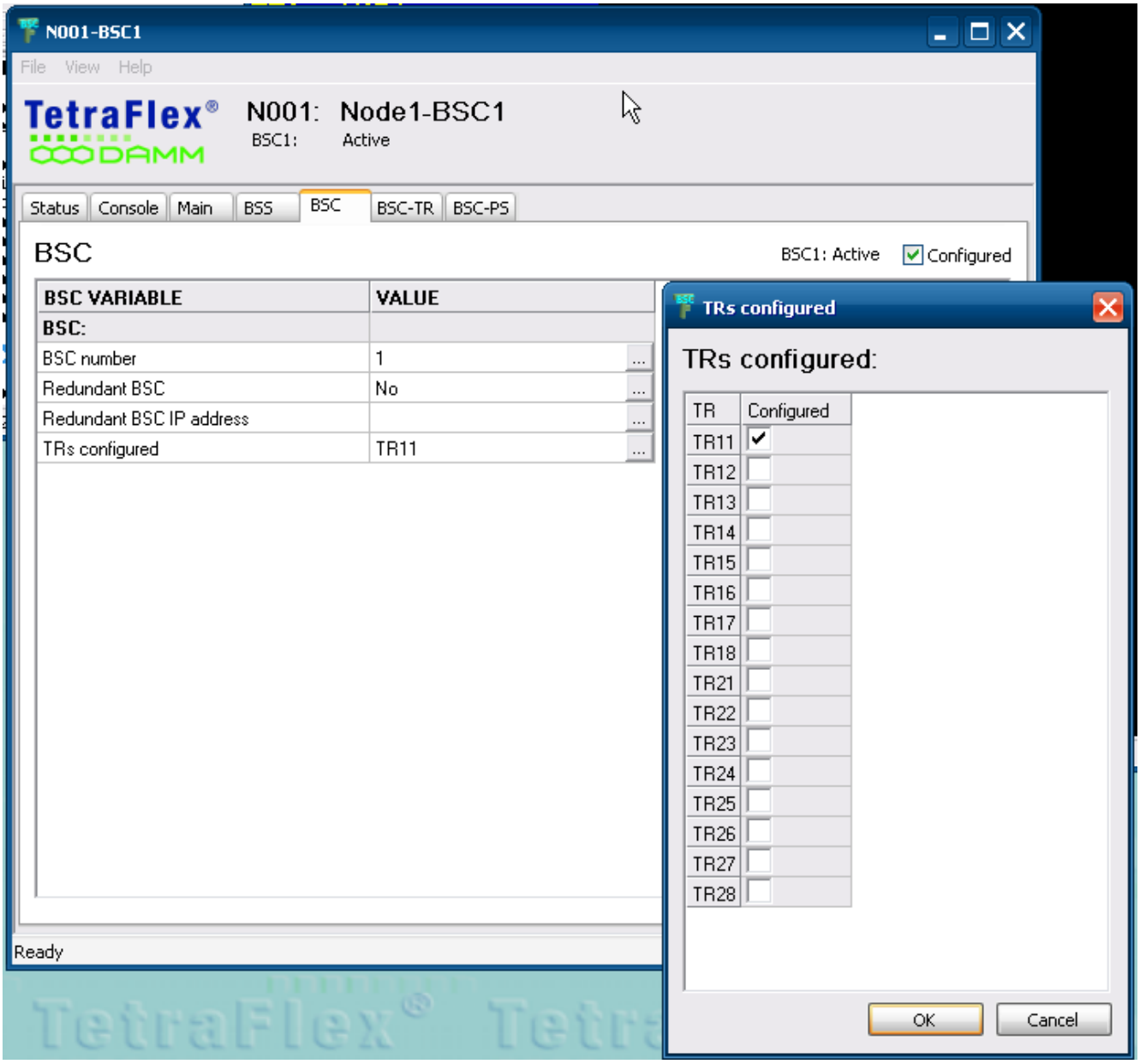
2.6.4 Add a transceiver

Adding a transceiver to a SB421 can be done either from the BSC-GUI or using OM command:

BSC-GUI:



Select the BSC tab and click on the TR's configured menu and then add the TR. When clicking Ok the setting is saved.

TetraOM: connect to the BSC Perform the following commands:

F75 <Enter>

This shows the configuration for TR 11-28
If the displayed message does not correspond to the actual number of TR, perform the command: F75/xx/ADD (F75/xx/REMOVE removes the TR again). xx =TR number e.g. 11.

2.6.4.1 Diversity configuration

Two TR421 may be used without the RF coaxial connection between them. In this case the system will behave normally as a 2 carrier system, but will NOT support diversity.

When using diversity set-up (Standard configuration), the RF coaxial connection must be installed and RX-B input (6dB pre gain) must be set

This configuration also applies to the 4 carrier configuration, where the carriers are defined as two 2 carrier systems.

2.6.4.2 RX-B setting (Diversity) in TetraOM:

24 Display setting
24+ Select RX-B input Cascaded (Standard setting)
24- Deselect RX-B input Cascaded

NOTE: This must be configured in both BS421

2.6.4.3 3 And 4 carrier operation

NOTE: Operation with 3 and 4 carriers with redundant BSC require a change to the HW of the BS421 and the SB421 (See the SB421 section for details) if the HW version stipulated on the serial number label is v1.
HW version v2 and forth has the possibility to change the setting via the TetraOM program.
This change is required to ensure correct BSC handover and synchronization of the carriers
The change cannot be made in the field. The system must be ordered for 4 carrier operation or the units may be returned to DAMM for modifications.

NOTE: For change in the field (trained staff only), please order a change kit from DAMM This kit includes a manual dealing with this issue and the necessary hardware, jumpers, screws, markings etc.

For a 4 carrier system, 2 of the BS421 is marked “MASTER” and 2 are marked “SLAVE”
One master and one slave are to be connected to each SB421, the master being TR1/TR3 and the slave TR2/TR4.

NOTE: A GPS antenna should at least be connected to TR1 and TR3

2.6.4.4 Synchronization

The TETRA Base Station TR's need to be time synchronized to operate correctly.

Most important, all TR's in a radio cell shall be time synchronized to ensure correct timing for the mobiles, when switching from the control channel to a traffic channel on another TR.

For a multi-cell systems, all radio cells are also recommended to be time synchronized to enable use of seamless handover (cell re-selection).

The Damm BS system has a flexible system to provide synchronization between individual Transceivers. Build-in GPS Receivers give absolute time synchronization to the radio cells. External Inputs can also be marked as Primary Sync. References.

When a BS is Network locked, automatic frequency correction of the Master Oscillator (RX and TX carrier frequencies) is provided, and Seamless Handover to other Network Synchronized Cells is activated.

The BS can be setup to run as either Sync Master 0 to 4 or Slave. The Masters shall preferably be provided with GPS antennas or an External Primary Sync source. The remaining BS's shall be setup as Slave and does not need a GPS antenna.

The BS421 is provided with one External 1PPS (1 Pulse Per Second) output and two external 1PPS inputs. The Slaves shall receive external 1PPS inputs connected to Masters.

In addition to the hardware 1PPS, sync messages are send every second on IP from the Masters to attached BS's.

A Master will indicate Master Mode, if:

1) Synchronized to the internal GPS RX or
2) Synchronized to an External Input marked as Primary and indicating Master Mode

The priority can be changed with OM command 72/MASTER/c
(c = 0-4 or S)

Master **0** priority:
1) Int. GPS RX
2) Ext. Master 1, Master Mode
3) Ext. Master 2, Master Mode
4) Ext. Master 3, Master Mode
5) Ext. Master 4, Master Mode
6) Ext. Master 1, Resync-only
7) Ext. Master 2, Resync-only
8) Ext. Master 3, Resync-only
9) Ext. Master 4, Resync-only
10) Int. Free-Run

Master **1** priority:
1) Ext. Master 0, Master Mode
2) Int. GPS RX
3) Ext. Master 2, Master Mode
4) Ext. Master 3, Master Mode
5) Ext. Master 4, Master Mode
6) Ext. Master 0
7) Ext. Master 2, Resync-only
8) Ext. Master 3, Resync-only
9) Ext. Master 4, Resync-only
10) Int. Free-Run

Master **2** priority:
1) Ext. Master 0, Master Mode
2) Ext. Master 1, Master Mode
3) Int. GPS RX
4) Ext. Master 3, Master Mode
5) Ext. Master 4, Master Mode
6) Ext. Master 0
7) Ext. Master 1
8) Ext. Master 3, Resync-only
9) Ext. Master 4, Resync-only
10) Int. Free-Run

Master **3** priority:
1) Ext. Master 0, Master Mode
2) Ext. Master 1, Master Mode
3) Ext. Master 2, Master Mode
4) Int. GPS RX
5) Ext. Master 4, Master Mode
6) Ext. Master 0
7) Ext. Master 1
8) Ext. Master 2
9) Ext. Master 4, Resync-only
10) Int. Free-Run

Master **4** priority:
1) Ext. Master 0, Master Mode
2) Ext. Master 1, Master Mode
3) Ext. Master 2, Master Mode
4) Ext. Master 3, Master Mode
5) Int. GPS RX
6) Ext. Master 0
7) Ext. Master 1
8) Ext. Master 2
9) Ext. Master 3
10) Int. Free-Run

Slave priority:
1) Ext. Master 0, Master Mode
2) Ext. Master 1, Master Mode
3) Ext. Master 2, Master Mode
4) Ext. Master 3, Master Mode
5) Ext. Master 4, Master Mode
6) Ext. Master 0
7) Ext. Master 1
8) Ext. Master 2
9) Ext. Master 3
10) Ext. Master 4
11) Int. GPS RX
12) Int. Free-Run

If no GPS synchronized Master or higher prioritized free-running Master is available at re-start, Masters will try initially to synchronize to lower prioritized free-running Masters.

A BS will resync automatically after a short time if Century Second and Phase Detector are out of sync with a valid sync source.

Masters shall be setup even if GPS antennas are not used and internal GPS RX is deselected, to ensure proper synchronization between all TR's.

Typical 1-carrier BS421 configuration:

- TR11: Master 1

OM command: 72/MASTER/1

Typical 2-carrier BS421 configuration with GPS on both carriers:

- TR11: Master 1
- TR12: Master 2
- TR11-OUT connected to TR12-IN1
- TR12-OUT connected to TR11-IN1

OM command:

TR11

72/MASTER/1
72/IN/G/+
72/IN/1/+
72/IN/1/-/172.016.001.012/000.0
72/OUT/172.016.001.012/+

TR12

72/MASTER/2
72/IN/G/+
72/IN/1/+
72/IN/1/-/172.016.001.011/000.0
72/OUT/172.016.001.011/+

Typical 3 or 4-carrier BS421 configuration:

- TR11: Master 1 (Powered of SB421-1)
- TR12: Slave (Powered of SB421-1)
- TR13: Master 2 (Powered of SB421-2)
- TR14: Slave (Powered of SB421-2)
- TR11-OUT connected to TR12-IN1, TR13-IN1 and TR14-IN1
- TR13-OUT connected to TR11-IN1, TR12-IN2 and TR14-IN2

  Interconnection board 1 second pulse sync indicators flashes synchronous when in sync

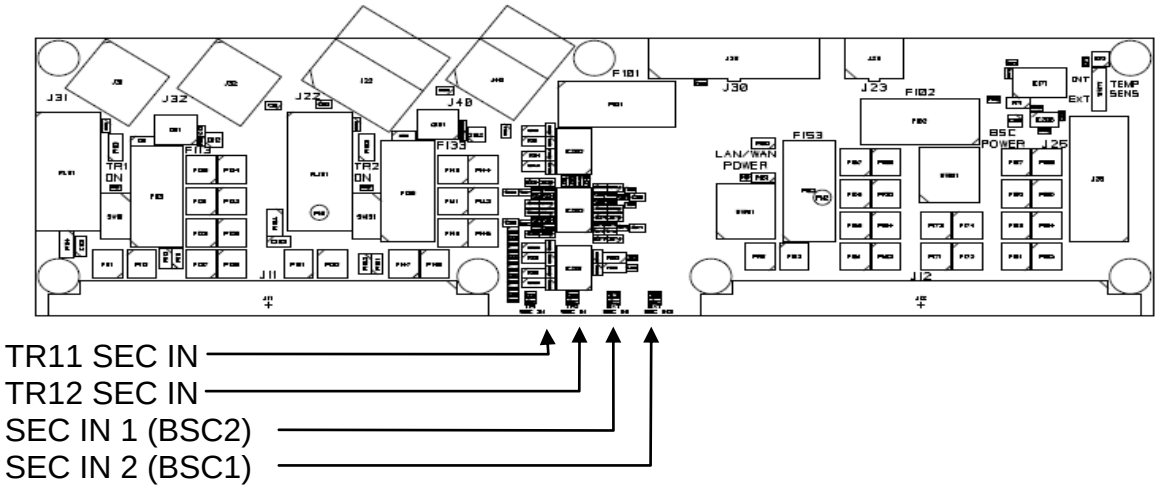


Figure 2-20: 1 second Sync indicators

NOTE: HW changes to SB421 interconnection board and TE2 and TR4 required

2.6.4.4.1 GPS setup commands

To enable GPS synchronization execute the following TetraOM commands: 72/IN/G/+

2.6.4.5 BS421 manual frequency adjustment procedure

If the BS is operating without GPS sync. (Free run) the reference oscillator has to be checked and adjusted one time a year.
Measure the BS421 transmitter frequency, the transmitter can be switch to CW mode for easier measurement.
Commands :

01+	;Local blocking
02/-	;Test mode
15/CW	;CW modulation
10+	;Start transmitter

Commands to adjust the reference oscillator:

31	;Display Sync status, note the DAC output value (OCXO Free Run value)
31/SET/nn.nnn	;Set the OCXO Free Run value, range from 00.000% to 99.999%
31/SAVE	;Save the OCXO Free Run value to flash

A change of 1% will give a frequency change about 0.1PPM

2.7 BS41x Configuration

2.7.1 Turn on Base Station power

Turn on the BS Power by turning on the switches on the front of the PS411 Power Supplies and the Mains outlet.

Power-up will take 2-3 minutes, mainly determined by the start-up time of Windows operating system on the BSC. After Windows re-boot and BSC start-up, all TR41x will re-boot, and the BSC red alarm LED turns off and the green Active LED turns on.

If a TR41x is not configured in the BSC, the yellow Power LED on the TR41x will proceed to flash.

During power-up the Power LED of the PS411 Power Supplies will flash until they receives configuration from the BSC.

2.7.2 Special precautions

NOTE: Batch commands (B/….) are not supported on TR411 and TR412 using the HDLC bus

2.7.3 Set-up of IP address

The IP address and net-mask shall be set-up in BSC412 Windows settings as the first configuration step. This is done either with:

- Connect a monitor and USB keyboard / mouse directly to the BSC or
- Connect your PC to the BSC via an Ethernet cable (crossed or straight rough) or
- Start-up Remote Desktop and connect to the IP address of the WAN Ethernet port

And then:

- Configure IP number, net-mask etc. to the required configuration for the LAN and WAN

Default factory settings (can be ordered to specific settings):

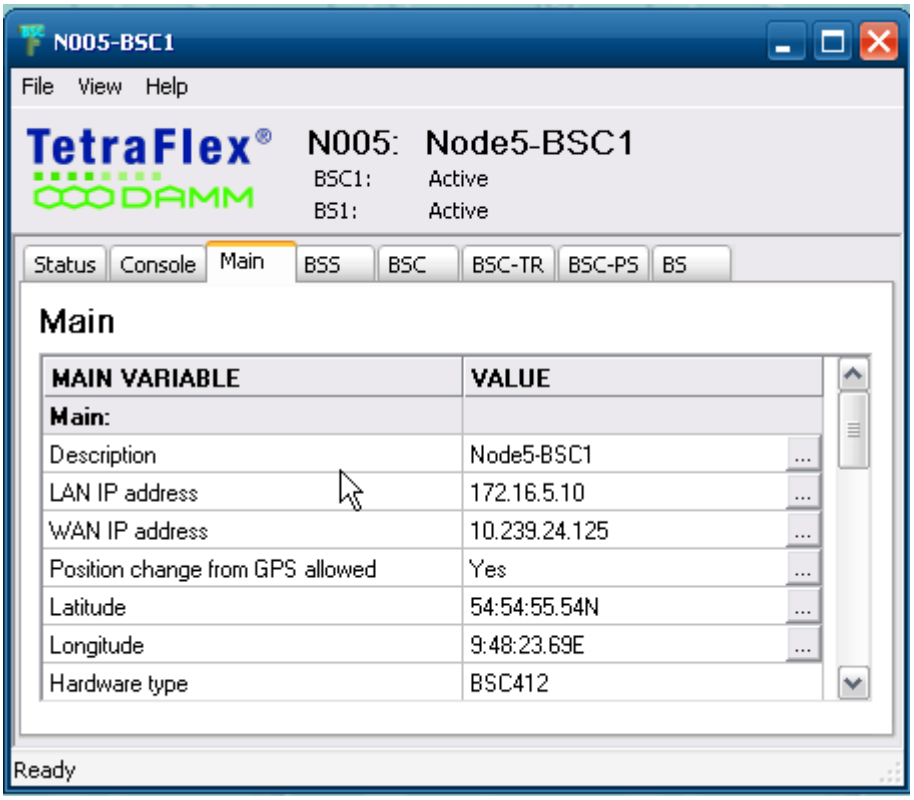
BSC1 LAN: 172.16.1*.10
BSC2 LAN (red.): 172.16.1*.19
BSC1 WAN: DHCP
BSC2 WAN: DHCP

* 1 for single node, or node1 in multinode. This will be 2 for node2 etc.

2.7.4 Setting the main parameters

The settings can be set and changed from the BSC GUI or with OM commands. Both are described in this chapter.

The BSC-GUI can be started from the Start menu – TetraFlex – BSC - BSCGUI:



First set the Main parameters from the Main tab

Description: e.g. Node5-BSC1 OM command M71/DESCR/NODE5-BSC1

The string should contain a description of the node or the geographical position of the BS site. If it is a single-carrier BS with directional antenna, the direction can also be included.

LAN IP address: Use the drop down box to select the LAN address setup from the Windows IP setting as described in 2.7.3. OM Command M71/IPADDR/LAN/172.016.005.010. The IP address must match the Windows LAN IP setting.

The example shows BSC1 in a multinode configured to Node 5.

WAN IP address: Use the drop down box to select the WAN address setup from the Windows IP setting as described in 2.7.3.
OM Command M71/IPADDR/WAN/010.239.024.125. The IP address must match the Windows WAN IP setting.

The example shows the WAN address set to match the company WAN IP address range.

Position change from GPS allowed: If set to "Yes" the Latitude and Longitude GPS coordinates are received from the GPS antenna and overwrites the settings in the *Latitude*

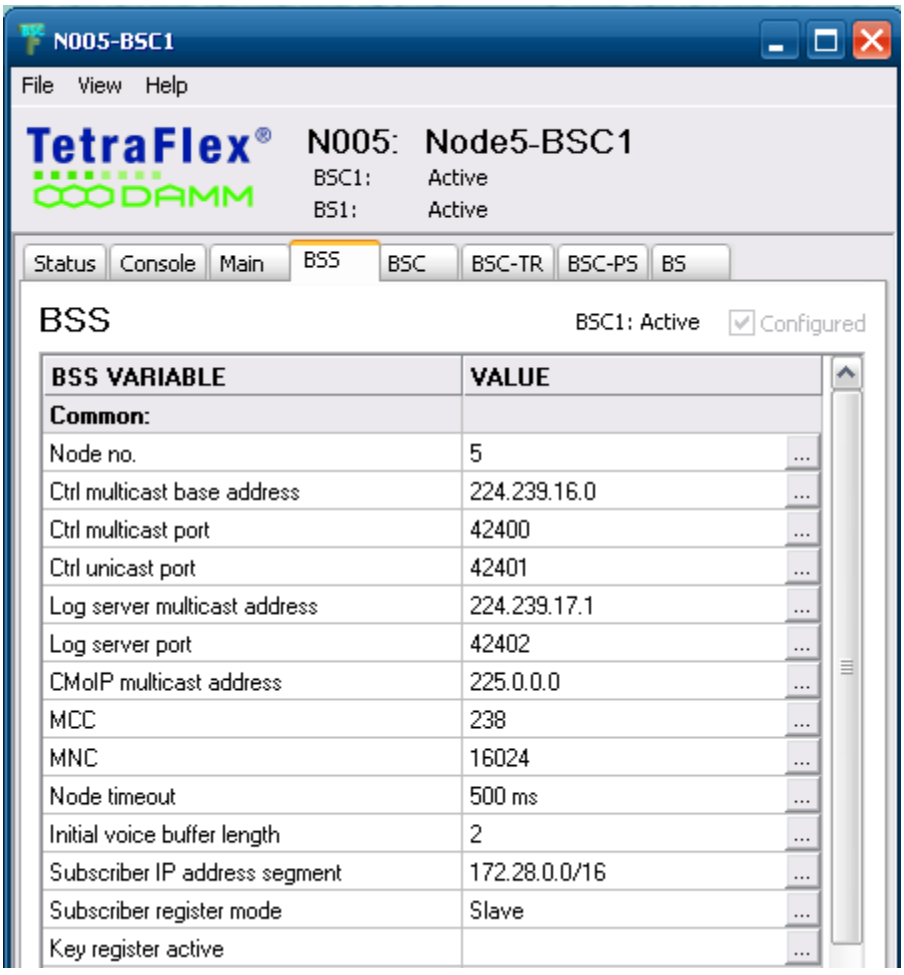
and *Longitude* fields. Set to “No” the Latitude and Longitude settings can be set manual. OM command M71/POS/GPS/+ for “Yes” and M71/POS/GPS/- for “No”

Latitude and Longitude: Manual setting of the Latitude and Longitude coordinates of the Node, This will be overwritten with the actual GPS position if *Position change from GPS allowed* is set to *Yes*. OM command H71/POS/54:54:55:54N/009:48:23:69E

All settings are saved immediately in the configuration file *CnfgMain.txt* when pressing the Ok button in the different settings and when executing the OM commands.

The rest of the fields on the Main tab are for information only and cannot be changed from the BSC-GUI.

Next step is to set the BSS settings- Select the BSS tab:



Most important is to set the **Node no**. This must be set to chosen node number. This example shows Node 5. OM command S71/NODENO/005

The remaining parameters can be set from NM too.

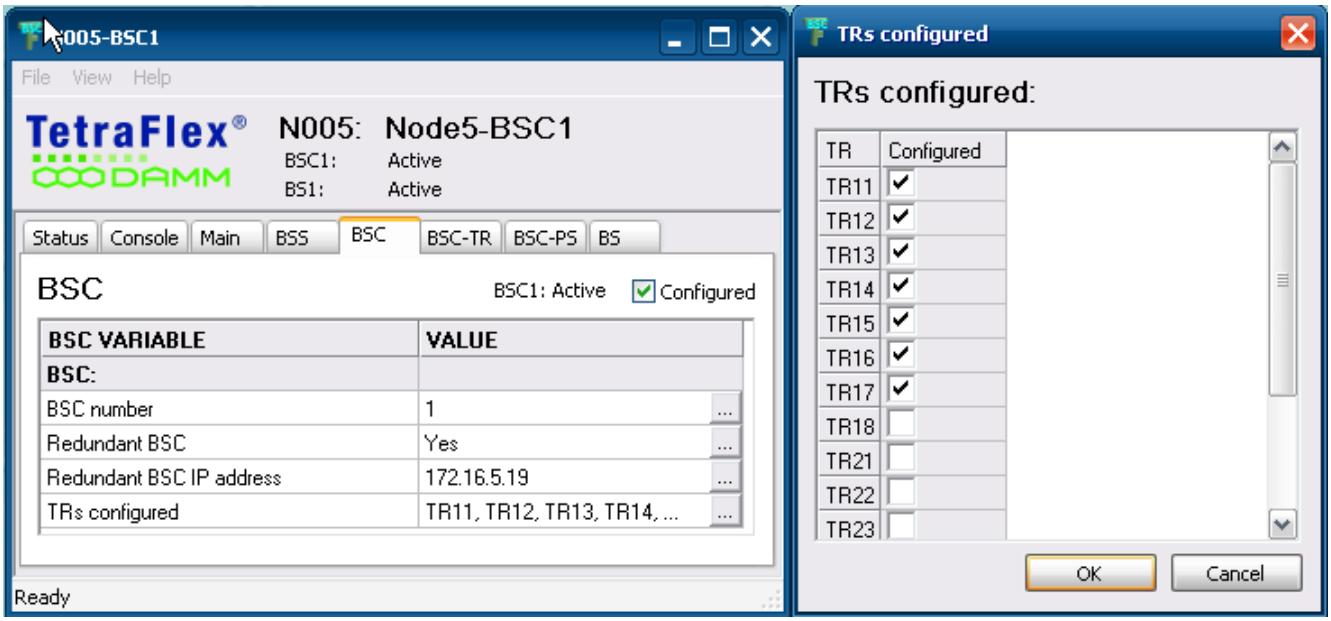
Setting redundant BSC see ref. 5 “TetraFlex 7.5 BS41x redundant setup.pdf”

2.7.5 Add a Transceiver

A new TR412 Transceiver can be inserted “live” into the Rack. If already configured in the BSC, the TR412 will automatically start-up. Before removing a TR412 it should be blocked and the TX stopped.

The settings can be set and changed from the BSC GUI or with OM commands. Both are described in this chapter.

The BSC-GUI can be started from the Start menu – TetraFlex – BSC - BSCGUI :



The Transceivers can be added and deleted from the BSC tab. OM command

F75 - to view configured TR’s
F75/nn/ ADD - To add new transceiver, where nn reflects the TR position 11 to 18

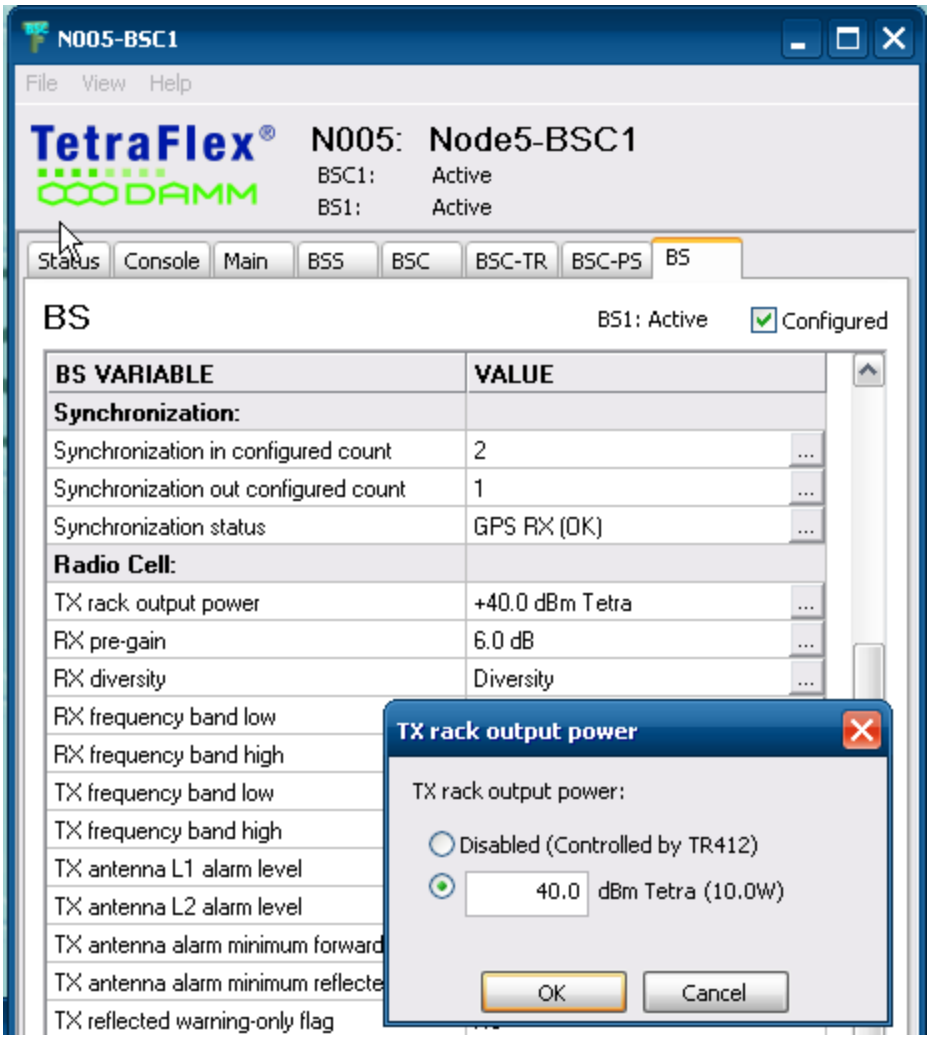
All TR412’s should be configured in the BSC.

The current TR configuration can be displayed from the BSC-TR and BS tab and OM command:

05 - Display Config /Status from BSC
13 - Display TX output power selection
22 - Display RX diversity selection
30 - Display RX-TX channel numbers
72- Display RX settings

2.7.6 TX Power

Setting the desired TX power level for all TR41x use the BSC-GUI, BS-Tab select the TX rack output power:



The setting is Tetra Mode output power at Rack TX Antenna connector. An insertion loss of the combiner system of 4.0dB is assumed. If the value is lower or higher than the TR412 limits, the TR412 will set the power to the minimum or maximum power respectively.

If set to Disabled (Controlled by TR412) the output is set to 0

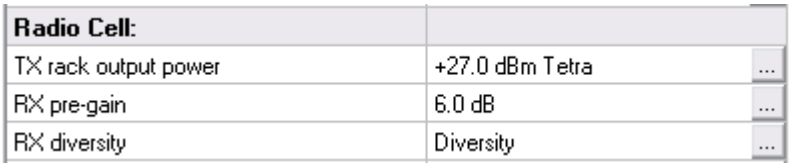
	Ant. conn. Tetra Power	TR412 Power
Standard TR412	+26.0dBm to +40.0dBm	1.0W to 25.0W
High power TR412	+30.0dBm to +44.0dBm	2.5W to 62.5W

OM Command:

H73/TXPWR/+nn.n -Change TX output power (at Rack TX connector)
nn.n: Output power (26.0..44.0 [dBm]), 00.0: Disabled (controlled of TR412 setting)

2.7.7 Diversity

Setting-up the diversity and TMA/TMD pre-gain can be done from the BSC-GUI, BS tab. Select RX pre-gain and RX diversity:



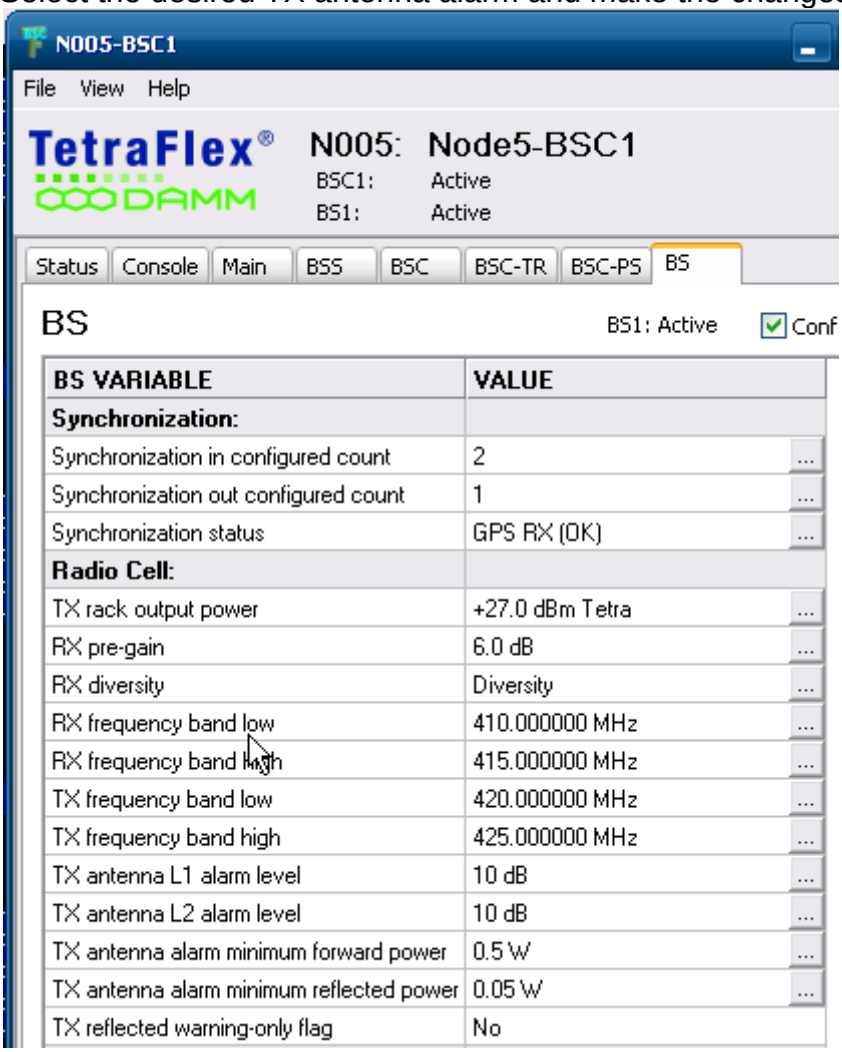
OM Command:

F73/RXDIV/n Where n reflects the diversity type
D = Diversity
A = RX-A antenna only
B = RX-B antenna only

F73/RXPREGAIN/n.n Where n reflects the dB value 0.0 to 9.9 (nominal 6.0)

2.7.8 TX alarm

Setting -up the TX antenna alarm configuration can be done from the BSC-GUI, BS tab. Select the desired TX antenna alarm and make the changes:



OM Command:

F73/TXANT/xx/yy/z.z/0.nn Where:

xx reflects TX antenna level 1 alarm setting 06 to 16 dB return loss
yy reflects TX antenna level 2 alarm setting 06 to 16 dB return loss
z.z reflects minimum forward power 0.2 to 9.0 watt
nn reflects minimum reflected power 0.01 to 0.99 watt

2.7.9 Add a Power Supply

A PS411 Power Supply can be inserted into and removed from the rack during normal BS operation. Before it is inserted or removed, be sure, that both switches on the front plate are in OFF position.

The PS411 automatically receives the configuration from the BSC at start-up. The configuration can be checked from the BSC-GUI - BS Tab

or with the command:

H76/nn/ADD

Where nn reflects the PS411 cassette position 11 to 47

2.7.10 Combiner adjustment

The combiner can be adjusted with this OM command:

A11	Address TR1
10	Check that Tx is on else Turn on TX with 10+
AT11	Address select combiner 1A (AT12 = combiner 1B)
01+	Local blocking on
12	Display TC test points (should be as close to 0 VDC as possible)
13/1/+	Increment fine adjust setting (TC1 in combiner 1A)
13/1/-	Decrement fine adjust setting (TC1 in combinder 1A)

Use 13/X/+ and - to adjust until you get the lowest possible VDC, check with OM 12 for each adjustment. X is TC number (1-4), Change to TC that needs adjustment

13/1/EE++++ Save setting for TC1 (not automatically saved without this command)

01 - Set local blocking to off again

2.7.11 Antenna measurement

Use the following OM command to check the antenna and cable conditions:

AU+ (AU/FORCED if there are no connection)
A12 – Shift to TR2
01+ local blocking conditional request
10/AUTO/D disable auto Tx
10+ Turn on Tx
32+ Turn on RFTL high
23+ Rx antenna measurement command

The measurement must show a value around -20dBr (+/- 3dBr) a lower value may indicate a bad receiver antenna (or cable)

Set local blocking to off again

01- Local blocking off

2.7.12 Save BSC and TR configuration

The various settings are from TetraFlex® version 7.5 saved automatically when making changes from BSC-GUI or OM-commands.

2.7.13 TMA/TMD installation adjustment

2.7.13.1 Introduction

This guide describes how to adjust the BS41x Tetra Base Station after installation of the TMA412 RX Tower Mounted Amplifier. The instruction is also valid only if the TMD412 is provided, as the TMD412 is identical to the TMA412 except for the additional Duplexer.

The TMA is to be connected with the BS using 3 shielded cables with a maximum insertion loss of 8dB. The adjustment procedure requires the loss of all 3 feeders to be identical.

The adjustment is done to adapt the TMA to the selected output power of the TR and to compensate the actual loss of the 3 feeders.

The TMA including feeder loss and AI411 input attenuation is recommended to run with a pre-gain of 6dB. This has been chosen as a compromise between sensitivity and dynamic range. It is not recommended to operate a higher gain.

Output power in analogue NMT/MPT mode is fixed to be twice the output power in Tetra mode. The following equivalent input levels at the TMA input from the RFTL are recommended:

Mode	RFTL level	TMA input (+6dB)	TR input
Analogue	**High**	**-105dBm**	**-99dBm**
Tetra	**High**	**-108dBm**	**-102dBm**
Analogue	**Low (-10dB)**	**-115dBm**	**-109dBm**
Tetra	**Low (-10dB)**	**-118dBm**	**-112dBm**

Note that RFTL low level (-10dB) is not supported in the first versions of the TR411.

2.7.13.2 Tools and Equipment

Operating the TetraOM System requires a PC to be connected to the BS, a screwdriver, and a short test cable.

The test cable must be a 50 cm long RG214 cable with two N-male connectors.

2.7.13.3 Adjustment Procedure

Step 1: Prepare the adjustment:

- Connect the PC to the BS, log-on and address a TR to be used for the adjustment. Any TR connected to the node can be used.
- Make Local Blocking (01+)
- Select test mode CW (02/- and 15/CW)
- Check the TX output power to be set to the required value (13).
- Check, the TMA pre-gain to be 6.0dB (72)
- Key the transmitter (10+) and activate the RFTL (32+)
- Display RSSI (R/21/0)
- Turn the 3 attenuators on AI411 “GAIN A”, “GAIN-B” and RFTL “OUT” to maximum RSSI (minimum attenuation).

Step 2: RFTL input level adjust
This step adjusts the RFTL input attenuator to give a fixed level on the RFTL mixer independent of the selected output power:

The attenuation shall be adjusted to the following:

TR power (Tetra)	TR power (Analogue)	Attenuator
25W	50W	15dB
12W	25W	12dB
6W	12W	9dB
3W	6W	6dB
1.5W	3W	3dB

- Turn RFTL input attenuator to minimum attenuation
- Register the RSSI
- Increase attenuation until the RSSI has decreased to the value from the table

Step 3: RFTL output level adjust
This step adjusts the RFTL output level at the BS TMA Test Connector to be correct, if the feeder loss is 8dB.

- Remove the feeder on the Test connector on top of the rack.
- Remove the feeder on the RX-A connector on top of the rack
- Connect the test cable between the Test connector and the RX-A connector.
- Adjust the RFTL out attenuator to give an RSSI of –47dBm on TR41x input.
- Remove the test cable and re-connect the feeders again

The –47dBm is related to the nominal test signal level of –105dBm at the TMA, with a coupling loss in the TMA in forward direction of 50dB and a feeder loss of 8dB.

Step 4: Feeder loss compensation adjust
This step adjusts the RFTL output attenuator and the RM input attenuators to compensate the feeder loss.

- Register the RSSI on the TMA input. If step 1 and 2 has been done correctly, the reading should be –105dBm, if the cable losses are 8dB. If the cable losses are less than 8dB, the input levels will be higher than –105dBm. The feeder loss will be: Feeder loss = 8-(105dBm+RSSI)/2 dB.
- Adjust with AI411 RFTL "OUT" the RSSI TMA input reading exactly half the way down to –105dBm. For example if reading –100dBm then adjust to –102.5dBm.
- Adjust the AI411 "GAIN A" to an RSSI input level on TMA-A input of –105dBm.
- Adjust the AI411 "GAIN B" to an RSSI input level on TMA-B input of –105dBm.

Step 5: Restarting the Base Station

It is recommended to make a complete restart of the BS after the installation procedure has finished ensuring, that a correct automatic start-up after power-down will take place.

- Turn off all the Output switches on the PS411 front plates
- Turn on all switches again

Step 6: Before the Base Station is left, always check that:

- All TR units are un-blocked (01-)
- Line by-pass switch is OFF
- No RED alarm indicators are illuminated
- Door is locked

2.7.13.4 BS41x manual frequency adjustment procedure

If the BS is operating without GPS sync. (Free run) the reference oscillator has to be checked and adjusted one time a year.
Measure the BS41x transmitter frequency, the transmitter can be switch to CW mode for easier measurement.
Commands to TR412

```
01+             ;Local blocking
02/-            ;Test mode
15/CW           ;CW modulation
10+             ;Start transmitter
```

Commands to adjust the reference oscillator:

```
H31             ;Display Sync status, note the DAC output value (OCXO Free Run value)
H31/SET/nn.nnn  ;Set the OCXO Free Run value,  range from 00.000% to 99.999%
H31/SAVE        ;Save the OCXO Free Run value to flash
```

A change of 1% will give a frequency change about 0.1PPM

2.8 NETWORK MANAGEMENT INSTALLATION

2.8.1 The DAMM Network management Application

The Network Management software (NM) is preinstalled on every SB421/ BS41x delivered with TetraFlex® and need no installation to run.

NM may be executed on any node from a remote desktop connection to the node or with a keyboard/mouse and display connected direct to a SB421 or a BSC412.

You can also use a PC which has an IP connection to the infrastructure. The NM is able to listen to the multicast which means, when using a PC the PC must be connected to the LAN.

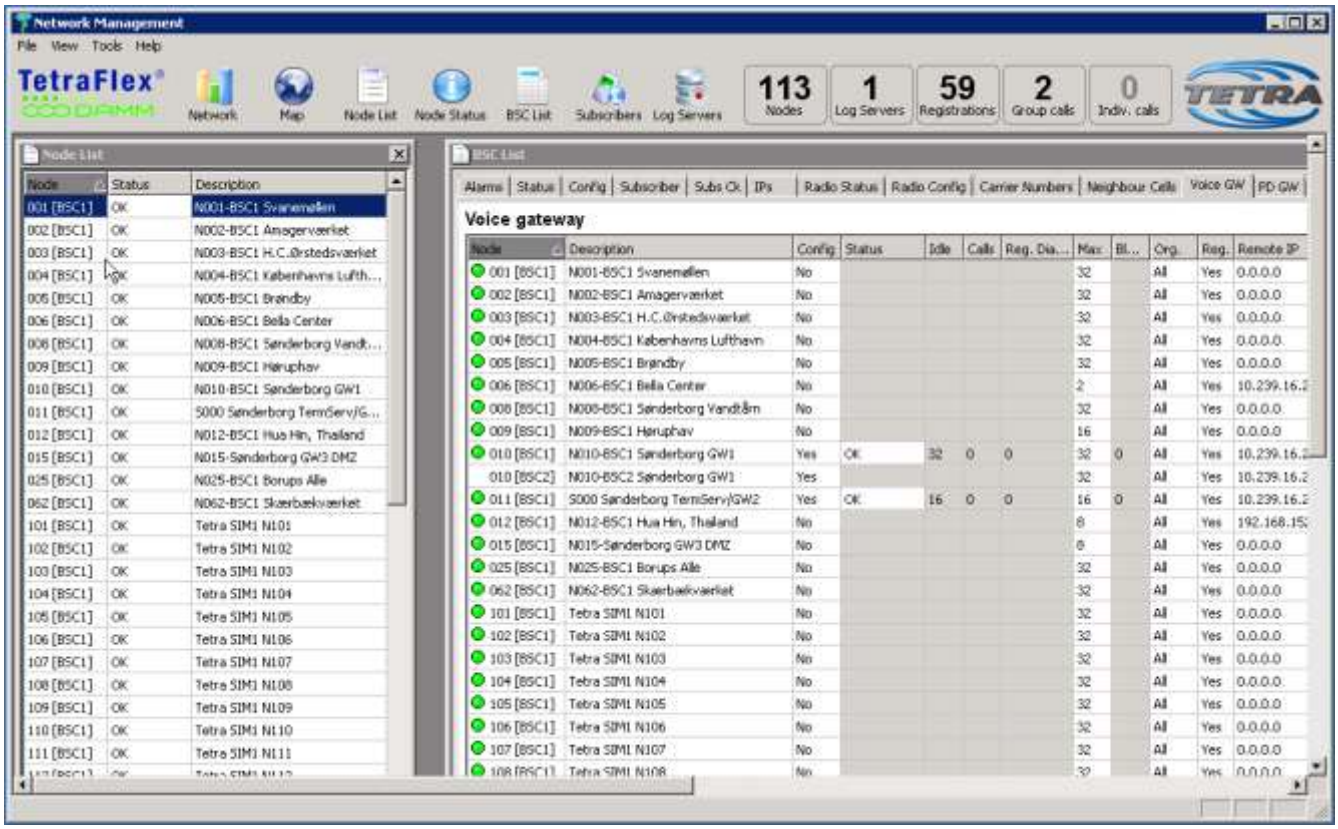


Figure 2-21: Network management main screen

2.8.2 NM Installation on an external PC

- If not already done, copy the Tetra directory from a BSC to the NM PC
- Execute the NM.vbs file. This will copy the NM program to the user profile and start up the NM application
- Create a shortcut on the desktop to the NM.vbs file

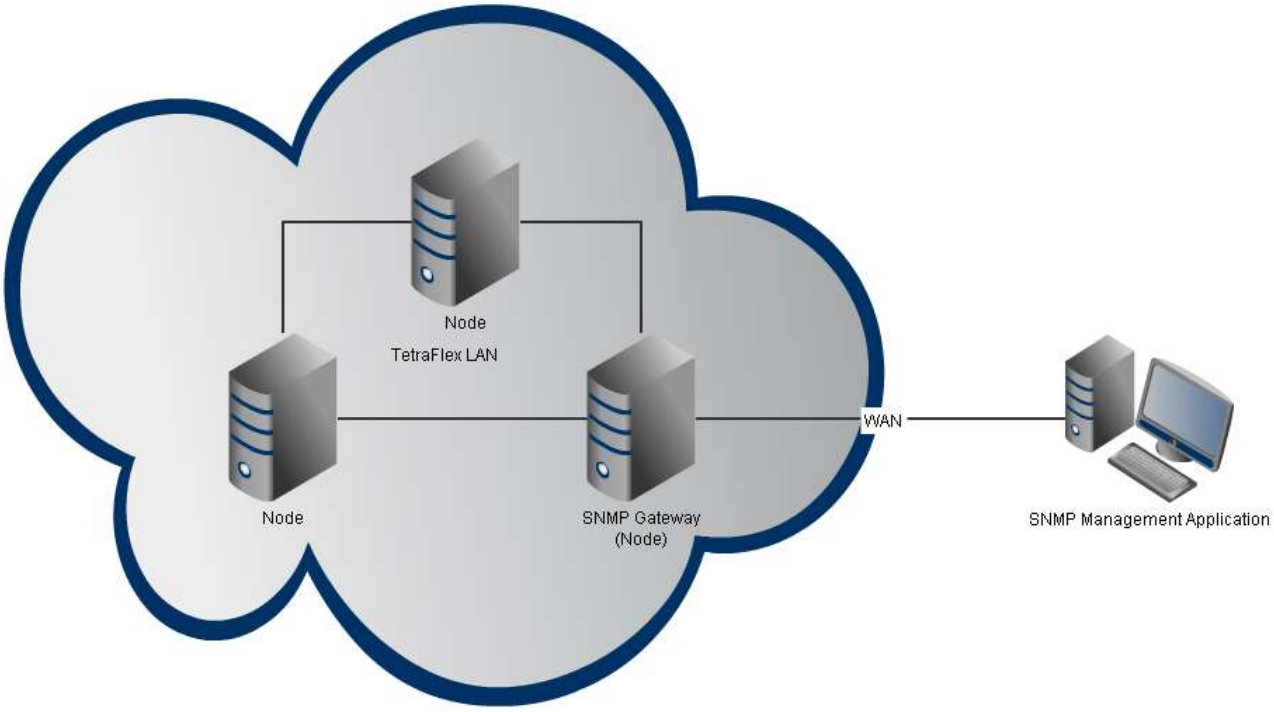
Refer to section 3.3.2 for NM User Manual

2.8.3 SNMP gateway

The SNMP gateway operates together with NM. To utilize SNMP you will need an SNMP Management Application. This application will gain access to the status of the TetraFlex network through the “SNMP Gateway”. This gateway could be a node in the TetraFlex network. In that case the PC which runs the SNMP Management Application will need to connect to this “SNMP gateway node” via the WAN connection.

The SNMP gateway must have the SNMP extension agent installed and will need to have NM running. NM is responsible for updating all of the node status variables, whilst the SNMP agent will service the SNMP requests.

The SNMP Management Application polls for the node status. Traps are not generated by the TetraFlex network. This is in accordance with recommendations found in the rfc1157.



The SNMP agent packets can be downloaded from www.damm.dk extranet software download site.

The SNMP agent packet consists of:

SNMPAgent.dll	This file is the actual SNMP extension agent. It works in correlation with the Windows SNMP service, which is already installed on the SB421 and BSC412. This extension agent is responsible for servicing SNMP requests.
SNMP_install.vbs	Script-file which will: • Stop the Windows SNMP Service. • Copy SNMPAgent.dll to SNMPAgent_.dll • Import registry settings required to install SNMPAgent_.dll. • Modify registry settings to make the SNMP Gateway node auto logon with the “tetra” user. • Copy shortcut to NM.bat file into startup folder.

	• Start Windows SNMP Service.
SNMPInstall.reg	Registry file containing registry settings necessary to install the SNMP extension dll. The settings in this file will be imported by the SNMP_Install.vbs file.
NM.exe	Network Management application. NM is regularly updating the BSC variables, so that the extension agent is able to service the SNMP request with the latest info.
Network Management.lnk	Shortcut to the NM.bat file located under C:\Tetra\Active\Pgm\NM.
DAMM-GLOBALMIB. Mib	Damm MIB tree

2.8.3.1 SNMP installation

To install the SNMP agent on the SB421 or BSC412 complete the following steps:

1. Copy “DAMM-GLOBAL-MIB.mib” into the documentation folder of the BSC “C:\Tetra\Active\Doc\”.
2. Copy SNMPAgent.dll, SNMP_install.vbs, SNMPInstall.reg, NM.exe and Network Management.lnk to the SNMP gateway node. The files should be placed in C:\Tetra\Active\Pgm\NM.
3. Run the SNMP_install.vbs file to install the SNMP extension dll and registry settings.
4. Start-up the Network Management application (NM). NM should be set to auto start to start-up automatically when the computer is restarted. The SNMP gateway will not operate without the NM.

2.8.3.2 SNMP Manually PC installation

If the Damm SNMP agent is to be installed on a PC instead of a SB421 or BSC412, you will have to install the agent manually. To manually install the Damm SNMP agent do the following:

1. Make sure the Windows SNMP Service is installed on the PC. It can be installed via: “Control Panel” – “Add or remove programs” – “Add/Remove Windows components” – “Management and monitoring tools” – “Simple Network Management Protocol”.
2. Copy SNMPAgent.dll, NM.exe and Network Management.lnk to the PC. The files should be placed at C:\Tetra\Active\Pgm\NM.
3. Copy the SNMPAgent.dll, and rename the copy “SNMPAgent_.dll”.
4. Install the SNMPAgent_.dll by entering the following settings into the registry:

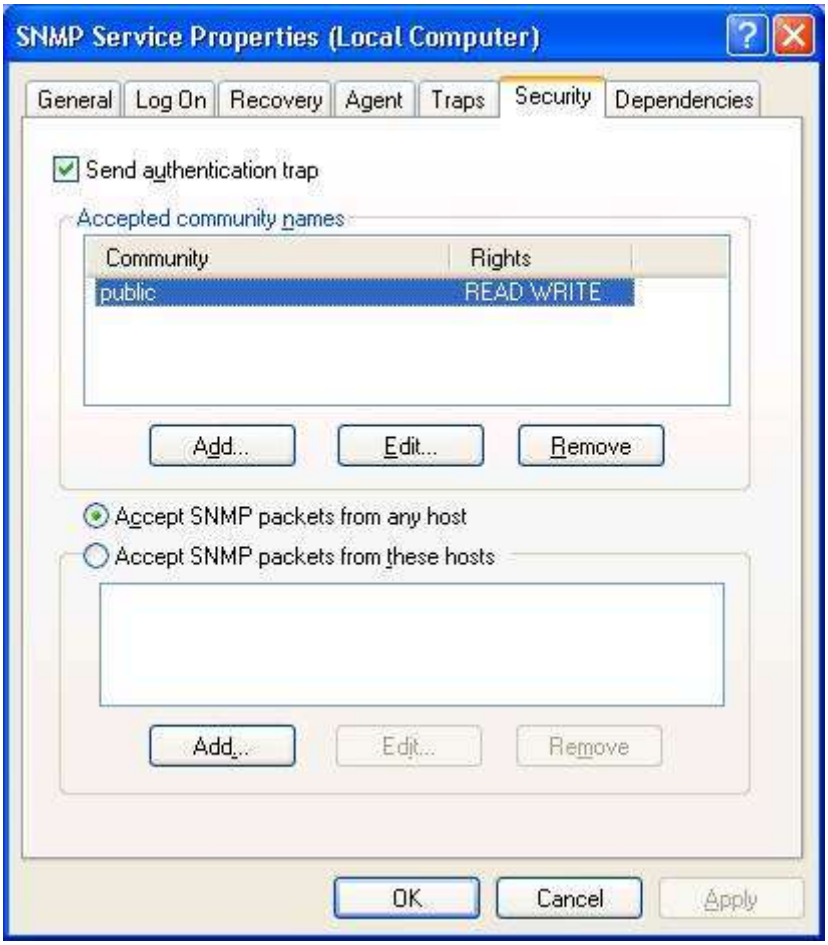
```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\Extensi
onAgents]
"TetraFlexSNMP"="SOFTWARE\\SNMP\\CurrentVersion"

[HKEY_LOCAL_MACHINE\SOFTWARE\SNMP\CurrentVersion]
"Pathname"="C:\\Tetra\\Active\\Pgm\\NM\\SNMPAgent_.dll"
```

5. Make the PC login automatically upon boot, by entering the following settings into the registry (exchange DefaultUserName and DefaultPassword with the correct username and password):

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"AutoAdminLogon"="1"
"DefaultUserName"="tetra"
"DefaultPassword"="tetra"
```

6. Place the Network Management.lnk file in the startup folder to make the Network Management application startup automatically upon boot..
7. Check the SNMP Security settings (start -> right click on ”my computer” -> manage -> Services and Applications -> Services -> SNMP Service -> Properties -> Security). These settings could be as shown in the example on the following figure:



A more safe solution is to restrict the SNMP access by ticking ”Accept SNMP packets from the hosts” and add the Host name, IP or IPX address of the specific known hosts.

8. Restart the Windows SNMP Service.
9. Start the Network Management application. NM should be set to auto start-up to make it start-up automatically when the computer is restarted. The SNMP gateway will not work without the NM.

2.8.3.3 SNMP MIB Tree

A SNMP Management Application uses the information in the DAMM-GLOBAL-MIB.MIB file for configuration and setup, please refer to the user guide for your SNMP Management Application to set it up.

SNMP gateway has been tested to work with WatchUp Gold 14.2

The following figure is a graphical representation of the DAMM-GLOBAL-MIB module (The Damm MIB tree).

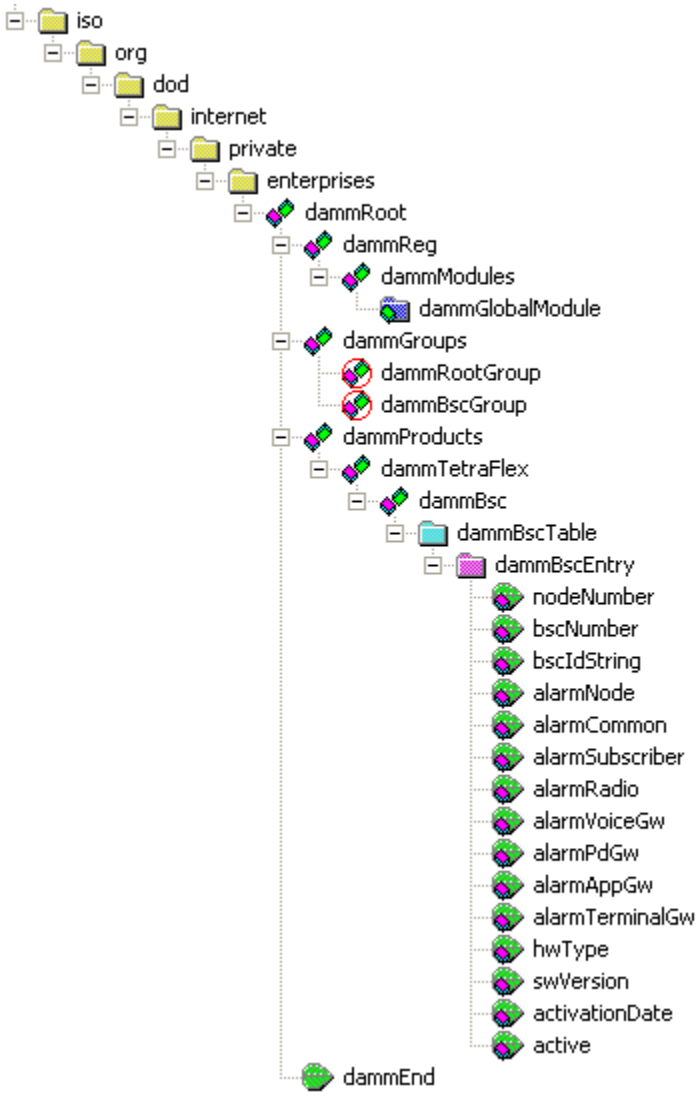


Figure 22: The DAMM-GLOBAL-MODULE

The most important variables are explained in detail in the following table.

Name	OID	Description
dammRoot	1.3.6.1.4.1.15228	The root of the Damm MIB tree.
dammGlobalModule	dammRoot.1.1.1	Contains info on when the MIB file was updated. This is not a scalar variable, which means the data is located in the mib file and isn't polled from the BSC.
dammBscTable	dammRoot.3.1.1.2	Contains a dammBscEntry for each BSC running in the system.
dammBscEntry	dammRoot.3.1.1.2.1	Contains each variable in a given BSC, which is going to be monitored.

nodeNumber	dammRoot.3.1.1.2.1.1	The node number of the BSC which is monitored. Values range from 1 to 999.
bscNumber	dammRoot.3.1.1.2.1.2	The BSC number of the polled BSC. Values range from 1-2. (Used for redundant BSCs).
bscIdString	dammRoot.3.1.1.2.1.3	The description for the given BSC.
alarmNode	dammRoot.3.1.1.2.1.4	Node alarm (0=OK, 1=Warning, 2=Alarm, 3=Blocked, 255=Not configured).
alarmCommon	dammRoot.3.1.1.2.1.5	Common alarm (0=OK, 1=Warning, 2=Alarm, 3=Blocked, 255=Not configured).
alarmSubscriber	dammRoot.3.1.1.2.1.6	Subscriber alarm (0=OK, 1=Warning, 2=Alarm, 3=Blocked, 255=Not configured).
alarmRadio	dammRoot.3.1.1.2.1.7	Radio alarm (0=OK, 1=Warning, 2=Alarm, 3=Blocked, 255=Not configured).
alarmVoiceGw	dammRoot.3.1.1.2.1.8	Voice Gateway alarm (0=OK, 1=Warning, 2=Alarm, 3=Blocked, 255=Not configured).
alarmPdGw	dammRoot.3.1.1.2.1.9	Packet Data Gateway alarm (0=OK, 1=Warning, 2=Alarm, 3=Blocked, 255=Not configured).
alarmAppGw	dammRoot.3.1.1.2.1.10	Application Gateway alarm (0=OK, 1=Warning, 2=Alarm, 3=Blocked, 255=Not configured).
alarmTerminalGw	dammRoot.3.1.1.2.1.11	Terminal Gateway alarm (0=OK, 1=Warning, 2=Alarm, 3=Blocked, 255=Not configured).
hwType	dammRoot.3.1.1.2.1.12	Hardware type (0=PC, 1=BSC421, 2=BSC412).
swVersion	dammRoot.3.1.1.2.1.13	Software version string.
activationDate	dammRoot.3.1.1.2.1.14	Activation date.
Active	dammRoot.3.1.1.2.1.15	BSC active status (1=active, 0=not active).

The DAMM-GLOBAL-MIB.MIB file can be found in c:\tetra\active\doc folder.

2.9 DISPATCHER INSTALLATION

2.9.1 The DAMM Dispatcher Application

The DAMM TetraFlex® Dispatcher is a Windows application consisting of the core TetraFlexApi.dll and the associated Graphical User Interface.

The DAMM TetraFlexApi.dll contains all the functionality to connect to the TetraFlex® Network and has a fully documented API to interface with the GUI.

The dispatcher is delivered with a Multi Lingual Graphical User Interface. The DAMM dispatcher is generic and intended for standard use. In case the user wants additional features, this may be accomplished by programming their own application or obtaining a third party application using the delivered TetraFlexApi.dll and the TetraFlexApi.h file

The TetraFlexApi.dll connects to an Application Gateway on a TetraFlex® node via a standard WAN IP connection.

For API installation, please refer to the Application Gateway installation section.

2.9.2 Dispatcher Installation:

The Dispatcher can only be installed outside the BSC, on a separate PC. It connects to the Application Gateway of the TetraFlex® through the WAN port.

Prerequisite for this connection to be successful is that the WAN port of an Application GW node is physically connected to a network - and that the WAN port of the BSC/ Windows is configured with an IP address inside the same subnet as the PC on which the Dispatcher is going to reside.

The dongle marked "API" must be inserted in the USB port of the Dispatcher PC before installing the Dispatcher. For the DAMM Dispatcher a dispatcher entry in the dongle must be present to allow the DAMM Dispatcher to start up. For a third party dispatcher, this entry is not relevant.

When the BSC.exe is started, the Dispatcher installation files are automatically placed in the C:\Tetra\Share\Dispatcher directory on the nodes:

Dispatcher_x86.msi	8.440 KB	Windows Installer P...	30-09-2011 14:59
Setup.exe	26 KB	Application	30-09-2011 14:59
SSCERuntime_x64-ENU.msi	3.568 KB	Windows Installer P...	07-09-2011 14:46
SSCERuntime_x86-ENU.msi	3.090 KB	Windows Installer P...	07-09-2011 14:46

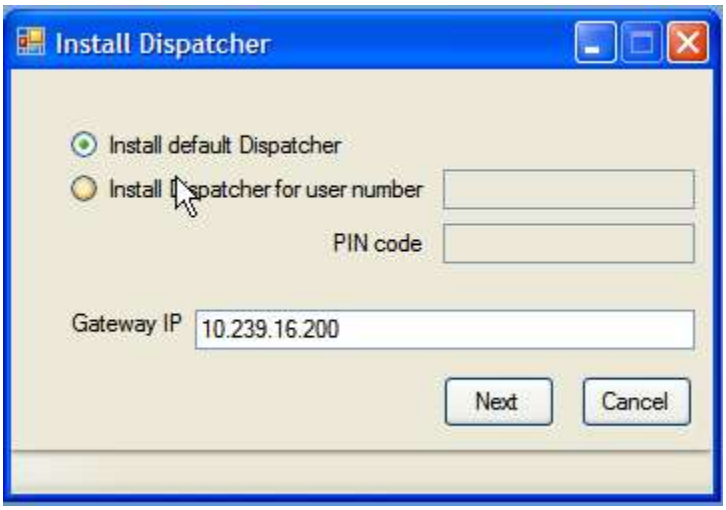
By accessing the share on the node where the Application Gateway is setup from an external PC, the Dispatcher Setup.exe can be executed and the Dispatcher installation starts.

The share looks like this seen from an external PC:

\\< IP address or node name >\TetraFlex\Dispatcher

< IP address or node name > is either the IP address or the DNS name of the node where youo install the Dispatcher from and where the Application Gateway is defined.

When the setup.exe program is executed this dialog comes up:



The dispatcher can be installed as default; this means that the dispatcher is installed in the directory c:\tetra\applications\dispatcher\default and the user number and PIN code has to be setup in dispatcher after the installation.

If using “Install dispatcher for user number” the user Application SSI number and PIN code that has been setup in the subscriber register must be typed in, in this case the Dispatcher is installed in the directory:

c:\tetra\applications\dispatcher\<user number> where the “user number” is the number you typed.

The installation process makes a shortcut to the dispatcher in the start menu on your PC:

“Tetraflex – Dispatcher 7.52 2011-10-14 – Default” where “date” is the date you made the installation followed by “Default” or the user number if the user number was used for the installation.

Please see also chapter 3 “Dispatcher” for setting up the dispatcher.

2.9.3 Dispatcher Installation on a PC with Windows 7

If problems occur with finding the node from where the dispatcher shall be installed, this setting in Windows 7 can help:

- click the start button and type secpol.msc in the search function.

- Browse to "Local Policies" -> "Security Options". Now look for the entry "Network Security: LAN Manager authentication level" and open it. Click on the dropdown menu and select "Send LM & NTLM - use NTLMv2 session security if negotiated". Apply the settings.

- In the Advanced sharing settings page of Network and sharing center, you need to set it as Work/Home profile. How to do it:

- -Enable network discovery
  -Turn on file and print sharing
  -Turn off password protected sharing
  -Use user accounts and passwords to connect to other computers

2.9.4 Configurations to be done on the node

The Application gateway must be enabled on the node where the Dispatcher has to be connected to, and the Application SSI must be defined in the subscriber register.

This can be done from the Network Manage (please see the relevant chapter in Network manager).

The following OM command can also be used to check the settings:

- M71 to verify the correct IP address of the BSC WAN.
- S75 and S75/CNFG/+ to check and enable the application gateway in the BSC.

2.10 LOG SERVER

Warning: When installing the Log Server on a system with a former database version, the log server backs up the old database and Log Client and starts up with a blank database. To view the content of the old databasse, use the back'ed up version of the Log Client.

2.10.1 General Description

The TetraFlex® Log Server software is delivered in 3 versions: Build in the BS41x and SB421, external Log Workstation and external Log Server.

The TetraFlex® Log Server software is installed as a service named "LogServer", which automatically starts when the windows system is powered up.

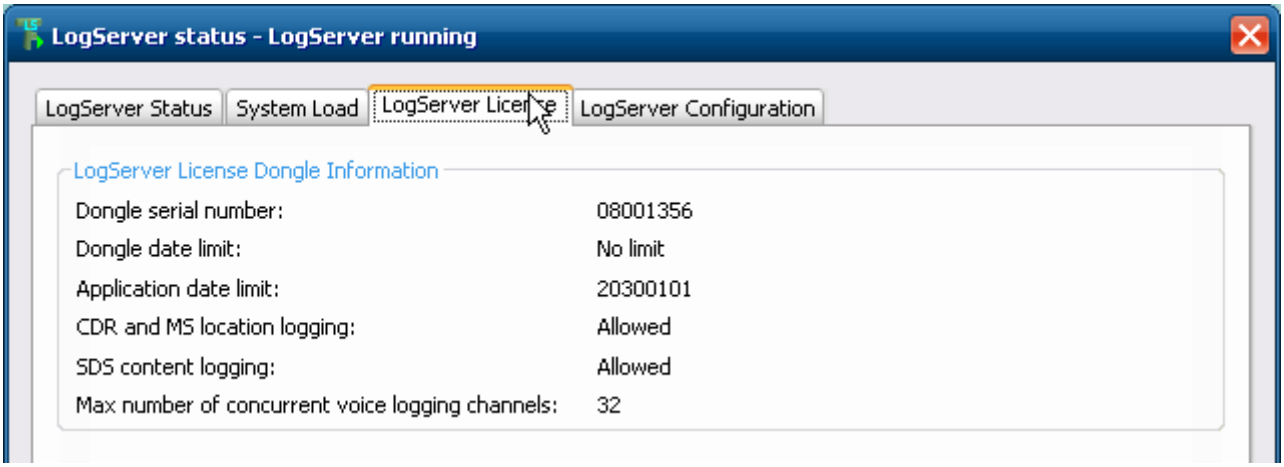
2.10.2 LogServer License

The TetraFlex® Log Server requires a USB License dongle to run. The dongle has two purposes, to protect the TetraFlex® Log Server software from being illegally used without any software license, and to store essential configuration and licensing values.
The dongle has a selection of settings, some of which are payable

The dongle must be present on the unit (BS41x, SB421, Log Workstation, and Log Server) where the TetraFlex® Log Server application is installed else it will not be able to run.

The log server is capable of logging statistics data if only a valid DAMM dongle is installed, but if CDR, Voice logging, MS registration and SDS logging is needed this must be set in the dongle.

From the log *server tray – LogServer License tab*, the following configuration values read from the dongle are shown:

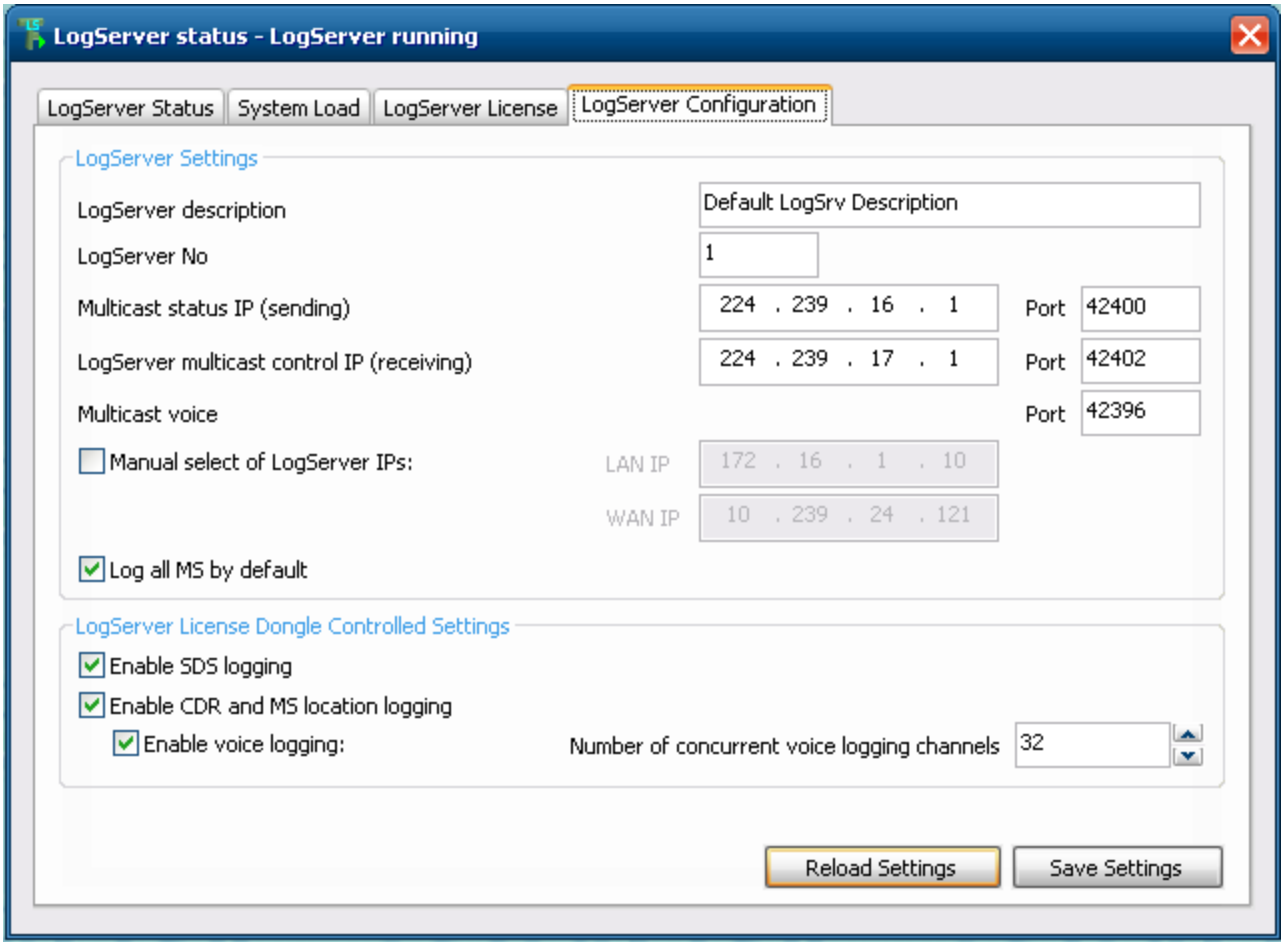


Dongle Configuration Values	
Name	Description
Dongle serial number	DAMM serial number of the dongle programming.
Dongle Date Limit	The date the dongle will cease to operate
Application Date Limit	If the application date (date compiled in the software) is newer than the Application date limit the application will no longer start. This means that it is not possible to upgrade the software with a newer one as the application date limit.
CDR and MS location logging	CDR and Voice logging allowed or not allowed. MS registration and RSSI measurement allowed or not allowed
SDS Content Log	Logging of SDS content allowed or not. This is also the case GPS coordinate logging.
Max. number of concurrent voice logging channels	Number of simultaneous voice channels which can be logged at a given time (0-255)

2.10.3 Configuration

The TetraFlex® Log Server's configuration is located in an ini file within the same folder as the executable one. The configuration is loaded during start up by the LogServer Service. The LogServer keeps the configuration in memory, it can be changed on the fly via the LogServer Tray user interface without restarting. When the LogServer service is running it owns the .ini file and changes in the configuration should always be made via the LogServerTray, since the LogServer service will overwrite the ini file if it detects any configuration differences.

LogServer Tray:



Please see the following LogServer.ini file description that corresponds to the fields in the *LogServer Configuration* tab except fields marked with * .

LogServer.ini Section [LogServer]			
Name	Type	Default Value	Description
`DBServer*`	String	`localhost`	This is either the machine name or IP address of the SQL Server.
`DBInitialCatalog*`	String	`TetraFlexLogDB`	This is the name of the database which should be connected to.
`DBLoginName*`	String	`root`	This is the login name to the database.
`DBLoginPwd*`	String	`tetra`	This is the password to the database.
`LogServerDescr`	String	`Default LogSrv Description`	This is a textual description of a maximum of 32 characters describing this instance of the LogServer. This info is sent to NM, and is visible there along

			with other LogServer settings as well.
LogServerNo	Int	25	Log server number
AutoDetectLocalIps	Int	1	This setting enables or disables automatic detection of which network interface is LAN and WAN. The LogServer needs to know which network interface is the "LAN" when joining multicast groups. It auto-detects this in the following way: 1st if a NIC is named "LAN" use this. 2nd if no "LAN" NIC found, use the logical interface which has an IP starting with the default LAN segment: 172.16.x.y 3rd if none of the above criteria is met, the use the first interface found. NIC=Network Interface Card
LanIp	String	0.0.0.0	This is only used when AutoDetectLocalIps=0.The LogServer will join its multicast groups via the network interface with this IP. It is only needed to specify this value in case of two or more network adapters. It is the IP towards the Tetra nodes that needs to be specified here.
WanIp	String	0.0.0.0	This is only displayed as info.
CtrlMulticastIp	String	224.239.16.1	This is the multicast IP address of the multicast group where the control messages flow.
CtrlMulticastPort	Int	42402	This is the multicast port number for Ctrl data.
LogSrvMulticastIp	String	224.239.17.1	This is the multicast IP address of the multicast group
LogSrvMulticastPort	Int	42402	This is the multicast port number
VoiceMulticastPort	Int	42396	This is the multicast port number for Voice.
CallInfoLogEnabled	Int	1	This setting can enable/disable CDR- and MS Registration logging. This setting only has effect when using a License dongle where Call Info Logging is allowed.

SdsLogEnabled	Int	1	This setting can enable/disable SDS logging. This setting only has effect when using a License dongle where SDS logging is allowed.
VoiceLoggingCh	Int	8	This setting defines how many concurrent calls can be voice logged. This setting only has effect when using a License dongle where voice logging is allowed.
LogAllMsByDefault	Int	1	This setting allows logging of non-configured MS in the LogServer when enabled. If a MS has been configured in the LogServer, it will use these values regardless of this setting. When this setting is disabled, the MS must be configured to be logged by the LogServer.

First time the TetraFlex® Log Server is launched, it will automatically generate the LogServer.ini file with the default parameters in the table above. In most cases, it will only be necessary to change the "LocalIp" if the TetraFlex® Log Workstation or Log Server machine has more than one network interface card.

2.10.4 Installation

2.10.4.1 Internal Log Server:

The Log Server is preinstalled on all 8GB CF cards (delivered with all SB421 today).

NOTE: The Log Server needs to have 1GB RAM to function properly (delivered with all SB421 today).

The log server is as default stopped from factory and need to be started when applicable. This can be done from the *Start menu – TetraFlex – LogServer- LogServer Restart.* This only works if the log server has been started once before.

If the Logserver never has been started you must use the install function from: *Start menu – TetraFlex – LogServer- LogServer Install.*

This will start the MySQL service, Log server application and the log server tray. This also will create a new empty database if not already created.

2.10.4.2 External Log Workstation and Log Server

The external Log Workstation and Log Server are pre-installed and preconfigured from DAMM at delivery.

If for any reason it has to be reinstalled this procedure must be followed:

This description is based on a Windows 7 platform installation, but it also applies to Windows Server 2008 platforms.

The installation procedure has been tested on a Dell Precision T3500 and on a Dell PowerEdge R710 that are the hardware used for the Log Workstation and the Log Server delivered from DAMM.

To install the Log Server, you have to follow these steps:

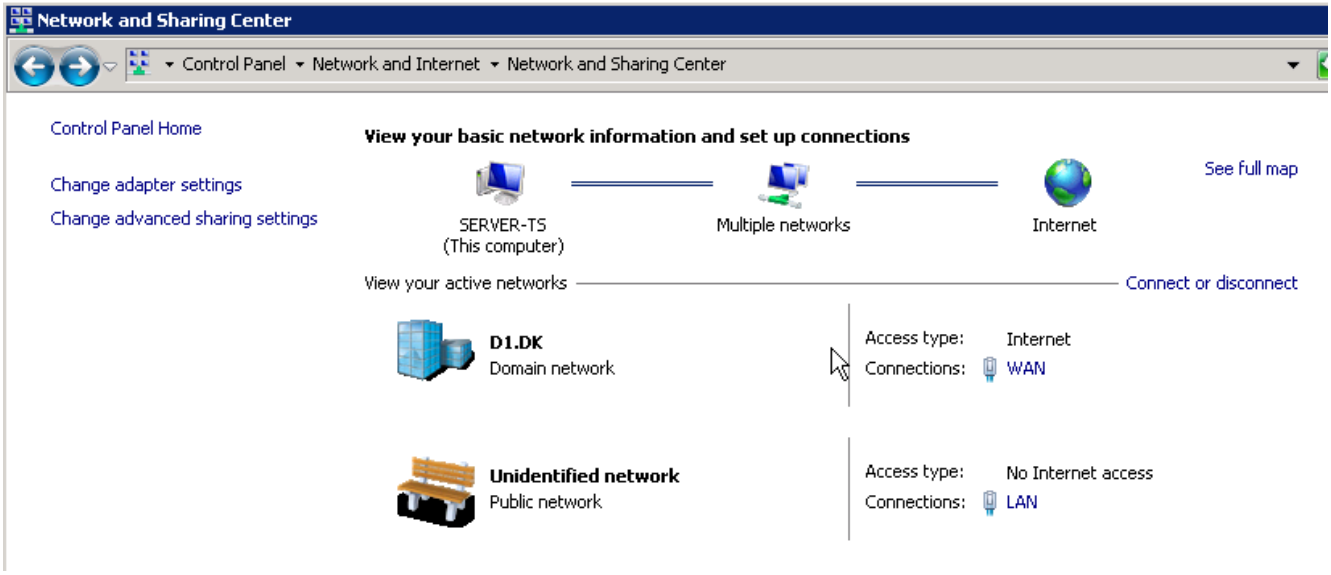
---

1. Rename NIC's to "LAN" and "WAN"
2. Disable "Automatic updates"
3. Change "Power Options" to high performance
4. Install "MySql ODBC 3.51 Driver" or later version
5. Install "MySql Community Server"
6. Install the MySQL GUI Tools
7. Create Tetra user
8. Copy Tetra apps
9. Install the Log Server
10. Add rule for firewall

1. Rename NIC's to "LAN" and "WAN"

Go to "Control Panel\Network and Internet\Network Connections"

Select the "LAN" Network interface card which should be the internal NIC on a Workstation. Look for the white "LAN" label on machine by the network card plug to identify it. Right click and select "Rename" from menu, name it "LAN".



If the machine has 2 NIC's:
Select the "WAN" Network interface card which should be the external NIC on a Workstation. Look for the white "LAN" label on machine by the network card plug to identify it. Right click and select "Rename" from menu, name it "WAN".
Set the Connection type to "Home or Work (private) networks"

2. Disable "Automatic updates"

Go to "Control Panel\System and Security\Windows Update\Change settings"
In the drop down options under "Important updates", select "Never check for updates (not recommended)"

3. Change "Power Options" to high performance

For Windows 7:
Right click on desktop and select "Personalize" from menu. In the lower right corner select "Screen saver". In the "Screen saver Settings" dialog select "Change Power Settings".
In the "Control Panel\Hardware and Sound\Power Options" dialog select the predefined "High Performance", which never puts the machine to sleep.

For windows Server 2008:
Go to "Control Panel\System and Security" and select "Power options". Select "High Performance" as preferred plan.

4. Install "MySql ODBC 3.51 Driver"

ODBC driver Version 3.51 can be found on the internet searching for “MySql ODBC 3.51”.
Run the msi file, use default settings.

NOTE: The LogClient and LogServer specifies that this driver version must be used, when using later versions they will fail.

5. Install "MySql Community Server"

The latest MySql Community Server can be found at http://dev.mysql.com/downloads/

There are 2 versions, a 32bit and a 64bit version, select the one that matches your hardware.

Right click Setup.exe and select "Run as administrator" and select the following:

Setup Type: Typical

- click next
- click Install
- Click next until Wizard Completed page
- Keep the Check mark in "Configure the MySql Server now", click finish.

- Now the "MySql Server Instance Configuration Wizard Ver 1.0.8" is launched, click next
- Keep the Check mark in "Detailed configuration", click next.
- Depending on the machine select either "Server Machine"(this is for a BSC) or "Dedicated MySQL Server Machine"
- (this is for LogServer running on PC without any other server applications)
- click Next
- On "Database Usage" select the "Multifunctional database", Click next
- Select the installation path. If possible select another partition than the c: drive.
- For Bsc: Select datadir d:\MySql Datafiles, click next
- Select the "Dicission support" number of concurrent connections (20 assumed), click next
- Enable TCP/IP Network option, disable Strict mode, click next
- Select the default language to "Standard Character set", click next
- Select "Install as Windows Service", launch the MysQL Server,
- deselect "Launch the MySql service automatically" only if data partition (d:) is present, click next
- Enter "tetra" as root password, Check "Enable root access from remote machines",
- click next and finally Execute

Please note that the first couple of Connection tries might fail, in that case simply press the retry button and you should get a connection.

The "MySQL" service is now installed.

6. Install the MySQL GUI Tools

The latest MySql Gui Tools can be found at http://dev.mysql.com/downloads/
use mysql-gui-tools-5.0-r12-win32.msi or later versions.
The package includes:

- MySQL Administrator
- MySQL Query Browser
- MySQL Migration tool

Install the complete package

7. Create Tetra user

Create the user 'tetra' with the password 'tetra'.
The 'Local Security Policy' setting: 'Password must meet complexity requirements' must be disabled, to allow the short 'tetra' password.

Find the setting here:
Open "Start->Administrative tools->Local Security Policy" window
In left pane: 'Security Settings->Account Policies->Password Policy'
To the right disable: 'Password must meet complexity requirements'

The 'tetra' user must have "Administrator rights".

8. Copy Tetra programs

The Log Server programs can be downloaded from www.damm.dk extranet by downloading the latest Tetraflex 7.5x version. Please read the release notes before installing.

9. Install the Log Server

Ensure that the IP settings are correct for LAN and WAN connectors. You should be able to get ping responses from the BSCs on the LAN segment. It might be necessary to add a persistent route, this is done by executing the following in a command shell:

route add 172.16.0.0 mask 255.255.0.0 172.16.0.1 -p

Insert License dongle, and wait till Windows has installed windows drivers.

Run "Start->All Programs->TetraFLex->LogServer->LogServer Install"
This will create the Tetra folder structure and copy the Log Server files and finally install the service.

Run the "LogServer Restart" shortcut. If running "LogServer Restart" for the first time a "User Account Control" dialog pops up with the following message:
"Do you want to allow the following program to make changes to this computer?"

Click the "Change when these notifications appear" link. In the new dialog set the slider control to "Never notify". Click OK, and Yes till all warning dialogs are closed.
The machine needs to be restarted before this new setting takes effect. Restart the machine and start the LogServer service using the "LogServer Restart" shortcut.

The "LogServer Restart" shortcut also starts the service and sets the LogServer startup type to "Automatic (Delayed start)".

This causes a delay of approx 2 minutes after power on before startup of the service. This is necessary because the dongle might not be ready when Log Server Service is started (only seen on machines with SSD disks and very short reboot times).

Executing the "LogServer Restart" will copy and generate the necessary LogClient install files.

Finally set the Notification level on the LogServerTray: right click on "Start" and select "Properties".
In the "Taskbar and Start Menu Properties" dialog go to tab "Taskbar" and select "Customize...".
In the Icon list change behavior for "Log Server Tray Application" to "Show icon and notifications".

10. Add rule for firewall

Go to "Control Panel\System and Security\Allow a program through Windows Firewall"
Select "Allow another program".
Browse to C:\Tetra\Applications\LogServer\LogServer.exe
Allow this for both Home (Private) and Public Network.
Allow also for LogClient.exe and MySql.exe.

2.10.4.3 Log Client:

The log client can be started either from the log server or an external PC. Before you can use the log client from an external PC it must be installed on this PC using this procedure:

Use a Explorer to connect to the "TetraFlex" share on the LogServer, right click the "\\<LogServer>\TetraFlex\LogClient\LogClientInstall.vbs" and select "Run as administrator" and follow the instructions on the screen.

A log Client link icon will appear on the desktop.

The Log Client may be started using any valid DAMM dongle for statistics display only.

2.10.4.4 Log Client installation on a PC with Windows 7:

If you can't find the node from where the dispatcher shall be installed, this setting in Windows 7 can help:

- click the start button and type secpol.msc in the search function.
- Browse to "Local Policies" -> "Security Options". Now look for the entry "Network Security: LAN Manager authentication level" and open it. Click on the dropdown menu and select "Send LM & NTLM - use NTLMv2 session security if negotiated". Apply the settings.

- In the “Advanced sharing settings” page of “Network and sharing center”, you need to have it set as “Work/Home profile”.

- Try :

    - Enable network discovery
    - Turn on file and print sharing
    - Turn off password protected sharing
    - Use user accounts and passwords to connect to other computers

2.10.4.5 SQL Server

2.10.4.5.1 General Description

The SQL Server used is a MySql server. The MySQL Community Edition is a free downloadable version of the world's most popular open source database that is supported by an active community of open source developers.

The TetraFlex® Log Server stores all data in the TetraFlexLogDB database. Some limitations for the MySql Community Server 5.0 are listed below:

- 256 TB of database disk space.
- 20 database connections at a time. The Log Server and the Log Client each uses 1 connection pr instance.

2.10.4.5.2 ODBC Access to SQL Server

Access to the MySql Server from database clients can be obtained via an ODBC driver. The latest MySql ODBC driver can be found at http://www.MySql.com.

2.10.4.6 Log server maintenance

This is described in chapter 3 Log client.

2.11 VOICE GATEWAY

Voice gateways can be activated on any node using the SIP protocol with Voice-over-IP (VoIP). The gateway is able to handle up to 31 simultaneous speech connections including conversion of speech from TETRA to A-law and vice versa, when running on the standard BSC412 platform and up to 15 simultaneous speech connections when running on a standard BSC421 platform. Up to 32 simultaneous speech connections are possible when a voice gateway is installed on a PC node.
The gateway does not provide any PABX features but has the capability to connect via the SIP protocol to an external PABX/gateway where routing, number modification, and protocol conversion (to e.g. ISDN or H.323) are handled. The gateway is tested to support the recommended Innovaphone V6 software, running on an IP400 (No PABX feature), IP800 or IP2000. Products from other manufacturers can easily be applied as well.

Each voice gateway is related to a node number. The SSI provided from the mobile station when making a call is not used in the system. Instead the system will always look in the calling mobiles profile and forward the call to the specified primary or alternate gateway node. This ensures predicted functionality independent of mobile programming.

Let us assume two organizations, one with the prefix 101 and the other with prefix 102, both have fixed phones with local numbers 301 and 302 and TETRA mobiles with local numbers 401 and 402. The user numbers in the subscriber register for the mobiles will for organization 1 be set to 101401 and 101402 and for the second organization 102401 and 102402. When making any call from 101401 the base station will add the prefix 101 from the profile to the called number. When dialing 402 the complete number will then be 101402. This is positively checked for existence in the subscriber register after which the base station will initiate a call to the SSI for that particular mobile.

When making a call from mobile 101401 to the number 301 the base station will add the prefix and get the number 101301. This does not exist in the subscriber register so instead the base station will make a call to the voice gateway indicated in the profile. When the system PABX receives the number 101301 it recognizes the prefix 101 as belonging to organization 1 and will route the call from the PABX with the prefix removed, effectively calling organizations 1's phone 301.

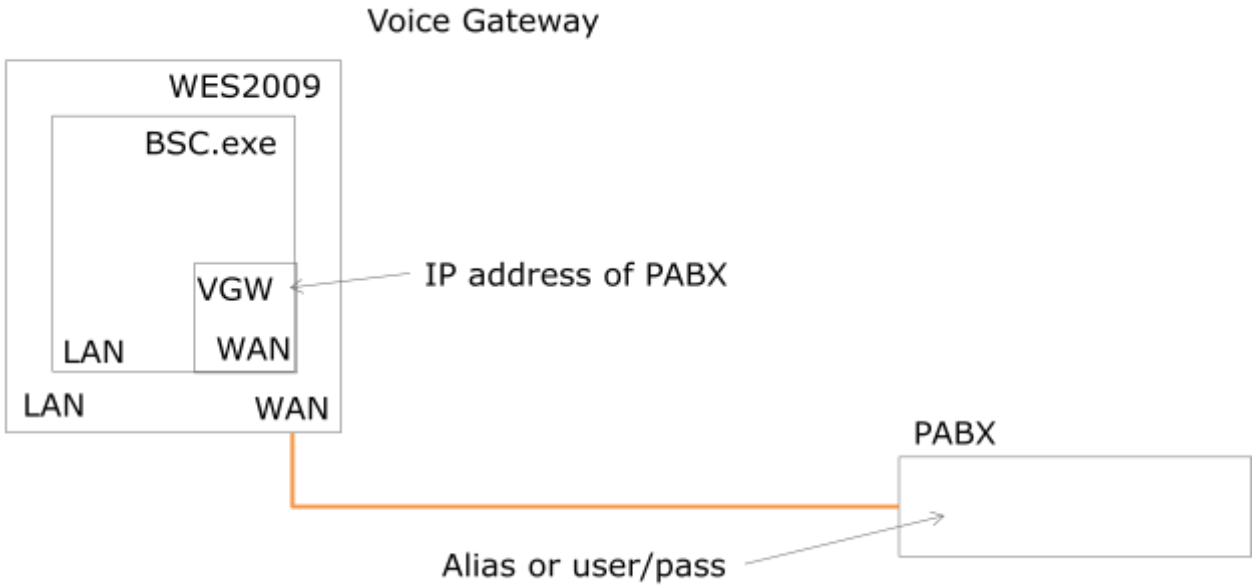
When a fixed phone in organization 1 calls the number 401 their PABX will recognize the number as a TETRA mobile and route it to the TETRA system PABX. The TETRA system PABX will add their prefix 101 to get the full number 101401 and call the TETRA gateway. The TETRA gateway will find the user number in the subscriber register and then create a call to the associated SSI.

The TetraFlex® System supports the unique feature of adding a fixed prefix to all PSTN calls made of mobiles with a specific profile. This prefix can be used in the interconnected PABX for routing analyses, allowing a single TetraFlex® gateway to route calls to different organizations.

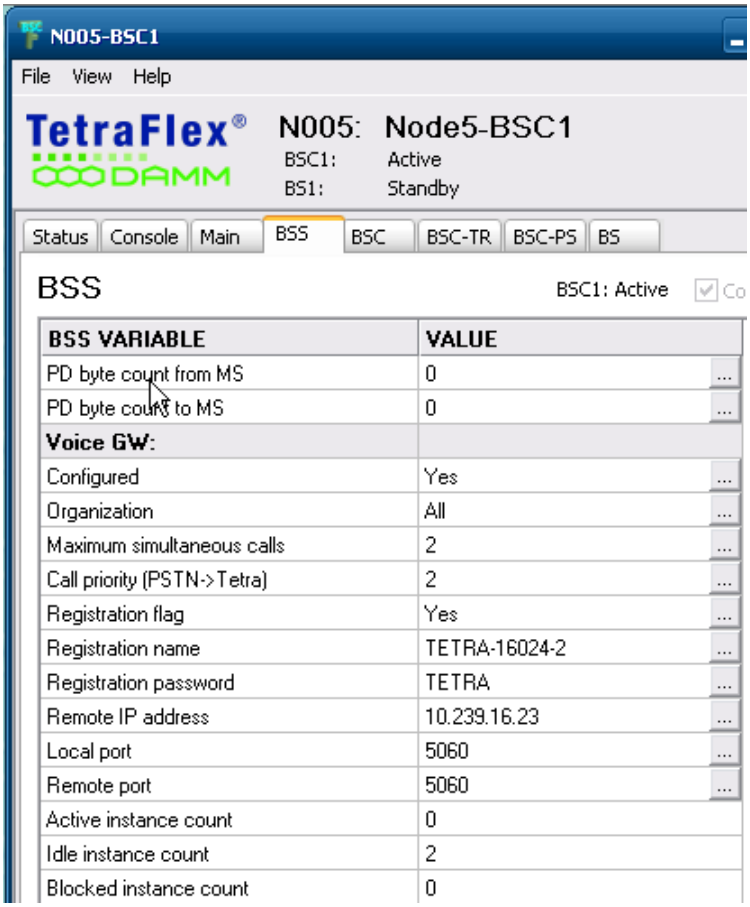
The TetraFlex® voice gateway supports incoming and outgoing duplex calls. It also provides full support to allow any PSTN phone (fixed, IP, GSM, etc.) to establish call in connection to group calls. The caller will initially be prompted for ID and pin code before the group attachment. All group communication can then be monitored in the phone. PTT activation can be done by a combination of key pressure and VOX (Voice Operated Transmit).
The voice gateway automatically makes SIP registration to the PABX. In case the redundant BSC takes over it will automatically re-register with the same name and its new IP Address giving full gateway hardware redundancy. In addition an alternate voice gateway can be established and defined in the subscriber register.

2.11.1 Voice Gateway configuration

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



To configure a Voice Gateway, use the TetraFlex NM application, BSC-GUI or the TetraFlex OM as described here (see also this manual in part 3 - Network Management – Voice GW):

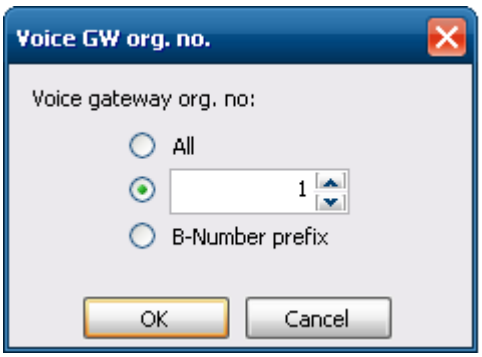


- The SIP registration name (Alias) must be unique and can only be generated by the BSC_GUI or OM command “S73/NAME/<SIP registration name>”. e.g. **“S73/NAME/TETRA-16024-2”**. The name must be entered as the SIP Alias name into the PABX as well SIP registration name and password cannot be generated by NM, only by BSC-GUI or OM commands.

- The SIP registration password is optional and can only be generated by BSC-GUI or the OM command “S73/PASSWORD/<password>”. e.g. “**S73/PASSWORD/TETRA**” (blank means no password). The password must be entered into the PABX as well.

- The Voice GW must be assigned to a node number to attach. This can be setup in the subscriber register in the different profiles where PABX access is desired 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.

- 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.

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

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

- Voice GW must be activated. Use NM, BSC-GUI or TetraOM command **S73/CNFG/+**

- The SIP registration name and password (if used) must be unique and entered into the Voice GW as well
- Use SIP registration must be set to YES.
- Remote IP address is the IP of the Voice GW (e.g. IP800)

The PABX samples are shown for the Innovaphone IP800, but may be any SIP compatible device.

The status of Voice GW can be verified using the BSC-GUI or with the OM command S13:

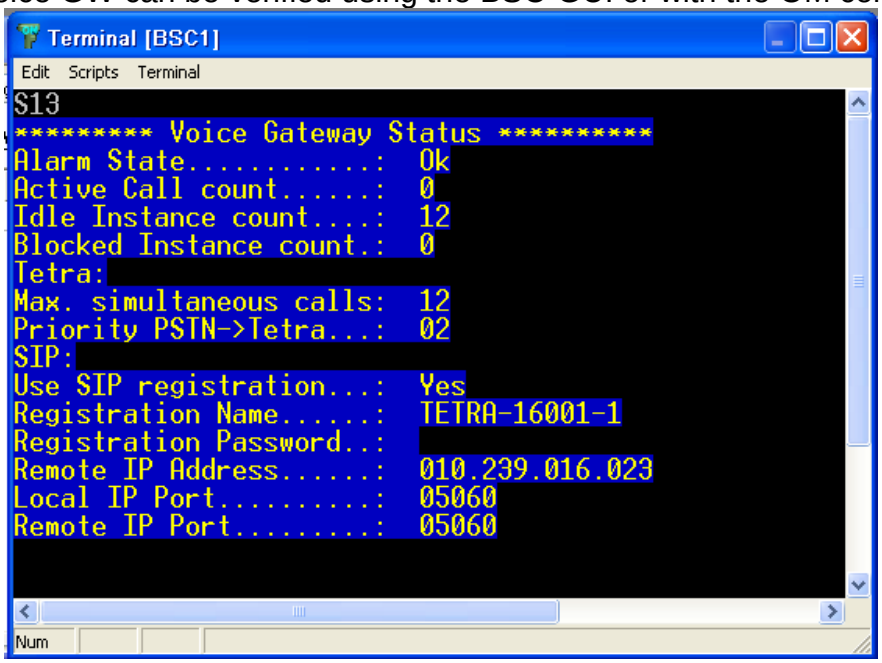


Figure 2-23: Voice Gateway Status

2.11.2 Innovaphone IP800 Configuration

For a detailed explanation of IP800 functions, please refer to the manufacturers manual

The IP address must be configured in the TetraOM, BSC-GUI or NM

Figure 2-24: Voice GW IP

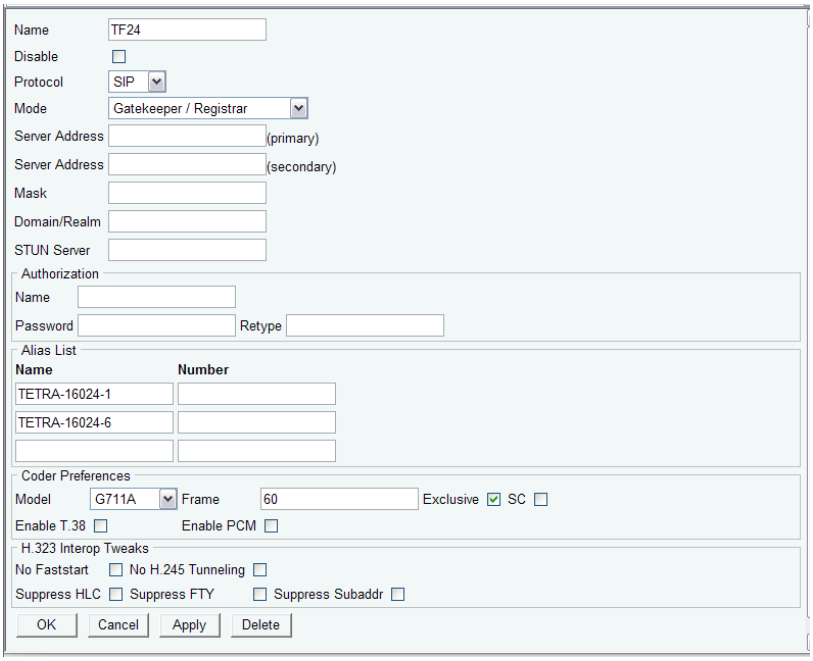


Figure 2-25: Gatekeeper registration

The Alias name and password (if used) must be consistent with the name defined in the BSC Voice GW

NOTE: To be able to enter registration mode “Gatekeeper / Registrar”, a “Gateway, Gatekeeper” license must be present in the IP800 unit. If this license is not present, the selection “Gatekeeper / Registrar” will not be shown

If IP800 GW license is not present, it is possible to connect without registration.
In this case the WAN port IP address must be entered in the IP800 “Server Address” field and the Voice GW selection in Network Management Reg. field must be changed to NO. Observe that this solution is not recommended and also this solution will NOT provide Voice GW alarms if connection is interrupted or broken. This solution also may prevent the use of a second voice gateway (dependent on SIP and subscriber timeouts - standard 32 sec).

2.11.2.1 Example of the IP800 objects.

Notice that the route table must be defined too.

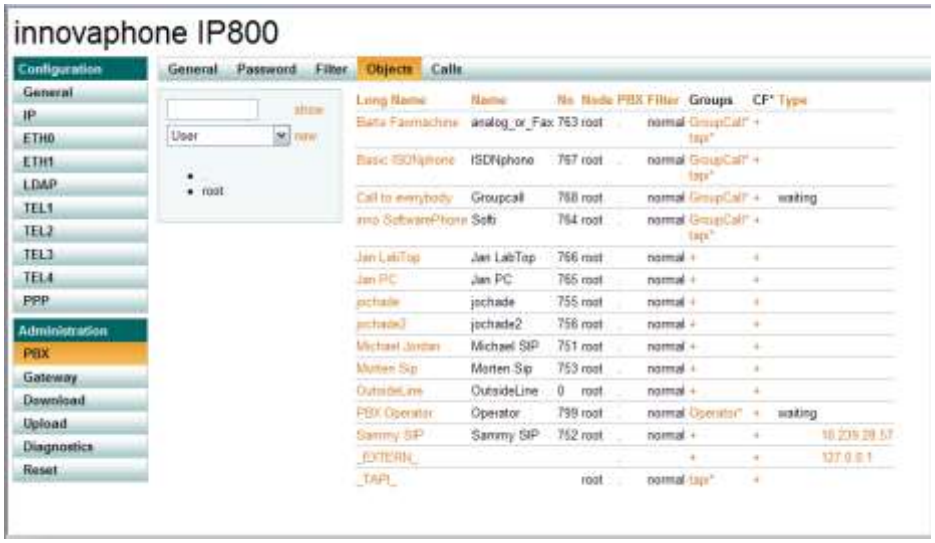


Figure 2-26: Objects in PABX mode (example)

2.11.2.2 IP 800 Route table example

Please note that this example shows an IP800 which serves as gateway for several TetraFlex® systems

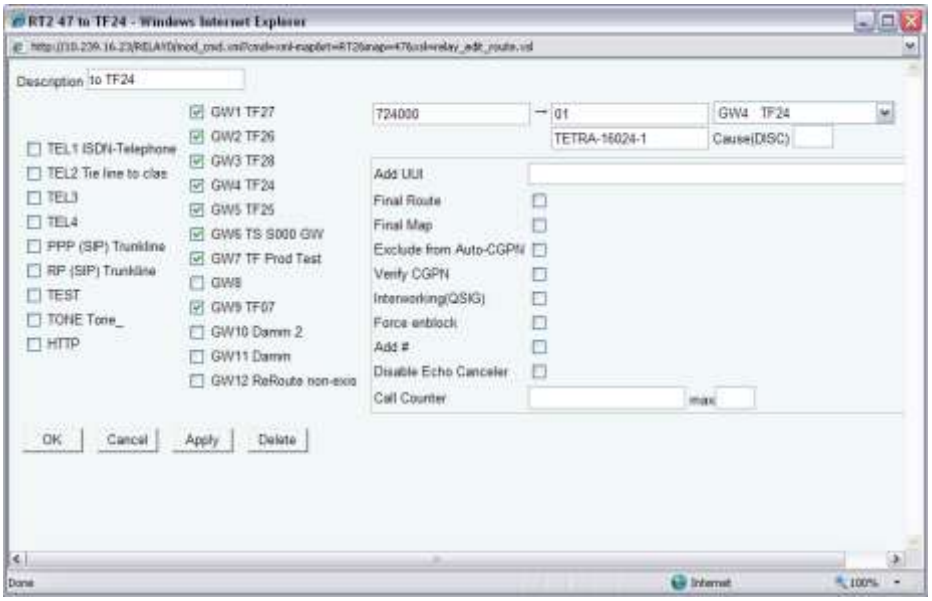


Figure 2-27: Route table example

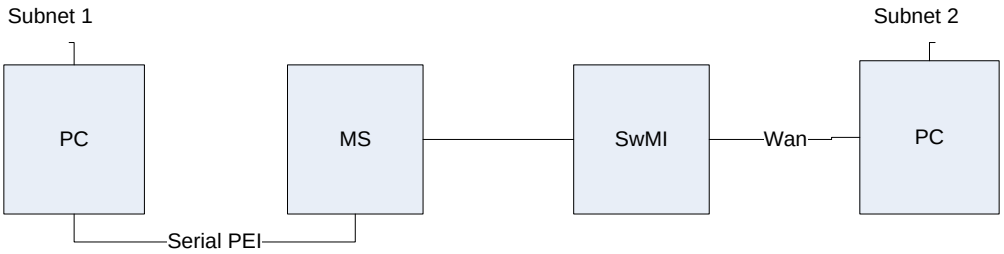
Dialing 724000 will be transformed into 01.

- 0 is the number presented to the TetraFlex and is then routed to the speech message
- 1 is the prefix chosen to distinguish different organizations on one GW

In this example several TetraFlex systems use the same GW i.e. TF24 to TF28 and more

2.12 PACKET DATA GATEWAY

The Packet Data Gateway can be used as a Gateway between two networks; in this case Subnet 2 connected to the Wan and another network Subnet 1 connected to a MS device.



The TetraFlex® System supports dynamic multi slot packet mode where Packet Data gateway/servers can be activated at any node supporting standard IP communication between TETRA Mobiles and attached units like laptops, application servers, workstations, FTP servers, WAP servers, etc. anywhere within the IP network/Internet.

Fixed IP addresses are allocated for the mobiles in the subscriber register allowing direct access to mobiles from different applications. Computers connected to the mobile have to be set to DHCP and automatically the system will provide them with an IP address, mask, DNS server, etc. The DNS server address is configured in the profile for the mobiles allowing mobiles to use their company DNS Server.

By default the TetraFlex® Packet Data gateway automatically announces itself to the connected IP segment with the RIPv2 protocol. The main router/default IP gateway therefore has to have RIPv2 activated as it ensures automatic rerouting to the redundant BSC when it takes over.

It is possible to set up two redundant PD gateways/servers in the mobiles profile. Note that the access to a packed data gateway is not needed for making IP communication between two mobiles as mobile to mobile packet data service always will be available.

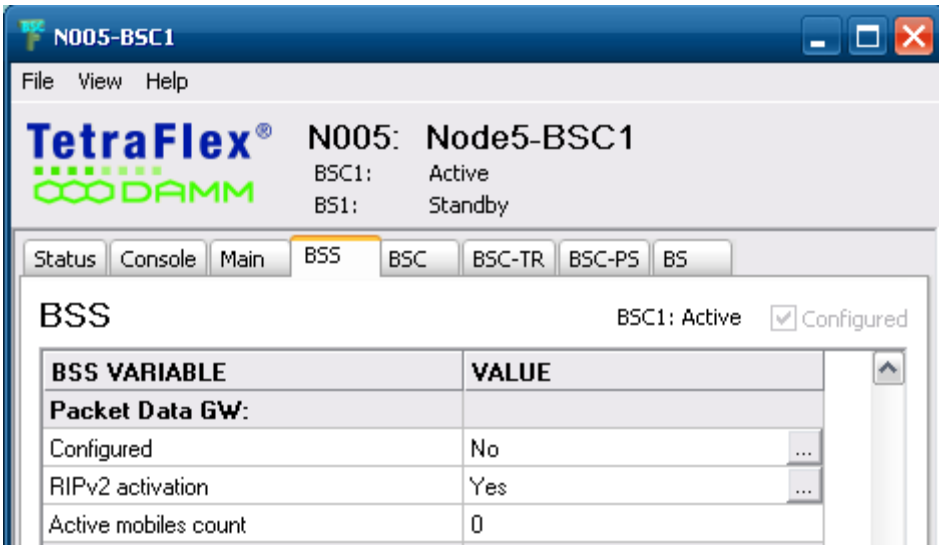
The TetraFlex® System has full support for multi slot PD giving an approximate throughputs from 3.5 to 14 Kbit/sec depending on the number of slots used. If possible the system will automatically assign 4 data slots at startup and then preempt data slots when necessary to assign slots for speech. Each data slot can be shared by two users making it possible to have a maximum of 8 packet data sessions running simultaneous. In case slots assigned for speech is available the packet data gateway will monitor timeslots every 5 seconds and reassign these for data transfer.

2.12.1 PD GW configuration

To configure the Packet Data gateway use the Network Management program (NM), BSC-GUI or the TetraOM application (OM)

NOTE: Packet Data GW configuration is only needed for Packet Data access from TetraFlex to the public world. PD access Tetra to Tetra is always available and need no configuration.

- BSC-GUI:



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

- Configured: Yes or No is PD GW active
- RIPv2: If Yes RIPv2 is used – If No Static routing is used.
- Active mobiles count: Numbers of active mobile connections

- TetraOM:
  - Activate the packet data gateway using **S74/CNFG/+**.
  - **S74/RIP/+** Activated RIP

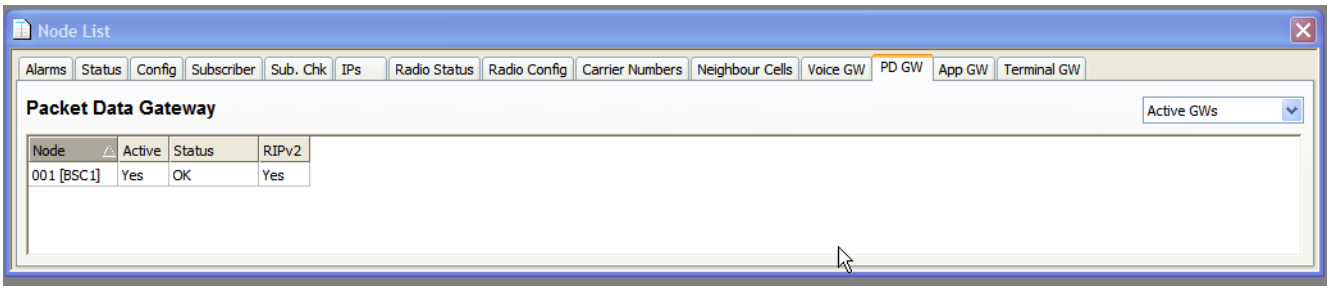
- Network Management
  These parameters can also be set from NM please see chapter 3 Network Manager

  - Use the OM command **S71/SUBIPADD/"IP address range"/"MASK"** to configure an IP address range defined by the MASK.
  - Configure the packet data gateway Node using the OM command **S21/"Profile number"/PGNODE/x/"Node Number".** Where x is 1 for primary GW and x is 2 for alternate GW

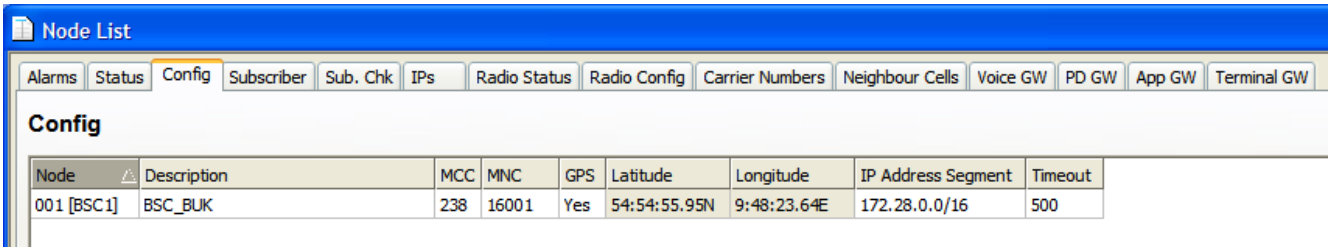
The following is information only

- Status

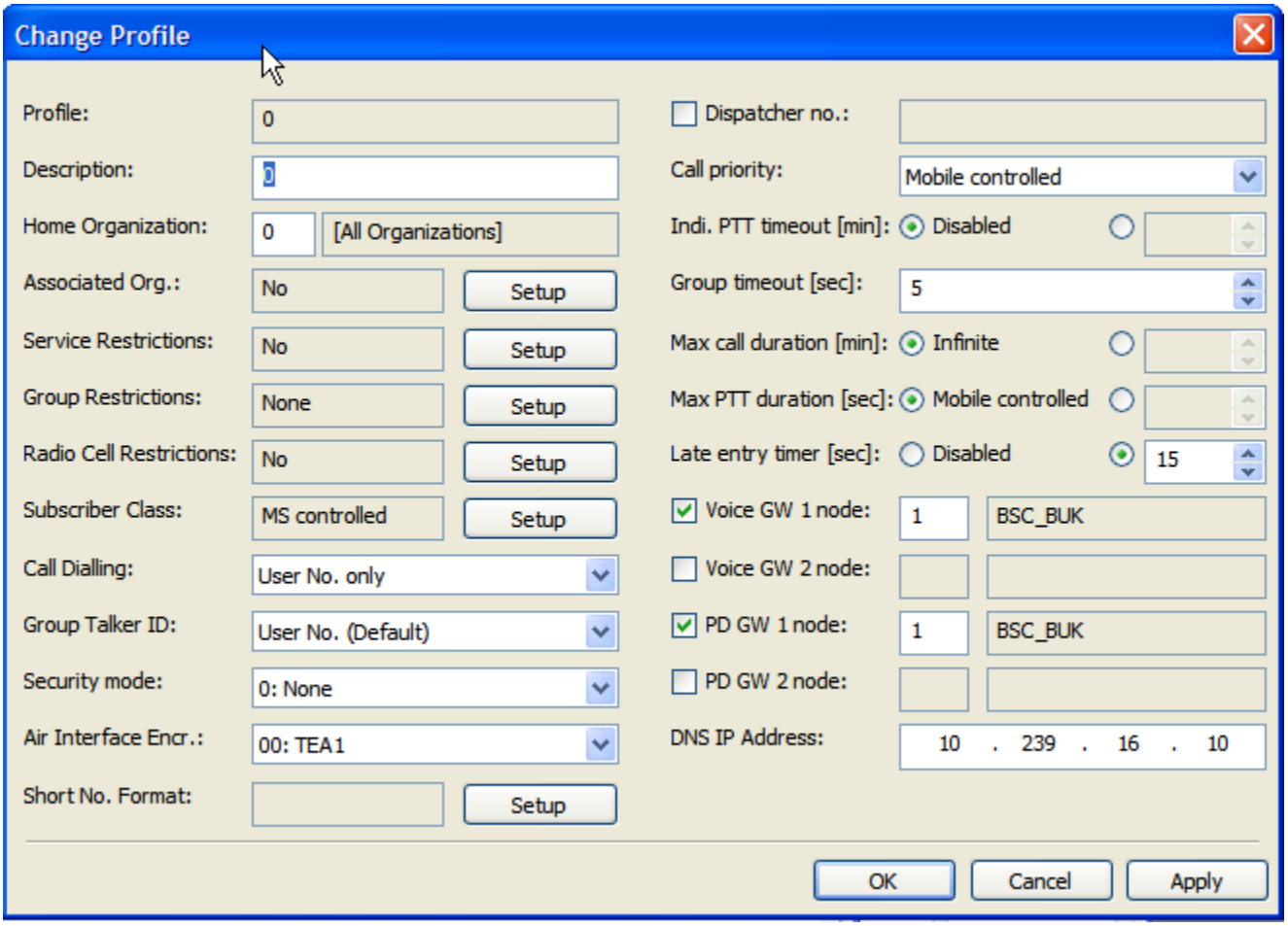
The drop down box "All Nodes" / "Active GWs" changes between display of active nodes only, or both active and not active nodes



- The IP Address Segment must be set from the Config dialog.

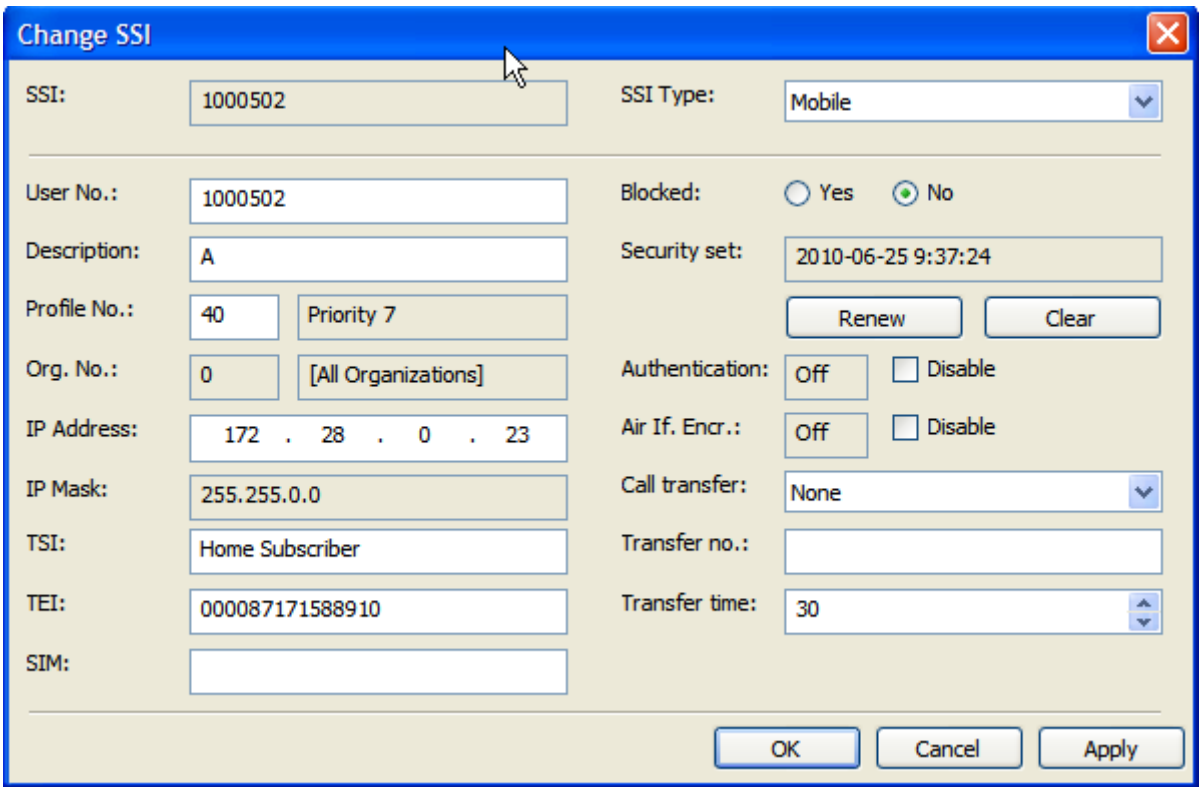


- From the Network Management configure a packet Node attachment (if not already done via TetraOM). This is done from setup in the subscriber register in the different profiles where PD-GW access is desired (PD GW must be active). In the dialog below PD GW 1 node is checked and Node 1 is attached for profile 0 (e.g. node name BSC_BUK).



- In the profile make sure the DNS IP address is configured and the packet data GW 1 node number is configured.

- If the MS is to be used for packet data transfers make sure an IP address is configured within the specific subscriber. E.g. Bellow: SSI 100502 has IP 172.28.0.23.



2.12.2 PC network configuration

Using a standard Windows XP machine use the following steps to setup the modem connection between the PC and the Tetra MS.

- Sepura
  - See Reference Document MOD-06-195 (Sepura Packet Data User Guide)

- Modem configuration
  - From the Control Panel open the “Phone and Modem Options”.
  - Chose the Modem banks and type the Add button to add a new hardware wizard.
  - On the hardware wizard select “Communications cable between two computers” and type next.
  - Chose the appropriate Com port connecting to the MS.
  - When Windows is finished configuration select properties on the modem connection.
  - Setup the Maximum Port speed to 38400 bps.

2.12.2.1 Network configuration

- From the Control Panel open the “Network Connections”
- Chose “Create a new connection” to create a direct connection.

- Select the network in the connection wizard and type “Set up an advanced connection”.
- Select “Connection directly to another computer” within the Advanced Connection Options.
- Configure the PC role for Guest.
- Assign an appropriate name for the connection.
- Select the modem device for connection.
- Configure the connection availability for anyone’s use.
- Make sure the Phone number is *99#.

2.12.2.2 MS configuration

To request the IP address from the SwMI subscriber database the MS must be configured for dynamically IP request

- Sepura
  - Open the radio programmer and upload the MS configuration.
  - Make sure the IP parameters are all configured to 0.0.0.0.
  - Set the MTU size to 1500.
  - Download the new nettings to the MS

2.12.3 Main router

For incoming attempts make sure a static route is configured for the packet data GW IP address.

2.13 APPLICATION GATEWAY

2.13.1 Application Programming Interface (API)

Application Gateways can be activated on any node, allowing applications/dispatchers to be connected to the system.
Several applications can connect simultaneously to an Application Gateway, and they will register to the system like a terminal by finding a working Application Gateway from its list of IP addresses. This allows Gateway redundancy between a redundant BSC as well as Application Gateway Nodes.
Applications are connected to the Gateway through the DAMM provided TetraFlexApi.dll Dynamic Link Library, which is handling the complete interface protocol. The TetraFlexApi.dll will also take care of its basic configuration and the Voice interface to PC sound system. The TetraFlexApi.dll is License Dongle protected.

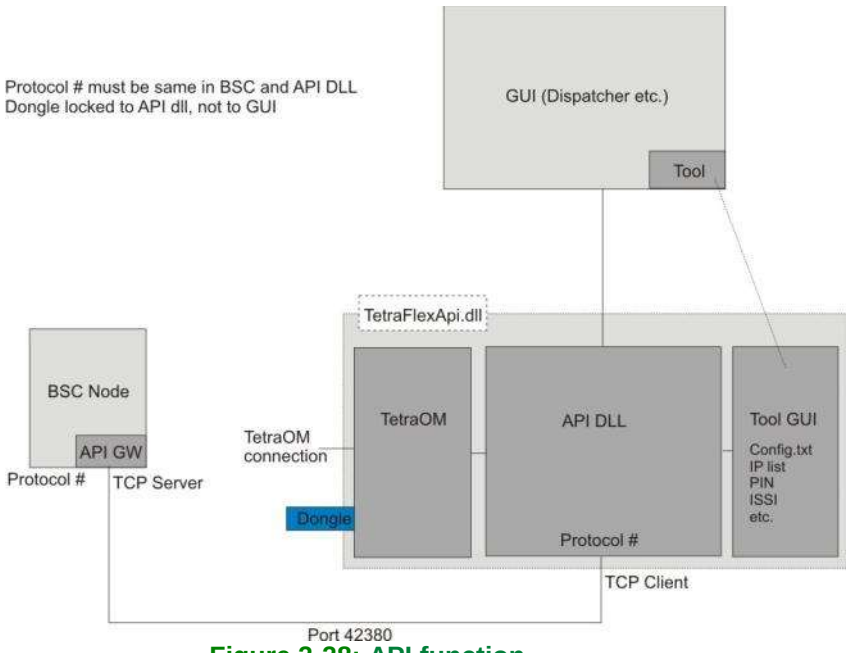


Figure 2-28: API function

At registration the TetraFlexApi.dll will check for identical protocol version numbers in the Gateway and TetraFlexApi.dll. System software updates will include an updated TetraFlexApi.dll, which shall be installed with all applications.
DAMM delivers an English standard Graphical User Interface (GUI) toolkit together with the TetraFlexApi.dll, which can be used as reference for development.

The Application Gateway and TetraFlexApi.dll initially gives access to functions like: Making Individual and Group Calls, discreet listening and connection to group calls, send and receive SDS and handle the setup of DGNA etc. You can use the Toolkit or Dispatcher to see what functions are available in the API.

2.13.2 Support

The TetraFlex API is the connection tool for the DAMM dispatcher application. The API itself is fully documented in the TetraFlexApi.h file, which can be used of third party vendors to create their own Applications.

The use of the API demands a combination of Tetra knowledge and programming skills. The API itself is an offer so users may be able to create their own applications e.g. their own Dispatcher.

API programming is not directly supported, but specific questions will be answered by DAMM support.

2.13.3 Compatibility

The API will be kept backward compatible, so that new versions of the TetraFlexApi.dll will support all methods contained in earlier released versions. That ensures that new TetraFlexApi.dll versions coming with new system software releases will always work together with GUI Applications written for earlier versions

2.13.4 Test applications

The SW package also includes an API toolkit SW programmed in C++, C# and Delphi for testing the different API calls without having to write an application.

2.13.5 API Configuration

The following criteria must be met to be able to access the API

- The Node Dongle must allow API
- The Node Dongle is delivered as default with 5 connections
- API client dongle must be present
- Configuration file must be defined
- Application subscriber must be defined in the subscriber register

2.13.6 API Installation

2.13.6.1 To install the API client (dispatcher)

- On the PC where the client must be installed press windows “Start” ->”Search” -> “Files and folders”
- Select “Printers, Computers or People”
- Select “A computer on the network”
- Insert the IP address of the WAN port on the GW node in question and select “Search”
- When search result appears, double click on the result
- Enter user name and password (standards = tetra and tetra)
- Now the shared directories are accessible
- Select the \tetra\share\dispatcher directory
- Run the dispatcher setup file – **setup.exe**

The API client and associated files will now be installed on the client PC in a directory called c:\Tetra\applications\Dispatcher\Default or the application SSI number you choose.

The API development files and test applications can be downloaded from www.damm.dk extranet.

Before the application (test application or dispatcher) can connect to the BSC node you must configure the system as it is described in the next section.

2.13.6.2 Bringing the API to work on your system:

2.13.6.2.1 In the subscriber register:

Create an application subscriber (SSI) and enter the relevant Application data

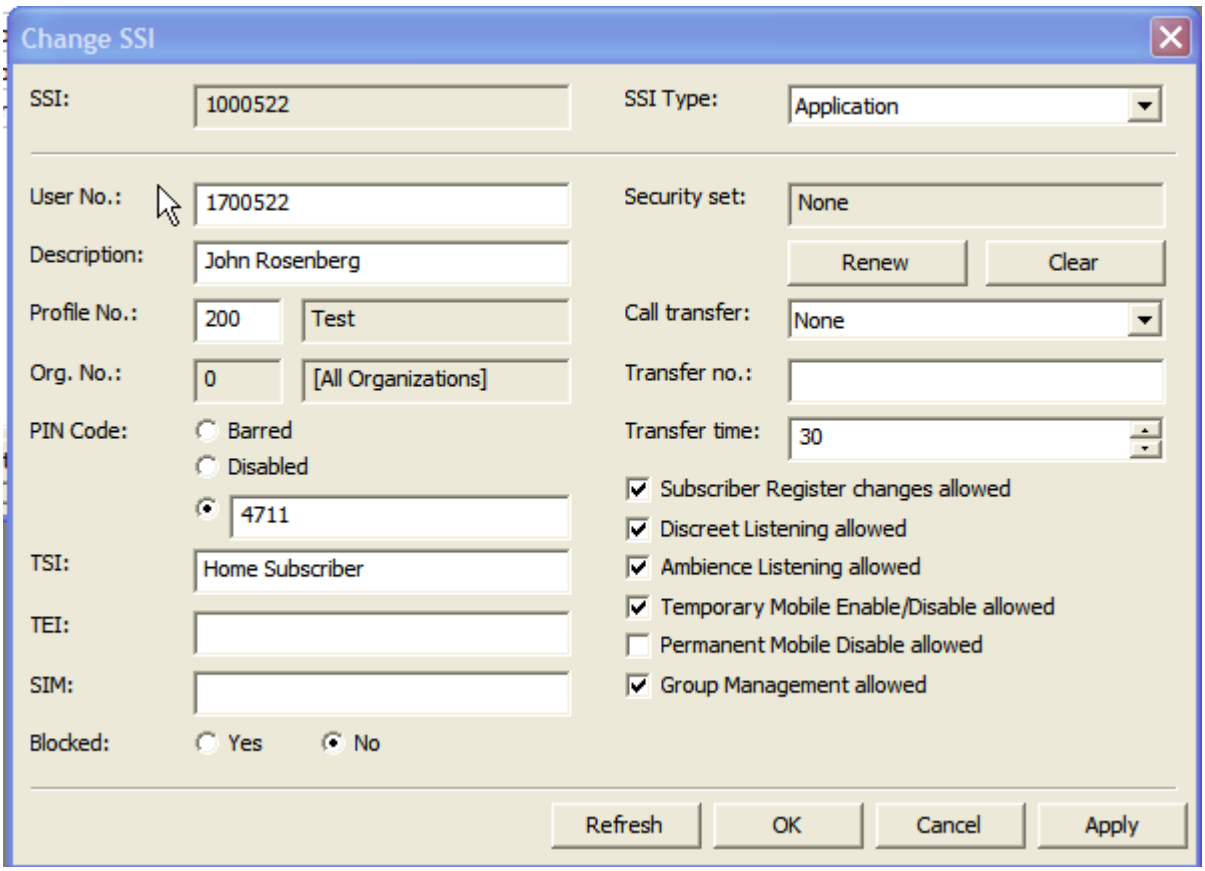


Figure 2-29: Application Subscriber

The API application (e.g. DAMM dispatcher) can either use the User No. or the TSI (Tetra Subscriber Identity MCC:MNC:SSI). The use of PIN code can be chosen and must match in the API settings.

2.13.6.2.2 In the Application (Dispatcher) folder:

Edit the "Config.txt" file with the correct data

- The config.txt must reflect a relevant TSI or User No. (the application SSI created in the subscriber register) for your system. Also enter the PIN code and user number assigned in the subscriber register. At least one gateway needs to be set. This is where the IP address of BSC WAN is entered. The IP address must contain full octets, so leading zeroes must be entered - e.g. 010.239.016.200.
- Save your changes.

```
;***********************************************
;***     TetraFlex API DLL Configuration     ***
;***********************************************
; DLL Version:  7.52 2011-09-09
; Date/time..:  2011-11-01 14:29:43

;***** 71 Common *****
71/IDPROMPT/-
71/USERNO/1700522
71/PIN/4711
71/OMPORT/42382
71/OMPIN/1841803245

;***** 72 Gateways *****
72/0/010.239.016.200/TetraStar
72/1/-
72/2/-
72/3/-
72/4/-
72/5/-
72/6/-
72/7/-
72/8/-
72/9/-
```

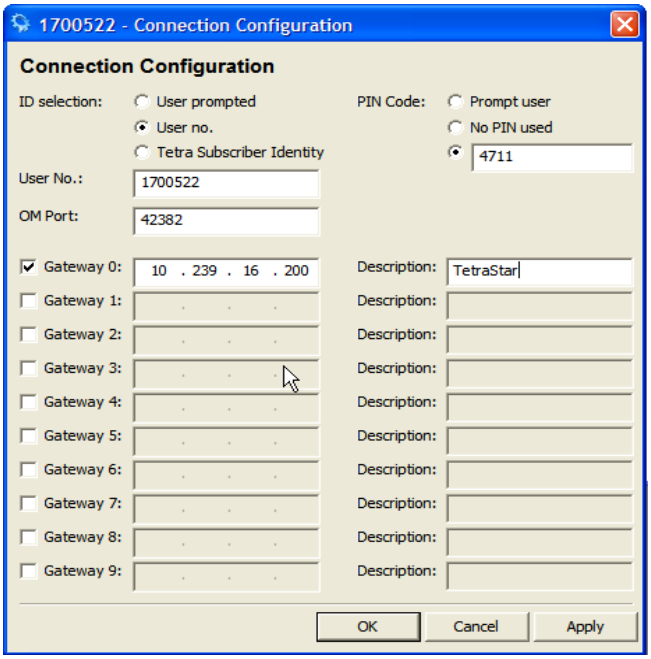


Figure 2-30: Configuration methods. Configuration file and dispatcher connection

- A different configuration method is to start the dispatcher and select: "Views -> Connection Configuration" from the top menu

Provided the previous steps have been accomplished, the Application will start up and initiate connection to the BSC.

.

2.13.7 API Dongle settings

E.g. of dongle settings for using the API DLL

Figure 2-31: Node dongle

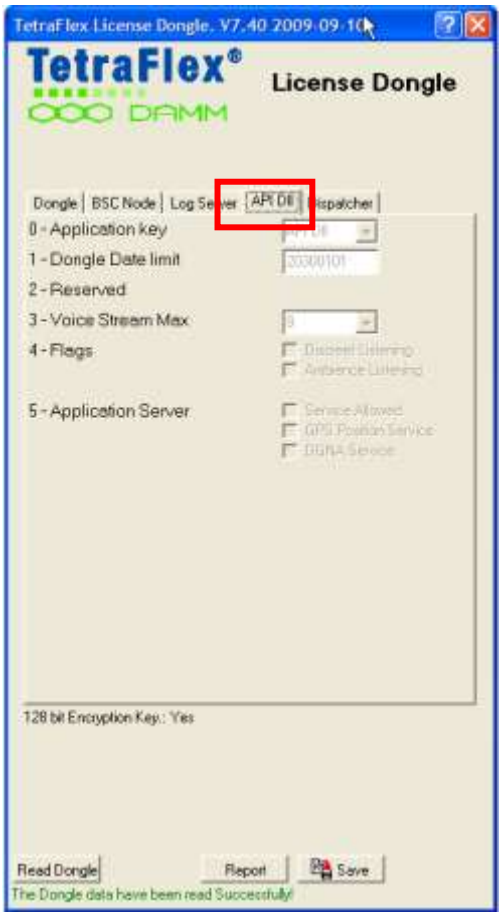


Figure 2-32: Client Dongle

To allow communication between the API.DLL and a Node, the Node Dongle must have the Application Gw. Conn. Max set to a number >0 to allow the Application GW to be used by the API.DLL (Dispatcher) and the Client Dongle (used in the PC) must have the API.DLL settings enabled

2.13.8 Configuration file

Examples of “how to use a txt editor” to set the connection configuration of the API DLL in the config.txt file:

NOTE: All blanks must be filled out. This means that a SSI must be 8 digits, MNC must be 5 digits, and IP address segments must be 3 digits and so on.

```
;************************************************
;***     TetraFlex API DLL Configuration     ***
;************************************************
; Date/time:  2008-12-15 10:11:39

;***** Common *****
71/SSI/01000092                  Application SSI must be defined in subscriber reg.
71/MNC/16029                     MNC Mobile Network Code (Same as in NM)
71/MCC/0238                      MCC Mobile Country Code (Same as in NM)
71/PIN/12345                     PIN: If use must also be defined in subscriber reg.
71/OMPORT/42382                  Access port for TetraOM (cannot use 42380)

;***** Gateways *****
72/0/010.239.028.003/BUK1        Range of node IP addresses where the API can
72/1/010.239.016.200/TetraStar   connect.
72/2/-                           The API will try to connect to first IP, if not present
72/3/-                           then the next will be tried and so on
72/4/-
72/5/-
72/6/-
72/7/-
72/8/-
72/9/-
```

2.13.9 Test of API function

To test if the API functionality is configured correctly, two methods may be used (API test tool or OM commands) **Both methods require the API to be initiated.**

2.13.9.1 API test tool

The API test tool can be downloaded from www.damm.dk extranet and is available in a C# version and in a Delphi version. The API test tool must be in the same directory as the config.txt file (e.g. c:\tetra\applications\dispatcher\default).

For initialization of the API

- Execute the API test tool TetraFlexApiTest_C#.exe
- Or TetraFlexApiTest_Delphi.exe

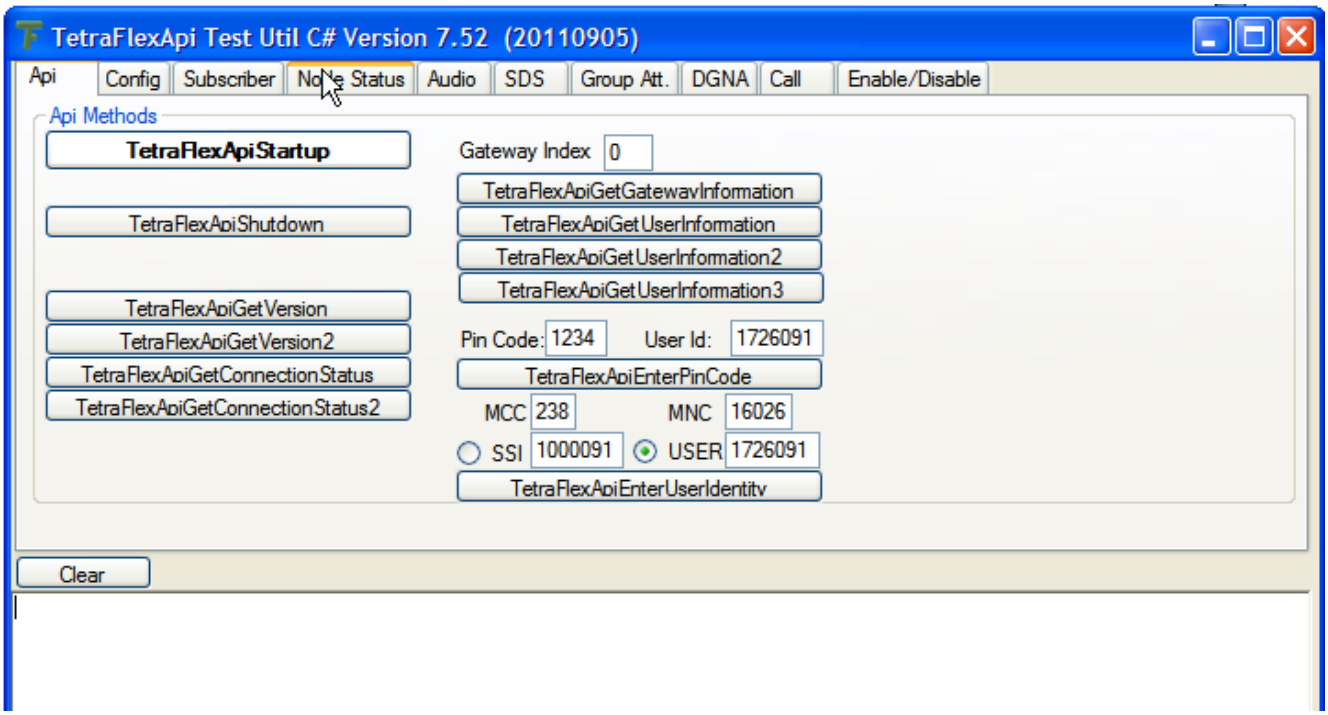
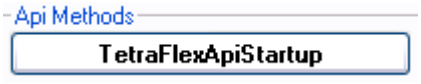


Figure 2-33: C# Test

- Select the  button.

- Check that the following message appears in the message field.

```
Int32 TetraFlexApiStartup(UINT32 HeaderVersionNumber);
Return : 0 (Successful initialisation of the API)
```

Figure 2-34: C# Test API

2.13.9.1.1 Check API connection

- Select the “TetraFlexAPiGetConnectionStatus” button

This will result in a message showing that the API is connected:

```
Int 32 TetraFlexApiGetConnectionStatus(out UInt16  NodeNumber,
                                       out byte    BscNumber,
                                       out UInt32  GatewayControlIpAddrOfNode,
                                       out UInt16  GatewayControlIpPortOfNode,
                                       out string  NodeDescriptionString);
Return                          : 1 (Connected)
NodeNumber                      : 10
BscNumber                       : 1
GatewayControlIpAddrOfNode      : (183439560): 10.239.16.200
GatewayControlIpPortOfNode      : 42380
NodeDescriptionString           : N010-BSC1 SÃ¸nderborg GW1
```

Figure 2-35: C# Test API connection

2.13.9.1.2 Test via TetraOM

To be able to connect to the API via TetraOM, the API must be initialized as described before.

- Install a TetraOM at the client PC
- Configure the OM to connect to the client PC IP address using the Port assigned in the configuration file (e.g. 42382).

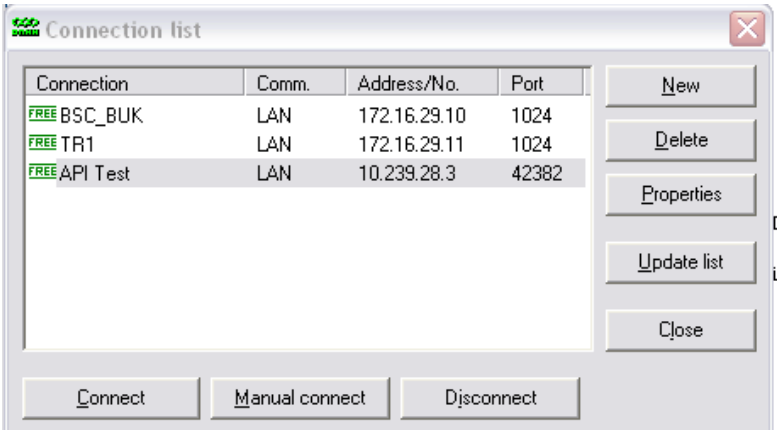


Figure 2-36: TetraOM connections

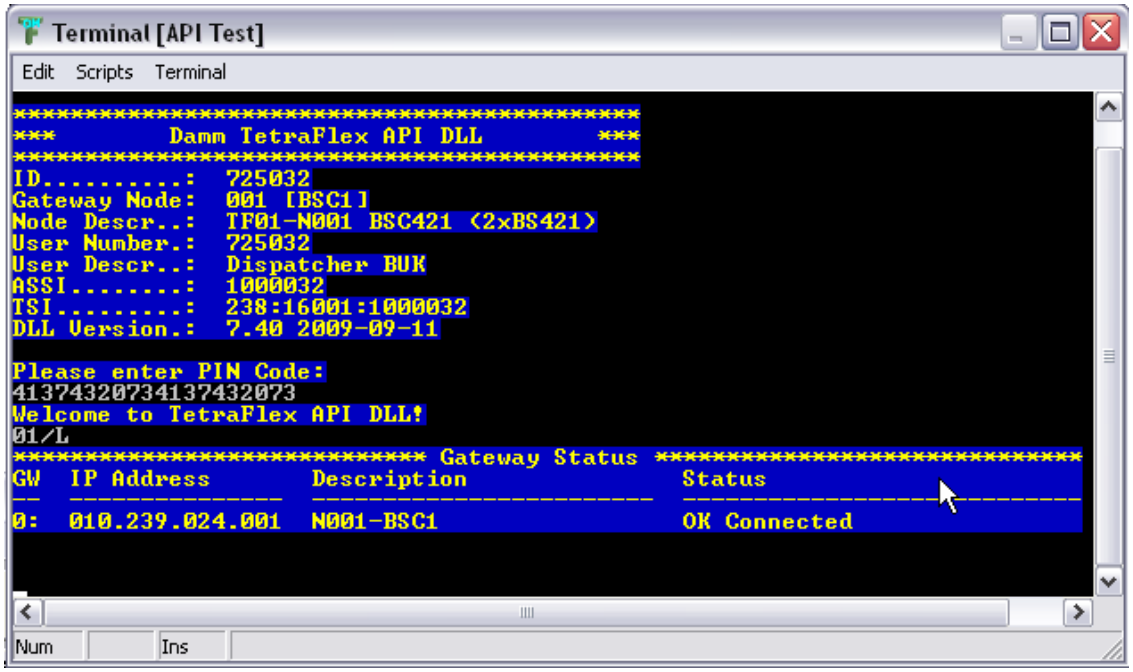


Figure 2-37: API connection status

- TetraOM command 01/L (R/01/L for dynamic) will show the connection status

2.13.9.1.3 Useful commands

- In the Config header press 

, or TetraOM command 30/CONFIG/GUI, the GUI configuration window opens.

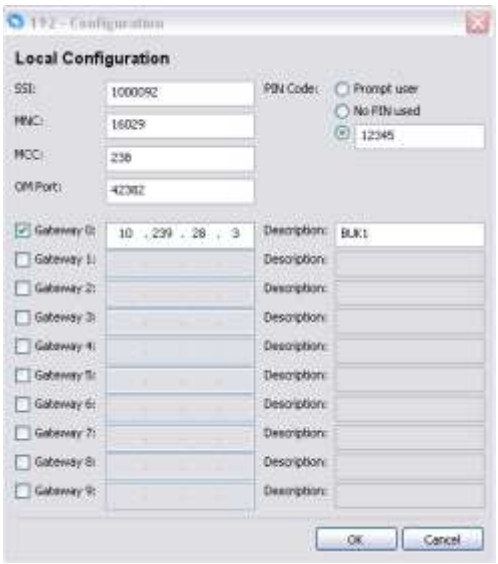


Figure 2-38: GUI Window

- In the Subscriber header press 

, or TetraOM command 30/SUBSCR/GUI, the GUI configuration window opens.

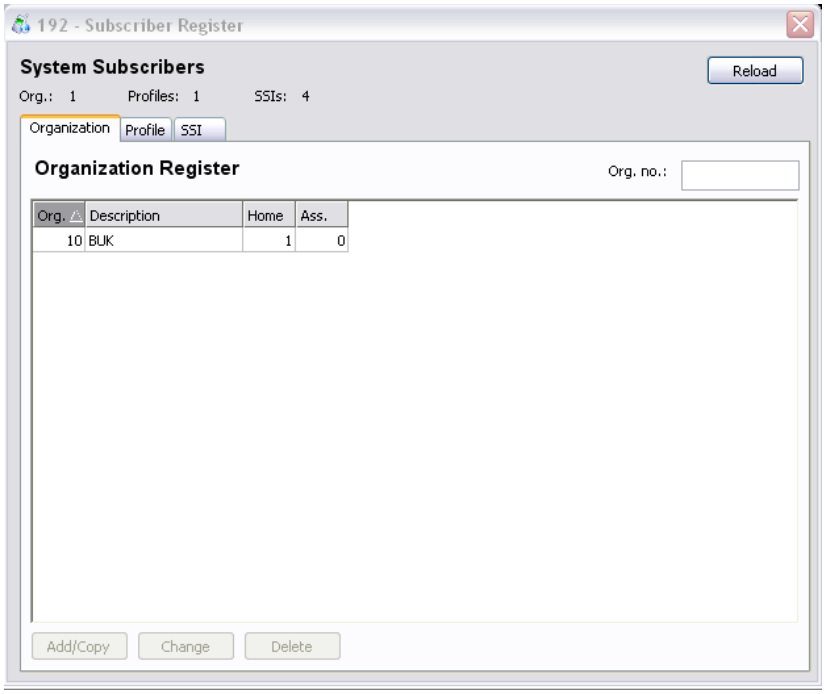


Figure 2-39: Subscriber window

2.14 TETRAOM

2.14.1 TetraOM

This section describes how to communicate with the BS4xx Base Stations and control applications in order to handle the units during installation and maintenance.
The TetraFlex® system incorporates a Base Station Controller, referred to in this document as the BSC

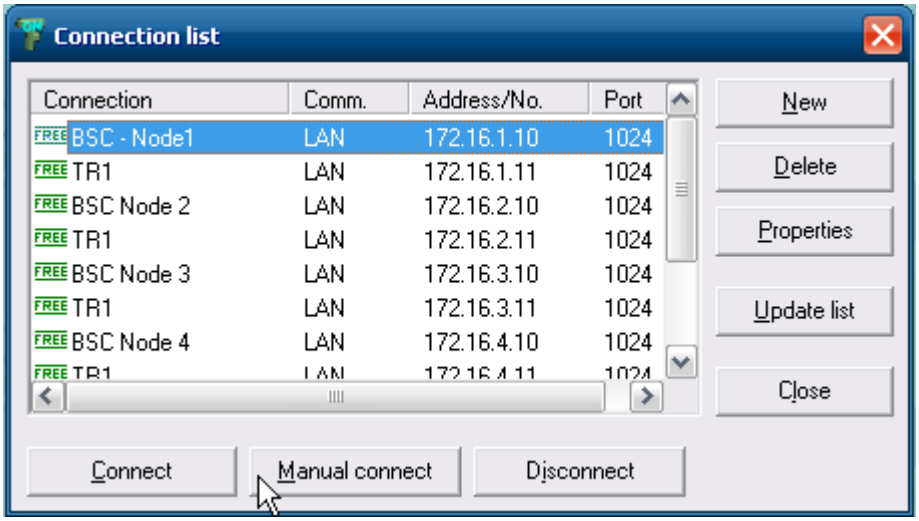
For a complete list of TetraOM commands see the TetraOM help files manual.

Several methods of communication are available depending on the actual need and tasks to be done.

Outdoor units (SB421/BS421) must be addressed by their IP address :

Default IP for TR #1 is 172.16.1.11, for TR #2 it is 172.16.1.012 and so on

Default IP for BSC #1 is 172.16.1.10, for BSC #2 (redundant BSC) 172.16.1.19



E.g. To check connection to BS421 on IP 172.16.1.11, ping the IP:

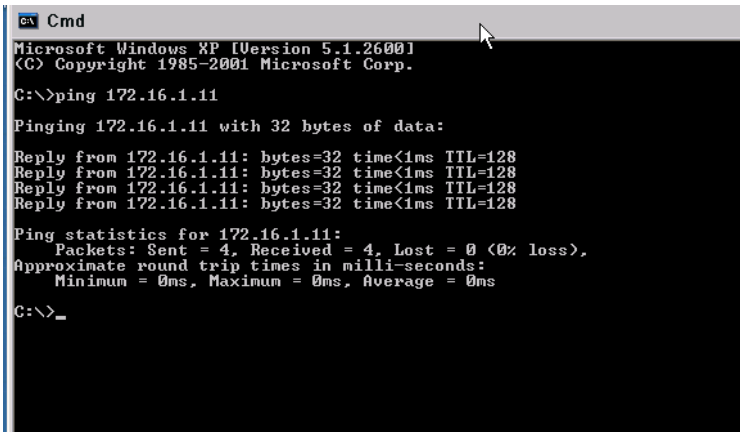


Figure 2-40: IP Ping

For the indoor BS41x, IP connection to the TR412's, combiner and Power supply is not possible and must be made via the HDLC bus.

To activate the HDLC bus UART, use TetraOM command **AU+**. If for some reasons the HDLC cannot be activated use **AU/FORCED** first.

For onsite situations, a CRT, keyboard, and mouse can be connected directly to the BSC with standard extension cables. This also allows monitoring of the Windows booting, modification of the BIOS CMOS set-up, and makes it possible to alter the IP address when lost.

When a TCP/IP connection is available, file transfer to and from the BSC is possible and may be used for backup, restore and software upgrade.

2.14.2 Power supply addressing outdoor (SB421)

The internal Power supply in the SB421 can be addressed with the OM command:

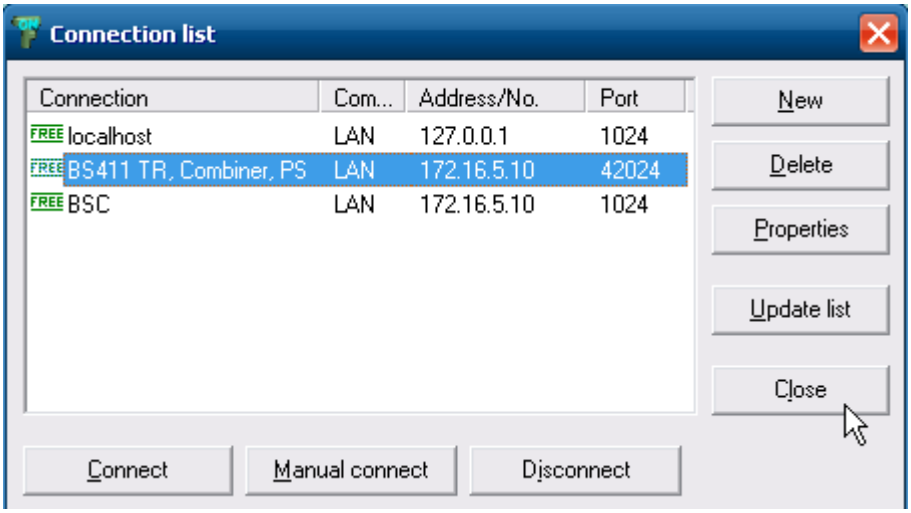
AP

When succeed, the response from the PS is `Address: AP [PS421]`

Note: The Power Supply can only be addressed when the SB421 IP address is selected in the connection list.

2.14.3 TR421, Combiner, Power supply addressing indoor (BS4xx)

To get access to these units the IP address for the BSC must be used and **Port 42024** as shown in the connection list below:



Then the units can then be addressed according to this scheme:

AU+	**Activate HDLC bus (TR412 only, not TR421)**
AU/FORCED	**If the HDLC connection is used by someone else**
A11…18	**Select TR 1 to TR 8 in rack 1**
A21… 28	**Select TR 1 to TR 8 in rack 2**
AP11…17	**Select PS1 to PS7 in rack 1**
AP21… 27	**Select PS 1 to PS7 in rack 2**
AT11…AT12	**Select combiner 1 or 2 in rack 1**
AT21…AT22	**Select combiner 1 or 2 in rack 2**

2.14.3.1.1 Functional Description

All test commands for the Transceiver, Power Supply and the Combiner (only in BS41x) consist of a 2-digit command in the range 00 to 99 with an optional parameter. Commands without parameters are display-only commands and will not make any changes. Therefore, it is possible to "page through" the commands to find the right one without any risk to change vital parameters.

The commands are divided into groups, covering the different functions in the TR. For example, all the TR commands are in the 10 to 19 group. If the first two characters are not representing a valid number in the 00 to 99 range, an error message will be displayed:

```
Invalid TR412 command
```

This is however not the case if the first character is a +, which are reserved for commands to the test box. In this case no response will be sent. If an unimplemented TR command is called, the following response is displayed:

```
Unimplemented command
```

2.14.3.1.2 Commands

OM commands organization:

M xx - Main BSC OM Commands
F xx - Base Station Controller (BSC) OM Commands
S xx - Base Station Switch (BSS) OM Commands
H xx - Base Station (BS) OM Commands (only for BS41x)

xx - OM Commands without a letter in front is used for TR, PS or TCC

2.14.3.1.3 Running commands

The TetraOM allows automatic execution of a TetraOM command repeated (R) or continuously (C):

R/"OM command" can be used to poll a state within the BSC,TR. PS, Combiner.
C/"OM command" can be used to view the messages from the message queue.

Example: R/07/S (Show the actual time date and century seconds)
C/63/N (Shows the GPS data stream from a BS421)

2.14.3.1.4 Simultaneous commands

From the TetraOM terminal window, it is possible to combine several TetraOM commands using the "|" (Pipe symbol).

Example: 00|03/A (shows software version and alarm flag list)

2.14.3.1.5 Local blocking mode

After power-on, the TR always starts in normal operating mode. If a given command requires local blocking, it is shown in the help area for the command. Commands that require local blocking are not available during normal operation for operator interference. If a protected command is called, the following response is displayed:

```
Local blocking necessary
```

Only commands with a parameter are protected. After activation of local blocking (01+), all commands except factory configuration commands are available.

2.14.3.2 Parameters

Two types of parameters are used.

Generally + is used as parameter to turn on, enable or step up and - is used as parameter to turn off, disable or step down.

E.g. 11+ (turn power supply on)
11- (turn power supply off

For more complex functions, a / is used as separator after the command no. followed by the necessary no. of characters for the actual function.

E.g. 13/27 (set output power to 27dBm)

If the parameter is not valid for the actual command, the following response is displayed:

```
Invalid parameter
```

2.14.3.3 Configuration

Many calibration and system parameters are stored locally in a sector of the Flash chip. At power-up and reset, all settings are copied into the workspace RAM, from where the different software tasks take the settings.

Any change in the configuration is only made in the workspace RAM. To store the new configuration locally, a save command shall be made. The configuration is divided into two separate entities:

- System configuration
- Factory configuration (only to be done by DAMM)

System configuration parameters can be changed with the 7x OM commands and are automatically saved.

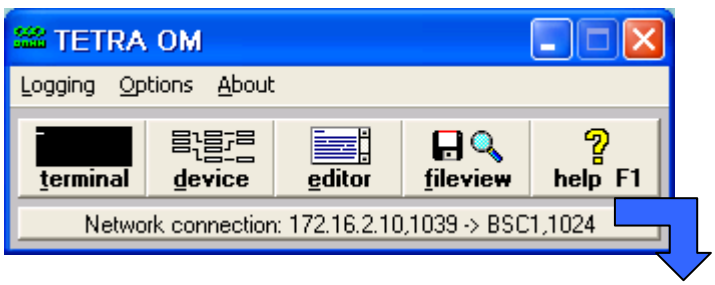
2.14.3.4 TetraOM set up

More possibilities exists “how to start the TetraOM program”:

- Start via the NM
- Start via BSC-GUI
- Start the TetraOM program from the start menu or the taskbar
- Start the TetraOM program on the BS421 directly using the VNC program.

The TetraOM program files are located on the BSC in the directory C:\Tetra\Active\Pgm\Om. It is possible to copy all files to a similar directory on your own PC and create a shortcut to the TetraOM.exe file for start-up. The PC must be on the same LAN as your nodes to connect to them with OM.

After starting the TetraOM program, the connection window is shown:



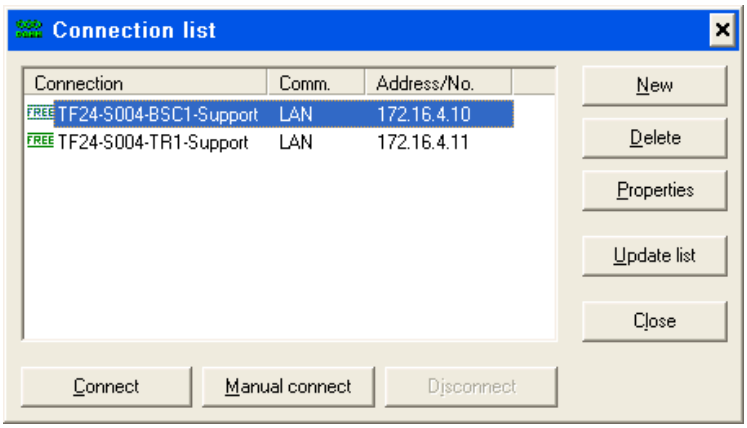
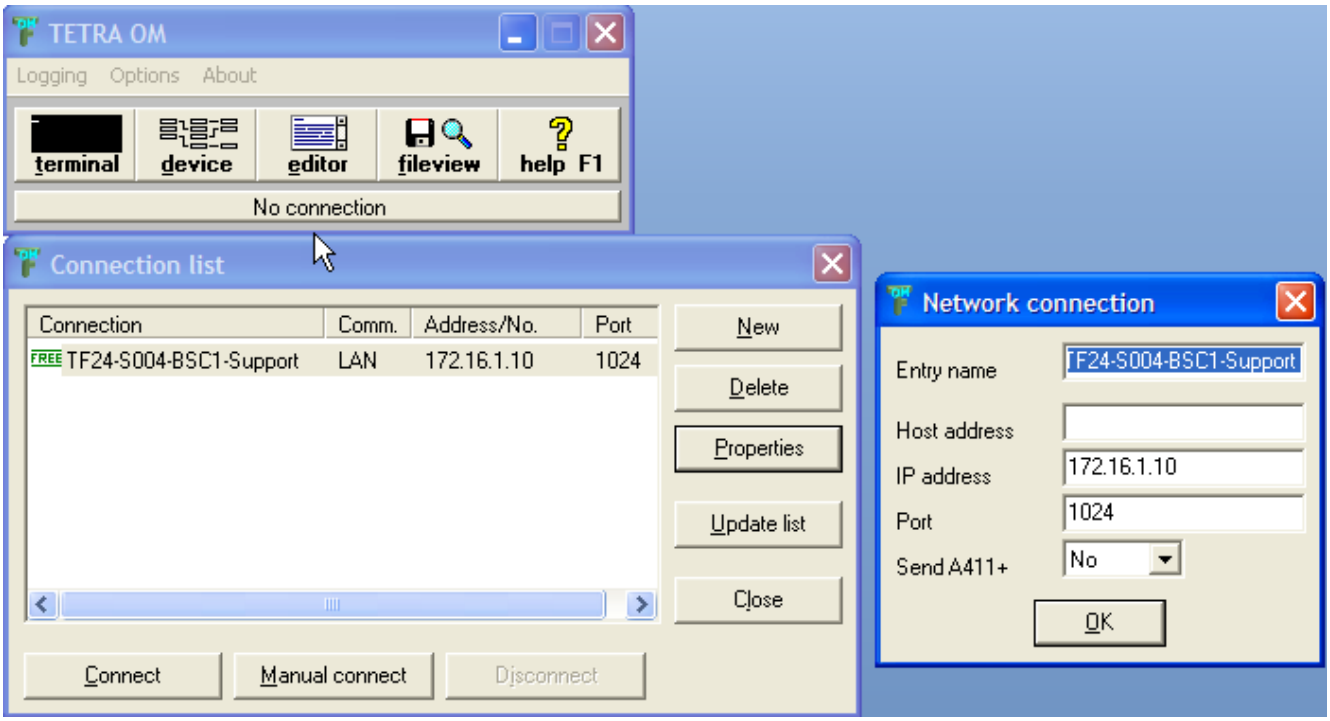


Figure 2-41: OM Connection

The connection list may be empty. To connect to the TR or BSC, a new entry in the list may be created by selecting New and afterwards double-click on the entry.
It is recommended to name the connection into some well defined name.
As an example this syntax might be used:

"System Number"-"Site Number"-"Unit Description"-"Organization"

E.g. TF24-S004-BSC1-Support



To make a new connection push the "New" button and select the connection type (normal Network) and fill out the entry name and IP address of the unit (*Send A411+* set to No).

The units can then be accessed with OM by clicking on the list and push Connect.

Manual connect is possible as well, selecting the Manual Connect button and manually entering the connection parameters.

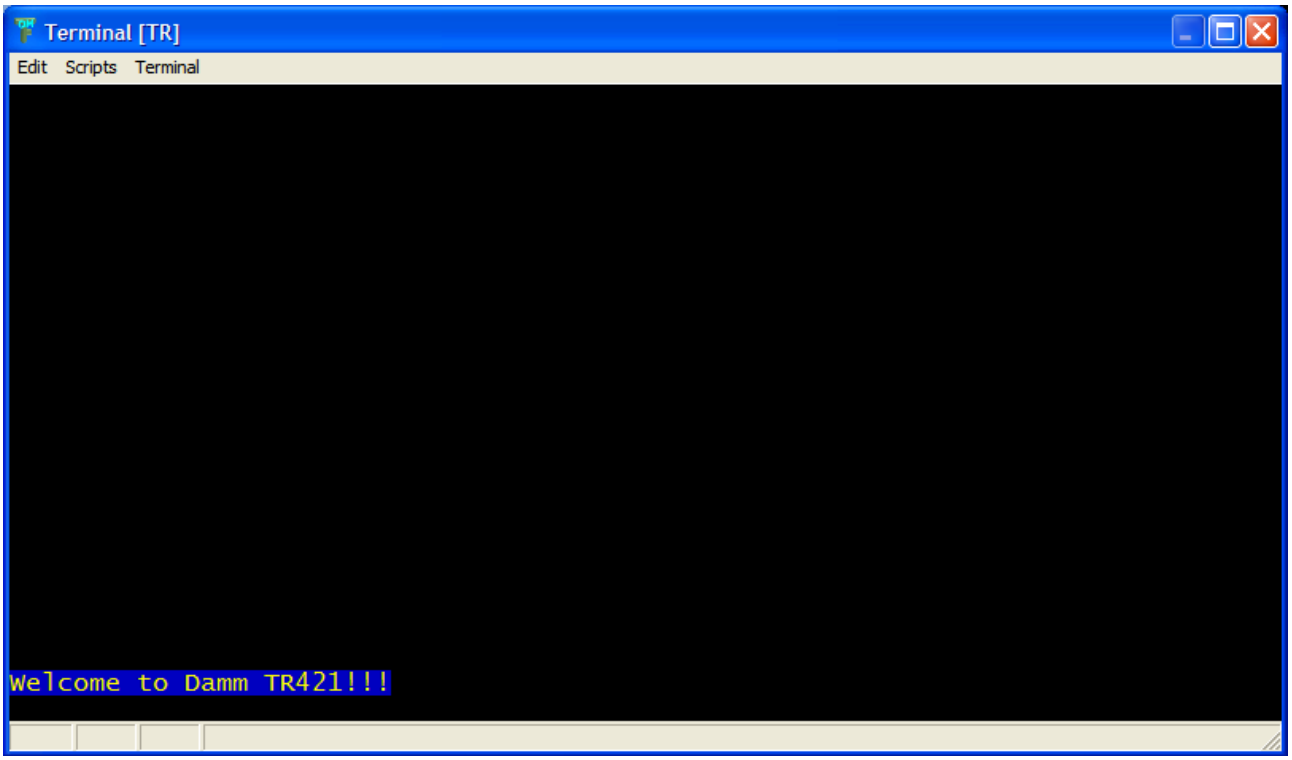


Figure 2-42: TetraOM communications window

When connected, the TetraOM communications window will appear.
Normally this window will be a black command screen with a welcome text or an error message if some commands have failed.

Communication with the BSC,TR, PS and Combiner (BS41x) is now possible by issuing TetraOM commands. As an example if command 71 is entered the TR will respond back as shown below:

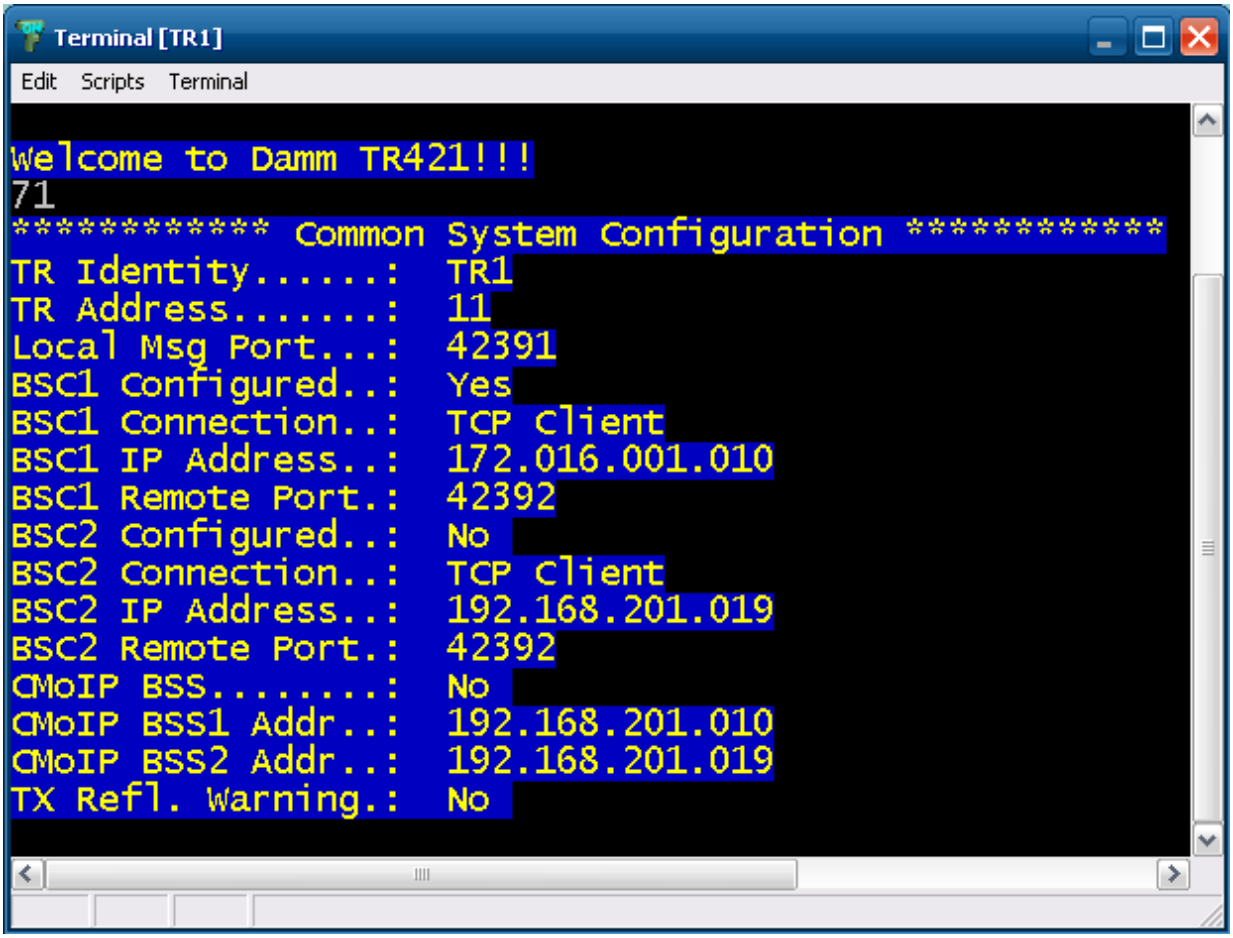


Figure 2-43: TR Identity

2.14.3.5 TetraOM Help

Most used commands will quickly be familiar. For more rare used commands a help system is available documenting all available commands and options, The HELP is accessed either by pressing F1 or clicking on the Help button.

The help system contains a help file for each device in the base station. Start to select the BSC (BS421), as this help file contains information about how to address the different devices.

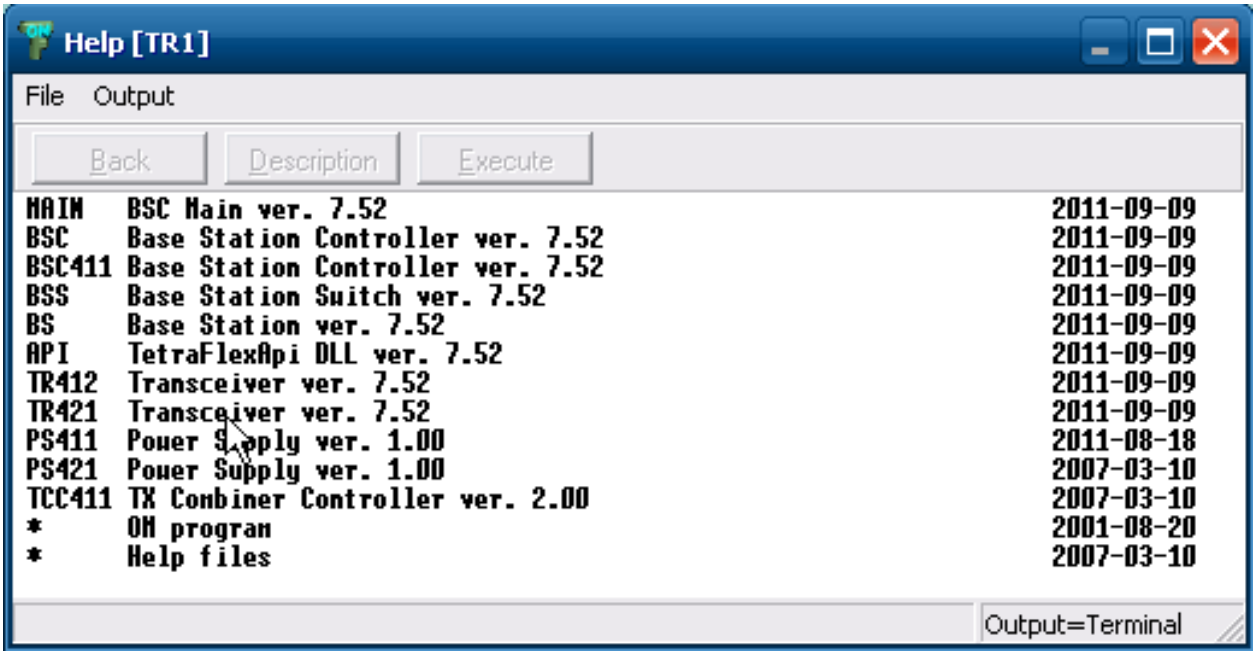


Figure 2-44: OM Help

After selecting a device a list of all available commands is shown:

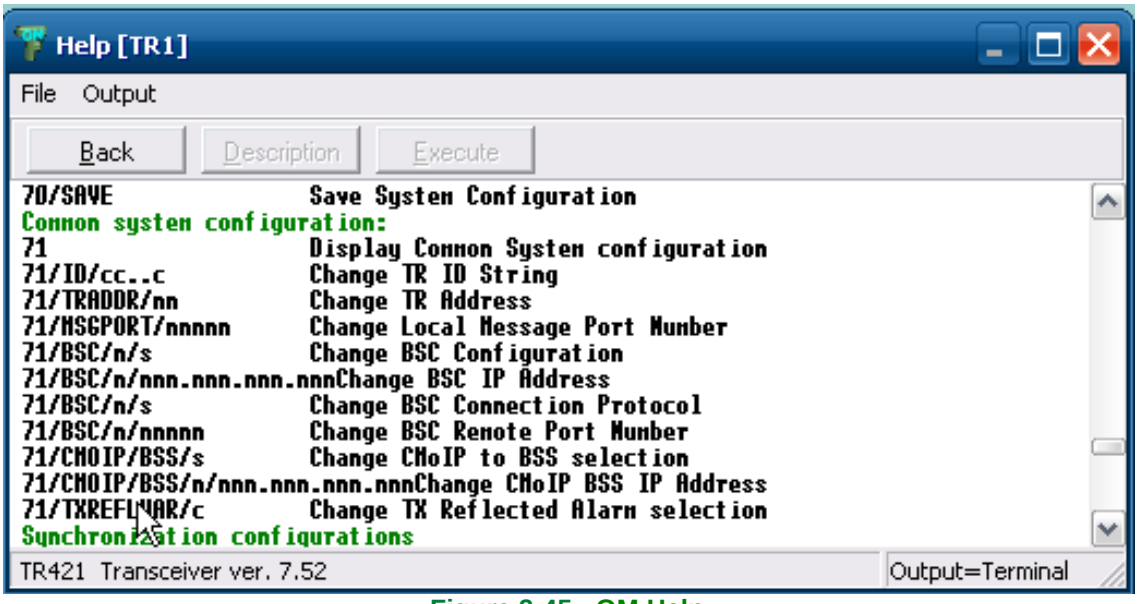


Figure 2-45: OM Help

After selecting a specific command, an execution window appears.
In this window the command syntax is explained and applicable command parameter(s) may be entered.
Please observe that all of the yellow fields must be filled out

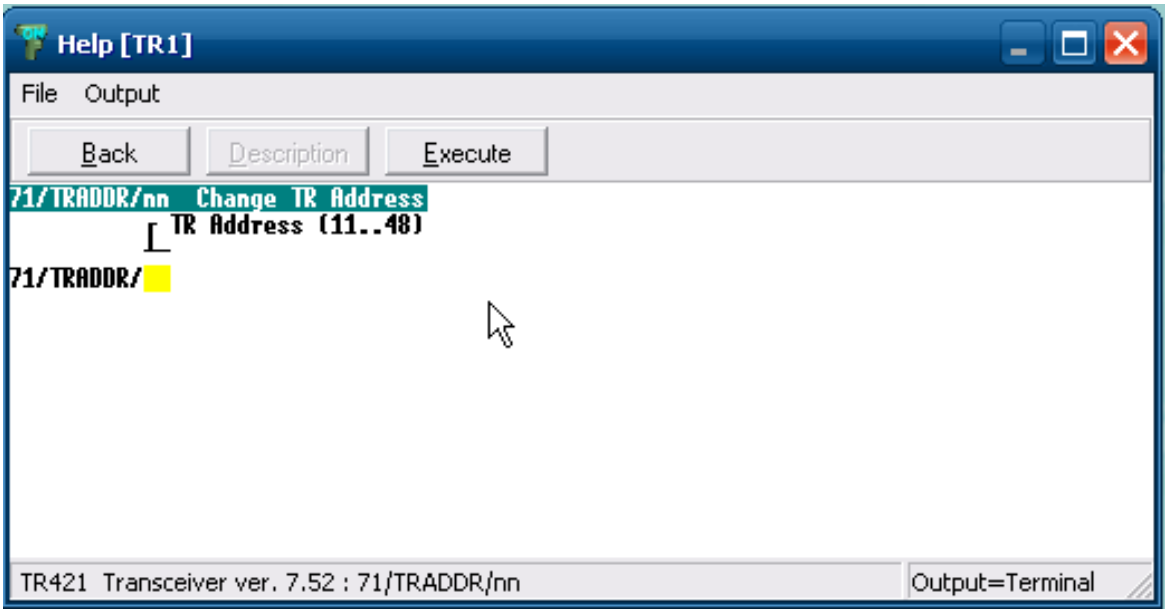


Figure 2-46: OM syntax

When the yellow spaces are filled out and the Execute button is selected (or the enter key is pressed), the command is send to the unit.
The TetraOM will return to the terminal window, and the command response is shown.
Don't forget to save (70/SAVE or F70/SAVE for the BSC)

2.14.3.6 TetraOM Editor

The TetraOM program also contains an Editor, where command files may be edited. When the editor is active, commands from the help system are put into the Editor instead. Command files can be sent from the Editor. Command files can also be executed directly from the disk.

Note that the system configuration files (Cnfgxxx.txt) on the BSC is ASCII files in a TetraOM compatible format, which can be edited directly in the TetraOM Editor. However they are normally created and updated automatically from the system.

2.14.3.7 TetraOM logging

Air Trace Logging

The TR has a built in functionality to collect all messages sent over the air interface using the TetraOM command 48. It is possible to setup logging to a file or log real-time to an air trace application.

2.14.3.7.1 Logging to File

- 48/FILE/"destination" – e.g. \CF-Card\tetra\work\trace1.lan, this saves the file on the TR, if you want to save the log file on the BSC or a PC on the network you must use the Host name and a shared folder on the BSC or PC (CE doesn't support num. IP address so you have to use the host name):

  e.g. 48/FILE/\\<host name>\<sharename>\<filename.lan>

  This will only work if the TR is allowed to logon to the host, it might be necessary to go to the TR with VNC and type the user name, password and domain of the host BSC or PC to get access.

- 48/"timeslot"/U — "timeslot" is the timeslot number. Collects unencrypted messages. To collect from several timeslots, repeat the command with different timeslot numbers
- 48/FILE/+ — Start collecting to file
- R/48 — could be used to verify trace session
- 48/FILE/- — Stop collecting to file

2.14.3.7.1.1 UDP transfer

48/UDP/"destination IP address"/"port number to be used"

- 48/"timeslot"/U — Collect unencrypted messages. It's possible to collect from several timeslots. 48+ could be used to collect from all timeslots
- 48/UDP/+ — Start trace session. R/48 could be used to verify trace session
- 48/UDP/- — Stop trace session
- 48-

2.14.3.7.1.2 Message logging from the test queue

- 65/N — Display only the message ID
- 65/N+ — Display content of the message

2.14.3.7.1.3 Creation of OM log files

- Select the TetraOM main form and chose logging.
- Browse to enter destination and filename.
- Click only terminal responses to collect the message responses exchanged between the TR, PS, Combiner and BSC.
- Type the TetraOM command to be logged: R/ or C/" TetraOM command".
- Enter the bottom 'Create' to start logging to file
- Enter the bottom 'Stop logging' to stop TetraOM logging to file.

2.14.3.8 Useful TetraOM Commands

Note: Nothing entered, does not mean that a command is not valid.
Only main commands are listed, subcommands may be present

BSS (Base Station Switch).

S00	SW Version
S00/C	Compiler options
S04	License dongle setting
S10	Nodes
S12	Radio Cell
S12/TS	Radio cell Timeslots Status
S13	Voice GW status
S14	Packet Data Status
S15	Application GW status
S20	Subscriber registers
S20/SAVE	Save actual register to text file
S20/READ	Load data from text file
S21	Subscriber profile
S21/nnnn	Show profile nnnn
S22	SSI Register Status
S65	Multicast / Unicast addresses
S71	General Node configuration

BSC (Base Station Controller):

F00	Version number
F15	TR status (Century Seconds)
F15/F	TR status (Frequency)
F98	Hardware ID information

BS421 (Transciever) :

00	SW Versions
02	TR operating mode
03/A	Alarm Flags*
05	BSC status
06	Network setting
10	TX key state
11	TX output
13	Power setting
21	RSSI level
31	OCXO sync
34	Display all CMoIP connections

63	Internal GPS status
63/VER	GPS module version
71	Common system configuration
71/TXREFLWR/c	SWR alarm setting
98	Hardware ID
99/RESTART	Restart BS421 (Soft restart)

***) Alarm BS 421 (OM command 03/A)**	**Comment**
00: TX PLL unlocked	Blocking Alarm (Hardware fault)
01: TX loop unstable	Blocking Alarm (Hardware fault)
03: TX temperature high	Blocking Alarm (TR421 temperature over 80˚C TX stopped)
06: TX output power	Blocking Alarm (Check TX out power)
07: TX ant. reflected L2	Blocking Alarm (can be changed to non blocking with command 71/TXREFLWAR/+)
08: TX ant. reflected L1	Non Blocking Alarm
10: RX PLL unlocked	Blocking Alarm (Hardware fault)
11: RX LO1 injection low	Non Blocking Alarm (Hardware fault)
16: 36.864MHz PLL unlocked	Blocking Alarm (Hardware fault)
18: L3 Frequency Setup	Non Blocking Alarm
19: DSP watchdog	Blocking Alarm
20: DSP Time Sync	Non Blocking Alarm
21: BSC Message Link	Blocking Alarm (No Link to BSC)
22: BSC1 Message Link	Non Blocking Alarm (No Link to BSC1)
23: BSC2 Message Link	Non Blocking Alarm (No Link to BSC2)
24: Time Sync	Non Blocking Alarm
25: Internal GPS RX	Non Blocking Alarm
26: External 1 Sync input	Non Blocking Alarm
27: External 2 Sync input	Non Blocking Alarm
28: Sync Phase Detector	Non Blocking Alarm
29: Century Second error	Non Blocking Alarm

TR412 (Transciever):

00	SW Versions
02	TR operating mode
03/A	Alarm Flags*
05	Display Config/ Status from BSC (BS)
10	TX key state
11	TX output
13	Power setting
21	RSSI level
31	OCXO sync
34	CMoIP downlink status
R/34	CMoIP downlink status Dynamic
98	Hardware ID

***) Alarm TR 412 (OM command 03/A)**	**Comment**
00: TX PLL unlocked	Blocking Alarm (Hardware fault)
01: TX VSWR protection	Blocking Alarm (Hardware fault)
03: TX temperature high	Blocking Alarm (TR412 temperature over 80˚C TX stopped)
04: TX volt. reference	
05: TX +26V supply	
06: TX output power	Blocking Alarm (Check TX out power)
07: TX ant. reflected L2	Blocking Alarm
08: TX ant. reflected L1	Non Blocking Alarm
09: TX combiner TP high	
10: RX PLL unlocked	Blocking Alarm (Hardware fault)
11: RX LO1 injection low	Non Blocking Alarm (Hardware fault)
12: RX LO2 injection low	
13: RX TMA/RMA L2	
14: RX TMA/RMA L1	

15: 12.8MHz PLL (2.048MHz)	
16: 36.864MHz PLL (8kHz)	Blocking Alarm (Hardware fault)
17: 1sec. missing	
18: L3 Frequency Setup	Non Blocking Alarm
19: DSP watchdog	Blocking Alarm
20: DSP Time Sync	Non Blocking Alarm
21: BSC Message Link	Blocking Alarm (No Link to BSC)
22: BSC1 Message Link	Non Blocking Alarm (No Link to BSC1)
23: BSC2 Message Link	Non Blocking Alarm (No Link to BSC2)

2.15 TR REMOTE DESKTOP COMMUNICATION (VNC)

2.15.1 VNC setup

An alternative way to communicate with the Base Station is to use the VNC program.

The TR is as a standard provided with a VNC Server to allow one user at a time to establish a remote desktop session with the TR.
To establish a remote session, start VNC on the Windows computer. (If it does not connect please check the VNC connection options “Format and encoding” change to “Raw”) You will get the following window:

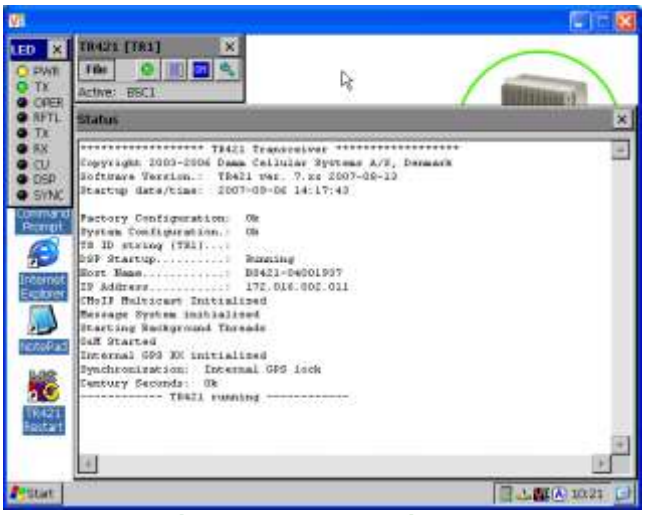


Figure 2-47: VNC picture

By pressing the LED, the LED window will close and give access to the “MY device” icon (or just move the active windows until my device icon is shown)

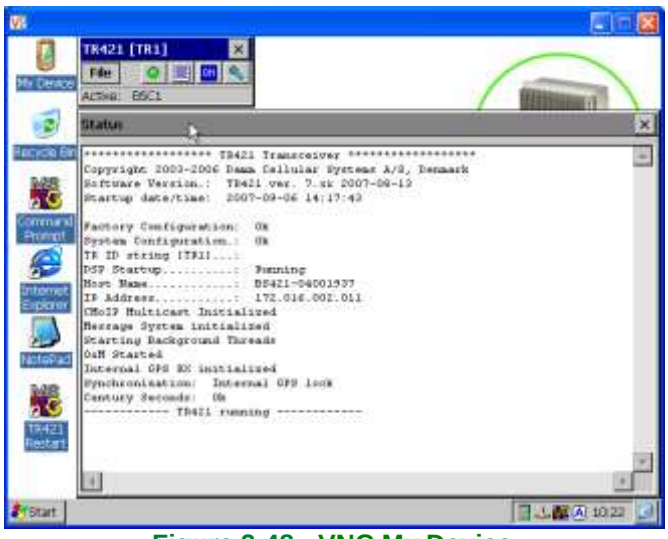


Figure 2-48: VNC My Device

Selecting “My Device” will open the device window

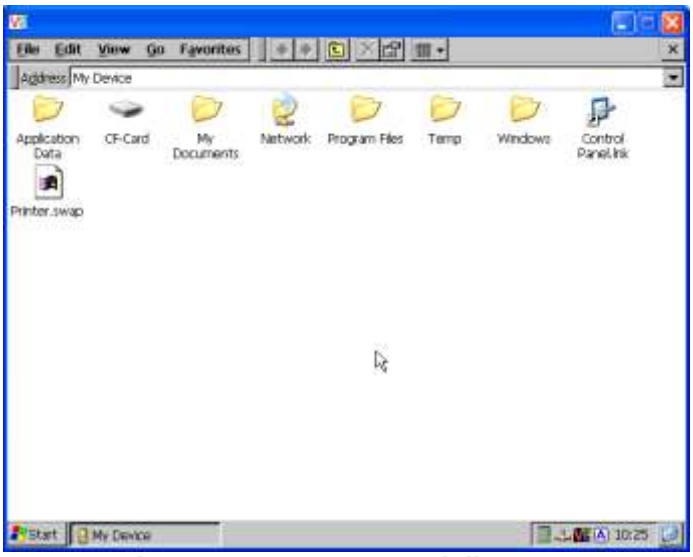


Figure 2-49: VNC CF card directory

The files on the TR are now accessible; for an instance the CF-Card directory contains all SW for the TR

You can now operate the Windows CE on the TR remotely from your computer.

2.15.2 File transfer via to/from TR

To copy, upgrade or backup files or software from the BS421 CF-card, select Start -> Search –> for files or folders
Select Computers and enter the IP address of the unit to be found.

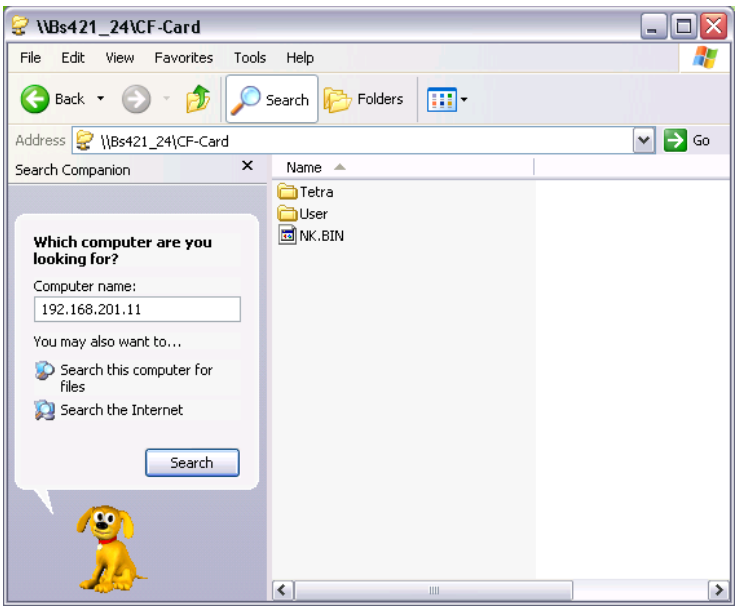


Figure 2-50: File Transfer

Now it is possible copy files to / from the CF-Card

2.15.3 Changing General setup and Sync

Pressing the tool icon will show a toolbox where it is possible to setup general parameters

- TR number
- TR ID string
- TX output
- RX-B input (6dB diversity preamble)
- BSC connection IP's
- Synchronization

For Sync and SyncOout, set the values to the opposite IP i.e. on TR1 set to TR2 IP and vice versa.

An option to restart the TR with the default values is present as well

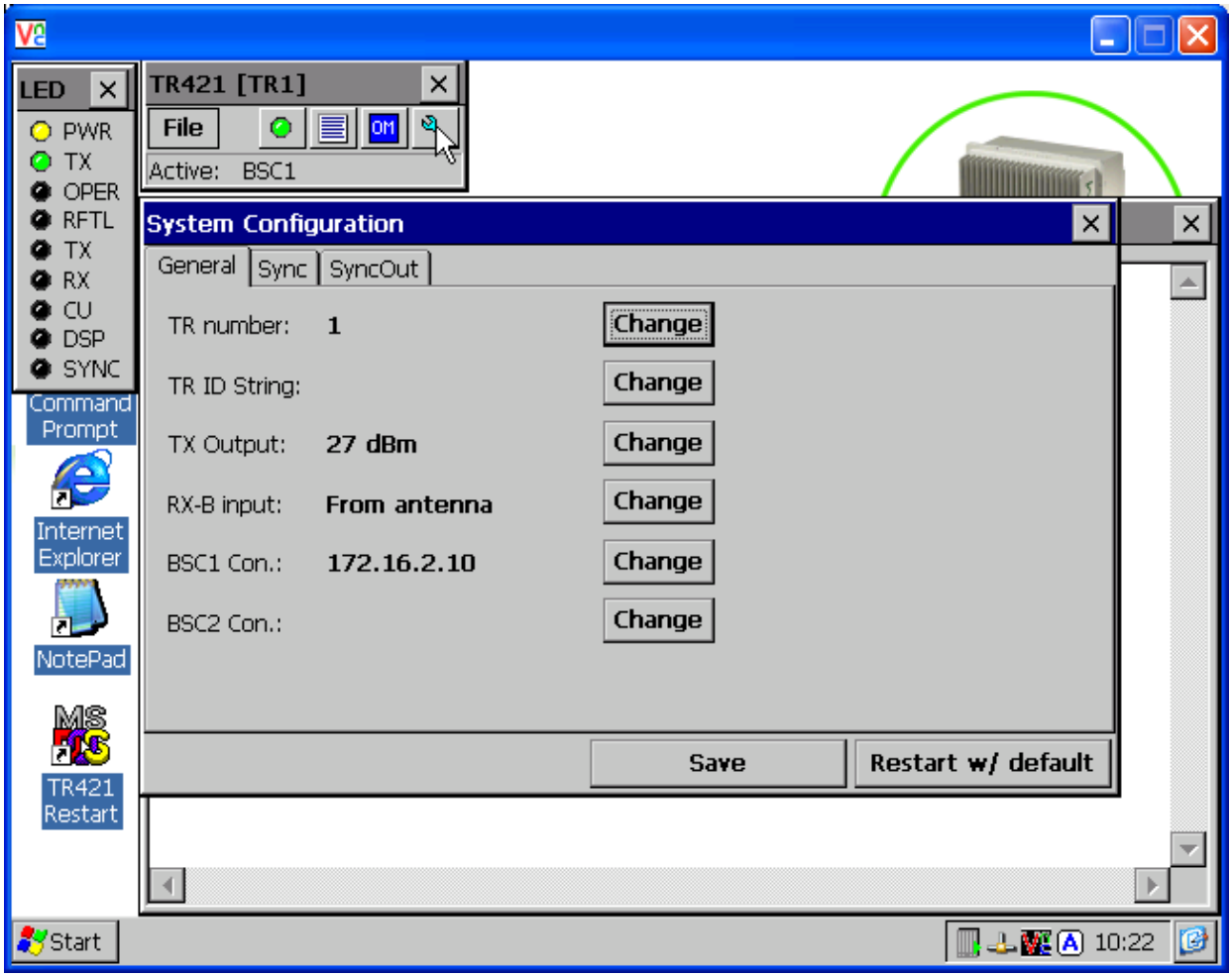


Figure 2-51: TR setup and sync

2.16 IP BACKBONE NETWORK LAYOUT AND CONFIGURATION

2.16.1 Multi node router considerations

From release 7.40 it is deemed mandatory to implement routers for realizing the interconnection. In fact it is not in relation to changes introduced in 7.40 that the routers have been mandatory. In fact the nature of multicast – when connected over switched networks (layer 2) can make problems with broadcast like behavior of the traffic. Meaning that a network which is shared with other users may be flooded with traffic from TetraFlex nodes

While saying that routers are mandatory – it is also a fact, that the rendezvous point (RP) router is mandatory. It may lead to the misconception that RP is single point of failure. In the basic configuration of the router network this might be correct – as the RP is sitting as hub for all other routers, i.e. all traffic passes here. However – there are router techniques available – making it possible to introduce load sharing and redundancy setup for RP's. Recommendations for this are under preparation. Cisco acronyms for this are MSDP (multicast source discovery protocol) and Anycast RP.

2.16.2 Network layout principle

As opposed to the virtual network between the TetraFlex® sites – which in its nature is a mesh network, the routers connecting the sites are connected in a star type network. The connections through the internet, which the routers use as their backbone, are all radiating like spokes in a wheel from one router that is announced as the rendezvous point.
The routers then facilitate mesh type communication around the network, through routing tables built inside the network.

In reality the multisite Tetra network from Damm Cellular Systems A/S is two or more release 7 TetraFlex® nodes – working together through an IP network. All parties are equal and no node is single point of failure.

The subscriber relevant information is contained in two registers. Inside the network, these registers are distributed and present on all nodes at all times. The distribution of the registers is done through multicast routing in the connecting router network. With respect to the registers and housekeeping of the same – a node is pointed out to contain the master mode register. This node keeps track of register checksums on all nodes in the network. In case of checksum mismatch on one or more nodes, the master register will initiate a download and overwrite of the relevant register(s).

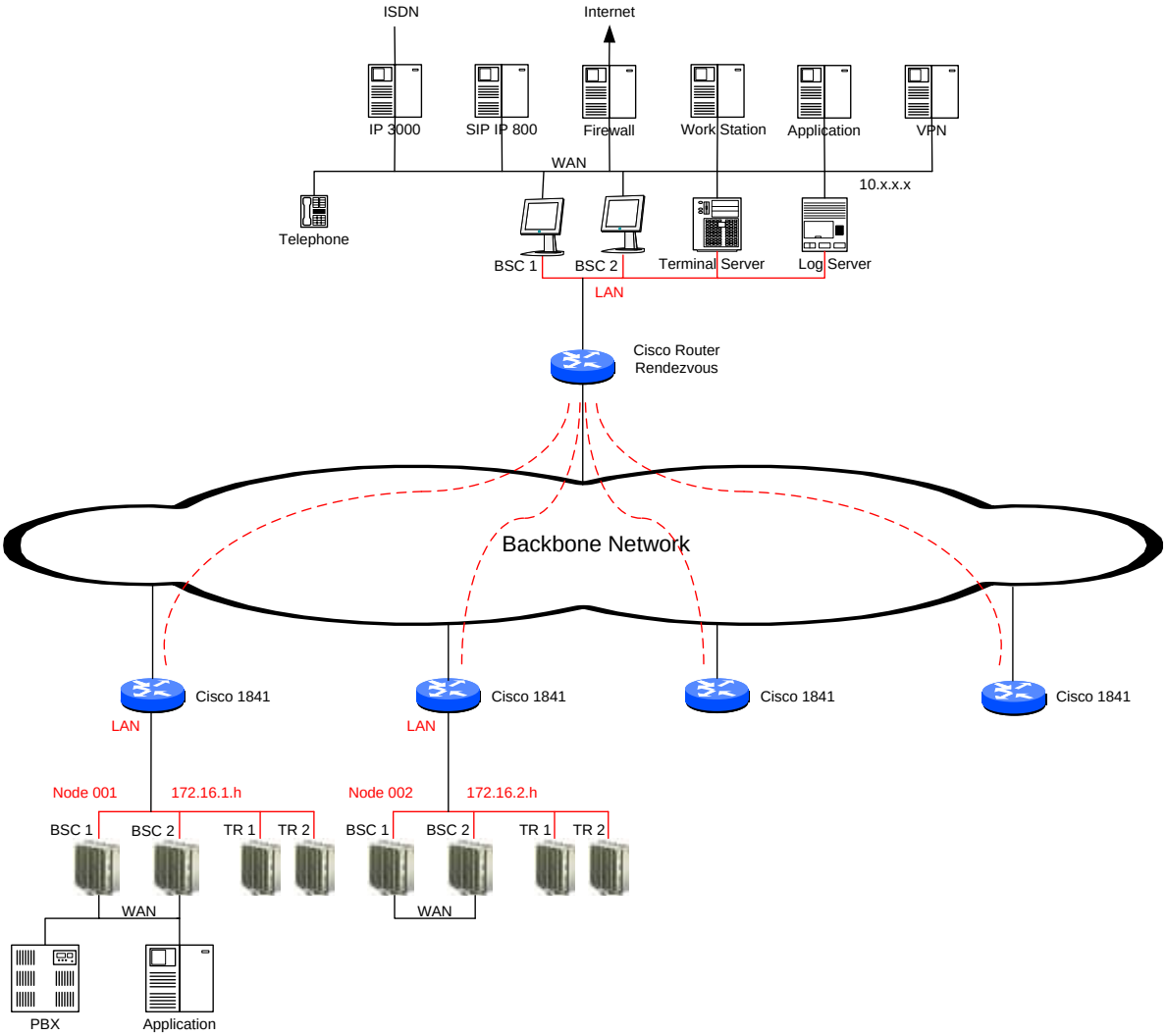


Figure 2-52: Backbone network principle

2.16.3 Backbone network physical connection

2.16.3.1 Outdoor/SB421

Installation of connection to router backbone for multinode TetraFlex is done via terminal points LAN_IN and LAN_OUT on the LAN+WAN connector of the below shown module. Connection is made from pins 8/7 and 6/5 using cat5 or cat6 networking cable and to the designated port on the router.
Please refer to section 1.1.4.5.8 for the full pin out of the cabling.

2.16.3.2 Indoor/BS41x

Internally in the BS41x rack the cabling for the LAN (and WAN) is connected to the connection box at the rack top.
For making connection from BSC LAN port – connect a cat5 or cat6 cable from the corresponding connector BSC1 or BSC2 LAN on the connector box to the designated LAN port on the router.

2.16.3.3 Redundant BSC – SB421 or BS41x

In case the node has redundant BSC – the router will need to have optional module installed. A 4-port switch module (HWIC-4ESW) is available from Cisco.

2.16.4 IP addressing schemes

IP addressing recommendation is based upon a 172.16.x.x address. Inside a given node – the 4th octet of the address is assigned as the host address: .10 and .19 for BSC1 and 2. .11, .12, .13 and .14 for the BS421's. The 3rd octet is reflecting the node number.
For IP interconnection via routers, the subnet mask is set to 255.255.255.0 or /24.
For IP interconnection via switched network, the subnet mask is set to 255.255.0.0 or /16.
If changing these masks – remember to change also in the DHCP server on outdoor type TetraFlex®.

All communication between the nodes in the multisite network is based purely upon IP. The network must provide both unicast routing and multicast routing. Group calls and register replication uses multicast communication and full duplex calls between two mobiles or to external PSTN via SIP also uses multicast although in nature being point to point
In TetraOM connection to the BSC – use the command S71 to display the relevant settings in regards to multicast networking.

224.239.016.000/28 is the default multicast address segment in use by the system for register replication and for signaling of call activity between BSCs in the TetraFlex® network. The address can be changed to meet special requirements. 224.238.016.000/28 results in a address of 224.239.16.1 for exchange of control packets between BSCs and for call signaling. Further an address of 224.239.16.3 is created – which is used for multicast traffic relating to discreet listening. 224.239.16.4 is the multicast address used for replicating the subscriber register

224.239.017.001 is the default multicast address in use for log server signaling. The address can be changed to meet special requirements, amongst others allowing for more than one log server.

225.000.000.000 is the so called CMoIP base address. CMoIP is the actual communication data stream. The address can be changed to meet special requirements. It is possible to change the two first octets of the address – whereas the two last octets are assigned automatically by the system. This base address describes in the given example an address range of 225.000.000.000 to 225.000.254.255.

The CMoIP address is assigned to calls in the TetraFlex system and signaled to all other BSCs through the signaling group 224.239.16.1. The assignment of CMoIP address is done by the originating BSC and is done as incremental and round robin – meaning start at 225.0.0.0, next call 225.0.0.1, and next 225.0.0.2 until 225.0.254.255. Then system restarts numbering from 225.0.0.0.

When a BSC starts up – it automatically involves the IGMP (Internet Group Management Protocol) and send off an "IGMP join" message to the network on the LAN. This "join" is sent

for both the signaling group and the log server group. The joining of the two groups will be active for as long as the BSC is active.

When a call is initiated, it is signaled to all other BSC on multicast group .1. All other active BSC will receive this message. The signaling makes it possible for all the BSC's to decide whether a given call is relevant to any terminal under its control. At same time – the originating BSC will assign a CMoIP address to the actual call and send an IGMP join message to the network to create the group in the routers. The address of this given group is contained in the signaling.

Any BSC that has interest in receiving the packets from the CMoIP group will make an IGMP join on the CMoIP address. After the call activity is terminated – the given CMoIP group will be taken down by IGMP disjoin messages.

The above mechanism is used both for group calls, full duplex calls, semi duplex calls and voice gateway calls.

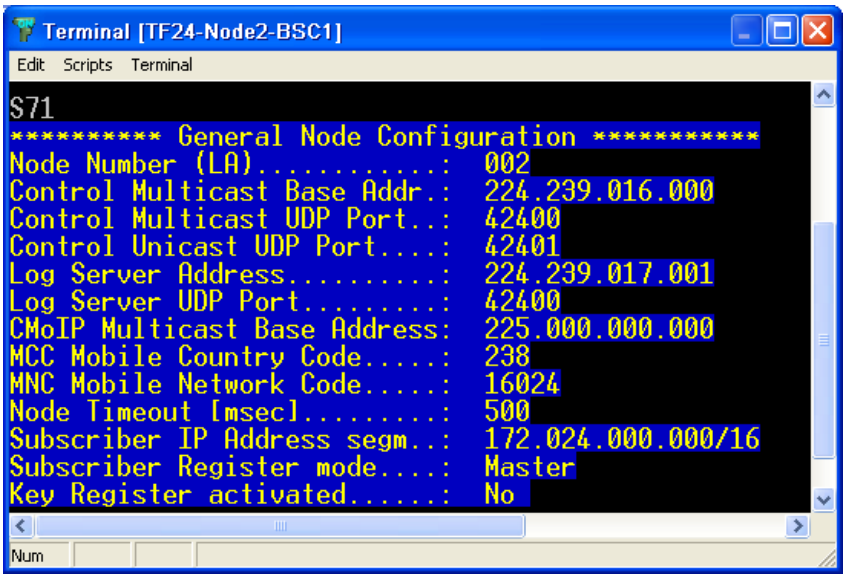


Figure 2-53: BSC multicast settings

If you need to alter any of these settings – use the following commands:

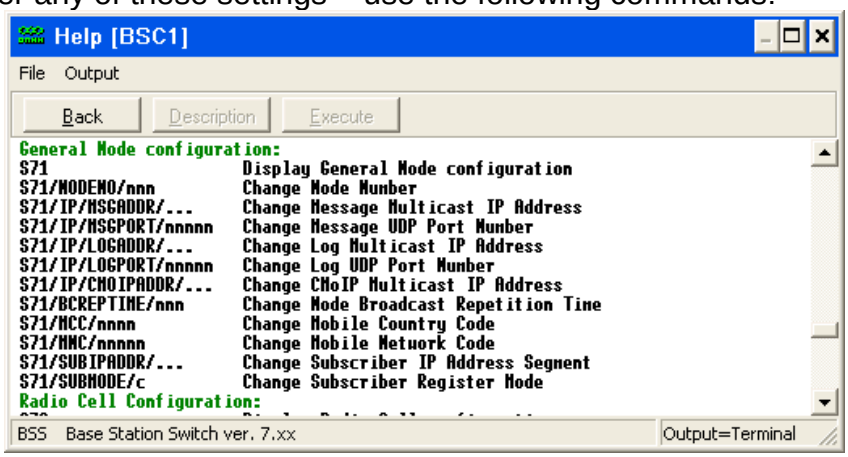


Figure 2-54: Applicable OM commands

Don't forget that in TetraOM, pressing "F1" will open the help files.

Instead of the default gateway entry on the LAN port settings in WinXP/WES2009, it is necessary for the routing of unicast and multicast packets – that the SB421 is told otherwise how to deliver the packets relevant for other parts of the network – to the router.

This is done by using the command tool – or DOS prompt if you wish – to enter a persistent routing to the LAN interface. Use the "Start" → "Run" in the start menu and type "cmd". This will open the command prompt window.

"route print" will give an output of all the routing information currently contained in the IP stack.

"route add" with "subnet" mask "subnet mask" "router interface address" –p will establish a permanent routing information into the stack of the XP. Look at example below for better understanding.

Example:
Route add 172.16.0.0 mask 255.255.0.0 172.16.1.1 –p adds a persistent route to the 172.16.0.0/16 network with default router 172.16.1.1
See also below figure.

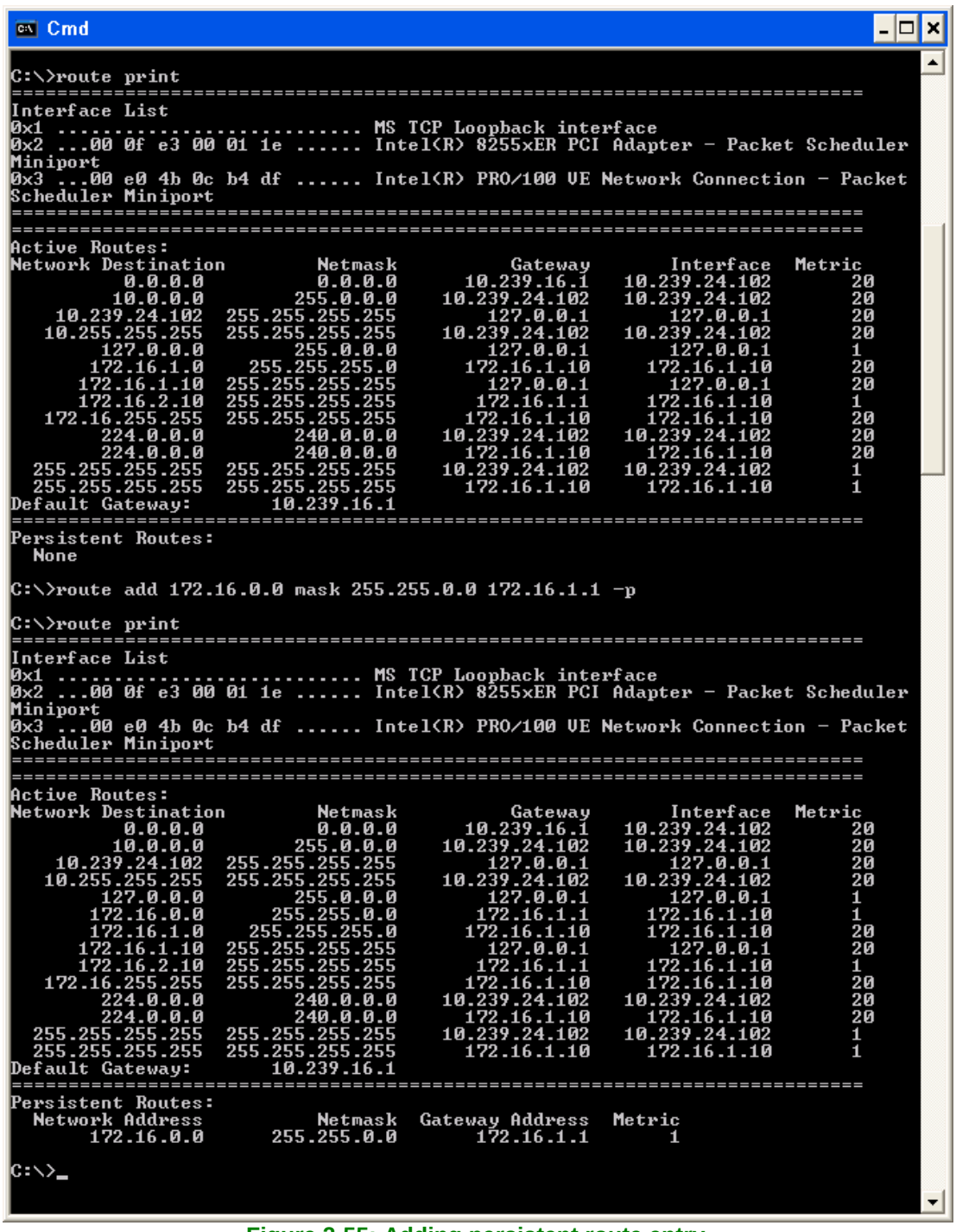


Figure 2-55: Adding persistent route entry

NOTE: Adding persistent route is not applicable when using switched network, i.e. without routers involved.

2.16.5 Considerations about network bandwidth

When designing a backbone network for the TetraFlex® multinode system it is applicable to take into account also the traffic load i.e. the bandwidth consumption originating from the various services available through the TetraFlex® system.

Activity in the TetraFlex® nodes may induce traffic load on the connecting IP backbone network. This load varies, depending on the type of activity.

2.16.5.1 Group call:

The communication scheme in use for group calls is point to multipoint. As the call type by nature is one too many – this is comparable to point to multipoint. The BSC with PTT'ing terminal will generate a stream of data packets.
All nodes with members of the same group as the PTT radio will receive the data stream and present it on their air interface. The CMoIP stream will be at approximately 12 Kbit/s on the LAN port of the SB421. After having passed the router the resulting bandwidth will be 22 Kbit/s. The difference is relating to the fact that IPSec and GRE both will add protocol overhead to the stream.
At the rendezvous point – the data stream will be replicated as applicable – resulting in one or more data streams leaving the rendezvous router (RP). Amount of outgoing streams from RP is decided through the IGMP mechanism.
To summarize: at the RP router – there will be one incoming voice stream with bandwidth 22 Kbit/s per active group call (from the PTT BSC). The amount of outgoing bandwidth is decided through IGMP and is 22 Kbit/s per receiving BSC. The incoming/outgoing pattern will change according to which node has the PTT activity

2.16.5.2 Full duplex:

Full duplex call is point to point. In TetraFlex® it is still transported as multicast. The full duplex call will generate a bidirectional voice packet stream. So at each BSC relating to the call there will be 12 Kbit/s outgoing and ingoing. Thus a full duplex call will load the RP with 2*22 Kbit/s in both ingoing and outgoing direction.

2.16.5.3 Half duplex:

Half duplex call is point to point. In TetraFlex® it is still transported as multicast. Half duplex call will generate a voice packet stream where the direction of packets is decided by the PTT BSC. So a half duplex call will load the RP with 22 Kbit/s ingoing and outgoing.

2.16.5.4 Replication:

The replication of subscribers is done via the signaling group and the replication group. All active BSCs are listening to the signaling group. When a master register decides to replicate because of checksum errors or a forced download of subscriber details is initiated through TetraOM, it results in a data stream from the BSC with the master register to the RP and outgoing stream from the RP as many as there are BSC's with faulty slave registers. The replication is done at a rate of 130 Kbit/s on the LAN – resulting in 158 Kbit/s on the "outside" port of router. So in a scenario with 10 nodes (1 master register and 9 slaves) this will result in RP load of 1*158 Kbit/s incoming and 1*158 Kbit/s outgoing if 1 slave register is faulty. If 2 slave registers are faulty the resulting load on RP is 1 ingoing and 2 outgoing streams.

2.16.5.5 Control packets:

There will, at all times when the network is activated, be a background load on the router network. The load origins from the control messages exchanged between the BSCs. The control packets will load the router network with 0.3 Kbit/s per active BSC.

2.16.5.6 Log server:

The load on the RP relating to a log server being present in the network depends on different factors. The log server must have connection to the multicast network. Any traffic, relevant to the log server, will be signaled to log server at the log server's multicast address. Log server will – in case it is configured to log a given activity – join the given CMoIP group. Joining the given CMoIP will make the data available for the log server. From this – it is log server configuration and network configuration dependant how the traffic to the log server loads the routers and especially the RP. As it is the same CMoIP stream that is joined – the bandwidth per logged activity is still 22 Kbit/s.

2.16.6 The IP interconnection scheme of TetraFlex® per site

All communication between the components of the TetraFlex® is based on IP. In relation to the outdoor type TetraFlex, the SB421 service box with its Windows XP operating system contains a DHCP server. IP address of the SB is x.x.x.10 and the 1st BS421 has IP address x.x.x.11, the 2nd BS421 has x.x.x.12, the 3rd has x.x.x.13 and the 4th has x.x.x.14. In case a redundant SB is in use, it must be numbered x.x.x.19.
The SB421 has the LAN address x.x.x.10 or x.x.x.19. The same must be the case for the BSC configuration on the given SB421.
In relation to indoor type TetraFlex® – the BSC412 must be configured LAN port x.x.x.10, respectively .19 for redundant BSC.
Above address assignments are guidelines. But to ensure efficient support in case of trouble – it is recommended to keep this structure.

Node No	BSC LAN	2nd BSC LAN	1st BS421	2nd BS421	3rd BS421	4th BS421
1	172.16.1.10	172.16.1.19	172.16.1.11			
2	172.16.2.10	172.16.2.19	172.16.2.11	172.16.2.12	172.16.2.13	172.16.2.14
3	172.16.3.10	172.16.3.19	N/A	N/A	N/A	N/A

Figure 2-56: Addressing examples

Above is shown a small example on addressing according to recommendation. Node 1 is a single carrier outdoor. Node 2 is a 4 carrier outdoor. Node 3 is an indoor. All three nodes have redundant BSC.
It can be observed that 3rd octet of IP address is equal to the node number.
Use the TetraOM to connect to the BSC locally. Issue command "F71" to check the local settings for the IP connections. The command will list the LAN and WAN IP addresses which are set in the BSC. Make sure these addresses correspond with the actual settings on the LAN and WAN cards in WinXP. Also this is where you set the IP address of the first TR on the system.

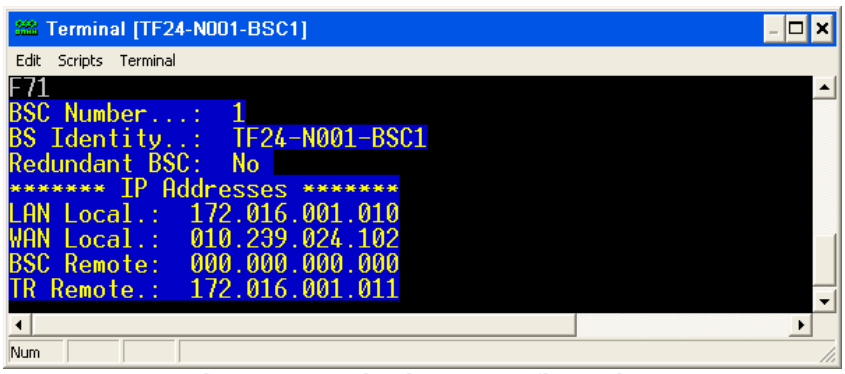


Figure 2-57: Viewing IP configuration

In case you need to alter these settings, use the below selection of commands:

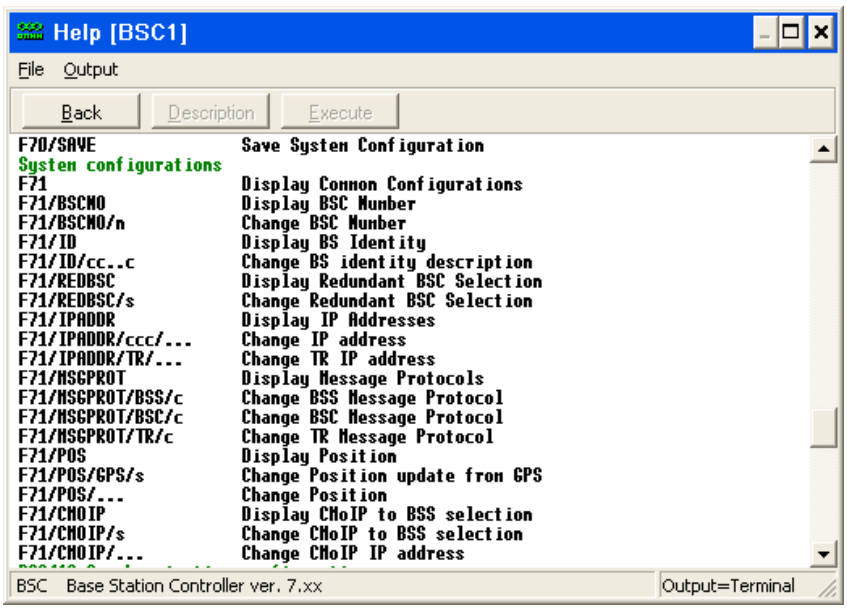


Figure 2-58: Applicable OM commands

Always remember that in TetraOM, pressing “F1” will open the help files.
The LAN port in the SB421 must have settings corresponding to the below example. Do not enter any default gateway settings on this port.

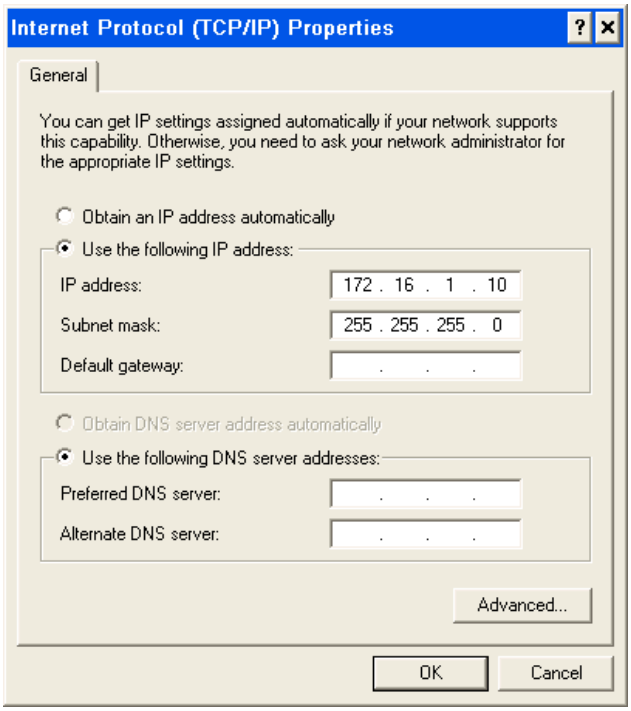


Figure 2-59: IP configuration of LAN interface card

2.16.7 Recommendation

It is strongly recommended that installers of the router network are familiar with IP networking, router technology and especially Cisco products.
If such familiarity does not exist, it is strongly recommended to seek advice with a knowledge Cisco installer.

2.16.8 Recommended router hardware

The router hardware recommended from Damm Cellular Systems A/S is a Cisco 1841 modular router.
This router type has been tested and verified with the TetraFlex® multisite system.
According to Cisco specifications – the 1841 router is capable of processing 75.000 pps (packets per second) – resulting in a theoretical maximum throughput of 38.4 Mbit/s.
If this capacity for some reason should not be sufficient – it may be considered to focus on the Cisco 2811 router. This offers 120.000 pps/61.44 Mbit/s capacity plus it offers support for 48V power supply.
Other router types and brands may be applicable. But in case the router type is not Cisco – Damm Cellular Systems A/S will not be able to offer any support.

2.16.9 Recommended router firmware

The recommended firmware for the Cisco 1841 router is

c1841-advsecurityk9-mz.124-15.T1.bin

This has been tested and verified with the TetraFlex® multisite system.
Any Cisco 1841 deployment with firmware revision lower than the specified – will not be supported.

2.16.10 Applicable router techniques

As described previously in this document the router network between the nodes must provide both unicast transport and multicast transport. Damm Cellular Systems A/S recommends the use of Cisco products and especially the 1841 modular router has been tested and found suitable for this purpose.
The following is a brief sketch of the techniques in use in the router network to form a routing that can cater for the needs of the TetraFlex multisite environment.

2.16.10.1 VPN

Using IPSec with 3DES encryption on all traffic between the routers maintains security and integrity of the voice and data transported between the nodes in the network.

2.16.10.2 Multicast networking

Multicast is a 1-to-many routing scheme. As opposed to unicast which is 1-to-1, the multicast allows a sender of information to address several receivers by sending one instance of the data. The multicast network replicates the sent data as applicable.

2.16.10.2.1 Routing multicast:

Protocol-Independent Multicast (PIM) is a family of multicast routing protocols that can provide one-to-many and many-to-many distribution of data over the Internet. The "protocol-independent" part refers to the fact that PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other traditional routing protocols such as Border Gateway Protocol (BGP) or in this specific case static routing entry. The way PIM is routing is known as RPF, reverse path forwarding. The routing path of multicast packets is based upon the routing path for unicast packets – but is turning it around by 180 degrees. In unicast – the routing table is built on destination i.e. where the packet needs to go. In multicast the routing is based on where the packet comes from. In popular, the PIM forwards packets on all interfaces belonging to a multicast group – except for the receiving interface.
A sub configuration of PIM is PIM Sparse Mode (PIM-SM).This version explicitly builds unidirectional shared trees rooted at a Rendezvous Point (RP) per group, and optionally creates shortest-path trees per source. PIM-SM generally scales fairly well for wide-area usage.

2.16.10.2.2 Group management in multicast:

The control of members of the multicast environment, i.e. the nodes around the network that need to send or receive multicast traffic is done by Internet Group Management Protocol (IGMP). IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections.
The TetraFlex release 7 supports version 3 of IGMP. Default setting in Cisco is version 2, but can be changed through configuration.